Universidad Nacional Autónoma de México

Facultad de Ciencias

Teoría de divisibilidad en dominios enteros

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C A

P R E S E N T A:

KAREN BERENICE SANTOS CONTRERAS

DIRECTORA DE TESIS:
Dr. Edith Corina Sáenz Valadez

CIUDAD UNIVERSITARIA, CD. MX. 2020

Teoría de divisibilidad en dominios enteros

Karen Berenice Santos Contreras

20 de enero de 2020

Índice general

Introducción **5**

1. Anillos e ideales **7**
1.1. Anillos 7
1.2. Ideales y sus operaciones 21
1.3. Ideales primos y maximales 26

2. Teoría de divisibilidad en dominios enteros **31**
2.1. Máximo común divisor y mínimo común múltiplo 31
2.2. Mínimo común múltiplo 43
2.3. M.c.d. propiedad y m.c.m. propiedad 45
2.4. Elementos primos e irreducibles 48
2.5. Dominios de factorización única 53
2.6. Dominios Euclidianos 56

3. Ejemplos interesantes **67**
3.1. Algunos ejemplos 67

Bibliografía **71**

Introducción

En esta tesis estudiamos una de las ramas más hermosas del álgebra, a saber, la teoría de divisibilidad en los dominios enteros (los cuales son un tipo importante de anillos). La tesis consta de 3 capítulos. En la sección 1 del primer capítulo establecemos las definiciones básicas de la Teoría de Anillos como lo son: Anillos, anillos conmutativos, anillos con uno, anillos con división, campos y dominios enteros. Además estudiamos en detalle los ejemplos clásicos de anillos. En la sección 2 de dicho capítulo estudiamos las nociones de ideal, ideal finitamente generado, ideal principal y dominio de ideales principales y concluimos esta sección probando que el anillo $\mathbb{Z}$ es un dominio de ideales principales. En la sección 3 estudiamos el concepto de ideal maximal y de ideal primo. En particular, probamos que todo ideal propio de un anillo finitamente generado está contenido en un ideal maximal.

En la sección 1 del capítulo 2 estudiamos la noción de un máximo común divisor en anillos conmutativos con uno y lo relacionamos con los anillos Euclidianos. Más adelante en la sección 6 estudiamos más en detalle a estos anillos. En la sección 2 del capítulo 2 estudiamos la noción de mínimo común múltiplo y en la sección 3 estudiamos aquellos anillos que satisfacen la propiedad del máximo común divisor y del mínimo común múltiplo. Luego, en la sección 4 estudiamos el concepto de elemento primo y elemento irreducible y en la sección 5 estudiamos los dominios de factorización única. Finalmente en la sección 6 estudiamos a los dominios Euclideanos y a los dominios cuadráticos.

En el capítulo 3 desarrollamos en detalle varios ejemplos interesantes en los cuales mostramos que los resultados recíprocos de ciertos resultados establecidos no son ciertos.

Para terminar, un agradecimiento a la doctora Diana Avella Alaminos por sus valiosas observaciones que me ayudaron a corregir varios errores para esta tesis.

Capítulo 1

Anillos e ideales

1.1. Anillos

Comenzamos esta sección mencionando los conceptos clave para el entendimiento de este trabajo. Así mismo desarrollamos ejemplos para facilitar la comprensión de los conceptos mencionados.

Empezamos pues mencionando la estructura que nos interesa en este trabajo, a saber los anillos y algunas propiedades de éstos.

Definición 1.1.1. Un anillo es una terna $(R, +, \cdot)$ que consiste de un conjunto no vacío R y dos operaciones binarias definidas sobre R, llamadas adición (o suma) y multiplicación (o producto), respectivamente y denotadas por $+$ y $\cdot$ tal que

1. $(R, +)$ es un grupo abeliano.
2. $(R, \cdot)$ es un semigrupo.
3. La operación multiplicación es distributiva por ambos lados sobre la operación suma.

Notemos que la operación adición y multiplicación son operaciones abstractas definidas en R.

Notación 1.1.2. A un anillo $(R, +, \cdot)$ lo denotamos simplemente por R.

Ahora veamos dos pequeños lemas que nos ayudarán a denotar de mejor manera al elemento neutro y a los inversos de un anillo.

Lema 1.1.3. *Sea R un anillo. Entonces, el elemento neutro e es único.*

Demostración. Supongamos que existe $e' \in R$ tal que es otro elemento neutro. Veamos que $e = e'$. En efecto, como $e \in R$ entonces se satisface que $e = e + e' = e'$. □

Notación 1.1.4. Por lo anterior podemos denotar al elemento neutro como 0_R o simplemente como 0 si ya se sabe en que anillo estamos trabajando.

Lema 1.1.5. *Sea R un anillo. Entonces para cada $a \in R$, existe un único $b \in R$ tal que $a + b = 0$*

Demostración. Sea $a \in R$. Por ser R un anillo sabemos que existe $b \in R$ tal que $a + b = 0$. Supongamos que existe otro inverso de a digamos $b' \in R$, este satisface $a + b' = 0$. Veamos que $b = b'$. En efecto esto se sigue de las siguientes igualdades:

$$b = 0 + b = (a + b') + b = (b' + a) + b = b' + (a + b) = b' + 0 = b'$$

□

Notación 1.1.6. Así podemos denotar al inverso de $a \in R$ como $-a \in R$.

Usando la Teoría general de grupos y los lemas anteriores podemos desglosar mejor la definición de anillo:

Un anillo R es un conjunto no vacío R, con dos operaciones binarias: $+ : R \times R \to R$ y $\cdot : R \times R \to R$ tales que satisfacen:

1. La adición es conmutativa, $\forall\ a, b \in R,\ a + b = b + a$.
2. La operación adición es asociativa, esto es, $\forall\ a, b, c \in R$ se tiene que $a+(b+c) = (a+b)+c$.
3. Existe un único $0 \in R$ tal que $\forall\ a \in R\ a + 0 = a$.
4. $\forall\ a \in R$ existe un único $-a \in R$ tal que $a + (-a) = 0$.
5. La operación multiplicación es asociativa, es decir, $\forall\ a, b, c \in R$ se tiene que $a\cdot(b\cdot c) = (a\cdot b)\cdot c$.
6. Y por último la propiedad que relaciona las dos operaciones, la distributividad por ambos lados, $\forall\ a, b, c \in R$ se tiene que
   a) $(a + b) \cdot c = a \cdot c + b \cdot c$,
   b) $c \cdot (a + b) = c \cdot a + c \cdot b$.

Definición 1.1.7. Decimos que R es un anillo finito si el conjunto R es finito.

Ahora veamos otros tipos de anillos, los cuales resultan de pedirle otras propiedades a la operación multiplicación.

Definición 1.1.8. Sea R un anillo.

1. R es un anillo conmutativo si $a \cdot b = b \cdot a\ \forall\ a, b \in R$. Si $a \cdot b = b \cdot a$ para un caso particular, expresamos este hecho diciendo que a y b conmutan.
2. R es un anillo con identidad (o con uno) si existe un elemento identidad para la operación multiplicación, normalmente se representa por el símbolo 1 y es tal que $a \cdot 1 = a = 1 \cdot a$ $\forall a \in R$.
3. Dado un anillo R con uno, un elemento $a \in R$ se dice que es *invertible*, o una *unidad*, si posee un inverso respecto a la multiplicación por ambos lados. Es decir, si existe $b \in R$ tal que $ab = 1_R = ba$.

Definición 1.1.9. Sea $(R, +, \cdot)$ un anillo conmutativo con uno. Decimos que

1. R es un anillo con división si $(R \setminus \{0\}, \cdot)$ es un grupo con la multiplicación.
2. R es un campo si $(R \setminus \{0\}, \cdot)$ es un grupo abeliano con la multiplicación.

Observación 1.1.10. Si R es un campo entonces la multiplicación es conmutativa, mientras que en un anillo con división la multiplicación no necesariamente es conmutativa. Es decir, todo campo es un anillo con división pero al revés no.

Teorema 1.1.11. *Sean R un anillo conmutativo con uno y $a \in R$ un elemento invertible (o unidad). Entonces el inverso multiplicativo de a es único.*

Demostración. Sea $a \in R$ tal que es un elemento invertible, esto es existe $b \in R$ tal que $ab = ba = 1$. Supongamos que existe $c \in R$ tal que $ac = ca = 1$. Veamos que $b = c$. Esto se sigue de las siguientes igualdades:

$$b = b \cdot 1 = b \cdot (ac) = (ba) \cdot c = 1 \cdot c = c$$

□

Notación 1.1.12. Por el teorema anterior, dado un elemento a de un anillo R con uno tal que es invertible, denotamos al inverso de a como a^{-1}.

Consideremos el conjunto $R = \{0\}$. Este es un anillo conmutativo con uno con las operaciones $0 + 0 = 0$ y $0 \cdot 0 = 0$. En R el neutro aditivo coincide con el neutro multiplicativo. A este anillo lo llamamos el **anillo trivial**.

Ejemplo 1.1.13. Ahora veamos algunos ejemplos de anillos.

1. Consideremos los siguientes conjuntos

   a) Los números enteros denotados por $\mathbb{Z}$

   b) los números racionales detonados por $\mathbb{Q}$

   c) los números reales denotados por $\mathbb{R}$

   Entonces los sistemas: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, donde $+$ y $\cdot$ son la suma y el producto que conocemos restringidas a sus respectivos conjuntos son anillos conmutativos con uno. Más aún, por la Teoría general de campos sabemos que tanto el anillo de los números racionales como el de los números reales son campos.

2. Consideremos $\mathbb{Z}$ el conjunto de los números enteros. Sea $n \in \mathbb{Z}$. Entonces el conjunto

   $$n\mathbb{Z} = \{nm : m \in \mathbb{Z}\},$$

   con las operaciones suma y producto definidas en $\mathbb{Z}$ restringidas al conjunto $n\mathbb{Z}$, es un anillo conmutativo sin embargo este anillo es tal que no tiene uno para $n \neq \pm 1$. Además notemos que si $n = 0$ entonces $n\mathbb{Z} = \{0\}$ es el anillo trivial.

3. Sea X un conjunto dado y $\mathcal{P}(X)$ su conjunto potencia. La diferencia simétrica de dos subconjuntos $A, B \subset X$ es el conjunto $A \triangle B$, donde

   $$A \triangle B = (A - B) \cup (B - A).$$

   Definimos la suma y el producto en $\mathcal{P}(X)$ como:

   $$A + B = A \triangle B, \qquad A \cdot B = A \cap B$$

Entonces el sistema $(\mathcal{P}(X), +, \cdot)$ es un anillo conmutativo con uno. Ya que, de la Teoría general de conjuntos, sabemos que la diferencia simétrica satisface ser asociativa para cualesquiera tres subconjuntos de X, es conmutativa pues la unión de conjuntos conmuta. Note que el elemento $\emptyset \in \mathcal{P}(X)$ es el neutro aditivo, además para cada elemento $A \in \mathcal{P}(X)$ existe su inverso aditivo que es el mismo pues $A + A = A\triangle A = (A - A) \cup (A - A) = \emptyset$. Por lo cual $(\mathcal{P}(X), +)$ es un grupo abeliano.

Sabemos que la operación $\cap$ es asociativa y conmutativa, faltaría probar la distributividad. Sean $A, B, C \in \mathcal{P}(X)$ notemos que $(A\triangle B) \cap C = C \cap (A\triangle B)$ por lo cual sólo hay que ver que $(A\triangle B) \cap C = A \cap C \triangle B \cap C$, en efecto lo anterior se debe a las siguientes igualdades que se obtienen de propiedades vistas

$$(A\triangle B)\cap C = [(A-B)\cup(B-A)]\cap C = [(A\cap B^c)\cup(B\cap A^c)]\cap C = (A\cap B^c\cap C)\cup(B\cap A^c\cap C).$$

Por otro lado

$$\begin{aligned} A \cap C \triangle B \cap C &= [(A \cap C) - (B \cap C)] \cup [(B \cap C) - (A \cap C)] \\ &= [(A \cap C) \cap (B^c \cup C^c)] \cup [(B \cap C) \cap (A^c \cup C^c)] \\ &= [(A \cap C \cap B^c) \cup (A \cap C \cap C^c)] \cup [(B \cap C \cap A^c) \cup (B \cap C \cap C^c)] \\ &= (A \cap C \cap B^c) \cup (B \cap C \cap A^c) \\ &= (A \cap B^c \cap C) \cup (B \cap A^c \cap C). \end{aligned}$$

Así $(\mathcal{P}(X), +, \cdot)$ es un anillo conmutativo. Notemos que el conjunto X es el uno del anillo pues $A \cap X = A$ para todo $A \in \mathcal{P}(X)$ de donde $(\mathcal{P}(X), +, \cdot)$ es un anillo conmutativo con uno.

Es interesante notar que si X es un conjunto no vacío entonces el sistema $(\mathcal{P}(X), \cup, \cap)$ ni el sistema $(\mathcal{P}(X), \cap, \cup)$ constituyen un anillo. Esto ya que no hay un elemento inverso respecto a la operación $\cup$ en el caso del primer sistema y tampoco un inverso respecto a la operación $\cap$ en el caso del segundo sistema.

4. Dado un anillo $(R, +, \cdot)$, podemos considerar el conjunto $M_n(R)$ de las matrices de $n \times n$ sobre R. Para describir los elementos del conjunto $M_n(R)$ consideremos el conjunto $I_n = \{1, 2, \ldots, n\}$. Un elemento de $M_n(R)$ es una función $f : I_n \times I_n \to R$, en la práctica identificamos tal función con sus valores $a_{ij} = f(i, j)$ que expresamos como la matriz cuadrada de $n \times n$

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

donde $a_{ij} \in R$. Para facilitar la escritura de un elemento en $M_n(R)$ usaremos la abreviatura (a_{ij}) para representar a una matriz de $n \times n$ cuya entrada (i, j) es a_{ij}. Las operaciones que hacen al sistema $(M_n(R), +, \cdot)$ un anillo están dadas por

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \qquad y \qquad (a_{ij}) \cdot (b_{ij}) = (c_{ij}),$$

donde

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}.$$

El elemento cero es la matriz de $n \times n$ cuyas entradas son todas cero, y notemos que $-(a_{ij}) = (-a_{ij})$ ya que $-a_{ij}$ está bien definido pues R es un anillo. Así para cada (a_{ij}) tenemos un inverso $(-a_{ij})$ por lo que el sistema $(M_n(R), +, \cdot)$ es un anillo, pero falla en ser un anillo conmutativo para $n > 1$ pues en general el producto de matrices no es conmutativo.

Ahora observemos que si R es un anillo con uno, entonces la matriz cuyos elementos de la diagonal son unos, o bien $a_{ii} = 1$ y ceros en otro caso actúa como la identidad multiplicativa. Podemos describir este hecho haciendo uso de la delta de Kronecker δ_{ij} la cual está definida como

$$\delta_{ij} = \begin{cases} 1, & \text{si } i = j \\ 0, & \text{si } i \neq j \end{cases} \qquad (i, j = 1, 2, \ldots, n),$$

Así la matriz identidad puede ser escrita de la forma (δ_{ij}).

5. Sea X un conjunto arbitrario distinto del vacío y sea $(R, +, \cdot)$ un anillo. Usamos la notación $fun(X, R)$ para denotar el conjunto que consta de todas las funciones de X en R, en símbolos

$$fun(X, R) = \{f \mid f : X \to R\}.$$

Para facilitar la notación escribiremos $fun\ R$ en lugar de $fun(X, R)$. Definimos la suma y el producto como sigue:

$$(f + g)(x) = f(x) +_R g(x), \qquad (f \cdot g) = f(x) \cdot_R g(x) \qquad \text{con } x \in X$$

Con estas definiciones podemos verificar fácilmente que $fun\ R$ es un anillo, cuyo elemento neutro es la función constante cero, es decir aquella que satisface que $f(x) = 0_R$ para todo $x \in X$, mientras que el inverso aditivo $-f$ de f está dado por $(-f)(x) = -f(x)$ para toda $x \in R$.

Es interesante notar que las propiedades algebraicas de $fun(X, R)$ están determinadas por las propiedades del anillo $(R, +, \cdot)$. Esto es, por ejemplo si R es un anillo con uno entonces el anillo $fun\ R$ tendrá una identidad multiplicativa dada por $1(x) = 1_R$ para todo $x \in X$.

6. Para el siguiente ejemplo consideremos el conjunto de los enteros módulo n, $\mathbb{Z}_n$. Recordemos que en $\mathbb{Z}_n$ definimos la clase de congruencia módulo n de a como el conjunto

$$[a] = \{x \in \mathbb{Z} : x \equiv a\ (mod\ n)\} = \{x \in \mathbb{Z} : x = a + kn \text{ para algún } k \in \mathbb{Z}\}.$$

Más aún, recordemos que de los cursos básicos de álgebra podemos definir a $\mathbb{Z}_n$ como el siguiente conjunto que consta de n elementos

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

En este conjunto definimos las siguientes operaciones para cada $[a], [b] \in \mathbb{Z}_n$

$$[a] +_n [b] = [a + b], \qquad [a] \cdot_n [b] = [ab].$$

Veamos que las operaciones anteriores están bien definidas, es decir que no dependen del representante que se ha elegido. Sean $[a], [b] \in \mathbb{Z}_n$ tales que $[a'] = [a]$ y $[b'] = [b]$. Mostremos que $[a'b'] = [ab]$. Como $a' \in [a'] = [a]$ entonces $a' \in [a]$, de donde $a' = a + kn$ análogamente $b' = b + jn$ para algunos $k, j \in \mathbb{Z}$, así

$$a'b' = (a + kn)(b + jn) = ab + (aj + bk + kjn)n,$$

de donde $a'b' \equiv ab(mod\ n)$ y así $[a'b'] = [ab]$. De manera análoga se comprueba que la suma no depende del representante elegido.

Con estas definiciones tenemos que $\mathbb{Z}_n$ es un anillo conmutativo con uno, observemos que varios de los axiomas de anillo se satisfacen en $\mathbb{Z}_n$ ya que se satisfacen en $\mathbb{Z}$. La ley distributiva, por ejemplo, se satisface en $\mathbb{Z}_n$ ya que es válida en $\mathbb{Z}$

$$\begin{aligned} [\ a\ ] \cdot_n ([\ b\ ] +_n [\ c\ ]) &= [\ a\ ] \cdot_n [\ b + c\ ] = [\ a(b + c)\ ] \\ &= [\ ab + ac\ ] = [\ ab\ ] +_n [\ ac\ ] \\ &= [\ a\ ] \cdot_n [\ b\ ] +_n [\ a\ ] \cdot_n [\ c\ ]. \end{aligned}$$

Notemos también que las clases de congruencia $[0]$ y $[1]$ actúan como el elemento cero y como la identidad multiplicativa respectivamente, mientras que la clase $[-a]$ es el inverso aditivo de $[a]$ en $\mathbb{Z}_n$.

7. Consideremos los enteros gaussianos, $\mathbb{Z}[i]$, definidos por

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\}.$$

Éstos son un subconjunto de los números complejos. Tomando la suma y el producto definidos en $\mathbb{C}$ tenemos que $\mathbb{Z}[i]$ es un anillo conmutativo con uno. Ya que si $a + bi, c + di \in \mathbb{Z}[i]$ tenemos que su suma y producto se quedan en este conjunto, pues

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i, \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]. \end{aligned}$$

El elemento neutro es el entero $0 = 0 + 0i$, para cada $a + bi \in \mathbb{Z}[i]$ su inverso aditivo es el elemento $-a + (-b)i \in \mathbb{Z}[i]$, y la identidad multiplicativa de $\mathbb{C}$ está en $\mathbb{Z}[i]$ pues $1 = 1 + 0i$, de donde $1 \in \mathbb{Z}[i]$.

Ejemplo 1.1.14. Ahora veamos un ejemplo de un anillo que nos será muy útil en el siguiente capítulo.

Consideremos un anillo conmutativo K. Denotamos por seq K a la totalidad de todas las secuencias infinitas

$$f = (a_0, a_1, \dots, a_k, \dots)$$

de elementos $a_k \in K$. Tales secuencias son llamadas las *series de potencias formales* o simplemente *series de potencias* sobre K.

Decimos que dos series de potencias

$$f = (a_0, a_1, a_2, \dots) \qquad \text{y} \qquad g = (b_0, b_1, b_2, \dots)$$

son iguales si, y sólo si son iguales término a término

$$f = g \text{ si, y sólo si } a_k = b_k \text{ para todo } k \geq 0.$$

Además definimos la suma y el producto como sigue:

$$f + g = (a_0 + b_0, a_1 + b_1, \dots),$$
$$fg = (c_0, c_1, c_2, \dots),$$

donde para cada $k \geq 0$ c_k está dada por

$$c_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Es decir, esta suma corre sobre todos los enteros $i, j \geq 0$ sujetos a la restricción de que $i + j = k$.

Con estas operaciones seq K es un anillo conmutativo, donde la secuencia $(0, 0, \dots)$ es el neutro aditivo, para cada $f = (a_0, a_1, \dots)$ tenemos un inverso aditivo dado por la secuencia $-f = (-a_0, -a_1, \dots)$.

Veamos que se satisface la ley de la distributividad. Esto es, para f, g, h en seq K tales que $f = (a_0, a_1, \dots), g = (b_0, b_1, \dots), h = (c_0, c_1, \dots)$, probemos que $f(g+h) = fg + fh$. Como el producto conmuta (ya que K es un anillo conmutativo), tenemos que $f(g+h) = (g+h)f$ por lo que sólo hay que probar la primera igualdad. Como

$$f(g + h) = (a_0, a_1, \dots)((b_0 + c_0, b_1 + c_1, \dots)) = (d_0, d_1, \dots)$$

donde

$$d_k = \sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} (a_i b_j + a_i c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j.$$

Por otro lado

$$fg + fh = ((a_0, a_1, \dots)(b_0, b_1, \dots)) + ((a_0, a_1, \dots)(c_0, c_1, \dots)) = (s_0, s_1, \dots) + (t_0, t_1, \dots)$$

donde

$$s_k = \sum_{i+j=k} a_i b_j \quad \text{y} \quad t_k = \sum_{i+j=k} a_i c_j$$
$$\text{así } s_k + t_k = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j = d_k,$$

por lo cual $f(g+h) = fg + fh$. Así seq K es un anillo conmutativo.

Para introducir una notación adicional definamos a ax como la siguiente secuencia

$$(0, a, 0, 0, \dots).$$

Esto es, ax es un miembro específico de seq K tal que el elemento a está en su segunda entrada y todas las demás son cero. De manera más general podemos definir el símbolo $ax^n,\ n \geq 1$, el cual denotara la secuencia

$$(0, \dots, 0, \text{a}, 0, \dots)$$

donde el elemento a aparece en la $(n+1)$ entrada. Por ejemplo,

$$ax^2 = (0, 0, a, 0, \dots)$$
$$ax^3 = (0, 0, 0, a, 0, \dots).$$

Con estas definiciones, cada serie de potencias

$$f = (a_0, a_1, \dots)$$

tiene una única representación de la forma

$$\begin{aligned} f &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \cdots + (0, \dots, 0, a_n, 0, \dots) + \dots \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \dots. \end{aligned}$$

Así el anillo de series de potencias formales seq K es aquel que consiste de todas las expresiones formales

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \dots,$$

donde los elementos $a_0, a_1, \dots$ son llamados los *coeficientes de* f y pertenecen a K. Denotaremos de manera más compacta a los elementos de seq K como $f = \sum a_k x^k$, notemos que el símbolo de suma es una suma formal y por tanto la convergencia no es un problema para nosotros.

Usando esta notación podemos reescribir la suma y el producto en el anillo de las series de potencias formales como sigue

$$\sum a_k x^k + \sum b_k x^k = \sum (a_k + b_k) x^k$$
$$(\sum a_k x^k)(\sum b_k x^k) = \sum c_k x^k,$$

donde

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}.$$

Para indicar la indeterminada x denotaremos por $K[[x]]$ en lugar de seq K y por $f(x)$ a un elemento de este anillo.

Más aún, si K es un anillo conmutativo con uno, entonces $K[[x]]$ posee un elemento identidad $(1, 0, 0, \dots)$ y lo denotamos por 1. Además podemos identificar la serie de potencias $0 + 1x + 0x^2 + 0x^3 + \dots$ con x de donde podemos tratar a x como un miembro especial de $K[[x]]$ denotado por la secuencia $x = (0, 1, 0, \dots)$. De este modo ax se convierte en el producto de elementos de $K[[x]]$

$$ax = (a, 0, 0, \dots)(0, 1, 0, \dots).$$

Como notación adicional omitiremos los términos con coeficientes cero y reemplazaremos $(-a_k)x^k$ por $-a_k x^k$ y por último denotaremos a $1x^k$ como x^k con $k \geq 1$. Con estas convenciones podemos tomar por ejemplo

$$1 + x^2 + x^4 + \cdots + x^{2n} + \cdots \in K[[x]],$$

como representación de la secuencia $(1, 0, 1, 0, \dots)$.

Así, podemos definir los polinomios en una variable (en x) sobre un anillo conmutativo con uno K, denotado por $K[x]$, como el conjunto

$$K[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_k \in K, \forall\, k \in \{0, 1, \dots, n\}, n \geq 0\}.$$

Esto es, $K[x]$ denota el conjunto de todas las series de potencias de $K[[x]]$ cuyos coeficientes son cero a partir de un índice en adelante (este índice particular varía dependiendo de la serie). Es decir, definimos un polinomio como una secuencia finita no nula de elementos de K. Por ejemplo, la secuencia $(1, 1, 1, 0, 0, \dots)$ es un polinomio sobre K pero la secuencia $(1, 0, 1, 0, \dots, 1, 0, \dots)$ no lo es.

Podemos definir la suma y el producto en $K[x]$ como las definimos en $K[[x]]$. Veamos que si $f(x) = \sum a_k x^k, g(x) = \sum b_k x^k$ son elementos de $K[x]$, con $a_k = 0$ para toda $k \geq n$ y $b_k = 0$ para toda $k \geq m$, entonces ambas operaciones son cerradas. Es decir, que la suma y el producto de elementos de $K[x]$ se queda en este conjunto. Esto se sigue de

$$\begin{aligned} a_k + b_k &= 0 \text{ para } k \geq \max\{m, n\} \\ \sum_{i+j=k} a_i b_j &= 0 \text{ para } k \geq m + n, \end{aligned}$$

así tenemos que $f(x) + g(x)$ y $f(x)g(x)$ pertenecen a $K[x]$. De esta forma $K[x]$ es un anillo conmutativo con uno.

Para continuar, veamos una definición en el anillo conmutativo con uno de los polinomios en una variable sobre un anillo conmutativo con uno K.

Definición 1.1.15. Sea $K[x]$ el anillo conmutativo con uno de los polinomios en una variable sobre el anillo K y $f(x) = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ un polinomio distinto de cero en $K[x]$. Decimos que a_n es el coeficiente principal de $f(x)$; y el entero n es el grado del polinomio al cual denotamos por $\text{gr}(f(x)) = n$.

Así el grado de un polinomio distinto de cero es un entero no negativo; para el polinomio cero su grado no está definido. También notemos que los polinomios con grado cero son los polinomios constantes distintos de cero.

Ejemplo 1.1.16. Veamos un ejemplo de la definición anterior.

