Capítulo

8

Anillos Especiales

8.1 Conceptos Básicos

En este capítulo nos dedicaremos al estudio de algunos anillos especiales que poseen ciertas condiciones adicionales, aparte de las propias de la definición, como por ejemplo los Dominios de Integridad, los Dominios de Factorización Unica y los Dominios Euclideanos.

A todo dominio de integridad se le puede asociar un cuerpo, llamado Cuerpo de Fracciones, en el cual se sumerge de la misma manera como los números enteros se insertan en los números racionales. Veremos como se construye este cuerpo de cocientes y el homomorfismo que permite obtener esta interesante conexión.

Una de las propiedades fundamentales del anillo de los números enteros es que todo entero se expresa de manera única como un producto de números primos. Esta propiedad se generaliza en forma natural a los Dominios de Integridad, originandose así el concepto de Dominio de Factorización Unica.

Existen algunos anillos que gozan de buenas propiedades de factorización y divisibilidad. Entre ellos se encuentran los Dominios Euclideanos, los cuales son a la vez dominios de Factorización Unica. Los ejemplos más conocidos de un Dominio Euclideano son los números enteros y los polinomios, pero también existen otros no tan usados como son los Enteros de Gauss. Haremos un estudio de estos enteros y sus propiedades más relevantes.

En todo este capítulo, cuando se diga anillo, supondremos que se trata de un anillo conmutativo con unidad.

Definición 8.1.1 *Sea R un anillo. Un ideal P de R ($P \neq R$), se dice* **ideal primo**, *si para todo a, b en R tales que $ab \in P$, entonces $a \in P$ ó $b \in P$.*

Ejemplo: Sea $R = \mathbb{Z}$ anillo de los enteros y J el ideal formado por los números pares. Entonces J es un ideal primo de R.

Definición 8.1.2 *Sea R un anillo. Un ideal M de R ($M \neq R$), se llama* **ideal maximal**, *si para todo ideal J tal que*

$$M \subseteq J \subseteq R$$

se tiene

$$M = J \quad ó \quad J = R$$

Proposición 8.1.1 *Sea P un ideal de R. Entonces P es un ideal primo si y sólo si R/P es un dominio de integridad.*

Demostración: $\Longrightarrow$) Sea P un ideal primo de R. Supongamos que existen elementos $a + P$ y $b + P$ en el anillo cociente R/P tal que

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

Luego

$$ab + P = P$$

y por lo tanto

$$ab \in P$$

Como P es un ideal primo, se tendrá

$$a \in P \quad ó \quad b \in P$$

Luego

$$a + P = 0 \quad ó \quad b + P = 0$$

Por lo tanto R/P, es un anillo conmutativo con unidad, el cual no tiene divisores de cero y luego es un Dominio de Integridad.

$\Longleftarrow$) Por otro lado supongase que R/P es un domino de integridad. Si P no es primo, existen elementos a y b en R tal que

$$a \notin P, \;\; b \notin P \quad \text{y} \quad ab \in P$$

Luego

$$a + P \neq 0 \quad \text{y} \quad b + P \neq 0$$

pero

$$(a + P)(b + P) = ab + P = 0$$

Esto implica que $a + P$ es un divisor de cero, lo cual es una contradicción. Luego $a \in P$ o $b \in P$.

Además $P \neq R$, pues $R/P \neq (0)$. En conclusión, el ideal P es primo.

♠

Proposición 8.1.2 *Sea M un ideal de un anillo R. Entonces M es maximal si y sólo si R/M es un cuerpo.*

Demostración: $\Longrightarrow$) Sabemos que R/M es un anillo conmutativo con unidad, pues R lo es. Solo falta probar que todo elemento de R/M distinto de cero es inversible, para que R/M sea un cuerpo.

Sea $a + M \neq 0$ en R/M. Luego construimos el ideal J de la forma siguiente:

$$J = Ra + M$$

Se tiene entonces que $M \subsetneq J$, pues $a \notin M$ y por ser M un ideal maximal, se deduce de la definición que

$$Ra + M = R \tag{8.1}$$

Como $1 \in R$ se tiene de (**??**)

$$ra + m = 1 \tag{8.2}$$

para algunos elementos $r \in R$ y $m \in M$. Por lo tanto, usando (**??**) se concluye

$$(r + M)(a + M) = 1 + M$$

Luego hemos probado que $r + M$ es el inverso de $a + M$.

$\Longleftarrow$) Supongase ahora que R/M sea un cuerpo. Sea I un ideal de R tal que

$$M \subseteq I \subseteq R$$

Si suponemos que $I \neq R$, entonces el ideal I/M es un ideal propio de R/M. Pero los únicos ideales de R/M son (0) y él mismo, pues R/M es un cuerpo. Luego

$$I/M = (0)$$

de donde

$$I = M$$

Por lo tanto M es un ideal maximal.

♠

Se sabe que todo cuerpo es un dominio de integridad, luego podemos combinar los dos teoremas anteriores para obtener:

Corolario 8.1.1 *Sea R un anillo. Entonces todo ideal Maximal es un ideal primo.*

Ejemplo 1: Sea I un ideal de $\mathbb{Z}$. Entonces I es un subgrupo del grupo aditivo de $\mathbb{Z}$, y por lo tanto es de la forma $I = (m)$ para algún $m \in \mathbb{Z}$. Si I es un ideal primo, entonces el elemento m debe ser un número primo. Caso contrario se tiene

$$m = n_1 n_2$$

con $1 < n_1 < m,\ \ 1 < n_2 < m$

Luego el producto de n_1 y n_2 está en el ideal I, pero $n_1 \notin I$ y $n_2 \notin I$. Por otro lado si p es un número primo, afirmamos que el ideal $P = (p)$ es un ideal primo. En efecto si para algunos n_1, n_2 se tiene

$$n_1 n_2 \in P,$$

se deduce que

$$n_1 n_2 = kp \quad \text{para algún} \quad k \in \mathbb{Z}$$

Luego

$$p | n_1 n_2$$

y por lo tanto

$$p | n_1 \quad \text{ó} \quad p | n_2$$

Si suponemos que $p|n_1$ se tiene

$$n_1 = sp \tag{8.3}$$

para algún s entero, y de (**??**) se deduce que $n_1 \in P$. Igualmente, si suponemos que $p|n_2$ se llega a que $n_2 \in P$. Por lo tanto el ideal P es primo.

