Temas de matemáticas

Álgebra superior II

Antonio Lascurain Orive

las prensas de ciencias

Antonio Lascurain Orive

Álgebra superior II

Facultad de Ciencias, UNAM
2019

las prensas de ciencias

512.00711

Lascurain Orive, Antonio, autor,
Álgebra superior. II / Antonio Lascurain Orive. -- 1ª edición.
-- Ciudad de México : Universidad Nacional Autónoma de México, Facultad de Ciencias, 2019.
x, 175 páginas : ilustraciones ; 22 cm. -- (Temas de matemáticas)

Incluye índice
ISBN 978-607-30-1423-6

1. Álgebra--Estudio y enseñanza (Superior) I. Universidad Nacional Autónoma de México. Facultad de Ciencias, editor.

Biblioteca Nacional de México No. de sistema[000709370]

Esta obra contó con el apoyo del proyecto PAPIME PE102716

Álgebra superior II
1a edición, 5 de enero de 2019

Facultad de Ciencias
Ciudad Universitaria, Delegación Coyoacán.
C.P. 04510. Ciudad de México

editoriales@ciencias.unam.mx
tienda.fciencias.unam.mx

ISBN: 978-607-30-1423-6

Diseño de portada: Laura Uribe y Eliete Martín del Campo

Impreso y hecho en México.

A Adda Stella

Prólogo

Álgebra superior II presenta temas introductorios de álgebra que se enseñan en el segundo semestre de las carreras de Matemáticas, Actuaría y Ciencias de la Computación de la Facultad de Ciencias de la UNAM. El texto es la continuación de *Álgebra superior I* [9] de mi autoría.

El libro cubre el programa vigente, es decir: la divisibilidad, el álgebra y la geometría básica de números complejos, y el anillo de los polinomios. Los enteros y los anillos Z_m, que también corresponden al temario de álgebra superior II, fueron tratados en [9]. Se discuten también otros temas que no son parte del temario, en particular, se prueba que los reales constituyen un campo y se amplía la discusión sobre los polinomios.

La demanda por parte de muchos estudiantes de mis notas manuscritas del curso Álgebra superior II fue lo que motivó la elaboración de este libro, basado en buena medida en el Cárdenas *et al.* [4]. El objetivo es que los alumnos cuenten con un texto claro, breve y formal del curso Álgebra superior II. Gran parte del texto conecta la discusión con otras áreas como la geometría y el cálculo (incluyendo 46 figuras), con la perspectiva de que las matemáticas no son ramas aisladas, y que los estudiantes podrán entender mejor el álgebra cuando se le relaciona con otras áreas. El libro no sólo cubre el plan vigente (2005), además toma en lo general la estructura del plan de estudios de 1966. También se desarrollan algunos buenos ejemplos que aparecen en [4], presentándolos sin embargo de manera más detallada, algunas veces relacionándolos con el cálculo e incluyendo gráficas.

En el primer capítulo, se describen el máximo común divisor y el mínimo común múltiplo para dos o más números; se resuelven para valores enteros todas las ecuaciones diofantinas lineales; se prueba el teorema fundamental de la aritmética; se exhiben diversos métodos para resolver múltiples sistemas de congruencias; se prueba también que los anillos $\mathbb{Z}_p$, p primo, son campos. Este capítulo podría llamarse introducción a la teoría de números, cabe señalar que esta rama de la matemática es de gran importancia y se relaciona con muchas áreas; en particular con la criptografía, véase por ejemplo [8]. La teoría de números también vincula la variable compleja, la geometría hiperbólica y la topología de las variedades de dimensión tres, como se puede apreciar en el

libro de posgrado [10]. Asimismo, es un hecho notable que la conjetura de Fermat (1637), que establece que la ecuación $a^n + b^n = c^n$, donde a, b, c son enteros positivos distintos a 1, se cumple solamente si $n = 2$, fue probada por el matemático inglés Andrew Wiles en 1996, usando funciones elípticas y formas modulares, temas profundos de la matemática, que relacionan la teoría de números con otras ramas como la geometría algebraica y la variable compleja.

En el segundo capítulo, definiendo los reales como expansiones decimales infinitas sin colas de nueves, se prueba de manera formal y detallada que estos números reales son en efecto un campo. Considero que –aunque el tratamiento de los reales con cortaduras de Dedekind es más elegante ([12])– para un estudiante del primer año de la carrera, éste resulta ser menos natural que el de las expansiones decimales infinitas. Asimismo, el método de clases de equivalencia de sucesiones de Cauchy no es muy apropiado para un estudiante del primer año de la carrera, quien puede identificar claramente los puntos de la recta con las expansiones decimales infinitas, sin embargo no tiene suficiente madurez matemática para pensar puntos como clases de equivalencia. Se prueban también algunos teoremas de densidad de los racionales y que éstos son exactamente los reales periódicos; se incluye también una discusión sobre aproximación y se compara con el método de Newton. La razón principal de incluir este capítulo es probar de manera simple y rápida que los números reales tienen estructura de campo.

En el tercer capítulo se prueban e ilustran resultados básicos de la geometría y el álgebra de los números complejos, poniendo énfasis en la parte geométrica, ya que de esta forma se vuelve transparente la ecuación $i^2 = -1$. Además, se define el argumento de un número complejo de manera multivaluada, lo cual prepara de manera correcta a los estudiantes para el aprendizaje de la variable compleja básica, basta por ejemplo pensar en la función logarítmica compleja. Este enfoque también simplifica sustancialmente diversos cálculos. Aunado a esto se incluyen muchas figuras y se mencionan métodos del cálculo para aproximar funciones trigonométricas y argumentos, como el teorema de Taylor. Los números complejos son esenciales en prácticamente todas las ramas de la matemática y algunas de la física, por ejemplo, permiten simplificar largos cálculos a cuentas más simples, como se puede constatar en las integrales impropias. Más aún, son una poderosa herramienta en la geometría, como se observa con las funciones de Moebius, es decir, las que van del plano en el plano, o más precisamente de la esfera en la esfera, y que son de la forma

$$z \longmapsto \frac{a\,z + b}{c\,z + d}, \quad a\,d - b\,c \neq 0, \quad a, b, c, d \in \mathbb{C}.$$

El último capítulo trata sobre algunos fundamentos del anillo de los polinomios, como son: el algoritmo de la división, los teoremas del factor y del residuo, teoremas básicos sobre polinomios con coeficientes enteros, el método de aproximación de Horner, la factorización de polinomios usando las derivadas y el máximo común divisor. Se prueba también el teorema de Sturm que permite aislar raíces, y se encuentran las soluciones a las ecuaciones de grado 3 y 4, mediante el teorema de Cardano–Ferro–Tartaglia y el método de Ferrari. Además, se prueban resultados sobre fracciones parciales, y se presentan polinomios simétricos en varias variables que describen a los coeficientes de los polinomios en términos de sus raíces. Los polinomios son fundamentales en las matemáticas y sus aplicaciones, en particular los llamados de Taylor han sido históricamente una herramienta básica para conocer el comportamiento de muchas funciones. Su utilidad e importancia aparece en casi todas las áreas, más aún, constituye uno de los objetos de estudio de áreas como la variable compleja, la geometría algebraica, así como varias ramas del álgebra.

El texto contiene diversos ejercicios (algunos avanzados). La razón de no incluir un número excesivo de ellos es proporcionar al estudiante una guía mínima para dominar la materia de manera rápida. Los temas de este libro pueden cubrirse en un semestre. Una posible distribución podría ser la siguiente: cuatro semanas para cubrir el capítulo de divisibilidad, tres semanas para el capítulo de reales, dos semanas y media para los números complejos, y cinco semanas y media para el capítulo de polinomios.

Otros libros de apoyo a los estudiantes de la materia Álgebra superior II son [1], [2] y [6].

Agradezco especialmente a Manuel Flores Galicia por la captura en *Latex* de mis notas para el curso Álgebra superior II, y por la elaboración de las figuras; asimismo mi agradecimiento a uno de los árbitros que leyó de manera cuidadosa el texto y sugirió muchas mejorías a lo largo de todo el libro.

Mi gratitud también a los colegas que me han enriquecido con sus comentarios sobre la enseñanza de esta asignatura, y a varios de mis alumnos por sus pertinentes intervenciones; a las autoridades de la Facultad de Ciencias y a la Dirección General de Asuntos del Personal Académico (DGAPA), que me apoyan en la publicación de este libro, con el proyecto PAPIME PE102716.

Índice general

1. Divisibilidad **1**
- 1.1. Fundamentos . . . 1
- 1.2. El algoritmo de la división . . . 4
- 1.3. El máximo común divisor y el mínimo común múltiplo . . . 7
- 1.4. Algoritmo de Euclides, Ecuaciones diofantinas . . . 13
  - 1.4.1. Algoritmo de Euclides . . . 13
  - 1.4.2. Ecuaciones Diofantinas . . . 15
- 1.5. Teorema fundamental de la aritmética . . . 18
- 1.6. Congruencias . . . 23
- 1.7. Los campos $\mathbb{Z}_p$ . . . 32

2. El campo de los números reales **33**
- 2.1. Los racionales . . . 33
- 2.2. Los números reales . . . 40
- 2.3. El supremo y el ínfimo . . . 44
- 2.4. Los reales son un campo . . . 47
- 2.5. Racionales = reales periódicos . . . 57
- 2.6. Exponentes fraccionarios . . . 62
  - 2.6.1. Raíces n-ésimas . . . 62
  - 2.6.2. Exponentes fraccionarios . . . 63
- 2.7. Aproximación, método de Newton . . . 66

3. Los números complejos **71**
- 3.1. Nociones básicas . . . 71
  - 3.1.1. Módulo . . . 71
  - 3.1.2. Argumento . . . 72
- 3.2. Multiplicación de complejos . . . 83
- 3.3. Los complejos son un campo . . . 88
- 3.4. Raíz cuadrada . . . 93
- 3.5. Raíces n-ésimas . . . 97

4. El anillo de los polinomios **103**
4.1. Definiciones . . . 103
4.2. El dominio entero $A[z]$ . . . 104
4.3. División con residuo . . . 108
4.4. Teoremas del residuo y del factor . . . 112
4.5. Polinomios de grado 2 . . . 117
4.6. División sintética . . . 119
4.7. Aproximaciones a raíces en polinomios reales . . . 122
4.8. Factorización de polinomios . . . 128
4.9. Raíces múltiples, derivadas . . . 131
4.10. Coeficientes, raíces y polinomios simétricos . . . 135
4.11. Factorización en polinomios reales . . . 138
4.12. El máximo común divisor . . . 140
4.13. Método de Sturm . . . 143
4.14. Funciones racionales, fracciones parciales . . . 149
4.15. Teorema de Cardano-Ferro-Tartaglia . . . 155
4.16. Método de Ferrari . . . 164

Glosario de símbolos **169**

Bibliografía **171**

Índice analítico **173**

Capítulo 1

Divisibilidad

1.1. Fundamentos

Dados m y n enteros, $n \neq 0$, su cociente

$$\frac{m}{n}$$

no es necesariamente un entero, por ejemplo 3/8, 4/3. En algunos casos sí: 6/2, 25/5, 169/13.

Definición 1. *Dados $m, n \in \mathbb{Z} \quad n \neq 0$, se dice que, n divide a m, si $m/n \in \mathbb{Z}$, o equivalentemente*

i) n es un divisor de m,

ii) n es un factor de m,

iii) m es un múltiplo de n,

iv) m es divisible entre n.

Se denota esta propiedad por $n \mid m$, por ejemplo $3 \mid 12,\ 7 \mid 49$. En caso contrario se escribe $n \nmid m$. La Definición 1 se puede reformular sin hacer referencia a cocientes.

Definición 2. *Sean $m, n \in \mathbb{Z}$ se dice que n divide a m, si existe $q \in \mathbb{Z}$ tal que $m = nq$.*

Si $n \neq 0$, ambas definiciones son equivalentes, ya que si n es divisor conforme a la primera definición se tiene $m/n = q \in \mathbb{Z}$ y $m = nq$, y viceversa, si n cumple la segunda definición $m = qn$ y como $n \neq 0$ se puede despejar. De cualquier manera, como no se han introducido a la discusión los racionales,

la Definición 2 es la adecuada. Además, incluye el caso $n = 0$. Nótese que el único número que tiene al cero como factor es 0. Además, todo entero es factor del cero.

La propiedad de ser divisor es reflexiva, ya que como $m = m \cdot 1 \ \forall \ m \in \mathbb{Z}$

$$m \mid m.$$

También es transitiva: dados $m, n, p \in \mathbb{Z}$ tales que $n \mid m \quad y \quad m \mid p, \quad$ se tiene

$$n \mid p.$$

Esto se sigue, ya que al existir $q, r \in \mathbb{Z}$ tales que $m = nq$ y $p = mr$, se tiene

$$p = nqr \ \ y \ \ n \mid p.$$

Las unidades de $\mathbb{Z}$: 1 y -1, no alteran la divisibilidad.

Proposición 1.1.1. *Sean $m, n \in \mathbb{Z}$ y $u, \ u'$ unidades (i.e., $u, u' = \pm 1$). Entonces $n \mid m \iff un \mid u'm$.*

DEMOSTRACIÓN. $\Rightarrow$) Si $m = nq, \ q \in \mathbb{Z}$, como existe $u_1 \in \mathbb{Z}$ ($u_1 = \pm 1$) tal que $uu_1 = 1$, se tiene

$$m = unu_1 q,$$

esto es, $un \mid m$ y $un \mid u'm$ (por transitividad).
$\Leftarrow$) Si $u'm = kun, \ k \in \mathbb{Z}$, tomando $u''u' = 1$ se sigue

$$m = u''kun.$$

□

Este resultado nos dice que al considerar la divisibilidad los signos no son relevantes (por lo que para estudiar esta propiedad, basta considerar solamente números naturales y el 0).

Corolario 1.1.2. *Sean $m, n \in \mathbb{Z}$, entonces $n \mid m \iff |n| \mid |m|$.*

Como $|m| = um$ y $|n| = u'n, \ u, u' = \pm 1$, este es simplemente un caso particular de la Proposición 1.1.1.

La divisibilidad ciertamente no es simétrica, sin embargo si $n \mid m$ y $m \mid n$, entonces $m = nu$, donde u es una unidad. Esto se sigue ya que las hipótesis implican $m = nk, \ n = tm, \ k, t \in \mathbb{Z}$. Por lo cual $m = tkm$ y $tk = 1$, *i.e.*, k es una unidad. Si $m = 0$, entonces también $n = 0$ y $0 = 1 \cdot 0$. Exhibimos ahora una propiedad que relaciona el orden con la divisibilidad.

Proposición 1.1.3. *Sean $m, n \in \mathbb{Z} - \{0\}$, tales que $n \mid m$, entonces*

$$|n| \leqslant |m|.$$

Demostración. Usamos el hecho de que el orden es compatible con el producto, véase, por ejemplo, [9], Proposición 6.4.3. Se sigue del Corolario 1.1.2 que $|m| = |n|q$. Obsérvese que $q \geqslant 1$. De otra manera, si $q \leqslant 0$, se tendría $|m| = |n|q \leqslant |n| \cdot 0 = 0$, lo que contradice $m \neq 0$.

Finalmente, si $q = 1$, $|m| = |n|$ y si $q > 1$ se tiene

$$|m| = |n|q > |n|.$$

□

El siguiente resultado muestra la relación de la suma y el producto con la divisibilidad.

Proposición 1.1.4. *Sean $m, n, p \in \mathbb{Z}$,*

(i) si $n \mid m$ y $n \mid p$, entonces $n \mid m + p$,

(ii) si $n \mid m$ y $p \in \mathbb{Z}$, entonces $n \mid mp$.

Demostración.

(i) Como $m = nk$ y $p = nt$,

$$m + p = nk + nt = n(k + t).$$

(ii) Si $m = nk$, $\quad mp = npk$.

□

Corolario 1.1.5. *Sean $m, n, p \in \mathbb{Z}$, tales que $n \mid m$ y $n \mid p$, entonces*

$$n \mid mk + pt \quad \forall\ k, t \in \mathbb{Z}.$$

Definición 3. *Dados $m, p \in \mathbb{Z}$, a los números de la forma $mk + pt$, $k, t \in \mathbb{Z}$ se les llama combinaciones lineales de m y p.*

El Corolario 1.1.5 se puede afinar aún más.

Corolario 1.1.6. *Un entero n es divisor de los enteros m y p (divisor común) si y sólo si n divide a cualquier combinación lineal de m y p.*

Demostración. La necesidad es el corolario anterior. La suficiencia se sigue ya que

$$n \mid m \cdot 0 + p \cdot 1 \quad \text{y} \quad n \mid m \cdot 1 + p \cdot 0.$$

□

Nótese que dados dos enteros, no cualquier otro entero es combinación lineal de ellos. Por ejemplo, 8 no es combinación lineal de 10 y de 25, ya que como $5 \mid 10$ y $5 \mid 25$, se tendría $5 \mid 8$, por el Corolario 1.1.5. También 17 no es combinación lineal de 15 y 24.

En general, si $t = km + sp$, y d es divisor común de m y p, necesariamente $d \mid t$ (Corolario 1.1.5). Probaremos posteriormente que esta última propiedad ($d \mid t$), cuando d es el máximo común divisor, es una condición suficiente para que t sea combinación lineal de m y p (Corolario (1.3.3)).

Definición 4. *Dados enteros $m_1, m_2, \ldots, m_k$, a los enteros de la forma*

$$c_1 m_1 + c_2 m_2 + \cdots + c_k m_k, \ c_i \in \mathbb{Z}, \ \forall\ i \in \{1, 2, \ldots, k\}$$

se les llama combinaciones lineales de $m_1, m_2, \ldots, m_k$.

Obsérvese que $\forall\ i, \ \ m_i$ es combinación lineal de $m_1, m_2, \ldots, m_k$.

EJERCICIOS 1.1

1. Exhiba cinco enteros que no sean combinación lineal de 6 y 10.

2. Pruebe que 26 no es combinación lineal de 5 y 10.

1.2. El algoritmo de la división

Dados 2 enteros, no siempre uno es factor del otro. Sin embargo, siempre se puede *dividir* obteniendo un *cociente* y un *residuo*. El siguiente resultado describe de manera precisa este hecho.

Teorema 1.2.1. (Algoritmo de la división) *Sean $a, b \in \mathbb{Z}, \ b \neq 0$, entonces existen q, r únicos tales que*

$$a = bq + r, \quad \textit{donde} \quad 0 \leqslant r < |b|.$$

Al número r se le llama el *residuo* (de dividir a entre b) y a q el *cociente*.

