SOBRE LA ESTRUCTURA DE LOS DOMINIOS EUCLIDIANOS

JHONNIER ESTEBAN CASALLAS MARIN

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

SOBRE LA ESTRUCTURA DE LOS DOMINIOS EUCLIDIANOS

JHONNIER ESTEBAN CASALLAS MARIN

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 Jazmin, Hugo, Orfenia, Sergio, Yudyth, quienes me acompañaron durante todo el proceso.

AGRADECIMIENTOS

Un agradecimiento especial a mi madre, padre y abuela, quienes me apoyaron en todas las decisiones que tomé.

Al profesor Héctor Pinedo, quien me brindó la confianza y paciencia necesarias para llevar acabo este trabajo de grado.

A Javier y Jamir, por ser los mejores compañeros que un estudiante podría desear.

A Yudyth, por ser quién que me impulsó a ser una mejor persona y sostuvo mi mano en los momentos difíciles.

Por último, a todas aquellas personas con las que tuve la oportunidad de cruzar palabras, ideas y momentos; en especial, aquellas personas con las que pude compartir esta bella ciencia, la matemática.

CONTENIDO

RESUMEN

TÍTULO: SOBRE LA ESTRUCTURA DE LOS DOMINIOS EUCLIDIANOS [*]

AUTOR: JHONNIER ESTEBAN CASALLAS MARIN [**]

PALABRAS CLAVE: ANILLO, ESTRUCTURA, DOMINIO EUCLIDIANO, DIVISIÓN CON RESTO.

DESCRIPCIÓN:

Los dominios euclidianos son una clase de dominios enteros que se estudiaron por primera vez en el contexto de la teoría de números y posteriormente se generalizaron en la teoría de anillos, dicha estructura algebraica nace del querer generalizar el algoritmo de la división de los números enteros a otro tipo de conjuntos, como lo son los anillos y los cuerpos.

El concepto de dominio euclidiano fue introducido por primera vez por el matemático alemán Ernst Eduard Kummer en el siglo XIX, en sus estudios sobre los números ideales. Sin embargo, la formalización moderna del concepto, tal y como se entiende hoy en día, se atribuye al matemático alemán David Hilbert a finales del siglo XIX y principios del XX, en sus trabajos sobre la teoría algebraica de los números y en su famoso libro ≪*Zahlbericht*≫ publicado en 1897.

Keith Conrad en [1] muestra dos formas de definir un dominio euclidiano, la primera es un dominio entero (anillo conmutativo con unidad y sin divisores de cero) en el cual existe una función (comunmente llamada función euclidea) d la cual cumple dos propiedades:

1. $0 \leq d(a) \leq d(ab)$ para todo a y b distintos de cero en el anillo.
2. Para todo a y b en el anillo con $b \neq 0$, es posible encontrar q y r en el anillo tal que $a = bq + r$, donde $r = 0$ o $d(r) < d(b)$.

La primera condición se conoce como la *d-desigualad* y la segunda condición es la definición de división con resto, Conrad da una segunda definición en la cual solo aparece la divisón con resto y menciona que es la definición usual de dominio euclidiano, sin embargo, para la primera definición, se dice que es un dominio euclidiano que posee una función euclidea que satisface la *d-desigualdad*.

En este trabajo de grado se estudiará la estructura de dominio euclidiano y se buscará obtener algunas propiedades de esta estructura sobre anillos cuadráticos.

---

[*] Trabajo de grado

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

[1] Keith CONRAD. “Remarks about Euclidean domains”. En: *https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf* (2020).

ABSTRACT

TITLE: ON THE STRUCTURE OF EUCLIDEAN DOMAINS. [*]

AUTHOR: JHONNIER ESTEBAN CASALLAS MARIN [**]

KEYWORDS: RING, STRUCTURE, EUCLIDEAN DOMAIN, DIVISION WITH REMAINDER.

DESCRIPTION:

Euclidean domains are a class of integer domains that were first studied in the context of number theory and later generalized in the theory of rings. This algebraic structure arises from the desire to generalize the algorithm of the division of integers to other types of sets, such as rings and fields.

The concept of Euclidean domain was first introduced by the German mathematician Ernst Eduard Kummer in the 19th century, in his studies on ideal numbers. However, the modern formalization of the concept, as it is understood today, is attributed to the German mathematician David Hilbert in the late 19th and early 20th century, in his work on algebraic number theory and in his famous book "*Zahlbericht*" published in 1897.

Keith Conrad in [1] shows two ways to define a Euclidean domain, the first is an integer domain (commutative ring with unity and no divisors of zero) in which there exists a function (commonly called a Euclidean function) d which satisfies two properties:

1. $0 \leq d(a) \leq d(ab)$ for all non-zero a and b in the ring.
2. For all a and b in the ring with $b \neq 0$, it is possible to find q and r in the ring such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

The first condition is known as the *d-inequality* and the second condition is the definition of division with remainder, Conrad gives a second definition in which only the division with remainder appears and mentions that it is the usual definition of Euclidean domain, however, for the first definition, it is said that it is a Euclidean domain that has a Euclidean function that satisfies the *d-inequality*.

In this thesis we will study the Euclidean domain structure and we will try to obtain some properties of this structure on quadratic rings.

---

[*] Bachelor Thesis

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

Introducción

Las estructuras algebraicas son objeto de estudio de un número considerable de investigaciones, cuyos resultados contribuyen en la exploración de nuevas propiedades que faciliten el planteamento y solución de algunos problemas relacionados con las mismas. En la teoría de anillos existe una estructura denominada dominio euclidiano, el cual es un anillo conmutativo R donde se puede definir una función euclidea d.

Esta función puede o no cumplir una serie de propiedades, una de ellas es la *d-desigualdad* (ver Definición 1.0.16), la cuál en algunas definiciones de dominio euclidiano hace aparición y en otras no, esto se debe a que es irrelevante para probar algunos teoremas importantes como por ejemplo: Todo dominio euclidiano es un *DIP* o, el algoritmo de Euclides en un dominio euclidiano termina después de un número finito de pasos y produce un máximo común divisor, sin embargo la *d-desigualdad* es importante si se desea demostrar que existe factorización irreducible en dominios euclidianos, sin tener que depender de una demostración de esta propiedad por métodos más abstractos.

La intención de esta monografía es estudiar las notas de Keith Conrad [1], donde se discuten algunas caracteristicas de una función euclidea $\tilde{d}$ definida a partir de la función euclidea d y analizar la estructura de dominios euclidianos sobre anillos cuadráticos.

Este trabajo está estructurado como sigue, primeramente se hace una comparación entre dos definiciones de dominios euclidianos con el objetivo de estipular que ambas están relacionadas (ver Teorema 2.0.4) luego, se estudian algunas características de la *d-desigualdad* con la finalidad de hacer uso de ella en algunas pruebas relacionadas con factorización irreducible, por último se hará un análisis sobre la estructura de dominio euclidiano en algunos anillos cuadráticos mediante resultados obtenidos a lo largo del trabajo.

1. Preliminares

En esta sección se mostrarán algunas definiciones y ejemplos útiles para la comprensión de todo el trabajo.

Definición 1.0.1. Un anillo R es un conjunto no vacío dotado de dos operaciones binarias llamadas suma $(+ : R \times R \to R)$ y producto $(\cdot : R \times R \to R)$ que satisfacen los siguientes axiomas:

- $(R, +)$ es un grupo abeliano.
- $(R, \cdot)$ es un semigrupo.
- El producto es distributivo respecto a la suma, es decir, dados a, b, c en R, entonces:
  - $a \cdot (b + c) = a \cdot b + a \cdot c$,
  - $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definición 1.0.2. Sea R un anillo y $S \subset R$ un subconjunto no vacío de R, se dice que S es subanillo de R si es un subgrupo de R y además es cerrado bajo el producto, i.e., dados $a, b \in S$, entonces $a - b \in S$ y $a \cdot b \in S$, donde $(+)$ y $(\cdot)$ son las operaciones de R restringidas a los elementos de S.

Definición 1.0.3. Sea R un anillo:

- Se dice que R es un anillo con unitario, si R posee neutro bajo la operación binaria producto y se denota como 1.
- Se dice que R es un anillo conmutativo, si $a \cdot b = b \cdot a$ para todo a y b en R.

Ejemplo 1.0.4. El conjunto $\mathbb{Z}$ con la suma y producto usual de enteros es un anillo conmutativo con unitario.

Definición 1.0.5. Sea R un anillo con unitario, un elemento $a \in R$ es una unidad si a es invertible bajo la operación binaria producto.

El conjunto de todas las unidades de R (elementos invertibles) se denota por $U(R)$. El inverso de a se denota por a^{-1}.

Ejemplo 1.0.6. $U(\mathbb{Z}) = \{-1, 1\}$

Definición 1.0.7. Un anillo R con unitario se dice que es un anillo con división, si $U(R) = R - \{0\}$.

Definición 1.0.8. Un anillo R se dice que es un cuerpo, si es un anillo conmutativo con división.

Ejemplo 1.0.9. El conjunto de todos los polinomios con coeficientes en un cuerpo $\mathbb{F}$ denotado por $\mathbb{F}[X]$, junto con las operaciones suma y producto usual de polinomios, es un anillo conmutativo y

$$U(\mathbb{F}[X]) = \{f \in \mathbb{F}[X] : f(x) = k, k \in \mathbb{F}, k \neq 0\}.$$

1.0.1. Dominios

Definición 1.0.10. Sea a un elemento distinto de cero en un anillo R, se dice que a es divisor de cero si existe b distinto de cero en R tal que $a \cdot b = 0$ o $b \cdot a = 0$.

Definición 1.0.11. Un anillo R es llamado dominio entero si R es un anillo conmutativo con unidad y sin divisores de cero.

En algunos textos, R bajo estas condiciones es denominado dominio de integridad o dominio integral.

Para facilitar la comprensión del texto, se escribirá $a \cdot b$ como ab.

Definición 1.0.12. Sea R un anillo con unitario:

- Si $I \subseteq R$ es un subconjunto no vació de R, se dice que I es un ideal si:
  - Para todo $a, b \in I$, $a - b \in I$,
  - Dado $a \in I$ y $r \in R$, entonces $ra, ar \in I$.
- Sea $a \in R$, se define el ideal generado por a como $\langle a \rangle := \{ra : r \in R\}$.
- Si $I \subseteq R$ es un ideal de R, se dice que I es un ideal principal, si existe un elemento $a \in R$ tal que $I = \langle a \rangle$.
- Un dominio entero R es llamado dominio de ideales principales si todo ideal de R es principal.

