UNIVERSIDAD NACIONAL DE PIURA

Facultad de Ciencias

Escuela Profesional de Matemática

PROGRAMA DE ACTUALIZACION Y TITULACION PROFESIONAL (PATPRO)

VERSION XI -2021

TRABAJO DE INVESTIGACION

RESIDUOS EN DOMINIOS EUCLIDIANOS

Presentado por:

Br. Marcos Claudio Flores Vergara

Línea de investigación: Matemática y Estadística

Piura, Perú

2022

UNIVERSIDAD NACIONAL DE PIURA

Facultad de Ciencias

Escuela Profesional de Matemática

PROGRAMA DE ACTUALIZACION Y TITULACION PROFESIONAL (PATPRO)

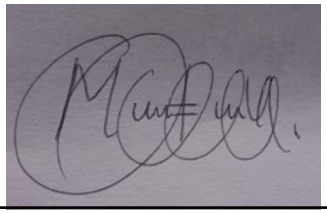
VERSION XI

TRABAJO DE INVESTIGACION

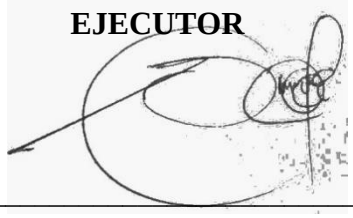
RESIDUOS EN DOMINIOS EUCLIDIANOS

LOS QUE SUSCRIBEN DECLARAN QUE EL PRESENTE TRABAJO DE INVESTIGACIÓN ES ORIGINAL EN SU CONTENIDO Y FORMA

Línea de investigación: Matemática y Estadística



Br. Marcos Claudio Flores Vergara
EJECUTOR



M. Sc. Segundo Basilio Correa Erazo
ASESOR

UNIVERSIDAD NACIONAL DE PIURA

Facultad de Ciencias

Escuela Profesional de Matemática

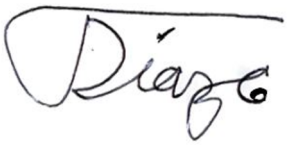
PROGRAMA DE ACTUALIZACION Y TITULACION PROFESIONAL (PATPRO)

VERSION XI

TRABAJO DE INVESTIGACION

RESIDUOS EN DOMINIOS EUCLIDIANOS

APROBADA EN CONTENIDO Y ESTILO POR



Dr. Elmer Porfirio Diaz Contreras

PRESIDENTE

Dr. José Antonio Gómez Navarro

SECRETARIO

Dr. Julio Enrique Lopez Castillo

VOCAL

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMÁTICA

ACTA DE SUSTENTACIÓN N° 04- PATPRO XI 2021- EPM-FC-UNP
Resolución de Consejo Universitario N° 0449-CU-2021

Los miembros del jurado calificador que suscriben, reunidos para evaluar el Trabajo de investigación titulado

RESIDUOS EN DOMINIOS EUCLIDIANOS

presentado por el Bachiller

FLORES VERGARA MARCOS CLAUDIO

oídas las observaciones y dadas respuestas a las preguntas formuladas, el Jurado Calificador declara:

APROBADO (**X**) DESAPROBADO ( )

Con la mención de: SOBRESALIENTE.

(**X**) En consecuencia queda en condición de ser ratificado por el consejo universitario de la Universidad Nacional de Piura y recibir el título profesional de LICENCIADO EN MATEMÁTICA;

Piura, 23 de abril del 2022.

Dr. Elmer Porfirio Díaz Contreras
Presidente

Dr. José Antonio Gómez Navarro
Secretario

Dr. Julio Enrique Lopez Castillo
Vocal

RESUMEN

En este trabajo, se caracteriza a los dominios euclidianos de resto único analizando las unidades para así determinar si es un campo o un anillo de polinomios sobre un campo. Se determinan a los dominios euclidianos con resto doble, mediante algunas estructuras cociente y un argumento de inducción para concluir que son isomorfos a los anillos de los numeros enteros. Presentamos además ejemplos de dominios euclidianos con resto múltiple mayor a dos.

PALABRAS CLAVES: dominios euclidianos, resto único, resto doble.

ABSTRACT

In this work, Euclidean domains of unique remainder are characterized by analyzing the units in order to determine if it is a field or a ring of polynomials over a field. Euclidean domains with double remainder are characterized by some quotient structures and an induction argument to conclude that they are isomorphic to the rings of integers. We also present examples of Euclidean domains with multiple remainder greater than two

KEY WORDS: Euclidean domains, unique remainder, double remainder.

ÍNDICE

INTRODUCCIÓN

En el estudio de estructuras algebraicas, la teoría de anillos tiene como objetivo caracterizar conjuntos que tienen propiedades similares a aquellas operaciones definidas para los enteros. A lo largo de las décadas de estudio de muchas clases especiales de anillos se encontraron propiedades que resultaron interesantes para el avance de la propia teoría y para aplicaciones en otras áreas como espacios métricos, teoría de códigos, etc.

En el álgebra abstracta, nace cierto interés por la teoría de anillos, pues es una estructura más completa, es decir, se piden más propiedades que para grupos e involucra a más de una ley de composición interna y con una inmensidad de ejemplos, que como se menciona antes da una generalización del conjunto de los enteros con sus operaciones de suma y producto. Fijándonos en los enteros tenemos una propiedad interesante y básica para todos; es el algoritmo de la división, a aquellos anillos donde se da esta característica son llamados dominios euclidianos, por ello será nuestro objeto de estudio.

Analizando esa propiedad notamos que, al realizar el algoritmo de la división sobre los enteros, se tiene doble resto, pero al considerarlo sobre los reales se obtiene resto único, debido a esto se creyó conveniente encontrar la característica principal de los dominios euclidianos, que los hace tener resto doble y resto único. En el caso de los dominios euclidianos de resto único se describirán algunos resultados para determinar que tengan esta propiedad resulta que el conjunto es un campo o es homeomorfo a un anillo de polinomios.

El proyecto consta de las siguientes partes: descripción y planteamiento del problema; objetivos, justificación de la investigación, esquema del contenido, aspectos administrativos, y referencias bibliográficas.

I. ASPECTOS DE LA PROBLEMÁTICA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En la teoría de anillos se generaliza la noción de los números enteros, bajo las operaciones usuales; una propiedad interesante y muy conocida es el algoritmo de la división. Aquellos anillos donde se dé esta característica son llamados dominios euclidianos.

Al realizar el algoritmo de la división sobre los enteros se obtiene doble resto, pero al aplicar el algoritmo sobre los reales se obtiene resto único. La propiedad de los restos no es un detalle que se precisa dentro de los cursos convencionales de álgebra. Y dado el caso que un estudio formal matemático requiere cierta generalización, entonces uno puede cuestionarse si siempre un dominio euclidiano con resto único es un campo ya que es la principal diferencia (de los reales con los enteros) y también si siempre un dominio euclidiano con resto doble es equivalente a los enteros. Es así que el trabajo tiene por objetivo principal la caracterización de la propiedad de resto único y doble

Por lo descrito anteriormente ¿Sera posible caracterizar la propiedad de resto único y doble sobre los dominios euclidianos?

En el presente trabajo se analizará ciertos comportamientos de la aplicación euclidiana mediante algunos teoremas del isomorfismo, anillos del polinomio, así como cierto tipo de anillos cocientes y unidades de anillo.

1.2. JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

Este trabajo se llevará a cabo porque los suscritos estamos interesados en caracterizar dominios euclidianos con resto único y doble. Partimos de que los numeros enteros son la primera interacción con un dominio euclidiano, de lo cual es bien conocido su algoritmo de la división teniendo doble residuo.

Los dominios euclidianos por lo general no admiten doble residuo, por ejemplo, el anillo de polinomios sobre un campo admite residuo único. En general no hay estudios sobre la cardinalidad de los residuos en un dominio euclidiano; es natural cuestionarse si al tener residuo único doble se pueda determinar alguna propiedad absoluta o en común

Una propiedad interesante muy conocida es el algoritmo de la división y aquellos anillos que la poseen son llamados dominios euclidianos. Evidentemente el algoritmo de la división sobre los enteros, puede generar doble resto, pero al considerarlo sobre cualquier campo se obtiene resto único.

En el presente trabajo se describe las propiedades que debe tener un conjunto para que tenga resto único o resto doble; dichas propiedades son estudiadas sobre las estructuras de cuerpos o anillos y de forma muy particular sobre un dominio euclidiano.

1.3. OBJETIVOS

1.3.1. Objetivo general

Caracterizar la propiedad del resto único y resto doble en los dominios euclidianos.

