PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

K teoría algebraica de anillos de grupos y sus aplicaciones

Tesis para optar el grado de Magister en Matemática que presenta

Carlos Arturo Hurtado Amaya

Dirigido por:

Dr. Christian Holger Valqui Haase

Miembros del jurado:

Dr. Julio César Alcántara Bode – PUCP (Perú)

Dr. Juan José Guccione – UBA (Argentina)

San Miguel, 2016

K teoría algebraica de anillos de grupos y sus aplicaciones

Carlos Arturo Hurtado Amaya

Tesis presentada a consideración del cuerpo docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú. Como parte de los requisitos para obtener el grado de Magíster en Matemática.

Miembros del jurado:

Dr. Julio César Alcántara Bode (Presidente)

Dr. Juan José Guccione (miembro)

Dr. Christian Holger Valqui Haase (asesor)

Papers should include more side remarks, open questions, and such. Very often, these are more interesting than the theorems actually proved. Alas, most people are afraid to admit that they don't know the answer to some question, and as a consequence they refrain from mentioning the question, even if it is a very natural one. What a pity! As for myself, I enjoy saying 'I do not know'.

Jean-Pierre Serre

Resumen

La K teoría algebraica de anillos de grupo ha sido ampliamente tratada en los últimos 40 años. Esto se debe en parte a las aplicaciones existentes en topología, teoría de números y teoría de representaciones.

Se presenta los anillos de grupo y algunos problemas relacionados con éstos, en particular, la conjetura de idempotencia de Kaplansky. Por otro lado, se introduce la K teoría algebraica de un anillo de grupo y se presenta una aplicación a la teoría de representaciones de grupos finitos.

Palabras clave: K teoría algebraica, Álgebra, Anillos de grupo.

Abstract

The algebraic K theory of group rings has been widely discussed in the past 40 years. This is due in part to existing applications in topology, number theory and representation theory .

We presente the group rings and some problems related to them, in particular, the idempotent conjecture of Kaplansky. On the other hand , we introduce the algebraic K theory of group rings and we introduce an application to representation theory of finite groups.

Keywords: Algebraic K theory, Algebra, Group rings.

Agradecimientos

Quiero expresar mi más sincero agradecimiento al profesor Christian Valqui por todas sus indicaciones en el desarrollo de esta tesis, su infinita paciencia en su guía e incondicional apoyo.

Por otra parte, agradezco las valiosas observaciones del jurado, Dr. Julio Alcántara y Dr. Juan José Guccione. Adicionalmente, también recibí sugerencias y aportes de Dra. Eugenia Ellis, por sus sugerencias en el capítulo 3 de la presente tesis.

También quiero agradecer todos los profesores de la maestría de matemáticas. En especial a los profesores Dr. Alfredo Poirier Schmitz y Dr. Christian Bernardo Figueroa Serrudo por sus cursos impartidos en la maestría y en los que tuve la oportunidad de ser su estudiante, así como su disposición de siempre atenderme cuando tenga una inquietud ya sea relacionada con las matemáticas, temas administrativos en el departamento de matemáticas o personales.

Finalmente, y no menos importante, quiero agradecer a Diana Patricia que me apoyó con su paciencia y comprensión en el transcurso de esta aventura que ha sido venir al Perú y el emprender mis estudios nuevamente. Además no puedo dejar pasar al pequeño Alejandro Gabriel quien ha alegrado nuestras vidas con esas noches de desvelo tan necesarias para el desarrollo del presento texto, su compañía en esos momentos ha sido invaluable.

Introducción

La temática central de la tesis son los anillos de grupo. Este tipo de estructuras han sido ampliamente estudiadas como lo demuestra el enciclopédico libro de Passman [Pas11] o [Seh78]. Además, actualmente poseen una gran cantidad de problemas no resueltos que involucran otras áreas de las matemáticas como teoría de operadores o análisis funcional.

Adicionalmente, el presente documento busca exponer diferentes cálculos y aspectos de la teoría K algebraica, en particular, los que involucran anillos de grupo. Este tema ha sido ampliamente tratado en los últimos 40 años, como lo demuestran los textos [Emm05], [Ros95] o [Kuk00]. Esto se debe en parte a las aplicaciones existentes de estas en la topología, teoría de números y teoría de representaciones.

Teniendo en cuenta lo anterior, se ha tratado de buscar un tema que conecte estos dos interéses. La conjetura de idempotencia de Kaplansky ha mostrado ser el puente que nos permite cumplir ambos objetivos.

El presente documento en principio obedece a un interés en exponer los problemas relacionados con los elementos idempotentes en un anillo de grupo y su relación con la teoría K algebraica. Esto es desarrollado en 3 capítulos que a continuación resumo.

El capítulo 1 esta dedicado a discutir los preliminares algebraicos necesarios para presentar $\mathrm{K}_0(R)$ y $\mathrm{K}_1(R)$ de un anillo R, así como la teoría de módulos sobre anillos de grupo. Se hace una breve introducción a la teoría de representaciones y se discute los casos donde RG es un anillo semisimple y cuando no.

El capítulo 2 muestra una aplicación de la teoría de los módulos sobre anillos de grupo al estudio de la conjetura de idempotencia[1]. La técnica presentada en este trabajo fue desarrollada por Emmanouil Ionais en [Emm01].

Siguiendo la presentación de la conjetura de idempotencia dada en [Emm01] se concluye que esta es satisfecha por todos los grupos abelianos libres de torsion. Este resultado

[1]La conjetura de idempotencia afirma que si R un dominio de integridad y G un grupo libre de torsión. entonces RG no posee idempotente no triviales.

no es del todo nuevo ya que en [Edw73] se demuestra para una clase de grupos que abarcan a estos grupos, lo notable en este punto es la estrategia empleada.

Como resultado propio y usando los desarrollos de Ionais se presenta una familia de grupos no conmutativos que satisfacen esta conjetura. Este resultado ejemplifica el alcanzado por Hyman Bass en [Bas76].

El capítulo 3 se presentan los funtores $\mathrm{K}_0(\cdot)$ y $\mathrm{K}_1(\cdot)$, se presentan sus principales propiedades y se calculan para varios tipos de anillos, haciendo énfasis en el cálculo de anillos de grupo.

En general, se calcula en detalle $\mathrm{K}_0(\mathbb{C}G)$ cuando G es un grupo finito y se presenta la relación de éste cálculo con el anillo de representaciones del grupo G. Adicionalmente, se enuncia la conjetura de Farell - Jones sobre anillos de grupo, así como un teorema que las relaciona, presentado en [BLR08].

Los dos apéndices tienen naturaleza distinta. El primero hace una introducción al lenguaje de las categorías, el cual es usado en todos los capítulos y el segundo es la clasificación de todos los subgrupos aditivos de $\mathbb{Q}$.

Existen desarrollos interesantes los cuales han sido dejados de lado por su extension, por ejemplo, $\mathrm{K}_0(\mathcal{O}_K)$ y $\mathrm{K}_1(\mathcal{O}_K)$ donde $\mathcal{O}_K$ es el anillos de enteros algebraicos de un cuerpo numérico. O la sucesión de Mayer-Vietoris para $\mathrm{K}_0(\cdot)$ y $\mathrm{K}_1(\cdot)$ y la presentación de éstos para una categoría abeliana. Realizarlos en este documento actualmente aumentaría considerablemente su tamaño.

El orden de la presentación esta relacionado con la comprensión que he adquirido sobre los anillos de grupo y la teoría K algebraica durante 2 años, he procurado de dar ejemplos de la mayoría de conceptos y de esta manera hacer una presentación lo más "Didáctica" posible. siempre teniendo en cuenta (o consideración) al lector, ya que no se asume ningún conocimiento especializado sobre el tema.

Carlos Hurtado

Contenido

Capítulo 1

Preliminares

El estudio de la K teoría algebraica esta fundamentado principalmente en la teoría de módulos y la teoría de anillos. Uno de los objetivos del presente capítulo es proveer al lector de una exposición de los conceptos. Otro objetivo de este capítulo es la exposición de los anillo de grupo a los cuales se les dedica una sección y se encuentra basada en los textos [MS08] ,[Seh78], [Pas11].

1.1 Módulos y Anillos

Iniciaremos nuestra presentación con el concepto de módulo. El lector en este punto solo debe recordar las propiedades básicas de grupo y anillo, es más que suficiente consultar [Hun03, capítulos I y III]). Comenzaremos desde los conceptos más "sencillos" hasta los más complejos con la esperanza de mejorar su comprensión.

A menos que se especifique lo contrario, por la palabra anillo se entenderá un anillo con unidad (no necesariamente conmutativo). Si R y S son anillos y $f : R \to S$ es un homomorfismo de anillos, entonces $f(1) = 1$, es decir, preservan los elementos identidad de cada anillo y para todo subanillo S de un anillo R se tiene que 1_R pertenece a S. Por último, denotaremos todo cuerpo con la letra $\mathbb{K}$.

Una operación que usaremos con frecuencia es el producto tensorial de R-módulos. A continuación la describiremos y daremos algunas propiedades.

Definición 1.1. *Sea M un R-módulo a derecha, N un R-módulo a izquierda y C un grupo abeliano (notado aditivamente), entonces una aplicación balanceada de $M \times N$ a C es una función $f : M \times N \to C$ tal que*

$$\begin{aligned} f(m_1 + m_2, n) =& f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) =& f(m, n_1) + f(m, n_2), \\ f(mr, n) =& f(m, rn). \end{aligned}$$

Para todo m, m_1, m_2 en M, n, n_1, n_2 en N y r en R.

Definición 1.2. *Sea M un R-módulo a derecha, N un R-módulo a izquierda. Sea F el grupo abeliano libre sobre el conjunto $M \times N$. Sea K el subgrupo de F generado por todos los elementos de la siguiente forma*

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$,
3. $(mr, n) - (m, rn)$

para todo m, m_1, m_2 en M, n, n_1, n_2 en n y r en R. El grupo cociente F/K es llamado el producto tensorial de M y N y es denotado por $M \otimes_R N$.

Por otro lado, siguiendo la notación de la anterior definición, la aplicación $i : M \times N \to M \otimes N$ dada por $f(m, n) = m \otimes n$ es balanceada. Esta función es llamada el morfismo canónico lineal. Es posible describir el producto tensorial mediante una propiedad universal.

Proposición 1.3. *Sea M un R-módulo a derecha, N un R-módulo a izquierda, y sea C un grupo abeliano. Si $g : M \times N \to C$ es una aplicación balanceada, entonces existe un único homomorfismo $\bar{g} : M \otimes N \to C$ tal que el siguiente diagrama*

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "i"] & C \\ M \otimes N \arrow[ur, "\bar{g}"'] & \end{tikzcd}$$

es conmutativo.

Demostración. ver [Hun03, capítulo IV, teorema 5.2] □

Por otro lado, el producto tensorial tiene las siguientes propiedades:

Proposición 1.4. *Sea R y S anillos*

1. *Si A es un R-módulo a derecha y B un R-módulo a izquierda, entonces $A \otimes_R R \simeq A$ y $R \otimes_R B \simeq B$.*
2. *Si A es un R-módulo a derecha, B un $R-S$-bimódulo y C un S-módulo entonces $(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C)$*
3. *Si $\{A_i | i \in I\}$ es una familia de R-módulos a derecha y $\{B_j | j \in J\}$ es una familia de R-módulos a izquierda, entonces*

$$\left(\sum_{i \in I} A_i\right) \otimes_R B \simeq \sum_{i \in I} (A_i \otimes_R B)$$
$$A \otimes_R \left(\sum_{j \in J} B_j\right) \simeq \sum_{j \in J} (A \otimes_R B_j)$$

Demostración. Ver [Hun03, Captiulo IV, Teorema 5.7, 5.8 y 5.9] □

El concepto de ideal de un anillo será de importancia en los resultados que desarrollaremos a lo largo de éste documento.

Definición 1.5. *Sea R un anillo y $S \subset R$ no vacío tal que S es cerrado bajo las operaciones de adición y multiplicación en R. Si S es un anillo bajo las operaciones de R restringidas a los elemento de S, entonces S es llamado un subanillo de R. Un subanillo I de un anillo R es un ideal a izquierda si satisface la condición*

Si r está en R y x en I entonces rx pertenece en I;

I es un ideal a derecha si satisface la condición

Si r está en R y x en I entonces xr pertenece en I;

I es un ideal (bilátero) si es un ideal a izquierda y a derecha.

Un resultado que se usará con frecuencia es el siguiente:

Proposición 1.6. *Sea R un anillo, I un ideal de R y M en R-módulo a izquierda. Sea*

$$IM = \left\{ \sum_{k=1}^{n} r_k m_k | r_k \in I, x_k \in M \right\}.$$

Entonces $(R/I) \otimes_R M \simeq M/IM$

Demostración. Considere la función $f : (R/I) \times M \to M/IM$, $f(\bar{r}, x) = \overline{rx}$. Tenemos que si $(\bar{r}, x) = (\bar{s}, x)$ entonces $\bar{s}x = rx + IM$ y $f(\bar{r}, x) = f(\bar{s}, x)$, luego f esta bien definida. De este modo, por la propiedad universal del producto tensorial, tenemos un único homomorfismo $\bar{f} : (R/I) \otimes_R M \to M/IM$, $\bar{f}(\bar{r} \otimes x) = \overline{rx}$. Por otro lado consideremos el homomorfismo $h : M/IM \to (R/I) \otimes_R M$ dado por $h(\bar{x}) = 1 \otimes x$ y observe que si $\bar{y} = \bar{x}$ entonces $y + IM = x + IM$ y así $x - y$ está en IM y $1 \otimes x = 1 \otimes y$, luego h esta bien definida, además $\bar{f}$ y h son inversas una de la otra. □

Este resultado tiene diversas aplicaciones, por ejemplo:

Corolario 1.7. *Sea R un anillo, I y J ideales de R, entonces $R/I \otimes R/J \simeq R/(I + J)$.*

Demostración. Por la proposición anterior $R/I \otimes R/J \simeq (R/I)/J(R/I)$, y por otro lado $J(R/I) = (I + J)/I$, luego $R/I \otimes R/J \simeq (R/I)/((I + J)/I) \simeq R/(I + J)$. □

Una observación que será útil en nuestro estudio es que si tenemos un anillo sin unidad, siempre es posible sumergirlo dentro de uno que si la posea. Esto nos permitirá considerar a los ideales como subanillos.

Teorema 1.8 (Teorema de extensión de Dorroh)**.** *Cualquier anillo R puede ser incrustado en un anillo S con unidad. El anillo S (el cual no es único) puede ser de característica 0 o de la misma característica de R.*

Demostración. Ver [Hun03, capítulo III teorema 1.10.] □

Definición 1.9. *Sea R un anillo, denotamos por $U(R)$ el grupo multiplicativo de las unidades de R*

Dado R un anillo siempre podemos considerar el anillo de matrices de orden $n \times m$ sobre R el cual denotaremos por $M_{n\times m}(R)$, el anillo de matrices cuadradas $M_n(R)$ y $GL_n(R)$ las unidades de este anillo.

Proposición 1.10. *Sea R un anillo y m, n, p, q en $\mathbb{N}$, entonces*

1. *Si A esta en $M_{m\times n}(R)$ entonces $I_m A = A = AI_n$.*

2. *Si A esta en $M_{m\times n}(R)$, B esta en $M_{n\times p}(R)$ y C esta en $M_{p\times q}(R)$ entonces $(AB)C = A(BC)$.*

3. *Si A esta en $M_{m\times n}(R)$, B y C están en $M_{n\times p}(R)$ y D esta en $M_{p\times q}(R)$ entonces $A(B + C) = AB + AC$ y $(B + C)D = BD + CD$.*

4. *Cuando identificamos R^m con $M_{1\times m}(R)$ cada homomorfismo $f : R^m \to R^n$ esta dado por la multiplicación a derecha por una única matriz A de $M_{m\times n}(R)$. Esto induce un isomorfismo de grupos aditivos*

$$Hom_R(R^m, R^n) \simeq M_{m\times n}(R)$$

y un isomorfismo de anillos

$$End_R(R^n) \simeq (M_n(R))^{op}$$

Demostración. Ver [Mag10, Capítulo 1, proposición 1.26] □

Existe una correspondencia entre los ideales de R y $M_n(R)$ como lo muestra el siguiente resultado.

Proposición 1.11. *Sea R un anillo y $M_n(R)$ el anillo de matrices de $n \times n$ sobre R. Entonces cualquier ideal U de $M_n(R)$ es de la forma $M_n(I)$ para un único ideal I de R.*

Demostración. [Lam01, Capítulo 1, teorema 3.1] □

Proposición 1.12. *Sea R un anillo*

1. *El centro del anillo $M_n(R)$ consiste en todas las matrices de la forma rI_n donde r esta en el centro de R.*

2. *El centro de $M_n(R)$ es isomorfo al centro de R*

Demostración. Ejercicio para el lector. □

En cierta forma el estudio de la K teoría algebraica depende de muchas de las propiedades de los anillos de matrices. Por otro lado, un ejemplo no menos importante de anillo es el anillo de polinomios en n indeterminadas y con coeficientes en R, el cual notaremos por $R[x_1, \ldots, x_n]$. También consideraremos el anillo de series de potencias formales en n indeterminadas el cual escribiremos por $R[[x_1, \ldots, x_n]]$.

Para concluir por un momento el uso del anillo $M_n(R)$, lo usaré para ejemplificar el concepto de condición de cadena, el cual deriva en el concepto de anillo Noetheriano y Artiniano.

Definición 1.13. *Sea M y N R-módulos a izquierda*

1. *Decimos que M satisface la condición ascendente de cadena sobre submódulos (o M es noetheriano) si para cualquier cadena*

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

de submódulos de M, existe un j tal que $M_j = M_i$ para todo $i \geq j$.[1]

2. *Decimos que M satisface la condición descendente de cadena sobre submódulos (o M es Artiniano) si para cualquier cadena*

$$N_1 \supset N_2 \supset N_3 \supset \cdots$$

de submódulos de M, existe un j tal que $N_j = N_i$ para todo $i \geq j$.

Definición 1.14. *Sea R un anillo*

1. *R es llamado Noetheriano a izquierda (o a derecha) si R satisface la condición de cadena ascendente sobre sus ideales a izquierda (o a derecha). R es Noetheriano si lo es a izquierda y derecha.*

2. *R es llamado Artiniano a izquierda (o a derecha) si R satisface la condición de cadena descendente sobre sus ideales a izquierda (o a derecha). R es Artiniano si lo es a izquierda y derecha.*

Damos algunos ejemplos sobre estos conceptos

Ejemplos. *El concepto de anillo Noetheriano y Artiniano existe en álgebra conmutativa como en álgebra no conmutativa.*

1. *Todo Anillo de Division D es Artiniano y también Noetheriano ya que la única cadena de ideales que se puede formar es $(0) \subset D$.*

2. *$\mathbb{Z}$ es un anillo Noetheriano ya que si*

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots$$

es una cadena ascendente de ideales, considere la sucesión de los generadores de los ideales de la cadena $\{a_i\}$ tal que $a_{i+1}|a_i$ donde a_i es entero. Sin perdida de generalidad, podemos suponer que $a_i \geq 0$, de esta forma $\{a_i\}$ es una sucesión decreciente de números positivos, luego posee un mínimo, y de esta forma, existe un k tal que $a_k = ua_i$ donde u es una unidad e $i \geq k$. Pero $\mathbb{Z}$ no es Artiniano ya que para cada a diferente de 1 y -1 la cadena

$$(a) \supset (a^2) \supset (a^2) \supset \cdots \supset (a^n) \supset$$

no se estabiliza. Este ejemplo puede ser generalizado a todo dominio de ideales principales.

[1]Esta situación se suele llamar, la estabilización de la cadena ascendente

3. *Demostremos la generalización sugerida en el punto anterior. Sea R un dominio de ideales principales, y sea*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

Una cadena ascendente de ideales, y considere $I = \bigcup_{n=1}^{\infty} I_n$. Tenemos que I es un ideal ya que si a, b están en I y t en R, existen k, m tal que $a \in I_k$ y $b \in I_m$. Si tomamos $h = \max\{k, m\}$ tenemos que a, b están en I_h y $a + b \in I_h$ y $ta \in I_h$, como $I_h \subset I$ vemos que $a + b \in I$ y $ta \in I$, Por otro lado $I = (r)$ para algún r en R, r esta en algún I_k para algún k en $\mathbb{N}$, de esta manera $I = (r) \subset I_n \subset I$ y por tanto, $I_k = I$, en conclusion $I_n = I$ para todo $n \geq k$.

4. *No todos los anillos noetherianos son dominios principales de ideales, por ejemplo $\mathbb{Z}[x_1, \ldots, x_n]$ es Noetheriano por el teorema de la base de Hilbert [AM73, Capítulo 7, teorema 7.5]. Pero no es un dominio de ideales principales.*

El concepto de anillo noetheriano no es exclusivo de los anillos conmutativos.

Ejemplo. *$M_n(R)$ es noetheriano a izquierda si y solo si R es noetheriano a izquierda. Ya que $M_n(R) \simeq R^{n^2}$ como R-módulo, luego si R es un anillo noetheriano a izquierda lo es como R-módulo, entonces $M_n(R)$ es un R-módulo a izquierda noetheriano. Por otro lado, si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ es una cadena de ideales, entones $M_n(I_1) \subset M_n(I_2) \subset \cdots \subset M_n(I_n) \subset \cdots$ es una cadena de ideales en $M_n(R)$.*

El estudio de ideales en un anillo ha desempeñado un papel histórico en esta teoría, aquí recordamos una definiciones importantes.

Definición 1.15. *Sea R un anillo, I un ideal y $S \subseteq R$*

1. *I es llamado un ideal primo si $I \neq R$ y para cualquier par de ideales A, B de R tales que $AB \subset I$ entonces $A \subset I$ o $B \subset I$*

2. *I es llamado un ideal maximal si $I \neq R$ y para cualquier ideal N tal que $M \subset N \subset R$ se tiene que $N = M$ o $N = R$.*

3. *S es llamado un subconjunto multiplicativamente cerrado si 1 esta en S y para cada a, b en S se tiene que ab esta en S.*

4. *S es llamado un m-sistema si, para cualquier a, b en S existe un r en R tal que arb esta en S.*

También es conocida esta proposición en la que se considera el caso donde el anillo es conmutativo

Teorema 1.16. *Sea R un anillo. Si I es un ideal de R tal que $I \neq R$ y para todo a, b en R tal que $ab \in I$ entonces $a \in I$ o $b \in I$ entonces I es un ideal primo, recíprocamente si I es primo y R es conmutativo, entonces I satisface la condición anterior.*

Demostración. ver [Hun03, Teorema 2.15 capítulo III] □

La conmutatividad es necesaria en esta proposición ya que si consideramos $M_n(\mathbb{K})$ el anillo de matrices cuadradas de $n \times n$ con entradas en un cuerpo $\mathbb{K}$ podemos ver que (0) es un ideal primo. Por otro lado siempre es posible encontrar dos matrices A, B tales que $0 = AB \in (0)$ pero $A \notin (0)$ y $B \notin (0)$. En general el comportamiento de los ideales primos esta dado por la siguiente proposición

Proposición 1.17. *Sea R un anillo y $P \subsetneq R$ un ideal, entonces las siguientes son equivalentes*

1. *P es primo.*
2. *Para a, b en R, $(a)(b) \subseteq P$ implica que $(a) \subseteq P$ o $(b) \subseteq P$.*
3. *Para a, b en R. $aRb \subseteq P$ implica que a o b están en P.*
4. *Para ideales a izquierda I, J de R, $IJ \subseteq P$ implica que $I \subseteq P$ o $J \subseteq P$.*
5. *Para ideales a derecha I, J de R, $IJ \subseteq P$ implica que $I \subseteq P$ o $J \subseteq P$.*

Demostración. Ver [Lam01, Capítulo 10, proposición 10.2] □

Un concepto relacionado con los ideales primos de un anillo, es el radical de un anillo. Para poder introducirlo tenemos que hacer un trabajo previo.

Corolario 1.18. *Sea R un anillo. Un ideal $P \subseteq R$ es primo si y solo si $R - P$ es un m-sistema.*

Proposición 1.19. *Sea $S \subseteq R$ un m-sistema, y P un ideal maximal respecto a la propiedad de que P es disjunto de S. Entonces P es un ideal primo.*

Demostración. Ver [Lam01, Capítulo 10, proposición 10.5] □

Definición 1.20. *Sea R un anillo e I un ideal, sea*

$$\begin{aligned}\sqrt{I} &= \{s \in R \mid \textit{cualquier } m\textit{-sistema } S \textit{ que contiene a } s,\ S \cap I \neq \emptyset\}\\ &\subseteq \{s \in R \mid s^n \in I \textit{ para algún } n \geq 1\}\end{aligned}$$

$\sqrt{I}$ es conocido como el radical del ideal I

En la anterior definición si R es un anillo conmutativo e I un ideal, y supongamos que s^n esta en I. Sea S cualquier m-sistema que contiene a s, así existe r en R tal que $s^n r$ esta en S, pero $S \subset I$ y de este modo $s \in \sqrt{U}$. y por tanto se tiene la igualdad en la definición.