Demostración. Probamos primero la unicidad:

Si

$$a = bq + r \qquad 0 \leqslant r < |b|,$$

y

$$a = bq' + r' \qquad 0 \leqslant r' < |b|,$$

se tiene

$$b(q - q') = r' - r$$

y

$$|b||q - q'| = |r - r'|.$$

Si $r = r'$, se tiene $q = q'$ y se sigue el resultado ($|b| \neq 0$). De otra manera se seguiría de la Proposición 1.1.3 que

$$|b| \leqslant |r' - r|.$$

Sin embargo, lo correcto es

$$|r' - r| < |b|.$$

Ya que por ejemplo, si

$$r' > r,$$

se tiene

$$0 \leqslant r' - r < r' < |b|$$

(el caso $r > r'$ es análogo).

Para probar la existencia se consideran casos:

Caso 1: $a,\ b > 0$.

$$\text{Sea} \qquad W = \{a - bk \ \mid \ k \in \mathbb{Z},\ a - bk \geqslant 0\},$$

como $a = a - b \cdot 0 \ \in W,\ W \neq \emptyset$.

Se afirma que r el menor elemento de W es el residuo buscado (el menor elemento existe por el principio del buen orden, r puede también ser 0).

Como $r = a - bq \geqslant 0$

$$a = bq + r \quad (r \geqslant 0),$$

por lo que basta probar que $r < b$. Esto se sigue, ya que si $r > b,\ r - b$ es un elemento menor a r que está en W, ya que

$$r - b = a - bq - b = a - b(q + 1).$$

Caso 2: $a > 0,\ b < 0$.

Aplicando el Caso 1 a a y $-b$, se tiene

$$a = (-b)q + r, \quad 0 \leqslant r < | - b|,$$

es decir

$$a = b(-q) + r, \quad 0 \leqslant r < |b|.$$

Caso 3: $a < 0,\ b < 0$.
El truco del Caso 2 no es suficiente, ya que

$$-a = (-b)q + r \quad \Longrightarrow \quad a = bq - r, \text{ pero } -r \leqslant 0.$$

Sin embargo, podemos escribir

$$a = bq + b - r - b = b(q + 1) + (-b - r),$$

y como

$$0 \leqslant r < |b| = -b,$$

se tiene

$$0 \leqslant -b - r < -b = |b|$$

y

$$-b - r \text{ es el residuo buscado.}$$

Caso 4: $a < 0,\ b > 0$.
La prueba de este caso queda como ejercicio para el lector. □

Ejemplos. Encontramos cocientes y residuos para $a = \pm 483$ y $b = \pm 25$.

$$a = 483, \quad b = 25.$$

$$\text{Como} \quad 483 = 25 \cdot 19 + 8, \quad \text{se obtiene} \quad q = 19 \quad \text{y} \quad r = 8.$$

$$a = 483, \quad b = -25.$$

$$\text{Como} \quad 483 = (-25)(-19) + 8, \quad \text{se obtiene} \quad q = -19 \quad \text{y} \quad r = 8.$$

$$a = -483, \quad b = 25.$$

$$\text{se tiene del 1er ejemplo, } -483 = 25(-19) - 8 = 25(-19) - 25 + 25 - 8$$

$$= 25(-20) + 17, \quad \text{y entonces } q = -20 \quad r = 17.$$

$$a = -483, \quad b = -25.$$

$$\text{Como } -483 = (-25)(19) - 8 + 25 - 25 \quad = \quad (-25)(20) + 17,$$

$$\text{se obtiene} \quad q = 20 \quad \text{y} \quad r = 17.$$

Aparentemente el algoritmo de la división es el método para encontrar los divisores de un número. Probaremos posteriormente que hay métodos más eficientes (descomposición en primos).

EJERCICIOS 1.2

1. Termine la prueba del Teorema 1.2.1.

2. Divida -1024 entre 21 y entre -21, -216 entre 11 y -17 entre 240.

1.3. El máximo común divisor y el mínimo común múltiplo

Definición 5. *Dados $a, b \in \mathbb{Z}$, alguno de éstos distinto de 0, el máximo común divisor de a y b es el mayor entero que es divisor de ambos números. Este número se denota por (a, b).*

Obsérvese que $(a, b) \geqslant 1$, ya que 1 es factor de todo entero, incluido el cero.

Ejemplo. Los divisores comunes de 120 y 36 son

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12,$$

por lo que

$$(36, 120) = 12.$$

En la discusión del MCD (máximo común divisor) podemos restringirnos a números positivos, ya que como se mostró antes los signos no alteran la divisibilidad (y el caso $a = 0$ o $b = 0$ es trivial).

Se mostró que si t es combinación lineal de a y b y d es un divisor común de a y b, entonces $d \mid t$. Mostramos ahora que esta última propiedad, aplicada al caso $d = (a, b)$, es suficiente, para que t sea combinación lineal de a y b.

Lema 1.3.1. *La combinación lineal positiva mínima de a y b es un divisor común de a y b.*

Demostración. Sea d la combinación lineal positiva mínima de a y b, entonces existen $s, t \in \mathbb{Z}$ tales que

$$d = as + bt.$$

Aplicando el algoritmo de la división a a y a d, se tiene

$$a = dq + r \qquad 0 \leqslant r < d.$$

Necesariamente $r = 0$, de otra forma (sustituyendo)

$$a = (as + bt)q + r \quad \text{y} \quad a(1 - sq) - btq = r,$$

contradiciendo que d es la combinación lineal mínima.

$$\therefore\ d \mid a, \quad \text{análogamente } d \mid b.$$

□

Teorema 1.3.2. *El MCD de a y b es la combinación lineal positiva mínima de a y b.*

Demostración. Sea $d = (a, b)$ y m la combinación lineal positiva mínima de a y b. Se sigue del Lema 1.3.1 que $m \mid a$ y que $m \mid b$, por lo que $m \leqslant d$ (d es el mayor de los divisores comunes). Por otra parte, como $d \mid a$ y $d \mid b$ se tiene que $d \mid m$ y por lo tanto $d \leqslant m$. □

Corolario 1.3.3. *Un entero c es combinación lineal de a y b $\iff$ $(a, b) \mid c$.*

Demostración. $\Rightarrow$) Es un caso particular del Corolario 1.1.5, ya que (a, b) es un divisor común.

$\Leftarrow$) Si $d = (a, b)$ se sigue del Teorema 1.3.2 que $d = ak + bt \quad k, t \in \mathbb{Z}$, y también por hipótesis, $c = md$, por lo cual

$$c = mak + mbt = a(mk) + b(mt).$$

□

EL Teorema 1.3.2 se puede reformular de manera más general.

Teorema 1.3.4. *Si $a, b, d \in \mathbb{N}$, las siguientes 4 condiciones son equivalentes:*

i) $d = (a, b)$, *i.e., d es el mayor de los divisores comunes de a y b,*

ii) *d es la combinación lineal positiva mínima de a y b,*

iii) *d es un divisor común de a y b que tiene la propiedad de que si t es otro divisor común (de a y b), entonces $t \mid d$,*

iv) *d es un divisor común de a y b que también es combinación lineal de éstos.*

Demostración. El Teorema 1.3.2 muestra que *i)* y *ii)* son equivalentes. También, *i)* y *ii)* $\Rightarrow$ *iii)*, ya que si t es un divisor común de a y b, t es factor de toda combinación lineal. Evidentemente *i)* y *ii)* $\Rightarrow$ *iv)*, por lo que basta probar que *iii)* $\Rightarrow$ *i)* y *iv)* $\Rightarrow$ *i)*, probamos la primera implicación y dejamos la segunda como ejercicio.

Sea $m \in \mathbb{N}$ tal que cumple *iii)* y $d = (a, b)$. Hay que probar que $m = d$. Se sigue de *iii)* que m es divisor común y entonces $m \leqslant d$, también se sigue de *iii)* que como d es divisor común $d \mid m$, por lo cual $d \leqslant m$ y $d = m$. □

Obsérvese que las condiciones *iii)* y *iv)* no usan el concepto de orden, por lo que sirven para definir el MCD en anillos no ordenados.

Definición 6. *Se dice que $a, b \in \mathbb{Z}$ son primos relativos o primos entre sí, si*

$$(|a|, |b|) = 1.$$

Ejemplo. Los números 13 y 18 son primos relativos. Sin embargo, 121 y 11 no lo son, ya que 11 es un divisor común.

Como consecuencia inmediata del Teorema 1.3.4 se tiene el siguiente resultado.

Corolario 1.3.5. *Dos números $a, b \in \mathbb{Z}$ son primos relativos si y sólo si $\exists\ s, t \in \mathbb{Z}$ tales que*

$$1 = as + bt.$$

Obsérvese que si $a \mid bc$, no necesariamente $a \mid b$ o $a \mid c$, por ejemplo, $10 \mid 8 \cdot 5$, pero $10 \nmid 8$ y $10 \nmid 5$; sin embargo se tiene el siguiente resultado.

Proposición 1.3.6. *Si $a \mid bc$ y $(a, b) = 1$, entonces $a \mid c$.*

Demostración. Como $1 = ka + tb$, donde $k, t \in \mathbb{Z}$, se tiene $c = kac + tbc$. Finalmente, $a \mid a$ y $a \mid bc$, entonces $a \mid c$. □

Este resultado se entenderá mejor posteriormente, a la luz de la descomposición en primos. Estudiamos ahora el concepto dual al MCD

Definición 7. *Dados $a, b \in \mathbb{Z} - \{0\}$, al menor múltiplo positivo de a y b se le llama mínimo común múltiplo de a y b (MCM), y se le denota por $[a, b]$.*

Evidentemente el conjunto de múltiplos comunes es no vacío, uno de ellos es $|ab|$, el menor existe por el PBO. Por ejemplo, si $a = 8$ y $b = 10$, los múltiplos positivos de a son $\{8, 16, 24, 32, 40, 48, \ldots\}$ y los de b, $\{10, 20, 30, 40, \ldots\}$, respectivamente, por lo que

$$[8, 10] = 40.$$

Exhibimos ahora otra caracterización del mínimo común múltiplo, que lo caracteriza en términos de otros múltiplos. Como en el caso del MCD, para evitar complicaciones innecesarias, se puede trabajar exclusivamente con números no negativos.

Teorema 1.3.7. *Sea m' un múltiplo común de $a, b \in \mathbb{N}$, entonces*

$$[a, b] \mid m'.$$

Demostración. Sea $m = [a, b]$, aplicando el algoritmo de la división se tiene

$$m' = mq + r, \quad 0 \leqslant r < m.$$

Ahora, como $a \mid m'$ y $a \mid m$ entonces $a \mid r$; análogamente $b \mid r$.

Si $r > 0$, r sería un múltiplo común menor a m,

$$\therefore \quad r = 0 \quad y \quad m \mid m'.$$

□

La propiedad del teorema anterior caracteriza al MCM.

Teorema 1.3.8. *Si m es un múltiplo común de $a, b \in \mathbb{N}$ que tiene la propiedad de que si m' es otro múltiplo común de a y b, necesariamente $m \mid m'$, entonces*

$$m = [a, b].$$

Demostración. Por definición $[a, b] \leqslant m$, y como $m \mid [a, b]$,

$$m \leqslant [a, b].$$

□

El MCD y el MCM están relacionados, por ejemplo si $a = 14$ y $b = 10$

$$(a, b)[a, b] = 2 \cdot 70 = ab,$$

esto sucede en general.

Teorema 1.3.9. *Dados $a, b \in \mathbb{N}$, siempre se cumple que*

$$ab = (a, b)[a, b].$$

Demostración. Como ab es un múltiplo común de a y b, se obtiene

$$ab = mt, \quad \text{donde } m = [a, b],$$

en virtud del Teorema 1.3.7. Se debe probar que $t = (a, b)$. Para probar esto usamos la propiedad *iii*) del Teorema 1.3.4.

Primero probamos que t es un divisor común: como $m = ar$, se tiene

$$ab = art, \quad \text{y} \quad a(b - rt) = 0,$$

$$\therefore \quad b = rt \quad \text{y} \quad t \mid b, \quad \text{análogamente} \quad t \mid a.$$

Ahora, si s es otro divisor común

$$a = sa' \quad \text{y} \quad b = sb',$$

y se tiene que $m' = a'b's$ es un múltiplo común de a y b, por lo que $m' = mq$. Finalmente,

$$mt = ab = a'sb's = m's = mqs$$
$$\therefore \quad m(qs - t) = 0 \quad \text{y} \quad s \mid t.$$

□

La idea de la prueba fue generar un múltiplo común "económicamente" con s, para expresar $ab = mt$, como $m(\text{entero})s$, usando la propiedad del Teorema 1.3.7. Una demostración más natural se exhibirá después con el teorema de descomposición en primos.

Los conceptos de MCD y MCM se extienden a más de 2 enteros.

Definición 8. *Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z} - \{0\}$ se define el MCD como el mayor divisor positivo de todos estos números, y el MCM como el menor múltiplo común positivo de todos estos números; éstos se denotan por $(a_1, a_2, \ldots, a_n)$ y $[a_1, a_2, \ldots, a_n]$.*

Ejemplos.

$$(6, 14, 28) = 2$$
$$[6, 14, 28] = 84,$$

ya que los múltiplos de 28 son $28,\ 56,\ 84 \quad \text{y} \quad 3 \nmid 28, \quad 3 \nmid 56.$

Teorema 1.3.10. *Sean $a_1, a_2, \ldots, a_n \in \mathbb{N}$ y d un divisor común tal que es combinación lineal de $a_1, a_2, \ldots, a_n$, entonces*

$$d = (a_1, a_2, \ldots, a_n).$$

Demostración. Sea $t = (a_1, a_2, \ldots, a_n)$, entonces $d \leqslant t$ y como $t \mid d$,

$$t \leqslant d \quad \therefore \quad t = d.$$

□

En la prueba del teorema anterior usamos el hecho de que si $t \mid a_i \quad \forall\, i$, entonces t es divisor de cualquier combinación lineal de las a_i (esto se prueba de manera análoga al Corolario 1.1.5).

Obsérvese que el Lema 1.3.1 y el Teorema 1.3.4 también son válidos para n naturales (mismas demostraciones). Nótese que también el Teorema 1.3.8 se cumple para n números. Estos hechos son útiles para resolver algunos de los ejercicios al final de esta sección.

Proposición 1.3.11. *Sean a, b primos relativos tales que $a \mid c$ y $b \mid c$, entonces $ab \mid c$.*

Demostración. Sea $c = ar$, como $b \mid c$ se tiene $b \mid ar$, y usando la Proposición 1.3.6 (como $(a, b) = 1$), se sigue que $b \mid r$ y $c = abt$ $(r = bt)$. □

Proposición 1.3.12. *Sean $a, b \in \mathbb{N}$, $d = (a, b)$, $da' = a$ y $db' = b$, entonces $[a, b] = da'b'$. Más aún, $(a', b') = 1$.*

Demostración. Ciertamente $da'b'$ es un múltiplo común, por lo que basta probar que si c es un múltiplo común $a'b'd \mid c$.

Obsérvese primero que $(a', b') = 1$, ya que como $d = a'dr + b'ds$, $r, s \in \mathbb{Z}$, se tiene

$$1 = a'r + b's.$$

Si c es un múltiplo común, $c = ak = a'dk$, también $b'd|c$ y por lo tanto $b'|a'k$ y $b'|k$,

$$\therefore \quad c = a'db't.$$

□

El Teorema 1.3.9 es un corolario inmediato de la Proposición 1.3.12, ya que si

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

entonces

$$d[a, b] = ab.$$

EJERCICIOS 1.3

1. Termine la prueba del Teorema 1.3.4.

2. Sean $a_1, a_2, \ldots, a_n \in \mathbb{N}$, y $d_j = (a_1, a_2, \ldots, a_j)$, $j \geqslant 2$, demuestre que $\forall\, j \geqslant 3 \quad d_j = (d_{j-1}, a_j)$. Calcule $(30, 42, 69)$ y $(96, 66, 108)$.

3. Sean $a_1, a_2, \ldots, a_n \in \mathbb{N}$ y $m_j = [a_1, a_2, \ldots, a_j]$, $j \geqslant 2$, demuestre que $\forall\, j \geqslant 3 \quad m_j = [m_{j-1}, a_j]$. Calcule $[6, 15, 9]$ y $[8, 12, 18]$.

4. Si $k, a, b \in \mathbb{N}$, pruebe que $(ka, kb) = k(a, b)$ y $[ka, kb] = k[a, b]$.

5. Probar que el Teorema 1.3.4 es válido para k naturales, donde $k \geqslant 2$.

1.4. Algoritmo de Euclides, Ecuaciones diofantinas

1.4.1. Algoritmo de Euclides

Sean $a, b \in \mathbb{N}$, si a es un múltiplo de b, $(a, b) = b$, de otra manera se puede aplicar iteradamente el algoritmo de la división, como se muestra a continuación, hasta obtener 0 como residuo.

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

como $0 < r_n < r_{n-1} < \ldots < r_2 < r_1 < b$, es claro que después de un número finito de pasos se obtiene un residuo 0, esto es, $r_{n+1} = 0$. A este proceso se le llama el **Algoritmo de Euclides**.

Proposición 1.4.1. *Dados $a, b \in \mathbb{N}$, se tiene que (a, b) es el último residuo distinto de cero en el algoritmo de Euclides, i.e., $(a, b) = r_n$.*

Para probar este resultado probamos primero un lema.

Lema 1.4.2. *Si $a = bq + r$, entonces*

$$(a, b) = (b, r).$$

Demostración. Como $(b, r) \mid b$ y $(b, r) \mid r$, se tiene que $(b, r) \mid a$, *i.e.*, $(b, r) \mid (b, a)$. También $(a, b) \mid r$, por lo que $(a, b) \mid (b, r)$,

$$\therefore \quad (a, b) = (b, r).$$

□

Demostración. (De la Proposición 1.4.1) Aplicando repetidamente el Lema 1.4.2 se tiene

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

□

El Algoritmo de Euclides nos permite dar un procedimiento para expresar el MCD como una combinación lineal de a y b. Esto se sigue del siguiente resultado.

Proposición 1.4.3. *Si r es combinación lineal de t y b y t lo es de a y b, entonces r es combinación lineal de a y b.*

Demostración.

$$\begin{aligned} r &= nt + sb \\ t &= ka + ub \\ \therefore \quad r &= (nk)a + (nu + s)b. \end{aligned}$$

□

Aplicando este resultado verificamos nuestra observación: como r_n es una combinación lineal de r_{n-1} y r_{n-2}, y r_{n-1} lo es de r_{n-2} y r_{n-3}, se tiene que r_n es combinación lineal de r_{n-2} y r_{n-3}; repitiendo el mismo procedimiento, r_n es combinación lineal de r_{n-3} y r_{n-4}, etcétera. Por lo cual r_n es combinación lineal de a y b.