1.3.2. Objetivos específicos

- Caracterizar mediante isomorfismo a los dominios euclidianos con residuo único
- Caracterizar mediante isomorfismo a los dominios euclidianos con residuo doble
- Mostrar la existencia de dominios euclidianos que admitan más de dos residuos

II. MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Mariela, C. P. (2010), determina que los dominios euclidianos son el soporte de nuevas estructuras algebraicas que predominan en muchas ramas del algebra moderna (algebra conmutativa, algebra homológica, geometría algebraica, teoría de numeros algebraicos, algebra lineal sobre anillos), además afirma que todo dominio euclidiano es un anillo de ideales principales y lo reciproco es falso.

Héctor, M. P., Julio, J.F., Daniela, S.E. y Ximena, T. P. (2008), usan el concepto de Dominio de Integridad como un hilo unificador entre teorías y disciplinas. Para ello, enfocan el estudio hacia una construcción de los enteros y sus más importantes conceptos de divisibilidad y factorización, para proseguir con una estructuración de tales propiedades aritméticas en el sentido algebraico. Continúan con representaciones de Dominios de Integridad conocidos y algunas de sus aplicaciones en la Teoría elemental de Números. Para finalizar, construyen el cuerpo de cocientes de un Dominio de Integridad, tema asociado a los enteros y su incidencia en la formulación de los números racionales.

Kevin, J. M. (2010), En su trabajo estudia los campos numéricos con norma-euclidianos de Galois. Comprobó que basado en la teoría de Heilbronn, para K un cuerpo numérico de Galois de primer grado (p=1); mostró que solo hay un número finito de campos de este tipo que son norma-euclidiana. En el caso de que p = 2 todos estos campos euclidianos normativos han sido identificado, pero para $p \neq 2$, poco más se sabe. Damos las primeras cotas superiores sobre los discriminantes de dichos campos cuando $p > 2$.

Sus métodos conducen a un simple algoritmo que permite generar una lista de campos candidatas con normas euclidianas hasta un discriminante dado, y proporciona algunos resultados computacionales

José, S.H. (2005), muestra al lector un (libro) modelo de aprendizaje, con más de cien resultados básicos entre los cuales se hallan definiciones, teoremas, corolarios y algunos ejemplos de anillos, dominios euclidianos, extensión de campos, ideales, entre otros conceptos del algebra abstracta. En las demostraciones usa textos de teoría de cuerpos y teoría de Galois

2.2. BASES TEÓRICAS

2.2.1. Anillos

La teoría de anillos surgió de la exploración de asuntos vinculados con la divisibilidad entre números enteros, del estudio simultáneo de divisibilidad de polinomios y hasta del caso de los cuerpos, concretamente, de los números racionales, números reales, números complejos y de los números algebraicos, de los cuaterniones, fracciones racionales y otros. En la etapa inicial, fueron las materias de la teoría de números y de la geometría algebraica las que propiciaron los conceptos de anillo, cuerpo e ideal. En su estructuración axiomática, tales ideas fueron fruto del esfuerzo de Dedekind y otros matemáticos a fines del siglo XIX.

Definición: Un anillo es un conjunto no vacío R, dotado con dos operaciones binarias, llamadas suma y multiplicación y denotadas como "+" y "·" respectivamente, tal que, para cada a, b ∈ R se cumplen las siguientes propiedades:

- $a + (b + c) = (a + b) + c$
- existe un unico $0 \in R$ tal que: $a + 0 = 0 + a = a$
- Para cada $a \in R$ existe un elemento $-a \in R$ tal que:
- $a + (-a) = (-a) + a = 0$
- $a.(b.c) = (a.b).c$
- $a.(b + c) = a.b + a.c$
- $(a + b).c = a.c + b.c$

Ejemplo. El conjunto M de las matrices reales de orden 2, con la adición y multiplicación de matrices es un anillo no conmutativo

Ejemplo. El conjunto $Q(\sqrt{3})$ de los numeros reales: $m + n\sqrt{3}$ donde $m, n \in Q$, con la adición y multiplicación es un anillo conmutativo.

CARACTERÍSTICAS DE UN ANILLO

Es el menor número "n" tal que:

$$\underbrace{1 + 1 + 1 + 1 + \cdots \ldots \ldots \ldots .1}_{\text{n veces}} = 0$$

Ejemplo: los números enteros tienen característica cero

2.2.2. Grupo

Las raíces históricas de la teoría de grupos son la teoría de las ecuaciones algebraicas, la teoría de números y la geometría. Euler, Gauss, Lagrange, Abel y Galois fueron los creadores que ponen los cimientos de esta rama del álgebra abstracta. Galois es reconocido como el primer matemático que relacionó esta teoría con la teoría de cuerpos, de lo que surgió la teoría de Galois. Además, usó la denominación de grupo o " inventó el término grupo.

Definición: un grupo es un conjunto no vacío G dotada de una ley de composición interna

$$\begin{aligned} G \times G &\longrightarrow G \\ (g_1, g_2) &\longrightarrow g_1 g_2 \end{aligned}$$

Que satisface las siguientes condiciones:

Asociatividad: para $g_1, g_2, g_3 \in G$ tenemos que

$$(g_1 g_2) g_3 = g_1 (g_2 g_3)$$

Elemento neutro: existe un elemento $e \in G$ (necesariamente único) tal que para todo $g \in G$ tenemos que (adecuarlo al formato)

$$ge = eg = g$$

Elemento inverso: para todo $g \in G$ existe un elemento $g^{-1} \in G$ (necesariamente único) tal que (adecuarlo al formato)

$$gg^{-1} = g^{-1}g = e$$

Ejemplo: los numeros reales

2.2.3. Dominio euclidiano

En teoría de anillos, un dominio euclidiano (también llamado anillo euclidiano) es un dominio integral que puede estar dotado de una función euclidiana que permite una adecuada generalización de la división euclidiana de los enteros. Aquí desarrollaremos las propiedades que cumple dicha función y su utilidad en otras estructuras algebraicas

Definición. Un dominio integro R es euclidiano cuando existe un mapeo
φ: R {0}→N

que satisface:

a) Para a ≠ 0, b ≠ 0 ∈ R, entonces φ(a)≤ φ(ab)
b) Dados a ≠ 0, b ≠ 0, existen q, r ∈ R tal que b = q.a + r donde r = 0 o φ(r)≤ φ(a)

Nota: φ es llamada función euclidiana.

Ejemplo. Para $a, b, \in Z$ con $a = 17$, b = 4, existen $q = 4$, $r = 1$, y la aplicación φ(.)|. |

$$17 = 4 \text{ x } 4+1 \qquad \text{y} \qquad |1| < |4|$$

Proposición 1.1. todo campo es un dominio euclidiano

Prueba. Sea K un campo, entonces para un par de elementos D, d ∈ K con d ≠ 0, entonces $\boldsymbol{D = \left(\frac{D}{d}\right) d}$, es decir como si el residuo es 0, es decir podemos asociarla a cualquier aplicación, en particular, $\boldsymbol{\varphi(k) = 1, \forall\, k \in K}$.

Observación. Para Z admite doble residuo, y por la proposición anterior sobre los campos tenemos resto único.

Estos detalles podrían pasar por alto, pero si nos preguntamos, ¿tienen algo de especial aquellos dominios euclidianos don doble resto y más aun de resto único?

2.2.4. Dominios euclidianos con cociente y resto único

Por la proposición 1.1 notamos que los campos bajo la función euclidiana se obtienen resto único, que en este caso es 0.

Lema 1.1. El cociente y el residuo son únicos si y solo si
$\varphi(a + b) \leq \max\{\varphi(a), \varphi(a)\}$ (1.1)

Prueba. (→) Supongamos que existen a, b no nulos tal que
$\varphi(a + b) > \max\{\varphi(a), \varphi(a)\}$
Entonces consideremos $a,\ a + b$ para el algoritmo de la división, y por (1.1) tenemos $a = 0(a + b) + a\ con\ \varphi(a) < \varphi(a + b)$
$a = 1(a + b) - b\ con\ \varphi(b) < \varphi(a + b)$

pero en estas igualdades hay una división con cociente y residuo que no son únicos.

(←) Si se verifica la inecuación $\varphi(a + b) \leq \max\{\varphi(a), \varphi(a)\}$. Dados c, a no nulos, y supongamos que no se cumple la unicidad en el cociente y en el residuo, es decir,
$c = qa + r,\ r = 0$ o con $\varphi(r) < \varphi(a)$ (1.2)
$c = q'a + r',\ r' = 0$ o con $\varphi(r') < \varphi(a)$ (1.3)
Con r ≠ r' 1 y q ≠ q', entonces $q - q' \neq 0$, por la condición 1) en la definición de dominio euclidiano
$\varphi(a) \leq \varphi((q - q')a)$

pero $0 = c - c = (q - q')a + (r - r')$, así

$\varphi(a) \leq \varphi\big((q - q')a\big) \leq \varphi(r' - r) \leq max\{\varphi(r'), \varphi(-r)\} < \varphi(a)$

lo cual es absurdo, así deben existir unicidad en el cociente y residuo.

