Un recorrido por los conceptos fundamentales del Álgebra

LUCIANO J. GONZÁLEZ

2022

Núcleo de Matemática Pura y Aplicada
Facultad de Ciencias Exactas y Naturales
Universidad Nacional de La Pampa
lucianogonzalez@exactas.unlpam.edu.ar
https://sites.google.com/view/numpa-unlpam/

El valor de un libro destinado a la enseñanza de las Matemáticas
se mide por la calidad de los problemas que le propone al estudiante,
ya que sin la participación activa de éste no existe, propiamente hablando,
enseñanza matemática; ni antigua ni moderna.

Norberto A. Fava

Índice general

1. Principio de Inducción **1**

1.1. Sumatorias y productorias 1
1.2. Conjuntos inductivos 3
1.3. Principio de inducción 4
Ejercicios propuestos 10

2. Combinatoria **13**

2.1. Permutaciones y Factorial 13
2.2. Permutaciones con repetición 15
2.3. Variaciones 15
2.4. Variaciones con repetición 18
2.5. Combinaciones 19
2.6. Combinaciones con repetición 20
2.7. Números combinatorios 22
2.8. El binomio de Newton 24
Ejercicios propuestos 27

3. Divisibilidad en $\mathbb{Z}$ **29**

3.1. El conjunto de los números enteros 29
3.2. La relación divide 30
3.3. El Teorema de la División Entera 34
3.4. Máximo común divisor 39
3.5. Números coprimos y ecuaciones diofánticas 43
3.6. Mínimo común múltiplo 48
3.7. Números primos 50
Ejercicios propuestos 56

4. Números Complejos **59**

4.1. El cuerpo de los números complejos 59
4.2. Representación geométrica y conjugado 64
4.3. Módulo 65
4.4. Forma trigonométrica o polar 68
4.5. Raíces n-ésimas 73
4.6. Raíces n-ésimas de la unidad 76

Ejercicios propuestos 80

5. Polinomios **81**
5.1. Definiciones 81
5.2. Suma y producto de polinomios 83
5.3. Divisibilidad en $K[X]$ 88
5.4. Polinomios irreducibles 94
5.5. Raíces de polinomios 97
5.6. Raíces y polinomios irreducibles en $\mathbb{R}[X]$ y $\mathbb{C}[X]$ 102
5.7. Acotación de raíces 109
Ejercicios propuestos 113

6. Estructuras Algebraicas **115**
6.1. Leyes de composición internas 115
6.2. Grupos 121
6.2.1. Subgrupos 127
6.3. Anillos 128
6.4. Homomorfismos 134
6.4.1. Homomorfismos de grupos 134
6.4.2. Homomorfismos de anillos 138
Ejercicios propuestos 140

Bibliografía **145**

Capítulo 1

Principio de Inducción

1.1. Sumatorias y productorias

Denotamos por $\mathbb{N}$ al conjunto de los números naturales. Así

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

Sobre el conjunto de números naturales tenemos definidas dos operaciones binarias muy conocidas: la **suma** (+) y el **producto** (.). Esto es, si $n, m \in \mathbb{N}$, entonces $n + m, n.m \in \mathbb{N}$. Estas dos operaciones tienen las siguientes propiedades que usaremos a lo largo del apunte sin mencionarlas: para todos números naturales $n, m, k \in \mathbb{N}$ se cumplen,

- **Asociativa**: $n + (m + k) = (n + m) + k$ y $n.(m.k) = (n.m).k$;
- **Conmutativa**: $n + m = m + n$ y $n.m = m.n$;
- **Distributiva**: $n.(m + k) = n.m + n.k$.

Sea $n \in \mathbb{N}$. Una **sumatoria** es una expresión de la forma $\sum_{i=1}^{n} a_i$ que expresa la suma de los términos $a_1, a_2, \dots, a_n$:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_{n-1} + a_n.$$

Ejemplo 1.1.

1. $\sum_{i=1}^{n} = 1 + 2 + \cdots + (n-1) + n.$
2. $\sum_{k=0}^{m} 3k = 3.0 + 3.1 + 3.2 + \cdots + 3.(m-1) + 3.m.$
3. $\sum_{i=1}^{n} 4 = 4 + 4 + \cdots + 4 = 4.n.$

Ejemplo 1.2. Consideremos la siguiente suma: $s = 1 + 2 + 4 + 8 + 16 + 32 + 64$. Vamos a expresar la suma s utilizando una sumatoria:

$$s = 1 + 2 + 4 + 8 + 16 + 32 + 64 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = \sum_{i=0}^{6} 2^i.$$

A continuación presentamos tres propiedades básicas que cumplen las sumatorias.

Proposición 1.3

Sea $n \in \mathbb{N}$. Las siguientes propiedades se cumplen:

(1) $\sum_{i=1}^{n+1} a_i = \sum_{i=1}^{n} a_i + a_{n+1}$.

(2) $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i)$.

(3) $c.\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} ca_i$.

Demostración. Solo vamos a indicar qué propiedades utilizar para demostrar estas propiedades, la prueba completa y en detalle queda a cargo del lector.

(1) Utilizar la asociatividad de la suma.

(2) Utilizar la conmutatividad y asociatividad de la suma.

(3) Utilizar que el producto distribuye con respecto a la suma. ■

Sea $n \in \mathbb{N}$. Una **productoria** es una expresión de la forma $\prod_{i=1}^{n} a_i$ que expresa el producto de los factores $a_1, a_2, \ldots, a_n$:

$$\prod_{i=1}^{n} a_i = a_1.a_2.\ldots.a_{n-1}.a_n.$$

Ejemplo 1.4. 1. $\prod_{i=1}^{5} i = 1.2.3.4.5.$ 2. $\prod_{i=1}^{n} 3^{i+1} = 3^2.3^3.\ldots.3^n.3^{n+1}$.

Proposición 1.5

Sea $n \in \mathbb{N}$. Entonces las siguientes propiedades se cumplen.

1. $\prod_{i=1}^{n+1} a_i = \prod_{i=1}^{n} a_i.a_{n+1}$.
2. $\prod_{i=1}^{n} c = c^n$.
3. $\prod_{i=1}^{n} a_i . \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} (a_i.b_i)$.

Demostración. A cargo del lector. ■

Problema 1.6

1. Desarrollar la siguiente sumatoria $\sum_{i=1}^{5} (2i+1)X^{2i}$.
2. Expresar como sumatoria la siguiente suma $1 + 8 + 27 + 64 + 125 + 216 + 343$.

1.2. Conjuntos inductivos

Definición 1.7

Un subconjunto A de $\mathbb{R}$ es llamado **inductivo** si cumple las siguientes dos condiciones:

1. $1 \in A$.
2. Si $x \in A$, entonces $x + 1 \in A$.

Ejemplo 1.8. El conjunto $\mathbb{N}$ de números naturales es inductivo. Sabemos que 1 es un número natural, así $1 \in \mathbb{N}$. Entonces $\mathbb{N}$ cumple la primer condición en la definición de conjunto inductivo. Ahora, para probar que $\mathbb{N}$ satisface la segunda condición, sea $x \in \mathbb{N}$. Esto es, x es un número natural. Entonces sabemos que $x + 1$ es también un número natural. Con lo cual $x + 1 \in \mathbb{N}$. Entonces, $\mathbb{N}$ también cumple la segunda condición. Por lo tanto, $\mathbb{N}$ es un conjunto inductivo.

Ejemplo 1.9. Veamos que el conjunto de números racionales $\mathbb{Q}$ es un conjunto inductivo. Es claro que $1 = \frac{1}{1} \in \mathbb{Q}$. Así $\mathbb{Q}$ cumple la primer condición de conjunto inductivo. Ahora, sea $x \in \mathbb{Q}$. Entonces, como x es racional, existen dos enteros a y b, con $b \neq 0$, tales que $x = \frac{a}{b}$. Ahora $x + 1 = \frac{a}{b} + 1 = \frac{a+b}{b} \in \mathbb{Q}$, pues $a + b$ y b son enteros. Entonces, $\mathbb{Q}$ cumple la segunda condición de conjunto inductivo. Por lo tanto, $\mathbb{Q}$ es un conjunto inductivo.

Ejemplo 1.10. El conjunto $\mathbb{Z} - \{0\}$ no es inductivo. Veamos que $\mathbb{Z} - \{0\}$ no cumple con la segunda condición de la definición de conjunto inductivo. Para ello, debemos encontrar un $x \in \mathbb{Z} - \{0\}$ tal que $x + 1 \notin \mathbb{Z} - \{0\}$. Si tomamos $x = -1$, tenemos que $x = -1 \in \mathbb{Z} - \{0\}$ y $x + 1 = 0 \notin \mathbb{Z} - \{0\}$. Por lo tanto, $\mathbb{Z} - \{0\}$ no es inductivo.

Ejemplo 1.11. Sea A el conjunto formado por todos los números naturales n que cumplen la identidad

$$1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1.$$

Esto es,

$$A = \{n \in \mathbb{N} : \ 1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1\}.$$

También podemos expresar al conjunto A utilizando sumatoria:

$$A = \{n \in \mathbb{N} : \ \sum_{i=1}^{n} 2^{i-1} = 2^n - 1\}.$$

Vamos a probar que el conjunto A es inductivo. Primero debemos comprobar que $1 \in A$. Para ello debemos reemplazar n por 1 en la ecuación $\sum_{i=1}^{n} 2^{i-1} = 2^n - 1$ y ver si se cumple la igualdad. Tenemos que $\sum_{i=1}^{1} 2^{i-1} = 2^{1-1} = 1$ y $2^1 - 1 = 1$. Entonces, $\sum_{i=1}^{1} 2^{i-1} = 2^1 - 1$, y por lo tanto $1 \in A$. Ahora debemos probar que A cumple con la segunda condición de la definición de conjunto inductivo. Para esto, debemos suponer que $x \in A$ y probar que $x + 1 \in A$.

Entonces, sea $x \in A$. Con lo cual x cumple la ecuación $\sum_{i=1}^{x} 2^{i-1} = 2^x - 1$. Debemos probar que $\sum i = 1^{x+1}2^{i-1} = 2^{x+1} - 1$. Comenzamos con el miembro izquierdo de la ecuación anterior:

$$\begin{aligned}
\sum_{i=1}^{x+1} 2^{i-1} &= \underbrace{\sum_{i=1}^{x} 2^{i-1}} + 2^{x+1-1} \\
&= 2^x - 1 + 2^x && \text{usamos que } \sum_{i=1}^{x} 2^{i-1} = 2^x - 1 \\
&= 2.2^x - 1 \\
&= 2^{x+1} - 1
\end{aligned}$$

Con lo cual que $\sum_{i=1}^{x+1} 2^{i-1} = 2^{x+1} - 1$, por lo tanto $x + 1 \in A$. Así, el conjunto A cumple las dos condiciones requeridas para ser inductivo.

Observación 1.12. Podemos observar que $\mathbb{N}$ es el conjunto inductivo "más pequeño". Esto es, si $A \subseteq \mathbb{R}$ es un conjunto inductivo, entonces $\mathbb{N} \subseteq A$. En efecto, sea $n \in \mathbb{N}$. Si $n = 1 \in A$, pues A es inductivo. Sea $n > 1$. Como $1 \in A$, tenemos que $2 = 1 + 1 \in A$. Luego, $3 = 2 + 1 \in A$. Continuando de esta forma llegaremos a que $n = (n-1) + 1 \in A$. Por lo tanto, $\mathbb{N} \subseteq A$.

Problema 1.13

Probar que el intervalo $(0, +\infty)$ es un conjunto inductivo. ¿El conjunto $(0, +\infty) - \{\frac{1}{2}\}$ es inductivo? y ¿el conjunto $(0, +\infty) - \{\frac{3}{2}\}$?

Problema 1.14

Sea $A \subseteq \mathbb{R}$ tal que $1 \in A$. Si A no es inductivo, ¿qué podemos afirmar?

1.3. Principio de inducción

El **principio de inducción** es una herramienta fundamental para probar que una propiedad o afirmación sobre los números naturales es verdadera. Consideremos la siguiente pregunta:

¿es verdad que para todo número natural $n \in \mathbb{N}$ se cumple que $n < 2^n$?

Podemos verificar que esa desigualdad se cumple para algunos valores de n:

$$n = 1 \implies 1 < 2 = 2^1 \qquad n = 3 \implies 3 < 8 = 2^3$$

$$n = 2 \implies 2 < 4 = 2^2 \qquad n = 4 \implies 4 < 16 = 2^4$$

Y podemos continuar comprobando que esta desigualdad se cumple para $n = 5, 6, \ldots$. Pero, como se darán cuenta, este proceso no lo podemos continuar indefinidamente dado que el

conjunto $\mathbb{N}$ es infinito. Con lo cual, necesitamos recurrir a otro argumento para verificar que la desigualdad anterior se cumple PARA TODOS los números naturales n.

Teorema 1.15: Principio de Inducción

Sea $P(n)$, $n \in \mathbb{N}$, una proposición sobre los números naturales. Si P satisface que

- **Caso base:** $P(1)$ es verdadera, y
- **Paso inductivo:** si $P(k)$ es verdadera, entonces $P(k+1)$ es verdadera,

entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Observación 1.16. Para probar que el Paso inductivo se cumple, debemos siempre suponer que $P(k)$ es verdadero, y a esto lo vamos a llamar la **hipótesis inductiva (H.I.)**

Demostración. Consideremos el siguiente conjunto

$$S = \{k \in \mathbb{N} : P(k) \text{ es verdadera}\}.$$

Observemos que $S \subseteq \mathbb{N}$. Ahora probaremos que S es inductivo. Por el Caso base sabemos que $P(1)$ es verdadera, entonces por definición del conjunto S tenemos que $1 \in S$. Así S cumple con la primer propiedad de conjunto inductivo. Probemos que la segunda propiedad de conjunto inductivo se cumple. Sea $k \in S$. Entonces $P(k)$ es verdadera. Por el Paso inductivo podemos concluir que $P(k+1)$ es verdadera. Luego $k+1 \in S$. Por lo tanto, S es inductivo. Ahora por la Observación 1.12 sabemos que $\mathbb{N}$ es el conjunto inductivo más pequeño, con lo cual $\mathbb{N} \subseteq S$. Entonces $S = \mathbb{N}$. Luego, por la definición del conjunto S, tenemos que $P(k)$ es verdadero para todo $k \in \mathbb{N}$. ■

Ejemplo 1.17. Probemos que para todo $n \in \mathbb{N}$, $n < 2^n$. Podemos considerar la forma proposicional $P(n) : \ n < 2^n$. Vamos a aplicar el Principio de Inducción a $P(n)$.

- **Caso base:** Primero tenemos que verificar que $P(1)$ es verdadera. Observemos que $P(1) : \ 1 < 2^1$, lo cual es verdadero.
- **Paso inductivo:** Ahora debemos probar el paso inductivo. Para ello debemos suponer que $P(k) : \ k < 2^k$ es verdadero (H.I.). Debemos probar que $P(k+1) : \ k+1 < 2^{k+1}$ es verdadero. Comenzamos: por la H.I. sabemos que $k < 2^k$. Entonces

$$k < 2^k \implies k+1 < 2^k + 1 \implies k+1 < 2^k + 1 < 2^k + 2^k = 2^{k+1}.$$

  Entonces, $P(k+1) : \ k+1 < 2^{k+1}$ es verdadero. Por lo tanto, como se cumplen las dos condiciones del Principio de Inducción podemos concluir que $n < 2^n$ para todo $n \in \mathbb{N}$. ■

Ejemplo 1.18. Probar que para todo $n \in \mathbb{N}$, se cumple que

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

La afirmación anterior nos dice que la suma de los primeros n números naturales da como resultado $\frac{n(n+1)}{2}$, para todo número natural n. También podemos observar que la afirmación anterior la podemos expresar usando sumatorias: vamos a probar que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \tag{1.1}$$

para todo $n \in \mathbb{N}$. Comenzamos:

- **Caso base:** Primero debemos probar que la afirmación (1.1) es verdad para $n = 1$:

  $$\sum_{i=1}^{1} i = 1 \qquad \text{y} \qquad \frac{1.(1+1)}{2} = 1.$$

  Entonces $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$. Por lo tanto, la afirmación (1.1) se verdad para $n = 1$.

- **Paso inductivo:** Primero suponemos que la afirmación (1.1) es verdad para un $n = k$ (nuestra hipótesis inductiva), esto es, suponemos que se cumple que

  $$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \tag{H.I.}$$

  Ahora debemos probar que la afirmación (1.1) es cumple para $n = k+1$, esto es, debemos probar que

  $$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

  Comenzamos:

  $$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\ &\overset{H.I.}{=} \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

  Así, probamos que la afirmación (1.1) se cumple para $n = k+1$.

Como se cumplen las dos condiciones del Principio de Inducción, la afirmación (1.1) es verdad para todo $n \in \mathbb{N}$. ■

Ejemplo 1.19. Probar que para todo $n \in \mathbb{N}$, $n^2 + n$ es un número par. Como ésta es una afirmación sobre los números naturales, podemos utilizar el Principio de Inducción para probarla. Comenzamos:

- **Caso base:** Debemos probar que se cumple para $n = 1$. Esto es, debemos probar que $1^1 + 1$ es un número par. Esto trivial porque $1^2 + 1 = 2$ y sabemos que 2 es par. Por lo tanto, la afirmación se cumple para $n = 1$.

- **Paso inductivo:** Suponemos que la afirmación se cumple para $n = k$. Esto es, suponemos que $k^2 + k$ es un número par (H.I.). Debemos probar que la afirmación es verdad para $n = k + 1$, esto es, debemos probar que $(k+1)^2 + (k+1)$ es par. Comenzamos: Por la H.I. sabemos que $k^2 + k$ es par, entonces $k^2 + k = 2.s$ para algún $s \in \mathbb{N}$. Ahora

$$\begin{aligned}(k+1)^2 + (k+1) &= k^2 + 2k + 1 + k + 1 \\ &= k^2 + k + 2(k+1) \\ &\overset{H.I.}{=} 2.s + 2(k+1) \\ &= 2(s + k + 1).\end{aligned}$$

  Como $(k+1)^2 + (k+1) = 2.q$ para algún $q \in \mathbb{N}$ (en este caso $q = s + k + 1$), $(k+1)^2 + (k+1)$ es un número par.

Como se cumplen las dos condiciones del Principio de Inducción, la afirmación es verdad para todo $n \in \mathbb{N}$. Esto es, probamos que $n^2 + n$ es par, para todo $n \in \mathbb{N}$. ■

Hemos visto y comprobado que el Principio de Inducción es muy útil para probar que ciertas afirmaciones son verdaderas para todo número natural n. Es claro que puede haber afirmaciones que no son verdad para todo número natural. Pero también hay ciertas afirmaciones que son verdaderas a partir de un número natural n_0, es decir, proposiciones $P(n)$ que son verdaderas para n_0, $n_0 + 1$, $n_0 + 2$, ... Por ejemplo, consideremos la afirmación $2n + 1 < n^2$. ¿Se cumple para todo número natural n? Pues no, para $n = 1$ no es verdad. Tampoco es verdad para $n = 2$, pues $2.2 + 1 = 5 \not< 4 = 2^2$. Pero podemos observar que

$$n = 3 \implies 2.3 + 1 = 7 < 9 = 3^2 \qquad n = 5 \implies 2.5 + 1 = 11 < 25 = 5^2$$

$$n = 4 \implies 2.4 + 1 = 9 < 16 = 4^2 \qquad n = 6 \implies 2.6 + 1 = 13 < 36 = 6^2$$

y podríamos continuar verificando que se cumple para $n = 7, 8, 9, \ldots$. Esto nos lleva a realizar la siguiente pregunta: ¿es verdad que $2n + 1 < n^2$ para todo $n \geq 3$? Para poder probar este tipo de afirmaciones necesitamos una versión "modificada" del Principio de Inducción.

Teorema 1.20: Principio de inducción desplazada

Sea $P(n)$ una afirmación sobre $\mathbb{N}$. Sea $n_0 \in \mathbb{N}$. Si P satisface que:

- **Caso base:** $P(n_0)$ es verdad, y
- **Paso inductivo:** si $P(k)$ es verdadero, con $k \geq n_0$, entonces $P(k+1)$ es verdadero,

entonces $P(n)$ es verdad para todo $n \geq n_0$.

Demostración. Consideremos el siguiente conjunto

$$S = \{1, 2, \ldots, n_0 - 1\} \cup \{n \in \mathbb{N} : P(n) \text{ es verdad}\}.$$

Notemos primero que $S \subseteq \mathbb{N}$. Ahora vamos a probar que S es un conjunto inductivo. Primero, es claro que $1 \in S$. Para probar la segunda condición en la definición de conjunto inductivo, sea $k \in S$. Debemos probar que $k+1 \in S$. Tenemos tres casos posibles: (i) $1 \leq k < n_0 - 1$; (ii) $k = n_0 - 1$; o (iii) $k \geq n_0$. Vamos a ver que en cualquiera de los tres casos se cumple que $k+1 \in S$.

- Caso (i): $1 \leq k < n_0 - 1$. Entonces $2 \leq k+1 < n_0$. Con lo cual, $k+1 \in S$.
- Caso (ii): $k = n_0 - 1$. Entonces $k+1 = n_0$. Por el Caso base tenemos que $P(n_0)$ es verdad, entonces por definición del conjunto S, $n_0 \in S$. Por lo tanto, $k+1 \in S$.
- Caso (iii): $k \geq n_0$. Por hipótesis $k \in S$. Entonces, como $k \geq n_0$ y $k \in S$, tenemos que $k \in \{n \in \mathbb{N} : P(n) \text{ es verdad}\}$. Así tenemos que $P(k)$ es verdadero. Por el Paso inductivo, tenemos que $P(k+1)$ es verdadero. Entonces, por definición del conjunto S tenemos que $k+1 \in S$.

Hemos probado que S es inductivo. Luego, por la Observación 1.12, tenemos que $\mathbb{N} \subseteq S$. Entonces $S = \mathbb{N}$. Esto es: $\{1, 2, \ldots, n_0 - 1\} \cup \{n \in \mathbb{N} : P(n) \text{ es verdadero}\} = \mathbb{N}$. Ahora, observando que $\mathbb{N} = \{1, 2, \ldots, n_0 - 1\} \cup \{n \in \mathbb{N} : n \geq n_0\}$, podemos concluir que $\{n \in \mathbb{N} : n \geq n_0\} \subseteq \{n \in \mathbb{N} : P(n) \text{ es verdadero}\}$. En otras palabras, $P(n)$ es verdad para todo natural $n \geq n_0$. ■

Ejemplo 1.21. Probar que para todo $n \geq 3$, se cumple que $2n + 1 < n^2$.

- **Caso base:** Debemos probar que es verdad para $n = 3$. Sabemos que $2.3 + 1 = 7 < 9 = 3^2$. Por lo tanto, se cumple el Caso base para $n = 3$.
- **Paso inductivo:** Supongamos que la afirmación es verdad para un $n = k \geq 3$. Esto es, $2k + 1 < k^2$. Debemos probar que la afirmación es verdad para $n = k + 1$. Esto es, debemos probar que $2(k+1) + 1 < (k+1)^2$. Comenzamos:

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 >_{\text{H.I.}} 2k + 1 + 2k + 1 \\ &= 2k + 2k + 2 \\ &= 2(k+1) + 2k > 2(k+1) + 1.\end{aligned}$$

  La última desigualdad se cumple porque: $k \geq 3 \implies 2k \geq 6 > 1$.

Por lo tanto, como se cumplen el Caso base y el Paso inductivo del Principio de inducción desplazada, podemos afirmar que $2n + 1 < n^2$ para todo número natural $n \geq 3$. ■

Hay otra versión del Principio de Inducción que suele ser de utilidad en ciertas ocasiones. Por ejemplo, consideramos la sucesión $(a_n)_{n \in \mathbb{N}}$ definida de la siguiente forma:

$$a_1 = 1 \qquad \text{y} \qquad a_{n+1} = 1 + \sum_{k=1}^{n} a_k. \tag{1.2}$$

Observemos que en la definición de la sucesión $(a_n)_{n\in\mathbb{N}}$, hemos especificado el valor del primer término a_1 de la sucesión y los términos restantes a_{n+1} se definen a partir de los anteriores: $a_1, a_2, \ldots, a_n$. Calculemos algunos de los primeros términos de la sucesión para ejemplificar la definición de dicha sucesión:

$$\begin{aligned}
a_1 &= 1\\
a_2 &= 1 + a_1 = 2\\
a_3 &= 1 + a_1 + a_2 = 4\\
a_4 &= 1 + a_1 + a_2 + a_3 = 8\\
a_5 &= 1 + a_1 + a_2 + a_3 + a_4 = 16\\
a_6 &= 1 + a_1 + a_2 + a_3 + a_4 + a_5 = 32\\
\vdots &= \quad \vdots
\end{aligned}$$

Es muy probable que el lector pueda adivinar y luego comprobar que los siguientes términos de la sucesión son $a_7 = 64$, $a_8 = 128, \ldots$. Luego, sería natural preguntarnos si es verdad que el n-ésimo término de la sucesión es igual a 2^{n-1}, es decir, ¿se cumple que $a_n = 2^{n-1}$ para todo $n \in \mathbb{N}$? Por lo que obtuvimos anteriormente esto se cumple para $n = 1, 2, \ldots, 8$. Pero ¿será verdad PARA TODOS los números naturales? Seguramente alguien sugerirá rápidamente aplicar el Principio de Inducción, y puede intentarlo, pero la cuestión es que el Principio de Inducción que hemos presentado anteriormente no es suficiente para probar esta afirmación. Necesitamos una nueva versión, que pasamos a enunciar.

Teorema 1.22: Principio de Inducción Completa

Sea $P(n)$ una afirmación sobre los números naturales. Si P satisface que:

- **Caso base:** $P(1)$ es verdadera, y
- **Paso inductivo:** si $P(1), P(2), \ldots, P(n)$ son verdaderas, entonces $P(n+1)$ es verdadera,

entonces $P(n)$ es verdad para todo $n \in \mathbb{N}$.

Para probar el teorema anterior necesitamos un resultado muy importante sobre los números naturales. Si bien lo que afirma el siguiente teorema parece trivialmente verdad, uno diría es "obvio", dicho teorema necesita una demostración. Por una cuestión de espacio y tiempo, omitiremos su demostración. El lector interesado puede ver la demostración en el Apéndice **??**.

Teorema 1.23: Principio de Buena Ordenación

Todo subconjunto A no vacío de $\mathbb{N}$ tiene un primer elemento.

Demostración del Principio de inducción completa. Comenzamos definiendo el siguiente conjun-

to:

$$H = \{n \in \mathbb{N} : P(n) \text{ es Verdadera}\}.$$

Notemos primero que $H \subseteq \mathbb{N}$. También observemos que deseamos probar que $H = \mathbb{N}$. Suponemos por absurdo que $H \neq \mathbb{N}$. Entonces $\mathbb{N} - H \neq \emptyset$. Como $\mathbb{N} - H$ es un subconjunto de $\mathbb{N}$ y no vacío, entonces por el Principio de Buena Ordenación tiene un primer elemento, que llamamos t. Es decir, $t \in \mathbb{N} - H$ y $t \leq k$, para todo elemento $k \in \mathbb{N} - H$. Como t es el menor elemento en $\mathbb{N} - H$, tenemos que para cada $s < t$, $s \in H$. Es decir, que $1, 2, \ldots, t-1 \in H$. Luego, por definición de H tenemos que $P(1), P(2), \ldots, P(t-1)$ son verdaderas. Entonces, por el Paso inductivo, tenemos que $P(t)$ es verdadera. Esto implica, por definición del conjunto H, que $t \in H$. Absurdo. Entonces, obtenemos que $H = \mathbb{N}$. Por lo tanto, $P(n)$ es verdadera para todo $n \in \mathbb{N}$. ■

Ejemplo 1.24. Dada la sucesión $(a_n)_{n\in\mathbb{N}}$ definida por (1.2), vamos a probar que para todo $n \in \mathbb{N}$, $a_n = 2^{n-1}$. Aplicamos el Principio de Inducción completa.

- **Caso base:** Por definición de la sucesión a_n tenemos que $a_1 = 1$ y claramente $2^{1-1} = 1$. Así $a_n = 2^{n-1}$ para $n = 1$.
- **Paso inductivo:** Supongamos que para todo $k < n+1$ tenemos que $a_k = 2^{k-1}$ (H.I.). Debemos probar que $a_{n+1} = 2^{(n+1)-1}$. Comenzamos: por definición de la sucesión $(a_n)_{n\in\mathbb{N}}$ tenemos que

$$a_{n+1} = 1 + \sum_{k=1}^{n} a_k \overset{(H.I.)}{=} 1 + \sum_{k=1}^{n} 2^{k-1} = 1 + (2^n - 1) = 2^n.$$

Por lo tanto, como se cumplen las dos condiciones del Principio de Inducción completa, tenemos que $a_n = 2^{n-1}$, para todo $n \in \mathbb{N}$. El lector puede probar usando el Principio de Inducción que para todo $n \in \mathbb{N}$, $\sum_{k=1}^{n} 2^{k-1} = 2^n - 1$ (ver Ejercicio 1.4).

Problema 1.25

Explique con sus propias palabras cuáles son las diferencias entre el Principio de Inducción, el Principio de Inducción Desplazada y el Principio de Inducción Completa.

Problema 1.26

¿Se cumple que $n^2 < 2^n$ para todo $n \in \mathbb{N}$? Si su respuesta es que si, probarlo. Si su respuesta es que no se cumple, ¿existe algún n_0 tal que $n^2 < 2^n$ para todo $n \geq n_0$? En caso que si, probarlo.

Ejercicios propuestos

Ejercicio 1.1. Probar las tres propiedades de la Proposición 1.3.

Ejercicio 1.2. Probar las tres propiedades de la Proposición 1.5.

Ejercicio 1.3. Determinar y justificar si los siguientes conjuntos son o no inductivos.

1. $A = [0, \infty)$.
2. $B = \mathbb{Q} - \{1/2\}$.

Ejercicio 1.4. Probar que para todo $n \in \mathbb{N}$ se cumple que $\sum_{k=1}^{n} 2^{k-1} = 2^n - 1$.

Ejercicio 1.5. Considerar la afirmación $(n-4)(n-10) > 0$. Determinar (justificando su repuesta) el número natural n_0 para el cual se cumple que $(n-4)(n-10) > 0$ para todo $n \geq n_0$.

Ejercicio 1.6. Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida de forma recursiva como sigue:

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1 \\ a_{n+2} &= a_n + a_{n+1}, \qquad \forall n \in \mathbb{N}. \end{aligned}$$

(Esta sucesión es conocida como la sucesión de Fibonacci). Probar por inducción la siguiente afirmación:

$$\text{Para todo } n \in \mathbb{N},\ a_n < \left(\tfrac{7}{4}\right)^n.$$

Ejercicio 1.7. Probar que para todo $n \in \mathbb{N}$,

$$\prod_{i=1}^{n} \left(1 + \frac{1}{i}\right) = n + 1.$$

Capítulo 2

Combinatoria

2.1. Permutaciones y Factorial

Ejemplo 2.1. Supongamos que un amigo ha olvidado su PIN para acceder al cajero automático, el cual consta de 4 dígitos. Sólo recuerda que los números de su PIN son 2, 7, 5 y 9, pero no recuerda en qué orden. Nos pide ayuda para saber cuántas combinaciones tiene que hacer cómo máximo para hallar su clave. Podemos proceder como sigue: Tenemos 4 lugares $\_\_\_\_\ \_\_\_\_\ \_\_\_\_\ \_\_\_\_$ para completar con los números 2, 7, 5 y 9. Entonces, para el primer lugar tenemos cuatro posibles elecciones: $\underbrace{\_\_\_\_}_{4}\ \_\_\_\_\ \_\_\_\_\ \_\_\_\_$. Ahora, como usamos uno de los números $\{2, 7, 5, 9\}$ para el primer lugar, tenemos tres posibilidades para el segundo lugar $\underbrace{\_\_\_\_}_{4}\ \underbrace{\_\_\_\_}_{3}\ \_\_\_\_\ \_\_\_\_$. Ya usamos un dígito para el primer lugar y uno para el segundo lugar, así nos quedan sólo dos posibilidades para completar el tercer lugar $\underbrace{\_\_\_\_}_{4}\ \underbrace{\_\_\_\_}_{3}\ \underbrace{\_\_\_\_}_{2}\ \_\_\_\_$. Y para último lugar nos queda una sola opción posible $\underbrace{\_\_\_\_}_{4}\ \underbrace{\_\_\_\_}_{3}\ \underbrace{\_\_\_\_}_{2}\ \underbrace{\_\_\_\_}_{1}$. Para cada una de las cuatro posibilidades del primer lugar, tenemos 3 posibilidades para el segundo, 2 posibilidades para el tercer lugar y una única posibilidad para el último lugar. Entonces el número total de combinaciones posible es: 4.3.2.1=24. ■

Ejemplo 2.2. Nuestro amigo anterior tiene una nueva pregunta para la cual desea nuestra ayuda. Él tiene 5 libros del colegio: uno de Matemática, uno de Física, uno de Biología, uno de Ciencias Sociales y uno de Geografía, los cuales tiene que ordenarlos es su repisa. Desea saber de cuántas formas es posible colocarlos en la repisa. Procedemos como sigue: para el primer lugar tiene cinco posibilidades (puede elegir cualquiera de los cinco libros); para cada elección del primer lugar tiene 4 posibles elecciones para colocar el segundo libro (si ya ubicó un libro en el primer lugar, le quedan 4 libros para el segundo lugar); para cada una de las elecciones del primer y segundo lugar tiene 3 posibles elecciones para ubicar un libro en el tercer lugar (si ya ubicó un libro en el primer lugar y un segundo libro en el segundo lugar, entonces le quedan sólo tres libros para colocar en el tercer lugar); para cada una de las elecciones del primer, segundo y tercer lugar tiene sólo dos posibles elecciones para el cuarto lugar (si ya ubicó un libro en el primer lugar, uno en el segundo y uno en el tercer

lugar, entonces sólo le quedan dos libros para colocar en el cuarto lugar); finalmente le queda un último libro para ubicar en el último lugar. Nos quedaría: $\underbrace{\quad}_{5}\ \underbrace{\quad}_{4}\ \underbrace{\quad}_{3}\ \underbrace{\quad}_{2}\ \underbrace{\quad}_{1}$.
Entonces, el número total de las posibles ordenaciones de los cinco libros es 5.4.3.2.1=120.

Las soluciones de los dos problemas anteriores que le ayudamos a resolver a nuestro amigo son muy similares y se pueden resolver utilizando una herramienta llamada *factorial*.

Definición 2.3

Dado un número entero $n \geq 0$, el **factorial** de n, denotado por $n!$, es el número natural definido por

$$0! = 1$$
$$n! = n.(n-1)! \quad \text{si } n > 0.$$

Ejemplo 2.4. Calculemos los primeros 6 factoriales:

$$0! = 1$$
$$1! = 1.(1-1)! = 1.0! = 1.1 = 1$$
$$2! = 2.(2-1)! = 2.1! = 2.1 = 1$$
$$3! = 3.(3-1)! = 3.2! = 3.2 = 6$$
$$4! = 4.(4-1)! = 4.3! = 4.6 = 24$$
$$5! = 5.(5-1)! = 5.4! = 5.24 = 120.$$

Ejemplo 2.5. Volvemos al problema de la ordenación de libros. ¿De cuántas formas se pueden ordenar 5 libros (distintos) en una estantería? Tenemos cinco lugares para colocar 5 libros. Así que el número total de posibilidades es 5.4.3.2.1=5!=120. Es decir, podemos ordenar los cinco libros de 120 formas distintas.

En resumen,

El factorial de n representa el número total de ordenar n objetos distintos.

Es decir, si tenemos n objetos distintos, la cantidad de formas que tenemos para ordenar esos n objetos es $n!$.

Problema 2.6

Supongamos que nuestro amigo tiene tres libros de Matemática (Matemática 1, 2 y 3), tiene tres libros de Biología (Biología 1, 2 y 3), tres libros de Química (Química 1, 2 y 3) y tres libros de Física (Física 1, 2 y 3). Tiene disponible en su habitación cuatro repisas en donde cada una entran sólo tres libros. Desea colocar en cada repisa los libros de la misma materia de forma ordenada (por ejemplo, en la primera repisa puede colocar los de Biología: B1 B2 B3, en la segunda los de Matemática: M1 M2 M3, e igual para las restantes repisas.) ¿De cuántas formas distintas puede realizar la ordenación de los libros?

2.2. Permutaciones con repetición

Ejemplo 2.7. Supongamos que queremos saber cuántas palabras distintas (recuerde que "palabra" es cualquier concatenación de letras con o sin sentido) podemos formar usando todas las letras de la palabra "ALAS". Tratemos de formar todas las palabras posibles:

AALS AASL ALAS ALSA ASAL ASLA LAAS LASA LSAA SAAL SALA SLAA.

Entonces hay 12 palabras distintas que podemos formar. Observemos que $12 \neq 4!$. Así que la cantidad de palabras distintas que podemos formar no es igual a la permutación de 4 objetos distintos. Esto es porque en la palabra "ALAS" tenemos dos letras que son iguales. Decimos que esta es una permutación con repetición.

Proposición 2.8

Dado un conjunto con m elementos, entre los cuales hay k_1 elementos iguales entre sí, hay otros k_2 elementos iguales entre sí, ..., hay otros k_r elementos iguales entre sí, el número total de **permutaciones con repetición** de esos m elementos es:

$$P_m^{k_1,k_2,\ldots,k_r} = \frac{m!}{k_1!.k_2!.\ldots.k_r!}.$$

Ejemplo 2.9. En una biblioteca tienen 5 libros de "Química I", 3 libros de "Biología general" y 6 libros de "Álgebra I". Se tienen que colocar los 14 libros en un solo estante. ¿De cuántas formas distintas se podrían ordenar? Tenemos 14 libros para ponerlos en 14 lugares disponibles, así que debe ser una permutación. Como tenemos 5 libros iguales de "Química I", 3 libros iguales de "Biología general" y 6 libros iguales de "Álgebra I", es permutaciones con repetición. El número total de ordenaciones posibles es:

$$P_{14}^{5,3,6} = \frac{15!}{5!.3!.6!} = 2.522.520.$$

2.3. Variaciones

Ejemplo 2.10. Se desea hacer una apuesta en una carrera de caballos seleccionando los tres primeros puestos. Si en la carrera participan 9 caballos ¿de cuántas formas se pueden elegir los tres primeros caballos? Tenemos que elegir una terna ordenada de los nueve caballos diciendo cuál llega primero, cuál llega segundo y cuál llega tercero. Tenemos que completar ____ ____ ____ con los nueve caballos que compiten. Para el primer lugar tenemos nueve posibilidades (podemos elegir cualquiera de los 9 caballos que corren) $\underbrace{\quad}_{9}$ ____ ____. Para el segundo puesto tenemos 8 posibilidades (los ocho caballos restantes) $\underbrace{\quad}_{9}$ $\underbrace{\quad}_{8}$ ____. Y finalmente para el tercer puesto tenemos 7 posibilidades (los 7 caballos que quedan después de haber elegido uno para el primer lugar y otro para el segundo puesto) $\underbrace{\quad}_{9}$ $\underbrace{\quad}_{8}$ $\underbrace{\quad}_{7}$. Resumiendo, para el primer lugar tenemos 9 posibles elecciones, para cada una de estas

nueve elecciones tenemos 8 posibilidades para elegir el segundo puesto, y para cada una de las elecciones del primer y segundo lugar tenemos 7 posibilidades para el tercer lugar. Por lo tanto, hay 9.8.7=504 formas de poder elegir los tres primeros puestos.

La solución al problema anterior es un caso particular de algo más general que se define de la siguiente forma.

Definición 2.11

Dados m elementos distintos, una **variación de m elementos de orden n** ($n \leq m$) es una selección ordenada formada por n de esos m elementos.

En otras palabras, una variación de orden n de m elementos es tomar de forma ordenada n elementos de los m que tenemos a disposición. Por ejemplo, supongamos que tenemos un saco con $m = 10$ bolas identificadas con las letras $a, b, \ldots, j$. Una variación de orden $n = 3$ de esas $m = 10$ bolas es tomar de la bolsa tres bolas de forma ordenada; es decir, metemos la mano y sacamos una bola, que resulta ser la bola c. Volvemos a meter la mano en el saco y sacamos una segunda bola, que por ejemplo resulta ser la h. Y por último volvemos a sacar una bola del saco y resulta ser la b. Entonces, la variación resultante es chb. Observe que el orden en la variación chb importa. No es lo mismo que la variación hbc, que significa que primero salio la bola h, segundo la bola b y tercero la bola c.

Proposición 2.12

Denotamos por V_m^n el número total de variaciones de orden n de m objetos. Entonces, tenemos que el número V_m^n es dado por la fórmula:

$$V_m^n = \frac{m!}{(m-n)!}.$$

Observación 2.13. Se puede dar una prueba que la fórmula $\frac{m!}{(m-n)!}$ da el número total de variaciones de orden n de m elementos. Ver por ejemplo [1].

Ejemplo 2.14. ¿Cuántas claves de 4 dígitos distintos se pueden formar utilizando los números del 1 al 9? Notamos que tenemos que elegir de forma ordenada 4 números distintos de los 9 números disponibles. Entonces, necesitamos saber el número de variaciones de orden 4 de 9 elementos: $V_9^4 = \frac{9!}{(9-4)!} = 9.8.7.6 = 3024$.

Ejemplo 2.15. Supongamos que tenemos a disposición las diez primeras letras del alfabeto $a, b, c, d, e, f, g, h, i, j$. Vamos a referirnos a "palabras" a concatenaciones de letras (con o sin significado). Por ejemplo, $adch$ es para nosotros una palabra. ¿Cuántas palabras de 5 letras podemos formar con las 10 letras $a, b, c, d, e, f, g, h, i, j$ sin repetir ninguna? Observe que en una palabra el orden en que aparecen la letras importa: las palabras abc y bca son distintas. Entonces, para responder a la pregunta debemos saber el número total de variaciones de 10 letras tomadas de a 5. Por lo tanto, podemos formar $V_{10}^5 = \frac{10!}{(10-5)!} = 10.9.8.7.6 = 30240$ palabras distintas sin repetir letras.

Ejemplo 2.16. Un candidato a gobernador de La Pampa está en campaña electoral y tiene sólo tiempo para visitar 4 de las 10 ciudades con más habitantes de La Pampa. ¿Cuántos itinerarios distintos puede hacer?

$$V_{10}^4 = \frac{10!}{(10-4)!} = 5040.$$

¿Cuántos itinerarios puede formar si decide que tiene que pasar por Santa Rosa? Podemos pensar en las cuatros posibilidades:

- Visita Santa Rosa en primer lugar: entonces tiene que elegir de forma ordenada 3 ciudades de las 9 restantes: V_9^3.
- Visita Santa Rosa en segundo lugar: entonces tiene que elegir de forma ordenada 3 ciudades (la primera en visitar, la tercera y la cuarta a visitar) de las 9 restantes: V_9^3.
- Visita Santa Rosa en tercer lugar: entonces tiene que elegir de forma ordenada 3 ciudades (la primera en visitar, la segunda y la cuarta a visitar) de las 9 restantes: V_9^3.
- Visita Santa Rosa en curto lugar: entonces tiene que elegir de forma ordenada 3 ciudades (la primera en visitar, la segunda y la tercera a visitar) de las 9 restantes: V_9^3.

Por lo tanto, el número de itinerarios posibles si quiere visitar Santa Rosa es: $V_9^3 + V_9^3 + V_9^3 + V_9^3 = 4.V_9^3 = 4.\frac{9!}{6!} = 2016$.

El ejemplo anterior ilustra el siguiente principio:

Principio de adición: *Si los eventos a ser contados están separados en casos disjuntos, el número total de eventos es la suma de los números de los distintos casos.*

Ejemplo 2.17. En un Club Social y Deportivo se debe formar una comisión integrada por un Presidente, un Vicepresidente y un Bocal. Para esos puestos se presentaron 10 socios. Entre ellos se encuentran Alejandro y Verónica que están enojados entre sí y no desean pertenecer de forma conjunta a la misma comisión. ¿Cuántas comisiones distintas se podrían formar de tal forma que Alejandro y Verónica no estén ambos en la misma comisión? Para determinar el número total de comisiones posibles, con la condición que Alejandro y Verónica no estén juntos, vamos a considerar tres casos:

Caso 1: En la comisión está Alejandro y no Verónica. En este caso a su vez vamos a considerar tres casos: (1) Alejandro está como presidente; (2) Alejandro está como Vicepresidente; (3) Alejandro está como Bocal. Observemos primero que estos tres casos son disjuntos, porque en una elección, Alejandro no puede estar, por ejemplo, como Presidente y Bocal al mismo tiempo. Ahora, en cualquiera de los tres casos Alejandro va a ocupar un lugar en la comisión (ya sea como Presidente, Vicepresidente o como Bocal) y quedan por seleccionar los otros dos lugares con los socios restante. Teniendo en cuenta que Verónica no va estar en la comisión (porque ya está

Alejandro) quedarían 8 posibles candidatos. Entonces el número de posibles comisiones en la que este Alejandro y no Verónica es: V_8^2 (Alejandro como Presidente) $+$ V_8^2 (Alejandro como Vicepresidente) $+$ V_8^2 (Alejandro como Bocal). Esto es, $3.V_8^2$.

Caso 2: En la comisión está Verónica y no Alejandro. Es análogo al caso anterior. Entonces, el número de comisiones posibles en la que esté Verónica y no Alejandro es $3.V_8^2$.

Caso 3: En la comisión no está Alejandro ni Verónica. En este caso tenemos que seleccionar 3 socios de los 8 candidatos (dejamos afuera a Alejandro y Verónica). Entonces, el número de comisiones en la que no participen Alejandro ni Verónica es V_8^3.

Por lo tanto, como los tres casos anteriores son disjuntos, tenemos que el número total de comisiones posibles en la que no estén juntos Alejandro y Verónica es: $3.V_8^2 + 3.V_8^2 + V_8^3$.

Problema 2.18

¿Cuántas banderas de tres colores en franjas horizontales se pueden confeccionar si se dispone de 8 colores entre los que se encuentran el rojo y azul, pero ambos no pueden estar en una misma bandera?

2.4. Variaciones con repetición

Definición 2.19

Una **variación con repetición** de orden n de m elementos es una sucesión ordenada formada por n elementos (no necesariamente distintos) de los m posibles.

Una variación con repetición de m objetos tomados de a n (de orden n) es una selección de n objetos (no necesariamente distintos) de los m objetos disponibles en forma ordenada. Es decir, si tenemos las letras a, b, c, d, e, entonces algunas variaciones con repetición de orden 3 de esas 5 letras son: $abc, aab, aba, baa, cbd, bcd, eee$, etc. ¿Cuántas son en total?

