# SOBRE ANILLOS FUERTEMENTE UNITARIOS Y CASI FUERTEMENTE UNITARIOS

ANDRÉS FELIPE CRUZ LÓPEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2024

# SOBRE ANILLOS FUERTEMENTE UNITARIOS Y CASI FUERTEMENTE UNITARIOS

ANDRÉS FELIPE CRUZ LÓPEZ

Trabajo de grado para optar al título de
Matemático

Director
Héctor Edonis Pinedo Tapia
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2024

## DEDICATORIA

Para mi madre, a quien le debo toda mi carrera profesional.
Para mi abuela, el más tierno de mis amores.

## AGRADECIMIENTOS

Gracias a Dios, Padre que nunca me ha abandonado y por quien todo esto fue posible.
Gracias a mi madre, por su fortaleza, su fuerza y su amor y apoyo incondicional.
Gracias a Natalia, amiga incondicional. Por su disponibilidad y paciencia.
Gracias a Javier, por su paciencia y su generosidad.
Gracias a mi familia.

**CONTENIDO**

## RESUMEN

**TÍTULO:** SOBRE ANILLOS FUERTEMENTE UNITARIOS Y CASI FUERTEMENTE UNITARIOS [*]

**AUTOR:** ANDRÉS FELIPE CRUZ LÓPEZ [**]

**PALABRAS CLAVE:** ANILLO UNITARIO, CUERPOS, CARACTERÍSTICA DE UN CUERPO, ANILLOS ARTINIANOS, ANILLOS REDUCIDOS, CUERPO ABSOLUTAMENTE ALGEBRAICO

**DESCRIPCIÓN:**El anillo $\mathbb{Z}_6$ de los enteros módulo $6$, cumple la propiedad de que posee identidad multiplicativa y además todos sus subanillos propios también posee uno. Se le ha dado el nombre de Anillos fuertemente unitarios a todos los anillos que cumplen la misma propiedad que $\mathbb{Z}_6$, esto es anillos que son unitarios y además todos sus subanillos propios también poseen uno (aunque no siempre coincida con el uno del anillo). De la misma manera también se denota por Anillos casi fuertemente unitarios a los anillos $R$ que no poseen identidad multiplicativa pero todos sus subanillos propios sí poseen uno. En este trabajo presentaremos una caracterización sencilla de los anillos fuertemente unitarios y de los anillos casi fuertemente unitarios y analizaremos su naturaleza relacionándolos con cuerpos absolutamente algebraicos de característica prima.

El documento se encuentra estructurado de la siguiente manera: en el primer capítulo, llamado Preliminares, se presentan algunas nociones sobre ideales, cuerpos y anillos artinianos que serán necesarias manejar por parte del lector para una buena comprensión de las siguientes secciones. En el capítulo posterior se presenta la definición de anillos fuertemente unitarios y se proporciona una caracterización de los mismos, relacionándolos con cuerpos de característica prima. Por último se exponen las principales características de la naturaleza de los anillos casi fuertemente unitarios, a la vez que se proporciona algunos teoremas que permiten diferenciarlos, en un tercer capítulo llamado Anillos casi fuertemente unitarios. Finalmente se encuentran los documentos y fuentes bibliográficas que se utilizaron en la realización de este trabajo en el apartado llamado Bibliografía.


---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

## ABSTRACT

**TITLE:** ON STRONGLY UNITAL RINGS AND ALMOST STRONGLY UNITAL RINGS [*]

**AUTHOR:** ANDRÉS FELIPE CRUZ LÓPEZ [**]

**KEYWORDS:** UNITAL RING, FIELDS, CHARACTERISTIC OF A FIELD, ARTINIAN RINGS, REDUCED RINGS, ABSOLUTELY ALGBRAIC FIELD.

**DESCRIPTION:**The ring $Z_6$ of integers modulo $6$ satisfies the property of having identity, and furthermore, all its proper subrings also have one. Rings that satisfy the same property as $Z_6$ are called strongly unital rings, which are rings that have one and all their proper subrings also have one (although it may not always coincide with the one of the ring). Similarly, Rings that don't have identity but all their proper subrings have one are denoted as almost strongly unitary Rings. In this paper, we will present a simple characterization of strongly unital rings and almost strongly unitarl rings and analyze their nature by relating them to absolutely algebraic fields of prime characteristic.

The document is structured as follows: in the first chapter, titled Preliminaries, some notions about ideals, fields, and artinian rings are presented, which will be necessary for the reader to grasp for a good understanding of the following sections. In the subsequent chapter, the definition of strongly unitarl rings is presented, along with a characterization of them, relating them to fields of prime characteristic. Finally, the main characteristics of the nature of almost strongly unital rings are exposed, while providing some theorems that allow distinguishing them, in a third chapter called Almost Strongly Unital Rings. Finally, the documents and bibliographic sources used in the completion of this work are found in the Bibliography section.


---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

## Introducción

Un anillo $(R, +, \cdot)$ es llamado unitario o unital si contiene un elemento identidad bajo la operación multiplicación, es decir, si existe un elemento $1_R \in R$ tal que $1_R \cdot a = a \cdot 1_R = a$, para todo $a$ en $R$. El elemento $1_R$ es llamado el unitario de $R$ o simplemente el 'uno' de $R$. Dado un subanillo propio $S$ de un anillo $R$ podemos encontrarnos en diferentes situaciones: $R$ es unitario pero $S$ no lo es, como en el caso de los enteros $\mathbb{Z}$, cuyo subanillo propio $2\mathbb{Z}$ no tiene uno; o que $R$ no es unital y sin embargo $S$ sí lo es, por ejemplo: el anillo $R := \left\{ \left( \begin{smallmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & c \end{smallmatrix} \right) | a, b, c \in \mathbb{R} \right\}$ no es unitario pero su subanillo $S := \left\{ \left( \begin{smallmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix} \right) | a \in \mathbb{R} \right\}$ sí lo es. Por último el caso en que tanto $R$ como $S$ son unitarios (aunque no necesariamente el uno de $S$ coincida con el uno de $R$), tal como $\mathbb{Z}_6$ cuyos subanillos son:

$$
\begin{aligned}
S_0 &= \{\bar{0}\} \\
S_1 &= \{\bar{0}, \bar{3}\} \\
S_2 &= \{\bar{0}, \bar{2}, \bar{4}\} \\
S_3 &= \mathbb{Z}_6
\end{aligned}
$$

y con algunos sencillos cálculos se puede comprobar que $1_{S_0} = \bar{0}, 1_{S_1} = \bar{3}, 1_{S_2} = \bar{4}$ y $1_{S_3} = \bar{1}$. Es decir que todo subanillo de $\mathbb{Z}_6$ es unitario. Los autores Oman y Stroud han llamado anillos fuertemente unitarios en el artículo [1] a los anillos que cumplen la misma propiedad mostrada de $\mathbb{Z}_6$. De acuerdo con esto, en [2] Oman y Senkoff han llamado anillos casi fuertemente unitarios a los anillos $R$ que no poseen identidad multiplicativa pero todos sus subanillos propios sí poseen uno.

El fundamento de este trabajo está en estudiar la clasificación de los anillos fuertemente unitarios, es decir, queremos encontrar todos los anillos $R$, salvo isomorfismos, tales que todo subanillo de $R$ sea unitario. También queremos presentar una caracterización de los anillos casi fuertemente unitarios utilizando cuerpos absolutamente algebraicos con característica prima.

---

[1] John OMAN Greig y STROUD. "Rings whose subrings have an identity". En: *Involve* 13.5 (2020), págs. 823-828.

[2] Evan OMAN Greig y SENKOFF. "Almost strongly unital rings". En: *Involve* (2022). URL: https://www.researchgate.net/publication/362013228_Almost_strongly_unital_rings.

# 1. Preliminares

En este capítulo se presenta información imprescindible para la comprensión y desarrollo del tema a estudiar en el presente trabajo. En primer lugar se exponen algunas nociones acerca de anillos cocientes y cuerpos, seguidamente se hace una breve introducción a la teoría de módulos culminando con la presentación de módulos y anillos artinianos. La lectura de este capítulo permitirá al interesado situarse de buena manera en el área científica en el que se desenvuelve este estudio.

## 1.1. Ideales y anillos cocientes

A continuación presentamos las definiciones de ideales y anillo cociente que permitirá una mejor comprensión de la naturaleza de los anillos casi fuertemente unitarios que serán presentados en los siguientes capítulos.

**Definición 1.1.1.** *Dado un anillo $R$ y un subanillo $I \leq R$ decimos que $I$ es un ideal de $R$, y escribiremos $I \lhd R$, si $y \cdot x \in I$ y $x \cdot y \in I$ para cualquier $x \in I$ y cualquier $y \in R$.*

**Ejemplo 1.1.2.** *Sea $n \in \mathbb{Z}$, entonces $n\mathbb{Z} = \{n \cdot a | a \in \mathbb{Z}\}$ es un ideal de $\mathbb{Z}$.*

**Proposición 1.1.3.** *Sea $R$ un anillo e $I \lhd R$. La relación $x \sim y \iff x - y \in I$ para todos $x, y \in R$ es un relación de equivalencia en $R$.*

**Definición 1.1.4.** *Sea $R$ un anillo e $I \lhd R$. El anillo $R/I = \{[x] | x \in R\}$ es llamado el **anillo cociente** de $R$ en $I$, donde $[x] = \{x + z : z \in I\}$ es la clase de equivalencia de $x \in R$ vía la relación presentada en la Proposición 1.1.3. La adición y la multiplicación de las clases están dadas por $[x] + [y] = [x + y]$ y $[x][y] = [xy]$ respectivamente, para todo $x, y \in R$.*

**Ejemplo 1.1.5.** *Sean $a, n \in \mathbb{Z}^+$. Considerando el ideal $I = n\mathbb{Z}$ de $\mathbb{Z}$, se obtiene que la relación de equivalencia de la Proposición 1.1.3 coincide exactamente con la relación de congruencia módulo $n$ en los enteros. Sabemos además que $a$ es congruente módulo $n$ con uno y solo un entero del conjunto $\{0, 1, \ldots, n-1\}$, de esta manera obtenemos el anillo cociente $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.*

**Definición 1.1.6.** *Sean $(R, +, \cdot)$ y $(S, \oplus, \circ)$ anillos. Una función $f : R \to S$ es llamada un **homomorfismo de anillos** si se cumple que*

I) $f(r + s) = f(r) \oplus f(s)$;

II) $f(r \cdot s) = f(r) \circ f(s)$

*para todos $r, s \in R$. Si un homomorfismo $f : R \to S$ es biyectivo diremos que es un* ***isomorfismo de anillos****, en ese caso diremos que $R$ y $S$ son isomorfos y lo notaremos por $R \cong S$.*

**Ejemplo 1.1.7.** *Sea $R$ un anillo e $I$ un ideal de $R$. La función $\phi : R \to R/I$ dada por $\phi(r) = r + I$ es un homomorfismo de anillos.*

Finalizamos esta sección recordando algunas nociones de teoría de Grupos que serán de utilidad en los siguientes resultados.

**Proposición 1.1.8.** ***(Teorema de Lagrange)*** *Sea $G$ un grupo finito y sea $H$ un subgrupo arbitrario de $G$. Entonces el orden de $H$ divide al orden de $G$.*

*Demostración.* Sean $G$ y $H$ como se mencionaron anteriormente. Como $G$ es finito, la relación de equivalencia dada por $g \sim f \Leftrightarrow gf^{-1} \in H$ con $f, g \in G$ define una cantidad finita de clases de equivalencia en $G$. Sea $n$ la cantidad de clases de equivalencia. Como todas las clases son disyuntas y además cada una posee $|H|$ elementos, entonces $n|H| = |H| + \cdots + |H| = |G|$. Luego el orden de $H$ divide al orden de $G$. □

Resaltamos también que la afirmación recíproca del Teorema de Lagrange no es siempre verdadera. En efecto, el grupo $A_4$ de todas las permutaciones pares de un conjunto de cuatro elementos tiene orden igual a $12$ y sin embargo es sencillo probar que no posee ningún subgrupo que contenga exactamente $6$ elementos. De todos modos es verdadero que si $G$ es un grupo abeliano finito con $n$ elementos y $m$ divide a $n$, entonces existe un subgrupo $H$ de $G$ que contiene exactamente $m$ elementos. Para finalizar recordemos que dado un grupo $G$ y $H$ un subgrupo de $G$, $H$ es llamado **subgrupo normal** de $G$ si $gng^{-1} \in H$ para todo $g \in G$ y $n \in H$. Un grupo $G$ es llamado **simple** si sus únicos subgrupos normales son sus subgrupos triviales.

## 1.2. Cuerpos

**Definición 1.2.1.** *Un* ***cuerpo*** *es un anillo conmutativo $\mathbb{F}$ con unidad en el que todo sus elementos no nulos son invertibles.*

**Ejemplo 1.2.2.** *Los conjuntos de los números racionales y los números reales, denotados por $\mathbb{Q}$ y $\mathbb{R}$ respectivamente, son cuerpos. Se suele denotar por $\mathbb{F}_q$ a un cuerpo finito $\mathbb{F}$ formado por $q$ elementos. El conjunto $\mathbb{Z}_p$ de los enteros módulo $p$ con $p$ primo, es un cuerpo finito con $p$ elementos.*

Dado un elemento $a$ en un cuerpo $\mathbb{F}$ y $n \in \mathbb{Z}$, denotamos por $n \cdot a$ la suma $a + a + ... + a$ con $n$ sumandos si $n > 0$ y $(-a) + (-a) + ... + (-a)$ con $|n|$ sumandos si $n < 0$; mientras que $n \cdot a = 0$ cuando $n = 0$. El conjunto $\langle a \rangle := \{n \cdot a : n \in \mathbb{Z}\}$ es llamado el **generado** de $a$.