Ejemplo. Usando algoritmo de Euclides, encontramos el MCD de a=242 y b=168, y con estos datos lo expresamos como combinación lineal de a y b.

$$\begin{aligned} 242 &= 168(1) + 74 \\ 168 &= 74(2) + 20 \\ 74 &= 20(3) + 14 \\ 20 &= 14(1) + 6 \\ 14 &= 6(2) + 2 \\ 6 &= 2 \cdot 3 \\ \therefore \quad (168, 242) &= 2, \end{aligned}$$

y

$$\begin{aligned} 2 &= 14 - 2(6) = 14 - 2(20 - 14) \\ &= 3 \cdot 14 - 2 \cdot 20 = 3(74 - 3 \cdot 20) - 2 \cdot 20 \\ &= 3 \cdot 74 - 11(20) = 3 \cdot 74 - 11(168 - 74 \cdot 2) \\ &= 25 \cdot 74 - 11(168) = 25(242 - 168) - 11(168) \\ &= 25(242) - 36(168) = 6050 - 6048. \end{aligned}$$

1.4.2. Ecuaciones Diofantinas

Estudiaremos ahora ecuaciones de la forma

$$ax + by = c, \qquad a, b, c \in \mathbb{Z}, \tag{1.1}$$

llamadas diofantinas. Consideremos primero el caso homogéneo, *i.e.*, $c = 0$.

Proposición 1.4.4. *Las soluciones enteras de la ecuación*

$$ax + by = 0, \tag{1.2}$$

$a, b \neq 0,\ (a, b) = 1,$ *son*

$$x = bt, \quad y = -at, \quad t \in \mathbb{Z}.$$

Demostración. Estas expresiones de x, y ciertamente son soluciones, probamos que son todas:

Si x, y es solución de (1.2), se tiene

$$by = -ax,$$

$$\therefore \quad b \mid ax,$$

y como $(a, b) = 1$, se sigue que $b \mid x$ (Proposición 1.3.6),

$$i.e., \quad x = bt,\ t \in \mathbb{Z}.$$

Por lo cual

$$by = -abt,$$

y entonces

$$y = -at.$$

□

Regresando a la ecuación general diofantina (1.1), obsérvese que el Corolario 1.3.3 se puede reformular como sigue:

Teorema 1.4.5. *La ecuación (1.1) tiene solución en $\mathbb{Z}$ si y sólo si*

$$(a, b) \mid c.$$

Recordamos que este resultado se sigue, ya que (a, b) es la combinación lineal positiva mínima. Para ilustrar el Teorema 1.4.5, consideramos la siguiente ecuación

$$15x + 21y = 10,$$

nótese que $(15, 21) = 3$. Sin embargo, $3 \nmid 10$, por lo que la ecuación no tiene solución entera.

Usando, el Algoritmo de Euclides se pueden encontrar soluciones particulares a las ecuaciones diofantinas. Esto es, hemos visto que con este algoritmo se encuentran $s, t \in \mathbb{Z}$ tales que

$$as + bt = d,$$

donde $d = (a, b)$. Escribiendo $c = dc'$, se tiene

$$asc' + btc' = c,$$

por lo que $x = sc'$ y $y = tc'$ es una solución de (1.1).

Por ejemplo,

$$30x + 8y = 140,$$

$$\begin{aligned} 30 &= 8 \cdot 3 + 6 & \qquad 2 &= 8 - 6 \cdot 1 \\ 8 &= 6 \cdot 1 + 2 & &= 8 - (30 - 3 \cdot 8) \\ 6 &= 2 \cdot 3 & &= 4 \cdot 8 - 30 \end{aligned}$$

$$\therefore \quad 140 = 70 \cdot 2 = 8(280) + 30(-70)$$

y

$$x = -70, \quad y = 280$$

es una solución.

Para poder encontrar todas las soluciones de (1.1) primero resolvemos el caso homogéneo (1.2).

Teorema 1.4.6. *Las soluciones de la ecuación (1.2) están dadas por*

$$x = -b't, \quad y = a't, \quad t \in \mathbb{Z},$$

donde $a = a'd,\ b = b'd,\ d = (a, b),\ a, b \neq 0$.

Demostración. Las soluciones de

$$ax + by = 0,$$

son las mismas que las de $a'x + b'y = 0$, ya que

$$a'dx + b'dy = 0 \iff a'x + b'y = 0,$$

por lo que el resultado se sigue de la Proposición 1.4.4. □

Los casos donde $a = 0$ o $b = 0$ son triviales. Si $a, b = 0$, toda pareja $(s, t) \in \mathbb{Z} \times \mathbb{Z}$ es solución de $ax + by = 0$, y $ax + by = c,\ c \neq 0,$ no tiene solución.

Si $a = 0$ y $b \neq 0$, cualquier pareja de la forma $(t, 0)$ es solución de

$$ax + by = 0,$$

y la ecuación $by = c,\ c \neq 0$ tiene solución $\iff b \mid c$. Ésta es única, ya que si $by_1 = by_2$, entonces $y_1 = y_2$. El otro caso, $b = 0$ y $a \neq 0$, es análogo.

Volviendo al caso general, las soluciones de (1.1) y (1.2) están muy relacionadas.

Lema 1.4.7. *Sea (x_0, y_0) una solución particular de (1.1) y (u, v) cualquier solución de (1.2), entonces*

$$(x_0 + u, y_0 + v)$$

es solución de (1.1), y viceversa toda solución de (1.1) es de esta forma.

Demostración.

$$(x_0 + u)a + (y_0 + v)b$$

$$= x_0a + y_0b + ua + vb = c + 0 = c.$$

Vicerversa, si

$$xa + yb = c,$$

entonces

$$(x - x_0)a + (y - y_0)b = c - c = 0.$$

$$\therefore \quad (x - x_0,\ y - y_0) \text{ es solución de (1.2).}$$

Escribiendo $x - x_0 = u$ y $y - y_0 = v,$ se sigue el lema, ya que entonces

$$x = x_0 + u, \quad y = y_0 + v.$$

□

Teorema 1.4.8. *El conjunto de todas las soluciones de (1.1), cuando $(a, b) \mid c$ y $a, b \neq 0$, está dado por*

$$x = x_0 - b't, \quad y = y_0 + a't, \quad t \in \mathbb{Z};$$

donde $a = a'd,\ b = b'd$ y (x_0, y_0) es una solución particular de (1.1).

Este resultado es consecuencia inmediata del Teorema 1.4.6 y el Lema 1.4.7. En consecuencia todas las soluciones de cualquier ecuación diofantina se pueden encontrar.

Ejemplo. Encontramos la solución general de la ecuación

$$25x + 35y = 200.$$

$$\begin{array}{ll} 35 = 25 \cdot 1 + 10 & 5 = 25 - 10 \cdot 2 \\ 25 = 10 \cdot 2 + 5 & 5 = 25 - 2(35 - 25) \\ 10 = 5 \cdot 2 & \quad = 3 \cdot 25 - 2 \cdot 35. \end{array}$$

Por lo que $5 = (35, 25)$ y como $40 \cdot 5 = 200$, una solución particular es

$$x_0 = 40 \cdot 3 = 120, \qquad y_0 = 40(-2) = -80.$$

Finalmente las soluciones de la homogénea son las mismas soluciones de la ecuación $5x + 7y = 0$, que son de la forma

$$x = 7t, \qquad y = -5t, \quad t \in \mathbb{Z},$$

por lo cual todas las soluciones de la ecuación original son

$$x = 120 + 7t, \qquad y = -80 - 5t, \quad t \in \mathbb{Z}.$$

EJERCICIOS 1.4

1. Resuelva: $30x + 24y = -18$, $49x - 14y = 70$, $-84x + 60y = 144$.

1.5. Teorema fundamental de la aritmética

Los números enteros se descomponen en factores irreducibles llamados primos, por ejemplo

$$120 = 60 \cdot 2 = 2^2 \cdot 3 \cdot 5 \cdot 2 = 2^3 \cdot 3 \cdot 5,$$

$$84 = 21 \cdot 4 = 7 \cdot 3 \cdot 2^2.$$

Definición 9. *Se dice que un número entero p distinto de ± 1 es primo, si sus únicos divisores son ± 1 y $\pm p$.*

Obsérvese que 0 no es primo (todo número es divisor del 0) y que p es primo si y sólo si $-p$ lo es. Los primeros primos positivos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 83, 89, 97, 101, 103, 107, 109, 113, 127, ...

Esto se verifica, notando que 3 y 7 no sean factores de los números, que no sean múltiplos de 5, o pares (véase la Proposición 1.5.4).

Nótese que si p es primo y $a \in \mathbb{Z}$ entonces

$$(a,p) = \begin{cases} p & \text{si } p \mid a, \\ 1 & \text{si } p \nmid a, \end{cases}$$

(si $p \nmid a$, el único divisor positivo común de p y a es 1).

Teorema 1.5.1. *Si un número primo p divide al producto ab, entonces $p \mid a$ o $p \mid b$.*

Demostración. Si p no divide a a, entonces $(p,a) = 1$ y en virtud de la Proposición 1.3.6 $p \mid b$. □

La propiedad establecida en el teorema anterior caracteriza los primos y al cero.

Corolario 1.5.2. *Sea $p \in \mathbb{Z}$, $p \neq \pm 1$, tal que satisface la siguiente propiedad: dados $a, b \in \mathbb{Z}$ tales que $p \mid ab$, se tiene que $p \mid a$ o $p \mid b$. Bajo esta hipótesis p es primo o $p = 0$.*

Demostración. Se puede suponer $p \geqslant 0$. Si $p \neq 0$ y p no es primo, existen naturales $a, b \neq 0$ tales que

$$p = ab, \quad 1 < a < p \ \text{ y } \ 1 < b < p.$$

Se sigue entonces que $p \nmid a$ y que $p \nmid b$, lo cual contradice la hipótesis sobre p, por lo tanto p es primo. Como el 0 solamente es factor de sí mismo, 0 también cumple esta propiedad. □

Teorema 1.5.3. (Teorema fundamental de la aritmética) *Dado $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, a se puede expresar como*

$$u\ p_1\ p_2 \cdots p_k, \tag{1.3}$$

donde $u = \pm 1$, y $p_1 \leqslant p_2 \cdots \leqslant p_k$ son números primos positivos, ésta descomposición es única.

Demostración. Basta probarlo para $a \in \mathbb{N}$, ya que si $-a = p_1\ p_2 \cdots p_k$, entonces $a = (-1)\ p_1\ p_2 \cdots p_k$.

Existencia. Sea $M \subset \mathbb{N}$, el conjunto de los números que no pueden descomponerse de la manera descrita en (1.3). Si $M \neq \emptyset$, por el principio del buen orden, M tiene un menor elemento a, este número no es un primo p, ya que $a = p$ es una descomposición tipo (1.3), por lo que

$$a = bc, \quad 1 < b < a \quad \text{y} \quad 1 < c < a,$$

y como $b, c \notin M$

$$b = p_1\ p_2 \cdots p_n \quad c = q_1\ q_2 \cdots q_m,$$

y

$$a = p_1\ p_2 \cdots p_n\ q_1\ q_2 \cdots q_m,$$

sin embargo reordenando los primos p_s y q_s en esta expresión se obtiene una descomposición del tipo (1.3) contradiciendo que $a \in M \ \therefore\ M = \emptyset$ y todo número tiene una descomposición en primos.

Unicidad. Se demuestra por inducción en el número de primos contados con multiplicidad que tiene la descomposición más *económica* de a, para simplificar se ignora (primero) el orden:

si $a = p$ y $a = q_1\ q_2 \cdots q_m$, entonces

$$p \mid q_1 \cdots q_m,$$

por lo que se sigue del Teorema 1.5.1 que

$$p \mid q_i, \quad \text{para algún } i \in \{1, 2, \ldots, m\},$$

i.e., $p = q_i$. Como $p = q_1\ q_2 \cdots q_i \cdots q_m$, se tiene

$$1 = q_1\ q_2 \cdots q_{i-1}\ q_{i+1} \cdots q_m,$$

y $q_j = 1 \quad \forall\ j \neq i$ (no hay divisores de 1 no triviales).

Suponiendo cierto para $n-1$, si

$$a = p_1 \cdots p_n \quad \text{y} \quad a = q_1 \cdots q_m, \quad m \geqslant n,$$

se tiene

$$p_1 \mid q_1 \cdots q_m \quad \text{y necesariamente} \quad p_1 \mid q_i,$$

para alguna i. Entonces $p_1 = q_i$, y por lo tanto

$$a' = p_2 \cdots p_n = q_1\ q_2 \cdots q_{i-1}\ q_{i+1} \cdots q_m.$$

Por hipótesis de inducción, $n = m$ y las colecciones $\{p_2, p_3, \ldots, p_n\}$ y $\{q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m\}$ contadas con repetición son iguales. Lo mismo es cierto para $\{p_1, \ldots, p_n\}$ y $\{q_1, \ldots, q_m\}$, y evidentemente ordenando estas colecciones, la expresión (1.3) es única. □

El Teorema 1.5.3 se puede refinar juntando los términos repetidos y obtener una expresión única para cualquier entero $a,\ a \neq 0, \pm 1$

$$a = \pm\ p_1^{m_1}\, p_2^{m_2} \cdots p_k^{m_k}, \quad m_i > 0,$$

donde

$$p_1 < p_2 < \cdots < p_k.$$

Algunas veces para comparar dos números es conveniente considerar potencias cero, *i.e.,*

$$a = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, \quad m_i \geqslant 0,$$

por ejemplo

$$24 = 2^3 \cdot 3 \cdot 5^0 \quad \text{y} \quad 40 = 2^3 \cdot 3^0 \cdot 5.$$

Un algoritmo útil para encontrar primos lo establece el siguiente resultado. En particular, la lista de los primeros primos enumerados al comienzo de esta sección.

Proposición 1.5.4. *Sea $a \in \mathbb{N}$, a no primo, entonces existe p primo tal que $p \mid a$ y $p \leqslant \sqrt{a}$.*

Demostración. Como a no es primo existen r, s tales que

$$a = rs, \quad 1 < r < a, \quad 1 < s < a,$$

sin perder generalidad $r \leqslant s$. Ahora, por el Teorema 1.5.3 existe p primo tal que $p \mid r$

$$\therefore \quad r = pr'.$$

Finalmente,

$$p^2 \leqslant p^2(r')^2 = r^2 \leqslant rs = a,$$

y

$$p \leqslant \sqrt{a}.$$

□

Por ejemplo, 131 es primo, ya que de otra manera existiría $p < \sqrt{131} < 12$ tal que $p \mid 131$, sin embargo $2, 3, 5, 7, 11$ no son divisores de 131.

Resulta que hay una infinidad de primos (ejercicio). La descomposición en primos es también útil para encontrar el MCD y el MCM, de dos enteros.

Teorema 1.5.5. *Sean $a, b \in \mathbb{N}$,*

$$a = p_1^{m_1} \cdots p_k^{m_k}, \quad b = p_1^{t_1} \cdots p_k^{t_k}, \quad t_j, m_j \geqslant 0 \ \forall \ j,$$

entonces

a) $(a, b) = p_1^{r_1} \cdots p_k^{r_k}$, *donde* $r_j = \min\{m_j, t_j\}$,

b) $[a, b] = p_1^{s_1} \cdots p_k^{s_k}$, *donde* $s_j = \max\{m_j, t_j\}$.

Demostración. Probamos a) y dejamos b) como ejercicio.

Sea $d = p_1^{r_1} \cdots p_k^{r_k}$, $\quad r_j = \text{mín}\{m_j, t_j\},\ j \in \{1, \ldots, k\}$, entonces

$$a = p_1^{m_1 - r_1} \cdots p_k^{m_k - r_k} \cdot d \quad \text{y} \quad d \mid a.$$

Ya que $\quad (m_j - r_j \geqslant 0,\ \forall\ j)$. Análogamente $d \mid b$.

Ahora si t es un divisor común de a y b,

$$t = p_1^{q_1} \cdots p_k^{q_k}$$

(t no contiene otros factores primos, ya que a, b no los tienen). Necesariamente $q_i \leqslant r_i$, si $\ q_j > r_j$ para alguna j

$$p_j^{q_j} \nmid a \quad \text{o} \quad p_j^{q_j} \nmid b.$$

$$\therefore \quad t \mid d \quad \text{y} \quad d = (a, b).$$

□

Como dados $m, n \in \mathbb{N} \cup \{0\}$,

$$m + n = \text{máx}\{m, n\} + \text{mín}\{m, n\},$$

se sigue del Teorema 1.5.5 una tercera prueba del Teorema 1.3.9, es decir

$$ab = (a, b)[a, b].$$

Ejemplo Si $a = 2^3 \cdot 3^4 \cdot 5$ y $b = 2 \cdot 3 \cdot 7$.

$$(a, b) = 2 \cdot 3$$

$$[a, b] = 2^3 \cdot 3^4 \cdot 5 \cdot 7.$$

EJERCICIOS 1.5

1. Demuestre, de manera análoga a la prueba del Teorema 1.5.3, que todo entero mayor a 1 es divisible entre un número primo.

2. Demuestre que hay una infinidad de primos.

3. Termine la prueba del Teorema 1.5.5.

4. Encuentre, a_1, a_2, a_3 números naturales tales que no cumplan la identidad $a_1\, a_2\, a_3 = (a_1, a_2, a_3)[a_1, a_2, a_3]$.

5. Generalice y pruebe el Teorema 1.5.5 para más de dos números naturales.

6. Demostrar que hay una infinidad de primos de la forma $4k + 3$.

7. Sea $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \in \mathbb{N}$, donde p_j son primos diferentes. Demuestre que el número de divisores de N es $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

8. Dado un natural N, pruebe que existen N naturales consecutivos que no son primos.

1.6. Congruencias

Se mostró en [9] que la divisibilidad determina naturalmente relaciones de equivalencia en $\mathbb{Z}$, y por ende los importantes anillos $\mathbb{Z}_m$.

Definición 10. *Se dice que $a, b \in \mathbb{Z}$ son congruentes módulo m, $m \in \mathbb{Z}$ fijo, si*

$$a - b = km, \text{ para alguna } k \in \mathbb{Z},$$

se escribe $a \equiv b \mod m$.

Obsérvese que esta relación es precisamente la relación de equivalencia que define los anillos $\mathbb{Z}_m$, *i.e.* los elementos de $\mathbb{Z}_m$ son las clases de equivalencia que consisten de todos los números en $\mathbb{Z}$ que son congruentes entre sí módulo m.

Por ejemplo, si $m = 2$ todos los pares son congruentes entre sí, ya que

$$2t \equiv 2n \mod 2 \quad \forall\, t, n \in \mathbb{Z},$$

y también los impares son congruentes entre sí, módulo 2

$$2t + 1 \equiv 2n + 1 \mod 2 \quad \forall\, t, n \in \mathbb{Z}.$$

Un par y un impar nunca son congruentes: si fuera el caso

$$2n + 1 \equiv 2t \mod 2$$

$$\Rightarrow 2 \mid 2n + 1 - 2t \quad \text{y} \quad 2 \mid 2(n - t) + 1,$$

y se tendría que $2 \mid 1$, lo cual es absurdo.

