ÍNDICE GENERAL

1. CONCEPTOS PRELIMINARES

1.1. Antecedentes

1.2. Teoría de grupos

aquí irá toda la teoría de grupos que se tenga que desarrollar previo a comenzar propiamente la tésis.

1.3. Anillos, Módulos y Álgebras

aquí también se tiene que escribir las definiciones, teoremas de morfías y todo lo de semisimplicidad.

2. GRUPO-ANILLOS

2.1. Hechos Básicos De Los Grupo-Anillos

En este capítulo se darán las definiciones formales matemáticas que dan paso al estudio de los grupo-anillos y se relacionará la teoría de grupos y anillos con esta nueva estructura matemática.

Considérese la siguiente construcción: Sea G un grupo cualquiera y R un anillo cualquiera. Entonces se define $RG := \{\alpha | \alpha \colon G \to R, |sop(\alpha)| < \infty\}$ donde $sop(\alpha) := \{g \in G : \alpha(g) \neq 0\}$, a el conjunto $sop(\alpha)$ se le llama el soporte de α. Se puede observar entonces que los elementos de RG son funciones con soporte finito.

Como RG es un conjunto de funciones, se puede considerar la suma usual de funciones para definir la operación suma en RG, a saber $+ \colon RG \times RG \to R$ de tal forma que si $\alpha, \beta \in RG$ entonces $(\alpha+\beta)(g) := \alpha(g)+\beta(g)$ para todo g elemento de G . Similarmente se puede definir la operación producto en RG como $\cdot \colon RG \times RG \to R$ de tal forma que si $u \in G$ $(\alpha \cdot \beta)(u) := \sum_{gh=u} \alpha(g)\beta(h)$. Con estas nociones en mente se procede a definir a un grupo-anillo.

Definición 1. *El conjunto RG con las operaciones $+$ y $\cdot$ mencionadas anteriormente es llamado el* ***grupo-anillo de G sobre R****. En el caso en que R es conmutativo a RG se le llama también el* ***grupo-algebra de G sobre R***

Ahora se procede a mostrar dos teoremas que son básicos para el estudio de esta nueva estructura algebraica.

Teorema 1. *Existe una copia de G en RG, es decir, se puede encontrar $G_1 \subset RG$ tal que existe un homomorfismo entre G y G_1.*

Demostración. Considérese la función $i \colon G \to RG$ tal que $x \mapsto \alpha$ donde $\alpha(x) = 1$ y

$\alpha(g) = 0$ si $g \neq 0$. Con la identificación anterior es fácil notar que i es una función inyectiva. En efecto, si $x, y \in G$ entonces $i(x) = \alpha$, $i(y) = \beta$, pero $\alpha \neq \beta$ si $x \neq y$, por definición. Ahora se probará que i es un homomorfismo de grupos. Nótese que $i(xy) = \gamma$, donde $\gamma(xy) = 1$ y $\gamma(g) = 0$ si $g \neq xy$. Por otro lado, $i(x)i(y) = \alpha\beta$ donde $(\alpha\beta)(u) = \sum_{gh=u} \alpha(g)\beta(h)$, pero el producto $\alpha(g)\beta(h)$ se anula a menos que $g = x$ y $h = y$, en cuyo caso la función vale 1, con lo que se ha demostrado que $i(x)i(y) = i(xy)$. □

Generalmente a i se le llama la función de inclusión, así que será la forma en que se nombrará de aquí en adelante.

Teorema 2. *Existe una copia de R en RG.*

Demostración. Considérese la función $v\colon R \to RG$ tal que $v(r) = \beta$ con $\beta(g) = r$ si $g = 1_G$ y $\beta(g) = 0$ si $g \neq 1_G$. Es claro que v es inyectiva y la demostración es exactamente igual que en el teorema anterior. Ahora falta probar que v es un homomorfismo de anillos (con la aclaración que el hecho que RG es un anillo se probará mas adelante). En efecto, $v(sr) = \theta$ donde $\theta(g) = sr$ si $g = 1_G$ y $\theta(g) = 0$ si $g \neq 1_G$. De manera similar se tiene que $v(s)v(r) = \gamma\beta$ donde $(\gamma\beta)(u) = \sum_{gh=u} \gamma(g)\beta(h)$ pero γ y β se anulan a menos que $g = h = 1_G$ y en ese caso $u = 1_G$, por lo que se ha probado que v es un homomorfismo de anillos. □

Con las identificaciones anteriores en mente es fácil probar la siguiente propiedad.

Propiedad 1. *Si $g \in G$ y $r \in R$ entonces $rg = gr$ en RG.*

Demostración. Nótese que $r = \gamma$ y $x = \alpha$ y usando la definición del producto en RG se ve que $rx = \gamma\alpha$ donde $(\gamma\alpha)(u) = \sum_{gh=u} \gamma(g)\alpha(h)$ pero por definición γ y α se anulan en todas partes excepto en $g = 1_G$ y $h = x$ respectivamente, por lo tanto $(\gamma\alpha)(u) = r$ cuando $u = x$ y $(\gamma\alpha)(u) = 0$ para $u \neq x$

Por otro lado $xr = \alpha\gamma$ dada por $(\alpha\gamma)(u) = \sum_{gh=u} \alpha(g)\gamma(h)$ de nuevo la función sólo existe cuando $g = x$ y $h = 1_G$ de esa forma $(\alpha\gamma)(u) = r$ cuando $u = x$ y se anula en cualquier otro caso, con la cual concluye la demostración. □

La definición de grupo-anillo que se presentó anteriormente es bastante rigurosa y además es bien definida, ya que se ha construido un espacio vectorial de funciones en el cual todas las operaciones tienen sentido, lo cual le brinda el soporte necesario para trabajar en álgebra. En algunas ocasiones resulta un poco tedioso y complicado estar trabajando sobre un espacio vectorial de funciones, así que se replanteará los grupo-anillos como *R-combinaciones lineales*, es decir, a cada elemento de RG se le asigna una combinación lineal de elementos de G con coeficientes en R, de la siguiente manera

$$\alpha = \sum_{g \in G} a_g g \tag{2.1}$$

donde $a_g \in R$ y $a_g \neq 0$ si $g \in sop(\alpha)$

Nota 1. *Con la identificación anterior se verifica que la suma de $\alpha, \beta \in RG$ es componente a componente, es decir $\alpha + \beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g$ y el producto está dado por $\alpha\beta = \sum_{g,h\in G} a_g b_h gh$*

Ahora es práctico establecer los siguientes teoremas:

Teorema 3. *RG es un grupo aditivo*

Demostración. Se procede por incisos:

1. Sean $\alpha, \beta, \gamma \in RG$ entonces $\alpha+(\beta+\gamma) = \sum_{g\in G} a_g g + \left(\sum_{g\in G} b_g g + \sum_{g\in G} c_g g\right) = \sum_{g\in G} a_g g + \left(\sum_{g\in G}(b_g + c_g)g\right) = \sum_{g\in G}(a_g + b_g + c_g)g = \sum_{g\in G}((a_g + b_g) + c_g)g = \left(\sum_{g\in G}(a_g + b_g)g\right) + \sum_{g\in G} c_g g = (\alpha + \beta) + \gamma$

2. Existe $0 \in RG$ tal que $0 + \gamma = \gamma + 0 = \gamma$ para cualquier $\gamma \in RG$. A saber $0 = \sum_{g\in G} 0 \cdot g$. Con esta identificación en mente se procede a hacer los cálculos: $\alpha + 0 = \sum_{g\in G}(a_g + 0)g = \sum_{g\in G}(0 + a_g) = \sum_{g\in G} a_g g = \alpha$

3. Existe $-\alpha$ tal que $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ para cualquier $\alpha \in RG$. En efecto $-\alpha = \sum_{g\in G} -a_g g$ y por lo tanto $\alpha + (-\alpha) = \sum_{g\in G}(a_g + (-a_g))g = \sum_{g\in G}((-a_g) + a_g)g = \sum_{g\in G} 0 \cdot g = 0$

iv) $\alpha+\beta = \sum_{g\in G} a_g g+\sum_{g\in G} b_g g = \sum_{g\in G}(a_g+b_g)g = \sum_{g\in G}(b_g+a_g)g = \beta+\alpha$ $\square$

La clausura de la operación + se sigue directamente de la definición. Vale la pena notar que para realizar esta prueba se uso simplemente el hecho que G es grupo y R es un anillo y por lo tanto satisfacen propiedades algebraicas respecto de sus operaciones.

Nótese que se ha probado que $(RG, +)$ es un grupo abeliano, lo cual será de utilidad para el siguiente teorema:

Teorema 4. *RG es un anillo con las operaciones $+$ y $\cdot$*

Demostración. Ya se ha probado que $(RG, +)$ es un grupo abeliano, por lo que a continuación se probará, de nuevo por incisos, que $(RG, \cdot)$ es asociativo y distributivo tanto por la derecha como por la izquierda:

1. $\alpha(\beta\gamma) = \left(\sum_{g\in G} a_g g\right)\left[\left(\sum_{g\in G} b_g g\right)\left(\sum_{g\in G} c_g g\right)\right] = \left(\sum_{g\in G} a_g g\right)\left(\sum_{g,h\in G} b_g c_h gh\right) = \sum_{f,g,h\in G} a_f(b_g c_h)f(gh) = \sum_{f,g,h\in G}(a_f b_g)c_h(fg)h = (\alpha\beta)\gamma$

2. $\alpha(\beta+\gamma) = \left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g + \sum_{g\in G} c_g g\right) = \sum_{g\in G} a_g g\left(\sum_{g\in G}(b_g + c_g)\right) = \sum_{g,h\in G} a_g(b_h + c_h)gh = \sum_{g,h\in G} a_g b_h gh + \sum_{g,h\in G} a_g c_h gh = \alpha\beta + \alpha\gamma$

3. $(\alpha+\beta)\gamma = \left(\sum_{g\in G}(a_g + b_g)g\right)\left(\sum_{g\in G} c_g g\right) = \sum_{g,h\in G}(a_g+b_g)c_h gh = \sum_{g,h\in G} a_g c_h gh+$

$\sum_{g,h\in G} b_g c_h gh = \alpha\gamma + \beta\gamma$ □

Es de interés estudiar la estructura algebraica de RG, así que se introduce una operación mas sobre RG

Definición 2. *Sea $\lambda \in R$ entonces se define el producto por elementos del anillo como:*

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \lambda a_g g \tag{2.2}$$

Con esta definición podemos proclamar el siguiente teorema

Teorema 5. *RG es un R -módulo*

Demostración. Ya se estableció en el teorema 3 que $(RG, +)$ es un grupo aditivo. De la definición anterior se sigue que $\lambda\gamma \in RG$. Ahora se procede por incisos:

1. $(\lambda_1 + \lambda_2)\alpha = \sum_{g\in G}(\lambda_1 + \lambda_2)a_g g = \sum_{g\in G} \lambda_1 a_g g + \sum_{g\in G} \lambda_2 a_g g = \lambda_1\alpha + \lambda_2\alpha$

2. $\lambda(\alpha + \beta) = \lambda \sum_{a_g + b_g} g = \sum g \in G\lambda(a_g + b_g)g = \sum_{g\in G} \lambda a_g g + \sum_{g\in G} \lambda b_g g = \lambda\alpha + \lambda\beta$

3. $\lambda_1(\lambda_2\alpha) = \lambda_1 \sum_{g\in G} \lambda_2 a_g g = \sum_{g\in G}(\lambda_1(\lambda_2 a_g))g = \sum_{g\in G}((\lambda_1\lambda_2)a_g)g = \lambda_1\lambda_2\alpha$

4. $1_R\alpha = \sum g \in G 1_R a_g g = \sum_{g\in G} a_g g$

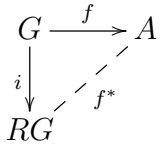
Y con esto concluye la prueba. □

Una extensión del resultado anteriormente presentado es que si R es un anillo conmutativo entonces RG es un álgebra sobre R. Se puede resaltar que si R es conmutativo entonces el rango de RG como módulo libre sobre R está bien definido,

de hecho si G es finito se tiene que $rango(RG) = |G|$

Ahora se establecerá un resultado de mucha importancia en los grupo-anillos, ya que relaciona a estos con los homomorfismos, que es uno de los objetivos del álgebra.

Proposición 1. *Sea G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subset A$ y cualquier función $f\colon G \to A$ tal que $f(gh) = f(g)f(h)$ para cualquier $g, h \in G$, existe un único homomorfismo de anillos $f^*\colon RG \to A$, que es R-lineal, tal que $f^* \circ i = f$, donde i es la función de inclusión. Lo anterior se reduce a decir que el siguiente diagrama es conmutativo:*



Demostración. Considérese la función $f^*\colon RG \to A$ tal que $f^*(g) = \sum_{g\in G} a_g f(g)$. Ahora solo falta hacer los cálculos correspondiente para mostrar que f^* es un homomorfismo de anillos. En efecto, $f^*(\alpha + \beta) = \sum_{g\in G}(a_g + b_g)f(g) = \sum_{g\in G} a_g f(g) + \sum_{g\in G} b_g f(g) = f^*(\alpha) + f^*(\beta)$.

Similarmente $f^*(\alpha\beta) = \sum_{g,h\in G} a_g b_h f(gh) = \sum_{g,h\in G} a_g b_h f(g)f(h) = f^*(\alpha)f^*(\beta)$. Ahora sea $r \in R$ entonces $f^*(r\alpha) = \sum_{g\in G} r a_g f(g) = r\sum_{g\in G} a_g f(g) = r f^*(\alpha)$ Sea $x \in G$ entonces $i(x) = \sum_{g\in G} a_g g$ donde $a_g = 1$ si $g = x$ y $a_g = 0$ en cualquier otro caso, por lo tanto $f^*(i(g)) = \sum_{g\in G} a_g f(g) = f(x)$. De los cálculos anteriores se sigue que $f^* \circ i = f$, con lo cual concluye la prueba. □

De la proposición anterior se deriva un corolario que no es mas que un caso especial de la misma, pero se establecerá por aparte porque será de utilidad en el desarrollo de este trabajo de graduación.

Corolario 1. *Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces, existe un único*

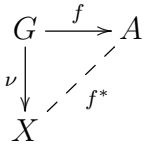
homomorfismo de anillos $f^*\colon RG \to RH$ *tal que* $f^*(g) = f(g)$ *para cualquier* $g \in G$. *Si* R *es conmutativo, entonces* f^* *es un homomorfismo de* $R-$ *álgebras, mas aún si* f *es un epimorfismo (monomorfismo), entonces* f^* *es también un epimorfismo (monomorfismso)*

Demostración. Usar el teorema anterior con $A = RH$ lo anterior se puede hacer porque RH es un anillo que contiene a R y hay una copia de H en RH, con lo cual se deriva que debe existir f^* homomorfismo $R-$ lineal de anillos tal que $f^*(g) = f(g)$ para cualquier elemento $g \in G$. Con lo cual concluye la prueba. □

De hecho la proposición 1 se puede utilizar como una definición de RG, como se sigue de la siguiente proposición:

Proposición 2. *Sea* G *un grupo y* R *un anillo. Sea* X *un anillo conteniendo* R *y* $\nu\colon G \to X$ *una función tal que* $\nu(gh) = \nu(g)\nu(h)$ *para todo* $g, h \in G$ *y tal que, para todo anillo* A *que contiene a* R *y cualquier función* $f\colon G \to A$ *que satisface* $f(gh) = f(g)f(h)$ *para todo* $g, h \in G$, *existe un único homomorfismo* R*-lineal* $f^*\colon X \to A$ *tal que el siguiente diagrama es conmutativo:*

Figura 1. **Definición alternativa para** RG



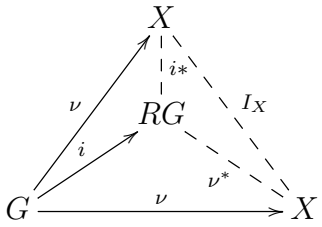
Fuente: elaboración propia con paquete **xymatrix** para computadora.

Entonces $X \simeq RG$

Demostración. La demostración es tan simple como notar que el diagrama de la figura 2 conmuta con I_X

□

Figura 2. **Diagrama Conmutativo**



Fuente: elaboración propia con paquete **xymatrix** para computadora.

Nota 2. *Si en el corolario 6 se hace* $H = \{1\}$ *y se considera la función* $m\colon G \to \{1\}$ *entonces esta función induce un homomorfismo de anillos* $\epsilon\colon RG \to R$ *tal que* $\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a(g)$.

Definición 3. *El homomorfismo* $\epsilon\colon RG \to R$ *dado por*

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

es llamado la ***función de aumento de RG*** *y su núcleo, denotado por* $\Delta(G)$*, es llamado el* ***el ideal de aumento*** *de* RG

Ahora se puede decir algunas propiedades importantes del ideal de aumento de RG. Nótese que si un elemento $\alpha = \sum_{g\in G} a_g g$ pertenece al ideal de aumento entonces $\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$ por lo tanto se puede escribir α de la siguiente forma:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1)$$

Por lo tanto es claro que cualquier elemento de la forma $g-1, g \in G$ pertenece a $\Delta(G)$, mas aún se acaba de probar que el conjunto $\{g-1 : g \in G, g \neq 1\}$ es un conjunto de generadores del ideal de aumento de RG. Por otro lado, de la definición de RG se sigue que el conjunto anterior en linealmente independiente, con lo cual se ha probado la siguiente proposición:

Proposición 3. *El conjunto* $\{g-1 : g \in G, g \neq 1\}$ *es base de* $\Delta(G)$ *sobre* R*. Es*

decir, se puede escribir

$$\Delta(G) = \left\{ \sum_{g \in G} a_g(g-1) : g \in G, g \neq 1, a_g \in R \right\}$$

donde, como es usual, se debe asumir que solo un número finito de los coeficientes a_g son distintos de cero.

Nótese que, en particular, si R es conmutativo y G es finito, entonces $\Delta(G)$ es un módulo libre sobre R con rango $|G| - 1$

Se concluye esta sección mostrando que el grupo-anillo RG donde R es conmutativo es un anillo con **involución**

Proposición 4. *Sea R un anillo conmutativo. La función $*\colon RG \to RG$ definida por*

$$\left(\sum_{g \in G} a(g)g \right)^* = \sum_{g \in G} a(g)g^{-1} \tag{2.3}$$

satisface:

1. $(\alpha + \beta)^* = \alpha^* + \beta^*$
2. $(\alpha\beta)^* = \beta^*\alpha^*$
3. $\alpha^* = \alpha$

Demostración. Se procede por incisos:

1. $\left(\sum_{g \in G}(a_g + b_g)g\right)^* = \sum_{g \in G}(a_g + b_g)g^{-1} = \alpha^* + \beta^*$
2. $\left(\sum_{g,h \in G}(a_g b_h)gh\right)^* = \sum_{g,h \in G} a_g b_h h^{-1}g^{-1} = \sum_{g,h \in G} b_h a_g h^{-1}g^{-1} = \beta^*\alpha^*$

3. $\left(\left(\sum_{g\in G} a_g g\right)^*\right)^* = \left(\sum_{g\in G} a_g g^{-1}\right)^* = \sum_{g\in G} a_g g$ □

2.2. Ideales de aumento

En lo que sigue es de mucho interés encontrar condiciones de R y G que permitan descomponer a RG como sumas directas de ciertos subanillos. Será de especial interés conocer cuando RG es un anillo semisimple para así poder escribirlo como sumas directas de ideales minimales.

Con este fin se hará un estudio de la relación que hay entre los subgrupos de G y los ideales de RG. Está relación tendrá mucho utilidad cuando se trate con problemas concernientes a la estructura y propiedades de RG. Estas relaciones aparecieron por primera vez en un artículo publicado por A. Jennings (dar cita) y, en la forma que se presentará en este trabajo, en el trabajo hecho por W. E. Deskins (dar cita). La idea de aplicarlo por primera vez en el estudio de la reducibilidad completa (como se hará en la siguiente sección) fue de I.G. Connell (dar cita).

Ya en materia de hecho, considérese el grupo G y el anillo R, se denotará con $\mathcal{S}(G)$ el conjunto de todos los subgrupos de G y con $\mathcal{I}(RG)$ el conjunto de los ideales por izquierda de RG.

Definición 4. *Para un subgrupo $H \in \mathcal{S}(G)$ se denota por $\Delta_R(G,H)$ el anillo por izquierda de RG generado por el conjunto $\{h-1 : h \in H\}$. Esto es,*

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} \alpha_h (h-1) : \alpha_h \in RG \right\} \tag{2.4}$$

Cuando se esté trabajando con un anillo fijo R se omitirá el subindíce y por lo tanto al ideal anterior se le denotará simplemente como $\Delta(G,H)$. Nótese que el ideal $\Delta(G,G)$ coincide con $\Delta(G)$, del cual se habló en la sección anterior.