Observación. Podemos asumir que $\varphi(1) = 0$, caso contrario definimos $v: R\backslash\{0\} \to N \cup \{0\}$ con $v(a) = \varphi(a) - \varphi(1)$, esta aplicación conserva las propiedades de φ, veamos:

Si a no es unidad, entonces

$$\boldsymbol{v(a) = \varphi(a) - \varphi(1) = \varphi(a.1) - \varphi(1) \geq \varphi(1) - \varphi(1) = 0}$$

Entonces $\boldsymbol{v(a) \geq 0}$

a) Sean a, b no nulos $\boldsymbol{v(ab) = \varphi(ab) - \varphi(1) \geq \varphi(a) - \varphi(1) = v(a)}$

b) Sean D, d ϵ R, entonces existen q, r ϵ R tal que $D = qd + r$ con

$\boldsymbol{r = 0\ o\ \varphi(r) \leq \varphi(d)}$, de este ultimo restamos a ambos lados $\boldsymbol{\varphi(1)}$, obtenemos

$$\boldsymbol{v(r) = \varphi(r) - \varphi(1) < \varphi(d) - \varphi(1) = v(d)}$$

Con este caso decimos que $\boldsymbol{v}$ es una función euclidiana sobre R si y solo si φ es una función euclidiana sobre R

Observación: $\boldsymbol{v(t) = 0}$ si y solo si t es unidad de R. Pues:

$$\boldsymbol{0 = v(1) = v(t.t^{-1}) \geq v(t) \geq 0}$$

Sea $\mathbf{F = \{u \in R / u\ es\ unidad\ en\ R\} \cup \{0\}}$.

Proposición 1.2. $\mathbf{F \subset R}$ es un campo.

Prueba:

a) Sean a, b ∈ R, por el lema 1.1 tenemos que

$\boldsymbol{0 \leq v(a + b) \leq max\{v(a), v(b)\} \leq max\{0, 0\} = 0}$, así $\boldsymbol{v(a + b) = 0}$

b) Sean a, b ∈ F, b≠0, entonces b^{-1} y a son unidades luego su producto también lo es. Así $ab^{-1} \in F$

Si $\mathbf{F = R}$, entonces R es un campo.

Ahora solo queda analizar el caso cuando F ⊊ R, por la observación anterior, tenemos elementos $p \in R$ tal que v(p) ∈ N, luego por el principio del buen orden, existe $a \in R\backslash F$ tal que $v(a) \leq v(x), \forall\ x \in R\backslash F$

Lema 1.2. Si $\boldsymbol{a \neq 0}$ es tal que $\boldsymbol{v(a)}$ es un mínimo positivo, para $\boldsymbol{b \neq 0 \in R}$ existe únicos $\mathbf{q_0, q_1, \dots\dots, q_k \in F}$ tal que

$$\mathbf{b = q_k a^k + \cdots \dots \dots \dots + q_1 a + q_0},\ \boldsymbol{q_k \neq 0}$$

Entonces la aplicación $\boldsymbol{b \to \sum q_j x^j}$ es un isomorfismo

Prueba. Notemos que $v(a) > 0$. Primero mostraremos que $v(a^k)$, con $\boldsymbol{k = 1, 2, 3, 4}$, ... Es estrictamente creciente. Por inducción sobre k;

Para $k = 0,\ v(a^0) = v(1) = 0 < v(a)$, ahora tomemos a, a^2 para el algoritmo de la división, así existen $q, r \in R$ tal que

$\boldsymbol{a = qa^2 + r}$ con $\boldsymbol{r = 0\ o\ v(r) < v(a^2)}$

Si $\boldsymbol{q \neq 0}$, entonces $\boldsymbol{a - r = qa^2}$, aplicando $\boldsymbol{v}$ en ambos lados

$\boldsymbol{v(a - r) = v(qa^2) \geq v(a^2) > v(r)}$ pero tenemos,

$\boldsymbol{v(a - r) \leq \max\{v(a), v(-r)\} \leq v(r)}$

lo cual es absurdo, así $q = 0\ \ o\ \ r = a$, por tanto $v(a) < v(a^2)$. Ahora supongamos que es estrictamente creciente hasta N, mostraremos que ocurre lo mismo para N+1, veamos: tomemos $a^N\ y\ a^{N+1}$ para el algoritmo de la división, entonces existen s, t ∈ R tal que
$\boldsymbol{a^N = sa^{N+1} + t}$ con $\boldsymbol{t = 0\ \ o\ \ v(t) < v(a^{N+1})}$

Si $\boldsymbol{s \neq 0}$, entonces $\boldsymbol{a^N - t = sa^{N+1}}$, aplicando $\boldsymbol{v}$ en ambos lados,

$\boldsymbol{v(a^N - t) = v(sa^{N+1}) \geq v(a^{N+1}) > v(t)}$, pero

$\boldsymbol{v(a^N - t) \leq \max\{v(a^N), v(t)\} \leq v(r)}$, y esto es absurdo, así que $\boldsymbol{s = 0\ \ o\ \ t = a^N}$, por lo tanto $\boldsymbol{v(a^N) < v(a^{N+1})}$

Entonces tenemos,

$\boldsymbol{0 = v(a^0) < v(a) < v(a^2) < v(a^3) < \cdots \ldots \ldots \ldots v(a^k) < v(a^{k+1}) < \cdots}$

Si $b \neq 0,\quad v(a^k) < v(b) < v(a^{k+1})\quad (*)$ para algún $k \geq 0$, luego usamos el algoritmo de la división para b y a^k, entonces existen $q_k, r \in R$ tal que

$b = q_k a^k + r\quad (**)$ con $r = 0\ o\ v(r) < v(a^k)$. Notamos que $q_k \neq 0$, pues de ser nulo entonces $b = r$, lo que implica que $v(b) = v(r) < v(a^k)$ y contradice (*).

Si $\boldsymbol{q_k}$ no es unidad, es decir $\boldsymbol{v(q_k) \geq v(a)}$, usaremos el algoritmo de la división para $\boldsymbol{q_k}$ y a, así tenemos

$\boldsymbol{q_k = la + m,\qquad m \in F\ \ y\ \ l \neq 0}$

Reemplazamos en (**), $b = (la + m)a^k + r = la^{k+1} + ma^k + r$, es decir
$\boldsymbol{la^{k+1} = b - ma^k - r}$, pero $\boldsymbol{v(r) < v(a^k) < v(b)}$ y como $\boldsymbol{m \in F}$,

$\boldsymbol{v(ma^k) = v(a^k) < v(b)}$, además $\boldsymbol{v(a^{k+1}) \leq v(la^{k+1})}$ entonces

$\boldsymbol{v(a^{k+1}) \leq v(la^{k+1}) \leq v(b - ma^k - r) \leq \max\{v(b), v(ma^k), v(r)\} \leq v(b)}$

Esto contradice (*), así q_k es una unidad. Procederemos por inducción, y se obtiene una combinación lineal finita de la forma,

$\boldsymbol{b = \sum_{j=0}^{k} q_j a^j,\quad q_j \in F}$

Ahora solo nos queda mostrar que es única esa combinación lineal, es decir, si
$\boldsymbol{0 = \sum_{j=m}^{n} s_j a^j,\ s_j \in F}$, con $\boldsymbol{s_m \neq 0}$, despejamos $\boldsymbol{s_m}$,

$\boldsymbol{-s = a(\sum_{j=m+1}^{n} s_j a^{j-m-1})}$

Aplicando a ambos lados $\boldsymbol{v}$, y como

$$\sum_{j=m+1}^{n} \boldsymbol{s_j a^{j-m-1}} \neq \mathbf{0} = \boldsymbol{v}(\mathbf{1}) = \boldsymbol{v}(-\boldsymbol{s_m}) \geq \boldsymbol{v}(\boldsymbol{a})$$

y esto contradice la elección de $\boldsymbol{a}$. Así todo los $\boldsymbol{s_j}$ son cero.

Para terminar la prueba, definamos, T: F[x] → R, dado por el homomorfismo de evaluación sobre $\boldsymbol{a}$. Claramente es un isomorfismo.

Teorema 1.1. Sea R un dominio euclidiano con $1 \neq 0$. Si el cociente y el residuo en R son únicos, R es un campo; si $R \neq F$, entonces R ≅ F[x].