Tomando $m = 7$ podemos verificar que los números $7k + 4$, $k \in \mathbb{Z}$, son todos congruentes entre sí

$$7k_1 + 4 \equiv 7k_2 + 4 \mod 7$$

$$\Leftrightarrow 7 \mid 7(k_1 - k_2).$$

Sin embargo, ningún número de la forma $7k + 3$, $k \in \mathbb{Z}$ es congruente con uno de la forma $7t + 6$, $t \in \mathbb{Z}$. Si fuera el caso

$$7k + 3 \equiv 7t + 6 \mod 7$$

$$\Rightarrow 7 \mid 7(k - t) + 6 - 3 \quad \text{y} \quad 7 \mid 6,$$

lo cual es imposible.

Recordamos la relación de equivalencia en $\mathbb{Z}$ definida en el primer curso (cf. [9], capítulo 6). Dada $m \in \mathbb{N}$ fija, $a, b \in \mathbb{Z}$ son equivalentes, denotado como $a \sim b$, si $a - b = km$. En otras palabras, $a \sim b$ si

$$a \equiv b \mod m.$$

En consecuencia, las congruencias cumplen las propiedades que definen una relación de equivalencia, es decir,

i) $a \equiv a \mod m, \quad \forall\, a \in \mathbb{Z},$

ii) si $a \equiv b \mod m, \quad$ entonces $\quad b \equiv a \mod m,$

iii) si $a \equiv b \mod m \quad$ y $\quad b \equiv c \mod m, \quad$ entonces $\quad a \equiv c \mod m.$

Las congruencias son compatibles con la suma y la multiplicación.

Proposición 1.6.1. $\forall\, a, b, c \in \mathbb{Z}$ *se tiene:*

i) Si $a \equiv b \mod m$*, entonces* $a + c \equiv b + c \mod m$.

ii) Si $a \equiv b \mod m$*, entonces* $ac \equiv bc \mod m$.

DEMOSTRACIÓN. *i)* Si $m \mid a - b, \quad$ entonces $\quad m \mid (a + c) - (b + c)$.

ii) Si $m \mid a - b, \quad$ entonces $\quad m \mid ca - cb$.

□

Para comprender mejor la relación de las congruencias con los anillos $\mathbb{Z}_m$ es útil observar que todo entero es congruente módulo m con exactamente uno de los números $0, 1, 2, 3, \ldots, m - 1$. De hecho, si al dividir un entero a entre m, su residuo es r, entonces $a \equiv r \mod m$. Como caso particular, en $\mathbb{Z}_5$ todo entero es congruente módulo 5 con 0, 1, 2, 3, o 4.

Obsérvese que se sigue del Teorema 1.5.1 que si p es un primo positivo y $ab \equiv 0 \mod p$, entonces $a \equiv 0 \mod p \quad$ o $\quad b \equiv 0 \mod p$.

Sin embargo, si

$$ab \equiv 0 \mod m,$$

no necesariamente $a \equiv 0 \quad$ o $\quad b \equiv 0 \mod m$. Por ejemplo, $3 \cdot 4 \equiv 0 \mod 6$, pero $3 \not\equiv 0 \mod 6$ y $4 \not\equiv 0 \mod 6$, o $5 \cdot 4 \equiv 0 \mod 10$, pero $5 \not\equiv 0 \mod 10$, y $4 \not\equiv 0 \mod 10$.

Las congruencias se pueden sumar y multiplicar.

Proposición 1.6.2. *Si* $a \equiv b \mod m$ *y* $c \equiv d \mod m$*, entonces*

i) $a + c \equiv b + d \mod m$.

ii) $ac \equiv bd \mod m$.

DEMOSTRACIÓN.

i) $m \mid a - b \quad$ y $\quad m \mid c - d \Rightarrow m \mid a + c - (b + d)$.

ii) Como $m \mid ac - bc \quad$ y $\quad m \mid bc - bd,$ se sigue que $\quad m \mid ac - bd.$ □

Obsérvese que si $a \equiv b \mod m$, entonces $a = b + km,\ k \in \mathbb{Z}$. Por lo que, tomando un representante en cada clase, y sumándole múltiplos de m, se obtienen todos los elementos que son congruentes entre sí.

Resolvemos ahora ecuaciones de congruencias con una incógnita. Consideramos primero un ejemplo

$$25x - 16 \equiv 0 \mod 21.$$

La solución de esta ecuación se puede encontrar interpretándola como una ecuación diofantina

$$25x - 16 = 21y,$$

i.e., $25x - 21y = 16$.

$$\begin{array}{rcl} 25 &=& -21(-1) + 4 \\ -21 &=& 4(-6) + 3 \\ 4 &=& 3 \cdot 1 + 1 \end{array} \qquad \begin{array}{rcl} 1 &=& 4 - 3 \\ &=& 4 - (-21 + 4 \cdot 6) \\ &=& 21 \cdot 1 - 4 \cdot 5 \\ &=& 21 - 5(25 - 21) \end{array}$$

$$\therefore \quad 1 = 25(-5) - 21(-6).$$

En consecuencia

$$16 = 25(-80) - 21(\textit{entero})$$

y -80 es una solución particular de la congruencia $25x \equiv 16 \mod 21$.

A esta congruencia le podemos asociar su congruencia *homogénea*

$$25x \equiv 0 \mod 21,$$

cuyas soluciones son $x = 21t,\ t \in \mathbb{Z}$ (ya que las soluciones de $25x - 21y = 0$ son $x = -21(-t), \quad y = 25t,\ t \in \mathbb{Z}$).

Las Proposiciones 1.6.3 y 1.6.4 prueban que todas las soluciones son

$$x = -80 + 21t,$$

en particular 4 es solución, $25 \cdot 4 \equiv 16 \mod 21$.

En general, la ecuación

$$ax + b \equiv 0 \mod m,$$

$(m, a) = 1$ siempre tiene solución, ya que en este caso existen $r, t, \in \mathbb{Z}$ tales que $rm + ta = 1$, por lo que

$$m(\textit{entero}) + (-b)ta = -b$$

y

$$a(-bt) + b \equiv 0 \mod m.$$

Esta observación se puede generalizar.

Proposición 1.6.3. *La congruencia* $ax + b \equiv 0 \mod m$ *tiene solución si y sólo si* $(a, m) \mid b$.

DEMOSTRACIÓN. Existe una solución si y sólo si existen enteros x, y tales que satisfacen la igualdad $ym = ax + b \Leftrightarrow ax - ym = -b$. Dicha solución existe si y sólo si $(a, m) \mid -b$ (cf. Teorema 1.4.5). □

Proposición 1.6.4. *Sea* x_1 *una solución de*

$$ax + b \equiv 0 \mod m, \quad (a, m) = 1. \tag{1.4}$$

Entonces,

i) *si* $x_1 \equiv x_2 \mod m$, *se sigue que* x_2 *también es solución,*

ii) *si* x_2 *es solución de (1.4)*

$$x_2 \equiv x_1 \mod m.$$

DEMOSTRACIÓN. *i)* La condición $x_1 - x_2 = km$, se puede escribir

$$x_2 = x_1 - km,$$

por lo que

$$ax_2 + b = a(x_1 - km) + b = ax_1 + b - akm,$$

y como

$$m \mid ax_1 + b, \quad m \mid -akm,$$

se sigue que

$$m \mid ax_2 + b.$$

ii) Si $m \mid ax_1 + b$ y $m \mid ax_2 + b$, entonces

$$m \mid a(x_1 - x_2),$$

y dado que $(a, m) = 1$

$$m \mid x_1 - x_2.$$

□

Obsérvese que la condición $(a, m) = 1$ sólo se usa en *ii)*. Si $(a, m) > 1$, *ii)* no se cumple, en general. Por ejemplo, si

$$4x - 4 \equiv 0 \mod 6,$$

se tiene que $x = 1$ y $x = -2$ son soluciones pero $1 \not\equiv -2 \mod 6$.

A continuación probamos el teorema chino del residuo, que resuelve un sistema de dos congruencias, bajo ciertas condiciones.

Teorema 1.6.5. (Teorema chino del residuo) *Sean* $(m,n)=1$, *entonces las congruencias*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{1.5}$$

tienen una solución común.

Demostración. Como $(1,m) \mid a$ la primera de las congruencias tiene una solución particular r_1 y por la Proposición 1.6.4 cualquier otra solución es de la forma

$$r_1 + km, \quad k \in \mathbb{Z}.$$

Ahora, $r_1 + km \equiv b \mod n$ tiene solución, ya que $(m,n)=1$. Esta congruencia es equivalente a $km \equiv b - r_1 \mod n$. Por lo que existe $k_1 \in \mathbb{Z}$, tal que

$$r_1 + k_1 m \quad \text{es solución de (1.5).}$$

□

Podemos también encontrar todas las soluciones.

Corolario 1.6.6. *Sean* x_1, x_2 *soluciones de (1.5), entonces*

$$x_1 \equiv x_2 \mod mn.$$

Más aún, si x_1 *es una solución particular de (1.5) y* $x_2 \equiv x_1 \mod mn$, *entonces* x_2 *es una solución de (1.5), en particular existe una solución* t *de (1.5) tal que*

$$0 \leqslant t < mn.$$

Demostración. Si $x_1 \equiv a \mod m$ y $x_2 \equiv a \mod m$, entonces se cumple que $x_1 \equiv x_2 \mod m$, análogamente $x_1 \equiv x_2 \mod n$, y por lo tanto

$$m \mid x_1 - x_2 \quad \text{y} \quad n \mid x_1 - x_2,$$

como $(m,n)=1$

$$mn \mid x_1 - x_2 \quad \text{(Proposición 1.3.6).}$$

La 2a afirmación es consecuencia inmediata de la Proposición 1.6.4. □

Obsérvese que el Corolario 1.6.6 exhibe todas las soluciones del sistema (1.5). Este sistema se puede generalizar.

Teorema 1.6.7. (Teorema chino generalizado) *Sean $m_1, m_2, \ldots, m_k$ primos relativos entre sí (dos a dos), entonces el sistema de congruencias*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_k \mod m_k \end{cases} \tag{1.6}$$

tiene solución. Más aún, si x_1 es solución de (1.6) y $x_1 \equiv x_2 \mod m_1 m_2 \cdots m_k$, entonces x_2 es solución, y viceversa si x_2 es solución de (1.6)

$$x_2 \equiv x_1 \mod m_1 m_2 \cdots m_k.$$

DEMOSTRACIÓN. Demostramos la primera parte, la segunda se prueba usando los mismos argumentos que en el Corolario 1.6.6.

$x \equiv a_1 \mod m_1$ tiene como soluciones $r_1 + k_1 m_1,\ k_1 \in \mathbb{Z},$ donde r_1 es una solución particular, ya que $(m_1, 1) = 1$.

Ahora, la congruencia

$$r_1 + k_1 m_1 \equiv a_2 \mod m_2$$

tiene solución, ya que $(m_1, m_2) = 1$,

$$\therefore \quad \text{existe } r_2 = r_1 + k_1 m_1$$

que es solución común a las primeras 2 congruencias y todas las soluciones son de la forma

$$\{r_2 + k_2 m_1 m_2\}, \quad k_2 \in \mathbb{Z}.$$

Ahora buscamos $k_2 \in \mathbb{Z}$ tal que

$$r_2 + k_2 m_1 m_2 \equiv a_3 \mod m_3,$$

como $(m_1 m_2, m_3) = 1$, existe $k_2 \in \mathbb{Z}$ tal que

$$r_3 = r_2 + k_2 m_1 m_2$$

es solución de las primeras 3 congruencias, etcétera. □

El siguiente resultado establece un método para encontrar una solución particular del sistema (1.6), y por ende resolverlo.

Teorema 1.6.8. *Dado un sistema de k congruencias como en* (1.6)*, se tiene que si $\forall i \in \{1, 2, \ldots, k\}, \quad b_i = N/m_i$, donde $N = m_1 m_2 \cdots m_k$, y se toman enteros c_i tales que cumplen la congruencia $b_i\, c_i \equiv 1 \mod m_i$, se sigue que*

$$x_0 = a_1 b_1 c_1 + a_2 b_2 c_2 + \cdots + a_k b_k c_k$$

es una solución particular de (1.6)*.*

Demostración. Se toma i fija, $1 \leq i \leq k$. Nótese que si $j \neq i$, se tiene que $m_i | b_j$, y por lo tanto

$$a_j b_j c_j \equiv 0 \mod m_i \ \forall j \ \ j \neq i.$$

A su vez esta última congruencia implica que $x_0 \equiv a_i b_i c_i \mod m_i$.

Finalmente, como $b_i c_i \equiv 1 \mod m_i$ se tiene que $a_i b_i c_i \equiv a_i \mod m_i$, y entonces $x_0 \equiv a_i \mod m_i$. □

Ejemplos.

1) Veamos como se resuelve la congruencia $16x - 9 \equiv 0 \mod 35$. Esta ecuación equivale a la ecuación diofantina

$$16x - 35y = 9,$$

para encontrar una solución particular, se muestra que 35 y 16 son primos relativos, y se expresa a 1 como combinación lineal de estos números.

$$\begin{array}{ll} 35 = 16 \cdot 2 + 3 & 1 = 16 - 3 \cdot 5 \\ 16 = 3 \cdot 5 + 1 & \quad = 16 - 5(35 - 16 \cdot 2) \\ & \quad = (-35)5 + 11 \cdot 16, \end{array}$$

y se obtiene, al multiplicar por 9 que

$$9 = (-35)(45) + 99(16),$$

entonces 99 es una solución particular. Todas las soluciones son de la forma

$$\{99 + t(35)\}, \quad t \in \mathbb{Z},$$

o

$$\{-6 + t(35)\}, \quad t \in \mathbb{Z}.$$

2) Resolvemos el siguiente sistema de congruencias

$$\begin{cases} x \equiv -2 \mod 3 \\ x \equiv -1 \mod 5 \\ x \equiv \ 3 \mod 7. \end{cases} \tag{1.7}$$

Como 3, 5 y 7 son primos relativos dos a dos hay soluciones. Una manera de encontrarlas es aplicar el Teorema 1.6.8 para encontrar una solución particular y por ende resolver el sistema. Sin embargo, es conveniente conocer otras técnicas de solución.

Las soluciones de la primera congruencia están dadas por

$$1 + 3k_1, \quad k_1 \in \mathbb{Z}.$$

Ahora, las soluciones de la congruencia $1 + 3k_1 \equiv -1 \mod 5$ son las misma que las de la congruencia

$$3k_1 \equiv -2 \mod 5. \tag{1.8}$$

Se podría resolver esta congruencia como una ecuación diofantina, o directamente evaluando en los primeros dígitos. Sin embargo, la aplicación de algunos trucos, en muchos casos, permite resolver este tipo de ecuaciones de manera más rápida. Nótese que (1.8) se cumple si y sólo si

$$6k_1 \equiv -4 \mod 5, \tag{1.9}$$

y como $5k_1 \equiv 0 \mod 5$ se tiene que (1.9) se cumple $\iff k_1 \equiv -4 \mod 5$. Por lo que tomando $k_1 = 1$, se sigue que todas las soluciones de las primeras dos congruencias en (1.7) están dadas por

$$4 + 15k_2, \quad k_2 \in \mathbb{Z}.$$

Finalmente, las soluciones de $4 + 15k_2 \equiv 3 \mod 7$, son aquéllas de la congruencia

$$15k_2 \equiv -1 \mod 7. \tag{1.10}$$

Como $14k_2 \equiv 0 \mod 7$, la ecuación (1.10) se cumple $\iff k_2 \equiv -1 \mod 7$.

Tomando $k_2 = 6$, se sigue que 94 es solución particular de (1.7), y también lo es -11. Por consiguiente, todas las soluciones de (1.7) están dadas por

$$-11 + t(3 \cdot 5 \cdot 7), \quad t \in \mathbb{Z}.$$

Al usar trucos para resolver congruencias hay que tener en cuenta que no todas las simplificaciones son válidas. Por ejemplo, si se quiere resolver

$$7x \equiv 6 \mod 30. \tag{1.11}$$

Multiplicando por 4 esta congruencia, se tiene $28x \equiv 24 \mod 30$, y escribiendo $30x \equiv 0 \mod 30$, se puede restar la primera congruencia de esta última y se obtiene $2x \equiv -24 \mod 30$, o $x \equiv -12 \mod 15$. Ahora, 3 es solución de esta última congruencia, sin embargo no es solución de (1.11). ¿Dónde estuvo el error?

3) Se resuelve, para $n \in \mathbb{Z}$, $n \neq 0, 1$, la congruencia

$$(3n-2)x + 5n \equiv 0 \mod 9n - 9.$$

Probamos primero que $(3n-2, 9n-9) = 1$, $\forall\ n \in \mathbb{Z}$.

$$9n - 9 = (3n-2)3 - 3,$$

sin embargo $-3 < 0$, podemos multiplicar todo por -1, y

$$-(9n-9) = (-3)(3n-2) + 3$$

$$3n - 2 = 3(n-1) + 1.$$

Por consiguiente

$$\begin{aligned} 1 &= 3n - 2 - 3(n-1) \\ &= 3n - 2 - (n-1)[-(9n-9) + 3(3n-2)] \\ &= -(n-1)[-(9n-9)] + (3n-2)[1 - 3(n-1)] \\ \therefore \quad 1 &= (3n-2)(-3n+4) + (n-1)(9n-9), \end{aligned}$$

y multiplicando por $-5n$

$$-5n = (15n^2 - 20n)(3n-2) + (9n-9)(entero),$$

i.e.,

$$15n^2 - 20n \quad \text{es una solución particular}$$

y todas las soluciones son

$$\{15n^2 - 20n + t(9n-9)\}, \quad t \in \mathbb{Z}.$$

EJERCICIOS 1.6

1. Demuestre que si $ac \equiv bc \mod m$ y $(m, c) = 1$, entonces $a \equiv b \mod m$ (Ley de la cancelación). Muestre también que si $(m, c) > 1$, esta afirmación no se cumple.

2. Sea $m \in \mathbb{N}$ fija, $a, b \in \mathbb{Z}$ tales que

$$\begin{aligned} a &= mq_1 + r_1 \qquad & 0 \leqslant r_1 < m, \\ b &= mq_2 + r_2 \qquad & 0 \leqslant r_2 < m. \end{aligned}$$

Demuestre que $a \equiv b \mod m \iff r_1 = r_2$.

3. Resuelva los siguientes sistemas de dos maneras: sin usar (y usando) el Teorema 1.6.8.

$$a) \begin{cases} x \equiv 5 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 7 \end{cases} \qquad b) \begin{cases} x \equiv 9 \mod 5 \\ x \equiv 1 \mod 11 \\ x \equiv 2 \mod 7. \end{cases}$$

1.7. Los campos $\mathbb{Z}_p$

Usando las propiedades de los primos es fácil ahora probar que si p es un primo $\mathbb{Z}_p$ es un campo. Usamos la notación usada en [9], esto es, $\overline{a}$ denota la clase de equivalencia del entero a en el anillo Z_m.

