República Bolivariana de Venezuela
Universidad Centroccidental Lisandro Alvarado
Decanato de Ciencias y Tecnología
Coordinación de Postgrado

Álgebras de Grupo de Grupos Abelianos Finitos y Algunas Aplicaciones a Problemas de Combinatoria

Lcda. Smelin Pereira

Barquisimeto, Mayo 2016

Smelin Pereira

Álgebras de Grupo de Grupos Abelianos Finitos y Algunas Aplicaciones a Problemas de Combinatoria

Área de Conocimiento: Teoría Combinatoria de Números

Tesis de Grado presentado ante la ilustre
Universidad Centroccidental Lisandro Alvarado,
como requisito para optar al grado académico de
Magister en Ciencias Mención Matemáticas.
Tutora: Dra. Luz Marchán

Barquisimeto, Mayo 2016

Dedicatoria

A Dios, Creador de los cielos y la tierra.

A mis hijos, Samuel y Grecia.

Agradecimientos

A Dios, con quien todo es posible.

A la Dra. Luz Marchán que, como tutora, me orientó y corrigió oportunamente.

A mi esposo Samuel, mi ayuda idónea.

A mis hijos Samuel y Grecia. Por ser mi inspiración para no rendirme.

Índice general

Resumen

Sea G un grupo abeliano finito y sea $R[G]$ el álgebra del grupo G sobre un dominio de integridad R. En este trabajo estudiamos condiciones sobre la estructura de una secuencia de elementos en G, digamos $g_1, g_2, \ldots, g_l$, para que

$$(X^{g_1} - a_1) \cdot (X^{g_2} - a_2) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in R[G].$$

Además aplicamos los resultados obtenidos, sobre estas condiciones estructurales, para dar solución a una variación de la conjetura de Snevily propuesta en [15] sobre transversales de cuadrados latinos aditivos.

Introducción

Sea G un grupo abeliano finito con notación aditiva. En las últimas décadas las álgebras de grupos $R[G]$ sobre un anillo conmutativo R adecuado, se han convertido en potentes herramientas para abordar una creciente variedad de problemas que han surgido en la teoría combinatoria y la teoría de números, muchos de estos problemas pueden ser reducidos al problema de estudiar condiciones estructurales sobre una secuencia dada $g_1, g_2, \ldots, g_l$ de elementos en G, de modo que se tenga

$(X^{g_1} - a_1) \cdot (X^{g_2} - a_2) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in R[G]$ para todo $a_1, a_2, \ldots, a_l \in R$.

En este trabajo estudiamos este problema, cuando R es un domino de integridad.

Sean $A = \{a_1, a_2, \ldots, a_k\}$ y $B = \{b_1, b_2, \ldots, b_k\}$ dos subconjuntos de un grupo abeliano G, Snevily ha conjeturado que, cuando el orden de G es impar, existe una reordenación de los elementos de B tal que los elementos $a_i + b_i$, con $1 \leq i \leq k$, son distintos dos a dos. Usando un método polinomial, Alon ha confirmado esta conjetura cuando el orden de G es primo [1]. Con una nueva aplicación de los métodos polinomiales, Dasgupta y otros, en [2], extendieron el resultado de Alon para p-grupos abelianos finitos en el caso $k < p$ y verificaron la conjetura de Snevily para todo grupo cíclico. En [6] Gao

y Wang, usando herramientas de las álgebras de grupo, probaron la conjetura para p-grupos abelianos finitos con $k < \sqrt{2p}$ y verificaron la conjetura para todo grupo abeliano finito de orden impar en el caso $k < \sqrt{p}$, donde p es el menor primo divisor del orden de G.

En este trabajo, usando algunos resultados relacionados con las álgebras de grupos, específicamente sobre $\mathbb{Z}[G]$, presentamos una demostración de la conjetura de Snevily, la cual fué publicada en [5], para p-grupos abelianos finitos cuando $2k < 1 + \sqrt{8p+1}$ y damos algunos resultados especiales relacionados con dicha conjetura.

Hemos estructurado el trabajo como se describe a continuación.

El primer capítulo está dedicado a dar las definiciones básicas, notación, terminología y resultados existentes relacionados con algunas estructuras algebraicas, con la intención que el lector pueda ubicarse rápidamente en el contexto, cabe destacar que en este capítulo hemos obviado las demostraciones de los resultados presentados, salvo aquellas para las cuales no se encontró referencia bibliográfica.

El segundo capítulo contiene la primera parte de los resultados principales. En este capítulo definimos las álgebras de grupos y mostramos algunas de sus propiedades, además, mostramos detalladamente las propiedades de los caracteres de grupos y su relación con las álgebras de grupos. Finalmente mostramos dos resultados centrales del trabajo.

En el tercer capítulo abordamos la conjetura de Snevily, aplicando los resultados principales sobre álgebras de grupos obtenidos en el Capítulo 2.

Capítulo 1

Preliminares

En este capítulo enumeramos algunas definiciones, notaciones y resultados concernientes a las estructuras algebraicas, con el propósito de recordar algunas nociones básicas del álgebra que serán usadas en el resto del trabajo. No presentamos demostraciones de los resultados, salvo aquellos para los cuales no encontramos una referencia apropiada.

En adelante, por $\mathbb{N}$ y $\mathbb{N}_0$ denotamos el conjunto de los números enteros positivos y no negativos, respectivamente. Para los números enteros a y b, denotamos por $[a, b]$ al siguiente conjunto

$$[a, b] := \{x \in \mathbb{Z} \colon a \leq x \leq b\}.$$

Y denotamos por $\mathrm{mcd}(a, b)$ al máximo común divisor de a y b.

Si A es un conjunto denotamos su cardinal por $\mathsf{card}(A)$.

1.1. Grupos

Definición 1.1.1. Un *semigrupo* es un conjunto no vacío G con una operación binaria sobre G la cual es:

(i) asociativa: $a(bc) = (ab)c$ para todo $a, b, c \in G$;

Un *monoide* es un semigrupo G el cual contiene un

(ii) elemento identidad $e \in G$ tal que $ae = ea = a$ para todo $a \in G$.

Un *grupo* es un monoide G tal que

(iii) para todo $a \in G$ existe un elemento inverso $a^{-1} \in G$ tal que $a^{-1}a = aa^{-1} = e$.

Un semigrupo G se dice que es *abeliano* ó *conmutativo* si su operación binaria es

(iv) conmutativa: $ab = ba$ para todo $a, b \in G$.

El *orden* de un grupo G es $|G| := \mathsf{card}(G)$. Sea G un grupo. Dado $a \in G$, el *orden* de a es el orden del subgrupo cíclico $\langle a \rangle$ y es denotado $\mathrm{ord}(a)$.

En adelante, usaremos notación aditiva para indicar la operación binaria de los grupos, y el elemento identidad será denotado por 0.

Teorema 1.1.1. *[10] Sea G un grupo y g un elemento en G con* $\mathrm{ord}(g) = n \in N$. *Para todo $m \in \mathbb{N}$ se cumple,*

$$\mathrm{ord}(mg) = \frac{n}{\mathrm{mcd}(m, n)}.$$

El *exponente* de un grupo G es el menor entero positivo n tal que $na = 0$, para todo $a \in G$ y es denotado $\exp(G)$.

Sean G y H grupos. Una función $f : G \to H$ tal que

$$f(g_1 + g_2) = f(g_1) + f(g_2) \text{ para todo } g_1, g_2 \in G,$$

es llamada *homomorfismo de grupos*. Si f es inyectiva, decimos que f es un *monomorfismo* de grupos, si es sobreyectiva decimos que es un *epimorfismo* de grupos y si es biyectiva decimos que es un *isomorfismo* de grupos.

Un grupo en el cual todo elemento tiene orden una potencia (≥ 0) de algún primo fijo p es llamado *p-grupo*. Un grupo que sea isomorfo a $\mathbb{Z}_p^n$, con p primo, es llamado *p-grupo elemental*.

Definición 1.1.2. Un grupo abeliano G es llamado *grupo torsión*, si todo elemento en G es de orden finito. Si el único elemento de orden finito en G es el elemento identidad, decimos que G es un *grupo libre de torsión*.

A continuación enunciamos el teorema de estructura para grupos abelianos finitamente generados.

Teorema 1.1.2. *[8] Todo grupo abeliano finitamente generado se puede expresar de la siguiente forma*

$$G \simeq C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus \mathbb{C}_{n_r} \oplus \mathbb{Z}^d,$$

donde $n_i | n_{i+1}$ *para todo* $i \in [1, r-1]$ *y* $d \in \mathbb{N}_0$. *En particular, si* G *es finito,*

$$G \simeq C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus \mathbb{C}_{n_r}.$$

Y si G *es finitamente generado y libre de torsión,*

$$G \simeq \mathbb{Z}^n,$$

para algún $n \in \mathbb{N}$.

Definición 1.1.3. Un grupo G es *ordenable* si G admite un orden total invariante a izquierda, esto es, G admite un orden total $\preceq$ tal que

$$g_1 \preceq g_2 \Rightarrow g + g_1 \preceq g + g_2, \quad \textit{para todo } g_1, g_2, g \in G.$$

Observemos que si $G_1 \simeq G_2$ y G_1 es ordenable, G_2 también lo es, ya que si $\phi : G_2 \to G_1$ es un isomorfismo, ϕ induce un orden en G_2 dado por $g_1 \preceq g_2 \Leftrightarrow \phi(g_1) \preceq \phi(g_2)$, el cual es invariante a izquierda.

Ejemplo 1.1.1. $(\mathbb{Z}^n, +)$ es un grupo ordenable. Basta considerar el orden lexicográfico sobre $\mathbb{Z}^n$.

El siguiente teorema nos da una condición suficiente y necesaria sobre los subgrupos de un grupo para que éste sea ordenable.

Teorema 1.1.3. *[11] Un grupo es ordenable si y solo si cualquier subgrupo finitamente generado de él lo es.*

Ejemplo 1.1.2. Todo grupo abeliano libre de torsión es ordenable. En efecto, sea G un grupo abeliano libre de torsión, sea H un subgrupo finitamente generado de G, H es libre de torsión. Por el Teorema 1.1.2, $H \simeq \mathbb{Z}^n$ para algún $n \in \mathbb{N}$. Como $\mathbb{Z}^n$ es ordenable entonces, H es ordenable y por Teorema 1.1.3, G es ordenable.

1.1.1. Secuencias finitas en grupos abelianos

La notación que damos aquí fue introducida por A. Geroldinger y F. Halter-Koch en [7].

Sea G un grupo abeliano. Una *secuencia* finita (o simplemente una secuencia) S sobre G es una lista finita de elementos de G, digamos $S = g_1, g_2, \ldots, g_l$; posiblemente con $g_i = g_j$ para ciertos $i \neq j$.

Para facilitar la notación de las secuencias, una secuencia S sobre un grupo abeliano G la escribiremos como un producto formal $S = g_1 \cdot g_2 \cdot \ldots \cdot g_l =$

$\prod_{i=1}^{l} g_i$ (el orden de colocación de los elementos es irrelevante). También podemos escribir la secuencia S como

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)},$$

donde $\mathsf{v}_g(S)$ es llamada *multiplicidad* de g en S (el número de veces que el elemento g aparece en la secuencia S).

El *soporte* de una secuencia S sobre G es el conjunto

$$\operatorname{supp}(S) := \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G.$$

Si $S = \prod_{g \in G} g^{\mathsf{v}_g(S)}$, llamamos *longitud* de S al entero

$$|S| := \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0.$$

En otras palabras, si escribimos $S = g_1 \cdot g_2 \cdot \ldots \cdot g_l$ entonces, $|S| = l$.

Si $\operatorname{supp}(S) = \{g_1, \ldots, g_l\}$, llamamos *número de cross* de S al número

$$\mathsf{k}(S) := \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)}.$$

El conjunto de todas las secuencias sobre G es denotado por $\mathcal{F}(G)$.

Decimos que una secuencia $S \in \mathcal{F}(G)$ es *libre de cuadrados* si $\mathsf{v}_g(S) \leq 1$ para todo $g \in G$. Observemos que una secuencia libre de cuadrados en $\mathcal{F}(G)$ puede ser vista como un subconjunto de G, si la identificamos con su soporte.

Terminaremos esta sección definiendo una propiedad vinculada con las secuencias en grupos abelianos, la cual está estrechamente relacionada con los resultados sobre combinatoria que presentamos en el Capítulo 3.

Dado $l \in \mathbb{N}_0$, denotamos por S_l al grupo de permutaciones de $[1, l]$.

Definición 1.1.4. Sea G un grupo abeliano y $l \in \mathbb{N}$. Decimos que l tiene la *propiedad* **P** para G si

> Para toda secuencia libre de cuadrados $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ y toda secuencia $\prod_{i=1}^{l} h_i \in \mathcal{F}(G)$, existe alguna permutación $\pi \in S_l$ tal que la secuencia $\prod_{i=1}^{l}(g_i + h_{\pi(i)})$ es libre de cuadrados.

Notemos que si G es finito, para verificar que $l \in \mathbb{N}$ tiene la propiedad **P** para G, podemos suponer $l \in [1, \exp(G)]$.

Ejemplo 1.1.3. Si G es un grupo libre de torsión entonces, todo $l \in \mathbb{N}$ tiene la propiedad **P** para G. En efecto, por ser G libre de torsión, G es ordenable (ver Ejemplo 1.1.2). Si $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ es libre de cuadrados y $\prod_{i=1}^{l} h_i \in \mathcal{F}(G)$ entonces, después de una reordenación de los términos de las secuencias (si es necesaria), podemos suponer $g_1 < g_2 < \ldots < g_l$ y $h_1 \leq h_2 \leq \ldots \leq h_l$, así $g_1 + h_1 < g_2 + h_2 < \ldots < g_l + h_l$, por lo que $(g_1 + h_1) \cdot (g_2 + h_2) \cdot \ldots \cdot (g_l + h_l)$ es libre de cuadrados.

Ejemplo 1.1.4. Sea G un grupo abeliano. Si $l = \mathrm{ord}(g)$, para algún $g \in G$ de orden finito entonces, l no tiene la propiedad **P** para G. Para verificar esto, basta considerar las secuencias $S = \prod_{i=1}^{l} g_i$, con $g_i = ig$ para $i \in [1, l]$, y $T = \prod_{i=1}^{l} h_i$, con $h_i = 0$ para $i \in [1, l-1]$ y $h_l = g$. Como $\mathrm{ord}(g) = l$, la secuencia S es libre de cuadrados. Sea $\pi \in S_l$ y sea $j \in [1, l]$ tal que $\pi(j) = l$, notemos que $h_{\pi(j)} = h_l = g$ y $h_{\pi(i)} = 0$ para $i \neq j$. Entonces, si $j = l$, $g_l + h_{\pi(l)} = lg + g = 0 + g = g_1 + h_{\pi(1)}$, análogamente, si $j < l$, $g_j + h_{\pi(j)} = g_j + h_l = jg + g = (j+1)g = g_{j+1} + h_{\pi(j+1)}$, de manera que la secuencia $\prod_{i=1}^{l}(g_i + h_{\pi(i)})$ no es libre de cuadrados. Como $\pi \in S_l$ es arbitraria, l no tiene la propiedad **P** para G.

1.2. Anillos

Definición 1.2.1. Un *anillo* es un conjunto no vacío R junto con dos operaciones binarias (usualmente denotadas como adición y multiplicación) tal que:

(i) $(R, +)$ es un grupo abeliano;

(ii) $(ab)c = a(bc)$ para todo $a, b, c \in R$ (multiplicación asociativa);

(iii) $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$ (leyes distributivas a izquierda y derecha).

Si además:

(iv) $ab = ba$ para todo $a, b \in R$,

entonces R se dice que es un *anillo conmutativo*. Si R contiene un elemento 1_R tal que

(v) $1_R a = a1_R = a$ para todo $a \in R$,

entonces R se dice que es un *anillo con identidad*.

Sean R_1 y R_2 anillos. Un homomorfismo de grupos $f : R_1 \to R_2$ tal que $f(ab) = f(a)f(b)$ para todo $a, b \in R_1$, es llamado *homomorfismo de anillos*. Si f es inyectiva, decimos que f es un *monomorfismo*, si es sobreyectiva decimos que es un *epimorfismo* y si es biyectiva decimos que es un *isomorfismo*.

Definición 1.2.2. Un elemento no nulo a en un anillo R se dice que es un *divisor de cero a izquierda* [respectivamente a derecha] si existe $b \in R$ no nulo tal que $ab = 0$ [respectivamente $ba = 0$]. Un *divisor de cero* es un elemento de R el cual es al mismo tiempo un divisor de cero a izquierda y a derecha.

Definición 1.2.3. Un elemento a en un anillo R con identidad se dice que es *invertible a izquierda* [respectivamente a derecha] si existe $c \in R$ [respectivamente $b \in R$] tal que $ca = 1_R$ [respectivamente $ab = 1_R$]. El elemento c [respectivamente b] es llamado un inverso a izquierda [respectivamente a derecha] de a. Un elemento $a \in R$ que es al mismo tiempo invertible a izquierda y derecha se dice que es *invertible* o que es una *unidad*.

El conjunto de unidades en un anillo R con identidad forman un grupo bajo la multiplicación y será denotado por $R^{\times}$.

Definición 1.2.4. Un anillo conmutativo R con identidad $1_R \neq 0$ y sin divisores de cero es llamado un *dominio de integridad*. Un anillo D con identidad $1_D \neq 0$ en el cual todo elemento no nulo es una unidad es llamado un *anillo de división*. Un *campo* es un anillo de división conmutativo.

En adelante, siempre que no haya confusión, para un anillo R con identidad, se denotará simplemente 1 a la identidad del anillo y supondremos siempre que $1 \neq 0$.

Definición 1.2.5. Sea R un anillo. Si existe el menor entero positivo n tal que $na = 0$ para todo $a \in R$, entonces se dice que R tiene *característica* n y lo denotamos por $\text{car}(R) = n$. Si no existe tal n decimos que R tiene *característica cero* $(\text{car}(R) = 0)$.

Observación 1.2.1. [8] Sea R un anillo conmutativo con identidad.