Proposición 1.21. *Sea R un anillo y I un ideal, $\sqrt{I}$ es igual a la intersección de todos los ideales primos que contienen a I. En particular $\sqrt{I}$ es un ideal en R*

Demostración. Ver [Lam01, Capítulo 10, proposición 10.5] □

Definición 1.22. *Sea R un anillo,*

1. *La intersección de todos los ideales maximales a izquierda de R es llamada el radical de Jacobson y es denotada por rad R.*

2. *Si R es un anillo conmutativo, entonces el nilradical de un anillo R es $\sqrt{(0)}$ y lo denotamos por $Nil(R)$.*

El estudio del radical de Jacobson nos permite definir una nueva clase de anillos denominada anillos locales.

Proposición 1.23. *Sea R un anillo, las siguientes condiciones son equivalentes:*

1. *R tiene un único ideal maximal a izquierda.*

2. *R tiene un único ideal maximal a derecha.*

3. *$R/rad\ R$ es un anillo de división.*

4. *$R - U(R)$ es un ideal de R.*

5. *$R - U(R)$ es un grupo bajo la adición.*

6. *Para cualquier n en $\mathbb{N}$, $a_1 + a_2 + a_3 + \ldots + a_n$ esta en $U(R)$ entonces existe un i, $1 \leq i \leq n$ tal que a_i esta en $U(R)$*

7. *$a + b$ esta en $U(R)$ implica que a esta en $U(R)$ o b esta en $U(R)$*

Demostración. Ver [Lam01, Capítulo 19,teorema 19.1] □

Ejemplos (Anillos locales)**.**

1. *Sea p un número primo, entonces $\mathbb{Z}/p^n\mathbb{Z}$ es un anillo local, para todo $n > 1$*

2. *Sea (f) un ideal maximal en $\mathbb{K}[x]$ donde $\mathbb{K}$ es un cuerpo, entonces $\mathbb{K}[x]/(f^n)$ es un anillo local para todo $n > 1$.*

3. *El anillo de series formales $\mathbb{K}[[x]]$ donde $\mathbb{K}$ es un cuerpo.*

4. *Sea p un número primo, el anillo $\mathbb{Z}_p = \mathbb{Z}[[x]]/(x - p)$ es un anillo local y se denomina anillo de enteros p-ádicos*

Una construcción que nos permitirá construir más ejemplos es la de localización de un anillo, en el presente trabajo solo se utilizará sobre anillos conmutativos.

Teorema 1.24. *Sea R un anillo conmutativo y S un conjunto multiplicativo*

1. *La relación definida sobre $R \times S$ por*

$$(r, s) \sim (m, t) \text{ si y solo si existe } u \text{ en } S \text{ tal que } u(rt - sm) = 0$$

es una relación de equivalencia.

2. *Sea $S^{-1}R$ el conjunto de todas las clases de equivalencia de la relación anterior. Entonces $S^{-1}R$ es un anillo conmutativo.*

3. *Si R es un dominio y 0 no esta en S, entonces $S^{-1}R$ es un dominio.*

4. *Si R es un dominio y $S = R - \{0\}$ entonces $S^{-1}R$ es un cuerpo conocido como el cuerpo de fracciones de R.*

Demostración. Ver [Hun03, Capítulo III, Teorema 4.3] □

Sea R un anillo conmutativo y P un ideal primo de R, entonces $S = R - P$ es un conjunto multiplicativo, ya que si x, y están en S, entonces x, y no están en P por tanto xy tampoco esta en P y por tanto xy esta en S. Esto motiva la siguiente definición.

Definición 1.25. *Sea R un anillo conmutativo y P un ideal primo de R, definimos la localización de R en P como*

$$R_P = S^{-1}R$$

donde $S = R - P$.

El siguiente teorema nos permite construir diferentes dominios de ideales principales a partir de uno dado.

Teorema 1.26. *Sea R un dominio de ideales principales y K su cuerpo de fracciones*

1. *Si D es un subanillo de K, tal que $R \subseteq D \subseteq K$, entonces D es una localización de R y también es un dominio de ideales principales.*

2. *Suponga además que R es un anillo local. Entonces los únicos subanillos intermedios $R \subseteq D \subseteq K$ son $D = R$ o $D = K$.*

Demostración. 1. Sea $R \subseteq D \subseteq K$, y $T = \{r \in R : \frac{1}{r} \in D\}$. Veamos que $D = T^{-1}R$. Dado $z \in D$, tomemos elementos coprimos a, b en R tales que $z = a/b$. Como R es un dominio de ideales principales, existen x, y en R tal que $ax + by = 1$, entonces en K

$$\frac{a}{b}x + y = \frac{1}{b}.$$

Como a/b, x e y están en D se obtiene que $1/b \in D$. Ya que $b \in R$ se concluye que $b \in T$. De este modo, $1/b \in T^{-1}$ y $a/b = a \cdot 1/b \in T^{-1}R$. Luego $D \subseteq T^{-1}R$. Por otra parte, supongamos que $c \in T^{-1}R$. Entonces existe a en R y b en T tales que $c = a \cdot 1/b \in D$. Como se tiene que si $b \in T$ entonces $1/b \in D$ y $a \in R \subset D$, entonces $a \cdot 1/b$ esta en D y de esta manera $T^{-1}R \subseteq D$ y por lo tanto $D = T^{-1}R$. Ahora veamos que D es un dominio de ideales principales. Sea J un ideal de $T^{-1}R$, entonces existe un ideal I en R tal que $J = IT^{-1}R$, pero $I = (r)$ para algún r en R. Sea j en J luego $j = kr\frac{a}{b}$ donde kr esta en I y a/b en $T^{-1}R$, luego $j \in (r)$ donde (r) es considerado como un ideal en $T^{-1}R$, por lo tanto $J \subseteq (r)$ en $T^{-1}R$. Por otro lado, sea $j \in (r)$ entonces $j = \frac{a}{b}r$ donde a/b esta en $T^{-1}R$ y r en I, luego j pertenece a $IT^{-1}R = J$ y $(r) \subseteq J$. De este modo, $(r) = J$, es decir, todo ideal es principal.

2. Ejercicio para el lector. Ver [Hun03, capítulo 3, teorema 4.4]

□

El teorema anterior nos proporciona una forma de construir dominios de ideales principales a partir de uno conocido, por ejemplo si $\mathbb{K}[X]$ el anillo de polinomios sobre un cuerpo, sabemos que es un dominio de ideales principales, luego si realizamos la localización respecto al conjunto multiplicativo $T = \{X^i : i \in \mathbb{N}\}$ tenemos que $S^{-1}\mathbb{K}[X]$ es un dominio de ideales principales. Este anillo es el anillo de polinomios de Laurent .

1.1.1 Módulos libres y proyectivos

En el presente trabajo estamos principalmente interesados en módulos libres y proyectivos, las siguientes proposiciones los describen.

Definición 1.27. *Sea R un anillo y T un conjunto, denotamos por $R^{(T)}$ la suma directa externa de una familia $(M_t)_{t\in T}$ de R-módulo a izquierda tal que $M_t = R$ es un R-módulo a izquierda para todo t en T*

Usando la notación de la definición anterior

Definición 1.28. *Sea $(a_t)_{t\in T}$ una familia de elementos de un R-módulo a izquierda E y considere la aplicación $u : R^{(T)} \to E$ dada por $u(f) = \sum_{t\in T} f(t)a_t$*

- *Decimos que $((a_t)_{t\in T})$ es una familia libre si u es inyectiva.*
- *Decimos que $((a_t)_{t\in T})$ es una base de E si u es biyectiva.*

Los módulos libres pueden ser caracterizados de varias formas, la siguiente proposición nos indica algunas.

Proposición 1.29. *Para cada R-módulo F, las siguientes condiciones son equivalentes:*

1. *F posee una base no vacía.*
2. *F es suma directa interna de una familia de módulos cíclicos sobre R, cada uno de los cuales es isomorfo como R-modulo a R.*
3. *F es isomorfo a una suma directa de copias del R-módulo R.*
4. *Existe un conjunto no vacío X y una función $i : X \to F$ con la siguiente propiedad: dado un R-módulo A y una función $f : X \to A$, existe un único homomorfismo de R-módulos $\bar{f} : F \to A$ tal que $\bar{f} \circ i = f$.*

Decimos que F es un módulo libre si satisface cualquiera de las condiciones anteriores.

Demostración. Ver [Hun03, capítulo IV, teorema 2.1] □

Además, los módulos proyectivos también tienen un papel importante en la K teoría algebraica como se mostrará más adelante, en este punto solo introduciremos sus propiedades básicas.

Definición 1.30. *Sea P un R-módulo a izquierda, decimos que P es módulo proyectivo si para cada homomorfismo sobreyectivo f y cada homomorfismo g, existe un homomorfismo h tal que el siguiente diagrama conmuta.*

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

De forma análoga a los módulos libres, los módulos proyectivos satisfacen las siguientes propiedades.

Proposición 1.31. *Sea R un anillo, las siguientes condiciones son equivalentes*

1. *P es un R-módulo proyectivo.*
2. *Cualquier sucesión exacta corta $0 \to A \to B \to P \to 0$ se descompone ($B \simeq A \oplus P$)*
3. *P es sumando directo de un modulo libre, es decir, existe Q en R-módulo a izquierda y F un R-módulo libre tales que $P \oplus Q \simeq F$*

Además, si P es un R-módulo proyectivo finitamente generado tenemos que P es un sumando directo de R^n para algún $n \in \mathbb{N}$

Demostración. Ver [Hun03] □

Una consecuencia de la proposición anterior, es que todo módulo libre es proyectivo. Pero en general, el recíproco no se tiene. Por ejemplo $P = \mathbb{Z}/2\mathbb{Z} \oplus (0)$ un submódulo proyectivo no libre de $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Por otro lado, no siempre el producto tensorial de dos módulos proyectivos es proyectivo. Sin embargo vale el siguiente resultado.

Proposición 1.32. *Sea R un anillo conmutativo. Si P, Q son R-módulos proyectivos finitamente generados, entonces $P \otimes Q$ es un R-modulo proyectivo finitamente generado.*

Demostración. Como P y Q son R-módulos proyectivos finitamente generados tenemos que existen R-módulos S, T y n, m en $\mathbb{N}$ tal que $P \oplus S \simeq R^n$ y $Q \oplus T \simeq R^m$, de este modo,

$$\begin{aligned} R^{nm} &\simeq R^n \otimes R^m \\ &\simeq (P \oplus S) \otimes (Q \oplus T) \\ &\simeq (P \otimes Q) \oplus [(P \otimes T) \oplus (Q \otimes S) \oplus (S \otimes T)] \\ &\simeq (P \otimes Q) \oplus K \end{aligned}$$

Luego $(P \otimes Q)$ es un sumando directo de R^{nm} y por tanto es un R-módulo proyectivo finitamente generado. □

Una proposición que será de importancia en el futuro es

Teorema 1.33 (Lema de Nakayama)**.** *Sea R un anillo entonces para cualquier ideal a izquierda J de R, las siguientes afirmaciones son equivalentes*

1. *$J \subset$ rad R.*
2. *Para cualquier R-módulo a izquierda M, si $JM = M$ entonces $M = 0$.*
3. *Para cualquier par de R-módulos a izquierda M y N tales que M/N es un R-módulo a izquierda, si $N + JM = M$ entonces $M = N$.*

Demostración. Ver [Lam01, Capítulo 2, teorema 4.22] □

Veamos la siguiente aplicación del lema anterior

Proposición 1.34. *Sea I un ideal radical en un anillo R. Para cada par de R-módulos P_1 y P_2, proyectivos finitamente generados tal que $P_1/IP_1 \simeq P_2/IP_2$ como R-módulos a izquierda, se tiene que $P_1 \simeq P_2$.*

Demostración. Denotemos por $\phi : P_1/IP_1 \to P_2/IP_2$ el isomorfismo entre P_1/IP_1 y P_2/IP_2 y consideremos el siguiente diagrama

$$\begin{tikzcd} & P \arrow[d, "\pi"] \arrow[ddl, "f"'] & \\ & P/IP \arrow[d, "\phi"] & \\ Q \arrow[r, "\pi"] & Q/IQ \arrow[r] & 0 \end{tikzcd}$$

donde π es el epimorfismo canónico. Como P es un R-módulo proyectivo finitamente generado, existe f tal que el diagrama es conmutativo. Si $q \in Q$ entonces $q + IQ = \phi(p + IP) = f(p) + IQ$ para algún p en P, y por tanto, $Q = f(P) + IQ$. Por el lema de Nakayama tenemos que $Q = f(P)$, de esta manera f es sobreyectiva. Si $K = \ker f$, tenemos la siguiente sucesión exacta corta

$$0 \longrightarrow K \xrightarrow{i} P \xrightarrow{f} Q \longrightarrow 0 \tag{1.1}$$

La cual se descompone porque Q es un R-módulo proyectivo finitamente generado (ver 1.31), luego

$$0 \longrightarrow K/IK \xrightarrow{\bar{i}} P/IP \xrightarrow{\varphi} Q/IQ \longrightarrow 0$$

es exacta. Como ϕ es un monomorfismo, $IK = K$. Dado que 1.1 se descompone, K es una imagen homomorfa de P y por tanto, es un R-módulo proyectivo finitamente generado y aplicando el lema de Nakayama $K = 0$ y por tanto f es un isomorfismo. □

Definición 1.35. *Sea P y Q dos R-módulos, decimos que son establemente isomorfos si existe un $n \in \mathbb{N}$ tal que $P \oplus R^n \cong Q \oplus R^n$*

Definición 1.36. *Sea R un anillo, decimos que R posee número de base invariante (NBI) si $R^n \simeq R^m$ como R-módulos a izquierda implica que $m = n$.*

Ejemplo. *Sea $\mathbb{K}$ un cuerpo, si $\mathbb{K}^n \simeq \mathbb{K}^m$ como $\mathbb{K}$-módulos, entonces $n = m$ ya que este es un isomorfismo de espacios vectoriales de dimension finita.*

El concepto de NBI también admite la siguiente interpretación, $R^n \simeq R^m$ si y solo si no existen matrices A en $M_{m\times n}(R)$ y B en $M_{n\times m}(R)$, $n \neq m$ con $AB = I_m$ y $BA = I_n$.

La siguiente proposición nos dará una gran cantidad de ejemplos

Proposición 1.37. *Sean R y S un anillo*

1. *Si R tiene NBI, entonces el anillo opuesto R^{op} tiene NBI.*
2. *Si R tiene NBI entonces $M_n(R)$ también tiene NBI para todo $n \geq 1$.*
3. *Sea $f : S \to R$ un homomorfismo de anillos y R tiene NBI, entonces S también tiene NBI*
4. *Si R es conmutativo entonces tiene NBI.*
5. *Cualquier anillo Noetheriano a izquierda tiene NBI.*

Demostración. Ver [Mag10, Capítulo 1, teorema 1.39] □

También es conveniente introducir el concepto de álgebra sobre un anillo, ya que esta relacionado con el de anillos de grupo.

Definición 1.38. *Sea A un anillo, A es llamado una álgebra sobre un anillo conmutativo R o una R-álgebra, si existe un homomorfismo de anillos $\varphi : R \to Z(A)$ donde $Z(A)$ es el centro de A.*

Ejemplo.
1. *Cualquier anillo es una $\mathbb{Z}$-álgebra*
2. *Si R es un anillo conmutativo, entonces $R[x_1, \ldots, x_n]$ y $M_n(R)$ son R-álgebras*
3. *Si R es un anillo conmutativo y G es un grupo, entonces RG el anillo de grupo es llamado el álgebra de grupo.*

1.1.2 Módulos y anillos semisimples

Un aspecto importante que diferencia el algebra conmutativa de la no conmutativa son los anillos y módulos semisimples. Además veremos que este concepto será de mucha utilidad a la hora de estudiar los anillos de grupo.

Definición 1.39. *Sea M un R-módulo a izquierda*

1. *M es simple si $M \neq 0$ y M no posee submódulos diferentes a (0) y M.*
2. *M es semisimple si cualquier submódulo de M es un sumando directo de M*

Los módulos semisimples sobre R poseen una clasificación dada por la siguiente proposición.

Proposición 1.40. *Sea M un R-módulo, entonces las siguientes afirmaciones son equivalentes:*

1. *M es semisimple*
2. *M es la suma directa de una familia de submódulos simples*
3. *M es la suma de una familia de módulos simples.*

Demostración. Ver [Lam01, Capítulo 1, teorema 2.4] □

El concepto de módulo semisimple también se puede extender a los anillos de la siguiente forma

Proposición 1.41. *Sea R un anillo, las siguientes afirmaciones son equivalentes:*

1. *Todas las sucesiones exactas cortas de R-módulo a izquierda se descomponen.*
2. *Para cada R-módulo a izquierda M es semisimple.*
3. *Para cada R-módulo a izquierda M finitamente generado es semisimple.*
4. *Para cada R-módulo a izquierda M cíclico es semisimple.*
5. *el R-módulo a izquierda R es semisimple.*

Si alguna de estas condiciones se tiene, se dice que R es semisimple a izquierda

Demostración. Ver [Lam01, Capítulo 1, teorema 2.5] □

Como consecuencia de esta proposición tenemos que

Corolario 1.42. *Sea R un anillo y semisimple a izquierda, entonces R es noetheriano y artiniano a izquierda simultáneamente.*

Los anillos semisimples a izquierda también poseen una caracterización

Proposición 1.43. *Sea R un anillo, las siguientes afirmaciones son equivalentes:*

1. *R es un anillo semisimple a izquierda*
2. *Para cada R-modulo M se tiene que es proyectivo.*
3. *Para cada R-modulo finitamente generado M se tiene que es proyectivo.*
4. *Para cada R-módulo M cíclico se tiene que M es un R-módulo proyectivo.*

Demostración. Ver [Lam01, Capítulo 1, teorema 2.8] □

Proposición 1.44 (Lema de Schur)**.** *Sea R un anillo y V un R-módulo a izquierda simple. Entonces $End_R(V)$ es un anillo de division*

Demostración. Sea $f \neq 0$ en $\mathrm{End}_R(V)$, entonces $\ker(f) \neq 0$ y $\mathrm{im}(f) \neq 0$, como $\ker(f)$ y $\mathrm{im}(f)$ son submódulos propios de V, tenemos que $\mathrm{im}(f) = V$ y $\ker(f) = \{0\}$ y por tanto f es invertible en $\mathrm{End}_R(V)$ □

Una fuente de ejemplos nos la proporciona la siguiente proposición

Proposición 1.45. *Sea D un anillo de division y sea $R = M_n(D)$. Entonces*

1. *R es simple, semisimple a izquierda, Noetheriano y Artiniano a izquierda.*
2. *R posee un único (salvo isomorfismos) R-módulo a izquierda simple denotado por V. R actúa fielmente sobre V y $R \simeq \bigoplus_{i=1}^{n} V$ en R-módulo a izquierda.*
3. *El anillo $\mathrm{End}_R(V)$, visto como un anillo operadores a derecha sobre V, es isomorfo a D.*

Demostración. Ver [Lam01, Capítulo 1, teorema 3.3] □

Los anillos semisimples satisfacen ciertas propiedades, una de ellas es la siguiente

Proposición 1.46. *Sea $R_1, \ldots, R_m$ un anillo, donde R_i es semisimple a izquierda para cada $i = 1, 2, \ldots, m$, entonces $R_1 \times R_2 \times R_3 \times \cdots \times R_m$ es semisimple a izquierda*

Demostración. Ver [Lam01, Capítulo 1, teorema 3.4] □

De esta manera llegamos al objetivo de esta sección que es clasificar todos los anillos semisimples.

Teorema 1.47 (Teorema de Wedderburn-Artin)**.** *Sea R un anillo semisimple a izquierda, entonces*

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times M_{n_3}(D_3) \times \cdots \times M_{n_r}(D_r)$$

Donde $D_1, \ldots, D_r$ son anillos de division, y $n_1, n_2, \ldots, n_r$ son enteros positivos. El número r es únicamente determinado, como las parejas $(n_1, D_1), \ldots, (n_r, D_r)$ (salvo permutación).

Demostración. Ver [Lam01, Capítulo 1, teorema 3.5] □

1.1.3 Cambio de anillos de escalares

Existen varias formas de introducir este concepto, la primera referencia en la que este tema es tratado sistemáticamente es [Bou70, Capítulo 2, No 13, A31]. La que daremos a continuación es una version usando el lenguaje de las categorías desarrollado en el apéndice A, tomada de [BK00].

1.1.3.1 Restricción de escalares

Sea $f : R \to S$ un homomorfismo de anillos y M un S-módulo, si r es un elemento de R definimos

$$r \cdot m = f(r)m$$

Es claro que esta nueva operación induce una estructura de módulo para M, y de esta manera, podemos considerar que M es un R-módulo a izquierda, el cual denotaremos por $f^\star M$. Por otro lado, si $\alpha : M \to N$ es un homomorfismo de módulos, entonces induce un homomorfismo

$$f^\star\alpha : f^\star M \to f^\star N.$$

Como resultado, hemos definido un funtor aditivo entre $f^\star : S - \mathbf{Mod} \to R - \mathbf{Mod}$. Este es denominado la restricción de escalares.

Proposición 1.48. *Sean R, S, T anillos*

1. *Si $id_R : R \to R$ es el homomorfismo identidad de R, entonces $(id_R)^\star$ es el funtor identidad $Id_R : R - \mathbf{Mod} \to R - \mathbf{Mod}$.*

2. *Dado los homomorfismos de anillos $f : R \to S$ y $g : S \to T$, existe un isomorfismo natural entre los funtores $(gf)^\star$ y $f^\star g^\star = (gf)^\star$.*

En el caso donde $f : R \to S$ sea la inclusion y por consiguiente R es un subanillo de S, decimos que $f^\star M$ es obtenido por restricción a R del anillo de escalares S. Es claro que toda familia $(M_i)_{i\in\lambda}$ en $S - \mathbf{Mod}$, se tiene que

$$f^\star\left(\prod_{i\in\lambda} M_i\right) = \prod_{i\in\lambda} f^\star M_i,$$
$$f^\star\left(\bigoplus_{i\in\lambda} M_i\right) = \bigoplus_{i\in\lambda} f^\star M_i.$$

Asimismo, todo sistema de generadores de $\rho_*(E)$ es un sistema de generadores de E. Por otro lado, dado el homomorfismo de anillos $f : R \to S$, el funtor inducido $f^\star$ tiene un comportamiento particular en cada subcategoría de $S - \mathbf{Mod}$

Proposición 1.49. *Sean R, S anillos y $f : R \to S$*

1. *El funtor $f^\star$ induce un funtor*

$$f^\star : S - \mathbf{Pmod} \to R - \mathbf{Pmod}$$

   si y solo si, $f^\star S$ esta en $R - \mathbf{Pmod}$.

2. *El funtor $f^\star$ induce un funtor*

$$f^\star : S - \mathbf{mod} \to R - \mathbf{mod}$$

   si y solo si, $f^\star S$ esta en R-módulo a izquierda.

Demostración. Teniendo en cuenta que $R-\mathbf{Pmod}$ y $R-\mathbf{Mod}$ son categorías plenas, solo es necesario verificar la acción de $f^\star$ sobre los módulos.

1. Supongamos primero que $f^\star S$ es un R-módulo proyectivo. Si M es un S-módulo proyectivo entonces M es un sumando directo de un módulo libre F, es decir, $M \oplus N \simeq F$, en particular $M \oplus N \simeq R^{(I)}$ para algún conjunto I, pero $f^\star M \oplus f^\star M \simeq (f^\star R)^{(I)}$, entonces tenemos que $f^\star M$ es un R-módulo proyectivo. El otro sentido se tiene por el hecho de que S es un S-módulo proyectivo.

2. Si M es un S-módulo finitamente generado, sea $\{m_1, \ldots, m_k\}$ su conjunto de generadores y supongamos que S tiene como conjunto de generadores a $\{s_1, \ldots, s_t\}$ como R-módulo. Entonces el conjunto de todos los productos $\{s_i m_j | 1 \leq i \leq k, 1 \leq j \leq t\}$ es finito y es el conjunto de generadores para $f^\star M$.

□

1.1.3.2 Extension de escalares

Sea $f : R \to S$ un homomorfismo de anillos, podemos considerar a S como un R-módulo usando la regla $r \cdot s = f(r)s$, de esta forma S puede ser considerado un $R-S$-bimódulo.

$$f_\star = - \otimes_R S = R - \mathbf{Mod} \to S - \mathbf{Mod}.$$

De esta forma, $f_\star(M) = M \otimes_R S$. Adicionalmente, si $\alpha : M \to N$ es un homomorfismo de módulos, entonces

$$f_\star(\alpha) = \alpha \otimes id_S : f_\star(M) \to f_\star(N)$$

lo cual nos lleva a la siguiente proposición

Proposición 1.50. *Sean R, S, T anillos*

1. *Si $id_R : R \to R$ es el homomorfismo identidad de R, entonces $(id_R)_\star$ es el funtor identidad.*

2. *Dado los homomorfismos de anillos $f : R \to S$ y $g : S \to T$, existe un isomorfismos natural entre los funtores $(gf)_\star$ y $f_\star g_\star$.*

Es de nuestro interés saber el comportamiento de este funtor en la categoría $R-\mathbf{Pmod}$. Eso esta resumido en la siguiente proposición

Proposición 1.51. *Sean R, S anillos y $f : R \to S$ un homomorfismo de anillos*

1. *Para cualquier conjunto T, $f_\star(N^{(T)}) = S^{(T)}$*

2. *$f_\star$ induce un funtor*
$$f_\star : R - \mathbf{Pmod} \to S - \mathbf{Pmod}$$

Demostración. Ver [BK00, Cápitulo 3, Teorema 3.3.7] □

1.1.4 Límites directos

En este apartado daremos la definición de una nueva construcción, el límite directo (o inductivo). Esta operación tiene importancia no solo en la K teoría algebraica sino en teoría algebraica de números y en topología.