En conclusión hemos demostrado que los únicos ideales primos de $\mathbb{Z}$ son de la forma: $P = (p)$ con p un número primo. Mostraremos que dichos ideales son también maximales.

En efecto, sea p un número primo, $P = (p)$ y J otro ideal tal que

$$P \subseteq J \subseteq \mathbb{Z}$$

Luego si suponemos que $P \neq J$, existe un elemento n, el cual está en J pero no en P. Por lo tanto $p \not| n$ y así se tendrá que p y n son un par de enteros primos relativos. Luego existen enteros x e y tales que

$$px + ny = 1$$

Ahora bien, de acuerdo a las propiedades de ideal de J se tendrá

$$px \in P \subseteq J$$

y

$$ny \in J$$

Luego

$$1 = px + ny \in J,$$

de donde

$$J = \mathbb{Z}$$

Luego hemos probado que todo ideal primo de $\mathbb{Z}$ es maximal.

Observación: Existen anillos que poseen ideales primos los cuales no son maximales. Sin embargo en el caso de los números enteros sí se tiene esta propiedad.

Ejemplo 2: Sea $R = \mathbb{Z} + \mathbb{Z}$ conjunto de parejas ordenadas de números enteros, con las operaciones:

Suma: $(a, b) + (c, d) = (a + c, b + d)$

Producto: $(a, b)(c, d) = (ac, bd)$

Entonces es fácil verificar que R es un anillo conmutativo con unidad.

Sean

$$I = \{(0, y) \mid y \in \mathbb{Z}\}$$

$$M = \{(2x, y) \mid x, y \in \mathbb{Z}\}$$

Entonces es fácil verificar que tanto I como M son ideales propios de R.

Además el ideal I es primo, pues si se tiene

$$(a, b)(c, d) \in I$$

entonces

$$ac = 0$$

Como $\mathbb{Z}$ es dominio de integridad, se tiene

$$a = 0 \quad \text{ó} \quad c = 0,$$

de donde

$$(a, b) \in I \quad \text{ó} \quad (c, d) \in I$$

Sin embargo I no es un ideal maximal, pues se tiene

$$I \subseteq M \subseteq R$$

y

$$M \neq I \ , \ M \neq R.$$

8.2 Cuerpo de Cocientes de un Dominio de Integridad

Si D es un Dominio de Integridad, no todos los elementos de D poseen un inverso bajo la multiplicación, como es el caso del anillo de los enteros.

Podemos entonces construir un cuerpo que contenga a D, de la misma forma como se construyen las fracciones de números enteros, el cual contiene a $\mathbb{Z}$ como un subanillo.

Esta construcción es muy similar a la construcción de los números racionales a partir de los enteros. Cuando se tiene una fracción $\frac{a}{b}$, entonces puede existir otra representación $\frac{e}{d}$ de la misma fracción. En tal caso se tiene que

$$\frac{a}{b} = \frac{c}{d}, \quad \text{si y sólo si} \quad ad = bc.$$

Esta condición de igualdad de fracciones, será el punto de partida de nuestra exposición.

Sea D un Dominio de Integridad y A el subconjunto del producto cartesiano $D \times D$, formados por pares de la forma (a, b), tal que $b \neq 0$.

Entonces definimos una relación A, mediante

$$(a, b) \sim (c, d) \quad \text{si y sólo si} \quad ad = bc$$

Proposición 8.2.1 *La relación " $\sim$ " es una relación de equivalencia.*

Demostración:

1) **Reflexiva:** Sea $(a, b) \in A$, entonces claramente

$$(a, b) \sim (a, b)$$

pues

$$ab = ba$$

2) **Simétrica:** Sea $(a, b) \sim (c, d)$. Entonces

$$ad = bc,$$

y como D es conmutativo, se obtiene

$$cb = da,$$

luego

$$(c, d) \sim (a, b)$$

3) **Transitiva:** Sea $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Luego

$$ad = bc,$$

y

$$cf = de$$

Multiplicando la primera ecuación por f, la segunda por b y luego restando ambas nos produce

$$adf - bde = 0$$

o sea

$$d(af - be) = 0$$

De la última ecuación se deduce

$$af - be = 0,$$

pues $d \neq 0$ y D es un dominio de integridad.

Por lo tanto

$$(a, b) \sim (e, f)$$

Con esto termina la demostración

♠

Una vez hecho esto, consideremos el conjunto cociente de todas las clases de equivalencia de esta relación y denotemoslo por F. Así pues

$$F = \{[a, b] \mid (a, b) \in A\}$$

donde $[a, b]$ denota la clase de equivalencia del elemento (a, b) en A.

Seguidamente, definimos en F un par de operaciones

Suma: $[a, b] + [c, d] = [ad + bc, bd]$

Producto: $[a, b][c, d] = [ac, bd]$

Notemos en primer lugar que $bd \neq 0$, puesto tanto b como d son no nulos y D es un dominio de integridad, y por lo tanto la suma y el producto de clases es una operación cerrada.

Probaremos que estas operaciones están bien definidas. Esto es, supongase que para algunos elementos $a, b, c, d, a', b', c', d'$ en D con $bd \neq 0$ y $b'd' \neq 0$, se tiene

$$[a, b] = [a', b']$$

$$[c, d] = [c', d']$$

Luego debemos tener

$$ab' = ba' \quad \text{y} \quad cd' = dc' \tag{8.4}$$

Por lo tanto

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a', b'] + [c', d'] = [a'd' + b'c', b'd']$$

Debemos probar entonces

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

o lo que es lo mismo

$$(ad + bc)b'd' = (a'd' + b'c')bd$$

si y sólo si

$$adb'd' + bcb'd' = a'd'bd + b'c'bd \tag{8.5}$$

Entonces si partiendo de las relaciones en (**??**), llegamos a probar la ecuación (**??**), la suma estará bien definida.

Para demostrar la igualdad (**??**) comenzaremos por desarrollar el lado izquierdo, hasta obtener el término de la derecha. Luego

$$\begin{aligned} adb'd' + bcb'd' &= ab'(dd') + cd'(bb') \\ &= ba'(dd') + dc'(bb') \\ &= a'd'bd + b'c'bd \end{aligned}$$

Con esto queda demostrado (**??**).