Ejemplo 1.0.13. Los anillos $\mathbb{Z}$ y $\mathbb{F}[X]$ para cualquier cuerpo $\mathbb{F}$, son dominios de ideales principales.

Definición 1.0.14. Sea R un anillo e $I \subset R$ un ideal no nulo, sea $x \in R$, se define la clase lateral a izquierda como $x + I := \{x + i : i \in I\}$ y el conjunto $R/I := \{x + I : x \in R\}$ como el conjunto cociente.

Observación 1.0.15. Definiendo las operaciones $(x + I) + (y + I) = (x + y) + I$ y $(x + I) \cdot (y + I) = (x \cdot y) + I$ con $x, y \in R$, entonces R/I es un anillo y se conoce como el anillo cociente.

Se escribirá $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Definición 1.0.16. Un dominio entero R es llamado euclidiano si existe una función $d : R \to \mathbb{N}$ con las siguientes dos propiedades:

1. $0 \leq d(a) \leq d(ab)$ para todo a y b distintos de cero en R.
2. Para todo a y b en R con $b \neq 0$ es posible encontrar q y r en R tal que $a = bq + r$, $r = 0$ o $d(r) < d(b)$.

Se llamará la primera condición de la Definición 1.0.16 como la *d-desigualdad*, además, se denotará a R como (R, d) para hacer énfasis en que R es un dominio euclidiano bajo la función d.

Ejemplo 1.0.17. Los anillos:

1. $\mathbb{Z}$, junto con $d(n) = |n|$.
2. $\mathbb{Z}[i]$, $\alpha = a + bi \in \mathbb{Z}[i]$ y $d(\alpha) = N(\alpha) = a^2 + b^2$.

son dominios euclidianos.

El anillo $\mathbb{F}[X]$ junto con la función euclidea $d(f) = deg(f)$ (Grado del polinomio) es un dominio euclidiano, sin embargo, si $f(x) = 0$, su valor bajo la función euclidea $d(f(x)) = deg(0)$ no está definido, esto se debe a que $f(x)$ puede ser un polinomio de un grado arbitrario donde todos los coeficientes que acompañan la variable son 0. Lo anterior es una razón por la que no se asume que $d(0)$ esté definido en la Definición 1.0.16. El siguiente ejemplo es un dominio euclidiano donde $d(0)$ sí está definido.

Ejemplo 1.0.18. Todo cuerpo $\mathbb{F}$, con $d(a) = 1$ para todo $a \neq 0$ y $d(0) = 0$ es un dominio euclidiano.

La Definición 1.0.16 es usada en los textos más comunes de álgebra abstracta, sin embargo, en [1], en la sección $8{,}1$ se encuentra una definición diferente en la que falta la *d-desigualdad*.

Definición 1.0.19. Un dominio entero R es llamado euclidiano si existe una función $d : R \to \mathbb{N}$ tal que R tiene divisón con resto respecto a d, esto es, para a y b en R con $b \neq 0$ se puede encontrar q y r en R tal que:

$$a = bq + r,\ r = 0 \text{ o } d(r) < d(b). \tag{1.1}$$

Se permitirá $a = 0$ puesto que bajo esta definición se puede usar $q = 0$ y $r = 0$, además, una función $d : R \to \mathbb{N}$ que satisface (1.1) es llamada una función euclidea sobre R, por lo que, un dominio euclidiano bajo la Definición 1.0.19 es un dominio entero que admite una función euclidea, en este orden de ideas, un dominio euclidiano bajo la Definición 1.0.16 es un dominio entero que admite una función euclidea que satisface la *d-desigualdad*.

Por lo anterior, es natural preguntarse si ¿la Definición 1.0.19 describe una mayor clase de anillos que la Definición 1.0.16?, la respuesta es que no, acontinuación se mostrará que todo dominio euclidiano (R, d) bajo la Definición 1.0.19 puede ser equipado con una función euclidea diferente $\tilde{d}$, tal que $(R, \tilde{d})$ sea un dominio euclidiano bajo la Definición 1.0.16.

---

[1] DUMMIT, David y FOOTE, Richard. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

2. Perfeccionamiento de la función euclidea

Suponga que (R, d) es un dominio euclidiano bajo la Definición 1.0.19, se va a definir una nueva función euclidea $\tilde{d} : R \to \mathbb{N}$ a partir de d, tal que $\tilde{d}$ satisfaga $\tilde{d}(a) \leq \tilde{d}(ab)$, entonces $(R, \tilde{d})$ será un dominio euclidiano bajo la Definición 1.0.16.

Definición 2.0.1. Sea $a \in R$ con $a \neq 0$,

$$\tilde{d}(a) := \text{mín}\{d(ab) \in \mathbb{N} : b \in R, b \neq 0\}.$$

Es de resaltar que $ab \neq 0$ pues $b \neq 0$ y R es un dominio entero, además $a = a \cdot 1$, entonces:

$$\tilde{d}(a) \leq d(a), \tag{2.1}$$

para todo $a \in R$.

Observación 2.0.2. Para cada $a \neq 0$ en R, se tiene que $\tilde{d}(a) = d(ab_0)$ para algún b_0 en R, por lo que es claro que $d(ab_0) = \tilde{d}(a) \leq d(ab)$ para todo $b \in R$ distinto de cero.

Ejemplo 2.0.3. Sea $1 \in R$ el neutro de la operación binaria producto, entonces $\tilde{d}(1) = \text{mín}\{d(b) : b \neq 0\}$, es decir, $\tilde{d}(1)$ es el *d-valor* más pequeño en R.

Teorema 2.0.4. *Sea (R, d) un dominio euclidiano bajo la Definición 1.0.19, entonces $(R, \tilde{d})$ es un dominio euclidiano bajo la Definición 1.0.16.*

Demostración. Sean $a, b \in R$, distintos de cero, se desea ver que $\tilde{d}(a) \leq \tilde{d}(ab)$, por la Observación 2.0.2 $\tilde{d}(ab) = d(abc)$ para algún $c \in R$ distinto de cero, luego, por la Definición 2.0.1

$$\tilde{d}(a) \leq d(abc) = \tilde{d}(ab).$$

Ahora, se quiere probar que en R se cumple el algoritmo de la división respecto a $\tilde{d}$. Sean $a, b \in R$ con $b \neq 0$, entonces $\tilde{d}(b) = d(bc)$ para algún $c \in R$ con $c \neq 0$, por el algortimo de la divisón sobre a, bc en (R, d), existen $q_0, r_0 \in R$ tal que

$$a = (bc)q_0 + r_0, \ r_0 = 0 \text{ o } d(r_0) < d(bc),$$

considere $q = cq_0$ y $r = r_0$, entonces $a = bq + r$, ahora bien, si $r_0 = 0$, entonces $r = 0$, por otro lado, si $r_0 \neq 0$, como $\tilde{d}(b) = d(bc)$ y $\tilde{d}(r) \leq d(r)$ por (2.1), en consecuencia

$\tilde{d}(r) \leq d(r) \leq d(bc) = \tilde{d}(b)$, por tanto

$$a = bq + r,\ r = 0 \text{ o } \tilde{d}(r) \leq \tilde{d}(b).$$

□

Se denominará a los elementos q y r mostrados en las Definiciones 1.0.16 y 1.0.19, como cociente y residuo respectivamente.

El Ejemplo 1.0.17 ilustra que en $\mathbb{Z}$ es posible escribir $a = bq + r$ con $0 < r \leq |b|$, además q y r son únicos y son determiandos a partir de a y b, también hay unicidad del cociente y residuo en $\mathbb{F}[X]$ como se ve en [1], sección $9{,}2$ Teorema 3, el cociente y el residuo también son únicos en todo cuerpo $\mathbb{F}$.

Con lo anterior planteado, surge la pregunta ¿Existirán otros dominios euclidianos donde el cociente y el residuo son únicos?, note que en $\mathbb{Z}[i]$ el cociente y el residuo no son únicos respecto a $d(\alpha) = N(\alpha)$.

Ejemplo 2.0.5. Sean $1 + 8i,\ 2 - 4i \in \mathbb{Z}[i]$ si dividimos $1 + 8i$ entre $2 - 4i$ obtendremos lo siguiente:

$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i \text{ y } 1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i,$$

donde ambos residuos cumplen que su norma sea 5, la cual es menor que $N(2-4i) = 20$.

El Teorema 2.0.7 permitirá dar respuesta a la pregunta anteriormente planteada, pero antes, considere el siguiente lema.

Lema 2.0.6. *Sea (R, d) un dominio euclidiano, las siguientes afirmaciones son equivalentes:*

1. *Para algún par de elementos $a,\ b \neq 0$ en R, existe un único par de elementos $q, r \in R$ tal que $a = bq + r$ con $r = 0$ o $d(r) < d(b)$.*
2. *$d(a + b) \leq \max\{d(a), d(b)\}$.*

Demostración. Note que 2 implica 1. En efecto, sean $a,\ b \neq 0$ en R, suponga que existen dos pares de elementos q_1, r_1 y q_2, r_2 en R con $q_1 \neq q_2$ y $r_1 \neq r_2$, tales que

$$a = bq_1 + r_1 \text{ con } d(r_1) < d(b),$$

$$a = bq_2 + r_2 \text{ con } d(r_2) < d(b).$$

Entonces

$$b(q_1 - q_2) = -(r_1 - r_2) \neq 0,$$

luego, por la *d-desigualdad*, $d(b) \leq d(r_1 - r_2)$, por tanto,

$$d(b) \leq d(-(r_1 - r_2)) = d(r_1 - r_2) \leq \text{máx}\{d(r_1), d(r_2)\} < d(b),$$

lo cual es una contradicción, entonces $q_1 = q_2$ y $r_1 = r_2$.