Ejemplo 2.20. ¿Cuántas contraseñas de tres dígitos se pueden formar usando los números 1,2,...,9 si no hay ninguna restricción? Tenemos que completar ____ ____ ____ con los nueve números disponibles. Para el primer lugar podemos elegir cualquiera de los nueve números disponibles. Para el segundo lugar, como no tenemos restricción alguna, podemos elegir cualquiera de los nueve números disponibles. Y por último para el tercer lugar, nuevamente como no tenemos restricción sobre la elección de los números, podemos elegir cualquiera de los nueve números disponibles. Entonces, para el primer lugar tenemos 9 posibles elecciones $\underbrace{\quad}_{9}$ ____ ____, para cada una de estas nueve elecciones tenemos 9 posibilidades para elegir el segundo puesto $\underbrace{\quad}_{9}$ $\underbrace{\quad}_{9}$ ____, y para cada una de las elecciones del primer y segundo lugar tenemos 9 posibilidades para el tercer lugar $\underbrace{\quad}_{9}$ $\underbrace{\quad}_{9}$ $\underbrace{\quad}_{9}$. Por lo tanto, hay $9.9.9 = 9^3 = 729$ contraseñas distintas.

Proposición 2.21

Denotamos por $V_{m,r}^n$ el número total de las variaciones con repetición de m elementos de orden n. Entonces,

$$V_{m,r}^n = m^n.$$

Ejemplo 2.22. ¿Cuántas patentes de automóviles de siete símbolos puede haber si cada patente debe estar formada por dos letras, tres dígitos y dos letras, en ese orden? Tanto las letras como los números pueden repetirse. Como hay 27 letras en el alfabeto y 10 dígitos, tenemos que pueden haber

$$V_{27,r}^2.V_{10,r}^3.V_{27,r}^2 = 27^2.10^3.27^2 \text{ pantentes distintas.}$$

2.5. Combinaciones

Ejemplo 2.23. Un entrenador de fútbol tiene a disposición cinco defensores centrales y tiene que elegir a dos para que formen la defensa. No importa el orden en que juegan en la defensa los dos jugadores elegidos. ¿Cuántas alineaciones posibles tiene para la defensa? Supongamos que llamamos a los cinco defensores por: a, b, c, d y e. Entonces las posibles defensas son:

$$\{a,b\},\ \{a,c\},\ \{a,d\},\ \{a,e\},\ \{b,c\},\ \{b,d\},\ \{b,e\},\ \{c,d\},\ \{c,e\},\ \{d,e\}.$$

Note que aquí $\{a,b\}$ significa que juegan en la defensa los jugadores a y b. Entonces, el entrenador tiene 10 posibles alineaciones para formar la defensa. ■

Definición 2.24

Dados m objetos, una **combinación** de orden n ($n \leq m$) de esos m objetos es cualquier elección de n objetos de los m disponibles.

Podemos reformular la definición anterior como:

Dado un conjunto A con m elementos, se llama **combinación** de orden n de esos m elementos a todo subconjunto de A con n elementos.

Observación 2.25. Es importante notar que en una combinación no es importante el orden en que se elijan los elementos. También, observe que en una combinación no se permiten repeticiones.

Proposición 2.26

Denotamos por C_m^n al número total de combinaciones de orden n de m elementos ($n \leq m$). Entonces

$$C_m^n = \frac{m!}{n!(m-n)!}.$$

Observación 2.27. Observemos que C_m^n es el número total de subconjuntos con n elementos de un conjunto con m elementos ($n \leq m$). En otras palabras, si A es un conjunto con m elementos, entonces C_m^n es la cantidad total de subconjuntos con n elementos de A que pueden formarse.

Ejemplo 2.28. En un curso de Álgebra hay 15 estudiantes, de los cuales 9 son chicas y 6 son chicos. El profesor les pide que elijan entre ellos a 5 estudiantes para que participen de una charla informativa en un colegio secundario. ¿Cuántas comisiones posibles se podrían formar? Se deben elegir 5 estudiantes de 15, y no importa el orden en que se elijan. Entonces, la cantidad total de posibles elecciones es:

$$C_{15}^5 = \frac{15!}{5!(15-5)!} = \frac{15.14.13.12.11.10!}{5!.10!} = 3003.$$

Suponga que ahora el Profesor pide que de los 5 estudiantes tres sean chicas y dos sean chicos. ¿Cuántas comisiones posibles se pueden formar? Tenemos que elegir 3 chicas de las 9 que hay en el curso, y el número total de posibles elecciones es C_9^3. Ahora para cada una de estas elecciones de las chicas tenemos que elegir a dos chicos de los 6 disponibles. El número total de elecciones de 2 chicos de 6 es: C_6^2. Resumiendo, para cada una de la C_9^3 elecciones de chicas tenemos C_6^2 elecciones posibles para los chicos. Entonces, el número total de posibles comisiones formadas por 3 chicas y 2 chicos es:

$$C_9^3.C_6^2 = \frac{9!}{3!.(9-3)!} \cdot \frac{6!}{2!(6-2)!} = 1260.$$

Ejemplo 2.29. Un Circo tiene 7 payasos, 5 malabaristas y 4 magos. Si tienen que salir a escena tres artista del mismo rubro, ¿cuántas son las posibles elecciones? Tenemos tres casos posibles: (1) salen 3 payasos a escena; (2) salen 3 malabaristas a escena; o (3) salen 3 magos a escena. Observemos que los tres casos son disjuntos. Si salen todos payasos, entonces el número de grupos posibles con 3 payasos que se pueden formar es C_7^3. Si salen todos malabarista, entonces el número de grupos posibles con 3 malabaristas que se pueden formar es C_5^3. Finalmente, si sales todos magos, entonces el número de grupos posibles con 3 magos que se pueden formar es C_4^3. Por lo tanto, el número total de las posibles elecciones para que salgan 3 artistas del mismo rubro es $C_7^3 + C_5^3 + C_4^3$.

Problema 2.30

Considere dos rectas paralelas distintas. Si sobre una recta se marcan 5 puntos y sobre la otra se marcan 7 puntos, ¿cuántos triángulos se pueden formar utilizando los puntos de ambas rectas?

2.6. Combinaciones con repetición

Ejemplo 2.31. Un Profesor de Álgebra desea regalarles, por el día del estudiante, a cada uno de sus 20 estudiantes una caja con cinco bombones. En el negocio donde va a comprar los bombones le ofrecen como oferta armar cajas de cinco bombones eligiendo entre sólo tres

sabores: Menta (M), Frutilla (F) y Licor (L). Así, el Profesor tiene que elegir de qué sabores, entre esos tres, serán los 5 bombones que irán en la caja para cada estudiante. Además, les prometió que a cada estudiante le tocaría una caja distinta. ¿Es posible que a cada estudiante le toque una caja distinta? Tratemos de armar todas las cajas posibles. La combinación M M M F L significa que la caja está formada por 3 bombones de menta, un bombón de frutilla y un bombón de licor. Observe que el orden en la caja no importa, la caja con la combinación M F L M M es la misma que la caja M M M F L. Entonces, tratemos de formar todas las cajas posibles:

M	M	M	M	M
M	M	M	M	F
M	M	M	F	F
M	M	F	F	F
M	F	F	F	F

F	F	F	F	F
F	F	F	F	L
F	F	F	L	L
F	F	L	L	L
F	L	L	L	L

L	L	L	L	L
L	L	L	L	M
L	L	L	M	M
L	L	M	M	M
L	M	M	M	M

M	F	L	M	M
M	F	L	M	F
M	F	L	M	L
M	F	L	F	F
M	F	L	F	L
M	F	L	L	L

Por lo tanto, se pueden armar en total 21 cajas distintas con cinco bombones de tres sabores. En conclusión, es posible que el Profesor le regale a cada estudiante una caja distinta, y le sobra una para él.

Observemos que en el ejemplo anterior hablamos de combinaciones porque elegimos 5 elementos (bombones) sin importar el orden en que fueron elegidos y en el que se permitía la repetición. Este tipo de problemas se pueden resolver con el siguiente concepto.

Proposición 2.32

Denotaremos por $C^n_{m,r}$ al número total de combinaciones con repetición de m objetos tomados de a n. Entonces, se tiene que el número $C^n_{m,r}$ de combinaciones con repetición de m objetos tomados de a n es dado por:

$$C^n_{m,r} = C^n_{m+n-1}.$$

Observación 2.33. A diferencia de los conceptos estudiados en las secciones anteriores, en $C^n_{m,r}$ no necesariamente n debe ser menor o igual a m. Se puede calcular por ejemplo $C^5_{2,r} = C^5_6 = 6$. En el Ejemplo 2.31 tuvimos que armar cajas de 5 bombones eligiendo entre bombones de 3 sabores. Es decir, tenemos $m = 3$ objetos tomados de a $n = 5$. Entonces las combinaciones con repetición son $C^5_{3,r} = C^5_7 = 21$.

Ejemplo 2.34. ¿Cuántos grupos de 3 letras se pueden formar con las letras a, b, c y d si se pueden repetir letras? Por ejemplo, un grupo podría ser abc, otro podría ser aab o también

ddd. Observemos que el orden no importa, por ejemplo, el grupo *aab* es el mismo que *aba*. Cómo estamos hablando de elegir tres elementos de cuatro sin importar el orden en que se eligen y podemos repetir, debemos utilizar combinaciones con repetición. Entonces, la cantidad total de grupos de 3 letras que se pueden formar utilizando las 4 letras es: $C^3_{4,r} = C^3_6 = 20$.

2.7. Números combinatorios

Definición 2.35

Los **números combinatorios** son números de la forma

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

con $n, k \in \mathbb{Z}$ y $0 \leq k \leq n$.

Observación 2.36. Observe que

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = C^k_n.$$

Ejemplo 2.37. Para cada $n \in \mathbb{N}$, se tiene que

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1.n!} = 1 \qquad \text{y} \qquad \binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!0!} = 1.$$

También tenemos que

$$\begin{aligned}
\binom{n}{1} &= \frac{n!}{1!(n-1)!} && \text{aplicamos la definición de número combinatorio} \\
&= \frac{n(n-1)!}{(n-1)!} && \text{en el numerador desarrollamos } n! \\
&= n && \text{simplificamos } (n-1)!
\end{aligned}$$

y

$$\begin{aligned}
\binom{n}{n-1} &= \frac{n!}{(n-1)!(n-(n-1))!} && \text{aplicamos la definición de número combinatorio} \\
&= \frac{n(n-1)!}{(n-1)!1!} && n-(n-1) = 1 \text{ y en el numerador desarrollamos } n! \\
&= n && \text{simplificamos } (n-1)!
\end{aligned}$$

Las siguientes dos proposiciones enuncian dos propiedades importantes de los números combinatorios.

Proposición 2.38

Para todos $n, k \in \mathbb{Z}$ con $0 \leq k \leq n$, tenemos que:

$$\binom{n}{k} = \binom{n}{n-k}.$$

Demostración. Aplicamos la definición de número combinatorio:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}. \qquad \blacksquare$$

A los números combinatorios $\binom{n}{k}$ y $\binom{n}{n-k}$ se los llaman **números combinatorios complementarios**.

Proposición 2.39: Propiedad de Stifel

Para todos $n, k \in \mathbb{Z}$ con $1 \leq k \leq n$, tenemos que:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Demostración. Aplicamos la definición de número combinatorio y operamos algebraicamente:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k.(k-1)!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)(n-k-1)!} + \frac{(n-1)!}{k.(k-1)!(n-1-k)!} \\
&= \frac{(n-1)!.k + (n-1)!.(n-k)}{k(k-1)!.(n-k).(n-1-k)!} \\
&= \frac{(n-1)!.(k+(n-k))}{k!.(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}. \qquad \blacksquare
\end{aligned}$$

La siguiente ordenación triangular de los números combinatorios es conocida con el nombre de **triángulo de Pascal (o Tartaglia)**

$$\begin{array}{lccccccccccccc}
n=0: & & & & & & \binom{0}{0} & & & & & & & \\
n=1: & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & \\
n=2: & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & \\
n=3: & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & \\
n=4: & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & \\
n=5: & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & \\
n=6: & & \binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} \\
n=7: & \binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7}
\end{array}$$

Ahora, si reemplazamos cada uno de los números combinatorios por el resultado que da, obtenemos la siguiente ordenación triangular.

$$
\begin{array}{lccccccccccccc}
n=0: & & & & & & & 1 & & & & & & \\
n=1: & & & & & & 1 & & 1 & & & & & \\
n=2: & & & & & 1 & & 2 & & 1 & & & & \\
n=3: & & & & 1 & & 3 & & 3 & & 1 & & & \\
n=4: & & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
n=5: & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
n=6: & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
n=7: & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

Problema 2.40

Probar que para todo $n, k \in \mathbb{Z}$ con $1 \leq k \leq n$ se cumple que

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

2.8. El binomio de Newton

Ahora vamos a utilizar los números combinatorios para hallar una expresión general para las potencias enteras positivas de binomios. Es decir, queremos encontrar una fórmula general que nos permita siempre poder desarrollar de forma algorítmica la potencia $(a+b)^n$, con $n \in \mathbb{N}$. Calculemos primero las primeras 5 potencias y veamos que patrón podemos hallar.

$$
\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= a^2+2ab+b^2 \\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4 \\
(a+b)^5 &= a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5.
\end{aligned}
$$

Observemos que los coeficientes en los términos a^ib^j cuando $n=2$ son $1\ \ 2\ \ 1$ y estos corresponden a los valores en la fila $n=2$ del triángulo de Pascal. Así que los podríamos reemplazar por ellos: $\binom{2}{0}\ \ \binom{2}{1}\ \ \binom{2}{2}$. De igual forma, si observamos los coeficientes de los términos a^ib^j en la potencia $(a+b)^3$ tenemos que ellos son $1\ \ 3\ \ 3\ \ 1$, y estos corresponden a los números combinatorios $\binom{3}{0}\ \ \binom{3}{1}\ \ \binom{3}{2}\ \ \binom{3}{3}$. Note que los coeficientes de los términos a^ib^j de las potencias para $n=4$ y $n=5$ corresponden, respectivamente, a los números combinatorios de las filas

de $n = 4$ y $n = 5$ en el triángulo de Pascal. Entonces, reemplazando obtenemos lo siguiente:

$$(a+b)^1 = \binom{1}{0}a + \binom{1}{1}b$$

$$(a+b)^2 = \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2$$

$$(a+b)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3$$

$$(a+b)^4 = \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4$$

$$(a+b)^5 = \binom{5}{0}a^5 + \binom{5}{1}a^4b + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}ab^4 + \binom{5}{5}b^5.$$

Por lo tanto, podemos hacer la siguiente conjetura:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

para todo $n \in \mathbb{N}$.

Si reemplazamos n por 1, 2, 3, 4 ó 5 sabemos por lo anterior que se cumple. Pero ¿valdrá para todo número natural n? La respuesta es sí. Lo probamos a continuación.

Teorema 2.41: El binomio de Newton

Sean $a, b \in \mathbb{R}$. Para todo $n \in \mathbb{N}$ se tiene que

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k. \tag{2.1}$$

Demostración. Vamos a probar (2.1) por inducción sobre $n \in \mathbb{N}$. Para $n = 1$ tenemos que

$$(a+b)^1 = a+b \qquad \text{y} \qquad \sum_{k=0}^{1} \binom{1}{k} a^{1-k}b^k = a+b.$$

Entonces, se cumple para $n = 1$. Ahora, sea $n > 1$ y supongamos que

$$(a+b)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} a^{(n-1)-k}b^k. \tag{H.I.}$$

Ahora,

$$\begin{aligned}(a+b)^n = (a+b)(a+b)^{n-1} &\overset{(H.I.)}{=} (a+b).\sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^k \\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^{k+1} \\ &= \binom{n-1}{0}a^n + \sum_{k=1}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=0}^{n-2}\binom{n-1}{k}a^{n-1-k}b^{k+1} + \binom{n-1}{n-1}b^n.\end{aligned}$$

Vamos a realizar el siguiente cambio de variable para la segunda sumatoria: sea $t = k+1$. Entonces $k = t-1$. Como $0 \leq k \leq n-2$, entonces $1 \leq t \leq n-1$. Ahora reemplazamos:

$$\sum_{k=0}^{n-2} \binom{n-1}{k} a^{n-1-k} b^{k+1} = \sum_{t=1}^{n-1} \binom{n-1}{t-1} a^{n-t} b^{t}. \tag{2.2}$$

Luego, por conveniencia, podemos cambiar la variable t en la sumatoria de la derecha en (2.2) por k. Nos queda

$$\sum_{k=0}^{n-2} \binom{n-1}{k} a^{n-1-k} b^{k+1} = \sum_{k=1}^{n-1} \binom{n-1}{k-1} a^{n-k} b^{k}. \tag{2.3}$$

Entonces, obtenemos que

$$\begin{aligned}
(a+b)^n &= \binom{n}{0} a^n + \sum_{k=1}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=1}^{n-1} \binom{n-1}{n-k} a^{n-k} b^k + \binom{n}{n} b^n \\
&= \binom{n}{0} a^n + \sum_{k=1}^{n-1} \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] a^{n-k} b^k + \binom{n}{n} b^n \\
&= \binom{n}{0} a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k + \binom{n}{n} b^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.
\end{aligned}$$

Por lo tanto, por el Principio de Inducción se cumple (2.1) para todo $n \in \mathbb{N}$. ■

Ejemplo 2.42. Utilicemos el binomio de Newton para hallar el desarrollo del polinomio $(3x - 2x^3)^4$.

$$\begin{aligned}
(3x-2x^3)^4 &= \sum_{k=0}^{4} \binom{4}{k} (3x)^{4-k} (-2x^3)^k \\
&= \binom{4}{0} (3x)^{4-0} (-2x^3)^0 + \binom{4}{1} (3x)^{4-1} (-2x^3)^1 + \binom{4}{2} (3x)^{4-2} (-2x^3)^2 + \\
&\qquad + \binom{4}{3} (3x)^{4-3} (-2x^3)^3 + \binom{4}{4} (3x)^{4-4} (-2x^3)^4 \\
&= 1.(3x)^4.1 + 4.(3x)^3(-2x^3) + 6.(3x)^2(-2x^3)^2 + 4.(3x)(-2x^3)^3 + 1.1.(-2x^3)^4 \\
&= 81x^4 - 216x^6 + 216x^8 - 96x^{10} + 16x^{12}
\end{aligned}$$

Ejemplo 2.43. Probemos que $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$. Aplicando el binomio de Newton obtenemos que:

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n}.$$

Ejemplo 2.44. Sea A un conjunto con n elementos. ¿Cuántos subconjuntos de A hay? Es decir, si $\mathcal{P}(A)$ es el conjunto de partes de A, ¿cuántos elementos tiene $\mathcal{P}(A)$? Recordemos que $\mathcal{P}(A) = \{B : B \subseteq A\}$. Entonces, $\mathcal{P}(A)$ está formado por: el conjunto vacío + todos

los subconjuntos formados por un solo elemento + todos los subconjuntos formados por dos elementos + ... + todos los subconjuntos formados por $n-1$ elementos + el conjunto A. Ahora, recordemos que $\binom{n}{k} = C_n^k$, así que $\binom{n}{k}$ es el número total de subconjuntos de A con k elementos (véase Observación 2.27). Entonces la cantidad de elementos de $\mathcal{P}(A)$ es:

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + 1 = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Ejemplo 2.45. Vamos a probar que $\sum_{k=0}^{n} \binom{n}{k} 2^{2k} = 5^n$. Aplicando el binomio de Newton obtenemos que:

$$\sum_{k=0}^{n} \binom{n}{k} 2^{2k} = \sum_{k=0}^{n} \binom{n}{k} 4^k = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 4^k = (1+4)^n = 5^n.$$

Problema 2.46

Determinar el valor de la siguiente sumatoria

$$\sum_{k=0}^{n} (-1)^n \binom{n}{k}.$$

Ejercicios propuestos

Ejercicio 2.1. Supongamos que Juan tiene 4 libros de novelas policiales, 3 libros de autoayuda y 5 libros de poesía. En su biblioteca le quedan disponibles sólo tres estantes para ubicar los 12 libros. Desea ubicar los libros por género en cada estante (es decir, en un estante poner todos los de poesía, en otro estante todos los de policiales y en otro todos los de autoayuda). ¿De cuántas formas distintas puede colocar los libros?

Ejercicio 2.2. Sea A un conjunto con n elementos. Determinar la cantidad de subconjuntos de A con un número par de elementos.

Ejercicio 2.3. Probar que para todo $n \in \mathbb{N}$,

$$\binom{2n}{n} < 4^n.$$

(*Consejo: Utilizar el Binomio de Newton*).

Ejercicio 2.4. Probar que

$$\binom{2n+2}{n+1} = 4\left(1 - \frac{1}{2n+2}\right)\binom{2n}{n}.$$

Capítulo 3

Divisibilidad en $\mathbb{Z}$

Para comprender la Matemática moderna, nada mejor que estudiar la más antigua de las ciencias, a saber, la Aritmética.

—-Norberto A. Fava

Este capítulo está dedicado al estudio de los números enteros. Uno de los conceptos fundamentales para el estudio de los números enteros es el Teorema de la División, el cual formaliza lo que sabemos acerca de dividir un número por otro. Otros conceptos fundamentales en la teoría de la Aritmética son el de número primo y el Teorema Fundamental de la Aritmética.

3.1. El conjunto de los números enteros

En esta sección hacemos un repaso muy breve sobre las propiedades de las operaciones (suma y producto) definidas sobre el conjunto de los números enteros.

El conjunto de los **números enteros** es

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Al igual que en el conjunto de los números naturales, en $\mathbb{Z}$ hay dos operaciones binarias: la **suma** $+$ y el **producto** $\cdot$. Estas operaciones tienen las siguientes propiedades que usaremos a lo largo del libro, muchas veces sin hacer mención explicita de ellas, por lo cual el lector debe tenerlas resente en todo momento. Para todos $a, b, c \in \mathbb{Z}$ se cumplen:

Propiedades de las operaciones

- **Asociativa:** $a + (b + c) = (a + b) + c \quad$ y $\quad a.(b.c) = (a.b).c$.
- **Conmutativa:** $a + b = b + a \quad$ y $\quad a.b = b.a$.
- **Elemento neutro para la suma:** Existe $0 \in \mathbb{Z}$ tal que $a + 0 = 0$.
- **Elemento neutro para el producto:** Existe $1 \in \mathbb{Z}$ tal que $a.1 = a$.
- **Elemento opuesto**: Para cada $a \in \mathbb{Z}$, existe $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.
- **Distributiva:** $a.(b + c) = a.b + a.c$.

Más propiedades útiles

(1) Si $a.b = 0$, entonces $a = 0$ ó $b = 0$.

(2) Si $a.b = a.c$ y $a \neq 0$, entonces $b = c$.

(3) Si $a.b = 1$, entonces $a = b = 1$ ó $a = b = -1$.

(4) $(-1).a = -a$.

(5) $-(-a) = a$.

(6) $(-a).b = a.(-b) = -(a.b)$.

(7) $-(a + b) = -a + (-b)$.

Observación 3.1. Usualmente escribiremos ab en lugar de $a.b$. También, escribiremos $a - b$ en lugar de $a + (-b)$, como es costumbre.

Observación 3.2. En la propiedad (2), para obtener la conclusión que $b = c$ del hecho $ab = ac$ es imprescindible que $a \neq 0$. Pues, se tiene $0.3 = 0.5$, pero $3 \neq 5$.

3.2. La relación divide

Definición 3.3

Sean $a, b \in \mathbb{Z}$. Diremos que a **divide** a b, y lo denotaremos por $a \mid b$, si existe un número entero k tal que $b = a.k$. En otras palabras,

$$a \mid b \iff \exists k \in \mathbb{Z} \text{ tal que } b = ak.$$

Si a divide a b diremos también que b es **múltiplo** de a. Entonces,

$$b \text{ es múltiplo de } a \iff \exists k \in \mathbb{Z} \text{ tal que } b = ak.$$

Ejemplo 3.4.

(1) 3 divide a 18, porque existe $6 \in \mathbb{Z}$ tal que $18 = 3.6$.

(2) $5 \mid -75$, porque $-75 = 5.(-25)$.

(3) Como $5.3 = 15$, tenemos que $5 \mid 15$.

(4) 108 es múltiplo de 3, porque 108=3.36.

Proposición 3.5

Para todos $a, b, c \in \mathbb{Z}$ se cumplen las siguientes propiedades.

(1) $a \mid a$.

(2) Si $a \mid b$, entonces $-a \mid b$, $a \mid -b$ y $-a \mid -b$.

(3) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(4) Si $a \mid b$ y $a \mid c$, entonces $a \mid (bx + cy)$ para todos $x, y \in \mathbb{Z}$.

(5) Si $a \mid b$ y $b \mid a$, entonces $|a| = |b|$.

Demostración. (1) Por la propiedad del elemento neutro para el producto, tenemos que $a = a.1$. Entonces, por definición de la relación divide $a \mid a$.

(2) Supongamos que $a \mid b$. Entonces, existe $k \in \mathbb{Z}$ tal que $b = ak$. Observemos que $ak = (-a)(-k)$. Luego, $b = (-a)(-k)$. Entonces, como $-k \in \mathbb{Z}$, por la definición de relación divide tenemos que $-a \mid b$. Ahora, si multiplicamos a ambos miembros por -1 a la igualdad $b = ak$, tenemos que $-b = -(ak) = a(-k)$. Entonces $a \mid -b$. También, $-b = -(ak) = (-a)k$, lo cual implica que $-a \mid -b$.

(3) Supongamos que $a \mid b$ y $b \mid c$. Entonces, existen $k, q \in \mathbb{Z}$ tales que $b = ak$ y $c = bq$. Reemplazando obtenemos que $c = (ak)q = a(kq)$. Como $kq \in \mathbb{Z}$, concluimos que $a \mid c$.

(4) Supongamos que $a \mid b$ y $a \mid c$. Sean $x, y \in \mathbb{Z}$. Tenemos que

$$a \mid b \implies \exists k \in \mathbb{Z} \text{ tal que } b = ak \implies bx = (ak)x = a(kx) \tag{3.1}$$

$$a \mid c \implies \exists q \in \mathbb{Z} \text{ tal que } c = aq \implies cy = (aq)y = a(qy). \tag{3.2}$$

Ahora sumamos miembro a miembro las igualdades (3.1) y (3.2)

$$bx + cy = a(kx) + a(qy) = a(kx + qy).$$

Entonces, como $kx + qy \in \mathbb{Z}$ obtenemos que $a \mid (bx + cy)$.

(5) Supongamos que $a \mid b$ y $b \mid a$. Entonces, existen $k, q \in \mathbb{Z}$ tales que $b = ak$ y $a = bq$. Reemplazamos y obtenemos lo siguiente

$$b = (bq).k \implies b = b(qk) \implies 1 = qk \implies q = k = 1 \text{ ó } q = k = -1.$$

Entonces tenemos que $b = a$ o $b = -a$. Por lo tanto, $|a| = |b|$. ■

Observación 3.6. Usando la relación divide podemos definir formalmente número par. Diremos que un entero a es **par** si 2 divide a a. Es decir,

$$a \text{ es par} \iff 2 \mid a \iff a = 2k \text{ para algún } k \in \mathbb{Z}.$$

Un entero a que no es par, es llamado **impar**.

Definición 3.7: Relación de congruencia

Sea $n \in \mathbb{N}$. Dados $a, b \in \mathbb{Z}$, se dice que a **es congruente** a b **módulo** n si $n \mid (a-b)$. Escribiremos $a \equiv_n b$ para decir que a es congruente a b módulo n.

Utilizando la definición de la relación divide tenemos que

$$a \equiv_n b \iff \exists k \in \mathbb{Z} \text{ tal que } a - b = n.k. \tag{3.3}$$

Ejemplo 3.8.

1. Sea $n = 3$. Entonces $5 \equiv_3 2$, porque $3 \mid (5-2)$.
2. Sea $n = 5$. Entonces $-1 \equiv_5 4$, porque $5 \mid (-1-4)$.
3. Tenemos que $-2 \equiv_7 33$, porque $-2 - 33 = -35 = 7(-5)$.

Proposición 3.9

Para cada $n \in \mathbb{N}$, la relación de congruencia $\equiv_n$ módulo n es una relación de equivalencia sobre $\mathbb{Z}$.

Demostración. Recordemos que una relación binaria sobre un conjunto A es de equivalencia si es reflexiva, simétrica y transitiva.
• Reflexiva: Sea $a \in \mathbb{Z}$. Como $a - a = 0 = n.0$, entonces por definición de congruencia, $a \equiv_n a$. Hemos probado que $a \equiv_n a$, $\forall a \in \mathbb{Z}$. Por lo tanto, $\equiv_n$ es reflexiva.
• Simétrica: Sean $a, b \in \mathbb{Z}$ y supongamos que $a \equiv_n b$. Entonces, existe $k \in \mathbb{Z}$ tal que $a - b = nk$. Multiplicando a ambos lados de la igualdad por -1 obtenemos que $b - a = -(nk) = n(-k)$ y $-k \in \mathbb{Z}$. Entonces, $b \equiv_n a$. Por lo tanto, $\equiv_n$ es simétrica.
• Transitiva: Sean $a, b, c \in \mathbb{Z}$. Supongamos que $a \equiv_n b$ y $b \equiv_n c$. Entonces,

$$\begin{aligned} a \equiv_n b &\implies \exists k \in \mathbb{Z} \text{ tal que } a - b = nk \\ b \equiv_n c &\implies \exists q \in \mathbb{Z} \text{ tal que } b - c = nq. \end{aligned}$$

Luego, si sumamos miembro a miembro las últimas dos igualdades obtenemos que

$$\begin{aligned} (a-b) + (b-c) &= nk + nq \\ a - c &= n(k+q). \end{aligned}$$

Como $k + q \in \mathbb{Z}$, obtenemos que $a \equiv_n c$. Por lo tanto, $\equiv_n$ es transitiva.

Por lo tanto, la relación de congruencia $\equiv_n$ módulo n es de equivalencia. ■

Proposición 3.10

Sea $n \in \mathbb{N}$ y sean $a, b, c, d \in \mathbb{Z}$. Entonces:

(1) Si $a \equiv_n b$ y $c \equiv_n d$, entonces $a + c \equiv_n b + d$.

(2) Si $a \equiv_n b$ y $c \equiv_n d$, entonces $ac \equiv_n bd$.

(3) Si $a \equiv_n b$, entonces para todo $m \in \mathbb{N}$, $a^m \equiv_n b^m$.

Demostración. (1) Supongamos que $a \equiv_n b$ y $c \equiv_n d$. Entonces,

$$\begin{aligned} a \equiv_n b &\implies \exists k \in \mathbb{Z} \text{ tal que } a - b = nk \\ c \equiv_n d &\implies \exists q \in \mathbb{Z} \text{ tal que } c - d = nq. \end{aligned}$$

Ahora sumamos miembro a miembro las dos igualdades anteriores:

$$\begin{aligned} (a - b) + (c - d) &= nk + nq \\ (a + c) - (b + d) &= n(k + q). \end{aligned}$$

Entonces, por definición de $\equiv_n$ obtenemos que $a + c \equiv_n b + d$.

(2) Supongamos que $a \equiv_n b$ y $c \equiv_n d$. Entonces,

$$\begin{aligned} a \equiv_n b &\implies \exists k \in \mathbb{Z} \text{ tal que } a - b = nk \implies (a - b)c = (nk)c \implies ac - bc = n(kc) \\ c \equiv_n d &\implies \exists q \in \mathbb{Z} \text{ tal que } c - d = nq \implies b(c - d) = b(nq) \implies bc - bd = n(bq). \end{aligned}$$

Ahora sumamos miembro a miembro las dos últimas igualdades:

$$\begin{aligned} (ac - bc) + (bc - bd) &= n(kc) + n(bq) \\ ac - bd &= n(kc + bq). \end{aligned}$$

Entonces, como $kc + bq \in \mathbb{Z}$, obtenemos que $ac \equiv_n bd$.

(3) Supongamos que $a \equiv_n b$. Vamos a probar por inducción sobre m que $a^m \equiv_n b^m$ para todo $m \in \mathbb{N}$.

- Para $m = 1$. Como $a \equiv_n b$, entonces $a^1 \equiv_n b^1$. Entonces, la afirmación es verdadera para $m = 1$.

- Supongamos que la afirmación se cumple para m. Esto es, supongamos que $a^m \equiv_n b^m$ (H.I.). Debemos probar que $a^{m+1} \equiv_n b^{m+1}$. Tenemos que $a \equiv_n b$ (hipótesis) y $a^m \equiv_n b^m$ (por la H.I.). Entonces por la propiedad (2) anterior, obtenemos que $aa^m \equiv_n bb^m$. Con lo cual, $a^{m+1} \equiv_n b^{m+1}$. Por lo tanto, por el Principio de Inducción podemos afirmar que $a^m \equiv_n b^m$ para todo $m \in \mathbb{N}$.

■

Notemos que la propiedad (2) de la proposición anterior implica que se cumple lo siguiente:

Si $a \equiv_n b$, entonces para todo $c \in \mathbb{Z}$, $ac \equiv_n bc$.

En efecto, si $a \equiv_n b$, entonces aplicando la propiedad (2) a $a \equiv_n b$ y $c \equiv_n c$ (pues, $\equiv_n$ es reflexiva) obtenemos que $ac \equiv_n bc$.

3.3. El Teorema de la División Entera

Teorema 3.11: Teorema de la División Entera

Para todo par de enteros a y b, con $b \neq 0$, existen dos únicos enteros q y r tales que

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|. \tag{3.4}$$

Diremos que q es el **cociente** y r es el **resto** de dividir a por b.

Demostración. Vamos a probar el teorema en dos partes. Primero probaremos la existencia de los dos enteros q y r que verifican las dos condiciones en (3.4), y luego probaremos que esos q y r son únicos.

► *Existencia:*

• Supongamos primero que $b > 0$. Definimos el siguiente conjunto:

$$A = \{x : \ x = a - bq, \ x \geq 0 \text{ y } q \in \mathbb{Z}\}^{1}.$$

Notemos que $a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$. Entonces, $x = a - b(-|a|) \in A$ (tomando $q = -|a|$). Luego, $A \subseteq \mathbb{N} \cup \{0\}$ y es no vacío. Por el Principio de Buena Ordenación (ver el Teorema 1.23) tenemos que A tiene un primer elemento. Llamamos r al primer elemento de A. Como $r \in A$, tenemos que $r = a - bq$ para un $q \in \mathbb{Z}$ y $r \geq 0$. Entonces $a = bq + r$ con $0 \leq r$. Solo nos falta probar que $r < b$. Supongamos, por absurdo, que $r \geq b$. Entonces $0 \leq r - b = a - bq + b = a - b(q + 1)$. Con lo cual $r - b \in A$ y $r - b < r$ (pues, $b > 0$), lo cual es absurdo pues r es el primer elemento de A. Entonces, $r < b$. Por lo tanto, $a = bq + r$ y $0 \leq r < b$.

• Supongamos ahora que $b < 0$. Luego $-b > 0$. Por lo que probamos recién, existen enteros q y r tales que $a = (-b)q + r$ y $0 \leq r < -b$. Entonces $a = b(-q) + r$ y $0 \leq r < |b|$. Resumiendo, hemos probado que existen q y r tales que $a = bq + r$ y $0 \leq r < |b|$.

► *Unicidad:* Supongamos que existen enteros q, q', r, r' tales que

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|$$
$$a = bq' + r' \quad \text{y} \quad 0 \leq r' < |b|.$$

[1] En otras palabras, el conjunto A está formado por todos los $x \geq 0$ que se pueden expresar como $a - bq$ con un $q \in \mathbb{Z}$.

Igualando las identidades anteriores, tenemos que

$$bq + r = bq' + r' \implies (q - q')b = r' - r \implies |q - q'||b| = |r' - r|.$$

Si $q \neq q'$, entonces $|q - q'| > 0$. Entonces $|b| \leq |q - q'||b| = |r' - r| < |b|$,[2] lo cual es absurdo. Por lo tanto, $q = q'$ y también $r = r'$. ■

Notemos que el Teorema de la División Entera nos garantiza que siempre existen el cociente y resto de dividir un entero a por otro entero b, pero no nos dice cómo hallar este cociente y resto. Una de las cosas que nos aporta la unicidad del cociente y resto es que no importa cómo hallemos el q y el r, si ellos verifican que $a = bq + r$ y $0 \leq r < |b|$, entonces q y r son, respectivamente, el cociente y resto de dividir a por b.

Ejemplo 3.12.

(1) El cociente y resto de dividir 43 por 3 son $q = 14$ y $r = 1$, respectivamente. En efecto, $43 = 3.14 + 1$ y $0 \leq 1 < 3$.

(2) Hallemos el cociente y resto de dividir 749 por 21. Aplicamos el algoritmo que aprendimos en la escuela para dividir dos números:

7	4	9	2	1
1	1	9	3	5
	1	4		

Entonces, sabemos que $749 = 21.35 + 14$ y $0 \leq 14 < 21$. Por lo tanto, 35 es el cociente y 14 el resto de dividir 749 por 21.

(3) Hallemos el resto de dividir -549 por 31. Primero hallamos el cociente y resto de dividir 549 por 31: 549=31.17+22. Ahora, si multiplicamos a ambos lados de la igualdad por -1 obtenemos que:

$$\begin{aligned} -549 &= -(31.17 + 22) \\ -549 &= 31.(-17) - 22 \\ -549 &= 31.(-17) - 22 + 31 - 31 \\ -549 &= 31.(-17) - 31 + 9 \\ -549 &= 31.(-18) + 9 \end{aligned}$$

Entonces, como $-549 = 31.(-18) + 9$ y $0 \leq 9 < 31$, tenemos que -18 es el cociente y 9 es el resto de dividir -549 por 31.

Ejemplo 3.13. Determinemos el cociente y resto de dividir 7935 por -32. Primero hallamos el cociente y resto de dividir 7935 por 32: 7935=32.247+31. Ahora,

$$7935 = 32.247 + 31 = (-32).(-247) + 31.$$

Entonces, -247 es el cociente y 31 es el resto de dividir 7935 por -32.

[2]Como $r < |b| \implies r - r' < |b| - r' < |b|$ y como $r' < |b| \implies r' - r < |b| - r < |b|$. Ahora, si $r' < r \implies |r' - r| = -(r' - r) = r - r' < |b|$. Si $r \leq r' \implies |r' - r| = r' - r < |b|$. En todos lo casos se tiene que $|r' - r| < |b|$.

Proposición 3.14

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces, b divide a a si y sólo si el resto de dividir a por b es cero.

Demostración. ($\Rightarrow$) Supongamos que b divide a a. Entonces, por definición de la relación divide, existe $k \in \mathbb{Z}$ tal que $a = bk$. Luego, como $a = bk + 0$ y $0 \leq 0 < |b|$, entonces 0 es el resto de dividir a por b.

($\Leftarrow$) Asumamos que el resto de dividir a por b es 0. Entonces, tenemos que $a = bq + 0 = bq$ con $q \in \mathbb{Z}$. Entonces, por definición de la relación divide, tenemos que $b \mid a$. ■

Recuerde que un entero a es par si 2 lo divide ($2 \mid a$), y un entero b es impar si 2 no lo divide. Ahora, por el Teorema de la División, si dividimos un entero por 2, hay sólo dos resto posibles: 0 y 1. Con lo cual, si b es impar, entonces el resto de dividir b por 2 es 1. Por lo tanto,

$$b \text{ es impar} \iff b = 2k + 1 \text{ para algún } k \in \mathbb{Z}.$$

Problema 3.15

Sean $a, b \in \mathbb{Z}$.

1. Probar que si a es par, entonces ab es par.
2. Probar que si a y b son impares, entonces ab es impar.

Ahora vamos a utilizar el Teorema de la División Entera para obtener una caracterización de la relación de congruencia módulo n, y así poder obtener una descripción total de las clases de equivalencias de la relación de congruencia.

Proposición 3.16

Sea $n \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$. Entonces,

$$a \equiv_n b \iff a \text{ y } b \text{ arrojan el mismo resto al ser divididos por } n.$$

Demostración. Sea $n \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$.

($\Rightarrow$) Supongamos que $a \equiv_n b$. Vamos a probar que a y b arrojan el mismo resto al ser divididos por n. Primero, por el Teorema de la División Entera, existen únicos $q_1, r_1 \in \mathbb{Z}$ tales que $a = nq_1 + r_1$ y $0 \leq r_1 < n$, y existen únicos $q_2, r_2 \in \mathbb{Z}$ tales que $b = nq_2 + r_2$ y $0 \leq r_2 < n$. Debemos probar que $r_1 = r_2$. Sabemos que $r_1 \leq r_2$ o $r_2 \leq r_1$. Supongamos que $r_2 \leq r_1$ (un argumento dual se puede usar si $r_1 \leq r_2$). Ahora,

$$a - b = (nq_1 + r_1) - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2)$$

Entonces, como $0 \leq r_1 - r_2 < n$, tenemos que $r_1 - r_2$ es el resto de dividir $a - b$ por n. Por otro lado, como $a \equiv_n b$, tenemos que existe $k \in \mathbb{Z}$ tal que $a - b = nk$. Esto nos dice, por

el Teorema de la División Entera, que 0 es el resto de dividir $a - b$ por n. Por la unicidad, tenemos que $r_1 - r_2 = 0$. Por lo tanto, $r_1 = r_2$.

($\Leftarrow$) Supongamos que a y b arrojan el mismo resto al ser divididos por n. Entonces, por el Teorema de la División Entera, existen únicos $q_1, q_2, r \in \mathbb{Z}$ tales que $a = nq_1 + r$, $b = nq_2 + r$ y $0 \leq r < n$. Entonces, $a - b = nq_1 + r - (nq_2 + r) = nq_1 - nq_2 = n(q_1 - q_2)$. Luego, por la definición de relación de congruencia (véase (3.3)) tenemos que $a \equiv_n b$. ■

La proposición anterior es importante porque nos ayudará a determinar exactamente todas las clases de equivalencia con respecto a la relación de congruencia módulo n. Dado $n \in \mathbb{N}$, notemos que la clase de equivalencia de un entero a, denotada por $[a]_n$, es el conjunto

$$\begin{aligned}[a]_n &= \{b \in \mathbb{Z} : b \equiv_n a\} \\ &= \{b \in \mathbb{Z} : \exists k \in \mathbb{Z}, \text{ tal que } b - a = nk\} \\ &= \{b \in \mathbb{Z} : b = nk + a \text{ con } k \in \mathbb{Z}\}.\end{aligned}$$

Veamos primero un ejemplo de cómo utilizamos la proposición anterior para hallar todas las clases de equivalencia de la relación $\equiv_n$.

Ejemplo 3.17. Sea $n = 5$ y hallemos las clases de equivalencias de los enteros 0, 1, 2, 3 y 4. Entonces,

- La clase de equivalencia del 0 es:

$$\begin{aligned}[0]_5 &= \{b \in \mathbb{Z} : b = 5k + 0 \text{ con } k \in \mathbb{Z}\} = \{b \in \mathbb{Z} : b = 5k \text{ con } k \in \mathbb{Z}\} \\ &= \{\ldots, \underbrace{-15}_{k=-3}, \underbrace{-10}_{k=-2}, \underbrace{-5}_{k=-1}, \underbrace{0}_{k=0}, \underbrace{5}_{k=1}, \underbrace{10}_{k=2}, \underbrace{15}_{k=3}, \ldots\}.\end{aligned}$$

- La clase de equivalencia del 1 es:

$$\begin{aligned}[1]_5 &= \{b \in \mathbb{Z} : b = 5k + 1 \text{ con } k \in \mathbb{Z}\} \\ &= \{\ldots, \underbrace{-14}_{k=-3}, \underbrace{-9}_{k=-2}, \underbrace{-4}_{k=-1}, \underbrace{1}_{k=0}, \underbrace{6}_{k=1}, \underbrace{11}_{k=2}, \underbrace{16}_{k=3}, \ldots\}.\end{aligned}$$

- La clase de equivalencia del 2 es:

$$\begin{aligned}[2]_5 &= \{b \in \mathbb{Z} : b = 5k + 2 \text{ con } k \in \mathbb{Z}\} \\ &= \{\ldots, \underbrace{-13}_{k=-3}, \underbrace{-8}_{k=-2}, \underbrace{-3}_{k=-1}, \underbrace{2}_{k=0}, \underbrace{7}_{k=1}, \underbrace{12}_{k=2}, \underbrace{17}_{k=3}, \ldots\}.\end{aligned}$$

- La clase de equivalencia del 3 es:

$$\begin{aligned}[3]_5 &= \{b \in \mathbb{Z} : b = 5k + 3 \text{ con } k \in \mathbb{Z}\} \\ &= \{\ldots, \underbrace{-12}_{k=-3}, \underbrace{-7}_{k=-2}, \underbrace{-2}_{k=-1}, \underbrace{3}_{k=0}, \underbrace{8}_{k=1}, \underbrace{13}_{k=2}, \underbrace{18}_{k=3}, \ldots\}.\end{aligned}$$

- La clase de equivalencia del 4 es:

$$\begin{aligned}[4]_5 &= \{b \in \mathbb{Z} : b = 5k + 4 \text{ con } k \in \mathbb{Z}\} \\ &= \{\ldots, \underbrace{-11}_{k=-3}, \underbrace{-6}_{k=-2}, \underbrace{-1}_{k=-1}, \underbrace{4}_{k=0}, \underbrace{9}_{k=1}, \underbrace{14}_{k=2}, \underbrace{19}_{k=3}, \ldots\}.\end{aligned}$$

Bien, hemos hallado las clases de equivalencia de 0, 1, 2, 3 y 4. ¿Y por qué no hallar también las clases de equivalencias, por ejemplo, de 5, 6, ..., o las clases de equivalencias del -1, -2, ...? La respuesta es que por la proposición anterior tenemos que las clases de equivalencias $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$ son exactamente todas las clases de equivalencia de la relación $\equiv_5$. En efecto, sea $a \in \mathbb{Z}$. Sea r el resto de dividir a por 5. Como $0 \leq r < 5$, entonces r es también el resto de dividir r por 5. Así, a y r arrojan el mismo resto al ser divididos por 5. Entonces, por la proposición anterior, $a \equiv_5 r$. Por lo tanto, $[a]_5 = [r]_5$[3]. Por ejemplo, hallemos las clases de equivalencia de 5, 6, -1, -2 y -236. Como sabemos que $5 \in [0]_5$, tenemos que $[5]_5 = [0]_5$. Como $6 \in [1]_5$, entonces $[6]_5 = [1]_5$. Como $-1 \in [4]_5$, entonces $[-1]_5 = [4]_5$. Como $-2 \in [3]_5$, entonces $[-2]_5 = [3]_5$. ¿Cuál es la clase de equivalencia del -236? Para hallar su clase de equivalencia, dividimos a -236 por 5 y hallamos su resto. Como $-236 = 5.(-48) + 4$, entonces 4 es el resto de dividir -236 por 5. Ahora, el resto de dividir 4 por 5 es obviamente 4. Entonces -236 y 4 arrojan el mismo resto al ser divididos por 5. Por lo tanto, por la proposición anterior $-236 \equiv_5 4$. Entonces, $[-236]_5 = [4]_5$. ■

Ahora enunciamos el resultado general sobre la obtención de todas las clases de equivalencia de la relación $\equiv_n$.