Consideremos el anillo conmutativo con uno de los polinomios en una variable sobre el anillo de los números enteros $\mathbb{Z}[x]$. Sean $f(x) = 1 + 4x^4 + 7x^6 + 0x^{20}, g(x) = 4 \in \mathbb{Z}[x]$. El coeficiente principal de $f(x)$ es 7 y el grado de $f(x)$ es 6. Para $g(x) = 4$ tenemos que el coeficiente principal es 4 y el grado de $g(x)$ es 0.

Mostremos que en los polinomios en una variable sobre un anillo conmutativo con uno R se satisface un análogo al algoritmo de la división.

Teorema (Algoritmo de la división para $R[x]$) 1.1.17. *Sea R un anillo conmutativo con uno y $f(x), 0 \neq g(x)$ polinomios en $R[x]$ tales que el coeficiente principal del polinomio $g(x)$ es un elemento invertible. Entonces existen únicos polinomios tales que $q(x), r(x) \in R[x]$ tales que*

$$f(x) = q(x)g(x) + r(x),$$

con $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$.

Demostración. Sea R un anillo conmutativo con uno y $f(x), 0 \neq g(x)$ polinomios en $R[x]$ tales que el coeficiente principal del polinomio $g(x)$ es un elemento invertible. Mostremos este teorema por inducción sobre el grado de $f(x)$. Si $f(x) = 0$ o $f(x) \neq 0$ y $\text{gr}(f(x)) < \text{gr}(g(x))$, existe una representación que cumple los requisitos del teorema al tomar $q(x) = 0$, $r(x) = f(x)$. Además, si $\text{gr}(g(x)) = 0$, tenemos que $g(x)$ es un elemento del anillo R, como el coeficiente principal de $g(x)$ es invertible, es suficiente tomar $q(x) = f(x)g(x)^{-1}$, $r(x) = 0$.

Supongamos que el teorema es cierto para polinomios de grado menor que n y sean $\text{gr}(f(x)) = n$, $\text{gr}(g(x)) = m$, con $n \geq m \geq 1$; esto es,

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_n \neq 0$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad b_m \neq 0 \quad (n \geq m).$$

El polinomio $f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$ pertenece al anillo $R[x]$ como el coeficiente asociado a la variable x^n es $a_n - a_nb_m^{-1}b_m = 0$, entonces el polinomio $f_1(x)$ tiene grado menor que n. Por lo tanto existen polinomios $q_1(x), r(x) \in R[x]$ tales que

$$f_1(x) = q_1(x)g(x) + r(x),$$

con $r(x) = 0$ o $\text{gr}(r(x)) \leq \text{gr}(g(x))$. Sustituyendo, obtenemos la siguiente identidad

$$f(x) = (q_1(x) + a_nb_m^{-1}x^{n-m})g(x) + r(x),$$

definimos a $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$, de donde $f(x) = q(x)g(x) + r(x)$. Por lo tanto tenemos la representación que se buscaba cuando $\text{gr}(f(x)) = n$.

Para demostrar la unicidad, supongamos que

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x),$$

con $r(x)$ y $r'(x)$ satisfaciendo los requerimientos del teorema. Luego, restando

$$r(x) - r'(x) = (q'(x) - q(x))g(x).$$

Como el coeficiente principal de $g(x)$ es invertible, se sigue que $q'(x) - q(x) = 0$ si, y sólo si $r(x) - r'(x) = 0$. Teniendo esto en mente, si $q'(x) - q(x) \neq 0$. Sabiendo que b_m no es un divisor de cero en R,

$$\text{gr}(q'(x) - q(x)g(x)) = \text{gr}(q'(x) - q(x)) + \text{gr}(g(x)) \geq \text{gr}(g(x)) > \text{gr}(r(x) - r'(x)),$$

lo cual es una contradicción, La última desigualdad se basa en el hecho de que los grados de $r(x)$ y $r'(x)$ son ambos menores que el grado de $g(x)$. Así, $q(x) = q'(x)$, lo cual implica que $r(x) = r'(x)$.

□

A los polinomios $q(x)$ y $r(x)$ que aparecen en el teorema 1.1.17 son llamados, respectivamente, el **cociente** y el **residuo** de dividir $f(x)$ por $g(x)$. Ahora veamos varias propiedades básicas que se satisfacen en un anillo cualquiera.

Teorema 1.1.18. *Sea R un anillo. Entonces para cualesquiera $a, b, c \in R$ se satisfacen las siguientes identidades:*

a) $0a = a0 = 0$,

b) $a(-b) = (-a)b = -(ab)$,

c) $-(-a) = a$,

d) $(-a)(-b) = ab$, *y*

e) $a(b - c) = ab - ac, (b - c)a = ba - ca$.

Demostración. Sean $a, b, c \in R$.

a) Veamos que $0a = 0 = a0$. Sabemos que $0 \in R$ es tal que para toda $d \in R$, $d + 0 = d = 0 + d$, en particular tenemos que $0 + 0 = 0$. De modo que

$$0a = (0 + 0)a = 0a + 0a, \text{ de donde } 0a = 0a + 0a,$$

así por la ley de la cancelación para el grupo aditivo $(R, +)$ tenemos que $0a = 0$, de manera análoga se demuestra que $a0 = 0$.

b) Mostremos ahora que $a(-b) = (-a)b = -(ab)$. Para esto usemos el lema 1.1.5 el cual nos dice que el inverso aditivo de un elemento es único. Sabemos que $-(ab)$ denota al inverso aditivo de ab, de modo que basta ver que $a(-b)$ o $(-a)b$ son tales que $ab + a(-b) = 0$, $ab + (-a)b = 0$.

En efecto, esto se sigue de las siguientes igualdades:

$$ab + a(-b) = a(b + (-b)) = a0 = 0,$$
$$ab + (-a)b = (a + (-a))b = 0a = 0,$$

así $a(-b) = -(ab) = (-a)b$.

c) Mostremos que $-(-a) = a$ para toda $a \in R$. Como $-a$ es el inverso aditivo de a, se tiene que

$$a + (-a) = 0 = -a + a,$$

de donde a es inverso aditivo de $-a$ y por el lema 1.1.5 se tiene que $-(-a) = a$.

d) Veamos ahora que $(-a)(-b) = ab$. Esto se sigue del inciso b) de este teorema

$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab$$

e) Mostremos ahora que $a(b - c) = ab - ac, (b - c)a = ba - ca$, se satisface para toda $a, b, c \in R$, esto se sigue del inciso b) pues

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$$

De manera análoga se demuestra que $(b - c)a = ba - ca$.

□

Sabemos que en el anillo trivial el elemento neutro coincide con la identidad multiplicativa. De hecho este es el único caso en el cual el neutro aditivo coincide con el uno de un anillo. El siguiente corolario prueba esta afirmación.

Corolario 1.1.19. *Sea R un anillo con uno. Si R no es el anillo trivial, entonces el elemento 0 y 1 son distintos.*

Demostración. Como $R \neq \{0\}$ tenemos que existe un elemento $0 \neq a \in R$. Supongamos que $1 = 0$. Como R es un anillo con uno existe $1 \in R$ tal que para toda $r \in R$ se satisface que $1r = r1 = r$, en particular para $a \in R$ se tiene que $a = 1a = 0a$ de donde por el teorema 1.1.18 tenemos que $a = a0 = 0$ lo cual es una contradicción pues $a \neq 0$. Así $1 \neq 0$. □

Del ejemplo 3. en 1.1.13 si A es el conjunto $\{a, b, c\}$, tenemos que $\{a\}, \{b\} \in \mathcal{P}(A)$ y además son tales que $\{a\} \neq \emptyset$, $\{b\} \neq \emptyset$ y $\{a\} \cdot \{b\} = \{a\} \cap \{b\} = \emptyset$. Esto es tenemos dos elementos que no son el cero del anillo sin embargo al multiplicarlos obtenemos el cero de nuestro anillo. Esto en el anillo de los números enteros no sucede, pues recordemos que si tomamos $a, b \in \mathbb{Z}$ tales que son elementos no cero entonces $a \cdot b \neq 0$. En la siguiente definición le daremos un nombre a los elementos que satisfacen la característica mencionada en $\mathcal{P}(A)$ con $A = \{a, b, c\}$.

Definición 1.1.20. Sea R un anillo y $0 \neq a \in R$.

1. Decimos que a es un *divisor izquierdo (derecho) de cero* en R si existe $0 \neq b \in R$ tal que $ab = 0, (ba = 0)$.

2. Un *divisor de cero* es un elemento $0 \neq a \in R$ tal que es un divisor izquierdo y derecho de cero.

Observación 1.1.21. Si R es un anillo conmutativo, entonces claramente un elemento $a \in R$ es un divisor izquierdo de cero si, y sólo si es un divisor derecho de cero.

Ejemplo 1.1.22. Ahora veamos algunos ejemplos de anillos con y sin divisores de cero.

1. Consideremos el anillo conmutativo con uno de los enteros módulo 8, esto es

$$\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}.$$

   Sean $[6], [4] \in \mathbb{Z}_8$ son elementos no nulos. Notemos que $[6] \cdot [4] = [24] = [0]$, esto es $[6]$ y $[4]$ son divisores de cero en $\mathbb{Z}_8$.

2. Sea A el conjunto $\{a, b, c\}$ y consideremos su conjunto potencia $\mathcal{P}(A)$. Sabemos que éste es un anillo conmutativo con uno, ver el ejemplo 3. de 1.1.13. Sean $\{a\}, \{b\} \in \mathcal{P}(A)$ son tales que $\{a\} \neq \emptyset$, $\{b\} \neq \emptyset$ y $\{a\} \cdot \{b\} = \{a\} \cap \{b\} = \emptyset$, esto es $\{a\}, \{b\}$ son divisores de cero en $\mathcal{P}(A)$.

3. Consideremos el anillo de los números racionales $\mathbb{Q}$. Sean $a, b \in \mathbb{Q}$ tales que $a \neq 0$ y $b \neq 0$. Supongamos además que $a \cdot b = 0$, como $\mathbb{Q}$ es un campo y $b \neq 0$ entonces existe $b^{-1} \in \mathbb{Q}$. Así multiplicando $ab = 0$ por el inverso de b a ambos lados obtenemos que

$$a = (ab)b^{-1} = 0b^{-1} = 0,$$

   de donde $a = 0$ pero esto es una contradicción por lo tanto no hay $a, b \in \mathbb{Q}$ tales que sean ambos no nulos y $ab = 0$. Por tanto en $\mathbb{Q}$ no tenemos divisores de cero.

En el anillo de los números enteros y en los campos que ya conocemos de los cursos básicos, tenemos una ley de la cancelación para el producto. Por ejemplo en $\mathbb{Z}$ sabemos que si $a, b, c \in \mathbb{Z}$ y son tales que $ac = bc$ con $c \neq 0$ entonces $a = b$. De hecho en la demostración usábamos fuertemente el hecho de que no tenemos divisores de cero, o bien $ab = 0$ si, y sólo si $a = 0$ o $b = 0$. Veamos un teorema que nos relaciona los divisores de cero con las leyes de la cancelación pero de manera más general, esto es en un anillo cualquiera.

Teorema 1.1.23. *Sea R un anillo. Entonces R no tiene divisores de cero si, y sólo si se satisfacen las leyes de la cancelación, esto es, para toda $a, b, c \in R$, $ab = ac$, $ba = ca$ con $a \neq 0$ implica que $b = c$.*

Demostración. Supongamos que R es un anillo tal que no tiene divisores de cero. Veamos que se satisfacen las leyes de la cancelación. Sean $a, b, c \in R$ tales que $ab = ac$, $a \neq 0$. Entonces $a(b - c) = 0$, por el teorema 1.1.18, y como $a \neq 0$ y R no tiene divisores de cero, tenemos que $b - c = 0$ así $b = c$. El argumento es el mismo para la identidad $ba = ca$.

Supongamos ahora que R es un anillo en el cual se satisfacen las leyes de la cancelación y $ab = 0$ para $a, b \in R$ con $a \neq 0$. Veamos que $b = 0$. Por el teorema 1.1.18 tenemos que $ab = a0$, como $a \neq 0$ cancelando a tenemos que $b = 0$. Similarmente, si $b \neq 0$ implica que $a = 0$. Así R no tiene divisores de cero.

□

El teorema anterior motiva la definición de dominio entero, la cual usaremos a lo largo del Capítulo 2.

Definición 1.1.24. Sea R un anillo conmutativo con uno. Decimos que R es un dominio entero si no tiene divisores de cero.

Ejemplo 1.1.25. Veamos los siguientes ejemplos.

1. Consideremos el anillo conmutativo con uno de los números enteros, $\mathbb{Z}$. De los cursos básicos de álgebra sabemos que en $\mathbb{Z}$ se satisface que para toda $a, b \in \mathbb{Z}$ $ab = 0$ si, y sólo si $a = 0$ o $b = 0$, de donde $\mathbb{Z}$ no tiene divisores de cero. Por tanto, $\mathbb{Z}$ es un dominio entero.

2. Consideremos un campo K. Dados $a, b \in K$ tales que $ab = 0$, tenemos que si $0 \neq a$ entonces existe a^{-1} y multiplicando la identidad tenemos que $(a^{-1}a)b = 1b = b = 0$. Por tanto, K es un dominio entero.

3. Del ejemplo 1.1.22 sabemos que el anillo conmutativo con uno de los enteros módulo 8, $\mathbb{Z}_8$ no es un dominio entero pues tiene divisores de cero. Por tanto $\mathbb{Z}_8$ no es un dominio entero. También por este mismo ejemplo sabemos que en general $\mathcal{P}(A)$ no es un dominio entero.

A continuación enunciamos algunas de las propiedades que se satisfacen en el anillo de los polinomios en una variable sobre un anillo conmutativo con uno K. Un corolario importante en el cual observamos qué sucede con $K[x]$ si el anillo que consideramos es un dominio entero.

Lema 1.1.26. *Sean K un anillo conmutativo con uno y $f(x), g(x) \in K[x]$ polinomios distintos de cero. Entonces se satisface sólo uno de los siguientes enunciados*

1. *$f(x)g(x) = 0$ en cuyo caso el grado del polinomio $f(x)g(x)$ no está definido.*

2. *$f(x)g(x) \neq 0$ en cuyo caso $gr(f(x)g(x)) \leq gr(f(x)) + gr(g(x))$.*

Además si K es un dominio entero como $f(x)$ y $g(x)$ son no nulos tenemos que $f(x)g(x)$ es distinto de cero y $\text{gr}(f(x)g(x)) = \text{gr}(f(x)) + \text{gr}(g(x))$.

Lema 1.1.27. *Sean K un anillo conmutativo con uno y $f(x), g(x) \in K[x]$ polinomios distintos de cero. Entonces se satisface sólo uno de los siguientes enunciados*

1. *$f(x) + g(x) = 0$.*

2. *$f(x) + g(x) \neq 0$ en cuyo caso $gr(f(x) + g(x)) \leq max\ \{gr(f(x)), gr(g(x))\}$.*

La demostración de estos lema se deja al lector. Ahora podemos enunciar el siguiente corolario, el cual nos dice que si K es un dominio entero entonces también lo debe de ser su anillo de polinomios.

Corolario 1.1.28. *Sea K un dominio entero. Entonces su anillo de polinomios en una variable $K[x]$ también es un dominio entero.*

Demostración. Se sigue directo del lema 1.1.26.

□

Dado un anillo R y S un subconjunto de R nos gustaría saber cuándo S resulta ser también un anillo.

Definición 1.1.29. Sea $(R, +, \cdot)$ un anillo y $S \subseteq R$ un subconjunto no vacío de R. Decimos que $(S, +, \cdot)$ es un subanillo de $(R, +, \cdot)$ si $(S, +, \cdot)$ es un anillo usando las operaciones restringidas.

Esta definición es adecuada, pero engorrosa, ya que debemos de verificar cada una de las propiedades de la definición de anillo para el subconjunto S. Es decir, debemos verificar que $(S,+)$ es un subgrupo de $(R,+)$, $(S,\cdot)$ es un semigrupo, y las dos leyes distributivas se satisfacen en S. Pero las leyes distributivas y las asociativas se satisfacen en S ya que se satisfacen en R y $S \subseteq R$, así verificar éstas no es necesario. Por tanto $(S,+,\cdot)$ es un subanillo de $(R,+,\cdot)$ si, y sólo si:

1. S es un subconjunto no vacío de R,
2. $(S,+)$ es un subgrupo de $(R,+)$, y
3. la operación $\cdot : S \times S \longrightarrow S$ es cerrada.

Recordemos de la teoría de grupos que $(S,+)$ es un subgrupo de $(R,+)$ si, y sólo si S es no vacío y $a-b \in S$ para todo $a,b \in S$. Con estas observaciones podemos caracterizar un subanillo de una manera más fácil.

Proposición 1.1.30. *Sea R un anillo y $\emptyset \neq S \subseteq R$. Entonces S, es un subanillo de R si, y sólo si*

1. *Para todo $a,b \in S$ se tiene que $a-b \in S$,*
2. *Para todo $a,b \in S$ se tiene que $ab \in S$.*

La demostración de esta proposición se deja al lector, es una consecuencia de las observaciones anteriores.

Ejemplo 1.1.31. Veamos los siguientes ejemplos de subanillos.

1. Sea R un anillo, entonces éste posee dos subanillos, el anillo $\{0\}$ trivial y R mismo. A éstos dos subanillos se les conocen como los **subanillos triviales** de R. Si existen otros subanillos de R los llamaremos **subanillos no triviales**. Usaremos el término **subanillo propio** para referirnos a un subanillo el cual es diferente de R.
2. Consideremos $(\mathbb{Z},+,\cdot)$ el anillo de los números enteros. Entonces $(2\mathbb{Z},+,\cdot)$ es un subanillo de $(\mathbb{Z},+,\cdot)$ y en general $(n\mathbb{Z},+,\cdot)$, con $0 \neq n \in \mathbb{Z}$ es un subanillo de $\mathbb{Z}$.
3. Consideremos el anillo $(\mathbb{Q},+,\cdot)$. Entonces $(\mathbb{Z},+,\cdot)$ es un subanillo propio de $(\mathbb{Q},+,\cdot)$.

1.2. Ideales y sus operaciones

En esta sección hablaremos sobre los ideales de un anillo. Éstos son una clase de subanillos de un anillo R a los que les añadimos una cerradura bajo la multiplicación de cualquier elemento $r \in R$. Este concepto nos será muy útil en el siguiente capítulo, pues varias de las propiedades las podemos expresar en términos de ideales.

Definición 1.2.1. Sea I un subanillo de un anillo R. Decimos que I es un ideal bilateral de R si, y sólo si para todo $r \in R$ y para toda $a \in I$ se tiene que $ar \in I$ y $ra \in I$.

De acuerdo a la proposición 1.1.30, podemos reescribir la definición de un ideal bilateral como sigue.

Definición 1.2.2. Sea I un subconjunto no vacío de un anillo R. Entonces I, es un ideal bilateral de R si, y sólo si

1. Para cada $a, b \in I$ se tiene que $a - b \in I$, y
2. Para toda $r \in R$ y para toda $a \in R$ se tiene que $ra, ar \in I$.

Decimos que I es un **ideal derecho** de R si se satisface 1. de la definición 1.2.2 y $ar \in I$ para cada $r \in R$ y $a \in I$. De manera análoga, I es un **ideal izquierdo** de R si se satisface 1. y para cada $r \in R$ y para cada $a \in I$ se tiene que $ra \in I$.

Observación 1.2.3. Si R es un anillo conmutativo entonces un ideal bilateral coincide con ser un ideal izquierdo o derecho de R.

Decimos que I es un **ideal** de R en lugar de un ideal bilateral. De modo que siempre que hablemos de ideales se entenderá que es un ideal bilateral, a menos que se indique lo contrario. Además si I es un subconjunto propio de R e I es un ideal entonces decimos que I es un **ideal propio** de R.

Ejemplo 1.2.4. Veamos los siguientes ejemplos.

1. Sea R un anillo conmutativo. Es claro que $\{0\}$ es un ideal propio de R y R es un ideal de R. Se les conoce como los **ideales triviales**.
2. Consideremos el anillo de los números enteros $\mathbb{Z}$. Sea $n\mathbb{Z} \subseteq \mathbb{Z}$ como en el ejemplo 1.1.13, entonces $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.
3. Sea R un anillo. Consideremos el anillo $fun(X, R)$ (ver ejemplo 1.1.13). Dado un $x \in X$ un elemento fijo denotamos por I_x al conjunto de todas las funciones tales que toman el valor de 0 en x; es decir,

$$I_x = \{f \in fun(X, R) : f(x) = 0\}.$$

Veamos que I_x es un ideal de $fun(X, R)$.

a) Sean $f, g \in I_x$. Entonces, por la definición de las operaciones en el anillo $fun(X, R)$, tenemos que

$$(f - g)(x) = f(x) - g(x) = 0 - 0 = 0.$$

De donde, $f - g \in I_x$.

b) Sean $f \in I_x$ y $h \in fun(X, R)$. Entonces,

$$(fh)(x) = f(x)h(x) = 0h(x) = 0,$$
$$(hf)(x) = h(x)f(x) = h(x)0 = 0,$$

así $fh, hf \in I_x$.

Por lo tanto I_x es un ideal de $fun(X, R)$. De manera más general podemos considerar S un subconjunto no vacío de X. Entonces el conjunto

$$I = \{f \in fun(X, R) : f(x) = 0 \text{ para toda } x \in S\},$$

es un ideal de $fun(X, R)$. Más aún, podemos expresar a este ideal como $I = \bigcap_{x \in S} I_x$, esto es, la intersección de los ideales I_x resulta ser de nuevo un ideal. Veremos en el siguiente teorema que esto no es sólo una coincidencia, de hecho cualquier intersección arbitraria de ideales (derechos, izquierdos) resulta ser un ideal (derecho, izquierdo).

Teorema 1.2.5. *Sean $\{I_i\}_{i \in A}$ una colección arbitraria de ideales (respectivamente ideales derechos, ideales izquierdos) de un anillo R. Entonces, $\bigcap_{i \in A} I_i$ es un ideal (respectivamente ideal derecho, ideal izquierdo).*

Demostración. Sea R un ideal y $\{I_i\}_{i \in A}$ una colección arbitraria de ideales.

1. $\bigcap_{i \in A} I_i$ es distinto del vacío pues $0_R \in I$ para todo $i \in A$.

2. Dados $a, b \in \bigcap_{i \in A} I_i$ tenemos que $a - b \in \bigcap_{i \in A} I_i$ ya que cada $(I_i, +)$ es un subgrupo de $(R, +)$.

3. Sea $r \in R$ y $a \in \bigcap_{i \in A} I_i$. Entonces para cada $i \in A$ tenemos que $ra \in I_i$ y $ar \in I_i$, de donde $ra \in \bigcap_{i \in A} I_i$ y $ar \in \bigcap_{i \in A} I_i$.

Por tanto $\bigcap_{i \in A} I_i$ es un ideal de R.

□

Definición 1.2.6. Sea R un anillo y $S \neq \emptyset$ un subconjunto de R. Definimos al ideal generado por el subconjunto S como

$$(S) = \bigcap \{I : S \subseteq I, \text{ con } I \text{ ideal de } R\}.$$

Observación 1.2.7. Veamos algunas observaciones de este ideal.
Notemos que $\{I : S \subseteq I, \text{ con I ideal de } R\}$ es no vacío, ya que R es un ideal de R y $S \subseteq R$. Es decir, $R \in \{I : S \subseteq I, \text{ con } I \text{ ideal de } R\}$. Además, (S) es el ideal más pequeño (respecto a la contención) tal que contiene a S, es decir si J es un ideal de R tal que $S \subseteq J$ entonces $(S) \subseteq J$.

Si el conjunto S consiste de un número finito de elementos $a_1, a_2, \ldots, a_n$, entonces el ideal generado por S lo denotamos por $(a_1, a_2, \ldots, a_n)$ en lugar de $(\{a_1, a_2, \ldots, a_n\})$. Además, decimos que éste es **finitamente generado** y sus generadores son los elementos a_i para $i = 1, 2, \ldots, n$. Notemos que en particular R es un ideal de sí mismo. De donde decir que R es finitamente generado es considerar a R como ideal finitamente generado, es decir $R = (a_1, a_2, \ldots, a_n)$. Además si R es un anillo con uno, R es generado por 1_R. Un ideal (a) generado por un sólo elemento de R se dice que es un **ideal principal**.

Observación y definición 1.2.8. Ahora tomemos el ideal principal derecho generado por a el cual denotamos por $(a)_d$ y es el conjunto

$$(a)_d = \bigcap \{I : a \in I \text{ con } I \text{ ideal derecho de } R\}.$$

Nos gustaría describir quiénes son los elementos de este ideal. Para esto tomemos $a \in I$, con I un ideal derecho de R. Como $(I,+)$ es un subgrupo de $(R,+)$ y $a \in (I,+)$ tenemos que $na \in (I,+)$ para toda $n \in \mathbb{Z}$. Además, dado que I es un ideal derecho para toda $r \in R$ tenemos que $ar \in R$.

Veamos que $A = \{na + ar : n \in \mathbb{Z}, r \in R\} = (a)_d = \bigcap\{I : a \in I \text{ con } I \text{ ideal derecho de } R\}$. Es claro que A es un ideal derecho de R tal que contiene a a, pues $a = 1a + a0$. Así $(a)_d \subseteq A$. Mostremos la otra contención. Sea $ma + ar \in A$, para cada I ideal derecho que contiene a a tenemos que $ar \in I$. Además como cada ideal derecho que contiene a a es un grupo tenemos que $ma \in I$. Así, $ma + ar \in I$ para cada ideal derecho que contenga a a. Por tanto $ma + ar \in (a)_d$. En conclusión, definimos al ideal derecho principal generado por a como el conjunto

$$(a)_d = \{na + ar : n \in \mathbb{Z}, r \in R\}.$$

Notemos que en general $\{ar : r \in R\} \neq (a)_d$ pues no podemos garantizar que a pertenezca a $\{ar : r \in R\}$. Si R es un anillo con uno, podemos escribir la expresión $na + ar \in (a)_d$ como sigue

$$na + ar = n(1_R a) + ar = (n1_R)a + ar = a(n1_R) + ar = a(n1_R + r) = ar',$$

donde $r' = n1_R + r$ es algún elemento de R. Esto es, el conjunto $(a)_d$ consta de todos los múltiplos derechos de a por elementos de R. Si R es un anillo con uno, denotamos por aR en lugar de $(a)_d$; es decir,

$$(a)_d = aR = \{ar : r \in R\}.$$

Usamos argumentos similares para demostrar que el ideal izquierdo principal generado por a es el conjunto

$$(a)_i = \{na + ra : n \in \mathbb{Z}, r \in R\}.$$

Además, si R es un anillo con uno, tenemos que el ideal izquierdo principal generado por a lo denotamos por Ra y es el conjunto

$$(a)_i = \{ra : r \in R\}.$$

Con respecto a los ideales bilaterales generados por un elemento a es un poco más complicado describir este conjunto. Es claro que los elementos ras, ra, as y na deben pertenecer al ideal (a) para $r, s \in R$ y $n \in \mathbb{Z}$. En general, la suma de dos elementos $ras, r'as'$ no es de la misma forma, por lo que, para tener un cierre bajo la suma, cualquier suma finita $\sum r_i a s_i$ con $r_i, s_i \in R$, debe pertenecer a (a). Por tanto, el ideal principal generado por a es el conjunto

$$(a) = \{na + ra + as + \sum_{\text{finita}} r_i a s_i : r, s, r_i, s_i \in R; n \in \mathbb{Z}\}.$$

En el caso de que R sea un anillo con uno, este conjunto se reduce a todas las sumas finitas $\sum r_i a s_i$ con $r_i, s_i \in R$. Además, de estas observaciones, si R es un anillo conmutativo con uno, el ideal generado por a es el conjunto

$$(a) = \{ar : r \in R\} = \{ra : r \in R\}.$$

Ejemplo 1.2.9. Veamos ahora algunos ejemplos.