El concepto de límites directos e inversos admite una generación en teoría de categorías, pero en nuestro caso, no la necesitamos, solo expondremos el caso particular en las categorías de R-módulos a izquierda, anillos y grupos.

Definición 1.52. *Sea I un conjunto y $\leq$ una relación tal que*

1. *$x \leq x$ para todo x en I.*

2. *Si $x \leq y$ e $y \leq z$ entonces $x \leq z$.*

3. *Si x, y están en I entonces existe z en I tal que $x \leq z$ y $y \leq z$.*

entonces decimos que $(I, \leq)$ es un conjunto dirigido

En el presente trabajo solo usaremos a $(\mathbb{N}, \leq)$ y $(\mathbb{N}, |)$ donde $\leq$ es la relación de orden usual de los números naturales y $|$ es la relación de divisibilidad de los números naturales ($a|b$ si existe un $c \in \mathbb{N}$ tal que $b = ac$).

Definición 1.53. *Sea $(I, \leq)$ un conjunto dirigido, Considere*

$$\{(M_i, \phi_{ij}) : i, j \in I\}$$

donde cada M_i es un R-módulo (o un anillo o un grupo) y $\phi_{ij} : M_i \to M_j$ un homomorfismo de R-módulos (de anillos o grupos) sujetos a las siguientes condiciones

1. *ϕ_{ij} esta definido siempre que $i \leq j$.*

2. *ϕ_{ii} es la identidad en M_i.*

3. *Si $i \leq j$ y $j \leq k$ entonces $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$, gráficamente*

$$\begin{tikzcd} M_i \arrow[r, "\varphi_{ij}"] \arrow[rr, bend right, "\varphi_{ik}"'] & M_j \arrow[r, "\varphi_{jk}"] & M_k \end{tikzcd}$$

entonces decimos que $\{M_i, \phi_{ij} : i, j \in I\}$ es un sistema dirigido de R-módulos a izquierda (de anillos o de grupos).

Este concepto admite una generalización cambiando los elementos M_i por objetos en una categoría $\mathcal{C}$ (ver A), como **Abe**, **Conj** o **Top** pero en este trabajo solo se estudiará esta construcción en R-módulos, anillos o grupos.

Proposición 1.54. *Sea $\{M_i, \phi_{ij} : i, j \in I\}$ un sistema dirigido de R-módulos a izquierda y considere la union disjunta $\sqcup_{i\in I}(M_i, i)$, definimos sobre este conjunto la relación de equivalencia $\backsim$ dada por $(m_i, i) \backsim (m_j, j)$ si y solo $\phi_{ik}(m_i) = \phi_{jk}(m_j)$ para algún k en I tal que $i \leq k$ y $j \leq k$. Entonces*

$$\left(\bigsqcup_{i\in I}(M_i, i)\right) / \backsim$$

es un R-módulo a izquierda.

Demostración. Veamos que $\backsim$ es una relación de equivalencia

- $(m_i, i) \backsim (m_i, i)$, ya que $\phi_{ii}(m_i) = m_i$.
- Si $(m_i, i) \backsim (m_j, j)$ entonces existe un k en I tal que $\phi_{ik}(m_i) = \phi_{jk}(m_j)$ y $i \leq k$ y $j \leq k$, pero esto es equivalente a afirmar que $(m_j, j) \backsim (m_i, i)$.
- Si $(m_i, i) \backsim (m_j, j)$ y $(m_j, j) \backsim (m_k, k)$ entonces existen s, t en I tal que $\phi_{is}(m_i) = \phi_{js}(m_j)$, $\phi_{jt}(m_i) = \phi_{kt}(m_k)$ y $i \leq s$, $j \leq s$, $j \leq t$ y $k \leq t$. Como $(I, \leq)$ es un conjunto dirigido, existe un v en I tal que $s \leq v$ y $t \leq v$, de este modo $\phi_{iv}(m_i) = \phi_{sv}(\phi_{jt}(m_i)) = \phi_{tv}(\phi_{jt}(m_j)) = \phi_{tv}(\phi_{kt}(m_k)) = \phi_{kv}(m_k)$. con $i \leq v$ y $k \leq v$, de este modo, $(m_i, i) \backsim (m_k, k)$.

Ahora debemos definir las operaciones sobre $(\sqcup_{i\in I}(M_i, i))/\backsim$ notaremos la clase de equivalencia $[(m_i, i)]$ como $[m_i]$, si tomamos a m_i en M_i y m_j en M_j escogemos algún k tal que $i \leq k$ y $j \leq k$ y entonces definimos

$$\begin{aligned} [m_i] + [m_j] &= [\phi_{ik}(m_i) + \phi_{jk}(m_j)] \\ r[m_i] &= [(rm_i)] \end{aligned}$$

Debemos verificar que estas operaciones están bien definidas. En este punto solo lo haremos para la suma. Si $[m_i] = [m_s]$ y $[m_j] = [m_t]$. Tenemos que

- Como $(m_i, i) \backsim (m_s, s)$ entonces existe un u en I tal que $\phi_{iu}(m_i) = \phi_{su}(m_u)$ y $i \leq u$ y $s \leq u$.
- Como $(m_j, j) \backsim (m_t, t)$ entonces existe un v en I tal que $\phi_{jv}(m_i) = \phi_{tv}(m_t)$ y $i \leq v$ y $s \leq v$.

Por tanto existe un k tal que $u \leq k$ y $v \leq k$, tal que existe k tal que $i \leq k$ y $j \leq k$, esta información puede ser codificada en el siguiente diagrama

$$\begin{tikzcd}
& & & M_k & & & \\
& M_u \arrow[urr, "\phi_{uk}"] & & & & M_v \arrow[ull, "\phi_{vk}"'] & \\
M_i \arrow[ur, "\phi_{iu}"] & & M_s \arrow[ul, "\phi_{su}"'] & & M_j \arrow[ur, "\phi_{jv}"'] & & M_t \arrow[ul, "\phi_{tv}"']
\end{tikzcd}$$

De este modo, $\phi_{ik} = \phi_{uk} \circ \phi_{iu}$ y $\phi_{jk} = \phi_{vk} \circ \phi_{jv}$

$$\begin{aligned}
[m_i] + [m_j] &= [\phi_{ik}(m_i) + \phi_{jk}(m_j)] \\
&= [\phi_{uk}(\phi_{iu}(m_i)) + \phi_{vk}(\phi_{jv}(m_j))] \\
&= [\phi_{uk}(\phi_{su}(m_s)) + \phi_{vk}(\phi_{tv}(m_t))] \\
&= [\phi_{sk}(m_s) + \phi_{tk}(m_t)] \\
&= [m_s] + [m_t]
\end{aligned}$$

Así que la suma esta bien definida. Una cuenta similar prueba que también lo está el producto por escalar y que

$$\left(\bigsqcup_{i\in I}(M_i, i)\right) / \backsim$$

es un R-módulo a izquierda $\square$

Esta proposición motiva la siguiente definición

Definición 1.55. *Sea $\{M_i, \phi_{ij} : i, j \in I\}$ un sistema dirigido de R-módulos, entonces el limite directo de este sistema es:*

$$\varinjlim M_i = \left(\bigsqcup_{i\in I}(M_i, i)\right) / \backsim$$

En la proposición que sigue, cuya prueba dejamos al lector, establecemos la propiedad universal del limite directo de R-módulos.

Proposición 1.56. *Sea $\{M_i, \varphi_{ij} : i, j \in I\}$ un sistema dirigido de R-módulos, $M = \varinjlim M_i$ su limite directo y definimos $\varphi_i : M_i \to M$ dado por $\varphi_i(m_i) = [m_i]$ para cada $i \in I$, entonces*

1. *Si $i \leq j$, entonces el diagrama*

$$\begin{tikzcd}
M_i \arrow[r, "\varphi_i"] \arrow[d, "\varphi_{ij}"] & M \\
M_j \arrow[ur, "\varphi_j"'] &
\end{tikzcd}$$

es conmutativo, es decir, $\varphi_j \circ \varphi_{ij} = \varphi_i$.

2. *Sea N un R-módulo a izquierda y $\{\chi_i | i \in I\}$ cualquier colección de homomorfismos $\chi_i : M_i \to N$ tales que $\chi_j \circ \varphi_{ij} = \chi_i$ con $i \leq j$. Entonces existe un único homomorfismo $\chi : M \to N$ y $\chi\varphi_i = \chi_i$, es decir, el siguiente diagrama*

$$\begin{tikzcd}
M_i \arrow[r, "\varphi_i"] \arrow[d, "\varphi_{ij}"] \arrow[rr, bend left, "\chi_i"] & M \arrow[r, "\chi"] & D \\
M_j \arrow[ur, "\varphi_j"'] \arrow[urr, bend right, "\chi_j"'] & &
\end{tikzcd}$$

es conmutativo.

Demostración. Ejercicio al lector. □

Antes de pasar a los ejemplos daremos unas proposiciones que facilitara los cálculos.

Proposición 1.57. *Sea $\{M_i, \phi_{ij} : i, j \in I\}$ un sistema dirigido de R-módulos y suponga que ϕ_{ij} es un monomorfismo para todo $i, j \in I$ con $i \leq j$. Entonces*

$$\varinjlim M_i = \bigcup_{i \in I} \varphi_i(M_i)$$

Demostración. Ver [Bou70] □

Veamos unos ejemplos que desarrollaremos a lo largo del presente documento.

Ejemplo. *Sea R un anillo*

- *Denotemos por $M_n(R)$ el anillo de matrices cuadradas de orden $n \times n$ con coeficientes en R y los homomorfismos*

$$\begin{aligned} \varphi_{nn+1} : M_n &\to M_{n+1} \\ A &\mapsto \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \end{aligned}$$

donde n esta en $\mathbb{N}$. Es claro que $\varphi_{nn} = Id_{M_n(R)}$ y $\varphi_{mh} \circ \varphi_{nm} = \varphi_{nh}$ para todo m, n, h tal que $n \leq m \leq h$, luego $\{M_i(R), \varphi_{ij} | i, j \in \mathbb{N}\}$ es un sistema dirigido y denotamos su límite directo por

$$M(R) = \varinjlim M_n(R) = \bigcup_{n=1}^{\infty} M_n(R).$$

Si consideramos este límite en la categoría de anillos, $M(R)$ es un anillo sin unidad, ya que si $M(R)$ tiene unidad la cual denotamos por U, existiría un n en $\mathbb{N}$ tal que U es unidad en $M_n(R)$ por 1.57, así $\varphi_{nn+1}(U)$ es una unidad en $M_{n+1}(R)$ lo cual es absurdo.

- *Denotemos por $GL_n(R)$ el grupo de unidades de $M_n(R)$ y los homomorfismos*

$$\begin{aligned} \varphi_{nn+1} : GL_n(R) &\to GL_{n+1}(R) \\ A &\mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

donde n esta en $\mathbb{N}$. Es claro que $\varphi_{nn} = Id_{M_n(R)}$ y $\varphi_{mh} \circ \varphi_{nm} = \varphi_{nh}$ para todo m, n, h tal que $n \leq m \leq h$, luego $\{M_i(R), \varphi_{ij} | i, j \in \mathbb{N}\}$ es un sistema dirigido y denotamos su límite directo en la categoría de grupos.

$$GL(R) = \varinjlim GL_n(R) = \bigcup_{n=1}^{\infty} GL_n(R).$$

- *Análogamente podemos definir*

$$SL(R) = \varinjlim SL_n(R)$$

- *Dado un número primo p, sea $\mathbb{F}_{p^m}$ el cuerpo finito de p^m elementos. Por teoría de Galois (ver [Hun03, capítulo V, corolario 5.6]), sabemos que F_{p^m} es único salvo isomorfismos. Además F_{p^m} es un subcuerpo de F_{p^n} si y solo si $m|n$. Por lo tanto*

$$\{\mathbb{F}_{p^{m!}}, \varphi_{ij}1, j \in (\mathbb{N}, |)\}.$$

donde $\varphi_{ij} : \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{j!}}$ es la inclusion, es un sistema dirigido, y así

$$\varinjlim \mathbb{F}_{p^{n!}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}.$$

Por otro lado, Sea $\overline{\mathbb{F}}_p$ la cerradura algebraica de $\mathbb{F}_p$, es claro que $\varinjlim \mathbb{F}_{p^{n!}} \subseteq \overline{\mathbb{F}}_p$. Además, si $p(x)$ en $\overline{\mathbb{F}}_p[x]$ entonces, existe un k en $\mathbb{N}$ tal que los coeficientes de $p(x)$ están en $\mathbb{F}_{p^k}$. También se sabe que un cuerpo de descomposición para $p(x)$ es una extension finita de $\mathbb{F}_{p^k}$, sea $\mathbb{F}_{p^h}$ dicha extension, como $\mathbb{F}_{p^h} \subseteq \mathbb{F}_{p^{h!}}$, tenemos que $p(x)$ también se descompone en $(\varinjlim \mathbb{F}_{p^{n!}})[x]$. De esta manera $\overline{\mathbb{F}}_p = \varinjlim \mathbb{F}_{p^{n!}}$.

1.2 Grupos

Sea G un grupo, siempre notado multiplicativamente (Salvo los grupos abelianos), el elemento identidad de G será notado por 1 o e dependiendo de la situación. Diremos que dos grupos G y H son isomorfos si existe un homomorfismo biyectivo entre ellos y lo denotaremos por $G \cong H$.

Definición 1.58. *Sea G un grupo y x, y elementos de G*

1. *$[x, y] = xyx^{-1}y^{-1}$ es llamado como el conmutador de x e y.*
2. *El grupo generado $G' = \langle\{[x, y] | x, y \in G\}\rangle$ es llamado el subgrupo de conmutadores de G.*

El subgrupo de conmutadores tiene la siguiente propiedad

Proposición 1.59. *Sea G y H grupos,*

1. *G' es un subgrupo normal de G y G/G' es abeliano*
2. *Si N es un subgrupo normal de G, entonces G/N es abeliano si y solo si $G' \subseteq N$.*
3. *Si $f : G \to H$ es un homomorfismo de grupos, entonces $f(G') \subseteq H'$*

Demostración. Ver [Hun03, Capítulo 2,teorema 7.8] para la prueba de 1 y 2, para probar 3, solo basta observar

$$f([x,y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1}$$

□

Como veremos en próximos capítulos esta proposición tendrá gran importancia. Continuamos con el resumen de propiedades que utilizaremos.

Definición 1.60. *Si H y K son subgrupos y x un elemento de un grupo G, el conjunto*

$$HxK = \{hxk : h \in H, k \in K\}$$

es llamada una (H,K)-clase bilateral

De forma análoga a las clases laterales de un grupo (ver [Hun03, teorema 4.2 y corolario 4.3 capítulo I]) tenemos un resultado para las clases bilaterales.

Teorema 1.61. *Sea H y K subgrupos de un grupo G*

1. *El grupo G es la union de (H,K)-clases bilaterales.*
2. *Dos (H,K)-clases bilaterales son iguales o disjuntas.*
3. *La clase bilateral HxK es una union de clases laterales a izquierda de H y una union de clases laterales a derecha de K.*

Demostración. Definimos $x \sim y$ si y solo si $x = hyk$ para algún h en H y k en K, tenemos que $\sim$ es una relación de equivalencia, luego el teorema es claro. □

Teorema 1.62. *Sea G un grupo abeliano entonces el conjunto $G_t = \{u \in G : |u|$ es finito $\}$ es un subgrupo de G, el cual se denomina subgrupo de torsión de G.*

Demostración. Ver [Hun03, Capítulo II, lemma 2.5] □

Decimos que un grupo abeliano es libre de torsión si $G_t = 0$. La hipótesis de ser abeliano es importante ya que si se considera el caso no conmutativo se pueden presentar casos en el cual G_t no es un grupo, por ejemplo,

1. Para G finito, considere $G = Q_8$ el grupo de los Cuaternios.
2. Para G infinito, considere $G = GL_2(\mathbb{Q})$.

Pese a lo anterior, es posible encontrar grupos no conmutativos libres de torsion, uno de ellos es el grupo discreto de Heisenberg, el cual se expondrá en detalle en el siguiente capítulo.

Siguiendo con los grupos abelianos libres de torsion, estos poseen la siguiente propiedad.

Teorema 1.63. *Un grupo abeliano G es libre de torsion puede ser sumergido en un espacio vectorial sobre $\mathbb{Q}$.*

Demostración. Sea G un grupo abeliano libre de torsion, entonces G es un $\mathbb{Z}$-módulo y considere el conjunto multiplicativo $S = \mathbb{Z}/\{0\}$. Entonces tenemos un homomorfismo de $\mathbb{Z}$-módulos entre G y $S^{-1}G$, dado por $f(x) = x/1$. Como G es libre de torsion, tenemos que G es inyectivo, además tenemos que $S^{-1}G$ es un $S^{-1}\mathbb{Z}$-módulo y $\mathbb{Q} = S^{-1}\mathbb{Z}$. □

Para finalizar, solo cabe recordar los teoremas relacionados a productos libres, en particular la estructura de los subgrupos de un grupo que es un producto libre de grupos.

Definición 1.64. *Sea $\{G_i | i \in I\}$ una familia de grupos. Un producto libre de los A_i es un grupo P y una familia de homomorfismos $j_i : G_i \to P$ tal que, para cada grupo G y cualquier familia de homomorfismos $f_i : G_i \to G$, existe un único homomorfismo $\varphi : P \to H$ tal que $\varphi \circ j_i = f_i$ para cada i en I.*

$$\begin{tikzcd} & P \arrow[d, "\varphi"] \\ G_i \arrow[ur, "j_i"] \arrow[r, "f_i"'] & G \end{tikzcd}$$

Denotaremos a P por $\ast_{i\in I} G_i$. No es difícil probar que el producto libre de grupos us único salvo isomorfismo. Para concluir existe un teorema que caracteriza los subgrupos de un grupo libre.

Teorema 1.65 (Teorema de los subgrupos de Kuroš)**.** *Sea H un subgrupo de un producto libre $\ast_{\lambda\in I} G_i$. Entonces H es un producto libre de la forma*

$$H = H_0 * \mathop{\ast}_{\lambda, d_\lambda} G_i \cap d_\lambda G_\lambda d_\lambda^{-1}$$

donde H_0 es un grupo libre, d_λ varia sobre un conjunto de los representantes de (H, G_λ)-clases bilaterales y λ varia sobre I.

Demostración. Ver [Rob95, Capítulo 6, teorema 6.3.1] o [Ser03, Capítulo 1, teorema 14]. □

Cabe destacar que esta proposición también se encuentra en [Kur60a, Capítulo IX,No. 34], la prueba incluida en esta referencia es de naturaleza combinatoria. Una razón por la que no se incluye la prueba de este teorema es su extensión y el uso de herramientas o construcciones o teorías que no tienen mayor relevancia con el tema que estamos estudiando.

Sin embargo, la prueba incluida en [Ser03, Capítulo 1, teorema 14] usa algunos conceptos expuestos en este documento (en particular, Limites directos) como otros conceptos que no se van a desarrollar en este texto (Árboles, grafos, productos amalgamados, etc.).

1.3 Anillos de grupo

Los anillos de grupos son el tema principal, por eso les vamos a dedicar este espacio y expondremos sus propiedades, así como los módulos sobre estos y la relación que estos guardan con la teoría de representaciones.

Definición 1.66. *Sea R un anillo y G un grupo. El anillo de grupo RG es el R-módulo libre*

$$RG = \bigoplus_{g \in G} Rg$$

con base G, provisto de la multiplicación dada por:

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{xy=g} a_x b_y\right) g.$$

Notemos que:

1. La unidad de RG es $1_R e$ donde 1_R es el elemento identidad de R y e es el elemento identidad de G

2. Podemos identificar los elementos de R en RG mediante la aplicación

$$\begin{aligned} R &\to RG \\ r &\mapsto re, \end{aligned}$$

   donde e es el elemento identidad de G. Claramente este es un homomorfismo de anillos.

3. De manera análoga, podemos identificar los elementos de G en RG mediante la aplicación

$$\begin{aligned} G &\to RG \\ g &\mapsto 1g, \end{aligned}$$

   donde 1 es el elemento identidad de R, de forma análoga, este es un homomorfismo de grupos.

4. Si R es un anillo conmutativo, entonces RG es llamado el álgebra de grupo.

Es claro que los elementos de G y las unidades de R son unidades de RG. Estas son las llamadas *unidades triviales*. De igual forma los divisores de cero y elementos idempotentes de R también los son en RG, estos se denominan *divisores de cero triviales* e *idempotentes triviales* respectivamente.

Existe otra descripción de un anillo de grupo la cual daremos a continuación

Definición 1.67. *Sea R un anillo , G un grupo $f : G \to R$ una función, definimos el soporte de f como*

$$Supp\ (f) = \{g \in G | f(g) \neq 0\}$$

Proposición 1.68. *Sea R un anillo , G un grupo y $\mathcal{F}$ el conjunto de todas las funciones de $f : G \to R$ tal que su soporte es finito, definimos las siguientes operaciones sobre $\mathcal{F}$*

- *(Suma) Si f, h están en $\mathcal{F}$ entonces $(f + h)(g) = f(g) + h(g)$ para todo g en G*
- *(Producto)Si f, h están en $\mathcal{F}$ entonces $(f * h)(g) = \sum_{u \in G} f(u)h(u^{-1}g)$ para todo g en G*

entonces $\mathcal{F}$ dotado con estas operaciones es un anillo e isomorfo a RG.

Demostración. Ver [Pas11, Capítulo 1.] □

Ejemplo. *Consideremos el caso del anillo de grupo $\mathbb{K}G$ donde $\mathbb{K}$ es un cuerpo y $G = \langle \zeta \rangle$ es un grupo cíclico.*

- *Si G es finito, podemos construir un homomorfismo $f : \mathbb{K}[x] \to \mathbb{K}G$ dado por $f(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\zeta + \cdots + a_n\zeta^n$, claramente este homomorfismo es sobreyectivo, además $(1 - x^n)$ es el núcleo de f, entonces $\mathbb{K}[x]/(1 - x^n) \simeq \mathbb{K}G$*
- *Si G es infinito, observamos que $f : \mathbb{K}[x] \to \mathbb{K}G$ pasa a ser un homomorfismo inyectivo, pero si consideramos $\mathbb{K}[x, x^{-1}]$ el anillo de polinomios de Laurent tenemos que $g : \mathbb{K}[x, x^{-1}] \to \mathbb{K}G$ definido por $\sum_{n\in\mathbb{Z}} a_nx^n \mapsto \sum_{n\in\zeta} a_n\zeta^n$, es un isomorfismo ya que $G \simeq \mathbb{Z}$, esto muestra además que $\mathbb{K}G$ es un dominio de ideales principales ya que $\mathbb{K}[x, x^{-1}]$ lo es (ver 1.26).*

Generalizando esta observaciones tenemos.

Proposición 1.69. *Sea G un grupo abeliano libre de torsion finitamente generado y $\mathbb{K}$ un cuerpo. Entonces para algún entero n, $\mathbb{K}G$ puede ser identificado con un anillo que se encuentra entre el anillo de polinomios en n indeterminadas $\mathbb{K}[x_1, \ldots, x_n]$ y su cuerpo de fracciones.*

Demostración. Por el teorema de grupos abelianos finitamente generados, tenemos que $G \simeq \langle\zeta_1\rangle \oplus \langle\zeta_1\rangle \oplus \cdots \oplus \langle\zeta_n\rangle$ donde $\langle\zeta_i\rangle$ es una suma directa de grupos infinitos cíclico para algún n. Tener en cuenta que cualquier elemento de G puede ser identificado de forma única como $\zeta_1^{m_1}\zeta_2^{m_2}\ldots\zeta_n^{m_n}$ para algunos $m_1, \ldots, m_n$ en $\mathbb{Z}$. Construimos la siguiente aplicación de $\mathbb{K}$-módulos $f : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}G$ donde $f(x_i) = \zeta_i$, tenemos que f es inyectiva, de esta forma $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{K}G$, por otro lado, si $\alpha \in \mathbb{K}G$, tenemos que para algún m suficientemente grande $(x_1 \cdots x_n)^m\alpha \in \mathbb{K}[x_1, \ldots, x_n]$, por lo tanto $\mathbb{K}G$ es un dominio de integridad y $\mathbb{K}G \subseteq \mathbb{K}(x_1, \ldots x_n)$. □

Siguiendo con nuestras observaciones, veremos la relación entre homomorfismos de grupos y anillos con los anillos de grupo.

- Sea $f : G \to H$ un homomorfismo de grupos. Este induce un homomorfismo de anillos $Rf : RG \to RH$, dado por

$$Rf\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_{f(g)} f(g)$$

.

- Sea $f : R \to S$ un homomorfismo de anillos. Este induce un homomorfismo de anillos $Gf : RG \to SG$, dado por

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

.

Existe un caso particular de lo expuesto en las observaciones anteriores, que motiva la siguiente definición.