**Definición 1.2.3.** *Sea $\mathbb{F}$ un cuerpo. La **característica** de $\mathbb{F}$ es el menor entero positivo $n$ tal que $n \cdot 1_{\mathbb{F}} = 0$. Si no existe tal entero, decimos que $\mathbb{F}$ tiene característica cero.*

**Ejemplo 1.2.4.** *$\mathbb{Z}_p$ con $p$ primo, es un cuerpo finito con característica $p$. Los conjuntos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son cuerpos infinitos con característica $0$.*

Percatémonos de que si $\{\mathbb{F}_i\}_{i \in I}$ es una familia de cuerpos tales que $1_{\mathbb{F}_i}$ es el mismo uno para cada cuerpo con $i \in I$, entonces $\bigcap_{i \in I} \mathbb{F}_i$ es un cuerpo. En efecto, es claro que $\bigcap_{i \in I} \mathbb{F}_i$ es conmutativo y además $1_{\mathbb{F}} \in \bigcap_{i \in I} \mathbb{F}_i$ por lo que la intersección no es vacía. Tampoco es difícil ver que $1_{\mathbb{F}}$ es también el uno de la intersección. Dado un elemento no nulo $x \in \bigcap_{i \in I} \mathbb{F}_i$, $x \in \mathbb{F}_i$ para todo $i \in I$, luego $x \in F_j$ para algún $j \in I$ y como $\mathbb{F}_j$ es cuerpo, existe un elemento $y \in \mathbb{F}_j$ tal que $xy = 1_{\mathbb{F}}$. Suponga que existe un $i \in I$ tal que $y \notin \mathbb{F}_i$ entonces como $x$ también pertenece a $\mathbb{F}_i$ y $\mathbb{F}_i$ es cuerpo, existe un elemento $z \in \mathbb{F}_i$ tal que $xz = 1_{\mathbb{F}} = xy$, esto es $x(z - y) = 0$ y como tanto $\mathbb{F}_i$ como $\mathbb{F}_j$ no poseen divisores de cero, entonces $z = y$. De esta manera $y \in \bigcap_{i \in I} \mathbb{F}_i$ y entonces todo elemento no nulo de $\bigcap_{i \in I} \mathbb{F}_i$ es invertible.

**Definición 1.2.5.** *Sea $\mathbb{F}$ un cuerpo. $P(\mathbb{F}) = \bigcap\{B \subset \mathbb{F} : B$ es subcuerpo de $\mathbb{F}\}$ es un subcuerpo de $\mathbb{F}$ llamado **subcuerpo primo** de $\mathbb{F}$. Se dice que $\mathbb{F}$ es un cuerpo primo si coincide con su subcuerpo primo.*

**Ejemplo 1.2.6.** *$\mathbb{Q}$ es el subcuerpo primo de $\mathbb{C}$. En efecto, si $\mathbb{F}$ es un subcuerpo de $\mathbb{C}$ entonces $1 \in \mathbb{F}$ y $\{n \cdot 1 : n \in \mathbb{Z}\} = \mathbb{Z} \subseteq \mathbb{F}$. Como $\mathbb{F}$ es cuerpo, para un entero $m \neq 0$, $m^{-1} = 1/m \in \mathbb{F}$ y por lo tanto $n/m \in \mathbb{F}$. Concluimos que $\mathbb{Q} \subseteq \mathbb{F}$ para cualquier subcuerpo $\mathbb{F}$ de $\mathbb{C}$ y así $\mathbb{Q} \subseteq P(\mathbb{C})$ y como $\mathbb{Q}$ es un subcuerpo de $\mathbb{C}$, $\mathbb{Q} = P(\mathbb{C})$.*

**Proposición 1.2.7.** *Sea $\mathbb{F}$ un cuerpo, entonces*

I) *El subcuerpo primo de $\mathbb{F}$ es el subcuerpo generado por $1_{\mathbb{F}}$;*

II) *$\mathbb{F}$ tiene característica cero o $\mathbb{F}$ tiene característica $p$, con $p$ un número primo;*

III) *Si $\mathbb{F}$ tiene característica cero, $P(\mathbb{F}) \cong \mathbb{Q}$; mientras que si $p > 0$ es la característica de $\mathbb{F}$, entonces $P(\mathbb{F}) \cong \mathbb{Z}_p$.*

*Demostración.* I) Sea $\mathbb{F}$ un cuerpo y $\mathbb{K}$ un subcuerpo de $\mathbb{F}$, entonces $1_{\mathbb{F}} \in \mathbb{K}$ y como $\mathbb{K}$ es cuerpo, el subcuerpo generado por $1_{\mathbb{F}}$ está contenido en $\mathbb{K}$. Como $\mathbb{K}$ es un subcuerpo arbitrario de $\mathbb{F}$ entonces el subcuerpo generado por $1_{\mathbb{F}}$ está contenido en $P(\mathbb{F})$ y así $P(\mathbb{F})$ es igual al subcuerpo generado por $1_{\mathbb{F}}$.

II) Sea $\mathbb{F}$ un cuerpo. Suponga que $\mathbb{F}$ tiene característica $n > 0$. Considere la función $\phi : \mathbb{Z} \to \mathbb{F}$ dado por $\phi(n) = n \cdot 1_{\mathbb{F}}$. Claramente $\phi$ es un homomorfismo de anillos. Como $Ker\phi \triangleleft \mathbb{Z}$ entonces $Ker\phi = m\mathbb{Z}$ para algún entero $m$. Como $n$ es la característica de $\mathbb{F}$ entonces $Ker\phi = n\mathbb{Z}$ y por el primer teorema de homomorfismos de anillos se cumple que $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong \phi(\mathbb{Z}) \subseteq \mathbb{F}$. Por otro lado si $n$ no es primo, $\mathbb{Z}_n$ tiene divisores de cero, luego $\mathbb{F}$ tendría divisores de cero, una contradicción puesto que $\mathbb{F}$ es cuerpo. Entonces $n$ es primo.

III) Si $\mathbb{F}$ tiene característica cero, la función $\gamma : \mathbb{Q} \to \mathbb{F}$ dada por $\gamma(m/n) = (m1_{\mathbb{F}})(n1_{\mathbb{F}})^{-1}$ es un homomorfismo de anillos inyectivo. En efecto, si $\gamma(m/n) = (m1_{\mathbb{F}})(n1_{\mathbb{F}})^{-1} = 0$ entonces $m1_{\mathbb{F}} = 0$ y como la característica de $\mathbb{F}$ es cero entonces $m = 0$. En este sentido, $\mathbb{Q}$ es el cuerpo *más pequeño* de característica cero y todo cuerpo de característica cero tiene un subcuerpo $\gamma(\mathbb{Q})$ isomorfo a $\mathbb{Q}$. Por otra parte, teniendo en cuenta el homomorfismo $\phi$ presentado en el ítem anterior, $\mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z}$ es isomorfo a un subanillo del cuerpo $P(\mathbb{F})$, por lo tanto siguiendo el procedimiento presentado en el Ejemplo 1.2.6, $P(\mathbb{F})$ contiene un subcuerpo $\mathbb{K}$ isomorfo a $\mathbb{Q}$, pero como $P(\mathbb{F})$ es el menor subcuerpo de $\mathbb{F}$, entonces $P(\mathbb{F}) = \mathbb{K} \cong \mathbb{Q}$. Si $\mathbb{F}$ tiene característica $p$ con $p$ primo, entonces $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \phi(\mathbb{Z})$. Como $p$ es primo, $\mathbb{Z}_p$ es cuerpo y así $\mathbb{Z}_p \cong \phi(\mathbb{Z}) = P(\mathbb{F})$.

□

**Ejemplo 1.2.8.** *Note que $\mathbb{Z}_p$ con $p$ primo es un cuerpo con característica $p$ y por el ítem III) de la Proposición 1.2.7, $P(\mathbb{Z}_p) = \mathbb{Z}_p$. Concluimos que $\mathbb{Z}_p$ es un cuerpo primo.*

Dado un cuerpo $\mathbb{F}$ denotaremos por $\mathbb{F}[x]$ al anillo formado por todos los polinomios en la variable $x$ con coeficientes en $\mathbb{F}$. Escribiremos como $x\mathbb{F}[x]$ el subanillo de polinomios de $\mathbb{F}[x]$ cuyo término constante es igual a cero. En el siguiente ejemplo proporcionamos, a partir de un cuerpo finito $\mathbb{F}_p$, un anillo que posee exactamente $p$ elementos y que además al multiplicar dos de sus elementos, escogidos arbitrariamente, se obtiene siempre un resultado nulo.

**Ejemplo 1.2.9.** *Sea $\mathbb{F}_p = \{0, \alpha_1, \cdots, \alpha_{p-1}\}$ un cuerpo finito con $p$ elementos. El conjunto $\langle x^2 \rangle$ es un ideal del anillo $x\mathbb{F}_p[x]$. Sean $f(x), g(x) \in x\mathbb{F}_p[x]$, entonces el grado de $(fg)(x)$*

*es mayor o igual que* $2$*. Luego* $(fg)(x) = x^2h(x) + \alpha x^2$*, para algún* $h(x) \in x\mathbb{F}_p[x]$ *y* $\alpha \in \mathbb{F}_p$*. Como* $h(x), \alpha x^2 \in \langle x^2 \rangle$ *entonces* $(fg)(x) \in [0]$ *del anillo cociente* $x\mathbb{F}_p[x]/\langle x^2 \rangle$*. Esto implica que* $x\mathbb{F}_p[x]/\langle x^2 \rangle$ *tiene multiplicación nula. Afirmamos que* $x\mathbb{F}_p[x]/\langle x^2 \rangle = \{[0], [\alpha_1 x], [\alpha_2 x], \cdots, [\alpha_{p-1} x]\}$*. En efecto, dado* $f(x) = \beta_n x^n + \cdots + \beta_1 x \in x\mathbb{F}_p[x]$*, entonces* $f(x) - \beta_1 x \in \langle x^2 \rangle$ *lo que implica que* $[f(x)] = [\beta_1 x]$*. Por otro lado es claro que si* $\alpha_i \neq \alpha_j$ *entonces* $[\alpha_i x] \neq [\alpha_j x]$*. De esta manera el anillo* $x\mathbb{F}_p[x]/\langle x^2 \rangle$ *posee* $p$ *elementos y tiene multiplicación trivial.*

**Definición 1.2.10.** *Sea* $\mathbb{F}$ *un cuerpo. Decimos que el cuerpo* $\mathbb{K}$ *es una* ***extensión*** *de* $\mathbb{F}$ *y escribiremos* $\mathbb{K}/\mathbb{F}$*, si* $\mathbb{F} \subset \mathbb{K}$*.*

**Definición 1.2.11.** *Sea* $\mathbb{K}/\mathbb{F}$ *una extensión de cuerpos y* $\alpha \in \mathbb{K}$*. Decimos que* $\alpha$ *es* ***algebraico*** *sobre* $\mathbb{F}$ *si existe un polinomio no nulo* $f(x) \in \mathbb{F}[x]$ *tal que* $f(\alpha) = 0$*. Si* $\alpha$ *no es algebraico se dice que* $\alpha$ *es* ***trascendente*** *sobre* $\mathbb{F}$*. El cuerpo* $\mathbb{K}$ *es llamado una* ***extensión algebraica*** *de* $\mathbb{F}$ *si todo elemento* $\alpha \in \mathbb{K}$ *es algebraico sobre* $\mathbb{F}$*.*

**Ejemplo 1.2.12.** *El número real* $\alpha = \sqrt{1 + \sqrt{3}}$ *es algebraico sobre* $\mathbb{Q}$*, pues* $\alpha$ *es un cero del polinomio* $x^4 - 2x^2 - 2$ *que está en* $\mathbb{Q}[x]$*.*

**Ejemplo 1.2.13.** *El número real* $\pi$ *es trascendente sobre* $\mathbb{Q}$*, sin embargo* $\pi$ *es algebraico sobre* $\mathbb{R}$*. Para una demostración de la trascendencia de* $\pi$ *el lector interesado puede consultar en* [3]*.*

Finalizamos esta sección con la definición de cuerpo absolutamente algebraico, objeto de vital importancia para la caracterización de los anillos fuertemente unitarios.

**Definición 1.2.14.** *Un cuerpo* $\mathbb{F}$ *es* ***absolutamente algebraico*** *si es algebraico sobre su subcuerpo primo.*

**Ejemplo 1.2.15.** *Sea* $\mathbb{K}/\mathbb{F}$ *una extensión de cuerpos y* $\alpha \in \mathbb{K}$*, definimos* $\mathbb{K}(\alpha) = \{f(\alpha) : f \in \mathbb{F}[x]\}$*. De acuerdo con esto,* $\mathbb{Q}(\sqrt{2})$ *es un cuerpo absolutamente algebraico pues es algebraico sobre* $\mathbb{Q}$ *que es su subcuerpo primo.*

### 1.3. Módulos y anillos artinianos

En esta sección presentamos una sencilla introducción a la teoría de módulos que permitirá ubicarse bien al lector para el cual esta área del álgebra es completamente

[3] Steve MAYER. *The Transcendence of* $\pi$. URL: `https://sixthform.info/maths/files/pitrans.pdf`.

ajena. Nos enfocamos principalmente en la noción de un anillo $R$ como un $R-$Módulo sobre sí mismo y la definición de módulos artinianos.

**Definición 1.3.1.** *Sea $(R, +, \cdot, 1_R)$ un anillo unitario. Un grupo abeliano $(M, +)$ se dice que tiene estructura de módulo a izquierda sobre el anillo $R$ o que es un $R$-**Módulo a izquierda** si existe una ley de composición externa por la izquierda entre $R$ y $M$, que a cada par $(r, m) \in R \times M$ le asocia un elemento $rm \in M$ tal que:*

I) $r_1(r_2m_1) = (r_1r_2)m_1$;

II) $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$;

III) $(r_1 + r_2)m_1 = r_1m_1 + r_2m_1$;

IV) $1_Rm_1 = m_1$;

*para todos $r_1, r_2 \in R$ y $m_1, m_2 \in M$.*

*De manera análoga se puede definir un $R$-módulo a la derecha. De ahora en adelante trabajaremos únicamente con $R-$módulos a la izquierda, para ello usaremos simplemente la expresión $R-$módulo, sin peligro de confusión.*

**Ejemplo 1.3.2.** *Todo espacio vectorial $V$ sobre un cuerpo $\mathbb{K}$ es un $\mathbb{K}$-módulo.*

**Ejemplo 1.3.3.** *Sea $I$ un ideal de un anillo $R$. Entonces $I$ es un $R-$módulo con la suma inducida por $R$ y la multiplicación heredada de $R$. De esta manera, si hacemos $I = R$, obtenemos que todo anillo $R$ es un $R-$módulo sobre sí mismo.*

**Definición 1.3.4.** *Sea $M$ un $R-$Módulo y $(N, +)$ un subgrupo de $(M, +)$. Diremos que $N$ es un $R-$submódulo de $M$, o simplemente un **submódulo** de $M$, si $rn \in N$ para todo $r \in R$ y todo $n \in N$. En este caso escribiremos $N \leq M$ para denotar que $N$ es un submódulo de $M$.*

**Ejemplo 1.3.5.** *Considerando un anillo $R$ como ejemplo de $R-$módulo sobre sí mismo obtenemos que sus submódulos coinciden exactamente con sus ideales a izquierda.*

Sea $M$ un $R$-módulo, los subgrupos $\{0\}$ y $M$ son llamados los submódulos triviales de $M$. Un submódulo de $M$ que no coincida con los mencionados anteriormente es llamado un submódulo propio de $M$. Un módulo $M$ es llamado simple si no posee submódulos propios.