Para el producto, la demostración es bastante similar. En efecto, supóngase que (**??**) es cierto y entonces se desea probar

$$[a, b][c, d] = [a', b'][c', d']$$

o lo que es equivalente a

$$[ac, bd] = [a'c', b'd']$$

Si y sólo si

$$ac(b'd') = bd(a'c') \tag{8.6}$$

Desarrollando el lado izquierdo de (**??**) y usando (**??**) se tiene

$$\begin{aligned} ac(b'd') &= ab'(cd') \\ &= (ba')(dc') \\ &= bd(a'c') \end{aligned}$$

Luego (**??**) se cumple, y por lo tanto el producto está bien definido.

Dejaremos como ejercicio para el lector la verificación de las propiedades de anillo de F, con este par de operaciones, en donde los elementos $[0, a]$ y $[a, a]$ actúan como elemento cero e identidad, donde a es cualquier elemento no nulo de D.

Para ver esto último, sea $[e, f] \in F$. Luego

$$\begin{aligned} [e, f] + [0, a] &= [ea + 0f, fa] \\ &= [ea, fa] \\ &= [e, f] \end{aligned}$$

$$\begin{aligned} [e, f][a, a] &= [ea, fa] \\ &= [e, f] \end{aligned}$$

Finalmente, probaremos que todo elemento no nulo $[a, b]$ de F, posee un inverso multiplicativo. En efecto, como $a \neq 0$, entonces $[b, a] \in F$ y además

$$\begin{aligned} [a, b][b, a] &= [ab, ba] \\ &= [a, a] \\ &= 1 \end{aligned}$$

Luego $[a, b]^{-1} = [b, a] \in F$. Resumiremos todos estos resultados en el siguiente teorema

Teorema 8.2.1 *Sea D un dominio de integridad cualquiera, entonces el conjunto*

$$F = \{[a,b] \mid a,b \in D \quad y \quad b \neq 0\}$$

es un cuerpo, el cual se denomina **Cuerpo de Cocientes de D**.

Teorema 8.2.2 *Sea D un dominio de integridad y F su cuerpo de fracciones. Entonces la aplicación*

$$\begin{array}{rccc} \phi & : & D & \longrightarrow & F \\ & & a & \longrightarrow & [a,1] \end{array}$$

es un homomorfismo inyectivo, el cual se denomina la **Inmersión Canónica** *de D en F.*

Demostración: Sean $a,b \in D$. Luego

$$\begin{array}{rcl} \phi(a+b) & = & [a+b,1] \\ & = & [a1+1b, 1\cdot 1] \\ & = & [a,1]+[b,1] \\ & = & \phi(a)+\phi(b) \end{array}$$

También

$$\begin{array}{rcl} \phi(ab) & = & [ab,1] \\ & = & [a,1][b,1] \end{array}$$

Además, probaremos que ϕ es $1:1$, para lo cual sean $a,b \in D$, tales que

$$\phi(a) = \phi(b)$$

Luego

$$[a, 1] = [b, 1]$$

de donde

$$a = b$$

Con esto se concluye la demostración.

♠

Ejercicios

1) Probar que si D es un dominio de integridad, entonces el ideal (0) es primo.

2) Sea R un anillo conmutativo con unidad, en donde los únicos ideales son (0) y R. Probar que R debe ser un cuerpo.

3) Probar la propiedad conmutativa para la suma y el producto en F.

4) Demuestre que si D es un dominio de integridad y K es un cuerpo que contiene a D, entonces K contiene a F.

5) Probar que todo cuerpo de característica 0, contiene una copia homomorfica del cuerpo $\mathcal{Q}$.

6) Probar que $\mathcal{Q}$ es el menor cuerpo que contiene a los números enteros.

7) Sean D y D' dos dominios de integridad y

$$\varphi : D \longrightarrow D'$$

un homomorfismo inyectivo. Probar que existe un homomorfismo inyectivo entre el cuerpo de cocientes de D y el cuerpo de cocientes de D'.

8) Probar que en todo dominio de integridad D se verifican las leyes de cancelación para el producto. Esto es,

$$\text{si} \quad a, b, c \quad \text{están en} \quad D \quad \text{y} \quad a \neq 0,$$

entonces

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

9) Probar que en todo anillo conmutativo con unidad, cualquier ideal está contenido en un ideal maximal.

10) Sean I, J dos ideales primos en $\mathbb{Z}$, tales que

$$I \cap J = (0).$$

Probar que

$$I + J = \mathbb{Z}$$

11) Sea D un dominio de integridad con cuerpo de cocientes K y sea $[a, b] \in K$. Entonces demostrar

i) $[af, bf] = [a, b] \quad \forall\ f \in K,\ f \neq 0.$
ii) $[a, b] + [c, b] = [a + c, b]$.
iii) $-[a, b] = [-a, b]$.

12) Sea D un cuerpo y K su cuerpo de fracciones. Demuestre que K es isomorfo a D.

13) Probar que $R = \mathbb{Z} \oplus \mathbb{Z}$ con las operaciones

$$(a, b) + (c, d) = (a + c), b + d)$$

$$(a, b)(c, d) = (ac, bd)$$

es un anillo conmutativo con unidad.

14) Sea R como en el ejercicio anterior. Probar que el conjunto

$$I = \{(0, y) \mid y \in \mathbb{Z}\}$$

es un ideal de R.

15) Sean $X = [3, 2]$ e $Y = [-5, 4]$ en el cuerpo cociente de $\mathbb{Z}$. Calcular

a) $X + Y$
b) XY
c) X^{-1}
d) Y^{-1}

8.3 Dominios de Factorización Unica

Definición 8.3.1 *Sea R un anillo y J un ideal de R. Entonces J se dice* **ideal principal** *si existe un elemento $a \in J$, tal que $J = (a)$.*

También se dice que J esta **generado** por el elemento a.

Definición 8.3.2 *Un dominio de integridad en donde todos los ideales son principales, se denomina* **dominio de ideales principales**.

Ejemplo: El anillo de los enteros $\mathbb{Z}$ es un dominio de ideales principales. Si I es un ideal de $\mathbb{Z}$, entonces I es un subgrupo del grupo abeliano $\mathbb{Z}$ con la suma, y por lo tanto I es de la forma (m) para algún $m \in \mathbb{Z}$.

Definición 8.3.3 *Sean a y b elementos en un anillo R, con $a \neq 0$. Diremos que a* **divide a** *b, si existe un elemento c en R, tal que $b = ac$.*

Usaremos el símbolo $a|b$ para indicar que el elemento a divide a b, como se hace para los números enteros.

Observación: Podemos definir en R una relación, mediante

$$a \sim b \quad \text{si y sólo si} \quad a|b$$

Entonces se puede verificar que esta relación es reflexiva y transitiva, pero no es simétrica en general.