Lema 1. *Sea H un subgrupo de un grupo G y sea S el conjunto de los generadores de H. Entonces, el conjunto $\{s-1 : s \in S\}$ es un conjunto de generadores de $\Delta(G,H)$ como ideal por izquierda de RG*

Demostración. Como S es un conjunto de generadores de H, cada elemento $1 \neq h \in H$ puede ser escrito en la forma $h = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdot s_r^{\epsilon_r}$ donde $s_i \in S$ y $\epsilon_i = \pm 1$, $1 \leq i \leq r$. Por lo tanto es suficiente probar que todo elemento de la forma $h-1$ con $h \in H$ pertenece al ideal generado por $\{s-1 : s \in S\}$. Para hacer esto se procede por inducción matemática sobre r.

Caso Base: Nótese que el menor caso sucede en $r = 2$. Por lo tanto sea $h \in H$ entonces $h - 1 = s_1^{\epsilon_1} s_2^{\epsilon_2} = s_1^{\epsilon_1}(s_2^{\epsilon_2} - 1) + (s_1^{\epsilon_1} - 1) \in (S)$ donde (S) es el ideal generado por $\{s-1 : s \in S\}$

Hipótesis de Inducción Supóngase que cualquier expresión de la forma $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} - 1) \in (S)$

Conclusión Considérese la expresión de la forma $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} s_{k+1}^{\epsilon_{k+1}} - 1)$, hágase la sustitución $x = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k}$ entonces $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} s_{k+1}^{\epsilon_{k+1}} - 1) = x s_{k+1}^{\epsilon_{k+1}} - 1 = x(s_{k+1}^{\epsilon_{k+1}} - 1) + (x-1) \in (S)$ ya que $x - 1, x(s_{k+1}^{\epsilon_{k+1}} - 1) \in (S)$ por la hipótesis de inducción. La prueba está casi completa, sola falta decir que si apareciera algún $\epsilon_i = -1$ se aplica la factorización $y^{-1} - 1 = y^{-1}(1-y)$ y el problema está resuelto. □

Para dar un mejor caracterización de $\Delta_R(G,H)$, denótese con $\mathcal{T} = \{q_i\}_{i \in I}$ un conjunto completo de representantes de clases izquierdas de H en G, un *transversal* de H en G. Se asumirá que siempre se elige como representante de la clase H en $\mathcal{T}$ a la unidad de G. De esa manera todo elemento $g \in G$ puede ser escrito de manera única en la forma $g = q_i h_j$ con $q_i \in \mathcal{T}$ y $h_j \in H$

Proposición 5. *El conjunto $B_H = \{q(h-1) : q \in \mathcal{T}, h \in H, h \neq 1\}$ es una base de*

$\Delta_R(G,H)$ *sobre* R.

Demostración. Se procede en dos partes, primero se debe probar que el conjunto dado es linealmente independiente y luego que también es un generador de $\Delta_R(G,H)$.

Independecia Lineal Supóngase que se tiene una combinación lineal de elementos de B_H que se anula, esto es $\sum_{i,j} r_{ij}q_i(h_j-1)=0$ con $r_{ij}\in R$. De lo anterior se sigue que $\sum_{i,j} r_{ij}q_i(h_j)-\sum_{i,j} r_{ij}q_i=0$ por lo tanto $\sum_{i,j} r_{ij}q_i(h_j)=\sum_{i,j} r_{ij}q_i$ lo cual se puede rescribir como $\sum_{i,j} r_{ij}q_ih_j=\sum_i\left(\sum_j r_{ij}q_i\right)$. En la igualdad anterior se puede observar que como $h_j\neq 1$ entonces necesariamente el lado izquierdo de la ecuación tienen distinto soporto que el lado derecho, por lo tanto ambos deben ser igual a cero, pero los elementos de G son linealmente independientes sobre R entonces $r_{ij}=0$ para todo i,j.

Generador Se debe probar que B_H es generador de $\Delta_R(G,H)$ para esto es suficiente demostrar que $g(h-1)$ se puede expresar como combinación lineal de elemtos de B_H. Para esto basta recordar que $g=q_ih_j$ para algún $q_i\in\mathcal{T}$ y $h_j\in H$ entonces $g(h-1)=q_ih_j(h-1)=q_i(h_jh-1)+(q_i-1)$ con lo que se demuestra lo que se pedía. □

Nota 3. *Es claro que si* $G=H$ *en la proposición anterior entonces* $\mathcal{T}=\{1\}$ *y por lo tanto* $B_H=\{(h-1,h\in H,h\neq 1)\}$ *y así esto se reduce a la proposición 3*

Ahora se explorará la opción usual cuando se está hablando de subgrupos, es decir, los subgrupos normales. De hecho, si $H\lhd G$ entonces el homomorfismo canónico $\omega: G\to G/H$ puede ser extendido a un epimorfismo, a saber

$$\omega*: RG\to R(G/H)$$

tal que

$$\omega^*\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \omega(g)$$

Proposición 6. *Con la notación anterior*

$$Ker(\omega^*) = \Delta(G,H)$$

Demostración. Considérese de nuevo $\mathcal{T}$ el transversal de H en G. Entonces, cada elemento $\alpha \in RG$ se puede escribir como $\alpha = \sum i, j r_{ij} q_i h_j$, $r_{ij} \in R$, $q_i \in \mathcal{T}$, $h_i \in H$. Si se denota $\overline{q_i} = \omega(q_i)$ entonces se tiene

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij}\right) \overline{q_i}$$

Entonces, $\alpha \in Ker(\omega^*)$ si y sólo si $\sum_j r_{ij} = 0$ para cada calor de i. Entonces si se tiene un $\alpha \in Ker(w^*)$ se puede escribir

$$\begin{aligned} \alpha &= \sum_i \left(\sum_j r_{ij}\right) \overline{q_i} && (2.5)\\ &= \sum_{ij} r_{ij} q_i (h_j - 1) \in \Delta(G,H) && (2.6) \end{aligned}$$

Con lo cual se tiene que $Ker(\omega^*) \subset \Delta(G,H)$. El hecho que $\Delta(G,H) \subset Ker(\omega^*)$ es trivial, por lo tanto $Ker(\omega^*) = \Delta(G,H)$ □

Corolario 2. *Sea H un subgrupo normal de G. Entonces $\Delta(G,H)$ es un ideal bilateral de RG y*

$$\frac{RG}{\Delta(G,H)} \simeq R(G/H)$$

Demostración. Como $Ker(\omega^*) = \Delta(G, H)$ entonces por el primer teorema de ismorfia $\frac{RG}{\Delta(G,H)} \simeq Im(\omega^*)$ pero como ω^* es sobreyectiva entonces $Im(\omega^*) = R(G/H)$ con lo que concluye la prueba. □

Hasta este punto se ha visto que hay una relación entre subgrupos normales de G e ideales bilaterales de RG, es decir, se pueden construir funciones de (S) a $\mathcal{I}(RG)$. La pregunta es entonces, ¿Qué pasa con las funciones en la otra vía?. Para responder esa pregunta considérese

$$\nabla(I) = \{g \in G \colon g - 1 \in I\}$$

Es fácil notar que $\nabla(I) = G \cap (1 + I)$

Lema 2. *$\nabla(I)$ es subgrupo de G*

Demostración. Se debe probar dos cosas:

1. Sean $g_1, g_2 \in \nabla(I)$ entonces

   $$g_1 g_2 - 1 = g_1(g_2 - 1) + (g_2 - 1) \in I$$

   por lo tanto $g_1 g_2 \in \nabla(I)$

2. Si $g\$in\nabla(I)$ entonces $g^{-1} - 1 = g^{-1}(1 - g) \in I$ de donde se sigue que $g^{-1} \in \nabla(I)$ □

Lema 3. *Si I es un ideal bilateral entonces $\nabla(I) \lhd G$*

Demostración. Se quiere probar que $gig^{-1} \in \nabla(I)$ entonces todo se reduce a demostrar que $gig^{-1} - 1 \in I$. Nótese que $gig^{-1} - 1 = gi(g^{-1} - 1) + (gi - 1)$ como I es ideal bilateral, entonces $gi(g^{-1} - 1) \in I$ y $(g_i - 1) \in I$ por lo tanto $gig^{-1} \in I$. □

Proposición 7. *Si $H \in (S)(G)$ entonces $\nabla(\Delta(G,H)) = H$*

Demostración. Sea $1 \neq x \in \nabla(\Delta(G,H))$ entonces $x-1 \in \Delta(G,H)$ por lo tanto se puede escribir

$$x - 1 = \sum_{i,j} r_{ij} q_i (h_j - 1).$$

Como 1 aparece en el lado izquierdo de la ecuación también debe aparecer en el lado derecho, por lo tanto alguno de los q_i debe ser $q_1 = 1$ por lo tanto hay en término de la forma $r_{1j}(h_j - 1)$. Nótese que todos los elementos de G del lado derecho de la ecuación son distintos a pares pero x debe aparecer allí, por lo tanto $x = h_j$. De lo anterior es inmediato que $\nabla(\Delta(G,H)) \subset H$. La otra contención es trivial. □

Según lo expuesto en la proposición anterior pareciera ser cierto que ∇ y $\Delta/$ son funciones inversas la una de la otra, pero esto no es cierto. Si se toma un ideal $I \in (I)(RG)$ entonces ¿Qué pasa con $\Delta(G, \nabla(I))$? Pues bien, sea $x \in \Delta(G, \nabla(I))$ entonces $x = \sum_{i,j} r_{ij} q_i (m_j - 1)$, $m_j \in \nabla(I)$ por lo tanto $m_j - 1 \in I$ y de alli que $x \in I$. Con eso se ha probado que $\Delta(G, \nabla(I)) \subset I$, pero la igualdad no es necesariamente cierta. Considérese $I = RG$ entonces $\nabla(RG) = G$ de donde $\Delta(G, \nabla(RG)) = \Delta G \neq RG$

2.3. Semisimplicidad

Con lo visto en la anterior sección ahora es accesible determinar condiciones necesarias y suficientes de R y G para que RG sea semisimple. Pero antes se probarán algunos resultados técnicos acerca de aniquiladores.

Definición 5. *Sea X un subconjunto de RG. El aniquilador de X por la izquierda es el conjunto*

$$Ann_i(X) = \{\alpha \in RG : \alpha x = 0, \forall x \in X\}$$

y de manera análoga el aniquilador de X por la derecha es el conjunto

$$Ann_d(X) = \{\alpha \in RG : x\alpha = 0, \forall x \in X\}$$

Definición 6. *Dado un grupo-anillo RG y un subconjunto finito X del grupo G, se denotará por $\hat{X}$ los siguientes elementos de RG*

$$\hat{X} = \sum_{x \in X} x$$

Lema 4. *Sea H un subgrupo de G y sea R un anillo.Entonces $Ann_d(\Delta(G,H)) \neq \{0\}$ si y sólo si H es finito. En ese caso, se tiene*

$$Ann_d(\Delta(G,H)) = \hat{H} \cdot RG$$

Mas aún, si $H \lhd G$ entonces $\hat{H}$ es central en RG y

$$Ann_d(\Delta(G,H)) = Ann_i(\Delta(G,H)) = RG \cdot \hat{H}$$

Demostración. Supóngase que $Ann_d(\Delta(G,H)) = \{0\}$ y considérese $\alpha = \sum_{g \in G} a_g g \in RG$, $\alpha \in Ann_d(\Delta(G,H))$ entonces

$$(h-1)\alpha = 0 \quad \text{para cada } h \in H \tag{2.7}$$

$$h\alpha - \alpha = 0 \tag{2.8}$$

$$\sum_{g \in G} a_g ah = \sum_{g \in G} a_g g \tag{2.9}$$

De la última ecuación se aprecia que $hg \in sop(\alpha)$ siempre y cuando $g \in sop(\alpha)$, pero $sop(\alpha)$ es finito, por tanto H es finito. De nuevo analizando la ecuación 2.9 se deduce que dado $g_0 \in sop(\alpha)$ entonces $hg_o \in sop(\alpha)$ para cualquier h elemento de H. De allí que se de la siguiente igualdad:

$$\alpha = a_{g_0}\hat{H}g_0 + \cdots + a_{g_t}\hat{H}g_t = \hat{H}\beta, \quad \beta \in RG$$

Lo anterior muestra que si H es finito entonces $Ann_d(\Delta(G,H)) \subset \hat{H}RG$. Por otro lado $h\hat{H} = \hat{H}$ ya que H es finito, entonces $h\hat{H} - \hat{H} = 0$ y por consiguiente $(h-1)\hat{H} = 0$ de donde $\hat{H}RG \subset Ann_d(\Delta(G,H))$

Por último si $H \lhd G$ entonces para todo g elemento de G se cumple que $gHg^{-1} = H$ de donde $g\hat{H}g^{-1} = \hat{H}$ de donde se concluye inmediatamente que $\hat{H}g = g\hat{H}$ lo cual prueba que $\hat{H}$ es central en RG y de alli se sigue fácilmente la conclusión. □

Del lema anterior se sigue el siguiente corolario.

Corolario 3. *Sea G un grupo finito. Entonces*

1. $Ann_i(\Delta(G)) = Ann_d(\Delta(G)) = R \cdot \hat{H}$

2. $Ann_d(\Delta(G)) \cap \Delta(G) = \{a\hat{G} : a \in R, a|G| = 0\}$

Demostración. Se procede por incisos

1. Ya se ha establecido que $\Delta(G,G) = G$, por lo tanto hágase $H = G$ en el teorema anterior y el resultado es inmediato.

2. Sea $x \in Ann_d(\Delta G) \cap \Delta G$ entonces $x = a\sum_{g\in G} g$ y además $x \in Ker(\omega^*)$ por tanto $Ker(x) = a\omega^*\hat{G} = a|G| = 0$ □

Lema 5. *Sea I un ideal bilateral de R. Supóngase que existe un ideal por la izquierda J tal que $R = I \oplus J$ (como $R-$ módulos). Entonces $J \subset Ann_d(I)$*

Demostración. Sea $x \in J$ y $y \in I$ entonces $yx \in J$, $yx \in I$ entonces $yx \in J \cap I$ por lo tanto $yx = 0$ de donde $x \in Ann_d(I)$ y por consiguiente $J \subset Ann_d(J)$ □

Lema 6. *Si el ideal de aumento de RG es un sumando directo de RG como un*

$RG-$módulo entonces G es finito y $|G|$ es invertible en R

Demostración. Las condiciones anteriores aseguran que existe J como en el lema anterior tal que $RG = \Delta G \oplus J$ de donde $J \subset \Delta G$ y por tanto $\Delta G \neq \{0\}$, con lo cual G es necesariamente finito. Por otra parte $1 \in RG$ entonces $1 = e_1 + e_2$ donde $e_1 \in \Delta G$ y $e_2 = a\hat{G}$, de lo cual se sigue que $\epsilon(1) = 1 = \epsilon(e_1) + \epsilon(e_2)$ pero $\epsilon(e_1) = 0$ por ser ΔG el núcleo de ϵ por ende se tiene $a|G| = 1$ con lo que se ha mostrado lo pedido. □

Ahora se está en disposición de determinar condiciones necesarias y suficientes en R y G para que el grupo-anillo RG sea semisimple. Los primeros resultados que apuntaron en esta dirección fueron dados por Maschkes, logros que están plasmados en el siguiente teorema:

Teorema 6 (Maschke)**.** *Sea G un grupo. Entonces, el grupo-anillo RG es semisimple si y sólo si las siguientes condiciones son verdaderas:*

1. *R es un anillo semisimple*

2. *G es finito*

3. *$|G|$ es invertible en R*

Demostración. Se procederá a probar las implicaciones en ambos sentidos:

1. En esta parte se asume que RG es semisimple, por lo tanto se puede utilizar el hecho que $\frac{RG}{\Delta(G)} = R$. De lo anterior se deduce que R es un cociente y ya se ha demostrado que los cocientes son simples. Por otro lado se sabe que $\Delta(G)$ es un ideal y de la semisimplicidad de RG se sabe que $\Delta(G)$ es sumando directo y del lema 6 se asegura que las condiciones (ii) y (iii) se satisfacen.

2. Para mostrar la segunda implicación, asúmase que (i), (ii) y (iii) son verdaderas. De (i) se sigue que RG es semisimple como $R-modulo$. [1] Considérese M como $RG-modulo$, tal que $M \in RG$, entonces existe N como R-modulo tal que

$$RG = M \oplus N$$

Sea $\pi RG \to M$ la proyección canónica asociada con la suma directa. Se define $\pi^*\colon RG \to M$ tal que:

$$x \mapsto \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx) \quad \text{para cada } x \in RG$$

Es claro que dicha función existe, ya que G es finito por (ii) y es $\frac{1}{|G|} < \infty$ por (iii). Se desea probar que π^* es un RG - homomorfismo tal que $(\pi^*)^2 = \pi^*$ y $M = Im(\pi^*)$, lo cual se muestra en dos partes a continuación:

Homomorfismo:
Basta demostrar que $\pi^*(ax) = a\pi^*(x) \quad$ para cada $a, g \in G$, ya que π^* ya es un R - homomorfismo. En efecto $\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x)$.

Ahora se tiene que $ga \in G$, por ser G un grupo, por lo tanto cuando g recorre todo G el producto ga también lo hará, ya que a es un elemento dado fijo. Por lo tanto la última expresión se puede volver a escribir como:

$$\pi^*(ax) = \frac{a}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x)$$

Sobreyectiva y Composición:
Nótese que $gm \in M$ ya que M es un RG - modulo, así que $\pi(gm) = gm$ y por

[1] Recordar que esto es por una propiedad de anillos que debo poner en el capitulo 1

lo tanto

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}(gm) = \frac{1}{|G|}|G|m = m$$

De lo anterior se sigue que $Im(\pi^*) \subset M$ y además $(\pi^*)^2 = \pi$. Por otro lado sea $m \in M$, entonces $\pi^*(m) = m \in Im(\pi^*)$, de donde $M \in Im(\pi^*)$.

Por lo anteriormente expuesto se sigue directamente que $Ker(\pi^*)$ es un RG - submodulo tal que $RG = M \oplus ker(\pi^*)$ □

Como es usual en ciencias, se explorará un caso particular del teorema anterior con la interrogante natural ¿Qué pasa si en lugar de un anillo se considera un campo?. La pregunta anterior se reduce a contemplar el caso $R = K$, donde K es un campo. Un campo siempre es semisimple, además se sabe que $|G|$ es invertible siempre y cuando $|G| \neq 0$, es decir, $car(K) \nmid |G|$, de donde se sigue el siguiente corolario:

Corolario 4. *Sea G un grupo finito y K un campo. Entonces KG es semisimple si y solo si $car(K) \nmid |G|$*

Aunque no es el objetivo de este trabajo de graduación dar una descripción de los grupo-álgebra, resulta tentador replantear el teorema de Wedderburn-Artin en este contexto, con lo cual se brinda mas información acerca de la estructura algebraica de un grupo-álgebra.

Teorema 7. *Sea G un grupo finito y sea K un campo tal que $car(K) \nmid |G|$. Entonces:*

1. *KG es suma directa de un numero finito de ideales bilaterales $\{B_i\}_{1\leq i\leq r}$, los componentes simples de KG. Cada B_i es una anillo simple.*

2. *Todo ideal bilateral de KG es suma directa de algunos de los miembros de la*

familia $\{B_i\}_{1\leq i\leq r}$

3. *Cada componente simple* B_i *es isomorfo a un anillo completo de matrices de la forma* $M_{n_i}(D_i)$*, donde* D_i *es un anillo de división conteniendo una copia isomorfa de* K *en su centro. Además el isomorfismo*

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

es un isomorfismo de álgebras.

4. *En cada anillo de matrices* $M_{n_i}(D_i)$*, el conjunto*

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ x_{n_i} & 0 & \dots & 0 \end{bmatrix} : x_1, x_2, \dots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

es un ideal minimal izquierdo. Dado $x \in KG$*, se considera* $\phi(x) = (\alpha_1, \dots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ *y se define el producto de* x *por un elemento* $m_i \in I_i$ *como* $xm_i = \alpha_i m_i$*. Con esta definición,* I_i *se convierte en un* KG *- módulo simple.*

5. $I_i \ncong I_j$*, si* $i \neq j$

6. *Cualquier* KG *- módulo simple es isomorfo a algún* I_i*,* $\quad 1 \leq i \leq r$

Se ha hecho énfasis en este resultado, ya que en el siguiente capitulo de este trabajo, se explorará la conexión entre este resultado y la teoría de representación de grupos.