Lema 1.7.1. *Si p es un primo, entonces $\mathbb{Z}_p$ es un dominio entero.*

Demostración. Si $\overline{a}\,\overline{b} = \overline{0}$ en $\mathbb{Z}_p$, donde $0 < a \leqslant p$ y $0 < b \leqslant p$. Entonces, $ab \equiv 0$ mód p, *i.e.*, $p \mid ab$ y necesariamente

$$p \mid a \quad \text{o} \quad p \mid b,$$

por lo cual $a = p$ o $b = p$, *i.e.*, $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$ y $\mathbb{Z}_p$ es un dominio entero, ya que no hay divisores (no triviales) de $\overline{0}$. □

Teorema 1.7.2. *$\mathbb{Z}_p$ es un campo.*

Demostración. Sea $1 \leqslant k < p$, fijo, considérese la colección $\{\overline{t}\,\overline{k}\}$ en $\mathbb{Z}_p$, donde t toma los valores $1, 2, 3, \ldots, p-1$.

Se afirma que todos estos valores representan números distintos en $\mathbb{Z}_p$, que no son $\overline{0}$. Si

$$\overline{t_1}\,\overline{k} = \overline{t_2}\,\overline{k} \quad \text{en } \mathbb{Z}_p,$$

entonces

$$t_1 k \equiv t_2 k \quad \text{mód } p,$$

y

$$p \mid (t_1 - t_2)k,$$

i.e., $p \mid t_1 - t_2$ (ya que $(k, p) = 1$). Por lo cual $t_1 = t_2$. En particular, la afirmación implica que $\exists\, t$ tal que $\overline{t}\,\overline{k} = \overline{1}$ y por lo tanto todo número tiene un inverso multiplicativo.

□

Capítulo 2

El campo de los números reales

2.1. Los racionales

Se construyen los racionales a partir de los enteros, se define una relación de equivalencia en

$$\mathbb{Z} \times (\mathbb{Z} - \{0\}) = \{ (a,b) \mid a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0 \},$$

$$(a,b) \sim (a',b') \quad \text{si} \quad ab' = ba'. \tag{2.1}$$

Por ejemplo $(4,6) \sim (2,3)$, ya que $4 \cdot 3 = 6 \cdot 2$.

Proposición 2.1.1. *La relación definida por (2.1) es de equivalencia.*

Demostración. Como $ab = ba,\ \sim$ es reflexiva. Como $ab' = ba'$ si y sólo si $a'b = b'a, \sim$ es simétrica. Finalmente, si $(a,b) \sim (a',b')$ y $(a',b') \sim (a'',b'')$, entonces $ab' = ba'$ y $a'b'' = b'a''$, por lo que $ab'b'' = ba'b''$ y $a'b''b = b'a''b,\ i.e.,$

$$ab'b'' = b'a''b,$$

y como $b' \neq 0\ \ ab'' = ba'',\ i.e.,\ (a,b) \sim (a'',b'')$, luego $\sim$ es transitiva. □

Provisionalmente denotaremos por

$$\overline{\left(\frac{a}{b}\right)}$$

a la clase de equivalencia de (a,b), obsérvese que $\overline{(\frac{a}{b})} = \overline{(\frac{a'}{b'})}$ si y sólo si $ab' = ba'$, en particular

$$\overline{\left(\frac{a}{b}\right)} = \overline{\left(\frac{ar}{br}\right)}, \quad \text{para cualquier } r \in \mathbb{Z},\ r \neq 0 \quad (abr = bar).$$

Definición 11. *Al conjunto de clases de equivalencia en* $\mathbb{Z} \times (\mathbb{Z} - \{0\})$,

$$\overline{\left(\frac{a}{b}\right)} = \{\ (x, y) \in \mathbb{Z} \times \mathbb{Z} - \{0\} \mid ay = bx\ \}$$

se les llama números racionales y se les denota por $\mathbb{Q}$.

Para simplificar la notación se escribe $\frac{a}{b}$ por $(\overline{\frac{a}{b}})$, obsérvese que con esta notación un mismo número se puede escribir de distintas maneras

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9}, \text{ etcétera.}$$

El siguiente paso es definir la suma y el producto en $\mathbb{Q}$.

Lema 2.1.2. *Si* $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$, *entonces*

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Demostración. Por hipótesis $ab' = ba'$, $cd' = c'd$. Por lo que usando estas relaciones se tiene

$$\begin{aligned}(ad + bc)(b'd') &= ab'dd' + cd'bb' \\ &= ba'dd' + c'dbb' = bd(a'd' + b'c').\end{aligned}$$

□

Se define la suma de dos racionales como sigue

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

se sigue del Lema 2.1.2 que esta operación está bien definida.

También se define el producto

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

esta operación también está bien definida, ya que si

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{y} \quad \frac{c}{d} = \frac{c'}{d'},$$

como $ab' = a'b$ y $cd' = c'd$, se deduce que

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Nótese que

$\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}$ (ejercicio).

Teorema 2.1.3. *Los racionales son un campo.*

Demostración. Algunas propiedades se siguen fácilmente

$$\begin{aligned} \frac{a}{b}+\frac{0}{1} &= \frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b}, \\ \frac{a}{b}+\frac{-a}{b} &= \frac{ab-ab}{b^2} = \frac{0}{b^2} \quad \left(\text{obsérvese que} \quad \forall\, b\neq 0 \quad \frac{0}{b}=\frac{0}{1}\right), \\ \frac{a}{b}+\frac{c}{d} &= \frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}, \end{aligned}$$

si $\frac{a}{b}$ es distinto de $\frac{0}{b}$, *i.e.*, $a\neq 0$,

$$\frac{a}{b}\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1},$$

al racional $\frac{b}{a}$ se le denota por $(\frac{a}{b})^{-1}$ y se le llama el inverso multiplicativo de $\frac{a}{b}$.

La asociatividad y la conmutatividad del producto son triviales. La asociatividad de la suma y la distributividad se prueban también fácilmente (ejercicio). □

Ahora estudiaremos el orden en $\mathbb{Q}$. Caracterizamos primero a los racionales positivos.

Lema 2.1.4. *Si* $\frac{a}{b}=\frac{a'}{b'}$, *entonces*

$$ab\in\mathbb{N}\Longleftrightarrow a'b'\in\mathbb{N}.$$

Demostración. Se tiene $ab'=ba'$, y por lo tanto $ab'bb'=ba'bb'$, *i.e.*, $ab(b')^2=a'b'b^2$, y por lo tanto

$$ab\in\mathbb{N} \;\Leftrightarrow\; ab(b')^2\in\mathbb{N} \;\Leftrightarrow\; a'b'b^2\in\mathbb{N} \;\Leftrightarrow\; a'b'\in\mathbb{N},$$

puesto que $tm^2\in\mathbb{N} \;\Rightarrow\; t\in\mathbb{N}$ (si $t\notin\mathbb{N}$ y $t\neq 0$, $-t\in\mathbb{N}$, por lo que $-tm^2\in\mathbb{N}$, lo cual contradice $tm^2\in\mathbb{N}$). □

Definición 12. *Los racionales positivos denotados por* $\mathbb{Q}^+$ *son aquellos de la forma* $\frac{a}{b}$, *donde* $ab\in\mathbb{N}$.

El lema anterior muestra que esta definición es correcta ya que no depende del representante. Denotaremos al racional $\frac{-a}{b}$ como $-\frac{a}{b}$, obsérvese que $\frac{-a}{b}=\frac{a}{-b}$.

Proposición 2.1.5 (Tricotomía)**.** $\forall\ \frac{a}{b} \in \mathbb{Q}$ *se cumple una y sólo una de las siguientes afirmaciones:*

i) $\frac{a}{b} \in \mathbb{Q}^+$,

ii) $\frac{a}{b} = \frac{0}{1}$,

iii) $-\frac{a}{b} \in \mathbb{Q}^+$.

Demostración. Si $ab \notin \mathbb{N},\ ab = 0$ o $-(ab) \in \mathbb{N}$, en el primer caso $a = 0$ y se cumple *ii*), en el segundo $(-a)b \in \mathbb{N}$ y $-\frac{a}{b} \in \mathbb{Q}^+$. □

Proposición 2.1.6. *Sumas y productos de racionales positivos son positivos.*

Demostración. Obsérvese que si $\frac{a}{b} \in \mathbb{Q}^+$, entonces $a, b \in \mathbb{N}$ o $-a, -b \in \mathbb{N}$, ya que si por ejemplo $a > 0$ y $b < 0$, entonces $ab < 0$. Por lo tanto podemos suponer $a, b > 0$, si $a, b < 0$ podemos reemplazar $\frac{a}{b}$ por $\frac{-a}{-b}$.

Bajo estas hipótesis como

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{y} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd},$$

y se puede suponer $a, b, c, d \in \mathbb{N}$, el resultado se sigue de manera inmediata de los axiomas de los naturales. □

Podemos definir ahora un orden en $\mathbb{Q}$.

Definición 13. *Sean* $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$*, se dice que* $\frac{a}{b}$ *es mayor que* $\frac{c}{d}$*, se escribe*

$$\frac{a}{b} > \frac{c}{d},$$

si $\frac{a}{b} + (-\frac{c}{d}) \in \mathbb{Q}^+$.

Obsérvese que $\frac{a}{b} \in \mathbb{Q}^+ \Leftrightarrow \frac{a}{b} > \frac{0}{1}$, esto se sigue ya que $\frac{a}{b} + \frac{-0}{1} = \frac{a \cdot 1 - 0 \cdot b}{b \cdot 1} = \frac{a}{b}$.

Proposición 2.1.7 (Tricotomía)**.** *Dados* $\frac{a}{b}$ *y* $\frac{c}{d} \in \mathbb{Q}$ *se cumple una y sólo una de las siguientes afirmaciones:*

i) $\frac{a}{b} > \frac{c}{d}$,

ii) $\frac{a}{b} = \frac{c}{d}$,

iii) $\frac{a}{b} < \frac{c}{d}$.

Demostración. Se sigue de la Proposición 2.1.5 que

$$\frac{a}{b}+\left(-\frac{c}{d}\right)\in\mathbb{Q}^+ \qquad \text{o} \qquad \frac{a}{b}+\left(-\frac{c}{d}\right)=\frac{0}{1}$$

$$\text{o} \quad -\left(\frac{a}{b}+\left(-\frac{c}{d}\right)\right)\in\mathbb{Q}^+.$$

Evidentemente las primeras 2 condiciones corresponden a *i)* y *ii)*, y como

$$-\left(\frac{a}{b}+\left(-\frac{c}{d}\right)\right)=\frac{-a}{b}+\frac{c}{d}$$

se sigue el resultado. Esto último se sigue ya que en $\mathbb{Q}$ vale la ley de la cancelación de la suma, y el inverso aditivo es único:

Si $\frac{a}{b}+\frac{c}{d}=\frac{a}{b}+\frac{e}{f}$, entonces $\frac{-a}{b}+(\frac{a}{b}+\frac{c}{d})=\frac{-a}{b}+(\frac{a}{b}+\frac{e}{f})$ y $\frac{c}{d}=\frac{e}{f}$ $\therefore$ $\frac{a}{b}+\frac{e}{f}=\frac{a}{b}+(\frac{-a}{b})=0 \Rightarrow \frac{e}{f}=\frac{-a}{b}$. □

Esta relación de orden también es transitiva:

Si $\frac{a}{b}>\frac{c}{d}$ y $\frac{c}{d}>\frac{e}{f}$, entonces $\frac{a}{b}>\frac{e}{f}$:

$$\text{como} \quad \frac{a}{b}-\frac{c}{d}\in\mathbb{Q}^+ \quad \text{y} \quad \frac{c}{d}-\frac{e}{f}\in\mathbb{Q}^+,$$

se tiene

$$\frac{a}{b}-\frac{e}{f}\in\mathbb{Q}^+.$$

Proposición 2.1.8.

i) *Si* $\frac{a}{b}>\frac{a'}{b'}$ *y* $\frac{c}{d}>\frac{c'}{d'}$, *entonces*

$$\frac{a}{b}+\frac{c}{d}>\frac{a'}{b'}+\frac{c'}{d'}.$$

ii) *Si* $\frac{a}{b}>\frac{a'}{b'}$, *entonces*

$$\frac{a}{b}+\frac{c}{d}>\frac{a'}{b'}+\frac{c}{d}.$$

iii) *Si* $\frac{a}{b}>\frac{a'}{b'}$ *y* $\frac{c}{d}>\frac{0}{1}$, *entonces*

$$\frac{ac}{bd}>\frac{a'c}{b'd}.$$

Demostración. La propiedad $i)$ se sigue directamente de la Proposición 2.1.6 y la $ii)$ se prueba de manera inmediata. Para probar $iii)$, se tiene

$$\frac{a}{b} - \frac{a'}{b'} \in \mathbb{Q}^+ \quad \text{y} \quad \frac{c}{d} \in \mathbb{Q}^+,$$

por lo que

$$\left(\frac{a}{b} - \frac{a'}{b'}\right)\frac{c}{d} \in \mathbb{Q}^+, \quad i.e.$$

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) > \left(\frac{a'}{b'}\right)\left(\frac{c}{d}\right).$$

□

Obsérvese que $\frac{a}{b} > \frac{c}{d} \Leftrightarrow -\frac{c}{d} > -\frac{a}{b}$, esto se sigue ya que $\frac{a}{b} - \frac{c}{d} \in \mathbb{Q}^+ \Leftrightarrow -\frac{c}{d} - (-\frac{a}{b}) \in \mathbb{Q}^+ \quad (-(\frac{-a}{b}) = \frac{-(-a)}{b} = \frac{a}{b})$.

Observamos ahora que los enteros están naturalmente incluidos en los racionales, para eso se define

$$i : \mathbb{Z} \longrightarrow \mathbb{Q} \quad \text{como} \quad i(a) = \frac{a}{1}.$$

Claramente i es inyectiva, ya que si $i(a) = i(b)$, se tiene

$$\frac{a}{1} = \frac{b}{1} \Leftrightarrow a = b.$$

Se conviene en denotar a la imagen de $i(\mathbb{Z})$ simplemente por $\mathbb{Z}$, y al racional $i(a) = \frac{a}{1}$ simplemente por a.

La inclusión i también preserva las operaciones de suma y producto:

$$i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = i(a+b),$$
$$i(a)i(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = i(ab).$$

Para probar las propiedades de los números reales es útil considerar el siguiente subconjunto de los racionales.

Definición 14. *Sea D el subconjunto de $\mathbb{Q}$, definido por los números de la forma*

$$\frac{a}{10^n}, \quad a \in \mathbb{Z}.$$

La representación decimal de $\frac{a}{10^n}$, se puede expresar escribiendo a con un punto a n lugares del extremo derecho, por ejemplo

$$\frac{325}{10^2} = \frac{325}{100} = 3.25,$$

$$\frac{4}{10^4} = \frac{4}{10000} = .0004,$$

también se denota $\frac{1}{10^n}$ por 10^{-n}.

No todos los racionales están en D, por ejemplo $\frac{1}{3} = .333\ldots$ (este hecho se mostrará de manera formal posteriormente).

Sin embargo, sumas finitas y productos finitos de números de D son números en D :

$$\frac{a}{10^n} + \frac{b}{10^m} = \frac{a \cdot 10^m + b \cdot 10^n}{10^n \cdot 10^m} = \frac{a \cdot 10^m + b \cdot 10^n}{10^{m+n}} \in D,$$

$$\frac{a}{10^n} \cdot \frac{b}{10^m} = \frac{ab}{10^{m+n}} \in D.$$

En expresión decimal los elementos de $D^+ = D \cap \mathbb{Q}^+$ se representan como

$$A.a_1a_2\ldots a_n,$$

donde $A \in \mathbb{N} \cup \{0\}$ y a_i son dígitos, es decir, elementos del conjunto $\{0, 1, \ldots, 9\}$ (n tan grande como se quiera). Los de $D^- = D \cap \mathbb{Q}^-$ como

$$-A.a_1a_2\ldots a_n,$$

por ejemplo, $\frac{-325}{100}$ se puede escribir como - 3.25 o -3.250.

Proposición 2.1.9. *Si $x, y \in D^+$,*

$$x = A.a_1a_2\ldots a_n, \qquad y = B.b_1b_2\ldots b_n,$$

entonces $x > y$, si se cumple una de las 2 siguientes condiciones:

a) $A > B$,

b) $A = B$, $a_i = b_i$ *si* $i < k$ *y* $a_k > b_k$.

Demostración.

$$x = \frac{Aa_1a_2\ldots a_n}{10^n} \qquad y = \frac{Bb_1b_2\ldots b_n}{10^n},$$

$$\begin{aligned} x > y \quad &\Leftrightarrow \quad \frac{Aa_1a_2\ldots a_n}{10^n} - \frac{Bb_1b_2\ldots b_n}{10^n} \ \in \ \mathbb{Q}^+ \\ &\Leftrightarrow \quad \frac{Aa_1a_2\ldots a_n - Bb_1b_2\ldots b_n}{10^n} \ \in \ \mathbb{Q}^+ \\ &\Leftrightarrow \quad Aa_1a_2\ldots a_n > Bb_1b_2\ldots b_n, \end{aligned}$$

y esta condición se cumple si a) o b) se cumplen. □

Obsérvese que las reglas de los signos son válidas en $\mathbb{Q}$, por ejemplo

$$\left(\frac{a}{b}\right)\left(\frac{-c}{d}\right) = \frac{a(-c)}{bd} = \frac{(-a)c}{bd} = \left(\frac{-a}{b}\right)\left(\frac{c}{d}\right) = -\left(\frac{a}{b}\right)\left(\frac{c}{d}\right), \quad \text{etcétera.}$$

Usando la expresión decimal en D esto se escribe, por ejemplo,

$$(-A.a_1a_2\ldots a_n)(-B.b_1b_2\ldots b_n) = (A.a_1a_2\ldots a_n)(B.b_1b_2\ldots b_n).$$

EJERCICIOS 2.1

1. Demuestre que
$$\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}.$$

2. Demuestre la asociatividad de la suma y la distributividad de los números racionales.

3. Pruebe que si
$$\frac{a}{b} > \frac{a'}{b'} \geqslant \frac{0}{1} \qquad \text{y} \qquad \frac{c}{d} > \frac{c'}{d'} \geqslant \frac{0}{1},$$
entonces
$$\frac{a}{b}\frac{c}{d} > \frac{a'}{b'}\frac{c'}{d'}.$$

2.2. Los números reales

Definición 15. *Los números reales no negativos son expresiones decimales infinitas de la forma*

$$A.a_1a_2a_3\ldots,$$

donde $A \in \mathbb{N} \cup \{0\}$ *y* $a_j \in \{0, 1, \ldots, 9\}$, *los puntos suspensivos indican que hay un número infinito de* a_j, *y se cumple que* $\forall\ n \in \mathbb{N}$, $\exists\ m > n$ *tal que* $a_m \neq 9$ *(es decir no hay colas infinitas de nueves).*

Excluyendo el $0.000\ldots$ se obtiene los reales positivos denotados por $\mathbb{R}^+$, los reales negativos son los reales positivos con un signo - antepuesto y se denotan por $\mathbb{R}^-$.

