Algunas consideraciones sobre la estructura algebraica de las funciones aritméticas

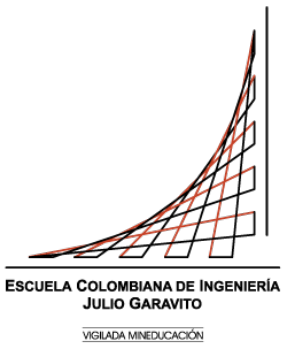
Trabajo de Grado

Autor:

Juan Esteban
LÓPEZ ARÉVALO

Dirigido por:

PhD. Julián Andrés
AGREDO ECHEVERRY



Programa de Matemáticas
UNIVERSIDAD ESCUELA COLOMBIANA DE
INGENIERÍA JULIO GARAVITO

NOVIEMBRE DE 2023

Resumen

Este documento se enfoca en el estudio de algunas estructuras y propiedades algebraicas fundamentales de la teoría de anillos en el conjunto de las funciones con dominio en los números naturales (sin el 0) a cualquier anillo, dotándolas de dos operaciones, la suma heredada de la estructura del anillo y la convolución de Drirchlet como producto. La primera parte del documento abordara algunos conceptos básicos de la teoría de grupos y anillos, además de definir el conjunto objetivo de estudio; se explorarán algunas propiedades heredadas del anillo sobre el cual toman valores las funciones, así como generalizaciones de funciones conocidas. La segunda parte del documento consistirá en el análisis de los ideales en el anillo de las funciones $R-$aritméticas, su relación con los ideales del anillo R y la existencia de los divisores de cero. Finalmente, se estudiarán algunas propiedades de los polinomios con coeficientes en las funciones $R-$aritméticas.

Palabras clave: Funciones aritméticas, Funciones R-aritméticas

Abstract

This document focuses on the study of some fundamental algebraic structures and properties of ring theory within the set of functions with a domain in the natural numbers (excluding 0) to any ring, equipping them with two operations: the sum inherited from the ring structure and the Dirichlet convolution as the product.

The first part of the document will address some basic concepts of group and ring theory, in addition to defining the target set of study; it will explore some properties inherited from the ring over which the functions take values, as well as generalizations of known functions.

The second part of the document will consist of the analysis of ideals in the ring of R-arithmetic functions, their relationship with the ideals of the ring R, and the existence of zero divisors.

Finally, some properties of polynomials with coefficients in R-arithmetic functions will be studied.

Key words: Funciones R-atitmeticas

Introducción

Las funciones del conjunto de números naturales al cuerpo de números complejos (funciones aritméticas) se han mostrado de especial importancia en distintas áreas de las matemáticas, especialmente la teoría de números y la variable compleja; por lo que se ha visto importante el estudio de tanto las estructuras algebraicas que estas tienen como las propiedades de los polinomios con coeficientes en este conjunto de funciones. En el trabajo se realiza un estudio de algunas estructuras algebraicas al cambiar el conjunto de llegada por cualquier anillo.

Índice

1. Preliminares

A continuación se presentan resultados y definiciones de Álgebra abstracta que se usaran con frecuencia durante el desarrollo de este trabajo. En esta sección se introducen los conceptos básicos y se enuncian algunos resultados, por lo general, sin incluir demostraciones. Se recomienda que para profundizar en estos tópicos ver [5], [4]

1.1. Concepto de semigrupo, grupo, anillo y cuerpo.

A continuación hacemos un repaso de algunas estructuras algebraicas importantes que emplearemos.

Definición 1.1. ***Operación binaria*** *Sea A un conjunto no vació. Una operación binaria en A es una función*

$$(\cdot) : A \times A \to A.$$

Una operación binaria sobre un conjunto A se dice

- *Asociativa, si para todo $a, b, c \in A$,*
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
- *Conmutativa, si para todo $a, b \in A$,*
$$a \cdot b = b \cdot a$$

Definición 1.2. *Sea S un conjunto con una operación binaria, $(\cdot) : S \times S \to S$. Un* ***elemento identidad*** *de S es un elemento $e \in S$ tal que $e \cdot x = x \cdot e = x$, para todo $x \in S$.*

Nota 1.1. *Sea S un conjunto con una operación binaria, $(\cdot) : S \times S \to S$. Si S tiene elemento identidad este es único. En efecto, sean $u, e \in S$ elementos identidad en S. Entonces, para todo $x, y \in S$ se cumple $x = x \cdot u = u \cdot x$ y $y = e \cdot y = y \cdot e$. En particular para $x = e$ y $y = u$, así $u = e \cdot u = e$.*

Definición 1.3. ***Semigrupos y monoides*** *Un semigrupo es una pareja ordenada $(S, \cdot)$ de un conjunto no vació S y una operación binaria asociativa $(\cdot)$ definida en S. Un semigrupo con elemento identidad es un monoide.*

Definición 1.4. ***Grupo*** *Un grupo es una pareja ordenada $(G, \cdot)$ de un conjunto no vació G y una operación binaria $(\cdot)$ en G tal que*

1. *La operación es asociativa.*
2. *G tiene un elemento identidad con la operación definida.*
3. *Todo elemento $a \in G$ tiene un inverso. Es decir, existe $a' \in G$ tal que*
$$a \cdot a' = a' \cdot a = e$$
donde e es la identidad (a' se suele escribir como a^{-1} si el grupo se usa con notación multiplicativa y $-a$ si se usa con notación aditiva).

Un grupo en el que además se cumple que su operación es conmutativa es llamado un grupo abeliano o grupo conmutativo.

Nota 1.2. *El elemento identidad para anillos con notación multiplicativa se suele escribir como 1, y cuando se usa notación aditiva se escribe como 0.*

Definición 1.5. *Un **subgrupo** de un grupo $(G, \cdot)$ es un subconjunto de G que hereda la estructura de grupo de $(G, \cdot)$.*

Nota 1.3. *Un subconjunto H de G es un **subgrupo** del grupo $(G, \cdot)$ si y solo si cumple*

1. *Si 1 es el elemento identidad de $(G, \cdot)$, $1 \in H$;*
2. *$x \in H$ implica $x^{-1} \in H$;*
3. *$x, y \in H$ implica $xy \in H$.*

Definición 1.6. ***Anillo*** *Un anillo es una tripleta $(R, +, \cdot)$ de un conjunto R no vació y dos operaciones binarias en R, una adición $+$ y otra multiplicación $\cdot$, tal que*

1. *$(R, +)$ es un grupo abeliano;*
2. *La operación $\cdot$ es asociativa;*
3. *La multiplicación distribuye sobre la suma. Es decir, para $a, b, c \in R$,*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Un anillo se dice conmutativo si la operación $(\cdot)$ es conmutativa
Si un anillo tiene identidad para la operación $(\cdot)$, se dice que es un anillo con identidad.

Definición 1.7. ***Dominio de integridad*** *Un dominio de integridad es un anillo conmutativo $(R, +, \cdot)$ para el cual $a, b \neq 0$ implica $ab \neq 0$.*

Definición 1.8. ***Cuerpo*** *Un cuerpo es un dominio de integridad $(R, +, \cdot)$ en el que $(R \setminus \{0\}, \cdot)$ es un grupo.*

Cuando las operaciones bajo las que $(R, +, \cdot)$ es un anillo o $(G, \cdot)$ es un grupo sean claras, se escribe simplemente el conjunto. Es decir, R y G en lugar de $(R, +, \cdot)$ y $(G, \cdot)$ respectivamente.

1.2. Ideales y homomorfismos

Definición 1.9. *Un **Homomorfismo** de un anillo R en un anillo S es una aplicación $\varphi : R \to S$ que preserva la suma y el producto. Es decir,*

- *Para todo $x, y \in R$, $\varphi(x + y) = \varphi(x) + \varphi(y)$*
- *Para todo $x, y \in R$, $\varphi(xy) = \varphi(x)\varphi(y)$*

*Si φ es inyectiva, se le llama un **monomorfismo**, si es sobreyectiva, un **epimorfismo**; y si es biyectiva un **isomorfismo***

Nota 1.4. *Un homomorfismo entre anillos con identidad preserva la identidad. Es decir, si R y S son anillos con identidad y $\varphi : R \to S$ un homomorfismo, $\varphi(1) = 1$.*

Definición 1.10. ***Ideales*** *Un ideal de un anillo R es un subgrupo I de $(R, +)$ tal que $x \in I$ implica $x \cdot y, y \cdot x \in I$ para todo $y \in R$. Un ideal es propio si $I \neq R$.*

Nota 1.5. *Los ideales se pueden entender como subgrupos que admiten multiplicación, si esta es en solo uno de los dos lados tenemos los siguientes casos*

- *Si se cumple que $y \in R$ y $x \in I$ implica $y \cdot x \in I$, I es llamado un ideal a izquierda.*

- *Si se cumple que $y \in R$ y $x \in I$ implica $x \cdot y \in I$, I es llamado un ideal a derecha.*

Definición 1.11. ***Ideal primo*** *Un ideal primo de un anillo conmutativo R es un ideal $I \neq R$ tal que $xy \in I$ implica $x \in I$ o $y \in I$.*

Definición 1.12. ***Ideal Maximal*** *Un ideal maximal de un anillo R es un ideal $M \neq R$ de R tal que no existe ideal I de R tal que $M \subsetneq I \subsetneq R$*

Definición 1.13. ***Anillo local*** *Un anillo se dice local cuando solo tiene un ideal maximal.*

Definición 1.14. ***Series de potencia formales*** *Sea R un anillo con identidad y $M = \{1, X, X^2, ...\}$ el monoide con la operación binaria,*

$$X^i \cdot X^j \to X^{i+j}$$

Una serie de potencias formal $A = \sum_{n=0}^{\infty} a_n X^n$ en la indeterminada X sobre el anillo R es una función $A : M \to R$ definida por $X^n \to a_n$.
Las series de potencia son sumadas punto a punto,

$$A + B = C \text{ donde } c_n = a_n + b_n \text{ para todo } n \in \mathbb{N}$$

La multiplicación definida por

$$AB = C \text{ donde } c_n = \sum_{k=0}^{n} a_k b_{n-k} \text{ para todo } n \in \mathbb{N}$$

Con estas operaciones el conjunto de series de potencias sobre indeterminada X, $R[\![X]\!]$; es un anillo.