Prueba. Es inmediato de los lemas 1.1 y 1.2.

Este teorema nos dice lo siguiente, para los dominios euclidianos con resto único, o bien es un campo K o un anillo de polinomios $K[x]$

Ejemplo. C[x] es dominio euclidiano con resto único.

2.2.5. Naturaleza de Z como dominio euclidiano con residuo doble

Con la sección anterior, tener un dominio euclidiano con resto único tiene una influencia determinante en la estructura a formar, para ser más precisos, o bien es un campo o un anillo de polinomios sobre un campo. De esta misma forma, es natural preguntar si al tener doble resto sea posible que el dominio euclidiano obedezca a una cierta estructura. Los siguientes definiciones y lemas en adelante aclararan si los dominios euclidianos disiparemos aquellas dudas.

Definición. Un dominio euclidiano (R, g) decimos que tiene la propiedad de residuo doble (p.r.d) si para cada par de elementos a, b ≠ 0 (a ∈ R, b ∈ R) tal que b no divide a, entonces existen exactamente dos pares (q_i, r_i), (i = 1, 2) tal que, $a = q_i b + r_i$,
Donde $\boldsymbol{g(r_i) < g(b)}$

Sea (R, g) un dominio euclidiano teniendo la propiedad de resto doble, R asumido como un conjunto infinito.

Denotemos

U(R): el grupo de unidades de R (grupo multiplicativo)

$$\boldsymbol{R^* = R \backslash \{0_R\}}$$

Definición: Dado un dominio euclidiano (R, g), $R_1 \subset R^*$ definido por

$$\boldsymbol{R_1 = \{x \in R^* : g(x) \leq g(y)\ \forall\ y\ \in R^*\}}$$

Si u ∈ U(R), g(u) = g(1_R). Recordemos que $g(1_R) \leq g(a), \forall\ a\ \in R^*$. Además, si $\mathbf{t} \in \mathbf{R_1}$, entonces $\mathbf{g(t) \leq g(1_R)}$, pero $\mathbf{g(1_R) \leq g(t)}$, así $\mathbf{g(t) = g(1_R)}$, luego $\mathbf{t}\ \in \mathbf{U(R)}$. de este modo, $\boldsymbol{R_1 = U(R)}$: unidades de R.

Definición. Para $\boldsymbol{n \geq 2}$,

$$\boldsymbol{R_n = \{x \in R^*: g(x) \leq g(y), \forall\, y \ \in R^* \backslash R_{n-1}\}}$$

Lema 1.3.

$$R^* = \bigcup_{n=1}^{\infty} R_n$$

Prueba. Acabamos de ver que $\boldsymbol{R_1 = U(R)}$, ahora

$$R_2 = \{x \in R^*: g(x) \leq g(y), \forall\, y \ \in R^* \backslash R_1\}$$

Si t $\in R_1$, entonces $g(t) \leq g(y), \forall\, y \ \in R^*$. Asi $g(t) \leq g(y), \forall\, y \ \in R^* \backslash R_1$, luego $\mathbf{t} \in \boldsymbol{R_1}$, entonces $\boldsymbol{R_1 \subseteq R_2}$,

ahora veamos por induccion sobre n, que $R_n \subseteq R_{n+1}$, $\forall\, n \geq 1$, hemos visto que para $n = 1$ si cumple. Asumamos que se cumple para $m > 2$, es decir

$\boldsymbol{R_{m-1} \subseteq R_m}$, entonces

$\boldsymbol{R^* \backslash R_m \subseteq R^* \backslash R_{m-1}}$

Sea $\mathbf{t} \in \boldsymbol{R_m}$, $\boldsymbol{g(t) \leq g(y), \forall\, y \ \in R^* \backslash R_{m-1}}$, en particular para todo $\boldsymbol{y \ \in R^* \backslash R_m}$, Entonces $\mathbf{t} \in \boldsymbol{R_{m+1}}$, es decir $\boldsymbol{R_m \subseteq R_{m+1}}$. Asi tenemos que

$\boldsymbol{R_1 \subseteq R_2 \subseteq R_3 \subseteq \cdots}$

Si $M = \cup R_n$, entonces $M \subseteq R^*$, ahora veamos la otra inclusion: para $s \in R^*$, entonces existe $q \in$ N tal que $s \in R_q = \{x \in R^*: g(s) = g(x)\}$, asi $R_q \subset M$, luego $R^* \subset M$.
Por lo tanto $\boldsymbol{M = R^*}$

Lema 1.4. Si $\mathbf{u} \in \mathbf{U(R)}$, con $\boldsymbol{u \neq \pm 1_R}$, entonces $\boldsymbol{1_R + u} \in \mathbf{U(R)}$.

Prueba. Primero notemos que $-u \neq u^2$, porque de ser asi, $-1 = u$, basta simplificar u.
Si $\boldsymbol{1_R + u} \notin \mathbf{U(R)}$, entonces no es una unidad, luego $\boldsymbol{1_R + u}$ no divide a $\boldsymbol{1_R}$.

Consideremos $\boldsymbol{1_R}$ y $\boldsymbol{1_R + u}$ en el algoritmo de la divsion, veamos

$$1_R = (1_R + u)1_R - u$$
$$1_R = (1_R + u)(1_R - u) + u^2 \quad (*)$$
$$1_R = (1_R + u).0 + 1_R$$

Pero (R, g) tiene la propiedad de residuo doble, pero $-u \neq u^2$ y $-u \neq 1_R$, entonces $u^2 = 1_R$, reemplazando en **(*)**, entonces $1_R = (1_R + u)(1_R - u) + u^2 = (1_R + u)(1_R - u) + 1$, asi $0 = (1_R + u)(1_R - u)$, pero esto es una contradiccion pues por hipotesis $u \neq \pm 1_R$.

Por lo tanto $\boldsymbol{1_R + u} \in \mathbf{U(R)}$.

Corolario 1.1. Sea $\boldsymbol{u} \in \mathbf{U}(\mathbf{R})$, $\boldsymbol{u} \neq \pm \mathbf{1}_{\boldsymbol{R}}$, entonces $\mathbf{1}_{\boldsymbol{R}} - \boldsymbol{u} \in \mathbf{U}(\mathbf{R})$

Prueba. Del mismo modo que lo anterior

Lema 1.5. si $S(R) = U(R) \cup \{0\}$. Entonces $S(R)$ no forma un campo bajo las operaciones de anillo de R.

Prueba. Supomgamos lo contrario. Esto es, supobgamos que $S(R)$ es un campo. Sea $\boldsymbol{r} \in \boldsymbol{R_2 \backslash R_1}$, luego r no divide a $\mathbf{1}_{\boldsymbol{R}}$, luego hacemos el agortimo de la divsivion para

$\mathbf{1}_{\boldsymbol{R}}$ y r, y como (R, g) posee la p.r.d, entonces

$$\mathbf{1}_{\boldsymbol{R}} = \boldsymbol{r}.\mathbf{0} + \mathbf{1}_{\boldsymbol{R}};\ \ \boldsymbol{g}(\mathbf{1}_{\boldsymbol{R}}) < \boldsymbol{g}(\boldsymbol{r})$$
$$\mathbf{1}_{\boldsymbol{R}} = \boldsymbol{r}.\boldsymbol{q} + \boldsymbol{u};\ \ \boldsymbol{g}(\boldsymbol{u}) < \boldsymbol{g}(\boldsymbol{r}),$$

Entonces $u \neq 1_R$ y como $g(u) < g(r)$, entonces $u \in R_1$ (unidad de R), por el corolario anterior $1_R - u = rq$ es una unidad, entonces r tambien lo sera, lo cual contradice que $r \in R_2 \backslash R_1$

Lema 1.6. denotemos $\mathbf{1}_{\boldsymbol{R}} + \mathbf{1}_{\boldsymbol{R}} = \mathbf{2}_{\boldsymbol{R}}$, entonces $\mathbf{2}_{\boldsymbol{R}}$ es no nulo ni unidad en R.

Prueba. Si $\mathbf{2_R} \in \mathbf{S(R)} = \mathbf{U(R)} \cup \{\mathbf{0_R}\}$.

Sean $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{U}(\boldsymbol{R})$, entonces

$u + v = u(1_R + u^{-1}v)$

Si $\mathbf{u^{-1}v} \neq \pm \mathbf{1_R}$, entonces $\boldsymbol{u} + \boldsymbol{v} \in \boldsymbol{U}(\boldsymbol{R})$, por el lema anterior $\mathbf{1}_{\boldsymbol{R}} + \boldsymbol{u} \in \boldsymbol{U}(\boldsymbol{R})$, asi queda analizar el caso: $\mathbf{u^{-1}v} = \pm \mathbf{1_R}$. Si

1) $\boldsymbol{u} = \boldsymbol{v}$, entonces $\boldsymbol{u} + \boldsymbol{v} = \mathbf{1}_{\boldsymbol{R}}\boldsymbol{u}$.