Definición 1.70. *Sea R un anillo y G un grupo. El homomorfismo*

$$\begin{aligned} \epsilon : RG &\to R \\ \sum_{g\in G} a_g g &\mapsto \sum_{g\in G} a_g \end{aligned}$$

es denominado aplicación de aumentación, y el ideal $I_G = \ker(\epsilon)$ es conocido como el ideal de aumentación.

Por otro lado, si consideramos ϵ un homomorfismo de R-módulos, entonces para cada $\alpha \in I_G$.

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

De esta manera, $I_G = \langle\{g-1 | g \in G\}\rangle$ como R-módulo y por tanto es libre sobre R.

Observaciones 1.1. • *Si G es un grupo, R un anillo y H un subgrupo de G, entonces la inclusion $i : H \to G$ induce un homomorfismo $Ri : RH \to RG$, como consecuencia podemos considerar a RG como un RH-módulo.*

- *Si S es un conjunto de representantes de clases laterales a izquierda de H en G, entonces G es union disjunta de las clases laterales Hs con $s \in S$. De este modo,*

$$RG = \bigoplus_{s\in S} RHs.$$

Teniendo en cuenta que $RHs \simeq RH$ como RH-módulo para todo $s \in S$, tenemos que RG es un RH-módulo libre.

- *Suponga que H es un subgrupo normal de G y R es un anillo, consideremos el grupo cociente $\bar{G} = G/H$, entonces la proyección canónica $\pi : G \to G/H = \bar{G}$ induce un homomorfismo de anillos $\pi : RG \to R\bar{G}$. Por otro lado, usando la proposición 1.6 vemos que*

$$R \otimes_{RH} RG = RH/I_H \otimes_{RH} RG \simeq RG/I_H RG \simeq R\bar{G}$$

donde I_H es el ideal de aumentación de $\epsilon : RH \to R$. La identificación se puede ver identificado a $1 \otimes g \in R \otimes_{RH} RG$ con $\bar{g}$ en $R\bar{G}$ para cualquier $g \in G$. Aquí se esta considerando a RG como un RH-módulo.

Proposición 1.71. *Sea R un anillo y G un grupo, entonces RG es conmutativo si y solo si R y G son conmutativos.*

Demostración. Supongamos que RG es conmutativo y como R puede ser identificado como un subanillo de RG se tiene que R es conmutativo, de igual forma para G. Por otro lado si R y G son conmutativos, tenemos que

$$\begin{aligned}\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) &= \sum_{g\in G}\left(\sum_{xy=g} a_x b_y\right) g.\\ &= \sum_{g\in G}\left(\sum_{yx=g} b_y a_x\right) g\\ &= \left(\sum_{g\in G} b_g g\right)\left(\sum_{g\in G} a_g g\right).\end{aligned}$$

De esta manera RG es un anillo conmutativo. ☐

Proposición 1.72. *Sea G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subset A$ y cualquier homomorfismo de monoides $f : G \to (A, \cdot)$. entonces existe un único homomorfismo de anillos $\bar{f} : RG \to A$, tal que el diagrama*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "i"'] & A \\ RG \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

es conmutativo.

Demostración. [MS08]. ☐

En este punto vamos a estudiar los objetos de la categoría $RG - \mathbf{Mod}$ y daremos una aplicación a la teoría de representaciones.

Veamos que si se tiene un módulo sobre un anillo R, este induce un módulo sobre el anillo de grupo RG para algún grupo G fijo.

- Sea M un R-módulo y G un grupo. Definimos MG el conjunto de todas las sumas finitas de la forma
$$\sum_{g\in G} m_g g$$
donde $m_g \in M$,

- Para $\sum_{g\in G} m_g g$, $\sum_{g\in G} n_g g$ en MG, decimos que $\sum_{g\in G} m_g g = \sum_{g\in G} n_g g$ si y solo si $m_g = n_g$ para todo g en G

- Sean $\sum_{g\in G} m_g g$, $\sum_{g\in G} n_g g$ en MG y $\sum_{g\in G} r_g g$ en RG. Definimos la suma y el producto por escalar en MG como
$$\sum_{g\in G} m_g g + \sum_{g\in G} n_g g = \sum_{g\in G} (m_g + n_g) g$$
$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} m_g g\right) = \sum_{g\in G}\left(\sum_{xy=g} r_x m_y\right) g.$$

De esta forma, se observa si se posee un R-módulo entonces siempre es posible construir un RG-módulo para cualquier grupo G dado.

Recuerde que si un R-módulo a izquierda M esta definido sobre un anillo conmutativo R, entonces es posible definir sobre él una estructura de módulo a derecha y viceversa. Ahora vamos a mostrar que esto mismo es cierto para cada módulo sobre un anillo de grupo.

Definición 1.73. *Sea R un anillo y G un grupo, definimos $\tau : RG \to RG$ por*
$$\tau\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g g^{-1}$$
la involución de RG sobre si mismo.

Podemos considerar a τ como un isomorfismo entre RG y $(RG)^{op}$, y en consecuencia no tenemos la necesidad de distinguir entre los RG-módulos a izquierda y derecha: Si M es un RG-módulo a derecha entonces podemos definir un módulo en RG-módulo a izquierda tomando $g \cdot m = mg^{-1}$ para todo g en G y m en M.

Para terminar esta sección, vamos a estudiar las representaciones (lineales) de un grupo.

Definición 1.74. *Sea G un grupo y $\mathbb{K}$ un cuerpo, Una representación de G es un espacio vectorial V sobre $\mathbb{K}$ y un homomorfismo $\rho : G \to Aut(V)$, donde $Aut(V)$ es el grupo de automorfismos de V.*

El estudio de las representaciones de un grupo G tiene un vínculo con los módulos sobre $\mathbb{K}G$.

Si $(V, +, \cdot)$ es un $\mathbb{K}G$-módulo y g, h están G, v, w en V y c en $\mathbb{K}$, entonces es posible construir una representación del grupo G. En efecto, damos un nombre a la aplicación $v \mapsto g \cdot v$. Como $\varphi(g) : V \to V$, dado por $\varphi(g)(v) = g \cdot v$, tenemos que:

$$\varphi(g)(v + cw) = g \cdot (v + cw) = g \cdot v + g \cdot cw = \varphi(g)(v) + c\varphi(g)(w)),$$

de esta manera, φ es una aplicación lineal para cada g en G y no es difícil corroborar que $\varphi(1) = Id_V$, y $\varphi(g) \circ \varphi(g^{-1}) = Id_V$, luego $\varphi(g)$ esta en $\text{Aut}(V)$ y la aplicación $G \to \text{Aut}(V)$, dada por $g \mapsto \varphi(g)$ es un homomorfismo de grupos.

Además si ρ es una representación de G, siempre es posible definir un $\mathbb{K}G$-módulo M. Estas observaciones motivan la siguiente definición

Definición 1.75. *Sea G un grupo y $\mathbb{K}$ un cuerpo. Una representación de G es un $\mathbb{K}G$-módulo M.*

Luego, considerar representaciones de un grupo o módulos sobre $\mathbb{K}G$ tienen el mismo significado. Finalizamos esta sección con un resultado de teoría de representaciones

Proposición 1.76 (Teorema de Maschke)**.** *Sea $\mathbb{K}$ un cuerpo y G un grupo finito, cuyo orden es unidad en $\mathbb{K}$. Entonces $\mathbb{K}G - \mathbf{Mod} = \mathbb{K}G - \mathbf{Pmod}$*

Demostración. Sea V un $\mathbb{K}G$-módulo y V_0 el $\mathbb{K}$-módulo obtenido de V por restricción de escalares. Consideramos el módulo $\mathbb{K}G \otimes_{\mathbb{K}} V_0$ obtenido de V_0 por extension de escalares y la función lineal $i : V \to \mathbb{K}G \otimes_{\mathbb{K}} V_0$ y $\pi : \mathbb{K}G \otimes_{\mathbb{K}} V_0 \to V$, las cuales están definidas por

$$i(v) = \frac{1}{|G|} \sum_{g \in G} g \otimes g^{-1}v \text{ y } \pi(g \otimes v) = gv$$

Para todo v en V y g en G, tenemos que i y π son homomorfismos de $\mathbb{K}G$-módulos y como $\pi \circ i = Id_V$, tenemos que i identifica a V como un sumando directo de $\mathbb{K}G \otimes_{\mathbb{K}} V_0$ el cual es libre, por tanto V es un $\mathbb{K}G$-módulo proyectivo. □

Este resultado admite una generalización también debida a Maschke

Proposición 1.77. *Sea R un anillo y G un grupo finito. Entonces RG es semisimple si y solo si R es semisimple y $|G|$ es una unidad en R.*

Demostración. [Lam01, Capítulo 2, teorema 6.1] □

La hipótesis sobre la finitud de $|G|$ es importante, teniendo en cuenta el siguiente resultado

Proposición 1.78. *Sea $R \neq 0$ un anillo y G un grupo infinito. Entonces RG no es semisimple*

Demostración. Considere $\epsilon : RG \to R$ el homomorfismo de aumentación y $I_G = \ker\ \epsilon$ el ideal de aumentación. Supongamos que RG es semisimple, entonces existe un ideal a izquierda J tal que $RG = I_G \oplus J$ donde $J \subset RG$. De este modo, existen elementos idempotentes no nulos e, f ortogonales (e+f=1) en RG tales que

$$I_G = R \cdot e \text{ y } J = R \cdot f.$$

Así, $I_G \cdot f = Re \cdot f = 0$, de esta manera, $(g-1)f = 0$ o $f = gf$ para cualquier elemento g de G, y considere τ un elemento de G que aparece en f con un coeficiente no nulo. Entonces $\sigma\tau$ aparece en f con el mismo coeficiente, para cualquier g en G. Esto significa que f esta representado por todos los elementos de G, Como G es infinito esto es absurdo por la definición de RG $\square$

Capítulo 2

Conjetura de idempotencia de Kaplansky

El objetivo del presente capítulo es describir una aplicación de la teoría desarrollada en el capítulo anterior en el estudio de la conjetura de idempotencia. Diversas técnicas se han usado para estudiarla y algunas de ellas guardan una relación con la K teoría algebraica. La que presentaremos está relacionada con los módulos proyectivos sobre un anillo de grupo y fue desarrollada por Ionnais Emmanouil en [Emm01].

2.1 Conjeturas de Kaplansky

Estas conjeturas y otros problemas sobre la teoría de los anillos fueron propuestos por Irving Kaplansky en [Kap57], y 13 después fueron analizados en [Kap70], en este último presenta el estado de cada problema, algunos de ellos ya habían sido solucionados pero aquellos que estaban relacionados con las álgebras de grupo (donde $\mathbb{K}$ es un cuerpo conmutativo y G un grupo, $A(G)$ es referida como el algebra de grupo de G sobre $\mathbb{K}$) no poseían mayor avance y son de nuestro interés.

En el presente trabajo nos referiremos a estas conjeturas de la siguiente forma:

- La conjetura de idempotencia (CI): Sea R un dominio de integridad y G un grupo libre de torsión, entonces RG no posee idempotentes no triviales.
- La conjetura del divisor de Cero (CCD): Sea R un dominio de integridad y G un grupo libre de torsión, entonces RG no posee Divisores de Cero.
- La conjetura de reducción (CR): Sea R un dominio de integridad y G un grupo libre de torsión, entonces RG es un anillo reducido.
- La conjetura de las unidades (CU): Sea R un dominio de integridad y G un grupo libre de torsión, entonces RG no posee unidades no triviales).

Esta es la forma en las que estas conjeturas se conocen en la mayoría de los textos consultados (ver [Lam01, (6.16) a (6.19)]). El objetivo de esta sección se puede resumir en probar las siguientes implicaciones

$$CU \Longrightarrow CR \Longleftrightarrow CCD \Longrightarrow CI$$

Por otro lado, veremos que la conjetura del divisor de cero es equivalente a la conjetura de nilpotencia, además, daremos algunos ejemplos de grupos que satisfacen la conjetura de idempotencia.

Definición 2.1. *Sea R un anillo, decimos que es R primo si* (0) *es un ideal primo.*

De la definición podemos observar que todo dominio de integridad es un anillo primo, y decir que un anillo R es primo es equivalente a afirmar que si $aRb = 0$ para a, b en R entonces $a = 0$ y $b = 0$.

Proposición 2.2. *Un anillo es primo si y solo si $M_n(R)$ es un anillo primo*

Demostración. Sea $R \neq 0$ no primo, entonces existe dos ideales I, J de R tales que $IJ = 0$, pero $M_n(I)M_n(J) = 0$, por tanto $M_n(R)$ no es primo. de forma análoga, si $M_n(R) \neq 0$ no es primo, entonces existe dos ideales U, V de $M_n(R)$ tales que $UV = 0$ pero por 1.11 existen ideales I, J no nulos de R tales que $U = M_n(I)$ y $V = M_n(J)$, además si $IJ = 0$ implica que $AB = 0$ de esta forma R no es primo. □

Teorema 2.3 (Teorema de Connell)**.** *Sea R un anillo y G un grupo. Entonces el anillo de grupo RG es primo si y sólo si R es primo y G no posee un subgrupo normal finito diferente de* $\{e\}$

Demostración. ver [Lam01, teorema (A) capítulo 4, pág. 161] □

Teorema 2.4. *La conjetura del divisor de cero es equivalente a la conjetura de reducción.*

Demostración. Sea RG un anillo de grupo y a y b RG tales que $ab = 0$, considere los ideales (a) y (b), el producto de estos ideales no puede ser igual al ideal (0) ya que RG es un anillo primo. De esta manera, existe un c en RG tal que $bca \neq 0$, luego $(bca)^2 = bcabca = 0$, así RG posee un elemento de la forma $x^2 = 0$ y $x \neq 0$. Por tanto RG posee un elemento nilpotente no trivial y por definición RG no es reducido.

Por otro lado, si RG no es reducido, entonces existe un elemento nilpotente no nulo x tal que $x^n = 0$ para algún n en $\mathbb{N}$, podemos considerar n tal que $x^2, \ldots, x^{n-1}$ sean no nulos, por tanto, x es un divisor de cero. □

Proposición 2.5. *La conjetura de divisor de cero implica la conjetura de idempotencia*

Demostración. Si RG posee un elemento idempotente e no trivial, entonces $e^2 = e$, es decir, $e(e-1) = 1$. Por tanto RG posee un divisor de cero diferente de 0 y 1. □

En el presente trabajo, nos enfocaremos en la conjetura de idempotencia, en las siguientes secciones expondremos una forma de analizar esta conjetura.

Proposición 2.6. *La conjetura de unidades implica la conjetura de reducción.*

Demostración. Supongamos que RG no es reducido, luego existe un elemento no nulo x tal que $x^n = 0$, y de esta manera $(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1$ luego se ha construido una unidad no trivial de RG. □

2.2 Técnicas para el estudio de la conjetura de idempotencia

Una pregunta válida es saber que técnicas se han desarrolla para resolver los problemas de Kaplansky, existen tres metodologías (según [Emm01])para estudiarla, en este apartado simplemente las enunciaremos y en si, presentaremos un estado del arte, más que entrar en detalle de como funciona cada una de ellas.

1. Reducción a característica positiva: Sea $e = a_1 g_1 + \ldots + a_n g_n$ un elemento de $\mathbb{C}G$ un elemento idempotente, y considere el subanillo $A = \mathbb{Z}[e_1, \ldots, e_n]$ de $\mathbb{C}$ generado por los e_i. Para cualquier ideal maximal M de A el cuerpo residual $\mathbb{K} = A/M$ es un cuerpo finito, de característica p. Por paso al cociente e define un idempotente en $\bar{e}$ en $\mathbb{K}G$ el cual puede ser estudiado por medio del operador de Frobenius $(x \mapsto x^p)$ sobre $\mathbb{G}$, por ejemplo en [Bas76] es usada esta técnica y se prueba que $\mathbb{C}G$ no posee idempotentes no triviales cuando G es un grupo lineal libre de torsion (es decir cuando G es un subgrupo libre de torsion de $GL_n(\mathbb{F})$ con $\mathbb{F}$ un cuerpo).

2. Homología cíclica: Uno de los resultados mas antiguos en la teoría de anillos de grupos se debe a Kaplansky sobre los valores de la traza canónica sobre elementos idempotentes de $\mathbb{C}G$, específicamente, el teorema dice [Edw73]

   Teorema 2.7. *Si F es un cuerpo de característica 0, G un grupo, y $e \neq 0, 1$ un elemento idempotente de FG, entonces $Tr(e)$ es un número real y $0 < Tr(e) < 1$.*

   Se puede mostrar que los idempotentes en $\mathbb{C}G$ son triviales estudiando la nilpotencia del operador de periodicidad en homología cíclica.

3. Reducción modulo el ideal de aumentación: Un elemento idempotente en $\mathbb{C}G$ define un modulo proyectivo sobre $\mathbb{C}G$, $P = \mathbb{C}Ge$, entonces podemos definir la coinvarianza de P, $P_G = P/I_G P$ donde I_G es el ideal de aumentación de $\mathbb{C}G$. Existe una relación entre la coinvarianza de P y e, si $P_G = 0$ entonces e se anula.

De estas metodologías en el presente trabajo expondremos la última, en parte por tener mayor conexión con la teoría que se ha desarrollado hasta el momento.

2.3 Reducción módulo el ideal de aumentación y la clase $\mathcal{P}$

Introduciremos una técnica para el estudio de la conjetura de idempotencia que relaciona los módulos proyectivos sobre un anillo de grupo presentada en [Emm05] y [Emm01]. En particular probaremos que la conjetura de idempotencia se tiene para todo grupo abeliano libre de torsion.

Recordemos que el epimorfismo de aumentación

$$\epsilon : \mathbb{C}G \to \mathbb{C}$$

está definido por $\epsilon\left(\sum_g a_g g\right) = \sum_g a_g$ y $I_G = \ker \epsilon$ el ideal de argumentación. Podemos ver que $\mathbb{C} = \mathbb{C}G/I_G$ como $\mathbb{C}G$-módulo a derecha y consideramos el funtor

$$\begin{aligned}(-)_G : \mathbb{C}G - \mathbf{Mod} &\longrightarrow \mathbb{C} - \mathbf{Mod},\\ A &\longmapsto A_G.\end{aligned}$$

donde

$$A_G = \mathbb{C} \otimes_{\mathbb{C}G} A = A/I_G A.$$

Este es el mayor cociente de A en el cual G actúa trivialmente.

Por otro lado, sea G un grupo y $g \neq 1$ un elemento de orden finito ($|g| = n$), entonces el elemento

$$e = \frac{1}{n}\left(1 + g + g^2 + \cdots + g^{n-1}\right) \in \mathbb{C}G$$

satisface $e^2 = e$, es decir, e es un idempotente no trivial y de esta manera $P = \mathbb{C}G(1-e)$ es un $\mathbb{C}G$-módulo proyectivo. Como $\epsilon(e) = 1$ tenemos que $1-e \in I_G$, y de esta manera, $P = \mathbb{C}G \cdot (1-e) = \mathbb{C}G \cdot (1-e)^2 \subset I_G \cdot (1-e) = I_G P$.

Esta situación motiva la siguiente definición

Definición 2.8. *Sea $\mathcal{P}$ la clase formada por todos los grupos G tales que si P es un $\mathbb{C}G$-módulo proyectivo, $P \neq 0$ entonces se tiene que $P_G \neq 0$.*

Observe que afirmar que un grupo G pertenece a la clase $\mathcal{P}$ es equivalente a que si para cada $\mathbb{C}G$-módulo proyectivo P tal que $P_G = 0$ entonces $P = 0$, usaremos esta equivalencia ocasionalmente.

Proposición 2.9. *Si un grupo G pertenece a $\mathcal{P}$, entonces G satisface la conjetura de idempotencia.*

Demostración. Sea G un grupo perteneciente a $\mathcal{P}$ y $e = \sum_{g \in G} e_g g \in \mathbb{C}G$ un elemento idempotente, donde $e_g \in \mathbb{C}$. Como $\epsilon(e) \in \mathbb{C}$ es un idempotente, tenemos que $\epsilon(e) = 0$ o 1, sin perdida de generalidad se puede suponer que $\epsilon(e) = 0$ y por tanto $e \in I_G$. Considerando el $\mathbb{C}G$-módulo proyectivo $P = \mathbb{C}Ge$ y teniendo en cuenta que $P = \mathbb{C}Ge^2 \subset I_g e = I_G P$, se obtiene, $P/I_G P = 0$ y por tanto $e = 0$ es un idempotente trivial. ☐

Antes de probar que la clase $\mathcal{P}$ no es vacía, daremos una proposición que nos permitirá saber cuando un grupo pertenece a $\mathcal{P}$ en términos del ideal I_G. Por la discusión inicial se tiene que un grupo G que pertenece a $\mathcal{P}$ necesariamente debe ser libre de torsion, nuestro objetivo inicial es mostrar que esta clase es no vacía y que posee relevancia en el estudio de la conjetura de idempotencia.

Definición 2.10. *Sea I un ideal de un anillo R, definimos $I^\infty = \bigcap_{n=1}^\infty I^n$*

Proposición 2.11. *Sea G un grupo y supongamos que el ideal de aumentación I_G del álgebra de grupo $\mathbb{C}G$ es tal que $I_G^\infty = 0$. Entonces G pertenece a $\mathcal{P}$.*

Demostración. Sea P un $\mathbb{C}G$-modulo proyectivo. Escogemos un $\mathbb{C}G$-módulo libre F que contiene a P como sumando directo y notamos que $P \cap JF = JP$ para cualquier ideal $J \subset \mathbb{C}G$. Observemos que si $I \subset \mathbb{C}G$ es un ideal tal que $P = IP$, entonces $P = I^\infty P$. Teniendo en cuenta que $P = I^n P \subset I^n F$ para todo $n \in \mathbb{N}$ y de este modo $P \subset \bigcap_n (I^n F) = \left(\bigcap_n I^n\right) F = I^\infty F$ concluimos que $P = P \cap I^\infty F = I^\infty P$. Si $P_G = P/I_G P = 0$, entonces $P = I_G P$ y por tanto $P = I_G^\infty P = 0$. □

Proposición 2.12. *El grupo aditivo de los números racionales $\mathbb{Q}$ pertenece a $\mathcal{P}$*

Demostración. Sea $G = \mathbb{Q}$ entonces $\mathbb{C}G$ puede ser identificado con $\mathbb{C}[t^a : a \in \mathbb{Q}]$ y $I_G = (t^a - 1 : a \in \mathbb{Q})$. Observemos que para cualquier $x \in I_G^n$ la k-ésima derivada $d^k x/dt^k$ se anula en $t = 1$ para todo $k < n$. Considere $x = \sum_{j=1}^m x_j t^{k_j}$ un elemento de I_G^∞ donde $x_j \in \mathbb{C}$ y k_j son números racionales *distintos.* Entonces $dx^i/dt^i|_{t=1} = 0$ para todo $i \geq 0$ y de esta forma podemos construir el siguiente sistema de ecuaciones.

$$\sum_{j=1}^{m} \left(\prod_{v=0}^{i-1} (k_j - v) \right) x_j = 0$$

para $i = 0, 1, 2, \ldots, m-1$. El determinante de este sistema lineal es no nulo, es más, podemos ver que es $\prod_{i<j}(k_j - k_i)$ y por ende, debemos tener que x_j es cero para todo $j = 1, \ldots, m$, luego $x = 0$ y de esta manera $I_G^\infty = 0$. Luego concluimos que $G \in \mathcal{P}$ por 3.3 □

Ahora nuestro objetivo es encontrar más grupos que pertenecen a $\mathcal{P}$, en particular, probaremos que todo grupo abeliano libre de torsion es un elemento de $\mathcal{P}$. Para ello necesitaremos los siguientes resultados previos.

Proposición 2.13. *La clase $\mathcal{P}$ es cerrada bajo subgrupos y extensiones*

Demostración. Sea H un subgrupo de un grupo G perteneciente a $\mathcal{P}$. Sean P un $\mathbb{C}H$-módulo proyectivo tal que $\mathbb{C} \otimes_{\mathbb{C}H} P = 0$ entonces $P' = \mathbb{C}G \otimes_{\mathbb{C}H} P$ es un $\mathbb{C}G$-módulo proyectivo con $\mathbb{C} \otimes_{\mathbb{C}G} P' = 0$; G esta en $\mathcal{P}$, tenemos que $P' = 0$. Pero P esta contenido (como sumando directo) en P' y por tanto $P = 0$, luego H esta en $\mathcal{P}$.

Ahora veremos que $\mathcal{P}$ es cerrada bajo extensiones. Sea N un grupo normal de un grupo G y supongamos que N y $\bar{G} = G/N$ pertenecen a $\mathcal{P}$. Si P es un $\mathbb{C}G$-módulo proyectivo con $\mathbb{C} \otimes_{\mathbb{C}G} P = 0$, entonces $\bar{P} = \mathbb{C} \otimes_{\mathbb{C}N} P$ es un $\mathbb{C}\bar{G}$-módulo proyectivo con $\mathbb{C} \otimes_{\mathbb{C}\bar{G}} \bar{P} = 0$. Como $\bar{G}$ esta en $\mathcal{P}$, tenemos que $\bar{P} = 0$ y por otro lado, como $\mathbb{C}$-módulo $\bar{P}$ es isomorfo a $\mathbb{C} \otimes_{\mathbb{C}N} P = P_N$, donde P es visto como $\mathbb{C}N$-módulo por restricción de escalares, además P es un $\mathbb{C}N$-módulo proyectivo y N pertenece a $\mathcal{P}$, luego $P = 0$ y de esto se sigue que G esta en $\mathcal{P}$. □

De esta forma combinando la anterior, tenemos que

- $\mathbb{Z}$ pertenece a $\mathcal{P}$. y de esta forma , cualquier grupo cíclico infinito satisface la conjetura de idempotencia, este resultado ya lo conocíamos de forma implícita si tenemos en cuenta la proposiciones 1.69 y 2.4.