1.3. Funciones Aritméticas

En esta sección hablaremos sobre el objeto central de estudio de este trabajo, las funciones aritméticas. El enfoque clásico de las funciones aritméticas recae sobre los complejos, en este trabajo haremos un enfoque novedoso y mas general sobre un anillo R arbitrario. Mas precisamente:

Definición 1.15. (Funciones R-aritméticas) *Sea R un anillo. Entonces, toda función $f : \mathbb{N} \to R$ la llamaremos función R-aritmética. El conjunto de funciones R-aritméticas lo notaremos por $\mathcal{A}(R)$; en el caso en que $R = \mathbb{C}$, f sera una función aritmética y notaremos $\mathcal{A}(\mathbb{C})$ como $\mathcal{A}$.*

A partir de este punto siempre que nos refiramos a R estaremos hablando de algún anillo.

Definición 1.16. *(***Convolución de Dirichlet)** *Definamos la operación $*$ sobre $\mathcal{A}(R)$, de forma que $* : \mathcal{A}(R) \times \mathcal{A}(R) \to \mathcal{A}(R)$*

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d)$$

También es usual ver la definición de la siguiente mannera,

$$(f * g)(n) = \sum_{ab=n} f(a) g(b)$$

Donde la suma es sobre $\{(a, b) \in \mathbb{N}^2 : ab = n\}$

Proposición 1.1. *La convolución de Dirichlet $*$ es asociativa.*

Demostración. Sean $f, g, h \in \mathcal{A}(R)$ y $n \in J$. Como la convolución es una suma finita sobre un anillo

$$(f * (g * h))(n) = \sum_{a|n} f(a)(g * h)(n/a)$$

$$= \sum_{a|n} \sum_{bc=\frac{n}{a}} f(a)g(b)h(c)$$
$$= \sum_{x \in A_n} x$$

donde $A_n = \{f(a)g(b)h(c) : a|n,\ bc = \frac{n}{a}\}$ luego

$$(f * (g * h))(n) = \sum_{abc=n} f(a)g(b)h(c),$$

pues que $A_n = \{f(a)g(b)h(c) : abc = n\}$.

Por otro lado

$$((f * g) * h)(n) = \sum_{c|n} (f * g)(n/c)h(c)$$
$$= \sum_{c|n} \sum_{ab=\frac{n}{c}} f(a)g(b)h(c)$$
$$= \sum_{x \in B_n} x$$

donde $B_n = \{f(a)g(b)h(c) : c|n,\ ab = \frac{n}{c}\}$ y como este conjunto es igual a $\{f(a)g(b)h(c) : abc = n\}$. Por lo tanto

$$((f * g) * h)(n) = \sum_{abc=n} f(a)g(b)h(c)$$

Así $((f * g) * h)(n) = (f * (g * h))(n)$ para todo $n \in J$. Luego $(f * g) * h = f * (g * h)$ □

Proposición 1.2. *La convolución de Dirichlet $*$ distribuye sobre la suma punto a punto.*

Demostración. Sean $f, g, h \in \mathcal{A}(R)$. Entonces, si $n \in J$,

$$\begin{array}{ll} & ((f+g) * h)(n) \\ = & \quad \langle \text{ Definición de } * \rangle \\ & \sum_{ab=n} (f+g)(a)h(b) \\ = & \quad \langle \text{ Definición de la suma puntual} \rangle \\ & \sum_{ab=n} (f(a)+g(a))h(b) \\ = & \quad \langle \text{ R es un anillo, luego el producto distribuye sobre la suma} \rangle \\ & \sum_{ab=n} f(a)h(b) + g(a)h(b) \\ = & \quad \langle \text{ R es un anillo, luego la suma es asociativa} \rangle \\ & \sum_{ab=n} f(a)h(b) + \sum_{ab=n} g(a)h(b) \\ = & \quad \langle \text{ Definición de convolución} \rangle \\ & (f * h)(n) + (g * h)(n) \end{array}$$

Luego, $(f + g) * h = f * h + g * h$. De manera análoga se demuestra $f * (g + h) = f * g + f * h$ □

Como resultado de las dos proposiciones anteriores se puede hacer la siguiente afirmación.

Teorema 1.1. *$\mathcal{A}(R)$ con la suma punto a punto y la convolución de Dirichlet es el anillo $(\mathcal{A}(R), +, *)$.*

Unas preguntas que surgen acerca del anillo $\mathcal{A}(R)$ es ¿Cuáles son las condiciones necesarias y suficientes para que este tenga unidad? y ¿Cuáles para que sea conmutativo?.

Proposición 1.3. *$\mathcal{A}(R)$ es conmutativo si y solo si R es conmutativo.*

Demostración. Supongamos que R es conmutativo. Si $f, g \in \mathcal{A}(R)$, entonces

$$\begin{aligned}
& (f*g)(n) \\
= & \quad \langle \text{ Defínción convolución de Dirichlet } \rangle \\
& \sum_{ab=n} f(a)g(b) \\
= & \quad \langle \text{ R es conmutativo } \rangle \\
& \sum_{ab=n} g(b)f(a) \\
= & \quad \langle\ ab = n \equiv ba = n\ \rangle \\
& \sum_{ba=n} g(b)f(a) \\
= & \quad \langle \text{ Definición de Convolución de Dirichlet } \rangle \\
& (g*f)(n)
\end{aligned}$$

Ahora, si R no es conmutativo, existen $x, y \in R$ tales que $xy \neq yx$. Luego, sean $f, g \in \mathcal{A}(R)$ definidas por

$$f(n) = \begin{cases} x & si \quad n = 1 \\ \\ 0 & si \quad n > 1 \end{cases}$$

$$g(n) = \begin{cases} y & si \quad n = 1 \\ \\ 0 & si \quad n > 1. \end{cases}$$

Entonces, $(f*g)(1) = xy \neq yx = (g*f)(1)$, lo que implica $g*f \neq f*g$. Así, $\mathcal{A}(R)$ no es conmutativo. Por lo tanto $\mathcal{A}(R)$ es conmutativo si y solo si R lo es. □

Proposición 1.4. *$\mathcal{A}(R)$ tiene elemento unidad si y solo si R tiene elemento unidad.*

Demostración. Sea R un anillo con elemento unidad, 1. La función $R-$aritmética,

$$\delta(n) = \begin{cases} 1 & si \quad n = 1 \\ \\ 0 & si \quad n > 1 \end{cases}$$

cumple que para todo $f \in \mathcal{A}(R)$,

$$\begin{aligned}
(f*\delta)(n) &= \sum_{ab=n} f(a)\delta(b) \\
&= \sum_{ab=n, b\neq 1} f(a)\delta(b) + f(n)\delta(1) \\
&= f(n)
\end{aligned}$$

Pues, para todo $b \neq 1$, $\delta(b) = 0$. Luego, $f*\delta = f$. De forma análoga se demuestra que $\delta * f = f$. Por lo tanto, la función δ es la unidad en $\mathcal{A}(R)$.

Ahora, si $\mathcal{A}(R)$ tiene como elemento unidad γ, entonces para todo $x \in R$ la función $x\delta * \gamma = x\delta = \gamma * x\delta$; donde

$$x\delta(n) = \begin{cases} x & Si \quad n = 1 \\ \\ 0 & Si \quad n > 1 \end{cases}$$

Entonces, $x\gamma(1) = (x\delta * \gamma)(1) = x\delta(1) = x$ y de manera análoga $\gamma(1)x = x$. Así $\gamma(1)$ es el elemento unidad de R. Por lo tanto, R es un anillo con unidad. □

A partir de ahora si $x \in R$, cuando escribamos $x\delta$ nos referimos a la función R-aritmética,

$$x\delta(n) = \begin{cases} x & Si \quad n = 1 \\ \\ 0 & Si \quad n > 1. \end{cases}$$

Definición 1.17. *Sea $S \subset \mathcal{A}(R)$. Entonces, el conjunto $1(S) = \{f(1) | f \in S\}$ lo llamaremos el conjunto de primeros valores de S.*

Definición 1.18. *Sea $S \subset R$. Entonces, el conjunto $F(S) = \{f \in \mathcal{A}(R) | f(1) \in S\}$ lo llamaremos el conjunto de funciones con primer valor en S.*

A menos que se indique lo contrario, R es un anillo con elemento unidad; el cual notaremos por 1. Entonces, por lo mostrado anteriormente $\mathcal{A}(R)$ también es un anillo con elemento unidad, δ.

Proposición 1.5. *Si R^* es el conjunto de unidades de R, entonces el conjunto de unidades de $\mathcal{A}(R)$, es $\mathcal{A}(R)^* = F(R^*)$*

Demostración. Sea f una unidad en $\mathcal{A}(R)$. Entonces, existe $g \in \mathcal{A}(R)$ tal que $f * g = g * f = \delta$. Luego, $f(1)g(1) = (f * g)(1) = \delta(1) = 1$. Así, $f(1) \in R^*$ por lo que, $f \in F(R^*)$.