Corolario 5. *Sea* G *un grupo finito y* K *un campo algebraicamente cerrado tal que* $car(K) \nmid |G|$*. Entonces:*

$$Kg \simeq \oplus_{i=1}^{r} M_{n_i}(K)$$

ss y $n_1^2 + n_2^2 + \dots + n_r^2 = |G|$

Demostración. Como $car(K) \nmid |G|$ es inmediato que

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

donde D_i es un anillo de división conteniendo una copia de K en su centro. Calculando la dimensión sobre K en ambos lados de la ecuación se tiene:

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K]$$

de donde se sique que cada anillo de división D_i es finito dimensional. Sea $0 \neq d_i \in D_i$ entonces $kd_i = 0$ implica que $k = 0$. Similarmente, dado $a_i \in D_i$ tal que $kd_i 0 a_i$ se tiene que $k = a_i d_i^{-1} \in K$ por ser K algebraicamente cerrado y por lo tanto $[D_i : K = 1]$ y $D_i = K$ para $1 \leq i \leq r$, con lo cual concluye la demostración. □

2.4. Grupo-Algebras de grupos abelianos

En esta sección se dará una descripción completa de grupo-anillo cuando el grupo es finito y además abeliano.

Como en la parte final de la sección anterior, se supone que K es un campo tal que $car(K) \nmid |G|$. Esta caracterización fue dada por primera vez por S. Perlis y G Walker (dar la referencia).

Se comenzará con el caso donde G es un grupo cíclico, así que se asume que $G =< a \colon a^n = 1 >$ y que K 4s un campo tal que $car(K) \nmid |G|$. Considérese la función $\phi \colon K[X] \to KG$ dada por

$$K[X] \ni f \mapsto f(a) \in KG$$

Debido a que la función ϕ consiste en tomar un polinomio de $K[G]$ y evaluarlo en a,

es obvio que ϕ es un epimorfismo de anillos y por lo tanto:

$$KG \simeq \frac{K[X]}{Ker(\phi)}$$

donde $ker(\phi) = \{f \in K[X] : f(a) = 0\}$. Como $K[X]$ es un dominio[2] de ideales principales se deduce que $Ker(\phi)$ es un ideal generado por el polinomio mónico f_0, de menor grado posible, tal que $f_0(a) = 0$.

Nótese que bajo el isomorfismo anterior, es claro que el elemento $a \in RG$ se mapea en $X + (f_0) \in \frac{K[X]}{(f_0)}$. Además de $a^n = 1$ se sigue que $X^n - 1 \in Ker(\phi)$, ya que si existiera un polinomio $f = \sum_{i=0}^{r} k_i x^i$ con $r < n$ entonces $f(a) \neq 0$ debido a que los elementos de $\{1, a, a^2, \ldots, a^r\}$ son linealmente independientes sobre K.De esa manera se puede asegurar que $Ker(\phi) = (X^n - 1)$ por lo que se satisface

$$KG \simeq \frac{K[X]}{(X^n - 1)}$$

Sea $X^n - 1 = f_1 f_2 \cdots f_t$ la descomposición de $X^n - 1$ como producto de polinomios irreducibles en $K[X]$. Como se está asumiendo que $char(K) \nmid n$, este polinomio debe ser separable y por lo tanto $f_i \neq f_j$ si $i \neq j$. Utilizando el teorema chino del residuo [3] se puede escribir:

$$KG \simeq \frac{K[X]}{f_1} \oplus \frac{K[X]}{f_2} \oplus \cdots \oplus \frac{K[X]}{f_t}$$

Utilizando este isomorfismo es fácil notar que el generador a tiene imagen $(X + (f_1), \ldots, X + (f_t))$.

Considérese ζ_i una raíz de f_i, $1 \leq i \leq t$. Entonces, se tiene $\frac{K[X]}{(f_i)} \simeq K(\zeta_i)$. Por lo tanto

[2]poner esto en el capitulo uno y hacer referencia

[3]también en la parte inicial y luego referencia a el

$$KG \simeq K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t)$$

Como todos los elementos $\zeta_i, \quad 1 \leq i \leq t$ son raíces de $X^n - 1$, se ha probado que KG es isomorfo a la suma directa de extensiones ciclotómicas de K. Finalmente baja este ultimo isomorfismo el elemento a tiene imagen $(\zeta_1, \zeta_2, \ldots, \zeta_t)$

Antes de continuar, se presentan algunos ejemplos para estudiar y comprender de mejor manera como trabajan las conclusiones anteriores.

Ejemplo 1. Sea $G =< a \colon a^7 = 1 >$ y $K = \mathbb{Q}$. En este caso la descomposición de $X^7 - 1$ en $\mathbb{Q}$ es

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

de esta forma si ζ es una raíz de la unidad de orden 7 distinta de 1, se puede escribir lo siguiente

$$\mathbb{Q}G = \mathbb{Q}(1) \oplus \mathbb{Q}(\zeta) = \mathbb{Q} \oplus \mathbb{Q}(\zeta)$$

Ejemplo 2. Sea $G =< a \colon a^6 = 1 >$ y $K = \mathbb{Q}$. La descomposición de $X^6 - 1$ en $\mathbb{Q}[X]$ es

$$X^6 - 1 = (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1)$$

entonces se obtiene

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right) \oplus \mathbb{Q}\left(\frac{1 + i\sqrt{3}}{2}\right)$$

donde $\frac{-1+\sqrt{3}}{2}$ es raíz de X^2+X+1 y $\frac{1+i\sqrt{3}}{2}$ es raíz de X^2-X+1, pero $\mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right) \simeq \mathbb{Q}\left(\frac{-1-i\sqrt{3}}{2}\right) \simeq \mathbb{Q}\left(\frac{-(1+i\sqrt{3})}{2}\right) \simeq \mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right)$

por lo que en realidad los últimos dos sumandos son iguales, dejando la expresión de la siguiente manera:

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right)$$

Los resultados anteriores dan una muy buena descripción de los grupos anillos cuando el anillo es un campo y el grupo es abeliano, por lo cual ahora se trabajará en un caso mas general.

Para poder hacer esto, se tratará de calcular todos los sumando directos en la descomposición de KG.

El lector debe recordar que para un d entero positivo dado, el polinomio ciclotómico de orden d, denotado por Φ_d , es el producto $\Phi_d = \prod_j (x-\zeta_j)$, donde ζ_j hace el recorrido por todas las raíces primitivas de la unidad de orden d. Tambień es conocido que $X^n - 1 = \prod_{d|n} \Phi_d$, es decir que $X^n - 1$ se puede expresar como el producto de todos los polinomios ciclotómicos Φ_d en $K[X]$, donde d es un divisor de n. Para cada d sea $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ la descomposición de Φ_d como producto de polinomios irreducibles en $K[X]$

Entonces la descomposición de KG puede ser escrita en la forma:

$$KG \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{K[X]}{(f_{d_i})} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} K(\zeta_{d_i})$$

donde ζ_{d_i} denota una raíz de f_{d_i}, $1 \leq i \leq a_d$. Para un d fijo, todos los elementos ζ_{d_i} son raíces primitivas de la unidad de orden d, por lo tanto, todos los

campos de la forma $K(\zeta_{d_i}), \quad 1 \leq i \leq a_d$ son iguales y se puede escribir simplemente

$$KG \simeq \oplus_{d|n} a_d K(\zeta_d)$$

donde ζ_d es una raíz primitiva de orden d y $a_d K[\zeta_d]$ denota la suma directa de a_d campos diferentes, todos ellos isomorfos a $K(\zeta_d)$.

Por otro lado, como $grad(f_{d_i}) = [K(\zeta_d) : K]$, se deduce que todos los polinomios tienen el mismo grado para $1 \leq i \leq a_d$. De esta forma, calculando el grado en la descomposición de Φ_d, se tiene

$$\phi(d) = a_d[K(\zeta_d) : K]$$

donde ϕ es la función totiente de Euler. Como G es un grupo cíclico de orden n, para cada divisor de n, el número de elementos de orden d en G, que se denota con n_d, es precisamente $\phi(d)$, entonces:

$$a_d = \frac{n_d}{|K(\zeta_d) : K|}$$

Ejemplo 3. Sea $G =< a \colon a^n = 1 >$ un grupo cíclico de orden n y $K = \mathbb{Q}$. Es conocido que el polinomio $X^n - 1$ se descompone en $\mathbb{Q}[X]$ como un producto de polinomios ciclotómicos, a saber:

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

y los polinomios Φ_d son irreducibles en $\mathbb{Q}[Q]$. Por lo tanto, en este caso en particular, la descomposición de $\mathbb{Q}G$ es:

$$\mathbb{Q}G \simeq \oplus_{d|n}\mathbb{Q}(\zeta_d)$$

Hay que notar, que como en casos anteriores, bajo este isomorfismo el generador a corresponde a la tupla cuyas entradas son raíces primitivas de la unidad de orden d, donde d es cualquier divisor positivo de n.

Finalmente se cerrará esta sección demostrando un hecho muy importante, a saber, que la caracterización anteriormente dada también es válida en los grupo-anillos con grupos abelianos finitos.

Teorema 8 (Perlis-Walker)**.** *Sea G un grupo finito abeliano de orden n y sea K un campo tal que $char(K) \nmid n$. Entonces*

$$KG \simeq \oplus_{d|n}a_dK(\zeta)$$

donde ζ_d es una raíz primitiva de la unidad de orden d y $a_d = \frac{n_d}{[K(\zeta_d):K]}$. En este fórmula n_d denota el número de elementos de orden d en G.

Demostración. Para proceder con la demostración es necesario enunciar y demostrar los siguientes lemas:

Lema 7. *Sea R un anillo conmutativo y G, H grupos, entonces $R(G\times H) \simeq (RG)H$ (el grupo-anillo de H sobre el anillo RG)*

Demostración. Considérese el conjunto $M_{n,\gamma} = \{g : (g,h) \in sop(\gamma)\}$. y la función $f\colon R(G\times H) \to (RG)H$ tal que $\gamma \mapsto \beta$ donde $\beta = \sum_{h\in H}\alpha_h h$ con $\alpha_h = \sum_{g\in M_{h,\gamma}} a_{gh}g$. Se debe demostrar que f es una función biyectiva y además es un homomorfismo de anillos.

Homomorfismo:

1. **Conserva sumas:** Sea $\gamma_1, \gamma_2 \in R(G \times H), \quad \gamma_1 = \sum_{g\in G, h\in H} a_{gh}(g,h), \quad \gamma_2 = \sum_{g\in G, h\in H} b_{gh}(g,h)$. De esta forma se tiene $f(\gamma_1) = \sum_{h\in H} \beta_h h, \quad \beta_h = \sum_{g\in M_{h,\gamma_1}} a_{gh}h$ y $f(\gamma_2) = \sum_{h\in H} \xi_h h, \quad \xi_h = \sum_{g\in M_{h,\gamma_2}} b_{gh}h$.

   Haciendo la operatoria se tiene:

$$f(\gamma_1) + f(\gamma_2) = \sum_{h\in H} (\beta_h + \xi_h)h = \sum_{h\in H} \alpha_h h$$

   en donde $\alpha_h = \beta_h + \xi_h$

   Por otro lado:

$$f(\gamma_1)+f(\gamma_2) = f\left(\sum_{g\in G, h\in H} (a_{gh} + b_{gh})g\right) = \sum_{h\in H} \alpha_h h, \quad \alpha_h = \sum_{g\in M_h, \gamma_1+\gamma_2} (a_{gh}+b_{gh})g$$

   De lo anterior se deduce fácilmente que $\alpha_h = \sum_{g\in M_{h,\gamma_1}} a_{gh}g + \sum_{g\in M_{h,\gamma_2}} b_{gh}g = \beta_h + \xi_h$

2. **Conserva productos:** Sean $\gamma_1, \quad \gamma_2 \in R(G \times H)$, entonces haciendo la operatoria:

$$\gamma_1\gamma_2 = \sum_{g,m\in G, h,n\in H} a_{gh}b_{mn}(g,h)(m,n)$$

   Como ya se ha probado que f conserva sumas, ahora es suficiente demostrar que dados $(g,h), \quad (m,n) \in (G \times H)$ se cumple que $f((g,h)(m,n)) = f((g,h))f((m,n))$ y que además f es $R-$lineal. En efecto, por un lado

$$f((g,h))f((m,n)) = (gh)(nm) = gnhm$$

y por el otro lado se tiene:

$$f((g,h)(n,m)) = f((gn,hm)) = gnhm$$

El hecho de que f es $R-$lineal se sigue directamente de la definición de f.

3. f **es inyectiva:** Para demostrar que f es inyectiva se debe demostrar que el único elemento que anula a f es elemento neutro de $R(G \times H)$. Para el efecto, considérese $\gamma \in R(G \times H), \quad \gamma = \sum_{g\in G, h\in H} a_{gh}(g,h)$ tal que $f(\gamma) = \sum_{h\in H} \alpha_h h = 0, \quad \alpha_h = \sum_{g\in M_{h,\gamma}=a_{gh}h}$, lo cual implica que $a_{gh} = 0$ para cada$g \in G, h \in H$, de donde $\gamma = 0$

4. f **es sobreyectiva:** Dado $\sum_{h\in h} \alpha_h h \in (RG)H$ se construye $\gamma = \sum_{g\in G, h\in H} a_{gh}(g,h)$, donde a_{gh}, es decir, el coeficiente de (g,h) es el mismo que el de g en α_h. Con lo que concluye la prueba. □

Lema 8. *Sea $\{R_i\}_{i\in I}$ una familia de anillos y sea $R = \oplus_{i\in I} R_i$. Entonces para cualquier grupo G se tiene $RG \simeq \oplus_{i\in I} R_i G$*

Demostración. Considérese la función $f\colon \oplus_{i\in I} R_i G \to RG$ dado por $(\alpha_1, \cdots, \alpha_n) \mapsto \sum_{g\in G} a_g g, \quad a_g = (a_g^{(1)}, \cdots, a_g^{(n)})$, donde $a_g^{(i)}$ es el coeficiente de g en $\alpha_i = \sum_{g\in G} a_g^{(i)} g$. Se debe comprobar que f es un homomorfismo de anillos.

1. **Conserva sumas:** Sean $\alpha = (\alpha_1, \cdots, \alpha_n), \quad \beta = (\beta_1, \cdots, \beta_n) \in \oplus_{i\in I} R_i G$, entonces su suma viene dada por $\gamma = (\alpha_1 + \beta_1, \cdots, \alpha_n + \alpha_n)$, y con ello la imagen de la suma seria $f(\gamma) = \sum_{g\in G} c_g g, \quad c_g = (a_g^{(1)}, \cdots, a_g^{(n)})$.

Por otro lado, se tiene:

$$\begin{aligned} f(\alpha)+f(\beta) &= \sum_{g\in G} a_g g + \sum_{g\in G} b_g g \\ &= \sum_{g\in G} (a_g + b_g) g \\ &= \sum_{g\in G} d_g g, \quad d_g = (a_g^{(1)} + b_g(1), \cdots, a_g^{(n)} + b_g(n)) \end{aligned}$$

por lo tanto $f(\alpha+\beta) = f(\alpha) + f(\beta)$

2. **Conserva productos:** Como en el caso anterior, se tiene $\gamma = \alpha\beta = (\alpha_1\beta_1, \cdots, \alpha_n\beta_n)$, y por lo tanto, su imagen bajo f, es $f(\gamma) = \sum_{u\in G} c_u u, \quad c_u = (c_u^{(1)}, \cdots, c_u^{(n)}), \quad c_u^{(i)} = \sum_{gh=u} a_g^{(i)} b_h^{(i)}$.

   Por otro lado, $f(\alpha) = \sum_{g\in G} a_g g, \quad f(\beta) = \sum_{g\in G} b_g g$, multiplicando, se obtiene $f(\alpha)f(\beta) = \sum_{u\in G} d_u u, \quad d_u = \sum_{gh=u} a_g b_h = \left(\sum_{gh=u} a_g^{(1)} b_g^{(1)}, \cdots, \sum_{gh=u} a_g^{(n)} b_g^{(n)}\right) = c_u$

3. f **es inyectiva:** Supóngase que $f(\alpha) = \sum_{g\in G} a_g g = 0$ entonces $a_g = (0, \cdots, 0)$, de donde $\alpha = (0, \cdots, 0)$

4. f **es sobreyectiva:** Dado $\sum_{g\in G} a_g g, \quad a_g = (a_g^{(1)}, \cdots, a_g^{(n)})$. Entonces se construye $\alpha = \left(\sum_{g\in G} a_g^{(1)} g, \cdots, \sum_{g\in G} a_g^{(n)} g\right)$ y es fácil verificar que $f(\alpha) = \sum_{g\in G} a_g g$ □

Para demostrar el teorema se procede por inducción sobre el orden de G. Supóngase que el resultado es válido para cualquier grupo abeliano de orden menor que n.

Sea G tal que $|G| = n$. Si G es generado no hay algo que demostrar. Si G no

fuera un grupo generado se puede utilizar el teorema de estructura [4] de los grupos finitos abelianos para escribir $G = G_1 x H$ donde H 4s generado y $|G_1| = n_1 < n$. Por hipótesis de inducción se puede escribir

$$RG_1 \simeq \oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})$$

donde $a_{d_1} = \frac{n_{d_1}}{[K(\zeta_{d_1}):K]}$ y n_{d_1} denota el numero de elementos de orden d_1 en G_1. Aplicando el lema 7 se cumple

$$RG = R(G_1 x H) \simeq (RG_1)H \simeq \left(\oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})\right) H$$

utilizando el lema 8 se obtiene

$$\left(\oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})\right) H \simeq \oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1}) H$$

Como H es cíclico se puede escribir

$$\oplus_{d_1|n_1} \oplus_{d_2||H|} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2})$$

donde $a_{d_2} = \frac{n_{d_2}}{[K(\zeta_{d_1}, \zeta_{d_2}):K(\zeta_{d_1})]}$ y n_{d_2} es el número de elementos en H de orden d_2.

Sea $d = [d_1, d_2]$ entonces por el teorema del elemento primitivo, se tiene $K(\zeta_d) = K(d_1, d_2)$ por tanto

$$KG \simeq \oplus_{d|n} a_d K(\zeta_d)$$

[4] poner en capitulo 1

con $a_d = \sum_{d1,d2} a_{d_1} a_{d_2}$ y donde la suma recorre todos los d_1, d_2 son números naturales tales que $[d_1, d_2] = d$. Por otro lado, del hecho que $[K(\zeta_d) : K] = [K(\zeta_{d_1,\zeta_{d_2}}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K]$ se tiene que:

$$a_d[K(\zeta_d : K)] = \sum_{d_1,d_2} a_{d_1} a_{d_2} [K(\zeta_{d_1,\zeta_{d_2}}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] = \sum_{d_1,d_2} n_{d_1} n_{d_2}$$

□

3. TEORÍA DE REPRESENTACIÓN DE GRUPOS

3.1. Definición y Ejemplos

Como se mencionó en el capítulo 1 [1] el concepto de **grupo de permutaciones** fue dado explícitamente por primera vez en las memorias de Galois en 1830, aunque la primera definición de grupo abstracto fue dado hasta en 1854 por Cayley, aunque pasó inadvertidamente por un tiempo, hasta que dicha definición fue dada nuevamente en repetidas ocasiones por varios matemáticos, a saber: Leopold Kronecker en 1870, Heinrich Martin Weber en 1882 y Ferdinand Georg Frobenius en 1887. De esa forma los grupos fueron considerados por mucho tiempo como objetos concretos antes de llegar a ser estudiados como estructuras algebraicas abstractas.

En este contexto histórico es natural hacer la pregunta: Dado un grupo abstracto ¿ Cómo se puede saber que grupo es -en particular - ? Es decir, ¿ Se puede decir cuando es un grupo de permutaciones, un grupo lineal o un grupo de transformaciones proyectivas - sólo por citar algunos ejemplos- ?

En 1879, durante las lecturas de un coloquio matemático realizado en Evanston, Illinois, Felix Klein planteó la posibilidad de representar un grupo abstracto dado como un grupo de transformaciones lineales (véase [1]).

Siguiendo estas ideas, Theodor Molien, Georg Frobenius, Issai Schur, William Burnside y Heinrich Maschke desarrollaron la teoría básica de la representación de grupos al inicio del siglo XX y Burnside presentó la primera exposición sistemática de este tema en su libro [2], que actualmente es considerado un libro clásico en este tema.

[1] ponerlo ejemplos en esta parte de la definición de grupos

La teoría de la representación se volvió mas importante a medida que se fueron obteniendo nuevos resultados.