1. Consideremos el anillo de los números enteros. Sea $n\mathbb{Z}$ (ver 1.1.13), este es un ideal principal, de hecho es el ideal generado por $n \in \mathbb{Z}$. Esto es

$$n\mathbb{Z} = (n) = \{na : a \in \mathbb{Z}\}$$

2. Consideremos el anillo conmutativo $2\mathbb{Z}$. Sea $(2) \subseteq 2\mathbb{Z}$, el ideal generado por 2. Como $2\mathbb{Z}$ es un anillo que no tiene uno, tenemos que

$$(2) \neq \{2n : n \in 2\mathbb{Z}\} = 4\mathbb{Z}.$$

De hecho, de la observación y definición 1.2.8 tenemos que

$$(2) = \{2n + 2r : n \in \mathbb{Z}, r \in 2\mathbb{Z}\}.$$

Más aún, $\{2n+2r : n \in \mathbb{Z}, r \in 2\mathbb{Z}\} = \{2(n+r) : n \in \mathbb{Z}, r \in 2\mathbb{Z}\}$. Como $2(n+r)$ resulta ser siempre un múltiplo de dos, podemos escribir este conjunto como sigue

$$\{2n + 2r : n \in \mathbb{Z}, r \in 2\mathbb{Z}\} = \{2(n + r) : n \in \mathbb{Z}, r \in 2\mathbb{Z}\} = \{2k : k \in \mathbb{Z}\} = 2\mathbb{Z}.$$

3. Consideremos el anillo conmutativo con uno de los polinomios en una variable sobre los números enteros $\mathbb{Z}[x]$. Veamos que el ideal $(2, x)$ no es un ideal principal. Supongamos que sí lo es, es decir existe $p(x) \in \mathbb{Z}[x]$ tal que $(2, x) = (p(x))$. Por lo tanto, $2 \in (p(x))$ y $x \in (p(x))$, es decir existen $t_1(x), t_2(x) \in \mathbb{Z}[x]$ tales que

$$\begin{aligned} 2 &= t_1(x)p(x) \\ x &= t_2(x)p(x). \end{aligned}$$

Esto quiere decir que $0 = \text{gr}(2) = \text{gr}(t_1(x)) + \text{gr}(p(x))$. Por lo tanto, $t_1(x)$ es una constante y $p(x)$ es constante. Esto es $t_1(x) = \pm 1$ y $p(x) = \pm 2$ o $t_1(x) = \pm 2$ y $p(x) = \pm 1$. Supongamos sin pérdida de generalidad que $t_1(x) = 1$ y $p(x) = 2$. Entonces $x = t_2(x)2$ de donde $t_2(x) = \frac{1}{2}x$ pero esto no es posible. Ahora si $t_1(x) = 2$ y $p(x) = 1$ entonces $(2, x) = (p(x)) = \mathbb{Z}[x]$, sin embargo esto tampoco es posible pues $(2, x)$ es un ideal propio. Por lo tanto, $(2, x)$ no es un ideal principal.

Ahora veamos una definición de anillos particulares que utilizaremos a lo largo de esta tesis.

Definición 1.2.10. Sea R un anillo.

1. Decimos que R es un anillo de ideales principales si cada ideal I de R es de la forma $I = (a)$ para algún $a \in R$.

2. Si R es un dominio entero tal que es un anillo de ideales principales, decimos que R es un dominio de ideales principales.

Veamos ahora un ejemplo importante de un anillo tal que es un dominio ideales principales. En el Capítulo 2. veremos más ejemplos de dominios de ideales principales.

Teorema 1.2.11. *El dominio entero $\mathbb{Z}$ es un dominio de ideales principales. De hecho, si I es un ideal de $\mathbb{Z}$ entonces $I = (n)$ para algún entero no negativo n.*

Demostración. Sea I un ideal del dominio entero $\mathbb{Z}$.

1. Si $I = \{0\}$, entonces este es el ideal principal generado por 0, es decir, para este caso $n = 0$.

2. Supongamos ahora que $I \neq 0$. Entonces, existe $0 \neq k \in I$ y $-k \in I$ ya que $-k = (-1)k$ e I es un ideal. De donde, el ideal I tiene números enteros positivos. Sea $n \in I$ el menor entero positivo tal que $n \in I$. Veamos que $I = (n)$. Es claro que $(n) \subseteq I$ ya que $n \in I$ e I es un ideal de $\mathbb{Z}$. Mostremos que $I \subseteq (n)$. Sea $a \in I$, por el algoritmo de la división tenemos que $a = nq + r$, con $0 \leq r < n$. Como $a, nq \in I$, se sigue que $a - nq = r \in I$. Si $r > 0$ tenemos una contradicción al hecho de que n es el entero positivo más pequeño en I. Por tanto, $r = 0$ y $a = nq \in (n)$. Así, $I \subseteq (n)$.

□

Concluimos la sección con la siguiente definición, ésta nos habla de dos operaciones que podemos realizar con los ideales de un anillo.

Definición 1.2.12. Sea R un anillo y J, I ideales de R.

1. Definimos la suma de I y J como el conjunto

$$I + J = \{a + b : a \in I, b \in J\}$$

2. Definimos el producto de I y J como el conjunto

$$IJ = \{ \sum_{finita} a_i b_i : a_i \in I, b_i \in J\}$$

1.3. Ideales primos y maximales

En esta sección vamos a estudiar dos tipos de ideales, los ideales maximales y primos. Comenzamos con la definición de ideal maximal. Luego, mencionamos un famoso resultado, el lema de Zorn, éste lo usamos para probar un teorema muy importante el cual nos dice que si R es un anillo finitamente generado entonces cada ideal propio de R está contenido en un ideal maximal. Finalizamos esta sección con la definición de un ideal primo y algunos ejemplos de éstos.

A lo largo de esta sección supondremos siempre, a menos que se diga lo contrario que R es un **anillo conmutativo con uno**. Por comodidad algunas veces escribiremos que R es un anillo.

Definición 1.3.1. Sea R un anillo conmutativo con uno. Un ideal I de R es un ideal maximal si

1. $I \neq R$

2. para cada ideal J de R tal que $I \subset J \subseteq R$, entonces $J = R$.

Expresado de manera un tanto vaga, un ideal es maximal si no es todo el anillo y no está contenido propiamente en ningún ideal propio más grande, es decir, el único ideal que puede contener a un ideal maximal es el anillo R y el mismo ideal.

Ejemplo 1.3.2. Veamos un ejemplo.

1. Consideremos a los números enteros $\mathbb{Z}$. Veamos que los ideales maximales de $\mathbb{Z}$ corresponden a los ideales generados por los números primos. Sea $n \in \mathbb{Z}$ tal que $n > 1$. Entonces (n) es maximal si, y sólo si n es primo.

   Supongamos que (n) es un ideal maximal de $\mathbb{Z}$ y que n no es un primo. Entonces, $n = n_1 n_2$ con $n_1, n_2 \in \mathbb{Z}$ tales que $1 < n_1 < n_2 < n$. Esto implica que los ideales (n_1) y (n_2) son tales que

   $$(n) \subset (n_1) \subset \mathbb{Z}, \qquad (n) \subset (n_2) \subset \mathbb{Z},$$

   lo cual es una contradicción al hecho de que (n) es maximal.

   Supongamos ahora que n es primo y que el ideal (n) no es maximal en $\mathbb{Z}$. Esto es, $(n) = \mathbb{Z}$ o bien existe otro ideal (m) tal que $(n) \subset (m) \subset \mathbb{Z}$. El primer caso no puede ocurrir ya que 1 no es un múltiplo de ningún número primo. Así, $(n) \subset (m)$, de donde $n = mk$ para algún $k \in \mathbb{Z}$ con $k > 1$. Sin embargo, esta igualdad no es posible ya que n es primo y por tanto no es un número compuesto. Por lo tanto, (n) es un ideal maximal.

En general, no es sencillo demostrar que un ideal I de un anillo conmutativo con uno R es maximal por medio de la definición. Para continuar, nuestro objetivo inmediato es obtener un resultado general suponiendo la existencia de muchos ideales maximales. Como se verá más adelante, el paso crucial en la demostración depende del lema de Zorn. Comenzamos recordando algunas definiciones para poder anunciar el lema de Zorn y otro lema.

Definición 1.3.3. Sea A un conjunto distinto del vacío. Un orden parcial sobre A es una relación $\leq$ sobre A que satisface lo siguiente

1. es reflexiva, esto es para cada $x \in A$ se tiene que $x \leq x$,
2. es antisimétrica, es decir para cualesquiera $x, y \in A$ tales que $x \leq y$ y $y \leq x$ entonces $x = y$,
3. es transitiva, esto es para cualesquiera $x, y, z \in A$ si $x \leq y$ y $y \leq z$ entonces $x \leq z$.

Definición 1.3.4. Un elemento maximal de A es un elemento $m \in A$ tal que si $m \leq x$ para algún $x \in A$ entonces $m = x$.

Definición 1.3.5. Sea $\emptyset \neq A$ un conjunto con un orden parcial $\leq$. Entonces

1. Un subconjunto B de A es una cadena si para todo $x, y \in B$ se tiene que $x \leq y$ ó $y \leq x$.
2. Una cota superior para $B \subseteq A$ es un elemento $u \in A$ tal que $b \leq u$ para todo $b \in B$.

Con estas definiciones ya podemos enunciar el lema de Zorn.

Lema de Zorn 1.3.6. *Si $\emptyset \neq A$ es un conjunto parcialmente ordenado en el cual toda cadena tiene una cota superior en A. Entonces A tiene al menos un elemento maximal.*

Consideremos ahora a A como una familia de subconjuntos de un conjunto dado y el orden parcial la relación de contención. Entonces tenemos el siguiente Lema.

Lema 1.3.7. *Sea $\mathcal{A}$ una familia no vacía de subconjuntos de un conjunto no vacío X tal que para cada cadena $\mathcal{C}$ en $\mathcal{A}$, la unión $\cup\mathcal{C}$ también pertenece a $\mathcal{A}$. Entonces $\mathcal{A}$ contiene un conjunto que es maximal en el sentido de que no está propiamente contenido en otro miembro de $\mathcal{A}$.*

Veamos que el Lema de Zorn implica este lema. Para poder usar el Lema de Zorn, basta mostrar que cada cadena en la familia $\mathcal{A}$ tiene una cota superior en $\mathcal{A}$. En efecto, supongamos que el Lema de Zorn se satisface y que si $\mathcal{A} = \{A_i\}_{i\in I}$ es una familia no vacía de subconjuntos de un conjunto (fijo) no vacío X. Además supongamos que para cada cadena $\mathcal{C}$ en $\mathcal{A}$, la unión $\cup\mathcal{C}$ también pertenece a $\mathcal{A}$. Veamos que $\mathcal{A}$ tiene un elemento maximal.

Afirmamos que $\bigcup_{A_i\in\mathcal{C}} A_i$ es una cota superior. En efecto, si $A_i \in \mathcal{C}$ tenemos que $A_i \subseteq \bigcup_{A_i\in\mathcal{C}} A_i$. Además como por hipótesis $\bigcup_{A_i\in\mathcal{C}} A_i \in \mathcal{A}$. De donde, $\bigcup_{A_i\in\mathcal{C}} A_i$ es una cota superior en $\mathcal{A}$. Por lo tanto por el Lema de Zorn $\mathcal{A}$ posee al menos un elemento maximal.

Ahora ya podemos anunciar y demostrar el siguiente teorema.

Teorema 1.3.8. *Sea R un anillo finitamente generado. Entonces cada ideal propio de R está contenido en un ideal maximal.*

Demostración. Sea R un anillo finitamente generado, esto es $R = (a_1, a_2, \ldots, a_n)$ e I un ideal propio de R. Consideremos la siguiente familia de ideales de R

$$\mathcal{A} = \{J : I \subseteq J \text{ y } J \text{ es un ideal propio de } R\}.$$

Esta familia es distinta del vacío ya que $I \in \mathcal{A}$. Ahora consideremos una cadena arbitraria $\{I_i\} = \mathcal{C}$ de ideales en $\mathcal{A}$ y $J = \bigcup_{I_s\in\mathcal{C}} I_s$. Veamos que J es una cota superior de la cadena $\mathcal{C}$ en $\mathcal{A}$.

Primero mostremos que J es un elemento de la familia $\mathcal{A}$. Esto es, mostremos que J es un ideal propio de R.

1. Notemos que $J \neq \emptyset$, ya que para cada $I_m \in \mathcal{C}$ tenemos que $0_R \in I_m$. Así, $0_R \in J$.

2. Veamos ahora que J es un ideal de R. Sean $a, b \in J$. Entonces, exiten $I_k, I_j \in \mathcal{C}$ tales que $a \in I_k$ y $b \in I_j$. Luego como $\mathcal{C}$ es una cadena tenemos que $I_k \subseteq I_j$ o bien $I_j \subseteq I_k$, sin pérdida de generalidad podemos suponer que $I_j \subseteq I_k$. Por lo tanto, $a, b \in I_k$ luego como I_k es un ideal tenemos que $a - b \in I_k \subseteq \bigcup_{I_s\in\mathcal{C}} I_s$. Además, los productos ra y $ar \in I_k \subseteq \bigcup_{I_s\in\mathcal{C}} I_s$. Por tanto, $\bigcup_{I_s\in\mathcal{C}} I_s = J$ es un ideal de R.

3. Ahora mostremos que J es un ideal propio de R. Para esto supongamos lo contrario, esto es $\bigcup_{I_s\in\mathcal{C}} I_s = J = R = (a_1, a_2, \ldots, a_n)$. Entonces, cada generador a_k pertenece a algún ideal I_k de la cadena $\{I_i\}$. Como son un número finito y $\{I_i\}$ es una cadena, existe un I_n tal que contiene a todos estos. Por lo tanto, $a_1, a_2, \ldots, a_n \in I_n$ pertenecen a I_n. En consecuencia, $I_n = R$ pero esto es una contradicción ya que I_n es un ideal propio. Por último, notemos que $I \subseteq J$ ya que $I \subseteq I_s$ para cada $I_s \in \mathcal{C}$. Así $J \in \mathcal{A}$.

   Por último J es una cota superior de $\mathcal{C}$ ya que si $I_t \in \mathcal{C}$ tenemos que $I_t \subseteq J = \bigcup_{I_s\in\mathcal{C}} I_s$.

   Así por el lema de Zorn, la familia $\mathcal{A}$ tiene al menos un elemento maximal M en $\mathcal{A}$. Se sigue de la definición de $\mathcal{A}$ que M es un ideal propio del anillo R tal que $I \subseteq M$. Afirmamos que M es un ideal maximal. Para ver esto, supongamos que K es un ideal de R tal que $M \subset K \subseteq R$. Como M es un elemento maximal de $\mathcal{A}$ entonces J no puede pertenecer a $\mathcal{A}$. Por consecuencia, el ideal J no es un ideal propio de R, es decir $J = R$. Concluimos que M es un ideal maximal de R tal que $I \subset M$.

□

El ideal maximal M que encontramos no necesariamente es único, veamos este hecho con el siguiente ejemplo.

Ejemplo 1.3.9. Consideremos el anillo finitamente generado de los números enteros $\mathbb{Z}$. Sea $0 \neq a \in \mathbb{Z}$ no invertible. Por el Teorema de Fundamental de la Aritmética tenemos que existen $p_1, p_2, \ldots, p_k \in \mathbb{Z}$ números primos tales que $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Tomemos sin pérdida de generalidad al número primo p_1. Es claro que $a \in (p_1)$. Además (p_1) es maximal ya que p_1 es primo. Así $(a) \subseteq (p_1)$ con (p_1) ideal maximal. De hecho $(a) \subseteq (p_i)$ para cada p_i en la factorización de a, es decir el ideal maximal que contiene al ideal generado por a no es único.

Para finalizar esta sección, damos la definición de un ideal primo y algunos ejemplos. Antes de definir formalmente estos ideales, consideremos el anillo de los números enteros. Tomemos el ideal principal (p) generado por un número primo $p \in \mathbb{Z}$. Si el producto $ab \in (p)$ con $a, b \in \mathbb{Z}$, entonces $p \mid ab$. Pero si un número primo divide a un producto, entonces necesariamente divide a uno de los factores. Es decir en este caso, $a \in (p)$ o $b \in (p)$. Por lo tanto, el ideal (p) tiene una propiedad interesante; cuando (p) contiene un producto, al menos uno de los factores debe pertenecer a (p). Esta observación sirve para sugerir y en parte para ilustrar la siguiente definición.

Definición 1.3.10. Sea R un anillo e I un ideal de R. Decimos que I es un ideal primo si para toda $a, b \in R$ tales que $ab \in I$ implica que $a \in I$ o $b \in I$.

Por inducción se puede mostrar que la definición 1.3.10 puede ser extendida a una cantidad finita de elementos: esto es un ideal I de R es primo si, cada que un producto $a_1 a_2 \ldots a_n$ de elementos de R pertenezca a I, entonces al menos un $a_i \in I$.

Ejemplo 1.3.11. Para dar por terminada esta sección veamos algunos ejemplos de ideales primos.

1. Consideremos un anillo cualquiera R. Entonces el ideal R es un ideal primo.

2. Sea R un anillo conmutativo con uno. Entonces R es un dominio entero si, y sólo si el ideal (0) es un ideal primo de R.

3. Consideremos el anillo de los números enteros $\mathbb{Z}$. Los ideales primos de $\mathbb{Z}$ son los ideales (n) donde n es un número primo, y los ideales (0) y $\mathbb{Z}$. Consideremos ahora el ideal (n) tal que n es compuesto $(n \neq 0, 1)$, esto es $n = n_1 n_2$, donde $1 < n_1, n_2 < n$. Indudablemente $n_1 n_2 = n \in (n)$. Sin embargo, como n_1 y n_2 no son múltiplos enteros de n, $n_1 \notin (n)$ y $n_2 \notin (n)$. Por lo tanto, cuando n es un número compuesto, el ideal (n) no es primo. Además notemos que el ideal (0) que es un ideal primo, no es un ideal maximal de $\mathbb{Z}$ ya que para todo ideal (n), con $n \neq 0$ tenemos que $(0) \subset (n)$. Por lo tanto no todo ideal primo es un ideal maximal.

Capítulo 2

Teoría de divisibilidad en dominios enteros

2.1. Máximo común divisor y mínimo común múltiplo

En el presente capítulo estudiaremos el concepto de divisibilidad en anillos conmutativos con uno. Veremos que varias de las propiedades con respecto a la divisibilidad en el anillo $\mathbb{Z}$ de los números enteros, se pueden generalizar a anillos conmutativos con uno.

Como recordaremos de los cursos básicos de álgebra, al definir la relación de divisibilidad definíamos un máximo común divisor. Para esto nosotros usábamos que $\mathbb{Z}$ era un conjunto ordenado sin embargo en un anillo conmutativo con uno cualquiera no tenemos necesariamente una relación de orden. Por lo cual daremos una definición alternativa. Esta definición será válida en el anillo de los números enteros pero nos permitirá trabajar de manera más general, permitiendo, en particular, máximos comunes divisores negativos.

Luego, caracterizaremos el concepto de un máximo común divisor y la existencia de éste. Veremos en el ejemplo 2.1.19 que no siempre tendremos la existencia de un máximo común divisor. También mostraremos que los ideales principales y el concepto de un máximo común divisor están estrechamente ligados.

Para abarcar más ejemplos definiremos algunos conceptos que retomaremos en la sección 2.6. Estas definiciones nos ayudarán a asimilar más el corolario 2.1.20. En este corolario caracterizamos los anillos conmutativos con uno en los que podemos garantizar la existencia de un máximo común divisor. Finalizaremos esta sección estableciendo la definición de primos relativos en un anillo conmutativo con uno y con un teorema sobre éstos.

En este capítulo supondremos siempre, a menos que digamos lo contrario, que R **es un anillo conmutativo con uno**. Por comodidad, algunas veces sólo escribiremos que R es un anillo.

Definición 2.1.1. Sean R un anillo conmutativo con uno y $0 \neq a$, b elementos de R. Decimos que a divide a b, si existe algún $c \in R$ tal que $b = ac$.

Notación 2.1.2. Denotamos la relación a divide a b con el símbolo $a \mid b$, en el caso de que a no divida a b lo denotamos como $a \nmid b$.

Podemos decir de otra forma que $a \mid b$ diciendo que a es *factor* de b, b es *divisible* por a o bien que b es *múltiplo* de a. Siempre que usemos la notación $a \mid b$ se entenderá que $a \neq 0$ aún cuando no se mencione. Note que si $b = 0$ siempre tendremos que $a \mid 0$ pues $0 = a0$ para todo $a \in R$.

Ejemplo 2.1.3. Veamos los siguientes ejemplos.

1. Consideremos el anillo conmutativo con uno de los números enteros $\mathbb{Z}$. Podemos tomar los enteros 6 y 9. Note que $6 \nmid 9$ pues no hay un entero $c \in \mathbb{Z}$ tal que $9 = 6c$. Por otra parte $3 \mid 6$ y $3 \mid 9$ pues existen los enteros 2 y $3 \in \mathbb{Z}$ tal que $6 = 3 \cdot 2$ y $9 = 3 \cdot 3$.

2. Consideremos $\mathbb{C}[x]$ el anillo de los polinomios en una variable sobre los números complejos. Sean $x^2 - 1$ y $x + 1 \in \mathbb{C}[x]$. Notemos que $(x + 1) \mid (x^2 - 1)$ pues existe $x - 1 \in \mathbb{C}[x]$ tal que $x^2 - 1 = (x + 1)(x - 1)$.

Ahora veamos un lema para generalizar varias de las propiedades que nosotros teníamos en el anillo de los números enteros $\mathbb{Z}$ respecto a la divisibilidad, pero ahora en un anillo conmutativo con uno.

Lema 2.1.4. *Sean R un anillo conmutativo con uno y a, b, c elementos de R. Entonces,*

1. $a \mid 0, 1 \mid a, a \mid a$;
2. $a \mid 1$ *si, y sólo si a es invertible;*
3. *si $a \mid b$, entonces $ac \mid bc$;*
4. *si $a \mid b$ y $b \mid c$, entonces $a \mid c$;*
5. *si $c \mid a$ y $c \mid b$ entonces $c \mid (ax + by)$ para todo x y y en R.*

Demostración. Sean $a, b, c \in R$

1. Veamos que $a \mid 0, 1 \mid a, a \mid a$. Por el teorema 1.1.18 sabemos que $0 = 0a$ asi tenemos que $a \mid 0$. Por el mismo teorema, sabemos que $a = 1 \cdot a$ de donde $1 \mid a$ y $a \mid a$.

2. Mostremos que $a \mid 1$ si, y sólo si a es invertible. Como $a \mid 1$ esto pasa si, y sólo si existe $c \in R$ tal que $1 = ac$ por la definición 1.1.8 tenemos que a es invertible.

3. Veamos ahora que si $a \mid b$ entonces $ac \mid bc$. Como $a \mid b$ entonces existe $r \in R$ tal que $b = ar$ multiplicando esta igualdad por c a ambos lados tenemos que $bc = (ar)c = (ac)r$ de donde $ac \mid bc$.

4. Supongamos ahora que si $a \mid b$ y $b \mid c$. Veamos que $a \mid c$. Como $a \mid b$ y $b \mid c$ entonces existen $r_1, r_2 \in R$ tales que $b = ar_1$ y $c = br_2$. Multiplicando la primera igualdad por r_2 tenemos que $br_2 = (ar_1)r_2$ de donde $c = a(r_1r_2)$ con $r_1r_2 \in R$. Es decir $a \mid c$.

5. Supongamos que $c \mid a$ y $c \mid b$. Esto es, existen $r_1, r_2 \in R$ tales que $a = cr_1$ y $b = cr_2$. Sean x, y elementos cualesquiera de R entonces multiplicando la primera igualdad por x y la segunda igualdad por y tenemos que $ax = c(r_1x), by = c(r_2y)$. Sumando estas igualdades y usando la propiedad distributiva de R obtenemos que $ax + by = c(r_1x + r_2y)$ donde $r_1x + r_2y \in R$. Por lo que $c \mid (ax + by)$ para cualesquiera $x, y \in R$.

□

Consideremos ahora los ideales generados por un elemento a y b en R. Como R es un anillo conmutativo con uno, por la observación y definición 1.2.8 tenemos que $(a) = \{ar_1 : r_1 \in R\}$ y $(b) = \{br_2 : r_2 \in R\}$. Queremos analizar cómo se relacionan estos ideales respectivamente si tenemos que $a \mid b$. Para esto enunciaremos el siguiente lema.

Lema 2.1.5. *Sean R un anillo conmutativo con uno y a, b elementos de R. Entonces $a \mid b$ si, y sólo si $(b) \subseteq (a)$.*

Demostración. Sean $a, b \in R$. Supongamos que $a \mid b$ esto es existe $c \in R$ tal que $b = ac$ de donde $b \in (a)$, por lo que $(b) \subseteq (a)$.

Veamos ahora que si $(b) \subseteq (a)$ entonces $a \mid b$. Como $(b) \subseteq (a)$. entonces $b \in (a)$ de donde existe $c_1 \in R$ tal que $b = ac_1$ por lo que $a \mid b$. □

Ejemplo 2.1.6. Veamos los siguiente ejemplos.

1. En los números enteros $\mathbb{Z}$. Sabemos que $3 \mid 6$ pues $6 = 3 \cdot 2$. Además como $\mathbb{Z}$ es un anillo conmutativo con uno entonces $(3) = \{3z : z \in \mathbb{Z}\}$ y $(6) = \{6z_2 : z_2 \in \mathbb{Z}\}$. Como $6 = 3 \cdot 2$ entonces $6 \in (3)$ de donde $(6) \subseteq (3)$.

2. Del ejemplo 2.1.3 sabemos que $x + 1 \mid x^2 - 1$ en $\mathbb{C}[x]$, esto es $x^2 - 1 = p(x)(x + 1)$ para algun $p(x) \in \mathbb{C}[x]$ por lo que $(x^2 - 1) \subseteq (x + 1)$.

Al hacernos preguntas que tienen que ver con la divisivibilidad, éstas pueden ser muy complicadas cuando tenemos elementos invertibles. Por ejemplo, si u es un elemento invertible de un anillo conmutativo con uno R, entonces para cada $a \in R$ tenemos que $a = a(uu^{-1})$ de donde $u \mid a$ y $u^{-1} \mid a$, esto es cada elemento invertible divide a cualquier elemento de R. Una situación extrema ocurre cuando tenemos elementos de un campo. Aquí cada elemento no cero a divide a cualquier otro elemento b, pues como a es no cero entonces existe a^{-1} de donde $b = b(aa^{-1})$. Sin embargo en el anillo $2\mathbb{Z}$ el elemento 2 no tiene ningún divisor pues no hay enteros $c, z \in \mathbb{Z}$ tal que $2 = cz$.

Por estas dificultades a continuación definimos lo que es un elemento *asociado*.