Definición 16. *Los números reales consisten en los números del conjunto*

$$\mathbb{R}^+ \cup \mathbb{R}^- \cup \{0\}.$$

Obsérvese que D se puede identificar con los reales con una cola infinita de ceros, por ejemplo,

$$\frac{325}{100} = 3.25000\ldots.$$

Nótese también que $\mathbb{Z} \subset D \subset \mathbb{R}$.

Definición 17. *Un orden en un conjunto S es una relación en S, denotada por $>$, que cumple las siguientes 2 condiciones:*

a) $\forall\ r, s, t \in S$ *tales que* $r > s$ *y* $s > t$ *se tiene* $r > t$ *(transitividad),*

b) $\forall\ r, s \in S$ *se cumple una y sólo una de las siguientes afirmaciones:*

$$r < s, \quad r = s \quad o \quad r > s \quad \textit{(tricotomía).}$$

Se extiende el orden en D a un orden en $\mathbb{R}$ de la siguiente manera:

1) $0 > x \qquad \forall\ x \in \mathbb{R}^-$.

2) $x > y \qquad \forall\ x \in \mathbb{R}^+, \forall\ y \in \mathbb{R}^-$.

3) $x > 0 \qquad \forall\ x \in \mathbb{R}^+$.

4) Dados 2 reales positivos

$$x = A.a_1a_2a_3\cdots,$$

$$y = B.b_1b_2b_3\cdots,$$

$x > y$ si se cumple alguna de las siguientes condiciones

a) $A > B$,

b) $A = B,\ a_i = b_i\ \ \forall\ i < n$ y $a_n > b_n$.

5) Si $x \in \mathbb{R}^+,\ y \in \mathbb{R}^+$, entonces

$$x > y \iff -y > -x.$$

Proposición 2.2.1. *El orden definido en* $\mathbb{R}$ *es en efecto un orden.*

Demostración. Para la transitividad, se prueba que si $x > y$ y $y > z$, entonces $x > z$. Si $x \in \mathbb{R}^+$ y $z = 0$ o $z \in \mathbb{R}^-$, se sigue de la definición. También, si $x = 0$ y $z \in \mathbb{R}^-$. Por lo que basta probarlo cuando $x, y, z \in \mathbb{R}^+$ o $x, y, z \in \mathbb{R}^-$. En el primer caso, si

$$\begin{aligned} x &= A.a_1a_2\cdots \\ y &= B.b_1b_2\cdots \\ z &= C.c_1c_2\cdots , \end{aligned}$$

se tiene $A \geqslant B \geqslant C$, si $A > C$ se sigue el resultado. Por otra parte, si $A = B = C$, como $x > y$, se tiene que para alguna n, $a_i = b_i \ \forall \ i < n$ y $a_n > b_n$.

En este caso, como $y > z$, sucede que, para alguna $j \leqslant n$,

$$a_j = b_j > c_j \quad \text{y} \quad b_i = c_i \ \ \forall\, i < j, \quad \text{y se obtiene} \quad x > z,$$

o

$$b_j = c_j \quad \forall\, j < n \quad \text{y} \quad a_n > b_n \geqslant c_n, \quad \text{por lo que} \quad x > z.$$

El caso $x, y, z \in \mathbb{R}^-$ se deduce del anterior, si $x < y$, y $y < z$, entonces se tiene $-x > -y$ y $-y > -z$, por lo que $-x > -z$ y $x < z$.

Tricotomía: si x, y no están ambos en $\mathbb{R}^+$ (o en $\mathbb{R}^-$), el resultado se sigue de manera inmediata por 1), 2) y 3). También, si $x, y \in \mathbb{R}^+$, el resultado se sigue de 4) y si $x, y \in \mathbb{R}^-$, éste se sigue de 5). □

Por ejemplo, $0 > -.002$, $1 > .99872$, $-2.3 > -2.8$. Obsérvese que se sigue de la Proposición 2.1.9, que el orden definido en D, como subconjunto de $\mathbb{Q}$, es el mismo que el definido como subconjunto de $\mathbb{R}$.

Los siguientes resultados muestran que el subconjunto D es *denso* en $\mathbb{R}$.

Teorema 2.2.2. $\forall\ \alpha, \beta \in \mathbb{R}$ *tal que* $\alpha < \beta$, *existe* $c \in D$ *tal que* $\alpha < c < \beta$.

Demostración.

Caso 1: $0 \leqslant \alpha < \beta$.

Sean

$$\begin{aligned} \alpha &= A.a_1a_2\cdots , \\ \beta &= B.b_1b_2\cdots . \end{aligned}$$

Si $A < B$, sea a_n tal que $a_n \neq 9$ y $a_n^* = a_n + 1$, tomando

$$c = A.a_1a_2\ldots a_n^*,$$

se tiene

$$\alpha < c < \beta.$$

Si $A = B$, sea n tal que $a_i = b_i$ si $i < n$ y $a_n < b_n$, tomando $m > n$ tal que $a_m \neq 9$, $a_m^* = a_m + 1$ y

$$c = A.a_1a_2 \cdots a_{m-1}a_m^*,$$

se tiene $c \in D$ y $\alpha < c < \beta$.

Caso 2: $\alpha < \beta \leqslant 0$.
Entonces $-\alpha > -\beta \geqslant 0$ y existe $c \in D$ tal que $-\alpha > c > -\beta$

$$\therefore \quad \alpha < -c < \beta.$$

Caso 3: $\alpha < 0 < \beta$.
Tomando $c = 0$ se sigue el resultado. □

Teorema 2.2.3. $\forall\ \alpha \in \mathbb{R}$ *y* $\forall\ n \in \mathbb{N}$, *existe* $a \in D$ *tal que* $a < \alpha < a + 10^{-n}$, *si* $\alpha > 0$ *se puede tomar* $a > 0$.

Demostración.

Caso 1: $\alpha \notin D$.
Si $\alpha > 0,\ \alpha = A.a_1a_2 \cdots$, tomando $a = A.a_1a_2 \cdots a_n$, se tiene

$$a < \alpha < a + 10^{-n} = \frac{Aa_1a_2 \cdots a_n}{10^n} + \frac{1}{10^n},$$

la primera desigualdad se sigue ya que existe $a_m \neq 0, m > n$ (puesto que $\alpha \notin D$), la 2a desigualdad se sigue ya que la expansión decimal de $a + 10^{-n}$ es *mayor* que la de

$$A.a_1a_2 \cdots a_n \text{ (se le está sumando 1 en el lugar } n\text{-ésimo).}$$

Si $\alpha < 0,\ \alpha = -A.a_1a_2 \cdots$, tomando $a = A.a_1a_2 \cdots a_n$,

$$a < -\alpha < a + 10^{-n},$$

como en el caso positivo, y se tiene

$$-(a + 10^{-n}) < \alpha < -a = -(a + 10^{-n}) + 10^{-n}.$$

Caso 2: $\alpha \in D$.
Se prueba primero $\alpha > 0$. El método anterior no funciona, por ejemplo, si $n = 1$ y $\alpha = .4$, $.4 < .4 + .1$, pero $.4$ no es menor que $.4$. Sin embargo, $.39 < .4 < .39 + .1 = .49$ lo cumple.

Para probar este caso, se toma $a = \alpha - 10^{-(n+k)} \in D$ tal que $a > 0,\ k \geqslant 1$ (esto se puede hacer, ya que $\alpha > 10^{-t}$ para t suficientemente grande). Por lo cual

$$a = \alpha - 10^{-(n+k)} < \alpha < \alpha + 10^{-(n+k)} = a + 2 \cdot 10^{-(n+k)} < a + 10^{-n},$$

puesto que $\frac{2}{10^k} < 1$.

El caso $\alpha < 0$ se sigue como en el Caso 1. Finalmente, si $\alpha = 0$, tomando $a = -10^{-(n+1)}$, se tiene $-10^{-(n+1)} < 0 < -10^{-(n+1)} + 10^{-n}$, ya que $10^{-(n+1)} < 10^{-n}$. □

EJERCICIO 2.2

1. Pruebe este último resultado (Teorema 2.2.3), usando el Teorema 2.2.2. Esta otra prueba es más breve, sin embargo la presentada en este texto es útil para entender la demostración del Lema 2.4.1.

2.3. El supremo y el ínfimo

Definición 18. *Sea $S \subset \mathbb{R}$, se dice que $\alpha \in \mathbb{R}$ es una cota superior (o inferior) de S si $\alpha \geqslant x$ (o $\alpha \leqslant x$) $\forall\ x \in S$.*

Definición 19. *Sea $S \subset \mathbb{R}$, se dice que S está acotado superiormente (o inferiormente) si existe alguna $\alpha \in \mathbb{R}$ tal que α es cota superior (o inferior).*

Definición 20. *Sea $S \subset \mathbb{R}$, se dice que α es el supremo de S si*

i) *α es cota superior de S,*

ii) *si β es cota superior de S, entonces $\alpha \leqslant \beta$, se escribe* $\sup S = \alpha$.

Nótese que el supremo es la menor de las cotas superiores. Además el supremo es único (ejercicio).

Definición 21. *Sea $S \subseteq \mathbb{R}$, se dice que α es el ínfimo de S si*

i) $\alpha \leqslant x,\ \forall\ x \in S$,

ii) *dada β cota inferior de S, $\beta \leqslant \alpha$.*

Se escribe $\inf S$, para denotar el ínfimo de S, y este número es la mayor de las cotas inferiores. También el ínfimo es único (ejercicio).

Teorema 2.3.1. *Sea $S \subseteq \mathbb{R}$ acotado superiormente (o inferiormente), entonces S tiene un supremo (o un ínfimo).*

Demostración. Se prueban distintos casos

Caso 1: Si $S \cap \mathbb{R}^+ \neq \emptyset$ y S está acotado superiormente, entonces S tiene un supremo.

Prueba. Sea C el conjunto de todas las cotas superiores de S, obsérvese que $C \neq \emptyset$ y $C \subseteq \mathbb{R}^+$. Sea

$$C_0 = \{m \in \mathbb{N} \cup \{0\} \mid m \text{ es la parte entera de algún elemento de } C\},$$

y sea A el menor elemento de C_0. Se define también

$$C_1 = \{t \in \{0, 1, \ldots, 9\} \mid A.tx_2x_3 \cdots \in C\},$$

y sea a_1 el menor de los elementos de C_1. Iterando este proceso se define

$$C_2 = \{t \in \{0, 1, \ldots, 9\} \mid A.a_1tx_3x_4 \cdots \in C\},$$

y a_2 el menor elemento de C_2, posteriormente se define C_3, y se sigue de manera inductiva.

Se afirma que

$$\alpha = A.a_1a_2a_3 \cdots$$

es el supremo de S:

i) α no tiene colas de nueves: si $a_n = 9$, existe $\gamma \in C$

$$\gamma = A.a_1a_2 \cdots a_nx_{n+1}x_{n+2} \cdots x_{n+r} \cdots$$

tal que $x_{n+r} \neq 9$ ($\gamma \in \mathbb{R}$), y necesariamente existe $m > n,\ m \leqslant n + r$, tal que $a_m < 9$:

Si $a_{n+1}, a_{n+2}, \cdots, a_{n+r-1} = 9$, entonces

$$x_{n+1}, x_{n+2}, \cdots, x_{n+r-1} = 9 \quad \text{y} \quad a_{n+r} \leqslant x_{n+r} < 9.$$

ii) α es cota superior de S : se prueba que dada $\beta \in S,\ \alpha \geqslant \beta$. Sea

$$\beta = B.b_1b_2 \cdots,$$

como existe $A.x_1x_2 \cdots \in C,\ A \geqslant B$. Si $A > B$, se tiene $\alpha > \beta$. En el caso $A = B$, como existe $A.a_1x_2 \cdots \in C,\ a_1 \geqslant b_1$, si $a_1 > b_1,\ \alpha > \beta$. Si $a_1 = b_1$, se toma $A.a_1a_2x_3 \cdots \in C$ y $a_2 \geqslant b_2$, etcétera. En consecuencia existe n tal que $a_n > b_n$ y $\alpha > \beta$ o $\forall\ n\ a_n = b_n$ y $\alpha = \beta$.

iii) α es la menor de las cotas superiores: sea β otra cota superior,

$$\beta = B.b_1b_2 \cdots,$$

$A \leqslant B$ por construcción, si $A < B$ ya está, si $A = B,\ a_1 \leqslant b_1$ (por construcción), si $a_1 < b_1$ terminamos, si $a_1 = b_1,\ a_2 \leqslant b_2$, etcétera.

Caso 2: Se prueba que si $S \subseteq \mathbb{R}^+,\ S \neq \emptyset,\ S$ tiene un ínfimo.
Prueba. Sea

$$C_0 = \{B \in \mathbb{N} \cup \{0\} \mid B.x_1x_2\cdots \in S\},$$

y $A = \min C_0$. Se define también

$$C_1 = \{t \in \{0,1,\ldots,9\} \mid A.tx_2x_3\cdots \in S\},$$

y $a_1 = \min C_1$. El siguiente paso es tomar

$$C_2 = \{t \in \{0,1,\ldots,9\} \mid A.a_1tx_3x_4\cdots \in S\},$$

y $a_2 = \min C_2$, etcétera.

Se afirma que $\alpha = A.a_1a_2a_3\cdots = \inf S$. La prueba es análoga al Caso 1.

i) No hay colas de nueves: dada n, sea $\gamma \in S$,

$$\gamma = A.a_1a_2\cdots a_nx_{n+1}x_{n+2}\cdots x_{n+r}\cdots,$$

$x_{n+r} < 9$. Si $a_{n+1}, a_{n+2}, \ldots, a_{n+r-1} = 9$, entonces $x_{n+1}, \ldots, x_{n+r-1} = 9$, y $a_{n+r} < 9$.

ii) α es cota inferior: si

$$\beta = B.b_1b_2\cdots \in S,$$

$A \leqslant B$ por definición, si $A < B$ acabamos. Si $A = B,\ a_1 \leqslant b_1$, si $a_1 < b_1$ ya está, si $a_1 = b_1,\ a_2 \leqslant b_2$, etcétera.

iii) α es la mayor de las cotas inferiores: sea $\beta = B.b_1b_2\cdots$ otra cota inferior. Como existe $A.x_1x_2\cdots \in S,\ B \leqslant A$, si $B < A$ ya está. Si $A = B$, como existe $A.a_1x_2\cdots \in S,\ b_1 \leqslant a_1$, etcétera.

Caso 3: Todo subconjunto no vacío S de $\mathbb{R},\ S \neq \emptyset$ y acotado superiormente tiene supremo.
Prueba. Si $S \cap \mathbb{R}^+ \neq \emptyset$ es el Caso 1. Si $S \cap \mathbb{R}^+ = \emptyset$, pero $0 \in S$, entonces $0{=}\sup S$: $x \leqslant 0, \forall\ x \in S$ y si $y < 0,\ y$ no es cota superior. Finalmente, si $S \cap \mathbb{R}^+ = \emptyset$ y $0 \notin S$, entonces $S \subset \mathbb{R}^-$. Sea S' el reflejado de S, es decir,

$$S' = \{x \in \mathbb{R} \mid\ -x \in S\}.$$

Por lo cual $S' \subset \mathbb{R}^+$ y por el Caso 2 existe $\alpha = \inf S'$, se afirma que

$$-\alpha = \sup\ S.$$

Esto se sigue, ya que si $x \in S$,

$$-x \in S' \quad \text{y} \quad \alpha \leqslant -x.$$

Por lo tanto, $-\alpha \geqslant x$ y $-\alpha$ es cota superior de S. También si y es cota superior de S, $-y$ es cota inferior de S' ($y \geqslant x \ \forall\ x \in S,\ -y \leqslant -x \ \ \forall -x \in S'$).

$$\therefore \quad -y \leqslant \alpha \quad \text{y} \quad y \geqslant -\alpha.$$

Caso 4: Si $S \subset \mathbb{R},\ S \neq \emptyset,\ S$ acotado inferiormente, entonces existe $\inf S$. Prueba. Sea

$$S' = \{x \in \mathbb{R} \mid -x \in S\}$$

el reflejado de S, se tiene que S' esta acotado superiormente y como en el Caso 3, si $\alpha = \sup S'$,

$$-\alpha = \inf S.$$

□

EJERCICIOS 2.3

1. Pruebe que el supremo y el ínfimo son únicos.

2.4. Los reales son un campo

Los algoritmos de la primaria, que se derivan de nuestras definiciones y la ley distributiva, permiten sumar y multiplicar números en D (ejercicio).

$$\begin{array}{r} 4.07 \\ +\ .02 \\ \hline 4.09 \end{array} \qquad\qquad \begin{array}{r} 3.14 \\ \times\ .19 \\ \hline 2826 \\ 314 \\ \hline .5966 \end{array}$$

Sin embargo esto no se aplica a los reales con expansiones infinitas de dígitos distintos de cero. Para definir estas operaciones aproximamos los reales por números en D.

Definición 22. *Sean* $\alpha, \beta \in \mathbb{R}$,

$$\begin{aligned} U &= \{x \in D \mid x \leqslant \alpha\}, \\ V &= \{y \in D \mid y \leqslant \beta\}, \\ y \quad C &= \{x + y \mid x \in U,\ y \in V\}, \end{aligned}$$

se define $\alpha + \beta = \sup C$.

Hay que probar que C está acotado superiormente tomando $a \in D$ tal que $a > \alpha$ y $b \in D$ que cumpla $b > \beta$ (si $\alpha = A.a_1a_2\cdots$, se puede tomar $a = A{+}1$, si $\alpha \in \mathbb{R}^-$, $a = 0$ etcétera). Se tiene $x < a \,\forall\, x \in U$ y $y < b \,\forall\, y \in V$,

$$\therefore \quad x + y < a + b,$$

y $a + b$ es una cota superior de C.

Definición 23. *Sean* $\alpha, \beta \in \mathbb{R}^+$,

$$\begin{aligned} A &= \{x \in D \mid 0 \leqslant x \leqslant \alpha\}, \\ V &= \{y \in D \mid 0 \leqslant y \leqslant \beta\}, \\ y \quad P &= \{xy \mid x \in A,\ y \in V\}, \end{aligned}$$

se define $\alpha\beta = \sup P$.

De nuevo P está acotado superiormente, ya que si $\alpha < a,\ \beta < b$, se tiene $\forall\, x \in A\ x < a$ y $\forall\, y \in B\ y < b$, por lo que $xy < ab$.

El producto de dos reales arbitrarios se define usando la regla de los signos, si $\alpha, \beta \in \mathbb{R}^+$,

$$\begin{aligned} (-\alpha)(\beta) &= \alpha(-\beta) = -(\alpha\beta) \\ (-\alpha)(-\beta) &= \alpha\beta \\ 0 \cdot \alpha &= 0(-\alpha) = -\alpha \cdot 0 = \alpha \cdot 0 = 0 \cdot 0 = 0. \end{aligned}$$

Obsérvese que estas definiciones extienden la suma y el producto en D. Si $\alpha, \beta \in D$, $\sup C = \alpha + \beta$, ya que evidentemente $\alpha + \beta$ es una cota superior de C y también es la menor ya que $\alpha + \beta \in C$. (La misma situación se cumple para el producto.)