Proposición 8.3.1 *Sean a y b elementos en un anillo R. Entonces si*

$$a|b \quad y \quad a|c,$$

se tiene

$$a|bx + cy$$

para todo par de elementos x, y en R.

Demostración: Fácil.

Definición 8.3.4 *Sea R un anillo. Un elemento $u \in R$, se dice* **unidad** *si existe v en R, tal que*

$$uv = 1$$

Observación: Es importante destacar la diferencia entre un elemento unidad de un anillo y la unidad del anillo, el cual siempre será denotado por el símbolo 1. El elemento 1 actua como elemento neutro para el producto, mientras que una unidad u no necesariamente satisface $ua = 1$ para todo a en el anillo. Obviamente, el 1 es una unidad en todo anillo.

Definición 8.3.5 *Un elemento a en un anillo R se dice* **elemento irreducible***, si a no es unidad y cada vez que se tenga una factorización del tipo*

$$a = bc$$

entonces b ó c es una unidad en el anillo.

Ejemplo: Se puede demostrar fácilmente que los elementos irreducibles del anillo $\mathbb{Z}$ de los enteros, son precisamente los números primos.

Proposición 8.3.2 *Sea D un dominio de integridad. Entonces si para algún par de elementos a y b en R se tiene que $a|b$ y $b|a$, se debe cumplir $a = ub$, donde u es una unidad.*

Demostración: Si $a|b$, existe un elemento c en R, tal que $b = ac$. Igualmente, si $b|a$ existe un elemento e en R, tal que $a = be$.

Combinando ambos resultados obtenemos

$$b = bec$$

de donde

$$b(1 - ec) = 0$$

Como $b \neq 0$ y D es un dominio de integridad, se deduce $ec = 1$, lo cual implica que e es una unidad.

♠

Definición 8.3.6 *Dos elementos a y b en un anillo R, se dicen* **asociados**, *si existe una unidad u en R, tal que*

$$a = bu$$

Observación: Si D es un dominio de integridad, entonces la relación de asociados en D es una relación de equivalencia.

Definición 8.3.7 *Un dominio de integridad D se dice* **Dominio de Factorización Unica** *si todo elemento $a \in D$, el cual no es 0 ni unidad, puede ser factorizado como un producto finito de elementos irreducibles, esto es*

$$a = p_1 \cdots p_s$$

donde los p_i son irreducibles.

Además si a tiene otra factorización distinta como producto de irreducibles, digamos

$$a = q_1 \cdots q_t$$

donde los q_j son irreducibles, entonces $s = t$ y cada p_i es asociado de algún q_j.

Más adelante probaremos que todo Dominio de Ideales Principales, es un Dominio de Factorización Unica. Antes, daremos un lema muy interesante el cual establece una condición de cadena en ideales, para cualquier Dominio de Ideales Principales.

Definición 8.3.8 *Sea R un anillo, entonces una* **cadena ascendentee de ideales** *es una familia de ideales de R, $\{I_i\}, i \geq 1$, tales que*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq I_{i+1} \subseteq \ldots$$

Lema 8.3.1 *Toda cadena ascendente de ideales $\{I\}_{i\geq 1}$ está acotada superiormente por un ideal J de R. Es decir*

$$I_i \subseteq J, \quad \forall i \geq 1$$

Demostración: Tomemos

$$J = \bigcup_{i\geq 1} I_i$$

Es claro que J contiene a todos los I_i. Afirmamos que J es un ideal de R.

En efecto, sean $a, b \in J$ y $r \in R$. Debemos probar entonces

1) $a \pm b \in J$

2) $ra \in J$

Si $a, b \in J$, entonces existen i_1, i_2, tales que

$$a \in I_{i_1} \quad \text{y} \quad b \in I_{i_2}$$

Sin pérdida de generalidad, podemos suponer que $i_1 > i_2$, de donde se tendrá entonces $a \in I_{i_1}$, $b \in I_{i_1}$ y como I_{i_1} es un ideal se tiene

$$a \pm b \in I_{i_1} \subseteq J$$

$$ra \in I_{i_1} \subseteq J$$

Luego se cumplen las condiciones 1) y 2) y con esto finaliza la prueba.

♠

Lema 8.3.2 *Sea D un dominio de ideales principales. Entonces toda cadena ascendente de ideales*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$$

es estacionaria.

Es decir, existe un entero positivo k tal que

$$I_n = I_k, \quad \forall n \geq k$$

Demostración: Sea

$$I = \bigcup_{i \geq 1} I_i$$

Entonces de acuerdo al lema amterior, I es un ideal de D, el cual contiene a todos los I_n. Luego el ideal I es principal, pues D es un dominio de ideales principales, y por lo tanto existe un elemento a en D tal que $I = (a)$.

Como I es una unión de conjuntos y $a \in I$, existe un miembro de la familia, digamos I_k tal que $a \in I_k$.

Luego si $n \geq k$ se tendrá

$$I = (a) \subseteq I_k \subseteq I_n \subseteq I$$

Por lo tanto

$$I_n = I_k$$

♠

Teorema 8.3.1 *Todo Dominio de Ideales Principales es un Dominio de Factorización Unica.*

Demostración: Sea D un dominio de ideales principales y a un elemento de D, el cual no es cero, ni es una unidad.

Si a es irreducible, entonces a es un producto de elementos irreducibles.

Supongase que a no es irreducible. Entonces existen un par de elementos a_1 y a_2 (no unidades) tales que

$$a = a_1 a_2$$

Si tanto a_1 como a_2 son irreducibles, entonces el teorema es cierto. Supongase que a_1 no es irreducible y hagamos $a_0 = a$. Luego se tiene una cadena de dos ideales

$$(a_0) \subsetneq (a_1)$$

Continuando de esta manera se tiene una cadena ascendente de ideales, estrictamente contenidos, de la forma

$$(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

Como D es un dominio de ideales principales, existe un k, tal que

$$(a_n) = (a_k), \quad \forall n \geq k.$$

Entonces el elemento a_k es un irreducible, pues si suponemos

$$a_k = bc$$

Se tendrá $a_{k+1} = b$, digamos y por lo tanto la igualdad

$$(b) = (a_{k+1}) = (a_k)$$

implica que b y a_k son asociados. Luego c es unidad.