Uno de los resultados mas importantes es el famoso teorema que establece que si p y q son números enteros primos y a, b enteros positivos, entonces cualquier grupo de orden $p^a q^b$ es soluble. [2] Este teorema fue demostrado en 1904 por William Burnside usando la teoría de representación de grupos y, como dato curioso, la primera demostración que no utiliza dicha teoría fue proporcionada por John Griggs Thompson mas de 60 años después (ver [3]).

William Burnside también conjeturó que todo grupo de orden impar es soluble. Esta conjetura fue un problema abierto hasta que Walter Feit y John Thompson dieron una demostración de esta conjetura en 1963 (ver [4]), usando para ello teoría de la representación.

Luego de hacer énfasis en la importancia histórica que tiene la teoría de representación de grupos, se entra a estudiar algunas definiciones de la misma.

Definición 7. *Sea G un grupo, R un anillo conmutativo y V un R-módulo libre de rango finito. Una* ***representación*** *de G sobre R, con espacio de representación V, es un homomorfismo de grupos $T\colon G \to GL(V)$, donde $GL(V)$ es el grupo de automorfismos de V. El rango de V es llamado* ***grado*** *de la representación T y se denotará como* $\deg(T)$.

Para $g \in G$ se denotará como $T_g\colon V \to V$ al automorfismo correspondiente bajo T. Así, si $g, h \in G$, se tiene que $T_{gh} = T_g \circ T_h$ y $T_1 = I$.

El caso en el que R es un campo es de particular importancia. Históricamente, este fue el primer caso que se estudió y es en ese contexto donde se obtuvieron la mayor parte de resultados.

[2] poner esto en el glosario o en donde corresponde: Un grupo G es soluble si hay una cadena de subgrupos $e = H_0 \subset H_1 \subset \cdots \subset H_n \subset H_n = G$ tal que para cada i, el subgrupo H_i es normal en H_{i+1} y el grupo cociente H_{i+1}/H_i es abeliano.

Si se escoge una R-base de V, se puede definir un isomorfismo ϕ de $GL(V)$ al grupo $GL(n,R)$ de matrices invertibles $n \times n$ con coeficientes en R, asignándole a cada automorfismo $T \in GL(V)$ su matriz respecto a la base dada. Esto da paso a la siguiente definición:

Definición 8. *Sea G un grupo y R un anillo conmutativo. Una representación matricial de G sobre R de grado n es un homomorfismo de grupos $T\colon G \to GL(n,R)$.*

Si $T\colon G \to GL(V)$ es una representación de G sobre R con espacio de representación V y se considera el isomorfismo $\phi\colon GL(V) \to GL(n,R)$ asociada a alguna $R-$ base, entonces $\phi \circ T\colon G \to GL(n,R)$ es una representación matricial de G. De manera similar, dada una representación matricial $T\colon G \to GL(n,R)$, entonces $\phi^{-1} \circ T\colon G \to GL(V)$ es una representación de G sobre R. Debido a este hecho, no se hará distinción entre representación y representación matricial.

Para ilustrar lo que se expuso anteriormente, se ha considerado necesario, exponer algunos ejemplos sencillos.

Ejemplo 4. Dado un grupo G y un anillo conmutativo R, la función $T\colon G \to GL(n,R)$ tal que a cada elemento G le asocia la matriz identidad de $GL(n,R)$ es una representación matricial de G. A esta función se le llama **representación trivial** de G sobre R de grado n.

Ejemplo 5. Sea G el grupo de Klein de cuatro elementos,es decir, $G = \{1, a, b, ab\}$. Este grupo tiene tres elementos de orden dos. Entonces $T\colon G \to GL(2,\mathbb{Z})$ es la función tal que:

$$\mathsf{T}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathsf{T}(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\mathsf{T}(b) = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \mathsf{T}(ab) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ejemplo 6. Sea S_n el grupo de simetrías de n símbolos y R un anillo conmutativo. Sea V un $R-$módulo libre de rango n con base $\{v_1, v_2, \cdots, v_n\}$. Para facilitar la comprensión de este ejemplo, se sugiere al lector imaginar que $V = \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{n}$ con su base canónica.

Por otra parte, considérese la función $f\colon S_n \to GL(V)$ de la siguiente manera: a cada elemento $\sigma \in S_n$, se le asigna la función $T_\sigma \in GL(V)$, que actúa, de manera natural, como:

$$T_\sigma(v_i) = v_{\sigma(i)}.$$

Como T_σ deja a la base intacta (salvo permutaciones), es claro que T_σ es un isomorfismo.

Es claro que T es un isomorfismo, por su definición, y por lo tanto una representación de S_n.

Como se puede apreciar una representación por si sóla puede ser poca descriptiva, por lo tanto se considera de mas utilidad conocer la representación matricial. Para este caso en particular, considérese $A(\sigma)$, la matriz asociada a T_σ, que se obtiene al calcular $T_\sigma(v_j)$ como combinación lineal de la base. Como $T_\sigma(v_j) = v_{\sigma(j)}$, entonces los coeficientes de la matriz anterior son cero en todas sus entradas excepto en $(\sigma(j), j)$, en la cual la entrada vale uno. De esta manera es fácil notar que $A(\sigma)$ es una matriz que tiene exactamente una entrada igual a uno en cada fila y columna y las demás iguales a cero. Dicha matriz se conoce como la **matriz de permutación**.

Ejemplo 7 (La representación Regular)**.** Sea G un grupo finito de orden n y R un anillo conmutativo. Se requiere definir una representación de G sobre R, para ello se considerará como espacio de representación a RG, es decir, a el grupo-anillo de G sobre R.

Considérese la función $T\colon G \to GL(RG)$ de la siguiente manera: a cada elemento $g \in G$ se le asigna la función lineal T_g que transforma a los elementos de la base por medio de multiplicación por la izquierda, esto es, $T_g(g_i) = gg_i$. Es claro que T es una representación de G, debido a que:

$$T_{gh}(y) = (gh)y = g(h(y)) = T_g T_h(y).$$

En este caso hay que recordar que G es una base de RG sobre R y se pueden enumerar, en algún orden, los elementos de G como sigue:

$$G = \{1 = g_1, g_2, \cdots, g_n\},$$

por lo tanto es fácil notar que en la correspondiente representación matricial con respecto a la base G de RG, la imagen de cualquier elemento $g \in G$ es una matriz de permutación, debido a la cerradura del producto en G.

La representación anterior usualmente es llamada la **representación regular de G sobre R**. Es importante notar que esta representación se construyó a partir de la multiplicación por la izquierda, así que sería mas apropiado llamarla representación regular por la izquierda de G sobre R. Para ilustrar de mejor manera a continuación se muestra un ejemplo:

Ejemplo 8. Sea $G = \{1, a, a^2\}$ un grupo cíclico de orden tres. Enumérese los elementos de G como $g_1 = 1$, $g_2 = a$, $g_3 = a^2$. Para encontrar la representación regular de a, basta con multiplicar por a los elementos de G por la izquierda:

$$ag_1 = g_2, \quad ag_2 = g_3, \quad ag_3 = g_1$$

entonces se tiene:

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_3, \quad T_a(g_3) = g_1,$$

por lo tanto la matriz asociada con a en la base dada es:

$$\rho(\mathsf{a}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

que no es más que una matriz de permutación.

Ejemplo 9. Considérese, de nuevo, el grupo de Klein de cuatro elementos, $G = \{1, a, b, ab\}$ con la numeración: $g_1 = 1$, $g_2 = a$, $g_3 = b$, $g_4 = ab$.

Para conocer la representación regular de a, se procede a multiplicar por la izquierda por a a los elementos de G:

$$ag_1 = g_2, \quad ag_2 = g_1, \quad ag_3 = g_4, \quad ag_4 = g_3,$$

entonces

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_1, \quad T_a(g_3) = g_4, \quad T_a(g_4) = g_3$$

y como en el ejemplo anterior, se puede obtener la representación matricial de a:

$$\rho(\mathsf{a}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

De manera similar se obtiene la representación matricial de los elementos restantes de G:

$$\rho(\mathsf{b}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \rho(\mathsf{ab}) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \rho(\mathsf{1}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Nota 4. *Ya se mencionó que $\rho(g)$ con $g \in G$ es una matriz de permutación, pero es*

importante hacer notar que si se toma $1 \neq g \in G$*, entonces para cualquier* $g_i \in G$ *se tiene que* $gg_i \neq g_i$*. Esto implica que para cualquier elemento* g_i *de la base se cumple que* $T_g(g_i) \neq g_i$ *y por ende los elementos de la diagonal de* $\rho(g)$ *son todos iguales a cero. Más aún, de lo anteriormente expuesto, se deduce que si* $g \neq 1$ *entonces* $tr(\rho(g)) = 0$ *si* $g \neq 1$ *y* $tr(\rho(g)) = |G|$ *si* $g = 1$*. Este resultado elemental es de mucha importancia cuando se está trabajando con la representación regular.*

Ejemplo 10. [Algunas representaciones de grupos cíclicos] Considérese el grupo cíclico $G = \{1, a, \cdots, a^{m-1}\}$ y sea K un campo. Si se desea construir una representación matricial $A\colon G \to GL(n, K)$ es necesario escoger la matriz $A(a)$, ya que por ser A un homomorfismo, las matrices de representación de los restantes elementos del grupo están determinadas por $A(a^r) = (A(a))^r$. Además para demostrar que A es un homomorfismo de grupos, basta con probar que $(A(a))^r = I$, para algún $r \in \mathbb{Z}$.

Supóngase que $\text{car}(K) \nmid m$ y que K contiene una raíz primitiva de la unidad de orden m, ξ. Entonces

$$A\colon G \to GL(1, K)$$

tal que, $A(a) = \xi$ es una representación, ya que $(A(a))^r = \xi^r = 1$ para algún r. Además, si $\{\xi_1, \cdots, \xi_m\}$ es un conjunto de todas las raíces de la unidad unidad de orden m que son distintas a pares entonces la función $B\colon G \to GL(m, K)$ dada por

$$\mathsf{B(a)} = \begin{pmatrix} \xi_1 & & \dots & 0 \\ 0 & \xi_2 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & \xi_m \end{pmatrix}$$

es una representación de G sobre K de grado m, ya que $\xi_i^r = 1$ para algún $r \in \mathbb{Z}$, entonces

$$(\mathsf{B(a)})^{\mathsf{r}} = \begin{pmatrix} \xi_1^r & & \dots & 0 \\ 0 & \xi_2^r & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & \xi_m^r \end{pmatrix} = I.$$

Nótese que esta representación es distinta a la representación regular, que en el caso de a, está dada por

$$\Gamma(a) = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Finalmente si $car(K) \mid m$ entonces se propone la representación $C\colon G \to GL(2, K)$, dada por

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

ya que $(\mathsf{C}(\mathsf{a}))^{\mathsf{r}} = \begin{pmatrix} 1 & r \cdot 1 \\ 0 & 1 \end{pmatrix} = I$ para $r \in \mathbb{Z}$, esto por que $\mathrm{car}(K) < \infty$.

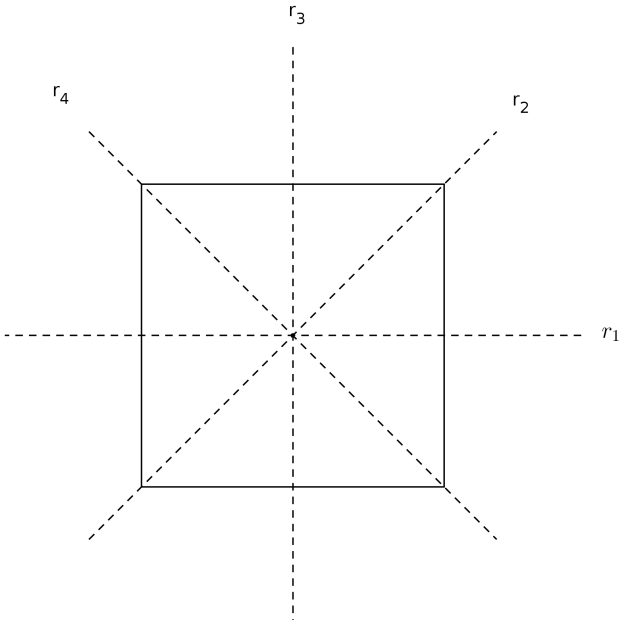
Ejemplo 11 (Representación de D_4)**.** Considérese el grupo de simetrías de un cuadrado. Este grupo de 8 elementos, a saber, las reflexiones a través de los ejes r_1, r_2, r_3, r_4 (véase la Figura 3) y las rotaciones con ángulos $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ y 2π alrededor del centro .

Sea a la rotación de ángulo $\frac{\pi}{2}$ y b la reflexión a través del eje r_2. Es fácil ver, bajo consideraciones geométricas, que cualquier otro elemento de este grupo se puede obtener por medio de a y b.

De manera mas abstracta, este grupo –que es llamado grupo diédrico de orden ocho y usualmente denotado por D_4 – puede ser definido con dos generadores que satisfacen las relaciones

$$a^4 = 1, \quad b^2 = 1, \quad baba = 1.$$

Figura 3. **Forma gráfica del grupo D_4**



Fuente: elaboración propia con programa para computadora geogebra.

Por lo tanto este grupo puede ser descrito como

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Como todas los elementos de este grupo están en terminos de a y b, entonces para encontrar una representación matricial $A\colon D_4 \to GL(n, K)$ sobre el campo K, será suficiente encontrar matrices $A(a)$, $B(b)$ tales que $A(a)^4 = I$, $A(b)^2 = I$, $A(b)A(a)A(b)A(a) = I$.

Es fácil determinar representaciones de grado uno para D_4 en un campo K de

característica diferente a dos, de la siguiente manera:

$$\begin{aligned} A(a) &= 1 \qquad & A(b) &= 1 \\ B(a) &= 1 \qquad & B(b) &= -1 \\ C(a) &= -1 \qquad & C(b) &= 1 \\ D(a) &= -1 \qquad & D(b) &= -1. \end{aligned}$$

Pensando en el significado geométrico de a y b, como dos funciones del plano al plano, se puede calcular sus matrices con respecto a la base canónica para obtener otra representación matricial de D_4:

$$\mathsf{W(a)} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad , \qquad \mathsf{W(b)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ejemplo 12 (Suma directa de representaciones)**.** Sean $T\colon G \to GL(V)$ y $S\colon G \to GL(W)$ dos representaciones de un grupo G sobre un anillo conmutativo R. Se puede definir una nueva representación $V \oplus W$, que es llamada la **suma directa** de dos representaciones dadas y se denota como $T \oplus S$, de la siguiente manera:

$$(T \oplus S)_g = T_g \oplus S_g, \quad \text{para cada } g \in G.$$

Si se eligen bases $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_m\}$ de V y N respectivamente y se denota por $g \mapsto A(g)$ y $g \mapsto B(g)$ las correspondientes representaciones matriciales en las bases dadas, entonces la representación matricial asociada a $T \oplus S$ con respecto a la base $\{(v_1, 0), \ldots, (v_n), (0, w_1), \ldots, (0, w_n)\}$ de $V \oplus W$, viene dada por

$$g \mapsto \begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}.$$

Los ejemplos anteriormente expuestos sirven de motivación para introducir algunos conceptos de teoría de la representación. En este trabajo se restringirán las representaciones al caso en el cual R es un campo, debido a que con este caso se logra

ilustrar la relación de teoría de representación con los problemas de grupo-anillos.

Primero considérese $T\colon G \to GL(V)$ una representación de un grupo G sobre un campo K y asúmase que $\phi\colon V \to W$ es un isomorfismo de espacios vectoriales sobre K. Entonces se puede definir una nueva representación $\overline{T}\colon G \to GL(W)$ por medio de $\overline{T_g}\colon \phi \circ T_g \circ \phi^{-1}$ para todo $g \in G$. Esto es, esencialmente, una copia de T. La relación entre estas dos representaciones está ilustrada en el siguiente diagrama:

$$\begin{array}{ccc} V & \xrightarrow{T_g} & V \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ W & \xrightarrow[\overline{T_g}]{} & W \end{array} .$$

Lo cual sugiere lo siguiente:

Definición 9. *Dos representaciones $T\colon G \to GL(V)$ y $\overline{T}\colon G \to GL(W)$ de un grupo G sobre el mismo campo K se dicen que son* ***equivalentes*** *si existe un isomorfismo $\phi\colon V \to W$ tal que $\overline{T_g} = \phi T_g \phi^{-1}$ para cualquier $g \in G$.*

Definición 10. *Dos representaciones matriciales $A\colon G \to GL(n,K)$ y $B\colon G \to GL(n,K)$ de un grupo G sobre un campo K se dicen equivalentes si existe una matriz invertible $U \in GL(n,K)$ tal que $A(g) = UB(g)U^{-1}$ para cualquier $g \in G$.*

Ejemplo 13. Sea G un grupo cíclico de orden m y K un campo que contiene a $\{\xi_1, \xi_2, \ldots, \xi_m\}$, el conjunto de todas las raíces distintas de la unidad de orden m. Entonces, si se consideran las representaciones B y Γ dadas en el ejemplo 10 con

$$\mathsf{U} = \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix}, \quad \mathsf{U} \in GL(n,K)^3$$

[3]Esto es evidente, ya que U es una matriz de Vandermonde con $det(\mathsf{U}) = \prod_{1 \le i < j \le m}(\xi_i - \xi_j) \neq 0$.

entonces, calculando por un lado se tiene

$$\mathsf{B(a)U} = \begin{pmatrix} \xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & \xi_m \end{pmatrix} \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix} = \begin{pmatrix} \xi_1^2 & \xi_1^3 & \cdots & \xi_1 \\ \xi_2^2 & \xi_2^3 & \cdots & \xi_2 \\ & & \cdots & \\ \xi_m^2 & \xi_m^2 & \cdots & \xi_m \end{pmatrix},$$

similarmente

$$\mathsf{U\Gamma(a)} = \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} \xi_1^2 & \xi_1^3 & \cdots & \xi_1 \\ \xi_2^2 & \xi_2^3 & \cdots & \xi_2 \\ & & \cdots & \\ \xi_m^2 & \xi_m^2 & \cdots & \xi_m \end{pmatrix}$$

con lo que se ha demostrado que $\mathsf{A(g)} = \mathsf{UB(g)U^{-1}}$, para cualquier $g \in G$ y concluye que B y $\mathsf{\Gamma}$ son equivalentes.

Considérese $T\colon G \to GL(V)$ una representación de un grupo G sobre el campo K, con espacio de representación V y asúmase que V contiene un subespacio W que es invariable bajo T, esto es, un subespacio tal que $T_g(W) \subset W$, para cualquier $g \in G$. Entonces se puede considerar el homomorfismo de grupos que asigna a cada elemento $g \in G$ la restricción de T_g al subespacio W. Por ser T_g la restricción se tiene entonces es claro que el homomorfismo anterior es una representación de G sobre K, con espacio de representación W.

Con el afán de dar una representación matricial de este hecho, considérese una base $\{w_1, w_2, \ldots, w_t\}$ de W y extiéndase a una base $\{w_1, \cdots, w_t, v_{t+1}, \cdots, v_n\}$ de V. Entonces la matriz asociada a cada función T_g, $g \in G$ con respecto a esa base es de la forma

$$\begin{pmatrix} \mathsf{A(g)} & \mathsf{B(g)} \\ 0 & \mathsf{C(g)} \end{pmatrix}$$

donde $\mathsf{A(g)} \in GL(t, K), C(g) \in GL(n-t, K)$ y $\mathsf{B(g)}$ es una matriz de $t \times (n-t)$. Estas consideraciones sugieren lo siguiente:

Definición 11. *Una representación $T\colon G \to GL(V)$ de un grupo G sobre un campo K es llamada irreducible si los únicos subespacios propios de V que son invariantes bajo T son los triviales, es decir, V y $\{0\}$.*

La representación es llamada **reducible** si V contiene subespacios no triviales que son invariantes bajo T.

Definición 12. *Una representación matricial $M\colon G \to GL(n, K)$ es llamada reducible si existe una matriz $\mathsf{U} \in GL(n, K)$ tal que para cualquier $g \in G$, se tiene que la matriz $\mathsf{U}M(g)U^{-1}$ es de la forma*

$$\mathsf{UM(g)U^{-1}} = \begin{pmatrix} \mathsf{A(g)} & \mathsf{B(g)} \\ 0 & C(g) \end{pmatrix}$$

El ejemplo 13 muestra que la representación regular de un grupo cíclico de orden m, sobre un campo K que contiene raíces de la unidad de orden m es reducible. De hecho, cualquier representación regular de un grupo finito $G \neq \{1\}$ sobre cualquier campo es reducible. En efecto, nótese que si en el espacio de representación RG se toma el elemento $\hat{G} = \sum_{g \in G} g$ entonces $T_g(\hat{G}) = \hat{G}$ por lo tanto el subespacio generado por $\hat{G}$ es invariante bajo T y $(\hat{G}) \neq RG$.