Lema 2.4.1. *Sea* $\alpha \in \mathbb{R}$ *tal que*

$$-10^{-n} < \alpha < 10^{-n} \quad \forall\, n \geqslant 0,$$

entonces $\alpha = 0$.

Demostración. Si α es un real no negativo, sea $\alpha = A.a_1a_2\cdots$. Como $\forall\, n$

$$A.a_1a_2\cdots < .\underbrace{00\ldots1}_{n\ lugares}0\cdots$$

$A = 0$ y $a_i = 0\ \forall\, i$.

Por otra parte si $\alpha \in \mathbb{R}^-$, $\alpha = -A.a_1a_2\cdots$,

$$-10^{-0} = -1 < \alpha \quad \text{y} \quad -1 < A,$$

y $A = 0$, también $-.1 < \alpha \ \therefore\ -1 < a_1$, por lo que $a_1 = 0$, etcétera. Es decir α no puede ser un real negativo. □

Teorema 2.4.2. *Sean $\alpha, \beta, \alpha', \beta' \in \mathbb{R}$, entonces*

i) si $\alpha' < \alpha, \beta' < \beta$, se tiene $\alpha' + \beta' < \alpha + \beta$,

ii) si $\alpha' < \alpha$, se tiene $\alpha' + \beta < \alpha + \beta$,

iii) si $\alpha > \alpha'$ y $\beta > 0$, se tiene $\alpha\beta > \alpha'\beta$.

Demostración. *i*) Sean

$$\begin{aligned} A &= \{x \in D \mid x \leqslant \alpha\}, \\ B &= \{x \in D \mid x \leqslant \beta\}, \\ A' &= \{x \in D \mid x \leqslant \alpha'\}, \\ B' &= \{x \in D \mid x \leqslant \beta'\}, \\ W &= \{x + y \mid x \in A,\ y \in B\}, \\ W' &= \{x + y \mid x \in A',\ y \in B'\}, \end{aligned}$$

por lo que $\alpha + \beta = \sup W$, $\alpha' + \beta' = \sup W'$.

Tomando $c_1 \in D$ tal que $\alpha' < c_1 < \alpha$ y c_1' tal que $\alpha' < c_1' < c_1$. Asi como $c_2, c_2' \in D$ tales que $\beta' < c_2' < c_2 < \beta$. Se tiene entonces que $x \leqslant c_1'$, $\forall\ x \in A'$ y $y \leqslant c_2'$ $\forall\ y \in B'$. Por consiguiente

$$x + y \leqslant c_1' + c_2' \quad \forall\ x \in A',\ y \in B' \quad \text{y}$$

$$\alpha' + \beta' = \sup W' \leqslant c_1' + c_2' < c_1 + c_2 \leqslant \sup W = \alpha + \beta.$$

ii) La demostración en este caso requiere más cuidado que el anterior ya que podemos intercalar c, c' entre α y α' como en *i*),

$$\alpha' < c' < c < \alpha,$$

pero ahora sólo hay una β (Figura 2.1). Se debe elegir $b \in D,\ 0 < b < \beta$, en función de c y c'.

Existe $n \in \mathbb{N}$ tal que $c - c' > \frac{1}{10^n}$ (por el Lema 2.4.1), y también $b \in D$ tal que

$$b < \beta < b + 10^{-n} \quad \text{(Teorema 2.2.3).}$$

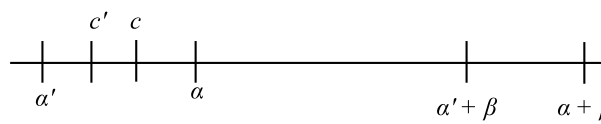


Figura 2.1: Demostración de *ii*)

$$\therefore \quad \alpha + \beta \geqslant b + c = b + c' + (c - c') > b + c' + 10^{-n} \geqslant \alpha' + \beta.$$

La 1a desigualdad es por definición, la 2a es la misma desigualdad en D, ya demostrada para $\mathbb{Q}$, y la última se sigue de la definición de supremo.

Obsérvese que tomar solamente $c \in D,\ \alpha' < c < \alpha$ y $b < \beta$ no necesariamente funciona: $\alpha + \beta \geqslant c + b$, pero $c + b$ no necesariamente es mayor que $\alpha' + \beta$.

iii) (Este caso es aún más complejo) Consideremos primero el caso $\alpha' > 0$, como en los casos anteriores se toman $c, c' \in D$ tales que $\alpha > c > c' > \alpha'$ y $m \in \mathbb{N}$ tal que $c - c' > 10^{-m}$.

Usando el Teorema 2.2.3 $\forall\ n \in \mathbb{N},\ \exists\ b_n \in D^+$ tal que $b_n < \beta < b_n + 10^{-n}$, obsérvese que los b_n se pueden tomar crecientes, ya que si $\beta \notin D,\ b_n$ consiste de cortar la expansión de β en el $n-$ésimo decimal, y si $\beta \in D,\ b_n$ consiste de restar a β términos de la forma 10^{-k}, y estas potencias de 10^{-1} se pueden ir tomando cada vez más pequeñas.

Se sigue de la definición y de la misma propiedad en $\mathbb{Q}$ (Proposición 2.1.8) que $\forall\ n$,

$$\alpha\beta \geqslant cb_n > (c' + 10^{-m})b_n,$$

y que

$$c'(b_n + 10^{-n}) \geqslant \alpha'\beta,$$

por lo que basta probar que para n adecuada

$$(c' + 10^{-m})b_n > c'(b_n + 10^{-n}).$$

Como estos números están en D, basta probar

$$10^{-m}b_n > c'10^{-n}.$$

Fijando una k y su respectiva b_k, se tiene $10^{-m}b_n > 10^{-m}b_k\ \forall\ n \geqslant k$, por lo que basta probar $10^{-m}b_k > c'10^{-n}$. Esto sucede si n es suficientemente grande, ya que entonces $\frac{c'}{10^n}$ es tan pequeño como se quiera, *i.e.*, menor a cualquier cantidad positiva.

Los demás casos se siguen fácilmente: si $\alpha' = 0,\ \alpha\beta > 0 = \alpha'\beta$. Si $\alpha' < 0$ y $\alpha > 0\ \alpha'\beta < 0$ y $\alpha\beta > 0$ (Reglas de los signos). Para $\alpha' < 0$ y $\alpha = 0,\ \alpha'\beta < 0 = \alpha\beta$. Finalmente, si $\alpha' < 0$ y $\alpha < 0,\ -\alpha' > -\alpha > 0$, $\therefore\ -\alpha'\beta > -\alpha\beta$ y $\alpha'\beta < \alpha\beta$. □

Obsérvese que el Teorema 2.4.2, inciso *iii*) implica que si $\alpha > \alpha' \geqslant 0$ y $\beta > \beta' \geqslant 0$, entonces

$$\alpha\beta > \alpha'\beta',$$

ya que $\alpha\beta > \alpha'\beta > \alpha'\beta'$.

Probamos ahora que los reales son un campo, obsérvese que la definición de suma y producto de reales implica de manera inmediata que éstas operaciones son conmutativas, por ejemplo,

$$\begin{aligned} \alpha+\beta &= \sup W = \beta+\alpha, \\ W &= \{x+y \mid x \leqslant \alpha,\ y \leqslant \beta,\ x,y \in D\} \\ &= \{y+x \mid x \leqslant \alpha,\ y \leqslant \beta,\ x,y \in D\}. \end{aligned}$$

Nótese que $\forall\ \alpha,\beta \in \mathbb{R}$ se tiene que $\alpha < \beta \iff -\beta < -\alpha$: si $\alpha,\beta \in \mathbb{R}^+$, esto se sigue de la definición, también si $\alpha,\beta \in \mathbb{R}^-$. Los otros casos son triviales.

Lema 2.4.3. $A.a_1a_2\cdots + (-A.a_1a_2\cdots) = 0.$

Demostración. $\forall\ n\ \exists\ b_n \in D$ tal que

$$b_n < A.a_1a_2\cdots < b_n + 10^{-n},$$

lo cual implica que también se tiene

$$-(b_n + 10^{-n}) < -A.a_1a_2\cdots < -b_n.$$

Usando el Teorema 2.4.2, podemos sumar las desigualdades y tenemos

$$-10^{-n} < A.a_1a_2\cdots + (-A.a_1a_2\cdots) < 10^{-n},$$

$$\therefore \quad A.a_1a_2\cdots + (-A.a_1a_2\cdots) = 0.$$

□

Lema 2.4.4. $\forall\ \alpha \in \mathbb{R}$,

$$\alpha + 0 = \alpha.$$

Demostración. Para cualquier natural $n\ \exists\ a_n \in D$ tal que

$$a_n < \ \alpha\ < a_n + 10^{-n}.$$

También usando el Teorema 2.4.2

$$a_n < \alpha + 0 < a_n + 10^{-n}$$

y por lo tanto

$$-(a_n + 10^{-n}) < -(\alpha + 0) < -a_n.$$

Finalmente, sumando se obtiene $-10^{-n} < \alpha - (\alpha + 0) < 10^{-n}$ y

$$\alpha = \alpha + 0.$$

□

Corolario 2.4.5. *Si* $\alpha, \beta \in \mathbb{R}$, *entonces*

$$\alpha > \beta \Longleftrightarrow \alpha + (-\beta) \in \mathbb{R}^+.$$

Demostración.

$$\alpha > \beta \Leftrightarrow \alpha + (-\beta) > \beta + (-\beta) = 0, \ i.e., \ \ \alpha + (-\beta) \in \mathbb{R}^+.$$

□

Lema 2.4.6. *La suma de reales es asociativa.*

Demostración. Dados $\alpha, \beta, \gamma \in \mathbb{R}$, $n \in \mathbb{N}$, existen $a_n, b_n, c_n \in D$ tales que

$$\begin{aligned} a_n < \alpha < a_n + 10^{-n}, \\ b_n < \beta < b_n + 10^{-n}, \\ c_n < \gamma < c_n + 10^{-n} \end{aligned}$$

(Teorema 2.2.3). Se sigue entonces del Teorema 2.4.2 (y la definición) que

$$a_n + b_n < \alpha + \beta < a_n + b_n + 2 \cdot 10^{-n},$$

y también

$$a_n + b_n + c_n < (\alpha + \beta) + \gamma < a_n + b_n + c_n + 3 \cdot 10^{-n}. \tag{2.2}$$

De manera análoga

$$a_n + b_n + c_n < \alpha + (\beta + \gamma) < a_n + b_n + c_n + 3 \cdot 10^{-n},$$

lo cual implica que

$$-a_n - b_n - c_n - 3 \cdot 10^{-n} < -[\alpha + (\beta + \gamma)] < -a_n - b_n - c_n. \tag{2.3}$$

Finalmente, sumando (2.2) y (2.3) se obtiene

$$-3 \cdot 10^{-n} < [(\alpha + \beta) + \gamma] - [\alpha + (\beta + \gamma)] < 3 \cdot 10^{-n}, \quad \forall \ n,$$

por lo cual

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

(en virtud del Lema 2.4.1). □

El inverso aditivo de un real es único: si α', α'' son dos inversos aditivos de α, se tendría

$$\alpha' = \alpha' + (\alpha + \alpha'') = (\alpha' + \alpha) + \alpha'' = 0 + \alpha'' = \alpha'',$$

denotaremos por $-\alpha$ al inverso aditivo de α.

Recordamos que se define el producto usando las reglas de los signos, tomando $\alpha, \beta \in \mathbb{R}^+$. Algo más general es cierto, $\forall\ \alpha, \beta \in \mathbb{R}$ estas leyes son válidas:

i) $(-\alpha)(-\beta) = \alpha\beta$,

ii) $(-\alpha)\beta = \alpha(-\beta) = -(\alpha\beta)$.

Esto se sigue por definición en el caso $\alpha, \beta \in \mathbb{R}^+$. Si $\alpha, \beta \in \mathbb{R}^-$, entonces $-\alpha, -\beta \in \mathbb{R}^+$, y por ejemplo

$$(-\alpha)(\beta) = -[(-\alpha)(-\beta)] = -(\alpha\beta).$$

En el caso $\alpha \in \mathbb{R}^+,\ \beta \in \mathbb{R}^-$ se tiene, por ejemplo

$$(-\alpha)(\beta) = [-(-\alpha)](-\beta) = \alpha(-\beta) = -(\alpha\beta),$$

ya que por definición $\alpha\beta = -[\alpha(-\beta)]$. Los demás casos se prueban de manera análoga. Como caso particular de las leyes de los signos tenemos

$$(-1)\alpha = -\alpha.$$

Lema 2.4.7. *El producto en* $\mathbb{R}$ *es asociativo.*

Demostración. Basta probarlo para reales positivos, el caso general se sigue de la regla de los signos, por ejemplo, si $\alpha, \beta, \gamma \in \mathbb{R}^+$ y dicha propiedad es válida en este caso

$$\begin{aligned} [(-\alpha)\beta](-\gamma) &= [-(\alpha\beta)](-\gamma) = (\alpha\beta)\gamma = \alpha(\beta\gamma) \\ &= (-\alpha)[-(\beta\gamma)] = (-\alpha)[\beta(-\gamma)]. \end{aligned}$$

Los demás casos se prueban análogamente.

Sean $\alpha, \beta, \gamma \in \mathbb{R}^+$, y $N \in \mathbb{N}$ tal que $\alpha, \beta, \gamma < N$. Además, $\forall\ n \in \mathbb{N}$ se toman $a_n, b_n, c_n \in D$ tales que

$$\begin{aligned} 0 < a_n < \ \alpha \ &< a_n + 10^{-n}, \\ 0 < b_n < \ \beta \ &< b_n + 10^{-n}, \\ 0 < c_n < \ \gamma \ &< c_n + 10^{-n}. \end{aligned}$$

Se sigue entonces del Teorema 2.4.2 que

$$a_n b_n < \alpha\beta < a_n b_n + (a_n + b_n)10^{-n} + 10^{-2n},$$

y

$$a_n b_n c_n < (\alpha\beta)\gamma < a_n b_n c_n + (a_n c_n + b_n c_n + a_n b_n)10^{-n} + (a_n + b_n + c_n)10^{-2n} + 10^{-3n}.$$

Obsérvese que

$$\begin{aligned}(a_n c_n + b_n c_n + a_n b_n)10^{-n} + (a_n + b_n + c_n)\cdot 10^{-2n} + 10^{-3n} &< 10^{-n}(3N^2) + 10^{-2n}(3N) + 10^{-3n} \\ &< 10^{-n}(3N^2 + 3N + 1) < 10^{-n}10^m,\end{aligned}$$

para m suficientemente grande. Por lo que

$$a_n b_n c_n < (\alpha\beta)\gamma < a_n b_n c_n + 10^{-n}10^m.$$

Análogamente

$$a_n b_n c_n < \alpha(\beta\gamma) < a_n b_n c_n + 10^{-n}10^m,$$

y el resultado se sigue de manera similar al Lema 2.4.6. □

Lema 2.4.8. $\alpha \cdot 1 = \alpha,\ \forall\ \alpha \in \mathbb{R}$.
La demostración queda como ejercicio para el lector.

Lema 2.4.9. *La ley distributiva es válida en* $\mathbb{R}$, *i.e.* $\forall\ \alpha, \beta, \gamma \in \mathbb{R}$,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

Demostración. Si α, β o γ es 0, el resultado es inmediato, por ejemplo si $\beta = 0$,

$$\alpha(0 + \gamma) = \alpha\gamma = \alpha \cdot 0 + \alpha\gamma.$$

Caso 1: $\alpha, \beta, \gamma > 0$.
$\forall\ n \in \mathbb{N},\ \exists\ a_n, b_n, c_n \in D$ tales que

$$\begin{aligned}0 < a_n < \ \ \alpha \ \ &< a_n + 10^{-n}, \\ 0 < b_n < \ \ \beta \ \ &< b_n + 10^{-n}, \\ 0 < c_n < \ \ \gamma \ \ &< c_n + 10^{-n},\end{aligned}$$

por lo cual

$$a_n b_n < \alpha\beta < a_n b_n + (a_n + b_n)\cdot 10^{-n} + 10^{-2n},$$

$$\text{y} \quad a_n c_n < \alpha\gamma < a_n c_n + (a_n + c_n)\cdot 10^{-n} + 10^{-2n}$$

$$\therefore\ a_n b_n + a_n c_n < \alpha\beta + \alpha\gamma < a_n b_n + a_n c_n + (2\cdot a_n + b_n + c_n)\cdot 10^{-n} + 2\cdot 10^{-2n}.$$

Si $\alpha, \beta, \gamma < N$ se tiene

$$a_n b_n + a_n c_n < \alpha\beta + \alpha\gamma < a_n b_n + a_n c_n + 10^{-n}(4N+2).$$

$$\text{También}\ \ b_n + c_n < \beta + \gamma < b_n + c_n + 2\cdot 10^{-n}$$

$$\text{y} \quad a_n(b_n + c_n) < \alpha(\beta+\gamma) < a_n(b_n + c_n) + (2a_n + b_n + c_n)10^{-n} + 2\cdot 10^{-2n}$$

$$< a_n b_n + a_n c_n + 10^{-n}(4N+2).$$

Como en el Lema 2.4.7, tomando m tal que

$$2 + 4N < 10^m,$$

se tiene $\forall\ n \in \mathbb{N}$

$$a_n b_n + a_n c_n < \alpha\beta + \alpha\gamma < a_n b_n + a_n c_n + 10^{m-n}$$

$$\text{y} \quad a_n b_n + a_n c_n < \alpha(\beta+\gamma) < a_n b_n + a_n c_n + 10^{m-n},$$

y los argumentos de los lemas anteriores muestran que

$$\alpha\beta + \alpha\gamma = \alpha(\beta+\gamma).$$

Caso 2: $\alpha < 0,\ \beta, \gamma > 0$.
Este caso se deriva del Caso 1, las leyes de los signos y la unicidad del inverso aditivo:

$$\begin{aligned} \alpha(\beta+\gamma) &= -[(-\alpha)(\beta+\gamma)] = -[(-\alpha)\beta + (-\alpha)\gamma] \\ &= -[-(\alpha\beta) + (-(\alpha\gamma))] = -[-(\alpha\beta + \alpha\gamma)] = \alpha\beta + \alpha\gamma. \end{aligned}$$

Caso 3: $\beta < 0,\ \gamma < 0$.
Usando los casos anteriores y las leyes de los signos,

$$\begin{aligned} \alpha(\beta+\gamma) &= -(\alpha[-(\beta+\gamma)]) = -(\alpha[(-\beta) + (-\gamma)]) \\ &= -[\alpha(-\beta) + \alpha(-\gamma)] = \alpha\beta + \alpha\gamma. \end{aligned}$$

Caso 4: β y γ tienen distinto signo (ejercicio). □

Lema 2.4.10. *Dado $\alpha \in \mathbb{R},\ \alpha \neq 0,\ \alpha$ tiene un inverso multiplicativo único.*

Demostración.