(i) Si R tiene característica p primo y $a_1, \ldots, a_l \in R$ entonces,

$$(a_1 + \ldots + a_l)^{p^n} = a_1^{p^n} + \ldots + a_l^{p^n}$$

(ii) Para $a, b \in R$ y $0 < n \in \mathbb{N}$ se cumple

$$a^n - b^n = (a-b)(\sum_{i=0}^{n-1} a^{n-1-i}b^i).$$

1.2.1. Ideales

Definición 1.2.6. Sea R un anillo y S un subconjunto no vacío de R que es cerrado bajo las operaciones de adición y multiplicación en R. Si S es en sí mismo un anillo bajo estas operaciones entonces, S es llamado un *subanillo de* R. Un subanillo I de un anillo R es un *ideal a izquierda* si cumple que

$$r \in R \quad \text{y} \quad x \in I \quad \Rightarrow \quad rx \in I;$$

I es un *ideal a derecha* si cumple que

$$r \in R \quad \text{y} \quad x \in I \quad \Rightarrow \quad xr \in I;$$

I es un *ideal* si es un ideal a izquierda y derecha.

Si P es un ideal en un anillo conmutativo R tal que $P \neq R$ y para todo $a, b \in R$

$$ab \in P \Rightarrow a \in P \ \text{ ó } \ b \in P, \tag{1.1}$$

entonces, decimos que P es un *ideal primo.*

Un ideal M en un anillo R se dice que es *maximal* si $M \neq R$ y para cualquier ideal N tal que $M \subseteq N \subseteq R$ se tiene $N = M$ o $N = R$.

Teorema 1.2.1. *[8] Sea M un ideal en un anillo conmutativo R con identidad. Si M es maximal entonces, el anillo cociente R/M es un campo.*

1.2.2. Anillo de los polinomios

Sea R un anillo y sea $R[x]$ el anillo de los polinomios sobre R en la indeterminada x, a saber, el conjunto de todos los símbolos

$$a_0 + a_1x + \ldots + a_nx^n,$$

donde n puede ser cualquier entero no negativo y donde los *coeficientes* $a_0, a_1, \ldots, a_n$ pertenecen todos a R.
Si $p(x) = a_0 + a_1x + \ldots + a_nx^n \neq 0$ y $a_n \neq 0$, entonces el *grado* de $p(x)$, denotado $\deg(p(x))$, es n; y el *coeficiente líder* es a_n.

El siguiente teorema garantiza que el algoritmo de la división es satisfecho en $R[x]$.

Teorema 1.2.2. *[8] Sea R un anillo con identidad y $f(x), g(x) \in R[x]$ polinomios no nulos tales que el coeficiente líder de $g(x)$ es una unidad en R. Entonces existen polinomios únicos $q(x), r(x) \in R[x]$ tales que*

$$f(x) = q(x)g(x) + r(x) \quad y \quad \deg(r(x)) < \deg(g(x)).$$

Teorema 1.2.3. *[8] Si R es un dominio de integridad, contenido en un campo F, y $f(x) \in R[x]$ tiene grado n entonces, $f(x)$ tiene a lo más n raíces distintas.*

1.2.3. Campos y extensiones de campos

Teorema 1.2.4. *[8] Sea F un campo y P la intersección de todos los subcampos de F entonces, P es un campo que no posee subcampos propios. Si $\text{car}(F) = p$ entonces, $P \simeq \mathbb{Z}_p$. Si $\text{car}(F) = 0$ entonces, $P \simeq \mathbb{Q}$.*

El campo P del teorema anterior es llamado *subcampo primo del campo* F.

Teorema 1.2.5. *[8] Si F es un campo y G es un subgrupo finito de $F^\times$ entonces, G es un grupo cíclico.*

Sea F un campo, y sea $\mu_n(F) := \{\xi \in F : \xi^n = 1\}$. $\mu_n(F)$ es no vacío, dado que $1 \in \mu_n(F)$, más aún, $\mu_n(\xi)$ es un subgrupo del grupo multiplicativo de elementos no nulos de F, en efecto, sean $\xi_1, \xi_2 \in \mu_n(K)$ entonces,

$$\begin{aligned}(\xi_1(\xi_2)^{-1})^n &= (\xi_1)^n((\xi_2)^{-1})^n \\ &= (\xi_1)^n((\xi_2)^n)^{-1} \\ &= 1(1)^{-1} \\ &= 1\end{aligned}$$

$\mu_n(F)$ es llamado *el grupo de las n-raíces de la unidad en F*, este grupo es cíclico (Teorema 1.2.5) y tiene orden a lo más n (Teorema 1.2.3). Una n-raíz de la unidad ξ es llamada *n-raíz primitiva de la unidad*, si $\xi^m \neq 1$ para todo $m \in [1, n-1]$.

Un campo F es una *extensión de un campo* K, si K es un subcampo de F.

Si F es un campo, extensión de un campo K, y $X \subseteq F$, el subcampo generado por $K \cup X$ es llamado el *subcampo generado por X sobre K*, y denotado por $K(X)$.

Sea F un campo extensión de un campo K, un elemento $u \in F$ se dice algebraico sobre K si u es raíz de un polinomio no nulo $f \in K[x]$. Por ejemplo, si $\xi \in \mathbb{C}$ es una n-raíz de la unidad, entonces ξ es algebraico sobre $\mathbb{Q}$ (ξ es

raíz de $x^n - 1$). El conjunto de todos los elementos de F que son algebraicos sobre K forman un anillo, llamado el *anillo de enteros algebraicos* de F sobre K.

1.3. Módulos y espacios vectoriales

Definición 1.3.1. Sea R un anillo. Un *R-módulo* (a izquierda) es un grupo abeliano aditivo A junto con una función $R \times A \to A$ (la imagen de (r, a) siendo denotada por ra) tal que para todo $r, s \in R$ y $a, b \in A$:

(i) $r(a + b) = ra + rb$.

(ii) $(r + s)a = ra + sa$.

(iii) $r(sa) = (rs)a$.

Si R tiene un elemento identidad 1_R y

(iv) $1_R a = a$ para todo $a \in A$,

entonces se dice que A es un *R-módulo unitario*. Si R es un anillo de división, entonces el R-módulo unitario es un *espacio vectorial* (a izquierda).

Un R-módulo a derecha (unitario) es definido similarmente vía una función $A \times R \to A$ denotada $(a, r) \mapsto ar$ y satisfaciendo las analogías obvias de (i)-(iv). De ahora en adelante, a menos que se especifique lo contrario, R-módulo significa R-módulo a izquierda y se entiende que todos los teoremas acerca de R-módulos a izquierda también son ciertos para R-módulos a derecha. Si R es conmutativo, es fácil verificar que todo R-módulo a izquierda A, puede dársele la estructura de un R-módulo a derecha definiendo $ar = ra$

para $r \in R, a \in A$. A menos que se especifique lo contrario, todo módulo A sobre un anillo conmutativo R se supone que es un módulo tanto a izquierda como a derecha con $ar = ra$ para todo $r \in R, a \in A$.

Ejemplo 1.3.1. Todo grupo abeliano aditivo G es un $\mathbb{Z}$- módulo unitario, con $na = a + a + \ldots + a$, n veces $(n \in \mathbb{Z}, a \in G)$.

Sean R un anillo y A y B R-módulos. Un homomorfismo de grupos $f : A \to B$ tal que $f(ra) = rf(a)$ para todo $a \in A$ y $r \in R$, es llamado *homomorfismo de módulos*. Si f es inyectiva, decimos que f es un *monomorfismo*, si es sobreyectiva decimos que es un *epimorfismo* y si es biyectiva decimos que es un *isomorfismo*. Si R es un anillo de división entonces, f es llamada *transformación lineal*.

Un subconjunto X de un R-módulo A se dice *linealmente independiente* si para $x_1, \ldots, x_n \in X$ distintos y $r_i \in R$.

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n = 0 \Rightarrow r_i = 0, \quad \text{para todo } \ i \in [1, n].$$

Un conjunto que no es linealmente independiente se dice que es *linealmete dependiente*.

Teorema 1.3.1. *[8] Si R es un anillo con identidad, A es un R-módulo unitario, y $Y \subseteq A$ entonces, Y genera a A si y solo si todo elemento de A puede ser escrito como combinación lineal:*

$$r_1y_1 + r_2y_2 + \ldots + r_ny_n \quad (r_i \in R,\ y_i \in Y,\ n \in \mathbb{N}).$$

Definición 1.3.2. Un subconjunto linealmente independiente de A que genera a A es llamado una *base* de A.

Definición 1.3.3. Un módulo unitario F sobre un anillo R con identidad, el cual tiene una base no vacía X, es llamado un *R-módulo libre* sobre el conjunto X.

Definición 1.3.4. Sea R un anillo con identidad y F un R-módulo libre. El número cardinal de cualquier base V de F es llamado *dimensión* (o *rango*) de F sobre R y denotado por $\dim_R V$ (o rgo(V)).

Ejemplo 1.3.2. Sea R un anillo, I un conjunto finito de índices y $R^I := \prod_I R = \{(a(i))_{i\in I} \mid a(i) \in R\}$. R^I es un R-módulo con base:
$e_j = (a(i))_{i\in I}$ con $a(i) = \begin{cases} 0 & \text{si } i \neq j, \\ 1 & \text{si } i = j \end{cases}$. Luego $\dim_R R^I = |I|$.

Teorema 1.3.2. *([8]) Si $f : V \to V'$ es una transformación lineal de espacios vectoriales sobre un anillo de división R entonces,*

$$\dim_R V = \dim_R(\mathrm{Ker}(f)) + \dim_R(Im(f)).$$

Terminamos esta sección mostrando un resultado que da una cota inferior para la dimensión de la imagen de la composición de transformaciones lineales.

Teorema 1.3.3. *Sea R un anillo de división, U un espacio vectorial sobre R de dimensión finita, $l \in \mathbb{N}$ y $\lambda_1, \ldots, \lambda_l : U \to U$ transformaciones R-lineales entonces,*

$$\dim_R(\lambda_1 \circ \ldots \circ \lambda_l)(U) \geq \sum_{i=1}^{l} \dim_R \lambda_i(U) - (l-1)\dim_R U$$

Demostración. Procederemos por inducción sobre l. Supongamos $l = 2$. Afirmamos que $\dim_R \ker(\lambda_1 \circ \lambda_2) \leq \dim_R \ker \lambda_1 + \dim_R \ker \lambda_2$, en efecto,

$$\begin{aligned} x \in \ker \lambda_2 \Rightarrow \lambda_2(x) = 0 \Rightarrow \lambda_1(\lambda_2(x)) = \lambda_1(0) \quad &\Rightarrow \quad \lambda_1 \circ \lambda_2(x) = 0 \\ &\Rightarrow \quad x \in \ker(\lambda_1 \circ \lambda_2) \end{aligned}$$

así $\ker \lambda_2 \subseteq \ker(\lambda_1 \circ \lambda_2)$. Si $\ker \lambda_2 = \ker(\lambda_1 \circ \lambda_2)$, evidentemente $\dim_R \ker(\lambda_1 \circ \lambda_2) \leq \dim_R \ker \lambda_1 + \dim_R \ker \lambda_2$. Supongamos que $\ker \lambda_2$ es subespacio propio de $\ker(\lambda_1 \circ \lambda_2)$. Sea $B_1 = \{u_1, \ldots, u_r\}$ una base de $\ker \lambda_2$, entonces existe un número finito de vectores $u_{r+1}, \ldots, u_k$ tales que $B = \{u_1, \ldots, u_r, u_{r+1}, \ldots, u_k\}$ es una base de $\ker(\lambda_1 \circ \lambda_2)$.

Por otro lado, $u_i \in \ker(\lambda_1 \circ \lambda_2) \Rightarrow \lambda_1 \circ \lambda_2(u_i) = 0 \Rightarrow \lambda_1(\lambda_2(u_i)) = 0 \Rightarrow \lambda_2(u_i) \in \ker \lambda_1 \ \forall i \in [1, k]$.

Observemos que $\{\lambda_2(u_{r+1}), \ldots, \lambda_2(u_k)\}$ es linealmente independiente, en efecto,

$$
\begin{aligned}
& \alpha_{r+1}\lambda_2(u_{r+1}) + \ldots + \alpha_k\lambda_2(u_k) = 0 \ \text{ para ciertos } \alpha_i \in K \\
\Rightarrow \ & \lambda_2(\alpha_{r+1}u_{r+1} + \ldots + \alpha_k u_k) = 0 \\
\Rightarrow \ & \alpha_{r+1}u_{r+1} + \ldots + \alpha_k u_k \in \ker \lambda_2 \\
\Rightarrow \ & \alpha_{r+1}u_{r+1} + \ldots + \alpha_k u_k = \alpha_1 u_1 + \ldots + \alpha_r u_r \ \ (B_1 \text{ es base de } \ \ker \lambda_2) \\
\Rightarrow \ & \alpha_1 u_1 + \ldots + \alpha_r u_r - \alpha_{r+1}u_{r+1} - \ldots - \alpha_k u_k = 0 \\
\Rightarrow \ & \alpha_i u_i = 0 \ \ \forall i \in [1, k] \quad (B \text{ es base de } \ \ker(\lambda_1 \circ \lambda_2)) \\
\Rightarrow \ & \lambda_2(\alpha_i u_i) = 0 \ \ \forall i \in [1, k] \\
\Rightarrow \ & \alpha_i \lambda_2(u_i) = 0 \ \ \forall i \in [r+1, k]
\end{aligned}
$$

luego, $\dim_R \ker \lambda_1 \geq k - r$. Así,

$$\dim_R \ker(\lambda_1 \circ \lambda_2) = k = r + (k - r) \leq \dim_R \ker \lambda_2 + \dim_R \ker \lambda_1$$

y por el Teorema 1.3.2

$$
\begin{aligned}
& \dim_R \ker(\lambda_1 \circ \lambda_2) \leq \dim_R \ker \lambda_2 + \dim_R \ker \lambda_1 \\
\Rightarrow \ & \dim_R U - \dim_R(\lambda_1 \circ \lambda_2)(U) \leq \dim_R U - \dim_R \lambda_2(U) + \dim_R U - \dim_R \lambda_1(U) \\
\Rightarrow \ & \dim_R(\lambda_1 \circ \lambda_2)(U) \geq + \dim_R \lambda_1(U) + \dim_R \lambda_2(U) - \dim_R U.
\end{aligned}
$$

Supongamos que para $\lambda_1, \ldots, \lambda_l : U \to U$

$$\dim_R(\lambda_1 \circ ... \circ \lambda_l)(U) \geq \sum_{i=1}^{l} \dim_R \lambda_i(U) - (l-1)\dim_R U$$

Sean $\lambda_1, \ldots, \lambda_l, \lambda_{l+1} : U \to U$ transformaciones R-lineales

$$\begin{aligned}
\dim_R(\lambda_1 \circ ... \circ \lambda_l \circ \lambda_{l+1}) &= \dim_R((\lambda_1 \circ ... \circ \lambda_l) \circ \lambda_{l+1}) \\
&\geq \dim_R(\lambda_1 \circ ... \circ \lambda_l) + \dim_R \lambda_{l+1} - \dim_R U \ (\text{ caso } l = 2) \\
&\geq \sum_{i=1}^{l} \dim_R \lambda_i(U) - (l-1)\dim_R U + \dim_R \lambda_{l+1} - \dim_R U \\
&= \sum_{i=1}^{l+1} \dim_R \lambda_i(U) - l \dim_R U
\end{aligned}$$

□

1.4. Álgebras

Definición 1.4.1. Sea R un anillo conmutativo con identidad. Un *R-álgebra* (o *álgebra sobre R*) A es un anillo A, tal que:

(i) $(A, +)$ es un R-módulo (a izquierda) unitario;

(ii) $r(ab) = (ra)b = a(rb)$ para todo $r \in R$ y $a, b \in A$. Un R-álgebra A que, como anillo, es un anillo de división, es llamada un *álgebra de división*.

Ejemplo 1.4.1. Todo anillo R es un grupo abeliano aditivo y por tanto un $\mathbb{Z}$-módulo. Es fácil ver que R es un $\mathbb{Z}$-álgebra.

Ejemplo 1.4.2. Todo anillo conmutativo R con identidad es un R-álgebra.

Sea R un anillo conmutativo con identidad y, A y B R-álgebras. Un *homomorfismo de R-álgebras* $f : A \to B$ es un homomorfismo de anillos que es también un homomorfismo de R-módulos.

Capítulo 2

Álgebras de grupo de grupos abelianos finitos

En este capítulo estudiamos las álgebras de grupo, específicamente, damos algunas de sus propiedades y presentamos los resultados principales. Como una herramienta para tal estudio, usamos las propiedades de los caracteres de un grupo, las cuales también presentamos en forma detallada. En adelante, supondremos que R es un anillo conmutativo con identidad $1 \neq 0$.

2.1. Álgebras de grupo

Definición 2.1.1. Sea R un anillo conmutativo y G un grupo abeliano finito. El *álgebra de grupo* $R[G]$ de G sobre R es el R-módulo libre con base $\{X^g : g \in G\}$ (construido con un símbolo X), en consecuencia los elementos de $R[G]$ son de la forma

$$a_1X^{g_1} + a_2X^{g_2} + \ldots + a_lX^{g_l}$$

donde $a_i \in R$ y $g_i \in G$ para todo $i \in [1, l]$. Este elemento puede ser denotado, en general, por

$$\sum_{g \in G} a_g X^g.$$

$R[G]$ es un álgebra sobre R con respecto a la adición definida por

$$\sum_{g \in G} a_g X^g + \sum_{g \in G} b_g X^g = \sum_{g \in G} (a_g + b_g) X^g,$$

el producto por un escalar dado por

$$a \sum_{g \in G} a_g X^g = \sum_{g \in G} (a a_g) X^g,$$

y dotada de la operación multiplicación definida por

$$(\sum_{g \in G} a_g X^g)(\sum_{g \in G} b_g X^g) = \sum_{g \in G} (\sum_{h \in G} a_h b_{g-h}) X^g.$$

Mostraremos que, en efecto, $R[G]$ es un R-álgebra.

Sean $\sum_{g \in G} a_g X^g$, $\sum_{g \in G} b_g X^g$ y $\sum_{g \in G} c_g X^g \in R[G]$.