Ahora se muestra que 1 implica 2. Suponga que existe un par de elementos $a, b \in R$ tal que

$$d(a + b) > d(a) \text{ y } d(a + b) > d(b).$$

Entonces para los elementos $a^2 - b^2 + b$ y $a + b$ la unicidad del cociente y residuo falla, puesto que

$$a^2 - b^2 + b = (a + b)(a - b) + b \text{ con } d(b) < d(a + b),$$

$$a^2 - b^2 + b = (a + b)(a - b + 1) - a \text{ con } d(-a) < d(a + b).$$

Por el Ejemplo 3.0.2 se tiene que $d(-a) = d(a)$, por lo tanto, queda demostrado. □

Teorema 2.0.7. *Si R es un dominio euclidiano donde el cociente y el residuo son únicos, entonces R es un cuerpo o $R = \mathbb{F}[X]$ para el cuerpo $\mathbb{F}$.*

Demostración. Suponga que el cociente y el residuo son únicos, entonces se cumple la equivalencia del Lema 2.0.6. Defina el conjunto

$$\mathbb{K} := U(R) \cup \{0\}.$$

Para ver que $\mathbb{K}$ es un cuerpo, es suficiente probar que toda suma de unidades es una unidad, sean $u_1, u_2 \in \mathbb{K}$, distintos de cero, entonces $d(u_1 + u_2) \leq \text{máx}\{d(u_1), d(u_2)\} = d(1)$, por el Corolario 3.0.3 se tiene que si $d(a) = d(1)$ entonces a es una unidad, por tanto $u_1 + u_2$ es una unidad y $\mathbb{K}$ es un cuerpo.

Si $R = \mathbb{K}$, entonces R es un cuerpo, por otro lado, si $R \neq \mathbb{K}$, se desea ver que si dado $a \neq 0$ con $d(a)$ el menor *d-valor*, para todo $0 \neq b \in R$, existen $q_0, \cdots, q_k \in \mathbb{K}$ tal que

$$b = q_k a^k + \cdots + q_1 a + q_0, \ q_k \neq 0.$$

Entonces el mapeo $b \mapsto \sum q_j x^j$ es un isomorfismo.

Primero note que la sucesión $d(a^k)$, $k = 0, 1, 2, \cdots$ es estrictamente creciente puesto que $d(a^k) < d(a^k a)$ (a^k es divisor propio de a^{k+1}), si $b \neq 0$, se tiene que $d(a^k) \leq d(b) < d(a^{k+1})$ para algún $k \geq 0$. Entonces $b = q_k a^k + r$ con $r = 0$ o $d(r) < d(a_k)$ (Como $d(a)$ es el menor *d-valor*, esto obliga a r a ser una unidad), note que $q_k \neq 0$, además si q_k no es unidad, se puede encontrar $m \in \mathbb{K}$ y $l \neq 0$ tales que $q_k = la + m$, por el Lema 2.0.6 se tiene que $d(b) \geq d(b - ma^k - r) = d(la^k) \geq d(a^{k+1})$ lo cual contradice la escogencia del b.

Si $r \neq 0$, se aplica nuevamente este argumento y por inducción se tiene que

$$b = \sum_{j=0}^{k} q_j a^j, \ q_j \in \mathbb{K}. \tag{2.2}$$

Finalmente, suponga que existe j talque $q_j \neq 0$ y sea $s = \min\{j : q_j \neq 0\}$, de

$$\sum_{j=0}^{k} q_j a^j = 0,$$

se tiene que

$$\sum_{j=s}^{k} q_j a^j = 0.$$

Expandiendo se obtiene la expresión $q_s a^s + q_{s+1} a^{s+1} + \cdots + q_k a^k = 0$, y multiplicando por a_s^{-1} a ambos lados de la igualdad y despejando q_s se tiene

$$-q_s = q_{s+1} a + \cdots + q_k a^{k-s},$$

de ahí, factorizando un a se escribe como:

$$-q_s = a(q_{s+1} + \cdots + q_k a^{k-s-1}).$$

Sea $y := q_{s+1} + \cdots + q_k a^{k-s-1}$, entonces por la *d-desigualdad* $d(a) \leq d(ay) = d(-q_s) = d(q_s) = d(1)$, lo cual contradice la escogencia del a, luego cada $q_j = 0$ y en consecuencia, la representación (3) es única. □

¿Por qué el anillo $\mathbb{Z}$ no aparece en el Teorema 2.0.7? resulta interesante, sin embargo es cierto, puesto que, el cociente y residuo en $\mathbb{Z}$ son únicos tomando $0 \leq r \leq |b|$, pero no en $\mathbb{Z}$ como dominio euclidiano, es decir, si $|r| \leq |b|$, entonces el cociente y el residuo no son

únicos.

Ejemplo 2.0.8. Considere $51/6$ en $\mathbb{Z}$, entonces $51 = 6 \cdot 8 + 3$ y $51 = 6 \cdot 9 - 3$.

Observación 2.0.9. Se dice que una función euclidea d es multiplicativa si satisface una propiedad aún más fuerte que la *d-desigualdad*, es decir, satisface que $d(ab) = d(a)d(b)$ con $d(a) \geq 1$, y donde $a \neq 0$.

Ejemplo 2.0.10. Los dominios euclidianos $(\mathbb{Z}, |n|)$, $(\mathbb{Z}[i], N(\alpha))$ tienen funciones euclideas multiplicativas. Sean $a, b \in \mathbb{Z}$, note que $a^2 = |a|^2$, entonces $a^2 = (-a)^2$, luego $|ab|^2 = (ab)^2 = a^2b^2 = |a|^2|b|^2 = (|a||b|)^2$, como $|ab|$ es positivo, entonces $|ab| = |a||b|$. Ahora, sean $\alpha = a + bi$ y $\beta = c + di$ en $\mathbb{Z}[i]$, entonces $N(\alpha\beta) = N((ac - bd) + (ad + bc)i) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)$.

En el dominio euclidiano $\mathbb{F}[X]$ la función euclidea $d(f) = deg(f)$ no es multiplicativa, dados $a(x), b(x) \in \mathbb{F}[X]$ distintos de la función nula, se tiene que

$$deg(a(x)b(x)) = deg(a(x)) + deg(b(x)),$$

si considera $d(f) = 2^{deg(f)}$, entonces $(\mathbb{F}[X], 2^{def(f)})$ es un dominio euclidiano cuya función euclidea es multiplicativa.

3. Algunas propiedades de la *d-desigualdad*

Sea (R, d) un dominio euclidiano, por el Teorema 2.0.4, se asume que d satisface la *d-desigualdad*, por lo cual, es posible probar las siguientes propiedades de d.

Teorema 3.0.1. *Sea (R, d) un dominio euclidiano, donde d satisface la d-desigualdad. Entonces:*

1. $d(a) \geq 1$*, para todo $a \in R$ distinto de cero.*
2. *Si $b \in U(R)$, entonces $d(ab) = d(a)$ para todo $a \in R$ distinto de cero.*
3. *Si $b \notin U(R)$ y $b \neq 0$, entonces $d(ab) > d(a)$, para todo $a \in R$ distinto de cero.*

Demostración. 1. Por la *d-desigualdad*, $d(1) \leq d(1 \cdot a) = d(a)$.

2. Por la *d-desigualdad*, $d(a) \leq d(ab)$; por otro lado, sea $c \in R$ el inverso de b, entonces la *d-desigualdad* implica
$$d(ab) \leq d((ab)c) = d(a).$$

3. Suponga que $d(a) = d(ab)$, usando el algoritmo de la divisón sobre a por ab tenemos que existen $q, r \in R$ tal que
$$a = (ab)q + r,\ r = 0 \text{ o } d(r) < d(ab).$$
Entonces
$$a(1 - bq) = r,\ r = 0 \text{ o } d(r) < d(a).$$
Como b no es invertible, entonces $1 - bq \neq 0$, luego $a(1 - bq) \neq 0$, además, si $r \neq 0$, la desigualdad $d(r) < d(a)$ implica
$$d(a(1 - bq)) < d(a),$$
lo cual contradice la *d-desigualdad*, que dice $d(a) \leq d(a(1 - bq))$.

□

Ejemplo 3.0.2. Sea $a \in R$, entonces $d(-a) = d(a)$, en efecto, como -1 es una unidad en R, por el item 2 del Teorema 3.0.1 $d(-a) = d((-a)(-1)) = d(a)$.

Corolario 3.0.3. *Sea (R, d) un dominio euclidiano donde d satisface la d-desigualdad, entonces $d(a) = d(1)$, sí y solo sí $a \in U(R)$, es decir, los elementos con el menor d-valor en R, son precisamente las unidades.*

Demostración. Considere $a = 1$ en los items 2 y 3 del Teorema 3.0.1. □

Ejemplo 3.0.4. Considere los siguientes dominios euclidianos:

- En $(\mathbb{Z}, |n|)$, los enteros que satisfacen que $|n| = |1|$ son $n = \pm 1$.
- En $(\mathbb{F}[X], deg(f))$, los polinomios $f \in \mathbb{F}[X]$ los cuales satisfacen que $deg(f) = deg(1) = 0$ son exactamente los polinomios constantes distintos de cero.

Corolario 3.0.5. *Sea (R, d) un dominio euclidiano donde d satisface la d-desigualdad, si a y b no son unidades, entonces $d(a)$ y $d(b)$ son ambos menores que $d(ab)$.*

Demostración. Es inmediato del item 3 del Teorema 3.0.1, puesto que si a y b no son invertibles, entonces ambos satisfacen el item 3. □

4. Factorización en Irreducibles

Una de las propiedades más importantes de los dominios euclidianos es que en ellos todo ideal es principal, es decir, todo dominio euclidiano es un dominio de ideales principales (*DIP*), algunos teoremas de *DIP* son más sencillos de probar en dominios euclidianos, a continuación se muestran dos teoremas sumamente importantes en dominios.

Definición 4.0.1. Sea R un dominio entero, un elemento $a \in R$ distinto de cero es llamado *irreducible* si no es una unidad y en cada factorización $a = bc$, alguno de los factores b o c es una unidad. Una no unidad no nula que no es irreducible se llama reducible.

Hay tres tipos de elementos distintos de cero en un dominio entero: unidades (los elementos invertibles, cuyos factores son siempre también unidades), irreducibles (no unidades cuyas factorizaciones en dos partes implican siempre un factor unidad) y reducibles (no unidades que admiten alguna factorización en un producto de dos no unidades). Note que en un cuerpo no hay elementos reducibles o irreducibles: todo es cero o una unidad. Así que si se quiere demostrar un teorema sobre la factorización irreducible, se evitan los cuerpos.

Teorema 4.0.2. *En un dominio euclidiano que no es un cuerpo, todo elemento no nulo es producto de irreducibles.*

Demostración. Sea (R, d) un dominio euclidiano que no es cuerpo. Por el Teorema 2.0.4 es posible asumir que $d(a) \leq d(ab)$ para todo a, b distintos de cero en R. Por lo tanto, se puede usar el Colorario 3.0.5, además, se demostrará la existencia de factorización irreducible por inducción sobre el *d-valor*.