- No todo subgrupo del grupo aditivo de los números racionales es cíclico, exponemos una clasificación de estos en el apéndice B, para todos ellos es valida la conjetura de idempotencia.
  Uno de los subgrupos de $\mathbb{Q}$ que no es cíclico es el llamado grupo de diádico, se define como los números racionales de la forma $a/2^j$ donde $a \in \mathbb{Z}$ y $j \in \mathbb{N}$. También puede ser considerado como:

$$\varinjlim\{2^{-i}\mathbb{Z}|i = 0, 1, 2, \ldots\}$$

Proposición 2.14. *Sea G un grupo $(H_\lambda)_\lambda$ una cadena de subgrupos de G y H la intersección de todos los H_λ. La intersección de la familia $(I_{H_\lambda}CG)_\lambda$ de $\mathbb{C}H$-submódulos de $\mathbb{C}G$ es igual a $I_H\mathbb{C}G$.*

Demostración. Observe que $I_H\mathbb{C}G$ siempre esta contenido en la intersección de los $I_{H_\lambda}CG$, sea $x \in \mathbb{C}G$ un elemento con $x \notin I_H\mathbb{C}G$. Considere el conjunto T de clases laterales a izquierda en G y recordemos la descomposición

$$\mathbb{C}G = \bigoplus_{t\in T} \mathbb{C}H \cdot t.$$

Escribimos $x = x_1t_1 + \cdots + x_nt_n$, entonces existe i_0 con $x_{i_0} \notin I_H$. Suponiendo que todos los t_i son distintos vemos que $t_it_j^{-1} \notin H$ para todo $i \neq j$ luego existen λ_{ij} con $t_it_j^{-1} \notin H_{\lambda_{ij}}$ para todo $i \neq j$. Así, buscamos un índice λ tal que $H_\lambda \subseteq H_{\lambda_{ij}}$ para todo $i \neq j$. Entonces $t_it_j^{-1} \notin H_\lambda$ y por tanto los t_i forman parte de un sistema de clases laterales a izquierda de H_λ en G, como $x_i \in CH \subseteq CH_\lambda$ para todo $i = 1, 2, \ldots, n$ tenemos que la expresión de x se encuentra en la descomposición

$$\mathbb{C}G = \bigoplus_{t\in T_\lambda} \mathbb{C}H_\lambda \cdot t.$$

Como $\mathbb{C}H \cap I_{H_\lambda} = I_H$, tenemos que $x_{i_0} \neq I_{H_\lambda}$, de esta manera, vemos que $x \notin I_{H_\lambda}\mathbb{C}G$. □

Proposición 2.15. *Sea G un grupo $(H_\lambda)_\lambda$ una cadena de subgrupos de G y H la intersección de todos los H_λ. Si P es un $\mathbb{C}G$-módulo proyectivo y $\mathbb{C} \otimes_{\mathbb{C}H_\lambda} P = 0$ para todo λ, entonces $\mathbb{C} \otimes_{\mathbb{C}H} P = 0$*

Demostración. Sea F un $\mathbb{C}G$-módulo libre que contiene a P como un sumando directo. Como $P/I_{H_\lambda}P = \mathbb{C} \otimes_{\mathbb{C}H_\lambda} P = 0$ tenemos que $P = I_{H_\lambda}P$ y por lo tanto $P \subseteq I_{H_\lambda}F$ para todo λ, luego de la proposición 2.14 tenemos que la intersección de la familia $(I_{H_\lambda}F)_\lambda$ es igual a I_HF. De este modo, $P \subseteq I_HF$, ya que P es un sumando directo de F como $\mathbb{C}G$-módulo y por tanto, como $\mathbb{C}H$-módulo por restricción de escalares. La intersección $P \cap I_HF$ coincide con I_HP, por lo tanto $P = P \cap I_HF = I_HP$, y de este modo, $\mathbb{C} \otimes_{\mathbb{C}H} P = P/I_HP = 0$. □

Corolario 2.16. *Sea G un grupo y P es un $\mathbb{C}G$-módulo proyectivo tal que $\mathbb{C}\otimes_{\mathbb{C}G} P = 0$. Entonces existe un subgrupo de G tal que $\mathbb{C}\otimes_{\mathbb{C}H} P = 0$, con H minimal respecto a esta propiedad.*

Demostración. Considere la siguiente clase

$$\mathcal{F} = \{H \leq G : \mathbb{C}\otimes_{\mathbb{C}H} P = 0\}$$

Observe que $\mathcal{F}$ no es vacío ya que G pertenece a $\mathcal{F}$. Definimos el siguiente orden sobre $\mathcal{F}$: $H \preceq T$ si $T \subseteq H$. Por la proposición 2.15 tenemos que toda cadena posee una cota superior en $\mathcal{F}$, aplicando el lema de Zorn obtenemos el resultado. □

Proposición 2.17. *Sea G un grupo y asuma que cualquier subgrupo no trivial de este admite un cociente no trivial el cual esta contenido en $\mathcal{P}$. Entonces G está en $\mathcal{P}$*

Demostración. Sea P en $\mathbb{C}G$-módulo proyectivo con $\mathbb{C}\otimes_{\mathbb{C}G} P = 0$ y escogemos un subgrupo H de G el cual es minimal respecto a la propiedad de $\mathbb{C}\otimes_{\mathbb{C}H} P = 0$. Tal grupo existe por el corolario 2.16. Si H es trivial entonces $\mathbb{C}\otimes_{\mathbb{C}H} P = C\otimes_{\mathbb{C}} P = P$ y por tanto $P = 0$. Si H no es trivial, entonces existe un subgrupo normal propio N de H tal que $\bar{H} = H/N$ esta en $\mathcal{P}$. Como $\mathbb{C}\otimes_{\mathbb{C}\bar{H}} (\mathbb{C}\otimes_{\mathbb{C}N} P) = \mathbb{C}\otimes_{\mathbb{C}H} P = 0$ y $\mathbb{C}\otimes_{\mathbb{C}N} P$ es un $\mathbb{C}\bar{H}$-módulo proyectivo, se tiene que $\mathbb{C}\otimes_{\mathbb{C}N} P = 0$. Pero esto es absurdo, pues contradice la minimalidad de H. □

Proposición 2.18. *La clase $\mathcal{P}$ es cerrada bajo productos directos*

Demostración. Sea $(G_i)_I$ una familia de grupos, tal que G_i pertenece a $\mathcal{P}$ y H un subgrupo no trivial del producto directo $G = \prod_i G_i$. Entonces H puede ser proyectado a un subgrupo no trivial H_i para cada uno de los G_i. Como $\mathcal{P}$ es cerrado bajo subgrupos (por 2.13), concluimos que G pertenece a $\mathcal{P}$ por 2.17 □

Como aplicación de la teoría desarrollada en este punto, tenemos el siguiente resultado.

Proposición 2.19. *La clases $\mathcal{P}$ contiene a todos los grupos abelianos libres de torsión.*

Demostración. Tenemos en cuenta que todo grupo abeliano libre de torsion se encuentra contenido en $V = \mathbb{Q}\otimes G$, el cual es un espacio vectorial sobre $\mathbb{Q}$, luego V es una suma directa de copias de $\mathbb{Q}$ y por tanto esta contenido en el producto directo de estas copias, como $\mathbb{Q}$ pertenece a $\mathcal{P}$ y esta clase es cerrada bajo subgrupos y productos directos. V pertenece a $\mathcal{P}$. □

Por el momento tenemos que todo grupo abeliano libre de torsion pertenece a la clase $\mathcal{P}$, una pregunta válida es si existe un grupo no conmutativo libre de torsión, en lo que resta de esta sección nos dedicaremos a responder esta pregunta.

Definición 2.20. *El subconjunto de $SL_3(\mathbb{Z})$*

$$\left\{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}\right\}$$

se denomina el grupo de Heisenberg discreto[1]. *y lo denotaremos por $\mathcal{H}_3(\mathbb{Z})$*

[1] También se le denomina el grupo de Heisenberg entero [LP96]

Claramente $\mathcal{H}_3(\mathbb{Z})$ es un subgrupo multiplicativo de $SL_3(\mathbb{Z})$ y además, podemos ver que es libre de torsion en virtud de la siguiente identidad

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nc + \binom{n}{2}ab \\ 0 & 1 & nb \\ 0 & 0 & 1 \end{pmatrix}.$$

Proposición 2.21. *El grupo discreto de Heisenberg pertenece a la clase $\mathcal{P}$*

Demostración. Considere la siguiente función

$$\varphi : \mathcal{H}_3(\mathbb{Z}) \to \mathbb{Z} \times \mathbb{Z}$$
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, b)$$

Claramente es un epimorfismo de grupos, y tiene por núcleo a

$$\ker \varphi = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : c \in \mathbb{Z} \right\},$$

el cual es isomorfo a $\mathbb{Z}$ y a su vez es el centro de $\mathcal{H}_3(\mathbb{Z})$, de esta manera, tenemos que $\mathcal{H}_3(\mathbb{Z})$ es extension (central) de $\mathbb{Z} \times \mathbb{Z}$ por $\ker \varphi$, pero estos últimos están en $\mathcal{P}$, luego por 2.13 tenemos que $\mathcal{H}_3(\mathbb{Z})$ pertenece a $\mathcal{P}$ □

El grupo discreto de Heisenberg admite la siguiente generalización,

$$\mathcal{H}_n(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & x_1 & x_2 & \dots & x_{n-1} & x_n & z \\ 0 & 1 & 0 & \dots & 0 & 0 & y_1 \\ 0 & 0 & 1 & \dots & 0 & 0 & y_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & y_{n-1} \\ 0 & 0 & 0 & \dots & 0 & 1 & y_n \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} : x_i, y_i, z \in \mathbb{Z}, 1 \leq i \leq n \right\}.$$

Este es un subgrupo multiplicativo de $SL_{n+2}(\mathbb{Z})$. Por otro lado, podemos escribir un elemento A de $\mathcal{H}_n(\mathbb{Z})$, de la siguiente forma,

$$\begin{pmatrix} 1 & a^t & c \\ 0 & I_n & b \\ 0 & 0 & 1 \end{pmatrix}$$

donde a, b pertenecen a $\mathbb{Z}^n$ [2] y c en $\mathbb{Z}$. Con esta notación podemos enunciar el siguiente

Corolario 2.22. *Para todo $n \geq 3$, $H_n(\mathbb{Z})$ pertenece a $\mathcal{P}$*

[2] Notamos los vectores, como vectores columna

Demostración. Definimos la función

$$H_n(\mathbb{Z}) \to \mathbb{Z}^n \times \mathbb{Z}^n, \quad \begin{pmatrix} 1 & a^t & c \\ 0 & I_n & b \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, b)$$

claramente este es un epimorfismo de grupos y su núcleo es isomorfo a $\mathbb{Z}$. De este modo $H_n(\mathbb{Z})$ es la extension de $\mathbb{Z}^n \times \mathbb{Z}^n$ por $\mathbb{Z}$ y por 2.13 tenemos el resultado. □

De esta manera hemos encontrado una familia de grupos no conmutativos libres de torsion que pertenecen a la clase $\mathcal{P}$.

Actualmente se conoce que la conjetura de idempotencia es afirmativa para una amplia gama de tipos de grupos (Noetherianos, supersolubles, Policiclicos de tipo finito). Sin embargo, para el grupo de automorfismos de un grupo libre de n letras ($n > 1$), $Aut(F\langle x_1, \ldots, x_n\rangle)$ no existe información si satisface o no la conjetura de idempotencia. Agradezco a Eugenia Ellis por proveer este ejemplo.

Para concluir esta sección expondremos una propiedad adicional de la clase $\mathcal{P}$.

Proposición 2.23. *La clase $\mathcal{P}$ es cerrada bajo productos libres*

Demostración. Sea $(G_i)_I$ una familia de grupos, tal que G_i pertenece a $\mathcal{P}$ y H un subgrupo no trivial del producto

$$G = \mathop{\ast}_{i \in I} G_i.$$

Entonces por el teorema de Kuroš 1.65 tenemos que H se descompone en un producto libre de un grupo libre y el producto libre de ciertos subgrupos de G los cuales son isomorfos (es más, conjugados en G) con los subgrupos G_i. Como $\mathcal{P}$ es cerrada bajo subgrupos 2.13 y $\mathbb{Z}$ esta en $\mathcal{P}$, tenemos que se tienen las condiciones de la proposición 2.17, y por tanto G pertenece a $\mathcal{P}$. □

2.4 Dependencia del anillo base y la clase $\mathcal{P}(k)$

En la anterior sección introducimos una técnica para estudiar la existencia de elementos idempotentes en kG donde G es un grupo libre de torsion y $\mathbb{C}$, pero podemos ver que k puede ser reemplazado por cualquier dominio de integridad, en particular, la proposición 2.9 es válida para todo dominio de integridad, lo cual motiva la siguiente definición

Definición 2.24. *Sea $\mathcal{P}$ la clase formada por todos los grupos G tal que si P es un kG-módulo proyectivo, $P \neq 0$ entonces se tiene que $P_G \neq 0$.*

Por otro lado, sea G de un grupo y g en G diferente de la identidad de orden finito n. Si k es un anillo conmutativo tal que G esta en $\mathcal{P}(k)$, entonces n no es unidad en k ya que si n es una unidad en k es posible encontrar a un kG-módulo proyectivo P (siguiendo los mismos pasos de la proposición 2.9) tal que $P_G = 0$.

Proposición 2.25. *Sea k, k' anillos conmutativos.*

1. *Suponga que existe un homomorfismo inyectivo $\varphi : k \to k'$. Entonces $\mathcal{P}(k') \subseteq \mathcal{P}(k)$.*

2. *Suponga que existe un homomorfismo de anillos $\varphi : k \to k'$ tal que k' es un k-módulo proyectivo. Entonces $\mathcal{P}(k) \subseteq \mathcal{P}(k')$.*

Demostración.

1. Sea G un grupo en $\mathcal{P}(k')$ y P un kG-módulo proyectivo tal que $k \otimes_{kG} P = 0$. entonces $P' = k'G \otimes_{kG} P = k' \otimes_k P$ es un $k'G$-módulo proyectivo y
$$k' \otimes_{k'G} P' = k' \otimes_{kG} P = k' \otimes_k (k \otimes_{kG} P)$$
de este modo $P' = 0$. Como P es un kG-módulo proyectivo, tenemos que también es proyectivo (y por tanto plano)como k-módulo, de esta manera, el homomorfismo inducido $P = k \otimes_k P \xrightarrow{\varphi \otimes id} k' \otimes_k P = P'$ es inyectivo, de esta manera $P = 0$.

2. Sea G un elemento de $\mathcal{P}(k)$ y P un $k'G$-módulo proyectivo con $k' \otimes_{k'G} P = 0$. Luego podemos considerar P_0 la restricción de escalares de P. Así P_0 es un kG-módulo proyectivo y como $k' \otimes_{k'G} P = 0$, tenemos que $P_0 = I_G(k)P_0$ donde $I_G(k)$ es el ideal de aumentación de kG y por tanto $k \otimes_{kG} P_0 = 0$. Por hipótesis sobre φ tenemos que $k'G$ es un kG-módulo proyectivo y por tanto P_0 es un kG-módulo proyectivo, de este modo, $P_0 = 0$ y $P = 0$.

□

Corolario 2.26. *Si k es un cuerpo y k' una k-algebra conmutativa, entonces $\mathcal{P}(k) = \mathcal{P}(k')$.*

Proposición 2.27. *Sea k un anillo conmutativo, $(J_i)_i$ una familia de ideales en k y $k_i = k/J_i$. Si $\bigcap_i J_i = (0)$ entonces $\bigcap_i \mathcal{P}(k_i) \subseteq \mathcal{P}(k)$.*

Demostración. Sea G es un grupo y supongamos que G esta en $\mathcal{P}(k_i)$ para todo i. Si P es un kG-módulo proyectivo con $k \otimes_{kG} P = 0$, entonces, para cualquier i, $P_i = k_iG \otimes_{kG} P = k_i \otimes_k P = P/J_iP$ es un k_iG-módulo proyectivo, además,
$$k_i \otimes_{k_iG} P_i = k_i \otimes_{kG} P = k_i \otimes (k \otimes_{kG} P) = 0,$$
y de esta forma, $P_i = 0$. Por lo tanto, $P = J_iP$ para todo i, considerando al kG-módulo proyectivo P, P se puede identificar como un k-módulo proyectivo; en particular P esta contenido en un k-módulo libre F. Pero $P = J_iP \subseteq J_iF$ para todo i y por nuestra hipótesis sobre la intersección de los J_i, tenemos que $P = 0$. □

Corolario 2.28. *Si G esta en $\mathcal{P}(\mathbb{F}_p)$ para un numero infinito de primos, entonces G esta $\mathcal{P}(\mathbb{Z})$.*

Corolario 2.29. *Sea $(k_i)_i$ una familia de anillos conmutativos y $k = \prod_i k_i$. Entonces $\mathcal{P}(k) = \bigcap_i \mathcal{P}(k_i)$.*

Demostración. Por la proposición 2.27 tenemos que $\bigcap_i \mathcal{P}(k_i) \subseteq \mathcal{P}(k)$. Por otro lado, para cualquier i la proyección en la i-ésima coordenada hace a k_i un k-módulo proyectivo y por la proposición 2.25, tenemos que $\mathcal{P}(k) \subseteq \mathcal{P}(k_i)$. □

Capítulo 3

Fundamentos de K teoría algebraica

La K teoría algebraica fue desarrollada por Alexander Grothendieck en el año 1957, y desde entonces ha aparecido una gran cantidad de textos ([Bas73], [Mil72] , [Sil81], [Sri07], [Kuk00], [Ros95], [Ina10], [Wei13]) y artículos dedicados a su exposición (ver [LS75]). La presente exposición recoge de cierta forma lo que pude aprender de estas fuentes.

3.1 Completación de un semigrupo abeliano

Veremos una técnica que nos permite construir un grupo abeliano a partir de un monoide abeliano, en cierto sentido, se puede considerar una generalización de la construcción de los números enteros $\mathbb{Z}$ usando los números naturales $\mathbb{N}$

Proposición 3.1. *Sea $(A, +)$ un monoide abeliano, definimos la relación $\sim$ sobre $A \times A$*

$$(a, b) \sim (c, d) \text{ si y solo si existe } u \in A \text{ tal que } a + d + u = b + c + u.$$

La relación $\sim$ es una relación de equivalencia.

Demostración.

Reflexiva $(a, b) \sim (a, b)$ si y solo si existe $u \in A$ tal que $a+b+u = b+a+u$. tomando cualquier u en A se tiene la condición.

Simétrica Si $(a, b) \sim (c, d)$ si y solo si existe $u \in A$ tal que $a + d + u = b + c + u$, pero esta ecuación es equivalente a $c+b+u = d+a+u$ ya que A es abeliano, entonces $(c, d) \sim (a, b)$.

Transitiva si $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$ entonces existen u y v en A tales que $a+d+u = b+c+u$ y $c+f+v = d+e+v$, de este modo $a+d+u+c+f+v = b+c+u+d+e+v$ pero esta ecuación es equivalente a $a+f+(c+d+u+v) = b+e+(c+d+u+v)$ luego si $w = c+d+u+v$ tenemos que $a+f+w = b+e+w$, es decir, $(a, b) \sim (e, f)$.

□

Definición 3.2. *Una completación de un semigrupo abeliano A es un grupo abeliano $K(A)$ dotado de una homomorfismo de semigrupos $\varphi : A \to K(A)$ que satisface la siguiente propiedad universal. Para cualquier grupo abeliano B y cualquier homomorfismo de monoides $f : A \to B$ existe un único homomorfismo de grupos $\bar{f} : K(M) \to A$ tal que el diagrama*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi"'] & B \\ K(A) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

conmutativo.

Primero daremos resultados de existencia de completación de un semigrupo conmutativo.

Proposición 3.3. *Sea $(A, +)$ un semigrupo abeliano, entonces A posee una completación la que denotaremos por $(K(A), \varphi)$. Además esta es única en el siguiente sentido; si H es un grupo abeliano y $\varphi' : A \to B$ es un homomorfismo de semigrupos, tal que satisfacen la definición, entonces existe un isomorfismo $\alpha : K(A) \to B$ tal que $\varphi' = \alpha \circ \varphi$.*

Demostración. En primera instancia veamos que $(K(A), \dot{+})$ es un grupo abeliano

Buena definición Sea $[a, b] = [a', b']$ y $[c, d] = [c', d']$ entonces $(a, b) \sim (a', b')$ y $(c, d) \sim (c', d')$, luego existen u y v en A tales que $a+b'+u = b+a'+u$ y $c+d'+v = d+c'+v$, por lo tanto

$$a + b' + u + c + d' + v = b + a' + u + d + c' + v,$$

es decir, $a+c+b'+d'+u+v = b+d+a'+c'+u+v$, por lo tanto $(a+c, b+d) \sim (a'+c', b'+d')$. En conclusión

$$[a + c, b + d] = [a' + c', b' + d']$$

Asociatividad Sean $[a, b]$, $[c, d]$ y $[e, f]$ en $K(A)$, entonces

$$\begin{aligned} ([a, b] \dot{+} [c, d]) \dot{+} [e, f] &= [a + c, b + d] \dot{+} [e, f] \\ &= [(a + c) + e, (b + d) + f] \\ &= [a + (c + e), b + (d + f)] \\ &= [a, b] \dot{+} [c + e, d + f] \\ &= [a, b] \dot{+} ([c, d] \dot{+} [e, f]). \end{aligned}$$

Elemento identidad De observar la definición vemos que $[a, b] \dot{+} [t, t] = [a+t, b+t] = [a, b]$, luego $[t, t]$, para t en A es el elemento neutro de $K(A)$.

Elemento inverso Dado $[a, b]$ en $K(A)$ observamos que $[a, b] \dotplus [b, a] = [a+b, a+b] = [t, t]$ entonces el inverso de $[a, b]$ es $[b, a]$.

Ahora solo falta ver que $(K(A), \varphi)$ satisface la propiedad universal, donde $\varphi : A \to K(A)$, $a \mapsto [a + a, a]$. Sea $f : A \to B$ un homomorfismo de monoides.

Existencia definimos como $\bar{f}([a, b]) = f(a) - f(b)$, debemos ver que esta bien definida y es un homomorfismo

Buena definición Sea $[a, b] = [a', b']$ entonces existe un u en A tal que $a + b' + u = b + a' + u$, luego $f(a + b' + u) = f(b + a' + u)$, de este modo, $f(a) + f(b') = f(b) + f(a')$, es decir, $\bar{f}([a, b]) = \bar{f}([a', b'])$.

Homomorfismo Sea $[a, b], [c, d]$, entonces

$$\begin{aligned}
\bar{f}([a, b] \dotplus [c, d]) &= \bar{f}([a + c, b + d]) \\
&= f(a + c) - f(b + d) \\
&= f(a) + f(c) - (f(b) + f(d)) \\
&= f(a) - f(b) + f(c) - f(d) \\
&= f([a, b]) + f([c, d]).
\end{aligned}$$

Para terminar, observe que $\bar{f} \circ \varphi(a) = \bar{f}([a + a, a]) = f(a + a) - f(a) = f(a)$, luego $\bar{f} \circ \varphi = f$ como era lo pedido.

Unicidad suponga que B es un grupo abeliano y $\varphi' : A \to B$ es un homomorfismo de semigrupos tal que para todo grupo abeliano C y todo homomorfismo de semigrupos $f : A \to C$ existe un único homomorfismo de $\bar{f} : B \to C$ tal que $\bar{f} \circ \varphi' = f$, observamos que $\varphi'(A)$ debe generar a B, pues de lo contrario denotamos por $B' =< \varphi'(A) >$ el subgrupo generado por $\varphi'(A)$, de esta manera, se tienen dos homomorfismos $\theta : B \to B \oplus B/B'$ con $(\varphi', 0) = \theta \circ \varphi'$, lo cual contradice la propiedad universal.

Por otro lado, considere el siguiente diagrama

$$\begin{tikzcd}
B \arrow[dr, "\beta"'] & A \arrow[l, "\varphi"'] \arrow[r, "\varphi"] \arrow[d, "\varphi'"'] & B \\
& K(A) \arrow[ur, "\alpha"] &
\end{tikzcd}$$

donde los homomorfismos α y β resultan de la propiedad universal de 3.2 así $\varphi = \beta \circ \varphi'$ y $\varphi' = \alpha \circ \varphi$, por tanto $\alpha \circ \beta \circ \varphi' = \varphi'$, entonces $\alpha \circ \beta$ es la identidad sobre la imagen de φ' y por tanto sobre todo B. De esta forma α es una inversa a izquierda de β. De forma similar $\beta \circ \alpha$ es la identidad sobre todo $K(A)$, de esta forma α tambien es una inversa a derecha de β y α es un isomorfismo.