Definición 2.1.7. Sea R un anillo conmutativo con uno, decimos que a y b en R son *elementos asociados* o simplemente que son *asociados* si $a = bu$, con u elemento invertible en R.

Observación 2.1.8. La relación $\sim$ definida en R por $a \sim b$ si, y sólo si a es asociado de b, es una relación de equivalencia. Veamos quiénes son las clases de equivalencia. Sea $a \in R$, la clase de equivalencia de a es el conjunto

$$[\ a\ ] = \{b \in R : a \text{ es asociado de } b\} = \{b \in R : a = bu, \text{ con } u \in R \text{ invertible}\}.$$

Es decir, la clase de equivalencia de a consta de todos los elementos $b \in R$ que son asociados de a. Dicho esto, la clase de equivalencia de la identidad es el conjunto

$$[1] = \{b \in R : 1 = bu, \text{ con } u \in R \text{ invertible}\} = \{b \in R : u^{-1} = b, \text{ con } u \in R \text{ invertible}\}.$$

Es decir, la clase de la identidad consta de todos los elementos invertibles del anillo R.

Ejemplo 2.1.9. Veamos algunos ejemplos

1. En el caso del conjunto de los números enteros $\mathbb{Z}$, los únicos asociados de un elemento $n \in \mathbb{Z}$ son $\pm n$. Pues ± 1 son los únicos elementos invertibles en $\mathbb{Z}$.

2. Tomemos el campo de los números racionales $\mathbb{Q}$ y sean $a, b \in \mathbb{Q}$ elementos no nulos. Como $\mathbb{Q}$ es un campo sabemos que cada elemento distinto de cero es invertible, además notemos que podemos expresar a como $a = b(\frac{a}{b})$ donde $\frac{a}{b} \neq 0$ es un elemento invertible, así cualesquiera dos elementos no nulos en $\mathbb{Q}$ son asociados.

3. Consideremos el dominio de los enteros gaussianos, $\mathbb{Z}[i]$

   $$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\}.$$

   Mostremos que en $\mathbb{Z}[i]$ los únicos elementos invertibles son ± 1 y $\pm i$. Supongamos que $a + bi \in \mathbb{Z}[i]$ tiene un inverso multiplicativo $c + di$. De donde $(a + bi)(c + di) = 1$ y de ésta usando el conjungado en los números complejos tenemos que $\overline{(a + bi)(c + di)} = \overline{1}$ es decir $(a - bi)(c - di) = 1$. Por tanto,

   $$1 = (a + bi)(c + di)(a - bi)(c - di) = (a^2 + b^2)(c^2 + d^2)$$

   Como a, b, c, d son enteros tenemos que $a^2 + b^2 = 1$ de donde $a = \pm 1$ y $b = 0$, o $a = 0$ y $b = \pm 1$. De donde sólo tenemos cuatro elementos invertibles ± 1, $\pm i$.

Ahora veamos un resultado que relaciona los elementos asociados con las propiedades de divisibilidad y éstos con los ideales principales.

Teorema 2.1.10. *Sean R un dominio entero, $a, b \in R$ tales que $a \neq 0$ y $b \neq 0$. Entonces los siguientes enunciados son equivalentes:*

1. *a y b son asociados,*
2. *$a \mid b$ y $b \mid a$,*
3. *$(a) = (b)$.*

Demostración. Sean a y b elementos no cero de R. Veamos que 1. implica 2. Supongamos que a y b son asociados, esto es existe $u \in R$ elemento invertible tal que $a = bu$ de donde $b \mid a$. Como u es invertible podemos multiplicar por su inverso u^{-1} a ambos lados de $a = bu$, así tenemos que $au^{-1} = b$ de donde $a \mid b$. Por tanto $a \mid b$ y $b \mid a$.

Veamos que 2. implica 1. Supongamos que $a \mid b$ y $b \mid a$, esto es existen $r_1, r_2 \in R$ tales que $b = ar_1$ y $a = br_2$ así $b = ar_1 = b(r_2 r_1)$. Como $b \neq 0$ por la ley de la cancelación tenemos que $r_2 r_1 = 1$, de donde r_1 es un elemento invertible de R tal que $b = ar_1$. Por lo que a y b son asociados.

Para ver que 2. si, y sólo si 3., por el lema 2.1.5 sabemos que $a \mid b$ y $b \mid a$ si, y sólo si $(b) \subseteq (a)$ y $(a) \subseteq (b)$, es decir, $(a) = (b)$. □

Ejemplo 2.1.11. Veamos los siguientes ejemplos.

1. Consideremos el anillo de los números enteros $\mathbb{Z}$. Sabemos que 5 y -5 son asociados ya que $5 = -5(-1)$ con -1 unidad en $\mathbb{Z}$.

   De donde $-5 \mid 5$. Además $-5 = 5(-1)$ de donde $5 \mid -5$. Por otro lado, sabemos que $(5) = \{5r : r \in \mathbb{Z}\} = \{(-5)s : s \in \mathbb{Z}\} = (5)$ (ver 1.2.8).

2. Consideremos el anillo de los polinomios en una variable sobre los complejos $\mathbb{C}[x]$, y sean $x+1, x^3+2x^2+3x+2 \in \mathbb{C}[x]$. Notemos que $x+1 \mid x^3+2x^2+3x+2$ pues existe $x^2+x+2 \in \mathbb{C}[x]$ tal que $x^3+2x^2+3x+2 = (x+1)(x^2+x+2)$. Pero $x^3+2x^2+3x+2 \nmid x+1$ ya que no existe $p(x) \in \mathbb{C}[x]$ tal que $(x^3+2x^2+3x+2)p(x) = x+1$, pues si existiera eso querría decir que $\text{gr}((x^3+2x^2+3x+2)p(x)) = \text{gr}(x+1)$ de donde $\text{gr}(x^3+2x^2+3x+2)+\text{gr}(p(x)) = \text{gr}(x+1)$ esto es $3+ \text{gr}(p(x)) = 1$ y como $\text{gr}(p(x)) \geq 0$ esto no es posible. De modo que los polinomios $x+1, x^3+2x^2+3x+2$ no son asociados.

   Dado que $x+1 \mid x^3+2x^2+3x+2$ entonces por el lema 2.1.5 tenemos que $(x^3+2x^2+3x+2) \subseteq (x+1)$. Como $x^3+2x^2+3x+2 \nmid x+1$ tenemos que $(x+1) \nsubseteq (x^3+2x^2+3x+2)$.

3. Consideremos el anillo de los enteros gaussianos $\mathbb{Z}[i]$. Sean $2+3i, -4+7i \in \mathbb{Z}[i]$. Notemos que $2+3i \mid -4+7i$ pues $(2+3i)(1+2i) = 2+3i+4i-6 = -4+7i$. Veamos que $-4+7i \nmid 2+3i$. Para esto supongamos lo contrario, esto es existe $a+bi \in \mathbb{Z}[i]$ tal que $2+3i = (a+bi)(-4+7i) = (-4a-7b)+(7a-4b)i$ de donde tenemos el siguiente sistema de ecuaciones

$$-4a - 7b = 2 \tag{2.1}$$
$$7a - 4b = 3. \tag{2.2}$$

   Multiplicando (2.1) por 7 y (2.2) por 4, y sumando ambas ecuaciones tenemos que $-65b = 26$ pero no hay un entero b tal que satisfaga esta condición. Por lo tanto $-4+7i \nmid 2+3i$. Así por el teorema anterior tenemos que $2+3i, -4+7i$ no son asociados.

Recordemos que en el anillo de los números enteros $\mathbb{Z}$ tenemos la definición de máximo común divisor. Queremos generalizar la definición de máximo común divisor a un dominio entero cualquiera. Por ello, necesitamos una definición donde no supongamos que el dominio entero tiene una relación de orden, pues no siempre tendremos dominios enteros ordenados (por ejemplo el dominio de los polinomios sobre el campo de los números complejos).

Definición 2.1.12. Sea R un anillo conmutativo con uno y sean $a_1, a_2, \ldots a_n$ elementos no nulos de R. Un elemento $d \in R$ es un máximo común divisor de $a_1, a_2, \ldots a_n$ si satisface las siguientes propiedades

1. $d \mid a_i$ para $i = 1, \ldots, n$,
2. Si $c \mid a_i$ para $i = 1, \ldots, n$ entonces $c \mid d$.

Note que la propiedad 1. quiere decir que d es un divisor común, mientras que la propiedad 2. nos habla de que tiene que ser el divisor más grande, pero en el sentido de que si existe otro

divisor común c éste tiene que dividir a d, esto es no se hace referencia a un orden.

Observe que la definición anterior habla de **un máximo común divisor** por lo cual nos podemos preguntar si existe algún otro.

Ejemplo 2.1.13. Veamos los siguientes ejemplos.

1. Consideremos el dominio entero $\mathbb{Z}$. Tenemos que si d es un máximo común divisor de a y b, entonces $-d$ es también un máximo común divisor. Como $d \mid a$ entonces existe $t \in \mathbb{Z}$ tal que $a = dt$ de donde $a = -d(-t)$ con $-t \in \mathbb{Z}$, análogamente obtenemos que $-d \mid b$. Además si existe $c' \mid a$ y $c' \mid b$ entonces $c' \mid d$ y como $-d \mid d$ entonces por el lema 2.1.4 tenemos que $c' \mid -d$. Por lo tanto $-d$ es un máximo común divisor.

2. Consideremos el campo de los números racionales $\mathbb{Q}$ y sean $a, b \in \mathbb{Q}$. Afirmamos que cualquier $0 \neq q \in \mathbb{Q}$ es un máximo común divisor. Veamos que q es un divisor común, en efecto, como

$$a = q\left(\frac{a}{q}\right) \text{ tenemos que } q \mid a$$
$$b = q\left(\frac{b}{q}\right) \text{ tenemos que } q \mid b$$

   así q es un divisor común. Sea $q' \in \mathbb{Q}$ tal que $q' \mid a$ y $q' \mid b$ veamos que $q' \mid q$. En efecto, de hecho sin usar que q' es un divisor común podemos expresar a q en términos de q' esto es $q = q'\left(\frac{q}{q'}\right)$. Así para cada par de elementos no nulos en $\mathbb{Q}$ cualquier elemento no nulo de este anillo es un máximo común divisor. Por tanto tenemos tantos máximos comunes divisores como elementos no nulos en $\mathbb{Q}$.

3. Consideremos el dominio entero $\mathbb{C}[x]$. Supongamos que $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$. Veamos que para cada polinomio constante $0 \neq c \in \mathbb{C}[x]$ tenemos que $cd(x)$ es un máximo común divisor de $a(x)$ y $b(x)$.

   Como $d(x) \mid a(x)$ entonces $a(x) = d(x)t(x)$ para algún $t(x) \in \mathbb{C}[x]$ de donde $a(x) = c \cdot d(x)(c^{-1} \cdot t(x))$ como $\mathbb{C}$ es un campo entonces $cc^{-1} = 1$, de donde $c \cdot d(x) \mid a(x)$, análogamente $c \cdot d(x) \mid b(x)$. Además, si $c'(x) \in \mathbb{C}[x]$ es tal que divide a $a(x)$ y $b(x)$ como $d(x) \mid c \cdot d(x)$ por el lema 2.1.4 tenemos que $c'(x) \mid c \cdot d(x)$, de donde $c \cdot d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$. Así tenemos tantos máximos comunes divisores de dos polinomios como elementos no nulos de $\mathbb{C}$.

Observación 2.1.14. De los ejemplos anteriores podemos observar que si d es un máximo común divisor de a, b elementos de un anillo conmutativo con uno R, entonces se tiene que du con u unidad en R también es un máximo común divisor de a y b, y viceversa si d' es un máximo común divisor de a y b entonces $d' = du'$ con u' unidad en R. Es decir el máximo común divisor es único salvo elementos asociados.

Lo anterior motiva el siguiente resultado.

Lema 2.1.15. *Sea R un anillo conmutativo con uno y sean $a_1, a_2, \ldots, a_n$ elementos no nulos de R tales que existe un máximo común divisor d. Entonces éste es único (salvo elementos asociados).*

Demostración. Sean $a_1, a_2, \ldots, a_n$ elementos no nulos de R tales que d es un máximo común divisor. Supongamos que existe $d' \in R$ tal que es otro máximo común divisor de $a_1, a_2, \ldots, a_n$, de donde d' es tal que satisface 1. y 2. de la definición anterior. Entonces por 2. tenemos que $d \mid d'$ y $d' \mid d$, así por el teorema 2.1.10 tenemos que d y d' son asociados. □

Notación 2.1.16. Denotaremos a un máximo común divisor d de $a_1, a_2, \ldots, a_n$, cuando exista, como

$$d = \text{mcd}(a_1, \ldots, a_n)$$

Ejemplo 2.1.17. Veamos los siguientes ejemplos.

1. Consideremos el anillo de los números enteros $\mathbb{Z}$. Sean $3, 15 \in \mathbb{Z}$. Veamos que -3 es un máximo común divisor de 3 y 15. Notemos que $-3 \mid 3$ y $-3 \mid 15$ pues $3 = -3(-1)$ y $15 = -3(-5)$. Por tanto -3 es un divisor común de 3 y 15. Ahora observemos que los divisores comunes de 3 y 15 son $\{1, -1, 3, -3\}$ y que cada uno de estos divide a -3. Por tanto -3 es un máximo común divisor de 3 y 15.

2. Consideremos el anillo conmutativo con uno $\mathbb{C}[x]$ y los polinomios $x^5 - 32, x^3 - 8$. Usando el algoritmo de la división tenemos que:

$$x^5 - 32 = (x^3 - 8)x^2 + (8x^2 - 32) \text{ con } \text{gr}(8x^2 - 32) < \text{gr}(x^3 - 8).$$
$$x^3 - 8 = (8x^2 - 32)\frac{1}{8}x + (4x - 8) \text{ con } \text{gr}(4x - 8) < \text{gr}(8x^2 - 32)$$
$$8x^2 - 32 = (4x - 8)(2x + 4) \text{ con residuo igual a cero.}$$

   De donde $4x - 8$ es un máximo común divisor de $x^5 - 32$ y $x^3 - 8$, pues es el último residuo distinto de cero.

De la Teoría elemental del anillo de los números enteros $\mathbb{Z}$ y del anillo de los polinomios en una variable $F[x]$ donde F es un campo, sabemos que dados $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ o en $F[x]$ existe un máximo común divisor. Además en estos anillos un máximo común divisor se puede expresar como combinción lineal de $a_1, a_2, \ldots, a_n$. De donde nos preguntamos si dado un anillo R y elementos $a_1, a_2, \ldots, a_n \in R$ existirá un máximo común divisor que se puede expresar como combinación lineal de $a_1, a_2, \ldots, a_n$. El siguiente resultado nos da una respuesta.

Teorema 2.1.18. *Sean R un anillo conmutativo con uno y $a_1, a_2, \ldots, a_n$ elementos no nulos de R. Entonces $a_1, a_2, \ldots, a_n$ tienen un máximo común divisor que se puede expresar de la siguiente forma*

$$d = r_1 a_1 + \cdots + r_n a_n,$$

con $r_i \in R$ para $i = 1, \ldots, n$ si, y sólo si, el ideal $(a_1, \ldots, a_n)$ es principal.

Demostración. Sean $a_1, a_2, \ldots, a_n \in R$ tal que $a_i \neq 0$ para $i = 1, 2, \ldots n$. Supongamos que $d = \text{mcd}(a_1, a_2, \ldots, a_n)$ existe y puede ser escrito de la forma $d = r_1 a_1 + r_2 a_2 \cdots + r_n a_n$ con $r_i \in R$ $i = 1, 2, \ldots, n$.

Veamos que $(a_1, \ldots, a_n) = (d)$.

Como $d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, esto quiere decir que $d \in (a_1, a_2, \ldots, a_n)$ por lo cual $(d) \subseteq (a_1, a_2, \ldots, a_n)$. Ahora mostremos que $(a_1, a_2, \ldots, a_n) \subseteq (d)$. Como $d \mid a_i$ para $i = 1, 2, \ldots, n$, pues d es un máximo común divisor de $a_1, a_2, \ldots, a_n$ entonces $a_i = x_i d$ con $x_i \in R$, $i = 1, 2, \ldots, n$.

Sea $y_1 a_1 + y_2 a_2 \cdots + y_n a_n \in (a_1, \ldots, a_n)$ por lo anterior este elemento lo podemos expresar de la siguiente forma:

$$y_1a_1 + y_2a_2 + \cdots + y_na_n = y_1(x_1d) + y_2(x_2d)\cdots + y_n(x_nd) = (y_1x_1 + y_2x_2\cdots + y_nx_n)d$$

de donde $y_1a_1+y_2a_2+\cdots+y_na_n \in (d)$. Y por tanto $(a_1, a_2, \ldots, a_n) \subseteq (d)$ de donde $(a_1, a_2, \ldots, a_n) = (d)$.

Ahora supongamos que $(a_1, a_2, \ldots, a_n)$ es un ideal principal de R, esto es $(a_1, a_2 \ldots, a_n) = (d)$ con $d \in R$. Veamos que $d = \text{mcd}(a_1, a_2, \ldots, a_n)$. Como $(a_1, a_2, \ldots, a_n) = (d)$ entonces $a_i \in (d)$, $i = 1, 2, \ldots, n$. De donde existen elementos $b_i \in R$ tales que $a_i = b_id$ esto es $d \mid a_i$ para $i = 1, 2, \ldots, n$. Ahora supongamos que existe $c \in R$ tal que $c \mid a_i$, $i = 1, \ldots, n$, es decir, $a_i = s_ic$ con $s_i \in R$, $i = 1, 2, \ldots, n$.

Como $d \in (a_1, a_2, \ldots, a_n)$ entonces $d = r_1a_1+r_2a_2+\cdots+r_na_n$ con $r_i \in R$ para $i = 1, 2, \ldots, n$. Por lo anterior podemos escribir esta igualdad como sigue

$$d = r_1a_1 + r_2a_2 + \cdots + r_na_n = r_1(s_1c) + r_2(s_2c) + \cdots + r_n(s_nc) = (r_1s_1 + r_2s_2\cdots + r_ns_n)c$$

con $r_1s_1 + r_2s_2 + \cdots + r_ns_n \in R$ de donde $c \mid d$.

Así $d = \text{mcd}(a_1, a_2, \ldots, a_n)$ y $d = r_1a_1 + r_2a_2\cdots + r_na_n$ con $r_i \in R$ para $i = 1, 2, \ldots, n$. □

Veamos ahora un ejemplo.

Ejemplo 2.1.19. 1. En el anillo de los números enteros $\mathbb{Z}$, calculemos el mcd$(371, 28)$. Para esto usemos el algoritmo de la división.

$$371 = 28(13) + 7$$
$$28 = 7(4) + 0$$

De donde el último residuo distinto de cero 7 es el mcd$(371, 28)$.

Así $(371, 28) = (7)$ y más aun, de la primera igualdad despejando a 7 tenemos que

$371 - 28(13) = 7$ es decir $7 = 371(1) + 28(-13)$.

Más adelante en el capítulo 3 veremos que existe un anillo que no es de ideales principales sin embargo podemos encontrar un máximo común divisor de dos elementos, también veremos un ejemplo en el cual no existe un máximo común divisor de dos elementos. El siguiente corolario nos asegura la existencia de éste siempre que R sea un anillo de ideales principales.

Corolario 2.1.20. *Sea R un anillo conmutativo con uno tal que es de ideales principales. Entonces cualquier conjunto finito de elementos distintos de cero $a_1, a_2 \ldots, a_n$ tiene un máximo común divisor y éste se puede expresar como*

$$mcd(a_1, a_2, \ldots, a_n) = r_1a_1 + r_2a_2 + \cdots + r_na_n$$

para una elección adecuada de $r_1, r_2, \ldots, r_n \in R$.

Demostración. Como R es un anillo de ideales principales tenemos que $(a_1, a_2, \ldots, a_n) = (d)$ por el teorema 2.1.18 tenemos que $\text{mcd}(a_1, a_2, \ldots, a_n) = d$ y lo podemos expresar como $d = r_1a_1 + r_2a_2\cdots + r_na_n$, $i = 1, \ldots, n$. □

Definición 2.1.21. Sean $a_1, a_2, \ldots, a_n$ elementos no cero de un anillo de ideales principales R y sea

$$\text{mcd}(a_1, a_2 \ldots, a_n) = r_1a_1 + r_2a_2 + \cdots + r_na_n \tag{2.3}$$

para $r_1, r_2, \ldots, r_n \in R$. A la identidad 2.3 la llamamos la **identidad de Bezout**.

Ejemplo 2.1.22. Veamos el siguiente ejemplo.

Consideremos el anillo de ideales principales de los números enteros, $\mathbb{Z}$. Sean $3, 9 \in \mathbb{Z}$. Sabemos que $3 = \text{mcd}(9, 3)$, además a éste lo podemos expresar de las siguientes formas

$$\text{mcd}(9, 3) = 3(1) + 9(0)$$
$$\text{mcd}(9, 3) = 3(-2) + 9(1).$$

Lo cual muestra que los elementos r_i no son necesariamente únicos.

Con el fin de considerar otros dominios enteros que nos ayuden a comprender el corolario anterior necesitaremos los siguientes resultados, que retomaremos más adelante en la sección 2.6.

Definición 2.1.23. Sea R un dominio entero. Decimos que R es un dominio *Euclidiano* (o dominio entero Euclidiano o dominio Euclidiano) si existe una función

$$\delta : R \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

llamada *valuación euclidiana* que satisface las siguientes condiciones

1. Para cualesquiera $a, b \in R$, ambos no cero, $\delta(ab) \geq \delta(a)$;
2. Para cualesquiera $a, b \in R$, con $b \neq 0$, existen $q, r \in R$ (llamados el *cociente* y el *residuo*) tales que $a = qb + r$, con $r = 0$ ó $\delta(r) < \delta(b)$.

Ejemplo 2.1.24. Veamos algunos ejemplos de dominios Euclidianos.

1. Consideremos el dominio entero de los números enteros $\mathbb{Z}$ y la función

   $$\delta : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

   dada por $\delta(a) =\mid a \mid$. Sabemos por los cursos básicos de álgebra que δ satisface

   a) $\mid ab \mid \geq \mid a \mid$ para cualesquiera $a, b \in R$ ambos no cero.

   b) Dados $a, b \in \mathbb{Z}$, $b \neq 0$. Por el algoritmo de la división tenemos que existen q y r (únicos) tales que $a = qb + r$ con $0 \leq r <\mid b \mid$ en particular $r = 0$ ó $0 < r <\mid b \mid$.
   Así $\mathbb{Z}$ es un dominio entero Euclidiano.

2. Consideremos un campo F, por el ejemplo 1.1.25 es un dominio entero y la valuación:

   $$\delta : F \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

   dada por $\delta(a) = 1$ para toda $a \in F, a \neq 0$. Ésta satisface trivialmente la primera condición, además dados $a, b \in F$, $b \neq 0$ tenemos que $a = b\left(\frac{a}{b}\right) + 0$, aquí $q = \frac{a}{b}$ y $r = 0$, por lo cual δ satisface la segunda condición y así F es un dominio entero Euclidiano.

3. Sea F un campo y considere el anillo de los polinomios en una variable sobre el campo F, es decir, $F[x]$ por el ejemplo (ver 1.1.28) sabemos que $F[x]$ es un dominio entero. Definamos la siguiente función

$$\delta : F[x] \setminus \{0(x)\} \longrightarrow \mathbb{Z}^+$$

dada por $\delta(p(x)) = \text{gr}(p(x))$. Sabemos que esta función satisface que

a) $\text{gr}(a(x)b(x)) \geq \text{gr}(a(x))$

b) Sabemos que en $F[x]$ se cumple el algoritmo de la división, esto es, dados $c(x) \neq 0(x)$ y $d(x) \in F[x]$, entonces existen $q(x), r(x) \in F[x]$ tales que $c(x) = q(x)d(x) + r(x)$ con $r(x) = 0(x)$ o $\text{gr}(r(x)) < \text{gr}(d(x))$.

De donde $F[x]$ es un dominio entero Euclidiano.

Ejemplo 2.1.25. Por último, veamos el siguiente ejemplo. Considere el anillo de los enteros gaussianos, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$. Éstos son un dominio entero. Luego, la valuación

$$\delta : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

dada por $\delta(a + bi) = a^2 + b^2$ satisface las condiciones 1. y 2. de la definición anterior. Para demostrar que $\mathbb{Z}[i]$ es un dominio Euclidiano necesitamos varias herramientas que veremos en la sección 2.6. Por lo cual dejaremos pendiente esta demostración. Sin embargo, mencionamos este ejemplo aquí para poder abarcar más dominios enteros.

Sabemos que los números enteros son un dominio de ideales principales. Sin embargo, no sabemos si el dominio Euclidiano $F[x]$ con F campo o bien los enteros gaussianos sean dominios de ideales principales. Por lo cual nos podemos preguntar si cada dominio Euclidiano es un dominio de ideales principales. El siguiente resultado responde a esta pregunta de manera afirmativa.

Teorema 2.1.26. *Cada dominio Euclidiano es un dominio de ideales principales.*

Demostración. Sean R un dominio Euclidiano con valuación δ y J un ideal de R.

1. Si $J = \{0\}$, entonces J es un ideal principal, ya que es el generado de cero, $J = (0)$.

2. Si $J \neq 0$, entonces existe $0 \neq a \in J$. Consideremos el conjunto S definido por:

$$S = \{\delta(b) : b \in J, b \neq 0\}.$$

Note que S es un conjunto no vacío, pues $\delta(a) \in S$ ya que $a \neq 0$ y por tanto podemos calcular su valuación. Así como S es un subconjunto no vacío de los enteros positivos por el principio del buen orden S posee un elemento mínimo. Sea $a_0 \in J$ tal que $\delta(a_0)$ es este elemento.

Afirmamos que $J = (a_0)$.

La contención $(a_0) \subseteq J$ es inmediata pues $a_0 \in J$. Veamos ahora que $J \subseteq (a_0)$. Sea $j \in J$, como R es un dominio Euclidiano tenemos que existen $q, r \in R$ tales que $j = a_0q + r$ con $r = 0$ ó $\delta(r) < \delta(a_0)$. Si $r \neq 0$ entonces $\delta(r) < \delta(a_0)$ además $r = j - a_0q$ con $j, a_0 \in J$ como es J un ideal tenemos que $j - a_0q \in J$, así $r \in J$ y $\delta(r) < \delta(a_0)$ pero esto es una contradicción al hecho de que $\delta(a_0)$ fuera mínimo. Por tanto $r = 0$ y así $j = a_0q$ de donde $j \in (a_0)$. Por lo tanto $J \subseteq (a_0)$ y así J es un ideal principal $J = (a_0)$.

□

Gracias al teorema anterior tenemos que los anillos considerados en el ejemplo 2.1.24 son dominios de ideales principales.

Ejemplo 2.1.27. Veamos los siguientes ejemplos.

1. Consideremos el conjunto de los números enteros $\mathbb{Z}$. Sabemos que $\mathbb{Z}$ es un anillo de ideales principales. De donde para cada $a_1, a_2, \ldots, a_n$ elementos no nulos de $\mathbb{Z}$ podemos encontrar un máximo común divisor.

2. Tomemos un campo F cualquiera. Como F es un dominio de ideales principales tenemos que para cualesquiera $a_1, a_2, \ldots, a_n \in F$ elementos no nulos, podemos encontrar un máximo común divisor.