Proposición 3.18

Dado $n \in \mathbb{N}$, todas las clases de equivalencia de la relación de congruencia módulo n son $[0]_n, [1]_n, \ldots, [n-1]_n$. Por lo tanto, el conjunto cociente es:

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

Demostración. Vamos a probar que $[0]_n$, $[1]_n$, ..., $[n-1]_n$ son exactamente todas las clases de equivalencias de la relación de congruencia $\equiv_n$. Primero, todas estas clases son distintas entre sí. En efecto, sean r_1 y r_2 distintos tales que $0 \leq r_1 < n$ y $0 \leq r_2 < n$. Entonces, r_1 y r_2 son dos restos posibles distintos de dividir un entero por n. Como r_1 es el resto de dividir r_1 por n y r_2 es el resto de dividir r_2 por n, y además $r_1 \neq r_2$, entonces $r_1 \not\equiv_n r_2$ (pues, no arrojan el mismo resto al ser divididos por n). Por lo tanto, $[r_1]_n \neq [r_2]_n$. Ahora probaremos que para todo $a \in \mathbb{Z}$, $[a]_n = [r]_n$ para algún $r \in \{0, 1, \ldots, n-1\}$. Sea $a \in \mathbb{Z}$. Sea r el resto de dividir a por n. Entonces, a y r arrojan el mismo resto al ser divididos por n. Entonces, $a \equiv_n r$ y $0 \leq r < n$. Entonces, $[a]_n = [r]_n$ y $r \in \{0, 1, \ldots, n-1\}$. Por lo tanto, el conjunto cociente dado por la relación de congruencia $\equiv_n$ es:

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

[3]Recordemos una propiedad de las clases de equivalencias: $a \sim b \iff b \in [a] \iff [b] = [a]$.

3.4. Máximo común divisor

Sean $a, b \in \mathbb{Z}$. Definimos los siguientes conjuntos:

$$\text{Div}(a,b) = \{d \in \mathbb{Z} : d \mid a \text{ y } d \mid b\} \qquad \text{y} \qquad \text{Div}_+(a,b) = \{d \in \mathbb{N} : d \mid a \text{ y } d \mid b\}.$$

Esto es, $\text{Div}(a,b)$ es el conjunto de todos los divisores comunes de a y b, y $\text{Div}_+(a,b)$ es el conjunto de todos los divisores positivos comunes de a y b.

Ejemplo 3.19. Los divisores de 30 son: 1, 2, 3, 5, 6, 10, 15, 30, -1, -2, -3, -6, -10, -15, -30. Y los divisores de 24 son: 1, 2, 3, 4, 6, 8, 12, 24, -1, -2, -3, -4, -6, -8, -12, -24. Entonces,

$$\text{Div}(30,-24) = \{-1,-6,-3,-2,1,2,3,6\} = \{\pm1,\pm2,\pm3,\pm6\} \quad \text{y}$$
$$\text{Div}_+(30,-24) = \{1,2,3,6\}.$$

Como podemos observar del ejemplo anterior, si a y b son enteros muy grandes, entonces no es sencillo hallar los divisores comunes entre ellos. Más adelante tendremos una forma más sencilla y algorítmica de encontrar todos los divisores comunes de dos enteros.

Proposición 3.20

Para todos $a, b \in \mathbb{Z}$, $\text{Div}(a,b) = \text{Div}(-a,b) = \text{Div}(a,-b) = \text{Div}(-a,-b)$.

Demostración. Vamos a probar que $\text{Div}(a,b) = \text{Div}(-a,b)$ por doble inclusión. Sea $d \in \text{Div}(a,b)$. Entonces, $d \mid a$ y $d \mid b$. Por la Proposición 3.5, tenemos que $d \mid -a$. Entonces, d divide a $-a$ y a b. Por lo tanto, $d \in \text{Div}(-a,b)$. Hemos probado que $\text{Div}(a,b) \subseteq \text{Div}(-a,b)$. Sea ahora $d \in \text{Div}(-a,b)$. Entonces, $d \mid -a$ y $d \mid b$. Por la Proposición 3.5, $d \mid a$. Con lo cual, $d \in \text{Div}(a,b)$. Entonces $\text{Div}(-a,b) \subseteq \text{Div}(a,b)$. Por lo tanto, $\text{Div}(a,b) = \text{Div}(-a,b)$. Las igualdades restantes se dejan a cargo del lector. ■

Definición 3.21: Máximo común divisor (mcd)

El **máximo común divisor (mcd)** de dos enteros a y b, no simultáneamente nulos, es el mayor elemento del conjunto $\text{Div}(a,b)$. Denotaremos por (a,b) el máximo común divisor de a y b.

Notemos que para todo par de enteros a y b, no simultáneamente nulos, $(a,b) = (b,a)$. Porque los conjuntos $\text{Div}(a,b)$ y $\text{Div}(b,a)$ son iguales.

Ejemplo 3.22. En el ejemplo 3.19 obtuvimos que $\text{Div}(30,-24) = \{\pm1,\pm2,\pm3,\pm6\}$. Entonces, $(30,-24) = 6$.

Proposición 3.23

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. Entonces, $(a,b) = (-a,b) = (a,-b) = (-a,-b)$.

Demostración. Esta proposición es consecuencia de la Proposición 3.20. Vamos a probar que $(a,b) = (-a,b)$. Por la Proposición 3.20, tenemos que $\text{Div}(a,b) = \text{Div}(-a,b)$. Entonces, el mayor elemento del conjunto $\text{Div}(a,b)$ es el mismo que el mayor elemento del conjunto $\text{Div}(-a,b)$. Por lo tanto, $(a,b) = (-a,b)$. ■

Ejemplo 3.24. En el Ejemplo 3.22 obtuvimos que $(30,-24) = 6$. Entonces, sabemos que

$$(30,24) = (-30,24) = (-30,-24) = (30,-24) = 6.$$

Como podemos observar, no es una tarea sencilla hallar el máximo común divisor de dos enteros. A continuación daremos un procedimiento para determinar el mcd de una forma muy sencilla y rápida. Este procedimiento o método se conoce con el nombre de Algoritmo de Euclides. Para esto necesitamos antes el siguiente resultado.

Proposición 3.25

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Si r es el resto de dividir a por b, entonces $(a,b) = (b,r)$.

Demostración. Como r es el resto de dividir a por b, tenemos que

$$a = bq + r \text{ con } q \in \mathbb{Z}.$$

Recordemos que (a,b) es el mayor elemento del conjunto $\text{Div}(a,b)$, y (b,r) es el mayor elemento del conjunto $\text{Div}(b,r)$. Vamos a probar que $\text{Div}(a,b) = \text{Div}(b,r)$.

($\subseteq$) Sea $d \in \text{Div}(a,b)$. Entonces $d \mid a$ y $d \mid b$. Observemos que $r = a - bq$. Ahora, como $d \mid a$ y $d \mid b$, tenemos por la Proposición 3.5 que $d \mid ax + by$ para todos $x, y \in \mathbb{Z}$. Tomando $x = 1$ y $y = -q$, obtenemos que $d \mid a - bq$. Entonces $d \mid r$. Con lo cual, $d \mid b$ y $d \mid r$, esto es, $d \in \text{Div}(b,r)$. Por lo tanto, $\text{Div}(a,b) \subseteq \text{Div}(b,r)$.

($\supseteq$) Ahora, sea $d \in \text{Div}(b,r)$. Entonces $d \mid b$ y $d \mid r$. Entonces, igual que antes, por la Proposición 3.5 tenemos que $d \mid bq + r$. Entonces, $d \mid a$. Con lo cual, $d \in \text{Div}(a,b)$. Entonces $\text{Div}(b,r) \subseteq \text{Div}(a,b)$.

Así, hemos probado que $\text{Div}(a,b) = \text{Div}(b,r)$. Con lo cual, el mayor elemento del conjunto $\text{Div}(a,b)$ coincide con el mayor elemento del conjunto $\text{Div}(b,r)$. Por lo tanto, $(a,b) = (b,r)$. ■

La proposición anterior es de mucha utilidad para hallar el máximo común divisor de dos enteros. Veamos primero un ejemplo concreto de cómo podemos utilizar dicha proposición y luego haremos la formulación general.

Ejemplo 3.26. Tratemos de determinar el mcd de $a = 831$ y $b = 42$. Dado que le resto de dividir 831 por 42 es $r = 33$ tenemos que $(831,42) = (42,33)$. Ahora, como el resto de dividir 42 por 33 es 9 obtenemos que $(42,33) = (33,9)$. Entonces, $(831,42) = (42,33) = (33,9)$. Continuando de esta forma, hasta donde podamos, obtenemos que

$$(831,42) = (42,33) = (33,9) = (9,6) = (6,3) = (3,0) = 3$$

Ahora presentamos la formulación general del procedimiento que realizamos en el ejemplo anterior.

El Algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. Podemos suponer, sin perdida de generalidad, que $b > 0$.
Sea r_1 el resto de dividir a por b.

- Si $r_1 = 0$, entonces $(a, b) = b$.

Si $r_1 \neq 0$, realizamos divisiones sucesivas hasta obtener un resto nulo:

$$\begin{array}{rcll} a & = & bq_1 + r_1 & 0 < r_1 < b \\ b & = & r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3 & 0 < r_3 < r_2 \\ \vdots & = & \vdots & \vdots \\ r_{n-2} & = & r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_nq_{n+1} & \end{array}$$

Observemos que $b > r_1 > r_2 > \ldots > r_n > 0$. Entonces, al cabo de un número finito de divisiones obtendremos un resto nulo (de lo contrario habría infinitos enteros positivos menores que b).

- Si el resto $r_{n+1} = 0$, entonces $(a, b) = r_n$ (esto se prueba en el siguiente teorema).

Teorema 3.27: Algoritmo de Euclides

El último resto no nulo en el desarrollo del algoritmo de Euclides es el máximo común divisor de a y b, esto es, $(a, b) = r_n$.

Demostración. Como r_1 es el resto de dividir a por b, entonces por la Proposición 3.25 tenemos que $(a, b) = (b, r_1)$. Observemos que r_2 es el resto de dividir b por r_1, entonces por la Proposición 3.25 tenemos que $(b, r_1) = (r_1, r_2)$. Entonces $(a, b) = (b, r_1) = (r_1, r_2)$. Continuando de esta forma obtendremos que

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n).$$

Ahora, como $r_{n-1} = r_nq_{n+1}$, tenemos que $r_n \mid r_{n-1}$. Así $(r_{n-1}, r_n) = r_n$. Por lo tanto, $(a, b) = r_n$. ■

Una forma sistemática y uniforme de aplicar el algoritmo de Euclides para obtener el máximo común divisor es mediante la siguiente tabla.

Ejemplo 3.28. Hallar el máximo común divisor de 129 y -27. Como $(129, -27) = (129, 27)$, vamos a determinar el mcd de 129 y 27. Entonces, aplicando el algoritmo de Euclides obtenemos que: Entonces, $(129, -27) = (129, 27) = 3$.

	q_1	q_2	q_3	$\cdots$		q_{n-1}	q_n	q_{n+1}	
a	b	r_1	r_2	$\cdots$	r_{n-3}	r_{n-2}	r_{n-1}	r_n	0

	4	1	3	2	
129	27	21	6	3	0

Proposición 3.29

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que

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

Demostración. Vamos a probar por el Principio de Inducción Completa que todos los restos r_k no nulos en el Algoritmo de Euclides se pueden expresar como $r_k = ax_k + by_k$, para algunos $x_k, y_k \in \mathbb{Z}$.

- **Caso base:** Veamos que se cumple para $k = 1$. Por el Algoritmo de Euclides tenemos que $a = bq_1 + r_1$. Entonces, $r_1 = a - bq_1$. Tomando $x_1 = 1$ y $y_1 = -q_1$, tenemos que $r_1 = ax_1 + by_1$. Por lo tanto, se cumple para $k = 1$.
- **Paso inductivo:** Supongamos que para todo $i < k + 1$, existen $x_i, y_i \in \mathbb{Z}$ tales que $r_i = ax_i + by_i$ (H.I.). Debemos probar que $r_{k+1} = ax_{k+1} + by_{k+1}$, para algunos $x_{k+1}, y_{k+1} \in \mathbb{Z}$. Por el Algoritmo de Eculides tenemos que $r_{k-1} = r_k q_{k+1} + r_{k+1}$. Entonces,

$$\begin{aligned}
r_{k+1} &= r_{k-1} - r_k q_{k+1} \\
r_{k+1} &= (ax_{k-1} + by_{k-1}) - (ax_k + by_k)q_{k+1} && (H.I.) \\
r_{k+1} &= a\underbrace{(x_{k-1} - x_k q_{k+1})}_{=x_{k+1}\in\mathbb{Z}} + b\underbrace{(y_{k-1} - y_k q_{k+1})}_{=y_{k+1}\in\mathbb{Z}} \\
r_{k+1} &= ax_{k+1} + by_{k+1}.
\end{aligned}$$

Por lo tanto, por el Principio de Inducción Completa, todo resto r_k no nulo del Algoritmo de Euclides se puede expresar como $r_k = ax_k + by_k$ para algunos $x_k, y_k \in \mathbb{Z}$. Entonces,

$$(a, b) = r_n = ax_n + by_n$$

para algunos $x_n, y_n \in \mathbb{Z}$. ■

Ejemplo 3.30. Vamos a expresar al mcd de 129 y -27 como combinación lineal de 129 y -27. Por el algoritmo de Euclides que aplicamos en el Ejemplo 3.19, obtuvimos que $3 = (129, -27)$. Vamos a utilizar la tabla del Ejemplo 3.19 para recobrar las sucesivas divisiones:

$$\begin{aligned}
129 &= 27.4 + 21 \implies 21 = 129 - 27.4 \\
27 &= 21.1 + 6 \implies 6 = 27 - 21 \\
21 &= 6.3 + 3 \implies 3 = 21 - 6.3
\end{aligned}$$

Ahora, a partir de la última igualdad, comenzamos a sustituir:

$$\begin{aligned}
3 &= 21 - 6.3 \\
3 &= (129 - 27.4) - (27 - 21).3 \\
3 &= 129 - 27.4 - 27.3 + 21.3 \\
3 &= 129 - 27.4 - 27.3 + (129 - 27.4).3 \\
3 &= 129 + 129.3 - 27.7 - 27.12 \\
3 &= 129.4 - 27.19. \quad \blacksquare
\end{aligned}$$

Ahora vamos a dar una caracterización de la definición de máximo común divisor. En otras palabras, vamos a dar una definición equivalente del concepto de máximo común divisor, esta definición es útil para resolver ciertos problemas.

Proposición 3.31

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos, un entero positivo d es el máximo común divisor de a y b si y sólo si verifica las siguientes condiciones:

(d1) $d \mid a$ y $d \mid b$;

(d2) Si $e \mid a$ y $e \mid b$, entonces $e \mid d$.

Demostración. ($\Rightarrow$) Sea $d = (a, b)$. Vamos a probar que d cumple las dos condiciones (d1) y (d2). Es obvio que d cumple la condición (d1) por que d es un divisor común de a y b. Para probar que d cumple (d2), supongamos que $e \in \mathbb{Z}$ cumple que $e \mid a$ y $e \mid b$. Como $d = (a, b)$, entonces por la Proposición 3.29 existen enteros $x, y \in \mathbb{Z}$ tales que $d = a.x + b.y$. Ahora, dado que $e \mid a$ y $e \mid b$, tenemos por la Proposición 3.5 que $e \mid (a.x + b.y)$. Entonces, $e \mid d$. Luego, d cumple la condición (d2).

($\Leftarrow$) Supongamos ahora que d es un entero que cumple las condiciones (d1) y (d2). Debemos probar que d es el máximo común divisor de a y b. Por la condición (d1) tenemos que d es un divisor común de a y b. Solo nos falta ver que d es el mayor divisor común de a y b. Sea e un divisor común de a y b. Esto es, $e \mid a$ y $e \mid b$. Entonces por la condición (d2) tenemos que $e \mid d$. Luego, $e \leq d$. Por lo tanto, d es el máximo común divisor de a y b. $\blacksquare$

3.5. Números coprimos y ecuaciones diofánticas

Definición 3.32

Diremos que dos enteros $a, b \in \mathbb{Z}$ son **relativamente primos** o **coprimos** si el máximo común divisor de a y b es 1, esto es, si $(a, b) = 1$.

Ejemplo 3.33. Los enteros 12 y 125 son coprimos porque $(12, 125) = 1$. Los entero 150 y 36 no son coprimos, porque $(150, 36) = 6$. También los enteros 180 y 4900 no son coprimos, porque 2 es un divisor común de 180 y 4900 con lo cual $(180, 4900) \geq 2$.

Ahora vamos a probar dos propiedades importantes de los números coprimos.

Proposición 3.34

Sean $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ y $(a, b) = 1$, entonces $a \mid c$.

Demostración. Sean $a, b, c \in \mathbb{Z}$ y supongamos que $a \mid bc$ y $(a, b) = 1$. Por la Proposición 3.29 tenemos que existen enteros x e y tales que $1 = ax + by$. Luego multiplicando por c ambos miembros obtenemos $c = acx + bcy$. Ahora, como $a \mid ac$ y $a \mid bc$, entonces por la Proposiciòn 3.5 tenemos que $a \mid (acx + bcy)$. Entonces, $a \mid c$. ■

Observación 3.35. Es importante observar que en la proposición anterior es fundamental la hipótesis que a y b son coprimos. Es decir, si un entero a divide al producto de dos enteros bc, entonces no necesariamente se cumple que a divide a b o a divide a c. En efecto, tenemos que $4 \mid 2.6$, pero $4 \nmid 2$ y $4 \nmid 6$.

Problema 3.36

1. Probar que si $ak \equiv_n bk$ y $(n, k) = 1$, entonces $a \equiv_n b$.
2. Mostrar que la condición "$(n, k) = 1$" en el inciso anterior es fundamental. Esto es, dar un ejemplo dónde $ak \equiv_n bk$ y $(n, k) \neq 1$, y no se cumple que $a \equiv_n b$.

Proposición 3.37

Sean $a, b, c \in \mathbb{Z}$. Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, entonces $ab \mid c$.

Demostración. En breve. ■

Observación 3.38. Notemos que en la proposición anterior la hipótesis que a y b son coprimos es necesaria. En efecto, por ejemplo $3 \mid 12$ y $6 \mid 12$, pero $3.6 \nmid 12$.

Ahora estamos en condiciones de estudiar ciertas ecuaciones particulares.

Definición 3.39: Ecuaciones diofánticas

Un **ecuación diofántica (lineal)** es una ecuación en dos incógnitas con coeficientes enteros, de la forma

$$ax + by = c$$

con $a, b, c \in \mathbb{Z}$, en la que sólo interesa hallar sus soluciones enteras.

Proposición 3.40

Sean $a, b, c \in \mathbb{Z}$. Entonces $(a, b) \mid c$ si y sólo si existen dos enteros x_0 e y_0 tales que $ax_0 + by_0 = c$.

Demostración. En breve. ■

La proposición anterior nos dice dos cosas. La implicación $(a,b) \mid c \implies \exists x_0, y_0 \in \mathbb{Z}$ tal que $(ax_0 + by_0 = c)$ nos dice que si el máximo común divisor de a y b divide a c, entonces la ecuación diofántica $ax + by = c$ tiene al menos una solución: (x_0, y_0). Por otro lado, la implicación $\exists x_0, y_0 \in \mathbb{Z}$ tal que $(ax_0 + by_0 = c) \implies (a,b) \mid c$ nos dice que si podemos escribir al entero c como combinación lineal de a y b con coeficientes enteros (x_0 e y_0), entonces el máximo común divisor de a y b divide a c.

Corolario 3.41

Sean $a, b, c \in \mathbb{Z}$. Entonces $(a,b) = 1$ si y sólo si existen dos enteros x_0 e y_0 tales que $ax_0 + by_0 = 1$.

Demostración. En breve. ■

Una de las implicaciones del corolario anterior nos dice que si a 1 lo podemos escribir como combinación lineal de los enteros a y b, entonces podemos concluir que a y b son coprimos, es decir, $(a,b) = 1$.

Proposición 3.42

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos y sea $d = (a,b)$. Sean $s, t \in \mathbb{Z}$ tales que $a = d.s$ y $b = d.t$. Entonces, $(s,t) = 1$.

Demostración. Como $d = (a,b)$, entonces por la Proposición 3.29 existen $x, y \in \mathbb{Z}$ tales que $d = ax + by$. Ahora utilizamos las hipótesis que $a = d.s$ y $b = d.t$ para reemplazar en la ecuación anterior:

$$\begin{aligned} d &= ax + by \\ d &= (ds)x + (dt)y \\ d &= d(sx + ty) \\ 1 &= sx + ty. \end{aligned}$$

Por lo tanto, como a 1 lo podemos escribir como combinación lineal de s y t, por el Corolario 3.41 obtenemos que $(s,t) = 1$. ■

Ejemplo 3.43. Vamos a encontrar, si existe, una solución de la ecuación diofántica $627x - 264y = 132$. Primero calculamos el máximo común divisor de 627 y -264, y comprobamos que este mcd divide a 132. Aplicamos el algoritmo de Euclides:

	2	2	1	2	
627	264	99	66	33	0

Como $(627, -264) = 33$ y $33 \mid 132$, entonces podemos afirmar por la Proposición 3.40 que la ecuación $627x - 264y = 132$ tiene al menos una solución entera. Ahora procedemos a

encontrar efectivamente una solución de la ecuación. Como hicimos en el Ejemplo 3.30, de la tabla anterior recobramos las divisiones sucesivas y despejamos los restos:

$$\begin{array}{rcl@{\qquad}rcl} 627 &=& 264.2+99 & \Longrightarrow & 99 &=& 627-264.2 \\ 264 &=& 99.2+66 & \Longrightarrow & 66 &=& 264-99.2 \\ 99 &=& 66.1+33 & \Longrightarrow & 33 &=& 99-66.1 \end{array}$$

Ahora, a partir de la última igualdad, comenzamos a sustituir:

$$\begin{aligned} 33 &= 99-66.1 \\ 33 &= 627-264.2-(264-99.2) \\ 33 &= 627-264.3+99.2 \\ 33 &= 627-264.3+(627-264.2).2 \\ 33 &= 627-264.3+627.2-264.4 \\ 33 &= 627.3-264.7 \end{aligned}$$

Como $132 = 33.4$, multiplicamos la última igualdad por 4:

$$\begin{aligned} 33.4 &= (627.3-264.7).4 \\ 132 &= 627.12-264.28. \end{aligned}$$

Por lo tanto, $x_0 = 12$ e $y_0 = 28$ es una solución de la ecuación diofántica $627x - 264y = 132$. ■

A continuación veremos como determinar todas las soluciones, si existen, de una ecuación diofántica.

Proposición 3.44

Sea $ax + by = c$ una ecuación diofántica y $d = (a, b)$. Si la ecuación $ax + by = c$ tiene una solución (x_0, y_0), entonces todas las soluciones de esta ecuación están dadas por los pares de enteros (x, y) tales que

$$\begin{cases} x &= x_0 + \dfrac{b}{d}.t \\ & \qquad t \in \mathbb{Z}. \\ y &= y_0 - \dfrac{a}{d}.t \end{cases}$$

Demostración. En breve. ■

Ejemplo 3.45. Hallar todas las soluciones de la ecuación $627x - 264y = 132$. En el Ejemplo 3.43 encontramos que $x_0 = 12$ e $y_0 = 28$ era una solución de la ecuación $627x - 264y = 132$. Recordemos que $(627, -264) = 33$. Entonces, todas las soluciones son:

$$\begin{cases} x &= 12 + \dfrac{(-264)}{33}.t \\ & \qquad t \in \mathbb{Z}. \\ y &= 28 - \dfrac{627}{33}.t \end{cases} \qquad \Longrightarrow \qquad \begin{cases} x &= 12 - 8.t \\ & \qquad t \in \mathbb{Z}. \\ y &= 28 - 19.t \end{cases}$$

Algunas soluciones particulares se pueden obtener eligiendo distintos valores del parámetro $t \in \mathbb{Z}$. Por ejemplo, tomando $t = -2$ obtenemos la solución (28, 66). Si elegimos $t = 1$, entonces obtenemos la solución (4, 9). Para cada valor de $t \in \mathbb{Z}$ que tomemos obtendremos una solución de la ecuación.

Ejemplo 3.46. Un club Social y Deportivo desea comprar algunas pelotas de fútbol y algunas de básquet. El club cuenta con \$135.000 para realizar la compra y decide comprar las pelotas en una tienda de deportes dónde hay ofertas de ambas pelotas. En dicha tienda cada pelota de fútbol cuesta \$4.800 y cada pelota de básquet cuesta \$3.900. ¿Cuántas pelotas de cada tipo puede comprar? Consideremos las variables x = cantidad de pelotas de fútbol e y = cantidad de pelotas de básquet. Entonces para responder la pregunta tenemos que hallar las soluciones de la ecuación diofántica $4800x + 3900y = 135000$. Observemos que los tres coeficientes $a = 4800$, $b = 3900$ y $c = 135000$ de la ecuación son múltiplos de 100. Entonces, en lugar de trabajar con la ecuación $4800x + 3900y = 135000$ podemos trabajar con la ecuación equivalente $48x + 39y = 1350$[4]. Primero hallamos el mcd de 48 y 39:

	1	4	3		
48	39	9	3	0	

Entonces $(48, 39) = 3$. Ahora recobramos las divisiones sucesivas y despejamos los restos:

$$\begin{array}{rcl} 48 = 39.1 + 9 & \Longrightarrow & 9 = 48 - 39 \\ 39 = 9.4 + 3 & \Longrightarrow & 3 = 39 - 9.4 \end{array}$$

Ahora, a partir de la última igualdad, comenzamos a sustituir:

$$\begin{aligned} 3 &= 39 - 9.4 \\ 3 &= 39 - (48 - 39).4 \\ 3 &= 39 - 48.4 + 39.4 \\ 3 &= 48.(-4) + 39.5 \end{aligned}$$

Ahora multiplicamos la última igualdad por 450:

$$\begin{aligned} 3.450 &= (48.(-4) + 39.5).450 \\ 540 &= 48.(-1800) + 39.2250 \end{aligned}$$

Entonces $x_0 = -1800$ e $y_0 = 2250$ es una solución de la ecuación $48x + 39y = 1350$ y así también es solución de la ecuación $4800x + 3900y = 135000$. Ahora, para hallar todas las soluciones de la ecuación $4800x + 3900y = 135000$ necesitamos determinar el mcd de 4800 y 3900. Entonces, $(4800, 3900) = 300$. Luego, todas las soluciones de la ecuación $4800x + 3900y = 135000$ son:

[4]Dos ecuaciones $ax + by = c$ y $a'x + b'y = c'$ se dicen que son equivalentes si ellas tienen exactamente las mismas soluciones.

$$\begin{cases} x &= -1800 + \dfrac{3900}{300}.t \\ \\ y &= 2250 - \dfrac{4800}{300}.t \end{cases} \quad t \in \mathbb{Z}. \quad \Longrightarrow \quad \begin{cases} x &= -1800 + 13.t \\ \\ y &= 2250 - 16.t \end{cases} \quad t \in \mathbb{Z}.$$

Como el club desea comprar al menos una pelota de cada deporte tenemos que $x > 0$ e $y > 0$. Debemos resolver las siguientes desigualdades para hallar los posibles valores del parámetro t:

$$\begin{aligned} x &> 0 \\ -1800 + 13.t &> 0 \\ 13.t &> 1800 \\ t &> \frac{1800}{13} \\ t &> 138{,}46 \end{aligned} \qquad \text{y} \qquad \begin{aligned} y &> 0 \\ 2250 - 16.t &> 0 \\ 2250 &> 16.t \\ \frac{2250}{16} &> t \\ 140{,}63 &> t \end{aligned}$$

Entonces, los posibles valores del parámetro t son (recuerde que t toma sólo valores enteros): $t = 139$ o $t = 140$. Con lo cual, las dos soluciones posibles de la ecuación con respecto a estos valores de t son:

$$\begin{aligned} t = 139 &\Longrightarrow x = 7 \text{ e } y = 26 \\ t = 140 &\Longrightarrow x = 20 \text{ e } y = 10. \end{aligned}$$

Por lo tanto, conclusión final, el club puede comprar 7 pelotas de fútbol y 26 de básquet o puede comprar 20 pelotas de fútbol y 10 de básquet. ■

3.6. Mínimo común múltiplo

Sean $a, b \in \mathbb{Z}$. Definimos el siguiente conjunto

$$\mathrm{M}(a,b) = \{x \in \mathbb{N} : x \text{ es múltiplo de } a \text{ y de } b\}.$$

Observemos que $x \in \mathrm{M}(a,b)$ si y sólo si $a \mid x$ y $b \mid x$.

Ejemplo 3.47.

- Los múltiplos comunes (positivos) de 2 y 3 son: $\mathrm{M}(2,3) = \{6, 12, 18, 24, \dots\}$.
- Los múltiplos comunes (positivos) de -12 y 8 son: $\mathrm{M}(-12,8) = \{24, 48, 72, \dots\}$.

Definición 3.48: Mínimo común múltiplo

Sean $a, b \in \mathbb{Z}$ no nulos. El **mínimo común múltiplo (mcm)** de a y b es el menor elemento del conjunto $\mathrm{M}(a,b)$ y se lo denota por $[a,b]$.

Ejemplo 3.49.

- $[2,3] = \min \mathrm{M}(2,3) = \min\{6,12,18,24,\dots\} = 6$.
- $[-12,8] = \min \mathrm{M}(-12,8) = \min\{24,48,72,\dots\} = 24$.

Como el lector podrá observar, a medida que los enteros a o b son cada vez más grandes (en valor absoluto) es más trabajoso determinar el mínimo común múltiplo de ellos. A continuación enunciaremos una propiedad acerca del mínimo común múltiplo y luego un resultado que nos ayudará a determinar de forma efectiva y sencilla el mínimo común múltiplo de dos enteros cualesquiera.

Proposición 3.50

Sean $a, b \in \mathbb{Z}$. Entonces, $[a,b] = [-a,b] = [a,-b] = [-a,-b]$.

Demostración. Primero hay que probar que $\mathrm{M}(a,b) = \mathrm{M}(-a,b) = \mathrm{M}(a,-b) = \mathrm{M}(-a,-b)$, cuya prueba es similar a la dada en la Proposición 3.20. Dejamos la comprobación al lector. Luego, si $\mathrm{M}(a,b) = \mathrm{M}(-a,b)$, entonces es claro que el menor elemento del conjunto $\mathrm{M}(a,b)$ es igual al menor elemento del conjunto $\mathrm{M}(-a,b)$. Por lo tanto, $[a,b] = \min \mathrm{M}(a,b) = \min \mathrm{M}(-a,b) = [-a,b]$. De forma análoga se prueban las otras igualdades. ■

Proposición 3.51

Sean $a, b \in \mathbb{Z}$ no nulos. Entonces

$$[a,b] = \frac{|ab|}{(a,b)}.$$

Demostración. Sean $a, b \in \mathbb{Z}$ no nulos. Supongamos primero que $a > 0$ y $b > 0$ y probemos que

$$[a,b] = \frac{ab}{d}.$$

Sea $d = (a,b)$. Entonces, existen enteros $a', b' \in \mathbb{Z}$ tales que

$$a = da' \qquad \text{y} \qquad b = db'. \tag{3.5}$$

Observemos que por la Proposición 3.42 tenemos que $(a',b') = 1$. Elijamos el número m como

$$m = a'b = \frac{a}{d}b = \frac{ab}{d}.$$

Entonces, m es múltiplo de b. Por otro lado, como

$$m = a'b = a'(db') = (da')b' = ab'$$

tenemos que m es también múltiplo de a. Esto es, m es múltiplo común de a y b. Ahora veamos que es el menor de todos los múltiplos comunes de a y b. Para ello, supongamos que $t \in \mathbb{Z}$ es otro múltiplo común de a y b. Debemos probar que $m \leq t$. Como t es múltiplo de a y b, tenemos que existen $k, q \in \mathbb{Z}$ tales que $t = aq$ y $t = bk$. Entonces, utilizando las ecuaciones de (3.5) obtenemos que

$$aq = bk \implies da'q = db'k \implies a'q = b'k.$$

Luego, $a' \mid b'k$. Como $(a', b') = 1$, entonces $a' \mid k$ (véase la Proposición 3.34). Así $k = a'k'$ para algún $k' \in \mathbb{Z}$. Entonces,

$$t = bk$$
$$t = ba'k'$$
$$t = mk'.$$

Con lo cual, $m \mid t$. Entonces $m \leq t$. Por lo tanto, m es el mínimo común múltiplo de a y b.

Sean ahora a y b enteros cualesquiera. Como $|a| > 0$ y $|b| > 0$, por lo recién probado y la Proposición 3.50 tenemos que

$$[a, b] = [|a|, |b|] = \frac{|a||b|}{d} = \frac{|ab|}{d}.$$

■

3.7. Números primos

Observemos que todo número entero a es siempre divisible por 1, -1, a y $-a$ (± 1 y $\pm a$ para abreviar). Estos son llamados los **divisores triviales** de a. En esta sección estudiaremos aquellos números enteros que tienen sólo como divisores a los triviales.

Definición 3.52

Un número entero a distinto de 0, 1 y -1 es llamado **primo** si sus *únicos* divisores son ± 1 y $\pm a$. Un número entero que no es primo será llamado **compuesto**.

Ejemplo 3.53.

Teorema 3.54

Todo entero $a \neq 0, 1, -1$, admite por lo menos un divisor primo positivo.

Demostración. Sea $a \neq 0, 1, -1$. Sea $m > 1$ el menor entero positivo que divide a a[5]. Vamos a probar, por absurdo, que m es primo. Supongamos que m no es primo. Entonces, existe un $k \in \mathbb{Z}$ tal que $k \mid m$ y $1 < k < m$. Como $k \mid m$ y $m \mid a$, tenemos que $k \mid a$. Es decir, que $k > 1$ es un divisor de a menor que m, lo cual es absurdo, pues m era el menor de los divisores de a. Por lo tanto, m es primo. ■

Ejemplo 3.55. Probar que para todo entero $a \neq 0, -1$, los enteros $2a + 1$ y $a(a + 1)$ son coprimos. Sea $d = (2a + 1, a(a + 1))$. Debemos probar que $d = 1$. Supongamos que $d \neq 1$. Entonces, existe un primo p que divide a d. Luego, como $p \mid d$ y $d \mid 2a + 1$, tenemos que

[5]Observe que si $\text{Div}_{>1}(a)$ es el conjunto de todos los divisores positivos de a mayores que 1, $\text{Div}_{>1}(a) \neq \emptyset$, pues $|a| \in \text{Div}_{>1}(a)$. Entonces, por el Principio de Buena Ordenación (**??**), existe el primer elemento de $\text{Div}_{>1}(a)$. Es decir, existe $m > 1$ que es el menor entero positivo que divide a a.

$p \mid 2a+1$. Análogamente, $p \mid a(a+1)$. Esto es $p \mid a^2+a$. Entonces, tenemos las siguientes implicaciones

$$p \mid 2a+1 \implies p \mid 2a^2+a$$
$$p \mid a^2+a \implies p \mid 2a^2+2a$$

Entonces p divide a $(2a^2+2a)-(2a^2+a)=a$. Esto es $p \mid a$. Esto implica que $p \mid 2a$. Luego, como $p \mid 2a+1$ y $p \mid 2a$, concluimos que $p \mid 1$, lo cual es absurdo. Este absurdo surgió de suponer que $d \neq 1$. Por lo tanto, $d=1$ y así los enteros $2a+1$ y $a(a+1)$ son coprimos. ■

Teorema 3.56: Euclides

Existen infinitos números primos.

Demostración. Vamos a probar que existen infinitos primos positivos. Para esto, vamos a suponer por absurdo que existe sólo un número finito de primos positivos. Supongamos que $p_1, p_2, \ldots, p_k$ son todos los enteros primos positivos. Sea $n = 1 + p_1.p_2.\ldots.p_k$. Así $n > 1$. Entonces, por el Teorema 3.54 sabemos que existe un primo positivo p que divide a n. Como los únicos primos positivos son $p_1, p_2, \ldots, p_k$, tenemos que $p = p_i$ para algún primo p_i. Entonces, $p \mid (p_1.p_2.\ldots.p_k)$. Luego, $p \mid (n - p_1.p_2.\ldots.p_k)$. Es decir, $p \mid 1$. Lo cual es absurdo. Por lo tanto, existen infinitos primos positivos. ■

Una propiedad importante y útil de los números primos es la siguiente.

Proposición 3.57

Sea p un entero primo y sean $a, b \in \mathbb{Z}$. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

Demostración. Sea p un entero primo y supongamos que $p \mid ab$. Si $(p,a)=1$, entonces por la Proposición 3.34 tenemos que $p \mid b$. Ahora si $d=(p,a) \neq 1$, entonces d es un divisor de p distinto de 1. Entonces $d = p$. Luego, $p \mid a$. ■

Ejemplo 3.58. Sean $a, b, c \in \mathbb{Z}$ tales que $(a,b)=1$ y $(a,c)=1$. Vamos a probar que $(a,bc)=1$. Supongamos, por absurdo, que $(a,bc) \neq 1$. Entonces, por el Teorema 3.54 existe un primo p tal que $p \mid (a,bc)$. Luego, $p \mid a$ y $p \mid bc$. Por la Proposición 3.57, tenemos dos posibilidades $p \mid b$ o $p \mid c$. Veamos que las dos posibilidades conducen a un absurdo.

• Si $p \mid b$, entonces tenemos que $p \mid a$ y $p \mid b$, con lo cual $p \mid (a,b)$. Esto es, $p \mid 1$, lo cual es absurdo pues p es primo.

• Ahora, si $p \mid c$, entonces tenemos que $p \mid a$ y $p \mid c$, con lo cual $p \mid (a,c)$. Esto es, $p \mid 1$, lo cual es absurdo pues p es primo.

Por lo tanto, se concluye que $(a,bc)=1$. ■

Teorema 3.59: Teorema Fundamental de la Aritmética (TFA)

Todo número entero $a \neq 0, 1, -1$ es, o bien un entero primo, o bien se puede escribir como ± 1 por un producto de números primos positivos. Esta factorización es única salvo el orden de los factores.

Demostración. Es suficiente probar el teorema para todo entero positivo $a \neq 0, 1$. Vamos a probar el teorema por inducción. Consideramos la proposición:

$$P(a): \ a, \text{ o bien es un entero primo, o bien es producto de enteros primos positivos}$$

El teorema queda demostrado si probamos que $P(a)$ es verdadera para todo $a \geq 2$. Vamos a usar el Principio de Inducción (véanse los Teoremas 1.20 y 1.22).

- **Caso base:** $P(2)$ es verdadera, porque sabemos que 2 es un entero primo.
- **Paso inductivo:** Supongamos que $P(k)$ es verdadera para todo $k < a$. Debemos probar que $P(a)$ es verdadera. Esto es, debemos probar que a o bien es un entero primo o bien es producto de primos. Si a es primo, entonces $P(a)$ es verdadera. Supongamos que a no es un entero primo. Esto es, a es un entero compuesto. Entonces, existen dos enteros b y c tales que $a = bc$ con $1 < b, c < a$. Por hipótesis inductiva tenemos que b es primo o es producto de primos, y c es un primo o es un producto de primos. En cualquier caso tenemos que $b = p_1.....p_s$ y $c = q_1.....q_t$ con p_i, q_j todos enteros primos. Entonces, $a = p_1.....p_s q_1.....q_t$. Luego, a es producto de primos. Entonces $P(a)$ es verdadera. Por lo tanto, por el Principio de Inducción $P(a)$ es verdadera para todo $a \geq 2$. Así, hemos probado que todo entero positivo a distinto de 0 y 1 o bien es un entero primo, o bien se puede escribir como producto de enteros primos.

Solo resta probar que la factorización es única. Supongamos que un entero a tiene dos factorizaciones en producto de primos, esto es, supongamos que

$$a = p_1.p_2.....p_s = q_1.q_2.....q_t \tag{3.6}$$

con p_i y q_j todos enteros primos. Observemos que $p_1 \mid (q_1.q_2.....q_n)$. Entonces, p_1 divide a alguno de los factores del producto $q_1.q_2.....q_t$. Reordenando si fuera necesario, podemos suponer que $p_1 \mid q_1$. Luego, como p_1 y q_1 son primos, tenemos que $p_1 = q_1$. Entonces, de (3.6) podemos simplificar $p_1 = q_1$, y nos queda

$$p_2.p_3.....p_s = q_2.q_3.....q_t. \tag{3.7}$$

Análogamente, $p_2 \mid (q_2.q_3.....q_t)$. Entonces, podemos suponer que $p_2 \mid q_2$. Con lo cual, $p_2 = q_2$. Así, cancelando $p_2 = q_2$ en ambos lados de la igualdad en (3.7) nos queda

$$p_3.....p_t = q_3.....q_s.$$

Continuando con este procedimiento iremos obteniendo que $p_i = q_i$, e iremos cancelando primos p_i de un lado de la igualdad y primos q_i del otro lado de la igualdad. Si $t < s$, entonces obtendríamos que $1 = q_{t+1}.....q_t$, lo cual es absurdo (pues implicaría que $q_{t+1} = \cdots = q_t = 1$). Si $s < t$, entonces tendríamos que $p_{s+1}.....q_t = 1$, lo cual es absurdo. Por lo tanto, $s = t$, y $p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_t = q_t$. ■

Ejemplo 3.60. Vamos a hallar la factorización en productos de primos de los enteros 360 y -980. Para cada entero n, vamos ir probando, de menor a mayor, si un primo positivo p

lo divide. Si n es divisible por p, para el cociente de la división probamos si es divisible por p. En caso que no, probamos si el cociente es divisible por el primo siguiente. Al final, cuando el cociente llegue a 1 o -1, multiplicamos los primos, contando las repeticiones, que nos fueron quedando. Por ejemplo,

360	2
180	2
90	2
45	3
15	3
5	5
1	

-980	2
-490	2
-245	5
-49	7
-7	7
-1	

Entonces,

$$360 = 2.2.2.3.3.5 = 2^3.3^2.5 \qquad \text{y} \qquad 980 = (-1)2.2.5.7.7 = (-1)2^2.5.7^2.$$

Del TFA y del ejemplo anterior, observamos que para cada entero $a \neq 0, 1, -1$, podemos agrupar los factores primos iguales entre sí en la factorización de a, y así obtener que $a = (\pm 1)p_1^{t_1}.p_2^{t_2}.\ldots.p_k^{t_k}$. Establecemos el TFA de esta forma:

Teorema Fundamental de la Aritmética (TFA)

Todo número entero $a \neq 0, 1, -1$ se puede escribir en forma única como

$$a = (\pm 1)p_1^{t_1}.p_2^{t_2}.\ldots.p_k^{t_k}$$

donde $k \in \mathbb{N}$, $t_1, t_2, \ldots, t_k$ son enteros positivos y los $p_1, p_2, \ldots, p_k$ son primos distintos.

La formulación anterior del TFA nos dice que podemos escribir a todo entero $a \neq 0, \pm 1$ de forma única como producto de potencias de primos distintos. Es importante siempre tener presente que el TFA no solo nos dice que a todo entero $a \neq 0, \pm 1$ lo podemos factorizar como un producto de primos, sino que también esta factorización es única. Este hecho de la unicidad en el TFA es una propiedad fundamental, y la cual se usará repetidamente.

A continuación veremos algunas aplicaciones del TFA.

Observación 3.61. Podemos observar que dos enteros a y b son relativamente primos si y sólo si los primos que aparecen en la factorización de a son todos distintos a los primos que aparecen en la factorización de b.

Ejemplo 3.62. Probemos que $\sqrt{2}$ es un número irracional. Supongamos, por absurdo, que $\sqrt{2}$ es racional. Entonces, $\sqrt{2} = \dfrac{a}{b}$ con a y b enteros tales que $(a, b) = 1$. Luego $\sqrt{2}b = a$, y así $2b^2 = a^2$. Por el TFA, obtenemos las factorizaciones de a y b en producto de primos:

$$a = 2^s p_1^{s_1}.\ldots.p_k^{s_k} \qquad \text{y} \qquad b = 2^t p_1^{t_1}.\ldots.p_k^{t_k}.$$

Entonces,

$$a^2 = (2^s p_1^{s_1}.\ldots.p_k^{s_k})^2 = 2^{2s} p_1^{2s_1}.\ldots.p_k^{2s_k} \qquad \text{y} \qquad b^2 = (2^t p_1^{t_1}.\ldots.p_k^{t_k})^2 = 2^{2t} p_1^{2t_1}.\ldots.p_k^{2t_k}.$$

Ahora $2b^2 = 2.2^{2t}p_1^{2t_1}.....p_k^{2t_k} = 2^{2t+1}p_1^{2t_1}.....p_k^{2t_k}$. Con lo cual

$$2^{2s}p_1^{2s_1}.....p_k^{2s_k} = 2^{2t+1}p_1^{2t_1}.....p_k^{2t_k}.$$

Luego, tenemos dos factorizaciones del mismo entero. Entonces, por la unicidad de la factorización obtenemos que $2s = 2t + 1$, lo que es absurdo, pues $2s$ es un entero par y $2t + 1$ es un entero impar. Por lo tanto, $\sqrt{2}$ es irracional.

Proposición 3.63

Sean $a, b \in \mathbb{Z}$ distintos de 0,1,-1. Supongamos que

$$a = (\pm 1)p_1^{s_1}.....p_k^{s_k} \qquad \text{y} \qquad b = (\pm 1)p_1^{t_1}.....p_k^{t_k}$$

son las factorizaciones en producto de primos de a y b, respectivamente. Entonces,

$$a \mid b \iff s_i \leq t_i, \forall i = 1, \ldots, k.$$

Demostración. ($\Rightarrow$) Supongamos que $a \mid b$. Debemos probar que $s_i \leq t_i$. Como $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = ac$. Como los únicos divisores primos de b son $p_1, \ldots, p_k$, tenemos que por el TFA el entero c se factoriza de la forma $c = (\pm 1)p_1^{r_1}.....p_k^{r_k}$ donde cada $r_i \geq 0$. Luego,

$$\begin{aligned}(\pm 1)p_1^{t_1}.....p_k^{t_k} &= (\pm 1)p_1^{s_1}.....p_k^{s_k}.(\pm 1)p_1^{r_1}.....p_k^{r_k} \\ (\pm 1)p_1^{t_1}.....p_k^{t_k} &= (\pm 1)p_1^{s_1+r_1}.....p_k^{s_k+r_k}.\end{aligned}$$

Entonces, por la unicidad de la factorización, tenemos que $t_i = s_i + r_i$ para todo $i = 1, \ldots, k$. Por lo tanto, $s_i \leq t_i$ para todo $i = 1, \ldots, k$.