Veamos que $(R[G], +)$ es un grupo abeliano.

$$\begin{aligned}
(\sum_{g \in G} a_g X^g + \sum_{g \in G} b_g X^g) + \sum_{g \in G} c_g X^g &= \sum_{g \in G} (a_g + b_g) X^g + \sum_{g \in G} c_g X^g \\
&= \sum_{g \in G} ((a_g + b_g) + c_g) X^g \\
&= \sum_{g \in G} (a_g + (b_g + c_g)) X^g \\
&= \sum_{g \in G} a_g X^g + (\sum_{g \in G} b_g X^g + \sum_{g \in G} b_g X^g)
\end{aligned}$$

$\sum_{g \in G} 0 X^g \in R[G]$ es tal que,

$$\begin{aligned}
\sum_{g \in G} a_g X^g + \sum_{g \in G} 0 X^g &= \sum_{g \in G} (a_g + 0) X^g \\
&= \sum_{g \in G} a_g X^g
\end{aligned}$$

Existe $\sum_{g\in G}(-a_g)X^g \in R[G]$ tal que

$$\begin{aligned}\sum_{g\in G} a_g X^g + \sum_{g\in G}(-a_g)X^g &= \sum_{g\in G}(a_g + (-a_g))X^g \\ &= \sum_{g\in G} 0X^g\end{aligned}$$

$$\begin{aligned}\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g &= \sum_{g\in G}(a_g + b_g)X^g \\ &= \sum_{g\in G}(b_g + a_g)X^g \\ &= \sum_{g\in G} b_g X^g + \sum_{g\in G} a_g X^g\end{aligned}$$

$(R[G], \cdot)$ es un semigrupo, en efecto,

$$\begin{aligned}[(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)](\sum_{g\in G} c_g X^g) &= (\sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g)(\sum_{g\in G} c_g X^g) \\ &= \sum_{g\in G}[\sum_{k\in G}((\sum_{h\in G} a_h b_{k-h})c_{g-k})]X^g \\ &= \sum_{g\in G}[\sum_{k\in G}(\sum_{h\in G}(a_h b_{k-h})c_{g-k})]X^g\end{aligned}$$

Por otro lado,

$$\begin{aligned}
& (\sum_{g\in G} a_g X^g)[(\sum_{g\in G} b_g X^g)(\sum_{g\in G} c_g X^g)] \\
= \; & (\sum_{g\in G} a_g X^g)(\sum_{g\in G}(\sum_{h\in G} b_h c_{g-h})X^g) \\
= \; & \sum_{g\in G}[\sum_{k\in G}(a_k(\sum_{h\in G} b_h c_{g-k-h}))]X^g \\
= \; & \sum_{g\in G}[\sum_{k\in G}(\sum_{h\in G} a_k(b_h c_{g-k-h}))]X^g \\
= \; & \sum_{g\in G}[\sum_{h\in G}(\sum_{k\in G} a_h(b_k c_{g-k-h}))]X^g \quad \text{(renombrando } h=k\text{)} \\
= \; & \sum_{g\in G}[\sum_{h\in G}(\sum_{t\in G} a_h(b_{t-h} c_{g-t}))]X^g \quad (k=t-h) \\
= \; & \sum_{g\in G}[\sum_{t\in G}(\sum_{h\in G} a_h(b_{t-h} c_{g-t}))]X^g \\
= \; & \sum_{g\in G}[\sum_{k\in G}(\sum_{h\in G} a_h(b_{k-h} c_{g-k}))]X^g \quad \text{(renombrando } t=k\text{)} \\
= \; & \sum_{g\in G}[\sum_{k\in G}(\sum_{h\in G} (a_h b_{k-h})c_{g-k})]X^g \\
= \; & [(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)](\sum_{g\in G} c_g X^g)
\end{aligned}$$

La multiplicación es distributiva con respecto a la suma, en efecto,

$$\begin{aligned}
(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g + \sum_{g\in G} c_g X^g) &= (\sum_{g\in G} a_g X^g)(\sum_{g\in G}(b_g + c_g)X^g) \\
&= \sum_{g\in G}(\sum_{h\in G} a_h(b_{g-h} + c_{g-h}))X^g \\
&= \sum_{g\in G}(\sum_{h\in G}(a_h b_{g-h} + a_h c_{g-h}))X^g \\
&= \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h} + \sum_{h\in G} a_h c_{g-h})X^g \\
&= \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g + \sum_{g\in G}(\sum_{h\in G} a_h c_{g-h})X^g \\
&= (\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g) + (\sum_{g\in G} a_g X^g)(\sum_{g\in G} c_g X^g)
\end{aligned}$$

Análogamente se prueba,

$$(\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g)(\sum_{g\in G} c_g X^g) = (\sum_{g\in G} a_g X^g)(\sum_{g\in G} c_g X^g) + (\sum_{g\in G} b_g X^g)(\sum_{g\in G} c_g X^g).$$

Ahora veamos que, $(R[G], +)$ es un R-módulo unitario. Sean $r, s \in R$ y $\sum_{g\in G} a_g X^g$,$\sum_{g\in G} b_g X^g \in R[G]$

$$\begin{aligned} r(\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g) &= r\sum_{g\in G}(a_g + b_g)X^g \\ &= \sum_{g\in G}(r(a_g + b_g))X^g \\ &= \sum_{g\in G}(ra_g + rb_g)X^g \\ &= \sum_{g\in G}(ra_g)X^g + \sum_{g\in G}(rb_g)X^g \\ &= r\sum_{g\in G} a_g X^g + r\sum_{g\in G} b_g X^g \end{aligned}$$

$$\begin{aligned} (r+s)\sum_{g\in G} a_g X^g &= \sum_{g\in G}((r+s)a_g)X^g \\ &= \sum_{g\in G}(ra_g + sa_g)X^g \\ &= \sum_{g\in G}(ra_g)X^g + \sum_{g\in G}(sa_g)X^g \\ &= r\sum_{g\in G} a_g X^g + s\sum_{g\in G} a_g X^g \end{aligned}$$

$$\begin{aligned} r(s\sum_{g\in G} a_g X^g) = r\sum_{g\in G}(sa_g)X^g &= \sum_{g\in G}(r(sa_g))X^g \\ &= \sum_{g\in G}((rs)a_g)X^g \\ &= (rs)\sum_{g\in G} a_g X^g \end{aligned}$$

$$1\sum_{g\in G} a_g X^g = \sum_{g\in G}(1a_g)X^g = \sum_{g\in G} a_g X^g.$$

Y por último, para $r \in R\,;\, f, h \in R[G]$ se tiene que $r(fh) = (rf)h = f(rh)$, en efecto, sean $f = \sum_{g\in G} a_g X^g$, $h = \sum_{g\in G} b_g X^g$ entonces

$$\begin{aligned} r(fh) = r[(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)] &= r[\sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g] \\ &= \sum_{g\in G}(r(\sum_{h\in G} a_h b_{g-h}))X^g \\ &= \sum_{g\in G}(\sum_{h\in G} r(a_h b_{g-h}))X^g \\ &= \sum_{g\in G}(\sum_{h\in G}(ra_h) b_{g-h})X^g \\ &= (\sum_{g\in G}(ra_g)X^g)(\sum_{g\in G} b_g X^g) \\ &= (r\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g) \\ &= (rf)h \end{aligned}$$

$$\begin{aligned} r(fh) = r[(\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)] &= r[\sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g] \\ &= \sum_{g\in G}(r(\sum_{h\in G} a_h b_{g-h}))X^g \\ &= \sum_{g\in G}(\sum_{h\in G} r(a_h b_{g-h}))X^g \\ &= \sum_{g\in G}(\sum_{h\in G} a_h(rb_{g-h}))X^g \\ &= (\sum_{g\in G}(a_g)X^g)(\sum_{g\in G}(rb_g)X^g) \\ &= (\sum_{g\in G}(a_g)X^g)(r\sum_{g\in G} b_g X^g) \\ &= f(rh). \end{aligned}$$

Ejemplo 2.1.1. Sea R un anillo conmutativo con identidad, G un grupo abeliano finito y $R[G]$ el álgebra de grupo de G sobre R, entonces para todo $g \in G$ y $n \in \mathbb{N}_0$, $(X^g)^n = X^{ng}$. Veamos, los casos $n = 0$ y $n = 1$ son evidentes.

Supongamos que para $r \geq 2$ se tiene que $(X^g)^r = X^{rg}$ entonces

$$\begin{aligned}
(X^g)^{r+1} &= (X^g)^r(X^g) \\
&= X^{rg}X^g \\
&= (\sum_{k\in G} a_k X^k)(\sum_{k\in G} b_k X^k), \text{ con } a_k = 0 \text{ para } k \neq rg,\ a_{rg} = 1, \\
&\qquad\qquad b_k = 0 \text{ para } k \neq g \text{ y } b_g = 1. \\
&= \sum_{k\in G}(\sum_{h\in G} a_h b_{k-h})X^k \\
&= a_{rg}b_{rg+g-rg}X^{rg+g} \\
&= a_{rg}b_g X^{rg+g} \\
&= X^{rg+g} \\
&= X^{(r+1)g}.
\end{aligned}$$

Ejemplo 2.1.2. Consideremos el anillo de enteros $\mathbb{Z}$ y el grupo abeliano finito $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. El álgebra de grupo $\mathbb{Z}[\mathbb{Z}_2]$ de $\mathbb{Z}_2$ sobre $\mathbb{Z}$ es el $\mathbb{Z}$-módulo generado por $\{X^{\bar{0}}, X^{\bar{1}}\}$. Si $f \in \mathbb{Z}[\mathbb{Z}_2]$ entonces

$$\begin{aligned}
f &= \sum_{g\in\mathbb{Z}_2} a_g X^g \quad a_g \in \mathbb{Z} \\
&= a_{\bar{0}}X^{\bar{0}} + a_{\bar{1}}X^{\bar{1}} \quad a_{\bar{0}}, a_{\bar{1}} \in \mathbb{Z} \\
&= aX^{\bar{1}} + b \quad a, b \in \mathbb{Z}.
\end{aligned}$$

Observar que el álgebra de grupo $R[G]$ de un grupo G sobre un anillo R, visto como un anillo, tiene la misma característica de R, en particular, si $\text{car}(R) \neq 0$ entonces, $\text{car}(R)f = 0$ para todo $f \in R[G]$.

Notemos también que podemos ver un anillo R como un subconjunto del álgebra de grupo $R[G]$ de un grupo G sobre R, escribiendo cada elemento $a \in R$ como $a = \sum_{g\in G} a_g X^g$, donde $a_g = 0, \forall g \neq 0, a_0 = a$ para todo

$a \in R$, de esta manera la multiplicación en R coincide con la multiplicación en $R[G]$ para los elementos de R vistos como elementos de $R[G]$, en efecto, sean $a, b \in R$

$$
\begin{aligned}
& (\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g), \text{ donde } a_g = 0, \forall g \neq 0 \text{ y } a_0 = a, \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad b_g = 0, \forall g \neq 0 \text{ y } b_0 = b. \\
= \quad & \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h}) X^g \\
= \quad & \sum_{g\in G}(a_0 b_g) X^g \\
= \quad & a_0 \sum_{g\in G} b_g X^g \\
= \quad & a_0 b_0 \\
= \quad & ab
\end{aligned}
$$

Observación 2.1.1. Sea $R[G]$ el álgebra de grupo de un grupo G sobre un anillo R.

(i) Un elemento de R es un divisor de cero de $R[G]$ si y solo si es un divisor de cero de R.

(ii) Un elemento de R es una unidad de $R[G]$ si y sólo si es una unidad de R.

En efecto,

(i) Sea $a \in R$ un divisor de cero de $R[G]$ entonces, existe $f = \sum_{g\in G} a_g X^g \in R[G]$, con a_g no todos nulos tal que $af = 0$, pero

$$af = 0 \Rightarrow a(\sum_{g\in G} a_g X^g) = 0 \Rightarrow \sum_{g\in G} a a_g X^g = 0 \Rightarrow a a_g = 0, \forall g \in G.$$

En particular, para $g' \in G$ tal que $a_{g'} \neq 0$, se tiene $aa_{g'} = 0$. Luego a es un divisor de cero de R.

El recíproco es evidente, ya que $R \subseteq R[G]$.

(ii) Sea $a \in R$ una unidad de $R[G]$ entonces, existe $f = \sum_{g\in G} a_g X^g \in R[G]$ tal que $af = 1_{R[G]}$, pero

$$\begin{aligned} af = 1_{R[G]} &\Rightarrow a(\sum_{g\in G} a_g X^g) = 1_{R[G]} \\ &\Rightarrow \sum_{g\in G} aa_g X^g = 1_{R[G]} \\ &\Rightarrow aa_g = 0, \forall g \in G \text{ y } aa_0 = 1 \text{ con } a_0 \in R, \end{aligned}$$

luego a es una unidad de R.

El recíproco es evidente, ya que $R \subseteq R[G]$.

Proposición 2.1.1. *Sea R un anillo conmutativo con identidad, G un grupo abeliano finito y $R[G]$ el álgebra de grupo de G sobre R.*

(i) La función $\varepsilon : R[G] \to R$, definida por

$$\varepsilon(\sum_{g\in G} a_g X^g) = \sum_{g\in G} a_g$$

es un epimorfismo de R-álgebras.

(ii) Para cada $f \in R[G]$ la función $\mu_f : R[G] \to R[G]$, definida por

$$\mu_f(g) = fg$$

es un homomorfismo de R-módulos.

Demostración. (i) Sean $\sum_{g\in G} a_g X^g$, $\sum_{g\in G} b_g X^g \in R[G]$

$$\begin{aligned}\varepsilon(\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g) &= \varepsilon(\sum_{g\in G}(a_g + b_g)X^g)\\ &= \sum_{g\in G}(a_g + b_g)\\ &= \sum_{g\in G} a_g + \sum_{g\in G} b_g\\ &= \varepsilon(\sum_{g\in G} a_g X^g) + \varepsilon(\sum_{g\in G} b_g X^g).\end{aligned}$$

Por otro lado,

$$\begin{aligned}\varepsilon((\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)) &= \varepsilon(\sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g)\\ &= \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})\\ &= \sum_{h\in G}(\sum_{g\in G} a_h b_{g-h})\\ &= \sum_{h\in G} a_h(\sum_{g\in G} b_g)\\ &= (\sum_{g\in G} a_g)(\sum_{g\in G} b_g)\\ &= \varepsilon(\sum_{g\in G} a_g X^g)\varepsilon(\sum_{g\in G} b_g X^g).\end{aligned}$$

Además, para $a \in R$

$$\begin{aligned}\varepsilon(a(\sum_{g\in G} a_g X^g)) = \varepsilon(\sum_{g\in G} a a_g X^g) &= \sum_{g\in G} a a_g\\ &= a(\sum_{g\in G} a_g)\\ &= a\varepsilon(\sum_{g\in G} a_g X^g).\end{aligned}$$

Sea $f = \sum_{g\in G} a_g X^g \in R[G]$, donde $a_g = 0, \forall g \neq 0$ y $a_0 = a$ entonces,

$$\varepsilon(\sum_{g\in G} a_g X^g) = \sum_{g\in G} a_g = a_0 = a.$$

Luego ε es un epimormismo de R-álgebras.

(ii) Sean $h_1 = \sum_{g\in G} a_g X^g$, $h_2 = \sum_{g\in G} b_g X^g$ y $f = \sum_{g\in G} c_g X^g$ elementos de $R[G]$, y sea $a \in R$

$$\begin{aligned} \mu_f(h_1 + h_2) &= f(h_1 + h_2) \\ &= fh_1 + fh_2 \quad (R[G] \text{ es un anillo}) \\ &= \mu_f(h_1) + \mu_f(h_2) \end{aligned}$$

$$\begin{aligned} \mu_f(ah_1) = f(ah_1) &= a(fh_1) \quad (R[G] \text{ es un } R\text{-álgebra}) \\ &= a\mu_f(h_1) \end{aligned}$$

□

Proposición 2.1.2. *Sea R un anillo conmutativo con identidad, G un grupo abeliano finito y $R[G]$ el álgebra de grupo de G sobre R. Para cada $f \in R[G]$ la función $\mu_f : R[G] \to R[G]$, definida por*

$$\mu_f(g) = fg,$$

(i) es sobreyectiva si y solo si $f \in R[G]^\times$.

(ii) es inyectiva si y solo si f no es un divisor de cero de $R[G]$.

Demostración. (i) Supongamos que μ_f es sobreyectiva entonces, para $1_{R[G]} \in R[G]$, existe $g \in R[G]$ tal que $1_{R[G]} = fg$, luego $f \in R[G]^\times$.

Sea $f \in R[G]^\times$ entonces, existe $g \in R[G]$ tal que $fg = 1_{R[G]}$, pero

$$\begin{aligned} fg = 1_{R[G]} &\Rightarrow (fg)h = h, \forall h \in R[G] \\ &\Rightarrow f(gh) = h, \forall h \in R[G] \\ &\Rightarrow \mu_f(gh) = h, \forall h \in R[G] \end{aligned}$$

Por tanto, μ_f es sobreyectiva.

(ii) Supongamos que f es un divisor de cero de $R[G]$ y μ_f inyectiva, entonces existe $h \in R[G]\backslash 0$ tal que $fh = 0$, pero

$$fh = 0 \Rightarrow \mu_f(h) = 0 = \mu_f(0) \Rightarrow h = 0,$$

lo cual es una notable contradicción, luego f no es un divisor de cero de $R[G]$.

Supongamos que f no es un divisor de cero de $R[G]$ y sean $g, h \in R[G]$ tales que $\mu_f(g) = \mu_f(h)$,

$$\begin{aligned} \mu_f(g) = \mu_f(h) \Rightarrow fg = fh \Rightarrow fg - fh = 0 &\Rightarrow f(g-h) = 0 \\ &\Rightarrow g - h = 0 \\ &\Rightarrow g = h, \end{aligned}$$

luego μ_f es inyectiva.

□

Proposición 2.1.3. *Sea R un campo, G un grupo abeliano finito y $R[G]$ el álgebra de grupo de G sobre R. Entonces todo elemento de $R[G]$, o es una unidad, o es un divisor de cero.*

Demostración. Sea $f \in R[G]$ tal que f no es un divisor de cero entonces, por Proposición 2.1.2, μ_f es inyectiva, de modo que $\ker(\mu_f) = \langle 0 \rangle$.
Como R es un campo, $R[G]$ es un espacio vectorial y, por Teorema 1.3.2,

$$dim_R(R[G]) = dim_R(\mathrm{Ker}(\mu_f)) + dim_R(Im(\mu_f)) = dim_R(Im(\mu_f)).$$

Luego, μ_f es sobreyectiva y la Proposición 2.1.2 implica que $f \in R[G]^\times$. □

2.2. Caracteres de grupos

En esta sección estudiaremos el grupo de caracteres de un grupo abeliano con valores en un campo K, específicamente mostramos algunas propiedades básicas de los caracteres, entre ellas, las propiedades de ortogonalidad. Principalmente estudiamos el caso especial en que el grupo tiene exponente n no nulo y K posee todas las n-raíces de la unidad.