3. Consideremos el anillo de los polinomios en una variable sobre los números complejos $\mathbb{C}[x]$. Por el ejemplo 2.1.24 tenemos que $\mathbb{C}[x]$ es un dominio Euclidiano y por el teorema 2.1.26 tenemos que $\mathbb{C}[x]$ es un dominio de ideales principales. De donde para cada $a_1(x), a_2(x), \ldots, a_n(x)$ polinomios no nulos de $\mathbb{C}[x]$ podemos encontrar un máximo común divisor.

4. Considere el anillo de los enteros gaussianos $\mathbb{Z}[i]$. Por el ejemplo 2.1.25 éste es un dominio Euclidiano y por el teorema 2.1.26 es un dominio de ideales principales. Por lo que para cualesquiera $a_1 + b_1 i, a_2 + b_2 i, \ldots, a_n + b_n i \in \mathbb{Z}[i]$ no nulos podemos encontrar un máximo común divisor.

Observación y definición 2.1.28. Sean R un anillo conmutativo con uno y $a_1, a_2, \ldots, a_n \in R$ tales que $R = (a_1, a_2, \ldots, a_n)$. Como $R = (1_R)$ tenemos que el ideal $(a_1, a_2, \ldots, a_n)$ es principal de donde por el teorema 2.1.18 existe $d \in R$ tal que es un máximo común divisor de $a_1, a_2, \ldots, a_n$. Además d se puede expresar como $d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ con $r_i \in R$ para $i = 1, \ldots, n$. Veamos que $1 \in R$ es un máximo común divisor.

1. Es claro que $1 \mid a_i$ para $i = 1, \ldots, n$.

2. Supongamos ahora que existe $c \in R$ tal que $c \mid a_i$ para $i = 1, \ldots, n$. Como $1 \in R = (a_1, a_2, \ldots, a_n)$ entonces $1 = s_1 a_1 + s_2 a_2 + \cdots + s_n a_n$. Dado que $c \mid a_i$ para $i = 1, \ldots, n$ por el teorema 2.1.4 tenemos que $c \mid s_1 a_1 + s_2 a_2 + \cdots + s_n a_n$, de donde $c \mid 1$.

Por lo tanto 1 es un máximo común divisor. Luego, por el lema 2.1.15 tenemos que d y 1 son asociados, esto es existe un elemento invertible $u \in R$ tal que $d = 1u = u$. Así d es un elemento invertible.

Cuando el máximo común divisor de $a_1, a_2, \ldots, a_n$ sea un elemento invertible diremos que $a_1, a_2, \ldots, a_n$ son ***primos relativos*** y lo denotaremos por $\text{mcd}(a_1, a_2, \ldots, a_n) = 1$.

Ejemplo 2.1.29. Para un mejor entendimiento de la observación y definición anterior consideremos los siguientes ejemplos.

1. Tomemos el anillo de los números enteros $\mathbb{Z}$ este es un anillo de ideales principales. Sean $-3, 5 \in \mathbb{Z}$. Veamos que un $\text{mcd}(-3, 5) = -1$.

   Notemos que $-1 \mid -3$ y $-1 \mid 5$ por lo tanto satisface la condición 1. de nuestra definición. Los divisores comunes de -3 y 5 solo son -1 y 1 ambos satisfacen que $-1 \mid -1$ y $1 \mid -1$ por

lo cual se satisface la condición 2. Así $\text{mcd}(-3,5) = -1$ y recordemos que los elementos invertibles de $\mathbb{Z}$ son -1 y 1. Por lo tanto el máximo común divisor de -3 y 5 es un elemento invertible. Por la observación y definición anterior tenemos que -3 y 5 son primos relativos. Y denotamos $\text{mcd}(-3,5) = 1$.

2. Consideremos el anillo de ideales principales $\mathbb{C}[x]$. Sean $x+1, x-1 \in \mathbb{C}[x]$. Veamos que son primos relativos. Al ser $\mathbb{C}[x]$ un dominio de ideales principales para cualquier número finito de polinomios no nulos podemos encontrar su máximo común divisor. Por lo visto en los cursos básicos de álgebra podemos aplicar el algoritmo de Euclides

$$\begin{aligned} x+1 &= (x-1)+2, \qquad 0 = \text{gr}(2) \leq \text{gr}(x-1) = 1, \\ x-1 &= 2(\frac{1}{2}x - \frac{1}{2}) \qquad \text{con el residuo igual a cero,} \end{aligned}$$

de donde un $\text{mcd}(x+1, x-1) = 2$. Recordemos que los elementos invertibles de $\mathbb{C}[x]$ son los polinomios constantes, es decir los elementos del campo $\mathbb{C}$. Así un máximo común divisor de estos dos polinomios es un elemento invertible, por tanto son primos relativos y denotamos $\text{mcd}(x+1, x-1) = 1$

3. Consideremos el anillo de los números racionales $\mathbb{Q}$. Como $\mathbb{Q}$ es un campo tenemos que es un dominio de ideales principales. Sean $\frac{1}{4}, \frac{3}{8} \in \mathbb{Q}$. En el ejemplo 2 de 2.1.13 vimos que cualquier elemento no nulo de $\mathbb{Q}$ es un máximo común divisor de dos elementos no nulos de este campo. Así $\frac{1}{2} \in \mathbb{Q}$ es un máximo común divisor de $\frac{1}{4}, \frac{3}{8}$. Como $\mathbb{Q}$ es un campo, tenemos que $\frac{1}{2}$ es un elemento invertible, así $\frac{1}{4}, \frac{3}{8}$ son primos relativos. Es decir cualesquiera dos elementos no nulos de $\mathbb{Q}$ son primos relativos.

Observación 2.1.30. Sea R un dominio de ideales principales y sean $a_1, a_2, \ldots, a_n$ elementos no nulos. Supongamos que $a_1, a_2, \ldots, a_n$ son primos relativos, esto es existe $d \in R$ un elemento invertible tal que $\text{mcd}(a_1, a_2, \ldots, a_n) = d$. Por el corolario 2.1.20 tenemos que

$$r_1 a_1 + r_2 a_2 + \cdots + r_n a_n = d,$$

como d es un elemento invertible existe d^{-1} tal que $dd^{-1} = 1_R$. Multiplicando la expresión anterior por d^{-1} tenemos que

$$(d^{-1}r_1)a_1 + (d^{-1}r_2)a_2 + \cdots + (d^{-1}r_n)a_n = d^{-1}d = 1.$$

Por lo tanto $a_1, a_2, \ldots, a_n$ son primos relativos si, y sólo si existen $s_1, s_2, \ldots s_n \in R$ tales que $s_1a_1 + s_2a_2 + \cdots + s_na_n = 1$. Este es un caso particular de la identidad de Bezout, cuando los elementos son primos relativos. Ahora veamos una aplicación de ésta.

Teorema 2.1.31. *Sea R un anillo de ideales principales y sean a, b, c elementos de R. Si $c \mid ab$ con a y c primos relativos. Entonces $c \mid b$.*

Demostración. Sean $a, b, c \in R$. Como a y c son primos relativos existen $r, s \in R$ tales que $1 = ra + sc$, de donde

$$b = 1b = (ra + sc)b = rab + scb.$$

Como $c \mid ab$ y $c \mid c$ entonces por el teorema 2.1.10 (5) tenemos que $c \mid rab + scb$, es decir $c \mid b$. □

2.2. Mínimo común múltiplo

Recordemos que en los números enteros $\mathbb{Z}$ tenemos la noción de un máximo común divisor y de un mínimo común múltiplo, por lo cual quisiéramos definir el concepto de un mínimo común múltiplo en un anillo conmutativo con uno. Luego, al igual que caracterizamos un máximo común divisor por medio de ideales principales también lo haremos con un mínimo común múltiplo.

Definición 2.2.1. Sean R un anillo conmutativo con uno y $a_1, a_2, \ldots, a_n \in R$ elementos no cero. Un elemento $m \in R$ es un mínimo común múltiplo de $a_1, a_2, \ldots, a_n$ si

1. $a_i \mid m$ para $i = 1, \ldots, n$ (es decir m es un múltiplo común)
2. si $a_i \mid c$ para $i = 1, \ldots, n$ entones $m \mid c$.

Esto es, m es un mínimo común múltiplo de $a_1, a_2, \ldots, a_n$ si es un múltiplo común de $a_1, a_2, \ldots, a_n$ y además es el más pequeño de todos, en el sentido de que si hay algún otro múltiplo común de $a_1, a_2, \ldots, a_n$ entonces el mínimo lo divide.

Ejemplo 2.2.2. Veamos algunos ejemplos.

1. Consideremos $\mathbb{Z}$ el anillo de los números enteros y sean $2, -5 \in \mathbb{Z}$. Veamos que -10 es un mínimo común múltiplo de 2 y -5.

   a) Notemos que $2 \mid -10$ y $-5 \mid -10$, por tanto satisface 1. de la definición.

   b) Sea $c \in \mathbb{Z}$ tal que $2 \mid c$ y $-5 \mid c$. Veamos que $-10 \mid c$. Como $2 \mid c$ y $-5 \mid c$ entonces existen $t_1, t_2 \in \mathbb{Z}$ tales que $c = 2t_1$ y $c = -5t_2$. Así $2t_1 = -5t_2$, de donde $2 \mid -5t_2$ como $\text{mcd}(2, -5) = 1$ por el teorema 2.1.31 tenemos que $2 \mid t_2$. Por tanto existe $t_3 \in \mathbb{Z}$ tal que $t_2 = 2t_3$. Sustituyendo en $c = -5t_2$ tenemos que

   $$c = -5t_2 = -5(2t_3) = -10t_3 \text{ con } t_3 \in \mathbb{Z},$$

   de donde $-10 \mid c$. Así -10 es un mínimo común múltiplo de 2 y -5. Una demostración análoga muestra que 10 también es un mínimo común múltiplo de 2 y -5.

2. Consideremos $\mathbb{C}[x]$ el anillo de los polinomios en una variable sobre el campo de los complejos. Sean $x^2 + 5x + 6, x^2 + 3x \in \mathbb{Z}$, de los cursos básicos de álgebra podemos factorizar estos polinomios en factores lineales de la siguiente forma:

   $$x^2 + 5x + 6 = (x + 2)(x + 3)$$
   $$x^2 + 3x = x(x + 3).$$

   Además de estos mismos cursos, teníamos una técnica para encontrar el mínimo común múltiplo en los polinomios sobre un campo K, en la cual tomábamos los factores lineales a su máxima potencia y los multiplicábamos. Es decir, en este caso el mínimo común múltiplo de $x^2 + 5x + 6, x^2 + 3x$ es el producto de los factores lineales $x(x + 2)(x + 3)$.

Con el ejemplo anterior y de manera análoga a la definición de un máximo común divisor, puede existir más de un mínimo común múltiplo, sin embargo éste será único salvo elementos asociados.

Lema 2.2.3. *Sean R un anillo conmutativo con uno y $a_1, a_2, \ldots, a_n \in R$ elementos no nulos tales que existe un mínimo común múltiplo. Entonces, éste es único (salvo elementos asociados).*

Demostración. La demostración de este lema es análoga al lema 2.1.15. □

Notación 2.2.4. Denotaremos a un mínimo común múltiplo de $a_1, a_2, \ldots, a_n$, cuando exista, como

$$m{=}\text{mcm}(a_1, a_2, \ldots, a_n).$$

De acuerdo al teorema 2.1.18 nos gustaría determinar y caracterizar la existencia de un mínimo común múltiplo de una cantidad finita de elementos no nulos de un anillo, usando ideales principales. Siguiendo esta idea enunciaremos el siguiente teorema que nos proporciona tal relación.

Teorema 2.2.5. *Sea R un anillo conmutativo con uno y $a_1, a_2, \ldots, a_n \in R$ elementos no nulos de R. Entonces $a_1, a_2, \ldots, a_n$ tienen un mínimo común múltiplo si, y sólo si el ideal $\bigcap_{i=1}^{n}(a_i)$ es principal.*

Demostración. Sea R un anillo con uno y $a_1, a_2, \ldots, a_n \in R$ elementos no nulos de R.

Supongamos que $m = \text{mcm}(a_1, a_2, \ldots, a_n)$ existe. Entonces $a_i \mid m$ para $i = 1, 2, \ldots, n$, esto es $m = a_i r_i$ con $r_i \in R, i = 1, 2, \ldots, n$, de donde $m \in (a_i)$ para cada $i = 1, 2, \ldots, n$. Así, $m \in \bigcap_{i=1}^{n}(a_i)$. Por tanto, $(m) \subseteq \bigcap_{i=1}^{n}(a_i)$. Veamos la otra contención. Sea $c \in \bigcap_{i=1}^{n}(a_i)$, esto es $c \in (a_i)$ para $i = 1, 2, \ldots, n$, de donde $c = a_i t_i$ con $t_i \in R, i = 1, 2, \ldots, n$. De donde, $a_i \mid c$ por lo que c es un múltiplo común de a_i para cada i, como m es el mínimo común múltiplo de $a_1, a_2, \ldots, a_n$ tenemos que $m \mid c$, esto es $c = ms$ para algún $s \in R$. Por lo tanto $c \in (m)$ y así $\bigcap_{i=1}^{n}(a_i) \subseteq (m)$. Es decir, $\bigcap_{i=1}^{n}(a_i) = (m)$ por lo que es un ideal principal.

Ahora veamos el recíproco. Supongamos ahora que $\bigcap_{i=1}^{n}(a_i)$ es un ideal principal. Veamos que $a_1, a_2, \ldots, a_n$ tienen un mínimo común múltiplo. Como $\bigcap_{i=1}^{n}(a_i)$ es principal entonces existe $m \in R$ tal que $\bigcap_{i=1}^{n}(a_i) = (m)$. Así $(m) \subseteq (a_i)$ para cada i, entonces $m \in (a_i)$ de donde $m = a_i t_i$ con $t_i \in R, i = 1, 2, \ldots, n$, es decir $a_i \mid m$. Por tanto, m es un múltiplo común de a_i para cada i. Sea $b \in R$ otro múltiplo común de $a_1, a_2, \ldots, a_n$, esto es $a_i \mid b$ entonces existe $u_i \in R$ tal que $b = a_i u_i$ para $i = 1, 2, \ldots, n$. Así, $b \in (a_i)$ para cada i, por lo cual $(b) \subseteq \bigcap_{i=1}^{n}(a_i) = (m)$, de donde $(b) \subseteq (m)$. Por el lema 2.1.5 tenemos que $m \mid b$. Por tanto m satisface 1. y 2. de la definición 2.2.1 por lo que $m = \text{mcm}(a_1, a_2, \ldots, a_n)$.

□

Ejemplo 2.2.6. Para concluir esta sección veamos algunos ejemplos.

1. Consideremos $\mathbb{Z}$ el anillo de los números enteros. Sean $2, -5 \in \mathbb{Z}$, recordemos que $(2) = \{2n : n \in \mathbb{Z}\}$ y $(-5) = \{-5m : m \in \mathbb{Z}\}$. Del ejemplo 2.2.2 sabemos que un $\text{mcm}(2, -5) = -10$. Veamos que $(2) \cap (-5) = (-10)$.

Sea $-10k \in (-10)$ es tal que $-10k = -5(2k)$ por tanto $-10k \in (-5)$. También $-10k = 2(-5k)$ por lo que $-10k \in (2)$. Así $(-10) \subseteq (2) \cap (-5)$.

Mostremos la otra contención. Sea $x \in (2) \cap (-5)$. Entonces, $x \in (2)$ y $x \in (-5)$ de donde $x = 2t_1$ y $x = -5t_2$ con $t_1, t_2 \in \mathbb{Z}$. Así, $2 \mid x$ y $-5 \mid x$ por lo que x es un múltiplo común de 2 y -5. Como -10 es el mínimo común múltiplo, tenemos que $-10 \mid x$, de donde $x = -10t_3$ con $t_3 \in \mathbb{Z}$. Luego, $x \in (-10)$ y por tanto $(2) \cap (-5) \subseteq (-10)$.

2. Tomemos $\mathbb{C}[x]$ el anillo de los polinomios en una variable sobre el campo de los números complejos. Sean $x^3 - 4x^2 + 3x - 2, x^2 - 1 \in \mathbb{C}[x]$. Análogamente al ejemplo 2.2.2 podemos factorizar estos polinomios de la siguiente forma

$$x^3 - 4x^2 + 3x - 2 = (x-1)^2(x-2)$$
$$x^2 - 1 = (x+1)(x-1)$$

de donde, un $\text{mcm}(x^3 - 4x^2 + 3x - 2, x^2 - 1) = (x+1)(x-2)(x-1)^2$. De modo que $((x-1)^2(x-2)) \cap ((x+1)(x-1)) = ((x+1)(x-2)(x-1)^2)$.

2.3. M.c.d. propiedad y m.c.m. propiedad

Siguiendo el razonamiento que hemos utilizando, dados $a_1, a_2, \ldots, a_n$ enteros, siempre podemos encontrar un máximo común divisor o un mínimo común múltiplo. En esta sección definiremos aquellos anillos que satisfacen esta propiedad. Además, veremos algunas propiedades que satisfacen un mínimo común múltiplo y un máximo común divisor.

Definición 2.3.1. Sea R un anillo conmutativo con uno. Decimos que R tiene la m.c.d. propiedad (m.c.m. propiedad) siempre que cualquier número finito de elementos no cero de R admitan un máximo común divisor (mínimo común múltiplo).

Ejemplo 2.3.2. Veamos algunos ejemplos.

1. Consideremos el anillo conmutativo con uno de los números enteros $\mathbb{Z}$. De los cursos básicos de álgebra sabemos que para cualesquiera $a_1, a_2, \ldots, a_n$ enteros no nulos, podemos encontrar un máximo común divisor y un mínimo común múltiplo. Es decir, $\mathbb{Z}$ posee la m.c.d. propiedad y la m.c.m. propiedad.

2. Consideremos ahora el anillo conmutativo con uno de los polinomios en una variable sobre el campo de los números complejos $\mathbb{C}[x]$. Por los cursos básicos de álgebra, sabemos que para cualquier número finito de polinomios no nulos podemos encontrar un mínimo común múltiplo y un máximo común divisor. Así, $\mathbb{C}[x]$ tiene la la m.c.d. propiedad y la m.c.m. propiedad.

El teorema 2.2.5 nos dice que R tiene la m.c.m propiedad si, y sólo si la intersección de un número finito de ideales principales (no cero) de R resulta ser un ideal principal. Basta decir que cada anillo de ideales principales satisface la m.c.m. propiedad y la m.c.d. propiedad.

Corolario 2.3.3. *Sea R un anillo conmutativo con uno tal que R es un anillo de ideales principales. Entonces R tiene la m.c.d. propiedad y la m.c.m. propiedad.*

Demostración. Sean R un anillo de ideales principales y $a_1, a_2, \ldots, a_n \in R$ elementos no nulos. Veamos que R tiene la m.c.d. propiedad, esto es, mostremos que existe el máximo común divisor de $a_1, a_2, \ldots, a_n$. En efecto, como R es un anillo de ideales principales entonces el ideal $(a_1, \ldots, a_n)$ es principal, luego por el teorema 2.1.18 tenemos que existe d máximo común divisor de $a_1, a_2, \ldots, a_n$. La demostración de que R tiene la m.c.m. propiedad es análoga. □

Ejemplo 2.3.4. Veamos algunos ejemplos.

1. Consideremos los números enteros $\mathbb{Z}$. Sabemos que $\mathbb{Z}$ es un dominio de ideales principales, de donde por el corolario anterior $\mathbb{Z}$ tiene la m.c.d. propiedad y la m.c.m propiedad.

2. Sean $\mathbb{C}[x]$ los polinomios en una variable sobre el campo de los números complejos. Como $\mathbb{C}[x]$ es un dominio de ideales principales tenemos que $\mathbb{C}[x]$ tiene la m.c.d. propiedad y la m.c.m propiedad.

3. Consideremos los enteros gaussianos $\mathbb{Z}[i]$. Sabemos que $\mathbb{Z}[i]$ es un dominio de ideales principales de donde para cualesquiera enteros gaussianos no nulos podemos encontrar un máximo común divisor y un mínimo común múltiplo. Por lo tanto, $\mathbb{Z}[i]$ tiene la m.c.d. propiedad y la m.c.m. propiedad.

Como ya vimos en un anillo de ideales principales, satisface ambas propiedades, esto nos hace preguntarnos qué pasa con estas propiedades en un anillo cualquiera. Para cerrar esta sección demostraremos que cualquier dominio entero tiene la m.c.d propiedad si, y sólo si tiene la m.c.m. propiedad. Para poder demostrar este hecho, necesitaremos herramientas que desarrollaremos a continuación.

Lema 2.3.5. *Sean R un dominio entero y $a_1, a_2, \ldots, a_n, r \in R$ elementos no nulos. Entonces se satisfacen los siguientes*

1. *Si el $mcm(a_1, a_2, \ldots, a_n)$ existe, entonces el $mcm(ra_1, ra_2, \ldots, ra_n)$ también existe y*

$$mcm(ra_1, ra_2, \ldots, ra_n) = r\,mcm(a_1, a_2, \ldots, a_n).$$

2. *Si el $mcd(ra_1, ra_2, \ldots, ra_n)$ existe, entonces el $mcd(a_1, a_2, \ldots a_n)$ también existe y*

$$mcd(ra_1, ra_2, \ldots, ra_n) = r\,mcd(a_1, a_2, \ldots, a_n)$$

Demostración. Sean R un dominio entero y $a_1, a_2, \ldots, a_n, r \in R$ tales que $a_i \neq 0, i = 1, \ldots, n$ y $r \neq 0$.

Probemos 1. Supongamos que $m = \text{mcm}(a_1, \ldots, a_n)$ existe. Entonces $a_i \mid m$ para cada i, de donde $ra_i \mid rm$. Sea $m' \in R$ un múltiplo común de $ra_1, \ldots ra_n$. Es decir, $ra_i \mid m'$ de donde $m' = (ra_i)t_i$ con $t_i \in R$ para cada i, así $m' = r(a_i t_i)$. Por lo tanto $r \mid m'$, esto es existe $s \in R$ tal que $m' = rs$. Así, tenemos las siguientes igualdades $rs = m' = ra_i t_i$ para cada i, como $r \neq 0$ por la ley de la cancelación tenemos que $s = a_i t_i$ con $i = 1, \ldots, n$. De donde, $a_i \mid s$ para cada i así s es un múltiplo común de a_i por tanto $m \mid s$. Como consecuencia, $rm \mid rs$ o bien $rm \mid m'$. Pero esto quiere decir que el $\text{mcm}(ra_1, ra_2, \ldots, ra_n)$ existe y es igual a $rm = r\text{mcm}(a_1, a_2, \ldots, a_n)$.

Para probar 2. supongamos que $c = \text{mcd}(ra_1, \ldots, ra_n)$ existe. Notemos que $r \mid ra_i$, esto es r es un divisor común de ra_i para cada i. Por lo tanto, $r \mid c$ esto es existe $t \in R$ tal que $c = rt$. Como $c \mid ra_i$, tenemos que $t \mid a_i$ para cada i, es decir t es un divisor común de a_i. Ahora consideremos $t' \in R$ un divisor común arbitrario de $a_1, a_2, \ldots, a_n$. Entonces $rt' \mid ra_i$ para $i = 1, 2, \ldots, n$ y por lo tanto $rt' \mid c$. Pero $c = rt$, así $rt' \mid rt$ o bien $t' \mid t$. Esto implica que el $\text{mcd}(a_1, a_2, \ldots, a_n)$ existe y es igual a t. Además

$$\text{mcd}(ra_1, ra_2, \ldots, ra_n) = c = rt = r\text{mcd}(a_1, a_2, \ldots, a_n)$$

□

Observación 2.3.6. Es posible que el $\text{mcd}(a_1, a_2, \ldots, a_n)$ exista sin la existencia del $\text{mcd}(ra_1, ra_2, \ldots, ra_n)$, esto explica la falta de simetría en el lema anterior. (ver ejemplo 3.1.1)

El siguiente lema a pesar de que tiene un carácter algo especializado, la información que contiene resulta ser muy útil.

Teorema 2.3.7. *Sean R un dominio entero y $a_1, a_2, \ldots, a_n, b_1, \ldots, b_n \in R$ elementos no cero tales que $a_1b_1 = a_2b_2 = \cdots = a_nb_n = x$. Entonces se satisfacen los siguientes.*

1. *Si el $mcm(a_1, a_2, \ldots, a_n)$ existe, entonces el $mcd(b_1, b_2, \ldots, b_n)$ también existe y satisface que*

$$mcm(a_1, a_2, \ldots, a_n)mcd(b_1, b_2, \ldots, b_n) = x$$

2. *Si el $mcd(ra_1, ra_2, \ldots, ra_n)$ existe para toda $0 \neq r \in R$, entonces el $mcm(b_1, b_2, \ldots, b_n)$ también existe y satisface que*

$$mcd(a_1, a_2, \ldots, a_n)mcm(b_1, b_2, \ldots, b_n) = x$$

Demostración. Sean R un dominio entero y $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in R$ elementos no cero. Probemos la primera afirmación. Sea $m = \text{mcm}(a_1, a_2, \ldots, a_n)$. Entonces $a_i \mid m$ para cada i, esto es existen $r_i \in R$ tales que $m = r_ia_i$. Como $x = a_ib_i$ con $i = 1, 2, \ldots, n$ tenemos que $mb_i = (r_ia_i)b_i = r_ix$, así $x \mid mb_i$ para cada i. Consideremos ahora $y \in R$ un divisor común de mb_i con $i = 1, 2, \ldots, n$. Entonces $ya_i \mid m(b_ia_i)$, esto es $ya_i \mid mx$ para cada i. Por lo tanto, xm es un múltiplo común de $ya_1, ya_2, \ldots, ya_n$. Además, por el lema 2.3.5 tenemos que $\text{mcm}(ya_1, ya_1, \ldots, ya_n) = ym$, por lo tanto por la definición de mínimo común múltiplo $ym \mid mx$, es decir $y \mid x$.

Recapitulando, hemos mostrado que $x \mid mb_i$ para cada i y siempre que $y \mid mb_i$, entonces $y \mid x$. De donde, $x = \text{mcd}(mb_1, mb_2, \ldots, mb_n)$. Luego por el lema 2.3.5 tenemos que

$$x = \text{mcd}(mb_1, mb_2, \ldots, mb_n) = m\text{mcd}(b_1, b_2, \ldots, b_n) = \text{mcm}(a_1, a_2, \ldots, a_n)\text{mcd}(b_1, b_2, \ldots, b_n)$$

La prueba de la segunda afirmación se deja al lector, esta se sigue del mismo razonamiento.

□

Ejemplo 2.3.8. Veamos ahora un ejemplo.

Consideremos el dominio entero de los números enteros $\mathbb{Z}$. Sean $a_1 = b_2$ y $a_2 = b_1 \in \mathbb{Z}$ elementos distintos de cero. Notemos que $a_1b_1 = a_2b_2 = x$. Sabemos que $\text{mcm}(a_1, a_2)$ existe (ver ejemplo 2.3.2). Luego, por el teorema 2.3.7 tenemos que

$$\text{mcm}(a_1, a_2)\text{mcd}(b_1, b_2) = \text{mcm}(a_1, a_2)\text{mcd}(a_2, a_1) = x = a_1a_2.$$

Recordemos que teníamos una propiedad similar cuando trabajamos el máximo común divisor y el mínimo común múltiplo en los números enteros en los cursos básicos de álgebra.