Por el Colorario 3.0.3, las unidades de R tienen el menor *d-valor*. Sea $a \in R$ con el segundo menor *d-valor*, se desea ver que a es irreducible. Suponga que a no es irreducible, entonces $a = bc$, donde b y c no son unidades, luego $d(b)$ y $d(c)$ son ambos menores que $d(a)$ por el Colorario 3.0.5. es decir, b y c deben ser unidades, luego a es una unidad, lo cual es una contradicción, puesto que a tiene el segundo menor *d-valor*.

Suponga ahora que $a \notin U(R)$ y que todas las no unidades con el menor *d-valor* admiten una factorización irreducible. Para probar que a admite una factorización irreducible, se supone que a no es irreducible, esto es, $a = bc$ donde b y c son no unidades, luego, por el Colorario 3.0.5 $d(b) < d(a)$ y $d(c) < d(a)$, entonces por hipótesis b y c admiten una factorzación irreducible, por lo tanto su producto a tiene una factorización irreducible. □

Note que en el siguiente teorema, la conclusión del Teorema 4.0.2 es cierta para *DIPs*, pero para probarlo, se necesitará del siguiente lema.

Lema 4.0.3. *Si R es un dominio entero y $0 \neq a \in R$ es una no unidad que no admite factorización en irreducibles entonces existe una inclusión estricta de ideales principales $\langle a \rangle \subset \langle b \rangle$, donde $0 \neq b$ es alguna otra no unidad que no admite factorización en irreducibles.*

Demostración. Por hipótesis a no es irreducible, por lo que existe alguna factorización $a = bc$ donde b y c no son unidades. Sí b y c admiten una factorización irreducible, entonces también a, en consecuencia, al menos alguno de los dos no tiene factorización irreducible, sin pérdida de generalidad, suponga que b no tiene factorización irreducible. Como c no es una unidad, la inclusión $\langle a \rangle \subset \langle b \rangle$ es estricta. □

Teorema 4.0.4. *En un DIP que no es un cuerpo, toda no unidad no nula es producto de irreducibles.*

Demostración. Suponga que hay un elemento a en el *DIP* que no es 0 ni una unidad y no tiene una factorización irreducible. Entonces, por el Lema 4.0.3, existe una inclusión estricta

$$\langle a \rangle \subset \langle a_1 \rangle,$$

donde a_1 no tiene factorización irreducible, del mismo modo, por el Lema 4.0.3, existe una inclusión estricta

$$\langle a_1 \rangle \subset \langle a_2 \rangle,$$

donde a_2 no tiene factorización irreducible. Este argumento (Aplicando inductivamente el Lema 4.0.3 al generador del siguiente ideal principal mayor) nos lleva a una cadena creciente infinita de ideales principales

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \cdots,$$

donde todas las inclusiones son estrictas, lo cual no es posible en un *DIP*.

En efecto, suponga que un *DIP* contiene una cadena infinita creciente de ideales:

$$I_0 \subset I_1 \subset I_2 \subset I_3 \cdots.$$

Definiendo

$$I = \bigcup_{n \geq 0} I_n,$$

se tiene que I es un ideal, debido a que los I_n son estrictamente crecientes, luego, cada conjunto finito de elementos de I se encuentra en un I_n común. Por lo tanto, I es cerrado bajo adición y multiplicaciones arbitrarias desde el anillo, ya que cada I_n es un ideal. Como se está en un *DIP*, I es un ideal principal, es decir, $I = \langle r \rangle$ para algún r en el anillo, ahora bien, como I es la unión de los I_n, r debe estar en algún I_N. Entonces, $\langle r \rangle \subset I_N$, puesto que I_N es un ideal, por ende

$$I = \langle r \rangle \subset I_N \subset I,$$

lo que significa

$$I = I_N,$$

pero esto es imposible, porque la inclusión $I_{N+1} \subset I$ se convierte en $I_{N+1} \subset I_N$ y se asumió que I_N es un subconjunto propio de I_{N+1}. Debido a esta contradicción, las no unidades no nulas en un *DIP* sin factorización irreducible, no existen. □

Observación 4.0.5. Note que la prueba del Teorema 4.0.4 en la dirección contrarecíproca, en un dominio entero que contenga una no unidad no nula a sin una factorización irreducible, debe haber un ideal no principal y de hecho tal ideal es $I := \bigcup_{n\geq 0}\langle a \rangle$, donde $a_0 = a$, a_n para $n \geq 1$ es un factor de a_{n-1} que no es una unidad o un múltiplo unitario de a_{n-1}, y a_n tiene factorización irreducible. La razón por la que I no puede ser principal es porque la prueba muestra que si I es principal entonces se llega a una contradicción con que a no tenga una factorización irreducible.

La prueba del Teorema 4.0.4 de que un *DIP* no contiene una cadena infinita de ideales estrictamente creciente es cierta para una clase de anillos más grande que los *DIP*.

Observación 4.0.6. Cuando existe un conjunto finito de elementos $X = \{x_1, x_2, \cdots, x_n\}$ en R e $I = \langle x_1, x_2, \cdots x_n \rangle := \{r_1x_1 + \cdots + r_nx_n : r_i \in R \text{ y } x_i \in X, \forall i \in \{1, \cdots, n\}, n \in \mathbb{N}\}$, se dice que I es un ideal finitamente generado. Si $I = \langle x_0 \rangle$, se está bajo la definición usual de ideal principal.

Teorema 4.0.7. *Un anillo conmutativo en el que cada ideal está finitamente generado no contiene una cadena infinita estrictamente creciente de ideales.*

Demostración. Note que la segunda parte de la demostración del Teorema 4.0.4 funciona en este contexto más general, luego, solo faltaría ver lo que pasa cuando un ideal I es finitamente generado, en vez de principal.

Si $I = \langle x_1, x_2, \cdots, x_m \rangle$, todos los $x_i's$ finitos están en algún I_N común (porque los I_N es una cadena creciente), por lo que, la contradicción se obtiene de la misma forma que en el Teorema 4.0.4, es decir: $I = I_N$, entonces $I_{N+1} \subset I_N$. □

Corolario 4.0.8. *En un dominio entero donde todo ideal es finitamente generado, toda no unidad no nula tiene una factorización irreducible.*

Demostración. Si existiera un elemento a que no es 0 o una unidad y que no admitiera una factorización irreducible entonces, de manera análoga a la prueba del Teorema 4.0.4, se podría producir una cadena infinita estrictamente creciente de ideales (principales). Pero no hay cadenas infinitas estrictamente crecientes de ideales en el anillo, por el Teorema 4.0.7. □

Observación 4.0.9. Un anillo conmutativo donde todo ideal es finitamente generado es llamado *Anillo Noetheriano*.

Ejemplo 4.0.10. Algunos anillos Noetherianos son:

- Los *DIP*.
- Los cuerpos.
- El anillo de polinomios $R[X]$ con R un anillo Noetheriano.

5. Anillos cuadráticos euclidianos y no euclidianos

La importancia de los dominios euclidianos es poder dar ejemplos de *DIP's*, sin embargo, los anillos más sencillos que pueden ser *DIP's* y no euclidianos se encuentran entre los anillos cuadráticos, esta sección contiene la teoría relevante sobre anillos cuadráticos, con el fin de concretar ejemplos claves de anillos cuadráticos que son euclidianos y no euclidianos.

Definición 5.0.1. Un *anillo cuadrático* es un anillo de la forma $\mathbb{Z}[\gamma] := \{a + b\gamma : a, b \in \mathbb{Z}\}$ donde γ es un número complejo el cual es raíz de un polinomio cuadrático irreducible $x^2 + cx + d \in \mathbb{Z}[X]$ con coeficiente principal 1. Se dirá que $\mathbb{Z}[\gamma]$ es *real* si γ es real e *imaginario* en el otro caso.

Ejemplo 5.0.2. Algunos anillos cuadráticos conocidos son:

- Los enteros Gaussianos $\mathbb{Z}[i]$ son un anillo cuadrático imaginario asociado al polinomio $x^2 + 1$.
- Cuando $m \in \mathbb{Z}$ no es un cuadrado perfecto, $\mathbb{Z}[\sqrt{m}]$ es cuadrático real siempre que $m > 0$ y cuadrático imaginario si $m < 0$.
- El anillo $\mathbb{Z}[(1 + \sqrt{5})/2]$ es cuadrático real, esto pues $(1 + \sqrt{5})/2$ es raíz de $x^2 - x - 1$.

5.0.1. Propiedades de algunos anillos cuadráticos Una propiedad fuerte de los anillos cuadráticos es la Propiedad 5.0.8, para comprenderla, primero se debe emplear algunos conceptos de homomorfismos.

Definición 5.0.3. Sean R, R' anillos y $f : R \to R'$ una función, se dirá que f es un homomorfismo de anillos si éste preserva operaciones, es decir, $f(a +_R b) = f(a) +_{R'} f(b)$ y $f(a \cdot_R b) = f(a) \cdot_{R'} f(b)$.

Observación 5.0.4. Si f es inyectiva, se dice que f es un monomorfismo, por otro lado, si f es sobreyectiva, entonces f es un epimorfismo, además, si f es biyectiva, se obtiene que f es un isomorfismo (en algunos textos denotan esto último como $R \cong R'$, haciendo alusión a que existe una función $f : R \to R'$ la cual es un isomorfismo).

Definición 5.0.5. Sea $f : R \to R'$ un homomorfismo de anillos, dos conjuntos especiales son *Ker*(f) e *Im*(f) los cuales se definen por:

$$\textit{Ker}(f) := \{x \in R : f(x) = 0_{R'}\},$$

$$\textit{Im}(f) := \{y \in R' : \exists x \in R \text{ tal que } y = f(x)\}.$$

Proposición 5.0.6. *Sea $f : R \to R'$ un homomorfismo de anillos, entonces:*

1. *Im(f) es subanillo de R'.*
2. *Ker(f) es un ideal de R.*

Demostración. 1. Sean $y_1, y_2 \in$ *Im*(f), entonces $y_1 = f(r_1)$ y $y_2 = f(r_2)$, para algunos $r_1, r_2 \in R$, luego, $f(r_1 - r_2) = y_1 - y_2$ y $f(r_1 r_2) = y_1 y_2$, es decir, $y_1 - y_2 \in$ *Im*(f) y $y_1 y_2 \in$ *Im*(f), por tanto *Im*(f) es subanillo de R'.