- Si 2_R es unidad, entonces $u + v \in U(R)$
- Si $2_R = 0$, entonces $u + v = 0 \in S(R)$

2) $\boldsymbol{u} = -\boldsymbol{v}$, entonces $\mathbf{u} + \mathbf{v} = \mathbf{0}$

Pero S(R) no es uncuerpo, asi $\mathbf{2}_{\boldsymbol{R}}$ no es unidad ni cero.

Observacion. Como $\mathbf{2}_{\boldsymbol{R}} = \mathbf{0}_{\boldsymbol{R}}$, entonces la caracteristica de R no es 2.

Ahora mostraremos que R tiene caracteristica cero.

Lema 1.7. $Char(R) = 0$ y para $n \geq 2$, n_R no es unidad ni cero, es decir $\boldsymbol{n}_{\boldsymbol{R}} \notin \boldsymbol{S}(\boldsymbol{R})$

Prueba. Para $n = 2$, cumple. Veamos por induccion, para $n \leq N - 1$, $n_R \notin S(R)$, con $N \geq 3$, mostraremos que $N_R \notin S(R)$.

Caso I. Si $\boldsymbol{N+1}$ es compuesto.

Supongamos que $\boldsymbol{N_R \in S(R)}$.

- N_R es no nulo, supongamos lo contrario, si $N_R = 0_R$, entonces $(N-1)_R = -1_R$ (unidad), lo cual es absurdo pues $(N-1)_R$ no es unidad.

- ahora mostraremos que $N_R \neq \pm 1_R$. Supongamos lo contrario,
  - $N_R = 1_R$, entonces $(N-1)_R = 0_R$ pero $(N-1)_R$ no es cero
  - $N_R = -1_R$, entonces $(N+1)_R = 0_R$, pero $N+1$ es compuesto, luego existen $1 < a, b < N+1$ tal que $ab = N+1$ con $a_R a_R = 0_R$, lo cual es absurdo.

Caso II. Si $\boldsymbol{N+1}$ es primo.

- N_R es no nulo. Supongamos lo contrario, si $N_R = 0_R$, entonces
- $(N-1)_R = -1_R$ (unidad) lo cual es absurdo pues $(N-1)_R$ no es unidad

- Ahora mostraremos que $N_R \neq \pm 1_R$. Supongamos lo contrario,
  - $N_R = 1_R$, entonces $(N-1)_R = 0_R$, pero $(N-1)_R$ no es cero.

  - $N_R = -1_R$, entonces $(N+1)_R = 0_R$, pero $N+1$ es primo impar, entonces $N+1 = 2q-1$, asi $(N+1)_R = 2_R q_R - 1_R$, luego $1_R = 2_R q_R$, pero 2_R no es unidad.

Como la caracteristica de un dominio integrpo es un numero primo y para cada p primo $p_R \neq 0$, entonces $Char(R) = 0$ y $n_R \in S(R)$

Lema 1.8. $\boldsymbol{R_n}$ es un conjunto finito.

Prueba. Primero mostraremos que $R_1 = \{1_R, -1_R\}$, veamos: supongamos que exsiten $u \neq \pm 1_R$, entonces $1_R + u \in U(R)$, ademas $1_R + u \neq \pm 1_R$, entonces $\boldsymbol{2_R + u = 1_R + (1_R + u) \in U(R)}$, del mismo modo $\boldsymbol{u - 2_R \in U(R)}$, pero

$\boldsymbol{u, u-2_R, u+2_R}$ son distintas dos a dos y ademas tenemos que

$$u = 2_R 0_R + u$$
$$u = 2_R 1_R + (u - 2_R)$$
$$u = 2_R(-1_R) + (2_{R+u})$$

pero hay mas de dos restos, esto contradice la propiedad de resto doble de R asumiendo que $\boldsymbol{R_{n-1}}$ es finito.

Sea $\boldsymbol{x \in R_n \backslash R_{n-1}}$.

Afirmacion. $\boldsymbol{R/(x)}$ es un anillo finito de $\boldsymbol{k = 1 + \frac{1}{2}(\#R_{n-1})}$

Sea $\boldsymbol{a \in R}$ y $\boldsymbol{a \notin (x)}$, entonces por la propiedad de doble residuo

$$a = rq_1 + r_1 r_1 \in R_{n-1}$$
$$a = rq_2 + r_2 r_2 \in R_{n-1}$$

Entonces $\bar{a} = \overline{r_1} = \overline{r_2}$ (elementos de $R\backslash(x)$), debido a $\bar{0}\, y\, r_1, r_1$ asocian al mismo elemento en $R/(x)$, entonces hay $k = 1 + \frac{1}{2}(\#R_{n-1})$

Pero por la hipotesis $\boldsymbol{R_{n-1}}$ es finito, entonces $\boldsymbol{R/(x)}$ es finito .

Si: $\oplus$: denota la adicion en $R/(x)$, entonces $(R/(x),\oplus)$ es un grupo finito con k elementos. En $R/(x)$

$k(1_R \oplus (x)) = k1_R \oplus (x) = (x)$, entonces $k1_R \in (x)$

Esto quiere decir que x es divisor de $k1_R$. Pero como (R, g) es un dominio euclidiano, entonces es un dominio de factorizacion unica (D.F.U), luego la cantidad de divisores $k1_R$ es finita pues $U(R)$ es finito. Ahora notemos que:

$x \in R_n\backslash R_{n-1}$ entonces $x|k1_R$

Entonces $R_n\backslash R_{n-1}$ es finito y como R_{n-1} tambien es finito $R_n = R_n\backslash R_{n-1} \cup R_{n-1}$, por tanto R_n es finito

Corolario 1.2. si $\boldsymbol{x \in R^*}$, $\boldsymbol{R/(x)}$ es un anillo finito

Notemos que si $\boldsymbol{x, y \in R_n\backslash R_{n-1}}$ para algun n, entonces

$\#(R/(x)) = \#(R/(y))$

Es decir, es independiente de la eleccion del element, asi tenemos,

Defincion: para $\boldsymbol{x \in R^*}$, denotamos $\#(\boldsymbol{R/(x)})$ por $\boldsymbol{N(x)}$

$$N: R^* \to Z^+$$
$$x \to N(x) = \#(R/(x))$$

Lema 1.9. la norma $N(x)$ de $x \in R^*$ es multiplicativa. Esto es para $x, y \in R^*$, $\boldsymbol{N(xy) = N(x)N(y)}$

Prueba. Sean $x, y \in R^*$, consideremos los anillos cocientes $R/(x)\ y\ (y)/(xy)$ y definimos la aplicación,

$\psi: R/(x) \to (y)/(xy)$

Dado por $\psi(a + (x)) = ay + (xy), a \in R$. Esta aplicación es un homomorfismo de grupos, pues $\psi(a + (x)) = \psi(a + (x)) + \psi(b + (x))$.

Ademas ψ es inyectivo pues, si $\psi(a + (x)) = \psi(b + (x))$, entonces $(a - b)y \in (xy)$, luego $(a - b) \in (x)$. Tambien se concluye que ψ es sobreyectivo de manera que evidente.

Asi,

$$N(x) = \frac{\#(y)}{\#(xy)} \qquad (*)$$

Por otro lado definimos la aplicación,

$$\theta: R/(xy) \to R/(y)$$

Dada por $\theta\big(a + (xy)\big) = a + (y)$, primero veamos que este bien definida: sean $\boldsymbol{a, b} \in \boldsymbol{R}$ tal que $\boldsymbol{a} + (\boldsymbol{xy}) = \boldsymbol{b} + (\boldsymbol{xy})$, entonces $\boldsymbol{a} - \boldsymbol{b} \in (\boldsymbol{xy}) \subset (\boldsymbol{y})$, asi $\boldsymbol{a} - \boldsymbol{b} \in (\boldsymbol{y})$, es decir, $\boldsymbol{a} + (\boldsymbol{y}) = \boldsymbol{b} + (\boldsymbol{y})$. Esta aplicación es un homomorfismo pues $\boldsymbol{\theta\big(a + b + (xy)\big) = a + b + (y) = \big(a + (y)\big)\big(a + (y)\big) = \theta(a + (xy))\theta(b + (xy))}$.