Ahora, si $f \in F(R^*)$, entonces existe $x \in R$ tal que $f(1)x = 1 = xf(1)$. Sea $g \in \mathcal{A}(R)$ definida recursivamente de la siguiente manera, $g(1) = x$. Supongamos que para todo $k < n$, $g(k)$ ya esta definido de manera que $(f * g)(k) = \delta(k)$. Como $\delta(n) = 0$, debemos definir $g(n)$ de forma en que $(f * g)(n) = 0$;

$$\begin{aligned} (f * g)(n) &= \sum_{ab=n} f(a)g(b) \\ &= \sum_{ab=n, a\neq 1} f(a)g(b) + f(1)g(n) \end{aligned}$$

y como $(f * g)(n) = 0$ y $xf(1) = 1$,

$$g(n) = -x \left(\sum_{ab=n, a\neq 1} f(a)g(b) \right).$$

Así, $f * g = \delta$, lo que significa que f es una unidad de $\mathcal{A}(R)$.
Queda demostrado que el conjunto de unidades de $\mathcal{A}(R)$, $\mathcal{A}(R)^*$ es $F(R^*)$. □

Definición 1.19. *Sea R un anillo, el conjunto de funciones multiplicativas sobre R es*

$$\mathcal{M}(R) = \{f \in \mathcal{A}(R) \mid f \neq 0 \ y \ gcd(a, b) = 1 \Rightarrow f(ab) = f(a)f(b)\}$$

Una propiedad importante de las funciones multiplicativas es que si R es un anillo sin divisores de cero y $f \in \mathcal{M}(R)$, $f(1) = f(1)f(1)$, entonces $f(1)(f(1) - 1) = 0$. Luego, $f(1) = 0$ o $f(1) = 1$. Si $f(1) = 0$, entonces para todo $n \in \mathbb{N}$, $f(n) = f(1)f(n) = 0$; lo que implica que f sea una aplicación nula, contradiciendo que $f \in \mathcal{M}(R)$. Por lo que, $f(1) = 1$ y por lo tanto $1(\mathcal{M}(R)) = \{1\}$.

Lema 1.1. *Sea R un anillo con unidad que no tiene divisores de cero. Entonces, Si $f, h \in \mathcal{M}(R)$, $g \in \mathcal{A}(R)$ y $(f * g) = h$ (Análogamente $g * f = h$), $g \in \mathcal{M}(R)$.*

Demostración. Sea $a \in \mathbb{N}$.

- Como $g(1) = f(1)g(1) = (f * g)(1) = h(1) = 1$, pues h y f son multiplicativas en un anillo sin divisores de cero. Así, $g(a \cdot 1) = g(a) = g(a)g(1)$.
- Ahora, si para todo $r < b$ con $gcd(a, r) = 1$ $g(ar) = g(a)g(r)$ y $b \in \mathbb{N}$ con $gcd(a, b) = 1$ debemos ver que $g(ab) = g(a)g(b)$.

  con $gcd(a, b) = 1$

$$
\begin{aligned}
& h(a)h(b) \\
= \quad & \langle\ h \text{ es multiplicativa}\ \rangle \\
& h(ab) \\
= \quad & \langle\ h = f * g \text{ y definición de } *\ \rangle \\
& \textstyle\sum_{d|ab} f(ab/d)g(d) \\
= \quad & \langle\ \text{Propiedad asociativa del anillo}\ \rangle \\
& \textstyle\sum_{d|ab,\ d<ab} f(ab/d)g(d) + f(1)g(ab) \\
= \quad & \langle\ f(1) = 1 \text{ y } \{d : d|ab, d < ab\} = \{d_1d_2 : d_1|a,\ d_2|b,\ d_1d_2 < ab\} \text{ pues } gcd(a, b) = 1\ \rangle \\
& \textstyle\sum_{d_1d_s<ab,\ d_1|a,\ d_2|b} f(d_1d_2)g(ab/d_1d_2) + g(ab) \\
= \quad & \langle\ f \text{ es multiplicativa e hipotesis de inducción}\ \rangle \\
& \textstyle\sum_{d_1d_s<ab,\ d_1|a,\ d_2|b} f(d_1)f(d_2)g(a/d_1)g(b/d_2) + g(ab) \\
= \quad & \langle\ 0 = -f(1)f(1)g(a)g(b) + f(1)f(1)g(a)g(b)\ \rangle \\
& \textstyle\sum_{d_1|a,\ d_2|b} f(d_1)f(d_2)g(a/d_1)g(b/d_2) - f(1)f(1)g(a)g(b) + g(ab) \\
= \quad & \langle\ \text{producto de sumatorias}\ \rangle \\
& \textstyle\left(\sum_{d_1|a} f(d_1)g(a/d_1)\right)\left(\sum_{d_2|a} f(d_2)g(b/d_2)\right) - f(1)f(1)g(a)g(b) + g(ab) \\
= \quad & \langle\ h = f * g, \text{ definición de } *,\ f(1) = 1\ \rangle \\
& h(a)h(b) - g(a)g(b) + g(ab)
\end{aligned}
$$

  Luego, $g(ab) = g(a)g(b)$.

Por lo tanto, $g \in \mathcal{M}(R)$.

□

Proposición 1.1. *Si R es un anillo sin divisores de cero, $(\mathcal{M}(R), *)$ es un grupo*

Demostración. Primero ve que la operación $*$ esta bien definida sobre $\mathcal{M}(R)$, es decir

$$* : \mathcal{M}(R) \times \mathcal{M}(R) \to \mathcal{M}(R).$$

Sean $f, g \in \mathcal{M}(R)$, se debe ver que $f * g, g * f \in \mathcal{M}(R)$.

Si $a, b \in \mathbb{N}$ y $gcd(a,b) = 1$,

$$\begin{aligned}
& [(f*g)(a)]\,[(f*g)(b)] \\
= \quad & \langle \text{ Definición de } * \rangle \\
& \left[\sum_{d_1|a} f(d_1)g(a/d_1)\right]\left[\sum_{d_2|b} f(d_2)g(b/d_2)\right] \\
= \quad & \langle \text{ Producto de sumatorias } \rangle \\
& \sum_{d_1|a,\ d_2|b} f(d_1)g(a/d_1)f(d_2)g(b/d_2) \\
= \quad & \langle\ f \text{ y } g \text{ son multiplicativas y } f(1) = g(1) = 1 \ \rangle \\
& \sum_{d_1|a,\ d_2|b} f(d_1d_2)g\left(\tfrac{ab}{d_1d_2}\right) \\
= \quad & \langle\ \{d : d|ab\} = \{d_1d_2 : d_1|a, d_2|b\} \text{ pues } gcd(a,b) = 1 \ \rangle \\
& \sum_{d|ab} f(d)g\left(\tfrac{ab}{d}\right) \\
= \quad & \langle \text{ Definición } * \rangle \\
& (f*g)(ab)
\end{aligned}$$

De igual manera,

$$\begin{aligned}
& [(g*f)(a)]\,[(g*f)(b)] \\
= \quad & \langle \text{ Definición de } * \rangle \\
& \left[\sum_{d_1|a} g(d_1)f(a/d_1)\right]\left[\sum_{d_2|b} g(d_2)f(b/d_2)\right] \\
= \quad & \langle \text{ Producto de sumatorias } \rangle \\
& \sum_{d_1|a,\ d_2|b} g(d_1)f(a/d_1)g(d_2)f(b/d_2) \\
= \quad & \langle\ f \text{ y } g \text{ son multiplicativas y } f(1) = g(1) = 1 \ \rangle \\
& \sum_{d_1|a,\ d_2|b} g(d_1d_2)f\left(\tfrac{ab}{d_1d_2}\right) \\
= \quad & \langle\ \{d : d|ab\} = \{d_1d_2 : d_1|a, d_2|b\} \text{ pues } gcd(a,b) = 1 \ \rangle \\
& \sum_{d|ab} g(d)f\left(\tfrac{ab}{d}\right) \\
= \quad & \langle \text{ Definición } * \rangle \\
& (g*f)(ab)
\end{aligned}$$

Ahora se demuestran las propiedades de grupo

1. Como la operación $*$ es asociativa en $(\mathcal{A}(R), +, *)$ también lo es en $(\mathcal{M}(R), *)$.
2. El elemento identidad es δ. Claramente $\delta \in \mathcal{M}(R)$, pues dado $a, b \in \mathbb{N}$ con $gcd(a,b) = 1$.
   - Si $ab = 1$, entonces $a, b = 1$. Luego, $\delta(ab) = 1 = \delta(a)\delta(b)$
   - Si $ab > 1$, entonces $a > 1$ o $b > 1$. Luego, $\delta(ab) = 0$ y $\delta(a)\delta(b) = 0$

   Así, $\delta \in \mathcal{M}(R)$.
3. Dado $f \in \mathcal{M}(R)$, $f(1) = 1$. Luego, $f \in \mathcal{A}(R)^*$, así existe $f^{-1} \in \mathcal{A}(R)$ que esta dado por la ecuación recursiva

$$f^{-1}(1) = 1$$
$$f^{-1}(n) = -\sum_{d|n,\ d\neq 1} f(d)f^{-1}(n/d)$$

   Como, $f * f^{-1} = \delta \in \mathcal{M}(R)$ por el **Lema 1.1**, $f^{-1} \in \mathcal{M}(R)$.