2. Sean $a, b \in$ *Ker*(f), entonces $f(a) = f(b) = 0$, luego $f(a-b) = 0$, es decir, $a-b \in$ *Ker*(f), por otro lado, sea $r \in R$, entonces $f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$, del mismo modo $f(ar) = 0$, es decir $ra, ar \in$ *Ker*(f), por tanto *Ker*(f) es ideal de R. □

El siguiente teorema permitirá demostrar la Proposición 5.0.8.

Teorema 5.0.7 (Primer Teorema de Isomorfismos)**.** *Sea $f : R \to S$ un homomorfismo de anillos, entonces $R/$Ker$(f) \cong$ Im(f).*

Demostración. Ver [1], página 243. □

Proposición 5.0.8. *Sea $\mathbb{Z}[\gamma]$ un anillo cuadrático con γ raíz del polinomio mónico irreducible x^2+cx+d en $\mathbb{Z}[X]$, entonces $\mathbb{Z}[\gamma]$ es isomoformo al cociente $\mathbb{Z}[X]/\langle x^2+cx+d\rangle$.*

Demostración. Considere la función $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\gamma]$, definida por $p(x) \mapsto \phi(p(x)) = p(\gamma)$, primero se verá que ϕ es un homomorfismo.

Sean $p(x), q(x) \in \mathbb{Z}[X]$, entonces

$$\phi(p(x) + q(x)) = \phi((p+q)(x)) = (p+q)(\gamma) = p(\gamma) + q(\gamma) = \phi(p(x)) + \phi(q(x)),$$

y

$$\phi(p(x)q(x)) = \phi((pq)(x)) = (pq)(\gamma) = p(\gamma)q(\gamma) = \phi(p(x))\phi(q(x)).$$

Además, dado $\alpha \in \mathbb{Z}[\gamma]$, entonces $\alpha = a + b\gamma = \phi(a + bx)$, luego ϕ es un epimorfismo, por tanto *Im*$(\phi) = \mathbb{Z}[\gamma]$. Ahora bien, *ker*$(\phi) = \langle x^2 + cx + d\rangle$. En efecto,

$$\textit{ker}(\phi) = \{p(x) \in \mathbb{Z}[X] : \phi(p(x)) = 0\},$$

$$\textit{ker}(\phi) = \{p(x) \in \mathbb{Z}[X] : p(\gamma) = 0\},$$

$$\textit{ker}(\phi) = \{p(x) \in \mathbb{Z}[X] : p(x) = (x^2 + cx + d)q(x) \text{ con } q(x) \in \mathbb{Z}[X]\},$$

$$\textit{ker}(\phi) = \{(x^2 + cx + d)q(x) : q(x) \in \mathbb{Z}[X]\},$$

$$\textit{ker}(\phi) = \langle x^2 + cx + d\rangle.$$

Por lo tanto, por el Teorema 5.0.7 se tiene que $\mathbb{Z}[X]/\langle x^2 + cx + d\rangle \cong \mathbb{Z}[\gamma]$. □

Definición 5.0.9 (Conjugado)**.** Si γ es una raíz de $x^2 + cx + d$, la segunda raíz es llamado el conjugado de γ y se define como $\overline{\gamma} := -c - \gamma$.

Además $\overline{\overline{\alpha}} = \alpha$, en especial si $c = 0$ y $d = -m$, entonces γ es raíz de $x^2 - m$, luego $\gamma = \pm\sqrt{m}$, entonces $\overline{\gamma} = -\gamma$ y $\overline{a + b\gamma} = a - b\gamma$.

Ejemplo 5.0.10. Algunos ejemplos de conjugados son:

- Si $\alpha = a + b\gamma \in \mathbb{Z}[\gamma]$, entonces $\overline{\alpha} = a + b\overline{\gamma} = a - cb - b\gamma$.
- Si $\gamma = \sqrt{2}$, entonces $\overline{a + b\sqrt{2}} = a - b\sqrt{2}$.
- Si $\gamma = (1 + \sqrt{5})/2$ raíz de $x^2 - x - 1$, entonces $\overline{a + b(1 + \sqrt{5})/2} = a + b(1 - \sqrt{5})/2$.

Definición 5.0.11 (Norma)**.** Sea $\alpha = a + b\gamma \in \mathbb{Z}[\gamma]$ con γ raíz de $x^2 + cx + d$, se define la norma de α como

$$N(\alpha) := \alpha\overline{\alpha} = a^2 - cab + db^2.$$

Este número es un entero y es cero si $\alpha = 0$. Para todo $m \in \mathbb{Z}$, se tiene que $N(m) = m^2$, en particular $N(\pm 1) = 1$. Cuando $\gamma = \sqrt{m}$, se obtiene que

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Se resalta el hecho de que la norma no necesariamente es positiva.

Ejemplo 5.0.12. Algunos ejemplos donde la norma no necesariamente es positiva son:

- Si $\gamma = \sqrt{2}$, entonces $N(a + b\sqrt{2}) = a^2 - 2b^2$ tiene valores positivos y negativos.

- Si $\gamma = (1+\sqrt{5})/2$, una raíz de $x^2 - x - 1$, entonces $N(a+b\gamma) = a^2 + ab - b^2 = (a + b/2) - 5b^2/4$ tiene valores positivos y negativos.
- Si $\gamma = \sqrt{-5}$, una raíz de $x^2 + 5$, entonces $N(a+b\gamma) = a^2 + 5b^2$ no tiene valores negativos.
- Si $\gamma = \sqrt{m}$, para algún $m \in \mathbb{Z}$, entonces $N(a+b\gamma) = a^2 - mb^2$ tiene valores positivos si $m < 0$ y negativos si $m > 0$.

Una propiedad interesante que satisface la norma es la siguiente.

Proposición 5.0.13. *La norma en la Definición 5.0.11 es multiplicativa, esto es, dados* $\alpha, \beta \in \mathbb{Z}[\gamma]$*, entonces* $N(\alpha\beta) = N(\alpha)N(\beta)$*.*

Demostración. Sean $\alpha, \beta \in \mathbb{Z}[\gamma]$, entonces

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta).$$

□

Varios anillos cuadráticos son dominios euclidianos con el valor absoluto de la *Norma* como función euclidea. En particular, $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-2}]$, son dominios euclidianos usando $d(\alpha) = |N(\alpha)|$.

Esto nos conduce a formular dos preguntas sobre los anillos cuadráticos ¿Son dominios euclidianos respecto a alguna función euclidea? o ¿Son dominios euclidianos con una función euclidea $d(\alpha) = |N(\alpha)|$? lo anterior se conoce como dominio euclideano normado.

5.0.2. El anillo cuadrático $\mathbb{Z}[\sqrt{14}]$ Existen anillos cuadráticos que son dominios euclidianos y que su función euclidea es $d(\alpha) = |N(\alpha)|$, también puede que exista una función euclídea en el anillo aunque el valor absoluto de la norma no sea una función euclídea. El primer ejemplo de esto fue dado en [2], se prueba que $\mathbb{Z}[(1+\sqrt{69})/2]$ es un dominio euclidiano y no un dominio euclidiano normado, un segundo ejemplo fue dado en [3], donde se prueba que $\mathbb{Z}[\sqrt{14}]$ es un dominio euclidiano, más no euclidiano normado, a continuación veremos la prueba de esto.

---

[2] David CLARK. "A quadratic field which is Euclidean but not norm-Euclidean". En: *manuscripta mathematica* 83.1 (1994), págs. 327-330.

[3] Malcolm HARPER. "$\mathbb{Z}[\sqrt{14}]$ is Euclidean". En: *Canadian Journal of Mathematics* 56.1 (2004), págs. 55-70.

Teorema 5.0.14. *El anillo $\mathbb{Z}[\sqrt{14}]$ no es un dominio euclidiano normado.*

Demostración. La idea principal de la demostración es probar que una ecuación específica no puede resolverse en $\mathbb{Z}[\sqrt{14}]$, suponga que $\mathbb{Z}[\sqrt{14}]$ es un dominio euclidiano normado cuya función euclidea es $d(\alpha) = |N(\alpha)| = |x^2 - 14y^2|$ con $\alpha = x + y\sqrt{14}$.

Considere la ecuación $1 + \sqrt{14} = 2\gamma + \rho$, donde $|N(\rho)| < |N(2)| = 4$. Suponga que posee una solución de la forma $\gamma = m + n\sqrt{14}$ y $\rho = a + b\sqrt{14}$ en $\mathbb{Z}[\sqrt{14}]$, entonces

$$1 + \sqrt{14} = (2m + a) + (2n + b)\sqrt{14},$$

de ahí que $a = 1 - 2m$, $b = 1 - 2n$, lo que significa que

$$|N((1 - 2m) + (1 - 2n)\sqrt{14})| < 4,$$

entonces

$$(2m - 1)^2 - 14(2n - 1)^2 = 0, \pm 1, \pm 2, \pm 3.$$

Note que el lado izquierdo es impar, así que el derecho debe ser ± 1 ó ± 3. Dado que $k^2 \equiv 1(\mod 8)$ con k impar, entonces

$$(2m - 1)^2 - 14(2n - 1)^2 \equiv 1 - 14 \equiv 3(\mod 8),$$

además la única opción posible sería 3 puesto que ± 1 y -3 no son congruentes con 3 módulo 8, entonces

$$(2m - 1)^2 - 14(2n - 1)^2 = 3.$$

Reduciendo esto módulo 7, se obtiene $3 \equiv (2m - 1)^2(\mod 7)$, lo cual es falso, puesto que 3 no es residuo cuadrático $(\mod 7)$. Se tiene una contradicción. □

La anterior prueba se hace con el fin de contradecir el *Criterio de Euler* el cual dice que un elemento a es un residuo cuadrático $\mod p$ con p primo sí, y solo sí, $a^{\frac{p-1}{2}} \equiv 1(\mod p)$, para el caso de la demostración anterior $3^{\frac{7-1}{2}} = 3^3 = 27 \equiv -1(\mod 7)$.

La función dada en `https://math.stackexchange.com/questions/1148364` nos permite verificar que $\mathbb{Z}[\sqrt{14}]$ junto con esa función, es un dominio euclidiano.

En [3] Teorema 5, se da una condición suficiente (en términos de dos primos admisibles) para que un anillo cuadrático que es un *DIP* sea un dominio euclidiano, ejemplo de esto $\mathbb{Z}[\sqrt{14}]$.