Definición 2.2.1. Una fución $\chi : (G, +) \to (K^X, \cdot)$ donde G es un grupo y K es un campo es llamada un *caracter* de G, si $\chi(g + h) = \chi(g)\chi(h)$ para todo $g, h \in G$, esto es, χ es un caracter del grupo G si es un homomorfismo de grupos.

Ejemplo 2.2.1. Sea $G = \langle g_1 \rangle$ un grupo cíclico finito de orden n, y sea K un campo que contiene una n-raíz de la unidad, digamos ξ.

La función $\chi : G \to K^\times$ dada por

$$\chi(mg_1) = \xi^m,$$

es un caracter de G, ya que para $m, t \in [1, n]$,

$$\chi((mg_1) + (tg_1)) = \chi((m + t)g_1) = \xi^{m+t} = \xi^m\xi^t = \chi(mg_1)\chi(tg_1).$$

Observación 2.2.1. Sea G un grupo con $\exp(G) = n$ y sea K un campo. Si $\chi : G \to K^\times$ es un caracter de G entonces,

(i) Para todo $g \in G$,

$$(\chi(g))^n = \chi(ng) = \chi(0) = 1_K$$

Así $Im(\chi) \subseteq \mu_n(K)$, de modo que $Hom(G, K^\times) = Hom(G, \mu_n(K))$.

(ii) $Hom(G, K^\times) = Hom(G, \mu_n(K))$ es un grupo con la multiplicación de funciones y elemento identidad $\chi_0 : G \to K^X$, dada por $\chi_0(g) = 1_K$. Al grupo $Hom(G, \mu_n(K))$ lo llamamos grupo de caracteres de G con valores en K.

(iii) Todo caracter $\chi \in Hom(G, K^\times)$ tiene una extensión a un homomorfismo de K-álgebras $\chi : K[G] \to K$, también denotado por χ, dado por

$$\chi(\sum_{g\in G} a_g X^g) = \sum_{g\in G} a_g \chi(g).$$

En efecto, sean $f_1 = \sum_{g\in G} a_g X^g, f_2 = \sum_{g\in G} b_g X^g \in K[G]$ y $a \in K$

$$\begin{aligned}
\chi(f_1 + f_2) &= \chi(\sum_{g\in G} a_g X^g + \sum_{g\in G} b_g X^g) \\
&= \chi(\sum_{g\in G} (a_g + b_g) X^g) \\
&= \sum_{g\in G} (a_g + b_g)\chi(g) \\
&= \sum_{g\in G} a_g \chi(g) + \sum_{g\in G} b_g \chi(g) \\
&= \chi(\sum_{g\in G} a_g X^g) + \chi(\sum_{g\in G} b_g X^g) \\
&= \chi(f_1) + \chi(f_2).
\end{aligned}$$

$$\begin{aligned}
\chi(f_1)\chi(f_2) &= \chi(\sum_{g\in G} a_g X^g)\chi(\sum_{g\in G} b_g X^g) \\
&= (\sum_{g\in G} a_g\chi(g))(\sum_{g\in G} b_g\chi(g)) \\
&= \sum_{h\in G}[a_h\chi(h)\sum_{k\in G} b_k\chi(k)] \\
&= \sum_{h\in G}[\sum_{k\in G} a_h\chi(h)b_k\chi(k)] \\
&= \sum_{h\in G}[\sum_{k\in G} a_h b_k\chi(h+k)] \\
&= \sum_{h\in G}[\sum_{g\in G} a_h b_{g-h}\chi(g)], \quad g = h+k \\
&= \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})\chi(g) \\
&= \chi(\sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})X^g) \\
&= \chi((\sum_{g\in G} a_g X^g)(\sum_{g\in G} b_g X^g)) \\
&= \chi(f_1 f_2).
\end{aligned}$$

$$\begin{aligned}
\chi(af_1) = \chi(a\sum_{g\in G} a_g X^g) = \chi(\sum_{g\in G} aa_g X^g) &= \sum_{g\in G} aa_g\chi(g) \\
&= a\sum_{g\in G} a_g\chi(g) \\
&= a\chi(\sum_{g\in G} a_g X^g) \\
&= a\chi(f_1).
\end{aligned}$$

2.2.1. Caracteres con valores en un campo de descomposición de un grupo

Definición 2.2.2. Sea G un grupo con $\exp(G) = n$, decimos que K es un *campo de descomposición de* G si $\mu_n(K) = \mu_n(\overline{K})$ para alguna clausura algebraica $\overline{K}$ de K, es decir, K contiene al grupo de n-raíces de la unidad.

Observación 2.2.2. [8] Sea G un grupo con $\exp(G) = n$ y K un campo.

(i) Si $\text{car}(K) \nmid n$, entonces K es un campo de descomposición de G si y solo si $|\mu_n(K)| = n$.

(ii) Si $\text{car}(K) = p$ con p primo y $n = p^e m$, donde $p \nmid m$, entonces K es un campo de descomposición de G si y solo si $|\mu_n(K)| = m$ ($x^n - 1 = x^{p^e m} - 1 = (x^m - 1)^{p^e}$).

La siguiente proposición garantiza que si K es un campo de descomposición de un grupo G, siempre existen caracteres no triviales de G sobre K.

Proposición 2.2.1. *Sea G un grupo abeliano finito con $\exp(G) = n > 1$, y sea K un campo de descomposición de G tal que $\text{car}(K) \nmid n$ entonces,*

(i) Si $g \in G \setminus \{0\}$, existe $\chi \in Hom(G, K^\times)$ tal que $\chi(g) \neq 1$.

(ii) Si $g \in G$ con $\text{ord}(g) < n$, existe $\chi \in Hom(G, K^\times)$, no trivial, tal que $\chi(g) = 1$.

Demostración. Sabemos que $G = C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_r}$, donde cada C_{n_i} es cíclico de orden n_i y $n_i | n_{i+1}$ para $i \in [1, r]$ (aquí $n_r = n$). Para $i \in [1, r]$, sea $\pi_i : G \to C_{n_i}$ el epimorfismo canónico. Y sea $\xi \in \mu_n(K)$ una n-raíz primitiva de la unidad, notemos que $\xi \in K$ (ya que K es campo de descomposición de G).

(i) Como $g \neq 0$, $\pi_i(g) \neq 0$ para algún $i \in [1, r]$, sin perder generalidad, podemos suponer $i = 1$. Supongamos que $C_{n_1} = \langle a \rangle$ y que $\pi_1(g) = ka$ para algún $k \in [1, n_1 - 1]$. Sea $\chi_1 : C_{n_1} \to K^\times$ dada por $\chi(ma) = \xi^m$,

sabemos que $\chi_1 \in Hom(C_{n_1}, K^\times)$ (ver Ejemplo 2.2.1). Luego $\chi = \chi_1 \circ \pi_1 \in Hom(G, K^\times)$ (χ es composición de homomorfismos), además,

$$\chi(g) = \chi_1(\pi_1(g)) = \chi_1(ka) = \xi^k \neq 1 \quad (\text{ ya que } k < n_1 \leq n_r = n).$$

(ii) Supongamos $g = 0$, por la parte (i) existe $\chi \in Hom(G, K^\times)$ no trivial y, por ser χ homomorfismo, $\chi(g) = \chi(0) = 1$. Supongamos $g \neq 0$. Como $\text{ord}(g) < n = n_r$, $\text{ord}(\pi_r(g)) < n_r$. Supongamos que $C_{n_r} = \langle a \rangle$ y que $\pi_r(g) = ka$ para algún $k \in [1, n_r - 1]$. Entonces,

$$\text{ord}(\pi_r(g)) = \text{ord}(ka) = \frac{n_r}{\text{mcd}(k, n_r)}$$

así, $\text{ord}(\pi_r(g))d = n_r$ siendo $d = \text{mcd}(k, n_r)$, además, $k = ld$ para algún $l \in \mathbb{Z}$.

Sea $\chi_1 : C_{n_r} \to K^\times$ dada por $\chi_1(ma) = (\xi^{\text{ord}(\pi_r(g))})^m$ entonces, $\chi_1 \in Hom(C_{n_r}, K^\times)$ (ver Ejemplo 2.2.1). χ_1 es no trivial, pues

$$\chi_1(a) = \xi^{\text{ord}(\pi_r(g))} \neq 1 \quad (\text{ord}(\pi_r(g)) < n_r = n),$$

además,

$$\chi_1(\pi_r(g)) = \chi_1(ka) = (\xi^{\text{ord}(\pi_r(g))})^k = \xi^{\text{ord}(\pi_r(g))k} = \xi^{\text{ord}(\pi_r(g))dl} = \xi^{nl} = 1$$

Finalmente, sea $\chi = \chi_1 \circ \pi_r \in Hom(G, K^\times)$ entonces, $\chi(a) = \chi_1(\pi_r(a)) = \chi_1(a) \neq 1$, por lo que χ es no trivial y $\chi(g) = \chi_1(\pi_r(g)) = 1$.

□

Ahora veremos que para todo grupo G y todo campo de descomposición K de G, tenemos $Hom(G, K^\times) \simeq G$, para ver esto probaremos un resultado previo.

Lema 2.2.1. *Sea K un campo y $G_1, G_2, \ldots, G_r$ grupos abelianos finitos entonces,*

$$Hom(G_1 \times G_2 \times \ldots \times G_r, K^\times) \simeq Hom(G_1, K^\times) \times Hom(G_2, K^\times) \times \ldots \times Hom(G_r, K^\times).$$

Demostración. Probemos el resultado para $r = 2$. Sea $\chi \in Hom(G_1 \times G_2, K^\times)$, sea $\chi_{G_1} : G_1 \to K$ y $\chi_{G_2} : G_2 \to K$ dadas por

$\chi_{G_1}(a) = \chi((a, 0))$ y $\chi_{G_2}(b) = \chi((0, b))$ para $a \in G_1$ y $b \in G_2$, respectivamente.

χ_{G_1} y χ_{G_2} son caracteres de G_1 y G_2 respectivamente, en efecto,

$$\begin{aligned} \chi_{G_1}(a_1 + a_2) &= \chi((a_1 + a_2, 0)) \quad \text{para } a_1, a_2 \in G_1 \\ &= \chi((a_1, 0) + (a_2, 0)) \\ &= \chi((a_1, 0))\chi((a_2, 0)) \\ &= \chi_{G_1}(a_1)\chi_{G_1}(a_2) \end{aligned}$$

Análogamente se ve que que $\chi_{G_2} \in Hom(G_2, R^\times)$. Además, para $\chi, \psi \in Hom(G_1 \times G_2, K^\times)$ y $g_1 \in G_1$ tenemos

$$\begin{aligned} (\chi\psi)_{G_1}(g_1) &= \chi\psi(g_1, 0) \\ &= \chi((g_1, 0))\psi((g_1, 0) \\ &= \chi_{G_1}(g_1)\chi_{G_1}(g_1) \end{aligned}$$

De modo que $(\chi\psi)_{G_1} = \chi_{G_1}\psi_{G_1}$, de forma análoga se prueba que $(\chi\psi)_{G_2} = \chi_{G_2}\psi_{G_2}$. Ahora, sea $\varphi : Hom((G_1 \times G_2), K^\times) \to Hom(G_1, K^\times) \times Hom(G_2, K^\times)$ dada por $\varphi(\chi) = (\chi_{G_1}, \chi_{G_2})$, φ es un isomorfismo de grupos, en efecto, sean

$\chi, \psi \in Hom((G_1 \times G_2), K^\times)$ entonces,

$$\begin{aligned} \varphi(\chi\psi) &= ((\chi\psi)_{G_1}, (\chi\psi)_{G_2}) \\ &= (\chi_{G_1}\psi_{G_1}, \chi_{G_2}\psi_{G_2}) \\ &= (\chi_{G_1}, \chi_{G_2})(\psi_{G_1}, \psi_{G_2}) \\ &= \varphi(\chi)\varphi(\psi) \end{aligned}$$

Sean $\chi, \psi \in Hom((G_1 \times G_2), K^\times)$ tales que $\varphi(\chi) = \varphi(\psi)$ entonces,

$$\begin{aligned} & \varphi(\chi) = \varphi(\psi) \\ \Rightarrow\ & (\chi_{G_1}, \chi_{G_2}) = (\psi_{G_1}, \psi_{G_2}) \\ \Rightarrow\ & \chi_{G_1} = \psi_{G_1} \ \wedge \ \chi_{G_2} = \psi_{G_2} \\ \Rightarrow\ & \chi_{G_1}(g_1) = \psi_{G_1}(g_1) \ \wedge \ \chi_{G_2}(g_2) = \psi_{G_2}(g_2), \ \forall\ (g_1, g_2) \in G_1 \times G_2 \\ \Rightarrow\ & \chi_{G_1}(g_1)\chi_{G_2}(g_2) = \psi_{G_1}(g_1)\psi_{G_2}(g_2) \\ \Rightarrow\ & \chi((g_1, g_2)) = \psi((g_1, g_2)) \\ \Rightarrow\ & \chi = \psi. \end{aligned}$$

Ahora, sea $\psi \in Hom(G_1, K^\times) \times Hom(G_2, K^\times)$, entonces $\psi = (\chi_1, \chi_2)$ con $\chi_i \in Hom(G_i, K^\times)$ para $i = 1, 2$. Sea $\chi \in Hom(G_1 \times G_2, K^\times)$ dada por $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$ entonces, $\chi_{G_i} = \chi_i$ para $i = 1, 2$, esto es, $\varphi(\chi) = \psi$. Luego φ es un isomorfismo.

Supongamos que para $t \geq 2$ se tiene

$$Hom(G_1 \times G_2 \times \ldots \times G_t, K^\times) \simeq Hom(G_1, K^\times) \times Hom(G_2, K^\times) \times \ldots \times Hom(G_t, K^\times)$$

entonces,

$$\begin{aligned} & Hom(G_1 \times G_2 \times \ldots \times G_{t+1}, K^\times) \\ = \; & Hom([G_1 \times G_2 \times \ldots \times G_t] \times G_{t+1}, K^\times) \\ \simeq \; & Hom([G_1 \times G_2 \times \ldots \times G_t], K^\times) \times Hom(G_{t+1}, K^\times) \;\; (\text{caso } r = 2) \\ \simeq \; & Hom(G_1, K^\times) \times Hom(G_2, K^\times) \times \ldots \times Hom(G_t, K^\times) \times Hom(G_{t+1}, K^\times). \end{aligned}$$

□

Teorema 2.2.1. *Sea G un grupo abeliano finito con $\exp(G) = n$. Si K es un campo de descomposición de G con $\text{car}(K) \nmid n$ entonces, $G \simeq Hom(G, K^\times)$.*

Demostración. Supongamos que G es cíclico entonces, $G = \langle a \rangle$ para algún $a \in G$ y $|G| = \exp(G) = n$. Cada caracter de G está determinado por su valor en a, en efecto, sea $\chi \in Hom(G, K^\times) = Hom(G, \mu_n(K))$ y sea $g \in G$, entonces $g = ma$ para algún $m \in [1, n]$, así

$$\chi(g) = \chi(ma) = \chi(a)^m$$

de modo que existen a lo más n caracteres de G, esto es,

$$|Hom(G, K^\times)| \leq n.$$

Ahora para $\xi \in \mu_n(K) \subseteq K^\times$, consideremos $\chi : G \to K^\times$ dada por $\chi(ma) = \xi^m$, entonces $\chi \in Hom(G, K^\times)$ (ver Ejemplo 2.2.1), notar que debido a que K es un campo de descomposición de G y $\text{car}(K) \nmid n$, entonces $|\mu_n(K)| = n$ (por Observación 2.2.2), de modo que existen al menos n caracteres de G, esto es,

$$|Hom(G, K^\times)| \geq n.$$

Por tanto $|Hom(G, K^\times)| = n = |G|$.

Veamos que $Hom(G, K^\times) = Hom(G, \mu_n(K))$ es cíclico. Sea $\xi_n \in K^\times$ una n-raíz primitiva de la unidad. Sea $\chi : G \to K^\times$ dada por $\chi(ma) = \xi_n^m$, $\chi \in Hom(G, K^\times)$. Notemos que $Hom(G, K^\times) = \langle\chi\rangle$, en efecto, sea $\psi \in Hom(G, K^\times)$ entonces, para $m \in \mathbb{Z}$

$$\begin{aligned}
\psi(ma) &= \psi(a)^m \\
&= (\xi_n^t)^m \text{ para algún } t \in \mathbb{Z} \ (\psi(a) \in \mu_n(K) = \langle\xi_n\rangle) \\
&= (\xi_n^m)^t \\
&= (\chi(ma))^t,
\end{aligned}$$

luego, $\psi = \chi^t$, en consecuencia $Hom(G, K^\times)$ es cíclico de orden n. Por tanto $G \simeq Hom(G, K^\times)$. En general, si G es un grupo abeliano finito,

$$G \cong C_{n_1} \oplus C_{n_2} \oplus ... \oplus C_{n_r}$$

con C_{n_i} cíclico y $n_i \mid n_{i+1}$ para todo $i \in [1, r]$, de modo que

$$\begin{aligned}
Hom(G, K^\times) &\simeq Hom(C_{n_1} \oplus C_{n_2} \oplus ... \oplus C_{n_r}, K^\times) \\
&\simeq Hom(C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}, K^\times) \\
&\simeq Hom(C_{n_1}, K^\times) \times Hom(C_{n_2}, K^\times) \times ... \times Hom(C_{n_r}, K^\times) \ (Lema) \\
&\simeq C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_r} \ (C_{n_i}\text{es cíclico para todo i} \in [1, r]) \\
&\simeq G.
\end{aligned}$$

□

2.2.2. Propiedades de ortogonalidad

Observación 2.2.3. Sea G un grupo abeliano finito con $\exp(G) = n > 1$, K un campo de descomposición de G con $\text{car}(K) \nmid n$ y $\widehat{G} = Hom(G, K^\times)$.