Además, a_k es un factor irreducible de a y por lo tanto se tiene

$$a = a_k e$$

Aplicando el mismo razonamiento al elemento e, se concluye que a es un producto de irreducibles. Además este proceso se termina después de un número finito de pasos, pues si los irreducibles $p_1, p_2, p_3, \ldots, p_n, \ldots$

aparecen en la factorización de a, se tendrá una cadena ascendente de ideales

$$(a) \subseteq (p_2 \dots p_n \dots) \subseteq (p_3 \dots p_n \dots) \subseteq \dots$$

la cual se detiene en algún momento.

Así pues queda probada la primera parte de la definición de Dominio de Factorización Unica.

Para probar la segunda parte, necesitamos algunos resultados previos sobre divisibilidad.

Proposición 8.3.3 *Sea a un elemnto irreducible en un Dominio de Ideales Principales D. Entonces el ideal (a) es maximal.*

Demostración: Sea I un ideal de D y supongamos

$$(a) \subseteq I \subseteq D.$$

El ideal I es un ideal principal y por lo tanto existe un elemento x en D, tal que $I = (x)$.

Luego

$$a \in (a) \subseteq (x),$$

y luego existe un elemento $y \in D$, tal que

$$a = xy$$

Como a es irreducible, se tiene que x o y es unidad. Si x es una unidad, entonces

$$(x) = I = D.$$

Si y es una unidad, se debe tener que a y x son asociados, luego

$$(x) = (a)$$

y por lo tanto

$$I = (a).$$

En conclusión se tiene que (a) es un ideal maximal.

♠

Proposición 8.3.4 *Sea D un Dominio de Ideales Principlales y a un elemento en D tal que $a|bc$, entonces si a es irreducible se tiene que $a|b$ ó $a|c$*

Demostración: De acuerdo a la proposición anterior se tiene que el ideal (a) es maximal y por lo tanto primo. Luego si $a|bc$ implica que $bc \in (a)$, y por lo tanto

$$b \in (a) \quad \text{o} \quad c \in (a)$$

esto es

$$a|b \quad \text{o} \quad a|c$$

♠

Proposición 8.3.5 *(Segunda parte del teorema)*

Sea D un dominio de Ideales Principales y a un elemento en D el cual se factoriza de dos maneras como productos irreducibles

$$a = p_1 \cdots p_s = q_1 \cdots q_t \tag{8.7}$$

entonces $s = t$ y cada p_i es un asociado de algún q_j

Demostración: Comenzamos por considerar el elemento p_1 en el lado izquierdo en (**??**) el cual es irreducible y divide al producto $q_1 \cdots q_t$. Por la proposición anterior se deduce que p_1 divide a alguno de los q_i, digamos $p_1|q_j$, para algún $1 \leq j \leq t$. Luego de acuerdo al ejercicio 6 se

debe tener que p_1 y q_j son asociados, esto es existe una unidad u_1 tal que

$$p_1 = u_1 q_j$$

Podemos entonces cancelar este elemento en (**??**) para tener una expresión

$$p_2 \cdots p_s = u_1 q_1 \cdots q_{i-1} q_{i+1} \cdots q_t \tag{8.8}$$

Continuando de esta manera, podemos cancelar todos los p_i en el lado derecho de (**??**), después de un número finito de pasos, hasta obtener una expresión de la forma

$$1 = u q_{i_1} \cdots q_{i_k} \tag{8.9}$$

con $k = t - s$ y u una unidad.

Como los q_i son irreducibles, no son unidades y por lo tanto en (**??**) se debe tener $k = 0$ o sea $t = s$.

♠

Concluiremos esta sección, dando una propiedad muy importante de los Dominios de Ideales Principales como lo es la existencia de Máximo Común Divisor entre dos elementos.

Definición 8.3.9 *Sea R un anillo y a, b dos elementos en R. Un elemento $d \in R$ se dice* **Máximo Común Divisor** *entre a y b, si*

i) $d|a$ y $d|b$

ii) Si c es un elemento de R, tal que

$$c|a \quad y \quad c|b$$

entonces $c|d$.

Usamos la notación $d = (a, b)$ para indicar el Máximo Común Divisor entre a y b.

Teorema 8.3.2 *Sea D un Dominio de Ideales Principales. Entonces el Máximo Común Divisor entre dos elementos a y b cualesquiera siempre existe, además existen elementos x e y en D tales que*

$$(a, b) = ax + by$$

Demostración: Sea I el ideal de D generado por a y b (ver problema 10) esto es

$$I = Da + Db$$

Los elementos de I son de la forma $r_1a + r_2b$ con r_1, r_2 en D. Como D es un Dominio de Ideales Principales, el ideal I es principal y por lo tanto existe un elemento d en D, tal que $I = (d)$.

Afirmamos que d es el Máximo Común Divisor entre a y b. En efecto, como $a \in I$ y $b \in I$, se tiene que $d|a$ y $d|b$.

Por otra parte, $d \in I$ y por lo tanto d es de la forma

$$d = ax + by$$

para algunos x, y en D.

Si c es un elemento en D, tal que

$$c|a \quad \text{y} \quad c|b$$

entonces

$$c|ax + by,$$

y por lo tanto

$$c|d$$

♠

Ejemplo: En el anillo $\mathbb{Z}$, todo par de números enteros a y b posee un Máximo Común Divisor, el cual se puede hallar usando la descomposición en factores primos de ambos elementos.

Por ejemplo si se quiere calcular el Máximo Común Divisor entre 18 y 30, se descomponen ambos números como producto de primos

$$18 = 2 \cdot 3^2$$

$$30 = 2 \cdot 3 \cdot 5$$

Luego $(18, 30) = 2 \cdot 3 = 6$

Definición 8.3.10 *Un elemento p en un anillo R se dice que es* **primo** *si p no es cero ni unidad y cada vez que p divide al producto de dos elementos a y b, entonces p divide a a o p divide a b.*

Ejemplo: En el anillo de los enteros $\mathbb{Z}$, todo elemento primo es irreducible y viceversa. Esto puede ser verificado fácilmente por el lector y lo dejamos como ejercicio.

Proposición 8.3.6 *Sea D un Dominio de Integridad. Entonces todo elemento primo en D es irreducible.*

Demostración: Sea p un elemento primo en D y supongase que existen b y c en D, tales que

$$p = bc \tag{8.10}$$

Luego se tiene $p|bc$ y como p es primo, por hipótesis, p debe dividir a alguno de los dos elementos, digamos $p|b$.