**Definición 1.3.6.** *Sea $M$ un $R-$Módulo sobre un anillo $R$. Un submódulo $N \neq M$ es un* ***submódulo maximal*** *en $M$ si*

$$N \subseteq N' \quad \Leftrightarrow \quad N' = N \quad \vee \quad N' = M$$

*para todo submódulo $N'$ de $M$.*

*Un submódulo $N \neq \{0\}$ es llamado* ***submódulo minimal*** *en $M$ si*

$$N' \subseteq N \quad \Leftrightarrow \quad N' = N \quad \vee \quad N' = \{0\}$$

*para todo submódulo $N'$ de $M$.*

**Ejemplo 1.3.7.** *Si $V$ es un $\mathbb{K}$-espacio vectorial sobre un cuerpo $\mathbb{K}$, los submódulos de $V$ son exactamente sus subespacios vectoriales. Si $V$ es de dimensión finita $n$, entonces sus subespacios de dimensión $n-1$ son sus submódulos maximales, y los minimales los de dimensión $1$. Si $V$ tiene dimensión infinita y base $\beta$, entonces sus subespacios minimales son como en el caso finito y para $b \in \beta$, el conjunto $\langle \beta \setminus \{b\} \rangle$ es un submódulo maximal de $V$.*

**Ejemplo 1.3.8.** *No todo módulo posee submódulos maximales o minimales. El conjunto de los números racionales $\mathbb{Q}$, considerandolo como un $\mathbb{Z}$-módulo, no posee submódulos minimales. En efecto dado un submódulo $\langle r \rangle$ de $\mathbb{Q}$ para un elemento no nulo $r \in \mathbb{Q}$, se cumple que $\langle 2r \rangle \subset \langle r \rangle$. Es decir, para todo submódulo $M$ de $\mathbb{Q}$ existe un submódulo $N \neq M$ de $\mathbb{Q}$ tal que $N \subset M$. $\mathbb{Q}$ tampoco posee sumbódulos maximales, la prueba de este hecho, relacionado con módulos finitamente generados, se puede encontrar en* [4] *p. 13.*

A continuación presentaremos la noción de homomorfismo de módulos y proporcionamos dos teoremas de homomorfismos de módulos que permiten relacionar algunos de sus submódulos.

**Definición 1.3.9.** *Sean $M$ y $N$ dos $R$-módulos. Una función $f : M \to N$ es un* ***homomorfismo de módulos*** *si para todos $m_1, m_2 \in M$ y todo $r \in R$ se cumple que*

---

[4] José Oswaldo LEZAMA. *Cuadernos de Álgebra*. Universidad Nacional de Colombia, 2020.

I) $f(m_1 + m_2) = f(m_1) + f(m_2)$;

II) $f(rm_1) = rf(m_1)$.

*De ahora en adelante escribiremos simplemente homomorfismo para referirnos a un homomorfismo de módulos cuando no haya peligro de confusión.*

**Ejemplo 1.3.10.** *La función identidad $1_M : M \to M$, donde cada elemento $m$ que pertenece a un $R-$módulo $M$ es enviado a sí mismo, es un homomorfismo de $R-$módulos. Diremos que un homomorfismo $f : M \to N$ es un **isomorfismo** si existe un homomorfismo $g : N \to M$ tal que $f \circ g = 1_N$ y $g \circ f = 1_M$.*

La siguiente proposición indica una manera alternativa de identificar si un homomorfismo es un isomorfismo de módulos.

**Proposición 1.3.11.** *Un homomorfismo $f : M \to N$ de $R$-módulos es un isomorfismo si y solo si $f$ es biyectiva.*

*Demostración.* Suponiendo que $f$ es un isomorfismo obtenemos que existe un homomorfismo $g$ tal que $g \circ f = 1_M$, esto implica que $f$ es inyectiva. De $f \circ g = 1_N$ se deduce que $f$ es a su vez sobreyectiva.
Por otro lado, si un homomorfismo $f : M \to N$ es biyectivo, entonces existe una función $g$ que es la inversa de $f$ y que verifica que $f \circ g = 1_N$ y $g \circ f = 1_M$. Basta probar que $g$ es un homomorfismo. Sean $n_1, n_2 \in N$. Como $f$ es sobreyectiva existen $m_1, m_2 \in M$ tal que $f(m_1) = n_1$ y $f(m_2) = n_2$. Ahora $g(n_1)+g(n_2) = g(f(m_1))+g(f(m_2)) = m_1+m_2$ y como $f$ es homomorfismo entonces $f(m_1+m_2) = n_1+n_2$, luego $m_1+m_2 = g(f(m_1+m_2)) = g(n_1+n_2)$. De esta manera se cumple que $g(n_1 + n_2) = g(n_1) + g(n_2)$. Además, si $r \in R$, existe un elemento $m \in M$ tal que $f(m) = n_1$, puesto que $f$ es sobreyectiva, esto es $m = g(f(m)) = g(n_1)$. Por otra parte, como $f$ es homomorfismo, $f(rm) = rf(m) = rn_1$ y aplicando $g$ a ambos lados de la ecuación obtenemos $rm = g(f(rm)) = g(rn_1)$, esto es $rg(n_1) = g(rn_1)$ y concluimos que $g$ es un homomorfismo. □

**Proposición 1.3.12.** *Sean $M$ y $N$ $R-$módulos y $f^* : M \to N$ un homomorfismo. Considere las funciones $j : M \to M/Ker(f^*)$ dada por $j(m) = m + Ker(f^*)$ para todo $m \in M$ y la función $i : Im(f^*) \to N$ dada por $i(n) = n$ para todo $n \in Im(f^*)$. Entonces existe una única función $f : M/Ker(f^*) \to Im(f^*)$ tal que*

I) $f^* = i \circ f \circ j$;

II) $f$ *es un isomorfismo.*

*Demostración.* Definamos la función $f : M/Ker(f^*) \to Im(f^*)$ dada por $f(m + Ker(f^*)) = f^*(m)$. Veamos que $f$ está bien definida. En efecto, si dado un representante $m \in M$ resulta que $m + Ker(f^*) = m' + Ker(f^*)$ para algún otro $m' \in M$, entonces $m - m' \in Ker(f^*)$, esto es $f^*(m - m') = f^*(m) - f^*(m') = 0$ de donde $f^*(m) = f^*(m')$. Como $f$ es un homomorfismo tenemos que $f^*$ también lo es. Ahora, dado un elemento $m \in M$ entonces $i(f(j(m))) = i(f(m + Ker(f^*))) = i(f^*(m)) = f^*(m)$ luego $f^* = i \circ f \circ j$. Por otro lado, como $f^* = i \circ f \circ j$ y el contradominio de $f$ es igual a $Im(f^*)$ tenemos que $f$ es sobreyectiva. Además si $m+Ker(f^*)$ y $m'+Ker(f^*)$ son dos clases de $M/Ker(f^*)$ tales que $f(m+Ker(f^*)) = f(m'+Ker(f^*))$ entonces $f^*(m) = f^*(m')$, luego $m-m' \in Ker(f^*)$ esto es $m + Ker(f^*) = m' + Ker(f^*)$. De esta manera $f$ es inyectiva y por lo tanto, biyectiva. Concluimos por la Proposición 1.3.11 que $f$ es un isomorfismo de módulos. □

La anterior proposición es de gran utilidad pues nos permite concluir que si $f : M \to N$ es un homomorfismo de $R$-módulos, entonces $\frac{M}{Ker(f)} \cong Im(f)$. La siguiente proposición, conocida en la literatura como el segundo teorema de isomorfismos de módulos, utilizará este isomorfismo para relacionar algunos cocientes de submódulos de un módulo $M$.

**Proposición 1.3.13.** ***(Segundo teorema de isomorfismos de módulos)*** *Sean $M_1$ y $M_2$ submódulos de un módulo $M$. Entonces se cumple que*

$$\frac{M_1}{M_1 \cap M_2} \cong \frac{M_1 + M_2}{M_2}.$$

*Demostración.* Definamos la función $f : M_1 \to \frac{M_1+M_2}{M_2}$ dada por $f(m) = m + M_2$ para todo $m \in M_1$. Claramente $f$ es un homomorfismo de módulos. Note que todo elemento de $\frac{M_1+M_2}{M_2}$ es de la forma $(m + n) + M_2$ para algún $m \in M_1$ y $n \in M_2$ y que además, como $(m + n) + M_2 = m + M_2$, $f(m) = m + M_2 = (m + n) + M_2$, luego $f$ es sobreyectiva. De acuerdo con lo anterior y con la Proposición 1.3.12 tenemos que $\frac{M_1}{Ker(f)} \cong Im(f) = \frac{M_1+M_2}{M_2}$. Por otro lado, dado un elemento $n \in M_1$, $n \in Ker(f)$ si y solo si $f(n) = n + M_2 = M_2$ es decir, si $n \in M_2$, de esta manera $Ker(f) = M_1 \cap M_2$. Concluimos que $\frac{M_1}{M_1 \cap M_2} \cong \frac{M_1+M_2}{M_2}$. □

**Definición 1.3.14.** *Dado un $R$-módulo $M$ y un subconjunto no vacío $S$ de $M$. Entonces el conjunto*

$$\langle S \rangle := \left\{ \sum_{i=1}^{n} r_i \cdot s_i : s_i \in S, r_i \in R, n \geq 1 \right\}$$

*es un submódulo de $M$ llamado* ***submódulo generado*** *por $S$.*

**Definición 1.3.15.** *Dado un $R$-módulo $M$ y una familia no vacía $\{M_i\}_{i\in I}$ de submódulos de $M$, llamamos* ***suma*** *de la familia, y notaremos por $\sum_{i\in I} M_i$, al submódulo generado por el conjunto $\bigcup_{i\in I} M_i$.*

Note que $\sum_{i\in I} M_i = \left\{\sum_{j=1}^{n} m_j : m_j \in \bigcup_{i\in I} M_i, n \geq 1\right\}$; luego $\sum_{i\in I} M_i$ es el menor submódulo de $M$ que contiene a todos los $M_i (i \in I)$ simultáneamente. Además para una familia finita de submódulos de $M$ se tiene que

$$M_1 + \cdots + M_n = \left\{\sum_{j=1}^{n} m_j : m_j \in M_j (1 \leq j \leq n)\right\}$$

**Proposición 1.3.16.** *Sea $\{M_i\}_{i\in I}$ una familia de submódulos de un $R-$módulo $M$. Las siguientes afirmaciones son equivalentes:*

I) *Todo elemento $m \in M$ se puede escribir de manera única como $m = \sum_{i\in I} m_i$ donde $m_i \in M_i$ para todo $i \in I$ y $m_i = 0$ excepto en una cantidad finita de índices $i$.*

II) *$M = \sum_{i\in I} M_i$ y si $\sum_{i\in I} m_i = 0$, con $m_i \in M$, entonces $m_i = 0$ para todo $i \in I$.*

III) *$M = \sum_{i\in I} M_i$ y $M_j \cap (\sum_{i\neq j} M_i) = \{0\}$ para todo $j \in I$.*

*Demostración.* Que todo elemento $m \in M$ se pueda escribir de manera única como $m = \sum_{i\in I} m_i$ donde $m_i \in M_i$ para todo $i \in I$ y $m_i = 0$ excepto en una cantidad finita de índices $i$ implica que $M \subseteq \sum_{i\in I} M_i$, entonces $M = \sum_{i\in I} M_i$. Además si $\sum_{i\in I} m_i = 0$ como $0 = \sum_{i\in I} 0_{M_i}$ y la representación de cada elemento es única, $m_i = 0$ para todo $i \in I$.
Por otro lado, dado un $j \in I$, sea $x \in M_j \cap (\sum_{i\neq j} M_i)$, entonces $x \in M_j$ y $x = \sum_{i\in I\setminus\{j\}} m_i$ con $m_i \in M_i$, $i \neq j$. Luego $0 = \sum_{i\in I} M_i$ donde $m_j = x$ y por II) $-x = m_j = 0$ entonces $x = 0$ y $M_j \cap (\sum_{i\neq j} M_i) = \{0\}$ para todo $j \in I$.
Finalmente suponga que existe un elemento $m \in M$ tal que $\sum_{i\in I} m_i = m = \sum_{i\in I} m'_i$. Entonces, para algún $j \in I$, $m_j - m'_j = \sum_{i\in I\setminus\{j\}} (m_i - m'_i) \in M_j \cap (\sum_{i\neq j} M_i) = \{0\}$, de esta manera $m_j = m'_j$ y entonces $m$ posee una representación única como suma de elementos de $M_i$ donde $m_i = 0$ excepto en una cantidad finita de índices. □

**Definición 1.3.17.** *Un $R-$módulo $M$ es llamado la* ***suma directa interna*** *de una familia $\{M_i\}_{i\in I}$ de submódulos de $M$ si cumple alguna y por tanto todas las condiciones equivalentes de la Proposición 1.3.16. Para denotar que $M$ es la suma directa de la familia $\{M_i\}_{i\in I}$ usaremos la notación $M = \bigoplus_{i\in I} M_i$.*