Observemos que si defino este homomorfismo es sobreyectivo, y cuyo nucleo es $(y)(xy)$, vemos, $\theta\big(a + (xy)\big) = (y)$, entonces $a + (y) = (y), a \in (y)$, luego su nucleo es $(y)(xy)$ y por el teorema del isomorfismo,

$$\frac{R(xy)}{(y)/(xy)} \simeq R/(y)$$

Tomando su cardinal, y de (*)

$$N(xy) = N(y)\#(y)/(xy) = N(y)N(x)$$

Lema 1.10. para $\boldsymbol{n \geq 2}$. Tenemos

$$R_n \backslash R_{n-1} = \{x \in R^*: N(x) = 1 + \tfrac{1}{2}(\#R_{n-1})\}$$

Prueba. De la afirmacion del lema 1.8, si $x \in R_n \backslash R_{n-1}$, entonces $\#(\boldsymbol{R/(x)}) = \boldsymbol{N(x) = 1 + \frac{1}{2}(\#R_{n-1})}$. Asi definimos los conjuntos disjuntos, para $\boldsymbol{n \geq 2}$

$$A_n = R_n \backslash R_{n-1}$$

$$B_n = x \in R^*: N(x) = 1 + \tfrac{1}{2}(\#R_{n-1})$$

Entonces $\boldsymbol{A_n \subseteq B_n}$. Notemos ademas que

$$R^* \backslash U(R) = \bigcup_{n=2}^{\infty} A_n = \bigcup_{n=2}^{\infty} B_n$$

Ahora supongamos que existe $n_0 \geq 2$ tal que $A_{n_0} \subsetneq B_{n_0}$, entonces existe $x_0 \in B_{n_0}$ y $x_0 \notin A_{n_0}$, de (1.5) existe $m_0 \neq n_0$ tal que $x_0 \in A_{m_0} \subset B_{m_0}$, lo cual es absurdo pues $\{B_n\}$ son disjuntos dos a dos. por lo tanto $A_n = B_n$

Lema 1.11. para $\boldsymbol{x, y \in R, g(x) < g(y) \leftrightarrow N(x) < N(y)}$

Prueba. Veamos,

$\rightarrow$ sean $\boldsymbol{x, y \in R}$ tal que

$$N(x) = 1 + \frac{1}{2}(\#R_{n-1})$$

$$N(y) = 1 + \frac{1}{2}(\#R_{n-1})$$

Notemos que si $x \neq y$, entonces $n \neq m$. Asi, si $N(x) < N(y)$, entonces $\boldsymbol{\#R_{n-1} < \#R_{m-1}}$, ademas para cada $\boldsymbol{n \in N, R_n < R_{n+1}}$, luego $\boldsymbol{R_n \subset R_m}$, cuando $\boldsymbol{x \in R_n \backslash R_m}$; asi cuando $\boldsymbol{n < m}$, $\boldsymbol{g(x) < g(y)}$

$\leftarrow$ supongamos que $g(x) < g(y)$. Escogamos n, m enteros positivos tal que $x \in R_n$ y $y \in R_m$. Entonces, $n < m$,

$\boldsymbol{R_m} = \{\, \boldsymbol{y \in R^*: g(y) \leq g(t)\ \forall\ t \in R^* \backslash R_{m-1}}\}$

$R_m - R_{m-1} = \{\, y \in R^*: N(y) = 1 + \frac{1}{2}(\#R_{m-1})\}$

esta desigualdad es estricta. Caso contrario $\boldsymbol{x \in R_m \backslash R_{m-1}}$

Lema 1.12. Tenemos

$$R_2 \backslash R_1 = \{\pm 2_R\}$$

Prueba. Notar que

$$R_2 \backslash R_1 = \{x \in R^*: N(x) = 1 + \frac{1}{2}(\#R_1)\}$$

pero $\boldsymbol{\#R_1 = 2}$, entonces $\boldsymbol{R_2 \backslash R_1 = \{x \in R^*: N(x) = 2\}}$, asi $\boldsymbol{\#[R/(x)] = 2}$. Luego

$$\boldsymbol{R/(x) = \{\overline{0}, \overline{1_R}\}}$$

mas aun, como son elementos distintos, entonces

$\overline{0_R} = 2(\overline{1_R}) = 2\big(1_R + (x)\big) = 2_R + (x) = (x)$, es decir $2_R = (x)$, entonces al estar en ese ideal principal, existe un $\boldsymbol{y} \in R^*$ tal que $xy = 2_R$, tomando norma en ambos lados, $N(y) = 1$, es decir, $\boldsymbol{y}$ es unidad, por conaiguiente $x = \pm 2_R$. Por lo tanto,

$\boldsymbol{N(x^2) = (N(x))^2 = 4}$

hacemos el algoritmo de la division para $\boldsymbol{1_R}$ y $\boldsymbol{x - 1_R}$,

$$1_R = -(x - 1_R) + x$$
$$1_R = -(x + 1_R)(x - 1_R) + x^2$$
$$1_R = 0_R(x - 1_R) + 1_R$$

Si $N(x - 1_R) > 4$, entonces $N(x) < N(x - 1_R)$, $N(x^2) = 4 < N(x - 1_R)$. Ademas $N(1_R) < N(x - 1_R)$. Pero esto contradice la propiedad de resto doble, asi

$\boldsymbol{N(x - 1_R) \leq 4}$. De forma similar podemos obtener lo siguiente

$N(\pm 1_R \pm x) \leq 4$

Ahora mostraremos que de $\pm x \pm 1_R$, no hay dos iguales. Notemos que x no es unidad ni cero, luego

- Si $1_R + x = -1_R + x$, entonces $2_R = 0$
- Si $1_R + x = 1_R - x$, entonces $2_R x = 0$
- Si $-1_R - x = 1_R + x$, entonces $-2_R = 2x$, es decir $x = -1_R$

Observemos que en congruencia modulo $\boldsymbol{2_R}$,

$$1_R + x = 2_R x + (1_R - x)$$
$$1_R + x = 2_R 1_R + (-1_R + x)$$
$$1_R + x = 2_R 0_R + (1_R + x)$$

Por la propiedad de resto doble, $N(2_R) \leq N(\pm 1_R \pm x) \leq 4$ *o* $N(2_R) \leq 4$, como $\boldsymbol{2_R = xy}$, entonces $\boldsymbol{N(y) \leq 2}$. Si todos los $(\pm \boldsymbol{1_R} \pm \boldsymbol{x})$ tiene norma menor a 4,

Entonces $N(2_R) < 4$, caso contrario contradice la propiedad de resto doble. Por Otro lado, si $\boldsymbol{N(2_R) < 4}$, entonces $\boldsymbol{N(2_R) = N(xy) = N(x)N(y) = 2N(y) < 4}$, asi

$\boldsymbol{N(y) = 1}$

Ahora sin perdida de generalidad sonsideremos, $N(1_R - x) = 4$. Si $N(a) = 4$, entonces $\#R/(a) = 4$, desde que cualquier de norma 4 es producto de irreducibles dividiendo 2_R, supongamos que $ab = 4_R$, para algun $b \in R$. Como R es un dominio de facturizacion (pues es dominio euclidiano), entonces $ab = 2_R 2_R$. Como $N(1_R - x) = 4$ y $xy = 2_R$, entonces $\boldsymbol{x}$ divide a $1_R - x$. O $\boldsymbol{y}$ divide a $1_R - x$. Si x divide $1_R - x$, entonces

$\boldsymbol{1_R - x} \in (\boldsymbol{x})$, pero al ser un ideal, cumple la cerradura bajo la suma, luego $(\boldsymbol{1_R - x}) + \boldsymbol{x} = \boldsymbol{1_R} \in (\boldsymbol{x})$, por lo que $\boldsymbol{x}$ es una unidad. Asi $\boldsymbol{y}$ divide a $\boldsymbol{1_R - x}$ y $\boldsymbol{N(y) = 2}$, por lo que $\boldsymbol{1 - x = \pm y^2}$. Ahora,

$$R_2 \backslash R_1 = \{x \in R^* : N(x) = 2\} = \{\pm x, \pm y\}$$

Mas aun, si $\boldsymbol{N(1_R - x) = 4}$, entonces

$$R_3 \backslash R_2 = \{x \in R^* : N(x) = 4\} = \{\pm x^2, \pm xy, \pm y^2\}$$

Desde que $\boldsymbol{N(1_R + x) \leq 4}$, y como $\boldsymbol{x}$ no divide a $\boldsymbol{1_R + x \neq 1_R - x}$, asi $\boldsymbol{1_R + x \neq \pm y^2}$ o $\boldsymbol{1_R + x \neq pmy}$. Luego

$$y^2 = (1_R + x)^2 = \pm(1_R - x)$$

- Si $(1_R + x)^2 = (1_R - x)$, entonces $x(x + 3_R) = 0$, pero como x es no nulo, luego $x = -3_R$ y por consiguiente, $y = \pm 2_R$, esto implica que $x = \pm 1_R$, lo cual es una contradiccion.