($\Leftarrow$) Supongamos que $s_i \leq t_i$ para todo $i = 1, \ldots, k$. Para cada $i = 1, \ldots, k$, $s_i \leq t_i$, entonces para cada $i = 1, \ldots, k$ $t_i = s_i + r_i$ con $r_i \geq 0$. Entonces

$$b = (\pm 1)p_1^{t_1}.....p_k^{t_k} = (\pm 1)p_1^{s_1+r_1}.....p_k^{s_k+t_k} = (\pm 1)p_1^{s_1}.....p_k^{s_k}.p_1^{r_1}.....p_k^{r_k} = ac$$

donde $c = p_1^{r_1}.....p_k^{r_k} \in \mathbb{Z}$. Por lo tanto, $a \mid b$. ■

La proposición anterior nos permite hallar de forma efectiva y sistemática todos los divisores de un entero a. Además, también podremos saber de antemano cuántos divisores tiene el entero a. Es claro que el conjunto total de divisores de a está formado por todos los divisores positivos de a y de los opuestos de los divisores positivos. Entonces, la cantidad total de divisores de un entero a es el doble de la cantidad de divisores positivos de a. Así, nos concentraremos en los divisores positivos. Tomemos un entero $a \neq 0, \pm 1$ y supongamos que $a = (\pm 1)p_1^{s_1}.p_2^{s_2}.....p_k^{s_k}$ es su factorización en producto de primos. Definimos el conjunto $\text{Div}_+(a) = \{x \in \mathbb{N} : x \mid a\}$. Entonces, por la proposición anterior tenemos que el conjunto de todos los divisores positivos de a es

$$\text{Div}_+(a) = \{p_1^{r_1}.p_2^{r_2}.....p_k^{r_k} : 0 \leq r_1 \leq s_1,\ 0 \leq r_2 \leq s_2,\ \ldots,\ 0 \leq r_k \leq s_k\}.$$

Para obtener un divisor positivo $x = p_1^{r_1}.....p_k^{r_k}$ de a debemos elegir un entero r_1 entre 0 y s_1, es decir, tenemos $(s_1 + 1)$ posibles elecciones $(0, 1, 2, \ldots, s_1)$; luego, para cada elección del

r_1, tenemos que elegir un entero r_2 entre 0 y s_2, es decir, tenemos (s_2+1) posibles elecciones $(0,1,\ldots,s_2)$; …; finalmente para cada una de las elecciones anteriores, debemos elegir un entero r_k entre 0 y s_k, es decir, tenemos (s_k+1) posibles elecciones $(0,1,\ldots,s_k)$. Por lo tanto, el número total de divisores positivos de a es

$$(s_1+1)(s_2+1)\ldots(s_k+1).$$

Y la cantidad total de divisores de a es

$$2(s_1+1)(s_2+1)\ldots(s_k+1).$$

Ejemplo 3.64. Sea $a = 2205$ y hallemos todos los divisores positivos de a. Primero factorizamos $a = 3^2.5.7^2$. Entonces, la cantidad total de divisores positivos de a es: $\#\mathrm{Div}_+(a) = (2+1)(1+1)(2+1) = 18$. Así sabemos que hay 18 divisores positivos de a (y por lo tanto, hay 36 divisores de a). Ahora

$$\mathrm{Div}_+(a) = \{x = 3^{r_1}.5^{r_2}.7^{r_3} : \ 0 \le r_1 \le 2,\ 0 \le r_2 \le 1,\ 0 \le r_3 \le 2\}$$
$$\mathrm{Div}_+(a) = \{3^0.5^0.7^0,\ 3^1.5^0.7^0,\ 3^2.5^0.7^0,\ 3^0.5^1.7^0,\ 3^1.5^1.7^0,\ 3^2.5^1.7^0,\ 3^0.5^0.7^1,\ 3^1.5^0.7^1,\ 3^2.5^0.7^1,$$
$$3^0.5^1.7^1,\ 3^1.5^1.7^1,\ 3^2.5^1.7^1,\ 3^0.5^0.7^2,\ 3^1.5^0.7^2,\ 3^2.5^0.7^2,\ 3^0.5^1.7^2,\ 3^1.5^1.7^2,\ 3^2.5^1.7^2\}.$$

Problema 3.65

1. Hallar la cantidad de divisores positivos de 144, ¿puede decir cuáles son?
2. Probar que si a es un cuadrado, entonces la cantidad de divisores positivos de a es un número impar.
3. Probar que si a no es un cuadrado, entonces la cantidad de divisores positivos de a es un número par.

Proposición 3.66

Sean $a, b \in \mathbb{N}$ distintos de 1. Supongamos que $a = p_1^{s_1}.\ldots.p_k^{s_k}$ y $b = p_1^{t_1}.\ldots.p_k^{t_k}$ son las factorizaciones en producto de primos de a y b, respectivamente. Entonces,

$$(a,b) = p_1^{m_1}.\ldots.p_k^{m_k} \qquad \text{y} \qquad [a,b] = p_1^{M_1}.\ldots.p_k^{M_k}$$

donde para cada $i = 1,\ldots,k$ tenemos que

$$m_i = \text{mín}\{s_i, t_i\} \qquad \text{y} \qquad M_i = \text{máx}\{s_i, t_i\}.$$

Demostración. En breve. ■

Ejemplo 3.67. Hallemos el máximo común divisor y el mínimo común múltiplo de 38808 y 32670. Vamos a utilizar el TFA. Primero encontramos las factorizaciones en producto de primos de los dos enteros:

$$38808 = 2^3.3^2.7^2.11 \qquad \text{y} \qquad 32670 = 2.3^3.5.11^2.$$

Luego, reescribimos la factorizaciones de ambos enteros completando en cada caso con los primos que faltan y elevándolos al cuadrado:

$$38808 = 2^3.3^2.5^0.7^2.11 \qquad \text{y} \qquad 32670 = 2.3^3.5.7^0.11^2.$$

Ahora, tenemos que:

$$\begin{aligned} 38808 &= 2^3.3^2.5^0.7^2.11 \\ 32670 &= 2.3^3.5.7^0.11^2 \\ (38808, 32670) &= 2^1.3^2.5^0.7^0.11^1 = 198 \\ [38808, 32670] &= 2^3.3^3.5.7^2.11^2 = 6403320. \end{aligned}$$

Ejercicios propuestos

La relación divide

El Teorema de la División

Ejercicio 3.1.

(a) Probar que para cada $x \in \mathbb{Z}$, $x^3 \equiv_3 x$.

(b) Probar que para cada $x \in \mathbb{Z}$, $x^5 \equiv_5 x$.

(c) En base a los dos incisos anteriores, formular una conjetura general y comprobarla para algunos otros casos.

Máximo común divisor

Ejercicio 3.2. Probar que $(a, b) = (a, b + ak)$, para todo $k \in \mathbb{Z}$.

Ejercicio 3.3. Probar que si $a \equiv_n b$, entonces $(a, n) = (b, n)$.

Números coprimos

Ejercicio 3.4. Sea $d = (a, b)$ y sean $a = da'$ y $b = db'$. Probar que $(a', b') = 1$.

Ejercicio 3.5. Probar que si $ka \equiv_n kb$ y $d = (n, k)$, entonces $a \equiv_{n/d} b$[6].

Ejercicio 3.6.

(a) Probar que si $(b, c) = 1$, entonces (a, b) y (a, c) son coprimos.

(b) Probar que si $(b, c) = 1$, entonces $(a, bc) = (a, b)(a, c)$. (*Consejo: Probar que cada miembro de la ecuación anterior divide al otro miembro. Para ello, usar el inciso anterior, la Proposición 3.29 y la Proposición 3.37.*)

[6] Aquí n/d es el cociente de dividir n por d. Es decir, n/d es el entero tal que $n = (n/d).d$.

Ejercicio 3.7. Probar las siguientes propiedades. Sean $a, b \in \mathbb{Z}$.

(a) $(a, b) = 1 \iff (a^n, b^m) = 1, \forall m, n \in \mathbb{N}$.

(b) $(a^n, b^n) = (a, b)^n, \forall n \in \mathbb{N}$.

(c) $(ma, mb) = |m|(a, b)$, para todo $m \in \mathbb{Z}$.

(d) Sea $m \in \mathbb{Z}$. Si $m \mid a$ y $m \mid b$, entonces $(a/m, b/m) = (a, b)/m$.[7] (*Consejo: Aplicar el inciso anterior*)

Mínimo común múltiplo

Ejercicio 3.8. Sean $a, b \in Z$ no nulos. Probar que $\mathrm{M}(a, b) = \mathrm{M}(-a, b) = \mathrm{M}(a, -b) = \mathrm{M}(-a, -b)$.

Números primos

Ejercicio 3.9. Sea $a \in \mathbb{Z}$ y p un entero primo. Probar que $(p, a) = 1$ o $(p, a) = p$.

Ejercicio 3.10. Sea $p \in \mathbb{Z}$ distinto de $0, \pm 1$. Supongamos que p cumple la siguiente propiedad: $\forall a, b \in \mathbb{Z}$, $p \mid ab \implies p \mid a$ o $p \mid b$. Probar que p es primo.

Ejercicio 3.11. Sea p un entero primo y sean $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$, con $n \in \mathbb{N}$. Probar que si $p \mid a_1.a_2.\ldots.a_{n+1}$, entonces $p \mid a_i$ para algún $i = 1, \ldots, n+1$.

Ejercicio 3.12. Probar las siguientes propiedades. Sean $a, b \in \mathbb{Z}$.

(a) Si $(a, b) = 1$, entonces $(a - b, a + b) = 1$ o 2.

Ejercicio 3.13. Sea $a \in \mathbb{Z}$. Vamos a denotar por $\tau(a)$ al número de divisores positivos de a. Esto es, si $a = \pm p_1^{e_1}.\ldots.p_k^{e_k}$, entonces $\tau(a) = (e_1 + 1).\ldots.(e_k + 1)$. Probar que si $a, b \in \mathbb{Z}$ y $(a, b) = 1$, entonces $\tau(ab) = \tau(a)\tau(b)$.

[7] Aquí a/m representa el cociente de dividir a por m. Es decir, a/m es el entero tal que $a = (a/m).m$. De igual manera para b/m y $(a, b)/m$.

Capítulo 4

Números Complejos

Todos sabemos que la ecuación $x^2 = -1$ no tiene solución en el conjunto de números reales $\mathbb{R}$. Es decir, sabemos que no existe ningún número real x tal que $x^2 = -1$. Esto es consecuencia del hecho de que el cuadrado de cualquier número real es siempre no negativo: $a^2 \geq 0$. El objetivo es construir el *menor* conjunto que contenga a los números reales y contenga un elemento, que denotaremos por i, que sea una solución de la ecuación $x^2 = -1$, esto es, que se cumpla que

$$i^2 = -1.$$

Además, es fundamental que en dicho conjunto estén definidas dos operaciones (suma y producto) que extiendan a las operaciones de suma y producto de números reales. Vamos a denotar a este conjunto por $\mathbb{C}$. También podemos observar que en $\mathbb{C}$ no sólo la ecuación $x^2 = -1$ tiene solución, sino que todas las ecuaciones de la forma $x^2 = a$ con $a \in \mathbb{R}$ tienen soluciones. Si $a \geq 0$, entonces $\sqrt{a} \in \mathbb{R} \subseteq \mathbb{C}$ es una solución[1]. Ahora, si $a < 0$, entonces $x = \sqrt{|a|}i$ es solución, en efecto, $x^2 = (\sqrt{|a|}i)^2 = (\sqrt{|a|})^2 i^2 = |a|(-1) = a$.

4.1. El cuerpo de los números complejos

Nuestro objetivo en esta sección es construir efectivamente el conjunto $\mathbb{C}$ de tal forma que tenga las propiedades mencionadas en la introducción de éste capítulo. Comenzamos. Sea

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}.$$

Entonces, nuestros nuevos "números", llamados *números complejos*, son pares ordenados (a, b) con $a, b \in \mathbb{R}$. Ahora necesitamos definir de forma conveniente en $\mathbb{C}$ dos operaciones:

[1] Es claro que para $a \geq 0$, la ecuación $x^2 = a$ tiene dos soluciones: $\sqrt{a}$ y $-\sqrt{a}$.

Sean $(a,b),(c,d) \in \mathbb{C}$.

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

Producto: $(a,b)(c,d) = (ac-bd, ad+bc)$.

Llamaremos a $\mathbb{C}$ con las dos operaciones recién definidas el **cuerpo de números complejos**.

Ejemplo 4.1. Sean $z = (-\frac{1}{2}, 3)$ y $w = (4,-1)$. Entonces

$$z+w = (-\tfrac{1}{2},3)+(4,-1) = (-\tfrac{1}{2}+4, 3-1) = (\tfrac{7}{2},2)$$

y

$$z.w = (-\tfrac{1}{2},3)(4,-1) = (-\tfrac{1}{2}.4 - 3.(-1), -\tfrac{1}{2}.(-1) + 3.4) = (1, \tfrac{25}{2}).$$

Problema 4.2

Realizar las siguientes operaciones.

(1) $(-\frac{2}{3},4) + \Big((2,-3).(\frac{1}{3},1)\Big)$.

(2) $(-1,1).\big((2,3)+(-5,7)\big)$.

Para operar algebraicamente con los números complejos necesitamos probar que las operaciones de suma y producto tienen las mismas propiedades que la de los números reales.

Proposición 4.3: Propiedades de la suma

La suma cumple las siguientes propiedades. Sean $z,u,w \in \mathbb{C}$. Entonces,

Asociativa: $z+(u+w) = (z+u)+w$.

Conmutativa: $z+u = u+z$.

Elemento neutro: Existe $(0,0) \in \mathbb{C}$ tal que $z+(0,0) = z$.

Opuesto: Para todo $z = (a,b) \in \mathbb{C}$, existe el complejo $-z = (-a,-b)$ tal que $z + (-z) = (0,0)$.

Demostración. Vamos a probar sólo la propiedad asociativa, las demostraciones de las restantes propiedades quedan a cargo del lector. Sean $z = (a,b)$, $u = (c,d)$ y $w = (e,f)$.

Entonces,

$$\begin{aligned}
z+(u+w) &= (a,b)+((c,d)+(e,f)) \\
&= (a,b)+(c+e,d+f) && \text{definición de la suma} \\
&= (a+(c+e),b+(d+f)) && \text{definición de la suma} \\
&= ((a+c)+e),(b+d)+f) && \text{asociativa de la suma de números reales} \\
&= (a+c,b+d)+(e,f) && \text{definición de la suma} \\
&= ((a,b)+(c,d))+(e,f) && \text{definición de la suma} \\
&= (z+u)+w. && \blacksquare
\end{aligned}$$

Ahora enunciamos las propiedades básicas del producto de números complejos.

Proposición 4.4: Propiedades del producto

El producto cumple las siguientes propiedades. Sean $z,u,w \in \mathbb{C}$. Entonces,

Asociativa: $z.(u.w) = (z.u).w$.

Conmutativa: $z.u = u.z$.

Elemento neutro: Existe $(1,0) \in \mathbb{C}$ tal que $z.(1,0) = z$.

Inverso: Para todo $z = (a,b) \neq (0,0)$, existe $z^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ tal que $z.z^{-1} = (1,0)$.

Demostración. Probamos sólo la propiedad asociativa, las demostraciones de las restantes propiedades quedan a cargo del lector. Sean $z = (a,b)$, $u = (c,d)$ y $w = (e,f)$. Por un lado calculamos $z.(u.w)$:

$$\begin{aligned}
z.(u.w) &= (a,b).((c,d).(e,f)) \\
&= (a,b).(ce-df,cf+de) && \text{definición del producto} \\
&= (a(ce-df)-b(cf+de),a(cf+de)+b(ce-df)) && \text{definición del producto} \\
&= (ace-adf-bcf-bde,acf+ade+bce-bdf).
\end{aligned}$$

Por otro lado calculamos $(z.u).w$:

$$\begin{aligned}
(z.u).w &= ((a,b).(c,d)).(e,f) \\
&= (ac-bd,ad+bc).(e,f) && \text{definición del producto} \\
&= ((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e) && \text{definición del producto} \\
&= (ace-bde-adf-bcf,acf-bdf+ade+bce) \\
&= (ace-adf-bcf-bde,acf+ade+bce-bdf)
\end{aligned}$$

Por lo tanto, podemos observar que

$$z.(u.w) = (ace-adf-bcf-bde,acf+ade+bce-bdf) = (z.u).w. \qquad \blacksquare$$

Problema 4.5

Sea $z = (-1, 3)$. Hallar z^{-1} y comprobar que $z.z^{-1} = 1$.

Proposición 4.6: Distributiva

Para todo $z, u, w \in \mathbb{C}$, se tiene que

$$z.(u + w) = z.u + z.w.$$

Demostración. A cargo del lector. ■

Para seguir trabajando con números complejos necesitamos introducir algunas definiciones. Sea $z = (a, b) \in \mathbb{C}$. Definimos:

La parte real de z: $\mathrm{Re}(z) = a$.

La parte imaginaria de z: $\mathrm{Im}(z) = b$.

Es decir, la primer coordenada del complejo $z = (a, b)$ es llamada la parte real de z, y la segunda coordenada de z es llamada la parte imaginaria de z. A los números complejos que son de la forma $(a, 0)$ los llamaremos **complejos reales**, y a los complejos que son de la forma $(0, b)$ con $b \neq 0$ los llamaremos **imaginarios puros**. Además, al número complejo $(0, 1)$ lo llamaremos **unidad imaginaria** y lo denotamos por

$$i = (0, 1)$$

ya que será fundamental para hallar otra forma de escribir a los números complejos.

Ahora vamos a realizar la siguiente convención: a los complejos reales $(a, 0)$ los vamos a denotar simplemente por a, así

$$a = (a, 0).$$

En otras palabras, estamos considerando que los números reales están representados dentro del conjunto de números complejos por medio de los complejos reales $a = (a, 0)$. Entonces $\mathbb{R} \subseteq \mathbb{C}$. Con lo cual hemos logrado uno de los objetivos buscados: extender el conjunto de números reales. Además, si $a = (a, 0)$ y $b = (b, 0)$ son dos complejos reales, entonces

$$(a, 0) + (b, 0) = (a + b, 0) = a + b \qquad \text{y} \qquad (a, 0)(b, 0) = (ab - 0.0, a.0 + 0.b) = (ab, 0) = ab.$$

Por lo tanto, observamos que las operaciones suma y producto de números complejos es una extensión de la suma y producto de números reales.

Observación 4.7. Ya estamos en condiciones de comprobar que la unidad imaginaria i es efectivamente la solución a la ecuación $x^2 = -1$. En efecto,

$$i^2 = i.i = (0, 1).(0, 1) = (0.0 - 1.1, 0.1 + 1.0) = (-1, 0) = -1.$$

Ahora, utilizando las propiedades básicas de las operaciones de suma y producto obtenemos lo siguiente: sea $z = (a, b) \in \mathbb{C}$, entonces

$$\begin{aligned} z &= (a, b) \\ &= (a, 0) + (0, b) \\ &= a + (b, 0)(0, 1) \\ &= a + bi. \end{aligned}$$

Por lo tanto, tenemos otra forma de representar a los número complejos.

Definición 4.8: Forma binómica

A todo número complejo $z = (a, b)$ lo podemos escribir como

$$z = a + bi. \qquad \textbf{(Forma binómica)}$$

Operar con números complejos en forma binómica es muy similar a operar con números reales.

Ejemplo 4.9. Sean $z = -1 + 2i$ y $w = 3 - 4i$. Entonces

$$z + w = (-1 + 2i) + (3 - 4i) = (-1 + 3) + (2 - 4)i = 2 - 2i$$

y

$$\begin{aligned} z.w &= (-1 + 2i)(3 - 4i) = (-1).3 + (-1)(-4i) + 2i.3 + 2i.(-4i) = -3 + 4i + 6i - 8i^2 \\ &= -3 + 10i - 8(-1) = 5 + 10i. \quad \blacksquare \end{aligned}$$

De la misma forma que en el conjunto de los números reales escribimos $\frac{a}{b}$ en lugar de ab^{-1}, en el conjunto $\mathbb{C}$ de complejos también a menudo solemos escribir $\frac{z}{w}$ en lugar de zw^{-1}. Las dos expresiones son válidas y usaremos la que nos resulte más cómodo en cada situación. Además podemos observar que

$$\frac{z}{w} = z.\frac{1}{w} = zw^{-1}.$$

También es útil notar que si $z = a + bi \neq 0$ está en forma binómica, entonces por la Proposición 4.4 tenemos que

$$\frac{1}{z} = z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Problema 4.10

Realizar las siguientes operaciones en forma binómica.

(a) $(3 + 6i) - (5 - 2i) + i$.

(b) $(3 + 5i)(-4 - 2i)(-1 + 4i)$.

(c) $\dfrac{4 + 2i}{1 - 2i} + \dfrac{3 + 4i}{1 - 2i}$.

(d) $(1 - i)^3(1 + i)$.

4.2. Representación geométrica y conjugado

En esta sección obtendremos otra forma de representar a los números complejos. Esta será una representación geométrica o gráfica. Recordemos que los números reales se pueden representar mediante los puntos de una recta. Ahora, los números complejos pueden ponerse en correspondencia biunívoca con los puntos del plano cartesiano formado por los ejes de coordenadas x (eje de las abscisas) e y (eje de las ordenadas). A esto se refiere la siguiente definición.

Definición 4.11: Representación geométrica

A cada número complejo $z = a + bi$ le hacemos corresponder el punto $P_z = (a, b)$ del plano cartesiano. Recíprocamente, a cada punto $P = (c, d)$ del plano cartesiano le hacemos corresponder el número complejo $z_P = c + di$, véase la Figura 4.1. Y estas asignaciones son biyectivas:

$$z = a + bi \implies P_z = (a, b) \implies z_{P_z} = a + bi = z$$

y

$$P = (c, d) \implies z_P = c + di \implies P_{P_z} = (c, d) = P.$$

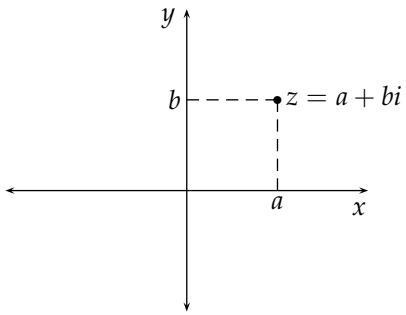

Figura 4.1: Representación geométrica

Definición 4.12: Conjugado

Sea $z = a + bi \in \mathbb{C}$. Llamaremos **conjugado** de z al número complejo

$$\overline{z} = a - bi \qquad \text{(Ver Figura 4.2).}$$

Problema 4.13

Representar gráficamente los siguientes números complejos y sus conjugados $z = 1 + 2i$, $u = -1 + 3i$, $w = 2 - i$, $z + u$ y $w - u$.

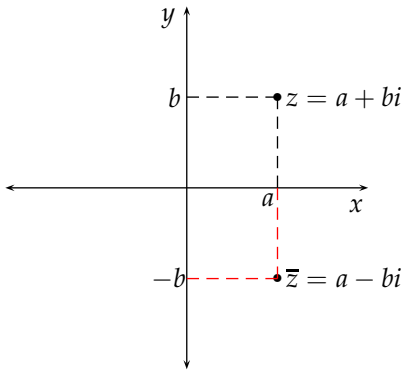

Figura 4.2: Conjugado

Proposición 4.14: Propiedades del conjugado

Sean $z, w \in \mathbb{C}$. Entonces:

1. $\overline{\overline{z}} = z$.
2. $z\overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2$.
3. $\overline{z+w} = \overline{z} + \overline{w}$.
4. $\overline{z.w} = \overline{z}.\overline{w}$.

Demostración. A cargo del lector. ■

Problema 4.15

Probar que las siguientes propiedades se cumplen para todo $z \in \mathbb{C}$.

(a) $z + \overline{z} = 2\mathrm{Re}(z)$.

(b) $z - \overline{z} = 2\mathrm{Im}(z)$.

4.3. Módulo

En esta sección presentamos otro concepto que es importante para el estudio de los números complejos.

Definición 4.16: Módulo

Sea $z = a + bi \in \mathbb{C}$. El **módulo** de z es el número real

$$|z| = \sqrt{a^2 + b^2}.$$

Así como los números complejos son representados como puntos en el plano cartesiano, el módulo de un número complejo tiene un sentido geométrico muy claro. Consideremos un complejo $z = a + bi$. Representamos a z en el plano cartesiano, ver Figura 4.3. Podemos

observar (Figura 4.3) que se forma un triángulo rectángulo entre el complejo z, el origen de coordenadas y el eje x, donde a y b son los catetos y el segmento $\overline{Oz}$ que une el origen de coordenadas con z es la hipotenusa. Entonces, por el Teorema de Pitágoras, tenemos que $\overline{Oz}^2 = a^2 + b^2$. Con lo cual $\overline{Oz} = \sqrt{a^2 + b^2} = |z|$. Por lo tanto, el módulo de z representa la longitud del segmento que une el origen de coordenadas con el complejo z en el plano cartesiano, véase la Figura 4.3.

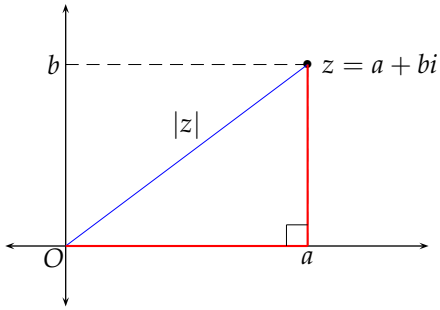

Figura 4.3: Módulo

Proposición 4.17: Propiedades

Sean $z, w \in \mathbb{C}$. Entonces:

1. $|z| \geq 0$, y $|z| = 0 \iff z = 0$.
2. $\mathrm{Re}(z) \leq |z|$ y $\mathrm{Im}(z) \leq |z|$.
3. $|z|^2 = z\overline{z}$.
4. $|z| = |\overline{z}| = |-z|$.
5. $|zw| = |z||w|$.
6. $|z + w| \leq |z| + |w|$ (Desigualdad triangular).
7. $||z| - |w|| \leq |z - w|$.

Demostración. Dejamos las pruebas de las propiedades 1., 2., 3. y 4. a cargo del lector. Para probar las restantes propiedades vamos a utilizar frecuentemente la propiedad 3. $|z|^2 = z\overline{z}$ y las propiedades del conjugado.

Sean $z, w \in \mathbb{C}$.

5.

$$|zw|^2 = (zw).(\overline{zw}) = z.w\overline{z}.\overline{w} = z.\overline{z}.w.\overline{w} = |z|^2|w|^2 = (|z||w|)^2 \implies |zw| = |z||w|.$$

6.

$$\begin{aligned}
|z+w|^2 &= (z+w)\overline{(z+w)} = (z+w)(\overline{z}+\overline{w}) \\
&= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \\
&= |z|^2 + z\overline{w} + \overline{z\overline{w}} + |w|^2 && \text{notar que } \overline{z\overline{w}} = \overline{z}w = w\overline{z} \\
&= |z|^2 + 2\mathrm{Re}(z\overline{w}) + |w|^2 && \text{ver inciso (a) del Problema 4.15} \\
&\leq |z|^2 + 2|z\overline{w}| + |w|^2 && \text{por la Proposición 4.17} \\
&= |z|^2 + 2|z||\overline{w}| + |w|^2 \\
&= |z|^2 + 2|z||w| + |w|^2 \\
&= (|z| + |w|)^2.
\end{aligned}$$

Luego hemos obtenido que $|z+w|^2 \leq (|z|+|w|)^2$. Entonces $|z+w| \leq |z|+|w|$.

7. Notemos que $||z|-|w||$ es el valor absoluto del número real $|z|-|w|$. Luego, por definición de valor absoluto, probar 7. es equivalente a probar que

$$-|z-w| \leq |z|-|w| \leq |z-w|.$$

Primero tenemos que

$$|z| = |(z-w)+w| \leq |z-w|+|w| \implies |z|-|w| \leq |z-w|.$$

Por otro lado, tenemos que

$$|w| = |(w-z)+z| \leq |w-z|+|z| \implies |w|-|z| \leq |w-z| = |z-w| \implies -|z-w| \leq |z|-|w|.$$

Hemos obtenido que $-|z-w| \leq |z|-|w| \leq |z-w|$. Por lo tanto, $||z|-|w|| \leq |z-w|$. ■

Podemos utilizar los números complejos para representar ciertos conjuntos o regiones del plano cartesiano. Veamos los siguientes ejemplos.

Ejemplo 4.18. Consideremos el siguiente conjunto de números complejos:

$$A = \{z \in \mathbb{C} : 1 \leq \mathrm{Re}(z) < 3\}.$$

Observemos que $z = (x,y) \in A$ si y sólo si $1 \leq x < 3$ e $y \in \mathbb{R}$. Entonces, obtenemos la región de la Figura 4.4

Ejemplo 4.19. Consideremos el siguiente conjunto de números complejos:

$$B = \{z \in \mathbb{C} : |z| < 2\}.$$

Recordemos que el módulo de un complejo z representa la distancia entre el origen de coordenadas y z. Entonces los complejos z que cumplen con la condición $|z| < 2$ son todos aquellos complejos z cuya distancia al origen es menor que 2. Notemos que todos los complejos z que cumplen la igualdad $|z| = 2$, son todos aquellos cuya distancia al origen es 2. Esto es, por definición de circunferencia, todos los complejos que están sobre la circunferencia centrada en el origen y radio 2. Pero como estamos buscando todos los z tales que $|z| < 2$, ellos son todos los complejos que están en el interior de la circunferencia con centro en el origen y radio 2, véase la Figura 4.5.

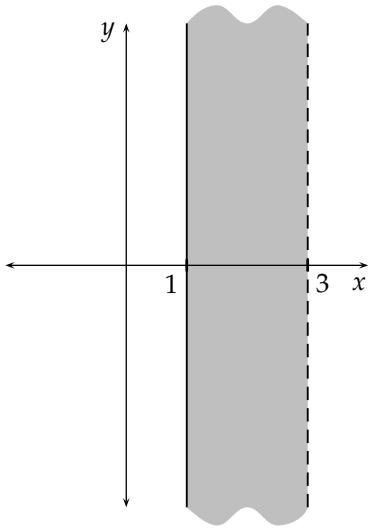

Figura 4.4: Ejemplo 4.18

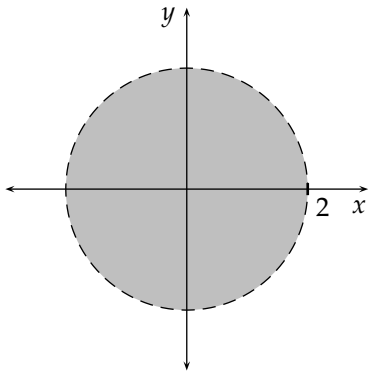

Figura 4.5: Ejemplo 4.19

Ejemplo 4.20. Consideremos la región R pintada en el plano cartesiano dado en la Figura 4.6. Trataremos de encontrar el conjunto de números complejos que represente dicha región. Podemos observar que los puntos (x, y) que se encuentran en la región R están en el exterior de la circunferencia con centro en el origen y radio 1 y dentro de la circunferencia con centro en el origen y radio 3. Entonces, un punto (x, y) se encuentra en la región R si y sólo si $1 < \sqrt{x^2 + y^2} < 3$. Entonces,

$$R = \{z \in \mathbb{C} : 1 < |z| < 3\}.$$

4.4. Forma trigonométrica o polar

En esta sección obtendremos otra forma de expresar a los números complejos, la cual resulta a menudo de mucha utilidad a la hora trabajar y operar con números complejos. Para esta sección es importante que el lector recuerde algunos conceptos básicos de trigonometría como el Teorema de Pitágoras, funciones trigonométricas y funciones trigonométricas inversas.

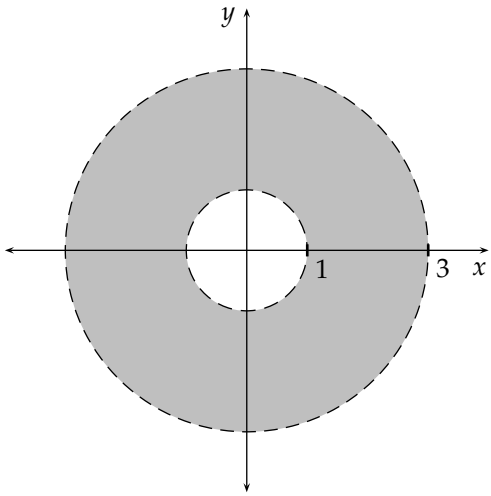

Figura 4.6: Ejemplo 4.20

Definición 4.21: Argumento

El **argumento** de un número complejo $z = a + bi \neq 0$ es el ángulo α formado por el segmento $\overline{Oz}$ y el semieje real positivo tal que $0 \leq \alpha < 2\pi$, véase la Figura 4.7. Denotamos el argumento de un complejo $z \neq 0$ por $\arg(z)$.

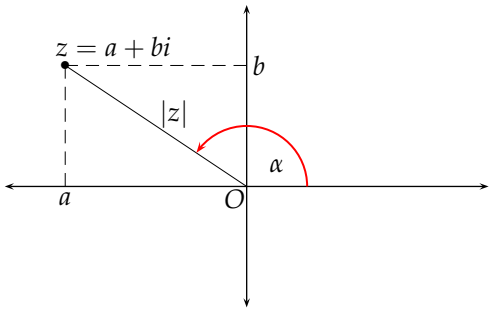

Figura 4.7: Argumento

Notemos que según la definición anterior, el argumento de $z = 0$ no está definido.

Ejemplo 4.22. Hallemos el argumento del complejo $z = 2 - 2i$. Primero es conveniente ubicar al número complejo en el plano cartesiano, véase la Figura 4.8. Observemos que $z = 2 - 2i$ se encuentra en el cuarto cuadrante. Ahora vamos a calcular el ángulo α^*, ver en la Figura 4.8. Entonces,

$$\alpha^* = \arctan\left(\frac{-2}{2}\right) = -\frac{\pi}{4}.$$

Entonces, el argumento de $z = 2 - 2i$ es:

$$\arg(z) = 2\pi - \frac{\pi}{4} = \frac{7}{4}\pi.$$

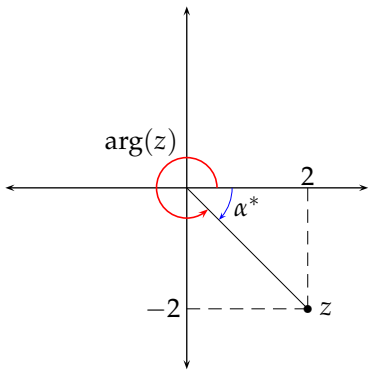

Figura 4.8: Ejemplo 4.22

Ahora estamos en condiciones de establecer otra forma de expresar a los números complejos, en este caso, utilizando el módulo y argumento.

Proposición 4.23: Forma polar o trigonométrica

Sea $z = a + bi \neq 0$ cualquier número complejo no nulo. Sea $\alpha = \arg(z)$. Entonces,

$$z = |z|\cos\alpha + i|z|\operatorname{sen}\alpha$$
$$z = |z|(\cos\alpha + i\operatorname{sen}\alpha). \qquad \textbf{(Forma polar)}$$

Demostración. Sea $z = a + bi \neq 0$ cualquier número complejo no nulo. Sea $\alpha = \arg(z)$, véase la Figura 4.9. Entonces, aplicando las razones trigonométricas con respecto al ángulo α tenemos que

$$\cos\alpha = \frac{a}{|z|} \qquad \text{y} \qquad \operatorname{sen}\alpha = \frac{b}{|z|}.$$

Luego, $a = |z|\cos\alpha$ y $b = |z|\operatorname{sen}\alpha$. Por lo tanto, obtenemos que

$$z = a + bi = |z|\cos\alpha + |z|\operatorname{sen}\alpha.i.$$ ■

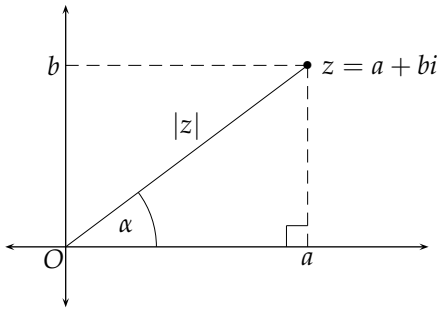

Figura 4.9: Forma polar o trigonométrica

En general, cuando trabajemos con números complejos en forma polar escribiremos

$$z = r.\operatorname{cis}\alpha$$

queriendo decir que r es el módulo de z, α es el argumento de z y $\operatorname{cis}\alpha = \cos\alpha + i\operatorname{sen}\alpha$.

Ejemplo 4.24. Expresemos al número complejo $z = -\sqrt{3} + i$ en forma polar. Primero, ubicamos a z en el plano cartesiano, véase la Figura 4.10. Observemos que z se encuentra en el segundo cuadrante. Ahora, tenemos que hallar el módulo y argumento de z. Para el módulo:

$$|z| = \sqrt{(-\sqrt{3})^2 + 1^2} = 2.$$

Para el argumento, primero calculamos el ángulo α^*, ver Figura 4.10.

$$\alpha^* = \arctan \frac{1}{-\sqrt{3}} = -\frac{\pi}{6}.$$

Entonces, teniendo en cuenta que z está en el segundo cuadrante (véase la Figura 4.10), tenemos que su argumento es:

$$\arg(z) = \pi - \frac{\pi}{6} = \frac{5}{6}\pi.$$

Por lo tanto,

$$z = 2\text{cis}\left(\frac{5}{6}\pi\right).$$

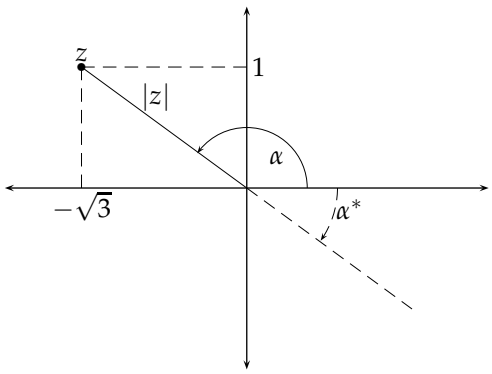

Figura 4.10: Ejemplo 4.10: Forma polar de $z = -\sqrt{3} + i$

Ahora veremos que es muy sencillo multiplicar y dividir números complejos en forma polar.

Proposición 4.25

Sean $z = r.\text{cis}\,\alpha$ y $w = s.\text{cis}\,\beta$ números complejos no nulos. Entonces:

1. $z.w = (r.s)\text{cis}\,(\alpha + \beta)$.
2. $\dfrac{z}{w} = \left(\dfrac{r}{s}\right)\text{cis}\,(\alpha - \beta)$.

Demostración. 1. Para demostrar la primera igualdad utilizaremos las siguientes identidades trigonométricas

$$\cos(\alpha + \beta) = \cos\alpha.\cos\beta - \text{sen}\,\alpha.\text{sen}\,\beta \quad \text{y} \quad \text{sen}\,(\alpha + \beta) = \cos\alpha.\text{sen}\,\beta + \text{sen}\,\alpha.\cos\beta.$$

Entonces,

$$\begin{aligned} z.w &= (r\text{cis}\,\alpha)(s\text{cis}\,\beta) = (rs)\text{cis}\,\alpha.\text{cis}\,\beta = (rs)(\cos\alpha + i\text{sen}\,\alpha)(\cos\beta + i\text{sen}\,\beta) \\ &= (rs)(\cos\alpha.\cos\beta + \cos\alpha.i\text{sen}\,\beta + i\text{sen}\,\alpha.\cos\beta + i\text{sen}\,\alpha.i\text{sen}\,\beta) \\ &= (rs)((\cos\alpha\cos\beta - \text{sen}\,\alpha\text{sen}\,\beta) + i(\cos\alpha\text{sen}\,\beta + \text{sen}\,\alpha\cos\beta)) \\ &= (rs)(\cos(\alpha+\beta) + i\text{sen}\,(\alpha+\beta)) \\ &= (rs)\text{cis}\,(\alpha+\beta). \end{aligned}$$

2. Vamos a utilizar la primera identidad. Así,

$$\left(\frac{r}{s}\right)\text{cis}\,(\alpha-\beta).w = \left(\frac{r}{s}\right)\text{cis}\,(\alpha-\beta).(s\text{cis}\,\beta) = \left(\frac{r}{s}.s\right)\text{cis}\,((\alpha-\beta)+\beta) = r\text{cis}\,\alpha = z.$$

Luego, como $z = \left(\frac{r}{s}\right)\text{cis}\,(\alpha-\beta).w$, tenemos que $\frac{z}{w} = \left(\frac{r}{s}\right)\text{cis}\,(\alpha-\beta)$. ■

El siguiente resultado es también muy útil en la práctica para operar con números complejos.

Teorema 4.26: Fórmula de De Moivre

Sea $z = r.\text{cis}\,\alpha$. Entonces, para todo $k \in \mathbb{Z}$,

$$z^k = r^k\text{cis}\,(k.\alpha).$$

Demostración. Sea $z = r.\text{cis}\,\alpha$. Primero probaremos por inducción que $z^n = r^n\text{cis}\,(n\alpha)$ para todo número natural n.

- **Caso base:** Probamos que se cumple para $n = 1$. Esto es obvio, pues $z^1 = z = r\text{cis}\,\alpha$ y $r^1\text{cis}\,(1.\alpha) = r\text{cis}\,(\alpha)$. Entonces, $z^1 = r^1\text{cis}\,(1.\alpha)$.
- **Paso inductivo:** Supongamos que $z^n = r^n\text{cis}\,(n\alpha)$ se cumple para un $n \in \mathbb{N}$ (H.I.). Debemos probar que $z^{n+1} = r^{n+1}\text{cis}\,((n+1)\alpha)$. Entonces,

$$\begin{aligned} z^{n+1} &= z^n.z \\ &= (r^n\text{cis}\,(n\alpha))\,(r\text{cis}\,\alpha) && \text{H.I.} \\ &= (r^n.r)(\text{cis}\,(n\alpha+\alpha)) && \text{Proposición 4.25} \\ &= r^{n+1}\text{cis}\,((n+1)\alpha) \end{aligned}$$

Entonces, $z^k = r^k\text{cis}\,(k.\alpha)$ se cumple para todo $k \in \mathbb{N}$. También se cumple cuando $k = 0$. En efecto, $z^0 = 1$ y $r^0\text{cis}\,(0.\alpha) = 1\text{cis}\,(0) = 1$. Con lo cual $z^0 = r^0\text{cis}\,(0.\alpha)$. Sólo nos resta probar que $z^k = r^k\text{cis}\,(k.\alpha)$ es verdad para todo entero negativo k. Sea $k \in \mathbb{Z}$ y $k < 0$. Entonces,

$$\begin{aligned} z^k &= \frac{1}{z^{-k}} \\ &= \frac{1}{r^{-k}\text{cis}\,(-k\alpha)} && \text{Utilizamos lo ya probado, pues } -k > 0 \\ &= \left(\frac{1}{r^{-k}}\right)\text{cis}\,(0-(-k\alpha)) && \text{Proposición 4.25 teniendo en cuenta que } 1 = 1.\text{cis}\,(0) \\ &= r^k\text{cis}\,(k\alpha). \end{aligned}$$

Por lo tanto, podemos afirmar que $z^k = r^k\text{cis}\,(k.\alpha)$ se cumple para todo entero k. ■

Ejemplo 4.27. Sean $z = \sqrt{3} + i$ y $w = \frac{3}{\sqrt{2}} + \frac{3}{\sqrt{2}}i$. Calculemos $z.w$, $\frac{z}{w}$ y z^4. Entonces, primero pasamos los complejos z y w a forma polar. Nos queda que $z = 2\text{cis}\left(\frac{\pi}{6}\right)$ y $w = 3\text{cis}\left(\frac{\pi}{4}\right)$. Entonces,

$$z.w = (2.3)\text{cis}\left(\frac{\pi}{6} + \frac{\pi}{4}\right) = 6\text{cis}\left(\frac{5}{12}\pi\right) = \frac{3(-1+\sqrt{3})}{\sqrt{2}} + \frac{3(1+\sqrt{3})}{\sqrt{2}}i \approx 1,5529 + 5,8i,$$

$$\frac{z}{w} = \left(\frac{2}{3}\right)\text{cis}\left(\frac{\pi}{6} - \frac{\pi}{4}\right) = \frac{2}{3}\text{cis}\left(-\frac{\pi}{12}\right) = \frac{2}{3}\text{cis}\left(\frac{23}{12}\pi\right) = \frac{1+\sqrt{3}}{3\sqrt{2}} + \frac{1-\sqrt{3}}{3\sqrt{2}}i$$
$$\approx 0,644 - 0,1725i$$

y

$$z^4 = 2^4\text{cis}\left(4.\frac{\pi}{6}\right) = 16\text{cis}\left(\frac{2}{3}\pi\right) = -8 + 8\sqrt{3}i.$$

4.5. Raíces n-ésimas

Una de las razones por la cual aparecieron o se crearon los números complejos fue con la intención de poder calcular raíces (cuadradas, cuartas, sextas, etc.) de números reales negativos. Como mencionamos en la introducción del capítulo, se pretendía que la ecuación $x^2 = -1$ tuviera una solución. Vimos en la Observación 4.7 que $i^2 = -1$, esto es, $i = \sqrt{-1}$; en otras palabras, i es una raíz cuadrada de -1. Aquí veremos que en realidad podemos calcular las raíces n-ésimas de todo número complejo.

Definición 4.28: Raíz n-ésima

Sea z un número complejo y sea $n \in \mathbb{N}$. Llamaremos **raíz n-ésima** de z a todo número complejo w tal que $w^n = z$.

Ejemplo 4.29. Sea $z = -1$. Sin mucha dificultad podemos observar que $w_1 = i$ y $w_2 = -i$ son dos raíces cuadradas de $z = -1$. Pues, $w_1^2 = i^2 = -1$ y $w_2^2 = (-i)^2 = -1$.

Problema 4.30

Hallar cuatro raíces cuartas distintas del complejo $z = 1$. Esto es, hallar cuatro números complejos w distintos tales que $w^4 = 1$.

Nuestro siguiente objetivo es tener un procedimiento efectivo y sencillo para obtener exactamente todas las raíces n-ésimas de un número complejo z.

Teorema 4.31

Sea $z \in \mathbb{C}$ no nulo y $n \in \mathbb{N}$. Entonces, existen exactamente n raíces n-ésimas de z, y ellas están determinadas por la siguiente ecuación:

$$w_k = \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z) + 2k\pi}{n}\right) \tag{4.1}$$

con $k = 0, 1, \ldots, n-1$.