5.0.3. Características de los *DIP's* y los dominios euclidianos Es claro que para poder demostrar que un dominio entero no es un *DIP*, basta con dar la cara explícita de un ideal del dominio que no sea principal, sin embargo, esto puede llegar a ser difícil, por consiguiente, se debe usar otro método; uno un poco más intuitivo es mostrar que ese dominio entero no tiene alguna propiedad que si tienen los *DIP's*, la descripción de esta propiedad es una generalización del teorema de las raíces racionales en $\mathbb{Z}[X]$ que dice que una raíz racional de un polinomio mónico en $\mathbb{Z}[X]$ es un número entero.

La generalización se basa en el siguiente lema, el cual afirma que los coeficientes de un *DIP* tienen una forma reducida, como los números racionales, para ello primero se definirá un cuerpo de fracciones.

Definición 5.0.15. Sea R un dominio entero, se dice que $\mathbb{K}$ es un cuerpo de fracciones de R, si éste es el menor cuerpo que contiene a R.

Este cuerpo $\mathbb{K}$ siempre existe y se construye como se ve en [4], página 176, éste cumple algunas propiedades que permiten mayor comprensión de los siguientes teoremas.

Ejemplo 5.0.16. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Antes de continuar, se debe dar varias definiciones clave para una mejor comprensión algunos teoremas que se encontrarán en esta sección.

Definición 5.0.17 (Divisor)**.** Sea $a \in R$, se dice que $c \in R$ es un divisor de a, si $a = kc$ con $k \in R$ y se denota como $c \mid a$.

Observación 5.0.18*.* Note que $c \mid a$ en un anillo R sí, y solo sí, $a \in \langle c \rangle$ sí, y solo sí $\langle a \rangle \subseteq \langle c \rangle$, en partícular, si d es un divisor común entre a y b, entonces $a, b \in \langle d \rangle$ y $\langle a \rangle, \langle b \rangle \subseteq \langle d \rangle$.

Definición 5.0.19 (Asociados)**.** Sean $a, b \in R$, se dice que a y b son asociados si existe $u \in U(R)$ tal que $a = bu$.

Observación 5.0.20*.* Si R es un dominio entero y $a \in R$, las unidades de R y los asociados con a se denominan divisores triviales de a.

Definición 5.0.21 (Máximo común divisor)**.** Sean $a, b \in R$, se dice que $d \in R$ es el máximo común divisor de a y b si:

---

[4] Allan CLARK. *Elements of abstract algebra*. Courier Corporation, 1984.

- $d \mid a$ y $d \mid b$.
- Si existe $c \in R$ tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Si d es un elemento de R que satisface las propiedades de la Definición 5.0.21, se denotará por $d = m.c.d(a, b)$, la Definición 5.0.21 también puede ser representada mediante ideales teniendo en cuenta la Observación 5.0.18.

Definición 5.0.22. Sea R un dominio entero, sean $a, b \in R$ e $I = \langle a, b \rangle$, entonces $d = m.c.d(a, b)$ si:

- $I \subseteq \langle d \rangle$.
- Si $\langle d' \rangle$ es un ideal principal de I, entonces $\langle d' \rangle \subseteq \langle d \rangle$.

De esta definición nace una condición suficiente sobre la existencia del máximo común divisor, si $\langle a, b \rangle = \langle d \rangle$, entonces $d = m.c.d(a, b)$.

Proposición 5.0.23. *Sea R un dominio entero, si dos elementos $d, d' \in R$ generan el mismo ideal principal, es decir $\langle d \rangle = \langle d' \rangle$, entonces d y d' son asociados, esto es, existe $u \in U(R)$ tal que $d' = du$.*

Demostración. La conclusión es clara si $d = d' = 0$, suponga que $d, d' \neq 0$, como $\langle d \rangle = \langle d' \rangle$, entonces $d \in \langle d' \rangle$, luego existe $x \in R$ tal que $d = xd'$, del mismo modo $d' \in \langle d \rangle$, luego existe un $y \in R$ tal que $d' = yd$, de ahí que $d = xyd$, por tanto $d(1 - xy) = 0$, como R es un dominio entero y $d \neq 0$, entonces $xy = 1$ por lo tanto, $x, y \in U(R)$. □

En partícular, si $d = m.c.d(a, b)$ y $d' = m.c.d(a, b)$, entonces $d' = du$, para algún $u \in U(R)$.

Ejemplo 5.0.24. Considere el dominio entero $\mathbb{Z}$ y los elementos $6, 15$. Es claro que $3 = m.c.d(6, 15)$, de igual forma $-3 = m.c.d(6, 15)$, por la proposición anterior, 3 y -3 deberían ser asociados, y en efecto lo son, note que $-3 = (-1) \cdot 3$ y $-1 \in U(\mathbb{Z})$.

Observación 5.0.25. La Proposición 5.0.23 y el Ejemplo 5.0.24 especifican y dan a entender que el máximo común divisor no es único, sin embargo, por abuso de notación hablaremos de *el* máximo común divisor pero siempre teniendo en cuenta que este no es único.

Definición 5.0.26 (Primos relativos)**.** Sean $a, b \in R$, se dice que a y b son primos relativos, si su máximo común divisor es $d = \pm 1$.

Lema 5.0.27 (Lema de Bezout)**.** *Sean R un dominio euclidiano y $a, b \in R$, entonces existe $d \in R$ tal que d es el máximo común divisor de a y b, además existen $u, v \in R$ tales que $d = au + bv$.*

Demostración. Sean $a, b \in R$, suponga que $d(b) \leq d(a)$, es decir, $a = bq_1 + r_1$ con $d(r_1) < d(b)$, realizando esto mismo una cantidad finita de veces hasta encontrar un residuo cero, se obtiene

$$b = r_1q_2 + r_2 \text{ con } d(r_2) < d(r_1),$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \text{ con } d(r_n) < d(r_{n-1}),$$

$$r_{n-1} = r_nq_n \text{ con } r_{n+1} = 0.$$

Esto se debe a que $d(b) > d(r_1) > d(r_2) > \cdots$ es una sucesión estrictamente decreciente de números naturales. Note que r_1 es de la forma $ax + by$ con $x, y \in R$ y, por inducción se verifica para todo r_i, sean $r_i = ax' + by'$ y $r_{i-1} = ax'' + by''$, entonces

$$r_i = -r_{i-1}q_i + r_{i-2} = a(x' - x''q_i) + b(y' - y''q_i),$$

en particular $r_n = au + bv$. Además r_n divide a r_n y r_{n-1}, luego divide a r_{n-2}. Por inducción se obtiene que r_n divide a a y b, además, como $r_n = au + bv$, cualquier divisor de a y b divide a r_n. Luego $d = r_n = m.c.d(a, b)$. □

Para demostrar el Teorema 5.0.29, se debe tener en cuenta el siguiente lema.

Lema 5.0.28. *Sea R un DIP y $\mathbb{K}$ su cuerpo de fracciones. Cada elemento de $\mathbb{K}$ es cociente de dos primos relativos de R.*

Demostración. Sea $\frac{a}{b} \in \mathbb{K}$, donde $a, b \in R$ con $b \neq 0$, por el Lema 5.0.27 existe $d \in R$ tal que $d = m.c.d(a, b)$. Removiendo ese factor común de a y b el cociente $\frac{a}{b}$ será un cociente irreducible.

Como $d = m.c.d(a, b)$ se tiene que $d|a$ y $d|b$, luego, $a = da'$ y $b = db'$, para algún $a', b' \in R$, entonces

$$\frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'},$$

$\frac{a'}{b'}$ es un cociente irreducible. En efecto, Como $d = m.c.d(a, b)$, por el Lema 5.0.27, $d =$

$ax + by$ para algún $x, y \in R$, luego

$$d = ax + by = da'x + db'y = d(a'x + b'y),$$

por tanto $1 = a'x + b'y$, es decir, a' y b' son primos relativos. □

Teorema 5.0.29. *Sea R un DIP y $\mathbb{K}$ su cuerpo de fracciones. Sea $f(x) \in R[X]$ mónico y $\alpha \in \mathbb{K}$, si $f(\alpha) = 0$, entonces $\alpha \in R$.*

Demostración. Por el Lema 5.0.28, una raíz de $f(x)$ en $\mathbb{K}$ puede escribirse como un cociente irreducible de la forma $\frac{a}{b}$, donde a, b son primos relativos.

Suponga que $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ con $n \geq 1$, entonces

$$0 = f\left(\frac{a}{b}\right) = \frac{a^n}{b^n} + c_{n-1}\left(\frac{a^{n-1}}{b^{n-1}}\right) + \cdots + c_1\left(\frac{a}{b}\right) + c_0.$$

Como $b \neq 0$, multiplicando toda la expresión por b^n tenemos

$$0 = a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n.$$

Cada término a la derecha de a^n es divisible por b, entonces $b|a^n$. Como a y b son primos relativos y R es un *DIP*, de $b|a^n$ se obtiene $b|1$. luego $b \in U(R)$. Por lo tanto $\frac{a}{b} = ab^{-1} \in R$. □

El siguiente resultado es una condición suficiente más no necesaria de que $\mathbb{Z}[\sqrt{m}]$ no es un *DIP*.

Teorema 5.0.30. *Si $m \in \mathbb{Z}$ no es un cuadrado perfecto y tiene factores primos repetidos, entonces $\mathbb{Z}[\sqrt{m}]$ no es un DIP.*

Demostración. Sea p un primo tal que $p^2|m$, entonces $m = p^2m'$. Como $\sqrt{m'} = \frac{\sqrt{m}}{p}$, se tiene que $\sqrt{m'}$ pertenece al cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$, considere el polinomio $f(x) = x^2 - m'$ el cual es mónico en $\mathbb{Z}[X] \subset \mathbb{Z}[\sqrt{m}][X]$, este polinomio tiene como raíz a $\sqrt{m'}$ en el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$ y no en $\mathbb{Z}[\sqrt{m}]$, luego, por el Teorema 5.0.29, $\mathbb{Z}[\sqrt{m}]$ no es un *DIP*. □

Ejemplo 5.0.31. Los anillos $\mathbb{Z}[\sqrt{12}] = \mathbb{Z}[2\sqrt{3}]$, $\mathbb{Z}[\sqrt{8}] = \mathbb{Z}[2\sqrt{2}]$ y $\mathbb{Z}[\sqrt{18}] = \mathbb{Z}[3\sqrt{2}]$ no son *DIP's*.