- Si $(1_R + x)^2 = -(1_R - x)$, entonces $x^2 + x + 2_R = 0$, asi $x = \frac{-1_R \pm \sqrt{1_R - 8_R}}{2}$, es decir,

$$\boldsymbol{2x + 1_R = \sqrt{-7_R} \in R}$$

como $\#\boldsymbol{R_3} = \#(\boldsymbol{R_3 - R_2}) + \#(\boldsymbol{R_2 - R_1}) + \#\boldsymbol{R_1} = \boldsymbol{12}$. Por el lema 1.10,

$$R_4 \backslash R_3 = \left\{ t \in R^* : N(t) = 1 + \frac{1}{2}(12) = 7 \right\}$$

Si $z \in R_4 \backslash R_3$, entonces z divide $\sqrt{-7_R} = 1_R + 2x = x - y$. Pero $\boldsymbol{x^2 \equiv xy = y^2}$ mód $\boldsymbol{z}$, lo cual contradice la propiedad de resto doble.

Por tanto $\boldsymbol{N(y) = \pm 1}$, y $\boldsymbol{R_2 \backslash R_1}$tiene solo como a elementos a $\boldsymbol{2_R}$ y $\boldsymbol{-2_R}$.

Teorema 1.2. Si: (R, g) es un dominio euclidiano con la propiedad de resto doble, entonces $R \cong Z$

Demostracion. La prueba es por induccion sobre la funcion norma. Tenemos que $\boldsymbol{R_1 = U(R) = \{\pm 1_R\}}$. Por un lema anterior, $\boldsymbol{R_2 \backslash R_1 = \{\pm 2_R\}}$. Ahora consideremos

$$n_R = 1_R + 1_R + \cdots + 1_R \ (n \ veces)$$

Entonces $N(n_R) = n$ para $n = 1$ y para $n = 2$. Supongamos que $N(k_R) = k$ para todo $\boldsymbol{k \leq (n - 1)}$.

Caso 1. Si $\boldsymbol{n}$ es compuesto, entonces por ser $N: R^* \to N$ multiplicativa, para una desacomposicion de $n = ab$, con $1 < a, b < n$, entonces $\boldsymbol{N(n_R) = N(a_R)\, N(b_R) = ab = n}$.

Caso 2. Si $\boldsymbol{n}$ es primo impar. Entonces, $\boldsymbol{(n + 1)}$ es par, luego

$$N((n+1)_R) = N\left(\frac{2(n+1)_R}{2}\right)$$
$$= N(2_R) N\left(\frac{(n+1)_R}{2}\right)$$

Pero $1 < \frac{n+1}{2} < n$, entonces $N\left(\frac{(n+1)_R}{2}\right) = \frac{(n+1)}{2}$, asi $N((n+1)_R) = n + 1$. Por otro lado

$$1_R = 1_R (n+1)_R - n_R$$

Entonces $N(n_R) \leq (n + 1)$. Pero 1_R tiene orden aditivo n en $R/(n_R)$ y asi n divide a $N(n_R)$. Entonces $N(n_R) = n$. Sea $y \in R^*$, entonces

$$\#\{x \in R^* : N(x) < N(y)\} = 2(N(y) - 1)\}$$

Luego existe $n \in N$ tal que $y \in R_n/R_{n-1} = \{y \in R^*: N(y) = 1 + \frac{1}{2}(\#R_{n-1})\}$, asi $\{\boldsymbol{x \in R^*: N(x) < N(y)}\} = \boldsymbol{R_{n-1}}$ y $\boldsymbol{\#R_{n-1} = 2N(y) - 1}$. Si hacemos $\boldsymbol{y = n_R}$, entonces

$$\{x \in R^*: N(x) < n\} = \{\pm 1_R, \pm 2_R, \pm 3_R \ldots \pm (n-1)_R\}.$$

Como

$$\cup_{n-1}^{\infty}\{x \in R^*: N(x) < n\} = R^*$$

entonces $\boldsymbol{R \cong Z}$ ó $\boldsymbol{R = Z}$, en cualquier caso, son isomorfos.

Ejemplos

Como primer ejemplo, consideremos $Z[i] = \{a + bi: a, b \in Z\}$, llamdo el anillo de los enteros gaussianos.

Definición. Sea $\boldsymbol{N}: \boldsymbol{Z[i]}\{\boldsymbol{0}\} \rightarrow \boldsymbol{Z^+}$, dada por

$\boldsymbol{N(a + bi) = a^2 + b^2 = (a + bi)\overline{a + ib}}$.

Proposicion 1.3. $(\boldsymbol{Z[i], N})$ es un dominio euclidiano.

Prueba. Sea $p, q\ en\ Z[i]$, consideremos el par $p\bar{q}, q\bar{q}$, el segundo termino es un número entero, $p\bar{q} = a + bi$ para algun $a, b \in Z$, y hacemos el algoritmo de la divsion para $a, q\bar{q}$ y para $b, q\bar{q}$, entonces existen $h_1, h_2 \in Z$ y $|r_1| \leq q\bar{q}\,/2$,

$\boldsymbol{|r_2| \leq q\bar{q}\,/2}$

Tal que

$$a = h_1 q\bar{q} + r_1$$
$$b = h_2 q\bar{q} + r_2$$

Luego

$$a + bi = (h_1 + ih_2)q\bar{q} + (r_1 + ir_2)$$

Y regresamos a su forma anterior,

$$p\bar{q} = (h_1 + ih_2)q\bar{q} + (r_1 + ir_2) \text{ con } r = r_1 + ir_2$$

Entonces $\boldsymbol{r\bar{q} = r_1 + ir_2 = (p - hq)\bar{q}}$ con $\boldsymbol{h = h_1 + ih_2}$, dividiendo $\boldsymbol{\bar{q}}$,

$$(r_1 + ir_2)/\bar{q} = r = p - hp \in Z[i]$$

Es decir, $\boldsymbol{p = hp + r}$.

Notemos que

$$N(r) = \frac{N(r_1 + ir_2)}{N(\bar{q})} = \frac{{r_1}^2 + {r_1}^2}{q\bar{q}} \leq \frac{1}{2}\frac{(q\bar{q})^2}{q\bar{q}} < N(q).$$

ademas para $a, b \in Z[i]$ no nulos, $N(ab) = ab\overline{ab} = (a\bar{a})(b\bar{b})$, pero al ser b no nulo $N(b) \geq 1$, entonces $N(ab) \geq N(a)$. Con esto concluimos la prueba.

Ahora hagamos algunas observaciones sobre el anillo de los enteros Gaussianos, de manera evidente no es isomorfo a Z, tampoco es un campo ni es isomorfo a anillo de polinomios sobre un campo. Entonces nuestros resultados anteriores nos aseguran que existen pares $\boldsymbol{Z[i]}$ que al efectuar la división podemos encontrar más de 2 restos.

Ejemplo. Consideremos $\mathbf{2} + \boldsymbol{i}$ y $\mathbf{1} + \boldsymbol{i}$ para el algoritmo de la división

$$2 + i = (1 + i)(1 - i) + i$$
$$2 + i = (1 + i)(2) - i$$
$$2 + i = (1 + i)(1) + 1$$
$$2 + i = (1 + i)(2 - i) - 1$$

Entonces hemos obtenido 4 residuos distintos.

Con este primer ejemplo podríamos pensar que algo similar a la p.r.d que tienen Z se podría extender para $Z[i]$, con cuatro residuos, pero veremos que no es posible, veamos con un ejemplo este hecho,

Ejemplo. Consideremos $7 + i, 7 \in Z[i]$, notemos que 7 no divide a $7 + i$ y los cocientamos,

$$7 + i = 7x1 + i$$
$$7 + i = 7x(1 + i) - 6i$$

pero solo obtenemos dos residuos.

Así como hay el anillo de los enteros Gaussianos, que hemos podido encontrar divisiones con 2 restos, 4 restos, también hay anillo denominado: anillo de enteros de Eisenstein.

Definición. Sea $\boldsymbol{\omega} \in \boldsymbol{C}$ una raíz cubica primitiva de $-\mathbf{1}$, digamos

$$\omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$$

y consideremos el conjunto

$$Z[\omega] = \{a + b\omega : a, b \in Z\} \subseteq C$$

Observacion.