Demostración. Sea $z \in \mathbb{C}$ no nulo y $n \in \mathbb{N}$. Primero veremos que toda raíz n-ésima de z es de la forma (4.1). Sea w una raíz n-ésima de z. Entonces, $w^n = z$. Observemos que w es distinto de cero (caso contrario z sería cero). Expresemos a w en forma polar: $w = r\text{cis}\,\theta$. Entonces, dado que w es una raíz n-ésima de z obtenemos que

$$\begin{aligned} w^n &= z \\ (r.\text{cis}\,\theta)^n &= |z|.\text{cis}\,(\arg(z)) \\ r^n.\text{cis}\,(n\theta) &= |z|.\text{cis}\,(\arg(z)). \end{aligned}$$

Luego, tenemos que

$$r^n = |z| \qquad \text{y} \qquad n\theta = \arg(z) + 2k\pi \quad \text{con } k \in \mathbb{Z}$$

y despejando r y θ nos queda que

$$r = \sqrt[n]{|z|} \qquad \text{y} \qquad \theta = \frac{\arg(z) + 2k\pi}{n} \quad \text{con } k \in \mathbb{Z}.$$

Entonces,

$$w = \sqrt[n]{|z|}\text{cis}\left(\frac{\arg(z) + 2k\pi}{n}\right) = w_k, \qquad \text{para algún } k \in \mathbb{Z}.$$

Ahora debemos probar que $w_0, w_1, \ldots, w_{n-1}$ son exactamente todas las raíces n-ésimas de z. Para ello, debemos probar que las raíces $w_0, w_1, \ldots, w_{n-1}$ son todas distintas, y que para cualquier entero t, w_t es igual a una de las raíces $w_0, w_1, \ldots, w_{n-1}$. Veamos primero que $w_0, w_1, \ldots, w_{n-1}$ son todas distintas. Sean $i, j \in \{0, 1, \ldots, n-1\}$ y supongamos que $j < i$. Con lo cual tenemos que $0 < i - j < n$. Supongamos por absurdo que $w_i = w_j$. Entonces

$$\begin{aligned} w_i &= w_j \\ \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z) + 2i\pi}{n}\right) &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z) + 2j\pi}{n}\right) \\ \text{cis}\left(\frac{\arg(z) + 2i\pi}{n}\right) &= \text{cis}\left(\frac{\arg(z) + 2j\pi}{n}\right) \\ \frac{\arg(z) + 2i\pi}{n} &= \frac{\arg(z) + 2j\pi}{n} + 2t\pi \\ \frac{\arg(z) + 2i\pi}{n} &= \frac{\arg(z) + 2j\pi + 2tn\pi}{n} \\ \arg(z) + 2i\pi &= \arg(z) + 2j\pi + 2tn\pi \\ i &= j + tn \\ \frac{i-j}{n} &= t \end{aligned}$$

La última igualdad nos dice que $\dfrac{i-j}{n}$ es un número entero. Pero teníamos que $0 < i - j < n$, con lo cual $0 < \dfrac{i-j}{n} < 1$. Absurdo. Por lo tanto, $w_i \neq w_j$.

Ahora sea $t \in \mathbb{Z}$. Probaremos que $w_t = w_k$ para un $k \in \{0, 1, \ldots, n-1\}$. Sean q y k respectivamente el cociente y resto de dividir t por n. Esto es, $t = nq + k$ y $0 \leq k < n$.

Observemos que $k \in \{0, 1, \ldots, n-1\}$. Entonces,

$$\begin{aligned} w_t &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2t\pi}{n}\right) \\ &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2(nq+k)\pi}{n}\right) \\ &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2k\pi}{n}+\frac{2nq\pi}{n}\right) \\ &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2k\pi}{n}+2q\pi\right) \\ &= \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2k\pi}{n}\right) \\ &= w_k \end{aligned}$$

Por lo tanto, hemos probado que $w_k = \sqrt[n]{|z|}.\text{cis}\left(\frac{\arg(z)+2k\pi}{n}\right)$ con $k = 0, 1, \ldots, n-1$ son exactamente todas las raíces n-ésimas de z. ■

Ejemplo 4.32. Hallar todas las raíces cuartas del complejo $z = -1 + \sqrt{3}i$. Primero hallamos el módulo y argumento de z. Tenemos que $|z| = 2$ y $\arg(z) = \frac{2}{3}\pi$ (dejamos los detalles al lector). Ahora, aplicando la fórmula (4.1) obtenemos

$$w_k = \sqrt[4]{2}.\text{cis}\left(\frac{\frac{2}{3}\pi+2k\pi}{4}\right)$$

para $k = 0, 1, 2, 3$. Entonces,

$$\begin{aligned} w_0 &= \sqrt[4]{2}.\text{cis}\left(\frac{\frac{2}{3}\pi+2.0\pi}{4}\right) = \sqrt[4]{2}.\text{cis}\left(\frac{1}{6}\pi\right) = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right) \\ w_1 &= \sqrt[4]{2}.\text{cis}\left(\frac{\frac{2}{3}\pi+2.1\pi}{4}\right) = \sqrt[4]{2}.\text{cis}\left(\frac{2}{3}\pi\right) = \sqrt[4]{2}\left(-\frac{\sqrt{1}}{2}+\frac{\sqrt{3}}{2}i\right) \\ w_2 &= \sqrt[4]{2}.\text{cis}\left(\frac{\frac{2}{3}\pi+2.2\pi}{4}\right) = \sqrt[4]{2}.\text{cis}\left(\frac{7}{6}\pi\right) = \sqrt[4]{2}\left(-\frac{\sqrt{3}}{2}-\frac{1}{2}i\right) \\ w_3 &= \sqrt[4]{2}.\text{cis}\left(\frac{\frac{2}{3}\pi+2.3\pi}{4}\right) = \sqrt[4]{2}.\text{cis}\left(\frac{5}{3}\pi\right) = \sqrt[4]{2}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right). \end{aligned}$$ ■

Sabemos que a todo número complejo z lo podemos representar de forma geométrica, y que el módulo y argumento de z tienen un sentido geométrico preciso. En el caso de las raíces n-ésimas de un complejo z también tenemos una representación geométrica clara.

Representación geométrica de la raíces n-ésimas

Sea $z \in \mathbb{C}$ no nulo y $n \in \mathbb{N}$. Entonces, las n raíces n-ésimas de z representan los n vértices de un polígono regular de n lados inscripto en la circunferencia con centro el origen de coordenadas y radio $\sqrt[n]{|z|}$.

Ejemplo 4.33. En el Ejemplo 4.32 obtuvimos que

$$w_0 = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right), \qquad w_1 = \sqrt[4]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$$
$$w_2 = \sqrt[4]{2}\left(-\frac{\sqrt{3}}{2} - \frac{1}{2}i\right), \qquad w_3 = \sqrt[4]{2}\left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$$

son las cuatro raíces cuartas del complejo $z = -1 + \sqrt{3}i$. Entonces, si representamos en el plano cartesiano estos cuatros complejos w_0, w_1, w_2, w_3 y los unimos por segmentos rectos obtenemos un polígono regular de cuatro lados inscripto en la circunferencia centrada en el origen y con radio $\sqrt[4]{2}$, ver la Figura 4.11.

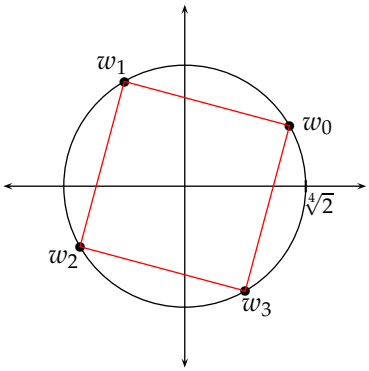

Figura 4.11: Ejemplo 4.33

4.6. Raíces n-ésimas de la unidad

Las **raíces n-ésimas de la unidad**, como el nombre lo indica, son las raíces n-ésimas del complejo unidad $z = 1$, y ellas vienen dadas por la ecuación (ver Teorema 4.31)

$$w_k = \operatorname{cis}\left(\frac{2k\pi}{n}\right)$$

con $k = 0, 1, \ldots, n-1$. Estas raíces se pueden utilizar para hallar todas las raíces n-ésimas de cualquier complejo z a partir de una conocida.

Proposición 4.34

Sea $z \in \mathbb{C}$ no nulo y sea w una raíz n-ésima de z. Si $u_0, u_1, \ldots, u_{n-1}$ son las n raíces n-ésimas de la unidad, entonces las n raíces n-ésimas de z son

$$w.u_0,\ w.u_1,\ \ldots,\ w.u_{n-1}.$$

Demostración. Sólo indicaremos qué debemos probar y dejaremos los detalles al lector. Las hipótesis son que w es una raíz n-ésima de z y $u_0, u_1, \ldots, u_{n-1}$ son las n raíces n-ésimas de la unidad. Debemos probar que $w.u_0, w.u_1, \ldots, w.u_{n-1}$ son exactamente las n raíces n-ésimas de z. Entonces hay que probar que $(w.u_i)^n = z$ para todo $i = 0, 1, \ldots, n-1$, y que si $i, j \in \{0, 1, \ldots, n-1\}$ distintos, entonces $w.u_i \neq w.u_j$. ■

Ejemplo 4.35. Sea $z = -2 - 2\sqrt{3}i$ y supongamos que conocemos una raíz cuarta de z: $w = \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2}i$. Ahora, no es difícil comprobar que $1, -1, i, -i$ son las cuatro raíces cuartas de la unidad. Entonces, las cuatro raíces cuartas de z son:

$$1.w = \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2}i \qquad i.w = -\frac{\sqrt{6}}{2} + \frac{\sqrt{2}}{2}i$$
$$(-1).w = -\frac{\sqrt{2}}{2} - \frac{\sqrt{6}}{2}i \qquad (-i).w = \frac{\sqrt{6}}{2} - \frac{\sqrt{2}}{2}i.$$

Entre las raíces de la unidad de orden n hay algunas que se distinguen por tener ciertas propiedades interesantes. Veamos cuáles son y qué propiedades tienen.

Definición 4.36

Se llama raíz n-ésima **primitiva** de la unidad, a aquellas raíces n-ésimas de la unidad que no son raíces de la unidad de un orden menor que n.

En otras palabras,

Un número complejo u es una raíz n-ésima **primitiva** de la unidad si $u^n = 1$ y $u^k \neq 1$ para todo número natural $k < n$.

Ejemplo 4.37. Comprobemos que $u = \text{cis}\left(\frac{\pi}{4}\right)$ es una raíz octava primitiva de la unidad. Primero comprobamos que u es efectivamente una raíz octava de la unidad:

$$u^8 = \text{cis}\left(8.\frac{\pi}{4}\right) = \text{cis}\,(2\pi) = 1.$$

Ahora verificamos que u no es raíz de la unidad de ningún orden menor que 8, es decir, debemos comprobar que $u^k \neq 1$ para todo $k = 1, 2, \ldots, 7$.

$$u^7 = \text{cis}\left(7.\frac{\pi}{4}\right) \neq 1 \qquad u^4 = \text{cis}\left(4.\frac{\pi}{4}\right) \neq 1$$
$$u^6 = \text{cis}\left(6.\frac{\pi}{4}\right) \neq 1 \qquad u^3 = \text{cis}\left(3.\frac{\pi}{4}\right) \neq 1$$
$$u^5 = \text{cis}\left(5.\frac{\pi}{4}\right) \neq 1 \qquad u^2 = \text{cis}\left(2.\frac{\pi}{4}\right) \neq 1$$

Por lo tanto, $u = \text{cis}\left(\frac{\pi}{4}\right)$ es una raíz octava primitiva de la unidad.

La siguiente proposición nos dice cómo hallar exactamente todas las raíces n-ésimas primitivas de la unidad. ■

Proposición 4.38

Las raíces n-ésimas primitivas de la unidad son:

$$w_k = \text{cis}\left(\frac{2k\pi}{n}\right)$$

con $k = 0, 1, \ldots n-1$ tales que n y k son relativamente primos.

Demostración. Sea $k \in \{0, 1, \ldots, n-1\}$. Ya sabemos que $w_k = \operatorname{cis}\left(\frac{2k\pi}{n}\right)$ es una raíz n-ésima de la unidad. Debemos probar que w_k es primitiva si y sólo si $(n, k) = 1$.

$\Leftarrow$) Supongamos que $(n, k) = 1$. Vamos a probar que w_k no es raíz de la unidad de ningún orden menor que n. Sea $0 < t < n$. Supongamos por absurdo que w_k es raíz de la unidad de orden t, es decir, que $w_k^t = 1$. Entonces,

$$\begin{aligned} w_k^t &= 1 \\ \operatorname{cis}\left(\frac{2kt\pi}{n}\right) &= \operatorname{cis}(0) \\ \frac{2kt\pi}{n} &= 2q\pi \\ kt &= qn. \end{aligned}$$

Luego, $n \mid kt$. Como $(n, k) = 1$, entonces $n \mid t$. Absurdo, pues $t < n$. Por lo tanto, $w_k^t \neq 1$ para todo $t = 0, 1, \ldots, n-1$. Esto es, w_k es una raíz primitiva n-ésima de la unidad.

$\Rightarrow$) Supongamos que w_k es una raíz primitiva n-ésima de la unidad. Debemos probar que $(n, k) = 1$. Supongamos que $(n, k) \neq 1$. Entonces, existe un entero primo positivo p tal que $p \mid n$ y $p \mid k$. Así, existen $a, b \in \mathbb{Z}$ tales que $n = a.p$ y $k = b.p$. Observemos que $a < n$. Ahora, reemplazando obtenemos que

$$w_k = \operatorname{cis}\left(\frac{2k\pi}{n}\right) = \operatorname{cis}\left(\frac{2bp\pi}{ap}\right) = \operatorname{cis}\left(\frac{2b\pi}{a}\right).$$

Con lo cual $w_k^a = 1$, es decir, que w_k es también raíz de la unidad de orden a y $a < n$. Esto contradice el hecho que w_k es primitiva de orden n. Por lo tanto, $(n, k) = 1$. ■

Ejemplo 4.39. Hallemos todas las raíces primitivas octavas de la unidad. Notemos que los $k = 0, 1, \ldots, 7$ que son relativamente primos con 8 son $k = 1, 3, 5, 7$. Entonces, las raíces octavas primitivas de la unidad son:

$$w_k = \operatorname{cis}\left(\frac{2k\pi}{8}\right) \qquad \text{con } k = 1, 3, 5, 7.$$

Estas son:

$$u_1 = \operatorname{cis}\left(\frac{1}{4}\pi\right) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \qquad u_5 = \operatorname{cis}\left(\frac{5}{4}\pi\right) = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

$$u_3 = \operatorname{cis}\left(\frac{3}{4}\pi\right) = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \qquad u_7 = \operatorname{cis}\left(\frac{7}{4}\pi\right) = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.$$

Proposición 4.40

Si u es una raíz n-ésima primitiva de la unidad, entonces $1, u, u^2, \ldots, u^{n-1}$ son las n raíces n-ésimas de la unidad.

Demostración. A cargo del lector. Sugerencia: teniendo como hipótesis que u es una raíz n-ésima primitiva de la unidad, hay que probar que $1, u, u^2, \ldots, u^{n-1}$ son exactamente las n raíces n-ésimas de la unidad. Para ello hay que probar dos cosas: (1) que $(u^i)^n = 1$ para todo $i \in \{0, 1, \ldots, n-1\}$; (2) para todos $i, j \in \{0, 1, \ldots, n-1\}$ distintos, $u^i \neq u^j$. ■

Sea $n \in \mathbb{N}$. Definimos el siguiente conjunto:

$$G_n = \{w \in \mathbb{C} : w^n = 1\} = \left\{ \text{cis}\left(\frac{2k\pi}{n}\right) : 0 \leq k \leq n-1 \right\}.$$

Esto es, G_n es el conjunto formado por todas las raíces n-ésimas de la unidad. Por ejemplo,

$$\begin{aligned}
G_1 &= \{\text{cis}\,(0)\} = \{1\} \\
G_2 &= \{\text{cis}\left(\frac{2k\pi}{2}\right) : k = 0, 1\} = \{1, -1\} \\
G_3 &= \{\text{cis}\left(\frac{2k\pi}{3}\right) : k = 0, 1, 2\} = \left\{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\right\} \\
G_4 &= \{\text{cis}\left(\frac{2k\pi}{4}\right) : k = 0, 1, 2, 3\} = \{1, -1, i, -i\}.
\end{aligned}$$

A continuación veremos que los conjuntos G_n satisfacen ciertas propiedades.

Proposición 4.41

Sea $n \in \mathbb{N}$. Entonces:

1. Si $w, v \in G_n$, entonces $w.v \in G_n$.
2. $\forall w \in G_n$, $w^{-1} \in G_n$.
3. $\forall w \in G_n$, $w^{-1} = \overline{w} = w^{n-1}$.
4. Si $w \in G_n$ y $n \mid m$, entonces $w \in G_m$.
5. Si $n \mid m$, entonces $G_n \subseteq G_m$.
6. $G_n \cap G_m = G_{(n,m)}$.

Antes de probar las propiedades anteriores, veamos que nos están diciendo. La propiedad 1. nos dice que el producto de dos raíces n-ésimas de la unidad, es una raíz n-ésima de la unidad. La propiedad 2. nos dice que si w es una raíz n-ésima de la unidad, entonces su inverso w^{-1} es también una raíz n-ésima de la unidad. La propiedad 3. nos dice que para las raíces n-ésimas de la unidad, su inverso coincide con su conjugado (y con la potencia a la $n-1$). Las propiedades 4. y 5. nos dicen, de dos formas distintas, que toda raíz de orden n de la unidad es también una raíz de orden m de la unidad, para todo múltiplo m de n. Finalmente, la propiedad 6. quiere decir que w es a la vez raíz n-ésima y m-ésima de la unidad si y sólo si w es raíz de orden (n, m) de la unidad, donde (n, m) es el máximo común divisor de n y m.

Demostración. A cargo del lector. ■

Ejercicios propuestos

Ejercicio 4.1. Completar las demostraciones de las propiedades enunciadas en la Proposición 4.3.

Ejercicio 4.2. Completar las demostraciones de las propiedades enunciadas en la Proposición 4.4.

Ejercicio 4.3. Demostrar la Proposición 4.6.

Ejercicio 4.4. Escribir en forma binómica los siguientes números complejos.

(a) $i^{18} - 3i^7 + i^2(1 - i^4) - (-i)^{26}$.

Ejercicio 4.5. Determinar la parte real e imaginaria de los siguientes números complejos.

(a) i. (b) $\frac{1}{i}$. (c) $\frac{1}{1-i}$. (d) $\frac{1+i}{1-i}$.

Ejercicio 4.6. Probar que las siguientes identidades se cumplen para todo par de números complejos z y w.

(a) $\mathrm{Re}(z+w) = \mathrm{Re}(z) + \mathrm{Re}(w)$.

(b) $\mathrm{Im}(z+w) = \mathrm{Im}(z) + \mathrm{Im}(w)$.

(c) $\mathrm{Re}(zw) = \mathrm{Re}(z)\mathrm{Re}(w) - \mathrm{Im}(z)\mathrm{Im}(w)$.

(d) $\mathrm{Im}(zw) = \mathrm{Re}(z)\mathrm{Im}(w) + \mathrm{Im}(z)\mathrm{Re}(w)$.

Ejercicio 4.7. Calcular las potencias sucesivas de i y establecer una regla que permita obtener el valor de i^n para cada entero positivo n.

Ejercicio 4.8. Probar las propiedades de la Proposición 4.14.

Ejercicio 4.9. Probar las propiedades 1., 2., 3. y 4. de la Proposición 4.17.

Ejercicio 4.10. Probar la Proposición 4.34.

Ejercicio 4.11. Probar las propiedades de la Proposición 4.41.

Capítulo 5

Polinomios

No se limite sólo a leerlo. Haga sus propias preguntas, busque sus propios ejemplos [...].
—-Paul R. Halmos

5.1. Definiciones

En esta sección daremos una definición clásica y semiformal de *polinomio* que podemos encontrar en la mayoría de los textos básicos de álgebra. Decimos que es semiformal porque hay ciertos aspectos de la definición que no están completamente bien definidos, sino que están entendidos de una forma intuitiva. La definición completamente formal de polinomio lleva un poco más de tiempo y espacio introducirla, y no es del todo adecuada o ideal para trabajar con polinomios de forma práctica. Es por eso que elegimos presentar la definición clásica en lugar de una definición completamente formal. El lector interesado en estudiar una definición formal de polinomio puede dirigirse a [3, 2, 1].

A lo largo de todo el capítulo K denotará o bien el conjunto $\mathbb{Q}$ de números racionales, o el conjunto $\mathbb{R}$ de números reales, o bien el conjunto $\mathbb{C}$ de números complejos.

Definición 5.1

Un **polinomio con coeficientes en** K es una expresión formal de la forma

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

donde $n \in \mathbb{N} \cup \{0\}$, X es una **indeterminada** en K, para cada $i = 0, 1, \ldots, n$, $a_i \in \mathrm{K}$ y son llamados los **coeficientes** del polinomio.

Denotaremos por $\mathrm{K}[X]$ al conjunto de todos los polinomios con coeficientes en K.

Ejemplo 5.2.

1. $f(X) = 2X^3 - X^2 + 3$ es un polinomio con coeficientes en $\mathbb{Q}$. Así $f(X) \in \mathbb{Q}[X]$. También es claro que $f(X) \in \mathbb{R}[X]$ y $f(X) \in \mathbb{C}[X]$.

2. $g(X) = -X^4 + \sqrt{2}X^2 + 2X - 1$ es un polinomio con coeficientes reales, esto es, $g(X) \in \mathbb{R}[X]$. Pero $g(X) \notin \mathbb{Q}[X]$, pues uno de sus coeficientes no es racional. También, debido a que todos los coeficientes de $g(X)$ son obviamente números complejos, tenemos que $g(X) \in \mathbb{C}[X]$.

3. El polinomio $p(X) = X^2 + i$ es tal que $p(X) \in \mathbb{C}[X]$, pero $p(X) \notin \mathbb{Q}[X]$ y $p(X) \notin \mathbb{R}[X]$.

Observación 5.3. Teniendo en cuenta que $\mathbb{Q} \subseteq \mathbb{R}$, tenemos que si $f(X)$ es un polinomio con coeficientes en $\mathbb{Q}$, entonces $f(X)$ es también un polinomio con coeficientes reales. Entonces, $\mathbb{Q}[X] \subseteq \mathbb{R}[X]$. Análogamente, teniendo en cuenta que $\mathbb{R} \subseteq \mathbb{C}$, tenemos que si $f(X)$ es un polinomio con coeficientes reales, entonces todos los coeficientes de $f(X)$ son también complejos, es decir, $f(X)$ es también un polinomio con coeficientes complejos. Entonces $\mathbb{R}[X] \subseteq \mathbb{C}[X]$. Por lo tanto,

$$\mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X].$$

Para poder trabajar con polinomios necesitamos introducir algunas definiciones básicas. Diremos que un polinomio $f(X) = a_n X^n + a_{n-1}X^{n-1} \cdots + a_1 X + a_0$ es **no nulo** si al menos uno de los coeficientes a_i es no nulo (distinto de 0). El polinomio nulo es aquel que tiene todos sus coeficientes nulos, y lo denotaremos simplemente por 0. También, a menudo por comodidad denotaremos a un polinomio $f(X)$ simplemente por f. Es decir que $f = f(X)$.

Definición 5.4

Sea $f(X) = a_n X^n + a_{n-1}X^{n-1} \cdots + a_1 X + a_0$ un polinomio no nulo con $a_n \neq 0$. Entonces:

- n es llamado el **grado** de $f(X)$ y lo denotaremos por $\text{gr}(f)$. Esto es, $\text{gr}(f) = n$.
- a_n es llamado el **coeficiente principal** de $f(X)$, y lo denotaremos por $\text{cp}(f)$.
- a_0 es llamado el **término independiente** de $f(X)$, y lo denotaremos por $\text{ti}(f)$.

Según a la definición anterior estamos considerando que el polinomio nulo $f = 0$ no tiene grado. El grado de un polinomio no nulo es la mayor potencia de la indeterminada X cuyo coeficientes es distinto de cero. Y este coeficiente es el coeficiente principal del polinomio.

Problema 5.5

Determinar el grado, el coeficiente principal y el término independiente del polinomio $f(X) = -3X^5 + \sqrt{3}X^2 - X - 4$. Indicar si $f(X)$ pertenece o no a los conjuntos $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

Definición 5.6

Dos polinomios

$$f(X) = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0$$

y

$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$$

son **iguales** si y sólo si $n = m$, y $a_i = b_i$ para todo $i = 0, 1, \ldots, n = m$.

Problema 5.7

¿Para qué valores de a, b y c son iguales los siguientes polinomios?

$p(X) = cX^5 - 6X^3 - 2X^2 + X - b + 3$ y $q(X) = -3X^5 + 2aX^3 - 2X^2 + X + 7$.

A los polinomios de la forma $f(X) = a_0$ (esto es, la indeterminada X no aparece en el polinomio, o en otras palabras, todos los coeficientes a_i de los términos X^i con $i > 0$ son cero) los llamaremos **polinomios constantes** de $\mathrm{K}[X]$. Por ejemplo, $f(X) = \frac{1}{2}$ y $g(X) = -\sqrt{2}$ son polinomios constantes de $\mathbb{R}[X]$. Es importante notar que un polinomio $f(X)$ es constante si y sólo si $f(X) = 0$ o $\mathrm{gr}(f) = 0$. Llamaremos **polinomio mónico** a todo polinomio cuyo coeficiente principal es 1. Esto es, $f(X)$ es mónico si y sólo si $\mathrm{cp}(f) = 1$.

5.2. Suma y producto de polinomios

En esta sección definiremos dos operaciones sobre el conjunto $\mathrm{K}[X]$ de polinomios con coeficientes en K. Estas dos operaciones son la suma y el producto de polinomios.

En ciertas ocasiones, como en la definición siguiente, es útil tener en cuenta la siguiente observación. Tomemos dos polinomios $f(X) = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0$ y $g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$. Si $n > m$, entonces podemos completar el polinomio $g(X)$ con coeficientes nulos hasta tener el términos n-ésimo:

$$g(X) = b_n X^n + \cdots + b_{m+1} X^{m+1} + b_m X^m + \cdots + b_a X + b_0$$

donde $b_n = b_{n-1} = \cdots = b_{m+1} = 0$. Por lo tanto, cuando sea necesario, podremos tomar dos polinomios de la forma $f(X) = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0$ y $g(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$. El lector debe notar que no estamos afirmando que $f(X)$ o $g(X)$ tengan grado n, pues no sabemos si $a_n \neq 0$ o $b_n \neq 0$.

Definición 5.8: Suma

Sean $f(X) = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0$ y $g(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$ dos polinomios. Definimos la **suma de polinomios** $f + g$ como sigue:

$$(f + g)(X) = (a_n + b_n) X^n + (a_{n-1} + b_{n-1}) X^{n-1} + \cdots + (a_1 + b_1) X + (a_0 + b_0).$$

Esto es, los coeficientes del polinomio suma $f+g$ se obtienen sumando correspondientemente los coeficientes de los términos semejantes de $f(X)$ y $g(X)$.

Ejemplo 5.9. Hay varios métodos o procedimientos prácticos para sumar polinomios, el lector lo hará de la forma que le sea más cómoda. Sean

$$f(X) = -2X^3 + 3X - 1 \qquad \text{y} \qquad g(X) = X^5 - X^4 + 2X^2 + 6X - 7.$$

Entonces,

$$\begin{aligned}(f+g)(X) &= (0+1)X^5 + (0-1)X^4 + (-2+0)X^3 + (0+2)X^2 + (3+6)X + (-1-7)\\ &= X^5 - X^4 - 2X^3 + 2X^2 + 9X - 8.\end{aligned}$$

Veamos a continuación que la suma de polinomios satisface propiedades análogas a las propiedades de la suma en los enteros.

Proposición 5.10

Sean $f, g, h \in \mathrm{K}[X]$.

- **Asociativa:** $f + (g+h) = (f+g) + h$.
- **Conmutativa:** $f + g = g + f$.
- **Elemento neutro:** El polinomio nulo 0 cumple que $0 + f = f$.
- **Opuesto:** Para cada $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathrm{K}[X]$, existe el polinomio $-f(X) = (-a_n)X^n + \cdots + (-a_1)X + (-a_0)$ tal que $f + (-f) = 0$.

Demostración. Sean $f(X) = a_n X^n + \cdots + a_1 X + a_0$, $g(X) = b_n X^n + \cdots + b_1 X + b_0$ y $h(X) = c_n X^n + \cdots + c_1 X + c_0$. Entonces:
Asociativa: Calculamos $f + (g+h)$ por un lado, y por otro $(f+g) + h$.

$$\begin{aligned}g + h &= (b_n + c_n)X^n + \cdots + (b_1 + c_1)X + (b_0 + c_0)\\ f + (g+h) &= (a_n + (b_n + c_n))X^n + \cdots + (a_1 + (b_1 + c_1))X + (a_0 + (b_0 + c_0)),\end{aligned}$$

y

$$\begin{aligned}f + g &= (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0)\\ (f+g) + h &= ((a_n + b_n) + c_n)X^n + \cdots + ((a_1 + b_1) + c_1)X + ((a_0 + b_0) + c_0).\end{aligned}$$

Como todos los coeficientes $a_i, b_i, c_i \in \mathrm{K}$ para todo i, y K es o bien $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, sabemos que la suma en cualquiera de esos conjuntos es asociativa. Entonces, para cada $i = 0, 1, \ldots, n$, tenemos que $a_i + (b_i + c_i) = (a_i + b_i) + c_i$. Luego, todos los coeficientes del polinomio $f + (g+h)$ coinciden correspondientemente con los coeficientes del polinomio $(f+g) + h$. Por lo tanto, $f + (g+h) = (f+g) + h$.

Conmutativa: Como la suma en K es conmutativa, tenemos que

$$\begin{aligned} f+g &= (a_n+b_n)X^n+\cdots+(a_1+b_1)X+(a_0+b_0)\\ &= (b_n+a_n)X^n+\cdots+(b_1+a_1)X+(b_0+a_0)\\ &= g+f. \end{aligned}$$

Elemento neutro: Recuerde que el polinomio nulo 0 es aquel que tiene todos sus coeficientes ceros. Entonces,

$$0+f=(0+a_n)X^n+\cdots+(0+a_1)X+(0+a_0)=a_nX^n+\cdots+a_1X+a_0=f.$$

Opuesto:

$$\begin{aligned} f+(-f) &= (a_n+(-a_n))X^n+\cdots+(a_1+(-a_1))X+(a_0+(-a_0))\\ &= (a_n-a_n)X^n+\cdots+(a_1-a_1)X+(a_0-a_0)\\ &= 0X^n+\cdots+0X+0\\ &= 0 \end{aligned}$$ ■

Ahora pasamos a definir el producto de polinomios. En la práctica, multiplicar polinomios es simplemente aplicar la propiedad distributiva, sumar términos semejantes y usar las propiedades de las potencias. Por ejemplo,

$$\begin{aligned} (X^3-2X)(2X^2+X+5) &= X^3.2X^2+X^3.X+X^3.5+(-2X).2X^2+(-2X).X+(-2X).5\\ &= 2X^5+X^4+5X^3-4X^3-2X^2-10X\\ &= 2X^5+X^4+X^3-2X^2-10X. \end{aligned}$$

Para dar una definición correcta y sin ambigüedad, debemos ser más formales.

Definición 5.11: Producto

Sean $f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$ y $g(X)=b_mX^m+b_{m-1}X^{m-1}+\cdots+b_1X+b_0$ dos polinomios de K$[X]$. Definimos el **producto de polinomios** $f.g$ como sigue:

$$f.g=c_{n+m}X^{n+m}+c_{n+m-1}X^{n+m-1}+\cdots+c_kX^k+\cdots+c_1X+c_0$$

donde para cada $k=0,1,\ldots,n+m-1,n+m$,

$$c_k=a_kb_0+a_{k-1}b_1+a_{k-2}b_2+\cdots+a_2b_{k-2}+a_1b_{k-1}+a_0b_k.$$

Veamos un poco más de cerca esta definición. Observemos que los coeficientes c_k del polinomio producto $f.g$ se obtienen sumando los productos a_ib_j siempre que $i+j=k$. Utilizando sumatorias podemos escribir

$$c_k=\sum_{i+j=k}a_ib_j.$$

Veamos como ejemplo algunos coeficientes del producto $f.g$:

$$\begin{aligned} c_0 &= a_0b_0 \\ c_1 &= a_1b_0 + a_0b_1 \\ c_2 &= a_2b_0 + a_1b_1 + a_0b_2 \\ c_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ \vdots &= \quad \vdots \end{aligned}$$

Hay varias formas o procedimientos para obtener el polinomio producto $f.g$. Es poco práctico tratar de aplicar la definición de producto de polinomios que dimos recién para hallar el polinomio producto $f.g$. Veremos en el ejemplo siguiente un procedimiento más directo para realizar productos de polinomios.

Ejemplo 5.12. Sean

$$f(X) = -2X^3 + 3X - 1 \qquad \text{y} \qquad g(X) = X^5 - X^4 + 2X^2 + 6X - 7.$$

Entonces, procedemos como sigue

$g =$	X^5	-	X^4	+		+	$2X^2$	+	$6X$	-	7									
$f =$				-	$2X^3$	+		+	$3X$	-	1									
$(-2X^3).g =$	$-2X^8$	+	$2X^7$	+		-	$4X^5$	-	$12X^4$	+	$14X^3$									
$(3X).g =$					$3X^6$	-	$3X^5$	+		+	$6X^3$	+	$18X^2$	-	$21X$					
$(-1).g =$						-	X^5	+	X^4	+		-	$2X^2$	-	$6X$	+	7			
Suma	$-2X^8$	+	$2X^7$	+	$3X^6$	-	$8X^5$	-	$11X^4$	+	$20X^3$	+	$16X^2$	-	$27X$	+	7			

Por lo tanto,

$$(f.g)(X) = -2X^8 + 2X^7 + 3X^6 - 8X^5 - 11X^4 + 20X^3 + 16X^2 - 27X + 7.$$

El lector interesado puede aplicar la Definición 5.11, para hallar cada uno de los coeficientes c_k del polinomio producto $f.g$ y comprobar que efectivamente se obtiene el polinomio anterior.

Proposición 5.13

Sea $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathrm{K}[X]$ y sea $b \in \mathrm{K}$. Entonces

$$b.f(X) = (ba_n)X^n + \cdots + (ba_1)X + (ba_0).$$

Demostración. Recordemos que b es un polinomio constante, es decir, que todos los coeficientes de los términos X^i con $i > 0$ son cero, y el término independiente es el mismo b. Entonces, asumiendo que $b_m, \ldots, b_1, b_0$ son los coeficientes del polinomio constante b, tenemos que $b_m = \cdots = b_1 = 0$ y $b_0 = b$. Luego, para cada $k = 0, 1, \ldots, n + m$, nos queda que

$$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_1b_{k-1}a_0b_k = a_kb + a_{k-1}0 + \cdots + a_10 + a_00 = a_kb$$

Entonces, para cada $k = 0, 1, \ldots, n+m$, tenemos que $c_k = a_k b$. Con lo cual,

$$b.f(X) = (a_{n+m}b)X^{n+m} + \cdots + (a_k b)X^k + \cdots + (a_1 b)X + (a_0 b).$$

Ahora bien, los coeficiente a_k que no son necesariamente cero son $a_0, a_1, \ldots, a_n$, el resto $a_{n+1}, \ldots, a_{n+m}$ son iguales a cero. Por lo tanto,

$$b.f(X) = (a_n b)X^n + \cdots + (a_1 b)X + (a_0 b) = (ba_n)X^n + \cdots + (ba_1)X + (ba_0). \quad \blacksquare$$

Ejemplo 5.14. Sea $g(X) = X^5 - X^4 + 2X^2 + 6X - 7$. Entonces

$$\frac{1}{2}g(X) = \frac{1}{2}X^5 - \frac{1}{2}X^4 + X^2 + 3X - \frac{7}{2}. \quad \blacksquare$$

Proposición 5.15

Sean $f, g, h \in \mathrm{K}[X]$.

- **Asociativa:** $f.(g.h) = (f.g).h$.
- **Conmutativa:** $f.g = g.f$.
- **Elemento neutro:** El polinomio constante 1 cumple que $1.f = f$.
- **Distributiva:** $f.(g+h) = f.g + f.h$.

Demostración. Las demostraciones de las propiedades asociativa y distributiva no son difíciles pero si muy tediosas, así que omitiremos sus pruebas y las dejamos a cargo del lector interesado. Las propiedades conmutativa y elemento neutro son consecuencia directa de la definición de producto y de las propiedades del producto en K. Dejamos estas pruebas a cargo del lector. $\blacksquare$

Proposición 5.16

Sean $p(X)$ y $q(X)$ dos polinomios no nulos de $\mathrm{K}[X]$. Entonces:

(1) $\mathrm{cp}(p.q) = \mathrm{cp}(p).\mathrm{cp}(q)$.

(2) $\mathrm{gr}(p+q) \leq \mathrm{gr}(p) + \mathrm{gr}(q)$.

(3) $\mathrm{gr}(p.q) = \mathrm{gr}(p) + \mathrm{gr}(q)$.

Demostración. Sean $p(X) = a_n X^n + \cdots + a_1 X + a_0$ y $q(X) = b_m X^m + \cdots + b_1 X + b_0$ dos polinomios tales que $a_n \neq 0$ y $b_m \neq 0$.

Por la Definición 5.11 del producto de polinomio tenemos que

$$(p.q)(X) = c_{n+m}X^{n+m} + c_{n+m-1}X^{n+m-1} + \cdots + c_k X^k + \cdots + c_1 X + c_0$$

donde para cada $k = 0, 1, \ldots, n+m-1, n+m$,

$$c_k = a_k b_0 + a_{k-1}b_1 + a_{k-2}b_2 + \cdots + a_2 b_{k-2} + a_1 b_{k-1} + a_0 b_k.$$

Como $a_n \neq 0$ y $b_m \neq 0$, obtenemos que el coeficiente $c_{n+m} = a_n b_m \neq 0$. Con lo cual,

$$\text{gr}(p.q) = n + m = \text{gr}(p) + \text{gr}(q) \qquad \text{y} \qquad \text{cp}(p.q) = c_{n+m} = a_n b_m = \text{cp}(p).\text{cp}(q).$$

Esto prueba (1) y (3).

Para probar (2) vamos a considerar varios casos.

Caso 1: Si $n < m$ (análogamente si $m > n$), entonces

$$(p+q)(X) = b_m X^m + \cdots + b_{n+1} X^{n+1} + (a_n + b_n) X^n + \cdots + (a_1 + b_1) X + (a_0 + b_0).$$

Con lo cual, como $b_m \neq 0$, tenemos que $\text{gr}(p+q) = m = \text{máx}\{\text{gr}(p), \text{gr}(q)\}$.

Caso 2: Si $n = m$ y $a_n + b_m \neq 0$, entonces

$$(p+q)(X) = (a_n + b_n) X^n + \cdots + (a_1 + b_1) X + (a_0 + b_0).$$

Luego, ya que $a_n + b_m \neq 0$, tenemos que $\text{gr}(p+q) = n = \text{máx}\{\text{gr}(p), \text{gr}(q)\}$.

Caso 3: Si $n = m$ y $a_n + b_m = 0$, entonces

$$(p+q)(X) = (a_{n-1} + b_{n-1}) X^{n-1} + \cdots + (a_1 + b_1) X + (a_0 + b_0).$$

Luego, $\text{gr}(p+q) \leq n - 1 < n = \text{máx}\{\text{gr}(q), \text{gr}(q)\}$[1]. En cualquiera de los tres casos, obtenemos que $\text{gr}(p+q) \leq \text{máx}\{\text{gr}(q), \text{gr}(p)\}$. Por lo tanto, se cumple (2). ■

Observación 5.17. La condición (3) de la Proposición 5.16 nos esta diciendo de forma implícita que si p y q son dos polinomios no nulos, entonces el polinomio producto $p.q$ es no nulo, porque podemos calcular su grado y este es $\text{gr}(p.q) = \text{gr}(p) + \text{gr}(q)$. Enunciaremos esto en la siguiente proposición.

Proposición 5.18

Sean $f(X)$, $g(X)$ y $h(X)$ polinomios en K[X]. Si $f.g = 0$, entonces $f = 0$ o $g = 0$.

Demostración. Asumamos que $f.g = 0$. Es decir, que $(f.g)(X)$ es el polinomio nulo. Ahora supongamos, por absurdo, que $f \neq 0$ y $g \neq 0$. Entonces, $\text{gr}(f) \geq 0$ y $\text{gr}(g) \geq 0$. Por la Proposición 5.16, tenemos que $\text{gr}(f.g) = \text{gr}(f) + \text{gr}(g) \geq 0$. Esto contradice el hecho que $f.g = 0$. Por lo tanto, $f = 0$ o $g = 0$. ■

Problema 5.19

Sean $f(X)$, $g(X)$ y $h(X)$ polinomios en K[X]. Probar que si $h \neq 0$ y $f.h = g.h$, entonces $f = g$.

5.3. Divisibilidad en K[X]

En la sección anterior definimos las operaciones de suma y producto entre polinomios y vimos que tenían las mismas propiedades que la suma y el producto de números enteros. En

[1] No podemos afirmar que $\text{gr}(p+q) = n - 1$ porque no sabemos si $a_{n-1} + b_{n-1} \neq 0$ o $a_{n-1} + b_{n-1} = 0$.

esta sección presentaremos ciertos conceptos definidos sobre polinomios que son análogos a aquellos dados para enteros. Desarrollaremos una teoría similar al caso de los números enteros pero para polinomios.

Definición 5.20

Sean $f(X)$ y $g(X)$ polinomios en $\mathrm{K}[X]$. Diremos que $f(X)$ **divide** a $g(X)$, y lo denotamos por $f(X) \mid g(X)$, si existe un polinomio $h(X) \in \mathrm{K}[X]$ tal que $g(X) = f(X).h(X)$.

Ejemplo 5.21. El polinomio $f(X) = X - 1$ divide al polinomio $g(X) = X^3 - X^2 + X - 1$, porque existe el polinomio $h(X) = X^2 + 1$ tal que $g(X) = f(X).h(X)$, dejamos esta comprobación a cargo del lector.

Problema 5.22

¿El polinomio $f(X) = X + 1$ divide al polinomio $g(X) = X^2 - 1$? Y ¿$f(X)$ divide a $h(X) = X^2 + X + 1$?

Veamos algunas propiedades básicas de la relación divide sobre $\mathrm{K}[X]$. Observe que estas propiedades son similares a las propiedades que tiene la relación divide definida sobre el conjunto de los números enteros.

Proposición 5.23

Sean $f(X), g(X), h(X) \in \mathrm{K}[X]$. Entonces:

1. $f \mid f$.
2. Si $f \mid g$ y $g \mid h$, entonces $f \mid h$.
3. Si $f \mid g$ y $f \mid h$, entonces $f \mid (a.g + b.h)$, para cualesquiera polinomios $a(X), b(X) \in \mathrm{K}[X]$.

Demostración. Las demostraciones de estas propiedades son análogas a aquellas propiedades de la relación divide sobre el conjunto de números enteros $\mathbb{Z}$, ver las pruebas de la Proposición 3.5. Dejamos las demostraciones a cargo del lector. ■

Teorema 5.24: Teorema de la División en $\mathrm{K}[X]$

Si $f(X)$ y $g(X)$ son dos polinomios de $\mathrm{K}[X]$ con $f(X) \neq 0$, entonces existen dos únicos polinomios $q(X)$ y $r(X)$ de $\mathrm{K}[X]$, llamados el **cociente** y **resto**, respectivamente, tales que

$$g(X) = f(X).q(X) + r(X) \quad \text{y} \quad r(X) = 0 \text{ o } \mathrm{gr}(r) < \mathrm{gr}(f).$$

Demostración. La demostración de este teorema es muy similar a la demostración del Teorema de la División en $\mathbb{Z}$. Dejamos los detalles de la prueba en el Apéndice para el lector interesado. ■

Con respecto al teorema anterior, hay que tener en cuenta dos detalles importantes. Primero: los polinomios $q(X)$ y $r(X)$ son los únicos dos que cumplen las dos condiciones del teorema. Así que no importa cómo los hallemos, si ellos efectivamente cumplen que $g(X) = f(X).q(X) + r(X)$ y $r(X) = 0$ o $\text{gr}(r) < \text{gr}(f)$, entonces $q(X)$ y $r(X)$ son respectivamente el cociente y resto de dividir $g(X)$ por $f(X)$. Segundo: el cociente y resto de dividir $g(X)$ por $f(X)$ pertenecen al mismo conjunto K[X] donde pertenecen $f(X)$ y $g(X)$. En el contexto del teorema anterior, diremos que $q(X)$ y $r(X)$ son, respectivamente, el cociente y resto de dividir $g(X)$ por $f(X)$.

Problema 5.25

(a) Justificar por qué $q(X) = X^2 - 2X + 1$ y $r(X) = 2X^2 + 1$ son, respectivamente, el cociente y resto de dividir $g(X) = X^5 - 2X^4 + 6X^2 - 5X + 3$ por el polinomio $f(X) = X^3 - X + 2$.

(b) ¿Son los polinomios $X^3 - X + 2$ y $2X^2 + 1$ el cociente y resto, respectivamente, de dividir $X^5 - 2X^4 + 6X^2 - 5X + 3$ por $X^2 - 2X + 1$?

En los siguientes dos ejemplos presentaremos dos procedimientos para hallar el cociente y resto de la división entre dos polinomios. El primer procedimiento sirve para para cualesquiera dos polinomios $f(X) \neq 0$ y $g(X)$, y el segundo procedimiento para algunos casos particulares, pero que será de gran utilidad en lo que sigue del capítulo.

Ejemplo 5.26 (División larga). Sea $f(X) = X^2 - 2X$ y $g(X) = X^4 - 3X^2 + 1$. Vamos a encontrar el cociente y resto de dividir $g(X)$ por $f(X)$. Llamaremos a $f(X)$ el divisor y a $g(X)$ el dividendo. Vamos a proceder paso a paso

Paso 1: Escribimos el dividendo y el divisor.

$$\begin{array}{llllll} X^4 & - & 3X^2 & + & 1 & \big| \; X^2 - 2X \end{array}$$

Paso 2: Multiplicamos el divisor por X^2 y anotamos el resultado debajo del dividendo

$$\begin{array}{llllll} X^4 & & - \; 3X^2 & + & 1 & \big| \; X^2 - 2X \\ X^4 & - \; 2X^3 & & & & \quad X^2 \end{array}$$

Paso 3: Restamos el dividendo por el resultado de multiplicar X^2 por el divisor.

$$\begin{array}{llllll} X^4 & & - \; 3X^2 & + & 1 & \big| \; X^2 - 2X \\ \underline{X^4} & \underline{- \; 2X^3} & & & & \quad X^2 \\ & 2X^3 & - \; 3X^2 & + & 1 & \end{array}$$

Paso 4: Ahora multiplicamos el divisor por $2X$ y anotamos el resultado debajo del resultado anterior.

$$\begin{array}{llllll} X^4 & & - \; 3X^2 & + & 1 & \big| \; X^2 - 2X \\ \underline{X^4} & \underline{- \; 2X^3} & & & & \quad X^2 + 2X \\ & 2X^3 & - \; 3X^2 & + & 1 & \\ & 2X^3 & - \; 4X^2 & & & \end{array}$$

Paso 5: Volvemos a restar.

$$\begin{array}{rl|l} & X^4 - 3X^2 + 1 & X^2-2X \\ - & X^4 - 2X^3 & \hline & \hline 2X^3 - 3X^2 + 1 & X^2+2X \\ - & 2X^3 - 4X^2 & \hline & \hline X^2 + 1 & \end{array}$$

Paso 6: Multiplicamos el divisor por 1 y anotamos el resultado debajo de la resta anterior.

$$\begin{array}{rl|l} & X^4 - 3X^2 + 1 & X^2-2X \\ - & X^4 - 2X^3 & \hline & \hline 2X^3 - 3X^2 + 1 & X^2+2X+1 \\ - & 2X^3 - 4X^2 & \hline & \hline X^2 + 1 & \\ & X^2 - 2X & \end{array}$$

Paso 7: Restamos nuevamente.

$$\begin{array}{rl|l} & X^4 - 3X^2 + 1 & X^2-2X \\ - & X^4 - 2X^3 & \hline & \hline 2X^3 - 3X^2 + 1 & X^2+2X+1 \\ - & 2X^3 - 4X^2 & \hline & \hline X^2 + 1 & \\ - & X^2 - 2X & \hline & \hline 2X + 1 & \end{array}$$

Aquí detenemos el procedimiento porque el último resultado obtenido $2X+1$ es un polinomio de grado 1 menor que el grado del divisor $f(X) = X^2 - 2X$. Entonces, obtenemos que $q(X) = X^2 + 2X + 1$ es el cociente y $r(X) = 2X + 1$ es el resto. El lector puede comprobar que efectivamente $q(X)$ y $r(X)$ verifican las condiciones $g(X) = f(X)q(X) + r(X)$ y $\mathrm{gr}(r) < \mathrm{gr}(f)$.