Definición 13. *Una representación $T\colon G \to GL(V)$ de un grupo G sobre un campo K es llamado completamente irreducible si para todo subespacio W que es invariante bajo T existe un subespacio invariante W' tal que $V = W \oplus W'$.*

Para entender de mejor manera esta definición se dará una interpretación en términos de matrices.

Sea $\{w_1, w_2, \ldots, w_t\}$ y $\{w_{t+1}, \ldots, w_n\}$ bases dadas para W y W' respectivamente, entonces $\{w_1, w_t, w_{t+1}, \ldots, w_n\}$ es una base de V y para cualquier $g \in G$ la

matriz de T_g con respecto a esta base es de la forma

$$\begin{pmatrix} \mathsf{A(g)} & 0 \\ 0 & \mathsf{B(g)} \end{pmatrix}$$

donde $\mathsf{A(g)}$ y $\mathsf{B(g)}$ son las matrices de representación de T_g en W y W' con respecto a las bases dadas.

Definición 14. *Una representación matricial $M\colon G \to GL(n,K)$ es llamada completamente reducible si cualquier representación matricial M de la forma*

$$\begin{pmatrix} \mathsf{A(g)} & \mathsf{B(g)} \\ 0 & \mathsf{C(g)} \end{pmatrix}$$

es equivalente a una representación matricial de la forma

$$\begin{pmatrix} \mathsf{A(g)} & 0 \\ 0 & \mathsf{D(g)} \end{pmatrix}.$$

3.2. Representación y Módulos.

En este sección se estudiará la conexión que hay entre módulos y representaciones. Dicha conexión se establece usando el concepto de grupo-anillo.

Proposición 8. *Sea G un grupo y R un anillo conmutativo con unidad. Entonces, existe una biyección entre representaciones de G sobre R y RG-módulos libres y de rango finito.*

Demostración. Dada una representación $T\colon G \to GL(V)$ de G sobre R, se asocia a ella el RG-módulo construido a partir de V manteniendo la misma estructura aditiva y definiendo el producto de un elemento $v \in V$ por un escalar $\alpha = \sum_{g\in G} a_g g \in RG$ como

$$\alpha v = \left(\sum_{g\in G} a_g g\right) v = \sum_{g\in G} a(g) T_g(v). \tag{3.1}$$

Usando está definición de producto se verifica:

1. Distributividad de la suma de escalares respecto al producto por escalar

$$\begin{aligned}(\alpha+\beta)v &= \left(\sum_{g\in G}(a_g+b_g)g\right)v \\ &= \sum_{g\in G}(a_g+b_g)T_g(v) \\ &= \sum_{g\in G}a_gT_g(v)+\sum_{g\in G}b_gT_g(v) \\ &= \alpha v+\beta v.\end{aligned}$$

2. Distributividad de la suma de elementos del módulo respecto al producto por escalar

$$\begin{aligned}\alpha(v+w) &= \left(\sum_{g\in G}a_gg(v+w)\right) \\ &= \sum_{g\in G}a_gT_g(v+w) \\ &= \sum_{g\in G}a_gT_g(v)+\sum_{g\in G}a_gT_g(w) \\ &= \alpha v+\alpha w.\end{aligned}$$

3. Para la asociatividad, por un lado se tiene

$$\begin{aligned}\alpha(\beta v) &= \left(\sum_{h\in G}a(g)h\right)\left(\sum_{g\in G}b(g)T_g(v)\right) \\ &= \sum_{h\in G}a(h)T_h\left(\sum_{g\in G}b(g)T_g(v)\right) \\ &= \sum_{h,g\in G}a(h)b(g)T_{hg}(v).\end{aligned}$$

Por otro lado se tiene

$$\begin{aligned}(\alpha\beta)v &= \left(\sum_{h,g\in G} a(h)b(g)hg\right)(v)\\ &= \sum_{h,g\in G} a(h)b(g)T_{hg}(v)\end{aligned}$$

con lo que se comprueba que $\alpha(\beta v) = (\alpha\beta)v$.

4. Considérese $\alpha = 1_G$, entonces

$$\begin{aligned}\alpha v &= T_{1_G}(v)\\ &= I(v)\\ &= v.\end{aligned}$$

Por lo expuesto anteriormente es fácil notar que la multiplicación por escalar definida en la ecuación 3.1 induce un RG-módulo.

Al converso, si M es un RG-módulo de rango finito sobre R, se define la representación de G sobre R asignando a cada elemento $g \in G$ el R-automorfismo $T_g \colon M \to M$ dado por $T_g(m) = gm$.

Nótese que dado $T \colon G \to GL(V)$ una representación de G sobre R y M su RG-módulo inducido, se tiene que S, la representación inducida por M, es tal que $S_g(m) = gm = \alpha m \simeq T_g(m)$, donde α es la imagen de la inmersión de G en RG dada en el teorema 1.

De manera similar, dado M un RG-módulo y $S \colon G \to GL(M)$ su representación inducida, entonces su RG-módulo inducido por la ecuación 3.1 deja invariante a M. Por lo tanto se ha demostrado que las aplicaciones construidas anteriormente son inversas la una de la otra. □

Como ejemplo considérese un grupo finito G y RG como un módulo sobre

sí mismo, de esta forma RG es de rango finito $|G|$ sobre R. Entonces, dado un elemento $x \in G$, la representación $T_x \colon RG \to RG$ viene dada por:

$$T_x \left(\sum_{g \in G} a(g)g \right) = x \left(\sum_{g \in G} a(g)g \right) = \left(\sum_{g \in G} a(g)gxg \right).$$

Esto significa que $x \in G$ actúa en los elementos de la base $G = \{g_1, \ldots, g_n\}$ multiplicándolos por la izquierda. En otras palabras, la representación asociada al RG-módulo RG es precisamente la representación regular de G.

Lema 9. *Sea $T \colon G \to GL(V)$ una representación de un grupo G sobre un campo K, con espacio de representación V, entonces un subespacio $W \subset V$ es invariante bajo T si y sólo si W es un KG-módulo de V.*

Demostración. Se procede a demostrar este hecho en dos partes:

1. Sea $W \subset V$ invariante bajo T, entonces $T_g(W) = W$ para cualquier $g \in G$. Sean $w_1, w_2 \in W$ se tiene que $T_g(w_1 + w_2) = T_g(w_1) + T_g(w_2) \in W$, así $T_g^{-1}(T_g(w_1 + w_2)) \in W$. Por otra parte, si se considera $\alpha = \sum_{g \in G} a(g)g$ entonces $\alpha w = \sum_{g \in G} a(g) T_g(w) \in W$ y por lo tanto W es un KG-módulo de V.

2. Sea W subespacio de V, $W \subset V$ y W un KG-módulo de V, entonces para $w \in W$ y $g \in RG$ se tiene $gw = 1 \cdot T_g(w) \in W$. □

Teorema 9. *Sea G un grupo y K un campo. Entonces:*

1. *Dos representaciones T y T' de G sobre R son equivalentes si y sólo si los correspondientes RG-módulos son isomorfos.*

2. *Una representación es irreducible (o completamente reducible) si y sólo si el correspondiente RG-módulo es irreducible (o completamente reducible).*

Demostración. Se procede a demostrar este lema por incisos:

1. Supóngase que T y T' son representaciones de G sobre K equivalentes, entonces existe $\phi\colon V \to W$ isomorfismo, donde V y W son los espacios de representación de T y T' respectivamente, tal que $T'_g = \phi T_g \phi^{-1}$ para cualquier $g \in G$. Entonces se probará que ϕ es isomorfismo de RG-módulos también. En efecto

$$\begin{aligned}
\phi(\alpha v) &= \phi\left(\sum_{g\in G} a(g)T_g(v)\right) \\
&= \sum_{g\in G} a(g)\phi(T_g(v)) \\
&= \sum_{g\in G} a(g)T'_g(\phi(v)) \\
&= \alpha\phi(v).
\end{aligned}$$

2. Supóngase que M y N son RG-módulos isomorfos, entonces existe $f\colon M \to N$ isomorfismo de RG-módulos. Sean T y T' las representaciones inducidas por M y N respectivamente, entonces:

$$\begin{aligned}
(fT_g f^{-1})(n) &= f\left(T_g\left(f^{-1}(n)\right)\right) \\
&= f\left(gf^{-1}(n)\right) \\
&= gf\left(f^{-1}(n)\right) \\
&= gn \\
&= T'_g(n)
\end{aligned}$$

   con lo que se comprueba que T y T' son equivalentes.

3. Si una representación T es irreducible, entonces los únicos subespacios de V que son invariantes bajo T son los triviales y ,por el lema anterior, los únicos submódulos de M, el módulo inducido por T, son los los triviales. De manera análoga se puede demostrar el converso. □

También es posible notar que si un RG-módulo M admite una descomposición como suma directa de submódulos $M = \oplus_{i=1}^{t} M_i$ y si T y T_i denota las representaciones correspondientes a estos módulos, entonces $T = \oplus_{i=1}^{t} T_i$.

En lo que sigue, se mostrará como la información que ya se conoce a cerca de los grupo-anillos se puede trasladar a términos de representaciones de grupos.

El lector deberá recordar que en el corolario 4, como consecuencia directa del teorema de Masckes, se demostró que si K es un campo tal que $\text{car}(K) \nmid |G|$, entonces KG es un anillo semisimple. Además, se demostró en el teorema [4] que en este caso todo KGmódulo es simple. Por lo tanto, en particular, se sigue inmediatamente que todo KGmódulo finito dimensional sobre K se puede escribir como suma directa de módulos irreducibles.

En términos de representaciones, esto significa que bajo estas condiciones, toda representación de G sobre K es la suma directa de representaciones irreducibles. Así, para determinar todas las representaciones de G sobre K, mediante equivalencia, es suficiente determinar todos los KGmódulos irreducibles, salvo isomorfismos.

Ahora, es necesario hacer uso del teorema de Wedderburn-Artin aplicado a grupo-anillos (teorema 7), el cual establece que el número de KG-módulos irreducibles que no son isomorfos entre sí, es precisamente el número de componentes simples de KG y estas están determinadas exclusivamente por la estructura de KG. En particular, es importante recordar que si se escribe KG en la forma

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

donde $D_i, 1 \leq i \leq r$, son anillos de división que contienen a K en sus centros, y si se calcula la dimensión en ambos lados de la ecuación, se tiene

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K].$$

[4] poner teorema en el cap 1 y hacer referencia

Por otro lado, se sabe que el módulo irreducible I_i correspondiente a la componente simple $M_{n_i}(D_i)$ es isomorfo a $D_i^{n_i}$. Como el grado de la correspondiente representación T_i viene dado por la dimensión de este módulo sobre K, se obtiene que

$$\deg(T_i) = [D_i^{n_i} : K] = n_i[D_i : K]$$

así, se puede escribir

$$|G| = \sum_{i=1}^{r} n_i \deg(T_i).$$

Ejemplo 14. Se mostró en el ejemplo 1 que si $G =< a >$ denota al grupo cíclico de orden siete, entonces

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta),$$

donde ζ denota una raíz primitiva de la unidad de orden siete. De lo anterior, las componentes simples de $\mathbb{Q}G$ son anillos de matrices de 1×1 sobre los anillos $\mathbb{Q}$ y $\mathbb{Q}(\zeta)$ respectivamente y por ende existen solamente dos representaciones irreducibles que no son equivalentes, S y T de G sobre $\mathbb{Q}$, con grados

$$\deg(S) = [\mathbb{Q} : \mathbb{Q}] = 1, \quad \deg(T) = [\mathbb{Q} : \mathbb{Q}] = 6.$$

Como las representaciones 1-dimensionales son equivalentes si y sólo si son iguales y como cualquier grupo admite la representación trivial $S\colon G \to GL(1, \mathbb{Q})$ dada por $S_g = 1$, para cada $g \in G$, entonces la representación 1-dimensional de G sobre $\mathbb{Q}$ es la trivial.

Para determinar T_a, de acuerdo a las consideraciones anteriores, se debe considerar el $\mathbb{Q}G$módulos irreducible $I_2 = D_2^{n_2}$ correspondiente a la segunda componente simple de $\mathbb{Q}$. Entonces, la representación $T\colon G \to GL(I_2)$ está dada por $T_a(v) = av$, para cada $v \in I_2$. En este caso, $n_2 = 1$ y $D_2 = \mathbb{Q}(\zeta)$, así que $I_2 = \mathbb{Q}(\zeta)$, donde la multiplicación por un elemento $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Q}G$ está dada por $\alpha v = \alpha_2 v$, para todo $v \in \mathbb{Q}(\zeta)$. Recordando que el elemento $a \in \mathbb{Q}(\zeta)$ le corresponde, vía isomorfismo,

el elemento $(1, \zeta) \in \mathbb{Q} \oplus \mathbb{Q}(\zeta)$ se tiene

$$T_a(v) = av = \zeta v, \quad v \in \mathbb{Q}(\zeta).$$

Por lo tanto, si se toma $\{1, \zeta, \zeta^2, \ldots, \zeta^5\}$ como una base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$, entonces la correspondiente matriz está dada por

$$\mathsf{A}(\mathsf{a}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

Ejemplo 15 (Representaciones del grupo diédrico de orden ocho.)**.** Se ha probado en ele ejemplo 11 que el grupo D_4 admite cuatro representaciones distintas de grado uno y una representación W de grado dos sobre $\mathbb{Q}$, por lo tanto existen cuatro componentes simples isomorfas a $\mathbb{Q}$. Sean $M_n(D)$ la componente simple correspondiente a la representación de grado dos. Como $2 = \deg(W) = n[D : \mathbb{Q}]$, entonces $n = 1$ y $[D : \mathbb{Q}]$ o $n = 2$ y $[D : \mathbb{Q}] = 1$.

Para el primer caso, se puede observar que $\mathbb{Q}D_4$ debe ser de la forma

$$\mathbb{Q}D_4 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus D \oplus D',$$

donde D' es una anillo de división con $[D' : \mathbb{Q}] = 2$. Es fácil notar que un anillo de división de dimensión dos sobre un campo tiene que ser conmutativo, entonces $\mathbb{Q}D_4$ es conmutativo, lo cual es una contradicción, ya que D_4 no es abeliano.

En consecuencia, se debe tener que $n = 2$ y $D = \mathbb{Q}$. De esta forma

$$\mathbb{Q}D_4 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}).$$

4. ELEMENTOS ALGEBRAICOS

4.1. Generalidades y definiciones

En este capítulo será de especial interés estudiar algunos elementos algebraicos en grupo-álgebras usando la representación regular que puede ser definida para un álgebra finito dimensional con unidad sobre un campo K de la siguiente manera.

Definición 15. *Sea* $T\colon A \to Hom_k(A,A)$ *tal que* $a \mapsto T_a \in Hom_k(A,A)$*, definida mediante multiplicación por la izquierda por* a*. Esto es,* T_a *es una aplicación tal que* $T_a(x) = ax$*, para cualquier* $x \in A$*.*

Se puede observar a partir de la definición que

$$\begin{aligned} T_{a+b} &= T_a + T_b \\ T_{ab} &= T_a T_b \\ T_{ka} &= kT_a \end{aligned}$$

para todo $a, b \in A$, $k \in K$. Mas aún, la aplicación $a \mapsto T_a$ es inyectiva debido a que $T_a(1) = a$. Eligiendo una base $\{a_1, \ldots, a_n\}$ de A sobre K se puede representar a T_a con una matriz $\rho(a)$, con lo que se obtiene la representación matricial:

$$a \mapsto \rho(a) \in M_n(K).$$

Si a es un elemento algebraico de A, esto es, si existe un polinomio no nulo $f(X) \in K[X]$ tal que $f(a) = 0$, entonces los valores propios de la matriz $\rho(a)$ también anulan a $f(X)$, debido al teorema de Cayley-Hamilton (véase [5–p 241]). De esta manera, por ejemplo, si a es un elemento nilpotente entonces los valores propios de $\rho(a)$ son todos cero. Si a es de orden multiplicativo finito, es decir, si $a^m = 1$ para algún m entero positivo, entonces los valores propios de $\rho(a)$ son raíces de la unidad de orden m.

Lema 10. *Sea G un grupo finito y K un campo. Sea p la representación regular de KG y $\gamma = \sum_{g\in G}\gamma(g)g \in KG$. Entonces la traza de $\rho(\gamma)$ viene dada por*

$$tr\rho(\gamma) = |G|\gamma(1).$$

Demostración. Se sabe que $tr\rho(\gamma)$ es independiente de la base elegida, así que se elige $G = \{g_1, \ldots, g_n\}$ como K-base para KG y se asume que $g_1 = 1$. Entonces

$$\rho(\gamma) = \rho\left(\sum_{g\in G}\gamma(g)g\right) = \sum_{g\in G}\gamma(g)\rho(g).$$

Para un elemento $g \neq 1 \in G$, se tiene $gg_i \neq g_i$, para $1 \leq i \leq n$, de donde se sigue que los elementos de la diagonal de la matriz $\rho(g)$ son todos nulos si $g \neq 1$. Así $\operatorname{tr}\rho(g) = 0$ si $g \neq 1$. Más aún, como $\rho(1)$ es la matriz identidad, se tiene que $\operatorname{tr}\rho(1) = n$. Entonces

$$\operatorname{tr}\rho(\gamma) = \sum_{g\in G}\gamma(g)\operatorname{tr}(g) = \gamma(1)\operatorname{tr}\rho(1) = \gamma(1)|G|.$$

□

Lema 11. *Sea $\gamma = \sum_{g\in G}\gamma(g)g$ una unidad de orden finito en el grupo-anillo integral $\mathbb{Z}G$ con G un grupo finito y asúmase que $\gamma(1) \neq 0$. Entonces $\gamma = \gamma(1) = \pm 1$.*

Demostración. Sea $|G| = n$ y supóngase que $\gamma^m = 1$ para algún entero positivo m. Si se considera la representación regular ρ del grupo-álgebra $\mathbb{C}G$ y a $\mathbb{Z}G$ como un subanillo de la misma, se tiene que $\operatorname{tr}\rho(\gamma) = n\gamma(1)$. Como $\gamma^m = 1$, entonces $(\rho(\gamma))^m = \rho(\gamma^m) = I$, de esto se sigue que $\rho(\gamma)$ es raíz del polinomio $X^m - 1$, cuyas raíces son todas distintas. Esto implica, por el teorema espectral(véase [5–p 214]) que existe una base de $\mathbb{C}G$ donde la matriz de $\rho(\gamma)$ es diagonal de la forma

$$\mathbb{A} = \begin{pmatrix} \xi_1 & & & \\ & \xi_2 & & \\ & & \ddots & \\ & & & \xi_n \end{pmatrix}, \quad \xi_i^m = 1.$$

Entonces $\operatorname{tr}\rho(\gamma) = \sum_{i=1}^{n} \xi_i$ y así

$$n\gamma(1) = \sum_{i=1}^{n} \xi_i.$$

Por lo tanto, aplicando valor absoluto,

$$\mid n\gamma(1) \mid = \left| \sum_{i=1}^{n} \xi_i \right| \leq \sum_{i=1}^{n} \mid \xi \mid = n.$$

Como $\mid n\gamma(1) \mid = n \mid \gamma(1) \mid \leq n$, entonces $\mid \gamma(1) \mid = 1$ y $|\sum_{i=1}^{n} \xi_i| = \sum_{i=1}^{n} \mid \xi_i \mid$, lo cual sucede si y sólo si $\xi_1 = \xi_2 = \cdots = \xi_n$.