Por lo tanto $b = pe$ para algún e en D, y sustituyendo en (**??**) nos da

$$p = bc = p(ec)$$

luego

$$p(1 - ec) = 0$$

De esto se deduce $1 = ec$, pues D es un Dominio de Integridad y $p \neq 0$, con lo cual c es una unidad.

Igualmente, la suposición $p|c$ nos lleva a concluir que b es unidad. Luego p es irreducible.

Observación: En un Dominio de Factorización Unica, los conceptos de elemento primo y elemento irreducible coinciden (ver problema 12). Pero en general esto no es cierto.

Ejemplo: Un Dominio de Integridad que no es Dominio de Factorización Unica.

Sea R el anillo de números complejos, definido por

$$R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

Para cada elemento

$$x = a + b\sqrt{-5} \quad \text{de} \quad R,$$

se define su **norma** mediante

$$N(x) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

Se demuestra entonces que la norma así definida satisface las propiedades

i) $N(x) = 0$ si y soló si $x = 0$.

ii) $N(x, y) = N(x)N(y)$, para todo x, y en R.

Se demuestra que R es un dominio de integridad y que las únicas unidades de R son 1 y -1. (Ver problemas 13-16).

En este anillo un elemento puede tener dos factorizaciones distintas como producto de elementos irrreducibles. Por ejemplo

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{8.11}$$

Mostraremos que $3, 2, (1 + \sqrt{-5})$ y $(1 - \sqrt{-5})$ son irreducibles, y además no son asociados entre si. Con esto quedará probado que R no es un Dominio de Factorización Unica.

Comenzaremos por probar que 3 es irreducible. En efecto si $3 = xy$ para algunos x, y en R, se tendrá entonces

$$9 = N(3) = N(x)N(y)$$

Luego los posibles valores para $N(x)$ son $1, 3$ y 9. Si $N(x) = 1$, entonces x es una unidad y estará probado que 3 es irreducible. Si $N(x) = 9$ se demuestra entonces que $N(y) = 1$ y por lo tanto y es una unidad. Entonces también en este caso estaremos probando que 3 es irreducible.

Veamos que la posibilidad $N(x) = 3$ nos lleva a una contradicción.

En efecto, haciendo $x = a + b\sqrt{-5}$, tendremos

$$3 = N(x) = a^2 + b^2 5$$

lo cual no se puede resolver para a y b números enteros.

De la misma forma se demuestra que 2 es irreducible.

Para probar que $1 + \sqrt{-5}$ es irreducible, supongamos nuevamente que $1 + \sqrt{-5} = xy$, para algunos x e y en R. Entonces

$$6 = N(1 + \sqrt{-5}) = N(x)N(y)$$

Luego las posibilidades para $N(x)$ son $1, 2, 3$ y 6. Si $N(x) = 1$ ó 6, entonces x o y es una unidad.

Sea

$$x = a + b\sqrt{-5}$$

luego si

$$N(x) = 2 \quad \text{ó} \quad 3$$

se tiene

$$3 = N(x) = a^2 + 5b^2$$

o bien

$$2 = N(x) = a^2 + 5b^2$$

lo cual es imposible para a y b enteros.

Luego hemos demostrado que $1+\sqrt{-5}$ es irreducible. La demostración de que $1-\sqrt{-5}$ es irreducible sigue los mismos pasos de la demostración anterior.

Finalmente notemos que ninguno de los elementos

$$2, 3, (1+\sqrt{-5}) \ , \ (1-\sqrt{-5}) \tag{8.12}$$

son asociados.

En efecto, los elementos $2, 3$ y $(1+\sqrt{-5})$ tienen normas distintas y por lo tanto no puede haber asociados entre ellos. Sin embargo $(1+\sqrt{-5})$ y $(1-\sqrt{-5})$ poseen la misma norma y debemos tratar este caso aparte. Si existe una unidad u en R tal

$$(1+\sqrt{-5}) = u(1-\sqrt{-5})$$

se tendrá

$$1+\sqrt{-5} = 1-\sqrt{-5} \quad \text{ó} \quad 1+\sqrt{-5} = -1+\sqrt{-5}$$

pues las únicas unidades de R son ± 1. Vemos que hemos llegado a una contradicción. Por lo tanto ninguno de los cuatro elementos dados en (**??**) son asociados entre ellos.

♠

Ejemplo: Un elemento irreducible no primo

Sea R el anillo del ejemplo anterior, en donde hemos probado que 2 es irreducible. Sin embargo probaremos que 2 no es primo.

De acuerdo a la relación (**??**) se tiene que 2 divide al producto $(1+\sqrt{-5})(1-\sqrt{-5})$. Probaremos que 2 no divide a ninguno de los factores, con lo cual se demuestra que 2 no es primo.

Supongase que 2 divida a $(1+\sqrt{-5})$, entonces se tiene

$$2 = x(1+\sqrt{-5})$$

Tomando normas se tiene

$$4 = 6N(x)$$

lo cual es imposible pues $N(x)$ es un entero mayor o igual que 1. De la misma manera se demuestra que 2 no divide a $1 - \sqrt{5}$.

Ejercicios

1) Demuestre que si dos elementos a y b en un dominio D son asociados, entonces $(a) = (b)$ y viceversa.

2) Sea R un anillo y a, b, c elementos en R. Probar que si

$$a|b \quad \text{y} \quad b|c$$

entonces

$$a|c$$

3) Probar que todo número primo en el anillo $\mathbb{Z}$ de los enteros es irreducible.

4) Probar que si I es un ideal de un anillo R, tal que I contiene una unidad, entonces $I = R$.

5) Expresar los números 1521 y 670 como un producto de irreducibles en $\mathbb{Z}$.

6) Probar que si a y b son dos elementos irreducibles tales que $a|b$, entonces a y b son asociados.

7) Probar que si u y v son unidades, entonces uv es una unidad.

8) Demuestre que el conjunto de las unidades forman un grupo bajo la multiplicación.

9) Hallar el conjunto de las unidades del anillo $\mathbb{Z}_{10}$.

10) Sean $x_1, \cdots, x_n$ elementos en un anillo R. Entonces definimos el conjunto

$$(x_1, \cdots, x_n) = \{r_1x_1 + \cdots + r_nx_n \mid r_i \in R\}$$

Probar que este conjunto es un ideal de R, el cual se llama **ideal generado por** $x_1, \cdots, x_n$.

11) Probar que en el anillo $\mathbb{Z}$ de los enteros, todo elemento primo es irreducible.