En el capítulo 3 mostraremos que existen anillos conmutativos con uno en los cuales no se satisface la m.c.d. propiedad ni la m.c.m. propiedad (ver 3.1.1 y 3.1.2). Finalizaremos esta sección con un teorema que relaciona la m.c.d. propiedad y la m.c.m. propiedad en un dominio entero.

Teorema 2.3.9. *Sea R un dominio entero. Entonces R tiene la m.c.d. propiedad si, y sólo si R tiene la m.c.m. propiedad.*

Demostración. Sean R un dominio entero y $b_1, b_2, \ldots, b_n \in R$ elementos no cero. Supongamos que R tiene la m.c.m. propiedad. Definimos $x = b_1 b_2 \ldots b_n$ y $a_k = b_1 b_2 \ldots b_{k-1} b_{k+1} \ldots b_n$ para $k = 1, 2, \ldots, n$. Para mostrar que R tiene la m.c.d. propiedad, veamos que $\text{mcd}(b_1, b_2, \ldots, b_n)$ existe. Notemos que $a_1 b_1 = a_2 b_2 = \cdots = a_n b_n = x$. Como R tiene la m.c.m. propiedad tenemos que el $\text{mcm}(a_1, a_2, \ldots, a_n)$ existe. Luego por el teorema 2.3.7 tenemos que $\text{mcd}(b_1, b_2, \ldots, b_n)$ existe y por lo tanto R tiene la m.c.d. propiedad.

Supongamos ahora que R tiene la m.c.d. propiedad. Sean $b_1, b_2, \ldots, b_n \in R$ elementos no cero. Análogamente definimos $x = b_1 b_2 \ldots b_n$ y $a_k = b_1 b_2 \ldots b_{k-1} b_{k+1} \ldots b_n$ para $k = 1, 2, \ldots, n$ y son tales que $a_1 b_1 = a_2 b_2 = \cdots = a_n b_n = x$. Luego, como R tiene la m.c.d. propiedad tenemos que para toda $0 \neq r \in R$ el $\text{mcd}(ra_1, ra_2, \ldots, ra_n)$ existe. Por lo tanto, por el teorema 2.3.7 tenemos que el $\text{mcm}(b_1, b_2, \ldots, b_n)$ existe y por lo tanto R tiene la m.c.m. propiedad. □

2.4. Elementos primos e irreducibles

Llegados a este punto ya tenemos bastante información sobre la divisibilidad en dominios enteros, sin embargo la pregunta principal de este trabajo continua sin respuesta: ¿Cuándo un anillo posee una teoría de factorización en la cual se satisfaga un teorema análogo al teorema fundamental de la aritmética? Para responder esta pregunta, en esta sección introducimos dos nuevos elementos: primos e irreducibles. Empezamos mencionando varias de las propiedades que satisfacen éstos. Luego, mostramos un teorema que relacionará estos nuevos conceptos con los ideales principales, con éste nos será un poco más fácil detectar los elementos primos e irreducibles.

Además, damos la definición de un dominio de factorización única y mostramos para que dominios enteros podemos garantizar que sean de factorización única. Finalizamos esta sección mostrando que cada dominio de ideales principales es un dominio de factorización única.

Definición 2.4.1. Sea R un dominio entero. Decimos que

1. un elemento $q \in R$ distinto de cero es un elemento primo si, y sólo si p no es invertible y si $p \mid ab$ implica que $p \mid a$ o $p \mid b$.

2. un elemento $q \in R$ distinto de cero es un elemento irreducible (o no factorizable) si, y sólo si q es no invertible y para cada factorización $q = ab$ con $a, b \in R$, implica que a es invertible o b es invertible.

En otras palabras, un elemento irreducible $q \in R$ es un elemento que no puede ser factorizado en R de manera no trivial, es decir, los únicos factores de q son sus asociados y los elementos invertibles de R. En algunos anillos como los anillos con división o los campos, donde cada elemento no cero posee un inverso multiplicativo, el concepto de un elemento irreducible no tiene significado.

Ejemplo 2.4.2. Veamos unos ejemplos.

1. Consideremos el dominio entero de los números enteros $\mathbb{Z}$. Sea $p \in \mathbb{Z}$ tal que es un número primo. Este satisface ser un elemento primo. Veamos que p es un elemento irreducible. Sean

$a, b \in \mathbb{Z}$ tales que $p = ab$. Como p es un entero primo entonces $a = \pm 1$ y $b = \pm p$ o $a = \pm p$ y $b = \pm 1$. De donde a o b son invertibles. Por lo tanto p es un elemento irreducible. En este ejemplo un elemento primo coincide con ser un elemento irreducible y viceversa.

2. Tomemos el dominio entero de los polinomios en una variable sobre el anillo de los números enteros $\mathbb{Z}[x]$. Sea $2x+2 \in \mathbb{Z}$. Notemos que $2x+2 = 2(x+1)$ pero 2 y $x+1$ no son invertibles en $\mathbb{Z}$. Por lo tanto $2x + 2$ no es un elemento irreducible.

   Veamos que $p(x) = 2x + 2$ no es primo. Sabemos que $2x + 2 \mid 2(x + 1)$, pero $2x + 2 \nmid 2$ pues si fuera así existe $t(x) \in \mathbb{Z}[x]$ tal que $(2x + 2)t(x) = 2$ de donde $\text{gr}(2x + 2) + \text{gr}(t(x)) = 0$ pero no hay forma que esto pase. Por tanto $2x + 2 \nmid 2$. Además $2x + 2 \nmid x + 1$, supongamos que sí lo divide entonces

$$x + 1 = (2x + 2)k(x)$$
$$x + 1 = 2(x + 1)k(x),$$

   con $k(x) \in \mathbb{Z}[x]$, de modo que $k(x) = \dfrac{1}{2}$ lo cual es una contradicción.

3. Consideremos el dominio entero los enteros gaussianos $\mathbb{Z}[i]$. Recordemos que los elementos invertibles de $\mathbb{Z}[i]$ son ± 1. Sea $5 \in \mathbb{Z}[i]$ es tal que $5 = (2 + i)(2 - i)$. Como $2 + i, 2 - i$ no son invertibles entonces 5 no es irreducible en $\mathbb{Z}[i]$.

4. Por último, consideremos el dominio entero de los polinomios en una variable sobre el campo de los complejos $\mathbb{C}[x]$. Sea $x + 2 \in \mathbb{C}[x]$. Veamos que es un elemento irreducible. Como los elementos invertibles de $\mathbb{C}[x]$ son los polinomios constantes, tenemos que $x+2$ no es invertible. Supongamos que $x+2 = p(x)t(x)$ para $t(x), p(x) \in \mathbb{C}[x]$. Mostremos que $p(x)$ o $t(x)$ es un polinomio constante y por tanto invertible. Como $x + 2 = p(x)t(x)$ entonces tenemos que

$$1 = \text{gr}(x + 2) = \text{gr}(p(x)) + \text{gr}(t(x)).$$

   Así $\text{gr}(p(x)) = 1$ y $\text{gr}(t(x)) = 0$ o $\text{gr}(p(x)) = 0$ y $\text{gr}(t(x)) = 1$. Por lo tanto $p(x)$ o $t(x)$ es constante.

En 1. del ejemplo 2.4.2 vimos que en el dominio de los números enteros todo elemento primo es un elemento irreducible y viceversa. Por lo cual nos podemos preguntar si existen elementos primos que no son elementos irreducibles, o bien elementos irreducibles que no son primos. Más adelante mostraremos que todo elemento primo es un elemento irreducible. Más aún, en el ejemplo 3.1.3 veremos que no necesariamente un elemento irreducible es un elemento primo.

Observación 2.4.3. Observemos que todo elemento asociado de un elemento irreducible (primo) es un elemento irreducible (primo). En efecto, supongamos que R es un dominio entero y que $r, q \in R$ son elementos asociados y q es un elemento irreducible. Veamos que r es un elemento irreducible. Como r es asociado de q tenemos que $r = uq$ con $u \in R$ invertible, de donde $q = u^{-1}r$. Notemos que r no es invertible ya que si lo fuera entonces $u^{-1}r$ sería invertible y en consecuencia q sería invertible lo cual es una contradicción pues q es un elemento irreducible. Ahora sean $s, t \in R$ tales que $r = st$. Veamos que s o t es invertible. Como $r = st$ multiplicando ambos lados por u^{-1} tenemos que $q = u^{-1}r = (u^{-1}s)t$. Dado que q es un elemento invertible entonces $u^{-1}s$ o t es invertible.

1. Si t es invertible, tenemos lo que necesitábamos.

2. Si $u^{-1}s$ es invertible, entonces existe $y \in R$ tal que $(u^{-1}s)y = 1_R$. Por lo tanto $s(u^{-1}y) = 1_R$ así s es un elemento invertible.

Por tanto concluimos que r es un elemento irreducible.

Con esto podemos anunciar el siguiente lema.

Lema 2.4.4. *Sea R un dominio entero, $a_1, a_2, \ldots, a_n \in R$ y $p \in R$ un elemento primo. Si $p \mid a_1 a_2 \ldots a_n$, entonces p divide al menos uno de los factores a_i con $i = 1, 2, \ldots, n$.*

Demostración. Sea R un dominio entero, $a_1, a_2, \ldots, a_n \in R$ y $p \in R$ un elemento primo. Demostremos este hecho por inducción. Para el caso base supongamos que $p \mid a_1$ trivialmente se satisface que p divide a algún a_i. Supongamos como hipótesis de inducción que si $p \mid a_1 a_2 \ldots a_{n-1}$ entonces $p \mid a_i$ para algún $i \in \{1, 2 \ldots, n-1\}$. Además, supongamos que $p \mid a_1 a_2 \ldots a_n$. Mostremos ahora que p divide a algún a_i. Como $p \mid a_1 a_2 \ldots a_n$ tenemos que $p \mid (a_1 a_2 \ldots a_{n-1})a_n$. Luego como p es un elemento primo tenemos que $p \mid a_1 a_2 \ldots a_{n-1}$ o $p \mid a_n$. Si $p \mid a_n$ tenemos lo que queríamos. Ahora si $p \mid a_1 a_2 \ldots a_{n-1}$ por hipótesis de inducción tenemos que $p \mid a_i$ para algún $i \in \{1, 2 \ldots, n-1\}$. □

En los números enteros cualquier elemento primo coincide con ser un elemento irreducible y viceversa. Mostremos que en un dominio entero cualquiera, los elementos primos son elementos irreducibles, pero viceversa no.

Lema 2.4.5. *Sea R un dominio entero. Entonces, todo elemento primo es irreducible.*

Demostración. Sea R un dominio entero y $p \in R$ tal que es primo. Veamos que p es irreducible. Supongamos que $p = ab$ para algunas $a, b \in R$. Entonces $p \mid ab$, como p es primo tenemos que $p \mid a$ o $p \mid b$. Sin pérdida de generalidad supongamos que $p \mid b$, esto es existe $c \in R$ tal que $b = pc$. De donde tenemos que $abc = pc = b$ luego por la ley de la cancelación $ac = 1$. Por lo tanto, a es invertible. De manera análoga se muestra que si $p \mid a$ obtenemos que b es invertible. Concluimos que p es irreducible. □

Ejemplo 2.4.6. Veamos unos ejemplos.

1. Consideremos el dominio entero los enteros gaussianos $\mathbb{Z}[i]$. En el ejemplo 2.4.2 mostramos que 5 no es un elemento irreducible en $\mathbb{Z}[i]$, luego por el lema 2.4.5 tenemos que 5 no es un elemento primo.

2. Consideremos el dominio entero de los polinomios en una variable sobre el campo de los complejos $\mathbb{C}[x]$. Sea $x + 2 \in \mathbb{C}[x]$, vimos que este polinomio no es un elemento irreducible (ver 2.4.2) luego por el lema 2.4.5 este polinomio no es un elemento primo.

En general un elemento irreducible no necesariamente es un elemento primo, esto lo veremos en el Capítulo 3. Sin embargo, cuando R es un dominio de ideales principales los elementos irreducibles y primos coinciden.

Teorema 2.4.7. *Sea R un dominio de ideales principales. Un elemento no cero $p \in R$ es irreducible si, y sólo si es un elemento primo.*

Demostración. Sea R un dominio de ideales principales y $0 \neq p \in R$. Supongamos que p es un elemento primo por el lema 2.4.5 tenemos que p es un elemento irreducible.

Supongamos ahora que p es un elemento irreducible y $p \mid ab$. Entonces existe $c \in R$ tal que $pc = ab$. Como R es un dominio de ideales principales entonces el ideal generado por p y a es principal, esto es

$$(p, a) = (d)$$

para algún $d \in R$. Así $p = rd$ para algún $r \in R$. Como p es un elemento irreducible tenemos que r o d es un elemento irreducible.

1. Si d es invertible entonces $(p, a) = (d) = R$. Así, existen $s, t \in R$ para los cuales $1 = sp+ta$. Entonces $b = b1 = b(sp + at) = bsp + (ba)t = p(bs) + (pc)t = p(bs + ct)$. Por lo tanto $p \mid b$.

2. Si r es invertible entonces $d = r^{-1}p$ y así $(p, a) = (d) \subseteq (p)$. De donde $a \in (p)$ y en consecuencia $p \mid a$.

Así en cualquier caso p es un elemento primo de R. □

Para continuar veamos qué ocurre en un dominio de ideales principales cuando tenemos una cadena de ideales.

Teorema 2.4.8. *Sea R un dominio de ideales principales. Si $\{I_n\}$, $n \in \mathbb{Z}^+$ es una secuencia infinita de ideales de R tal que*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots,$$

entonces existe un entero m tal que $I_n = I_m$ para toda $n > m$.

Demostración. Sea R un dominio de ideales principales. Consideremos $\{I_n\}$, $n \in \mathbb{Z}^+$ una secuencia infinita de ideales de R tal que

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

Es sencillo ver que $I = \cup I_n$ es un ideal de R (ver el argumento del teorema 1.3.8). Como R es de ideales principales tenemos que $I = (a)$ para algún $a \in R$. Luego, el elemento a pertenece a alguno de los ideales de la unión, digamos I_m. Para $n > m$, tenemos que

$$I = (a) \subseteq I_m \subseteq I_n \subseteq I \ ;$$

por lo tanto, $I_n = I_m$. □

Con el siguiente lema veremos que los ideales primos y maximales pueden describirse en términos de elementos primos e irreducibles. Decimos que un ideal principal de un anillo R es un **ideal principal maximal** si es maximal (respecto a la inclusión) en el conjunto de los ideales principales propios de R.

Lema 2.4.9. *Sea R un dominio entero y $p \in R$ un elemento distinto de cero. Entonces se satisfacen los siguientes enunciados*

1. *p es un elemento irreducible de R si, y sólo si (p) es un ideal principal maximal;*

2. *p es un elemento primo de R si, y sólo si el ideal principal $(p) \neq R$ es un ideal primo.*

Demostración. Sea R un dominio entero y $0 \neq p \in R$. Probemos 1. Supongamos que p es un elemento irreducible. Sea (a) un ideal principal de R tal que $(p) \subset (a) \subseteq R$. Así $p \in (a)$, es decir existe $r \in R$ tal que $p = ra$. Como p es un elemento irreducible, entonces r o a es invertible .

1. Si r es invertible entonces $a = r^{-1}p \in (p)$. Por lo tanto $(a) \subseteq (p)$, lo cual es una contradicción.

2. Si a es invertible, entonces $(a) = R$.

Por lo tanto no hay ideales principales entre (p) y el anillo R. Así, (p) es un ideal principal maximal.

Supongamos ahora que (p) es un ideal principal maximal de R y que p es un elemento reducible. Entonces p admite una factorización $p = ab$ donde $a, b \in R$, a, b no invertibles. Si p es invertible entonces $(p) = R$, pero esto es una contradicción pues (p) es un ideal propio. Si $a \in (p)$, entonces $a = rp$ para algún $r \in R$; de donde $p = ab = (rp)b$. Por las leyes de la cancelación $1 = rb$, así b es invertible pero esto es una contradicción. Por lo tanto, $a \notin (p)$ dando la inclusión propia $(p) \subset (a)$. Luego, si $(a) = R$ tendríamos que a posee un inverso, lo cual es una contradicción. Así, $(p) \subset (a) \subset R$, contradiciendo el hecho de que (p) es un ideal principal maximal. Por lo tanto p es un elemento irreducible.

Probemos ahora 2. Supongamos que p es un elemento primo de R. Veamos que $(p) \neq R$ y que el ideal (p) es un ideal primo. Como p es un elemento primo entonces p no es invertible de donde $1 \notin (p)$. Por lo tanto $R \neq (p)$. Sea $ab \in (p)$. Entonces existe $r \in R$ tal que $ab = pr$, esto es $p \mid ab$. Así $p \mid a$ o $p \mid b$. Si $p \mid a$ tenemos que $a \in (p)$. Y si $p \mid b$ tenemos que $b \in (p)$. En consecuencia, (p) es un ideal primo de R.

Supongamos ahora que $(p) \neq R$ es un ideal primo y que $p \mid ab$ con $a, b \in R$. Mostremos que p es un elemento primo. Como $(p) \neq R$ entonces $1 \notin (p)$ ya que si $1 \in (p)$ entonces $(p) = R$ lo cual es una contradicción. Así, no existe $s \in R$ para el cual $ps \neq 1$. Por lo tanto p no es invertible. Como $p \mid ab$, entonces $ab \in (p)$. Luego como (p) es un ideal primo, se sigue que $a \in (p)$ o $b \in (p)$. Por lo tanto $p \mid a$ o $p \mid b$. Así p es un elemento primo de R. □

Cuando R es un dominio de ideales principales, el lema 2.4.9 puede resumirse por el siguiente teorema.

Teorema 2.4.10. *Sea R un dominio de ideales principales y $\{0\} \neq (p)$ un ideal de R. Entonces, (p) es un ideal principal maximal (primo) si, y sólo si p es un elemento irreducible (primo).*

Demostración. Esta demostración es directa del lema 2.4.9. □

Ejemplo 2.4.11. Veamos unos ejemplos.

1. Consideremos el dominio de ideales principales de los números enteros $\mathbb{Z}$. Sabemos que un número primo p coincide con un elemento primo. De donde por el teorema 2.4.10, (p) es un ideal maximal en $\mathbb{Z}$.

2. Tomemos el dominio de ideales principales de los enteros gaussianos $\mathbb{Z}[i]$. Sabemos que 5 no es irreducible, luego por el teorema 2.4.10 tenemos que (5) no es un ideal primo.

3. Consideremos el dominio de ideales principales de los polinomios en una variable sobre el campo de los números complejos $\mathbb{C}[x]$. Sea $2 + x \in \mathbb{C}[x]$. Como $2 + x$ es un polinomio irreducible tenemos que el ideal $(2 + x)$ es un ideal maximal.

Para finalizar esta sección veamos que cada elemento de R tal que es no invertible y distinto de cero es divisible por algún primo. Esto es una consecuencia inmediata del teorema 2.4.10.

Corolario 2.4.12. *Sea R un dominio de ideales principales y $0 \neq a \in R$ tal que a es no invertible. Entonces, existe un primo $p \in R$ tal que $p \mid a$.*

Demostración. Sea R un dominio de ideales principales y $0 \neq a \in R$ no invertible. Como a es no invertible entonces $(a) \neq R$. Entonces, como R es finitamente generado, por el teorema 1.3.8 tenemos que existe un ideal maximal M de R tal que $(a) \subseteq M$. Como R es un dominio de ideales principales, entonces $M = (p)$. Luego por el teorema 2.4.10 tenemos que p es un elemento primo. Por lo tanto, $(a) \subseteq (p)$, es decir $p \mid a$.

□

2.5. Dominios de factorización única

Sabemos que en el dominio de los números enteros $\mathbb{Z}$ cada entero n diferente de 0 y 1 tiene una factorización única en números primos. En este capítulo empezamos la tarea de generalizar esta propiedad a dominios enteros. Comenzamos dando la definición de un dominio de factorización única. Damos los ejemplos clásicos de dominios de factorización única, pues necesitamos más herramientas para desarrollar más ejemplos. Finalizamos la sección mostrando que si R es un dominio de ideales principales, entonces R es un dominio de factorización única.

Definición 2.5.1. Sea R un dominio entero. Decimos que R es un dominio de factorización única si se satisfacen los siguientes enunciados:

1. para cada elemento $a \in R$ distinto de cero y no invertible, puede ser factorizado como un producto finito de elementos irreducibles;

2. si $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ son dos factorizaciones de a en elementos irreducibles, entonces $s = t$ y existe una permutación φ en los índices tal que p_i y $q_{\varphi(i)}$ son asociados $(i = 1, 2, \dots, s)$.

Ejemplo 2.5.2. Veamos algunos ejemplos clásicos de la teoría elemental de álgebra.

1. Consideremos el dominio entero de los números enteros $\mathbb{Z}$. Sea $0 \neq a \in \mathbb{Z}$ no invertible. Por el Teorema Fundamental de la Aritmética a tiene una factorización única en elementos irreducibles (primos). Esto es existen $p_1, p_2, \dots, p_k \in \mathbb{Z}$ irreducibles (primos) tales que $a = p_1 p_2 \dots p_k$. Por lo tanto $\mathbb{Z}$ es un dominio de factorización única.

2. Consideremos ahora el dominio entero de los polinomios en una variable sobre el campo de los números complejos $\mathbb{C}[x]$. Sabemos que en $\mathbb{C}[x]$ existe un análogo al Teorema Fundamental de la Aritmética, por lo tanto $\mathbb{C}[x]$ es un dominio de factorización única.

Para ver ejemplos de dominios enteros que no sean dominios de factorización única nos faltan varias herramientas que construiremos a lo largo de esta sección y la sección siguiente. En el Capítulo 3. veremos este ejemplo.

En resumen, un dominio entero es un dominio de factorización única si posee una teoría de factorización en la cual se mantiene el análogo del Teorema Fundamental de la Aritmética. En el ejemplo 2.5.2 podemos observar que en ambos casos los dominios enteros que consideramos

son dominios de ideales principales. Por lo cual pretendemos mostrar que cualquier dominio de ideales principales es un dominio de factorización única. Para demostrar este hecho veamos primero el siguiente teorema.

Teorema 2.5.3. *Sea R un dominio de ideales principales. Entonces, cada $a \in R$ distinto de cero y no invertible tiene una factorización en un producto finito de primos (irreducibles).*

Demostración. Sea R un dominio de ideales principales y $0 \neq a \in R$ no invertible. Por el corolario 2.4.12 existe un primo $p_1 \in R$ tal que $p_1 \mid a$. Entonces $a = p_1a_1$ para algún $0 \neq a_1 \in R$, de donde $(a) \subset (a_1)$. Si $(a) = (a_1)$, tendríamos que $a_1 = r_1a$ para algún $0 \neq r_1 \in R$. Se sigue que $a = p_1a_1 = p_1(r_1a)$, como $0 \neq a$ por las leyes de la cancelación tenemos que $1 = p_1r$, lo cual es una contradicción al hecho de que p_1 es no invertible. Así tenemos la inclusión propia $(a) \subset (a_1)$.

Si a_1 es invertible entonces $a = p_1a_1$ tiene una factorización en un producto finito de primos, ya que a es en sí mismo un elemento primo (ver 2.4.3). Si a_1 no es invertible, entonces por el corolario 2.4.12 existe $p_2 \in R$ primo tal que $p_2 \mid a_1$. Esto es $a_1 = p_2a_2$ para algún $a_2 \in R$, de donde $(a_1) \subseteq (a_2)$. Si $(a_1) = (a_2)$, tendríamos que $a_2 = r_2a_1$ para algún $r_2 \in R$. Luego, $a_1 = p_2a_2 = p_2(r_2a_1)$ y por las leyes de la cancelación $1 = p_2r_2$ lo cual es una contradicción. Por lo tanto $(a_1) \subset (a_2)$. Nuevamente si a_2 es invertible, entonces a se puede expresar como un producto finito de primos $a = p_1a_1 = p_1p_1'$ donde $p_1' = p_2a_2$ es un elemento primo ya que es un asociado de un elemento primo (ver 2.4.3). Si a_2 no es un elemento primo continuaremos este proceso, así obtenemos la siguiente cadena de ideales principales

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \ldots,$$

con $a_{n-1} = p_na_n$ para algún $p_n \in R$ primo. Este proceso continúa mientras a_n no sea invertible. Pero por el teorema 2.4.8 tenemos que esta cadena eventualmente termina. Es decir, a_n debe poseer un inverso para alguna n y

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) = R.$$

Así concluimos que el elemento a se puede expresar como un producto finito de primos

$$a = p_1p_2 \ldots p_{n-1}p_n',$$

donde $p_n' = p_na_n$, es decir p_n' es un asociado de un elemento primo, de donde p_n' es primo. □

Para ilustrar el siguiente corolario, veamos un ejemplo.

Ejemplo 2.5.4. Consideremos el dominio de ideales principales de los números enteros $\mathbb{Z}$. Sea $10 \in \mathbb{Z}$ por el Teorema Fundamental de la Aritmética $10 = 2 \cdot 5$. Veamos quién es el producto de los ideales $(2)(5)$. Sabemos que

$$(2)(5) = \{ \sum_{finita} a_ib_i : a_i \in (2), b_i \in (5)\}$$

(ver 1.2.12). Como $a_i \in (2)$ entonces existe $k_i \in \mathbb{Z}$ tal que $a_i = 2k_i$, analogamente existe $t_i \in \mathbb{Z}$ tal que $b_i = 5t_i$ así

$$\begin{aligned}(2)(5) = \{ \sum_{finita} a_ib_i : a_i \in (2), b_i \in (5)\} = \{ \sum_{finita} (2k_i)(5t_i) : k, t \in \mathbb{Z}\} = \\ = \{10 \sum_{finita} k_it_i : k_i, t_i \in \mathbb{Z}\} = \{10z : z \in \mathbb{Z}\} = (10).\end{aligned}$$

Es decir, en este caso el ideal generado por 10 se puede expresar como el producto de dos ideales primos. Veamos que esto lo podemos generalizar a cualquier dominio de ideales principales.

Corolario 2.5.5. *Sea R un dominio de ideales principales. Entonces cada ideal no trivial es el producto de un número finito de ideales primos (maximales).*

Demostración. Sea R un dominio de ideales principales e I un ideal no trivial de R. Entonces existe $0 \neq a \in R$ tal que $I = (a)$. Por el teorema 2.5.3 a puede ser factorizado como un producto finito de primos, digamos $a = p_1 p_2 \dots p_k$ donde p_i es un elemento primo de R. Veamos que $(a) = (p_1 p_2 \dots p_k) = (p_1)(p_2)\dots(p_k) = \{ \sum_{finita} a_1 a_2 \dots a_k : a_i \in (p_i)\}$. Es claro que $(a) \subseteq (p_1)(p_2)\dots(p_k)$. Mostremos la otra contención. Sea $b \in (p_1)(p_2)\dots(p_k) = \{ \sum_{finita} a_1 a_2 \dots a_k : a_i \in (p_i)\}$, entonces $b = \sum_{finita} a_1 a_2 \dots a_k$ donde $a_i \in (p_i)$. Como $a_i \in (p_i)$ existe $t_i \in R$ tales que $a_i = t_i p_i$. Por lo tanto

$$b = \sum_{finita} a_1 a_2 \dots a_k = \sum_{finita} t_1 p_1 \dots t_k p_k = \sum_{finita} (p_1 \dots p_k) t' \in (p_1 p_2 \dots p_k)$$

donde $t' = t_1 t_2 \dots t_k$. Por lo tanto $(a) = (p_1 p_2 \dots p_k) = (p_1)(p_2)\dots(p_k)$. □

Ahora veamos un resultado célebre en el anillo de los números enteros.