$\square$

Proposición 3.4. *Sea A un semigrupo abeliano, $(F(A), \dotplus)$ el grupo abeliano libre generado por los elementos de A y $R(A)$ el subgrupo de $F(A)$ generado por los elementos de la forma $a \dotplus b - (a + b)$, con $a, b \in A$. Entonces*

$$K(A) \cong F(A)/R(A)$$

Demostración. Recuerde que $F(A)$ también satisface una propiedad universal (ver [Hun03], capítulo II teorema 1.1) luego por la proposición 3.3 se obtiene el resultado. □

Por tanto, podemos considerar la completación de un semigrupo conmutativo A de dos formas, la primera la cual fue expuesta en 3.3 y la segunda la que se describe en la proposición anterior, las ventajas de tener esta nueva definición se evidencian en la siguiente proposición

Proposición 3.5. *Sea A un monoide abeliano. Entonces*

1. *Cualquier elemento de $K(A)$ puede ser escrito como $[m] - [s]$ para algunos elementos m, s de A*
2. *si a, b están en A, entonces $[a] = [b]$ en $K(A)$ si y solo si $a + c = b + c$ para algún c en A.*
3. *el mapa de monoides $A \times A \to K(A)$, $(a, b) \to [a] - [b]$ es sobreyectivo.*
4. *Suponga que B es un submonoide de A tal que para cualquier a en A existe un b en B tal que $a + b$ pertenece a B, entonces $K(B)$ es un subgrupo de $K(A)$, cualquier elemento de $K(A)$ es de la forma $[m] - [l]$ para m en A y l en B. Si $[a] = [b]$ para cada a, b en M, entonces existe un c en L tal que $a + c = b + c$.*

Demostración.

1. Cualquier elemento de $F(A)$ es una combinación lineal de de las clases

$$\alpha_1[a_1] + \cdots + \alpha_n[a_n]$$

donde α_i esta en $\mathbb{Z}$ y a_i en A, cada coeficiente puede ser transformado en 1 o -1 por separación de los $\alpha_i[a_i]$ en sumas. Adicionando $0 = [a_i] - [a_i]$ con $a_i \in A$ de ser necesario, podemos asumir que 1 y -1 son los coeficientes de la combinación lineal. Por conmutatividad en A y por la relación en $F(A)/R(A)$, un elemento puede ser escrito de la forma

$$[u_1] + \cdots + [u_t] - ([v_1] + \cdots + [v_s]) = [u_1 + \cdots + u_t] - [v_1 + \cdots + v_t]$$

para u_i y v_i en A.

2. Supongamos que $[a] - [b] = 0$ en $K(A)$ entonces, en el grupo abeliano libre $F(A)$ tenemos

$$[a] - [b] = \sum([a_i + b_i] - [a_i] - [b_i]) - \sum([c_j + d_j] - [c_j] - [d_j])$$

la anterior expresión puede ser escrita de la forma

$$[a] \sum([a_i] + [b_i]) + \sum([c_j + d_j]) = [b] + \sum([a_i + b_i] + \sum([c_j] + [d_j])$$

Por otro lado, en un grupo abeliano libre, dos sumas de generadores $\sum[s_i]$ y $\sum[t_j]$ son iguales si y solo si tiene la misma cantidad de términos, tenemos que los generadores difieren por una permutación σ en el sentido en que $t_i = x_{\sigma(i)}$. Así los generados de la anterior ecuación solo difieren por una permutación, esto significa que en A la suma de los términos a derecha e izquierda es la misma, es decir,

$$[a]\sum([a_i]+[b_i])+\sum([c_j+d_j]) = [b]+\sum([a_i+b_i]+\sum([c_j]+[d_j])$$

3. Es consecuencia de 1.

4. Fue desarrollada en la proposiciones 3.1 y 3.3

□

En la practica los monoides conmutativos que se completan poseen una propiedad adicional que motiva las siguientes definiciones.

Definición 3.6. 1. *Sea $(A,+)$ un monoide conmutativo. Decimos que $(A,+)$ satisface la propiedad cancelativa si para todo a,b y c en A se tiene que $a+c=b+c$ implica que $a=b$.*

2. *Sea $(A,+)$ un monoide conmutativo y B un submonoide de A, decimos que B es cofinal si para cualquier a en A existe un b en B tal que $a+b$ están en B.*

Corolario 3.7. *A esta inyectado en $K(A)$ si y solo si M satisface la propiedad cancelativa.*

Proposición 3.8. *Sea A_1 y A_2 dos monoides y $A = A_1 \times A_2$ entonces $K(A) \simeq K(A_1) \oplus K(A_2)$*

Demostración. Sea $(K(A_i), \varphi_i)$, $i = 1,2$ las completaciones de A_1 y A_2 , entonces, luego considere el siguiente diagrama

$$\begin{tikzcd}
A_i \arrow[r, "\iota_i"] \arrow[rr, bend left, "f_i"] \arrow[d, "\varphi_i"] & A \arrow[r, "\varphi"] & K(A) \\
K(A_i) \arrow[urr, "\bar{f}_i"'] & &
\end{tikzcd}$$

donde ι_i es la inclusion de A_i en A, $i = 1,2$ y $(K(A), \varphi)$ es la completación de A, luego $f_i = \varphi \circ \iota_i$ es un homomorfismo de monoides para $i = 1,2$ y por la propiedad de la completación existe un único $\bar{f}_i$ tal que el diagrama conmuta, por otro lado, por la propiedad universal del coproducto en la categoría de grupos abelianos

$$\begin{tikzcd}
 & K(A) & \\
K(A_1) \arrow[ur, "\bar{f}_1"] \arrow[r, "i_1"'] & K(A_1) \oplus K(A_2) \arrow[u, "g"] & K(A_2) \arrow[ul, "\bar{f}_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

donde i_1 y i_2 son los mapas de inclusion, tenemos que existe un único homomorfismo $g : K(A_1) \oplus K(A_2) \to K(A)$ y por la unicidad del teorema 3.3, tenemos que $K(A_1) \oplus K(A_2) \simeq K(A)$ □

3.2 El grupo de Grothendieck y K_0 de un anillo

Recordemos que si $\mathcal{C}$ es una categoría denotamos por $\mathsf{Esq}((\mathcal{C})$ (ver definición A.11) el esqueleto de la categoría

Definición 3.9. *Sea R un anillo, Definimos el grupo K cero de un anillo R, $K_0(R)$ como la completación de semigrupo conmutativo* $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$, *donde* $R-\mathbf{pmod}$ *es la categoria de R-módulos proyectivos finitamente generados.*

Primero, veamos que $\mathsf{Esq}(R - \mathbf{pmod})$ es un conjunto. Como estamos trabajando en la categoría $R - \mathbf{pmod}$ y por 1.31, para cada objeto P de $R - \mathbf{pmod}$ existe un n tal que $P \oplus Q \simeq R^n$ para algún n, $\mathsf{Esq}(R - \mathbf{pmod})$ esta en correspondencia con el conjunto de submódulos que son sumandos directos de R^n para algún n.

Por otro lado si P, Q, S, T son R-módulos proyectivos finitamente generados, $P \simeq S$ y $Q \simeq T$ entonces $P \oplus Q \simeq T$. De este modo $\oplus$ es una operación bien definida sobre $(\mathsf{Esq}(R - \mathbf{pmod})$ y además, tenemos los isomorfismos

$$P \oplus (Q \oplus R) \simeq (P \oplus Q) \oplus R$$
$$P \oplus Q \simeq Q \oplus P$$
$$P \oplus \{0\} \simeq P.$$

De esta forma $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$ es un monoide abeliano. Por otro lado, si R es un anillo conmutativo entonces por 1.32 tenemos que $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$ es un semianillo conmutativo.

En virtud de la proposition 3.4, tenemos que la definición anterior es equivalente a afirmar que que

$$K_0(R) = F((\mathsf{Esq}(R - \mathbf{pmod}), \oplus))/R((\mathsf{Esq}(R - \mathbf{pmod}), \oplus))$$

donde $F(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$ es el grupo abeliano libre con base $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$, notaremos en este punto los elementos de $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$ por $< P >$ y $R(A)$ el subgrupo generado por los símbolos $< P \oplus Q > - < P > - < Q >$.

En $K_0(R)$ tenemos que $[P] + [Q] = [P \oplus Q]$. Pero si consideramos una sucesión exacta

$$0 \to P \to N \to Q \to 0$$

donde P, Q, N, como Q es proyectivo $N \simeq P \oplus Q$.

Teorema 3.10. *Sea R un anillo, entonces $[P] = [Q]$ en $K_0(R)$ si y solo si P y Q son establemente isomorfos.*

Demostración. Si $P \oplus R^n \simeq Q \oplus R^n$ entonces $[P \otimes R^n] = [Q \otimes R^n]$ en $\mathrm{K}_0(R)$ entonces $[P] + [R^n] = [Q] + [R^n]$ y por tanto $[P] = [Q]$.

Por otro lado, trabajando en $F = F(\mathsf{Esq}(R - \mathbf{pmod}), \oplus)$, tenemos que

$$\begin{aligned} < P > - < Q > &= \sum_i < A_i \oplus B_i > - < A_i > - < B_i > \\ &- \sum_j < C_j \oplus D_j > - < C_j > - < D_j > \end{aligned}$$

$$\begin{aligned} < P > + \sum_i < A_i > + < B_i > + \sum_j < C_j \oplus D_j > =&< Q > + \sum_i < A_i \oplus B_i > \\ &+ \sum_j < C_j > + < D_j > \end{aligned}$$

Como F es un grupo abeliano libre, el número de elementos en cada miembro de la igualdad deben ser los mismos. Si tomamos $A = \bigoplus_i A_i$, $B = \bigoplus_i B_i$, $C = \bigoplus_i C_i$ y $D = \bigoplus_i D_i$, tenemos que

$$\begin{aligned} P \oplus A \oplus B \oplus C \oplus D &\simeq Q \oplus A \oplus B \oplus C \oplus D \\ P \oplus M &\simeq Q \oplus M \end{aligned}$$

donde $M = A \oplus B \oplus C \oplus D$. Pero M es un R-módulo proyectivo finitamente generado, luego existe n en $\mathbb{N}$ y un R-módulo N en tal que $M \oplus N \simeq R^n$, de esta manera

$$\begin{aligned} P \oplus M \oplus N &\simeq Q \oplus M \oplus N \\ P \oplus R^n &\simeq Q \oplus R^n \end{aligned}$$

De esta manera P y Q son establemente isomorfos. □

Por otro lado existen condiciones bajo las cuales $\mathrm{K}_0(R) \simeq \mathbb{Z}$

Teorema 3.11. *Sea R un anillos tal que todo R-modulo proyectivo finitamente generado es libre y R posee número de base invariante (ver definición 1.36) entonces $\mathrm{K}_0(R) \cong \mathbb{Z}$.*

Demostración. Dado un R-módulo proyectivo finitamente generado P tenemos que existe un n en $\mathbb{N}$ tal que $P \cong R^n$, entonces $[P] = [R^n] = n[R]$ en $K_0(R)$, luego $[R]$ es un generador de $K_0(R)$, por otro lado si existe un $n[R] = 0$ entonces existe un k en $\mathbb{N}$, tal que $R^n \oplus R^k \cong R^k \oplus 0$ ya que R posee número de base invariante entonces $n + k = k$ es decir $n = 0$. Así observamos que $K_0(R)$ es un conjunto cíclico de orden infinito y por tanto isomorfo a $\mathbb{Z}$. □

La siguiente proposición muestra que $\mathrm{K}_0(\cdot)$ es un funtor

Proposición 3.12. *Sean R, S, T anillos y $f : R \to S$ un homomorfismo de anillos, entonces f induce un homomorfismo de grupos*

$$\begin{aligned} K_0(f) : K_0(R) &\to K_0(S) \\ [P] &\mapsto [P \otimes_f S] \end{aligned}$$

Además,

- *Si* $Id_R : R \to R$ *el homomorfismo identidad, entonces* $K_0(Id_R) = Id_{K_0(R)}$.
- *Si* R,S *y* T *son anillos,* $f : R \to S$ *y* $g : S \to T$ *son homomorfismos de anillos, entonces* $K_0(g \circ f) = K_0(g) \circ K_0(f)$.

Es decir, $K_0(\cdot) : \mathbf{Ani} \to \mathbf{Abe}$ *es un funtor.*

Demostración. Para ver que $\mathrm{K}_0(f)$ es un homomorfismo de grupos, observamos que S puede ser considerado como un R-módulo a derecha definiendo el producto por escalar $S \times R \to S$ por medio de $(s, r) \mapsto sf(r)$. De esta forma, consideramos a S como un $R - S$-bimódulo. Además, para cada R-módulo proyectivo finitamente generado P se puede ver como un $R - \mathbb{Z}$-bimódulo, de esta forma $S \otimes_R P$ es un $S - \mathbb{Z}$-bimódulo por la proposición 1.32. De esta manera $S \otimes_R P$ es un S-módulo. Escribiremos, $S \otimes_f P$ en vez de $S \otimes_R P$.

Como $S \otimes_f R \simeq S$, para $S \to S \otimes_f R$, $s \mapsto s \otimes 1$, tiene inversa inducida por $S \times R \to S$ dado por $(s, r) \mapsto sf(r)$. Si P es un R-módulo proyectivo finitamente generado, entonces existe un R-módulo Q y un n en $\mathbb{N}$ tal que $P \oplus Q \simeq R^n$, entonces

$$\begin{aligned}(S \otimes_f P) \oplus (S \otimes_f Q) &\simeq S \otimes_f (P \oplus Q)\\ &\simeq S \otimes_f R^n\\ &\simeq (S \otimes_f R)^n\\ &\simeq S^n\end{aligned}$$

entonces $S \otimes_f P$ es un S-módulo proyectivo finitamente generado. Para concluir observe que

$$\mathrm{K}_0(f)([P \oplus Q]) = [S \otimes_f (P \oplus Q)] = [(S \otimes_f P) \oplus (S \otimes_f Q)] = \mathrm{K}_0(f)([P]) + \mathrm{K}_0(f)([Q])$$

Por otro lado, si $f = Id_R$, es claro que $K_0(Id_R) = Id_{K_0(R)}$ y si $f : R \to S$ y $g : S \to T$ entonces

$$\mathrm{K}_0(g) \circ \mathrm{K}_0(f)([P]) = \mathrm{K}_0(g)[S \otimes_f P] = [T \otimes_g (S \otimes_f P)]$$

como

$$T \otimes_g (S \otimes_f P) \simeq (T \otimes_g S) \otimes_f P = T \otimes_{g \circ f} P$$

obtenemos que $\mathrm{K}_0(g \circ f) = \mathrm{K}_0(g) \circ \mathrm{K}_0(f)$. ☐

Si R es un anillo conmutativo entonces $(\mathsf{Esq}(R - \mathbf{pmod}), \oplus, \otimes)$ es un semianillo conmutativo y su completación $\mathrm{K}_0(R)$ tiene estructura de anillo conmutativo. La proposición anterior sigue siendo valida y por lo tanto podemos definir el funtor $\mathrm{K}_0(\cdot) : \mathbf{CAni} \to \mathbf{CAni}$.

Corolario 3.13. *Para cada* R, S *de anillos,* $f : R \to S$ *y* $g : S \to R$ *homomorfismos de anillos tales que* $g \circ f = Id_S$*, entonces:*

1. $K_0(f)$ *es un monomorfismo y* $K_0(g)$ *es un epimorfismo.*
2. $K_0(S) = K_0(R) \oplus \ker(K_0(g))$.

Esta propiedad tiene una aplicación al cálculo de $\mathrm{K}_0(RG)$, teniendo en cuenta los homorfisnmos $i : R \to RG$ y $\epsilon : RG \to R$, donde, i es la identificación de R en RG dada por $r \mapsto r1_G$ y ϵ es el homomorfismo de aumentación. Como $\epsilon \circ i = Id_R$ por la proposición anterior

$$\mathrm{K}_0(RG) = \mathrm{K}_0(R) \oplus \ker(\mathrm{K}_0(\epsilon)).$$

Vamos a indagar un poco sobre el comportamiento de $\mathrm{K}_0(f)$ si f es un monomorfismo o un epimorfismo

Proposición 3.14. *Sea $f : R \to S$ un epimorfismo, Entonces $K_0(f) : K_0(R) \to K_0(S)$ esta dado por $[P] \mapsto [\overline{P}]$ donde $\overline{P} = P/JP$, donde $J = \ker f$.*

Demostración. Es inmediata de la observación que $\overline{P} \simeq S \otimes_f P$ por la proposición (1.6). □

Proposición 3.15. *Sea $f : R \to S$ un epimorfismo y $1 + \ker f \subset U(R)$, Entonces $K_0(f) : K_0(R) \to K_0(S)$ es un monomorfismo.*

Demostración. Veamos que ker $\mathrm{K}_0(f)$ es cero. Como todo elemento de $\mathrm{K}_0(R)$ puede ser escrito como $[P]-[Q]$ donde P, Q son R-módulos projectivos finitamente generados, así, $[P]-[Q]$ esta en ker $\mathrm{K}_0(f)$ siempre que $[\overline{P}]-[\overline{Q}] = 0$ Por la proposición 3.14, $\overline{P}$ y $\overline{Q}$ son establemente isomorfos, y por tanto, existe un n tal que $\overline{P} \oplus R^n \simeq \overline{Q} \oplus R^n$. Como $\overline{P \oplus R^n} \simeq \overline{Q \oplus R^n}$, y por la proposición 1.34, tenemos que $P \oplus R^n \simeq Q \oplus R^n$ y por tanto $[P]-[Q] = 0$ en $\mathrm{K}_0(R)$. □

En este punto ya tenemos suficientes propiedades para calcular la K teoría de un buen número de anillos, comenzaremos con los anillos más familiares $\mathbb{Z}$ y $\mathbb{K}[x]$ donde K es un cuerpo.

Teorema 3.16. *Sea R un dominio de ideales principales y sea M un R-módulo finitamente generado. Entonces M es isomorfo a una suma directa de R-módulos cíclicos, es decir,*

$$M \cong R^r \oplus R/(f_1) \oplus \cdots \oplus R/(f_m)$$

para algún $r \geq 0$ y elementos no nulos $f_1, \ldots, f_m$ de R no necesariamente distintos y los cuales no son unidades y los que satisface la relación $f_1|f_2|\cdots|f_m$. El rango n y los ideales $(f_1), (f_2), \ldots, (f_k)$ están únicamente determinados por M.

Demostración. Ver en [Hun03, capítulo IV teorema 6.12] o [DF03, capítulo 12 teoremas 5 y 9.] □

Una consecuencia que tenemos de este teorema es que todo R-módulo finitamente generado es proyectivo siempre que R un dominio de ideales principales. Usando este teorema obtenemos.

Proposición 3.17. *Si R es un dominio de ideales principales, entonces $K_0(R) \cong \mathbb{Z}$.*

Demostración. Por 3.16, Si M es un R-módulo proyectivo finitamente generado, entonces es de la forma

$$M \cong R^n \oplus R/(f_1) \oplus \cdots \oplus R/(f_k)$$

para algunos elementos $f_1, \ldots, f_k$ en R. Además el rango n es determinado únicamente por M. Para cualquier f en R, la multiplicación por izquierda por f induce la siguiente sucesión exacta corta

$$0 \longrightarrow R \xrightarrow{f} R \longrightarrow R/(f) \longrightarrow 0\,.$$

Por tanto $[R] = [R] + [R/(f)]$ en $K(R)$, luego $[R/(f)] = 0$ para cualquier $f \neq 0$, de esto se sigue que $[M] = n[R]$. □

Esto muestra que $K_0(\mathbb{Z})$, $K_0(\mathbb{Z}[i])$, $K_0(\mathbb{K})$, $K_0(\mathbb{K}[G])$ donde G es un grupo cíclico infinito y $K_0(\mathbb{K}[x])$, donde $\mathbb{K}$ es un cuerpo, son isomorfos a $\mathbb{Z}$.

A continuación procederemos a calcular la teoría K de los anillos locales, de forma similar a los dominios de ideales principales. Se puede ver que $R-\mathbf{pmod} = R-\mathbf{fmod}$ siempre que R es un anillo local.

Proposición 3.18. *Si R es un anillo local, entonces $K_0(R) \cong \mathbb{Z}$.*

Demostración. Basta considerar la proyección canónica $\pi : R \to R/J$ donde J es el ideal maximal de R y aplicar la proposición 3.15. □

Proposición 3.19. *Sean S y T anillos entonces $K_0(S \times T) \simeq K_0(S) \oplus K_0(T)$*

Demostración. Teniendo en cuenta que $\mathsf{Esq}(R \times S - \mathbf{pmod}) \simeq \mathsf{Esq}(R - \mathbf{pmod}) \times \mathsf{Esq}(S - \mathbf{pmod})$ como monoides y por la proposición 3.8 obtenemos el resultado. □

Corolario 3.20. *Sea $R = \prod_{i=1}^{n} R_i$ un producto directo de anillos, entonces $K_0(R) = \bigoplus_{i=1}^{n} K_0(R_i)$*

Corolario 3.21. *Sea m un entero positivo, y $m = p_1^{m_1} \cdots p_k^{m_k}$ su representación canónica en factores primos. Entonces por el teorema chino de los restos y las proposiciones anteriores obtenemos*

$$K_0(\mathbb{Z}/(m)) \cong K_0\left(\prod_{i=1}^{k} \mathbb{Z}/(p_i^{m_i})\right) \cong \prod_{i=1}^{k} K_0(\mathbb{Z}/(p_i^{m_i})) \cong \mathbb{Z}^k$$

Una pregunta natural y pertinente al tema de estudio es ¿cuándo RG es un anillo local?. Para ello tenemos el siguiente teorema

Proposición 3.22. *Sea R un anillo y G un grupo*

1. *Si AG es local entonces A es local y G es un p-grupo y p esta en rad R.*

2. *Si A es local, G es un p-grupo localmente finito*[1] *y p esta en rad A entonces RG es local.*

3. *Si G es un grupo abeliano entonces RG es local si y solo si A es local, G es un p-grupo y p esta en rad R.*

Demostración. Ver [Nic72, Teorema] □

Entonces gracias a este teorema tenemos que si $R = \mathbb{Z}_p$ el anillo de enteros p-ádicos y $G = \mathbb{Z}/p^n\mathbb{Z}$ es el grupo cíclico de p^n elementos, entonces $\mathrm{K}_0(RG) \simeq \mathbb{Z}$ para todo $n \geq 1$.

En este punto hemos calculado K_0 de algunos anillos muy conocidos como $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{Z}_{(p)}$, es momento de introducir algunos casos de anillos no conmutativos. Como siempre, partimos de los anillos familiares en este caso el anillo de matrices con coeficientes en un cuerpo, para ello usaremos el concepto de invariancia Morita.

Definición 3.23. *Sean R y S anillos. R y S son Morita equivalentes si las categorías de $R-\mathbf{Mod}$ y $S-\mathbf{Mod}$ son equivalentes, en tal caso, escribimos $R \cong_M S$.*

Un hecho conocido es que R y $M_n(R)$, el anillo de matrices con coeficientes en R, son Morita equivalentes (ver [BK00]).

Teorema 3.24. *$K_0(R)$ es Morita invariante, es decir, si $R \cong_M S$ entonces $K_0(R) \cong K_0(S)$, en particular $K_0(M_n(\mathbb{K})) \cong \mathbb{Z}$.*

Demostración. Ver [Wei13, Capítulo 2] □

El anterior teorema nos da muchas aplicaciones y nos acerca más al objetivo de estudio que es la K teoría algebraica de anillos de grupo y es hora de usar toda la maquinaria desarrollada en el capítulo 1.

Proposición 3.25. *Sea R un anillo semisimple, entonces*

$$K_0(R) \simeq \mathbb{Z}^r$$

para algún r.

Demostración. Como R es semisimple entonces por el teorema de Wedderburn-Artin tenemos que

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times M_{n_3}(D_3) \times \cdots \times M_{n_r}(D_r)$$

Donde $D_1, \ldots, D_r$ son anillos de division, y $n_1, n_2, \ldots, n_r$ son enteros positivos. El número r es únicamente determinado, como las parejas $(n_1, D_1), \ldots, (n_r, D_r)$ (salvo permutación), De este modo

$$\begin{aligned}
\mathrm{K}_0(R) &\simeq \mathrm{K}_0(M_{n_1}(D_1) \times M_{n_2}(D_2) \times M_{n_3}(D_3) \times \cdots \times M_{n_r}(D_r)) \\
&\simeq \mathrm{K}_0(M_{n_1}(D_1)) \oplus \mathrm{K}_0(M_{n_2}(D_2)) \oplus \mathrm{K}_0(M_{n_3}(D_3)) \oplus \cdots \oplus \mathrm{K}_0(M_{n_r}(D_r)) \\
&\simeq \mathrm{K}_0(D_1) \oplus \mathrm{K}_0(D_2) \oplus \mathrm{K}_0(D_3) \oplus \cdots \oplus \mathrm{K}_0(D_r) \\
&\simeq \mathbb{Z}^r
\end{aligned}$$

□

[1] Un grupo G es localmente finito si para cualquier subgrupo finitamente generado H entonces H es finito.