Así queda demostrado que $(\mathcal{M}(R), *)$ □

Corolario 1.1. *Si R es un anillo y $f, g \in \mathcal{M}(R)$, entonces $f * g \in \mathcal{M}(R)$.*

Ejemplo 1.1. *Si $R = \mathbb{Z}$, $\mathcal{A}(\mathbb{Z})^* = F(\{1, -1\})$. En particular, la función idénticamente uno $f \equiv 1$ tiene inversa; y resultado de teoría de números, sabemos que es la función μ de Möbius*

$$\mu(n) = \begin{cases} 1 & Si \quad n = 1 \\ (-1)^l & Si \quad n = p_1 \cdots p_l \\ 0 & Si \quad Existe\ p\ primo\ t.q\ p^2 | n \end{cases}$$

Luego si

$$F(n) = \sum_{d|n} g(d) = (g * f)(n),$$

entonces, $(F * \mu)(n) = g(n)$. El cual es el teorema de inversión de Möbius.

Es natural plantearse si existe la función μ de Möbius en el anillo de funciones R-aritméticas para anillos distintos de $\mathbb{Z}$. Efectivamente, si el anillo tiene elemento unidad, podemos definir en $\mathcal{A}(R)$ el análogo a la función μ de Möbius. La pregunta ahora es; ¿sigue siendo esta la inversa de la función idénticamente la unidad? Para dar respuesta a esto, tenemos el siguiente ejemplo.

Ejemplo 1.2. *Sea R un anillo con unidad. Por las discusiones anteriores se sabe que la función idénticamente 1, $f \equiv 1$ tiene inversa. y la inversa de esta es la función μ de Möbius, donde*

$$\mu(n) = \begin{cases} 1 & Si \quad n = 1 \\ (-1)^l & Si \quad n = p_1 \dots p_l \\ 0 & Si \quad Existe\ p\ primo\ t.q\ p^2 | n \end{cases}$$

Para la prueba es útil primero ver que $\mu,\ f \in \mathcal{M}(R)$.
Sean $a, b \in \mathbb{N}$ con $gcd(a, b) = 1$. Entonces,

- *Si $ab = 1$, entonces $a, b = 1$. Así, $\mu(ab) = 1 = \mu(a)\mu(b)$*
- *Si existe un primo p tal que $p^2 | ab$, entonces $p \nmid a$ o $p \nmid b$; en cualquiera de los dos casos $p^2 | a$ o $p^2 | b$. Por lo que $\mu(a)\mu(b) = 0 = \mu(ab)$.*
- *Si $a = p_1 \cdots p_r$ y $b = q_1 \cdots q_s$, donde $p_1, ..., p_r$ son primos distintos y $q_1, ..., q_s$ son primos distintos. Para todo $1 \leq i \leq r$ y $1 \leq j \leq s$, $p_i \neq q_j$, pues $gcd(a, b) = 1$. Así,*

$$\mu(ab) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(a)\mu(b).$$

Por otro lado, $f(ab) = 1 = f(a)f(b)$. Así, tanto μ como f son multiplicativas.

Ahora se continua con la demostración. Como $\mathcal{A}(R)$ es un anillo, basta demostrar que $\mu * f = \delta$. Primero se demuestra lo siguiente.

Sea $n \geq 1$ y p un primo, entonces

$$\begin{aligned} & (\mu * f)(p^n) \\ = & \quad \langle \text{ Definición de } * \rangle \\ & \sum_{a|p^n} \mu(a) f(p^n/a) \\ = & \quad \langle \ f \equiv 1, \text{ los divisores de la potencia de un primo } \rangle \\ & \sum_{i=0}^{n} \mu(p_i) \\ = & \quad \langle \text{ Definición de } \mu \rangle \\ & 0 \end{aligned}$$

Aquí lo que se mostró fue que para todo primo p y todo entero positivo n, $(\mu * f)(p^n) = 0$.

Ahora, como $\mu, f \in \mathcal{M}(R)$, entonces $\mu * f \in \mathcal{M}(R)$. Luego, dado $n \in \mathbb{N}$.

- *Si $n > 1$, por el teorema fundamental de la aritmética, $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$, donde para todo i, p_i es un primo y α_i un entero positivo. Entonces,*

$$\begin{aligned} & (\mu * f)(n) \\ = & \quad \langle \text{ Teorema fundamental de la aritmética } \rangle \\ & (\mu * f)(p_1^{\alpha_1} \cdots p_l^{\alpha_l}) \\ = & \quad \langle \ \mu * f \text{ es multiplicativa } \rangle \\ & (\mu * f)(p_1^{\alpha_1}) \cdots (\mu * f)(p_l^{\alpha_l}) \\ = & \quad \langle \text{ Por la discusión anterior } \rangle \\ & 0 \end{aligned}$$

- *Si $n = 1$, $(\mu * f)(1) = 1 = (f * \mu)(1)$. Esto claramente se cumple pues*

$$(\mu * f)(1) = \mu(1) f(1) = \mu(1) = 1$$

$$(f * \mu)(1) = f(1)\mu(1) = \mu(1) = 1$$

Así, $\mu * f = \delta$ y por lo tanto $f^{-1} = \mu$.

Otra pregunta sobre la estructura de $\mathcal{A}(R)$ es, ¿puede llegar a ser este un cuerpo?. La respuesta es negativa a menos que $R = \{0\}$. Sea

$$f(n) = \begin{cases} 0 & Si \quad n \neq 2 \\ \\ 1 & Si \quad n = 2\} \end{cases}$$

Por lo mencionado anteriormente, $f \notin \mathcal{A}(R)^*$. Pero, $f \neq 0$.
De la discusión anterior se despliega la siguiente observación

Observación 1.1. *$\mathcal{A}(R)$ nunca es un cuerpo.*

2. Estructuras de $\mathcal{A}(R)$

Ya hemos visto que $\mathcal{A}(R)$ es un anillo con sus operaciones de adición y convolución. Ahora exploraremos la propiedades algebraicas que este anillo posee.

2.1. Ideales de $\mathcal{A}(R)$

Lema 2.1. *Si I es un ideal a izquierda de R, entonces $F(I)$ es un ideal a izquierda de $\mathcal{A}(R)$.*

Demostración. Si $f, g \in F(I)$, entonces $f(1), g(1) \in I$. Luego, $(f \pm g)(1) = f(1) \pm g(1) \in I$. Así, $f \pm g \in F(I)$. Por lo que $F(I)$ es un subgrupo aditivo de $\mathcal{A}(R)$. Ahora, si $f \in F(I)$ y $g \in \mathcal{A}(R)$, $(g * f)(1) = g(1)f(1) \in I$, luego $g * f \in I$. Por lo tanto $F(I)$ es un ideal a izquierda. □

Lema 2.2. *Si I es un ideal a izquierda de $\mathcal{A}(R)$, entonces $1(I)$ es un ideal a izquierda de R.*

Demostración. Si $a, b \in 1(I)$, entonces existen $f, g \in I$ tales que $f(1) = a$ y $g(1) = b$. Luego,

$$a \pm b = f(1) \pm g(1) = (f \pm g)(1) \in 1(I)$$

pues, $f, g \in I$. En consecuencia, $1(I)$ es un subgrupo aditivo de R. Ahora, si $a \in 1(I)$ y $b \in R$, existe $f \in I$ tal que $f(1) = a$. Luego, como I es un ideal a izquierda de $\mathcal{A}(R)$, $b\delta * f \in I$. Por lo tanto $ba = (b\delta * f)(1) \in 1(I)$. Así, $1(I)$ es un ideal. □

Proposición 2.1. *Las siguientes proposiciones serán útiles para demostrar los lemas que vendrán más adelante.*

1. *Si I es un ideal distinto de R, $F(I) \neq \mathcal{A}(R)$.*
2. *Si $I \neq \mathcal{A}(R)$ es un ideal a izquierda en $\mathcal{A}(R)$, $1(I) \neq R$.*

Demostración. En base al lema anterior, tenemos que

1. Si $I \neq R$, $1 \notin R$. Luego, $\delta \notin F(R)$. Por lo tanto $F(R) \neq \mathcal{A}(R)$.

2. Si $I \neq \mathcal{A}(R)$, entonces por proposición 1.5, para todo $f \in I$, $f(1) \neq 1$, luego $1 \notin 1(I)$. Por lo tanto $1(I) \neq R$.