Así $n\gamma(1) = n\xi_1$ y $\gamma(1) = \xi_1 = \pm 1$. Se concluye que $\rho(\gamma) = \pm I$, de donde, $\gamma = \pm 1$. □

Corolario 6. *Supóngase que $\gamma = \sum_{g\in G} \gamma(g)g$ es una unidad central en el grupo-anillo integral $\mathbb{Z}G$ con G un grupo finito de orden finito. Entonces γ es de la forma $\gamma = \pm g$ con $g \in \mathcal{Z}(G)$.*

Demostración. Sea $\gamma = \sum_{g\in G} \gamma(g)g$ una unidad central de orden m. Supóngase que $\gamma(g_0) \neq 0$, para algún $g_0 \in G$. Entonces γg_0^{-1} es también una unidad de orden finito en $\mathbb{Z}G$. Mas aún, el coeficiente de 1 en la expresión de γg_0^{-1} es $\gamma(g_0) \neq 0$, de donde $\gamma g_0^{-1} = \pm 1$ y por lo tanto $\gamma = \pm g_0$. □

Una consecuencia inmediata del corolario anterior es el siguiente

Teorema 10. *Sea A un grupo abeliano finito. Entonces, el grupo de torsión de las unidades del grupo-anillo integral $\mathbb{Z}A$ es igual $\pm A$.*

Ahora se desea hacer un estudio de los elementos idempotentes. Es evidente que en cualquier anillo con unidad el 0 y el 1 son elementos idempotentes. Estos elementos son llamados **idempotentes triviales** de un anillo. Se verá a continuación que los elementos idempotentes e en un grupo-álgebra están fuertemente influenciados por

su primer coeficiente $e(1)$.

Teorema 11. *Sea G un grupo finito y K un campo de característica cero. Supóngase que $e \in KG$ y e es idempotente. Entonces:*

1. $e(1) \in \mathbb{Q}$

2. $0 \leq e(1) \leq 1$

3. $e(1) = 0 \Leftrightarrow e = 0$ *y* $e(1) = 1 \Leftrightarrow e = 1$.

Demostración. Considérese la representación regular de KG escrita con respecto a la base G de KG. Entonces, por el lema 10, se tiene que $\operatorname{tr} \rho = \mid G \mid e(1)$. Más aún, como $e^2 = e$, $\rho(e)$ satisface el polinomio $X^2 - X = X(X-1)$ y por lo tanto $\rho(e)$ puede ser diagonalizada. Los valores propios de $\rho(e)$ son 0 o 1 ya que $\rho(e)$ es idempotente. Debido a que la traza es la suma de los valores propios, se tiene que $\operatorname{tr} \rho(e) = r$, donde r es el número de valores propios iguales a 1 y por lo tanto también es el rango de $\rho(e)$. Se concluye entonces que $0 \leq e(1) \leq 1$.

Nótese que $e(1) = 0$ si y sólo si el rango de $\rho(e)$ es 0 y eso pasa sólo si $e = 0$. Similarmente $e(1) = 1$ si y sólo si el rango de $\rho(e)$ es $\mid G \mid$, lo cual pasa sólo si $\rho(e)$ es la matriz identidad, es decir, si $e = 1$. □

4.2. Elementos Idempotentes

Se ha demostrado en el teorema 11 que si K es un campo de característica cero y G es un grupo finito, entonces cualquier elemento idempotente $e \in KG$ cumple que $e(1) \in \mathbb{Q}$. Se dará, en esta sección, un resultado análogo a este resultado, donde K tiene característica $p > 0$.

Teorema 12. *Sea K un campo de característica $p > 0$ y sea G cualquier grupo.*

Supóngase que $e \in KG$ es un idempotente. Entonces $e(1) \in F_p$, donde F_p es el subcampo primo de K.

La demostración de este resultado está fuera del alcance de este trabajo, pero se recomienda al lector consultar [6].

En el teorema 11 se demostró el teorema anterior cuando la característica del campo es cero con la condición de que el grupo sea finito, pero dicho resultado es válido aún cuando el grupo es infinito, pero su demostración requiere el uso de resultados previos de teoría de números. Para la demostración del siguiente resultado, se sugiere al lector consultar [6]

Teorema 13. *Sea G un grupo cualquiera y K un campo de característica cero. Supóngase que $e = e^2 = \sum e(g)g \in KG$. Entonces:*

1. $e(1) \in \mathbb{Q}$

2. $0 \leq e(1) \leq 1$

3. $e(1) = 0 \Leftrightarrow e = 0$ *y* $e(1) = 1 \Leftrightarrow e = 1$.

Supóngase que $e = e^2 \in \mathbb{Z}G$, como $e(1)$ es un entero, se sigue del teorema anterior que $e = 0$ o $e = 1$. Así, se obtiene el siguiente

Corolario 7. *El grupo-anillo integral $\mathbb{Z}G$ sólo contiene idempotentes triviales, para cualquier grupo G.*

4.3. Unidades de Torsión

Se demostró en el lema 11 que si G es un grupo finito, $\gamma \in \mathbb{Z}G$ es una unidad de orden finito y $\gamma(1) \neq 0$ entonces $\gamma = \pm 1$.Dicho resultado es válido también cuando

G es un grupo infinito.

Teorema 14. *Sea* $\gamma = \sum \gamma(g)g \in \mathbb{Z}G$ *que satisface* $\gamma^n = 1$, *para algún entero positivo* n. *Si* $\gamma(1) \neq 0$ *entonces* $\gamma = \pm 1$.

Demostración. Sea $\mathbb{C}[X]$ el anillo de polinomios con coeficientes en $\mathbb{C}$. Considérese el homomorfismo $\phi\colon \mathbb{C}[X] \to \mathbb{C}[\gamma]$ dada por $X \mapsto \gamma$. El kernel de este homomorfismo es el ideal $<f(X)>$ generado por el polinomio minimal $f(X)$ de γ. Entonces $f(X)$ divide a $X^n - 1$ y por lo tanto tiene sus raíces distintas. Así, se tiene

$$\mathbb{C}[\gamma] \simeq \frac{\mathbb{C}[X]}{<f(X)>} \simeq \mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C} \simeq \oplus_i \mathbb{C}e_i,$$

donde los e_i son idempotentes ortogonales primitivos de $\mathbb{C}[\gamma]$. De lo anterior, se puede escribir $\gamma = \sum_i \xi_i e_i$ donde $\xi_i \in \mathbb{C}$, $\xi_i^n = 1$ y $e_i e_j = \delta_{ij} e_j$, con δ_{ij} la función delta de Kronecker.

Calculando el primer coeficiente en ambos lados de la ecuación y usando el teorema 13 se obtiene

$$\gamma(1) = \sum \xi_i e_i(1) = \sum \xi_i \frac{r_i}{s}, \quad \text{con } r_i, s \in \mathbb{Z}, \quad r_i, s \geq 0.$$

Entonces, $s\gamma(1) = \sum \xi_i r_i$. De igual manera; como $\sum e_i = 1$ se tiene que $1 = \sum \frac{r_i}{s}$, así $\sum r_i = s$. De donde

$$\mid s\gamma(1) \mid = \left| \sum \xi_i r_i \right| \leq \sum \mid \xi \mid\mid r_i \mid = \sum \mid r_i \mid = s.$$

Como $\mid s\gamma(1) \mid \leq s$, se tiene $\mid \gamma(1) \mid = 1$ y también $|\sum \xi_i r_i| = \sum \mid \xi_i \mid\mid r_i \mid$. Se sigue que todos los ξ_i son iguales y $\gamma = \sum \xi_1 e_1 = \xi_1 = \gamma(1) \in \mathbb{Z}$. □

Este último resultado tiene bastantes consecuencias útiles. El lector deberá recordar que, como se mostró en la preposición 4, hay una involución estándar en $\mathbb{Z}G$ dada por

$$\gamma = \sum \gamma(g)g \mapsto \gamma* = \sum \gamma(g)g^{-1},$$

tal que

$$\begin{aligned}(\gamma^*)^* &= \gamma \\ (\gamma+\mu)^* &= \gamma^*+\mu^* \\ (\gamma\mu)^* &= \mu^*\gamma^* \\ (c\gamma)^* &= c\gamma^*,\end{aligned}$$

para todo $\gamma, \mu \in \mathbb{Z}G$ y $c \in \mathbb{Z}$. Más aún,

$$(\gamma\gamma^*)(1) = \sum(\gamma(g))^2$$

lo cual implica que $\gamma\gamma^* = 0$ si y sólo si $\gamma = 0$.

Corolario 8. *Supóngase que $\gamma \in \mathbb{Z}G$ tiene la propiedad de conmutar con γ^*. Si γ es una unidad central de orden finito, entonces $\gamma = \pm g_0$ para algún $g_0 \in G$.*

Demostración. Por hipótesis $\gamma^n = 1$ para algún entero positivo n y $\gamma\gamma^* = \gamma^*\gamma$, por lo tanto $(\gamma\gamma^*) = 1$. Más aún, $(\gamma\gamma^*)(1) = \sum\gamma(g)^2 \neq 0$. Entonces, por el teorema anterior, $\gamma\gamma^* = 1$. De esta manera, existe un único coeficiente $\gamma(g_0)$ que es distinto de cero. Se concluye entonces que $\gamma = \pm g_0$. □

Como consecuencia inmediata se tiene

Corolario 9. *Todas las unidades centrales de orden finito en $\mathbb{Z}G$ son triviales.*

Corolario 10. *Si A es un grupo abeliano cualquiera, entonces todas las unidades de torsión de $\mathbb{Z}A$ son triviales.*

4.4. Elementos nilpotentes

Ahora se desea clasificar los grupo-álgebras KG de un grupo finito G sobre un anillo K tal que KG no tiene elementos nilpotentes no triviales. Es posible observar

que si $\text{car}(K) = p > 0$ y G contiene un elemento g tal que $g^{p^n} = 1$ para algún entero positivo n, entonces $(g-1)^{p^n} = g^{p^n} - 1 = 0$. De esto se sigue el resultado

Proposición 9. *Si K es un campo de característica $p > 0$ y G contiene p-elementos, entonces KG contiene elementos nilpotentes.*

A partir de este punto se asumirá que G es finito, $p \leq 0$ y que si $p > 0$ entonces G no tiene p-elementos. Supóngase que KG no contiene elementos nilpotentes a excepción de los triviales y sea $e \in KG$ un idempotente. Entonces, para cada $x \in KG$, el idempotente $\eta = ex(1-e)$ satisface $\eta^2 = 0$ y por lo tanto $ex = exe$. Similarmente si $\eta = (1-e)xe$ entonces $\eta^2 = 0$ y $xe = exe$, con lo que se comprueba que e es central. Ahora para cualquier $g \in G$, el elemento $e = \frac{\hat{g}}{\circ(g)} = \frac{\sum_{i=1}^{\circ(g)} g^i}{\circ(g)}$ es idempotente y por lo tanto es central. Esto significa que el subgrupo $<g>$ es normal para cualquier $g \in G$. Se sigue del teorema [1] que G es abeliano o hamiltoneano.

En el caso que G sea hamiltoneano, $G = K_8 \times E \times A$, donde K_8 es el grupo de cuaterniones de orden ocho, $E^2 = 1$ y A es un grupo abeliano de orden impar. Para obtener más información de este caso es necesario hacer un estudio mas profundo del grupo-álgebra FK_8, donde F es un campo.

Proposición 10. *Sea K un campo de característica $p \geq 0$ y sea G un grupo finito. Si KG no tiene elementos nilpotentes entonces todos los idempotentes de KG son centrales y G es abeliano o Hamiltoniano.*

En lo que sigue el lector deberá recordar el concepto de números cuaterniones. Los números cuaterniones, con coeficientes racionales, se escriben como sumas directas de espacios vectoriales:

$$H_{\mathbb{Q}} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

con su ya conocida multiplicación (véase [9–p. 31]). Se puede definir formalmente

[1] poner el teorema en el capítulo 1 que sustenta esta parte y luego hacer referencia

una estructura similar sobre cualquier campo F. Considérese el espacio vectorial

$$H(F) = F \oplus Fi \oplus Fj \oplus Fk$$

y defínase la multiplicación distributivamente con $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$ y $ki = j = -ik$. De esta forma $H(F)$ es un anillo no conmutativo.

Para un elemento $\alpha = a + bi + cj + dk \in H(F)$ se define:

$$\overline{\alpha} = a - bi - cj - dk$$

y

$$\alpha' = a - bi + cj + dk.$$

Luego de hacer algunos cálculos sencillos se obtiene

Lema 12. *1.* $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$

2. $\alpha'\alpha = (a^2 + b^2 - c^2 - d^2) + (2ac + 2bd)j + (2ad - 2bc)k$

Al escalar $N(\alpha) := \alpha\overline{\alpha}$ *se le llama la norma de* α.

Proposición 11. *El álgebra de los cuaterniones* $H(F)$ *tiene divisores de cero si y sólo si la ecuación* $X^2 + Y^2 = -1$ *tiene solución en* F.

Demostración. Supóngase que existen elementos $a, b \in F$ tal que $a^2 + b^2 = -1$. Entonces, para $\alpha = a + bi + j$ se tiene $N(\alpha) = \alpha\overline{\gamma} = 0$; α es divisor de cero en $H(F)$.

Falta demostrar que si $H(F)$ tiene divisores de cero, entonces la ecuación $X^2 + Y^2 = -1$ tiene soluciones en F. Cuando F es de característica dos se tiene $1+0 = -1$ entonces se asumirá que $\text{car}(F) \neq 2$. Supóngase que existen elementos $\alpha = a + bi + cj + dk \neq 0$ y $\beta \neq 0 \in H(F)$ tal que $\alpha\beta = 0$. Entonces, $\overline{\alpha}\alpha\beta = N(\alpha)\beta = 0$ de donde $N(\alpha) = a^2 + b^2 + c^2 + d^2 = 0$. Si alguno de los coeficientes de α es cero, se tiene que la ecuación $X^2 + Y^2 = -1$ solución en F. Si, por el contrario, todos los coeficientes

de α son distintos de cero se puede considerar $\alpha'\alpha\beta = 0$ y del lema 12 se sabe que $\gamma = \alpha'\alpha$ a lo sumo tiene tres coeficientes no nulos y por lo tanto $N(\gamma)\beta = 0$ implica que $X^2 + Y^2 = -1$ tiene solución en F. Por último falta considerar el caso en que $\gamma = 0$, en cuyo caso se tiene, por el lema 12, que $a^2 + b^2 - c^2 - d^2 = 0$ y de $N(\alpha) = 0$ se sigue que $a^2 + b^2 + c^2 + d^2 = 0$ entonces $a^2 + b^2 = 0$, de donde $\left(\frac{a}{b}\right)^2 + 0 = -1$. □

Este resultado se puede ampliar de la siguiente manera.

Proposición 12. *Las siguientes proposiciones son equivalentes:*

1. *El álgebra de los cuaterniones $H(F)$ no tiene divisores de cero*

2. *La ecuación $X^2 + Y^2 = -1$ no tiene solución en F*

3. *$H(F)$ es un anillo de división*

Demostración. Para la demostración de esta proposición solo falta probar que si $H(F)$ no tiene divisores de cero entonces es un anillo de división. Sea $0 \neq \alpha \in H(F)$ entonces $\overline{\alpha}\alpha = N(\alpha) \neq 0$ y por lo tanto $\alpha\left(\frac{\overline{\alpha}}{N(\alpha)} = 1\right)$. □

Teorema 15. *Supóngase que* $\text{car}(F) \neq 2$. *Entonces el álgebra de los cuaterniones $H(F)$ es un anillo de división o isomorfo a $M_2(F)$, el anillo de matrices de 2×2 sobre el campo F. La última opción sucede únicamente si $X^2 + Y^2 = -1$ tiene solución en F.*

Demostración. Se debe demostrar que si $H(F)$ no es un anillo de división entonces es isomorfo a $M_2(F)$. En efecto, supóngase que existen $x, y \in F$ tal que $x^2 + y^2 = -1$.

Considérese la aplicación $\theta\colon H(F) \to M_2(F)$ dada por:

$$\begin{aligned}
\theta(i) &= \begin{pmatrix} x & y \\ y & -x \end{pmatrix} \\
\theta(j) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
\theta(k) &= \begin{pmatrix} -y & x \\ x & y \end{pmatrix} \\
\theta(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

□

y por extensión lineal en F. Para demostrar que θ es biyectiva, basta demostrar que las cuatro matrices dadas anteriormente son linealmente independientes en F, es decir, si existen $a, b, c, d \in F$ tal que

$$a\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + b\begin{pmatrix} x & y \\ y & -x \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} -y & x \\ x & y \end{pmatrix} = 0$$

entonces $a = b = c = d = 0$. En efecto, de la ecuación anterior se obtiene

$$\begin{aligned}
a + bx - dy &= 0 \\
by + c + dx &= 0 \\
by - c + dx &= 0 \\
a - bx + dy &= 0
\end{aligned}$$

un sistema de ecuaciones en a, b, c, d don determinante $4(x^2 + y^2) \neq 0$, entonces la única solución de dicho sistema es la trivial, de donde $H(F) \simeq M_2(F)$.

Por lo expuesto en esta sección, el lector podrá intuir que es esencial poder trabajar con álgebras de cuaterniones sobre campos ciclótomicos de la forma $F = \mathbb{Q}(\xi)$, donde ξ es una raíz primitiva de la unidad.

Teorema 16. *Sea $F = \mathbb{Q}(\xi_m)$ un campo ciclotómico, con ξ_m una raíz primitiva de la unidad de orden m, donde m es un entero impar mayor que 1. Entonces, la ecuación $X^2 + Y^2 = -1$ tiene solución en F si y sólo si el orden multiplicativo de 2 módulo m es par.*

Para la demostración de dicho teorema y una lectura más profunda de este tema el lector puede consultar [7]. Como consecuencia de este teorema se tiene

Lema 13. *Sea $F = \mathbb{Q}(\xi_m)$ como en el teorema anterior. Entonces $H(F)$ tiene divisores de cero si y sólo si el orden multiplicativo de 2 módulo m es par.*

Ahora se describe la estructura algebraica del grupo-álgebra $F(K_8)$.

Lema 14. *Sea F un campo de característica distinta de 2. Entonces,*

$$FK_8 \simeq 4F \oplus H(F).$$

Demostración. Se escribe K_8 como

$$K_8 = <a, b\colon a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1}>$$

y del hecho que $\overline{K_8} = \frac{K_8}{K_8'}$ [2] es el grupo de Klein de cuatro elementos se tiene

$$F\overline{K_8} \simeq F \oplus F \oplus F \oplus F.$$

Por otro lado, como existe $\phi\colon FK_8 \to H(F)$ endomorfismo dada por $a \mapsto i$, $b \mapsto j$, se sigue que $H(F)$ es isomorfo a algún sumando simple de FK_8 y contando las dimensiones se obtiene el resultado. □

Ahora se tiene la capacidad de clasificar las grupo-álgebras FG con la propiedad que FG no contenga elementos nilpotentes.

[2] dar referencia al capítulo 1

Teorema 17. *Sea F un campo de característica $p > 0$ y sea G un grupo finito. Entonces FG no tiene elementos nilpotentes si y sólo si G es un p'-grupo abeliano.*

Demostración. Supóngase que FG no tiene elementos nilpotentes. Entonces de las proposiciones 9 y 10 se tiene que G es un p'-grupo y que G es abeliano o Hamiltoniano. Supóngase que G es hamiltoneano. Entonces $p \neq 2$.Más aún, siempre se puede resolver $X^2 + Y^2 = -1$ en un campo con p elementos (y por lo tanto también en F). Entonces FK_8 tiene elementos nilpotentes por el teorema 15 y el lema 14. Así, G debe ser abeliano. Para el converso basta notar que FG, siendo semisimple y conmutativo, es suma directa de campos. □

Existen caracterización cuando el campo tiene característica cero, a continuación se presentan los resultados sin su demostración, pero se recomienda al lector consultar [8].

Teorema 18. *Sea G un grupo finito de orden $2^k m$ con $(2, m) = 1$. Entonces $\mathbb{Q}G$ no tiene elementos nilpotentes si y sólo si G es abeliano o Hamiltoniano con la propiedad de que el orden de 2 módulo m sea impar.*

Teorema 19. *Sea G un grupo nilpotente finitamente generado. El grupo-anillo $\mathbb{Z}G$ no tiene elementos nilpotentes si y sólo si cada subgrupo finito de G es normal y sucede alguna de las siguientes:*

1. *$T(G)$, el conjunto de los elementos de torsión de G, es un subgrupo abeliano*

2. *$T(G) = K_8 \times E \times A$, donde E es un 2-grupo elemental abeliano y A es un grupo abeliano de orden impar m tal que el orden multiplicativo de 2 módulo m es impar.*

5. UNIDADES DE LOS GRUPO-ANILLOS

5.1. Algunas formas de construir unidades

Sea R un anillo. Se entiende por $\mathcal{U}(R) = \{x \in R \colon (\exists y \in R)xy = yx = 1\}$. En particular, dado un grupo G y un anillo R, $\mathcal{U}(RG)$ denota al grupo de unidades del grupo-anillo RG. Como la función de aumento $\mathcal{E} \colon RG \to R$, dada por $\mathcal{E}\left(\sum a(g)g\right) = \sum a(g)$, es un homomorfismo de anillos, se tiene que $\mathcal{E}(u) \in \mathcal{U}(R)$, para todo $u \in \mathcal{U}(RG)$. Se denotará como $\mathcal{U}_1(RG)$ el subgrupo de unidades de aumento 1 en $\mathcal{U}(RG)$, a saber

$$\mathcal{U}_1(RG) = \{u \in \mathcal{U}(RG) \colon \mathcal{E}(u) = 1\}.$$

Para una unidad u del grupo-anillo integral $\mathbb{Z}G$ se tiene que $\mathcal{E}(u) = \pm 1$, entonces es claro que

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

De la misma manera, para un anillo R arbitrario se tiene que

$$\mathcal{U}(RG) = \mathcal{U}(R) \times \mathcal{U}_1(RG).$$

No se conocen muchas formas para construir unidades. La mayoría de las construcciones conocidas son antiguas y elementales. A lo largo de este capítulo, se mostrará y describirá algunas de estas construcciones, donde se trabajará principalmente con grupo-álgebras KG sobre un campo K y con el grupo-anillo integral $\mathbb{Z}G$.