12) Demuestre que si D es Dominio de Factorización Unica, entonces todo elemento irreducible es primo.

13) Sea $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq C$ con las operaciones de suma y multiplicación de números complejos. Probar que R es un anillo conmutativo con unidad.

14) La norma en el anillo R del ejemplo anterior, se define por

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

Probar que esta norma satisface las propiedades

i) $N(x) \geq 0$ para todo $x \in R$
ii) $N(x) = 0$ si y sólo si $x = 0$
iii) $N(xy) = N(x)N(y)$ para todo x, y en R.

15) Probar que el anillo R del problema 13 es un Dominio de Integridad.

16) Probar que las unidades u del anillo R están caracterizadas por la condición $N(u) = 1$. Determine todas las unidades de este anillo.

17) Dos elementos x e y en un anillo R se dicen primos relativos si $(x, y) = 1$. Probar que si x e y son primos relativos, entonces

$$Rx + Ry = R.$$

18) Probar que si p es un número primo y $p \not| a$ entonces $(p, a) = 1$.

19) Demuestre que existen infinitos números primos.

20) Demuestre que existen infinitos primos de la forma $4n + 1$.

21) Probar que la relación de asociados en un anillo R, define una relación de equivalencia.

22) Sean a y b enteros positivos, los cuales se factorizan como producto de primos

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \qquad \alpha_i \geq 0$$

$$b = p_1^{\beta_1} \cdots p_t^{\beta_t} \qquad \beta_i \geq 0$$

Probar que

$$(a, b) = p_1^{\gamma_1} \cdots p_t^{\gamma_t}$$

donde $\gamma_i = \min\{\alpha_i, \alpha_i\}, \quad 1 \leq i \leq t.$

8.4 Dominios Euclideanos

Definición 8.4.1 *Un Dominio de Integridad D se dice* **Dominio Euclideano**, *si existe una función*

$$d : D\backslash\{0\} \longrightarrow \mathbb{Z}^+$$

tal que

i) Para a y b en D, no nulos, se tiene

$$d(a) \leq d(ab)$$

ii) Para a y b en D, no nulos, existen elementos q y r en D tales que

$$a = qb + r$$

con $r = 0$ o $d(r) < d(b)$.

Ejemplo: El anillo de los enteros $\mathbb{Z}$ con la función $d(x) = |x|$ es un Dominio Euclideano. La propiedad $i)$ es consecuencia inmediata de la definición de valor absoluto para números enteros y la propiedad $ii)$ es precisamente el algoritmo de división para los enteros.

Teorema 8.4.1 *Sea D un Dominio Euclideano. Entonces D es un Dominio de Ideales Principales.*

Demostración: Sea I un ideal de D. Entonces debemos probar que I es un ideal principal.

Si $I = (0)$, entonces es claro que I es principal. Sea $I \neq (0)$. Luego existe un elemento $a \in I$ tal que

$$d(a) = \min\{d(x) | x \in I\} \tag{8.13}$$

Sea $x \in I$. Entonces por ser D un Dominio Euclideano, existen elementos q y r en D tales que

$$x = qa + r \tag{8.14}$$

con $r = 0$ o $d(r) < d(a)$.

Veamos que la condición $d(r) < d(a)$ nos lleva a una contradicción. En efecto, de (**??**) tenemos que $r = x - qa$ y por lo tanto $r \in I$. Luego $d(r) \geq d(a)$, por (**??**), y entonces la posibilidad $d(r) < d(a)$ queda descartada. La única alternativa posible es $r = 0$ en (**??**), lo cual nos da: $x = qa$. Esto es $I \subseteq (a)$.

La otra inclusión es evidente y en consecuencia el ideal I es principal generado por a.

♠

Corolario 8.4.1 *Todo Dominio Euclideano es un Dominio de Factorización Unica.*

Demostración: Consecuencia del Teorema anterior y del teorema **??**.

♠

Si D es un Dominio Euclideano, entonces D tiene una unidad 1 y los elementos unidades están caracterizados de la forma siguiente

Proposición 8.4.1 *Sea u un elemento en un Dominio Euclideano D, entonces u es una unidad si y sólo si $d(u) = d(1)$.*

Demostración: Supongamos que u es una unidad, y sea v en D tal que

$$uv = 1$$

Entonces

$$d(1) = d(uv) \geq d(u) \geq 1$$

Luego $d(u) = 1$

Por otro lado, si $d(u) = 1$, sean q y r tales que

$$1 = uq + r$$

con $r = 0$ o $d(r) < d(u)$.

Como $d(r) \geq 1$, por definición de la función d debemos tener $r = 0$. Luego $uq = 1$ y así vemos que u es una unidad.

♠

En un Dominio Euclideano D, dado cualquier par de elementos a y b, entonces el Máximo Común Divisor entre ellos siempre existe, pues D es un Dominio de Ideales principales. Afortunadamente, en los Dominios Euclideanos se puede calcular el Máximo Común Divisor mediante un algoritmo, llamado método de Euclides, el cual depende de las propiedades de la función d.

Teorema 8.4.2 *(Método de Euclides para calcular el Máximo Común Divisor) Sean a y b dos elementos en un Dominio Euclideano D y consideremos las divisiones sucesivas*

$$\begin{aligned} b &= aq_0 + r_1 \quad , \quad d(r_1) < d(a) \\ a &= r_1 q_1 + r_2 \quad , \quad d(r_2) < d(r_1) \\ r_1 &= r_2 q_2 + r_3 \quad , \quad d(r_2) < d(r_2) \\ &\vdots \\ r_i &= r_{i+1} q_{i+1} + r_{i+2} \quad , \quad d(r_{i+2}) < d(r_{i+1}) \\ &\vdots \end{aligned} \tag{8.15}$$

Entonces existe un $n \geq 0$ *tal que*

$$r_n = r_{n+1} q_{n+1}$$

y además se cumple $r_{n+1} = (a, b)$.

Demostración: La sucesión de elementos $\{r_i\}_{i \geq 1}$ satisface

$$d(r_1) > d(r_2) > \cdots > d(r_I) >$$

Por ser una sucesión de números positivos, la cual es decreciente, debe ser finito y por lo tanto se debe tener, para algún $n \geq 0$

$$r_{n+2} = 0 \quad , \quad r_{n+1} \neq 0$$

Es decir, r_{n+1} es el último resto distinto de cero en (**??**). Afirmamos que r_{n+1} es el Máximo Común Divisor entre a y b.