Veamos una aplicación de esta proposición. Sea $R = \mathbb{C}S_3$. donde S_3 es el grupo de permutaciones de 3 elementos. Por 1.77 tenemos que R es semisimple, además

$$\mathbb{C}S_3 \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}).$$

De esta manera

$$\mathrm{K}_0(\mathbb{C}S_3) \simeq \mathbb{Z}^3.$$

Para concluir esta sección, veremos que 3.25 tiene una interpretación en términos de la teoría de representaciones, esta presentación esta basada en el texto [FH99]

Definición 3.26 (Anillo de representación)**.** *Sea G un grupo finito. Denotamos por F el grupo abeliano libre generado por todas las clases de isomorfismo de representaciones de G, y R el subgrupo generado por todos los elementos de la forma $V \oplus W - V - W$, entonces $R(G) = F/G$ es llamado el anillo de representaciones de G.*

Otra forma de considerar a $R(G)$ es como le conjunto de todas las combinaciones lineales de la forma $\sum a_i V_o$ de todas las representaciones irreducibles de G. La estructura de anillo para $R(G)$ esta dada por el producto tensorial, definida sobre los generadores de $R(G)$ y extendida por linealidad.

Dada una representación V de un grupo G siempre es posible asociar una función de la forma

$$\begin{aligned} \chi_V : G &\to \mathbb{C} \\ g &\mapsto \mathrm{Tr}(g : V \to V) \end{aligned}$$

En este contexto χ_V es llamado un carácter de G. De lo anterior observe que $\chi_V(g) = \chi_V(hgh^{-1})$ para todo h en G. Es decir, χ_V es constante sobre las clases de conjugación de G. Este tipo de funciones se llaman funciones de clase

Definición 3.27. *Sea G un grupo finito. Denotamos por $\mathbb{C}_{class}$ el conjunto de todas las funciones de clase sobre G.*

Proposición 3.28. *El número de representaciones irreducibles de G es igual al número de clases de conjugación de G. Equivalentemente, sus caracteres $\{\chi_V\}$ forman una base ortonormal de $\mathbb{C}_{class}(G)$.*

Demostración. [FH99, Lectura 2,Proposicion 2.30] □

De esta manera, si G es un grupo finito. Tenemos que

$$\mathrm{K}_0(\mathbb{C}G) \simeq \mathbb{Z}^c,$$

donde c es el número de clases de conjugación de G.

Pese a lo que hemos hecho en la presente sección, el cálculo de $\mathrm{K}_0(RG)$ es un problema abierto en el caso general, es más, existe una conjetura al respecto.

Conjetura 3.29 (Farell - Jones para $K_0(\cdot)$)**.** *Sea G un grupo libre de torsion y sea R un anillo regular*[2]*. Entonces la aplicación inducida en $K_0(\cdot)$ por el homomorfismo $i : R \to RG$ es biyectiva.*

Adicionalmente, existe una relación entre esta conjetura y la conjetura de Kaplansky. en este punto solo la presentamos y remitimos al lector a la referencia.

Teorema 3.30. *Sea G un grupo y R un anillo tal que sus idempotentes son triviales. Suponga que*

$$K_0(R) \otimes_{\mathbb{Z}} \mathbb{Q} \to K_0(RG) \otimes_{\mathbb{Z}} \mathbb{Q}$$

es un isomorfismo. Entonces 0 y 1 son los únicos idempotentes en RG siempre que una de las siguientes condiciones se satisface:

1. *R es un cuerpo de característica cero.*
2. *RG es establemente finito*
3. *R es un anillo de division y G es sofic.*

Demostración. Ver [BLR08, Teorema 1.12] □

3.3 El grupo de Whitehead y $K_1(R)$ de un anillo

Sea R un anillo (siempre con unidad), $e_1, \ldots, e_n$ (notados como vectores columna) la base canónica de R^n, $GL_n(R)$ el grupo de de unidades de $M_n(R)$ y $GL(R) = \varinjlim GL_n(R)$.

Definición 3.31. *Una matriz M en $GL_n(R)$ es llamada elemental si es de la forma $I_n + \alpha e_{ij}$ donde I_n es la matriz identidad, $e_{ij} = e_i e_j^t$, $1 \leq i \neq j \leq n$, donde e_i y e_j son los vectores de la base canónica de R^n* [3] *y α en R.*

Si denotamos por E_n el subgrupo generado por todas las matrices elementales, vemos que $E_n \subseteq GL_n(R)$. Otra construcción asociada a $E_n(R)$ es considerar el sistema inductivo $\{E_i, \varphi_{ij} | i, j\}$ donde

$$\begin{aligned} \varphi_{n,n+1} : E_n &\to E_{n+1} \\ A &\mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

y su limite inductivo $E(R) = \varinjlim E_n$, claramente $E(R)$ es un subgrupo de $GL(R)$,

Lema 3.32 (Whitehead)**.** *Si R es un anillo, entonces $E(R) = [GL(R), GL(R)]$.*

[2]Decimos que un anillo R es regular si es Noetheriano y cualquier R-módulo finitamente generado M posee una resolución proyectiva finita

[3]otra forma de ver esta situación es, e_{ij} es la matriz cuyas entradas son nulas salvo la entrada de la fila i y columna j la cual es 1

Demostración. Observamos que $e_{ij}e_{kl} = (e_i e_j^t)(e_k e_l^t) = e_i(e_j^t e_k)e_l^t$ pero $e_j^t e_k$ es el producto interno entre e_j y e_k el cual solo puede ser 1 o 0, de esta manera,

$$e_{ij}e_{kl} = \begin{cases} 0, & \text{si } j \neq k; \\ e_{il}, & \text{si } j = k. \end{cases}$$

también tenemos que si $i \neq j$ entonces

$$\begin{aligned}(I_n + \alpha e_{ij})(I_n - \alpha e_{ij}) &= (I_n + \alpha e_i e_j^t)(I_n - \alpha e_i e_j^t) \\ &= I_n - \alpha e_i e_j^t + \alpha e_i e_j^t - \alpha^2 (e_i e_j^t)(e_i e_j^t) \\ &= I_n - \alpha^2 (e_i e_j^t)(e_i e_j^t) \\ &= I_n\end{aligned}$$

de esta manera $(I_n + \alpha e_i e_j^t)^{-1} = I_n - \alpha e_i e_j^t$, y usando estos cálculos podemos probar que

$$\begin{aligned}[I_n + \alpha e_{ik}, I_n + e_{kj}] &= (I_n + \alpha e_{ik})(I_n + e_{kj})(I_n - \alpha e_{ik})(I_n - e_{kj}) \\ &= (I_n + \alpha e_{ik} + e_{kj} + \alpha e_{ij})(I_n - \alpha e_{ik})(I_n - e_{kj}) \\ &= (I_n + \alpha e_{ik} + e_{kj} + \alpha e_{ij} - \alpha e_{ik})(I_n - e_{kj}) \\ &= (I + e_{kj} + a e_{ij})(I_n - e_{kj}) \\ &= I_n + \alpha e_{ij},\end{aligned}$$

siempre que $k \neq i$ y $k \neq j$. Por tanto $I_n + \alpha e_{ij} = [I_n + \alpha e_{ik}, I_n + e_{kj}]$. Esto muestra que $E(R) \subseteq [GL(R), GL(R)]$. Por otro lado, si $A \in GL_n(R)$ entonces

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -A^{-1} & I_n \end{pmatrix} \begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$

Luego $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ pertenece a $E_{2n}(R)$. Considerando A, B en $GL(R)$, existe un n tal que A, B en $GL_n(R)$. Entonces

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & B^{-1}A^{-1} \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix}$$

De esta manera $[GL(R), GL(R)] \subset E(R)$. □

Corolario 3.33. *Si* $n \geq 3$ $[E_n(R), E_n(R)] = SL_n(R)$

Definición 3.34. *Sea R un anillo con unidad, entonces $K_1(R) = GL(R)/E(R)$.*

A diferencia de lo expuesto de $\mathrm{K}_0(R)$, $\mathrm{K}_1(R)$ ha surgido de la abelianización de $GL(R)$ y por decirlo de una manera, de *"Matrices"*, entonces si consideramos a A en $GL_m(R)$ y B en $GL_n(R)$ tenemos que A y B representan la misma clase en $\mathrm{K}_1(R)$ si y solo si B puede ser obtenida de A por medio de la siguientes operaciones

1. Operaciones elementales entre filas

2. Operaciones elementales entre columnas

3. Si B es de la forma $\begin{pmatrix} A & 0 \\ 0 & I_r \end{pmatrix}$ donde I_r es la matriz identidad de $r \times r$ para algún r.

Estas observaciones nos dicen que $K_1(R) \simeq \{0\}$ si y solo si cualquier matriz de $GL_n(R)$ puede ser reducida en una secuencias de las anteriores operaciones. En conclusion el cociente $GL(R)/E(R)$ mide la obstrucción que poseen las matrices con coeficientes en R al ser reducidas por medio de operaciones elementales.

Análogamente al estudio de $\mathrm{K}_0(R)$, podemos observar que $\mathrm{K}_1(R)$ posee propiedades similares, es decir, es un funtor entre **Ani** y **Abe**, el cual, en algunos textos es conocido con el funtor Bass-Whitehead.

Proposición 3.35. *Sea $f : R \to S$ un homomorfismo de anillos. Entonces este induce un homomorfismo entre grupos abelianos $K_1(f) : K_1(R) \to K_1(S)$.*

Demostración. Teniendo en cuenta que $f : R \to S$ induce un homomorfismo de grupos $GL(f) : GL(R) \to GL(S)$ y por 1.59 y tenemos que la asignación $K_1(R) : GL(R)/E(R) \to GL(S)/E(S)$ esta bien definida. □

Proposición 3.36. *Sea R un anillo, entonces $K_1(M_n(R)) \simeq K_1(R)$.*

Demostración. Como ya hemos visto $GL(M_n(R)) \simeq GL(R)$, el cual se extiende a un isomorfismo entre $K_1(M_n(R))$ y $K_1(R)$. □

Proposición 3.37. *Sea R y S anillos y $R \times S$ el anillo con las operaciones coordenada a coordenada, entonces $K_1(R \times S) \simeq K_1(R) \oplus K_1(S)$.*

Demostración. Teniendo en cuenta que $GL(R \times S) \simeq GL(R) \times GL(S)$ la prueba es similar a la anterior. □

Supongamos por un momento que R es un anillo conmutativo y sea $U(R)$ las unidades de R. Para cada n en $\mathbb{N}$, tomamos

$$\det_n : GL_n(R) \to U(R)$$

y teniendo en cuenta el sistema directo de $GL(R)$, $\{GL_i(R), \varphi_{ij} | i, j \in \mathbb{N}\}$ tenemos que

$$\begin{tikzcd} GL_i(R) \arrow[dd, "\varphi_{ij}"'] \arrow[dr, "\det_i"] & \\ & U(R) \\ GL_j(R) \arrow[ur, "\det_j"'] & \end{tikzcd}$$

Es un diagrama conmutativo, y por tanto induce un homomorfismo de grupos

$$\det : GL(R) \to U(R)$$

Tenemos que $E(R) \subseteq SL(R) = \ker \det$ y por tanto det induce un homomorfismo entre $\mathrm{K}_1(R)$ y $U(R)$

Definición 3.38. *Sea R un anillo conmutativo, denotaremos por $SK_1(R)$ al cociente $SL(R)/E(R)$.*

Para cada anillo conmutativo R podemos considerar la sucesión exacta de grupos abelianos

$$0 \longrightarrow U(R) = GL_1(R) \xrightarrow{\varphi_1} K_1(R) \xrightarrow{\det} U(R) \longrightarrow 0\,.$$

Luego, tenemos que $K_1(R) \simeq U(R) \oplus SK_1(R)$

Proposición 3.39. *Sea $\mathbb{K}$ un cuerpo conmutativo de característica 0, entonces $K_1(\mathbb{K}) \simeq U(\mathbb{K})$*

Demostración. Recordemos un resultado de álgebra lineal: toda matriz invertible sobre $\mathbb{K}$ de determinante 1 es producto de matrices elementales, esto es $E_n(\mathbb{K}) = SL_n(\mathbb{K})$ y por tanto $K_1(R) \simeq U(R)$ □

El resultado anterior admite una generalización

Proposición 3.40. *Si R un anillo local, entonces $K_1(R) \simeq U(R)$.*

Demostración. Ver [Sri07, Capítulo 1,ejemplo 1.6] □

Proposición 3.41. *Sea $\mathbb{K}$ un cuerpo de característica cero y G un grupo finito tal que su orden es una unidad en $\mathbb{K}$, entonces*

$$K_1(\mathbb{K}G) \simeq \prod_{i=1}^{r} U(\mathbb{D}_i),$$

para algún r en $\mathbb{N}$, y algunos anillos de division $D_1, \ldots, D_r$

Demostración. Por el teorema de Weddeburn-Artin tenemos que

$$\mathbb{K}G \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times M_{n_3}(D_3) \times \cdots \times M_{n_r}(D_r),$$

donde $D_1, \ldots, D_r$ son anillos de division, y $n_1, n_2, \ldots, n_r$ son enteros positivos. El número r es únicamente determinado, como las parejas $(n_1, D_1), \ldots, (n_r, D_r)$ (salvo permutación), entonces

$$\begin{aligned}
\mathrm{K}_1(\mathbb{K}G) &\simeq \mathrm{K}_1(M_{n_1}(D_1) \times M_{n_2}(D_2) \times M_{n_3}(D_3) \times \cdots \times M_{n_r}(D_r)) \\
&\simeq \mathrm{K}_1(M_{n_1}(D_1)) \oplus \mathrm{K}_1(M_{n_2}(D_2)) \oplus \mathrm{K}_1(M_{n_3}(D_3)) \oplus \cdots \oplus \mathrm{K}_1(M_{n_r}(D_r)) \\
&\simeq \mathrm{K}_1(D_1) \oplus \mathrm{K}_1(D_2) \oplus \mathrm{K}_1(D_3) \oplus \cdots \oplus \mathrm{K}_1(D_r) \\
&\simeq \prod_{i=1}^{r} U(D_i).
\end{aligned}$$

□

En general, el cálculo de $K_1(RG)$ donde R es un anillo y G es un grupo, es mucho más difícil que en el caso de $K_0(RG)$, como se puede evidenciar en [Kuk00, capitulos 1 y 2],

Apéndices

Apéndice A

Teoría de Categorías

Esta sección se ha basado en los siguientes textos [BK00], [Awo10], [Mit65]y [Pop73]. Iniciaremos introduciendo los objetos fundamentales de la teoría de categorías y seguidamente definiremos algunos tipos particulares, como son las categorías aditivas y abelianas estas ultimas serán de utilidad en la K teoría algebraica.

A.1 Categorías y Funtores

Definición A.1. *Una categoría $\mathcal{C}$ esta definida por la siguiente información:*

1. *Una clase Ob C, cuyos elementos se denominan los objetos de $\mathcal{C}$*

2. *Para cada par de objetos A, B en Ob C un conjunto $Mor_{\mathcal{C}}(A,B)$ cuyos elementos son llamados morfismos entre A y B. La unión*

$$Mor\,(\mathcal{C}) = \bigcup_{(A,B)} Mor_{\mathcal{C}}(A,B)$$

donde (A,B) recorre la clase Ob $C \times$ Ob C es denominada la clase de morfismos de $\mathcal{C}$.

3. *Para cada terna de objetos A, B y C en Ob C, existe una función $\theta(A,B,C)$ denominada el mapa de composición*

$$\theta(A,B,C) : Mor_{\mathcal{C}}(A,B) \times Mor_{\mathcal{C}}(B,C) \to Mor_{\mathcal{C}}(A,C),$$

la imagen de la pareja (f,g) respecto a $\theta(A,B,C)$ se denomina Composición y la denotaremos por $g \circ f$, y satisface las siguientes propiedades

   (a) Dados f en $Mor_{\mathcal{C}}(A,B)$, g en $Mor_{\mathcal{C}}(B,C)$ y h en $Mor_{\mathcal{C}}(C,D)$ se tiene que

$(h \circ g) \circ f = h \circ (g \circ f)$, *es decir, el siguiente diagrama*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "g\circ f"'] \arrow[drr, bend left=60, "(h\circ g)\circ f"] \arrow[drr, bend right=60, "h\circ(g\circ f)"'] & B \arrow[d, "g"] \arrow[dr, "h\circ g"] & \\
& C \arrow[r, "h"] & D
\end{tikzcd}$$

es conmutativo

(b) *Para cada* A *en* $Ob\ C$ *existe un morfismo* i_A *en* $Mor_{\mathcal{C}}(A, A)$ *tal que*

$$i_A \circ f = f \qquad g \circ i_A = g$$

para todo f *en* $Mor_{\mathcal{C}}(B, A)$ *y* g *en* $Mor_{\mathcal{C}}(A, B)$

Por otro lado, si para una categoría $\mathcal{C}$ se tiene que Ob C es un conjunto, decimos que $\mathcal{C}$ es una categoría pequeña.

Ejemplos.

- **Conj** *denota la categoría de los conjuntos cuyos objetos son conjuntos y sus morfismos son funciones entre un par de conjuntos, es decir*

$$Ob\ \mathbf{Conj} = \{\text{Clase de todos los conujuntos}\}$$
$$Mor_{\mathbf{Conj}}(A, B) = \{\text{conjunto de todas las funciones entre } A \text{ y } B\}$$

- **Grp**, *denota la categoría de los grupos cuyos objetos son conjuntos y sus morfismos son homomorfismos de grupos entre un par de grupos.*

- **Ani** *denota la categoría de los anillos cuyos objetos son anillos y sus morfismos son homomorfismo de anillos entre un par de anillos.*

- $R-$**Mod** *para cualquier anillo* R*, denota la categoría de los módulos a izquierda sobre un anillo* R *cuyos objetos son módulos a izquierda y sus morfismos son homomorfismos de módulos entre un par de módulos.*

- **Top** *denota la categoría de espacios topológicos cuyos objetos son espacios topológicos y sus morfismos son funciones continuas entre un par de espacios topológicos.*

Los ejemplos anteriores tienen la característica que los objetos son conjuntos con propiedades adicionales. No todas las categorías son de esta forma, para ilustrar este hecho veamos los siguientes ejemplos

- *Sea* (X, τ) *es un espacio topológico, definimos la categoría* $\mathbf{Top}(X)$*, con la siguiente información*

$$Ob\ \mathbf{Top}(X) = \tau$$

Para cada U, V *en* Ob $\mathbf{Top}(X)$

$$Mor_{\mathbf{Top}(X)}(U,V) = \begin{cases} \{i\}, & Si\ U \subseteq V; \\ \emptyset, & Si\ U \subsetneq V, \end{cases}$$

donde $i : U \to V$, *es la inclusion.*

- *Sea* G *un grupo, denotamos por* $G_\circ$ *la categoría formada por la siguiente información*

$$Ob\ G_\circ = \{\circ\}$$
$$Mor_{G_\circ}(\circ, \circ) = G,$$

donde la ley de composición es la operación del grupo.

- *Sea* R *un anillo, Denotamos por* $Mat(R)$ *la categoría formada por la siguiente información*

$$Ob\ Mat(R) = \mathbb{N}$$

Para cada n, m *en Ob Mat(R) definimos*

$$Mor_{Mat(R)}(n,m) = M_{n\times m}(R)$$

Donde $M_{n\times m}(R)$ *es el anillo de matrices de* $n \times m$ *con coeficientes en* R, *y la composición es el producto de matrices.*

Definición A.2. *Sean* $\mathcal{C}$ *y* $\mathcal{D}$ *categorías, decimos que* $\mathcal{D}$ *es una subcategoría de* $\mathcal{C}$ *si satisface las siguientes condiciones*

1. $Ob\ D \subseteq Ob\ C$.

2. *Para cada* A, B *en* $Ob\ D$ *tenemos que* $Mor_{\mathcal{C}}(A,B) \subseteq Mor_{\mathcal{C}}(A,B)$

3. *La composición de morfismo en* $\mathcal{D}$ *es la inducida por la composición de los morfismos en* $\mathcal{C}$

4. *Para cada* A *en* $\mathcal{D}$ *tenemos que el morfismo identidad es el mismo morfismo identidad de la categoría* $\mathcal{C}$,

Ejemplos.

- *Sea* **Abe** *la categoría formada por todos los subgrupos abelianos. Esta es una subcategoría de* **Grp**.

- *Sea* **CAni** *la categoría formada por todos los anillos conmutativos. Esta es una subcategoría de* **Ani**.

- *Sea* R *un anillo, la categoría* $R - \mathbf{mod}$ *formada por todos los* R*-módulos finitamente generados. Es una subcategoría de* $R - \mathbf{Mod}$.

- *Sea R un anillo, la categoría $R-$* **Fmod** *formada por todos los R-módulos libres. Es una subcategoría de $R-$* **Mod**.
- *De forma similar, se pueden definir la categoría $R-$***Pmod** *de todos los R-módulos proyectivos.*
- *la categoría $R-$* **Fmod** *posee una subcategoría que denotaremos por $R-$* **fmod** *conformada por todos los R-módulos libres finitamente generados.*
- *De forma similar, la categoría $R-$* **Pmod** *posee una subcategoría $R-$* **pmod** *conformada por todos los R-módulos proyectivos finitamente generados.*

Definiremos el concepto de funtor entre dos categorías.

Definición A.3. *Sean $\mathcal{C}$ y $\mathcal{D}$ categorías, un funtor covariante (respectivamente contravariante) $F : \mathcal{C} \to \mathcal{D}$ esta definido por*

1. *Una función $F : Ob\ C \to Ob\ D$.*
2. *Para cada par de objetos A, B de $Ob\ C$ se define una función denotada por $F(A, B) : Mor_{\mathcal{C}}(A, B) \to Mor_{\mathcal{D}}(F(A), F(B))$, respectivamente*

$$F(A, B) : Mor_{\mathcal{C}}(A, B) \to Mor_{\mathcal{D}}(F(B), F(A));$$

tal que si escribimos $F(f)$ para $F(A, B)(f)$, tenemos que cumple las siguientes condiciones:

   (a) $F(i_A) = i_F(A)$,

   (b) $F(g \circ f) = F(g) \circ F(f)$, *(respectivamente $F(g \circ f) = F(f) \circ F(g)$).*

para cualesquiera morfismos f, g compatibles para la composición y para cada objeto B de $\mathcal{D}$.

En el presente documento la palabras funtor siempre significara funtor covariante. A continuación damos algunos ejemplos

Ejemplo. 1. *Sea $\mathcal{C}$ una categoría denotamos por $Id_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ el funtor obtenido de la siguiente forma: Para cualquier objeto X de $\mathcal{C}$, $Id_{\mathcal{C}}(X) = X$ y para cada f en $Mor_{\mathcal{C}}(X, Y)$, $Id_{\mathcal{C}}(f) = f$, este funtor es llamado “el funtor identidad de $\mathcal{C}$”.*

2. *Sea $S :$* **Top** $\to$ **Conj** *el funtor obtenido de la siguiente forma: Para cualquier (X, τ) en* **Top** *$S(X) = X$ y para cualquier (X, τ) y (Y, σ) en* **Top** *y f en $Mor_{\mathbf{Top}}(X, Y)$, definimos $S(f) = f$ la función correspondiente, S es un funtor llamado “el funtor olvido”*

3. *Sea $c :$* **Grp** $\to$ **Abe** *definido por la siguiente asignación, si G esta en* **Grp** *entonces $c(G) = G/G'$ donde G' es el subgrupo conmutador de G (ver 1.59), y si G, H están en* **Grp**.

Definición A.4. *Sea $\mathcal{C}$ y $\mathcal{D}$ dos categorías y F, G dos funtores entre $\mathcal{C}$ y $\mathcal{D}$, Una transformación natural*[1] *$T : F \to G$ asigna a cada objeto X de $\mathcal{C}$ un morfismo $T_X : F(X) \to G(X)$ en $\mathcal{D}$, tal que para cada morfismo f en $Mor_{\mathcal{C}}(X, Y)$, tenemos que el siguiente diagrama*

$$\begin{tikzcd} F(X) \arrow[r, "F(f)"] \arrow[d, "T_X"'] & F(Y) \arrow[d, "T_Y"] \\ G(X) \arrow[r, "G(f)"'] & G(Y) \end{tikzcd}$$

es conmutativo, es decir, $T_Y \circ F(f) = G(f) \circ T_X$.

El concepto de transformación natural nos permitirá hablar de la equivalencia entre dos categorías.