Ejemplo 16 (Unidades Triviales)**.** Un elemento de la forma rg, donde $r \in \mathcal{U}(R)$ y $g \in G$, tiene inversa $r^{-1}g^{-1}$. Los elementos de esta forma son llamados **unidades triviales** de RG. De esta manera, por ejemplo, los elementos $\pm g, g \in G$ son las unidades triviales del grupo-anillo integral $\mathbb{Z}G$. Si K es un campo, entonces las unidades triviales de KG son los elementos de la forma $kg, k \in K, k \neq 0, g \in G$. Hablando de manera general, los grupo-anillos contienen unidades no triviales.

Ejemplo 17. Sea $\eta \in R$ tal que $\eta^2 = 0$, entonces se tiene $(1+\eta)(1-\eta) = 1$. De este

hecho, tanto $1+\eta$ como $1-\eta$ son unidades de R. De la misma manera, si $\eta \in R$ es tal que $\eta^k = 0$ para algún entero positivo k, entonces se tiene que

$$(1-\eta)(1+\eta+\eta^2+\cdots+\eta^{k-1}) = 1-\eta^k = 1,$$

$$(1+\eta)(1-\eta+\eta^2+\cdots\pm\eta^{k-1}) = 1\pm\eta^k = 1.$$

Así, $1\pm\eta$ son unidades de R. Estas unidades son llamadas **unidades unipotentes** de R. En un grupo-álgebra KG sobre un campo de característica $p > 0$ se puede iniciar la búsqueda de unidades unipotentes investigando a los elementos nilpotentes. Si $g \in G$ es de orden p^n, entonces $(1-g)^{p^n} = 0$, de esta forma se demuestra que $\mu = 1-g$ es nilpotente.

En este caso $1-\eta = g$ es trivial, pero $1+\eta = 2-g$ es no trivial, a menos qu $\text{car}(K) = 2$. Nótese que $g-g^2 = g(1-g)$ también es nilpotente, entonces $1+g-g^2$ es una unidad no trivial si $g^2 \neq 1$.

En el teorema 18 y 17 se clasificaron todos los grupos finitos tal que el grupo-álgebra KG no tiene elementos nilpotentes. Se vera entonces que las grupo-álgebras de grupos finitos casi siempre tienen unidades no triviales.

Proposición 13. *Sea G un grupo tal que no es libre de elementos de torsión y K un campo de característica $p \leq 0$. Entonces KG sólo tiene unidades triviales si y sólo si se cumple alguna de las siguientes condiciones*

1. $K = F_2$ *y* $G = C_2$ *o* C_3

2. $K = F_3$ *y* $G = C_2$

Demostración. Supóngase que todas las unidades de KG son triviales. Considérese $N = <a>$ subgrupo finito de G de orden n. Si no existe $b \in G$ que normalize a N, entonces $\eta = (a-1)(1+a+\cdots+a^{n-1})$ es no nulo, pero $\eta^2 = (a-1)b(1+a+\cdots+a^{n-1})(a-1)b(1+a+\cdots+a^{n-1}) = 0$, de esa cuenta, $\eta+1$ es unidad no trivial de

KG, proposición que contradice la hipótesis, de donde se concluye que todo subgrupo finito de G es normal.

Sea H un subgrupo finito propio de G y considérese $\hat{H} = \sum_{h \in H} h$. Es fácil notar que $\hat{H}$ es central y $\hat{H}^2 = |H|\hat{H}$. Tómese $g \in G - H$ fijo. Si $|H| = 0$ en K entonces $\hat{H}^2 = 0$ y $g + \hat{H}$ es una unidad no trivial de KG con inverso $g^-1(1 - g^-1\hat{H})$. Si $|H| \neq 0$ en K, entonces $e = \frac{1}{H}\hat{H}$ es idempotente central y $e + g(1 - e)$ es una unidad no trivial con inverso $e + g^-1(1 - e)$. En ambos casos se llega a una contradicción, por lo que se concluye que $G = <a>$ es de orden primo.

Si $\text{car}(K) = p$ entonces $1 + c\hat{G}, c \in K$ es una unidad no trivial, a menos que $p = 2$ y $K = F_2$.

Por otro lado, si $\text{car}(K) \neq p$ entonces, del hecho que $K<a>$ es semisimple y conmutativo, $K<a>$ es suma directa de campos, a saber

$$K<a> \simeq K \oplus K(\zeta) \oplus K(\theta) \oplus + \cdots$$

donde $\zeta, \theta, \cdots$ son raíces de la unidad de orden p. Bajo este isomorfismo, se tiene $a \mapsto (1, \zeta, \theta, \cdots)$, por lo que una unidad trivial $ka^i, 0 \neq kinK$ tiene imagen $(k, k\zeta^i, k\theta^i, \cdots)$. Nótese que si la descomposición de $K<a>$ tuviera más de dos componentes se tendrían unidades de la forma $(1, \zeta, 1, \cdots)$ que no corresponden a unidades triviales de $K<a>$. Entonces se debe tener

$$K<a> \simeq K \oplus E, E = K(\zeta), |K| = q, |E| = q^r, \circ(a) = p$$

. Contando el número de unidades y de elementos se tiene

$$p(q - 1) = (q - 1)(q^r - 1), p^q = q \cdot q^r.$$

De la condición anterior, se calcula que $q^p = q(p - 1)$ y $q^{p-1} = p + 1$, lo cual sólo es posible para $q = 2$ y $p = 3$ o $q = 3$ y $p = 2$. Con lo que se demuestra que $K = F_2$ y $G = C_3$ o $K = F_3$ y $G = C_2$.

Para el converso, una simple inspección demuestra que $F_2C_2, F_3C_3 \simeq F_2 \oplus F_4$ y $F_3C_2 \simeq F_3 \oplus F_3$ tiene dos, tres y cuatro unidades triviales, lo cual coincide con el número de unidades triviales en cada caso. □

En este punto, se ha llegado al punto en el que se desea clasificar los grupos de torsión G de tal forma que el grupo-anillo entero $\mathbb{Z}G$ tenga solo unidades triviales.

Ejemplo 18. En el ejemplo 17 se dio la construcción de unidades unipotentes a partir de elementos nilpotentes. Ahora se verán elementos nilpotentes en particular que también poseen esa característica.

Supóngase que R tiene divisores de cero, es decir, se pueden encontrar elementos $x, y \in R$ no nulos tales que $xy = 0$. Si t es algún otro elemento de R entonces $\eta = ytx$ es no nulo tal que $\eta^2 = (ytx)(ytx) = ytxytx = 0$, así $1 + \eta$ es una unidad. En el caso especial cuando $R = \mathbb{Z}G$ es un grupo-anillo entero, una manera sencilla de obtener un divisor de cero es considerar un elemento $a \in G$ de orden finito $n > 1$, entonces $a-1$ es divisor de cero, ya que $(a-1)(1+a+\cdot+a^{n-1}) = 0$. De esa manera, tomando cualquier elemento $b \in G$, se puede construir una unidad de la forma

$$\mu_{a,b} = 1 + (a-1)b\hat{a}, \text{ con } \hat{a} = 1 + a + \cdots + a^{n-1} \tag{5.1}$$

Definición 16. *Sean $a \in G$ un elemento de orden finito n y b cualquier otro elemento de G. La unidad $\mu_{a,b}$ dada por la ecuación 5.1 es llamada unidad bicíclica del grupo-anillo $\mathbb{Z}G$. Se denotará por $\mathcal{B}_2$ el subgrupo de $\mathcal{U}(\mathbb{Z}G)$ generado por todas las unidades bicíclicas de $\mathbb{Z}G$.*

Es claro que si $a, b \in G$ conmutan, entonces $\mu_{a,b} = 1$. Se desea saber para que casos $\mu_{a,b}$ es una unidad trivial de $\mathbb{Z}G$.

Proposición 14. *Sean g, h elementos de un grupo G con $\circ g = n < \infty$. Entonces, la unidad bicíclica $\mu_{g,h}$ es trivial si y sólo si h normaliza $a <g>$, en cuyo caso $\mu_{g,h} = 1$.*

Demostración. Supóngase que h normaliza a $<g>$, entonces $h^{-1}gh = g^j$, para algún entero positivo$j$. De esto se tiene $gh = g^j h$ y como $g^j\hat{g} = \hat{g}$, se tiene $gh\hat{g} = h\hat{g}$. Haciendo los cálculos $\mu_{g,h} = 1 + (g-1)h\hat{g} = 1 + gh\hat{g} - h\hat{g} = 1$.

Para el converso, supóngase que $\mu_{g,h}$ es trivial, entonces, del hecho que $\mathcal{E}(\mu_{g,h}) = 1$, existe $x \in G$ tal que $\mu_{g,h} = x$. De esta cuenta, se tiene

$$1 + (1-g)h\hat{g} = x$$

y de esta ecuación se infiere que

$$1 + h(1 + g + g^2 + \cdots + g^{n-1}) = x + gh(1 + g + g^2 + \cdots + g^{n-1}).$$

Si $x = 1$ se tiene que $h = ghg^i$ para algún entero positivo i. Si $x \neq 1$ entonces $h \notin <g>$, pero 1 aparece en el lado izquierdo de la ecuación, por lo que también debe aparecer en el lado derecho, esto es, existe k entero positivo tal que $ghg^k = 1$ entonces $h = g^{-1}g^{-k} = g^{-(k+1)}$ y por lo tanto $h \in <g>$, lo cual es una contradicción. □

Como consecuencia inmediata se tiene el resultado:

Proposición 15. *Sea G un grupo finito. El grupo $\mathcal{B}_2$ es trivial si y sólo si todo subgrupo de G es normal.*

Proposición 16. *Toda unidad bicíclica $\mu_{g,h} \neq 1$ de $\mathbb{Z}G$ es orden infinito.*

Demostración. Dado $\mu_{g,h} = 1 + (g-1)h\hat{g}$ se tiene

$$\mu_{g,h}^s = (1 + (g-1)h\hat{g}^s = 1 + s(g-1)h\hat{g})$$

entonces $\mu_{g,h}^s = 1$ si y sólo si $(g-1)h\hat{g} = 0$, lo cual sucede solo si $\mu_{g,h} = 1$. □

Se desea explorar que pasa cuando se trabaja con grupos conmutativos finitos. El lector deberá recordar la definición de la función totiente de Euler ϕ. Dado n,

un entero positivo, se cumple que si la factorización de n en producto de números primos es $n = p_1^{n_1} \cdots p_t^{n_t}$, entonces

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_t^{n_t-1}(p_t - 1).$$

Una propiedad de mucha importancia es el famoso teorema de Euler: Si m y n son primos relativos entonces $i^{\phi(n)} \equiv 1(\text{mod n})$.

Definición 17. *Sea g un elemento de orden n en un grupo G. Una unidad cíclica de Bass* [1] *es un elemento del grupo-anillo $\mathbb{Z}G$ de la forma:*

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi n}}{n}\hat{g}$$

donde i es un entero tal que $1 < i < n - 1$ y $(i, n) = 1$.

Como es natural, se debe mostrar que μ_i es una unidad. Es claro que, para $g \in G, \mu_i$ pertenece al grupo-anillo $\mathbb{Q}<g>$. Se vió en el ejemplo 3 que $\mathbb{Q}<g> \simeq \oplus_{d|n}\mathbb{Q}(\zeta_d)$ donde ζ_d es una raíz primitiva de la unidad de orden d. Más aún, bajo este isomorfismo, la proyección de g en cada componente es la respectiva raíz de la unidad, así que un elemento de la forma $(1 + g + \cdots + g^{i-1})$ proyecta, en cada componente, un elemento de la forma:

$$1 + \zeta_d + \cdots + \zeta_d^{i-1} \in \mathbb{Z}[\zeta_n].$$

Si $\zeta_d \neq 1$, entonces el elemento ζ_d es invertible en $\mathbb{Z}[\zeta_d]$ y es llamada unidad ciclotómica. De lo anterior, el inverso de α_d es

$$\alpha_d^{-1} = \frac{\zeta_d - 1}{\zeta_d^i - 1} = \frac{\zeta_d^{ik}}{\zeta_d^i - 1} = 1 + \zeta_d^i + \cdots + \zeta_d^{i(k-1)},$$

donde k es cualquier entero tal que $ik \equiv 1(\text{mod } n)$. Es claro que $\alpha_d^{-1} \in \mathbb{Z}[\zeta_d] \in \mathbb{Z}[\zeta_n]$.

Para la primer componente las cosas cambian, ya que la proyección es precisamente el valor i, que no es invertible. Ahora bien, como $(i, n) = 1$ y aplicando

[1] Hyman Bass(5 de Octubre, 1932) es un matemático Americano conocido por sus trabajos en Álgebra y en Matemática educativa.

el teorema de Euler, se tiene que $i^{\phi(n)} = 1 + tn$ para algún $t \in \mathbb{Z}$. Considérese el elemento

$$(1 + g + \cdots + g^{i-1})^{\phi(n)} - t\hat{g}$$

y nótese que $\hat{g}$ es cero en cualquier componente $\mathbb{Q}(\zeta_d)$, con $\zeta_d \neq 1$, por lo que la proyección de μ_i e cada una de estas componentes es una unidad. Ahora, analizando el caso de la primera componente de nuevo, se puede observar que dicha proyección es $i^{\phi(n)} - tn = 1$, con lo cual se prueba que la proyección sobre dicha componente también es unidad. Más aún, se obtuvo que $-t = \frac{1-i^{\phi(n)}}{n}$, por lo que el elemento $(1 + g + \cdots + g^{i-1})^{\phi(n)} - t\hat{g})$ considerado anteriormente es precisamente μ_i. De esta forma se ha demostrado que la proyección de μ_i en todas las componente de $\oplus_{d|n}\mathbb{Z}[\zeta_d]$ es una unidad. Si se denota por R la preimagen de este anillo bajo el isomorfismo, se tiene que μ_i es unidad en R.

Proposición 17. *Sea g un elemento de orden finito en un grupo G. Entonces, el elemento*

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{g},$$

donde i es un entero tal que $1 < i < n - 1$ y $(i, n) = 1$, es invertible y su inversa es

$$\mu_i^{-1} = (1 + g^i + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\hat{g},$$

donde k es cualquier entero tal que $ik \equiv 1 (mod\ n)$.

Proposición 18. *Sea g un elemento de orden finito n en un grupo G y sea l un entero tal que $1 < l < n - 1$ y $(l, n) = 1$. Entonces, la unidad cíclica de Bass*

$$\mu_l = (1 + g + \cdots + g^{l-1})^{\phi(n)} + \frac{1 - l^{\phi(n)}}{n}\hat{g}$$

es de orden infinito.

Demostración. Se sabe que

$$\mathbb{Q}<g> \simeq \mathbb{Q} \oplus \cdot \oplus \mathbb{Q}(\zeta^d) \oplus \cdots \oplus \mathbb{Q}(\zeta),$$

donde ζ es una raíz primitiva de la unidad de orden n y d representa a los divisores de n. Más aún, en el isomorfismo se tiene

$$g \mapsto (1, \ldots, \zeta^d, \ldots, \zeta).$$

Sea μ_l como en la proposición. Se requieren demostrar que la proyección $\mu_l(\zeta)$ en la última componente es de orden infinito. Primero nótese que dicha proyección es de la forma $\mu_l(\zeta) = (1 + \zeta + \cdots + \zeta^{l-1})^{\phi(n)}$, de esa cuenta, si $(1 + \cdots + \zeta^{l-1})^{\phi(n)}$ fuera de orden finito, entonces se tendría que $(1 + \cdots + \zeta^{l-1})$ sería de orden finito. Como $\{\pm\zeta^t \colon 0 \leq t \leq n-1\}$ son todas raíces de la unidad de $\mathbb{Q}(\zeta)$, se tendría que $(1+\cdots+\zeta^{l-1}) = \pm\zeta^s$ para algún entero positivo s. Multiplicando la última ecuación por $(1-\zeta)$ se observa que $1-\zeta^l = \pm\zeta^s(1-\zeta)$. Así, tomando valores absolutos, se obtiene $\mid 1-\zeta^l \mid = \mid 1-\zeta \mid$. Escribiendo $\zeta = \cos\theta + i\sin\theta$, por el teorema de DeMoivre, se tiene $\zeta^l = \cos(l\theta) + i\sin(l\theta)$, de donde se deduce que $\mid 1-\zeta \mid^2 = \mid 1-(\cos\theta+i\sin\theta) \mid^2 = 2(1-\cos\theta)$ y $\mid 1-\zeta^l \mid^2 = \mid 1-(\cos(l\theta)+i\sin(l\theta) \mid^2 = 2(1-\cos(l\theta))$, de esa cuenta, $\cos\theta = \cos(l\theta)$, lo cual implica que $l\theta = \theta$, lo cual implica que $l\theta = \theta$ o $l\theta = 2\pi - \theta$, por lo tanto $\zeta^l = \zeta$ o $\zeta^l = \zeta^{-1}$. En cualquiera de los dos casos se obtiene una contradicción, lo cual demuestra que μ_l tiene orden infinito. □

Nota 5. *En la definición de unidad cíclica de Bass μ_l, l está en el rango $1 < l < n-1$. Si se toma $l = n-1$ se tiene*

$$\mu_l = (1 + g + \cdots + g^{n-2})^{\phi(n)} + \frac{1 - l\phi(n)}{n}\hat{g}.$$

La proyección de μ_l sobre cualquier componente es $(-g^{-1})^{\phi(n)}$ y $\mu_l = (-g^{-1})^{\phi(n)}$ es trivial. Así mismo, de la restricción $1 < l < n-1$, se tiene que $n \geq 5$ para que μ_l esté definida.

Nota 6. *Lo proposición anterior demuestra que μ_l es una unidad no trivial.*

Ejemplo 19. Ahora considérese $g \in G$ un elemento de orden impar, $n \neq 1$ y el elemento

$$\mu = 1 - g + g^2 - \cdots + g^{c-1},$$

donde $(c, 2n) = 1$. Entonces la proyección en cada componente de $\mathbb{Q}<g>$ es una unidad ciclótomica y como la proyección en la primera componente es 1, se tiene que μ es una unidad en $\mathbb{Z}<g>$. Esta unidad es llamada una **unidad alternante**.

5.2. Unidades Triviales

En el capítulo anterior se demostró que si G es un grupo abeliano, entonces todas las unidades de torsión de $\mathbb{Z}G$ son triviales. Ahora en esta sección se hará un breve estudio de los grupos G que hacen que todas las unidades de $\mathbb{Z}G$ sean triviales.

El lector deberá recordar que una unidad trivial de $\mathbb{Z}G$ es un elemento de la forma $\pm g, g \in G$. Así, si todas las unidades de $\mathbb{Z}G$ son triviales, entonces se tiene que $\mathcal{U}(\mathbb{Z}\mathbb{G}) = \pm G$. Esta condición se traduce, en términos de unidades normalizadas, como $\mathcal{U}_1(\mathbb{Z}G) = G$.