Ejemplo 5.27. Determinar el cociente y resto de dividir el polinomio $g(X) = 2X^4 - X^3 - 2$ por el polinomio $f(X) = 2X^2 + X + 1$. Aplicamos el algoritmo de la división larga:

$$\begin{array}{rl|l} & 2X^4 - X^3 - 2 & 2X^2+X+1 \\ - & 2X^4 + X^3 + X^2 & \hline & \hline - 2X^3 - X^2 - 2 & X^2-X \\ - & -2X^3 - X^2 - X & \hline & \hline X - 2 & \end{array}$$

Por lo tanto, el cociente es $q(X) = X^2 - X$ y el resto es $r(X) = X - 2$.

El siguiente procedimiento para realizar la división entre polinomios sirve sólo si el divisor es un polinomio de la forma $X - a$.

Ejemplo 5.28 (Regla de Ruffini). Consideremos hallar el cociente y resto de dividir el polinomio $g(X) = X^3 - 2X + 1$ por el polinomio $f(X) = X - 2$. Vamos a proceder como sigue.

Paso 1: Escribimos en una fila a todos los coeficientes (también los que no parecen, que son iguales a cero) del polinomio $g(X)$ de la mayor a la menor potencia, y un renglón más abajo escribimos el opuesto del término independiente del polinomio divisor $f(X)$: $-\text{ti}(f) = -(-2) = 2$.

	1	0	-2	1
2				

Paso 2: Bajamos el coeficiente 1 al tercer renglón.

	1	0	-2	1
2				
	1			

Paso 3: Ahora multiplicamos 2 por el coeficiente 1 y anotamos el resultado en el segundo renglón debajo del coeficiente 0.

	1	0	-2	1
2		2		
	1			

Paso 4: Ahora sumamos el coeficiente cero con el valor debajo de él, y colocamos el resultado en el tercer renglón.

	1	0	-2	1
2		2		
	1	2		

Paso 5: Multiplicamos 2 por el resultado de la suma anterior y anotamos el resultado en el segundo renglón debajo del coeficiente -2.

	1	0	-2	1
2		2	4	
	1	2		

Paso 6: Sumamos el coeficiente -2 con el resultado debajo de él, y colocamos el resultado en el tercer renglón.

	1	0	-2	1
2		2	4	
	1	2	2	

Paso 7: Multiplicamos 2 por el resultado de la suma anterior y colocamos el resultado en el segundo renglón debajo del coeficiente 1.

	1	0	-2	1
2		2	4	4
	1	2	2	

Paso 8: Sumamos el coeficiente 1 con el valor debajo de él y anotamos el resultado en el tercer renglón.

	1	0	-2	1
2		2	4	4
	1	2	2	5

Terminamos el procedimiento. Ahora, el cociente de la división se arma utilizando los valores 1, 2, 2 del último renglón de la siguiente forma: como el polinomio dividendo $g(X)$ es de grado 3, el polinomio cociente será de grado 2: $q(X) = aX^2 + bX + c$. En este caso los coeficientes del cociente serán: $a = 1$, $b = 2$ y $c = 2$. Entonces, el cociente es: $q(X) = X^2 + 2X + 2$. Y el resto de la división es $r(X) = 5$ (es el último valor del tercer renglón). El lector puede comprobar que se cumplen las dos condiciones $g(X) = f(X)q(X) + r(X)$ y $r(X) = 0$ o $\text{gr}(r) < \text{gr}(f)$.

Ejemplo 5.29. Determinar el cociente y resto de dividir el polinomio $g(X) = 2X^5 - 6X^3 + 4X^2 - 7$ por el polinomio $f(X) = X + 3$. Aplicamos la división por Ruffini. Notar que el término independiente de f es 3, entonces en el algoritmo de Ruffini debemos colocar -3.

	2	0	-6	4	0	-7
-3		-6	18	-36	96	288
	2	-6	12	-32	96	281

Por lo tanto, el cociente de la división es: $q(X) = 2X^4 - 6X^3 + 12X^2 - 32X + 96$, y el resto es $r(X) = 281$.

Ejemplo 5.30. Hallar el cociente y resto de dividir el polinomio $g(X) = -3X^4 + 2X^2 - X + 2$ por el polinomio $f(X) = 2X - 3$. A pesar de que el polinomio divisor $f(X)$ no es de la forma $X - a$, vamos a aplicar el algoritmo de Ruffini. Consideramos el polinomio $f'(X) = X - \frac{3}{2}$. Observe que $f(X) = 2.f'(X)$. Dividimos, aplicando Ruffini, a $g(X)$ por el polinomio $f'(X)$, obteniendo como cociente a $q'(X)$ y resto a $r(X)$ (dejamos a cargo del lector hallar $q'(X)$ y $r(X)$). Entonces, $g(X) = f'(X)q'(X) + r(X)$ y $r(X) = 0$ o $\text{gr}(r) < \text{gr}(f') = \text{gr}(f)$. Luego, podemos escribir $g(X) = 2.f'(X).\frac{1}{2}q'(X) + r(X) = f(X).q(X) + r(X)$ donde $q(X) = \frac{1}{2}q'(X)$. Por lo tanto, $q(X)$ y $r(X)$ son, respectivamente, el cociente y resto de dividir $g(X)$ por $f(X) = 2X - 3$.

Ahora podemos conectar la relación divide con el Teorema de la división en $\text{K}[X]$.

Proposición 5.31

Sean $f(X)$ y $g(X)$ dos polinomios en $\text{K}[X]$. Entonces, $f(X)$ divide a $g(X)$ si y sólo si el resto de dividir $g(X)$ por $f(X)$ es el polinomio nulo.

Demostración. A cargo del lector. ■

5.4. Polinomios irreducibles

En el capítulo 3 vimos que los números enteros primos son de vital importancia ya que ellos nos permiten factorizar a todo entero $a \neq 0, \pm 1$ como un producto de números primos y la factorización es única salvo el orden de los factores (véase Teorema 3.59). En el caso de polinomios sucede algo similar. En $\mathrm{K}[X]$ hay ciertos polinomios, que los llamaremos *polinomios irreducibles*, que nos permitirán factorizar a todo polinomio no constante como un producto de polinomios irreducibles.

Recordemos que un polinomio $f(X)$ es una constante si y sólo si $f(X)$ es el polinomio nulo ($f(X) = 0$) o $\mathrm{gr}(f) = 0$. Entonces, un polinomio $g(X)$ es no constante si y sólo si $\mathrm{gr}(g) > 0$.

Definición 5.32

Diremos que un polinomio no constante $p(X)$ de $\mathrm{K}[X]$ es **irreducible** en $\mathrm{K}[X]$ si no se puede expresar como producto de dos polinomios no contantes en $\mathrm{K}[X]$.

Veamos a continuación algunas observaciones y ejemplos que nos ayuden a entender mejor la definición de polinomio irreducible. Veamos primero una forma equivalente de definir polinomio irreducible.

Un polinomio no constante $p(X)$ de $\mathrm{K}[X]$ es **irreducible** en $\mathrm{K}[X]$ si $p(X) = f(X)g(X)$ con $f(X), g(X) \in \mathrm{K}[X]$, entonces $f(X)$ es una constante o $g(X)$ es una constante.

Ahora, debería ser claro que un polinomio no constante $p(X)$ de $\mathrm{K}[X]$ no es irreducible en $\mathrm{K}[X]$ si y sólo si existen dos polinomios no constantes (de grado positivo) $f(X), g(X) \in \mathrm{K}[X]$ tales que $p(X) = f(X)g(X)$.

Observación 5.33. Recuerde que K denota $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Cuando indicamos que un polinomio es o no irreducible es fundamental indicar en qué conjunto $\mathbb{Q}[X]$, $\mathbb{R}[X]$ o $\mathbb{C}[X]$ es o no irreducible dicho polinomio. Puede suceder que un polinomio sea irreducible en $\mathbb{Q}[X]$ pero no lo sea en $\mathbb{R}[X]$.

Observación 5.34. Observe que en la definición de polinomio irreducible, los polinomios constantes no son considerados a ser o no ser irreducibles.

Ejemplo 5.35.

1. El polinomio $f(X) = X^2 - 2 \in \mathbb{R}[X]$ no es irreducible en $\mathbb{R}[X]$ porque $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$. Esto es, $f(X)$ es no es irreducible en $\mathbb{R}[X]$ porque lo podemos escribir como el producto de dos polinomios no constantes $X - \sqrt{2}$ y $X + \sqrt{2}$ de $\mathbb{R}[X]$.

2. Sin embargo el polinomio $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$. Esto es, estamos afirmando que a $f(X)$ no lo podemos expresar como el producto de dos polinomios $p(X)$ y $q(X)$ no constantes de $\mathbb{Q}[X]$. Probemos esta afirmación. Supongamos que $f(X) = p(X)q(X)$ y que $p(X)$ y $q(X)$ son polinomios no constantes de $\mathbb{Q}[X]$. Estos

es, $\text{gr}(p) > 0$, $\text{gr}(q) > 0$ y $\text{gr}(f) = 2$. Entonces, por la Proposición 5.16 tenemos que $\text{gr}(p) = \text{gr}(q) = 1$. Además, $1 = \text{cp}(f) = \text{cp}(p).\text{cp}(q)$. Entonces, tenemos que los polinomios $p(X)$ y $q(X)$ son de grado 1 y mónicos. Es decir, son de la forma $p(X) = X + b$ y $q(X) = X + c$ con $b, c \in \mathbb{Q}[X]$. Ahora

$$\begin{aligned} f(X) &= p(X)q(X) \\ X^2 - 2 &= (X + b)(X + c) \\ X^2 - 2 &= X^2 + (b + c)X + (bc) \end{aligned}$$

Entonces, por la igualdad de polinomios, tenemos que $b + c = 0$ y $bc = -2$. De la primera ecuación tenemos que $b = -c$, y reemplazando en la segunda nos queda $(-c)c = -2$. Con lo cual, $c^2 = 2$. Esto es absurdo porque no existe ningún número racional que su cuadrado nos dé 2. Este absurdo surgió de suponer que a $f(X)$ no era irreducible en $\mathbb{Q}[X]$. Por lo tanto, $f(X)$ es irreducible en $\mathbb{Q}[X]$.

Ejemplo 5.36. El polinomio $f(X) = X^2 + 1 \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$ (para probar esto usar un argumento similar al ejemplo anterior), pero no es irreducible en $\mathbb{C}[X]$ por que $f(X) = X^2 + 1 = (X - i)(X + i)$, donde $X - i$ y $X + i$ son polinomios no constantes de $\mathbb{C}[X]$.

La tarea de determinar si un polinomio es o no irreducible no es sencilla, depende mucho del tipo de polinomio que estemos analizando. De aquí en adelante iremos estudiando e incorporando distintas herramientas que nos permitirán analizar si un polinomio es o no irreducible.

Proposición 5.37

Todo polinomio $f(X) \in \text{K}[X]$ de grado 1 es irreducible en $\text{K}[X]$.

Demostración. Sea $f(X) \in \text{K}[X]$ de grado 1. Supongamos que $f(X) = p(X)q(X)$ con $p(X)$ y $q(X)$ polinomios en $\text{K}[X]$. Luego, $1 = \text{gr}(f) = \text{gr}(p) + \text{gr}(q)$. Entonces, tenemos que $\text{gr}(p) = 0$ (y $q(X) = 1$) o $\text{gr}(q) = 0$ (y $p(X) = 1$). Esto es, $p(X)$ es constante o $q(X)$ es constante. Por lo tanto, $f(X)$ es irreducible. ■

Ahora enunciaremos el teorema que nos asegura que a todo polinomio no constate lo podemos factorizar como producto de una constante por un producto de polinomios irreducibles mónicos, y que además dicha factorización es única salvo el orden de los factores.

A todo polinomio no nulo $f(X) = a_n X^n + \cdots + a_1 X + a_0$ lo podemos escribir como producto de una constante por un polinomio mónico. Si $a_n \neq 0$, entonces $f(X) = a_n(X^n + \frac{a_{n-1}}{a_n} + \cdots + \frac{a_1}{a_n}X + \frac{a_0}{a_n})$, donde el polinomio $g(X) = X^n + \frac{a_{n-1}}{a_n} + \cdots + \frac{a_1}{a_n}X + \frac{a_0}{a_n}$ es mónico. Por ejemplo, al polinomio $f(X) = -3X^4 + 2X^2 - X + 5$ lo podemos escribir como $f(X) = -3(X^4 - \frac{2}{3}X^2 + \frac{1}{3}X - \frac{5}{3})$.

Teorema 5.38: Teorema Fundamental de la Aritmética en $\mathrm{K}[X]$

Todo polinomio $f(X)$ no constante de $\mathrm{K}[X]$ puede expresarse de la forma

$$f(X) = ap_1(X)^{e_1}.p_2(X)^{e_2}.\ldots.p_s(X)^{e_s}$$

donde $a \in \mathrm{K}$, $p_1(X), p_2(X), \ldots, p_s(X)$ son polinomios irreducibles mónicos en $\mathrm{K}[X]$ y $e_1, e_2, \ldots, e_s \in \mathbb{N}$. Esta factorización es única salvo el orden de los factores.

Demostración. En breve. ■

Hallar la factorización de un polinomio como producto de polinomios irreducibles mónicos no es tampoco una tarea sencilla. De aquí en adelante iremos presentando distintos procedimientos para poder determinar las factorizaciones de ciertos polinomios.

Es importante notar que la factorización de un polinomio depende de en dónde lo factoricemos. Es decir, las factorizaciones de un polinomio $f(X) \in \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$ pueden ser distintas en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$. Veamos el siguiente ejemplo.

Ejemplo 5.39. Consideremos el polinomio $f(X) = -3X^6 + 6X^4 + 3X^2 - 6$ y determinemos su factorización en producto de polinomios irreducibles mónicos en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

$$\begin{aligned}
f(X) &= -3X^6 + 6X^4 + 3X^2 - 6 \\
&= -3(X^6 - 2X^4 - X^2 + 2) && \text{Factor común -3} \\
&= -3[(X^6 - 2X^4) + (-X^2 + 2)] && \text{Asociamos} \\
&= -3[X^4(X^2 - 2) - (X^2 - 2)] && \text{Factor común } X^4 \text{ y factor común -1} \\
&= -3(X^4 - 1)(X^2 - 2) && \text{Factor común } (X^2 - 2) \\
&= -3(X^2 + 1)(X^2 - 1)(X^2 - 2) && \text{Diferencia de cuadrados} \\
&= -3(X^2 + 1)(X + 1)(X - 1)(X^2 - 2) && \text{Diferencia de cuadrados}
\end{aligned}$$

Aquí nos detenemos porque los polinomios $X^2 + 1$, $X + 1$, $X - 1$ y $X^2 - 2$ son irreducibles mónicos en $\mathbb{Q}[X]$. Por lo tanto,

$$f(X) = -3(X^2 + 1)(X + 1)(X - 1)(X^2 - 2)$$

es la factorización de $f(X)$ en producto de polinomios irreducibles mónicos en $\mathbb{Q}[X]$. Ahora, veamos que pasa con la factorización de $f(X)$ en $\mathbb{R}[X]$. Podemos observar que los polinomios $X^2 + 1$, $X + 1$ y $X - 1$ son también irreducibles mónicos en $\mathbb{R}[X]$, pero el polinomio $X^2 - 2$ no es irreducible en $\mathbb{R}[X]$ porque se puede escribir como $X^2 - 2 = (X + \sqrt{2})(X - \sqrt{2})$. Entonces,

$$f(X) = -3(X^2 + 1)(X + 1)(X - 1)(X + \sqrt{2})(X - \sqrt{2})$$

es la factorización de $f(X)$ en $\mathbb{R}[X]$, ya que ahora si todos los factores son polinomios irreducibles mónicos en $\mathbb{R}[X]$. Finalmente, pasamos a la factorización en $\mathbb{C}[X]$. En $f(X) = -3(X^2 + 1)(X + 1)(X - 1)(X + \sqrt{2})(X - \sqrt{2})$ el único polinomio que no es irreducible en

$\mathbb{C}[X]$ es el polinomio X^2+1, que puede escribirse como $X^2+1=(X+i)(X-i)$. Entonces, reemplazando obtenemos que

$$f(X) = -3(X+i)(X-i)(X+1)(X-1)(X+\sqrt{2})(X-\sqrt{2})$$

es la factorización de $f(X)$ en producto de polinomios irreducibles mónicos en $\mathbb{C}[X]$. Resumiendo, el polinomio $f(X) = -3X^6+6X^4+3X^2-6$ se factoriza en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ como:

$$\begin{aligned} f(X) &= -3(X^2+1)(X+1)(X-1)(X^2-2) && \text{en } \mathbb{Q}[X] \\ f(X) &= -3(X^2+1)(X+1)(X-1)(X+\sqrt{2})(X-\sqrt{2}) && \text{en } \mathbb{R}[X] \\ f(X) &= -3(X+i)(X-i)(X+1)(X-1)(X+\sqrt{2})(X-\sqrt{2}) && \text{en } \mathbb{C}[X]. \end{aligned}$$

Ejemplo 5.40. Hallar la factorización de $f(X)=\frac{1}{2}X^4-X^2-\frac{3}{2}$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$. Primero podemos observar que el polinomio $f(X)$ es del estilo cuadrático (todas las potencias de X son potencias de 2). Así que hacemos una cambio de variable. Consideramos $Y=X^2$. Si reemplazamos en $f(X)$ nos queda el polinomio

$$\begin{aligned} g(Y) &= \frac{1}{2}Y^2 - Y - \frac{3}{2} \\ &= \frac{1}{2}\left(Y^2 - \frac{1}{2}Y - 3\right) \\ &= \frac{1}{2}\left(Y+\frac{3}{2}\right)(Y-2). \end{aligned}$$

Entonces, $f(X)=\frac{1}{2}(X^2+\frac{3}{2})(X^2-2)$. Entonces, las factorizaciones de $f(X)$ en producto de polinomio irreducibles mónicos son:

$$\begin{aligned} f(X) &= \frac{1}{2}\left(X^2+\frac{3}{2}\right)(X^2-2) && \text{en } \mathbb{Q}[X] \\ f(X) &= \frac{1}{2}\left(X^2+\frac{3}{2}\right)(X-\sqrt{2})(X+\sqrt{2}) && \text{en } \mathbb{R}[X] \\ f(X) &= \frac{1}{2}\left(X-\sqrt{\frac{3}{2}}i\right)\left(X+\sqrt{\frac{3}{2}}i\right)(X-\sqrt{2})(X+\sqrt{2}) && \text{en } \mathbb{C}[X]. \end{aligned}$$

5.5. Raíces de polinomios

El concepto de *raíz* es muy importante en el estudio de polinomios ya que nos brinda mucha información acerca del comportamiento de los mismos. Conocer las raíces de un polinomio es muy útil porque nos ayuda a analizar la irreducibilidad o no del polinomio, y nos permite en muchos casos hallar su factorización.

Sea $a \in \mathrm{K}$ y sea $f(X)=a_nX^n+\cdots+a_1X+a_0$ un polinomio de $\mathrm{K}[X]$. Se llama **valor numérico** de f en a al número

$$f(a) = a_na^n+\cdots+a_1a+a_0.$$

En otras palabras, el valor numérico de f en a es el resultado de reemplazar en $f(X) = a_n X^n + \cdots + a_1 X + a_0$ la indeterminada X por a y operar algebraicamente en K.

Definición 5.41

Dado un polinomio $f(X) \in \mathrm{K}[X]$, diremos que un valor $a \in \mathrm{K}$ es **raíz** de f si $f(a) = 0$.

Problema 5.42

Sea $f(X) = -X(X^2 - 3)(X^2 + 2)$. ¿Es $\sqrt{3}$ una raíz de $f(X)$? Hallar cinco raíces distintas de $f(X)$.

Teorema 5.43: Teorema del resto

Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Entonces, el resto de dividir el polinomio $f(X)$ por el polinomio $X - a$ es $f(a)$.

Demostración. Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Sean $q(X)$ y $r(X)$ el cociente y resto, respectivamente, de dividir $f(X)$ por $X - a$. Entonces $f(X) = (X - a)q(X) + r(X)$ y $r(X) = 0$ o $\mathrm{gr}(r) < 1$. Como $r(X) = 0$ o $\mathrm{gr}(r) < 1$, tenemos que $r(X)$ es una constante, digamos $r(X) = c \in \mathrm{K}$ Luego, $f(X) = (X - a)q(X) + c$. Entonces, $f(a) = (a - a)q(a) + c = c$. Por lo tanto, $f(a)$ es el resto de dividir $f(X)$ por $X - a$. ■

Ejemplo 5.44. Consideremos el polinomio $g(X) = 2X^5 - 6X^3 + 4X^2 - 7$ y hallemos el resto de dividir $g(X)$ por el polinomio $X + 3$. Entonces, por el Teorema del Resto $g(-2) = 2(-2)^5 - 6(-2)^3 + 4(-2)^2 - 7 = 281$ es el resto de dividir $g(X)$ por $X + 3$ (compare con el Ejemplo 5.29).

Corolario 5.45

Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Entonces, $f(X)$ es divisible por $X - a$ si y sólo si a es raíz de f.

Demostración. Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$.

($\Leftarrow$) Supongamos que $f(X)$ es divisible por $X - a$ en $\mathrm{K}[X]$. Esto significa que existe un polinomio $p(X) \in \mathrm{K}[X]$ tal que $f(X) = (X - a)p(X)$. Entonces. $f(a) = (a - a)p(a) = 0$. Por lo tanto, a es una raíz de $f(X)$.

($\Rightarrow$) Supongamos que a es una raíz de $f(X)$. Esto es, $f(a) = 0$. Sean $q(X)$ y $r(X)$ el cociente y resto, respectivamente, de dividir $f(X)$ por $X - a$. Entonces $f(X) = (X - a)q(X) + r(X)$. Por le Teorema del Resto sabemos que el $r(X) = f(a) = 0$. Luego, $f(X) = (X - a)q(X)$. Lo cual implica que $f(X)$ es divisible por $X - a$. ■

Definición 5.46

Sea $f(X) \in \mathrm{K}[X]$. Diremos que $a \in \mathrm{K}$ es una raíz de **orden de multiplicidad** m si existe un polinomio $g(X)$ tal que

$$f(X) = (X-a)^m g(X) \quad \text{y} \quad g(a) \neq 0.$$

Si $m = 1$, diremos que a es una **raíz simple**, y si $m > 1$ diremos que a es una **raíz múltiple**.

Ejemplo 5.47. Consideremos el polinomio $f(X) = X^3 - 3X + 2$. Podemos observar que $X = 1$ es una raíz de f. Deseamos conocer el orden de multiplicidad de la raíz $X = 1$. Entonces, comenzamos por dividir el polinomio $f(X)$ por el polinomio $X - 1$ usando la regla de Ruffini:

	1	0	-3	2
1		1	1	-2
	1	1	-2	0

Entonces, tenemos que $f(X) = (X-1)(X^2 + X - 2)$. Ahora comprobamos si $X = 1$ es raíz del polinomio $X^2 + X - 2$. Es directo observar que efectivamente $X = 1$ es raíz de $X + X - 2$, así que dividimos este polinomio por $X - 1$:

	1	1	-2
1		1	2
	1	2	0

Entonces, $X^2 + X - 2 = (X-1)(X+2)$. Con lo cual, $f(X) = (X-1)^2(X+2)$. Luego, $f(X) = (X-1)^2 g(X)$ donde $g(X) = X + 2$ y $g(1) = 3 \neq 0$. Por lo tanto, $X = 1$ es una raíz múltiple (raíz doble o de orden 2) de $f(X)$.

La regla de Ruffini es una herramienta muy útil para determinar el orden de multiplicidad de una raíz. A continuación veremos una serie de ejemplos. Primero observemos que en el ejemplo anterior dividimos dos veces por el polinomio $X - 1$, obteniendo resto cero. Esto se puede simplificar un poco aplicando la regla de Ruffini de forma consecutiva: vamos a dividir consecutivamente por el polinomio $X - 1$, comenzando a dividir el polinomio $f(X) = X^3 - 3X + 2$:

	1	0	-3	2
1		1	1	-2
	1	1	-2	0
1		1	2	
	1	2	0	

Entonces, como los restos de dividir por $X - 1$ nos fueron dando cero, podemos concluir de aquí directamente que $f(X) = (X-1)^2(X+2)$.

Ejemplo 5.48. Consideremos el polinomio $f(X) = X^5 - 6X^4 + 11X^3 - 2X^2 - 12X + 8$. Afirmamos que $X = 2$ es una raíz de f. Vamos a utilizar la regla de Ruffini para determinar el orden de multiplicidad de la raíz $X = 2$. A continuación vamos a dividir consecutivamente por el polinomio $X - 2$, comenzando a dividir $f(X)$ por $X - 2$, hasta hallar el primer resto no nulo.

	1	-6	11	-2	-12	8
2		2	-8	6	8	-8
	1	-4	3	4	-4	0
2		2	-4	-2	4	
	1	-2	-1	2	0	
2		2	0	-2		
	1	0	-1	0		
2		2	4			
	1	2	$3 \neq 0$			

Entonces podemos afirmar que $X = 2$ es una raíz múltiple de orden 3. En efecto, por la regla de Ruffini, utilizando la última división que nos dio resto cero, tenemos que $f(X) = (X-2)^3(X^2-1)$. Ahora, es sencillo observar que $X^2 - 1$ se factoriza como $X^2 - 1 = (X + 1)(X - 1)$. Entonces, $f(X) = (X-2)^3(X+1)(X-1)$ es la factorizacion de $f(X)$ en K$[X]$ y sus raíces son 2 (de orden 3), -1 (simple) y 1 (simple).

Ejemplo 5.49. Determinar las raíces del polinomio $f(X) = 3X^5 + 6X^4 + 3X^3 - 3X^2 - 6X - 3$ y su factorización en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ sabiendo que $X = -1$ es raíz de $f(X)$. Aplicamos la regla de Ruffini (dividiendo por $X + 1$) consecutivamente hasta hallar el primer resto no nulo.

	3	6	3	-3	-6	-3
-1		-3	-3	0	3	3
	3	3	0	-3	-3	0
-1		-3	0	0	3	
	3	0	0	-3	0	
-1		-3	3	-3		
	3	-3	3	$-6 \neq 0$		

Entonces, considerando hasta la última división cuyo resto es cero, nos queda que $f(X) = (X+1)^2(3X^3 - 3)$. Ahora es sencillo observar que $X = 1$ es raíz del polinomio $3X^3 - 3$. Aplicando la regla de Ruffini para dividir el polinomio $3X^3 - 3$ por $X - 1$, obtenemos que $3X^3 - 3 = 3(X-1)(X^2 + X + 1)$. Entonces,

$$f(X) = (X+1)^2 3(X-1)(X^2+X+1) = 3(X+1)^2(X-1)(X^2+X+1).$$

Esta es la factorización en producto de polinomios irreducibles en $\mathbb{R}[X]$ porque $X^2 + X + 1$ no tiene raíces reales. En efecto, aplicando la fórmula cuadrática al polinomio $X^2 + X + 1$ hallamos que sus raíces (complejas) son:

$$\frac{-1 \pm \sqrt{1^2 - 4.1.1}}{2.1} = \frac{-1 \pm \sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i.$$

Luego, $X^2+X+1=\left(X-\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\right)\left(X-\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\right)$. Entonces

$$f(X)=3(X+1)^2(X-1)\left(X+\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\left(X+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$$

es la factorización de $f(X)$ en $\mathbb{C}[X]$. Además observamos que las raíces de $f(X)$ son: -1 (raíz doble), 1, $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ y $-\frac{1}{2}-\frac{\sqrt{3}}{2}i$ (simples).

Proposición 5.50

Sea $f(X)\in \mathrm{K}[X]$ y $a\in \mathrm{K}$. Entonces, a es raíz de orden de multiplicidad m si y sólo si $f(X)$ es divisible por $(X-a)^m$ pero no es divisible por $(X-a)^{m+1}$.

Demostración. Sea $f(X)\in \mathrm{K}[X]$ y $a\in \mathrm{K}$.

($\Leftarrow$) Supongamos que a es una raíz de $f(X)$ de orden m. Por definición, esto significa que existe un polinomio $g(X)\in \mathrm{K}[X]$ tal que

$$f(X)=(X-a)^m g(X) \qquad \text{y} \qquad g(a)\neq 0.$$

Claramente, $f(X)=(X-a)^m g(X)$ implica que $f(X)$ es divisible por $(X-a)^m$. Probemos ahora que $f(X)$ no es divisible por $(X-a)^{m+1}$. Supongamos por absurdo que si. Entonces, existe un polinomio $h(X)\in \mathrm{K}[X]$ tal que $f(X)=(X-a)^{m+1}h(X)$. Luego, tenemos que $(X-a)^m g(X)=(X-a)^{m+1}f(X)$. Cancelando nos queda $g(X)=(X-a)f(X)$ (véase el Problema 5.19). Con lo cual, $g(a)=0$. Absurdo! Por lo tanto, $f(X)$ no es divisible por $(X-a)^{m+1}$.

($\Rightarrow$) Ahora supongamos que $f(X)$ es divisible por $(X-a)^m$ y no es divisible por $(X-a)^{m+1}$. Tenemos que probar que a es una raíz de orden m de $f(X)$. Bien, como $f(X)$ es divisible por $(X-a)^m$ sabemos que existe un polinomio $g(X)$ tal que $f(X)=(X-a)^m g(X)$. Entonces $f(a)=0$, y vemos que a es raíz de f. Afirmamos que $g(a)\neq 0$. Pues si $g(a)=0$, entonces por el Corolario 5.45 tenemos que $g(X)$ es divisible por $X-a$. Esto es, existe $h(X)\in \mathrm{K}[X]$ tal que $g(X)=(X-a)h(X)$. Luego $f(X)=(X-a)^{m+1}h(X)$. Lo que implica que $f(X)$ es divisible por $(X-a)^{m+1}$, un absurdo. En conclusión, $f(X)=(X-a)^m g(X)$ y $g(a)\neq 0$. Por lo tanto, a es una raíz de $f(X)$ de orden m. ■

Teorema 5.51

Si f es un polinomio de grado n, entonces f tiene a lo sumo n raíces.

Demostración. Haremos la demostración por inducción sobre el grado de los polinomios. Esto es, probaremos por inducción la siguiente afirmación:

Para todo $n\in\mathbb{N}$, si f es un polinomio de grado n, entonces f tiene a lo sumo n raíces.

- **Caso base:** Debemos probar que la afirmación anterior es verdadera para $n=1$. Esto es, debemos probar que si f es un polinomio de grado 1, entonces tiene a lo sumo una raíz. Sea $f(X)$ de grado 1. Entonces $f(X)$ es de la forma $f(X)=aX+b$. Es claro que la única raíz de f es $X=-\frac{b}{a}$. Con lo cual se cumple que f tiene a lo sumo una raíz.

- **Paso inductivo:** Supongamos que se cumple para $n-1$. Esto es, suponemos que todo polinomio de grado $n-1$ tiene a los sumo $n-1$ raíces (H.I.). Sea $f(X)$ un polinomio de grado n. Si f no tiene raíces, entonces se cumple que tiene a lo sumo n raíces. Si f tiene una raíz a, entonces por el Corolario 5.45 tenemos que $f(X) = (X-a)g(X)$ para algún polinomio $g(X)$. Observemos que las raíces de $f(X)$ son a y las raíces de $g(X)$. Como $g(X)$ es de grado $n-1$, por la H.I. sabemos que $g(X)$ tiene a lo sumo $n-1$ raíces. Por lo tanto, $f(X)$ tiene a los sumo $1+(n-1) = n$ raíces.

Esto prueba el teorema. ■

El siguiente teorema es muy importante en el estudio de polinomios. La demostración de este teorema escapa al alcance de este libro.

Teorema 5.52: Teorema Fundamental del Álgebra

Todo polinomio no constante con coeficientes en $\mathbb{C}$ tiene por lo menos una raíz en $\mathbb{C}$.

Corolario 5.53

Todo polinomio $f(X)$ de grado n con coeficientes en $\mathbb{C}$ tiene exactamente n raíces $z_1, z_2, \ldots, z_n$ (contando multiplicidad) en $\mathbb{C}$ y $f(X) = a_n(X-z_1)(X-z_2)\ldots(X-z_n)$ con $a_n \in \mathbb{C}$.

Demostración. Este corolario se puede probar usando inducción sobre el grado de los polinomio. Esto es, debemos probar por inducción la siguiente afirmación:

Para todo $n \in \mathbb{N}$, si $f(X) \in \mathbb{C}[X]$ es de grado n, entonces $f(X)$ tiene exactamentre n raíces y
$$f(X) = a_n(X-z_1)(X-z_2)\ldots(X-z_n).$$

En el paso inductivo es fundamental usar el Teorema Fundamental del Álgebra y luego hay que aplicar el Corolario 5.45. Dejamos los detalles al lector. ■

Problema 5.54

¿Cuántas raíces complejas tiene el polinomio $f(X) =$

5.6. Raíces y polinomios irreducibles en $\mathbb{R}[X]$ y $\mathbb{C}[X]$

En esta sección continuamos estudiando las raíces reales y complejas de polinomios en $\mathbb{R}[X]$ y $\mathbb{C}[X]$ y la factorización en producto de polinomios irreducibles. Comenzamos introduciendo una definición que nos será de utilidad.

Definición 5.55

Sea $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 \in \mathrm{K}[X]$. Se llama polinomio **derivado** al polinomio $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2X + a_1$.

El operador derivada cumple las propiedades usuales que se estudian en análisis.

Proposición 5.56

Sea $f(X), g(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Entonces:

1. $(f+g)' = f' + g'$.
2. $(f.g)' = f'g + fg'$.
3. $((X-a)^m)' = m(X-a)^{m-1}$, para todo $m \in \mathbb{N}$.

Demostración. Dejamos las demostraciones de estas propiedades a cargo del lector. ■

Los siguientes dos proposiciones son resultados auxiliares que necesitamos para probar la Proposición 5.60.

Proposición 5.57

Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Entonces, a es raíz de f de orden m si y sólo si a es raíz de f y a es raíz del polinomio derivado f' de orden $m-1$.

Demostración. La demostración se encuentra en el Apéndice **??**. ■

Definimos por recurrencia polinomios derivados de orden superior:

$$\begin{aligned} f^{(0)}(X) &= f(X) \\ f^{(1)}(X) &= f'(X) \\ f^{(n+1)}(X) &= \left(f^{(n)}(X)\right)' \qquad \forall n \in \mathbb{N}. \end{aligned}$$

Por ejemplo, $f^{(2)} = (f')' = f''$, $f^{(3)} = (f^{(2)})' = (f'')' = f'''$, ...

Proposición 5.58

Sea $f(X) \in \mathrm{K}[X]$ y $a \in \mathrm{K}$. Entonces, a es raíz de f de orden m si y sólo si $f(a) = f'(a) = f''(a) = \cdots = f^{(m-1)}(a) = 0$ y $f^{(m)}(a) \neq 0$.

Demostración. La demostración se encuentra en el Apéndice **??**. ■

Ejemplo 5.59. Consideremos el polinomio $f(X) = -2X^5 + 3X^4 - 4X^3 + 5X^2 - 2$ y determinemos el orden de multiplicidad de la raíz $X = 1$. En efecto, $X = 1$ es raíz de f: $f(1) = 0$. Ahora, $f'(X) = -10X^4 + 12X^3 - 12X^2 + 10X$. Entonces $f'(1) = 0$. Derivamos el polinomio $f'(X)$: $f''(X) = -40X^3 + 36X^2 - 24X + 10$. Evaluamos en $X = 1$: $f''(1) = -18 \neq 0$. Por lo tanto, $X = 1$ es una raíz múltiple de orden 2 del polinomio $f(X)$.

Proposición 5.60

Sea $f(X) \in \mathbb{R}[X]$. Si $z \in \mathbb{C}$ es una raíz de $f(X)$, entonces $\overline{z}$ es también una raíz de $f(X)$. Además, z y $\overline{z}$ tienen el mismo orden de multiplicidad.

Demostración. Sea $f(X) = a_nX^n + \cdots + a_1X + a_0$ un polinomio con coeficientes reales y supongamos que $z \in \mathbb{C}$ es una raíz de $f(X)$ de orden de multiplicidad m. Veamos primero que $\overline{z}$ es también raíz de f. Tenemos que:

$$\begin{aligned} f(\overline{z}) &= a_n\overline{z}^n + \cdots + a_1\overline{z} + a_0 \\ &= \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} \\ &= \overline{a_n}\overline{z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n + \cdots + a_1 z + a_0} \\ &= \overline{f(z)} \\ &= \overline{0} \\ &= 0. \end{aligned}$$

Entonces, $\overline{z}$ es raíz de $f(X)$. Ahora probaremos que $\overline{z}$ es raíz de orden m de f. Como los coeficientes de $f(X)$ son reales, tenemos que los coeficientes del k-ésimo polinomio derivado $f^{(k)}(X)$ tiene también coeficientes reales[2]. Por lo que acabamos de probar sabemos que

$$z \text{ es raíz de } f^{(k)}(X) \text{ si y sólo si } \overline{z} \text{ es raíz de } f^{(k)}(X).$$

Luego, como z es raíz de orden m de f, tenemos por la Proposición 5.58 que

$$f(z) = f'(z) = \cdots = f^{(m-1)}(z) = 0 \text{ y } f^{(m)}(z) \neq 0.$$

Entonces,

$$f(\overline{z}) = f'(\overline{z}) = \cdots = f^{(m-1)}(\overline{z}) = 0 \text{ y } f^{(m)}(\overline{z}) \neq 0.$$

Por lo tanto, $\overline{z}$ es raíz de $f(X)$ de orden m. ■

Corolario 5.61

Todo polinomio con coeficientes reales de grado impar tiene por lo menos una raíz real.

Demostración. Sea $f(X)$ un polinomio con coeficientes reales de grado impar. Supongamos por absurdo que f no tiene ninguna raíz real. Entonces, todas sus raíces son complejas. Ahora, teniendo en cuenta que las raíces complejas vienen de a pares y con el mismo orden de multiplicidad, tenemos por ejemplo que $z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_n, \overline{z_n}$ son todas las raíces de f (contando multiplicidad). Entonces, por el Corolario 5.53, obtenemos que $f(X) = a_n(X - z_1)(X - \overline{z_1})(X - z_2)(X - \overline{z_2}) \ldots (X - z_n)(X - \overline{z_n})$. Luego, $\text{gr}(f) = 2n$. Es decir, que el grado de f es par, lo cual es absurdo. Por lo tanto, f tiene al menos una raíz real. ■

Proposición 5.62

Si $f(X) \in \text{K}[X]$ es de grado mayor o igual a 2 y tiene una raíz en K, entonces f no es irreducible en $\text{K}[X]$.

[2]Se puede probar por inducción sobre k que: para todo $k \in \mathbb{N}$, si $f(X) \in \mathbb{R}[X]$, entonces $f^{(k)}(X) \in \mathbb{R}[X]$.

Demostración. Sea $f(X) \in \mathrm{K}[X]$ de grado ≥ 2 y supongamos que $a \in \mathrm{K}$ es raíz de $f(X)$. Entonces, por el Corolario 5.45, $X - a$ divide a $f(X)$. Luego, existe $g(X) \in \mathrm{K}[X]$ tal que $f(X) = (X - a)g(X)$. Como $\mathrm{gr}(f) \geq 2$ y $\mathrm{gr}(X - a) = 1$, tenemos que $\mathrm{gr}(g) \geq 1$. Esto es, g no es constante. Entonces, f es el producto de dos polinomios no constantes. Por lo tanto, f no es irreducible. ■

Proposición 5.63

Los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1.

Demostración. Por la Proposición 5.4, sabemos que todo polinomio de grado 1 es irreducible. Ahora veamos que son los únicos polinomios irreducibles en $\mathbb{C}[X]$. Sea $f(X) \in \mathrm{K}[X]$ tal que $\mathrm{gr}(f) \geq 2$. Entonces, por el Teorema 5.52, existe un $z \in \mathbb{C}$ que es raíz de f. Luego, por la Proposición 5.6 tenemos que f no es irreducible. Así hemos probado que todo polinomio de $\mathbb{C}[X]$ de grado mayor que 1 no es irreducible. Por lo tanto, los únicos que son irreducibles en $\mathbb{C}[X]$ son los de grado 1. ■

Proposición 5.64

Los únicos polinomio irreducibles en $\mathbb{R}[X]$ son los de grado 1 y los polinomios $f(X) = aX^2 + bX + c$ de grado 2 tales que $b^2 - 4.a.c < 0$.

Demostración. Por la Proposición 5.4 sabemos que todos los polinomios de grado 1 son irreducibles. Ahora vamos a analizar que sucede con todos los polinomios de grado mayor que 1, separando por casos. Sea $f(X) \in \mathbb{R}[X]$.

- Supongamos $f(X) = aX^2 + bX + c$ es de grado 2 y $b^2 - 4.a.c < 0$. Por la fórmula cuadrática sabemos que f no tiene raíces reales. Entonces podemos afirmar que f es irreducible. En efecto, supongamos por absurdo que f no es irreducible. Esto es, f se puede escribir como producto de dos polinomios no constantes. Como el grado de f es 2, tenemos que $f(X) = a(X - r_1)(X - r_2)$ con $r_1, r_2 \in \mathbb{R}$. Luego r_1 y r_2 son raíces reales de f, lo cual es absurdo, pues f no tiene raíces reales. Por lo tanto, f es irreducible.

- Supongamos $f(X) = aX^2 + bX + c$ es de grado 2 y $b^2 - 4.a.c \geq 0$. Entonces, por la fórmula cuadrática, f tiene al menos una raíz real. Entonces, por la Proposición 5.6, tenemos que f no es irreducible.

- Supongamos que f es de grado impar mayor que 2. Por el Corolario 5.6 sabemos que f tiene al menos una raíz real. Entonces, por la Proposición 5.6, f no es irreducible.

- Supongamos que f es de grado par mayor que 2 (esto es, $\mathrm{gr}(f) \geq 4$ y es par). Si f tiene al menos una raíz real, entonces f no es irreducible. Si f no tiene raíces reales, entonces todas sus raíces son complejas. También sabemos que las raíces complejas del polinomio real $f(X)$ vienen de a pares (Proposición 5.60). Supongamos que $z_1, \overline{z_1}, \ldots, z_m, \overline{z_m}$

son todas las raíces complejas de f (contando multiplicidades). Por el Corolario 5.53 tenemos que

$$\begin{aligned} f(X) &= a(X-z_1)(X-\overline{z_1})\dots(X-z_m)(X-\overline{z_m}) \\ &= a(X^2-2\mathrm{Re}(z_1)X+|z_1|^2)\dots(X^2-2\mathrm{Re}(z_m)X+|z_m|^2). \end{aligned}$$

Podemos observar que $f(X)$ es el producto de polinomios de $\mathbb{R}[X]$ no constantes. Por lo tanto, f no es irreducible.

Hemos analizado todos los polinomios de $\mathbb{R}[X]$, y los únicos que resultaron irreducibles son los de grado 1 y los polinomios $f(X) = aX^2 + bX + c$ de grado 2 tales que $b^2 - 4.a.c < 0$. ■

Problema 5.65

Sea $z \in \mathbb{C} - \mathbb{R}$. ¿El polinomio $f(X) = (X-z)(X-\overline{z})$ pertenece a $\mathbb{R}[X]$? ¿Es $f(X)$ irreducible en $\mathbb{R}[X]$?

Finalizamos esta sección estudiando algunos métodos, procedimientos y estrategias para hallar las raíces de polinomios y su factorización.

Teorema 5.66: Teorema de Gauss

Sea $f(X) = a_nX^n + \dots + a_1X + a_0$ un polinomio con coeficientes enteros. Sea $\frac{p}{q} \in \mathbb{Q}$ (con p y q coprimos) una raíz de f. Entonces, $p|a_0$ y $q|a_n$.

Demostración. Como $\frac{p}{q}$ es raíz de f tenemos que

$$\begin{aligned} a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1\frac{p}{q} + a_0 &= 0 \\ a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \dots + a_1\frac{p}{q} + a_0 &= 0 \\ q^n\left(a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \dots + a_1\frac{p}{q} + a_0\right) &= q^n.0 \\ a_np^n + a_{n-1}p^{n-1}q + \dots + a_1pq^{n-1} + a_0q^n &= 0 \\ a_np^n + a_{n-1}p^{n-1}q + \dots + a_1pq^{n-1} &= -a_0q^n \\ p\left(a_np^{n-1} + a_{n-1}p^{n-2}q + \dots + a_1q^{n-1}\right) &= -a_0q^n. \end{aligned}$$

Entonces, obtenemos que $p| - a_0q^n$. Como p y q son coprimos, tenemos que $p| - a_0$ y así $p|a_0$. Por otro lado, haciendo un argumento análogo al anterior obtenemos que

$$q(a_{n-1}p^{n-1} + \dots + a_1pq^{n-2} + a_0q^{n-1}) = -a_np^n.$$

Entonces, $q|a_n$. Esto completa la demostración. ■

Tratemos de analizar y comprender el teorema anterior. El resultado anterior nos afirma que si el polinomio $f(X)$ (con coeficientes enteros) tiene una raíz racional $\frac{p}{q}$, entonces el numerador p debe dividir al término independiente de f y el denominador q debe dividir al

coeficiente principal de f. Es decir, si tenemos un polinomio $f(X) = a_nX^n + \cdots + a_1X + a_0$ con coeficientes enteros y deseamos hallar, si existen, sus raíces racionales, debemos buscar entre los números racionales $\frac{p}{q}$ tales que $p|a_0$ y $q|a_n$. Veamos el siguiente ejemplo.