Sea $\varphi : G \to Hom(\widehat{G}, K^{\times})$ dada por $\varphi(g) = \varphi_g$, donde $\varphi_g : \widehat{G} \to K^{\times}$ es definida por $\varphi_g(\chi) = \chi(g)$ entonces, φ es un isomorfismo, en efecto, φ está bien definida ya que para $g \in G$ y $\chi, \psi \in \widehat{G}$ se tiene,

$$\varphi_g(\chi\psi) = (\chi\psi)(g) = \chi(g)\psi(g) = \varphi_g(\chi)\varphi_g(\psi)$$

Para $g_1, g_2 \in G$ y $\chi \in \widehat{G}$ se tiene,

$$\begin{aligned} \varphi(g_1 + g_2)(\chi) = \varphi_{g_1+g_2}(\chi) &= \chi(g_1 + g_2) \\ &= \chi(g_1)\chi(g_2) \\ &= \varphi_{g_1}(\chi)\varphi_{g_2}(\chi) \\ &= (\varphi_{g_1}\varphi_{g_2})(\chi) \\ &= (\varphi(g_1)\varphi(g_2))(\chi) \end{aligned}$$

de donde, $\varphi(g_1 + g_2) = \varphi(g_1)\varphi(g_2)$, es decir, φ es homomorfismo de grupos
Si $\varphi(g_1) = \varphi(g_2)$ para $g_1, g_2 \in G$ entonces,

$$\begin{aligned} \varphi_{g_1}(\chi) = \varphi_{g_2}(\chi), \quad \forall \chi \in \widehat{G} &\Rightarrow \chi(g_1) = \chi(g_2), \quad \forall \chi \in \widehat{G} \\ &\Rightarrow \chi(g_1)\chi(g_2)^{-1} = 1, \quad \forall \chi \in \widehat{G} \\ &\Rightarrow \chi(g_1 - g_2) = 1, \quad \forall \chi \in \widehat{G} \\ &\Rightarrow g_1 = g_2, \quad \text{por Proposición 2.2.1 } (i) \end{aligned}$$

Proposición 2.2.2. *Sea G un grupo abeliano finito con $\exp(G) = n$, K un campo de descomposición de G con $\mathrm{car}(K) \nmid n$ y $\widehat{G} = Hom(G, K^{\times})$. Se cumple*

(i) Propiedades de adición

a. Si $\chi \in \widehat{G}$ *entonces,*

$$\sum_{g\in G}\chi(g) = \begin{cases} |G| & si\ \chi = \chi_0, \\ 0 & si\ \chi \neq \chi_0 \end{cases}$$

b. Si $g \in G$ *entonces,*

$$\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} |G| & si\ g = 0, \\ 0 & si\ g \neq 0 \end{cases}$$

(ii) Relaciones de Ortogonalidad

a. Si $\chi, \psi \in \widehat{G}$ *entonces,*

$$\sum_{g\in G}\chi(g)\psi^{-1}(g) = \begin{cases} |G| & si\ \chi = \psi, \\ 0 & si\ \chi \neq \psi \end{cases}$$

b. Si $g, h \in G$ *entonces,*

$$\sum_{\chi\in\widehat{G}}\chi(g)\chi^{-1}(h) = \begin{cases} |G| & si\ g = h, \\ 0 & si\ g \neq h \end{cases}$$

(iii) Si $f \in K[G]$*, digamos* $f = \sum_{g\in G} a_g X^g$ *entonces,*

$$a_g = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f)\chi(-g)\ \textit{para todo}\ g \in G.$$

En particular, $f = 0$ *si y solo si* $\chi(f) = 0$ *para todo* $\chi \in \widehat{G}$*. Además, si* $\chi(f) \neq 0$ *para toda* $\chi \in Hom(G, K^\times)$*, entonces* $f \in K[G]^\times$*.*

Demostración. $(i)a.$ Sea $\chi \in \widehat{G}$, si $\chi = \chi_0$ entonces

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi_0(g) = \sum_{g\in G} 1 = |G|$$

Si $\chi \neq \chi_0$, tomamos $g_0 \in G$ tal que $\chi(g_0) \neq 1$ entonces,

$$\begin{aligned} \chi(g_0)\sum_{g\in G}\chi(g) &= \sum_{g\in G}\chi(g_0)\chi(g) \\ &= \sum_{g\in G}\chi(g_0 + g) \\ &= \sum_{g\in G}\chi(g) \end{aligned}$$

Luego $(\chi(g_0)-1)\sum_{g\in G}\chi(g)=0$ implicando que

$$\sum_{g\in G}\chi(g)=0 \ \text{ (pues } \chi(g_0)\neq 1).$$

$(i)b.$ Siendo φ el isomorfismo de la Observación 2.2.3, y sustituyendo en $(i)a.$ a G por $\widehat{G}$, tenemos para $g\in G$,

$$\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\varphi_g(\chi)=\begin{cases}|G| & \text{si } \varphi_g=\varphi_0,\\ 0 & \text{si } \varphi_g\neq\varphi_0\end{cases}$$

Como φ es un isomorfismo, obtenemos

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}|G| & \text{si } g=0,\\ 0 & \text{si } g\neq 0\end{cases}$$

$(ii)a.$ Si $\chi,\psi\in\widehat{G}$ entonces por $(i)a.$,

$$\sum_{g\in G}\chi(g)\psi^{-1}(g)=\sum_{g\in G}(\chi\psi^{-1})(g)=\begin{cases}|G| & \text{si } \chi\psi^{-1}=\chi_0,\\ 0 & \text{si } \chi\psi^{-1}\neq\chi_0\end{cases}$$

obtenemos así,

$$\sum_{g\in G}\chi(g)\psi^{-1}(g)=\begin{cases}|G| & \text{si } \chi=\psi,\\ 0 & \text{si } \chi\neq\psi\end{cases}$$

$(ii)b.$ Si $g,h\in G$ entonces,

$$\begin{aligned}\sum_{\chi\in\widehat{G}}\chi(g)\chi^{-1}(h) &= \sum_{\chi\in\widehat{G}}\chi(g)[\chi(h)]^{-1}\\ &= \sum_{\chi\in\widehat{G}}\chi(g)\chi(-h)\\ &= \sum_{\chi\in\widehat{G}}\chi(g-h)\end{aligned}$$

por $(i)a.$,

$$\sum_{\chi\in\widehat{G}}\chi(g-h)=\begin{cases}|G| & \text{si } g-h=0,\\ 0 & \text{si } g-h\neq 0\end{cases}$$

así,

$$\sum_{\chi\in\widehat{G}}\chi(g)\chi^{-1}(h)=\begin{cases}|G| & \text{si } g=h,\\ 0 & \text{si } g\neq h\end{cases}$$

(iii) Si $f=\sum_{g\in G}a_gX^g\in K[G]$, por $1(b)$ es claro que,

$$\begin{aligned}a_g &= \frac{1}{|G|}\sum_{h\in G}[a_h(\sum_{\chi\in\widehat{G}}\chi(h-g))]\\ &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}[\sum_{h\in G}a_h\chi(h)\chi(-g)]\\ &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f)\chi(-g).\end{aligned}$$

En particular, $f=0$ si y solo si $\chi(f)=0$ para todo $\chi\in\widehat{G}$, en efecto, si $f=0$ entonces $\chi(f)=0$ ya que $\chi\in\widehat{G}$.

Si $\chi(f)=0$ para todo $\chi\in\widehat{G}$ entonces $a_g=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f)\chi(-g)=0$ por tanto $f=0$.

Si $\chi(f)\neq 0$ entonces

$$f=\sum_{g\in G}a_gX^g \quad \text{y} \quad f^{-1}=\sum_{g\in G}b_gX^g$$

con

$$a_g=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f-g) \quad \text{y} \quad b_g=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi^{-1}(f)\chi(-g),$$

en efecto,

$$ff^{-1}=\sum_{g\in G}(\sum_{h\in G}a_hb_{g-h})X^g.$$

si $f-h=0$ entonces por $(i)b$.

$$a_h=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(f-h)=1 \quad \text{y}$$

$b_{g-h} = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi^{-1}(f)\chi(h-g) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi^{-1}(f)\chi(f)\chi(-g) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi(-g)$,

luego,

$$b_{g-h} = \begin{cases} 1 & \text{si } g = 0, \\ 0 & \text{si } g \neq 0 \end{cases}$$

por lo que para $h = f$

$$a_h b_{g-h} = \begin{cases} 1 & \text{si } g = 0, \\ 0 & \text{si } g \neq 0 \end{cases}$$

Si $h \neq f$ entonces por $(i)b.$ $a_h = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi(f-h) = 0$ y por tanto $a_h b_{g-h} = 0$ para todo $g \in G$.

□

2.3. Resultados Principales

En esta sección presentamos los resultados principales, los cuales básicamente dan condiciones para que ciertos elementos de la forma $(X^g - 1)$, en un álgebra de grupo $R[G]$ de un grupo G sobre un dominio de integridad R, sean invertibles en $R[G]$, o sean divisores de cero. A menos que se especifique lo contrario, en adelante, si R es un anillo y G es un grupo, $R[G]$ será el álgebra de grupo de G sobre R.

Proposición 2.3.1. *Sea G un grupo abeliano finito, sea $g \in G$ con $\mathrm{ord}(g) = n \in \mathbb{N}$, y sea R un dominio de integridad.*

(i) Si $a \in R$, entonces $X^g - a$ es un divisor de cero de $R[G]$ si y solo si $a^n = 1$.

(ii) Si $\mathrm{car}(R) \nmid n$, $l \in \mathbb{N}$ y $n_1, \ldots, n_l \in [1, n-1]$, entonces

$$(X^{n_1 g} - 1) \cdot \ldots \cdot (X^{n_l g} - 1) \neq 0 \in R[G].$$

Demostración. Supongamos que $n \geq 2$. Sea $R[T]$ el anillo de los polinomios con coeficientes en R e indeterminada T, y sea $\varphi : R[T] \to R[G]$ el único homomorfismo de R-álgebras satisfaciendo $\varphi(T) = X^g$. Entonces

$$\mathrm{Ker}(\varphi) = (T^n - 1)R[T], \tag{2.1}$$

en efecto, sea $f(T) = (T^n - 1)h(T) \in (T^n - 1)R[T]$ entonces

$$\begin{aligned} \varphi(f(T)) &= \varphi(T^n - 1)\varphi(h(T)) \\ &= [(X^g)^n - 1]\varphi(h(T)) \\ &= [X^0 - 1]\varphi(h(T)) \quad (\mathrm{ord}(g) = n) \\ &= 0 \end{aligned}$$

luego, $(T^n - 1)R[T] \subseteq \mathrm{Ker}(\varphi)$.

Sea $f(T) \in \mathrm{Ker}(\varphi)$, por Teorema 1.2.2, existen $h(T), r(T) \in R[T]$ tales que $f(T) = (T^n - 1)h(T) + r(T)$ con $\deg r(T) < n$, de modo que $r(T) = \sum_{i=1}^{k} a_i T^i$ con $k < n$ así,

$$\begin{aligned} 0 = \varphi(f(T)) &= \varphi(T^n - 1)\varphi(h(T)) + \varphi(r(T)) \\ &= ((X^g)^n - 1)\varphi(h(T)) + \varphi(r(T)) \\ &= (X^0 - 1)\varphi(h(T)) + \varphi(r(T)) \quad (\mathrm{ord}(g) = n) \\ &= \varphi(r(T)) \\ &= \sum_{i=1}^{k} a_i (X^g)^i \\ &= \sum_{i=1}^{k} a_i X^{ig} \end{aligned}$$

Como para cada $i \in [1, k]$ se tiene $i < n$ entonces, $ig \neq jg$ para todo $i, j \in$

$[1,k]$ por tanto,

$$\sum_{i=1}^{k} a_i X^{ig} = 0 \Rightarrow a_i = 0 \ \forall i \in [1,k]$$

de donde, Ker$\varphi \subseteq (T^n-1)R[T]$

(i) Si $a \in R$ entonces,

$$1-a^n = (X^g)^n - a^n = (X^g - a)f, \quad \text{donde} \quad f = \sum_{j=1}^{n-1} (X^g)^j a^{n-1-j}.$$

Como $f = \varphi(\tilde{f})$ donde $\tilde{f} = \sum_{j=1}^{n-1} T^j a^{n-1-j} \in R[T]$ tal que $\deg(\tilde{f}) < n$, tenemos $f \neq 0$ (por (2.1) los polinomios en el Kerφ tienen grado mayor o igual a n).

Si $a^n = 1$, entonces $(X^g - a)f = 0$, y así $X^g - a$ es un divisor de cero de $R[G]$. Si $a^n \neq 1$, entonces $0 \neq a^n - 1 \in R$, con R un dominio de integridad (no tiene divisores de cero) entonces, $a^n - 1$ no es un divisor de cero de R y por la Observación 2.1.1, $a^n - 1$ no es un divisor de cero de $R[G]$. Si $X^g - a$ es un divisor de cero de $R[G]$ entonces existe $0 \neq f_1 \in R[G]$ tal que $(X^g - a)f_1 = 0$; así

$$\begin{aligned} & 1-a^n = (X^g - a)f \\ \Rightarrow \quad & (1-a^n)f_1 = (X^g - a)f_1 f = 0 \\ \Rightarrow \quad & 1-a^n \ \text{ es un divisor de cero de } \ R[G], \end{aligned}$$

contradicción al hecho de que $1-a^n$ no es un divisor de cero de $R[G]$. Por tanto $X^g - a$ no es un divisor de cero de $R[G]$.

(ii) Supongamos que $f = (X^{n_1 g}-1)\cdot \ldots \cdot (X^{n_l g}-1) = 0$ entonces, $\varphi(\tilde{f}) = 0$ donde $\tilde{f} = (T^{n_1}-1)\cdot \ldots \cdot (T^{n_l}-1)$, así $\tilde{f} \in$ Kerφ, es decir,

$$\tilde{f} = (T^{n_1}-1)\cdot \ldots \cdot (T^{n_l}-1) = (T^n-1)\hat{f} \ \text{ con } \ \hat{f} \in R[T].$$

Como $\text{car}(R) \nmid n$, existe una $n-$raíz primitiva de la unidad w en algún campo que contiene a R. Entonces $w^n - 1 = 0$ y por tanto

$$\tilde{f}(w) = (w^n - 1)\hat{f}(w) = 0,$$

sin embargo, como $n_1, \ldots, n_l \in [1, n-1]$,

$$w^{n_i} - 1 \neq 0 \ \ \forall\, i \in [1, l]$$

lo que implica que, $\tilde{f}(w) = (w^{n_1} - 1) \cdot \ldots \cdot (w^{n_l} - 1) \neq 0$, pues R es un dominio de integridad, en contradicción con el hecho de que $\tilde{f}(w) = 0$. Por tanto $f = (X^{n_1 g} - 1) \cdot \ldots \cdot (X^{n_l g} - 1) \neq 0$

□

Proposición 2.3.2. *Sea G un p-grupo abeliano finito.*

(i) Sea R un dominio de integridad de característica p y $f \in R[G]$. Entonces $f \in R[G]^\times$ si y sólo si $\varepsilon(f) \in R^\times$.

(ii) Si $f \in \mathbb{Z}[G]$ y $\varepsilon(f) \notin p\mathbb{Z}$, entonces f no es un divisor de cero de $\mathbb{Z}[G]$.

Demostración. Sea $n = \exp(G) = p^r$.

(i) Por la Observación 2.1.1 tenemos $(X^g)^n = X^{ng} = X^0 = 1$ para todo $g \in G$, entonces $f^n = \varepsilon(f)^n$ para todo $f \in R[G]$, en efecto, sea $f =$

$a_1X^{g_1} + a_2X^{g_2} + \ldots + a_lX^{g_l}$ entonces,

$$\begin{aligned} f^n = (\sum_{i=1}^{l} a_iX^{g_i})^n &= \sum_{i=1}^{l}(a_iX^{g_i})^n \qquad (\mathrm{car}(R[G]) = \mathrm{car}(R) = p) \\ &= \sum_{i=1}^{l} a_i^n(X^{g_i})^n \\ &= \sum_{i=1}^{l} a_i^n \\ &= (\sum_{i=1}^{l} a_i)^n \qquad (\mathrm{car}(R) = p) \\ &= \varepsilon(f)^n \qquad \text{para todo } f \in R[G]. \end{aligned}$$

Sea $f \in R[G]^\times$ entonces existe $g \in R[G]$ tal que $fg = 1_{R[G]}$, pero

$$\begin{aligned} fg = 1_{R[G]} \Rightarrow \varepsilon(fg) = 1 &\Rightarrow \varepsilon(f)\varepsilon(g) = 1 \\ &\Rightarrow \varepsilon(f) \in R^\times \end{aligned}$$

Sea $f \in R[G]$ tal que $\varepsilon(f) \in R^\times$ entonces existe $r \in R$ tal que $\varepsilon(f)r = 1$ pero,

$$\begin{aligned} \varepsilon(f)r = 1 &\Rightarrow \varepsilon(f)\varepsilon(g) = 1 \qquad (g \in R[G],\ \varepsilon \text{ es epimorfismo}) \\ &\Rightarrow \varepsilon(fg) = 1 \\ &\Rightarrow \varepsilon(fg)^n = 1 \\ &\Rightarrow (fg)^n = 1_{R[G]} \\ &\Rightarrow f^ng^n = 1_{R[G]} \qquad (R[G] \text{ es conmutativo}) \\ &\Rightarrow f(f^{n-1}g^n) = 1_{R[G]} \\ &\Rightarrow f \in R[G]^\times. \end{aligned}$$

(ii) Sea $\varphi : \mathbb{Z}[G] \to \mathbb{Z}/p\mathbb{Z}[G]$ el epimorfismo canónico y $f = \sum_{g\in G} a_gX^g$.