**Ejemplo 1.3.18.** *Sea $R$ un anillo unitario y considere el $R-$módulo sobre sí mismo. Sea $e \in R$ tal que $e^2 = e$, entonces $R = Re \bigoplus R(1-e)$. En efecto, dado un elemento $r \in R$ se cumple que $r = re + r - re = re + r(1-e) \in Re \bigoplus R(1-e)$ luego $R = Re + R(1-e)$. Por otro lado si $x \in Re \cap R(1-e)$ entonces existen $r, s \in R$ tal que $x = re$ y $x = s(1-e)$, luego $x = re = re^2 = xe = (s - se)e = se - se^2 = 0$.*

**Definición 1.3.19.** *Un $R-$módulo $M$ es llamado descomponible si existen $N_1, N_2$ submódulos propios de $M$ tal que $M = N_1 \bigoplus N_2$. En caso contrario se dice que $M$ es indescomponible.*

**Ejemplo 1.3.20.** *El anillo $\mathbb{Z}_6$ es descomponible. En efecto $\mathbb{Z}_6 = \{\bar{0}, \bar{2}, \bar{4}\} \bigoplus \{\bar{0}.\bar{3}\}$.*

**Ejemplo 1.3.21.** *Todo dominio entero $R$ es indescomponible. En efecto, si $e$ es un elemento idempotente de $R$, entonces $e(e-1) = 0$ y como $R$ es dominio entero, $e = 0$ ó $e = 1$. El Ejemplo 1.3.18 nos indica que $R = Re + R(1-e)$ luego los únicos submódulos de $R$ que cumplen esta condición son $\{0\}$ y $R$.*

Recordemos que dado un conjunto $A \neq \varnothing$, la relación de inclusión $\subseteq$ genera un orden parcial en el conjunto potencia de $A$. Un sucesión de elementos $(I_n)_{n\in\mathbb{N}}$ de partes de $A$ es llamada una **cadena descendente** si $I_{n+1} \subseteq I_n$ para todo $n \in \mathbb{N}$. Con frecuencia escribiremos una cadena descendente como $\cdots \subseteq I_n \subseteq \cdots \subseteq I_2 \subseteq I_1$.
Un subconjunto $I$ de $A$ es llamado una cota inferior de una sucesión $(I_n)_{n\in\mathbb{N}}$ si $I \subseteq I_n$ para todo $n \in \mathbb{N}$.

De manera recíproca se pueden definir las nociones de cadena ascendente y cota superior.

**Definición 1.3.22.** *Sea $R$ un conjunto no vacío. Una cadena descendente de subconjuntos $(I_n)_{n\in\mathbb{N}}$ de $R$ es llamada **estacionaria** si existe algún $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$ para todo $n > n_0$. Diremos que un conjunto $A$ de subconjuntos de $R$ cumple la **condición de cadena descendente (C.C.D)** si toda cadena descendente de $A$ es estacionaria.*

**Definición 1.3.23.** *Sea $M$ un $R-$Módulo. $M$ es llamado **artiniano** si el conjunto de sus submódulos, ordenado por la inclusión, cumple la condición de cadena descendente.*

**Ejemplo 1.3.24.** *Un espacio vectorial $V$ es de dimensión finita si y solo si es artiniano como un $\mathbb{K}-$módulo para un cuerpo $\mathbb{K}$. En efecto, si $V$ es dimensión finita entonces todos sus submódulos también lo son, luego toda cadena descendente de submódulos de $V$ es*

*estacionaria. Suponga que $V$ es dimensión infinita con base $\beta = \{\beta_1, \beta_2, \cdots\}$ entonces los submódulos $\cdots \subset \langle \beta \setminus \{\beta_1, \beta_2, \cdots, \beta_{n+1}\}\rangle \subset \langle \beta \setminus \{\beta_1, \beta_2, \cdots, \beta_n\}\rangle \subset \cdots \subset \langle \beta \setminus \{\beta_1, \beta_2\}\rangle \subset \langle \beta \setminus \{\beta_1\}\rangle$ de $V$ forman una cadena descendente infinita, luego $V$ no sería artiniano.*

Note que al considerar un anillo $R$ como un $R-$módulo sobre sí mismo, podemos decir también que $R$ es un anillo artiniano a izquierda si el conjunto de sus ideales cumplen la condición de cadena descendente. De forma análoga se puede definir un anillo artiniano a derecha. De ahora adelante nos fijaremos solo en el primer caso por lo que solo escribiremos **anillo artiniano** para decir que un anillo es artiniano a izquierda.

**Ejemplo 1.3.25.** *$\mathbb{Z}$ no es artiniano. En efecto, la sucesión descendente de los ideales $\{2^n\mathbb{Z}\}_{n\in\mathbb{N}}$ de $\mathbb{Z}$ no cumple la condición de cadena descendente pues $2^{n+1}\mathbb{Z} \subset 2^n\mathbb{Z}$ para todo natural $n$.*

**Proposición 1.3.26.** *Sea $M = M_1 + \cdots + M_k$ una suma finita (no necesariamente directa) de $R-$módulos. Entonces $M$ es artiniano si y solo si $M_1, ..., M_k$ son artinianos.*

*Demostración.* Suponga que $M$ es artiniano. Note que una cadena descendente de submódulos de $M_i$ es también una cadena descendente de submódulos de $M$ y es por lo tanto estacionaria. Luego $M_i$ es artiniano para todo $1 \leq i \leq k$. Para probar la afirmación recíproca haremos inducción matemática en $k$.
Para el caso base suponga $k = 2$, es decir $M = M_1 + M_2$. Entonces, echando mano de la Proposición 1.3.13, se cumple que

$$\frac{M}{M_1} = \frac{M_1 + M_2}{M_1} \cong \frac{M_2}{M_1 \cap M_2}$$

Como $M_2$ es artiniano y $M_1 \cap M_2$ es un submódulo de $M_2$ entonces $\frac{M_2}{M_1 \cap M_2}$ es artiniano. De esta manera $M_1$ y $M/M_1$ son artinianos. Veamos que $M$ es artiniano.
Sea $\cdots \subset M_n \subset \cdots \subset M_2 \subset M_1$ una cadena descendente de submódulos de $M$. Consideremos los módulos $M_i^{'} = M_i \cap M_1$ y $M_i^{''} = \frac{M_i + M_1}{M_1}$. Las cadenas $(M_i^{'})_{i\in\mathbb{N}}$ y $(M_i^{''})_{i\in\mathbb{N}}$ son estacionarias, entonces existe un natural $n_0$ tal que $M_i^{'} = M_{n_0}^{'}$ y $M_i^{''} = M_{n_0}^{''}$ para todo $i > n_0$. Del segundo teorema de isomorfismos tenemos que

$$\frac{M_1 + M_i}{M_1} = \frac{M_i}{M_1 \cap M_i}$$

esto es $\frac{M_i}{M_i^{'}} \cong M_i^{''}$. Entonces la cadena es estacionaria y así $M$ es artiniano.

Para el paso inductivo suponga que el resultado es válido para $k-1$ sumandos y que $M=(M_1+\cdots+M_{k-1})+M_k$ donde ambos sumandos son artinianos. De acuerdo al paso anterior $M$ también es artiniano. □

**Ejemplo 1.3.27.** *Sea $\{M_i\}_{i\in I}$ una familia de $R-$Módulos con $I$ un conjunto infinito numerable. Entonces $M=\bigoplus_{i\in I}M_i$ no es artiniano.*

*Demostración.* Suponga $I=\{i_1,i_2,\cdot,i_n,\cdots\}$. Entonces para $n\in\mathbb{N}$, los ideales

$$\cdots \bigoplus_{i\in I\setminus\{i_1,i_2,\cdots,i_{n+1}\}} M_i \subsetneq \bigoplus_{i\in I\setminus\{i_1,i_2,\cdots,i_n\}} M_i \subsetneq \cdots \subsetneq \bigoplus_{i\in I\setminus\{i_1,i_2\}} M_i \subsetneq \bigoplus_{i\in I\setminus\{i_1\}} M_i$$

forman una cadena estrictamente decreciente de ideales no nulos de $M$. Por lo tanto $M$ no sería artiniano. □

**Proposición 1.3.28.** *Sea $\{R_i\}_{1\leq i\leq n}$ una familia finita de anillos Artinianos. Entonces $R=R_1\times\cdots\times R_n$ es Artiniano.*

*Demostración.* Haremos la demostración para el caso $R=R_1\times R_2$ con $R_1$ y $R_2$ anillos artinianos. El resultado se puede extender de manera sencilla una cantidad finita de veces utilizando inducción matemática.
Podemos definir una estructura de $R-$módulo a izquierda en cada $R_1$ y $R_2$ de la siguiente manera:

$$\begin{aligned}(r_1,r_2)\cdot a_1 &= r_1\cdot a_1 \qquad \forall(r_1,r_2)\in R,\quad \forall a_1\in R_1\\ (r_1,r_2)\cdot a_2 &= r_2\cdot a_2 \qquad \forall(r_1,r_2)\in R,\quad \forall a_2\in R_2\end{aligned}$$

De acuerdo con el Ejemplo 1.3.5 los submódulos de $R_i$ son los ideales a izquierda de $R_i$ para $i=1,2$, entonces los $R-$módulos $R_1$ y $R_2$ son artinianos y por la Proposición 1.3.26, $R$ es artiniano. □

## 2. Anillos fuertemente unitarios

En este capítulo proporcionamos una introducción a los anillos fuertemente unitarios proporcionando algunas características de su naturaleza y finalizaremos con un resultado que permite caracterizar los anillos fuertemente unitarios a partir de cuerpos absolutamente algebraicos con característica prima.

### 2.1. Anillos fuertemente unitarios y anillos reducidos

Dado un anillo no nulo $R$ diremos que es un **anillo fuertemente unitario** si todo subanillo $S$ de $R$ tiene unidad.

**Ejemplo 2.1.1.** *El anillo $R = \mathbb{Z}_{15}$ es fuertemente unitario. En efecto, los subanillos de $\mathbb{Z}_{15}$ son $S_1 := \{\overline{0}\}$, $S_2 := \{\overline{0}, \overline{5}, \overline{10}\}$, $S_3 := \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$ y $S_4 := R$. La unidad de $S_1$ es $\overline{0}$, la unidad de $S_2$ es $\overline{10}$, la unidad de $S_3$ es $\overline{6}$, y el uno de $S_4$ es $\overline{1}$.*

Una observación natural que vale la pena resaltar es que si $R$ es un anillo fuertemente unitario, entonces todo subanillo no trivial de $R$ también lo es, puesto que todos sus subanillos serán también subanillos de $R$.

**Ejemplo 2.1.2.** *El anillo $\mathbb{Z}_6$ es fuertemente unitario y sus subanillos propios $R_2 = \{\overline{0}, \overline{2}, \overline{4}\}$ y $R_3 = \{\overline{0}, \overline{3}\}$ también lo son.*

Para el estudio de los anillos fuertemente unitarios necesitaremos hacer uso del concepto de elemento nilpotente el cual proporcionamos a continuación.

**Definición 2.1.3.** *Un elemento $\alpha$ de un anillo $R$ es llamado **nilpotente** si existe un entero positivo $n$ tal que $\alpha^n = 0$. Si $R$ no tiene elementos nilpotentes diferentes de cero, entonces se dice que $R$ es reducido.*

**Ejemplo 2.1.4.** *En $\mathbb{Z}_{16}$ la clase $\overline{4}$ es un elemento nilpotente pues $\overline{4}^2 = \overline{0}$ .*

**Ejemplo 2.1.5.** $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$ *es un anillo reducido. Más aún, todo dominio entero es un anillo reducido. En efecto, sea $r \in R \setminus \{0\}$ con $R$ un dominio entero tal que existe un entero positivo $n$ que cumple que $r^n = 0$. Entonces $rr^{n-1} = 0$ y como $R$ no posee divisores de cero, $r^{n-1} = 0$, esto es $rr^{n-2} = 0$ y de nuevo concluimos que $r^{n-2} = 0$. Continuando iterativamente obtenemos que $r^2 = 0$, una contradicción.*

Las siguientes proposiciones nos permiten distinguir a los anillos fuertemente unitarios a partir de las propiedades de sus elementos. Primero probaremos un lema que será necesario para demostrar dichas afirmaciones.

**Lema 2.1.6.** *Sea $R$ un anillo y $\alpha \in R$. Si $\alpha^2 = 0$ implica que $\alpha = 0$, entonces $R$ es reducido.*

*Demostración.* Sea $R$ un anillo, $\alpha \in R$ y $n \in \mathbb{Z}^+$, queremos ver que si $\alpha^n = 0$ entonces $\alpha = 0$. Como para cualquier entero $n \in \mathbb{Z}^+$ existe un entero $m$ tal que $n + m = 2^t$ para algún $t \in \mathbb{N}$, basta probar que esta el lema se cumple para las potencias positivas de $2$. Suponga que $\alpha^{2^t} = 0$ para algún $t \in \mathbb{N}$, entonces $(\alpha^{2^{t-1}})^2 = 0$ y por hipótesis $\alpha^{2^{t-1}} = 0$; de la misma manera $(\alpha^{2^{t-2}})^2 = 0$ y por el mismo argumento se tiene que $\alpha^{2^{t-2}} = 0$. Realizando el mismo procedimiento una cantidad finita de veces se obtiene que $\alpha^2 = 0$, luego $\alpha = 0$ y $R$ es reducido. □

**Proposición 2.1.7.** *Todo anillo fuertemente unitario es reducido.*

*Demostración.* Sea $R$ un anillo fuertemente unitario y $\alpha \in R$. Suponga que $\alpha^2 = 0$, entonces el conjunto $S := \{n\alpha : n \in \mathbb{Z}\}$ es un subanillo de $R$ con multiplicación trivial. Como $R$ es fuertemente unitario $S$ tiene identidad multiplicativa $1_S$, pero $1_S = 1_S^2 = 0$ y por lo tanto $S = \{0\}$ y $\alpha = 0$. De esta manera $R$ es un anillo reducido por el Lema 2.1.6. □

**Ejemplo 2.1.8.** *El anillo $M_2(\mathbb{Z})$ de las matrices de dimensión $2 \times 2$ y entradas los números enteros no es reducido ya que la matriz $A = \left(\begin{smallmatrix} 4 & 2 \\ -8 & -4 \end{smallmatrix}\right)$ es nilpotente pues $A^2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. De acuerdo a la proposición anterior $M_2(\mathbb{Z})$ no es fuertemente unitario. Para un ejemplo concreto note que el conjunto $M_2(2\mathbb{Z})$ de las matrices de dimensión $2 \times 2$ y entradas los números pares es un subanillo propio de $M_2(\mathbb{Z})$ que no tiene uno.*

Para la demostración de la siguiente proposición será necesario echar mano del teorema chino del residuo para anillos conmutativos que se presenta a continuación.