□

Lema 2.3. *Si I es un ideal maximal a izquierda de R, entonces $F(I)$ es un ideal maximal a izquierda de $\mathcal{A}(R)$.*

Demostración. Si I es un ideal maximal a izquierda de R, $F(I)$ es un ideal a izquierda de $\mathcal{A}(R)$. Ahora, sea K un ideal a izquierda de $\mathcal{A}(R)$ tal que $F(I) \subsetneq K$. Entonces, existe $f \in K \setminus F(I)$, es decir $f \in K$ tal que $f(1) \notin I$. Luego, el ideal a izquierda de I generado por $I, f(1)$ es igual a R, pues $I \subsetneq \langle I, f(1)\rangle_{izq}$. Por lo tanto existen $m \in I$ y $r \in R$ tales que, $m + rf(1) = 1$. Y como $m \in I$, $m\delta \in F(I) \subset K$; y del hecho de que K es un ideal, $r\delta * f \in K$. Luego, $g = m\delta + r\delta * f \in K$, pero $g(1) = m + rf(1) = 1$, lo que implica que g es una unidad de $\mathcal{A}(R)$. Por lo tanto $K = \mathcal{A}(R)$. □

Lema 2.4. *Si I es un ideal maximal a izquierda de $\mathcal{A}(R)$, entonces $1(I)$ es un ideal maximal a izquierda de R.*

Demostración. Como I es un ideal, $1(I)$ es un ideal. Sea K un ideal a izquierda en R tal que $1(I) \subsetneq K$. Entonces, existe $a \in K \setminus 1(I)$, es decir existe $a \in K$ tal que para todo $f \in I$, $f(1) \neq a$. Luego, $a\delta \notin I$, entonces $I \subsetneq \langle I, a\delta\rangle_{izq} = \mathcal{A}(R)$ pues I es maximal. Por lo que existen $g \in I$ y $r \in \mathcal{A}(R)$ tales que $g + (r * a\delta) = \delta$, entonces $1 = g(1) + r(1)a$ y como $a \in K$ y $g(1) \in 1(I) \subset K$, $1 = g(1) + r(1)a \in K$, lo que implica $K = R$. Por lo tanto $1(I)$ es un ideal maximal a izquierda. □

Lema 2.5. *Sean $A, B \subset R$ y $C \subset \mathcal{A}(R)$. Entonces,*

- $1(F(A)) = A$
- $C \subset F(1(C))$
- *Si* $F(A) = F(B)$*, entonces* $A = B$

Demostración. Sean A, B y C como en el enunciado.

- Sea $x \in A$. Entonces, $x\delta \in F(A)$ y como $x = x\delta(1)$, $x \in 1(F(A))$. Luego, $A \subset 1(F(A))$.
  Ahora, si $x \in 1(F(A))$, existe $f \in F(A)$ tal que $f(1) = x$, pero como $f \in F(A)$, $x = f(1) \in A$
- Sea $f \in C$. Luego, $f(1) \in 1(C)$, entonces $f \in F(1(C))$. Por lo tanto $C \subset F(1(C))$.
- Sea $F(A) = F(B)$. Ahora, si $a \in A$, entonces $a\delta \in F(A) = F(B)$. Luego, $a = a\delta(1) \in B$. Por lo tanto $A \subset B$. De forma análoga se demuestra la otra con tenencia de donde se obtiene la igualdad.

□

Corolario 2.1. *Si* I *es un ideal maximal a izquierda en* $\mathcal{A}(R)$*,* $I = F(1(I))$.

Demostración. Por el lema 2.5 se tiene que $B \subset F(1(B))$. Ahora, como B es maximal, $F(1(B)) = B$ o $F(1(B)) = \mathcal{A}(R)$ □

En el siguiente ejemplo mostraremos que la contenencia puede ser estricta.

Ejemplo 2.1. *Consideremos el ideal* $A = \{0\}$*, luego* $F(1(A)) = \{f \in \mathcal{A}(R) : f(1) \in 1(A)\}$*, esto es,*

$$F(1(A)) = \{f \in \mathcal{A}(R) : f(1) = 0\}$$

Ahora, si $R \neq \{0\}$*,* $F(1(A)) \neq \{0\}$.

En particular, si I es un ideal maximal a izquierda en $\mathcal{A}(R)$, $1(I)$ es un ideal a izquierda en R. Luego, $F(1(I))$ es un ideal a izquierda de $\mathcal{A}(R)$. Y como I es maximal a izquierda y $I \subset F(1(I)) \subsetneq \mathcal{A}(R)$, $I = F(1(I))$. Lo que nos lleva al siguiente corolario.

Teorema 2.1. *R es un anillo local a izquierda si y solo si $\mathcal{A}(R)$ es un anillo local a izquierda.*

Demostración. Si R es un anillo local a izquierda con ideal maximal M, $F(M)$ es un ideal maximal a izquierda de $\mathcal{A}(R)$. Ahora, si K es un ideal maximal a izquierda de $\mathcal{A}(R)$, $1(K)$ es un ideal maximal a izquierda de R. Por lo que $M = 1(K)$ y por el corolario del lema 2.5 $F(M) = F(1(K)) = K$. Por lo tanto $F(M)$ es el único ideal maximal a izquierda de $\mathcal{A}(R)$. Luego, $\mathcal{A}(R)$ es local a izquierda.
Ahora, si $\mathcal{A}(R)$ es un anillo local a izquierda con ideal maximal M, $1(M)$ es un ideal maximal a izquierda de R. Sea K un ideal maximal a izquierda de R. Entonces, $F(K)$ es un ideal a izquierda de $\mathcal{A}(R)$. Luego, $F(K) = M$, por lo que $1(F(K)) = 1(M)$. Y por el lema 2.5, $K = 1(M)$. Por lo tanto $1(M)$ es el ideal maximal a izquierda de R. Así R es local. □

Lema 2.6. *si I es ideal primo, $F(I)$ es ideal primo.*

Demostración. Sea I un ideal primo en R. Entonces, $F(I)$ es un ideal. Ahora, si $f * g \in F(I)$, $f(1)g(1) \in I$; y como I es un ideal primo, $f(1) \in I$ o $g(1) \in I$. Por lo tanto, $f \in F(I)$ o $g \in F(I)$. Así, $F(I)$ es un ideal primo en $\mathcal{A}(R)$. □

Podemos ver una fuerte relación entre los conjuntos $F(I)$, $1(I)$ con los ideales de $\mathcal{A}(R)$ y R respectivamente. Esto se da pues son la imagen inversa y directa de un homomorfismo

Definición 2.1. *Sea $\iota : \mathcal{A}(R) \to R$, la función dada por la ecuación*

$$\iota(f) = f(1). \quad (\forall f \in \mathcal{A}(R))$$

Teorema 2.2. *La aplicación ι es un epimorfismo*

Demostración. Para realizar la demostración primero se prueba que ι es un homomorfismo.
Sean $f, g \in \mathcal{A}(R)$. Entonces,

$$\begin{aligned} & \iota(f+g) \\ = & \quad \langle \text{ Definición de } \iota \rangle \\ & (f+g)(1) \\ = & \quad \langle \text{ Definición de la suma en } \mathcal{A}(R) \rangle \\ & f(1)+g(1) \\ = & \quad \langle \text{ Definición de } \iota \rangle \\ & \iota(f)+\iota(g) \end{aligned}$$

Así, ι conserva la adición. Para ver que tambien conserva el producto se realiza lo mismo

$$\begin{aligned} & \iota(f*g) \\ = & \quad \langle \text{ Definición de } \iota \rangle \\ & (f*g)(1) \\ = & \quad \langle \text{ Convolución de Dirichlet } \rangle \\ & f(1)g(1) \\ = & \quad \langle \text{ Definición de } \iota \rangle \\ & \iota(f)\iota(g) \end{aligned}$$

Por lo tanto, ι es un homomorfismo.
Falta demostrar que ι es sobreyectiva. Sea $r \in R$, entonces $\iota(r\delta) = r\delta(1) = r$. Así, ι es un epimorfismo. □

Proposición 2.2. *Sea $S \subset \mathcal{A}(R)$, entonces $1(S) = \iota(S)$*

Demostración. Si $r \in 1(S)$, entonces, existe una función $f \in S$ tal que $f(1) = r$; por lo tanto, $r = \iota(f)$. Lo que implica $r \in \iota(S)$. De donde se concluye, $1(s) \subset \iota(S)$.
Ahora, si $r \in \iota(S)$, entonces, existe $f \in S$ tal que $\iota(f) = r$, luego $f(1) = r$. Por lo que, $r \in 1(S)$. Así, $\iota(S) \subset 1(S)$. Por lo tanto, $1(S) = \iota(S)$. □

Proposición 2.3. $\ker(\iota) = F(\{0\})$.

Demostración. La demostración se realiza usando lógica calculatoria

$$\begin{aligned} & f \in \ker(\iota) \\ \equiv \quad & \langle \text{ Definición de kernel } \rangle \\ & \iota(f) = 0 \\ \equiv \quad & \langle \text{ Definición de } \iota \rangle \\ & f(1) = 0 \\ \equiv \quad & \langle \text{ Definición de } F(\{0\}) \rangle \\ & f \in F(\{0\}) \end{aligned}$$

Así, la proposición queda demostrada. □

Como dado $S \subset R$,

$$\iota^{-1}(S) = \bigcup_{r \in S} r\delta + ker(\iota),$$

Es fácil ver que $F(S) = \bigcup_{r\in S} r\delta + ker(\iota)$. Sea $x \in \bigcup_{r\in S} r\delta + ker(\iota)$. Entonces, existen $r \in S$ y $f \in ker(\iota)$ tales que $x = r\delta + f$. Así,

$$x(1) = r\delta(1) + f(1) = r \in S$$

luego, $x \in F(S)$. Por lo que $\bigcup_{r\in S} r\delta + ker(\iota) \subset F(S)$.
Por otro lado, si $x \in F(S)$, $x(1) \in S$. Luego,

$$x = x(1)\delta + x - x(1)\delta$$

y como

$$(x - x(1)\delta)(1) = x(1) - (x(1)\delta)(1) = 0$$

podemos decir que $x - x(1)\delta \in F(\{0\}) = \ker(\iota)$. Así, $x \in \bigcup_{r\in S} r\delta + ker(\iota)$. por lo que $F(S) \subset \bigcup_{r\in S} r\delta + ker(\iota)$. Concluyendo así que $\bigcup_{r\in S} r\delta + ker(\iota) = F(S)$.

La discusión anterior nos lleva a enunciar la siguiente proposición.

Proposición 2.4. *Si $S \subset R$, $\iota^{-1}(S) = F(S)$.*

2.2. Dominio de Integridad.

Cuando R es un anillo de integridad se puede definir una norma que nos permite deducir otras propiedades algebraicas de las funciones $R-$aritméticas.