Teorema (Euclides) 2.5.6. *Hay una infinidad de números primos en el anillo de los números enteros $\mathbb{Z}$.*

Demostración. Consideremos el anillo de los números enteros $\mathbb{Z}$. Supongamos que hay un número finito de números primos, digamos $p_1, p_2, \dots, p_k$. Consideremos el entero positivo

$$a = p_1 p_2 \dots p_k + 1.$$

Notemos que ninguno de los primos p_i en la lista divide a a. Si a fuera divisible por p_i para algún i, entonces $p_i \mid a - p_1 p_2 \dots p_k$. Así $p_i \mid 1$, pero esto no es posible pues p_i no es invertible. Como $a > 1$ tenemos que a no es invertible, luego por el teorema 2.5.3 existe un primo tal que es factor de a. Así, a es divisible por un primo que no está en la lista. Por lo tanto, no hay una lista finita de números primos.

□

En el teorema 2.5.3 probamos que en un dominio de ideales principales cada elemento que es no invertible y distinto de cero tiene una factorización en primos, veamos ahora que esta factorización es única.

Teorema 2.5.7. *Sea R un dominio de ideales principales. Entonces R es un dominio de factorización única.*

Demostración. Sea R un dominio de ideales principales y $0 \neq a \in R$ no invertible. Por el teorema 2.5.3 sabemos que a tiene una factorización en elementos primos, es decir $a = p_1 p_2 \dots p_k$ con $p_i \in R$ elementos primos. Mostremos ahora que esta factorización es única. Supongamos que existe otra factorización de a, esto es $a = q_1 q_2 \dots q_m$ con $q_i \in R$ elementos primos y $k \leq m$. Como $a = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m$ tenemos que $p_1 \mid q_1 q_2 \dots q_m$, se sigue que p_1 divide a algún q_i para $1 \leq i \leq m$. Renumerando, si es necesario, podemos suponer que $p_1 \mid q_1$. Ahora, p_1 y q_1 son elementos primos de R, con $p_1 \mid q_1$, de modo que deben ser asociados esto es $q_1 = p_1 u$ para algún

elemento invertible $u \in R$. Así $p_1 p_2 \dots p_k = p_1 u q_2 \dots q_m$. Luego, por las leyes de la cancelación tenemos que

$$p_2 \dots p_k = u q_2 \dots q_m.$$

Continuando con este argumento, tenemos que (luego de k pasos)

$$1 = u_1 u_2 \dots u_k q_{k+1} \dots q_m.$$

Como q_i son elementos no invertibles, entonces $k = m$. Además cada p_i es asociado de algún q_i y viceversa. Por lo tanto, estas dos factorizaciones en elementos primos son idénticas, aparte del orden en que aparecen los factores y del reemplazo de factores por sus asociados. □

Veamos que el recíproco de este teorema no es siempre cierto. Para mostrar esto necesitaremos el siguiente teorema.

Teorema 2.5.8. *Sea R un dominio de factorización única. Entonces $R[x]$ es dominio de factorización única.*

Demostración. Ver [2, pág. 125] □

Ejemplo 2.5.9. Mostremos un ejemplo de un dominio entero que es de factorización única pero no es un dominio de ideales principales. Consideremos el dominio entero de los polinomios en una variable sobre los números enteros $\mathbb{Z}[x]$. Como $\mathbb{Z}$ es un dominio de factorización única entonces $\mathbb{Z}[x]$ también es un dominio de factorización única, pero no es un dominio de ideales principales.

Observación 2.5.10. Sea R un dominio de factorización única. Mostremos que en R los elementos primos e irreducibles coinciden. Como R es en particular un dominio entero tenemos que todo elemento primo es un elemento irreducible. Consideremos ahora $p \in R$ un elemento irreducible. Veamos que p es primo. Supongamos que $p \mid ab$, es decir existe $c \in R$ tal que $pc = ab$. Dado que R es de factorización única entonces a, b y c se pueden factorizar en elementos primos como

$$a = p_1 p_2 \dots p_n, \quad b = q_1 q_2 \dots q_m, \quad \text{y} \quad c = t_1 t_2 \dots t_s.$$

Así, tenemos que

$$p_1 p_2 \dots p_n q_1 \dots q_m = ab = p t_1 t_2 \dots t_s.$$

Como la factorización de ab es única, el elemento p debe ser asociado de p_i o de q_i, y, en consecuencia, p divide a a o b.

2.6. Dominios Euclidianos

En esta sección retomamos los dominios Euclidianos. Estos surgen al generalizar el algoritmo de la división de los números enteros a anillos arbitrarios. Comenzamos reescribiendo la definición de estos dominios y algunas de las propiedades que ya se vieron en la sección 2.1.

Definición 2.6.1. Sea R un dominio entero. Decimos que R es *Euclidiano* (o dominio entero Euclidiano o dominio Euclidiano) si existe una función

$$\delta : R \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

llamada *valuación euclidiana* que satisface las siguientes condiciones

1. Para cualesquiera $a, b \in R$, ambos no cero, $\delta(ab) \geq \delta(a)$;
2. Para cualesquiera $a, b \in R$, con $b \neq 0$, existen $q, r \in R$ (llamados el *cociente* y el *residuo*) tales que $a = qb + r$, con $r = 0$ ó $\delta(r) < \delta(b)$.

Para recordar algunos ejemplos de dominios Euclidianos ver 2.1.24. Veamos ahora algunas propiedades de un dominio Euclidiano.

Lema 2.6.2. *Sea R un dominio Euclidiano con valuación δ. Entonces se satisfacen los siguientes*

1. *para cada $0 \neq a \in R$ se tiene que $\delta(a) \geq \delta(1)$;*
2. *si $a, b \in R$ son elementos no nulos tales que son asociados, entonces $\delta(a) = \delta(b)$;*
3. *un elemento $0 \neq a \in R$ es invertible si, y sólo si $\delta(a) = \delta(1)$.*

Demostración. Sean R un dominio Euclidiano con valuación δ y $a, b \in R$ elementos no nulos. Probemos 1. Sabemos que $a = a1$, de donde

$$\delta(a) = \delta(a1) \geq \delta(1).$$

Mostremos 2. Para esto supongamos que a y b son asociados. Entonces $a = bu$ con $u \in R$ un elemento invertible, de donde $b = au^{-1}$. Así

$$\delta(a) = \delta(bu) \geq \delta(b) \qquad \text{y} \qquad \delta(b) = \delta(au^{-1}) \geq \delta(a).$$

Por lo tanto $\delta(a) = \delta(b)$.

Por último demostremos 3. Supongamos que $0 \neq a \in R$ es un elemento invertible en R, es decir existe $b \in R$ tal que $ab = 1$. Por 1. tenemos que

$$\delta(a) \leq \delta(ab) = \delta(1) \leq \delta(a),$$

por lo tanto $\delta(a) = \delta(1)$.

Supongamos ahora que $0 \neq a \in R$ es tal que $\delta(a) = \delta(1)$. Aplicando el inciso 3. de la definición 2.6.1 tenemos que

$$1 = qa + r,$$

con $r = 0$ o $\delta(r) < \delta(a)$. Si $\delta(r) < \delta(a)$, entonces $\delta(r) < \delta(1)$, lo cual no puede pasar. Así $r = 0$, de donde $1 = aq$. Por lo tanto a es invertible en R. □

Ejemplo 2.6.3. Veamos un ejemplo para introducir el siguiente teorema. Recordemos que el dominio entero de los números enteros $\mathbb{Z}$ es un dominio Euclidiano con la valuación

$$\delta : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

dada por $\delta(a) =\mid a \mid$ (ver 2.1.24). Observemos que para $a = 7$ y $b = 4$ tenemos que

$$7 = 4(1) + 3 \text{ con } \mid 3 \mid < \mid 4 \mid$$
$$7 = 4(2) + (-1) \text{ con } \mid -1 \mid < \mid 4 \mid.$$

Por lo cual, con esta definición el cociente y el residuo no son necesariamente únicos. Notemos que en el algoritmo de la división de los cursos básicos de álgebra pedíamos que el residuo fuera mayor que cero.

El siguiente teorema nos muestra las condiciones necesarias y suficientes para que en un dominio Euclidiano el cociente y el residuo sean únicos.

Teorema 2.6.4. *Sean R un dominio Euclidiano y $a, b \in R$ distintos de cero. Entonces el cociente y el residuo son únicos si, y sólo si*

$$\delta(a+b) \leq max\{\delta(a), \delta(b)\}.$$

Demostración. Sea R un dominio Euclidiano con valuación δ. Supongamos que el cociente y el residuo son únicos. Sean $a, b \in R$ elementos no cero tales que

$$\delta(a+b) > max\{\delta(a), \delta(b)\}.$$

Entonces, podemos escribir a b como sigue

$$b = 0(a+b) + b$$
$$b = 1(a+b) - a.$$

Como a y $-a$ son asociados tenemos que

$$\delta(-a) = \delta(a) \leq max\{\delta(a), \delta(b)\} < \delta(a+b),$$

además $\delta(b) < \delta(a+b)$. Por lo tanto para b y $a+b$ el cociente y el residuo no es único, lo cual es una contradicción. Por lo tanto, $\delta(a+b) \leq max\{\delta(a), \delta(b)\}$.

Supongamos ahora que se satisface la desigualdad para cualesquiera dos elementos no nulos $a, b \in R$ y que a tiene dos representaciones. Digamos

$$a = qb + r \text{ con } r = 0 \text{ o } \delta(r) < \delta(b),$$
$$a = q'b + r' \text{ con } r' = 0 \text{ o } \delta(r') < \delta(b),$$

donde $r \neq r'$ o $q \neq q'$. Notemos que $r \neq r'$ si, y sólo si $q \neq q'$. Como $qb + r = q'b + r'$ tenemos que $(q-q')b = r - r'$, así si $r \neq r'$ entonces $r - r' \neq 0$. Luego $(q-q')b \neq 0$ y por tanto $q - q' \neq 0$. De manera similar si $q \neq q'$ como $b \neq 0$ entonces $(q-q')b \neq 0$ y por tanto $r - r' \neq 0$. Por lo tanto $r \neq r'$ y $q \neq q'$. Luego como R es un dominio Euclidiano tenemos que

$$\delta(b) \leq \delta((q-q')b) = \delta(r - r') < max\{\delta(r), \delta(-r')\} < \delta(b).$$

Pero esto es una contradicción, como ya observamos que $r \neq r'$ si, y sólo si $q \neq q'$ tenemos que $r = r'$ y $q = q'$.

□

Corolario (Algoritmo de la división para $\mathbb{Z}$) 2.6.5. *Si $a, b \in \mathbb{Z}$, con $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que*

$$a = qb + r, \quad 0 \leq r < \mid b \mid.$$

Demostración. Consideremos la valuación dada por $\delta(n) = \mid n \mid$. Sean $a, b \in \mathbb{Z}$ con b no nulo. Primero veamos el caso en que b es un entero positivo y sea S el siguiente conjunto

$$S = \{a - tb : t \in \mathbb{Z} \text{ y } a - tb \geq 0\}.$$

Veamos que para cualquier entero a este conjunto es distinto del vacío.

1. Si $a > 0$, entonces $a - 0b > 0$. Por lo tanto $a \in S$.
2. Si $a \leq 0$, haciendo $t = a - 1$, obtenemos que $a - tb = a - (a-1)b = a(1-b) + b > 0$, ya que $1 - b \leq 0$. Por lo tanto $a - tb \in S$.

Así, para cualquier entero a tenemos que S es un subconjunto no vacío de $\mathbb{Z}^+ \cup \{0\}$. Luego, por el principio del buen orden para $\mathbb{Z}^+ \cup \{0\}$ sea r el elemento mínimo de S. Entonces existe $q \in \mathbb{Z}$ tal que $r = a - qb$, de donde $a = qb + r$ con $r \geq 0$. Veamos ahora que $r <\mid b \mid$. Supongamos que $b > 0$ y que $r \geq b = \mid b \mid$. Entonces $r - b \geq 0$, así

$$0 \leq r - b = a - qb - b = a - (q+1)b.$$

Se sigue que $r - b = a - (q+1)b \in S$ y es tal que $r - b < r$ pues $b > 0$, lo cual contradice que r sea el mínimo de S. Por lo tanto existen q y r con las condiciones requeridas.

Supongamos ahora que $b < 0$. Por lo probado en el caso anterior, como $-b > 0$, existen dos enteros q y r tales que $a = (-b)q + r$ y $0 \leq r < -b = \mid b \mid$. Entonces, se tiene que $a = b(-q) + r$ con $0 \leq r < -b = \mid b \mid$.

Probemos la unicidad. Supongamos que existen $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales que $a = q_1 b + r_1$ y $a = q_2 b + r_2$, con $0 \leq r_1 <\mid b \mid$ y $0 \leq r_2 <\mid b \mid$. Entonces

$$b(q_1 - q_2) = r_1 - r_2.$$

así $b \mid r_1 - r_2$ y por la Teoría básica de divisibilidad tenemos que $\mid b \mid \leq \mid r_1 - r_2 \mid$. Como $0 \leq r_1 <\mid b \mid$ y $0 \leq r_2 <\mid b \mid$, por los cursos básicos de álgebra tenemos que $\mid r_1 - r_2 \mid <\mid b \mid$. Por lo tanto $r_1 - r_2 = 0$, es decir $r_1 = r_2$. Por último, $b(q_1 - q_2) = r_1 - r_2 = 0$ y como $b \neq 0$ tenemos que $q_1 - q_2 = 0$ y por tanto $q_1 = q_2$. □

La factorización única en el dominio de los números enteros $\mathbb{Z}$ está estrechamente ligada con el algoritmo de la división. Por lo tanto queremos demostrar que para dominios enteros en los cuales existe un análogo al algoritmo de la división, podemos probar la unicidad de una factorización. Para mostrar este hecho veamos primero el siguiente resultado.

Teorema 2.6.6. *Cada dominio Euclidiano es un dominio de ideales principales.*

Demostración. Ver 2.1.26. □

Enunciemos un ejemplo que no todo dominio de ideales principales es un dominio Euclidiano.

Ejemplo 2.6.7. Consideremos el dominio entero

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

con $\omega = \frac{1}{2}(1 + \sqrt{-19})$. Es un dominio de ideales principales, sin embargo $\mathbb{Z}[\omega]$ no es un dominio Euclidiano. Por falta de espacio no veremos esta demostración.

Corolario 2.6.8. *Cada dominio Euclidiano es un dominio de factorización única.*

Demostración. Sea R un dominio Euclidiano. Por el teorema 2.6.6 tenemos que R es un dominio de ideales principales. Luego por el teorema 2.5.7 tenemos que R es un dominio de factorización única. □

Para concluir este capítulo veamos dos nuevos dominios enteros: el campo de los números cuadráticos y los dominios cuadráticos. Empezamos mencionando qué significa que un entero n sea libre de cuadrados.

Definición 2.6.9. Sea $1 \neq n \in \mathbb{Z}$. Decimos que n es un entero libre de cuadrados si para todo $b \in \mathbb{Z}^+$ con $b > 1$ tenemos que b^2 no divide a n en $\mathbb{Z}$.

Ejemplo 2.6.10. Veamos algunos ejemplos.

1. Consideremos $n = 2$. Los únicos divisores de 2 son $\{-2, -1, 1, 2\}$. Notemos que ninguno de estos divisores es de la forma b^2 para algún $b \in \mathbb{Z}$ con $b > 1$. Por lo tanto 2 es un entero libre de cuadrados.

2. Consideremos $n = -3$. De manera análoga, los divisores de -3 son $\{-3, -1, 1, 3\}$. Por lo tanto -3 es un entero libre de cuadrados.

3. Sea $n = 40$. Este entero no es libre de cuadrados, pues $4 \mid 40$ y $4 = 2^2$.

Lema 2.6.11. *Sea $n \in \mathbb{Z}$ un entero libre de cuadrados. Entonces $\sqrt{n} \notin \mathbb{Q}$.*

Demostración. Sea $n \in \mathbb{Z}$ tal que es libre de cuadrados. Supongamos que $\sqrt{n} \in \mathbb{Q}$. Por lo tanto existen $a, b \in \mathbb{Z}$ $b \neq 0$ y sin factores comunes tales que

$$\sqrt{n} = \frac{a}{b}.$$

Así, $n = \dfrac{a^2}{b^2}$. Luego como $n \in \mathbb{Z}$ y a, b no tienen factores en común tenemos que $b^2 = 1$. Por tanto $n = a^2$, pero esto es una contradicción pues n es libre de cuadrados. □

Definición 2.6.12. Sea $1 \neq n \in \mathbb{Z}$ un entero libre de cuadrados. Definimos el campo cuadrático $\mathbb{Q}(\sqrt{n})$ como el conjunto

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}.$$

Notemos que cuando $n > 0$ el campo cuadrático $\mathbb{Q}(\sqrt{n})$ es un subconjunto de los números reales, y cuando $n < 0$ el campo cuadrático $\mathbb{Q}(\sqrt{n})$ es un subconjunto de los números complejos.

Observación 2.6.13. Sean $n_1, n_2 \in \mathbb{Z}$ enteros libres de cuadrados. Entonces $\mathbb{Q}(\sqrt{n}_1) = \mathbb{Q}(\sqrt{n}_2)$ si, y sólo si $n_1 = n_2$.

Es claro que si $n_1 = n_2$ entonces sus respectivos campos cuadráticos coinciden. Veamos que si $\mathbb{Q}(\sqrt{n}_1) = \mathbb{Q}(\sqrt{n}_2)$ entonces $n_1 = n_2$. Como $\mathbb{Q}(\sqrt{n}_1) = \mathbb{Q}(\sqrt{n}_2)$ y $\sqrt{n}_1 \in \mathbb{Q}(\sqrt{n}_1)$ tenemos que existen $a, b \in \mathbb{Q}$ tales que $\sqrt{n}_1 = a + b\sqrt{n}_2$. De donde

$$n_1 = a^2 + 2ab\sqrt{n}_2 + b^2 n_2.$$

Si $a \neq 0$ y $b \neq 0$ entonces tenemos que

$$\sqrt{n}_2 = \frac{n_1 - a^2 - b^2 n_2}{2ab} \in \mathbb{Q}.$$

Por el lema 2.6.11 esto no es posible, por lo tanto $a = 0$ o $b = 0$.

1. Si $b = 0$ tenemos que $\sqrt{n}_1 = a$. De donde $n_1 = a^2$, lo cual es una contradicción pues n_1 es libre de cuadrados.

2. Si $a = 0$ tenemos que $\sqrt{n}_1 = 0 + b\sqrt{n}_2 = b\sqrt{n}_2$ de donde $n_1 = b^2 n_2$. La única forma en la que esto es posible es cuando $b = 1$. Por lo tanto $\sqrt{n}_1 = \sqrt{n}_2$, de donde $n_1 = n_2$.

Cada elemento $\alpha = a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ da origen a otro elemento $\overline{\alpha} = a - b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$. A este elemento $\overline{\alpha}$ lo llamamos **el conjugado** de α. Cuando $n < 0$ tenemos que $\overline{\alpha}$ es el complejo conjugado usual de α.

Para estudiar las propiedades de divisibilidad del campo cuadrático $\mathbb{Q}(\sqrt{n})$, introducimos el concepto de la norma de un elemento, éste es un análogo a la noción del valor absoluto que tenemos en el dominio de los números enteros $\mathbb{Z}$.

Definición 2.6.14. Sea $\alpha = a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$. Definimos la norma de α como el producto de α por su conjugado $\overline{\alpha}$ y la denotamos por $N(\alpha)$. Es decir,

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - b^2 n.$$

Lema 2.6.15. *Sean $\alpha, \beta \in \mathbb{Q}(\sqrt{n})$. Entonces $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.*

Demostración. Sean $\alpha, \beta \in \mathbb{Q}(\sqrt{n})$, tales que $\alpha = a + b\sqrt{n}$ y $\beta = c + d\sqrt{n}$, con $a, b, c, d \in \mathbb{Q}$. Por un lado

$$\overline{\alpha}\overline{\beta} = (a - b\sqrt{n})(c - d\sqrt{n}) = (ac + bdn) - (ad + bc)\sqrt{n}.$$

Y por otra parte

$$\overline{\alpha\beta} = \overline{(a + b\sqrt{n})(c + d\sqrt{n})} = \overline{(ac + bdn) + (ad + bc)\sqrt{n}} = (ac + bdn) - (ad + bc)\sqrt{n}.$$

Por lo tanto $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$. □

Ejemplo 2.6.16. Veamos algunos ejemplos.

1. Consideremos el campo cuadrático $\mathbb{Q}(\sqrt{-2})$. Sean $\frac{1}{3} + \sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$. Entonces la norma de este elemento es

$$N(\frac{1}{3} + \sqrt{-2}) = (\frac{1}{3} + \sqrt{-2})(\frac{1}{3} - \sqrt{-2}) = \frac{1^2}{3^2} - 1^2(-2) = \frac{19}{9}.$$

2. Tomemos el campo cuadrático $\mathbb{Q}(\sqrt{17})$. Sea $1 + 2\sqrt{17} \in \mathbb{Q}(\sqrt{17})$. Calculemos la norma de este elemento

$$N(1 + 2\sqrt{17}) = (1 + 2\sqrt{17})(1 - 2\sqrt{17}) = 1^2 - 2^2(17) = -67.$$

Esto muestra que la norma de un elemento no necesariamente es un número entero positivo. Veamos algunas propiedades de la norma de un elemento en el campo cuadrático $\mathbb{Q}(\sqrt{n})$.

Lema 2.6.17. *Sean $\alpha, \beta \in \mathbb{Q}(\sqrt{n})$. Entonces se satisfacen los siguientes*

1. *$N(\alpha) = 0$ si, y sólo si $\alpha = 0$;*
2. *$N(\alpha\beta) = N(\alpha)N(\beta)$;*
3. *$N(1) = 1$.*

Demostración. Sea $\alpha \in \mathbb{Q}(\sqrt{n})$. Probemos 1. Supongamos que $N(\alpha) = a^2 - b^2 n = 0$, esto pasa si, y sólo si $a = 0$ y $b = 0$. Ya que si $b \neq 0$ tendríamos que $n = \dfrac{a^2}{b^2} = \left(\dfrac{a}{b}\right)^2$. Como n es un número entero $b = 1$ o $\dfrac{a}{b} \in \mathbb{Z}$, pero esto querría decir que n no es libre de cuadrados, lo cual es una contradicción. Luego si $b = 0$ tenemos que $a^2 = 0$, y así $a = 0$. Por lo tanto $\alpha = 0$.

Probemos 2. Sean $\alpha, \beta \in \mathbb{Q}(\sqrt{n})$, tales que $\alpha = a + b\sqrt{n}$ y $\beta = c + d\sqrt{n}$, con $a, b, c, d \in \mathbb{Q}$. Por el lema 2.6.15 tenemos que

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

□

Por último probemos 3. Como $N(1) = N(1^2)$ por 2. tenemos que

$$N(1) = N(1^2) = N(1)N(1) = N(1)^2.$$

Por lo tanto $N(1) = 1$.

Aunque hemos etiquetado a $\mathbb{Q}(\sqrt{n})$ como un campo, en realidad no hemos demostrado que sea así. Mostremos esto en el siguiente teorema.

Teorema 2.6.18. *Sea n entero libre de cuadrados. Entonces, el campo cuadrático $\mathbb{Q}(\sqrt{n})$ es un campo.*

Demostración. Sea $\mathbb{Q}(\sqrt{n})$ el campo cuadrático. Es sencillo ver que $\mathbb{Q}(\sqrt{n})$ es un anillo conmutativo con uno. Veamos que para cualquier $0 \neq \alpha \in \mathbb{Q}(\sqrt{n})$ podemos encontrar un inverso multiplicativo. Como $\alpha \neq 0$ entonces el elemento $\beta = \dfrac{\overline{\alpha}}{N(\alpha)}$ pertenece al campo cuadrático $\mathbb{Q}(\sqrt{n})$. Más aún, tomando el producto de estos dos elementos tenemos que

$$\alpha\beta = \alpha\frac{\overline{\alpha}}{N(\alpha)} = \frac{N(\alpha)}{N(\alpha)} = 1.$$

Por lo tanto β es el inverso multiplicativo de α. Y así $\mathbb{Q}(\sqrt{n})$ es un campo. □

Contenido en cada campo cuadrático $\mathbb{Q}(\sqrt{n})$ se encuentra el dominio entero

$$\mathbb{Z}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}.$$

Llamaremos a este conjunto el **dominio cuadrático**. Es sencillo ver que este conjunto es un anillo conmutativo con uno. Luego como $\mathbb{Z}(\sqrt{n}) \subset \mathbb{Q}(\sqrt{n})$ y $\mathbb{Q}(\sqrt{n})$ es en particular un dominio entero (ya que es un campo), tenemos que $\mathbb{Z}(\sqrt{n})$ es también un dominio entero, ya que si no lo fuera implicaría que existe un divisor de cero en $\mathbb{Q}(\sqrt{n})$.

Notemos que si $\alpha \in \mathbb{Z}(\sqrt{n})$ entonces $\overline{\alpha} \in \mathbb{Z}(\sqrt{n})$. Así como $\mathbb{Z}(\sqrt{n})$ es cerrado bajo la conjugación, la norma nos permite tener una visión clara de los conjuntos de elementos invertibles e irreductibles en estos dominios. Por ejemplo, la propiedad multiplicativa de la norma, transfiere cualquier factorización $\alpha = \beta\gamma$ de un elemento $\alpha \in \mathbb{Z}(\sqrt{n})$ a una factorización $N(\alpha) = N(\beta)N(\gamma)$ del entero $N(\alpha)$. Esto es muy útil para demostrar el siguiente lema.

Lema 2.6.19. *Sea $\alpha \in \mathbb{Z}(\sqrt{n})$. Entonces los siguientes se satisfacen*

1. *$N(\alpha) = \pm 1$ si, y sólo si α es invertible en $\mathbb{Z}(\sqrt{n})$;*

2. *Si $N(\alpha) = \pm p$, donde p es un número primo, entonces α es un elemento irreducible de $\mathbb{Z}(\sqrt{n})$.*

Demostración. Sea $\alpha \in \mathbb{Z}(\sqrt{n})$. Probemos 1. Supongamos que $N(\alpha) = \pm 1$. Es decir, $\alpha\overline{\alpha} = \pm 1$, por lo tanto $\alpha \mid 1$. De donde α es invertible. Supongamos ahora que α es invertible, esto es existe $\beta \in \mathbb{Z}(\sqrt{n})$ tal que $\alpha\beta = 1$. Entonces,

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

Como $N(\alpha), N(\beta)$ son números enteros, tenemos que $N(\alpha) = \pm 1$.