**Teorema 2.1.9.** ***(Teorema chino del residuo para anillos conmutativos)*** *Sea $R$ un anillo conmutativo. Si $I_1, \cdots, I_n$ son ideales coprimos de $R$, es decir $I_i \oplus I_j = R$ para $i \neq j$, entonces $R/(I_1 \times \cdots \times I_n) \cong R/I_1 \times \cdots \times R/I_n$.*

*Demostración.* Haremos la prueba para el caso en que $R = I_1 \oplus I_2$. El resultado se puede extender para una cantidad finita $n$ de ideales por medio de inducción matemática.
Consideremos el homomorfismo de anillos $\pi : R \to R/I_1 \times R/I_2$ con $\pi(r) = (r + I_1, r + I_2)$ donde cada elemento $r \in R$ es enviado al par ordenado conformado por sus proyecciones a cada uno de los cocientes. Como $R = I_1 \times I_2$ entonces todo elemento $r$ en $R$ es de la

forma $i+j$ con $i \in I_1$ y $j \in I_2$. Los elementos de $R/I_1$ son de la forma $r+I_1 = (i+j)+I_1 = j+I_1 = \bar{j}$, de la misma manera los elementos de $R/I_2$ son de la forma $\bar{i}$ con $i \in I_1$. Por lo tanto, dada una pareja $(\bar{j}, \bar{i}) \in R/I_1 \times R/I_2$ se tiene que $r = i+j$ cumple que $\pi(r) = (\bar{j}, \bar{i})$ luego $Im(\pi) = R/I_1 \times R/I_2$.Veamos que $Ker(\pi) = I_1 \times I_2$. Sea $r = i+j \in Ker\pi$, entonces $\pi(r) = (0,0)$ pero como $\pi(i+j) = (\bar{j}, \bar{i})$ entonces $j \in I_1$ y $i \in I_2$ y de esta manera $r \in I_1 \cap I_2$. También tenemos que $1 = x+y$ con $x \in I_1$ y $y \in I_2$ y así $r = rx + ry \in I_1 \times I_2$. Por otro lado si $r = i+j \in I_1 \times I_2$, entonces $r = \sum_{k=1}^{n} i_k j_k \in I_1 \times I_2$ y como $I_i$ $(i = 1, 2)$ son ideales, $r \in I_1 \cap I_2$. De esta manera $\pi(r) = (r+I_1, r+I_2) = (0,0)$ y entonces $r \in Ker(\pi)$.
Concluimos por el primer teorema de isomorfismos de anillos que $R/(I_1 \times I_2) \cong R/I_1 \times R/I_2$. □

**Proposición 2.1.10.** *Sea $R$ un anillo conmutativo, reducido y finito, entonces $R \cong F_1 \times ... \times F_n$ para alguna cantidad finita $n$ de cuerpos finitos $F_1, ..., F_n$.*

*Demostración.* Sea $R$ un anillo con las condiciones mencionadas. Como $R$ es finito, existe una cantidad finita $P_1, ..., P_n$ de ideales primos minimales de $R$ y como $R$ es reducido tenemos que $P_1 \times \cdots \times P_n = \{0\}$ y que $P_i \oplus P_j = R$ para $1 \leq i, j \leq n$. De esta manera $R \cong R/\{0\} = R/(P_1 \times \cdots \times P_n)$. Por otro lado, el Teorema 2.1.9 garantiza que $R/(P_1 \times \cdots \times P_n) = R/P_1 \times \cdots \times R/P_n$. Como $P_i$ es primo, tenemos que $R/P_i \cong F_i$ con $F_i$ un cuerpo finito. Concluimos que $R \cong R/P_1 \times \cdots \times R/P_n \cong F_1 \times ... \times F_n$ donde cada $F_i$ es un cuerpo finito. □

La demostración del siguiente teorema, aunque sencilla, requiere el uso del Teorema de Wederburn y varios resultados relacionados con cuerpos finitos. La prueba se puede revisar en [5], p. 367.

**Teorema 2.1.11.** ***(Jacobson)*** *Sea $R$ un anillo con división tal que para todo $r \in R$ existe un entero positivo $n(r) > 1$, que depende de $r$, tal que $r^n = r$, entonces $R$ es un cuerpo conmutativo.*

### 2.2. Caracterización de Anillos Fuertemente Unitarios

En esta sección nos proponemos relacionar los anillos fuertemente unitarios con los cuerpos absolutamente algebraicos de característica prima. Para iniciar recordemos que un número entero $n$ es llamado libre de cuadrados si al expresarlo como producto de números primos, todos ellos tienen exponente igual a $1$.

---

[5] I.N. HERSTEIN. *Topics in Algebra*. Blaisdell Publishing Co., 1964.

**Definición 2.2.1.** *Sea $R$ un anillo con unidad. El subanillo $P(R) := \{n \cdot 1_R : n \in \mathbb{Z}\}$ de $R$ es llamado el* ***subanillo primo*** *de $R$.*

Note que el homomorfismo $\phi : \mathbb{Z} \to P(R)$ dado por $\phi(n) = n \cdot 1_R$ garantiza, por el primer teorema de isomorfismos de anillos, que $\mathbb{Z}/Ker\phi \cong P(R)$. Puesto que los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ para algún entero $m$ concluimos que $P(R) \cong \mathbb{Z}$ ó $P(R) \cong \mathbb{Z}_m$ para algún entero positivo $m$. Suponga además que $b \in R$ , si $n \cdot 1_R \in P(R)$ entonces $(n \cdot 1_R)b = b(n \cdot 1_R)$, esto quiere decir que $P(R) \subseteq Z(R)$ el centro de $R$.

**Lema 2.2.2.** *Sea $R$ un anillo fuertemente unitario. Entonces $P(R) \cong \mathbb{Z}_n$ para algún entero $n > 1$ libre de cuadrados.*

*Demostración.* Sea $R$ un anillo fuertemente unitario. Como $\mathbb{Z}$ no es un anillo fuertemente unitario, descartamos que $P(R) \cong \mathbb{Z}$ y entonces $P(R) \cong \mathbb{Z}_n$ para algún $n \geq 1$. Además como $R$ es diferente de cero, tenemos que $n > 1$. Por otra parte, por la Proposición 2.1.7, $P(R)$ es reducido. Sea $f$ el isomorfismo que existe entre $P(R)$ y $\mathbb{Z}_n$, procedemos por contradicción. Suponga que $n$ no es libre de cuadrados, entonces $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ donde $e_i > 1$ para algún $1 \leq i \leq k$. Sin pérdida de generalidad suponga que $\{e_1, \cdots, e_j\}$ $(j \leq k)$ es el conjunto de todos los exponentes mayores que $1$ y sea $e = max\{e_1, \cdots, e_j\}$, entonces $n$ divide a $(p_1p_2\cdots p_k)^e$ y por lo tanto $f(p_1p_2\cdots p_k)^e = 0$, pero esto contradice el hecho de que $P(R)$ es reducido. Concluimos que $n$ es libre de cuadrados. □

**Lema 2.2.3.** *Sea $\mathbb{F}$ un cuerpo finito y sea $f(x) \in \mathbb{F}[x]$ un polinomio distinto de cero. Entonces $\mathbb{F}[x]/\langle f(x)\rangle$ es finito.*

*Demostración.* Suponga $\mathbb{F}$ un cuerpo finito y $f(x) \in \mathbb{F}[x]$ un polinomio no nulo con grado $n \geq 0$. Como $\mathbb{F}$ es cuerpo, la función $N : \mathbb{F}[x] \to \mathbb{Z}$ dada por $N(0) = 0$ y $N(f(x)) = Grado$ de $f = \delta f$ si $f \neq 0$, resulta una norma euclídea luego $\mathbb{F}[x]$ es un dominio euclidiano y por lo tanto un dominio de ideales principales. Tenemos que $\langle f(x)\rangle$ es un ideal principal de $\mathbb{F}[x]$ y por el algoritmo de la división todo elemento del cociente $\mathbb{F}[x]/\langle f(x)\rangle$ se puede expresar de la forma $g(x)f(x)+r(x)$ donde $0 \leq N(r(x)) < n$ y $g(x) \in \mathbb{F}[x]\backslash\{0\}$. Concluimos que $|\mathbb{F}[x]/\langle f(x)\rangle| \leq |\{\alpha_{n-1}x^{n-1} + ... + \alpha_1 x + \alpha_0 : \alpha_i \in \mathbb{F}\}| = |\mathbb{F}^n| = |\mathbb{F}|^n$ y como $\mathbb{F}$ es finito, $\mathbb{F}[x]/\langle f(x)\rangle$ es finito. □

**Lema 2.2.4.** *Sea $R$ un anillo con unidad. El anillo $R[x]$ de polinomios con entradas en $R$ sobre la variable $x$ no es fuertemente unitario.*

*Demostración.* Si $R$ es igual a cero, entonces $R[x]$ es trivial y por lo tanto no es fuertemente unitario, de acuerdo a la definición de anillo fuertemente unitario. Suponga

entonces que $R$ no es trivial; vamos a mostrar que el subanillo $xR[x]$ de los polinomios con término constante cero no es un anillo unitario. Sea $f(x)$ un polinomio arbitrario de $xR[x]$, entonces $1_R x \cdot f(x) \neq 1_R x$. Esto quiere decir que $f(x)$ no puede ser el uno de $xR[x]$, pero como fue tomado arbitrariamente concluimos que $xR[x]$ no tiene uno y por lo tanto $R[x]$ no es fuertemente unitario. □

**Definición 2.2.5.** *Sea $R$ un anillo con unidad y un subanillo $S$ de $R$ contenido en $Z(R)$, el centro de $R$. Para $a \in R$, definimos* $S[a] := \{s_0 + s_1 a + ... + s_n a^n : s_i \in S, n \in \mathbb{N}\} = \{f(a) : f(x) \in S[x]\}$.

Note que $S[a]$ es un subanillo de $R$ que contiene a $S$ pero no necesariamente contiene a $a$. Si $R$ es un anillo con unitario $1_R$ y $1_R \in S$ entonces $a \in S[a]$ y además $S[a]$ es el menor subanillo de $R$ que contiene a $S$ y a $a$.

**Proposición 2.2.6.** *Suponga $R$ un anillo fuertemente unitario. Entonces para todo elemento $\alpha \in R$ existe un entero positivo $n$ (que depende de $\alpha$) tal que $\alpha^n = \alpha$. Además $R$ es conmutativo.*

*Demostración.* Sea $R$ un anillo fuertemente unitario y $\alpha \in R$. Por el Lema 2.2.2, $P(R) \cong \mathbb{Z}_m$ para algún entero positivo $m > 1$ libre de cuadrados, suponga $m = p_1 p_2 ... p_k$.
Por el Teorema chino del residuo tenemos que $\mathbb{Z}_m \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$, luego $P(R) \cong \mathbb{Z}_{p_1} + \cdots + \mathbb{Z}_{p_k}$. Sea $\phi$ el isomorfismo de anillos entre $\mathbb{Z}_{p_1} + \cdots + \mathbb{Z}_{p_k}$ y $P(R)$. Si definimos $S_i = \phi(Z_{p_i})$, obtenemos que $P(R) = \phi(\mathbb{Z}_{p_1} + \cdots + \mathbb{Z}_{p_k}) = \phi(\mathbb{Z}_{p_1}) + \cdots + \phi(\mathbb{Z}_{p_k}) = S_1 + \cdots + S_k$ y como $P(R) \subseteq Z(R)$, entonces cada $S_i \subset Z(R)$.
Fijemos un $i$ tal que $1 \leq i \leq k$. Note que $P(R)[\alpha]$ es fuertemente unitario pues es subanillo de $R$, luego $S_i[\alpha]$ es fuertemente unitario. Como $S_i \cong \mathbb{Z}_{p_i}$ existe una función $f_i : \mathbb{Z}_{p_i}[x] \to S_i[x]$ sobreyectiva y es claro que la función $g_i : S_i[x] \to S_i[\alpha]$ dada por $g_i(f(x)) = f(\alpha)$ es sobreyectiva; por lo tanto $h = g_i \circ f_i$ es sobreyectiva y por el primer teorema de isomorfismos de anillos tenemos que $\mathbb{Z}_{p_i}[x]/Ker(h) \cong S_i[\alpha]$. Si $Ker(h) = \{0\}$ entonces $\mathbb{Z}_{p_i}[x] \cong S_i[\alpha]$ y $\mathbb{Z}_{p_i}[x]$ sería fuertemente unitario pero esto contradice el Lema 2.2.4. Concluimos que $Ker(h)$ no es trivial.
Puesto que el $Ker(h)$ es un ideal de $\mathbb{Z}_{p_i}[x]$ y $\mathbb{Z}_{p_i}[x]$ es un dominio de ideales principales, existe un polinomio $k(x) \in \mathbb{Z}_{p_i}[x]$ tal que $Ker(h) = \langle k(x) \rangle$ y por el Lema 2.2.3, $S_i[\alpha] \cong \mathbb{Z}_{p_i}[x]/\langle k(x) \rangle$ es finito. Como $P(R)[\alpha] = (S_1 + S_2 + \cdots S_k)[\alpha] = S_1[\alpha] + ... + S_k[\alpha]$ y el $1 \leq i \leq k$ fue arbitrario, $P(R)[\alpha]$ es un anillo finito. Además la Proposición 2.1.7 implica que $P(R)[\alpha]$ es reducido. Así que $P(R)[\alpha]$ es un anillo finito, conmutativo y reducido (y como consecuencia de la Proposición 2.1.10), $P(R)[\alpha] \cong F_1 \times ... \times F_j$ para algunos cuerpos

finitos $F_1, ..., F_j$. Llamemos $F$ al isomorfismo entre $F_1 \times ... \times F_j$ y $P(R)$.
Sea $a$ un elemento no nulo en $F_i$ $(1 \leq i \leq j)$, entonces $a^{|F_i|} = a$, es decir $a^{|F_i|-1} = 1$. Esto implica que para todo elemento $\beta \in F_1 \times ... \times F_j$ se cumple que $\beta^{(|F_1|-1)(|F_2|-1)\cdots(|F_j|-1)} = 1$ y multiplicando por $\beta$ a ambos lados de la igualdad obtenemos que $\beta^{(|F_1|-1)(|F_2|-1)\cdots(|F_j|-1)+1} = \beta$. Esto quiere decir que existe un entero $n > 1$ tal que $\beta^n = \beta$ para todo elemento $\beta \in F_1 \times ... \times F_j$. Como $R$ es un anillo unitario, $\alpha \in P(R)[\alpha]$ y entonces existe un elemento $\gamma \in F_1 \times ... \times F_j$ tal que $F(\gamma) = \alpha$. Por lo probado anteriormente tenemos que existe un entero positivo $m$ tal que $\gamma = \gamma^m$, luego $\alpha^m = F(\gamma)^m = F(\gamma^m) = F(\gamma) = \alpha$. Por el Teorema 2.1.11 concluimos que $R$ es conmutativo. □