Definición 2.2. *La siguiente función $\mathfrak{y} : \mathcal{A}(R) \to \mathbb{Z}$*

$$\mathfrak{y}(f) = \begin{cases} 0 \quad Si \quad f = 0 \\ \\ n \quad Sif \neq 0 \quad donde\ n = min\{k | f(k) \neq 0\} \end{cases}$$

sera llamada una norma en $\mathcal{A}(R)$

Proposición 2.5. *Sean $f, g \in \mathcal{A}(R)$, entonces $\mathfrak{y}(f * g) = 0$ o $\mathfrak{y}(f * g) \geq \mathfrak{y}(f)\mathfrak{y}(g)$. Si R es un dominio de integridad, $\mathfrak{y}(f * g) = \mathfrak{y}(f)\mathfrak{y}(g)$.*

Demostración. Sean $a = \mathfrak{y}(f)$ y $b = \mathfrak{y}(g)$, entonces para todo $k < ab$,

$$(f * g)(k) = \sum_{ij=k} f(i)g(j) = 0$$

Pues si $ij = k < ab$ y $i \geq a$, $aj \leq ij < ab$. Luego, $j < b$. Por lo que para todo $ij = k < n$, $f(i)g(j) = 0$. Así,

$$\mathfrak{y}(f * g) \geq \mathfrak{y}(f)\mathfrak{y}(g)$$

Ahora, si R es un dominio de integridad,

$$\begin{aligned}(f * g)(ab) &= \sum_{ij=ab} f(i)g(j) \\ &= f(a)g(b) \neq 0\end{aligned}$$

Pues, $f(a), g(b) \neq 0$. Por lo tanto $\mathfrak{y}(f * g) = \mathfrak{y}(f)\mathfrak{y}(g)$ □

Corolario 2.2. *R es un dominio de integridad si y solo si $\mathcal{A}(R)$ es un dominio de integridad.*

Demostración. Si R es un dominio de integridad y $f, g \in \mathcal{A}(R) \setminus \{0\}$, $\mathfrak{y}(f) > 0$ y $\mathfrak{y}(f) > 0$. Entonces,

$$\mathfrak{y}(f * g) = \mathfrak{y}(f)\mathfrak{y}(g) > 0.$$

Por lo tanto $\mathcal{A}(R)$ es un dominio de integridad.

Ahora, si R no es un dominio de integridad, existen $a, b \in R \setminus \{0\}$ tales que $ab = 0$. Luego, $a\delta * b\delta = 0$. Y como $a\delta, b\delta \neq 0$, $\mathcal{A}(R)$ no es un dominio de integridad. □

2.3. Dimensión de $\mathcal{A}(R)$

En esta sección estudiaremos algunas características referentes a la dimensión de *Krull* y a la condición de la cadena ascendente en el anillo $\mathcal{A}(R)$.

Proposición 2.6. *Para un conjunto parcialmente ordenado $(X, \leq)$ las siguientes condiciones son equivalentes.*

1. *Toda sucesión ascendente infinita $x_1 \leq x_2 \leq \cdots x_n \leq \cdots$ de elementos de X termina. Es decir, existe $N \in \mathbb{N}$ tal que si $n \geq N$, $x_n = x_N$.*
2. *No existe sucesión estrictamente ascendente infinita de elementos de X.*
3. *Todo subconjunto no vació $S \subset X$ tiene un elemento maximal de S en S.*

Nota 2.1. *Un elemento x de un conjunto parcialmente ordenado $(X, \leq)$ es maximal si no existe $y \in X$ tal que $y > x$*

Demostración. Para realizar la demostración, veremos que (1) ⇒ (2) ⇒ (3) ⇒ (1).

(1) ⇒ (2) Sea $(x_n)_n$ una sucesión infinita de X estrictamente ascendente, en particular $(x_n)_n$ es una sucesión ascendente. Luego, por (1), existe $N \in \mathbb{N}$ tal que si $n \geq N$, $x_n = x_N$. Contradiciendo que $(x_n)_n$ es estrictamente ascendente. Así, $(x_n)_n$ no puede existir.

(2) $\Rightarrow$ (3) Suponga que existe un $S \subset X$ no vació que no tiene elemento maximal. Entonces, para cada elemento $x \in S$, existe $y \in S$ tal que $x < y$. Así, Tomando $x_1 \in S$, existe $x_2 \in S$ tal que $x_1 < x_2$. Ahora, si suponemos que para todo $i \leq n$, esta definido $x_i \in S$ de modo que $x_1 < x_2 < \cdots < x_n$, entonces como S no tiene maximal, existe x_{n+1} tal que $x_n < x_{n+1}$. Siendo así $(x_n)_n$ una sucesión en $S \subset X$ estrictamente creciente e infinita; contradiciendo (2). Por lo tanto, todo subconjunto S de X debe de tener elemento maximal.

(3) $\Rightarrow$ (1) Sea $(x_n)_n$ una sucesión creciente en X. Si $S = \{x_n | n \in \mathbb{N}\}$, este es un subconjunto de X no vacío, así que por (3), existe $x_N \in S$ tal que para ningún $n \in \mathbb{N}$, $x_n > x_N$. Ahora, como $(x_n)_n$ es ascendente entonces para todo $n \geq N$, $x_N \leq x_n$. Por lo tanto, para todo $n \geq N$, $x_n = x_N$.

Así, la proposición queda demostrada. □

Definición 2.3. *Un conjunto parcialmente ordenado, $(X, \leq)$ cumple la* ***condición de la cadena ascendente*** *o (c.c.a), si No existe sucesión estrictamente ascendente infinita de elementos de X.*

Ahora se define la condición de la cadena ascendente para los ideales de un anillo,

Definición 2.4. *Sea R un anillo conmutativo, la condición de la cadena ascendente aplicada a ideales de R tiene tres formas equivalentes.*

(a) Toda sucesión ascendente infinita $I_1 \subset I_2 \subset \cdots I_n \subset \cdots$ de ideales de R termina. Es decir, existe $N \in \mathbb{N}$ tal que si $n \geq N$, $I_n = I_N$.

(b) No existe sucesión estrictamente ascendente infinita de ideales de R.

(c) Toda colección no vacía S de ideales de R, tiene un elemento maximal de S en S.

Los anteriores son enunciados equivalentes por la **Proposición 2.6**.

Definición 2.5 (**Anillo Noetheriano**). *Un anillo conmutativo es Noetheriano cuando sus ideales satisfacen la (c.c.a).*

Teorema 2.3. *$\mathcal{A}(\mathcal{R})$ nunca es Noetheriano.*

Demostración. Sea $\mathfrak{P} = \{p_1, p_2, ...,\} \cup \{1\}$ el conjunto de todos los primos, con el 1, $\mathfrak{P}_i = \mathfrak{P} \setminus \{p_1, ..., p_i\}$ y $\prod(\mathfrak{P}_i)$ el conjunto de todos los múltiplos de elementos en $\mathfrak{P}_i$ y el 1

$$\prod(\mathfrak{P}_i) = \{n \in \mathbb{N} | \exists q_1, ..., q_n \in \mathfrak{P}_i \ y \ n = q_1 \cdots q_n\}.$$

Ahora, se define el siguiente ideal de $\mathcal{A}(R)$,

$$\mathfrak{p}_i = \{f \in \mathcal{A}(R) | f(n) = 0, \ \forall n \in \prod(\mathfrak{P}_i)\}.$$

Claramente si $f \in \mathfrak{p}_i$, $f(1) = 0$; pues $1 \in \mathfrak{P}_i$. Veamos que $\mathfrak{p}_i$ es un ideal de $\mathcal{A}(R)$ para cada $i \in \mathbb{N}$. En efecto,

- Sean $f, g \in \mathfrak{p}_i$. Entonces, dado $n \in \prod(\mathfrak{P}_i)$

$$(f + g)(n) = f(n) + g(n) = 0 + 0 = 0.$$

y

$$(f - g)(n) = f(n) - g(n) = 0 + 0 = 0.$$

Así, $f + g, f - g \in \mathfrak{p}_i$.

- Sean $f \in \mathfrak{p}_i$ y $h \in \mathcal{A}(R)$. Entonces, dado $n \in \prod(\mathfrak{P}_i)$

$$(f * h)(n) = \sum_{d|n} f(d)h(n/d) = 0$$

  Pues si $n \in \prod(\mathfrak{P}_i)$ y $d|n$, $d \in \prod(\mathfrak{P}_i)$. Así, $f * h \in \mathfrak{p}_i$.