Ejemplo 5.67. Hallemos todas las raíces racionales, si existen, del polinomio $f(X) = 4X^4 + 4X^3 - 3X^2 - 2X + 1$. Lo primero que debemos hacer es buscar los divisores del término independiente de f: $\mathrm{Div}(1) = \{\pm 1\}$, y los divisores del coeficiente principal de f: $\mathrm{Div}(4) = \{\pm 1, \pm 2, \pm 4\}$. Ahora consideramos todos los racionales $\frac{p}{q}$ con $p \in \mathrm{Div}(1)$ y $q \in \mathrm{Div}(4)$. Entonces, las posibles raíces racionales son

$$\frac{p}{q} = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}.$$

Ahora solo nos queda determinar si algunas de ellas son raíces de f. Para ello debemos simplemente ir comprobando que $f\left(\frac{p}{q}\right) = 0$. Comenzamos (simplemente por nuestra conveniencia) por ver si $X = \frac{1}{2}$ es raíz de f. Además, no solo vamos a chequear si $X = \frac{1}{2}$ es raíz sino que también vamos a determinar su orden de multiplicidad. Para ello vamos a utilizar la regla de Ruffini:

	4	4	-3	-2	1
$\frac{1}{2}$		2	3	0	-1
	4	6	0	-2	0
$\frac{1}{2}$		2	4	2	
	4	8	4	0	
$\frac{1}{2}$		2	5		
	4	10	$9 \neq 0$		

Entonces, $X = \frac{1}{2}$ es raíz de f de orden 2. Además

$$f(X) = (X - \tfrac{1}{2})^2(4X^2 + 8X + 4) = 4(X - \tfrac{1}{2})^2(X^2 + 2X + 1) = 4(X - \tfrac{1}{2})^2(X + 1)^2.$$

Entonces, podemos observar que $X = -1$ es también raíz de f de orden 2. Finalmente concluimos que las raíces de f son: $X = \frac{1}{2}$ (doble) y $X = -1$ (doble). Además, $f(X) = 4(X - \frac{1}{2})^2(X + 1)^2$ es la factorización de f en producto de polinomios irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

Ejemplo 5.68. Hallar todas las raíces del polinomio $f(X) = 8X^8 - 12X^7 + 10X^6 - 13X^5 - 9X^4 + 19X^3 + 5X^2 - 6X - 2$ y su factorización en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y en $\mathbb{C}[X]$. Vamos a seguir los siguientes pasos.

(1) Determinamos las posibles raíces racionales $\frac{p}{q}$ con $p \in \mathrm{Div}(-2) = \{\pm 1, \pm 2\}$ y $q \in \mathrm{Div}(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$. Entonces las posibles raíces racionales son:

$$\tfrac{p}{q} \in \{\pm 1, \pm\tfrac{1}{2}, \pm\tfrac{1}{4}, \pm\tfrac{1}{8}, \pm 2\}.$$

(2) Comenzamos a aplicar la regla de Ruffini con los racionales $\frac{p}{q}$ antes mencionados hasta encontrar una raíz. Arrancamos probando con $X = 1$:

	8	-12	10	-13	-9	19	5	-6	-2
1		8	-4	6	-7	-16	3	8	2
	8	-4	6	-7	-16	3	8	2	0
1		8	4	10	3	-13	-10	-2	
	8	4	10	3	-13	-10	-2	0	
1		8	12	22	25	12	2		
	8	12	22	25	12	2	0		
1		8	20	42	67	79			
	8	20	42	67	79	$81 \neq 0$			

Entonces, $f(X) = (X-1)^3(8X^5 + 12X^4 + 22X^3 + 25X^2 + 12X + 2)$. Ahora, probamos si alguno de los otros racionales $\frac{p}{q}$ es raíz del polinomio $8X^5 + 12X^4 + 22X^3 + 25X^2 + 12X + 2$. Probamos con $X = -\frac{1}{2}$:

	8	12	22	25	12	2
$-\frac{1}{2}$		-4	-4	-9	-8	-2
	8	8	18	16	4	0
$-\frac{1}{2}$		-4	-2	-8	-4	
	8	4	16	8	0	
$-\frac{1}{2}$		-4	0	-8		
	8	0	16	0		
$-\frac{1}{2}$		-4	2			
	8	-4	$18 \neq 0$			

Entonces, $8X^5 + 12X^4 + 22X^3 + 25X^2 + 12X + 2 = (X + \frac{1}{2})^3(8X^2 + 16)$. Luego

$$f(X) = (X-1)^3(X+\tfrac{1}{2})^3(8X^2+16) = 8(X-1)^3(X+\tfrac{1}{2})^3(X^2+2).$$

(3) Nos resta solo hallar las raíces del polinomio $X^2 + 2$ (que sabemos que no son reales). Podemos observar directamente que las raíces son $X = \sqrt{2}i$ y $X = -\sqrt{2}i$. Entonces $X^2 + 2 = (X - \sqrt{2}i)(X + \sqrt{2}i)$. Entonces

$$f(X) = 8(X-1)^3(X+\tfrac{1}{2})^3(X^2+2) = 8(X-1)^3(X+\tfrac{1}{2})^3(X-\sqrt{2}i)(X+\sqrt{2}i).$$

Por lo tanto, las raíces de $f(X)$ son: 1 (de orden 3), $-\frac{1}{2}$ (de orden 3), $\pm\sqrt{2}i$ (simples). Además, las factorizaciones de f son:

$$f(X) = 8(X-1)^3\left(X+\frac{1}{2}\right)^3(X^2+2) \qquad \text{en } \mathbb{Q}[X] \text{ y en } \mathbb{R}[X]$$

$$f(X) = 8(X-1)^3\left(X+\frac{1}{2}\right)^3\left(X-\sqrt{2}i\right)\left(X+\sqrt{2}i\right) \qquad \text{en } \mathbb{C}[X].$$

5.7. Acotación de raíces

A veces determinar el valor exacto de una raíz puede resultar ser realmente una tarea muy difícil. En esta sección veremos algunos resultados que nos permiten obtener cotas superior e inferiores de las raíces reales de un polinomio con coeficientes reales.

Proposición 5.69: Regla de Laguerre-Thibault

Sea $f(X) = a_n X^n + \cdots + a_1 X + a_0$ un polinomio con coeficientes reales y tal que $a_n > 0$. Si al dividir $f(X)$ por $X - a$, con $a \geq 0$, todos los coeficientes del cociente y del resto son no negativos, entonces a es una cota superior de las raíces reales de f.

Demostración. Supongamos que se cumplen las hipótesis de la proposición. Esto es, $f(X) \in \mathbb{R}[X]$, $a_n > 0$ y todos los coeficientes del cociente y resto de dividir $f(X)$ por $X - a$ son no negativos. Sea $q(X)$ el cociente de dividir $f(X)$ por $X - a$. Por el Teorema 5.43 tenemos que $f(X) = (X - a)q(X) + f(a)$. Por las hipótesis de la proposición sabemos que todos los coeficientes del cociente $q(X)$ y $f(a)$ son no negativos. Tomemos ahora un número real cualquiera b tal que $b > a \geq 0$. Como todos los coeficientes del polinomio $q(X)$ son no negativos, tenemos que $q(b) > 0$. Entonces, obtenemos lo siguiente

$$f(b) = \underbrace{(b-a)}_{>0}\underbrace{q(b)}_{>0} + \underbrace{f(a)}_{\geq 0} > 0.$$

Con lo cual, $f(b) \neq 0$, es decir, b no es una raíz de $f(X)$. Luego, toda raíz c de $f(X)$ debe ser $c \leq a$. En otras palabra, todas las raíces reales de f deben ser menores o iguales a a. ■

Ejemplo 5.70. Hallemos una cota superior para las raíces reales del polinomio $f(X) = X^5 + 2X^4 - 5X^3 + 8X^2 - 7X - 3$. Aplicando el Teorema 5.6 de Gauss, el lector puede comprobar que el polinomio $f(X)$ no tiene raíces racionales. Sin embargo, como el grado de f es impar, sabemos que tiene al menos una raíz real. Vamos a hallar una cota superior para las raíces reales de f. Para esto debemos dividir a $f(X)$ por un polinomio de la forma $X - a$, con $a \geq 0$, tal que los coeficientes del cociente y del resto sean no negativos. El objetivo sería tratar de hallar un valor pequeño de a. Comenzamos probando con $a = 1$. Dividimos a $f(X)$ por $X - 1$:

	1	2	-5	8	-7	-3
1		1	3	-2	6	-1
	1	3	-2	6	-1	-4

Observamos que uno (en realidad 2) de los coeficientes del cociente es negativo. Luego, no se cumplen las hipótesis de la regla de Laguerre-Thibault. Probemos ahora con $a = \frac{3}{2}$. Dividimos a $f(X)$ por $X - \frac{3}{2}$:

	1	2	-5	8	-7	-3
$\frac{3}{2}$		$\frac{3}{2}$	$\frac{21}{4}$	$\frac{3}{8}$	$\frac{201}{16}$	$\frac{267}{32}$
	1	$\frac{7}{2}$	$\frac{1}{4}$	$\frac{67}{8}$	$\frac{89}{16}$	$\frac{171}{32}$

Entonces, como todos los coeficientes del cociente y del resto son no negativos, podemos afirmar por la regla de Laguerre-Thibault que $\frac{3}{2}$ es una cota superior para las raíces reales de f. Esto es, si r es una raíz real de $f(X)$ entonces $r \leq \frac{3}{2}$.

Notemos que para aplicar la regla de Laguerre-Thibault el coeficiente principal del polinomio en cuestión debe ser positivo. ¿Qué sucede cuando el coeficiente principal es negativo?

Corolario 5.71

Sea $f(X) = a_n X^n + \cdots + a_1 X + a_0$ un polinomio con coeficientes reales y tal que $a_n < 0$. Entonces, a es una cota superior de las raíces reales de $f(X)$ si y sólo si a es una cota superior de las raíces reales del polinomio $-f(X)$.

Demostración. Es consecuencia del hecho que los polinomios $f(X)$ y $-f(X)$ tienen exactamente las mismas raíces. Entonces, una cota superior de las raíces reales de uno de ellos es una cota superior de las raíces reales del otro. ■

Ejemplo 5.72. Determinar una cota superior para las raíces reales del polinomio $f(X) = -2X^5 + 7X^2 - 3$. Por el corolario anterior, es equivalente a determinar una cota superior de las raíces reales del polinomio $-f(X) = 2X^5 - 7X^2 + 3$. Dividimos el polinomio $-f(X)$ por $X - 2$:

	2	0	0	-7	0	3
2		4	8	16	18	36
	2	4	8	9	18	39

Entonces, 2 es una cota superior de las raíces reales del polinomio $-f(X)$. Por lo tanto, 2 es una cota superior de las raíces reales de $f(X)$.

Sabemos cómo hallar una cota superior para las raíces reales de cualquier polinomio en $\mathbb{R}[X]$. Ahora veremos como podemos obtener cotas inferiores para las raíces reales.

Proposición 5.73

Sea $f(X)$ con coeficientes reales. Un número real $a < 0$ es cota inferior de las raíces reales de $f(X)$ si y sólo si $-a$ es una cota superior de las raíces reales del polinomio $f(-X)$.

Demostración. Sea $f(X) \in \mathbb{R}[X]$ y $a < 0$. Primero observemos lo siguientes:

$$c \text{ es una raíz de } f(X) \text{ si y sólo si } -c \text{ es una raíz de } f(-X).$$

($\Rightarrow$) Supongamos que $-a$ es una cota superior de las raíces reales de $f(-X)$. Esto es, $-a \geq c$, para toda raíz c de $f(-X)$. Sea c una raíz de $f(X)$. Entonces $-c$ es raíz de $f(-X)$. Entonces, por hipótesis, $-a \geq -c$. Con lo cual $a \leq c$. Así hemos probado que $a \leq c$ para toda raíz c de f. Por lo tanto, a es una cota inferior de las raíces reales de $f(X)$.

($\Leftarrow$) Análogamente. ■

Es decir que para hallar un cota inferior $a < 0$ para las raíces reales de un polinomio $f(X)$, debemos hallar una cota superior $-a > 0$ para las raíces del polinomio $f(-X)$.

Ejemplo 5.74. Hallar una cota inferior de las raíces reales del polinomio $f(X) = X^3 - 3X^2 + 5X + 4$. Por la Proposición 5.73, debemos determinar una cota superior de las raíces reales del polinomio $f(-X) = (-X)^3 - 3(-X)^2 + 5(-X) + 4 = -X^5 - 3X^2 - 5X + 4$. Como el coeficiente principal de $f(-X)$ es negativo, debemos hallar una cota superior de las raíces reales del polinomio $-f(-X) = X^5 + 3X^2 + 5X - 4$. Dividimos el polinomio $-f(-X)$ por $X - 1$:

	1	3	5	-4
1		1	4	9
	1	4	9	5

Entonces, 1 es una cota superior para las raíces reales del polinomio $-f(-X)$. Luego, 1 es cota superior de las raíces de $f(-X)$. Por lo tanto, -1 es un cota inferior de las raíces reales de $f(X)$.

Acotar las raíces reales de un polinomio $f(X)$ significa hallar una cota inferior a y una cota superior b de las raíces reales de $f(X)$. Entonces, podemos afirmar que las raíces reales de $f(X)$, si existen, se encuentran todas en el intervalo $[a, b]$. Es claro que deseamos obtener cotas inferiores y superiores útiles, en el sentido que tratamos de hallar una cota inferior lo más grande posible y hallar una cota superior lo más pequeña posible, para saber con mayor exactitud dónde se encuentran las raíces reales de $f(X)$. No es lo mismo afirmar que las raíces reales de $f(X)$ están en el intervalo $[-100, 100]$ que afirmar que están en el intervalo $[-5, 3]$, por ejemplo.

Ejemplo 5.75. Acotar las raíces reales del polinomio $f(X) = X^4 + X^3 - X^2 - X - 3$. Para resolver este ejemplo debemos hallar una cota inferior y una cota superior de las raíces del polinomio $f(X)$. Comenzamos por hallar una cota superior. Como el coeficiente principal de $f(X)$ es $1 > 0$ podemos aplicar directamente la regla de Laguerre-Thibault. Dividimos el polinomio $f(X)$ por $X - \frac{3}{2}$:

	1	1	-1	-1	-3
$\frac{3}{2}$		$\frac{3}{2}$	$\frac{15}{4}$	$\frac{33}{8}$	$\frac{75}{16}$
	1	$\frac{5}{2}$	$\frac{11}{4}$	$\frac{25}{8}$	$\frac{27}{16}$

Entonces, $\frac{3}{2}$ es una cota superior de las raíces reales de $f(X)$. Ahora pasamos a determinar una cota inferior de las raíces reales. Para ello, debemos hallar una cota superior de las raíces reales del polinomio $f(-X) = X^4 - X^3 - X^2 + X - 3$. Aplicamos la regla de Laguerre-Thibault. Dividimos el polinomio $f(-X)$ por $X - 2$:

	1	-1	-1	1	-3
2		2	2	2	6
	1	1	1	3	3

Entonces, 2 es una cota superior de las raíces reales de $f(-X)$. Luego, -2 es una cota inferior de las raíces reales de $f(X)$. Por lo tanto, concluimos que las raíces reales del polinomio $f(X)$ se encuentran en el intervalo $[-2, \frac{3}{2}]$.

Los resultados anteriores nos permitieron conocer entre que dos valores se encuentran las raíces reales de un polinomio. Ahora veremos dos resultados que nos permitirán tener una estimación del número de raíces reales. Es decir, saber aproximadamente cuántas raíces reales positivas y negativas tiene un polinomio.

Teorema 5.76: Regla de Descartes

Sea $f(X) = a_n X^n + \cdots + a_1 X + a_0$ un polinomio con coeficientes reales y ordenado en forma decreciente de las potencias de X. El número de raíces positivas de f contando multiplicidades es menor o igual que el número de variaciones de signo de los coeficientes de f, y difiere del mismo en un número par.

Ejemplo 5.77. Determinar el número de raíces reales positivas del polinomio $f(X) = X^5 + 2X^4 - 5X^3 + 8X^2 - 7X - 3$. Podemos observar que f tiene 3 variaciones de signo:

$$f(X) = X^5 \underbrace{+2X^4 - 5X^3}_{1 \text{ var}} + 8X^2 - 7X - 3 \qquad f(X) = X^5 + 2X^4 \underbrace{-5X^3 + 8X^2}_{2 \text{ var}} - 7X - 3$$

$$f(X) = X^5 + 2X^4 - 5X^3 \underbrace{+8X^2 - 7X}_{3 \text{ var}} - 3$$

El número de raíces positivas debe diferir del número de variaciones de signo en un número par. Esto es, si v es el número de variaciones de signo y r es el número de raíces positivas, entonces $v - r$ debe ser igual a un número par. Entonces, $3 - r = 0$ o $3 - r = 2$. Entonces, $r = 3$ o $r = 1$. Por lo tanto, el número de raíces reales positivas de f es 3 o 1.

Veamos ahora cómo podemos estimar el número de raíces reales negativas de un polinomio.

Corolario 5.78: Regla de Descartes

Sea $f(X) = a_n X^n + \cdots + a_1 X + a_0$ un polinomio con coeficientes reales y ordenado en forma decreciente de las potencias de X. El número de raíces negativas de f contando multiplicidades es menor o igual que el número de variaciones de signo de los coeficientes de $f(-X)$, y difiere del mismo en un número par.

Ejemplo 5.79. Hallar el número de raíces reales negativas del polinomio $f(X) = X^5 + 2X^4 - 5X^3 + 8X^2 - 7X - 3$. Para ello debemos primero determinar el número de variaciones de signo de los coeficientes del polinomio $f(-X) = -X^5 + 2X^4 + 5X^3 + 8X^2 + 7X - 3$. Podemos observar que hay dos variaciones de signo:

$$f(X) = \underbrace{-X^5 + 2X^4}_{1 \text{ var}} + 5X^3 + 8X^2 \underbrace{+7X - 3}_{2 \text{ var}}.$$

Entonces, si r denota el número de raíces negativas de f, tenemos que $2 - r$ debe ser igual a un número par. Luego, $2 - r = 0$ o $2 - r = 2$. Así $r = 2$ o $r = 0$. Por lo tanto, f tiene 2 o 0 raíces reales negativas.

Cerramos esta sección con una estrategia para determinar las raíces de un polinomio. Los pasos para hallar las raíces del un polinomio $f(X) \in \mathbb{R}[X]$ son:

(1) Acotar las raíces reales de $f(X)$ (esto es, hallar una cota inferior y una cota superior de las raíces reales de f).

(2) Determinar el número de raíces positivas y el número de raíces negativas de f.

(3) Determinar las posibles raíces racionales de f (Teorema 5.6 Gauss).

(4) Basarse en la información de los puntos (1) y (2) para determinar cuáles de las posibles raíces racionales (obtenidas en el punto (3)) son candidatas a ser efectivamente raíces de f.

(5) Aplicar la regla de Ruffini con las posibles raíces obtenidas en el punto anterior. Teniendo en cuenta los puntos (1) y (2), repetir este paso con todos los valores convenientes del punto anterior.

Ejemplo 5.80. Hallar las raíces del polinomio $f(X) = 2X^8 - 7X^7 - 8X^6 + 44X^5 + X^4 - 85X^3 + 11X^2 + 48X + 12$. Vamos a seguir los pasos de la estrategia anterior.

Ejercicios propuestos

Ejercicio 5.1. Sean $f(X), g(X) \in \mathrm{K}[X]$. Probar que:

(a) $\mathrm{cp}(f.g) = \mathrm{cp}(f).\mathrm{cp}(g)$.

(b) $\mathrm{ti}(f.g) = \mathrm{ti}(f).\mathrm{ti}(g)$.

Ejercicio 5.2. Probar las propiedades 1., 2. y 3. de la Proposición 5.23.

Ejercicio 5.3. Sean $f(X), g(X) \in \mathrm{K}[X]$ y sea $a \in \mathrm{K}$. Probar los siguiente.

(a) $f \mid g \iff a.f \mid g$.

(b) $f \mid g \iff f \mid a.g$.

(c) Si $f \mid g$ y $\mathrm{gr}(f) = \mathrm{gr}(g)$, entonces $g = c.f$ para alguna constante $c \in \mathrm{K}$.

Ejercicio 5.4. Sea $f(X) \in \mathbb{R}[X]$ de grado 2. Probar que $f(X)$ es irreducible en $\mathbb{R}[X]$ si y sólo si $f(X)$ no tiene raíces reales.

Ejercicio 5.5. Completar la prueba de la Proposición 5.73.

Capítulo 6

Estructuras Algebraicas

Una buena cantidad de ejemplos, tantos como sea posible, es indispensable para una comprensión profunda de cualquier concepto, y cuando quiero aprender algo nuevo, mi primer trabajo es construir uno.

—-Paul R. Halmos

6.1. Leyes de composición internas

Definición 6.1

Sea A un conjunto. Una **ley de composición interna** sobre A es una función

$$*\colon A \times A \to A.$$

En otras palabras, una ley de composición interna $*\colon A \times A \to A$ sobre A es una regla que asigna a cada par (a, b) de elementos de A un único elemento $a * b$ de A. Esto es,

$$\begin{array}{rccc} *\colon & A \times A & \to & A \\ & (a, b) & \mapsto & a * b \end{array}$$

Ejemplo 6.2. La operación suma (+) de números naturales es una ley de composición interna sobre $\mathbb{N}$, porque para cada par de números naturales $(m, n) \in \mathbb{N} \times \mathbb{N}$, le corresponde uno y sólo un elemento de $\mathbb{N}$: $m + n$. Lo que estamos diciendo es que efectivamente la operación suma es una función de $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$, en símbolos, $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Ejemplo 6.3. Consideremos la operación resta (-) entre números naturales. Esto es, a cada par (m, n) de números naturales le hacemos corresponder el número $m - n$. Esta asignación no es una ley de composición interna sobre $\mathbb{N}$, porque no se cumple que a todo para (m, n) de números naturales le hace corresponder uno y sólo un número natural. Por ejemplo, al par (3,7) le hace corresponder el valor $3 - 7 = -4$ que no pertenece a $\mathbb{N}$. Sin embargo, si consideramos la operación resta entre números enteros, entonces es efectivamente una ley de composición interna sobre $\mathbb{Z}$.

Ejemplo 6.4. Definimos la operación $\oplus$ sobre $\mathbb{Z}$ como sigue:

$$a \oplus b = a + b - 3, \quad \text{para cada par } (a, b) \in \mathbb{Z} \times \mathbb{Z}.$$

La operación $\oplus$ es una ley de composición interna sobre $\mathbb{Z}$ porque para cada par (a, b) de enteros, la suma $a + b$ es un entero, y la diferencia $a + b - 3$ es también un entero. Entonces, $a \oplus b$ es un entero. Por ejemplo

$$3 \oplus 6 = 3 + 6 - 3 = 6, \qquad (-2) \oplus 8 = (-2) + 8 - 3 = 3, \qquad (-1) \oplus 0 = (-1) + 0 - 3 = -4.$$

Ejemplo 6.5. Sean A y B dos conjuntos no vacíos. Definimos la operación

$$\bowtie : (A \times B) \times (A \times B) \to (A \times B)$$

sobre $A \times B$ como sigue: para $(a_1, b_1), (a_2, b_2) \in A \times B$,

$$(a_1, b_1) \bowtie (a_2, b_2) = (a_1, b_2).$$

La asignación $\bowtie$ es de hecho una ley de composición interna. En efecto, dados dos elementos $(a_1, b_1), (a_2, b_2) \in A \times B$, tenemos que $(a_1, b_1) \bowtie (a_2, b_2) = (a_1, b_2) \in A \times B$, pues $a_1 \in A$ y $b_2 \in B$. ■

Problema 6.6

Determinar si las siguientes asignaciones son leyes de composición internas sobre los correspondientes conjuntos.

(a) La operación producto sobre $\mathbb{Z}$: $(a, b) \mapsto a.b$.

(b) La operación división sobre $\mathbb{Z}$: $(a, b) \mapsto a/b$.

(c) La operación división sobre $\mathbb{Q}$: $(a, b) \mapsto a/b$.

(d) La operación $\odot$ sobre $\mathbb{N}$: $(a, b) \mapsto a \odot b = a.b + 5$.

Ahora que sabemos qué es una ley de composición interna, deseamos estudiar qué propiedades satisfacen estas operaciones. Por ejemplo, si consideramos la suma en $\mathbb{Z}$, lo enteros, sabemos que la suma es asociativa: $a + (b + c) = (a + b) + c$; es conmutativa: $a + b = b + a$; el cero cumple que $a + 0 = a$ para todo $a \in \mathbb{Z}$; y para cada $a \in \mathbb{Z}$, existe un entero $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$. Vamos a generalizar estas propiedades.

Definición 6.7

Sea A un conjunto y $*\colon A \times A \to A$ una ley de composición interna.

- Diremos que la operación $*$ es **asociativa** si se cumple que

$$a * (b * c) = (a * b) * c, \qquad \text{para todos } a, b, c \in A.$$

- Diremos que $*$ es **conmutativa** si cumple que

$$a * b = b * a, \qquad \text{para todos } a, b \in A.$$

- Diremos que un elemento $e \in A$ es **neutro** (con respecto a $*$) si

$$e * a = a \ \text{ y } \ a * e = a, \qquad \text{para todo } a \in A.$$

- Sea e un elemento neutro. Diremos que un elemento $a \in A$ es **invertible** si existe un elemento $b \in A$ tal que

$$a * b = e \ \text{ y } \ b * a = e.$$

  En tal caso, diremos que b es el **inverso** de a.

Ejemplo 6.8. Recordemos la operación $\oplus$ sobre $\mathbb{Z}$ del Ejemplo 6.4: para $a, b \in \mathbb{Z}$,

$$a \oplus b = a + b - 3.$$

Veamos qué propiedades cumple dicha operación.

- ¿Es $\oplus$ asociativa? Sean $a, b, c \in \mathbb{Z}$.

$$a \oplus (b \oplus c) = a \oplus (b + c - 3) = a + (b + c - 3) - 3 = a + b + c - 6 \tag{6.1}$$

  y

$$(a \oplus b) \oplus c = (a + b - 3) \oplus c = (a + b - 3) + c - 3 = a + b + c - 6. \tag{6.2}$$

  De (6.1) y (6.2) podemos observar que $a \oplus (b \oplus c) = (a \oplus b) \oplus$. Entonces, $\oplus$ es asociativa.

- ¿Es $\oplus$ conmutativa? Sean $a, b \in \mathbb{Z}$.

$$a \oplus b = a + b - 3 = b + a - 3 = b \oplus a.$$

  Por lo tanto, $\oplus$ es conmutativa.

- ¿Existe algún elemento $e \in \mathbb{Z}$ tal que $a \oplus e = a$[1], para todo $a \in \mathbb{Z}$? Sea $a \in \mathbb{Z}$. Planteamos la siguiente ecuación:

$$a \oplus x = a \implies a + x - 3 = a \implies x = 3.$$

[1] Observe que es suficiente verificar que se cumple que $a \oplus e = a$, porque ya que $\oplus$ es conmutativa, entonces $e \oplus a = a \oplus e = a$.

Ahora comprobamos que 3 es un elemento neutro para $\oplus$:

$$a \oplus 3 = a + 3 - 3 = a.$$

Efectivamente, 3 es un elemento neutro.

- Sabiendo que 3 es el elemento neutro con respecto a $\oplus$, veamos que elementos de $\mathbb{Z}$ son invertibles. Sea $a \in \mathbb{Z}$. Planteamos la ecuación:

$$a \oplus x = 3 \implies a + x - 3 = 3 \implies x = 6 - a.$$

Ahora comprobemos que cada $a \in \mathbb{Z}$ es invertible con elemento inverso $6 - a \in \mathbb{Z}$:

$$a \oplus (6 - a) = a + (6 - a) - 3 = 3.$$

Por lo tanto, todo $a \in \mathbb{Z}$ es invertible, y su inverso es $6 - a$.

Ejemplo 6.9. Sea X un conjunto no vacío y sea $\mathcal{P}(X) = \{A : A \subseteq X\}$ el conjunto de partes de X. Consideremos la unión de conjuntos:

$$\cup \colon \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X).$$

Si $A, B \in \mathcal{P}(X)$, entonces $A, B \subseteq X$. Luego $A \cup B \subseteq X$. Entonces $A \cup B \in \mathcal{P}(X)$. Por lo tanto, la unión de conjuntos es una ley de composición interna sobre $\mathcal{P}(X)$. Recordando lo que sabemos sobre el álgebra de conjuntos, vamos a determinar qué propiedades cumple la unión.

- $\cup$ es asociativa: $A \cup (B \cup C) = (A \cup B) \cup C$, para todos $A, B, C \in \mathcal{P}(X)$.
- $\cup$ es conmutativa: $A \cup B = B \cup A$, para todos $A, B \in \mathcal{P}(X)$.
- $\emptyset \in \mathcal{P}(X)$ es el elemento neutro: para cada $A \in \mathcal{P}(X)$, $A \cup \emptyset = A$.
- No todos los elementos de $\mathcal{P}(X)$ tienen inverso. Sea $A \subseteq X$ tal que $A \neq \emptyset$. Entonces $\emptyset \neq A \subseteq A \cup B$, para todo $B \in \mathcal{P}(X)$. Luego, $A \cup B \neq \emptyset$, para todo $B \in \mathcal{P}(X)$. Con lo cual A no tiene inverso.

Ejemplo 6.10. Sea $\circledast \colon (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z})$ definida por

$$(a, b) \circledast (c, d) = (ad + c, bd).$$

Es directo notar que $\circledast$ es una ley de composición interna sobre $\mathbb{Z} \times \mathbb{Z}$. Veamos qué propiedades satisface $\circledast$ sobre $\mathbb{Z} \times \mathbb{Z}$.

- ¿Es $\circledast$ asociativa? Sean $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}$. Tenemos que

$$(a, b) \circledast [(c, d) \circledast (e, f)] = (a, b) \circledast (cf + e, df) = (adf + cf + c, bdf) \tag{6.3}$$

y

$$[(a, b) \circledast (c, d)] \circledast (e, f) = (ad + c, bd) \circledast (e, f) = (adf + cf + c, bdf). \tag{6.4}$$

Entonces, de (6.3) y (6.4) obtenemos que $(a, b) \circledast [(c, d) \circledast (e, f)] = [(a, b) \circledast (c, d)] \circledast (e, f)$. Por lo tanto, $\circledast$ es asociativa.

- ¿Es $\circledast$ conmutativa? Sean $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}$. Tenemos que

$$(a,b) \circledast (c,d) = (ad+c, bd) \quad \text{y} \quad (c,d) \circledast (a,b) = (cb+a, db).$$

Podemos observar que $ad+c$ no es necesariamente igual $cb+a$. Así, $\circledast$ no debe ser conmutativa. Demos un ejemplo concreto para ver esto. Sean $(1,2),(-2,3) \in \mathbb{Z} \times \mathbb{Z}$. Calculamos

$$\begin{aligned}(1,2) \circledast (-2,3) &= (1.3+(-2), 2.3) = (1,6)\\ (-2,3) \circledast (1,2) &= (-2.2+1, 3.2) = (-3,6).\end{aligned}$$

Entonces, $(1,2) \circledast (-2,3) \neq (-2,3) \circledast (1,2)$. Conclusión, $\circledast$ no es conmutativa.

- ¿Existe un elemento neutro? Sea $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ y plantemos la siguiente ecuación

$$\begin{aligned}(a,b) \circledast (x,y) &= (a,b)\\ (ay+x, by) &= (a,b)\\ ay+x = a \text{ y } by &= b.\end{aligned}$$

Si suponemos que $b \neq 0$, entonces $by = b$ implica que $y = 1$. Reemplazando $y = 1$ en $ay + x = a$ obtenemos que $x = 0$. Entonces, el candidato a ser neutro es $(0,1)$. Veamos si efectivamente lo es. Sea $(a,b) \in \mathbb{Z}$,

$$(a,b) \circledast (0,1) = (a.1+0, b.1) = (a,b).$$

Por lo tanto, $e = (0,1)$ es el neutro.

- ¿Cada elemento $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ es invertible? Sea $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ y planteamos la siguiente ecuación:

$$\begin{aligned}(a,b)(x,y) &= (0,1)\\ (ay+x, by &= (0,1)\\ ay+x = 0 \text{ y } by &= 1.\end{aligned}$$

De $by = 1$, obtenemos que $b = 1$ (e $y = 1$) o $b = -1$ (e $y = -1$). Luego, no todos los elementos de $\mathbb{Z} \times \mathbb{Z}$ son invertibles. En efecto, por ejemplo, $(1,3)$ no tiene inverso, porque $3 \neq 1, -1$. ■

Problema 6.11

Se define la operación $\diamond$: $(\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z})$ por:

$$(a,b) \diamond (c,d) = (a+c, b+d).$$

Determinar si $\diamond$ es efectivamente una ley de composición interna y qué propiedades satisface.

Ahora veremos dos propiedades importantes acerca de las leyes de composición interna. La primer propiedad nos dice que para una ley de composición interna puede haber a lo sumo un elemento neutro. Es decir, si e y d son elementos neutros (con respecto a una misma ley de composición interna), entonces $e = d$.

Proposición 6.12

Sea $*\colon A \times A \to A$ una ley de composición interna asociativa. Sean e y d dos elementos de A tales que

$$a * e = a \quad \text{y} \quad e * a = a, \ \forall a \in A \tag{6.5}$$

y

$$a * d = a \quad \text{y} \quad d * a = a, \ \forall a \in A. \tag{6.6}$$

Entonces, $e = d$.

Demostración. Supongamos que e y d cumplen (6.5) y (6.6), respectivamente. Por (6.5) tenemos que $d * e = d$ (pues se cumple para todo elemento de A, en particular para el d). Por otro lado, usando (6.6), tenemos que $d * e = e$ (pues se cumple para todo elemento de A, en particular para el e). Entonces, tenemos que:

$$d \overset{(6.5)}{=} d * e \overset{(6.6)}{=} e \implies d = e.$$

■

La segunda propiedad nos dice que para una ley de composición interna, si un elemento a es invertible, entonces su inverso es único.

Proposición 6.13

Sea $*\colon A \times A \to A$ una ley de composición interna asociativa y sea e el elemento neutro. Sea $a \in A$. Supongamos que b y c son dos elementos de A que satisfacen lo siguiente:

$$a * b = e \quad \text{y} \quad b * a = e \tag{6.7}$$

y

$$a * c = e \quad \text{y} \quad c * a = e. \tag{6.8}$$

Entonces $b = c$.

Demostración. Sea $a \in A$ y supongamos que b y c son dos elementos que cumples (6.7) y (6.8), respectivamente. Entonces,

$$\begin{aligned}
a * b &= e && \text{por (6.7)} \\
c * (a * b) &= c * e && \text{operamos a izquierda miembro a miembro por } c \\
(c * a) * b &= c && \text{usamos asociativa y que } e \text{ es neutro} \\
e * b &= c && \text{por (6.8)} \\
b &= c. &&
\end{aligned}$$

■

6.2. Grupos

Definición 6.14

Diremos que un par $\langle G, * \rangle$ es un **grupo** si G es un conjunto no vacío y $*$ es una ley de composición interna sobre G que cumple las siguiente propiedades.

- $*$ es asociativa.
- Existe un elemento neutro e (con respecto a $*$).
- Cada elemento de G es invertible (con respecto a $*$).

Diremos que un grupo $\langle G, * \rangle$ es **abeliano** si además $*$ es conmutativa.

Observemos que por la Proposición 6.12 sabemos que el elemento neutro de un grupo G es único. Usualmente denotaremos por e al elemento neutro. Y por la Proposición 6.13 tenemos que el inverso de cada elemento de un grupo G es también único. Es decir, si a es un elemento de un grupo G, entonces existe un único elemento b tal que $a * b = e$ y $b * a = e$. Para cada elemento a de un grupo G, denotaremos por a^{-1} a su elemento inverso. Esto es, para cada $a \in G$, $a^{-1} \in G$ y es el único tal que $a * a^{-1} = e$ y $a^{-1} * a = e$.

A menudo al inverso de un elemento a lo llamaremos **opuesto** y lo denotaremos por $-a$ en lugar de a^{-1}.

Ejemplo 6.15. Sabemos que la operación suma entre enteros es asociativa, conmutativa, existe el $0 \in \mathbb{Z}$ tal que $a + 0 = 0$ para todo $a \in \mathbb{Z}$ y para cada entero a, existe su opuesto $-a$ tal que $a + (-a) = 0$. Por lo tanto, $\langle \mathbb{Z}, + \rangle$ es un grupo abeliano. De forma similar tenemos que $\langle \mathbb{R}, + \rangle$ es también un grupo abeliano (ver **??**).

Ejemplo 6.16. En la Sección 4.1 (véase Proposición 4.3) probamos que la operación suma entre números complejos es asociativa, conmutativa, tiene un elemento neutro y que todo complejo tiene un opuesto. Por lo tanto, $\langle \mathbb{C}, + \rangle$ es un grupo abeliano.

Ejemplo 6.17. Consideremos el producto . usual sobre $\mathbb{R}$. Es claro que el producto . es una ley de composición interna sobre $\mathbb{R}$, que es asociativa, conmutativa y 1 es elemento neutro. Pero $\langle \mathbb{R}, . \rangle$ no es un grupo. Cada $a \in \mathbb{R}$ no nulo, tiene un inverso que es $\frac{1}{a}$. Pero el 0 no tiene inverso, es decir, no existe ningún número real b tal que $0.b = 1$. Entonces, en $\mathbb{R}$ no todos los elementos son invertibles. Ahora si $\mathbb{R}^* = \{a \in \mathbb{R} : a \neq 0\}$, entonces es claro que $\langle \mathbb{R}^*, . \rangle$ es efectivamente un grupo abeliano.

Ejemplo 6.18. Recordemos la ley de composición interna $\oplus$ sobre $\mathbb{Z}$ dada en el Ejemplo 6.1. En el Ejemplo 6.2 probamos que $\oplus$ es asociativa, conmutativa, que $e = 3$ es el elemento neutro, y que para cada $a \in \mathbb{Z}$, $6 - a$ es el inverso de a. Por lo tanto, $\langle \mathbb{Z}, \oplus \rangle$ es un grupo abeliano.

Quizás en estos momentos el lector se estará preguntando si hay grupos que no sean abelianos. La respuesta es sí, hay y de hecho muchos grupos que no son abelianos, pero ellos son un poco menos habituales que los abelianos, pero igualmente importantes.

Ejemplo 6.19. Sea X un conjunto y consideremos el conjunto

$$\mathcal{F}(X) = \{f\colon X \to X : f \text{ es biyectiva}\}.$$

En palabras, $\mathcal{F}(X)$ es el conjunto de todas las funciones biyectivas de X en X. Vamos definir una operación sobre $\mathcal{F}(X)$ como sigue: sea

$$\circ\colon \mathcal{F}(X) \times \mathcal{F}(X) \to \mathcal{F}(X)$$

definida por: para $f, g \in \mathcal{F}(X)$,

$$f \circ g \text{ es la función composición de } f \text{ con } g$$

esto es, $(f \circ g)(x) = f(g(x))$ (véase **??**). Veamos que $\langle \mathcal{F}(X), \circ \rangle$ es un grupo, y que no es abeliano.

- $\circ$ es asociativa. Ya fue probado en **??**.
- Existencia de elemento neutro. Sea $id_X\colon X \to X$ la función identidad, esto es, $id_X(x) = x$ para todo $x \in X$. Es claro que id_X es biyectiva (véase **??**). Ahora probemos que $id_X \circ f = f$ y $f \circ id_X = f$, para toda $f \in \mathcal{F}(X)$. Sea $f \in \mathcal{F}(X)$. Tomemos un $x \in X$. Tenemos que

  $$(id_X \circ f)(x) = id_X(f(x)) = f(x) \quad \text{y} \quad (f \circ id_X)(x) = f(id_X(x)) = f(x).$$

  Entonces $id_X \circ f = f$ y $f \circ id_X = f$. Por lo tanto, $id_X \in \mathcal{F}(X)$ es el elemento neutro.
- Elementos invertibles. Sea $f \in \mathcal{F}(X)$. Como $f\colon X \to X$ es biyectiva, existe su función inversa $f^{-1}\colon X \to X$ la cual es también biyectiva. Entonces, $f^{-1} \in \mathcal{F}(X)$ y cumple con

  $$f \circ f^{-1} = id_X \quad \text{y} \quad f^{-1} \circ f = id_X.$$

  Entonces, f^{-1} es el inverso de f. Por lo tanto, cada elemento de $\mathcal{F}(X)$ es invertible.

Por lo tanto, podemos concluir que $\langle \mathcal{F}(X), \circ \rangle$ es un grupo. Veamos que este grupo no es abeliano. Sea $X = \{a, b, c\}$. Consideremos las funciones $f\colon X \to X$ y $g\colon X \to X$ definidas por

x	$f(x)$
a	b
b	c
c	a

x	$g(x)$
a	c
b	b
c	a

Ahora, calculamos, por ejemplo,

$$(f \circ g)(a) = f(g(a)) = f(c) = a \quad \text{y} \quad (g \circ f)(a) = g(f(a)) = g(b) = b.$$

Luego, como $(f \circ g)(a) \neq (g \circ f)(a)$, tenemos que $f \circ g \neq g \circ f$. Por lo tanto, $\circ$ no es conmutativa, y así el grupo $\langle \mathcal{F}(X), \circ \rangle$ no es abeliano. ■

Problema 6.20

Sea $M(\mathbb{R}, 2)$ el conjunto de todas las matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cuadradas de 2×2 con entradas reales ($a, b, c, d \in \mathbb{R}$). Probar que $M(\mathbb{R}, 2)$ con la suma usual de matrices es un grupo abeliano. Recuerde que la suma de matrices se define como sigue:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

Veamos algunos propiedades básicas que nos ayudarán a la hora de operar algebraicamente en grupo.

Proposición 6.21

Sea $\langle G, * \rangle$ un grupo. Entonces, para todos $a, b, c \in G$ se cumplen las siguientes propiedades.

1. Si $a * b = a * c$, entonces $b = c$.
2. $(a * b)^{-1} = b^{-1} * a^{-1}$.
3. $(a^{-1})^{-1} = a$.

Demostración. 1. Procedemos como sigue:

$$\begin{aligned} a * b &= a * c && \text{hipótesis} \\ a^{-1} * (a * b) &= a^{-1} * (a * c) && \text{operamos miembro a miembro por } a^{-1} \\ (a^{-1} * a) * b &= (a^{-1} * a) * c && \text{por propiedad asociativa} \\ e * b &= e * c \\ b &= c. \end{aligned}$$

2. Vamos a probar que $b^{-1} * a^{-1}$ es el inverso de $a * b$. Tenemos que

$$\begin{aligned} (b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b && \text{por propiedad asociativa} \\ &= b^{-1} * e * b \\ &= b^{-1} * b \\ &= e. \end{aligned}$$

De igual forma obtenemos que

$$(a * b) * (b^{-1} * a^{-1}) = e.$$

Entonces, como el inverso de un elemento es único (véase página 121), tenemos que el inverso de $a * b$ es $b^{-1} * a^{-1}$, esto es, $(a * b)^{-1} = b^{-1} * a^{-1}$.

3. Dado a^{-1} es el inverso de a, tenemos que

$$\begin{aligned} a * a^{-1} &= e \\ (a * a^{-1}) * (a^{-1})^{-1} &= e * (a^{-1})^{-1} \\ a * (a^{-1} * (a^{-1})^{-1})) &= (a^{-1})^{-1} \\ a * e &= (a^{-1})^{-1} \\ a &= (a^{-1})^{-1}. \end{aligned}$$

■

Problema 6.22

Sea $\langle G, * \rangle$ un grupo. Operar algebraicamente para las siguientes expresiones.

1. $(a^{-1} * b)^{-1}$.
2. $(c^{-1} * a * b^{-1})^{-1}$.

Problema 6.23

Sea $\langle G, * \rangle$ un grupo.

1. Probar por inducción que para todo $n \in \mathbb{N}$ y $a_1, a_2, \ldots, a_n \in G$ se cumple

$$(a_1 * a_2 * \cdots * a_{n-1} * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_2^{-1} * a_1^{-1}.$$

2. Probar que $(a^{-1} * c * d^{-1} * b^{-1})^{-1} = b * d * c^{-1} * a$.

En todo grupo $\langle G, . \rangle$ podemos definir inductivamente las potencias enteras como sigue: para cada $a \in G$,

$$\begin{cases} a^0 = e \\ a^n = a^{n-1}.a & \forall n \geq 1 \\ a^{-n} = (a^{-1})^n & \forall n \geq 1. \end{cases}$$

Observemos que si $n \geq 1$, entonces tenemos que

$$a^n = \underbrace{a.a.\ldots.a}_{n \text{ veces}}$$

y

$$a^{-n} = (a^{-1})^n = \underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{n \text{ veces}}.$$

Ahora probamos que se cumplen las propiedades usuales de las potencias.

Proposición 6.24

Sea $\langle G, . \rangle$ un grupo. Entonces, para todo $a \in G$ y para todos $m, n \in \mathbb{Z}$, se cumplen:

1. $a^m.a^n = a^{m+n}$,
2. $(a^n)^{-1} = a^{-n}$.
3. $(a^{-1})^n = a^{-n}$.
4. $(a^m)^n = a^{m.n}$.

Demostración. Sea $a \in G$. Sean $m, n \in \mathbb{Z}$.

1. Vamos probarlo para los distintos casos.

Caso 1: $m, n \geq 0$. Entonces,

$$a^m.a^n = (\underbrace{a.a.\ldots.a}_{m \text{ veces}})(\underbrace{a.a.\ldots.a}_{n \text{ veces}}) = \underbrace{a.a.\ldots.a.a.a.\ldots.a}_{m+n \text{ veces}} = a^{m+n}.$$

Caso 2: $m \geq 0$ y $n < 0$. Entonces,

$$a^m.a^n = a^m.(a^{-1})^{-n} = \underbrace{a.a.\ldots.a}_{m \text{ veces}}.\underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{-n \text{ veces}}.$$

Ahora, si $m \leq -n$, entonces

$$a^m.a^n = \underbrace{a.a.\ldots.a}_{m \text{ veces}}.\underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{-n \text{ veces}} = \underbrace{a^{-1}.\ldots.a^{-1}}_{-n-m \text{ veces}} = (a^{-1})^{-n-m} = a^{m+n}.$$

Si $m > -n$, entonces

$$a^m.a^n = \underbrace{a.a.\ldots.a}_{m \text{ veces}}.\underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{-n \text{ veces}} = \underbrace{a.\ldots.a}_{m-(-n) \text{ veces}} = a^{m+n}.$$

Entonces, $a^m.a^n = a^{m+n}$.

Caso 3: $m < 0$ y $n \geq 0$. Análogamente al caso anterior.

Caso 4: $m < 0$ y $n < 0$. Entonces,

$$\begin{aligned} a^m.a^n &= (a^{-1})^{-m}.(a^{-1})^{-n} = \underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{-m \text{ veces}}.\underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}}_{-n \text{ veces}} \\ &= \underbrace{a^{-1}.a^{-1}.\ldots.a^{-1}.a^{-1}.a^{-1}.\ldots.a^{-1}}_{-m-n \text{ veces}} = (a^{-1})^{-m-n} = a^{m+n}. \end{aligned}$$

2. Por el 1. tenemos que $a^n.a^{-n} = a^{n-n} = a^0 = e$. Entonces,

$$\begin{aligned} a^n.a^{-n} &= e \\ (a^n)^{-1}.a^n.a^{-n} &= (a^n)^{-1}.e \\ ((a^n)^{-1}.a^n).a^{-n} &= (a^n)^{-1} \\ e.a^{-n} &= (a^n)^{-1} \\ a^{-n} &= (a^n)^{-1}. \end{aligned}$$

3. y 4. quedan como ejercicio al lector. ■

Antes de continuar con el estudio general de grupos veamos el siguiente ejemplo que será a su vez fuente de muchos grupos abelianos.