Un dominio entero R con la propiedad del Teorema 5.0.29 es llamado *integralmente cerrado*, por lo que el Teorema 5.0.30 dice que todo *DIP* es un dominio integralmente cerrado, por ende, los dominios enteros que no sean integralmente cerrados no pueden ser *DIP's*, observese la contenencia:

Dominios euclidianos $\subset$ *DIP's* $\subset$ Dominios integralmente cerrados.

Un ejemplo de esto puede verse en el Ejemplo 5.0.31. El siguiente teorema permitirá especificar los elementos invertibles de un anillo cuadrático.

Teorema 5.0.32. *En un anillo cuadrático $\mathbb{Z}[\gamma]$, las unidades son exactamente los elementos $\alpha \in \mathbb{Z}[\gamma]$ con $N(\alpha) = \pm 1$.*

Demostración. Si α es invertible, esto es que, existe $\beta \in \mathbb{Z}[\gamma]$ tal que $\alpha\beta = 1$, de ahí que, aplicando la norma a ambos lados de la igualdad se tiene

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1,$$

recuerde que $U(\mathbb{Z}) = \{-1, 1\}$, entonces $N(\alpha) = \pm 1$.

Por otro lado, si $N(\alpha) = \pm 1$, entonces $\alpha\overline{\alpha} = \pm 1$, por lo tanto, α es invertible (con inverso $\pm\overline{\alpha}$). □

Ejemplo 5.0.33. Las unidades de $\mathbb{Z}[\sqrt{2}]$ se construyen a partir de las soluciones enteras de la ecuación $x^2 - 2y^2 = \pm 1$, una solución es $x = 1$ y $y = 1$, en consecuencia, una unidad es $1 + \sqrt{2}$ y sus potencias también son unidades (las unidades son cerrados bajo la multiplicación), luego $\mathbb{Z}[\sqrt{2}]$ tiene infinitas unidades.

Ejemplo 5.0.34. Las unidades de $\mathbb{Z}[\sqrt{3}]$ se contruyen a partir de las soluciones enteras de la ecuación $x^2 - 3y^2 = \pm 1$, note que no hay soluciones para $x^2 - 3y^2 = -1$ puesto que esta ecuación no tiene soluciones módulo 3, esto es $x^2 \equiv -1(\mod 3)$ no tiene soluciones, luego las unidades en $\mathbb{Z}[\sqrt{3}]$ son aquellas que satisfacen que $x^2 - 3y^2 = 1$, una solución es $x = 2$ y $y = 1$, luego $2 + \sqrt{3}$ es una unidad y sus potencias generan infinitas unidades.

Ejemplo 5.0.35. Las unidades de $\mathbb{Z}[\sqrt{-2}]$ se construyen a partir de las soluciones enteras de $x^2 + 2y^2 = 1$, note que el lado derecho de la igualdad es mayor que 1 si $y \neq 0$, luego las únicas soluciones son $x = \pm 1$ y $y = 0$, por lo tanto, $\mathbb{Z}[\sqrt{-2}]$ solo tiene dos unidades.

El siguiente teorema sobre los dominios euclidianos es la clave para demostrar más adelante que ciertos dominios integrales no son euclidianos. Nótese que la demostración no requiere que la función euclídea sobre el anillo satisfaga inicialmente la *d-desigualdad*.

Teorema 5.0.36. *Sea R un dominio euclidiano que no es cuerpo. Existe $a \in R$ tal que en $R/\langle a\rangle$ cada clase de equivalencia está representado por 0 o unidades de R.*

Demostración. Como R no es cuerpo, hay elementos de R que no son 0 ni una unidad. Sea d la función euclidea sobre R. Se escoge un $a \in R$ tal que a no es cero ni una unidad y $d(a)$ sea el mínimo *d-valor*. Para cada $x \in R/\langle a\rangle$, se tiene que $x = aq + r$ para algunos $q, r \in R$ con $r = 0$ o $d(r) < d(a)$, si $r \neq 0$ entonces la desigualdad $d(r) < d(a)$ obliga a r ser una unidad, luego, $x \equiv r(\mod a)$, por tanto, cada clase de equivalencia en $R/\langle a\rangle$ está representado por 0 o unidades de R. □

Se ha demostrado que si R es un dominio euclidiano que no es un cuerpo, entonces hay un elemento de R (en concreto, una no unidad con el menor *d-valor*) cuyo módulo con todos los elementos de R es congruente a 0 o una unidad de R. Un dominio que no es un cuerpo y que no tiene ningún elemento cuyo módulo con todos los elementos del dominio es congruente a 0 o una unidad de R, no puede ser un dominio euclidiano.

5.0.4. El anillo cuadrático $\mathbb{Z}[(1+\sqrt{-19})/2]$ Para poder demostrar el Teorema 5.0.40, se deben conocer algunos conceptos sobre la teoría algebraica de números (Ver apéndice) y los siguientes resultados.

Proposición 5.0.37. *Sea $\mathbb{F}$ un cuerpo y sea $f(x) \in \mathbb{F}[X]$, entonces $f(x)$ tiene un factor de grado uno sí, y solo sí $f(x)$ tiene una raíz en $\mathbb{F}$.*

Demostración. Si $f(x)$ tiene un factor de grado uno, como $\mathbb{F}$ es un cuerpo, es posible asumir que ese factor es mónico, es decir, $f(x) = p(x)(x - \alpha)$, luego $f(\alpha) = 0$. por otro lado, suponga que existe $\beta \in \mathbb{F}$ tal que $f(\beta) = 0$, dado que $(\mathbb{F}[X], deg(f))$ es un dominio euclidiano, entonces se puede escribir a $f(x)$ como $f(x) = q(x)(x - \beta) + r$ con $deg(r) < deg(x - \beta)$, es decir r es constante y como $f(\beta) = 0$, entonces $r = 0$, por ende, $f(x)$ tiene un factor de grado uno.

□

Lema 5.0.38 (Criterio de irreducibilidad)**.** *Sea $\mathbb{F}$ un cuerpo y $f(x) \in \mathbb{F}[X]$ de grado menor o igual a 3. Entonces $f(x)$ es irreducible sí, y solo sí, $f(x)$ no tiene ninguna raíz en $\mathbb{F}$.*

Demostración. Esto se deduce inmediatamente de la proposición anterior, ya que un polinomio de grado dos o tres es reducible si y sólo si tiene un factor de grado uno. □

Lema 5.0.39. *Sea R el anillo de enteros de un cuerpo cuadrático imaginario, si $d \equiv 1(\mod 4)$, un entero primo p genera el ideal primo $\langle p\rangle$ en R sí, y solo sí, el polinomio mónico $x^2 - x + \frac{1-d}{4}$ es irreducible en $\mathbb{F}_p[X]$.*

Demostración. Considere el cuerpo cuadrático $\mathbb{Q}[\sqrt{d}]$, y suponga que $d \equiv 1(\mod 4)$. Note que $R = \mathbb{Z}[(1+\sqrt{d})/2] \cong Z[X]/\langle x^2 - x + \frac{1-d}{4}\rangle$, además, un entero primo p sigue siendo primo en R sí, y solo sí, $R' = R/\langle p\rangle$ es un cuerpo, para simplificar las cuentas, observe el siguiente diagrama:

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\text{Ker}_{\langle p\rangle}} & \mathbb{F}_p[X] \\ \Big\downarrow{\scriptstyle \text{Ker}_{\langle x^2-x+\frac{1-d}{4}\rangle}} & & \Big\downarrow{\scriptstyle \text{Ker}_{\langle x^2-x+\frac{1-d}{4}\rangle}} \\ R & \xrightarrow[\text{Ker}_{\langle p\rangle}]{} & R' \end{array}$$

El diagrama prueba que R' es un cuerpo sí, y solo sí $x^2 - x + \frac{1-d}{4}$ es irreducible en $\mathbb{F}_p[X]$. □

Teorema 5.0.40. *El anillo cuadrático $\mathbb{Z}[(1+\sqrt{-19})/2]$ es un DIP y no un dominio euclidiano.*

Demostración. Considere el cuerpo cuadrático $\mathbb{Q}[\sqrt{-19}]$, como $-19 \equiv 1(\mod 4)$, por el Teorema A.0.8 el anillo de enteros de $\mathbb{Q}[\sqrt{-19}]$ es $\mathcal{O}_{\mathbb{Q}[\sqrt{-19}]} = \mathbb{Z}[(1+\sqrt{-19})/2]$.

Usando el Teorema A.0.21, se puede determinar el grupo de clase de R. Primero se debe ver que R es un *DIP*. Como $-19 \equiv 1(\mod 4)$, entonces $\mu = \sqrt{\frac{|-19|}{3}} \approx 2{,}52$, luego el único entero primo que no excede μ es 2. Note que $x^2 - x + \frac{1-(-19)}{4} = x^2 - x + 5$ es irreducible en $\mathbb{F}_2[X]$, por lo tanto, por el Lema 5.0.39, $\langle 2\rangle$ es un ideal primo de R. Dado que $\langle 2\rangle$ es un ideal principal, por la Observación A.0.19 $[\langle 2\rangle]$ es la identidad, entonces por el item 2 del Teorema A.0.21, el grupo de clase de R es el trivial, en consecuencia, por el Teorema A.0.14 R es un *DIP*.

Para ver que R no es un dominio euclidiano, suponga que sí lo es. Sea $\alpha = x + y(1+\sqrt{-19})/2$, considere la función euclidea

$$d(\alpha) = N(\alpha) = x^2 + xy + 5y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4}.$$

Note que esta norma siempre es positiva y si $y \neq 0$, entonces $N(\alpha) \geq \frac{19y^2}{4} \geq \frac{19}{4} > 4$, es decir, si $x = 0$, la norma siempre es mayor a 4, sin embargo, si $y = 0$, $N(\alpha) = 1$ se satisface cuando $x = \pm 1$, luego, las unidades de R son ± 1. Sea $a \in R$ una no unidad no nula tal que $N(a)$ sea minimal. para algún $b \in R$, se tiene que $b = aq + r$, donde $r = 0$ o $N(r) < N(a)$, por el Teorema 5.0.36, $r \in \{0, \pm 1\}$. Dado que las únicas posibilidades para r son $0, \pm 1$, hay como máximo tres elementos en $R/\langle a \rangle$, $0 + \langle a \rangle, \pm 1 + \langle a \rangle$, por tanto, $R/\langle a \rangle \cong \mathbb{Z}_2$ o $\mathbb{Z}_3$.