Así, $\mathfrak{p}_i$ es un ideal de $\mathcal{A}(R)$ distinto de $\mathcal{A}(R)$.
Sea $i \in \mathbb{N}$. Entonces, $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$. En efecto, Como $\mathfrak{P}_{i+1} \subset \mathfrak{P}_i$, $\prod(\mathfrak{P}_{i+1}) \subset \prod(\mathfrak{P}_i)$. Entonces, dado $f \in \mathfrak{p}_i$, y $n \in \prod(\mathfrak{P}_{i+1})$, como $\prod(\mathfrak{P}_{i+1}) \subset \prod(\mathfrak{P}_i)$, $f(n) = 0$. Así, $f \in \mathfrak{p}_{i+1}$. Por lo tanto, $\mathfrak{p}_i \subset \mathfrak{p}_{i+1}$.
Ahora, si

$$f(n) = \begin{cases} 0 & n \neq p_{i+1} \\ 1 & n = p_{i+1} \end{cases}$$

$f \in \mathfrak{p}_i$, pero $f \notin \mathfrak{p}_{i+1}$. por lo que queda demostrado que $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$. Teniendo una sucesión infinita, estrictamente creciente de ideales, $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots$ de $\mathcal{A}(R)$; por lo tanto $\mathcal{A}(R)$ no es un anillo Noetheriano. □

Definición 2.6. *En un anillo conmutativo R, la altura $hgt(\mathfrak{p})$ de un ideal primo $\mathfrak{p}$ de R es el supremo de la longitud de las sucesiones estrictamente decrecientes de ideales primos de R,*

$$\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_m.$$

Definición 2.7. *La dimensión de Krull de un anillo es el supremo de las alturas de los ideales primos del anillo.*

Teorema 2.4. *la dimensión de Krull de $\mathcal{A}(R)$ es mayor que la de R.*

Demostración. Sea H_R el conjunto de las alturas de los ideales primos de R y $H_{\mathcal{A}(R)}$ el conjunto de las alturas de los ideales primos de $\mathcal{A}(R)$.
Si $h \in H_R$, entonces existe un ideal primo I de R con $hgt(I) = h$. Es decir, para cada $k < h$, existe una cadena estrictamente descendiente de ideales primos de R contenidos de I de longitud $k+1$, sea esta $(I_i)_{i=1}^{k+1}$, con $I_0 = I$. Por el **Lema 2.6** $\mathcal{I}_i = F(I_i)$ es un ideal primo de $\mathcal{A}(R)$ para cada $1 \leq i \leq k+1$. Además por el **Lema 2.5**, $i \neq j$, implica $\mathcal{I}_i \neq \mathcal{I}_j$. Y como $I_{i+1} \subsetneq I_i$, $\mathcal{I}_{i+1} = F(I_{i+1}) \subset F(T_i) = \mathcal{I}_i$. Así, $\mathcal{I}_\prime$ es un ideal de $\mathcal{A}(R)$ con $h \leq hgt(\mathcal{I}_0) = h_0$. Por lo tanto, para cada cada $h \in H_R$, existe $h_0 \in H_{\mathcal{A}(R)}$ tal que $h \leq h_0$. Por lo tanto,

$$\sup H_R \leq \sup H_{\mathcal{A}(R)}.$$

Es decir, la dimensión de *Krull* de $\mathcal{A}(R)$ es mayor que la de R. □

3. Polinomios en $\mathcal{A}(R)$

Buscamos generalizar algunas propiedades para los polinomios con coeficientes en las funciones aritméticas. El caso donde R es igual a los complejos ha sido desarrollado en [2], el caso para cualquier anillo R se establecerá en lo que sigue, veremos que en particular se generalizan muchas propiedades del caso complejo.

3.1. Anillo de polinomios

Definición 3.1. ***Anillo de polinomios*** *Sea R un anillo. El anillo de polinomios sobre R con indeterminada x, notado por $R[x]$, es el conjunto de símbolos $a_0 + a_1x + \cdots + a_nx^n$ donde n puede ser cualquier entero no negativo y donde los coeficientes $a_1, a_2, ..., a_n \in R$.*

Sean $p(x), q(x) \in R[x]$, con $p(x) = a_0 + a_1x + \cdots + a_nx^n$ y $q(x) = b_0 + b_1x + \cdots + b_mx^m$; diremos que $p(x) = q(x)$ si y solo si para todo entero $i \geq 0$, $a_i = b_i$.

Nuevamente si $p(x), q(x) \in R[x]$, con $p(x) = a_0+a_1x+\cdots+a_nx^n$ y $q(x) = b_0+b_1x+\cdots+b_mx^m$ definiremos $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$, donde para cada i, $c_i = a_1+b_i$. Y definiremos $p(x)q(x) = d_0 + d_1x + \cdots + d_tx^t$ donde para cada i $d_i = \sum_{j=0}^{i} a_jb_{i-j}$.

Definición 3.2. ***Derivada de un polinomio.*** *Sí R es un anillo y $f(x) \in R[x]$ con*

$$f(x) = a_0 + a_1x + \cdots a_ix^i + \cdots x_nx^n,$$

entonces la derivada de $f(x)$, escrita como $f'(x)$ es el polinomio

$$f'(x) = a_1 + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}.$$

Este es claramente un polinomio en $R[x]$.

Definición 3.3. ***Raíz de un polinomio*** *Si $p(x) \in R[x]$, entonces un elemento a en algún anillo de extensión de R es llamada una raíz del polinomio $p(x)$ si $p(a) = 0$.*

3.2. Raíces de polinomios en $\mathcal{A}(R)$

Teorema 3.1. *Si $T(g) \in \mathcal{A}(R)[g]$ con*

$$T(g) = a_d * g^{*d} + \cdots + a_1g + a_0,$$

*$F_T(x) = a_d(1)x^d + \cdots a_1(1)x + a_0(1)$ un polinomio en $R[x]$ y $z_0 \in R$ tal que $F_T(z_0) = 0$ y $F'_T(z_0) \in R^*$, entonces existe un **único** $f \in \mathcal{A}(R)$ tal que $f(1) = z_0$ y $T(f) = 0$.*

Demostración. Sean T, F_T y z_0 como en el enunciado del teorema.
Debemos definir $f \in \mathcal{A}(R)$ de forma que $T(f) = 0$. Es decir, para todo $n \in \mathbb{N}$, se debe cumplir que $T(f)(n) = 0$, y como

$$\begin{aligned} T(f)(n) &= \sum_{i=0}^{d} (a_i * f^{*i})(n) \\ &= \sum_{i=0}^{d} \sum_{ml=n} a_i(m) f^{*i}(l) \end{aligned}$$

tenemos que

$$0 = \sum_{i=0}^{d} \sum_{ml=n} a_i(m) f^{*i}(l) \tag{1}$$

Ahora, definamos $f \in \mathcal{A}(R)$ de forma recursiva.

1. Para 1 definamos, $f(1) = z_0$
2. Supongamos que para $0 \leq k < n$, $f(k)$ esta definido de forma que cumple la ecuación (1). Sea $h_i = a_i * f^{*i}$. Entonces,

$$h_i(n) = \sum_{n_0 \cdots n_i = n} a_i(n_0) f(n_1) \cdots f(n_i) = ia_i(1) f(1)^{i-1} f(n) + \sum_{(n_0,\ldots,n_i) \in A_n^i} a_i(n_0) f(n_1) \cdots f(n_i)$$

Donde, $A_n^i = \{(n_0, ..., n_i) \in \mathbb{N}^i | n_0 \cdots n_i = n, \nexists\ 1 \leq j \leq i\ t.q\ n_j = n\}$. Ahora, como $f(n)$ debe cumplir,

$$0 = \sum_{i=0}^{d} h_i(n) = F'(f(1))f(n) + \sum_{i=0}^{d} \sum_{(n_0,...,n_i)\in A_n^i} a_i(n_0)f(n_1)\cdots f(n_i)$$

Luego,

$$F_T'(f(1))f(n) = -\sum_{i=0}^{d} \sum_{(n_0,...,n_i)\in A_n^i} a_i(n_0)f(n_1)\cdots f(n_i)$$

Y como $f(1) = z_0$ y $F_T'(z_0) \in R^*$,

$$f(n) = -\left(\sum_{i=0}^{d} \sum_{(n_0,...,n_i)\in A_n^i} a_i(n_0)f(n_1)\cdots f(n_i)\right) F_T'(z_0).$$

Así, la función $f \in \mathcal{A}(R)$ cumple $T(f) = 0$ y es la única que cumple las condiciones del teorema. □

Corolario 3.1. *Sea R cuerpo de característica 0. Si $T(g) \in \mathcal{A}(R)[g]$ con*

$$T(g) = a_d * g^{*d} + \cdots + a_1 g + a_0,$$

*$F_T(x) = a_d(1)x^d + \cdots a_1(1)x + a_0(1)$ un polinomio en $R[x]$ y $z_0 \in R$ una raíz simple de F_R, entonces existe un **único** $f \in \mathcal{A}(R)$ tal que $f(1) = z_0$ y $T(f) = 0$.*

Demostración. Basta demostrar que si z_0 es un cero simple de F_T, entonces $F_T(z_0) \in R^* = R \setminus \{0\}$. Sea z_0 es un cero simple de F_T, entonces

$$F_T(x) = (x - z_0)g(x), \quad (g(x) \in R[x]\ y\ g(z_0) \neq 0)$$

Así, $F_T'(z_0) = g(z_0) + (z_0 - z_0)g'(z_0) = g(z_0) \neq 0$. Luego, $F_T'(z_0) \in R^*$. □

Definición 3.4. *Sea $\mathbb{P}$ el conjunto de números primos. y $\mathbb{P}^* = \{p^k | p \in \mathbb{P}, k \in \mathbb{N}\}$*

Definición 3.5. *Si R es un anillo tal que $\mathbb{Q} \subset R$, diremos que una función $f \in \mathcal{M}(R)$ tal que para $p^k \in \mathbb{P}^*$, $f(p^k) = \frac{f(p)^k}{k!}$ es **exponencialmente multiplicativa***

Lema 3.1. *Toda función en $\mathcal{M}(R)$ esta completamente determinada por sus valores en $\mathbb{P}^*$*

Definición 3.6. *Sea $p \in \mathbb{P}$. Definimos $\mathcal{A}_p(R) = \{f \in \mathcal{A}(R) : Si\ para\ todo\ k \in \mathbb{N}_0\ n \neq p^k, f(n) = 0\}$; este es un anillo.*

Lema 3.2. $\mathcal{A}_p(R) \approx R[\![x]\!]$

Demostración. Sea $\phi_p : \mathcal{A}_p(R) \to R[\![x]\!]$ el isomorfismo definido por $\phi_p(f) = \sum_{n=0}^{\infty} f(p^n)x^n$. Para ver que este es un isomorfismo, tomaremos $f, g \in \mathcal{A}_p(R)$.