1. Si $a + b\omega, c + d\omega \in Z[\omega]$, entonces para la suma tenemos que $(a + b\omega)(c + d\omega) = (a + c) + (b + d)\omega \in Z[\omega]$.

2. $a + b\omega, c + d\omega \in Z[\omega]$, $(a + b\omega)(c + d\omega) = (ac - bd) + (ad + bc + bd)\omega \in Z[\omega]$, pues $\omega^2 = \omega - 1$

De este modo $Z[\omega]$ es un anillo conmutativo con unidad, y es un dominio entero por ser un subconjunto de C.

ahora mostraremos que que $\boldsymbol{Z[\omega]}$ es un dominio euclidiano.

Defincion. Sea $\boldsymbol{N}: \boldsymbol{Z}[\boldsymbol{\omega}] \rightarrow \boldsymbol{N} \cup \{\mathbf{0}\}$ dado por

$$N(a+b\omega) = |a+b\omega|^2 = a^2 + ab + b^2$$

Proposicion 1.4. $(\boldsymbol{Z}[\boldsymbol{\omega}], \boldsymbol{N})$ es un dominio euclidiano**.**

Prueba. Sean $\boldsymbol{u} = \boldsymbol{a} + \boldsymbol{b\omega}$ y $\boldsymbol{v} = \boldsymbol{c} + \boldsymbol{d\omega}$ en $\boldsymbol{Z}[\boldsymbol{\omega}]$,

$$\begin{aligned}\frac{u}{v} = \frac{a+b\omega}{c+d\omega} &= \frac{(a+b\omega)(\overline{c+d\omega})}{N(c+d\omega)} \\ &= \frac{(a+b\omega)(c+d\bar{\omega})}{N(c+d\omega)} \\ &= \frac{(a+b\omega)(c+d(1-\omega))}{N(c+d\omega)} \\ &= \frac{ac+ad+bd}{c^2+d^2+cd} + \frac{bc+bd-ad}{c^2+d^2+cd}\,\omega = \alpha + \beta\omega\end{aligned}$$

Como $\boldsymbol{\alpha}\ \boldsymbol{y}\ \boldsymbol{\beta} \in \boldsymbol{Q}$, entonces existen $\boldsymbol{m}, \boldsymbol{n} \in \boldsymbol{Z}$ tal que

$|\boldsymbol{\alpha} - \boldsymbol{m}| \leq \frac{\mathbf{1}}{\mathbf{2}}$ y $|\boldsymbol{\beta} - \boldsymbol{n}| \leq \frac{\mathbf{1}}{\mathbf{2}}$, entonces

$$\begin{aligned}N\left(\frac{u}{v} - (m+n\omega)\right) &= N\big((\alpha-m) + (\beta-n)\omega\big) \\ &= (\alpha-m)^2 + (\beta-n)^2 + (\alpha-m)(\beta-n) \\ &\leq (\alpha-m)^2 + (\beta-n)^2 + |\alpha-m||\beta-n| \\ &\leq \tfrac{3}{4} < 1\end{aligned}$$

Esto verifica el algoritmo de la división y puesto que N es multiplicativa entonces $N(ab) \geq N(a)$ para $a, b \in Z[\omega]$ no nulos

Veamos que ocurre con respecto a los residuos. Así como el anillo de los enteros Gaussianos, el anillo de los enteros de Eisenstein no es un anillo isomorfo a Z, no es un campo, tampoco isomorfo a un anillo de polinomios sobre un campo. Entonces deben existir elementos tal que efectuar el algoritmo de la división podamos encontrar más de 2 residuos. Veamos

Ejemplo. Consideremos $\mathbf{2} + \boldsymbol{\omega}$ y $\mathbf{1} + \boldsymbol{\omega}$ en $\boldsymbol{Z}[\boldsymbol{\omega}]$, entonces

$$\begin{aligned}2+\omega &= (1+\omega)x2 - \omega \\ 2+\omega &= (1+\omega)x1 + 1 \\ 2+\omega &= (1+\omega)(2-\omega) + (\omega-1)\end{aligned}$$

Y solo hay tres residuos.

2.3. HIPÓTESIS

Es posible caracterizar la propiedad de resto único y doble sobre los dominios euclidianos mediante una función euclidiana.

III. MARCO METODOLÓGICO

3.1. ENFOQUE

De acuerdo con el enfoque de investigación, esta puede ser cuantitativa. En esta tesina, se asumió el enfoque cuantitativo; puesto que este enfoque es secuencial y probatorio. Cada etapa procede a la siguiente y no se puede eludir pasos. El orden es riguroso, aunque desde luego, podemos redefinir alguna fase. Parte de una idea que va acotándose y, una vez delimitada, se derivan objetivo y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y se determinan variables; se traza un plan para justificarlas, y se extrae una serie de conclusiones.

3.2. TIPO

La investigación es de tipo básica, pura o fundamental, pues se utiliza las teorías existentes para profundizar en ellas, generando nuevos conocimientos o criterios.

La investigación que se va a desarrollar tiene diseño inductivo - deductivo tratando de ser lo más exhaustivo posible en cada demostración.

Se empezará definiendo los términos básicos con respecto a los dominios euclidianos, posteriormente se demostrarán proposiciones y lemas necesarios para luego caracterizar la propiedad de resto único y propiedad de doble residuo.

3.3. MÉTODOS Y PROCEDIMIENTOS

Primero describimos los conceptos de dominio euclidiano y de función euclidiana la cual se usará para determinar la condición necesaria y suficiente para los dominios euclidianos de resto único, de ello se podrá obtener la caracterización el cual será demostrar que los dominios euclidianos de resto único son campos o anillo de polinomios sobre un campo. Luego respecto a los dominios euclidianos de resto doble, analizaremos su grupo de unidades el cual nos permitirá calcular la nulidad de su característica, de igual forma este análisis nos permitirá que este dominio euclidiano es isomorfo a $\mathbb{Z}$.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Cuando se caracterizan a los dominios euclidianos usamos una equivalencia de residuo único y la aplicación euclidiana, para después estudiar las unidades del Dominio, de la cual podemos determinar si es un cuerpo o se asocia a un anillo de polinomios sobre un cuerpo. Para los dominios euclidianos con residuo doble, usamos los anillos cocientes y comportamientos en la cardinalidad de estos anillos cocientes, así como teoremas del isomorfismo

Concluimos que $(Q[x], \varphi)$ con $\varphi(P) = grad(P)$ es dominio euclidiano con resto único, y (Z, φ) con $\varphi(x) = |x|$ es dominio euclidiano con doble residuo.

4.2. DISCUSIONES

Según el objetivo general, caracterizar la propiedad de resto único y doble en los dominios euclidianos

CONCLUSIONES

Se demostró que los dominios euclidianos con residuo único son isomorfos a un campo o un anillo de polinomios sobre un campo

Se demostró que los dominios euclidianos con resto doble son isomorfismos al anillo de los números enteros

Se demostró que existen dominios euclidianos con resto múltiple mayor a 2

REFERENCIAS BIBLIOGRÁFICAS

Galovich, S. (1978). A Characterization of the Integers Among Euclidean Domains, The American Mathematical Monthly, vol. 85 No. 7, pp. 572-575.

Hall, F. M. (1969). «Section 3.6». An Introduction to Abstract Algebra 2. Cambridge University Press. ISBN 0521084849.

Heilbronn, H. (1938). On Euclid's algorithm in real quadratic fields, Pro. Cambrigde Phil. Soc. 34, pp. 521-526.

Herstein, I. N. (1975). «Section 3.9». Topics in Algebra. Wiley. ISBN 0471010901.

Jodeit, M. A. Jr. (1967). Uniqueness in the División Algorithm, The American Mathematical Monthly, Vol. 74, No. 7, pp. 835-836.

ANEXOS

MATRIZ DE CONSISTENCIA

TÍTULO: RESIDUOS EN DOMINIOS EUCLIDIANOS			
Problema	**Objetivos**	**Hipótesis**	**Variables**
¿Sera posible caracterizar la propiedad de resto único y doble sobre los dominios euclidianos?	**Objetivo general** Caracterizar la propiedad del resto único y resto doble en los dominios euclidianos 1. Objetivos específicos Caracterizar mediante isomorfismo a los dominios euclidianos con residuo único 2. Caracterizar mediante isomorfismo a los dominios euclidianos con residuo doble 3. mostrar la existencia de dominios euclidianos que admitan más de dos residuos	Es posible caracterizar la propiedad de resto único y doble sobre los dominios euclidianos mediante una función euclidiana.	Variables independientes • Propiedades básicas de los numeros enteros • Resultados básicos sobre campos y anillos Variable dependiente • Caracterización de la propiedad de resto único y doble sobre los dominios euclidianos