Ahora probemos 2. Supongamos que α tiene la propiedad de que $N(\alpha) = \pm p$, con p un número primo. Como $N(\alpha) \neq 0, 1$, el elemento α es distinto de cero y es no invertible en $\mathbb{Z}(\sqrt{n})$. Si $\alpha = \beta\gamma$ es una factorización de α en $\mathbb{Z}(\sqrt{n})$, entonces

$$N(\beta)N(\gamma) = N(\alpha) = \pm p.$$

Como p es un número primo, se sigue que $N(\beta)$ o $N(\gamma)$ debe valer ± 1. Por lo anterior, concluimos que β o γ es invertible en $\mathbb{Z}(\sqrt{n})$. Por lo tanto α es un elemento irreducible en $\mathbb{Z}(\sqrt{n})$. □

Ejemplo 2.6.20. Consideremos el dominio de los enteros gaussianos $\mathbb{Z}[i] = \mathbb{Z}(\sqrt{-1})$. Veamos quiénes son los elementos invertibles en este dominio entero. Sea $\alpha \in \mathbb{Z}[i]$ tal que $\alpha = a + bi$ y α es invertible, esto es $N(\alpha) = a^2 + b^2 = 1$, suponemos que la norma es positiva ya que a^2, b^2 son enteros positivos. Como $a^2 + b^2 = 1$, esta ecuación tiene por soluciones $a = 0$ y $b = \pm 1$ o $a = \pm 1$ y $b = 0$. Por lo tanto, los elementos invertibles de $\mathbb{Z}[i]$ son ± 1 y $\pm i$.

Sabemos que los dominios cuadráticos $\mathbb{Z}(\sqrt{n})$ son dominios enteros, por lo cual nos podríamos preguntar si éstos también resultan ser dominios de factorización única. Para responder esta pregunta, nos gustaría mostrar que $\mathbb{Z}(\sqrt{n})$ es un dominio Euclidiano. Una valuación que se ocurre de manera inmediata es aquella dada por $\delta(a) =\mid N(\alpha) \mid$ para $\alpha \in \mathbb{Z}(\sqrt{n})$. En el siguiente teorema demostramos que los dominios cuadráticos $\mathbb{Z}(\sqrt{-1}), \mathbb{Z}(\sqrt{-2}), \mathbb{Z}(\sqrt{2}), \mathbb{Z}(\sqrt{3})$, son dominios Euclidianos y en consecuencia son dominios de factorización única.

Teorema 2.6.21. *Cada uno de los dominios $\mathbb{Z}(\sqrt{n})$, donde $n = -1, -2, 2, 3$, es un dominio de factorización única.*

Demostración. Consideremos los dominios cuadráticos $\mathbb{Z}(\sqrt{n})$ para $n = -1, -2, 2, 3$, y consideremos la función $\delta : \mathbb{Z}(\sqrt{n}) \longrightarrow \mathbb{Z}^+$ definida por $\delta(\alpha) =\mid N(\alpha) \mid$. Veamos que la función δ es una valuación Euclidiana para $n = -1, -2, 2, 3$. Claramente $\delta(\alpha) = 0$ si, y sólo si $\alpha = 0$, por tanto $\delta(\alpha) \geq 1$ para toda $\alpha \neq 0$. Si $\alpha, \beta \in \mathbb{Z}(\sqrt{n})$ y ambos son distintos de cero, por propiedades de la norma y el valor absoluto tenemos que

$$\delta(\alpha\beta) =\mid N(\alpha\beta) \mid=\mid N(\alpha)N(\beta) \mid=\mid N(\alpha) \mid\mid N(\beta) \mid= \delta(\alpha)\delta(\beta) \geq \delta(\alpha) \cdot 1 = \delta(\alpha).$$

Como $\beta \neq 0$, el producto $\alpha\beta^{-1} \in \mathbb{Q}(\sqrt{n})$ y se puede escribir de la forma $\alpha\beta^{-1} = a + b\sqrt{n}$ para $a, b \in \mathbb{Q}$. Podemos seleccionar enteros x, y (los más cercanos a a y b) tales que

$$\mid a - x \mid\leq \frac{1}{2}, \qquad\qquad \mid b - y \mid\leq \frac{1}{2}.$$

Sea $\sigma = x + y\sqrt{n}$. Entonces $\sigma \in \mathbb{Z}(\sqrt{n})$ y

$$\mid N(\alpha\beta^{-1} - \sigma) \mid=\mid N((a - x) + (b - y)\sqrt{n}) \mid=\mid (a - x)^2 - n(b - y)^2 \mid$$

Luego, por la elección de y y x tenemos que

$$-\frac{n}{4} \leq (a-x)^2 - n(b-y)^2 \leq \frac{1}{4}, \quad \text{si} \quad n \geq 0$$
$$0 \leq (a-x)^2 - n(b-y)^2 \leq \frac{1}{4} - \frac{n}{4}, \quad \text{si} \quad n \leq 0.$$

En términos de la función δ

$$\delta(\alpha\beta^{-1} - \sigma) = \mid (a-x)^2 - n(b-y)^2 \mid < 1,$$

para $n = -1, -2, 2, 3$. Haciendo $\rho = \beta(\alpha\beta^{-1} - \sigma)$, tenemos que $\alpha = \sigma\beta + \rho$. Como $\alpha, \beta\sigma \in \mathbb{Z}(\sqrt{n})$, por la identidad anterior $\rho \in \mathbb{Z}(\sqrt{n})$. Más aún, por las propiedades que satisface δ tenemos lo siguiente

$$\delta(\rho) = \delta(\alpha\beta^{-1} - \sigma) = \delta(\beta)\delta(\alpha\beta^{-1} - \sigma)) < \delta(\beta).$$

Luego, para cada $\alpha, \beta \in \mathbb{Z}(\sqrt{n})$ ambos distintos de cero, tenemos que existe $\rho \in \mathbb{Z}(\sqrt{n})$ tal que $\alpha = \sigma\beta + \rho$ y $\delta(\rho) < \delta(\beta)$. Así, se cumple la definición 2.6.1, por tanto $\mathbb{Z}(\sqrt{n})$ es un dominio Euclidiano y por el corolario 2.6.8 es un dominio de factorización única para $n = -1, -2, 2, 3$. □

Consideremos el dominio cuadrático de los enteros gaussianos, veamos que $\mathbb{Z}[i]$ es un dominio Euclidiano y en consecuencia un dominio de factorización única.

Lema 2.6.22. *Sean $a, b \in \mathbb{Z}$, $a > 0$. Entonces existen $q, r \in \mathbb{Z}$ tales que $b = aq + r$ con $\mid r \mid \leq \frac{a}{2}$.*

Demostración. Sean $a, b \in \mathbb{Z}, a > 0$. Por el algoritmo de Euclides existen $q, r \in \mathbb{Z}$ tales que $b = aq + r$ con $0 \leq r < a$. Si $r \leq \frac{a}{2}$ se sigue el resultado. Si $r > \frac{a}{2}$ tenemos que $b = a(q+1) + (r-a)$, y además $\mid r - a \mid < \frac{a}{2}$.

□

Corolario 2.6.23. *El dominio de los enteros gaussianos $\mathbb{Z}[i]$ es un dominio de factorización única.*

Demostración. Consideremos el dominio de los enteros gaussianos $\mathbb{Z}[i]$ y la función δ en $\mathbb{Z}[i]$ dada por $\delta(\alpha) = N(\alpha)$, trivialmente esta función satisface 1. y 2. de la definición 2.6.1. Veamos que se satisface 3. de esta definición. Sean $\alpha = a + bi$ y $\beta = c + di \in \mathbb{Z}[i]$, $\beta \neq 0$. Como $\mathbb{Z}[i] \subset \mathbb{Q}[i]$ tenemos que

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{a' - b'i}{c^2+d^2} \text{ con } a', b' \in \mathbb{Z}.$$

Llamemos $\gamma = c^2 + d^2 = N(\beta) \in \mathbb{Z}^+$. Por el lema 2.6.22 tenemos que existen $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales que

$$a' = \gamma q_1 + r_1 \text{ con } \mid r_1 \mid \leq \frac{\gamma}{2},$$

$$b' = \gamma q_2 + r_2 \text{ con } \mid r_2 \mid \leq \frac{\gamma}{2}.$$

Definamos $\sigma = q_1 + q_2 i \in \mathbb{Z}[i]$. Luego,

$$\frac{\alpha}{\beta} = \frac{a'}{\gamma} + \frac{b'}{\gamma} i = \frac{\gamma q_1 + r_1}{\gamma} + \frac{\gamma q_2 + r_2}{\gamma} i = q_1 + q_2 i + \frac{r_1 + r_2 i}{\gamma} = \sigma + \frac{r_1 + r_2 i}{\gamma}.$$

Multiplicando esta expresión por β tenemos que $\alpha = \beta\sigma + \beta\frac{r_1 + r_2 i}{\gamma}$, definimos $\rho = \beta\frac{r_1 + r_2 i}{\gamma}$. Por lo tanto $\alpha = \beta\sigma + \rho$. Veamos que $\rho = 0$ o bien $N(\rho) < N(\beta)$. Si $\rho = 0$ se sigue el resultado. Mostremos que si $\rho \neq 0$ entonces $N(\rho) < N(\beta)$.En efecto, este hecho se deduce de las siguientes igualdades

$$N(\rho) = N\left(\beta\frac{r_1 + r_2 i}{\gamma}\right) = N(\beta)N\left(\frac{r_1 + r_2 i}{\gamma}\right) = \gamma\frac{r_1^2 + r_2^2}{\gamma^2} \leq \frac{1}{\gamma}\left(\left(\frac{\gamma}{2}\right)^2 + \left(\frac{\gamma}{2}\right)^2\right) = \frac{\gamma}{2} < \gamma.$$

Por lo tanto $N(\rho) < N(\beta)$. □

Con este resultado, concluimos este capítulo. No todos los dominios cuadráticos $\mathbb{Z}(\sqrt{n})$ son dominios de factorización única, por ejemplo $\mathbb{Z}(\sqrt{6})$ no es un dominio de factorización única, esto lo mostraremos en el Capítulo 3.

Capítulo 3

Ejemplos interesantes

3.1. Algunos ejemplos

En este capítulo trabajamos ejemplos interesantes en los cuales mostramos que varios recíprocos de afirmaciones vistas anteriormente resultan no ser ciertos. Dicho esto comenzamos con nuestro primer ejemplo, el cual nos muestra la existencia de un máximo común divisor de una cantidad finita de elementos $a_1, a_2, \ldots, a_n$ de un dominio entero R pero no existe un máximo común divisor de los elementos $ra_1, ra_2, \ldots, ra_n$ para alguna $r \neq 0$ en el dominio entero.

Ejemplo 3.1.1. Consideremos el dominio entero $\mathbb{Z}(\sqrt{-5})$. Sean $9, 3(2+\sqrt{-5}) \in \mathbb{Z}(\sqrt{-5})$. Veamos quiénes son los divisores comunes de estos elementos. Sea $c \in \mathbb{Z}(\sqrt{-5})$ tal que es un divisor común, esto es $c \mid 9$ y $c \mid 3(2+\sqrt{-5})$. Por lo tanto existen $t_1, t_2 \in \mathbb{Z}(\sqrt{-5})$ tales que $9 = ct_1$ y $3(2+\sqrt{-5}) = ct_2$. Tomando la norma tenemos que $N(c) \mid N(9)$ y $N(c) \mid N(3(2+\sqrt{-5}))$. Luego como $N(9) = 81$ y $N(3(2+\sqrt{-5})) = 81$ basta buscar quiénes son los divisores de 81 para encontrar la norma del elemento c.

Como $c \in \mathbb{Z}(\sqrt{-5})$ entonces existen $a, b \in \mathbb{Z}$ tales que $c = a + b\sqrt{-5}$ así, $N(c) = a^2 + b^2 5$. Además sabemos que los divisores enteros de 81 son $\pm 1, \pm 3, \pm 9, \pm 81$, como la norma del elemento c debe ser positiva podemos excluir los divisores negativos. Luego, para encontrar el elemento c basta con resolver las siguientes ecuaciones y excluir algunas soluciones:

$$a^2 + b^2 5 = 1, \quad a^2 + b^2 5 = 3, \quad a^2 + b^2 5 = 9, \quad a^2 + b^2 5 = 81.$$

1. Tomemos la ecuación $a^2 + b^2 5 = 3$. Si $b \neq 0$ entonces $a^2 + b^2 5 \geq 5$, por lo tanto para que pudiese tener solución b tiene que ser cero. Si $b = 0$ entonces $a^2 = 3$, sin embargo no hay entero a tal que satisfaga esta condición. Por lo tanto la ecuación $a^2 + b^2 5 = 3$ no tiene solución.

2. La ecuación $a^2 + b^2 5 = 1$ tiene por soluciones $a = \pm 1, b = 0$, ya que si $b \neq 0$ entonces $a^2 + b^2 5 \geq 5$ y en consecuencia $a^2 + b^2 5 > 1$.

3. Consideremos la ecuación $a^2 + b^2 5 = 9$. Si $b = 0$ entonces $a^2 = 9$, así $a = \pm 3$. Si $b \neq 0$ entonces las posibles soluciones son $a = \pm 2$ y $b = \pm 1$. Para $b > 2, b < -2$ tenemos que $b^2 > 4$, luego $b^2 5 > 20$ y por ende $a^2 + b^2 5 > 9$. Por lo tanto las únicas soluciones en este caso son $a = \pm 3$ y $b = 0$ o $a = \pm 2$ y $b = \pm 1$.

4. Por último tomemos la ecuación $a^2 + b^2 5 = 81$. Veamos para cuáles valores tiene solución. Podemos considerar la gráfica P asociada a esta ecuación (ver figura 3.1). Para saber cuáles soluciones (a, b) serán enteras, podemos trazar las líneas horizontales $b = \pm 1, \pm 2, \pm 3$ y fijarnos en qué punto interseca con la gráfica de la ecuación, si su valor en a es un número entero entonces la pareja (a, b) es una solución entera de la ecuación. De este modo los puntos $A = (-6, 3), B = (-9, 0), C = (9, 0), D = (6, 3), E = (-6, -3), F = (6, -3)$ son soluciones enteras de la ecuación $a^2 + b^2 5 = 81$. De la gráfica a simple vista no se puede detectar si cuando $b = 4$ el valor en a es un número entero, por esta razón debemos calcular este valor, como $b = 4$ entonces $a^2 = 81 - 16 = 65$ sin embargo no hay un entero a que satisfaga esta condición. De esta manera los divisores de 9 y $3(2 + \sqrt{-5}) = 6 - 3\sqrt{-5}$ son

$$\pm 1, \pm 3, 2 + \sqrt{-5}, -2 - \sqrt{-5}.$$

Ahora notemos que de estos divisores comúnes ninguno divide al otro, esto es fallan con la propiedad 2. de la definición 2.1.12, por tanto $\text{mcd}(3 \cdot 3, 3(2 + \sqrt{-5})$ no existe. Pero, por otra parte $\text{mcd}(3, 2 + \sqrt{-5}) = 1$. Se sigue que solamente el lado derecho de la formula

$$\text{mcd}((3 \cdot 3, 3(2 + \sqrt{-5}) = 3\text{mcd}(3, 2 + \sqrt{-5}),$$

esta definido en $\mathbb{Z}(\sqrt{-5})$. Por tanto la recíproca del inciso 2. del lema 2.3.5 no es cierta.

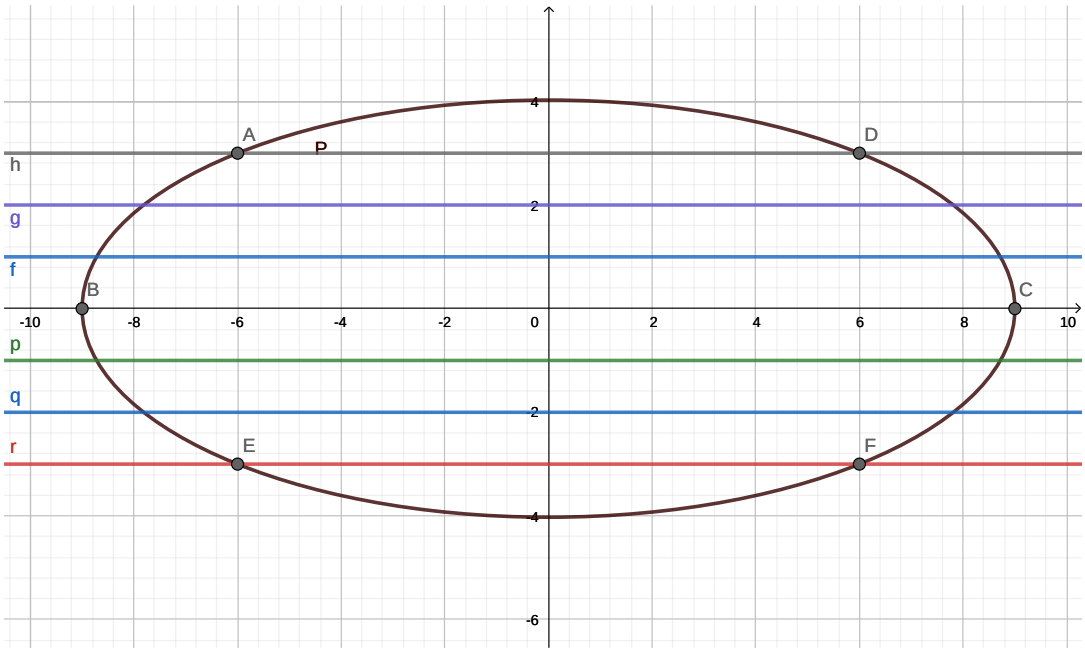

Figura 3.1: Gráfica asociada a la ecuación $a^2 + b^2 5 = 81$

Así como no podemos encontrar un máximo común divisor para 9 y $6+3\sqrt{-5}$ en $\mathbb{Z}(\sqrt{-5})$ tenemos que éste dominio cuadrático no satisface la m.c.d. propiedad. Veamos $\mathbb{Z}(\sqrt{-5})$ tampoco satisface la m.c.m. propiedad, mostrando dos elementos tales que no tengan un mínimo común múltiplo.

Ejemplo 3.1.2. Consideremos el dominio cuadrático $\mathbb{Z}(\sqrt{-5})$ y sean $2, 1+\sqrt{-5} \in \mathbb{Z}(\sqrt{-5})$. Notemos que 1 es un máximo común divisor de 2 y $1+\sqrt{-5}$, pero no existe un mínimo común múltiplo. Supongamos que sí existe, por 1. del teorema 2.3.7 tenemos que

$$\text{mcm}(2, 1+\sqrt{-5})\text{mcd}(2, 1+\sqrt{-5}) = 2(1+\sqrt{-5}).$$

Como $\text{mcd}(2, 1+\sqrt{-5}) = 1$ tenemos que $\text{mcm}(2, 1+\sqrt{-5}) = 2(1+\sqrt{-5})$. Observemos que 6 es un múltiplo común de 2 y $1+\sqrt{-5}$, ya que $2 \mid 6$ y $1+\sqrt{-5} \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Dado que $2(1+\sqrt{-5})$ es un mínimo común múltiplo entonces $2(1+\sqrt{-5}) \mid 6$. Esto es existe $a+b\sqrt{-5} \in \mathbb{Z}(\sqrt{-5})$ tal que

$$\begin{gathered} 2(1+\sqrt{-5})(a+b\sqrt{-5}) = 6, \\ 2a - 10b + (2b+2a)\sqrt{-5} = 6. \end{gathered}$$

De donde tenemos que $2a-10b = 0$ y $b+a = 0$, por tanto $b = -a$. Así $2a-10b = 2a+10a = 12a = 6$, pero esto es una contradicción pues $a \in \mathbb{Z}$. Por lo tanto, no existe un mínimo común múltiplo de 2 y $1+\sqrt{-5}$ en $\mathbb{Z}(\sqrt{-5})$.

Sabemos que en un dominio entero todo elemento primo es un elemento irreducible, sin embargo la recíproca de esta afirmación no es cierta. Mostremos un ejemplo de un elemento irreducible que no es un elemento primo.

Ejemplo 3.1.3. Consideremos el dominio cuadrático $\mathbb{Z}(\sqrt{-5})$. Veamos que 3 es un elemento irreducible en $\mathbb{Z}(\sqrt{-5})$. Supongamos que 3 no es un elemento irreducible, es decir 3 se puede factorizar como $3 = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$ ambos no invertibles. Tomando la norma tenemos que

$$9 = N(3) = N(\alpha)N(\beta).$$

Como $N(\alpha), N(\beta) \in \mathbb{Z}^+$ entonces $N(\alpha) = 3 = N(\beta)$. Si $\beta = a+b\sqrt{-5}$ entonces $N(\beta) = a^2+b^2 5$ y por tanto $3 = a^2+b^2 5$. Sin embargo, en el ejemplo 3.1.1 mostramos que esta ecuación no tiene solución. Por lo tanto 3 es un elemento irreducible. Veamos ahora que 3 no es un elemento primo. Notemos que

$$9 = (2+\sqrt{-5})(2-\sqrt{-5}),$$

y $3 \mid 9$. Así, $3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$ pero 3 no divide a $2+\sqrt{-5}$ ni a $2-\sqrt{-5}$. Supongamos que sí, es decir que 3 divide alguno, sin pérdida de generalidad supongamos que $3 \mid 2+\sqrt{-5}$. Entonces existen $a, b \in \mathbb{Z}$ tales que $2+\sqrt{-5} = 3(a+b\sqrt{-5}) = 3a+3b\sqrt{-5}$. De donde $3a = 2$ y $3b = 1$, sin embargo no existen enteros a, b tales que satisfagan estas dos condiciones. Por lo tanto 3 no es un elemento primo.

Para nuestro siguiente ejemplo recordemos el teorema 2.1.18, este teorema nos dice que si R es un anillo conmutativo con uno y $a_1, a_2, \ldots a_n$ son elementos distintos de cero de R tales que tienen un máximo común divisor y éste se puede expresar de la forma $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ para algunos $r_1, r_2, \ldots, r_n \in R$ si, y sólo si el ideal $(a_1, a_2, \ldots, a_n)$ es principal. Mostremos que la condición de que el máximo común divisor se pueda expresar de esa forma es muy fuerte.

Ejemplo 3.1.4. Consideremos el dominio cuadrático $\mathbb{Z}(\sqrt{-5})$. Entonces $\mathbb{Z}(\sqrt{-5})$ no es un dominio de ideales principales. Tomemos el ideal $(3, 2+\sqrt{-5})$ y supongamos que es un ideal principal. Luego, por el teorema 2.1.18 como $(3, 2+\sqrt{-5})$ es principal y $\text{mcd}(3, 2+\sqrt{5}) = 1$ tenemos que 1 se puede expresar de la siguiente forma $1 = \alpha 3 + \beta(2+\sqrt{-5})$ para $\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$. Entonces existen $a, b, c, d \in \mathbb{Z}$ tales que $\alpha = a + b\sqrt{-5}$ y $\beta = c + d\sqrt{-5}$. Por lo tanto sustituyendo

$$1 = \alpha 3 + \beta(2+\sqrt{-5}) = (a + b\sqrt{-5})3 + (c + d\sqrt{-5})(2+\sqrt{-5}).$$

Luego al realizar las operaciones correspondientes tenemos que

$$1 = (3a + 2c - 5d) + (3b + 2d + c)\sqrt{-5}.$$

Por lo tanto, $1 = 3a + 2c - 5d$ y $0 = 3b + 2d + c$, como $0 = 3b + 2d + c$ entonces $c = -3b - 2d$ sustituyendo en $1 = 3a + 2c - 5d$ tenemos que

$$1 = 3a + 2c - 5d = 3a + 2(-3b - 2d) - 5d = 3a - 6b - 4d - 5d = 3(a - 2b - 3d),$$

es decir 1 es un múltiplo de 3, lo cual es una contradicción. Por lo tanto el ideal $(3, 2+\sqrt{-5})$ no es un ideal principal. De hecho aún cuando existe un máximo común divisor de 3 y $2+\sqrt{-5}$ a éste no lo podemos expresar como $1 = 3r_1 + (2+\sqrt{-5})r_2$.

En el Capítulo 2. mostramos que los dominios cuadráticos $\mathbb{Z}(\sqrt{-1}), \mathbb{Z}(\sqrt{-2}), \mathbb{Z}(\sqrt{2}), \mathbb{Z}(\sqrt{3})$, son dominios de factorización única. Veamos ahora que el dominio cuadrático $\mathbb{Z}(\sqrt{-6})$ no es un dominio de factorización única.

Ejemplo 3.1.5. Consideremos el dominio cuadrático $\mathbb{Z}(\sqrt{-6})$ y $10 \in \mathbb{Z}(\sqrt{-6})$. Entonces podemos expresar a 10 de las siguientes formas

$$10 = (2+\sqrt{-6})(2-\sqrt{-6}) \quad \text{y} \quad 10 = 5 \cdot 2.$$

Veamos que $2+\sqrt{-6}, 2-\sqrt{-6}, 5, 2$ son elementos irreducibles. De manera análoga al ejemplo 3.1.3 podemos mostrar que 5 y 2 son elementos irreducibles. Falta mostrar que $2+\sqrt{-6}, 2-\sqrt{-6}$ son elementos irreducibles. Calculando la norma de estos elementos

$$N(2+\sqrt{-6}) = 10 = N(2-\sqrt{-6})$$

Supongamos que $2+\sqrt{-6}$ no es un elemento irreducible, esto es existen $\alpha, \beta \in \mathbb{Z}(\sqrt{-6})$ no invertibles tales que

$$2+\sqrt{-6} = \alpha\beta.$$

De donde, $5 \cdot 2 = 10 = N(2+\sqrt{-6}) = N(\alpha)N(\beta)$. Por lo tanto $N(\alpha) = 5$ y $N(\beta) = 2$ ó $N(\alpha) = 2$ y $N(\beta) = 5$. Sin perdida de generalidad supongamos que $N(\alpha) = 5$ y $N(\beta) = 2$. Como $\alpha, \beta \in \mathbb{Z}(\sqrt{-6})$ entonces $\alpha = a + b\sqrt{-6}$ y $\beta = c + d\sqrt{-6}$. De donde

$$5 = a^2 + b^2 6 \quad \text{y} \quad 2 = c^2 + d^2 6.$$

Tomando la primera ecuación, si $b \neq 0$ entonces $b^2 6 \leq 6$ y así $a^2 + b^2 6 > 5$. Por lo tanto $b = 0$, de donde $a^2 = 5$ pero no hay un entero que satisfaga esta condición. Análogamente se puede mostrar que la ecuación $2 = c^2 + d^2 6$ no tiene soluciones enteras. Por lo tanto $2+\sqrt{-6}$ es un elemento irreducible, de la misma forma se muestra que $2-\sqrt{-6}$ es un elemento irreducible.

Así, podemos expresar a 10 como dos productos diferentes en elementos irreducibles, $10 = (2+\sqrt{-6})(2-\sqrt{-6})$ y $10 = 5 \cdot 2$, es decir tenemos dos factorizaciones en elementos irreducibles distintas en $\mathbb{Z}(\sqrt{-6})$. Por lo tanto $\mathbb{Z}(\sqrt{-6})$ no es un dominio de factorización única.

Bibliografía

[1] D. Avella, G. Campero, E. C. Sáenz, Notas de Álgebra Superior II, 2018.

[2] D. M. Burton, A first course in rings and ideals, Addison-Wesley publishing company, 1970.

[3] H. Cárdenas, E. Lluis, F. Raggi, F. Tomás, Álgebra Superior, Trillas, 1990 (reimp. 2010).

[4] D. S. Dummit, R. M. Foote, Abstract Algebra, John Wiley and Sons, 2004.

[5] I. N. Herstein, Álgebra Moderna, Trillas, 1990 (reimp. 2008).

[6] J. J. Rotman, A first course in abstract algebra, Pearson Prentice Hall, 1995.