Lema 15. *Sea G un grupo de torsión tal que $\mathcal{U}_1(\mathbb{Z}G) = G$. Entonces todo subgrupo de G es normal.*

Demostración. Para demostrar este lema, es suficiente demostrar que todo subgrupo cíclico de G es normal. De esta forma, supóngase que existe un subgrupo cíclico $<g>$ de G que no es normal, es decir, existe $h \in G$, tal que $h^{-1}gh \notin <g>$ y se sigue de la proposición 14 que la unidad bicíclica $u = 1 + (1 - g)h\hat{g}$ es no trivial. □

Es sabido que si G es un grupo abeliano, entonces sus subgrupos son normales. Además, se recuerda al lector que todo grupo de torsión no abeliano G tal que todos sus subgrupos son normales es llamado un grupo Hamiltoneano, este grupo tiene la forma

$$G = K_8 \times E \times A,$$

donde E es un 2-grupo abeliano elemental - todo elemento $a \neq 1$ en E es de orden 2-, A es un grupo abeliano donde todos sus elementos son de orden impar y K_8 es

el grupo de los cuaterniones de orden ocho:

$$K_8 = <a, b\colon a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1}>$$

Proposición 19. *Sea G un grupo de torsión tal que $\mathcal{U}_1(\mathbb{Z}G) = G$. Entonces G es abeliano de exponente igual a $1, 2, 3, 4$ o 6, o bien, G es un 2-grupo hamiltoneano.*

Demostración. Del lema anterior se sigue que G es abaliano o bien G es hamiltoneano. Primero supóngase que G es abeliano. Si su exponente es diferente de $1, 2, 3, 4$ o 6 entonces G contiene un elemento de orden n, con $n = 5$ o $n > 6$. En ambos casos, se tiene que $\phi(n) > 2$ - ya que $\phi(n) \equiv (\text{mod}2)$ - y la proposición 18 demuestra que G contiene una unidad cíclica de Bass que es no trivial.

De manera análoga, si G es hamiltoneano pero no es un 2-grupo, entonces G contiene un elemento $x \in A$ de orden $p > 2$. Entonces, el elemento $g = ax$ tiene orden $n = 4p$ y, de nuevo, $\phi(n) > 2$, por lo que G contiene una unidad cíclica de Bass. □

La condición dada en la proposición anterior también es suficiente, pero su demostración no es tan trivial. Se demostrará este hecho a través de una serie de lemas.

Lema 16. *Sea G un grupo tal que las unidades de $\mathbb{Z}G$ son triviales y C_2 un grupo cíclico de orden 2. Entonces las unidades de $\mathbb{Z}(G \times C_2)$ también son triviales.*

Demostración. Sea $C_2 = <a\colon a^2 = 1>$. Como $\mathbb{Z}(G \times C_2) \simeq (\mathbb{Z}G)C_2$, un elemento $u \in \mathbb{Z}(G \times C_2)$ puede ser escrito de la forma $u = \alpha + \beta a$ donde $\alpha, \beta \in \mathbb{Z}G$. Debido a que u es unidad, tiene que existir otro elemento $u^{-1} = \gamma + \delta a$ tal que

$$(\alpha + \beta a)(\gamma + \delta a) = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)a = 1.$$

Entonces

$$\begin{aligned} \alpha\gamma + \beta\delta &= 1 \\ \alpha\delta + \beta\gamma &= 0. \end{aligned}$$

Así, se tiene

$$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \beta\delta + \alpha\delta + \beta\gamma = 1$$

$$(\alpha - \beta)(\gamma - \delta) = \alpha\gamma + \beta\delta - (\alpha\delta + \beta\gamma) = 1$$

lo cual demuestra que $(\alpha + \beta)$ y $(\alpha - \beta)$ son unidades en $\mathbb{Z}G$ y por lo tanto son unidades triviales. Entonces, existen $g_1, g_2 \in G$ tales que

$$\alpha + \beta = \pm g_1, \quad \alpha - \beta = \pm g_2.$$

De estas últimas igualdades, se sigue que $\alpha = \frac{1}{2}(\pm g_1 \pm g_2)$, pero como los coeficientes de α deben ser enteros, tiene que ser cierto que $g_1 = \pm g_2$. De esta manera, se tienen dos opciones:

$$\alpha + \beta = \alpha - \beta = \pm g_1$$

o

$$\alpha + \beta = -(\alpha - \beta) = \pm g_1.$$

Para el primer caso, se obtiene $\alpha = \pm g_1$ y $\beta = 0$, mientras que para el segundo caso $\alpha = 0$ y $\beta = \pm g_1$. En ambos casos se obtiene que u es trivial. □

Lema 17. *Las unidades del grupo-anillo $\mathbb{Z}K_8$ son triviales.*

Demostración. En este punto, vale la pena recordar que

$$K_8 = \{1, a, b, ab, a^2, a^3, a^2b, ab^3\}.$$

Entonces, todo elemento $\alpha \in \mathbb{Z}K_8$ es de la forma

$$\alpha = x_0 + x_1a + x_2b + x_3ab + y_0a^2 + y_1a^3 + y_2a^2b + y_3ab^3.$$

Ahora, téngase en consideración al anillo de cuaterniones integrales, esto es, el anillo

$$H = \{m_0 + m_1 i + m_2 j + m_3 k \colon m_0, m_1, m_2, m_3 \in \mathbb{Z}\}.$$

Es fácil ver que las únicas unidades de H son $\pm 1, \pm i, \pm j, \pm k$. Ahora considérese el epimorfismo $\phi \colon \mathbb{Z}K_8 \to H$ dado por

$$\alpha \mapsto (x_0 - y_0) + (x_1 - y_1)i + (x_2 - y_2)j + (x_3 - y_3)k.$$

Por ser un morfismo, si α es unidad en $\mathbb{Z}K_8$ entonces $\phi(\alpha)$ es unidad de H; por lo tanto, para algún índice r, $\quad 0 \leq r \leq 3$, se debe cumplir que

$$\begin{aligned} x_r - y_r &= 1 \\ x_s - y_s &= 0 \text{ si } s \neq r. \end{aligned}$$

Por otro lado, es fácil notar que a^2 es central y que $\frac{K_8}{<a^2> \simeq C_2 \times C_2}$. Si se denota como $\bar{g}$ la clase de un elemento $g \in K_8$ bajo el cociente y como $\psi \colon \mathbb{Z}K_8 \to \mathbb{Z}\left(\dfrac{K_8}{< a^2 >}\right)$, la extensión de la proyección canónica $K_8 \to \left(\dfrac{K_8}{< a^2 >}\right)$ hacia $\mathbb{Z}K_8$, se tiene que

$$\psi(\alpha) = (x_0 + y_0) + (x_1 + y_1)\bar{a} + (x_2 + y_2)\bar{b} + (x_3 + y_3)\bar{a}\bar{b}.$$

Se sigue del lema anterior que las unidades de $\mathbb{Z}(C_2 \times C_2)$ son triviales. Así, para algún índice $h, 0 \leq h \leq 3$, se tiene

$$\begin{aligned} x_h + y_h &= \pm 1 \\ x_k + y_k &= 0, \text{ si } h \neq k. \end{aligned}$$

Es fácil notar que $r = h$ y

$$x_r = \mp 1, y_r = 0, x_s = y_s = 0, \text{ si } s \neq r,$$

o

$$x_r = 0, y_r = \pm 1, x_s = y_s = 0 \text{ si } s \neq r.$$

En ambos casos se llega a que α es unidad trivial de $\mathbb{Z}K_8$. $\square$

Lema 18. *Sea ζ una raíz primitiva de la unida de orden 3 o 4. Entonces, las unidades del anillo ciclotómico $\mathbb{Z}[\zeta]$ son simplemente $\{\pm\zeta^i\}$*

Demostración. Se considerará primero el caso en que ζ es una raíz cúbica de la unidad. Recordemos que el polinomio minimal de ζ es $X^2 + X + 1$, así que todo elemento $\alpha \in \mathbb{Z}[\zeta]$ es de la forma $\alpha = a + b\zeta$, con $a, b \in \mathbb{Z}$. Supóngase que α es una unidad de $\mathbb{Z}[\zeta]$. Dado que la aplicación $f\colon \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$ dada por $f(x+y) = x + y\zeta^2$ es un automorfismo, se sigue que $\alpha' = a + b\zeta^2$ es también una unidad y así

$$\alpha\alpha' = (a + b\zeta)(a + b\zeta^2) = a^2 + b^2 + ab(\zeta + \zeta^2) = a^2 + b^2 - ab$$

es también una unidad, pero $\alpha\alpha' \in \mathbb{Z}$, así que $a^2 + b^2 - ab = \pm 1$. Supóngase, sin pérdida de generalidad, que $\mid a \mid \geq \mid b \mid$. Si $b \neq 0$, se sigue $a^2 + b^2 > ab \pm 1$, lo cual es una contradicción.

Si $b = 0$, entonces $\alpha = a \in \mathbb{Z}$ es una unidad y $\alpha = \pm 1$. Si $b = 1$, se tiene que $a^2 + 1 = a \pm 1$ lo cual implica que $a^2 = a$ o $a^2 - a + 2 = 0$. Para el primer caso se tiene $a = 0$ o $a = 1$ y para el segundo caso no se tiene solución en los enteros. Si $a = 0$ se tiene $\alpha = b\zeta$ y como $\mid \alpha \mid = 1$, se sigue que $\alpha = \pm\zeta$. Finalmente, si $a = b = 1$ se tiene que $\alpha = 1 + \zeta = -\zeta^2$. El caso en que ζ es raíz primitiva de la unidad de orden cuatro es aún más fácil, ya que $\zeta = i$ y los elementos en $\mathbb{Z}[i]$ son de la forma $\alpha = a + bi, a, b \in \mathbb{Z}$, es decir que $\alpha \in \mathbb{C}$ y por lo tanto $a = \pm 1$ y $b = 0$ o $a = 0$ y $b = \pm 1$ □

Teorema 20 (Higman)**.** *Sea G un grupo de torsión. Entonces, todas las unidades de $\mathbb{Z}G$ son triviales si y sólo si G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ o 6 o G es un 2-grupo hamiltoneano.*

Demostración. La condición necesaria ya se ha demostrado. Para probar la condición suficiente, considérese el caso en que G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ o 6 y supóngase que G es finito. En este caso, el teorema 8 asegura que

$$\mathbb{Q}G \simeq \oplus_{d|n} a_d \mathbb{Q}(\zeta_d)$$

donde ζ_d denota a las raíces primitivas de la unidad de orden d y $a_d = \dfrac{\eta_d}{\mid K(\zeta_d : K \mid)}$. En esta fórmula, η_d denota el número de elementos de orden d en G. En otra palabras, solamente las raíces de la unidad cuyos órdenes son iguales a los órdenes de los elementos en G aparecen en la descomposición. Sea R la preimagen, bajo el isomorfismo, del orden

$$M = \oplus_{d|n} a_d \mathbb{Z}[\zeta_d].$$

Nótese que si G es como se propuso al inicio, entonces G es de la forma

$$\begin{aligned}
G &\simeq C_2 \times \cdots \times C_2, \\
G &\simeq C_3 \times \cdots \times C_3, \\
G &\simeq C_4 \times \cdots \times C_4, \\
G &\simeq C_2 \times \cdots \times C_2 \times C_3 \times \cdots \times C_3, \\
G &\simeq C_2 \times \cdots \times C_2 \times C_4 \times \cdots \times C_4.
\end{aligned}$$

Sin embargo, por el lema 16, se puede asumir que G es del segundo o del tercer tipo. En ambos casos, se sigue del lema 18 que todas las unidades de R son triviales y por lo tanto de orden finito. Como $\mathcal{U}(\mathbb{Z}G)$ está contenido en R, también sus unidades son de orden finito, como G es abeliano, se sigue que estas deben ser triviales. En el caso en que G es un 2-grupo hamiltoneano la conclusión se sigue directamente del lema 16 y 18 $\square$

6. Aplicaciones

En este capítulo se darán los conceptos básicos de teoría de códigos. Se empezará dando una descripción del sistema de comunicación como lo propuso Claude E. Shannon [1] en 1948. En esta parte también se introducirán todos los conceptos básicos del sistema de comunicación como canal, codificador, decodificador y código. Una vez la teoría básica está dada se hace un breve estudio de los códigos lineales, para terminar este capítulo con una clase de códigos en particular, los cíclicos.

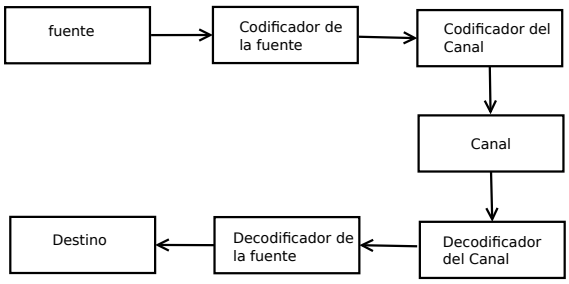
6.1. Sistema de Comunicación

La figura 4 muestra un sistema de comunicación de una **fuente** a un **destino** mediante un **canal**. La comunicación puede ser en el dominio del espacio - es decir, de un punto a otro - o en el dominio del tiempo - es decir, al guardar información en algún punto en el tiempo para ser recuperada posteriormente-. La codificación de la fuente tiene doble propósito. Primero, servir como traductor entre la salida de la fuente y la entrada al canal. Por ejemplo, si la información transmitida de la fuente al destino está en señal análoga y el canal espera recibir señal digital, se necesitará una conversión de análoga a digital en la fase de codificación y un convertidor de señal digital a análoga en la gase de decodificación. Como segunda función se podría requerir que el codificador de la fuente comprima la salida de la fuente para economizar en la longitud de la transmisión, eso significa que en el otro extremo, el decodificador de la fuente necesitará descomprimir la señal.

Algunas aplicaciones necesitan que el decodificador restaure la información para que sea idéntica a la original, en cuyo caso se dice que la compresión es **sin pérdidas**.

[1] Claude Elwood Shannon (Míchigan, 30 de abril de 1916 - 24 de febrero de 2001) fue un ingeniero electrónico y matemático estadounidense, recordado como «el padre de la teoría de la información»

Figura 4. Sistema de Comunicación propuesto por Shannon



Fuente: Elaboración propia con software Dia.

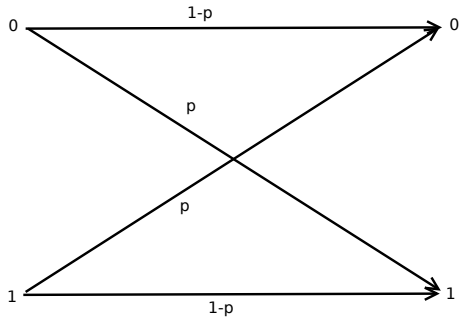
Otras aplicaciones, como la mayoría de transmisiones de audio e imágenes, permiten una diferencia -controlada- o distorsión entre la información original y la restaurada, así que esta posibilidad es usada para lograr mayor compresión. En este caso se dice que la compresión es **con pérdidas.**

Los canales no son perfectos debido a limitaciones físicas y de ingeniería, es decir, su salida puede diferir de su entrada debido al ruido o a defectos de fabricación.

Más aún, en algunos casos el diseño requiere que el formato de la información de salida del canal difiera del formato de entrada. Además hay aplicaciones tales como los medios de almacenamiento masivo mágnetico y óptico, donde no se permiten ciertos patrones en el flujo de bits a transmitir. Dado esto, el rol principal del codificador del canal, es superar estas limitaciones y hacer el canal tan transparente como sea posible, tanto desde el punto de vista de la fuente como del destino.

Es así como entran a participar los códigos. Los códigos fueron inventados para corregir errores en los canales de comunicación debido al ruido. Por ejemplo, supóngase que hay un cable telegráfico desde Ciudad de Guatemala hasta Ciudad de Panamá, mediante el cual se pueden transmitir unos y ceros. Usualmente cuando

Figura 5. Canal Binario Simétrico



Fuente: Elaboración propia con software Dia.

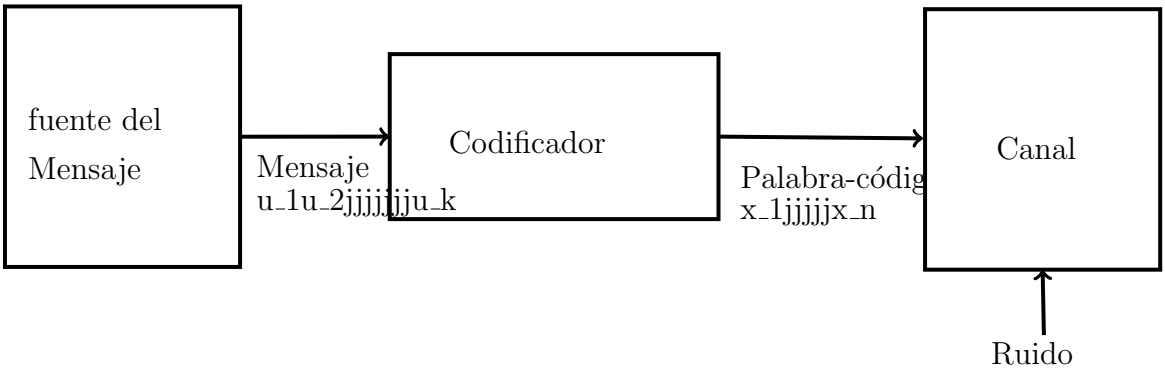
un cero es enviado se recibe un cero, pero ocasionalmente un cero puede ser recibido como un uno o un uno como un cero. Supóngase que en promedio, 1 de cada 100 símbolos se recibe de forma errónea, es decir, por cada símbolo hay una probabilidad $p = 1/100$ de que ocurra un error en el canal. A esto se le llama un canal binario simétrico y se denota como BSC. Además supóngase que se enviarán muchos mensajes importantes por ese cable y se necesita enviarlos de manera rápida y segura. Los mensajes ya se encuentran escritos como cadenas de ceros y unos, producidos, quizás, por alguna computadora.

Se van a **codificar** estos mensajes para darles una protección en contra del ruido del canal. Un bloque de k símbolos del mensaje $u = u_1 \dots u_k, u_i = 0$ o 1, será codificado como una **palabra-código** $x = x_1 \dots x_n, x_i = 0$ o 1 donde $n \geq k$ (véase la figura 6). Estas palabra-códigos forman un código. La primera parte de la palabra-código consiste en ele mensaje mismo:

$$x_1 = u_1, x_2 = u_2, \dots, x_k = u_k,$$

seguido de $n - k$ símbolos de comparación $x_{k+1,\dots,x_n}$. Los símbolos de comparación

Figura 6. Proceso de Codificación



Fuente: Elaboración propia con software Dia y exportado a TEX

son elegidos de tal forma que las palabra-códigos satisfagan

$$H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = Hx^t = 0,$$

donde la matriz H de $(n-k) \times k$ es la matriz de comparación de paridad del código, dada por

$$H = [A \mid I_{n-k}], \tag{6.1}$$

donde A es una matriz fija de $(n-k) \times k$ de ceros y unos y

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

es la matriz identidad de $(n-k) \times (n-k)$. La aritmética en la ecuación 6.1 se hace en módulo 2, es decir que se está trabajando con el campo $\mathbb{Z}_2$.

Ejemplo 20. La matriz de comparación de paridad

$$H = \left(\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

define un código con $k = 3$ y $n = 6$. Para este código

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

El mensaje $u_1u_2u_3$ es codificado en la palabra-código $x = x_1x_2x_3x_4x_5x_6$ que empieza con el propio mensaje:

$$x_1 = u_1, x_2 = u_2, x_3 = u_3,$$

seguido de tres símbolos de comparación $x_4x_5x_6$ tales que $Hx^t = 0$, es decir, se cumple

$$x_2 + x_3 + x_4 = 0, \tag{6.2}$$

(6.3)

CONCLUSIONES

1. Conclusiones (c_y_r.tex)

RECOMENDACIONES

1. Recomendaciones (c_y_r.tex)

BIBLIOGRAFÍA

[1] T. Hawkins. *The origins of the Theory of Group Characters*, Archive Hist. Exact Sci. 7 (1970-71). p. 142-170.

[2] WILLIAM, Burnside, *The theory of Groups of Finite Order*. 2da ed. Cambridge: Cambridge University Press, 1911.

[3] GOLDSHMIDT, David. *A group theoretic proof of the p^aq^b theorem for odd primes*. Math. Z. 13 (1970). p 373-375.

[4] WALTER, Feit y JHON, Thompson. *The solvability of groups of odd order*. Pacific J. Math. 15 (1963). p 775-1029.

[5] SERGE, Lang. *Linear Algebra*. 3ra ed. Nueva York: Springer-Verlag, 2004. 308 p.

[6] DONALD, Passman. *The algebraic structure of group rings*. New York: Wiley-Interscience, 1977. 550 p.

[7] CLAUDE, Moser. *Representation de -1 comme somme de carres dans un corps cyclotomique quelconque*. J. Number Theory 5 (1973), 138-141.

[8] SUDARSHAN, Sehgal. *Topics in Group Rings*.New York: Marcel Dekker, 1978. 233 p.

[9] NATHAN, Herstein. *Topics in Algebra*. 2nda ed. New York: Macmillah, 1986 . 381 p.