**Observación 2.2.7.** *El hecho de que $m$ sea un entero libre de cuadrados es necesario para que la prueba anterior funcione. Consideremos por ejemplo que si un número entero $n > 1$ no es libre de cuadrados entonces el conjunto $N(\mathbb{Z}_n) := \{\alpha \in \mathbb{Z}_n : \exists m \in \mathbb{N}, \alpha^m = 0\}$ es un subanillo propio (puesto que $\bar{1} \notin N(\mathbb{Z}_n)$) y no nulo de $\mathbb{Z}_n$(en efecto, de acuerdo con la notación de la demostración del Lema 2.2.2 si $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, $\overline{p_1 \cdots p_k}^e = \overline{(p_1 \cdots p_k)^e} = \bar{0}$ y entonces $N(\mathbb{Z}_n) \neq 0$). De esta manera el anillo $\mathbb{Z}_n[x]/N(\mathbb{Z}_n)[x] \cong (\mathbb{Z}_n/N(\mathbb{Z}_n))[x]$ resultaría ser infinito (pues $N(\mathbb{Z}_n)$) es no nulo y propio). Por otro lado, si $m$ no es libre de cuadrados, aunque $K$ sea un ideal no nulo de $\mathbb{Z}_m[x]$ no siempre $\mathbb{Z}_m[x]/K$ es finito.*

El anillo $\mathbb{Z}_{15}$ es un anillo fuertemente unitario y de acuerdo con la Proposición 2.2.6 para cada elemento $\alpha \in \mathbb{Z}_{15}$ existe un entero $n$ tal que $\alpha^n = \alpha$. En efecto se tiene que $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^5 = \overline{2}$, $\overline{3}^5 = \overline{3}$, $\overline{4}^3 = \overline{4}$, $\overline{5}^3 = \overline{5}$, $\overline{6}^2 = \overline{6}$, $\overline{7}^5 = \overline{7}$, $\overline{8}^5 = \overline{8}$, $\overline{9}^3 = \overline{9}$, $\overline{10}^2 = \overline{10}$, $\overline{11}^3 = \overline{11}$, $\overline{12}^5 = \overline{12}$, $\overline{13}^2 = \overline{13}$ y $\overline{14}^3 = \overline{14}$.

**Definición 2.2.8.** *Sea $R$ un anillo e $I \triangleleft R$. Diremos que I es **indescomponible** si no existen ideales $I_1, I_2$ de $R$ distintos de cero tal que $I = I_1 \oplus I_2$. Un anillo $R$ es **indescomponible** si es indescomponible considerándolo como un ideal de sí mismo. Diremos que un anillo $R$ es **descomponbible** en caso contrario.*

Note que la definición de que un anillo $R$ sea indescomponible implica que si $R = I \oplus J$ entonces $I = R$ (lo que implica que $J = \{0\}$) ó $I = \{0\}$ (y entonces $J = R$).

**Lema 2.2.9.** *Sea $R$ un anillo. Suponga que $R$ no contiene un ideal que sea una suma directa interna infinita de ideales no nulos de $R$, entonces $R = I_1 \oplus I_2 \oplus ... \oplus I_n$ donde cada $I_i$ es un ideal indescomponible de $R$ para $1 \leq i \leq n$.*

*Demostración.* Probaremos la afirmación contrapositiva. Sea $R$ un anillo que no es igual a la suma directa interna finita de ideales indescomponibles, entonces $R$ es descomponible. Luego $R = J_1 \oplus I_1$ para algunos ideales $I_1, J_1$ no nulos de $R$. Como $R$ no es suma directa interna de ideales indescomponibles podemos asegurar, sin pérdida de generalidad, que $I_1$ es descomponible, entonces $I_1 = J_2 \oplus I_2$ para algunos ideales $I_2, J_2$ diferentes de cero. Ahora $R = J_1 \oplus J_2 \oplus I_2$. De nuevo, como $R$ no es suma directa interna de ideales descomponibles se puede concluir, sin pérdida de generalidad, que $I_2$ es descomponible. Entonces $I_2 = J_3 \oplus I_3$ con $J_3, I_3$ ideales no nulos y $R = J_1 \oplus J_2 \oplus J_3 \oplus I_3$. Note que siempre es posible descomponer el ideal $I_n$ en dos ideales no nulos $I_{n+1}$ y $J_{n+1}, (n \in \mathbb{N}^+)$, puesto que por hipótesis $R$ no es igual a la suma directa interna finita de ideales indescomponibles, así que continuando iterativamente concluimos que $I_1$ es un ideal de $R$ que es una suma directa interna infinita de ideales no nulos de $R$. □

**Lema 2.2.10.** *Sea $R$ un anillo. Si $R$ es finito, conmutativo y reducido entonces $R$ tiene uno.*

*Demostración.* Este lema es un caso específico de un resultado más general que afirma que todo anillo artiniano que no tiene ideales nilpotentes diferentes de cero es un anillo unitario semisimple. Es claro que como $R$ es finito, sus ideales también lo son, luego toda cadena estrictamente descendente de ideales de $R$ debe ser finita, luego $R$ es artiniano. Además si $I$ es un ideal nilpotente de $R$, existe un entero positivo $m$ tal que $I^m = 0$ y dado $x \in I$, $x^m \in I^m$, luego $x^m = 0$ y como $R$ es reducido, $x = 0$ y así $I = \{0\}$. De esta manera $R$ no contiene ideales nilpotentes distintos de cero. □

La prueba del anterior lema se puede encontrar en [6], p. 22. Concluimos esta sección enunciado un teorema importante que relaciona los anillos fuertemente unitarios con los cuerpos absolutamente algebraicos presentados en las secciones anteriores. Este resultado permite caracterizar los anillos fuertemente unitarios a partir de cuerpos de característica prima mediante isomorfismos.

**Teorema 2.2.11.** *Sea $R$ un anillo no trivial. Entonces $R$ es fuertemente unitario si y solo si existe un entero positivo $n$ tal que $R \cong F_1 \times \cdots \times F_n$ donde cada uno de los $F_i$ es un cuerpo absolutamente algebraico de característica prima.*

*Demostración.* Sea $R$ un anillo fuertemente unitario. Afirmamos que no existe un ideal de $R$ que sea una suma directa interna infinita de ideales no nulos de $R$. Suponga que

---

[6] P. James JANS. *Rings and Homology*. Holt, Rinehart, y Winston Inc., 1964.

sí existe tal ideal y sea $X$ un conjunto infinito de índices e $\{I_x : x \in X\}$ el conjunto de ideales no nulos de $R$ que generan la suma directa interna. Es claro que $J = \bigoplus_{x\in X} I_x$ es un ideal, y por lo tanto un subanillo, de $R$. Por otro lado, sea $i_{x_1} + i_{x_2} + ... + i_{x_n}$ un elemento arbitrario de $J$ con $x_1, x_2, ..., x_n$ una cantidad finita de elementos de $X$. Como $X$ es infinito existe un elemento $x_{n+1}$ en $X$ diferente a todos los $x_1, x_2, ..., x_n$ tal que $I_{x_{n+1}}$ es un ideal de $R$ que posee algún elemento $a \neq 0$. Puesto que tanto $\sum_{x\in X\setminus\{x_{n+1}\}} I_x$ y $I_{x_{n+1}}$ son ideales de $R$, el producto $(i_{x_1} + i_{x_2} + ... + i_{x_n})a \in \sum_{x\in X\setminus\{x_{n+1}\}} I_x \cap I_{x_{n+1}} = \{0\}$ puesto que $J$ es una suma directa interna. Esto implica que $(i_{x_1} + i_{x_2} + ... + i_{x_n})a = 0 \neq a$, lo cual quiere decir que $i_{x_1} + i_{x_2} + ... + i_{x_n}$ no puede ser el uno de $J$ pues al multiplicarlo por $a$ el resultado es diferente de $a$. Como el elemento $i_{x_1} + i_{x_2} + ... + i_{x_n}$ fue elegido arbitrariamente, entonces ningún elemento de $\bigoplus_{x\in X} I_x$ puede ser el uno de $J$ (ya que siempre encontraremos otro elemento en $J$ distinto de cero que al multiplicarlo por él, el resultado sea igual a cero). Por lo tanto $J$ no posee uno, pero esto contradice que $R$ sea un anillo fuertemente unitario. Concluimos que la afirmación es verdadera y por el Lema 2.2.9 existen $I_1, ..., I_n$ ideales no nulos indescomponibles de $R$ tal que $R = I_1 \oplus ... \oplus I_n$.

Considere la función $f : I_1 \times ... \times I_n \to R$ dada por $f(i_1, ..., i_n) = i_1 + ... + i_n$. Dados $(i_1, ..., i_n), (j_1, ..., j_n) \in I_1 \times ... \times I_n$, es claro que $f(i_1+j_1, ..., i_n+j_n) = f(i_1, ..., i_n)+f(j_1, ..., j_n)$ y como $R$ es suma directa de los ideales $I_1, ..., I_n$ siempre que $p \neq q$ se tiene que $i_p j_q = 0$ y por lo tanto $f(i_1j_1, ..., i_nj_n) = i_1j_1 + ... + i_nj_n = (i_1 + ... + i_n)(j_1 + ... + j_n) = f(i_1, ..., i_n)f(j_1, ..., j_n)$. De esta manera, $f$ es un isomorfismo de anillos y así

$$R \cong I_1 \times ... \times I_n \tag{2.1}$$

Para terminar la primera parte de la prueba solo falta demostrar que cada uno de los ideales $I_i, 1 \leq i \leq n$, es un cuerpo absolutamente algebraico de característica prima. Basta probar esta afirmación para $F := I_1$.

Como $F$ es un subanillo de $R$ y $R$ es fuertemente unitario, existe el elemento uno $1_F$ de $F$. Note que si $e$ es un elemento idempotente de $F$ entonces $e = 0$ o $e = 1_F$, pues si existe un elemento idempotente $e \neq 0, 1$ de $F$ entonces $Fe$ y $F(1_F - e)$ son ideales diferentes de cero de $R$ tales que $F = Fe \oplus F(1_F - e)$, pero esto contradice el hecho de que $F$ sea indescomponible. Veamos ahora que $F$ es un cuerpo. Por la Proposición 2.2.6, $F$ es conmutativo. Sea $r$ un elemento no nulo de $F$, entonces $Fr \subset F$ es un ideal no nulo de $R$ y tiene una identidad multiplicativa $e^*$. Como $e^*$ es idempotente, $e^* = 0$ o

$e^* = 1_F$. Si $e^* = 0$, entonces $Fr = \{0\}$, contradicción, luego $e^* = 1_F$ y $1_F \in Fr$. De esta manera existe un elemento $a \in F$ tal que $1_F = ar$ y entonces $r$ es invertible. Concluimos que $F$ es un cuerpo.

Dado un elemento $\alpha \in F$ existe, por la Proposición 2.2.6 y por el isomorfismo de la ecuación (2.1), un entero $m$ tal que $\alpha^m = \alpha$, entonces $\alpha$ es raíz del polinomio $1_F x^m - 1_F x \in P(F)[x]$ y $F$ es absolutamente algebraico. Por otro lado, si la característica de $F$ es cero entonces $P(F)$ es isomorfo a $\mathbb{Q}$, pero existen elementos $a \in \mathbb{Q}$ tal que $a^n \neq a \quad \forall n \in \mathbb{Z}$, lo que contradice la Proposición 2.2.6, por lo tanto $F$ tiene característica $p$ con $p$ primo.

Recíprocamente, suponga que $R \cong F_1 \times \cdots \times F_n$ donde cada $F_i$ es un cuerpo absolutamente algebraico de característica prima y sea $S$ un subanillo no trivial de $R$. Queremos ver que $S$ tiene uno. Llamaremos $f$ al isomorfismo entre $R$ y $F_1 \times \cdots \times F_n$.
Para $1 \leq i \leq n$, sea $\pi_i : R \to F_i$ la proyección de $f$ en la $i$-ésima coordenada y $\pi(S) = \{1 \leq i \leq n : \pi_i(S) \neq 0\}$. Sin pérdida de generalidad, podemos suponer que $\pi(S) = \{1, 2, ..., r\}$ para algún $r$ tal que $1 \leq r \leq n$. Para cada $1 \leq i \leq r$, sea $x_i$ un elemento de $S$ tal que $\pi_i(x_i) \neq 0$ y considere el subanillo $S'$ de $S$ generado por $x_1, ..., x_n$. Si llamamos $K_i$ al subcuerpo primo de cada cuerpo $F_i$, tenemos por el isomorfismo $f$ que

$$f(S') \leq K_1(\pi_1(x_1), \pi_1(x_2), ..., \pi_1(x_r)) \times \cdots \times K_n(\pi_n(x_1), \pi_n(x_2), ..., \pi_n(x_r)).$$

Como todos los $F_i$ poseen característica prima, cada $K_i$ (que es el subcuerpo generado por $1_{F_i}$) es finito y además, como también todos los $F_i$ son absolutamente algebraicos, cada elemento $\pi_i(x_j)$ es algebraico sobre $K_i$. Por lo tanto cada extensión $K_i(\pi_i(x_1), \pi_i(x_2), ..., \pi_i(x_r))$ es un cuerpo finito lo que implica que $f(S')$ es finito. Esto implica que $S'$ es finito. Note que como todo cuerpo es conmutativo y reducido tenemos por el isomorfismo que $R$ es conmutativo y reducido. De esta manera $S'$ es finito, conmutativo y reducido y por el Lema 2.2.10, $S'$ tiene identidad multiplicativa $1_{S'}$. Suponga $f(1_{S'}) = (e_1, e_2, ..., e_r, 0, ..., 0)$. Note que $x_i \in S'$, entonces $1_{S'} x_i = x_i$ y, como $\pi_i(x_i) \neq 0$, se cumple que $\pi_i(1_{S'})\pi_i(x_i) = \pi_i(x_i)$ y $e_i = \pi_i(1_{S'}) = 1_{F_i}$ para cada cuerpo $F_i$. De esta manera $f(1_{S'}) = (1_{F_1}, 1_{F_2}, ..., 1_{F_r}, 0, ..., 0)$ y por lo tanto $1_{S'}$ es también el uno de $S$. Concluimos que todo subanillo $S$ de $R$ es unitario y queda completada la prueba. □

## 3. Anillos casi fuertemente unitarios

En este capítulo estamos interesados en estudiar los anillos que no poseen uno pero sin embargo sus subanillos propios sí tienen unidad, estos anillos son llamados **casi fuertemente unitarios**, a continuación presentamos algunos resultados relacionados con los anillos fuertemente unitarios del capítulo anterior.