Entonces,

$$\begin{aligned}
\varepsilon(\varphi(f)) = \varepsilon(\sum_{g\in G}(a_g + p\mathbb{Z})X^g) &= \sum_{g\in G}(a_g + p\mathbb{Z}) \\
&= (\sum_{g\in G} a_g) + p\mathbb{Z} \\
&= \varphi(\sum_{g\in G} a_g) \\
&= \varphi(\varepsilon(f)) \\
&\neq 0 \quad (\text{pues } \varepsilon(f) \notin p\mathbb{Z})
\end{aligned}$$

Como $0 \neq \varepsilon(\varphi(f)) \in \mathbb{Z}/p\mathbb{Z}$ entonces, $\varepsilon(\varphi(f)) \in (\mathbb{Z}/p\mathbb{Z})^\times$ y, dado que $\mathbb{Z}/p\mathbb{Z}$ es un dominio de integridad de característica p, por (i), $\varphi(f) \in (\mathbb{Z}/p\mathbb{Z}[G])^\times$. Supongamos ahora que f es un divisor de cero en $\mathbb{Z}[G]$. Entonces existe algún $g \in \mathbb{Z}[G]$ tal que $g \neq 0$ y $fg = 0$, supongamos que $g \in p\mathbb{Z}[G]$ entonces, $g = \sum_{g\in G} p^{k_g} b_g X^g$ con $k_g \in \mathbb{N}$ y $b_g \in \mathbb{Z} \setminus p\mathbb{Z}$, sea $m = \text{mín}\{k_g : g \in G\} \geq 1$. Luego,

$$\begin{aligned}
fg = 0 &\Rightarrow (\sum_{g\in G} a_g X^g)(\sum_{g\in G} p^{k_g} b_g X^g) = 0 \\
&\Rightarrow \sum_{g\in G}(\sum_{h\in G} a_h p^{k_{g-h}} b_{g-h}) X^g = 0 \\
&\Rightarrow \sum_{h\in G} a_h p^{k_{g-h}} b_{g-h} = 0, \quad \forall g \in G \\
&\Rightarrow p^m \sum_{h\in G} a_h p^{k_{g-h}-m} b_{g-h} = 0 \\
&\Rightarrow \sum_{h\in G} a_h p^{k_{g-h}-m} b_{g-h} = 0
\end{aligned}$$

Sea $g' = \sum_{g\in G} c_g X^g$, donde $c_g = p^{k_g - m} b_g$; sea $g_0 \in G$ tal que $k_{g_0} = m$,

es claro que $g' \notin p\mathbb{Z}$ ya que $c_{g_0} = b_{g_0} \notin p\mathbb{Z}$ y

$$\begin{aligned} fg' &= \sum_{g\in G}(\sum_{h\in G} a_h c_{g-h})X^g \\ &= \sum_{g\in G}(\sum_{h\in G} a_h p^{k_{g-h}-m} b_{g-h})X^g \\ &= 0. \end{aligned}$$

Entonces $\varphi(g') \neq 0$ y $\varphi(f)\varphi(g') = \varphi(fg') = 0$, obtenemos así una contradicción al hecho de que $\varphi(f)$ es una unidad (ver la Proposición 2.1.3).

□

Proposición 2.3.3. *Sea G un grupo abeliano finito, R un anillo conmutativo, $k \in \mathbb{N}$, $g_1, \ldots, g_k \in G$, $a_1, \ldots, a_k \in R$ y*

$$V := \{b \in R[G] \mid (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k)b = 0\}.$$

(i) Un elemento

$$b = \sum_{\sigma\in G} b(\sigma)X^\sigma \in R[G]$$

pertenece a V si y solo si, para todo $\sigma \in G$ y $m_1, \ldots, m_k \in \mathbb{N}$, tenemos

$$(-1)^{k-1}(\prod_{i=1}^{k} a_i^{m_i})b(\sigma+\sum_{i=1}^{k} m_i g_i) = \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i^{m_i})b(\sigma+\sum_{i\in I} m_i g_i). \tag{2.2}$$

(ii) Sea $g_1, \ldots, g_k \in G$ elementos independientes, con $\mathrm{ord}(g_i) = n_i \geq 2$ y $a_i^{n_i} = 1$ para todo $i \in [1,k]$. Sea $\Omega \subset G$ un conjunto de representantes para $G/\langle g_1, \ldots, g_k\rangle$ y M el conjunto de todas las $(k+1)-$uplas $(\tau, m_1, \ldots, m_k)$, donde $\tau \in \Omega$, $m_1, \ldots, m_k \in [0, n_i - 1]$ para todo $i \in$

$[1,k]$, *y* $m_i = 0$ *para al menos un* $i \in [1,k]$. *Entonces tenemos:*

Para cualquier familia $(a(\tau, m_1, \ldots, m_k))_{(\tau,m_1,\ldots,m_k)\in M} \in R^M$ *existe un único* $b \in V$ *tal que*

$$b(\tau + \sum_{i=1}^{k} m_i g_i) = a(\tau, m_1, \ldots, m_k), \quad \textit{para todo} \quad (\tau, m_1, \ldots, m_k) \in M. \tag{2.3}$$

En particular, V *es un* $R-$*módulo libre y*

$$\mathrm{rgo}(V) = |M| = |G|(1 - \prod_{i=1}^{k}(1 - \frac{1}{n_i})).$$

Demostración. (i) Para cada $k \in \mathbb{N}$, sea

$$\prod_{i=1}^{k}(X^{g_i} - a_i) \sum_{\sigma\in G} b(\sigma)X^{\sigma} = \sum_{\sigma\in G} b_k(\sigma)X^{\sigma}. \tag{2.4}$$

Probaremos, por inducción sobre k, que para todo $\sigma \in G$ tenemos

$$b_k(\sigma + \sum_{i=1}^{k} g_i) = \sum_{j=0}^{k}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i). \tag{2.5}$$

Para $k = 0$, no hay nada que probar.

Para $k \geq 1$, supongamos que

$$b_{k-1}(\sigma + \sum_{i=1}^{k-1} g_i) = \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i). \tag{2.6}$$

$$
\begin{aligned}
& \sum_{\sigma\in G} b_k(\sigma)X^\sigma \\
= & \prod_{i=1}^{k}(X^{g_i}-a_i)\sum_{\sigma\in G} b(\sigma)X^\sigma \\
= & (X^{g_k}-a_k)\prod_{i=1}^{k-1}(X^{g_i}-a_i)\sum_{\sigma\in G} b(\sigma)X^\sigma \\
= & (X^{g_k}-a_k)\sum_{\sigma\in G} b_{k-1}(\sigma)X^\sigma \\
= & \sum_{\sigma\in G} b_{k-1}(\sigma)X^{\sigma+g_k} - \sum_{\sigma\in G} a_k b_{k-1}(\sigma)X^\sigma \\
= & \sum_{\sigma\in G} b_{k-1}(\sigma-g_{_k})X^\sigma - \sum_{\sigma\in G} a_k b_{k-1}(\sigma)X^\sigma \ \ (\text{renombrando } \ \sigma=\sigma-g_k) \\
= & \sum_{\sigma\in G}(b_{k-1}(\sigma-g_{_k})-a_k b_{k-1}(\sigma))X^\sigma.
\end{aligned}
$$

Luego, $b_k(\sigma) = b_{k-1}(\sigma - g_k) - a_k b_{k-1}(\sigma)$ y por lo tanto, para todo $\sigma \in G$,

$$
\begin{aligned}
& \sum_{j=0}^{k}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) + (-1)^k \sum_{\substack{I\subset[1,k]\\|I|=k}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \{ \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) + \sum_{\substack{I\subset[1,k]\\|I|=j\\k\in I}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) \} + \\
& (-1)^k \sum_{\substack{I\subset[1,k]\\|I|=k}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \{ \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) + \sum_{\substack{I\subset[1,k-1]\\|I|=j-1}} (\prod_{i\in I} a_i) a_k b(\sigma + \sum_{i\in I} g_i + g_k) \} + \\
& (-1)^k \sum_{\substack{I\subset[1,k-1]\\|I|=k-1}} (\prod_{i\in I} a_i) a_k b(\sigma + \sum_{i\in I} g_i + g_k) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) + \sum_{j=1}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j-1}} (\prod_{i\in I} a_i) a_k b(\sigma + \sum_{i\in I} g_i + g_k) + \\
& (-1)^k \sum_{\substack{I\subset[1,k-1]\\|I|=k-1}} (\prod_{i\in I} a_i) a_k b(\sigma + \sum_{i\in I} g_i + g_k) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) + \sum_{j=1}^{k}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j-1}} (\prod_{i\in I} a_i) a_k b(\sigma + \sum_{i\in I} g_i + g_k) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) - a_k \sum_{j=1}^{k}(-1)^{j+1} \sum_{\substack{I\subset[1,k-1]\\|I|=j-1}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i + g_k) \\
= \; & \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) - a_k \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k-1]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i + g_k) \\
= \; & b_{k-1}(\sigma + \sum_{i=1}^{k-1} g_i) - a_k b_{k-1}(\sigma + g_k + \sum_{i=1}^{k-1} g_i) \quad \text{(hipótesis inductiva)} \\
= \; & b_k(\sigma + \sum_{i=1}^{k} g_i)
\end{aligned}
$$

Por definición, $b \in V$ si y solo si $b_k(\sigma) = 0$ para todo $\sigma \in G$ o, equivalentemente, $b_k(\sigma + g_1 + ... + g_k) = 0$ para todo $\sigma \in G$. Por (2.5),

$$b_k(\sigma + g_1 + ... + g_k) = \sum_{j=0}^{k}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) = 0$$

$$\Leftrightarrow \quad \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) = -(-1)^k (\prod_{i=1}^{k} a_i) b(\sigma + \sum_{i=1}^{k} g_i)$$

$$\Leftrightarrow \quad \sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i) b(\sigma + \sum_{i\in I} g_i) = (-1)^{k-1} (\prod_{i=1}^{k} a_i) b(\sigma + \sum_{i=1}^{k} g_i)$$

luego, $b \in V$ si y solo si, para todo $\sigma \in G$ (2.2) es cierto para $m_1 = m_2 = \ldots = m_k = 1$. Así resta probar que (2.2) es cierto para todo $m_1, \ldots, m_k \in \mathbb{N}^k$ probando que es cierto para $(1, \ldots, 1) \in \mathbb{N}^k$.

Si $(m_1, \ldots, m_k) \in \mathbb{N}^k$ y (2.2) es cierto para $(1, \ldots, 1) \in \mathbb{N}^k$, entonces el elemento asociado b pertenece a V y $(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k) b = 0$. Esto, la Observación 1.2.1 y el hecho de que el anillo $R[G]$ es conmutativo implica que

$$\begin{aligned} & (X^{m_1 g_1} - a_1^{m_1}) \cdot \ldots \cdot (X^{m_k g_k} - a_k^{m_k}) b \\ = \; & (X^{g_1} - a_1)(\sum_{i=0}^{m_1 - 1} a^{m_1 - 1 - i} X^{ig}) \cdot \ldots \cdot (X^{g_k} - a_k)(\sum_{i=0}^{m_k - 1} a^{m_k - 1 - i} X^{ig}) b \\ = \; & 0 \end{aligned}$$

y así (2.2) es cierto para $(m_1, \ldots, m_k) \in \mathbb{N}^k$.

(ii) Sea $\overline{M} = \Omega \times [0, n_1 - 1] \times \ldots \times [0, n_k - 1]$. Tengamos en cuenta que,

$$a_i^{n_i} = 1 \Rightarrow a_i a_i^{n_i - 1} = 1 \Rightarrow a_i \in R^{\times}.$$

Sea $\varphi : R^M \to V$, dada por

$$\begin{aligned}\varphi((a(\tau, m_1, \ldots, m_k))_{(\tau,m_1,\ldots,m_k)\in M}) &= b^* \\ &= \sum_{\sigma\in G} b(\sigma)X^\sigma.\end{aligned}$$

Como $g_1, \ldots, g_k$ son idependientes, todo $\sigma \in G$ tiene una representación única

$$\sigma = \tau + \sum_{i=1}^{k} m_i g_i \text{ con } (\tau, m_1, \ldots, m_k) \in \overline{M}, \text{ (ya que ord}(g_i) = n_i)$$

Si $m_i = 0$ para algún $i \in [1, k]$, entonces $(\tau, m_1, \ldots, m_k) \in M$ y la siguiente definición para $b(\sigma)$ tiene sentido,

$$b(\sigma) = b(\tau + \sum_{i=1}^{k} m_i g_i) = a(\tau, m_1, \ldots, m_k)$$

Si $m_i \neq 0 \, \forall i \in [1, k]$, definimos $b(\sigma)$ como sigue,

$$\begin{aligned} b(\sigma) &= b(\tau + \sum_{i=1}^{k} m_i g_i) \\ &= (-1)^{1-k}(\prod_{i=1}^{k} a_i^{-m_i})[\sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i^{m_i}) b(\sigma + \sum_{i\in I} m_i g_i)] \\ &= (-1)^{1-k}(\prod_{i=1}^{k} a_i^{-m_i})[\sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i^{m_i}) b(\sigma + \sum_{i=1}^{k} m_{i_I} g_i)] \end{aligned}$$

con $m_{i_I} = m_i$ si $i \in I$ y $m_{i_I} = 0$ si $i \notin I$ de modo que, para al menos un $i \in [1, k]$, $m_{i_I} = 0$ (ya que $|I| = j \leq k - 1$). Luego,

$$b(\tau+\sum_{i=1}^{k} m_i g_i) = (-1)^{1-k}(\prod_{i=1}^{k} a_i^{-m_i})[\sum_{j=0}^{k-1}(-1)^j \sum_{\substack{I\subset[1,k]\\|I|=j}} (\prod_{i\in I} a_i^{m_i}) a(\tau, m_{1_I}, \ldots, m_{k_I})]$$

Observemos que, por la forma en que hemos definido a φ, $b(\tau+\sum_{i=1}^{k} m_i g_i)$ satisface (2.2) para todo $(\tau, m_1 \ldots m_k) \in \Omega \times [1, n_1 - 1] \times \ldots \times [1, n_k - 1]$,

como $a_i^n = 1$ para todo $i \in [1,k]$, se sigue que $b(\sigma + \sum_{i=1}^{k} m_i g_i)$ satisface (2.2) para todo $\sigma \in G$ y $m_1 \dots m_k \in \mathbb{N}$. Entonces, por (i), $b^* \in V$ por tanto φ está bien definida. Más aún, se puede ver que φ, es un homomorfismo. Además

$$\begin{aligned} & \varphi((a(\tau, m_1, \dots, m_k))_{\tau, m_1, \dots, m_k} \in M) = 0 \\ \Rightarrow \quad & b(\sigma) = 0 \quad \forall \sigma \in G \\ \Rightarrow \quad & b(\tau + \sum_{i=1}^{k} m_i g_i) = 0 \quad \forall (\tau, m_1, \dots, m_k) \in M \subseteq \overline{M} \\ \Rightarrow \quad & a(\tau, m_1, \dots, m_k) = 0 \quad \forall (\tau, m_1, \dots, m_k) \in M \end{aligned}$$

luego, φ es inyectiva.

Ahora, sea $b^* \in V$, $b^* = \sum_{\sigma \in G} b(\sigma) X^\sigma$. Consideremos la familia

$$(a(\tau, m_1, \dots, m_k))_{(\tau, m_1, \dots, m_k) \in M} = (b(\tau, m_1, ..., m_k))_{(\tau, m_1, \dots, m_k) \in M}) \in R^M$$

entonces, por (i),

$$\begin{aligned} & \varphi((a(\tau, m_1, \dots, m_k))_{(\tau, m_1, \dots, m_k) \in M}) \\ = \quad & \varphi((b(\tau, m_1, \dots, m_k))_{(\tau, m_1, \dots, m_k) \in M}) \\ = \quad & b^*. \end{aligned}$$

Luego φ es sobreyectiva.

Por lo tanto la asignación $(a(\tau, m_1, ..., m_k))_{(\tau, m_1, \dots, m_k) \in M} \mapsto b^*$ define un isomorfismo $R^M \tilde{\to} V$, y dado que $g_1, ..., g_k$ son independientes, $\mathrm{ord}(g_i) = n_i$ y $\prod_{i=1}^{k}(n_i - 1)$ representa el número en el que todos los $m_i \neq 0$, tenemos

$$\mathrm{rgo}(V) = \dim(V) = \dim(R^M) = |M| = |\Omega|(\prod_{i=1}^{k} n_i - \prod_{i=1}^{k}(n_i - 1)),$$

y $|\Omega| = \frac{|G|}{n_1 \cdot \ldots \cdot n_k}$.

□

Teorema 2.3.1. *Sea G un grupo abeliano finito, R un dominio de integridad, $l \in \mathbb{N}$, $k \in [1, l]$, y sea $g_1, \ldots, g_l \in G$ tales que $g_1, \ldots, g_k$ son independientes. Para $i \in [1, l]$ sea $n_i = \mathrm{ord}(g_i) \geq 2$, y supongamos que*

$$\sum_{i=1}^{l} \frac{1}{n_i} - \sum_{i=2}^{k} (-1)^i \sum_{1 \leq \nu_1 < \ldots < \nu_i \leq k} \frac{1}{n_{\nu_1} \cdot \ldots \cdot n_{\nu_i}} < 1. \tag{2.7}$$

Entonces,

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \quad \textit{para todo} \quad a_1, \ldots, a_l \in R.$$

Si $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ y $\mathsf{k}(S)$ denota el número de cross de S, entonces (2.7) es cierto si, o $\mathsf{k}(S) < 1$, o $\mathsf{k}(S) \leq 1$ y $k \geq 2$.

En particular, si p es el menor divisor primo de $\exp(G)$ y $|S| < p$, entonces

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0.$$

Demostración. Podemos suponer que R es un campo (el campo de cocientes del dominio de integridad R). Si $a_i^{n_i} \neq 1$ para algún $i \in [1, l]$ entonces, por la Proposición 2.3.1, $X^{g_i} - a_i$ no es un divisor de cero de $R[G]$, y por la Proposición 2.1.3, $X^{g_i} - a_i$ es una unidad de $R[G]$ luego,

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0.$$

Supongamos que $a_i^{n_i} = 1$ para todo $i \in [1, l]$. Sea $V = \{b \in [G] \mid (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)b = 0\}$, entonces la Proposición 2.3.3 implica que

$$\dim_R(V) = |G|(1 - \prod_{i=1}^{k}(1 - \frac{1}{n_i})) \tag{2.8}$$

Sea $\varphi : R[G] \to R[G]$ dada por $\varphi(f) = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)f$, φ es un homomorfismo de R-módulos, en efecto, sean $f, g \in R[G]$ y $r \in R$ entonces

$$\begin{aligned} \varphi(f+g) &= (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)(f+g) \\ &= (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)f + (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)g \\ &= \varphi(f) + \varphi(g) \end{aligned}$$

y, $\varphi(rf) = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)(rf) = r(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)f = r\varphi(f)$.