En primer lugar, se tienen las relaciones

$$\begin{aligned} r_n &= r_{n+1} q_{n+1} \\ r_{n-1} &= r_n q_n + r_{n+1} \\ &\vdots \\ r_1 &= r_2 q_2 + r_3 \\ a &= r_1 q_1 + r_2 \\ b &= aq_0 + r_1 \end{aligned} \tag{8.16}$$

De la ecuación (**??**) se deduce que $r_{n+1}|r_n$

Luego $r_{n+1}|r_nq_n+r_{n+1}$ y por lo tanto $r_{n+1}|r_{n-1}$. Continuando de esta manera, se llega a demostrar que r_{n+1} divide a todos los r_i restantes, $1 \leq i \leq n$. Luego $r_{n+1}|r_1q_1 + r_2$ y por lo tanto $r_{n+1}|a$. También $r_{n+1}|aq_0 + r_1$, lo cual implica que $r_{n+1}|b$.

Finalmente, sea c un elemento de D, tal que $c|a$ y $c|b$. Entonces usando (**??**), tendremos

$$c|b - aq_0$$

y por lo tanto $c|r_1$.

Continuando este proceso en el sistema de ecuaciones en (**??**), se llega a demostrar que $c|r_i$ para todo $1 \leq i \leq n$ y por lo tanto $c|r_{n+1}$.

Luego r_{n+1} satisface las dos condiciones de Máximo Común Divisor entre a y b.

♠

Este algoritmo se puede utilizar para hallar el Máximo Común Divisor entre dos números a y b.

Ejemplo 1: Hallar $(345, 20)$

Tenemos entonces

$$\begin{aligned} 345 &= 20 \times 17 + 5 \\ 20 &= 5 \cdot 4 \end{aligned}$$

luego $(345, 20) = 5$

Cerramos esta sección con el estudio de un Dominio Euclideano muy especial, el cual fue descubierto por el matemático alemán Carl Friedrich Gauss $(1777 - 1855)$, en relación al problema de determinar que números enteros positivos se pueden expresar como suma de dos cuadrados.

Ejemplo 2: (Enteros de Gauss) Sea A el conjunto de números complejos de la forma

$$A = \{x + iy \mid x, y \in \mathbb{Z}\}$$

Dejaremos como ejercicio para el lector, el probar que A es un Dominio de Integridad. Probaremos que A es un Dominio Euclideano con la función

$$d(x + iy) = x^2 + y^2 \tag{8.17}$$

para todo $x + iy \in A$.

Notemos en primer lugar que la función

$$d : A \longrightarrow \mathbb{Z}^+$$

está bien definida, pues si $x+yi \in A$, entonces x e y son números enteros y por lo tanto $d(x + iy)$ es un entero positivo. Además si $a = x + iy$ entonces

$$d(a) = (x + iy)(x - iy) = a\overline{a}$$

donde $\overline{a}$ denota el conjugado de a.

Luego d tiene la propiedad de una norma

$$d(ab) = d(a)d(b)$$

En efecto:

$$\begin{aligned} d(ab) &= (ab)\overline{(ab)} \\ &= (ab)(\overline{a}\overline{b}) \\ &= d(a)d(b) \end{aligned}$$

Por lo tanto la función d satisface la propiedad $i)$ de la definición de un Dominio Euclideano:

$$d(ab) \geq d(a)$$

para todos a y b en A con $a \neq 0$ y $b \neq 0$.

Probaremos que A satisface la condición $ii)$ de la definición.

Sean a y b en A con $a \neq 0$. Entonces se tiene el número complejo $\frac{a}{b} = \alpha + \beta i$, donde $\alpha, \beta \in \mathcal{Q}$. Luego existen enteros x e y tales que

$$|x - \alpha| \leq \frac{1}{2} \quad \text{y} \quad |\beta - y| \leq \frac{1}{2}$$

Si tomamos $q = x + iy$, se tiene que

$$a = qb + (a - qb) \tag{8.18}$$

y además se cumple

$$d\left(\frac{a}{b} - q\right) = (\alpha - x)^2 + (\beta - y)^2 < \frac{1}{2}$$

Luego hacemos $r = a - qb$ y $r = 0$, o bien

$$\begin{aligned} d(r) &= d(a - qb) \\ &= d(b)d\left(\frac{a}{b} - q\right) \\ &\leq \frac{1}{2}d(b) < d(b) \end{aligned}$$

En conclusión, hemos demostrado que A es un Dominio Euclideano.

Ejercicios

1) Mostrar que todo cuerpo F es un Dominio Euclideano.

2) Sea D un Dominio Euclideano. Mostrar que para cada par de elementos a y b, los elementos q y r en la definición, no son necesariamente únicos. Usar un contraejemplo.

3) Probar que todo elemento a en un Dominio Euclideano satisface

$$d(1) \leq d(a)$$

4) Probar que para todo x en un Dominio Euclideano se tiene

$$d(x) = d(-x)$$

5) Probar que si a y b no son unidades de un Dominio Euclideano D, entonces

$$d(a) < d(ab)$$

6) Usando el método de Euclides, calcular
   a) $(1560, 68)$
   b) $(752, 541)$
   c) $(1110, 720)$
   d) $(212, 2703)$

7) Expresar el Máximo Común Divisor entre a y b como una combinación $d = ax + by$ para los siguientes pares de enteros

   a) $(120, 45)$
   b) $(615, 814)$
   c) $(1714, 48)$
   d) $(248, 623)$

8) Probar que el conjunto A de los Enteros de Gauss definido por

$$A = \{x + iy \mid x, y \in \mathbb{Z}\}$$

es un Dominio de Integridad.

9) Sea $x = 3 + 2i$ e $y = -1 + 4i$ en A. Hallar

   a) $x + y$
   b) xy
   c) x/y
   d) $d(x)$,$d(y)$

e) $d(xy)$

10) Hallar todas las unidades en el anillo A de los Enteros de Gauss.

11) Probar que si x es un número racional, entonces existe un entero z tal que $|x - z| \leq \frac{1}{2}$.

12) Hallar el cociente y el resto de la división de $a = 10 + 2i$ entre $b = 2 - i$.

13) Probar que si a y b son elementos de un Dominio Euclideano D, tales que $d(a) = d(b)$, entonces se tiene $(a) = (b)$.

14) Demuestre que 2 no es un elemento irreducible en los Enteros de Gauss.