Ejemplo 6.25. Sea $n \in \mathbb{N}$. Consideremos la congruencia $\equiv_n$ módulo n y consideremos el conjunto cociente $\mathbb{Z}/\equiv_n$, que lo denotaremos de aquí en adelante por $\mathbb{Z}_n$. Entonces por la Proposición 3.18 tenemos que

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

Recordemos también que para todo entero a, $[a]_n = [r]_n$ para algún $r = 0, 1, \ldots, n-1$ (los restos posibles de dividir a por n). Definimos sobre el conjunto $\mathbb{Z}_n$ una operación suma

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

como sigue: para cada $[a]_n, [b]_n \in \mathbb{Z}_n$,

$$[a]_n + [b]_n = [a+b]_n. \tag{6.9}$$

Veamos que $\mathbb{Z}_n$ con la suma definida en (6.9) es un grupo abeliano.

- $+$ es una ley de composición interna. En efecto, sea r el resto de dividir $a+b$ por n. Entonces $[a]_n + [b]_n = [a+b]_n = [r]_n$.
- Asociativa: sean $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$, entonces

$$\begin{aligned}
[a]_n + ([b]_n + [c]_n) &= [a]_n + [b+c]_n && \text{por (6.9)} \\
&= [a + (b+c)]_n && \text{por (6.9)} \\
&= [(a+b) + c]_n && \text{por la asociativa de la suma en } \mathbb{Z} \\
&= [a+b]_n + [c]_n && \text{por (6.9)} \\
&= ([a]_n + [b]_n) + [c]_n && \text{por (6.9)}
\end{aligned}$$

  Entonces, $[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$. Por lo tanto, la suma es asociativa.
- Conmutativa: sean $[a]_n, [b]_n \in \mathbb{Z}_n$, entonces

$$[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n.$$

  Entonces, la suma es conmutativa.
- El elemento $[0]_n \in \mathbb{Z}_n$ es el neutro. En efecto, sea $[a]_n \in \mathbb{Z}_n$, entonces

$$[a]_n + [0]_n = [a+0]_n = [a]_n.$$

- Inverso. Sea $[a]_n \in \mathbb{Z}_n$. Sea r el resto de dividir $-a$ por n. Entonces, tenemos que $[-a]_n = [r]_n \in \mathbb{Z}_n$ y $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n$. Por lo tanto, $[-a]_n$ es el inverso de $[a]_n$.

Por lo tanto, hemos probado que $\langle \mathbb{Z}_n, + \rangle$ es un grupo abeliano.

+	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

Cuadro 6.1: Tabla de la operación suma en $\mathbb{Z}_5$

Ejemplo 6.26. Tomando $n = 5$, sabemos por el ejemplo anterior que $\langle \mathbb{Z}_5, + \rangle$ es un grupo abeliano con $[a]_5 + [b]_5 = [a+b]_5$. Por ejemplo,

$$[2]_5 + [4]_5 = [2+4]_5 = [6]_5 = [1]_5 \quad \text{y} \quad [4]_5 + [4]_5 = [8]_5 = [3]_5.$$

Vamos a construir una tabla con todas las operaciones, dejamos los cálculos al lector. Véase la Tabla 6.1.

Observando la tabla podemos ver por ejemplo que el inverso de $[2]_5$ es $[3]_5$ y el inverso de $[1]_5$ es $[4]_5$. ■

6.2.1. Subgrupos

Definición 6.27

Sea $\langle G, . \rangle$ un grupo. Diremos que un subconjunto $H \subseteq G$ es un **subgrupo de** G si cumple lo siguiente:

1. $e \in H$;
2. si $a, b \in H$, entonces $a.b \in H$;
3. si $a \in H$, entonces $a^{-1} \in H$.

Ejemplo 6.28. Sea $\langle G, . \rangle$ un grupo. Entonces los subconjuntos $\{e\}$ y G de G son subgrupos de G. Estos son llamados los subgrupos triviales de G. Por ejemplo, tenemos $\{0\}$ y $\mathbb{Z}$ son los subgrupos triviales del grupo $\langle \mathbb{Z}, + \rangle$. ■

Ejemplo 6.29. Consideremos el grupo multiplicativo $\langle \mathbb{R} - \{0\}, . \rangle$ con el producto usual de reales. Entonces, $\mathbb{Q} - \{0\}$ es un subgrupo de $\mathbb{R} - \{0\}$. Veamos que se cumplen las tres condiciones de la Definición 6.27:

1. El neutro del grupo $\mathbb{R} - \{0\}$ es 1. Y 1 es un racional no nulo, entonces $1 \in \mathbb{Q} - \{0\}$.
2. Sean $a, b \in \mathbb{Q} - \{0\}$. Entonces $a = \frac{m}{n}$ y $b = \frac{s}{t}$ son $m, n, s, t \in \mathbb{Z} - \{0\}$. Luego,

$$a.b = \frac{m}{n} \cdot \frac{s}{t} = \frac{m.s}{n.t} \in \mathbb{Q} - \{0\}$$

ya que $m.s$ y $n.t$ son enteros no nulos.

3. Sea $a \in \mathbb{Q} - \{0\}$. Entonces existen $m, n \in \mathbb{Z} - \{0\}$ tal que $a = \frac{m}{n}$. Entonces,

$$a^{-1} = \left(\frac{m}{n}\right)^{-1} = \frac{n}{m} \in \mathbb{Q} - \{0\}.$$

Por lo tanto, $\mathbb{Q} - \{0\}$ es un subgrupo de $\mathbb{R} - \{0\}$. ■

Ejemplo 6.30. Consideremos nuevamente el grupo multiplicativo $\langle \mathbb{R} - \{0\}, . \rangle$ con el producto usual de reales. Sea

$$H = \{x \in \mathbb{R} - \{0\} : x = 1 \text{ o } x \text{ es un irracional}\}.$$

¿Es H un subgrupo de $\mathbb{R} - \{0\}$? Veamos si satisface las condiciones de la Definición 6.27.

1. El neutro del grupo $\mathbb{R} - \{0\}$ es 1, y $1 \in H$ por definición de H.

2. Sean $a, b \in H$. Si a y b son irracionales, ¿$a.b$ es un irracional? La respuesta es no necesariamente. Veamos un ejemplo concreto. Sean $\sqrt{2}, \sqrt{8} \in H$. Ahora $\sqrt{2}.\sqrt{8} = \sqrt{16} = 4$ y claramente 4 no es un irracional. Entonces $\sqrt{2}.\sqrt{8} \notin H$. Por lo tanto, H no es un subgrupo de $\mathbb{R} - \{0\}$. ■

Problema 6.31

Considerar el grupo abeliano $\langle \mathbb{C}, + \rangle$ de los números complejos con la suma usual de complejos. Probar que el conjunto $H = \{z \in \mathbb{C} : z = a + b\sqrt{2}i \text{ con } a, b \in \mathbb{Z}\}$ es un subgrupo de $\langle \mathbb{C}, + \rangle$.

6.3. Anillos

Muchos de los conjuntos numéricos con los que hemos trabajado hasta el momento, como por ejemplo $\mathbb{Z}$, $\mathbb{R}$ y $\mathbb{C}$, tienen asociados dos leyes de composición interna. Por ejemplo, los conjuntos $\mathbb{Z}$, $\mathbb{R}$ y $\mathbb{C}$ tienen asociadas dos operaciones: la suma y el producto. Además, estas operaciones están relacionadas entre si por medio de la propiedad distributiva: el producto distribuye con respecto a la suma. Otro conjunto que tiene asociado naturalmente dos leyes de composición interna es el conjunto $K[X]$ (con K siendo $\mathbb{Z}$, $\mathbb{R}$ o $\mathbb{C}$) de polinomios con coeficientes en K; las leyes son la suma y el producto de polinomios. Y sabemos también que en $K[X]$ el producto distribuye con respecto a la suma. Los ejemplos de conjuntos con dos leyes de composición interna abundan. Enunciamos el concepto abstracto que reúnen todos los ejemplos recién mencionados.

Definición 6.32

Un **anillo** es un conjunto A con dos leyes de composición interna, llamadas **suma (+)** y **producto (.)**, lo denotamos por $\langle A, +, . \rangle$, que satisface las siguientes condiciones:

1. $\langle A, + \rangle$ es un grupo abeliano.
2. El producto . es asociativa y existe un elemento $1 \in A$ que es neutro con respecto al producto ., esto es, $a.1 = a$ y $1.a = a$ para todo $a \in A$.
3. Para todos $a, b, c \in A$, se cumplen

$$a.(b + c) = a.b + a.c \quad \text{y} \quad (b + c).a = b.a + c.a$$

llamada la propiedad distributiva.

Para trabajar de forma adecuada con anillos, necesitamos hacer algunas convenciones. Para un anillo $\langle A, +, . \rangle$, tenemos que $\langle A, + \rangle$ es un grupo abeliano, así que tiene un elemento neutro. Lo denotaremos por 0. Es decir, 0 es elemento neutro de A con respecto a la suma: $a + 0 = a$ para todo $a \in A$. Y al elemento neutro de A con respecto al producto lo denotaremos por 1: $a.1 = a = 1.a$ para todo $a \in A$. Como $\langle A, + \rangle$ es grupo abeliano, cada elemento a tiene un inverso a^{-1}. LLamaremos **opuesto** a los inversos con respecto a la suma y lo de notaremos por $-a$ en lugar de a^{-1}. Notemos que $\langle A, . \rangle$ no es necesariamente un grupo, así que no todos los elementos tienen inverso. Diremos que un elemento b es inverso de a si $a.b = b.a = 1$ y como es usual lo denotaremos por a^{-1}. Resumimos todo esto en el cuadro 6.2.

	Neutro	Inverso	Notación
La suma	0	opuesto	$-a$
El producto	1	inverso (si existe)	a^{-1} (si existe)

Cuadro 6.2: Convenciones en anillos

Definición 6.33

Diremos que un anillo $\langle A, +, . \rangle$ es **conmutativo** si el producto es conmutativo. Esto es, $a.b = b.a$, para todo $a, b \in A$.

Definición 6.34

Diremos que un anillo $\langle A, +, . \rangle$ es un **dominio de integridad** si es conmutativo y cumple la siguiente condición:

$$a.b = 0 \implies a = 0 \text{ o } b = 0. \tag{6.10}$$

Ejemplo 6.35. Los siguientes son ejemplos de dominios de integridad, donde las operaciones son las usuales estudiadas en los capítulos anteriores: $\langle \mathbb{Z}, +, . \rangle$, $\langle \mathbb{R}, +, . \rangle$, $\langle \mathbb{C}, +, . \rangle$ y $\langle \mathrm{K}[X], +, . \rangle$. Por ejemplo, veamos el caso de $\mathbb{C}$. En la Sección 4.1 probamos que la suma de números complejos es asociativa, conmutativa, existe un elemento neutro que es el 0 (o $(0,0)$) y todo complejo $z = a + bi$ tiene un opuesto $-z = -a - bi$. Entonces, $\langle \mathbb{C}, + \rangle$ es un grupo abeliano. Con respecto al producto en $\mathbb{C}$, vimos que es asociativo, conmutativo, tiene un elemento neutro que es el complejo 1 y probamos que el producto distribuye con respecto a la suma (véase Proposición 4.6). Entonces $\langle \mathbb{C}, +, . \rangle$ es un anillo conmutativo. Para ver que $\mathbb{C}$ es un dominio de integridad, sean $z, w \in \mathbb{C}$ y supongamos que $z.w = 0$. Si $z = 0$, entonces se cumple la condición (6.10). Si $z \neq 0$, entonces existe su inverso z^{-1}. Ahora

$$z.w = 0 \implies z^{-1}.z.w = z^{-1}.0 \implies w = 0.$$

Entonces se cumple la condición (6.10). Por lo tanto, $\langle \mathbb{C}, +, . \rangle$ es un dominio de integridad.

Ejemplo 6.36. Sea $n \in \mathbb{Z}$. Por el Ejemplo 6.25 sabemos que $\langle \mathbb{Z}_n, + \rangle$ es un grupo abeliano donde $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ y $[a]_n + [b]_n = [a+b]_n$. Podemos ahora considerar naturalmente sobre $\mathbb{Z}_n$ otra operación que la llamaremos producto. Definimos el producto

$$. : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

de la siguiente forma: para $[a]_n, [b]_n \in \mathbb{Z}_n$,

$$[a]_n.[b]_n = [ab]_n. \tag{6.11}$$

Entonces, $\langle \mathbb{Z}_n, +, . \rangle$ es un anillo conmutativo. Veamos que se cumplen las condiciones de la Definición 6.32.

- $\langle \mathbb{Z}_n, + \rangle$ es un grupo abeliano. Fue probado en el Ejemplo 6.25.
- El producto . es asociativo: En efecto, sean $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$, entonces

  $$[a]_n.([b]_n.[c]_n) = [a]_n.[bc]_n = [a(bc)]_n = [(ab)c]_n = [ab]_n.[c]_n = ([a]_n.[b]_n).[c]_n.$$

  El elemento $[1]_n \in \mathbb{Z}_n$ es neutro con respecto al producto. En efecto, sea $[a]_n \in \mathbb{Z}_n$, entonces

  $$[a]_n.[1]_n = [a.1]_n = [a]_n \quad \text{y} \quad [1]_n.[a]_n = [1.a]_n = [a]_n.$$

- Veamos que se cumple la propiedad distributiva. Sean $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$. Entonces

  $$\begin{aligned}
  [a]_n.([b]_n + [c]_n) &= [a]_n.[b+c]_n && \text{por (6.9)} \\
  &= [a(b+c)]_n && \text{por (6.11)} \\
  &= [ab+ac]_n && \text{propiedad distributiva en } \mathbb{Z} \\
  &= [ab]_b + [ac]_n && \text{por (6.9)} \\
  &= [a]_n.[b]_n + [a]_n.[c]_n && \text{por (6.11)}
  \end{aligned}$$

  De igual forma podemos probar que $([b]_n + [c]_n).[a]_n = [b]_n.[a]_n + [c]_n.[a]_n$.

Entonces, $\langle \mathbb{Z}_n, +, . \rangle$ es un anillo. Veamos que es conmutativo. Debemos probar que el producto es conmutativo. Sean $[a]_n, [b]_n \in \mathbb{Z}$. Entonces

$$[a]_n.[b]_n = [ab]_n = [ba]_n = [b]_n.[a]_n.$$

Por lo tanto, $\langle \mathbb{Z}_n, +, . \rangle$ es un anillo conmutativo. ■

Al anillo conmutativo $\langle \mathbb{Z}_n, +, . \rangle$ se lo denomina el **anillo de enteros módulo** n.

Problema 6.37

Sea $M(\mathbb{R}, 2)$ el conjunto de todas las matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cuadradas de 2×2 con entradas reales $(a, b, c, d \in \mathbb{R})$. Probar que $M(\mathbb{R}, 2)$ con la suma usual de matrices (véase el Problema 6.20) y con el producto usual de matrices es un anillo. Mostrar que este anillo no es conmutativo. Recuerde que el producto de matrices se define como sigue:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

Sea $\langle A, +, . \rangle$ un anillo. Sean $a, b \in A$. Sabemos que $-b$ es el opuesto de b, esto es, $b + (-b) = 0$. En lugar de escribir $a + (-b)$, escribiremos $a - b$. Veamos ahora las siguientes propiedades.

Proposición 6.38

Sea $\langle A, +, . \rangle$ un anillo y sean $a, b, c \in A$. Entonces

1. $a.0 = 0.a = 0$.
2. $a.(-b) = (-a).b = -(a.b)$.
3. $(-a).(-b) = a.b$.
4. $a.(b - c) = ab - ac$.
5. $(-1).a = -a$[1]
6. $(-1)(-1) = 1$.

[1]Observe que en la ecuación $(-1).a = -a$, el -1 no es un entero, sino que -1 es el opuesto del elemento neutro 1 en el anillo A.

Demostración. Sean $a, b, c \in A$.

1.

$$\begin{aligned} a.0 &= a.(0+0) && \text{sabemos que 0+0=0} \\ a.0 &= a.0 + a.0 && \text{propiedad distributiva} \\ -a.0 + a.0 &= -a.0 + (a.0 + a.0) && \text{sumamos a ambos miembros el opuesto de a.0} \\ 0 &= (-a.0 + a.0) + a.0 && \text{un elemento más su opuesto da 0, y por asociatividad} \\ 0 &= 0 + a.0 \\ 0 &= a.0 \end{aligned}$$

2.

$$\begin{aligned} a(-b) + a.b &= a(-b+b) && \text{distributiva} \\ &= a.0 \\ a(-b) + a.b &= 0 \\ (a.(-b) + a.b) - (a.b) &= 0 - (a.b) && \text{sumamos a ambos miembro } -(a.b) \\ a.(-b) + (a.b - a.b) &= -(a.b) \\ a.(-b) + 0 &= -(a.b) \\ a.(-b) &= -(a.b). \end{aligned}$$

De forma similar se prueba que $(-a).b = -(a.b)$.

3.

$$\begin{aligned} (-a).(-b) &= -(a.(-b)) && \text{por la propieadad 2.} \\ &= --(a.b) && \text{por la propieadad 2.} \\ &= a.b && \text{por la propiedad 3. de la Proposición 6.21.} \end{aligned}$$

Las pruebas de las propiedades 4., 5. y 6. se dejan como ejercicio al lector. ■

A menudo se comete la equivocación de tratar a un anillo como si fuera un grupo con respecto al producto. No lo es. Es decir, es importante notar que si $\langle A, +, . \rangle$ es un anillo, entonces $\langle A, . \rangle$ no es necesariamente un grupo. Un error muy común es asumir que todos los elementos de un anillo tienen un inverso, lo cual no es cierto. Por ejemplo, si $a.b = a.c$ y $a \neq 0$, no podemos concluir que $b = c$. Esta ley de cancelación no vale en todos los anillos, sólo vale en ciertos anillos especiales, a los que llamamos dominios de integridad. Veamos estas observaciones con un ejemplo y una proposición.

Ejemplo 6.39. Consideremos el anillo de enteros módulo 6 $\langle \mathbb{Z}_6, +, . \rangle$. A continuación presentamos las tablas de las operaciones suma y producto.

+	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

.	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

De la tabla del producto, podemos observar que no existe ningún elemento $[x]_6$ de $\mathbb{Z}_6$ que sea inverso de $[2]_6$. Es decir, no existe ningún $[x]_6 \in \mathbb{Z}_6$ tal que $[2]_6.[x]_6 = [1]_6$. De igual forma, podemos observar que $[3]_6$ y $[4]_6$ tampoco son invertibles en $\mathbb{Z}_6$. En cambio, $[5]_6$ si es invertible, y su inverso es el mismo $[5]_6$, pues $[5]_6.[5]_6 = [1]_6$. También podemos mostrar, mirando la tabla del producto, que no se cumple la ley de cancelación: tenemos que $[3]_6.[2]_6 = [3]_6.[4]_6$, pero $[2]_6 \neq [4]_6$. ■

Proposición 6.40

Sea $\langle A, +, . \rangle$ un dominio de integridad. Entonces se cumple la ley de cancelación, esto es, para todos $a, b, c \in A$,

$$a.b = a.c \text{ y } a \neq 0 \implies b = c.$$

Demostración. Sean $a, b, c \in A$ y supongamos que $a.b = a.c$ y $a \neq 0$. Entonces,

$$\begin{aligned} a.b &= a.c \\ a.b - a.c &= a.c - a.c && \text{sumamos a ambos miembros el opuesto de } a.c \\ a.(b-c) &= 0 && \text{por propiedad distributiva.} \end{aligned}$$

Ahora, como A es un dominio de integridad y $a.(b-c) = 0$, tenemos que $a = 0$ o $b - c = 0$. Pero por hipótesis $a \neq 0$, entonces $b - c = 0$. Por lo tanto, $b = c$. ■

Definición 6.41

Una **cuerpo** es un anillo conmutativo $\langle K, +, . \rangle$ en el cual, todo elemento no nulo de K es invertible.

En otras palabras,

Diremos que un anillo conmutativo $\langle K, +, . \rangle$ es un **cuerpo** si para todo $a \in K$ tal que $a \neq 0$, existe un elemento $b \in K$ tal que $a.b = 1$.

Ejemplo 6.42. En el Ejemplo 6.35 vimos que $\langle \mathbb{R}, +, \cdot \rangle$ es un anillo conmutativo, y sabemos que para todo número real no nulo a, existe su inverso $a^{-1} = \frac{1}{a}$ tal que $a.a^{-1} = 1$. Por lo tanto, $\langle \mathbb{R}, +, . \rangle$ es un cuerpo.

Ejemplo 6.43. En el Ejemplo 6.35 probamos que $\langle \mathbb{C}, +, \cdot \rangle$ es un anillo conmutativo. Sabemos que para cada complejo no nulo z, existe su inverso z^{-1} tal que $z.z^{-1} = 1$ (véase 4.4). Entonces, $\langle \mathbb{C}, +, \cdot \rangle$ es un cuerpo.

Proposición 6.44

Si $\langle K, +, \cdot \rangle$ es un cuerpo, entonces $\langle K, +, \cdot \rangle$ es un dominio de integridad.

Demostración. A cargo del lector. Véase el Ejemplo 6.35. ■

Proposición 6.45

Sea $\langle K, +, \cdot \rangle$ un cuerpo. Entonces, $\langle K - \{0\}, \cdot \rangle$ es un grupo abeliano.

Demostración. Sea $\langle K, +, \cdot \rangle$ un cuerpo. Primero veamos que el producto $\cdot$ es una ley de composición interna en $K - \{0\}$. Sean $a, b \in K - \{0\}$. Como $a \neq 0$ y $b \neq 0$, entonces dado que $\langle K, +, \cdot \rangle$ es un dominio de integridad, tenemos que $a.b \neq 0$. Esto es, $a.b \in K - \{0\}$. Por definición de cuerpo sabemos que $\langle K, +, \cdot \rangle$ es un anillo conmutativo, con lo cual la operación producto $\cdot$ es asociativa, conmutativa y tiene un elemento neutro $1 \in K - \{0\}$. Además, por definición de cuerpo, para cada $a \in K$ no nulo ($a \neq 0$) es invertible. Esto es, para cada $a \neq 0$, existe $b \neq 0$ tal que $a.b = 1$. Por lo tanto, $\langle K - \{0\}, + \rangle$ es un grupo abeliano. ■

Problema 6.46

Sea $\langle K, +, \cdot \rangle$ un cuerpo. Sean $a, b \in K$ con $a \neq 0$. Probar que la ecuación $ax + b = 0$ tiene una única solución.

6.4. Homomorfismos

6.4.1. Homomorfismos de grupos

Definición 6.47

Sean $\langle G_1, *_1 \rangle$ y $\langle G_2, *_2 \rangle$ dos grupos. Diremos que una función $f \colon G_1 \to G_2$ es un **homomorfismo de grupo** si se cumple que para todos $a, b \in G_1$,

$$f(a *_1 b) = f(a) *_2 f(b).$$

Proposición 6.48

Sean $\langle G_1, *_1 \rangle$ y $\langle G_2, *_2 \rangle$ dos grupos. Sea $f \colon G_1 \to G_2$ un homomorfismo de grupo. Entonces,

1. $f(e_1) = e_2$.
2. $f(a^{-1}) = f(a)^{-1}$.

Demostración. 1. Dado que f es un homomorfismo tenemos que

$$\begin{aligned} f(e_1) &= f(e_1 *_1 e_1) \\ f(e_1) &= f(e_1) *_2 f(e_1) \\ f(e_1)^{-1} *_2 f(e_1) &= f(e_1)^{-1} *_2 (f(e_1) *_2 f(e_1)) \\ e_2 &= f(e_1). \end{aligned}$$

2. Sea $a \in G_1$. Entonces,

$$\begin{aligned} a *_1 a^{-1} &= e_1 \\ f(a *_1 a^{-1}) &= f(e_1) \\ f(a) *_2 f(a^{-1}) &= e_2 \\ f(a^{-1}) &= f(a)^{-1}. \end{aligned}$$

■

Ejemplo 6.49. Sea $\langle \mathbb{R}^*, . \rangle$ el grupo multiplicativo de los reales no nulos y sea $\langle \mathbb{R}, + \rangle$ el grupo de los reales con la suma. Definimos la función $f\colon \mathbb{R} \to \mathbb{R}^*$ definida por: para cada $x \in \mathbb{R}$,

$$f(x) = e^x$$

Probemos que f es un homomorfismo de grupo. Sean $x, y \in \mathbb{R}$. Utilizando las propiedades de las potencias reales tenemos que

$$f(x+y) = e^{x+y} = e^x . e^y = f(x).f(y).$$

Entonces, f es un homomorfismo de grupo. El elemento neutro del grupo $\langle \mathbb{R}, + \rangle$ es el 0 y el neutro del grupo $\langle \mathbb{R}^*, . \rangle$ es el 1. Comprobamos que se cumple la propiedad 1. de la Proposición 6.48: $f(0) = e^0 = 1$. También vemos que se comprueba la la propiedad 2. de la Proposición 6.48: sea $x \in \mathbb{R}$, $f(-x) = e^{-x} = (e^x)^{-1} = f(x)^{-1}$. ■

Ejemplo 6.50. Sea $\langle \mathbb{R}, + \rangle$ el grupo de los reales con la suma. Consideremos el grupo $M(\mathbb{R}, 2)$ de las matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cuadradas de 2×2 con entradas reales ($a, b, c, d \in \mathbb{R}$) con la suma usual de matrices (véase 6.20). Se define la función $h\colon \mathbb{R} \to M(\mathbb{R}, 2)$ como sigue:

$$f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Entonces, h es un homomorfismo de grupo. En efecto, sean $a, b \in \mathbb{R}$,

$$f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = f(a) + f(b). \quad ■$$

Problema 6.51

Sea $\langle G, . \rangle$ un grupo. Se define la función $f\colon G \to G$ por: para todo $a \in G$, $f(a) = e$. Probar que f es un homomorfismo.

Problema 6.52

Considere el grupo $\langle \mathbb{Z}, + \rangle$ y el grupo $\langle \mathbb{Z}_5, + \rangle$ (véase el Ejemplo 6.26). Sea $\pi \colon \mathbb{Z} \to \mathbb{Z}_5$ la función definida por: $\pi(a) = [a]_5$, para todo $a \in \mathbb{Z}$. Probar que π es un homomorfismo de grupo.

Proposición 6.53

Sean $f \colon \langle G_1, *_1 \rangle \to \langle G_2, *_2 \rangle$ y $g \colon \langle G_2, *_2 \rangle \to \langle G_3, *_3 \rangle$ dos homomorfismos de grupos. Entonces la función composición $g \circ f \colon G_1 \to G_3$ es un homomorfismo de grupo.

Demostración. Debemos probar que para todos $a, b \in G_1$, se cumple que

$$(g \circ f)(a *_1 b) = (g \circ f)(a) *_3 (g \circ f)(b).$$

Sean $a, b \in G_1$. Entonces,

$$\begin{aligned}
(g \circ f)(a *_1 b) &= g(f(a *_1 b)) && \text{por composición de funciones} \\
&= g(f(a) *_2 f(b)) && \text{por ser } f \text{ un homomorfismo} \\
&= g(f(a)) *_3 g(f(b)) && \text{por ser } g \text{ un homomorfismo} \\
&= (g \circ f)(a) *_3 (g \circ f)(b) && \text{por composición de funciones}
\end{aligned}$$

Por lo tanto, $g \circ f$ es un homomorfismo de grupo. ■

Problema 6.54

Sea $\langle G, . \rangle$ un grupo y sea $f \colon G \to G$ la función definida por: para cada $x \in G$, $f(x) = x^{-1}$. ¿Es f un homomorfismo? Si no lo es, ¿qué condición debe cumplir el grupo G para que f sea un homomorfismo?

Definición 6.55

Sea $f \colon \langle G_1, *_1 \rangle \to \langle G_2, *_2 \rangle$ un homomorfismo de grupos. Llamaremos al conjunto

$$\mathrm{Nu}(f) = \{x \in G_1 : f(x) = e_2\}$$

el **núcleo** de f, y al conjunto

$$\mathrm{Img}(f) = \{f(x) : x \in G_1\}$$

lo llamaremos la **imagen** de f.

Proposición 6.56

Sea $f \colon \langle G_1, *_1 \rangle \to \langle G_2, *_2 \rangle$ un homomorfismo de grupos. Entonces, f es inyectiva si y sólo si $\mathrm{Nu}(f) = \{e_1\}$.

Demostración. $\Rightarrow$) Supongamos que f es inyectiva. Notemos que siempre $e_1 \in \mathrm{Nu}(f)$, pues $f(e_1) = e_2$ (ver Proposición 6.48). Sea $x \in \mathrm{Nu}(f)$. Entonces, por definición del núcleo tenemos que $f(x) = e_2$. Como $f(x) = e_2 = f(e_1)$, entonces por ser f inyectiva obtenemos que $x = e_1$. Por lo tanto, el único elemento en $\mathrm{Nu}(f)$ es el e_1. Esto es, $\mathrm{Nu}(f) = \{e_1\}$.

$\Leftarrow$) Supongamos que $\mathrm{Nu}(f) = \{e_1\}$. Probemos que f es inyectiva. Sean $a, b \in G_1$ y supongamos que $f(a) = f(b)$. Entonces,

$$\begin{aligned}
f(a) &= f(b) && \\
f(a)^{-1} *_2 f(a) &= f(a)^{-1} *_2 f(b) && \\
f(a^{-1}) *_2 f(a) &= f(a^{-1}) *_2 f(b) && \text{Proposición 6.48} \\
f(a^{-1} *_1 a) &= f(a^{-1} *_1 b) && \text{por ser } f \text{ homomorfismo} \\
f(e_1) &= f(a^{-1} *_1 b) && \\
e_2 &= f(a^{-1} *_1 b). &&
\end{aligned}$$

Entonces, $a^{-1} *_1 b \in \mathrm{Nu}(f) = \{e_1\}$. Así $a^{-1} *_1 b = e_1$. Entonces $b = a$. Por lo tanto, f es inyectiva. ■

Proposición 6.57

Sea $f\colon \langle G_1, *_1\rangle \to \langle G_2, *_2\rangle$ un homomorfismo de grupos. Entonces,

1. $\mathrm{Nu}(f)$ es un subgrupo de G_1.
2. $\mathrm{Img}(f)$ es un subgrupo de G_2.

Demostración. 1. Debemos probar que las tres condiciones de la Definición 6.27 se cumplen para $\mathrm{Nu}(f)$.

1. Como $f(e_1) = e_2$, entonces $e_1 \in \mathrm{Nu}(f)$.
2. Sean $a, b \in \mathrm{Nu}(f)$. Entonces, $f(a) = e_2$ y $f(b) = e_2$. Luego, $f(a *_1 b) = f(a) *_2 f(b) = e_2 *_2 e_2 = e_2$. Entonces, $a *_1 b \in \mathrm{Nu}(f)$.
3. Sea $a \in \mathrm{Nu}(f)$. Así $f(a) = e_2$. Entonces, $f(a^{-1}) = f(a)^{-1} = e_2^{-1} = e_2$. Por lo tanto, $a^{-1} \in \mathrm{Nu}(f)$.

Entonces, $\mathrm{Nu}(f)$ es un subgrupo de G_1.

2. Debemos probar que las tres condiciones de la Definición 6.27 se cumplen para $\mathrm{Img}(f)$.

1. Como $e_2 = f(e_1)$, entonces $e_2 \in \mathrm{Img}(f)$.
2. Sean $f(x), f(y) \in \mathrm{Img}(f)$. Entonces, como $f(x) *_2 f(y) = f(x *_1 y) \in \mathrm{Img}(f)$, tenemos que $f(x) *_2 f(y) \in \mathrm{Img}(f)$.
3. Sea $f(x) \in \mathrm{Img}(f)$. Luego, $f(x)^{-1} = f(x^{-1}) \in \mathrm{Img}(f)$.

Por lo tanto, $\mathrm{Img}(f)$ es un subgrupo de G_2. ■

Ejemplo 6.58. Considere el homomorfismo $\pi\colon \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}_5, + \rangle$ (véase el Problema 6.52). Vamos a determinar el núcleo de π. Usando la definición de núcleo, la definición de π y lo que sabemos de congruencias, tenemos que

$$a \in \mathrm{Nu}(\pi) \iff \pi(a) = [0]_5 \iff [a]_5 = [0]_5 \iff a \in [0]_5.$$

Entonces, $\mathrm{Nu}(\pi) = [0]_5$. Recordando que $[0]_5 = \{5k : k \in \mathbb{Z}\}$, entonces

$$\mathrm{Nu}(\pi) = \{5k : k \in \mathbb{Z}\}. \quad \blacksquare$$

6.4.2. Homomorfismos de anillos

Definición 6.59

Sean $\langle A, +_A, .{}_A \rangle$ y $\langle B, +_B, .{}_B \rangle$ anillos. Diremos que una función $f\colon A \to B$ es un **homomorfismo de anillos** si:

(H1) $f(a +_A a') = f(a) +_B f(a')$;

(H2) $f(a._A a') = f(a)._B f(a')$;

(H3) $f(1_A) = 1_B$.

Ejemplo 6.60. Consideremos el anillo de enteros $\langle \mathbb{Z}, +, . \rangle$ y el anillo de enteros módulo n $\langle \mathbb{Z}_n, +, . \rangle$. Se define la función $f\colon \mathbb{Z} \to \mathbb{Z}_n$ por $f(a) = [a]_n$. Probemos que f es un homomorfismo de anillos. Sean $a, b \in \mathbb{Z}$.

(H1)

$$\begin{aligned} f(a+b) &= [a+b]_n && \text{por definición de la función } f \\ &= [a]_n + [b]_n && \text{por definición de la operación +, ver (6.9)} \\ &= f(a) + f(b) && \text{definición de la función } f \end{aligned}$$

(H2)

$$\begin{aligned} f(a.b) &= [a.b]_n && \text{por definición de la función } f \\ &= [a]_n.[b]_n && \text{por definición de la operación } \cdot\text{, ver (6.11)} \\ &= f(a).f(b) && \text{por definición de la función } f \end{aligned}$$

(H3) $f(1) = [1]_n$, por definición de f.

Entonces se cumplen las tres condiciones de la definición de homomorfismo de anillos. Por lo tanto, f es un homomorfismo de anillos. $\blacksquare$

Ejemplo 6.61. Consideremos el cuerpo $\mathbb{C}$ de los números complejos y el anillo $M(\mathbb{R},2)$ de matrices cuadradas de 2×2 con las operaciones de suma y producto usuales de matrices (véase 6.20 y 6.37, respectivamente). Se define la función $f:\mathbb{C}\to M(\mathbb{R},2)$ por

$$f(a+bi)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}.$$

Probemos que f es un homomorfismo de anillos. Sean $z=a+bi$ y $w=c+di$ complejos.

(H1)

$$\begin{aligned} f(z+w) &= f((a+b)+(c+d)i) && \text{por definición de la suma en } \mathbb{C}\\ &= \begin{pmatrix} a+b & c+d\\ -(c+d) & a+b\end{pmatrix} && \text{por definición de } f\\ &= \begin{pmatrix} a & b\\ -b & a\end{pmatrix}+\begin{pmatrix} c & d\\ -d & c\end{pmatrix} && \text{por definición de la suma en } M(\mathbb{R},2)\\ &= f(a+bi)+f(c+di) && \text{por definición de } f\\ &= f(z)+f(w). \end{aligned}$$

(H2) Calculamos primero $f(z.w)$:

$$\begin{aligned} f(z.w) &= f((ac-bd)+(ad+bc)i) && \text{por definición del producto en } \mathbb{C}\\ &= \begin{pmatrix} ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{pmatrix} && \text{por definición de } f \end{aligned} \tag{6.12}$$

Por otro lado calculamos $f(z).f(w)$:

$$\begin{aligned} f(z).f(w) &= \begin{pmatrix} a & b\\ -b & a\end{pmatrix}.\begin{pmatrix} c & d\\ -d & c\end{pmatrix} && \text{por definición de } f\\ &= \begin{pmatrix} ac-bd & ad+bc\\ -bc-ad & -bd+ac\end{pmatrix} && \text{por definición del producto de matrices}\\ &= \begin{pmatrix} ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{pmatrix}. \end{aligned} \tag{6.13}$$

Entonces, de (6.12) y (6.13) obtenemos que $f(z.w)=f(z).f(w)$.

(H3) $f(1)=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, que es el neutro con respecto al producto en $M(\mathbb{R},2)$. ■

Problema 6.62

Considere el anillo conmutativo $\langle\mathbb{C},+,\cdot\rangle$ y la función $f:\mathbb{C}\to\mathbb{C}$ definida por $f(z)=\overline{z}$. Probar que f es un homomorfismo de anillos.

Veamos algunas propiedades básicas que cumplen los homomorfismos de anillo.

Proposición 6.63

Sean A y B anillos y sea $f\colon A \to B$ un homomorfismo de anillo. Entonces, para todos $a, b \in A$ se cumplen las siguientes propiedades.

1. $f(-a) = -f(a)$.
2. $f(0) = 0$.
3. $f(a-b) = f(a) - f(b)$.
4. Si a es invertible, entonces $f(a)$ es invertible. Además, $f(a^{-1}) = (f(a))^{-1}$.

Demostración. Las pruebas de las propiedades 1. y 2. son análogas a las dadas en la Proposición 6.48. La propiedad 3. es consecuencia de las propiedades 1. y 2. Probemos 4. Sea $a \in A$ y supongamos que es invertible. Entonces, existe $a^{-1} \in A$ tal que $a.a^{-1} = 1_A$. Luego,

$$\begin{aligned} a.a^{-1} &= 1_A \\ f(a.a^{-1}) &= f(1_A) \\ f(a).f(a^{-1}) &= 1_B. \end{aligned}$$

Entonces obtenemos que $f(a^{-1})$ es el inverso de $f(a)$. Por lo tanto, $f(a)$ es invertible y su inverso es $f(a^{-1})$, así $f(a)^{-1} = f(a^{-1})$. ■

Problema 6.64

Sea $f\colon A \to B$ un homomorfismo de anillos. Probar por inducción que para todo $n \in \mathbb{N}$, $f(a^n) = f(a)^n$ para todo $a \in A$.

Ejercicios propuestos

Leyes de composición interna

Ejercicio 6.1. Para las siguientes dos operaciones, determinar si son leyes de composición interna y qué propiedades satisfacen.

(a) Sea $\bullet\colon (\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z}) \to (\mathbb{Z}\times\mathbb{Z})$ definida por

$$(a,b)\bullet(c,d) = (ad+bc, bd).$$

(b) Sea $\star\colon (\mathbb{Q}\times\mathbb{Q})\times(\mathbb{Q}\times\mathbb{Q}) \to (\mathbb{Q}\times\mathbb{Q})$ definida por

$$(a,b)\star(c,d) = (ad+bc, bd).$$

Ejercicio 6.2. Sea $\odot\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ la ley de composición definida por: para $a, b \in \mathbb{N}$, $a \odot b = a.b + 1$. Determinar qué propiedades satisface.

Grupos

Ejercicio 6.3. Probar que en todo grupo abeliano $\langle G, . \rangle$ se cumplen las siguientes propiedades. Para todos $a, b \in G$,

(a) $(a.b)^{-1}) = a^{-1}.b^{-1}$.

(b) Para todo $k \in \mathbb{Z}$, $(a.b)^k = a^k.b^k$.

Ejercicio 6.4. Probar las propiedades de la potencia 3. y 4. de la Proposición 6.24.

Ejercicio 6.5. Sea $\langle G, . \rangle$ un grupo y sean $a, b, c \in G$. Probar que:

(a) $a.b = c$ si y sólo si $b = a^{-1}.c$.

(b) $a.b = c.a$ si y sólo si $a.b.a^{-1} = c$.

(c) $a.b = b.a$ si y sólo si $a^{-1}.b^{-1} = b^{-1}.a^{-1}$.

(d) $a.b = b.a$ si y sólo si $a.b.a^{-1}.b^{-1} = e$.

Ejercicio 6.6. Sea $\langle G, . \rangle$ un grupo. Sean $a, b \in G$. Probar que la ecuación $a.x = b$ tiene una única solución.

Anillos

Ejercicio 6.7. Construir las tablas de las operaciones suma y producto del anillo conmutativo $\langle \mathbb{Z}_8, +, . \rangle$. Mostrar que este anillo no es un dominio de integridad. Hallar en $\mathbb{Z}_8$ los elementos que son invertibles y sus inversos.

Ejercicio 6.8. Probar que el siguiente conjunto

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

con las operaciones usuales de suma + y producto · de matrices (véase y 6.20 y 6.37, respectivamente) es un anillo. ¿Es conmutativo?

Ejercicio 6.9. Consideremos el conjunto

$$M_{\mathbb{C}} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

Probar que $\langle M_{\mathbb{C}}, +, . \rangle$ con las operaciones de suma + y producto · usuales de matrices (véase y 6.20 y 6.37, respectivamente) es un anillo conmutativo. ¿Es $\langle M_{\mathbb{C}}, +, . \rangle$ un dominio de integridad?

Ejercicio 6.10. Probar que las siguientes identidades se cumplen en todo anillo conmutativo $\langle A, +, . \rangle$. Sean $a, b \in A$.

$$(a+b)^2 = a^2 + 2.a.b + b^2 \qquad \text{y} \qquad (a+b)(a-b) = a^2 - b^2.$$

Ejercicio 6.11. Probar las propiedades 4., 5. y 6. de la Proposición 6.38.

Ejercicio 6.12. Sea $\langle M_{\mathbb{C}}, +, . \rangle$ el anillo conmutativo del Ejercicio 6.9. Probar que para cada $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ no nulo de $M_{\mathbb{C}}$, se tiene que $A^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$ es el inverso de A. ¿Es $\langle M_{\mathbb{C}}, +, . \rangle$ un cuerpo?

Ejercicio 6.13. Probar que el anillo $\langle \mathbb{Z}_5, +, . \rangle$ es un cuerpo.

Ejercicio 6.14. Consideremos el conjunto de los números racionales

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

con las operaciones de suma y producto usuales:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{y} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Probar que $\langle \mathbb{Q}, +, \cdot \rangle$ es un cuerpo.

Ejercicio 6.15. Probar la Proposición 6.44.

Ejercicio 6.16. Sean A y B dos anillos. Probar que el conjunto $A \times B$ con las operaciones suma y producto definidas como: para todos $(a_1, b_1), (a_2, b_2) \in A \times B$,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{y} \quad (a_1, b_1).(a_2, b_2) = (a_1.a_2, b_1.b_2)$$

es un anillo. Si A y B son conmutativos, ¿también lo es el anillo $A \times B$?

Ejercicio 6.17. Considerar los anillos $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Considerar el anillo $\mathbb{Z}_2 \times \mathbb{Z}_3$ definido como en el Ejercicio anterior. Construir las tablas de las operaciones suma y producto del anillo $\mathbb{Z}_2 \times \mathbb{Z}_3$. Determinar los elementos invertibles en $\mathbb{Z}_2 \times \mathbb{Z}_3$. ¿Es el anillo $\mathbb{Z}_2 \times \mathbb{Z}_3$ un cuerpo?

Homomorfismos

Ejercicio 6.18. Para cada una de las siguientes funciones, determinar si es o no un homomorfismo de grupo.

(a) $m\colon \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ dada por $m(x) = 2x$.

(b) $f\colon \langle \mathbb{R}^*, \cdot \rangle \to \langle \mathbb{R}, + \rangle$ dada por $f(x) = \ln(x)$.

(c) $g\colon \langle \mathbb{C}, + \rangle \to \langle \mathbb{R}, + \rangle$ dada por $g(z) = |z|$.

(d) $h\colon \langle \mathbb{C}^*, \cdot \rangle \to \langle \mathbb{R}^*, \cdot \rangle$ dada por $h(z) = |z|$.

(e) $tr\colon \langle M(\mathbb{R}, 2), + \rangle \to \langle \mathbb{R}, + \rangle$ dada por $tr \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d$.

Ejercicio 6.19. Sea $f\colon \langle G_1, *_1 \rangle \to \langle G_2, *_2 \rangle$ un homomorfismo de grupos. Probar que para todo $n \in \mathbb{N}$ se tiene que $f(x^n) = f(x)^n$, para todo $x \in G$.

Ejercicio 6.20. Sea $f\colon \langle G_1, *_1\rangle \to \langle G_2, *_2\rangle$ un homomorfismo de grupos. Sea H un subgrupo de G_1. Probar que $f(H) = \{f(x) : x \in G_1\}$ es un subgrupo de G_2.

Ejercicio 6.21. Para las funciones del Ejercicio 6.18 que sean homomorfismos, hallar su núcleo y su imagen.

Ejercicio 6.22. Determinar si las siguientes funciones son o no homomorfismos de anillos. Los anillos son considerados con las operaciones usuales.

(a) Sea $f\colon \mathbb{R} \to M(\mathbb{R}, 2)$ definida por $f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

(b) Sea $g\colon \mathbb{C} \to \mathbb{C}$ definida por $g(z) = |z|$.

(c) Sea $h\colon M(\mathbb{R}, 2) \to M(\mathbb{R}, 2)$ definida por $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

(d) Sea $\varphi\colon M(\mathbb{R}, 2) \to \mathbb{R}$ definida por $\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a$.

(e) Sea R el anillo definido en el Ejercicio 6.8. Sea $\psi\colon R \to \mathbb{R}$ definida por $\psi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$.

Ejercicio 6.23. Probar las propiedades 1., 2. y 3. de la Proposición 6.63.

Ejercicio 6.24. Sean $f\colon A \to B$ y $g\colon B \to C$ dos homomorfismos de anillos. Probar que la función composición $g \circ f\colon A \to C$ es un homomorfismo de anillos.

Bibliografía

[1] M. Abad. *Elementos de Álgebra*. EdiUNS, 2003.

[2] N. A. Fava. *El número*. Docencia S.A., Buenos Aires, 1978.

[3] E. R. Gentile. *Notas de Álgebra I*. EUDEBA, Buenos Aires, 1984.

[4] E. R. Gentile. *Notas de Álgebra*. Universidad de Buenos Aires - Facultad de Ciencias Exactas y Naturales - Departamento de Matemática. Fascículo 22 Cursos y Seminarios de Matemática. Buenos Aires, 1965.

[5] T. Krick. *Álgebra I*. Universidad de Buenos Aires, 2017.

[6] W. LeVeque. *Elementary theory of naumbers*. Dover, 1990.

[7] B. E. Meserve. *Fundamental concepts of algebra*. Dover, 1981.

[8] A. Rojo. *Álgebra I*. El Ateneo, 1996.

[9] C. Sanchez. *Lecciones de Álgebra* Universidad de Buenos Aires, 2014.