**Proposición 3.0.1.** *Si $R$ es un anillo tal que todo subanillo propio de $R$ es unitario entonces $R$ es conmutativo.*

*Demostración.* Sea $R$ un anillo tal que todo subanillo propio tiene uno. Consideramos dos casos:

**Caso 1:** Existe un elemento $r \in R$ tal que $R$ es generado (como anillo) por $r$, esto es $R = \{a_1 r + a_2 r^2 + ... + a_n r^n : a_i \in \mathbb{Z}, n \in \mathbb{Z}^+\}$. Claramente $R$ es conmutativo.

**Caso 2:** $R$ no es generado por ningún elemento de $R$. Sea $\alpha$ un elemento no nulo de $R$, vamos a mostrar que existe un entero $r$ tal que $\alpha^{r+1} = \alpha$. Considere el conjunto $S := \{a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n : a_i \in \mathbb{Z}, n \in \mathbb{Z}^+\}$. Es claro que $S$ es un subanillo propio no trivial de $R$ y por lo tanto es unitario. Además todo subanillo de $S$ es un subanillo propio de $R$ así que tiene uno, luego $S$ es fuertemente unitario y por el Teorema 2.2.11, existe $n \in N$ tal que $S \cong F_1 \times \cdots \times F_n$ donde cada $F_i$ es un cuerpo absolutamente algebraico de característica prima. Por lo tanto, como $\alpha \in S$, podemos suponer que $\alpha = (a_1, a_2, ..., a_n)$ con $a_i \in F_i$, $1 \leq i \leq n$. Para cada $i$ denotamos por $K_i$ el subcuerpo primo de $F_i$, entonces cada extensión $K_i(a_i)$ es un cuerpo finito, puesto que es una extensión algebraica simple de un cuerpo finito. Suponga $|K_i| = m_i$ y $a_i \neq 0$, entonces ${a_i}^{m_i - 1} = 1$ por el Teorema de Lagrange. Sea $r = (m_1 - 1)(m_2 - 1) \cdots (m_n - 1)$ entonces $\alpha^r = (a_1^r, ..., a_n^r) = (1, ..., 1)$, esto significa que $\alpha^{r+1} = \alpha$ y por el Teorema 2.1.11, tenemos que $R$ es conmutativo. □

**Ejemplo 3.0.2.** *El anillo $M_2(2\mathbb{Z})$ no posee unidad luego no es fuertemente unitario. De la misma manera, como no es conmutativo, tampoco es casi fuertemente unitario.*

**Proposición 3.0.3.** *Todo grupo abeliano, finito y simple es isomorfo a $\mathbb{Z}_p$ con $p$ un número primo.*

*Demostración.* Sea $G$ un grupo abeliano, simple y con $p$ elementos, entonces $G \cong \mathbb{Z}_p$. Veamos que $p$ es primo. Sea $a$ un entero divisor de $p$. Como $G$ es abeliano, por la afirmación recíproca del teorema de Lagrange existe un subgrupo $H$ de $G$ tal que

$|H| = a$. Note que si $G$ es un grupo abeliano entonces todos sus subgrupos son normales, entonces $H$ es normal y como $G$ es simple, $H = \{0\}$ y $a = 1$ ó $H = G$ y $a = p$. Concluimos que $p$ es primo. □

Un hecho que debe ser tomado en cuenta es que si $G$ es un grupo con $p$ elementos existe un isomorfismo de grupos $\phi : (G, +) \to (\mathbb{Z}_p, +)$. Esta misma función $\phi$ es un isomorfismo entre los anillos $(G, +, \cdot)$ y $(\mathbb{Z}_p, +, \cdot)$ con la suma usual y el producto nulo. Este resultado implica que cualesquiera dos anillos $R_1$ y $R_2$ que posean la misma cantidad prima $p$ de elementos y tengan multiplicación trivial son isomorfos entre sí, este hecho será usado de manera frecuente a continuación.

**Lema 3.0.4.** *Sea $R$ un anillo no trivial tal que no contiene ideales propios a la izquierda, entonces $R$ es un anillo con división ó $R \cong x\mathbb{F}_p[x]/\langle x^2 \rangle$ para algún número primo $p$.*

*Demostración.* Sea $R$ un anillo no nulo tal que sus únicos ideales a izquierda son $\{0\}$ y $R$. Consideramos dos casos:

**Caso 1:** Existe un elemento no nulo $r \in R$ que es divisor de cero, es decir $xr = 0$ para algún elemento $x \neq 0 \in R$. Entonces $x, 0 \in Ann_R(r) = \{a \in R : ar = 0\}$ (el ideal anulador de $r$), y por hipótesis, $Ann_R(r) = R$.
Consideremos el grupo abeliano $\mathbb{Z}r = \{mr : m \in \mathbb{Z}\}$. Como $Ann_R(r) = R$, obtenemos que $\mathbb{Z}r$ es un ideal a izquierda no nulo de $R$ y por lo tanto, $\mathbb{Z}r = R$. Como todos los subgrupos aditivos de $\mathbb{Z}r$ son también ideales de $R$, entonces ellos son triviales o son iguales a $R$, por lo tanto $\mathbb{Z}r$ es un grupo abeliano simple y por la Proposición 3.0.3 posee una cantidad prima $p$ de elementos. Como $R = \mathbb{Z}r = Ann_R(r)$, el producto de dos elementos arbitrarios de $R$ es siempre igual a cero.
Entonces $R$ es un anillo con multiplicación trivial que posee $p$ elementos al igual que el anillo $x\mathbb{F}_p[x]/\langle x^2 \rangle$ (Ejemplo 1.2.9), concluimos que $R \cong x\mathbb{F}_p[x]/\langle x^2 \rangle$.

**Caso 2:** $R$ no tiene divisores (no nulos) de cero. Sea $r \neq 0 \in R$, entonces $Rr$ es un ideal no nulo a la izquierda de $R$ y por lo tanto $Rr = R$ y existe un elemento $a \in R$ tal que $r = ar$, esto es $ar = a^2r$ y $(a - a^2)r = 0$. Como $r$ no es divisor de cero, $a = a^2$. Por otro lado como $r = ar$ y $r \neq 0$, $a \neq 0$ y, por hipótesis, $a$ no es un divisor de cero. Sea $x \in R$ un elemento arbitrario, entonces $xa = xa^2$, esto es $a(x - xa) = 0$ y como $a$ no es divisor de cero, $x = xa$. De manera similar se ve que $ax = x$, de donde se concluye que $a = 1_R$. Veamos ahora que $R$ es un anillo con división. Sea $x \in R \setminus \{0\}$, entonces $Rx = R$ y $1_R = yx$ para algún elemento no nulo $y \in R$, esto prueba que todo elemento diferente de cero de $R$ tiene inverso multiplicativo a izquierda. Por otro lado, como $1_R = yx$, $y = yxy$ y

multiplicando a la izquierda por el inverso multiplicativo a izquierda de $y$, obtenemos que $1 = xy$ y $R$ es un anillo con división. □

Antes de proporcionar la caracterización de los anillos casi fuertemente unitarios necesitaremos probar los siguientes dos lemas que permiten conocer mejor la naturaleza de los anillos artinianos y la relación de esta característica de un anillo con el hecho de que posea o no identidad multiplicativa.

**Lema 3.0.5.** *Un anillo $R$ artiniano, conmutativo y reducido es un anillo con uno.*

*Demostración.* Sea $R$ un anillo artiniano conmutativo y reducido. Sin pérdida de generalidad suponga que $R$ no es trivial. Para empezar mostraremos que existen ideales maximales en $R$. Para ello primero mostraremos que dado un elemento no nulo $r$ de $R$ existe un ideal primo $P$ de $R$ tal que $r \notin P$. Considere el conjunto $S := \{r^n : n \in \mathbb{Z}^+\}$. Denotaremos por $\Gamma$ la colección de todos los ideales de $R$ que son disjuntos con $S$. Como $R$ es reducido, $r$ no es nilpotente y entonces $\{0\} \in \Gamma$, luego $\Gamma \neq \emptyset$. Ordenando $\Gamma$ con la relación de inclusión obtenemos, por el Lema de Zorn, que existe un ideal $I$ maximal de $\Gamma$. $I$ es un ideal propio de $R$ pues $r \notin I$. Solo falta ver que $I$ es primo. Procedemos por contradicción: suponga que existen elementos $x, y \in R$ tal que $xy \in I$ pero $x \notin I$ y $y \notin I$. Como $I \subset \langle I, x\rangle$ e $I$ es ideal maximal de $\Gamma$ entonces $\langle I, x\rangle \cap S \neq \emptyset$. Por el mismo argumento $\langle I, y\rangle \cap S \neq \emptyset$. Por lo tanto existen $a, b \in \mathbb{Z}^+$ tal que $i_1 + sx + mx = r^a$ y $i_2 + ty + ny = r^b$ para algunos $i_1, i_2 \in I, s, t \in R$ y $n, m \in \mathbb{N}$. De esta manera $r^a r^b = (i_1+sx+mx)(i_2+ty+ny) = i_1 i_2 + i_1(ty+ny) + i_2(sx+mx) + (st+sn+mt+mn)xy \in I$ (puesto que $xy \in I$) pero esto implica que $r^{a+b} \in I$ lo cual es una contradicción pues $I \cap S = \emptyset$. Concluimos entonces que $I$ es un ideal primo.
Ahora queremos ver que si $R$ es un dominio entero entonces es un cuerpo. Suponga que $R$ es un dominio entero y sea $r$ un elemento no nulo de $R$. Note que $\cdots \subseteq Rr^n \subseteq Rr^{n-1} \subseteq \cdots \subseteq Rr^2 \subseteq Rr$ es una cadena descendiente de ideales no nulos de $R$, entonces, como $R$ es artiniano, existe un natural $n$ tal que $Rr^{n+1} = Rr^n$. Como $r^{n+1} \in Rr^n$ y $Rr^n = Rr^{n+1}$, existe un elemento $e \in R$ tal que $r^{n+1} = er^{n+1}$. Luego $r^n(r - er) = 0$ y como $R$ no posee divisores de cero y $r \neq 0$ entonces $r = er$, esto es $er = e^2 r$. Por el mismo argumento obtenemos que $e = e^2$ y como $R$ es reducido $e \neq 0$, procediendo de la misma manera que en el caso 2 de la prueba del Lema 3.0.4 concluimos que $e := 1_R$ es el uno de $R$. Veamos ahora que todo elemento no nulo $r$ de $R$ es invertible. Como $Rr^n = Rr^{n+1}$ y $R$ tiene uno entonces existe $a \in R$ tal que $r^n = ar^{n+1}$, esto es $r^n(1_R - ar) = 0$ y como $R$ es dominio entero entonces $1_R = ar$, luego $r$ es invertible. De esta manera concluimos que si $R$ es