Por el Teorema 1.3.2, $\dim_R R[G] = \dim_R \mathrm{Ker}\varphi + \dim_R Im\varphi$ implicando que

$$|G| = \dim_R V + \dim_R (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_k)R[G]$$

y por (2.8),

$$\dim_R (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k)R[G] = |G| - \dim_R V = |G| \prod_{i=1}^{k} (1 - \frac{1}{n_i}). \quad (2.9)$$

Para $i \in [k+1, l]$ consideramos el conjunto $V_i = \{b \in R[G] \mid (X^{g_i} - a_i)b = 0\}$, nuevamente la Proposición 2.3.3 implica que

$$\dim_R V_i = |G|(1 - (1 - \frac{1}{n_i})) = |G|\frac{1}{n_i}, \quad (2.10)$$

además consideremos $\varphi_i : R[G] \to R[G]$ dada por $\varphi_i(f) = (X^{g_i} - a_i)f$, φ_i es un homomorfismo de R-módulos y por el Teorema 1.3.2,

$$\dim_R R[G] = \dim_R \mathrm{Ker}\varphi_i + \dim_R Im\varphi_i \Rightarrow |G| = \dim_R V_i + \dim_R (X^{g_i} - a_i)R[G]$$

y por (2.10),

$$\dim_R (X^{g_i} - a_i)R[G] = |G| - \dim_R V_i = |G| - |G|\frac{1}{n_i} = |G|(1 - \frac{1}{n_i}). \quad (2.11)$$

Por el Teorema 1.3.3, (2.9), (2.11) y (2.7) tenemos:

$$\begin{aligned}
& \dim_R(X^{g_1}-a_1)\cdot\ldots\cdot(X^{g_l}-a_l)R[G] \\
= \;& \dim_R(\varphi\circ\varphi_{k+1}\circ\ldots\circ\varphi_l) \\
\geq \;& \dim_R\varphi(R[G])+\sum_{i=k+1}^{l}\dim_R\varphi_i(R[G])-((l-k+1)-1)\dim_R(R[G]) \\
= \;& \dim_R(X^{g_1}-a_1)\cdot\ldots\cdot(X^{g_k}-a_k)R[G]+\sum_{i=k+1}^{l}\dim_R\varphi_i(R[G])-(l-k)|G| \\
= \;& |G|\prod_{i=1}^{k}(1-\frac{1}{n_i})+\sum_{i=k+1}^{l}|G|(1-\frac{1}{n_i})-(l-k)|G| \\
= \;& |G|[\prod_{i=1}^{k}(1-\frac{1}{n_i})+l-k-\sum_{i=k+1}^{l}\frac{1}{n_i})-l+k] \\
= \;& |G|[\prod_{i=1}^{k}(1-\frac{1}{n_i})-\sum_{i=k+1}^{l}\frac{1}{n_i})] \\
= \;& |G|[1-\sum_{i=1}^{l}\frac{1}{n_i}+\sum_{i=2}^{k}(-1)^i\sum_{1\leq\nu_1<\ldots<\nu_i\leq k}\frac{1}{n_{\nu_1}\cdot\ldots\cdot n_{\nu_i}}] \text{ (inducción sobre n).} \\
> \;& 0
\end{aligned}$$

Por lo tanto, $(X^{g_1}-a_1)\cdot\ldots\cdot(X^{g_l}-a_l)\neq 0$. Por otro lado, afirmamos que

$$\sum_{i=2}^{k}(-1)^i\sum_{1\leq\nu_1<\ldots<\nu_i\leq k}\frac{1}{n_{\nu_1}\cdot\ldots\cdot n_{\nu_i}}=\prod_{i=1}^{k}(1-\frac{1}{n_i})-1+\sum_{i=1}^{k}\frac{1}{n_i}\geq 0,$$

en efecto, para $k=1$ se tiene evidentemente la igualdad, para $k=2$ se tiene $\frac{1}{n_1n_2}\geq 0$. Supongamos que para $k\geq 2$ se cumple que $\prod_{i=1}^{k}(1-\frac{1}{n_i})-1+\sum_{i=1}^{k}\frac{1}{n_i}\geq 0$, entonces

$$\begin{aligned}
\prod_{i=1}^{k+1}(1-\frac{1}{n_i})-1+\sum_{i=1}^{k+1}\frac{1}{n_i} &= \prod_{i=1}^{k}(1-\frac{1}{n_i})(1-\frac{1}{n_{k+1}})-1+\sum_{i=1}^{k}\frac{1}{n_i}+\frac{1}{n_{k+1}} \\
&= \prod_{i=1}^{k}(1-\frac{1}{n_i})-\prod_{i=1}^{k}(1-\frac{1}{n_i})(\frac{1}{n_{k+1}})-1+\sum_{i=1}^{k}\frac{1}{n_i}+\frac{1}{n_{k+1}} \\
&= [\prod_{i=1}^{k}(1-\frac{1}{n_i})-1+\sum_{i=1}^{k}\frac{1}{n_i}]+\frac{1}{n_{k+1}}(1-\prod_{i=1}^{k}(1-\frac{1}{n_i}))
\end{aligned}$$

notemos además que,

$$\forall i[1,k],\ \ 1-\frac{1}{n_i}<1 \Rightarrow \prod_{i=1}^{k}(1-\frac{1}{n_i})<1 \ \ \Rightarrow \ \ -\prod_{i=1}^{k}(1-\frac{1}{n_i})>-1$$

$$\Rightarrow \ \ 1-\prod_{i=1}^{k}(1-\frac{1}{n_i})>0$$

$$\Rightarrow \ \ \frac{1}{n_{k+1}}(1-\prod_{i=1}^{k}(1-\frac{1}{n_i}))>0$$

de este hecho y de la hipótesis inductiva obtenemos lo deseado. con igualdad si y solo si $k=1$. sabemos que

$$\mathsf{k}(S)=\sum_{i=1}^{l}\frac{1}{\mathrm{ord}(g_i)}=\sum_{i=1}^{l}\frac{1}{n_i}$$

Luego,

$$\mathsf{k}(S)\leq 1 \Rightarrow \mathsf{k}(S)-1\leq 0\leq \sum_{i=2}^{k}(-1)^i\sum_{1\leq\nu_1<\ldots<\nu_i\leq k}\frac{1}{n_{\nu_1}\cdot\ldots\cdot n_{\nu_i}}$$

de allí que (2.7) es cierto.

Si p es el menor divisor primo de $\exp(G)$ y $|S|<p$, entonces

$$\begin{aligned}
&\mathrm{ord}(g_i)\mid \exp(G)\\
\Rightarrow\ &\mathrm{ord}(g_i)\geq p \qquad (p \text{ es el menor divisor primo de } \exp(G))\\
\Rightarrow\ &\frac{1}{\mathrm{ord}(g_i)}\leq\frac{1}{p}\\
\Rightarrow\ &\sum_{i=1}^{l}\frac{1}{\mathrm{ord}(g_i)}\leq\sum_{i=1}^{l}\frac{1}{p}\\
\Rightarrow\ &\mathsf{k}(S)\leq\frac{l}{p}=\frac{|S|}{p}<1 \quad (|S|<p)
\end{aligned}$$

luego, (2.7) es cierto y por tanto $(X^{g_1}-a_1)\cdot\ldots\cdot(X^{g_l}-a_l)\neq 0$. □

Corolario 2.3.1. *Sea G un grupo cíclico de orden $n\geq 2$, $g_1,\ldots,g_{n-1}\in G$ y K un campo de descomposición de G. Entonces las siguientes afirmaciones son equivalentes:*

(a) $(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) \neq 0$ *para todo* $a_1, \ldots, a_{n-1} \in K^\times$.

(b) $\mathrm{ord}(g_1) = \ldots = \mathrm{ord}(g_{n-1}) = n$.

Demostración. $(b) \Rightarrow (a)$ Sea $S = g_1 \cdot \ldots \cdot g_{n-1} \in \mathcal{F}(G)$ entonces,

$$\mathsf{k}(S) \leq \sum_{i=1}^{n-1} \frac{1}{\mathrm{ord}(g_i)} = \sum_{i=1}^{n-1} \frac{1}{n} = \frac{n-1}{n} < 1$$

luego, por el Teorema 2.3.1,

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) \neq 0$$

para todo $a_1, \ldots, a_{n-1} \in K^\times$.

$(a) \Rightarrow (b)$ Supongamos, por reducción al absurdo, que $\mathrm{ord}(g_i) < n$ para algún $i \in [1, n-1]$, digamos $\mathrm{ord}(g_1) < n$. Probaremos que existen $a_1, \ldots, a_{n-1} \in \mu_n(K)$ satisfaciendo

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) = 0.$$

CASO 1: $\mathrm{car}(K) \nmid n$. Sea $\Omega = \{\chi \in Hom(G, K^\times) \mid \chi(g_1) \neq 1\}$. Como $\mathrm{ord}(g_1) < n$, por la Proposición 2.2.1 (ii), se sigue que $\chi(g_1) = 1$ para al menos un caracter no trivial $\chi \in Hom(G, K^\times)$, y así obtenemos $|\Omega| \leq n-2$, digamos $\Omega = \{\chi_2, \ldots, \chi_s\}$, donde $s \in [1, n-1]$ y $|\Omega| = s - 1$. Sea

$$f = (X^{g_1} - 1) \prod_{i=2}^{s} (X^{g_i} - \chi_i(g_i)) \prod_{i=s+1}^{n-1} (X^{g_i} - 1) \in K[G].$$

Si $\chi \in \Omega$ entonces, $\chi = \chi_i$ para algún $i \in [2, s]$ de modo que,

$$\chi(X^{g_i} - \chi_i(g_i)) = \chi_i(X^{g_i} - \chi_i(g_i)) = \chi_i(g_i) - \chi_i(g_i) = 0,$$

luego $\chi(f) = 0$ (χ es un homomorfismo de K-álgebras).

Si $\chi \notin \Omega$ entonces $\chi(g_1) = 1$ de modo que

$$\chi(X^{g_1} - 1) = \chi(g_1) - 1 = 1 - 1 = 0,$$

luego $\chi(f) = 0$ (χ es un homomorfismo de K-álgebras). Entonces $\chi(f) = 0$ para todo $\chi \in Hom(G, K^\times)$ y así, por la Proposición 2.2.2 (3), $f = 0$.

CASO 2: $car(K) = p \mid n$. Sea $n = p^e m$, donde $e, m \in \mathbb{N}$ y $p \nmid m$. Entonces K contiene el campo $F = P(\xi_m)$, donde P es el subcampo primo de K y ξ_m es una m-raíz primitiva de la unidad. Por Teorema 1.2.4, sabemos que $P \simeq \mathbb{Z}_p$. Podemos suponer que $K = F$. Sea $\zeta \in \mathbb{C}$ una n-raíz primitiva de la unidad, $L = \mathbb{Q}(\zeta)$, R el anillo de enteros en L, el cual sabemos que es $\mathbb{Z}[\zeta]$, y $\mathfrak{p}$ un ideal maximal de R con $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Entonces, $R/\mathfrak{p} \simeq K$ [9].

Denotemos por $\phi : R[G] \to K[G]$ a la composición de la extensión del epimorfismo canónico $R \to R/\mathfrak{p}$ con la extensión del isomorfismo $R/\mathfrak{p} \simeq K$. Por CASO 1 (con $K = L \subseteq \mathbb{C}, \text{car}(L) = 0$), existen $a_1, \ldots, a_{n-1} \in \mu_n(L)$ tal que $f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) = 0$. Sea $\mu_n(L) = \langle \xi \rangle$ donde $\xi \in \mathbb{C}$ es una n-raíz primitiva de la unidad. Sea $\hat{\xi} \in \mu_n(L)$ entonces $\hat{\xi} = \xi^k$ para algún $k \in \mathbb{Z}$. Supongamos que $\xi^k \in \mathfrak{P}$ entonces, por ser R maximal, R es primo, por lo que $\xi^k \in \mathfrak{p}$ pero, $\xi^k \in \mathfrak{p} \Rightarrow \xi \in \mathfrak{p} \Rightarrow \xi^n = 1 \in \mathfrak{p} \Rightarrow \mathfrak{p} = R$, en contradicción con el hecho de que $\mathfrak{p}$ es un ideal maximal. Luego $\mu_n(L) \subseteq R \backslash \mathfrak{p}$, se sigue que $a_1, \ldots, a_{n-1} \notin \mathfrak{p}$ luego, $a_1 + \mathfrak{p}, \ldots, a_{n-1} + \mathfrak{p} \in R/\mathfrak{p} \simeq K$ son todos distintos de cero así, $\phi(a_1), \ldots, \phi(a_{n-1}) \in K^\times$ y dado que ϕ es la composición de la extensión del epimorfismo canónico $R \to R/\mathfrak{p}$ con la extensión del isomorfismo $R/\mathfrak{p} \cong K$, se tiene finalmente, $0 = \phi(f) = (X^{g_1} - \phi(a_1)) \cdot \ldots \cdot (X^{g_{n-1}} - \phi(a_{n-1})) \in K[G]$ en contradicción con (a). □

A continuación proporcionamos un ejemplo de una secuencia $g_1 \cdot \ldots \cdot g_{p+1}$ en un p-grupo abeliano elemental conteniendo dos elementos independientes tal que $(X^{g_1} - 1) \cdot \ldots \cdot (X^{g_{p+1}} - 1) = 0 \in \mathbb{Z}[G]$.

Ejemplo 2.3.1. Sea G un p-grupo abeliano elemental (para un primo p arbitrario), $g, h \in G$ dos elementos independientes, R un anillo conmutativo,

$$S = gh\prod_{i=1}^{p-1}(g+ih) \in \mathcal{F}(G) \quad \text{y} \quad f = (1-X^g)(1-X^h)\prod_{i=1}^{p-1}(1-X^{g+ih}) \in R[G].$$

Probaremos que $f = 0$. Ya que existe un homomorfismo natural $\varphi : \mathbb{Z}[G] \to R[G]$ (la extensión del homomorfismo $\varphi_0 : \mathbb{Z} \to R$ dado por $\varphi_0(n) = n1_R$), podemos suponer $R = \mathbb{Z}$, y claramente, es suficiente mostrar que $f = 0 \in K[G]$ para algún campo K de números algebraicos. Sea K el campo de las p-raíces de la unidad sobre $\mathbb{Q}$. Entonces K es un campo de descomposición de G, y es suficiente probar que $\chi(f) = 0$ para todo $\chi \in Hom(G, K^\times)$ (ver Proposición 2.2.2). Sea $\chi \in Hom(G, K^\times)$. Si $\chi(g) = 1$ ó $\chi(h) = 1$, entonces obviamente $\chi(f) = 0$. Supongamos que $\chi(g) = \zeta$ y $\chi(h) = \zeta^k$, donde $\zeta \in K$ es una p-raíz primitiva de la unidad y $k \in [1, p-1]$ (todos los elementos de $\mu_p(K)$ distintos de 1 son raíces primitivas de la unidad por ser p primo, y por lo tanto generadores de $\mu_p(K)$). Consideremos $\bar{k} \in \mathbb{Z}_p$, como $\mathbb{Z}_p$ es un campo existe $j \in [1, p-1]$ tal que $\bar{k}\bar{j} = \bar{1}$ pero, $\bar{k}\bar{j} = \bar{1} \Rightarrow \bar{k}(\overline{p-j}) = -\bar{1} \Rightarrow \bar{k}(\overline{p-j}) + \bar{1} = \bar{0} \Rightarrow k(p-j) + 1 \equiv 0 \mod p$. Entonces existe $i \in [1, p-1]$ tal que $ki + 1 \equiv 0 \mod p$ y

$$\begin{aligned}
\chi(f) &= (1-\chi(g))(1-\chi(h))\prod_{i=1}^{p-1}(1-\chi(g+ih)) \\
&= (1-\zeta)(1-\zeta^k)\prod_{i=1}^{p-1}(1-\chi(g)\chi(h)^i) \\
&= (1-\zeta)(1-\zeta^k)\prod_{i=1}^{p-1}(1-\zeta^{1+ki})
\end{aligned}$$

Como $1 + ki \equiv 0 \mod p$ para algún $i \in [1, p-1]$, tenemos que $1 + ki$ es un múltiplo de p, por tanto $\zeta^{1+ki} = 1$ implicando $\zeta^{1+ki} - 1 = 0$, de allí que

$\chi(f) = 0.$

Capítulo 3

Aplicaciones a Transversales de cuadrados latinos aditivos

3.1. Transversales de cuadrados latinos aditivos

Los cuadrados latinos han sido estudiados durante siglos. Sin embargo, fue en 1779 cuando Leonhard Euler los definió formalmente. Euler utilizó letras del latín como elementos de tales cuadrados, llamándolos cuadrados latinos. En este capítulo mostraremos algunas aplicaciones de los cuadrados latinos, es sorprendente la gran variedad de áreas matemáticas en donde dichos cuadrados ofrecen resultados importantes, por ejemplo, en la estadística, la teoría de gráficas y la criptología.

En esta sección aplicaremos los resultados principales obtenidos en la sección anterior, sobre álgebras de grupo, al problema de encontrar transversales latinas en matrices de Cayley de grupos abelianos finitos. No estudiaremos estas nociones combinatorias a profundidad, pero describiremos el problema en términos de secuencias en un grupo abeliano finito y daremos un enfoque un poco más general.

En adelante, para $l \in \mathbb{N}$, denotamos por S_l al grupo de permutaciones de $[1, l]$, y denotamos por sgn, a la función signo $\mathsf{sgn} : S_l \to \{-1, 1\}$, que asigna a cada $\pi \in S_l$ el valor 1 o -1, según π sea par (π se escribe como producto de un número par de trasposiciones) o impar (π se escribe como producto de un número impar de trasposiciones), respectivamente.

Cuadrados latinos y transversales latinas

Una *tabla de adición de Cayley* de un grupo finito es una tabla que describe cómo es la operación de dicho grupo. Dado el grupo finito $G = g_1, g_2, \ldots, g_n$, su tabla de adición de Cayley tendrá n filas y n columnas. En la fila i, columna j, aparece el resultado de la operación $g_i + g_j$, es decir, una tabla de adición de Cayley es la parte no sombreada de la siguiente tabla.

$+$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 + g_1$	$g_1 + g_2$	$\cdots$	$g_1 + g_n$
g_2	$g_2 + g_1$	$g_2 + g_2$	$\cdots$	$g_2 + g_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
g_n	$g_n + g_1$	$g_n + g_2$	$\cdots$	$g_n + g_n$

La matriz de orden $n \times n$

$$\begin{bmatrix} g_1 + g_1 & g_1 + g_2 & \cdots & g_1 + g_n \\ g_2 + g_1 & g_2 + g_2 & \cdots & g_2 + g_n \\ \vdots & \vdots & \vdots & \vdots \\ g_n + g_1 & g_n + g_2 & \cdots & g_n + g_n \end{bmatrix}$$

es una *matriz de Cayley* del grupo G.