Definición A.5. *Sea $\mathcal{C}$ y $\mathcal{D}$ dos categorías y F, G, H funtores entre $\mathcal{C}$ y $\mathcal{D}$, $T : F \to G$ y $K : G \to H$ dos transformaciones naturales,*

1. *La composición de T y K la que denotamos por $K \circ T$ como la transformación natural definida para cada objeto por $(K \circ T)_X = K_X \circ T_X$.*
2. *Decimos que $T : F \to G$ es un isomorfismo natural si existe una transformación natural $T^{-1} : G \to F$ tal que $T \circ T^{-1} = Id_G$ y $T^{-1} \circ T = Id_F$*
3. *Decimos que dos categorías son naturalmente equivalentes si existe un isomorfismo natural entre ellas.*

A.2 Objetos especiales y morfismos

Definición A.6. *Sea $\mathcal{C}$ una categoría y f en $Mor_{\mathcal{C}}(A, B)$*

1. *f es llamado un monomorfismo si $fu = fv$ implica que $u = v$ para cualquier par de morfismos u, v en $Mor_{\mathcal{C}}(X, A)$ y para cualquier X en $Ob\ C$.*
2. *f es llamado un epimorfismo si $uf = vf$ implica que $u = v$ para cualquier par de morfismos u, v en $Mor_{\mathcal{C}}(B, X)$ y para cualquier X en $Ob\ C$.*
3. *f es un bimorfismo si f es un monomorfismo y un epimorfismo.*
4. *f es una retracción si existe un morfismo g en $Mor_{\mathcal{C}}(B, A)$ tal que $fg = I_B$.*
5. *f es una sección si existe un morfismo g en $Mor_{\mathcal{C}}(B, A)$ tal que $gf = I_A$.*
6. *f es un isomorfismo si f es una retracción y una sección.*

[1] También es llamado morfismo funtorial

Un hecho que se debe tener en cuenta y que diferencia la teoría de categorías del álgebra usualmente conocida es el uso que le da a la palabra epimorfismo (Homomorfismo sobreyectivo), monomorfismo (Homomorfismo inyectivo) e isomorfismo (Homomorfismo biyectivo). Por ejemplo, en **Ani** existen epimorfismos que son inyectivos, por ejemplo la inclusion de $\mathbb{Z}$ en $\mathbb{Q}$ o la inclusion de $\mathbb{Q}$ en $\mathbb{R}$ como morfismo en la categoría de espacios Hausdorff, es un epimorfismo pero no es un homomorfismo sobreyectivo.

Definición A.7. *Sea $\mathcal{C}$ una categoría. Decimos que $\mathcal{C}$ es una categoría balanceada si todo bimorfismo es un isomorfismo.*

Un ejemplo de una categoría balanceada es $R-\mathbf{Mod}$.

Proposición A.8. *Sea $\mathcal{C}$ una categoría y f en $Mor_{\mathcal{C}}(A,B)$*

1. *Si f es una retracción entonces f es un epimorfismo.*
2. *Si f es una sección entonces f es un monomorfismo.*
3. *Si f es una retracción (o una sección) y es también un monomorfismo (o epimorfismo) entonces f es un isomorfismo.*

Ahora veremos a un objeto A de una categoría en función de su conjunto de morfismo $\mathrm{Mor}_{\mathcal{C}}(A,X)$ donde X varia en $\mathrm{Ob}\,\mathcal{C}$

Definición A.9. *Sea $\mathcal{C}$ una categoría y A en $Ob\,\mathcal{C}$*

1. *X es un objeto inicial si para cualquier B en $Ob\,(C)$ se tiene que $Mor_{\mathcal{C}}(X,B)$ posee un solo elemento.*
2. *X es un objeto final si para cualquier A en $Ob\,(C)$ se tiene que $Mor_{\mathcal{C}}(A,X)$ posee un solo elemento.*
3. *X es un objeto cero de $Ob\,(C)$ si es un objeto inicial y final.*

Es claro que si $\mathcal{C}$ tiene un objetos inicial, final o cero, entonces estos son únicos salvo isomorfismo, Por otro lado si A y B están en $\mathrm{Ob}\,\mathcal{C}$ y $\mathcal{C}$ posee un objeto cero (el cual denotamos por 0) considere

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend left, "0_{AB}"] & 0 \arrow[r, "g"] & B \end{tikzcd}$$

tenemos que f y g son únicas ya que 0 es un objeto cero, por tanto $g \circ f$ es única. Esta aplicación se llama el morfismo cero y la denotamos por 0_{AB}.

Proposición A.10. *Sea $\mathcal{C}$ una categoría, y considere la relación sobre $Ob\,\mathcal{C}$:*

$$A \simeq B \text{ si y solo si existe un isomorfismo } f \text{ en } Mor_{\mathcal{C}}(A,B).$$

Entonces $\simeq$ es una relación de equivalencia.

Demostración. Ejercicio al lector. (tener en cuenta las definiciones en A.6) □

Definición A.11. *Sea $\mathcal{C}$ una categoría*

1. *La clase de equivalencia del objeto A bajo la relación descrita en la proposición A.10 es llamado el tipo de A y es denotada por $[A]$.*

2. *El conjunto de todos los tipos de de la categoría $\mathcal{C}$ es llamado el esqueleto de la categoría $\mathcal{C}$ y es denotado por $\mathsf{Esq}(\mathcal{C})$.*

3. *Decimos que la categoría $\mathcal{C}$ posee un esqueleto pequeño si $\mathsf{Esq}(\mathcal{C})$ es un conjunto.*

A.3 Operaciones entre objetos

En esta sección daremos unas técnicas para crear nuevos objetos y morfismos en una categoría a partir de otros. Una de las primeras construcciones que podemos tratar de replicar son las que nos da la teoría de conjuntos.

Definición A.12. *Sea $\mathcal{C}$ una categoría y A, B en $Ob\,\mathcal{C}$ tal que*

1. *Si α en $Mor_{\mathcal{C}}(A, B)$ es un monomorfismo A es llamado un subobjeto de B. y α es llamada la inclusion de A en B. Si α no es un isomorfismo, decimos que A esta contenido propiamente en B.*

2. *Si α en $Mor_{\mathcal{C}}(A, B)$ es un epimorfismo A es llamado un objeto cociente de A.*

3. *Un objeto X es el producto de A y B, denotado $A \prod B$ si y solo si existe morfismos $\pi_1 : X \to A$, $\pi_2 : X \to B$, llamadas proyecciones canónicas tal que para cualquier otro objeto Y y un par de morfismos $f_1 : Y \to A$, $f_2 : Y \to B$ existe un único morfismo $f : Y \to X$ tal que el siguiente diagrama conmuta:*

$$\begin{tikzcd} & Y \arrow[dl, "f_1"'] \arrow[d, "f"] \arrow[dr, "f_2"] & \\ A & A \prod B \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & B \end{tikzcd}$$

4. *Un objeto X es la suma directa (o coproducto) de A y B, denotado $A \coprod B$ si y solo si existe morfismos $i_1 : A \to X$, $i_2 : B \to X$, llamadas inclusiones canónicas tal que para cualquier otro objeto Y y un par de morfismos $f_1 : A \to Y$, $f_2 : B \to Y$ existe un único morfismo $f : X \to Y$ tal que el siguiente diagrama conmuta:*

$$\begin{tikzcd} & Y & \\ A \arrow[ur, "f_1"] \arrow[r, "i_1"'] & A \coprod B \arrow[u, "f"] & B \arrow[ul, "f_2"'] \arrow[l, "i_2"] \end{tikzcd}$$

Las anteriores son un intento por tener las operaciones de teoría de conjuntos en una categoría arbitraria.

Definición A.13. *Sea $\mathcal{C}$ una categoría y A, B en $Ob\,\mathcal{C}$ tal que*

1. *Sea f, g en $Mor_{\mathcal{C}}(A, B)$, decimos que u en $Mor_{\mathcal{C}}(K, A)$ es un igualador para f y g si*

   (a) $f \circ u = g \circ u$.

   (b) *Si existe u' en $Mor_{\mathcal{C}}(K', A)$ con $f \circ u' = g \circ u'$, entonces existe un único h en $Mor_{\mathcal{C}}(K', K)$ tal que el siguiente diagrama*

$$\begin{tikzcd}
& K' \arrow[dl, "h"'] \arrow[dr, "u'"] & & \\
K \arrow[rr, "u"'] & & A \arrow[r, shift left] \arrow[r, shift right] & B
\end{tikzcd}$$

   conmuta.

2. *Sea f, g en $Mor_{\mathcal{C}}(A, B)$, decimos que v en $Mor_{\mathcal{C}}(B, H)$ es un coigualador para f y g si*

   (a) $v \circ f = v \circ g$.

   (b) *Si existe v' en $Mor_{\mathcal{C}}(B, H')$ con $v' \circ f = v' \circ g$, entonces existe un único t en $Mor_{\mathcal{C}}(H, H')$ tal que el siguiente diagrama*

$$\begin{tikzcd}
& & H' & \\
A \arrow[r, shift left] \arrow[r, shift right] & B \arrow[ur, "v'"] \arrow[rr, "v"'] & & H \arrow[ul, "t"']
\end{tikzcd}$$

   conmuta.

3. *Sea f en $Mor_{\mathcal{C}}(A, B)$ y $\mathcal{C}$ una categoría con objeto cero. Se denomina núcleo de f al igualador de f y 0_{AB}.*

4. *Sea f en $Mor_{\mathcal{C}}(A, B)$ y $\mathcal{C}$ una categoría con objeto cero. Se denomina conúcleo de f al coigualador de f y 0_{AB}.*

A.4 Categorías Aditivas y Abelianas

Daremos la definición de una categoría preaditiva, aditiva y abeliana, esta última es importante en K teoría algebraica.

Definición A.14. *Sea $\mathcal{C}$ una categoría. Decimos que $\mathcal{C}$ es preaditiva si satisface la siguientes condiciones:*

1. *Para cualquier pareja de objetos A, B en $Ob\,\mathcal{C}$, $Mor_{\mathcal{C}}(A, B)$ tiene estructura de grupo abeliano.*

2. *La estructura de grupo abeliano en $Mor_{\mathcal{C}}(A, B)$ es tal que el mapa de composición*
$$\theta(A, B, C) : Mor_{\mathcal{C}}(A, B) \times Mor_{\mathcal{C}}(B, C) \to Mor_{\mathcal{C}}(A, C)$$
es bilineal, es decir, para f, f' en $Mor_{\mathcal{C}}(A, B)$ y g, g' en $Mor_{\mathcal{C}}(B, C)$, se tiene que
$$\theta(A, B, C)(f + f', g) = \theta(A, B, C)(f, g) + \theta(A, B, C)(f', g) \quad (A.1)$$
$$\theta(A, B, C)(f, g + g') = \theta(A, B, C)(f, g) + \theta(A, B, C)(f, g + g') \quad (A.2)$$
para cualquier A, B, C en $Ob\,\mathcal{C}$.

Unas observaciones derivadas de la definición.

- Si denotamos por $\theta(A, B, C)(f, g) = g \circ f$ entonces las ecuaciones A.1 toman la forma
$$g \circ (f + f') = g \circ f + g \circ f'$$
$$(g + g') \circ f = g \circ f + g' \circ f$$
- Para cualquier par de objetos (A, B) de $\mathcal{C}$ denotamos el elemento neutro de $\mathrm{Mor}_{\mathcal{C}}(A, B)$ por 0_{AB}, entonces para cualquier terna de objetos (A, B, C) de $\mathcal{C}$ tenemos que $0_{BC} \circ 0_{AB} = 0_{AC}$, de este modo, para cualquier f en $\mathrm{Mor}_{\mathcal{C}}(A, B)$ tenemos que
$$0_{BC} \circ (0_{AB} + f) = 0_{BC} \circ f = 0_{AC} = 0_{BC} \circ 0_{AB} + 0_{BC} \circ f$$
- Si $\mathcal{C}$ posee un objeto cero, entonces por definición $\mathrm{Mor}_{\mathcal{C}}(0, A)$ solo contiene un elemento 0_{0A}, y claramente para cualquier pareja A, B de objetos de $\mathcal{C}$ tenemos que $0_{AB} = 0_{0B} \circ 0_{A0}$.

Definición A.15. *Sea $\mathcal{C}$ una categoría preaditiva, entonces $\mathcal{C}$ es una categoría aditiva si para cada par de objetos A, B existe su suma directa $A \coprod B$.*

Definición A.16. *Sea $\mathcal{C}$ una categoría aditiva en la cual*

1. *Para cada par de objetos A y B en $\mathcal{C}$ y f en $Mor_{\mathcal{C}}(A, B)$ entonces existe el núcleo y conúcleo de f.*
2. *Cualquier monomorfismo es un núcleo y cualquier epimorfismo es un conúcleo.*

Entonces $\mathcal{C}$ es llamada una categoría abeliana.

Existen diferentes definiciones de categorías abelianas. En [Pop73, Capítulo 2] se discuten la gran mayoría de ellas. Para terminar este anexo introduciremos el teorema de sumergimiento de Freyd-Mitchell.

Teorema A.17 (Teorema del sumergimiento de Freyd-Mitchell)**.** *Si $\mathcal{C}$ es una categoría abeliana pequeña, entonces existe R en* **Ani** *y un funtor exacto y plenamente fiel entre $\mathcal{C}$ y $R-$***Mod** *el cual sumerge a $\mathcal{C}$ como una subcategoria plena en el sentido que*
$$Hom_{\mathcal{C}}(M, N) \simeq Hom_{R-\mathbf{Mod}}(M, N).$$

Demostración. Ver [Fre66,] (todo el libro esta dedicado a la prueba de este teorema). □

En consecuencia, podemos asumir que toda categoría abeliana pequeña *esta contenida* en una categoría de módulos sobre un anillo.

Apéndice B

Subgrupos aditivos de los racionales

En este apéndice nos proponemos estudiar los subgrupos del grupo aditivo de los números racionales $(\mathbb{Q},+)$, y poderlos clasificar. Esto fue estudiado en [BZ51] y aquí presentaremos una construcción alterna, inspirada de [Kur60b, pag. 49]. Recordemos que si $a_1,\ldots,a_n$ son números enteros, entonces su máximo común divisor es denotado por $(a_1,\ldots,a_n)$ y su mínimo común múltiplo como $[a_1,\ldots,a_n]$. Remitimos al lector que desconozca sus propiedades a consultar cualquier libro de teoría de números, por ejemplo, [NZM91]

Por otro lado no es difícil encontrar subgrupos de $(\mathbb{Q},+)$ que no sean cíclicos, por ejemplo

- Sea $G=\{a/2^j|a,j\in Z\}$ (el grupo Diádico racional) es un subgrupo de $(\mathbb{Q},+)$ pero no es cíclico. Si G es generado por una fracción $a/2^j$, no existiría un entero m tal que
$$\frac{1}{2^{j+1}}=m\frac{a}{2^j}.$$
- Sea $H=\{a/b|a\in\mathbb{Z}, b \text{ es un entero libre de cuadrados}\}$. H es un subgrupo de $(\mathbb{Q},+)$ y tampoco es un subgrupo cíclico ya que no es finitamente generado.

Sea G un subgrupo de $(\mathbb{Q},+)$, como $\mathbb{Q}$ es contable, tenemos que podemos enumerar los elementos de G, sea $G=\{x_1,x_2,\ldots,x_n,\ldots\}$ una enumeración de los elementos de G, luego, definimos los subgrupos $G_i=<x_1,x_2,\ldots,x_i>$ generados por los primeros i elementos de G bajo la enumeración escogida. De esta manera, obtenemos la siguiente cadena ascendente de grupos

$$G_1\subseteq G_2\subseteq G_3\subseteq\cdots\subseteq G_m\subseteq\cdots \tag{B.1}$$

Claramente, esta cadena se puede expresar en términos de un sistema inductivo en la categoría de grupos, $(G_i,\varphi_{i,j})$ donde $\varphi_{i,i+1}:G_i\to G_{i+1}$ es la inclusion, de esta manera, $S=\varinjlim G_i$. En este punto podemos esperar dos situaciones

1. La cadena B.1 se estabiliza, es decir, existe un m en $\mathbb{N}$ tal que $G_m=G_k$ para todo $k\geq m$, de este modo podemos concluir que S es finitamente generado

2. La cadena B.1 no se estabiliza.

Si estamos en la primera situación, tenemos el siguiente resultado

Proposición B.1. *Sea $S = \langle x_1, \ldots, x_n \rangle$ un grupo finitamente generado de $(\mathbb{Q}, +)$. Entonces S es cíclico.*

Demostración. Escribimos $x_i = a_i/b_i$ y consideramos $r = a/b$ donde $a = (a_1, \ldots, a_n)$ y $b = [b_1, \ldots, b_n]$. De esta manera, tenemos que existen enteros m_i, tales que $x_i = m_i r$ y por tanto $\langle x_1, \ldots, x_n \rangle \subseteq < r >$, por otro lado, vemos que $\langle x_1, \ldots, x_n \rangle$ es un subgrupo de un grupo cíclico, luego el también lo es. ☐

Solo nos queda analizar la segunda situación,

Proposición B.2. *Si G es un subgrupo de $(\mathbb{Q}, +)$ y G no es finitamente generado, entonces existe a en $\mathbb{N}$ y una sucesion de enteros $n_0, n_1, \ldots, n_m$ tal que*

$$G = \left\{ \frac{ma}{n_0 \cdot n_1 \cdots n_k} | m \in \mathbb{Z}, k \in \mathbb{N} \right\}$$

Demostración. Si G no es finitamente generado, la cadena (B.1) no se estabiliza, pero teniendo en cuenta B.1, ésta esta compuesta de grupos cíclicos, es decir,

$$\langle y_1 \rangle \subseteq \langle y_2 \rangle \subseteq \langle y_3 \rangle \subseteq \cdots \subseteq \langle y_m \rangle \subseteq \cdots , \tag{B.2}$$

donde $y_i = a_i/b_i$ con $(a_i, b_i) = 1$, sin perdida de generalidad podemos suponer que $a_i > 0$ para todo i en $\mathbb{N}$. Como $\langle y_i \langle \subseteq \rangle y_{i+1} \rangle$ entonces existe un entero m_i tal que $y_i = m_i y_{i+1}$ y de esta forma tenemos la ecuación

$$b_{i+1} a_i = m_i a_{i+1} b_i, \tag{B.3}$$

y de este forma, $b_i | b_{i+1} a_i$. Pero $(a_i, b_i) = 1$ entonces $b_i | b_{i+1}$, y por lo tanto existe un entero n_i tal que $b_{i+1} = n_i b_i$. Reemplazando en (B.3), obtenemos

$$n_i a_i = m_i a_{i+1}. \tag{B.4}$$

Como $(a_{i+1}, b_{i+1}) = 1$, tenemos que $(a_{i+1}, n_i) = 1$ y por (B.4) tenemos que $a_{i+1} | n_i a_i$. De este modo $a_{i+1} | a_i$, y si consideramos al sucesión de números enteros $a_1, a_2, \ldots, a_n, \ldots$ observamos que es decreciente, y por tanto existe un j en $\mathbb{N}$ tal que $a_j = a_k$ para todo $k \geq j$, De los $a_1, a_2, \ldots, a_j$ podemos escoger el mínimo de ellos, sea a_k dicho entero $a_1, a_2, \ldots, a_k, \ldots, a_j$ de esta forma la condición $a_{k+1} | a_k$ es imposible entonces podemos reducir aun mas la cadena, eliminando los términos mayores que a_k. Se concluye en este caso que $a_k = a_1 = a_2 = \ldots$.

En definitiva si llamamos a el mínimo de la sucesión de la sucesión $\{a_i\}$ y $b_1 = n_0$ la cadena se transforma en

$$\langle a/n_0 \rangle \subseteq \langle a/(n_0 \cdot n_1) \rangle \subseteq \langle a/(n_0 \cdot n_1 \cdot n_2) \rangle \subseteq \cdots \subseteq \langle a/(n_0 \cdot n_1 \cdot n_2) \cdot \cdots \cdot n_m \rangle \subseteq \cdots . \tag{B.5}$$

observe que a es primo relativo con todos los n_k, de esta manera, la sucesión $n_0, n_1, \ldots, n_m, \ldots$ esta formada por primos relativos dos a dos y como S es la union de todos estos subgrupos encajados, tenemos el resultado. ☐

Con esto hemos clasificado todos los grupos de $(\mathbb{Q}, +)$. Por otro lado, si comparamos esta presentación con la realizada en [BZ51], vemos que los autores comienzan fijando una enumeración de los números primos (orden natural) desde un inicio a diferencia de nosotros que comenzamos enumerando los elementos del subgrupo y esa numeración es la que fijamos. Luego ellos definen diversos subgrupos de $(\mathbb{Q}, +)$ y su clasificación consiste en mostrar que ellos son los únicos.

Bibliografia

[AM73] Michael Atiyah and Igor Macdonald. *Introducción al álgebra conmutativa*. Reverte, Barcelona, 1973.

[Awo10] Steve Awodey. *Category Theory*. Oxford University Press, 2 edition, 8 2010.

[Bas73] Hyman Bass, editor. *Algebraic K-Theory I. Proceedings of the Conference Held at the Seattle Research Center of Battelle Memorial Institute, August 28 - September 8, 1972: Higher K-Theories (Lecture Notes in Mathematics)*. Springer, 1st ed. 1973. 2nd printing 1986 edition, 1 1973.

[Bas76] Hyman Bass. Euler characteristic and characters of discrete groups. *Inventiones mathematicae*, 35:155–196, 1976.

[BK00] A. J. Berrick and M. E. Keating. *Categories and Modules with K-Theory in View*. Cambridge University Press, 1 edition, 6 2000.

[BLR08] Arthur Bartels, Wolfgang Lück, and Holger Reich. On the Farrell–Jones conjecture and its applications. *Journal of Topology*, 1(1):57–86, 2008.

[Bou70] N. Bourbaki. *Algèbre: Chapitres 1 à 3*. Springer; Réimpression inchangée de la 2e éd. 1970 edition (2006-12-11), 1970.

[BZ51] Ross A. Beaumont and H. S. Zuckerman. A characterization of the subgroups of the additive rationals. *Pacific J. Math.*, 1(2):169–177, 1951.

[DF03] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3 edition, 7 2003.

[Edw73] Formanek Edward. Idempotent in noetherian group rings. *Canadian journal of mathematics*, XXV(2):366–369, 1973.

[Emm01] Ioannis Emmmanouil. Projective modules, augmentation and idempotent in group ring. *Journal of Pure and Applied Algebra*, 1(158):161–160, 2001.

[Emm05] Ioannis Emmanouil. *Idempotent Matrices over Complex Group Algebras*. Springer, 2005.

[FH99] William Fulton and Joe Harris. *Representation Theory: A First Course*. Springer, corrected edition, 7 1999.

[Fre66] Peter Freyd. *Abelian Categories*. Joanna Cotler Books, international edition edition, 12 1966.

[Hun03] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer, 8 edition, 2 2003.

[Ina10] Hvedri Inassaridze. *Algebraic K-Theory*. Springer, softcover reprint of hardcover 1st ed. 1995 edition, 12 2010.

[Kap57] I. Kaplansky. Problems in the theory of rings. In Albert A. A., editor, *Linear Algebras*, number 502. National Academy of Sciences - National Research Council, 1957.

[Kap70] Irving Kaplansky. Problems in the theory of rings revisited. *Amer. Math: Mounthly*, 77:445–454, 1970.

[Kuk00] Aderemi Kuku. *Representation Theory and Higher Algebraic K-Theory*. Chapman and Hall/CRC, 1 edition, 1600.

[Kur60a] A. G. Kurosh. *Theory of Groups*, volume 2. American Mathematical Society, 2nd revised edition edition, 1 1960.

[Kur60b] A. G. Kurosh. *Theory of Groups*, volume 1. American Mathematical Society, 2nd revised edition edition, 1 1960.

[Lam01] Tsi-Yuen Lam. *A First Course in Noncommutative Rings*. Springer, 2nd edition, 6 2001.

[LP96] Soo Teck Lee and Judith A. Parker. The cohomology of the integer Heisenber group. *Journal of Algebra*, 184:230–250, 1996.

[LS75] TY Lam and MK Siu. K0 and K1–An introduction to algebraic K-theory. *American Mathematical Monthly*, 1(1):329–364, 1975.

[Mag10] Bruce A. Magurn. *An Algebraic Introduction to K-Theory*. Cambridge University Press, 1 edition, 2 2010.

[Mil72] John Milnor. *Introduction to Algebraic K-Theory*. Princeton University Press, first edition edition, 1 1972.

[Mit65] Barry Mitchell. *Theory of categories*. Academic Press, first edition edition, 10 1965.

[MS08] César Polcino Milies and Sudarshan Sehgal. *An Introduction to Group Rings*. Springer, softcover reprint of the original 1st ed. 2002 edition, 5 2008.

[Nic72] WK Nicholson. Local group rings. *Canadian Mathematical Bulletin*, 15(1):137–138, 1972.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley, 5 edition, 1 1991.

[Pas11] Donald S. Passman. *The Algebraic Structure of Group Rings*. Dover Publications, reprint edition, 9 2011.

[Pop73] M. Popescu. *Abelian Categories with Applications to Rings and Modules*. London Mathematical Society Monographs. Academic Press Inc, 12 1973.

[Rob95] Derek Robinson. *A Course in the Theory of Groups*. Springer, 2nd edition, 10 1995.

[Ros95] Jonathan Rosenberg. *Algebraic K-Theory and Its Applications*. Number 147 in Graduate Texts in Mathematics. Springer, 1st ed 1994. corr. 2nd printing 1995 edition, 12 1995.

[Seh78] Sudarshan K. Sehgal. *Topics in Group Rings*. Marcel Dekker Inc, 0 edition, 6 1978.

[Ser03] Jean-Pierre Serre. *Trees*. Springer, 1st ed. 1980. corr. 2nd printing 2002 edition, 1 2003.

[Sil81] J.R. Silvester. *Introduction to Algebraic K-Theory*. Chapman and Hall/CRC, 1st edition edition, 6 1981.

[Sri07] Vasudevan Srinivas. *Algebraic K-Theory*. (Modern Birkhäuser Classics). Birkhäuser, 2nd edition, 11 2007.

[Wei13] Charles A. Weibel. *The K-Book: An Introduction to Algebraic K-Theory*. American Mathematical Society, 6 2013.