un dominio entero entonces es un cuerpo.
Lo anterior mostrado es suficiente para demostrar que todo ideal primo de $R$ es maximal. En efecto, sea $I$ un ideal primo de $R$, entonces $R/I$ es dominio entero y artiniano. Por lo mostrado anteriormente, $R/I$ es cuerpo. Como $R/I$ es cuerpo, $I$ es un ideal maximal de $R$.
Ahora probaremos la siguiente afirmación: $R$ solo tiene una cantidad finita de ideales primos. Para empezar sea $B$ la colección de todas las intersecciones finitas de ideales primos de $R$. Como mostramos anteriormente que si $r$ es un elemento no nulo de $R$ existe un ideal primo $P$ de $R$ tal que $r \notin P$, sabemos que $B \neq \emptyset$. Como $R$ es artiniano no existen cadenas estrictamente descendentes infinitas de elementos de $B$ (que resultan ser también ideales de $R$) en $R$, por lo tanto existe un elemento minimal en $B$. Sea $P_1 \cap \cdots \cap P_n$ aquel elemento minimal de $B$ para algún $n \in \mathbb{N}$. Queremos probar que $P_1, \cdots, P_n$ son exactamente todos los ideales primos de $R$. Suponga que existe otro ideal primo $P_{n+1}$ de $R$, entonces $P_1 \cap \cdots \cap P_n \cap P_{n+1} \subseteq P_1 \cap \cdots \cap P_n$, pero por minimalidad tenemos que $P_1 \cap \cdots \cap P_n \cap P_{n+1} = P_1 \cap \cdots \cap P_n$, entonces $P_1 \cap \cdots \cap P_n \subseteq P_{n+1}$. Note que no puede suceder que $P_{n+1} \subseteq P_i$ para todo $i$, $1 \leq i \leq n$, pues en ese caso $P_{n+1}$ sería primo pero no maximal, lo que contradice lo mostrado arriba luego $P_i \subsetneq P_{n+1}$ para algún $i$ $(1 \leq i \leq n)$. Pero de nuevo esto no puede suceder pues contradice lo mostrado anteriormente: cada primo $P_i$ es maximal. Concluimos que $R$ contiene una cantidad finita de ideales primos.
Sean $P_1, \cdots, P_n$ todos los ideales primos de $R$. Sabemos que $R/P_i$ es un dominio entero para $i$ $(1 \leq i \leq n)$ y como sabemos que con las hipótesis planteadas si $R/P_i$ es dominio entero entonces es cuerpo, solo basta probar que $R \cong R/P_1 \times \cdots \times R/P_n$, pues de esta manera $R$ sería isomorfo al producto finito de anillos que tienen uno. Para ello definimos la función $\phi : R \to R/P_1 \times \cdots \times R/P_n$ dada por $\phi(r) = (\bar{r}, \ldots, \bar{r})$ donde en cada casilla $i$-ésima la clase $\bar{r}$ denota el cociente $P_i + r$. Es claro que $\phi$ es un homomorfismo. Además un elemento $a \in R$ pertenece a $P_1 \cap \cdots \cap P_n$ si y solo si $\phi(a) = 0$, luego $P_1 \cap \cdots \cap P_n = Ker(\phi)$. Como $R$ es reducido, ya mostramos anteriormente que dado un $r$ en $R \backslash \{0\}$ existe un ideal primo $P_i$ de $R$ al cual $r$ no pertenece, por lo tanto $r \notin Ker(\phi)$ y entonces $Ker(\phi) = \{0\}$ esto implica que $\phi$ es inyectiva. Veamos ahora que $\phi$ es sobreyectiva. Como $\phi(R)$ es clausurativo bajo la adición basta probar que $(\bar{0}, \ldots, \bar{x}, \ldots, \bar{0})$ posee una preimagen bajo $\phi$ para cualquier elemento $x \in R$, y cualquier casilla $i$-ésima (suponga sin perdida de generalidad $i = 1$), esto es: queremos encontrar un elemento $r \in R$ tal que $r - x \in P_1$ y $r \in P_2 \cap \cdots \cap P_n$ (considerando claramente que $n > 1$). Si $P_2 \cap \cdots \cap P_n \subseteq P_1$, entonces existe algún $j$ $(2 \leq j \leq n)$ tal que $P_j \subsetneq P_1$, puesto que $P_1$ es primo. Pero esto es una

contradicción pues $P_j$ es maximal. Luego, como $P_1$ es maximal, $P_1 \subseteq P_1 + (P_2 \cap \cdots \cap P_n)$ y $(P_2 \cap \cdots \cap P_n) \not\subset P_1$, se cumple que $P_1 + (P_2 \cap \cdots \cap P_n) = R$ . De esta manera existen $s \in P_1$ y $r \in P_2 \cap \cdots \cap P_n$ tal que $s + r = x$, esto es $r - x = -s \in P_1$. Por lo tanto, $\phi$ es sobreyectiva. Concluimos que $\phi$ es un isomorfismo y de esta manera, $R$ es isomorfo al producto finito de anillos unitarios, es decir que $R$ posee uno. □

**Lema 3.0.6.** *Sea $R$ un anillo conmutativo tal que todos sus subanillos propios son artinianos. Además $R$ posee un subanillo propio $S$ con un elemento idempotente $e \neq 0$, entonces $R$ es artiniano.*

*Demostración.* Sean $e$, $S$ y $R$ como se mencionaron en la hipótesis. Procederemos por contradicción. Suponga que $R$ no es artiniano, entonces existe una cadena infinita estrictamente decreciente $\cdots \subsetneq I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1$ de ideales no nulos de $R$. Como $e$ es un elemento idempotente, el conjunto $J := \{me : m \in \mathbb{Z}\}$ es un subanillo de $S$ y como $S$ es un subanillo propio de $R$, $J$ también resulta ser un subanillo propio de $R$. Podemos construir un epimorfismo de anillos $\phi : \mathbb{Z} \to J$ dado por $\phi(m) = me$ y entonces, por el primer teorema de isomorfismo de anillos, $J \cong \mathbb{Z}/Ker(\phi) \cong \mathbb{Z}/n\mathbb{Z}$ para algún entero $n \geq 0$. Si $n = 0$, $J \cong \mathbb{Z}$ y $J$ no sería artiniano, pero esto contradice el hecho de que todo subanillo propio de $R$ es artiniano; por lo tanto $J$ es un anillo finito. Suponga que la cardinalidad de $J$ es igual a $n$.
Para todo número entero positivo $k$ tenemos que $J_k := J + I_k$ es un subanillo de $R$. Además, para cada $k \in \mathbb{Z}^+$, $I_k$ es un ideal de $J_k$, luego $\cdots \subsetneq I_{k+2} \subsetneq I_{k+1} \subsetneq I_k$ es una cadena infinita estrictamente decreciente de ideales de $J_k$. Como cada subanillo propio de $R$ es artiniano, concluimos que $J_k = R$ para todo entero positivo $k$.
Para $k \in \mathbb{Z}^+$, definimos la función $f : R/I_{k+1} \to R/I_k$ dada por $f(r + I_{k+1}) = r + I_k$. Es claro que $f$ está bien definida pues $I_{k+1} \subsetneq I_k$ para todo $k > 0$. Como para todo $r, s \in R$, $f((r + s) + I_{k+1}) = (r + I_k) + (s + I_k) = f(r + I_{k+1}) + f(s + I_{k+1})$ y $f(rs + I_{k+1}) = rs + I_k = (r + I_k)(s + I_k) = f(r + I_{k+1})f(s + I_{k+1})$, se tiene que $f$ es un homomorfismo de anillos, claramente sobreyectivo. Además si $r \in I_k \setminus I_{k+1}$, se tiene que $r + I_{k+1}$ no pertenece a la clase del cero en $R/I_{k+1}$ pero $f(r + I_{k+1}) = r + I_k = 0$ en $R/I_k$, concluimos entonces que para todo $k \in \mathbb{Z}^+$ existe un homomorfismo de anillos $f : R/I_{k+1} \to R/I_k$ sobreyectivo y no inyectivo; luego dado un $m \in \mathbb{N}$ existe un ideal $I_k$ de $J$, tal que $m < |I_k|$ siempre que $k \in \mathbb{Z}^+$; es decir, si $k \in \mathbb{Z}^+$, no existe una cota superior finita para las cardinalidades de los $R/I_k$.
Para finalizar sea $k \in \mathbb{Z}^+$. Como $|J| = n$, vale que $|J/I_k| = |\{j + I_k : j \in J\}| \leq n$ y como $J_k = R$ entonces $R/I_k = J_k/I_k = (J + I_k)/I_k = J/I_k$, lo que implica que

$|R/I_k| = |J/I_k| \leq n$, pero esto contradice el hecho de que los cardinales de los $R/I_k$ no tengan una cota superior. Concluimos entonces que $R$ debe ser artiniano. □

Note que de acuerdo con la prueba anterior es posible simplificar un poco el Lema 3.0.6, aplicándolo a los anillos que estamos estudiando, de la siguiente manera: Suponga que $R$ es un anillo con uno, con un subanillo propio unitario y que cada subanillo propio de $R$ tiene uno, entonces el subanillo primo $P(R)$ de $R$ es artiniano y no puede ser igual a $R$. Como $P(R) \ncong \mathbb{Z}$, $P(R) \cong \mathbb{Z}_n$ para algún entero $n > 1$. Entonces $1$ es un elemento idempotente diferente de cero de $J := P(R)$ y de acuerdo a la demostración, $R$ es artiniano.

**Teorema 3.0.7.** *Sea $R$ un anillo diferente de cero, entonces todo subanillo propio de $R$ tiene unidad si y solo si se cumple alguna de las siguientes afirmaciones:*

I) *Existe un entero positivo $n$ tal que $R \cong F_1 \times \cdots \times F_n$ donde cada uno de los $F_i$ es un cuerpo absolutamente algebraico de característica prima, ó*

II) *$R \cong x\mathbb{F}_p[x]/\langle x^2 \rangle$ para algún número primo $p$.*

*Demostración.* Sea $R$ un anillo diferente de cero. Suponga que todo subanillo propio de $R$ tiene identidad multiplicativa. Si $R$ tiene uno, por el Teorema 2.2.11 tenemos que $R$ es el producto directo finito de cuerpos absolutamente algebraicos de característica prima.
Suponga entonces que $R$ no tiene uno. Por la Proposición 3.0.1 tenemos que $R$ es conmutativo. Queremos ver que $R$ tiene exactamente $p$ elementos con $p$ primo y que su multiplicación es nula. Para eso mostraremos primero que $R$ posee un elemento nilpotente diferente de cero. Procederemos por contradicción. Suponga que $R$ es reducido. Consideraremos dos casos:

**Caso 1:** $R$ no tiene un subanillo propio, entonces los únicos ideales de $R$ pueden ser $\{0\}$ y $R$. Como $R$ es reducido, $R \ncong x\mathbb{F}_p[x]/\langle x^2 \rangle$ y el Lema 3.0.4 implica que $R$ es un cuerpo y por lo tanto tendría identidad multiplicativa $1_R$, lo cual es una contradicción.

**Caso 2:** $R$ tiene algún subanillo propio. Note que si $S$ es un subanillo propio de $R$, $S$ tiene elemento identidad $1_S$ y cada subanillo de $S$ es un subanillo propio de $R$ y por lo tanto tiene uno. De acuerdo con esto, todo subanillo propio $S$ de $R$ es fuertemente unitario. Por el Teorema 2.2.11, como todo subanillo propio $S$ de $R$ es unitario entonces, $S$ es un producto finito de cuerpos y por lo tanto, de acuerdo con la Proposición 1.3.28, $S$ es artiniano. Concluimos entonces que todos los subanillos propios de $R$ son artinianos;

además como $1_S$ es un elemento idempotente de $S$ diferente de cero, por el Lema 3.0.6 se cumple que $R$ es artiniano. Como $R$ es un anillo conmutativo, reducido y artiniano, por el Lema 3.0.5 obtenemos que $R$ es un anillo unitario, una contradicción.

Concluimos entonces que $R$ no es reducido y tiene un elemento $\alpha \neq 0$ tal que $\alpha^n = 0$ para algún entero positivo $n$. Por el Lema 2.1.6 podemos asumir, sin pérdida de generalidad, que $\alpha^2 = 0$ y entonces el subanillo propio $S := \{m\alpha : m \in \mathbb{Z}\}$ de $R$ no es reducido. Como todo subanillo propio de $R$ es un producto finito de cuerpos, tenemos que todo subanillo propio de $R$ es reducido, esto quiere decir que como $S$ es un subanillo no nulo de $R$ que no es reducido, $S = R$. Note que si $G \neq \{0\}$ es un subgrupo aditivo de $R$, se tiene que $G$ es un subanillo de $R$ con multiplicación nula, y además (como es también subanillo de $S$) no es reducido; de donde $G = R$. Por lo tanto $(R, +)$ no posee subgrupos propios normales, es decir, que $(R, +)$ es un grupo abeliano simple y por la Proposición 3.0.3, isomorfo a $\mathbb{Z}_p$ con $p$ primo. De lo anterior $R$ posee $p$ elementos y, como $R = S$, $R$ tiene multiplicación trivial de donde concluimos, siguiendo la prueba del Lema 3.0.4 que $R \cong x\mathbb{F}_p[x]/\langle x^2\rangle$.
Recíprocamente, si $R \cong F_1 \times \cdots \times F_n$ donde cada uno de los $F_i$ es un cuerpo absolutamente algebraico de característica prima, el Teorema 2.2.11 implica que $R$ es fuertemente unitario y entonces es casi fuertemente unitario.
Si $R \cong x\mathbb{F}_p[x]/\langle x^2\rangle$ con $p$ primo, $R$ es un anillo con $p$ elementos y multiplicación trivial, entonces $R$ no tendría uno y el único subanillo de $R$ sería $\{0\}$ que es claramente unitario. □

El siguiente corolario expone de manera más clara la naturaleza de los anillos casi fuertemente unitarios relacionándolos con sus ideales propios y con el anillo cociente de polinomios con coeficientes un cuerpo finito $\mathbb{F}_p$ con $p$ primo.

**Corolario 3.0.8.** *Suponga $R$ un anillo diferente de cero y que no es un anillo con división. Entonces las siguientes afirmaciones son equivalentes:*

I) *Los únicos ideales a la izquierda de $R$ son $\{0\}$ y $R$.*

II) *$R \cong x\mathbb{F}_p[x]/\langle x^2\rangle$ para algún número primo $p$.*

III) *$R$ no es unitario, pero todo subanillo propio de $R$ es unitario.*

*Demostración.* Sea $R$ un anillo no nulo que no es anillo con división. Si los únicos ideales a la izquierda de $R$ son $\{0\}$ y $R$, entonces por el Lema 3.0.5, $R \cong x\mathbb{F}_p[x]/\langle x^2\rangle$ para algún

número primo $p$ y $R$ es casi fuertemente unitario por el Teorema 3.0.7. Sea $I$ un ideal a izquierda de $R$. Como $R$ es casi fuertemente unitario, $I$ es unitario y tiene uno $1_I$. Si $1_I \neq 0$ entonces $I = R$, si $1_I = 0$ entonces $I = \{0\}$. □

## Bibliografía


HERSTEIN, I.N. *Topics in Algebra*. Blaisdell Publishing Co., 1964 (vid. pág. 24).

JANS, P. James. *Rings and Homology*. Holt, Rinehart, y Winston Inc., 1964 (vid. pág. 28).

LEZAMA, José Oswaldo. *Cuadernos de Álgebra*. Universidad Nacional de Colombia, 2020 (vid. pág. 15).

MAYER, Steve. *The Transcendence of* $\pi$. URL: `https://sixthform.info/maths/files/pitrans.pdf` (vid. pág. 13).

OMAN Greig y SENKOFF, Evan. "Almost strongly unital rings". En: *Involve* (2022). URL: `https://www.researchgate.net/publication/362013228_Almost_strongly_unital_rings` (vid. pág. 8).

OMAN Greig y STROUD, John. "Rings whose subrings have an identity". En: *Involve* 13.5 (2020), págs. 823-828 (vid. pág. 8).