Notemos que en una matriz de Cayley de un grupo finito G, cada elemento del grupo aparece una y solo una vez en cada fila y cada columna. Así cada

fila y cada columna es una permutación de los elementos del grupo. Notemos también que existen a lo mas $n!$ matrices de Cayley asociadas a un grupo de orden n.

Ejemplo 3.1.1. Una matriz de Cayley de $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ es

$$C = \begin{bmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{0} \\ \overline{2} & \overline{3} & \overline{4} & \overline{0} & \overline{1} \\ \overline{3} & \overline{4} & \overline{0} & \overline{1} & \overline{2} \\ \overline{4} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \end{bmatrix}$$

Definición 3.1.1. Un cuadrado latino L de orden n es una matriz de orden $n \times n$, cuyos elementos pertenecen a un conjunto finito A de cardinalidad n, y cada uno de ellos aparece exactamente una vez en cada fila y en cada columna de L.

Ejemplo 3.1.2. Una matriz de Cayley de un grupo finito de orden n es un cuadrado latino con base G. En particular, la matriz de Cayley del Ejemplo 3.1.1, es un cuadrado latino de orden 5 con base $\mathbb{Z}_5$.

Definición 3.1.2. Una *transversal* de una matriz A de orden $n \times n$ es una colección de n posiciones de la matriz A, tal que cualquiera dos de ellas no están en la misma fila ni en la misma columna. Una transversal de una matriz, es una *transversal latina* si las entradas de la matriz en las posiciones de la transversal son distintas dos a dos.

Ejemplo 3.1.3. Una transversal de la matriz C del Ejemplo 3.1.1 es

$$\{(1,1), (3,5), (5,4), (2,2), (4,3)\},$$

esta trasversal no es una transversal latina, ya que las entradas en la posición $(5,4)$ y $(2,2)$ son ambas iguales a $\overline{2}$. Sin embargo, $\{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ es una transversal latina de C.

Ejemplo 3.1.4. No todas las matrices de Cayley poseen transversales latinas, por ejemplo la matriz de Cayley de $\mathbb{Z}_2$,

$$\begin{bmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{bmatrix}$$

no posee transversales latinas.

Existencia de transversales latinas en algunos cuadrados latinos aditivos

Una conjetura de Snevily ([15] Conjetura 1) afirma que, toda submatriz de orden $k \times k$ de una matriz de Cayley de un grupo abeliano finito de orden n impar, posee una transversal latina.

Observar que la conjetura de Snevily falla si G es un grupo abeliano finito de orden par, pues en tal caso, G posee un elemento x de orden 2. Luego,

$$\begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix}$$

es una submatriz de una matriz de Cayley de G que no posee transversales latinas.

Como cada entrada de la matriz de Cayley C de un grupo G proviene de sumar dos elementos de G, cada transversal de una submatriz A de C de orden $k \times k$, determina dos secuencias libres de cuadrados en $\mathcal{F}(G)$ de longitud k, digamos $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ y $b_1 \cdot b_2 \cdot \ldots \cdot b_k$. Ahora, que la submatriz C posea una transversal latina, equivale a decir que existe $\pi \in S_n$ tal que

las k sumas $a_i + b_{\pi(i)}$ con $1 \leq i \leq k$ son distintas dos a dos, esto es, k tiene la propiedad $\mathbf{P}$. Recíprocamente, dadas dos secuencias libres de cuadrados de longitud k en $\mathcal{F}(G)$, digamos $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ y $b_1 \cdot b_2 \cdot \ldots \cdot b_k$, podemos construir una matriz de Cayley, que posea una submatriz de orden $k \times k$ de tal manera que sus entradas sean $a_i + b_i$ para $1 \leq i \leq k$, si la submatriz posee una transversal latina entonces, k tiene la propiedad $\mathbf{P}$. De modo que la siguiente conjetura implica la conjetura de Snevily .

Conjetura 3.1.1. [Conjetura de Snevily][15] Si G es un grupo abeliano finito de orden n impar, entonces todo $l \in [1, n]$ tiene la propiedad $\mathbf{P}$ para G.

Alon probó la Conjetura de Snevily para gupos de orden primo [1], y en [2] podemos encontrar una prueba para grupos cíclicos de orden impar. Un caso especial de la Conjetura de Snevily es la siguiente conjetura.

Conjetura 3.1.2. [15] Si G es un grupo abeliano finito de orden n impar y p es el menor primo que divide a $\exp(G)$, entonces todo $l \in [1, p]$ tiene la propiedad $\mathbf{P}$ para G.

Las Conjeturas 3.1.1 y 3.1.2 son equivalentes para grupos cíclicos de orden primo. La conjetura 3.1.2 fue probada para p-grupos elementales en [2].

El Teorema 2.3.1 y un resultado en [2] que determina el producto del determinante por el permanente de una matriz de Vandermonde, nos permitirán ofrecer un nuevo enfoque de la Conjetura 3.1.2.

Definición 3.1.3. Sea R un anillo conmutativo, $l \in \mathbb{N}$ y M una matriz de orden $l \times l$ con entradas en R, es decir, $M = (x_{i,j})_{l \times l} \in \mathbb{M}_{l \times l}(R)$. Se define:

El permanente de M, denotado por $\mathsf{Perm}M$, como

$$\mathsf{Perm}M = \sum_{\pi \in S_l} x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{l,\pi(l)}.$$

El determinante de M, denotado por $\mathsf{Det}M$, como

$$\mathsf{Det}M = \sum_{\pi \in S_l} \mathsf{sgn}(\pi) x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{l,\pi(l)}.$$

Observemos que si R tiene característica 2 entonces, el determinante y el permanente de una matriz con entradas en R coinciden.

Definición 3.1.4. Sea R un anillo conmutativo, $l \in \mathbb{N}$ y $x_1, x_2, \ldots, x_l \in R$. La matriz de Vandermonde generada por $x_1, x_2, \ldots, x_l$, se define como

$$V(x_1, x_2, \ldots, x_l) := \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_l \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{l-1} & x_2^{l-1} & \ldots & x_l^{l-1} \end{bmatrix}.$$

Teorema 3.1.1. *[4]* $\mathsf{Det}V(x_1, x_2, \ldots, x_l) = \prod_{1 \leq i < j \leq l} (x_j - x_i)$.

La siguiente proposición determina el producto del determinante por el permanente de la matriz de Vandermonde.

Proposición 3.1.1. *[2] Sea R un anillo conmutativo, $l \in \mathbb{N}$ y $x_1, \ldots x_l$, $y_1, \ldots, y_l \in R$. Entonces*

$$\mathsf{Det}V(x_1, x_2, \ldots, x_l)\mathsf{Perm}V(y_1, y_2, \ldots, y_l) = \sum_{\pi \in S_l} \prod_{1 \leq i < j \leq l} (x_j y_{\pi(j)} - x_i y_{\pi(i)})$$

Teorema 3.1.2. *Sea G un grupo abeliano finito de orden impar, $l \in \mathbb{N}$, $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ una secuencia libre de cuadrados y $\prod_{i=1}^{l} h_i \in \mathcal{F}(G)$ cualquier secuencia de longitud l. En cada uno de los siguientes casos, existe una permutación $\pi \in S_l$ tal que la secuencia $\prod_{i=1}^{l}(g_i + h_{\pi(i)})$ es libre de cuadrados:*

(i) G *es un* p*-grupo,* $l < p$ *y* $\mathsf{Det}V(X^{g_1}, \ldots, X^{g_l}) \neq 0 \in \mathbb{Z}[G]$.

(ii) G *es cíclico y* $\mathsf{Perm}V(X^{h_1}, \ldots, X^{h_l})$ *no es un divisor de cero en* $\mathbb{Z}[G]$.

(iii) Para la secuencia

$$S = \prod_{1 \leq i < j \leq l} (g_j - g_i)(h_j - h_i) \in \mathcal{F}(G)$$

se tiene que $\mathsf{k}(S) < 1$*, o* $\mathsf{k}(S) \leq 1$ *y* $\operatorname{supp}(S)$ *contiene al menos dos elementos independientes.*

Demostración. Por la Proposición 3.1.1 tenemos

$$\begin{aligned} & \mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \\ = & \sum_{\pi \in S_l} \prod_{1 \leq i < j \leq l} (X^{g_j + h_{\pi(j)}} - X^{g_i + h_{\pi(i)}}). \end{aligned}$$

Es suficiente probar que

$$\mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \neq 0.$$

En ese caso, existe $\pi \in S_l$ tal que

$$\prod_{1 \leq i < j \leq l} (X^{g_j + h_{\pi(j)}} - X^{g_i + h_{\pi(i)}}) \neq 0$$

así, la secuencia $(g_1 + h_{\pi(1)}) \cdot \ldots \cdot (g_l + h_{\pi(l)})$ es libre de cuadrados.

(i) Por la definición de permanente, tenemos

$$\begin{aligned} \varepsilon(\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l})) &= \varepsilon(\sum_{\pi \in S_l} X^{0h_{\pi(1)}} X^{1h_{\pi(2)}} \cdot \ldots \cdot X^{(l-1)h_{\pi(l)}}) \\ &= \varepsilon(\sum_{\pi \in S_l} X^{\sum_{i=1}^{l} (i-1)h_{\pi(i)}}) \\ &= \sum_{\pi \in S_l} 1 = |S_l| = l! \notin p\mathbb{Z} \ \ (l < p) \end{aligned}$$

Así $\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l})$ no es un divisor de cero en $\mathbb{Z}[G]$ (por la Proposición 2.3.2). Como $\mathbb{Z}[G]$ es un dominio de integridad y $\mathsf{Det}V(X^{g_1}, \ldots, X^{g_l}) \neq 0 \in \mathbb{Z}[G]$, entonces

$$\mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \neq 0$$

(ii) Como la secuencia $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ es libre de cuadrados entonces $g_j - g_i \neq 0$ además $0 = \mathrm{car}(\mathbb{Z}) \nmid \mathrm{ord}(g_j - g_i)$. Entonces por la Proposición 2.3.1 tenemos

$$\prod_{1 \leq i < j \leq l} (X^{g_j - g_i} - 1) \neq 0,$$

y como $X^{g_i} \in \mathbb{Z}[G]^{\times}$ para todo $i \in [1, l]$, obtenemos

$$\mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l}) = \prod_{1 \leq i < j \leq l} (X^{g_j} - X^{g_i}) = \prod_{1 \leq i < j \leq l} X^{g_i}(X^{g_j - g_i} - 1) \neq 0.$$

Como $\mathsf{Perm}V(X^{h_1}, \ldots, X^{h_l})$ no es un divisor de cero en $\mathbb{Z}[G]$ entonces,

$$\mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \neq 0$$

(iii) Veremos las matrices $V(X^{g_1}, \ldots, X^{g_l})$ y $V(X^{h_1}, \ldots, X^{h_l})$ como matrices sobre $K[G]$, donde $K = \mathbb{Z}/2\mathbb{Z} = [\overline{0}, \overline{1}]$ denota el campo con dos elementos. Es suficiente probar que $f = \mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \neq 0 \in K[G]$. Tenemos

$$\begin{aligned}
f &= \mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Perm}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \\
&= \mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l})\mathsf{Det}V(X^{h_1}, X^{h_2}, \ldots, X^{h_l}) \quad (\mathrm{car}(K) = 2) \\
&= \prod_{1 \leq i < j \leq l} (X^{g_j} - X^{g_i}) \prod_{1 \leq i < j \leq l} (X^{h_j} - X^{h_i}) \\
&= \prod_{1 \leq i < j \leq l} X^{g_i + h_i}(X^{g_j - g_i} - \overline{1})(X^{h_j - h_i} - \overline{1}) \neq 0
\end{aligned}$$

pues $X^{g_i+h_i} \in K[G]^\times$ y

$$\prod_{1\le i<j\le l} (X^{g_j-g_i}-\overline{1})(X^{h_j-h_i}-\overline{1}) \neq 0$$

por el Teorema 2.3.1.

□

Corolario 3.1.1. *Sea G un grupo abeliano finito de orden impar, $l \in \mathbb{N}$, $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ una secuencia libre de cuadrados y $\prod_{i=1}^{l} h_i \in \mathcal{F}(G)$ cualquier secuencia de longitud l. En cada uno de los siguientes casos, existe una permutación $\pi \in S_l$ tal que la secuencia $\prod_{i=1}^{l}(g_i+h_{\pi(i)})$ es libre de cuadrados:*

(i) G es un p-grupo, $l < p$ y para la secuencia

$$S = \prod_{1\le i<j\le l} (g_j - g_i) \text{ tenemos } \mathsf{k}(S) < 1.$$

(ii) G es un p-grupo y $2l < 1 + \sqrt{8p+1}$.

(iii) La secuencia $\prod_{i=1}^{l} h_i$ es libre de cuadrados, y $2l < 1 + \sqrt{4p+1}$, donde p denota el divisor primo mas pequeño de $|G|$.

Demostración. (i) Tenemos

$$\mathsf{Det}V(X^{g_1}, X^{g_2}, \ldots, X^{g_l}) = \prod_{1\le i<j\le l} (X^{g_j}-X^{g_i}) = \prod_{1\le i<j\le l} X^{g_i} \prod_{1\le i<j\le l} (X^{g_j-g_i}-\overline{1})$$

Como el primer factor es una unidad en $\mathbb{Z}[G]$, y el segundo factor no es un divisor de cero (por el Teorema 2.3.1), la afirmación se sigue del Teorema 3.1.2.

(ii) Como $\prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ es libre de cuadrados, la secuencia $S = \prod_{1\le i<j\le l}(g_j - g_i)$ satisface $\mathrm{ord}(g_j - g_i) \ge p$ pero,

$$\begin{aligned}\mathrm{ord}(g_j - g_i) \ge p \;&\Rightarrow\; \frac{1}{\mathrm{ord}(g_j - g_i)} \le \frac{1}{p} \\ &\Rightarrow\; \mathsf{k}(S) = \sum_{1\le i<j\le l} \left(\frac{1}{\mathrm{ord}(g_j - g_i)}\right) \le \sum_{1\le i<j\le l} \frac{1}{p} = \frac{1}{p}\binom{l}{2}\end{aligned}$$

además,

$$\begin{aligned}2l < 1 + \sqrt{8p+1} \Rightarrow (2l-1)^2 < 8p+1 \;&\Rightarrow\; 4l^2 - 4l + 1 < 8p + 1 \\ &\Rightarrow\; l(l-1) < 2p \\ &\Rightarrow\; \frac{l(l-1)}{2p} < 1\end{aligned}$$

entonces $\mathsf{k}(S) < 1$, luego la afirmación se sigue de la parte (i)

(iii) Como ambas, $g_1 \cdot \ldots \cdot g_l$ y $h_1 \cdot \ldots \cdot h_l$, son libres de cuadrados

$$S = \prod_{1\le i<j\le l} (g_j - g_i)(h_j - h_i) \in \mathcal{F}(G)$$

satisface

$$\mathsf{k}(S) = \sum_{1\le i<j\le l} \left(\frac{1}{\mathrm{ord}(g_j - g_i)} + \frac{1}{\mathrm{ord}(h_j - h_i)}\right) \le \frac{2}{p}\binom{l}{2},$$

además,

$$\begin{aligned}2l < 1 + \sqrt{4p+1} \Rightarrow (2l-1)^2 < 4p+1 \;&\Rightarrow\; 4l^2 - 4l + 1 < 4p + 1 \\ &\Rightarrow\; l(l-1) < p \\ &\Rightarrow\; \frac{l(l-1)}{p} < 1\end{aligned}$$

entonces $\mathsf{k}(S) < 1$, luego la afirmación se sigue del Teorema 3.1.2.

□

Conclusiones

En este trabajo estudiamos las álgebras de grupo sobre un grupo abeliano finito G, basados en el artículo [5], mostramos algunos divisores de cero en las álgebras de grupo sobre un dominio de integridad y definimos algunos homomorfismos especiales sobre ellas. También estudiamos condiciones para que dada una secuencia $g_1, g_2, \ldots, g_l$ de elementos en un grupo abeliano finito G, se tenga

$$(X^{g_1} - a_1)(X^{g_2} - a_2)\ldots(X^{g_l} - a_l) \neq 0 \in R[G] \text{ para todo } a_1, a_2, \ldots, a_l \in R$$

donde R es un dominio de integridad. Aplicamos los resultados obtenidos sobre álgebras de grupos, para abordar una conjetura de Snevily en [15], la cual se verifica para un caso especial, además mostramos algunas variaciones de dicha conjetura. En general, la conjetura de Snevily permanece abierta.

Referencias

[1] N. Alon (2000). Additive Latin transversals, *Isr. J. Math.* **117**, 125–130.

[2] S. Dasgupta, G. Károlyi, O. Serra, and B. Szegedy (2001). Transversals of additive Latin squares, *Isr. J. Math.* **126**, 17–28.

[3] H. Davenport (1966). *Proceedings of the midwestern conference on group theory and number theory*. Ohio State University.

[4] P. Garret (2007). *Abstrac Algebra*. Chapman & Hall, CRC Press.

[5] W. Gao, A. Geroldinger and F. Halter-Koch (2009). Groups algebra of finite abelian groups and their applications to combinatorial problems, *Rocky mountain journal of mathematics*. **39**, 805–823.

[6] W. Gao and D.J. Wang (2004). Additive Latin transversals and group rings, *Isr. J. Math.* **140** , 375–380.

[7] A. Geroldinger and F. Halter-Koch. Non-Unique Factorizations (2006). *Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics*. Chapman & Hall/CRC.

[8] T. Hungerford (1974), *Algebra*. Springer-Verlag, New York.

[9] S. Lang (1994), *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York.

[10] D. Malik, J. Mordeson, M. Sen (2007), *Introduction to abstract algebra*. Creighton University.

[11] A. Navas (2010). On the dynamics of left ordenable groups, *Annales de I'nstitut Fourier*. **60** 1685–1740.

[12] J. Olson (1969). A combinatorial problem on finite abelian groups I, *Journal of Number Theory*. **1** , 8-10.

[13] J. Olson (1969). A combinatorial problem on finite abelian groups II, *Journal of Number Theory*. **1**, 195-199.

[14] K. Rogers (1963). A combinatorial problem in Abelian groups, *Proc. Cambridge Phil. Soc.* **59** , 559–562.

[15] H. Snevily (1999). The Cayley addition table of $\mathbb{Z}_n$, *Amer. Math. Monthly*. **106** 584–585.