1. La siguiente cadena de igualdades se cumple por la definición de ϕ_p.

$$\begin{aligned}\phi_p(f+g) &= \sum_{n=0}^{\infty}(f(p^n) + g(p^n))x^n \\ &= \sum_{n=0}^{\infty} f(p^n)x^n + \sum_{n=0}^{\infty} g(p^n)x^n \\ &= \phi_p(f) + \phi_p(g).\end{aligned}$$

2. Ahora, partiendo de $\phi_p(f*g) = \sum_{n=0}^{\infty}(f*g)(p^n)x^n$, de la definición de la convolución se tiene que $(f*g)(p^n) = \sum_{k=0}^{n} f(p^{n-k})g(p^k)$. Luego,

$$\phi_p(f*g) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} f(p^{n-k})g(p^k)x^{n-k}x^k = \left(\sum_{n=0}^{\infty} f(p^n)x^n\right)\left(\sum_{n=0}^{\infty} g(p^n)x^n\right)$$

   Así, $\phi_p(f*g) = \phi_p(f)\phi_p(g)$ y por lo tanto, ϕ_p es un homomorfismo.

3. Para ver que es inyectiva, basta con recordar que la igualdad de series de potencias se mira por la igualdad en cada coeficiente, y que si $f \in \mathcal{A}_p(R)$, $f(k) = 0$ si $k \neq p^n$ para todo $n \in \mathbb{N}_0$. Así, si $\phi_p(f) = \phi_p(g)$, $f = g$.

4. Veamos que es sobreyectiva. Sea $\sum_{n=0}^{\infty} a_n x^n \in R[\![x]\!]$. Definamos $f \in \mathcal{A}_p(R)$, de la siguiente forma,

$$f(n) = \begin{cases} a_n & Si\ n = p^k\ para\ k \in \mathbb{N}_0 \\ \\ 0 & En\ otro\ caso \end{cases}$$

   Así, $f(p^k) = a_{p^k}$ para cada $k \in \mathbb{N}_0$. Por lo tanto, $\phi_p(f) = \sum_{n=0}^{\infty} a_n x^n$

Terminando así de demostrar que ϕ_p es un isomorfismo. □

Definición 3.7. *La función proyección sobre $\mathcal{A}_p(R)$, es $\pi_p : \mathcal{A}(R) \to \mathcal{A}_p(R)$ definida por*

$$\pi_p(f)(n) = \begin{cases} 0 & Si\ n \neq p^k\ para\ todo\ k \in \mathbb{N}_0 \\ \\ f(n) & Si\ n = p^k\ para\ algun\ k \in \mathbb{N}_0 \end{cases}$$

Esta es un epimorfismo entre los dos anillos.

Definición 3.8. ***Funcion exponencial.*** *Sea R un anillo tal que $\mathbb{Q} \subset R$. Definiremos la función $exp : R \to R[\![x]\!]$ de la siguiente forma que*

$$exp(r) = \sum_{n=0}^{\infty} \frac{1}{n!} r^n x^n.$$

Proposición 3.1. *Si R es un anillo tal que $\mathbb{Q} \subset R$ y $r, s \in R$, $exp(r)exp(s) = exp(r+s)$.*

Demostración. Sean $r, s \in R$, entonces de la definición de exp, se sigue que

$$\begin{aligned} exp(r)exp(s) &= \left(\sum_{n=0}^{\infty} \frac{r^n x^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{s^n x^n}{n!}\right) \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \frac{r^{n-k}x^{n-k}}{(n-k)!}\frac{s^k x^k}{k!}\right) \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \frac{r^{n-k}}{(n-k)!}\frac{s^k}{k!}\right) x^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \binom{n}{k} r^{n-k}s^k\right)\frac{1}{n!}x^n \end{aligned}$$

Ahora, por el teorema del binomio sobre cuerpos abelianos se tiene que

$$exp(r)exp(s) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \binom{n}{k} r^{n-k}s^k\right)\frac{1}{n!}x^n$$

$$= \sum_{n=0}^{\infty} \frac{(r+s)^n}{n!} x^n$$
$$= exp(r+s)$$

□

Corolario 3.2. *Si $r \in R$, $d \in \mathbb{N}$ y se tiene la ecuación $exp(r) = S^d$ con $S \in [\![R]\!]$ a ser determinado, entonces $S = exp\left(\frac{r}{d}\right)$, es una solución de la ecuación.*

Demostración. Sean r y d como en el enunciado. Como

$$\begin{aligned} exp\left(\frac{r}{d}\right)^d &= \prod_{i=1}^{d} exp\left(\frac{r}{d}\right) \\ &= exp\left(\sum_{i=1}^{d} \frac{r}{d}\right) \\ &= exp\left(d\frac{r}{d}\right) \\ &= exp(r) \end{aligned}$$

□

Teorema 3.2. *Si $\mathbb{Q} \subset R$, $d \in \mathbb{Z}^+$ y $a \in \mathcal{M}(R)$ es exponencialmente multiplicativa, entonces existe $f \in \mathcal{A}(R)$ tal que $f^{*d} = a$ y*

$$f(p^k) = \frac{1}{k!} \frac{a^k(p)}{d^k}$$

Demostración. Como $a \in \mathcal{M}(R)$, $a(1) = 1 \in R^*$. Así, el polinomio,

$$T(g) = g^{*d} - a \in \mathcal{A}(R)[g]$$

es tal que

$$F_T(x) = x^d - a(1) = x^d - 1;$$

donde 1 es raíz de $F_T(x)$, además $F'(1) = d$, y como $\mathbb{Q} \subset R$, $d \in R^*$. Ahora, por el **teorema 5.1** existe $f \in \mathcal{A}(R)$ tal que $T(f) = 0$ y $f(1) = 1$.
Sea $p \in \mathbb{P}$. Por el **Lema 5.1**, el isomorfismo $\phi_p : \mathcal{A}_p(R) \to R[\![x]\!]$, cumple que;

$$\phi(\pi_p(a)) = \sum_{k=0}^{\infty} a(p^k)x^k = \sum_{k=0}^{\infty} \frac{a(p)^k}{k!} x^k = exp(a(p)) \tag{2}$$

y que

$$\phi(\pi_p(f)^{*d}) = \phi(\pi_p(f))^d = \left(\sum_{k=0}^{\infty} f(p^k)x^k\right)^d \tag{3}$$

Como $\phi(\pi_p(f)^{*d}) = \phi(\pi_p(a))$, de las ecuaciones (2) y (3) se cumple que

$$\left(\sum_{k=0}^{\infty} f(p^k)x^k\right)^d = exp(a(p))$$

Entonces, por el corolario de la **Proposición 3.1**, $exp\left(\frac{a(p)}{d}\right)$ es una solución, luego

$$\sum_{k=0}^{\infty} f(p^k)x^k = exp\left(\frac{a(p)}{d}\right) = \sum_{k=0}^{\infty} \frac{a(p)^k}{k!d^k}x^k$$

Por lo tanto, por la igualdad de las series de potencia formales se sigue la igualdad $f(p^k) = \frac{1}{k!}\frac{a(p)^k}{d^k}$.

□

Conclusiones

El anillo de funciones aritméticas tiene ciertas propiedades algebraicas que se desprenden directamente de las propiedades de $\mathbb{C}$. Si se decide cambiar el anillo sobre el cual las funciones toman valores, es posible apreciar de forma clara algunas de estas, como es el caso de ser dominio de integridad o ser local. A su vez identificaron propiedades en $\mathcal{A}(R)$ que no dependen del anillo; por ejemplo, que $\mathcal{A}$ no sea Noetheriano ni un cuerpo, no dependen de las propiedades de $\mathbb{C}$ si no de la misma estructura en $\mathcal{A}(R)$. Por ultimo, se ha encontrado una manera de generalizar algunas propiedades de los polinomios con coeficientes en el anillo de funciones aritméticas para las funciones $R-$aritméticas, restringiendo a R a cierto tipo de anillos.

Bibliografía

[1] Goswami, A. (2023) Some remarks on the ring of arithmetical functions, arXiv.org. Available at: https://arxiv.org/abs/2302.01072 (Accessed: 25 November 2023).

[2] Glöckner, H., Lucht, L.G. and Porubský, Š. (2007) 'Solutions to arithmetic convolution equations', Proceedings of the American Mathematical Society, 135(6), pp. 1619–1629. doi:10.1090/s0002-9939-07-08738-2.

[3] Elliott, J. (2008) 'Ring structures on groups of arithmetic functions', Journal of Number Theory, 128(4), pp. 709–730. doi:10.1016/j.jnt.2007.07.011.

[4] Grillet, P.A. (2007) Abstract Algebra (1 vols). 2nd edn. Springer (GTM).

[5] Herstein, I.N. (1975) Topics in Algebra. New York: Wiley.

[6] Cashwell, E. D. and Everett, C. J., The ring of number-theoretic functions, Pacific Jour. Math, (1959) 9, 975–985.

[7] Castañeda García, A. (2023). La función zeta de Riemann y su relación con otras funciones aritméticas. Escuela Colombian de Ingeniería.