Note que el polinomio $x^2 - x + 5$ tiene una raíz en R, puesto que

$$x^2 - x + 5 = \left(x - \left(-\frac{1 + \sqrt{-19}}{2}\right)\right)\left(x - \left(-1 + \frac{1 + \sqrt{-19}}{2}\right)\right).$$

Entonces $x^2 - x + 5$ tiene una raíz en $R/\langle a \rangle$, pero $x^2 - x + 5$ no tiene raíces en los cuerpos $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Por lo tanto, $R/\langle a \rangle$ no puede ser isomorfo a $\mathbb{Z}_2$, ni a $\mathbb{Z}_3$, es decir, en $R/\langle a \rangle$ cada clase de equivalencia no está representado por 0 y unidades de R, luego R no es un dominio euclidiano. □

A. Apéndice

El siguiente apéndice contiene información relevante para poder demostrar el Teorema 5.0.40, para más detalles consultar [5] y [6] capítulo 13.

A.0.1. Teoría Algebraica de Números

Preliminares en extensiones de cuerpos y anillos

Definición A.0.1 (Extensiones de Cuerpos)**.** Sean $\mathbb{E}$ y $\mathbb{F}$ cuerpos, se dice que $\mathbb{E}$ es una *extensión* de $\mathbb{F}$ si $\mathbb{F} \subseteq \mathbb{E}$ y se denota $\mathbb{E}/\mathbb{F}$.

Observación A.0.2*.* Si $\mathbb{E}/\mathbb{F}$ es una extensión de cuerpos, entonces $\mathbb{E}$ es un $\mathbb{F}-$espacio vectorial y la dimensión de $\mathbb{E}$ sobre $\mathbb{F}$ se denota por $[\mathbb{E} : \mathbb{F}]$. Una extensión $\mathbb{E}/\mathbb{F}$ es finita si $[\mathbb{E} : \mathbb{F}]$ es finita.

Definición A.0.3 (Extensiones de Anillos)**.** Sean R y S anillos, se dice que S es una *extensión* de R si $R \subseteq S$.

Definición A.0.4 (Enteros Algebraicos)**.** Sea S una extensión de R, un elemento $\gamma \in S$ es llamado *entero* sobre R si es raíz de un polinomío mónico $f(x) \in R[X]$.

Observación A.0.5*.* Si $\alpha \in \mathbb{C}$ es entero sobre $\mathbb{Z}$, entonces es llamando *entero algebraico*.

Definición A.0.6. Sea $\mathbb{E}/\mathbb{Q}$ una extensión de cuerpos. Se denota el conjunto de todos los enteros algebraicos que pertenecen a $\mathbb{E}$ como

$$\mathcal{O}_{\mathbb{E}} := \{\gamma \in \mathbb{E} : (\exists f(x) \in \mathbb{Z}[X])(f(\gamma) = 0) \text{ con } f(x) \text{ mónico y no nulo}\}.$$

Observación A.0.7*.* El conjunto $\mathcal{O}_{\mathbb{E}}$ es un anillo (más aún, es subanillo de $\mathbb{E}$) (Ver [5], p. 21 y 22).

---

[5] Juan RUEDA. "El grupo de clase de un anillo de enteros algebraicos". Disponible en: `https://noesis.uis.edu.co/handle/20.500.14071/14441`. Trabajo de Pregrado. Bucaramanga, Colombia: Universidad Industrial de Santander, 2023.

[6] Michael ARTIN. *Algebra*. Vol. 2. Pearson, 2014.

Teorema A.0.8. *Sea d un entero libre de cuadrados. Entonces el anillo de enteros algebraicos de $\mathbb{Q}[\sqrt{d}]$ es*

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \textit{si } d \equiv 2, 3 (\mod 4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \textit{si } d \equiv 1 (\mod 4). \end{cases}$$

Demostración. Ver [5], página 23. □

Definición A.0.9. Sea $\mathbb{E}/\mathbb{Q}$ una extensión finita, un subconjunto $F \subset \mathbb{E}$ es llamado ideal fraccionario de $\mathcal{O}_{\mathbb{E}}$, si existe un ideal $I \subset \mathcal{O}_{\mathbb{E}}$ y un elemento no nulo $a \in \mathcal{O}_{\mathbb{E}}$ tal que

$$F = a^{-1} \cdot I := \left\{ a^{-1} i : i \in I \right\},$$

donde a^{-1} es el inverso de a en el cuerpo $\mathbb{E}$.

Definición A.0.10 (Producto de ideales)**.** Sean $I, J \subset R$ ideales no nulos, entonces el producto de I y J se define por

$$I \cdot J := \left\{ \sum_i \alpha_i \beta_i : \alpha_i \in I \text{ y } \beta_i \in J \right\}.$$

El Grupo de Clase

Definición A.0.11 (Clases de equivalencia)**.** Sean I y J dos ideales fraccionarios de $\mathcal{O}_{\mathbb{E}}$. Se dirá que I y J son equivalentes si difieren entre sí, por un ideal principal, esto es

$$[I] = [J] \iff I = J \cdot \langle u \rangle,$$

para algún $u \in U(\mathbb{E})$.

Se denota solo $[I]$, a la clase del ideal I y se define como $[I] = \{J \subset R : I \sim J\}$.

Definición A.0.12 (Grupo de clase)**.** El grupo de clase de $\mathcal{O}_{\mathbb{E}}$ es un grupo cuyos elementos son las clases de equivalencia de la Definición A.0.11

En el grupo de clase se puede definir la siguiente operación

$$[I] \cdot [J] := [I \cdot J],$$

esta operación dota al grupo de clase, la estructura de grupo multiplicativo donde la identidad es $[\mathcal{O}_{\mathbb{E}}]$ y satisface $[I]^{-1} = [I^{-1}]$ (los elementos de I^{-1} se definen como se ve en [5] p. 33.

Teorema A.0.13. *El grupo de clase del anillo de enteros $\mathcal{O}_{\mathbb{E}}$ es finito.*

Demostración. Ver [5], página 40. □

Teorema A.0.14. *El grupo de clase de $\mathcal{O}_{\mathbb{E}}$ es trivial sí, y solo sí, $\mathcal{O}_{\mathbb{E}}$ es un DIP.*

Demostración. Ver [5], página 40. □

Otra forma de obtener el grupo de clase La idea principal es dar una caracterización sobre el grupo de clase para hacer algunos cálculos sencillos. Por el Teorema A.0.8, para el problema inicial se tiene que $d = -19 \equiv 1(\mod 4)$ entonces $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ es el anillo de enteros del cuerpo cuadrático $\mathbb{Q}[\sqrt{-19}]$.

En secciones anteriores se presentó el concepto de anillo cuadrático $\mathbb{Z}[\gamma]$, del mismo modo se definen los cuerpos cuadráticos $\mathbb{Q}[\gamma]$ y se dice que es imaginario si γ es imaginario. Para concretar otra forma de obtener el grupo de clase, en [6] p. 398, se define una constante particular como se ve en la siguiente definición.

Definición A.0.15. Sea R el anillo de enteros de un cuerpo cuadrático imaginario, se define la constante μ como:

$$\mu = \begin{cases} 2\sqrt{\frac{|d|}{3}} & \text{si } d \equiv 2,3(\mod 4), \\ \sqrt{\frac{|d|}{3}} & \text{si } d \equiv 1(\mod 4). \end{cases}$$

Esta constante es estudiada por Artin en [6], la cual permitirá determinar con mayor facilidad el grupo de clase del anillo de enteros R.

Definición A.0.16 (Ideal Conjugado)**.** Sea $I \subset R$ un ideal no nulo, se define el conjugado de I como $\overline{I} := \{\overline{\alpha} : \alpha \in I\}$ el cual también es un ideal.

Lema A.0.17. *Sea R el anillo de enteros de un cuerpo cuadrático imaginario e $I \subset R$ un ideal distinto de cero. El producto $I \cdot \overline{I}$ es un ideal principal, generado por un entero positivo n, esto es que $I \cdot \overline{I} = \langle n \rangle = nR$.*

Demostración. Ver [6], página 391. □

Definición A.0.18 (Norma de un ideal)**.** Sea $I \subset R$ un ideal no nulo, la norma de I se define como $N(I) = n \iff I \cdot \overline{I} = \langle n \rangle$.

Observación A.0.19. Como $I \cdot \overline{I}$ es un ideal principal, entonces la clase de $[I \cdot \overline{I}]$ es la identidad.

Definición A.0.20 (Ideal Primo)**.** Sea $P \subset R$ un ideal no nulo, se dice que P es un ideal primo si $ab \in P$ implica $a \in P$ o $b \in P$.

Por último, el Teorema A.0.21 presenta una forma de determinar el grupo de clase de un anillo de enteros haciendo uso de la constante μ anteriormente definida.

Teorema A.0.21. *Sea R el anillo de enteros de un cuerpo cuadrático imaginario, entonces:*

1. *Toda clase de ideal contiene un ideal J tal que $N(J) \leq \mu$.*
2. *El grupo de clase es generado por las clases de ideales primos P cuya norma es un entero primo p y $p \leq \mu$.*

Demostración. Ver [6], página 399. □

Bibliografía

ARTIN, Michael. *Algebra*. Vol. 2. Pearson, 2014 (vid. págs. 37, 39, 40).

CLARK, Allan. *Elements of abstract algebra*. Courier Corporation, 1984 (vid. pág. 29).

CLARK, David. "A quadratic field which is Euclidean but not norm-Euclidean". En: *manuscripta mathematica* 83.1 (1994), págs. 327-330 (vid. pág. 27).

CONRAD, Keith. "Remarks about Euclidean domains". En: *https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf* (2020) (vid. págs. 6-8).

DUMMIT, David y FOOTE, Richard. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004 (vid. págs. 12, 14, 25).

HARPER, Malcolm. "$\mathbb{Z}[\sqrt{14}]$ is Euclidean". En: *Canadian Journal of Mathematics* 56.1 (2004), págs. 55-70 (vid. págs. 27, 28).

RUEDA, Juan. "El grupo de clase de un anillo de enteros algebraicos". Disponible en: https://noesis.uis.edu.co/handle/20.500.14071/14441. Trabajo de Pregrado. Bucaramanga, Colombia: Universidad Industrial de Santander, 2023 (vid. págs. 37-39).