Existencia

Caso 1: $\alpha > 0$.

$$\text{Sea } M = \{x \in D^+ \mid x\alpha \leqslant 1\},$$

si $\beta = \sup M$, se afirma que

$$\alpha\beta = 1. \tag{2.4}$$

M está acotado superiormente, ya que si $\alpha = A.a_1a_2\cdots a_n\cdots$, $A \neq 0$ o $a_n \neq 0$, en ambos casos, $1 \leqslant 10^n \cdot \alpha$, ya que

$$10^n\alpha \geqslant 10^n(A.a_1a_2\cdots a_n) \geqslant 1.$$

Por lo cual 10^n es cota superior de M (si $t \in M$, $t\alpha \leqslant 1 \leqslant 10^n \cdot \alpha$ y por lo tanto $t \leqslant 10^n$ (Teorema 2.4.2).

Nótese que si $0 < \gamma < \beta$, entonces $\gamma\alpha < 1$. Esto se sigue ya que $\exists\, t \in M$ tal que $\gamma < t < \beta$ y $\gamma\alpha < t\alpha < 1$.

Ahora, probamos (2.4). $\forall\ n$ sea $b_n \in D$ tal que

$$b_n < \beta < b_n + 10^{-n},$$

se sigue de la observación anterior que

$$b_n\alpha < 1 < (b_n + 10^{-n})\alpha, \tag{2.5}$$

(si $(b_n + 10^{-n})\alpha \leq 1$, $b_n + 10^{-n} \in M$ y como $\beta < b_n + 10^{-n}$, β no sería cota superior). Usando el Teorema 2.4.2 se tiene también que

$$b_n\alpha < \beta\alpha < (b_n + 10^{-n})\alpha. \tag{2.6}$$

Finalmente, si $1 \neq \beta\alpha$, digamos $1 < \beta\alpha$, usando (2.5) y (2.6), $\forall\ n \in \mathbb{N}$

$$b_n\alpha < 1 < \beta\alpha < (b_n + 10^{-n})\alpha.$$

Si 10^m es cota superior de α se tendría $0 < \beta\alpha - 1 < 10^{-n}\alpha < 10^{m-n}\ \forall n$, lo cual es una contradicción. En este último paso usamos el hecho de que las desigualdades $0 < a_1 < a_2 < a_3 < a_4$ implican $0 < a_3 - a_2 < a_4 - a_1$ (ejercicio).

Caso 2: $\alpha < 0$.

Se sigue del Caso 1 que $\exists\ \beta \in \mathbb{R}$ tal que $\beta(-\alpha) = 1$, por lo que $\alpha(-\beta) = 1$.

Unicidad

Si $\alpha\beta = \alpha\gamma = 1$, $\beta \neq \gamma$. Para $\alpha > 0$, se tiene (por las leyes de los signos) que $\beta, \gamma > 0$, digamos $\beta < \gamma$. En virtud del Teorema 2.4.2, $\alpha\beta < \alpha\gamma$, lo cual es una contradicción.

Para $\alpha < 0$, se tiene

$$(-\alpha)(-\beta) = (-\alpha)(-\gamma) = 1$$

y por el caso anterior, $-\beta = -\gamma$. □

Hemos probado:

Teorema 2.4.11. ***Los números reales son un campo.***

EJERCICIOS 2.4

1. Muestre con un ejemplo que los algoritmos de la primaria de la suma y la multiplicación de números en D se derivan de nuestras definiciones y de la ley distributiva.

2. Demuestre el Lema 2.4.8.

3. Demuestre que si $\alpha \in \mathbb{R}^+,\ \beta \in \mathbb{R}^-$, entonces $(\alpha\beta) = (-\alpha)(-\beta)$.

4. Termine las pruebas de los Lemas 2.4.9 y 2.4.10.

2.5. Racionales = reales periódicos

Se identificaron los números en D con números reales, identificamos ahora todos los racionales.

Definición 24. *Sea*

$$j : \mathbb{Q} \longrightarrow \mathbb{R},$$

dada por $j(\frac{a}{b}) = ab^{-1}$.

Esta inclusión está bien definida: $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow ab^{-1} = cd^{-1}$. Obsérvese que:

a) j es inyectiva:

$$j\left(\frac{a}{b}\right) = j\left(\frac{c}{d}\right) \Leftrightarrow ab^{-1} = cd^{-1} \Leftrightarrow ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}.$$

b) j preserva la suma:

$$j\left(\frac{a}{b}\right) + j\left(\frac{c}{d}\right) = j\left(\frac{a}{b} + \frac{c}{d}\right) \quad \text{(ejercicio)}.$$

c) j preserva productos:

$$j\left(\frac{a}{b}\right) j\left(\frac{c}{d}\right) = ab^{-1}cd^{-1} = ac(bd)^{-1} = j\left(\frac{ac}{bd}\right).$$

d) j preserva el orden:

$$\frac{a}{b} > \frac{c}{d} \Leftrightarrow j\left(\frac{a}{b}\right) > j\left(\frac{c}{d}\right) \quad \text{(ejercicio)}.$$

De ahora en adelante identificaremos $\mathbb{Q}$ con $j(\mathbb{Q})$, y usaremos ambas notaciones para cocientes:

$$\frac{\alpha}{\beta} = \alpha\beta^{-1}, \quad \beta \neq 0.$$

Como $D \subset \mathbb{Q}$, se tiene que $\mathbb{Q}$ es denso en los reales (Teorema 2.2.3).

Representación decimal de racionales

Es necesario identificar ésta definición de racionales, $\frac{m}{n}$ como mn^{-1}, con la expresión decimal (obtenida en cursos elementales).

Teorema 2.5.1. *Sea*

$$\frac{m}{n} = B.b_1b_2\cdots \in \mathbb{Q},$$

y también $A \in \mathbb{N}$, $a_1, a_2, a_3, \ldots \in \{0, 1, \ldots, 9\}$ *tales que*

$$\begin{cases} nA \leqslant m < n(A+1), \\ n(A.a_1) \leqslant m < n(A.a_1 + 10^{-1}), \\ n(A.a_1a_2) \leqslant m < n(A.a_1a_2 + 10^{-2}), \\ \vdots \quad \vdots \quad \vdots \end{cases} \tag{2.7}$$

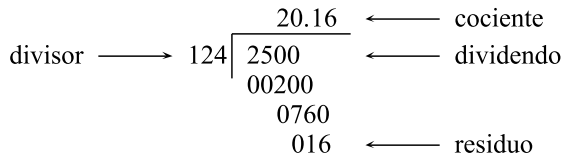
entonces

$$B.b_1b_2\cdots = A.a_1a_2\cdots .$$

Antes de probar el teorema, observamos que (2.7) es el algoritmo que se enseña en los cursos básicos de aritmética.

Ejemplo

$$\frac{2500}{124}$$



$$\begin{array}{rcccl} 124(20) & \leq & 2500 & < & 124(20+1) \\ 124(20.1) & \leq & 2500 & < & 124(20.2) \\ 124(20.16) & \leq & 2500 & < & 124(20.17) \\ \vdots & & \vdots & & \vdots \end{array}$$

Algoritmo (usando repetidas veces la ley distributiva):

$$\begin{aligned} 250(10) &= 2(124)(10) + 20, \\ 20 &= 0(124) + 20 \\ &= (124)(.1) + 7.6, \\ 7.6 &= (.06)(124) + .16 \end{aligned}$$

$$\begin{aligned} 2500 &= 20(124) + (.1)(124) + 7.6 \\ &= (20.1)(124) + (.06)(124) + .16 \\ &= 124(20.16) + .16 \end{aligned}$$

Obsérvese que en (2.7) las desigualdades de la izquierda se obtienen ya que los residuos son $\geqslant 0$, y los de la derecha, ya que al dividir se toma el mayor número posible con dicha propiedad, de otra manera estaríamos dividiendo mal.

Demostración. (Del Teorema 2.5.1) Las identidades (2.7) se pueden reescribir como:

$$\begin{array}{rcccl} 0 & \leqslant & m - nA & < & n \\ 0 & \leqslant & m - n(A.a_1) & < & n(10^{-1}) \\ 0 & \leqslant & m - n(A.a_1a_2) & < & n(10^{-2}) \\ \vdots & & \vdots & & \vdots \end{array}$$

o

$$\begin{array}{rcl} 0 \leqslant & \dfrac{m}{n} - A & < 1 \\ 0 \leqslant & \dfrac{m}{n} - A.a_1 & < 10^{-1} \\ 0 \leqslant & \dfrac{m}{n} - A.a_1a_2 & < 10^{-2} \\ \vdots & \vdots & \vdots \end{array}$$

Como $\dfrac{m}{n} = B.b_1b_2\cdots$, se tiene

$$\begin{array}{rcl} 0 \leqslant & B.b_1b_2\cdots - A & < 1 \quad \text{y} \\ A \leqslant & B.b_1b_2\cdots & < A+1 \end{array}$$

$$\therefore \quad A \leqslant B < A+1 \quad \text{y} \quad A = B.$$

También

$$\begin{array}{rcl} 0 \leqslant & A.b_1b_2\cdots - A.a_1 & < 10^{-1} \\ \therefore \quad A.a_1 \leqslant & A.b_1b_2\cdots & < A.a_1 + .1, \end{array}$$

$$\text{y} \quad a_1 \leqslant b_1 < a_1 + 1, \quad \text{por lo que} \quad a_1 = b_1.$$

Iterando este argumento se obtiene

$$B.b_1b_2\cdots = A.a_1a_2\cdots .$$

□

Algunos números reales tiene una expansión decimal periódica, por ejemplo,

$$\frac{8}{3} = 2.66\ldots, \qquad \frac{17}{11} = 1.5454\ldots,$$

estos periodos se denotan como

$$2.\widehat{6} \quad \text{o} \quad 1.\widehat{54}.$$

Probaremos que los reales periódicos son precisamente los racionales. Nótese que dado $\alpha \in \mathbb{R}$,

$$\begin{array}{c} \alpha = A.a_1a_2\cdots , \\ \alpha(10) = Aa_1.a_2a_3\cdots . \end{array} \tag{2.8}$$

Dejamos la verificación de este hecho como ejercicio.

Teorema 2.5.2. *Un número real es periódico si y sólo si es racional.*

Demostración. $\Rightarrow$) Basta probar el caso $\alpha \in \mathbb{R}^+$ periódico, digamos

$$\alpha = A.a_1 \cdots a_m \widehat{a_{m+1} \cdots} a_n,$$

α se puede escribir como

$$A.a_1 \cdots a_m + .\underbrace{00\cdots0}_{m\ lugares} \widehat{a_{m+1} \cdots} a_n \quad \text{(ejercicio)}.$$

Ahora, usando (2.8) se tiene

$$\begin{aligned} 10^m\alpha &= 10^m(A.a_1 \cdots a_m) + .\widehat{a_{m+1} \cdots} a_n \\ &= 10^m A + 10^{m-1}a_1 + \cdots + 10a_{m-1} + a_m + .\widehat{a_{m+1} \cdots} a_n. \end{aligned}$$

También aplicando los mismos argumentos

$$10^n\alpha = 10^n A + 10^{n-1}a_1 + \cdots + 10a_{n-1} + a_n + .\widehat{a_{n+1} \cdots} a_n,$$

(obsérvese que $a_{n+1} = a_{m+1}$). Por lo cual

$$\begin{aligned} (10^n - 10^m)\alpha &= 10^n A + 10^{n-1}a_1 + \cdots + a_n \\ &\quad -(10^m A + 10^{m-1}a_1 + \cdots + a_m) = B \in \mathbb{Z}. \end{aligned}$$

$$\therefore \quad \alpha \in \mathbb{Q}, \quad \text{ya que} \quad \alpha = \frac{B}{10^n - 10^m}.$$

$\Leftarrow$) Sea $\alpha = \frac{m}{n} \in \mathbb{Q}^+$.

En el algoritmo de la división, sin tomar en cuenta decimales, los residuos siempre son menores que n (el divisor). Además, el algoritmo consiste en ir considerando sucesivamente a estos residuos como los dividendos (agregándoles un 0). Por consiguiente, si un residuo aparece por segunda vez, se repite exactamente el mismo proceso que cuando apareció la primera vez.

Finalmente, como hay un número finito de números menores a n, algún residuo necesariamente se repite (en menos de n pasos), obteniéndose un número periódico. □

Ilustramos la prueba de la suficiencia en el Teorema 2.5.2 con dos ejemplos.

$$\begin{array}{r|l} & 73.846153 \\ 13 & 960 \\ & \underline{\mathbf{050}} \\ & 110 \\ & 060 \\ & 80 \\ & 020 \\ & 70 \\ & \underline{\mathbf{50}} \end{array}$$

$$\therefore \quad \frac{960}{13} = 73.846153\widehat{84615}.$$

o

$$\frac{1}{3} = 0.333\ldots = 0.\widehat{3}.$$

EJERCICIOS 2.5

1. Pruebe que la inclusión $j : \mathbb{Q} \longrightarrow \mathbb{R}$ preserva la suma y el orden.

2. Demuestre que dado $\alpha \in \mathbb{R},\ \alpha = A.a_1a_2\cdots,\ \alpha(10) = Aa_1.a_2a_3\cdots$.

3. Complete el detalle faltante en la prueba de la necesidad del Teorema 2.5.2.

2.6. Exponentes fraccionarios

2.6.1. Raíces n-ésimas

Teorema 2.6.1. $\forall\ \alpha \in \mathbb{R}^+$ *y* $\forall\ n \in \mathbb{N}$, *existe un único* $\beta \in \mathbb{R}^+$ *tal que*

$$\beta^n = \alpha,$$

este real se denota por $\sqrt[n]{\alpha}$.

DEMOSTRACIÓN. Se puede suponer $n \geq 2$ y $\alpha \neq 1$.

Existencia

Sea

$$W = \{x \in \mathbb{R}^+ \mid x^n < \alpha\}.$$

W está acotado superiormente:

$$\gamma = \text{máx}\,\{1, \alpha\} \text{ es cota superior:}$$

si $\alpha > 1$, entonces $\alpha^n > \alpha > x^n\ \forall\ x \in W$, y por lo tanto $x < \alpha = \gamma$, y si $\alpha < 1,\ x^n < 1$ y $x < 1 = \gamma$ (en estos argumentos usamos el ejercicio 2.6.1.1).

Se afirma que si $\beta = \sup W$, entonces $\beta^n = \alpha$.

Para probar esto, nótese que si r es suficientemente grande, $\beta - 10^{-r} > 0$, y como $\beta - 10^{-r} > 0$ no es cota superior de W, $\exists\ x,\ x > \beta - 10^{-r}$, tal que $x^n < \alpha$ y también $(\beta - 10^{-r})^n < \alpha$, por lo tanto

$$(\beta - 10^{-r})^n < \alpha < (\beta + 10^{-r})^n \tag{2.9}$$

$\forall\ r$ suficientemente grande.

Finalmente, obtenemos estimaciones para estas cotas de α :

$$(\beta + 10^{-r})^n = \sum_{j=0}^{n} \binom{n}{j} \frac{\beta^{n-j}}{10^{jr}} < \beta^n + \frac{k}{10^r} \sum_{j=1}^{n} \binom{n}{j} = \beta^n + \frac{k}{10^r}(2^n - 1),$$

donde $k = \text{máx}\{\beta^{n-1}, 1\}$. También

$$\begin{aligned}(\beta - 10^{-r})^n &= \sum_{j=0}^{n} \binom{n}{j} \frac{\beta^{n-j}(-1)^j}{10^{jr}} = \beta^n + \sum_{j=1}^{n} (-1)^j \binom{n}{j} \frac{\beta^{n-j}}{10^{jr}} \\ &> \beta^n - \sum_{j=1}^{n} \binom{n}{j} \frac{\beta^{n-j}}{10^{jr}} > \beta^n - \frac{(2^n - 1)k}{10^r}.\end{aligned}$$

Reemplazando estas desigualdades en (2.9) se tiene

$$\beta^n - \frac{c}{10^r} < \alpha < \beta^n + \frac{c}{10^r}, \quad c \text{ constante, } c > 0,$$

o

$$-\frac{c}{10^r} < \alpha - \beta^n < \frac{c}{10^r}, \quad \forall\ r \text{ suficientemente grande,}$$

o

$$-\frac{1}{10^r} < \frac{\alpha - \beta^n}{c} < \frac{1}{10^r}.$$

$$\therefore \quad \alpha = \beta^n.$$

Unicidad

Si $\beta > \gamma,\ \beta^n > \alpha^n$, por lo tanto existe un real único tal que

$$\beta^n = \alpha.$$

□

EJERCICIOS 2.6.1

1. Si $0 < x < y$, pruebe que $0 < x^n < y^n$.

2.6.2. Exponentes fraccionarios

Definición 25. *Si $\alpha \in \mathbb{R}$ y $n \in \mathbb{N}$ se define*

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdots \alpha}_{n \text{ veces}},$$

y si $\alpha \in \mathbb{R} - \{0\}$, $\alpha^{-n} = (\alpha^n)^{-1}$.

Nótese que $(\alpha^n)^{-1} = (\frac{1}{\alpha})^n$. Por convención $\alpha^0 = 1$.

Observación.

i) $\alpha^m\alpha^n = \alpha^{m+n}$.

ii) $(\alpha^m)^n = \alpha^{mn}$.

Prueba de *i)* $\alpha^m\alpha^n = \underbrace{(\alpha\cdots\alpha)}_{m\ veces}\underbrace{(\alpha\cdots\alpha)}_{n\ veces}$. También, si $m > 0,\ n < 0$, si $p = -n$

$$\alpha^m\alpha^n = \underbrace{(\alpha\cdots\alpha)}_{m\ veces}\underbrace{(\frac{1}{\alpha}\cdots\frac{1}{\alpha})}_{p\ veces} = \alpha^{m-p} = \alpha^{m+n},$$

etcétera.
Prueba de *ii)* $(\alpha^m)^n = \overbrace{\underbrace{(\alpha\cdots\alpha)}_{m\ veces}\cdots\underbrace{(\alpha\cdots\alpha)}_{m\ veces}}^{n\ veces} = \alpha^{mn}$.

Si $m < 0$ o $n < 0$ se reemplaza la misma expresión por $\frac{1}{\alpha}$, etcétera.

Proposición 2.6.2. *Dados* $\alpha, \beta \in \mathbb{R}^+,\ n, m \in \mathbb{N}$, *se tiene*

a) $\sqrt[n]{\alpha}\sqrt[n]{\beta} = \sqrt[n]{\alpha\beta}$.

b) $\sqrt[m]{\sqrt[n]{\alpha}} = \sqrt[nm]{\alpha}$.

c) $(\sqrt[n]{\alpha})^m = \sqrt[n]{\alpha^m}$.

d) $\sqrt[n]{\alpha^m} = \sqrt[s]{\alpha^r} \iff \frac{m}{n} = \frac{r}{s}$, *donde* $r, s \in \mathbb{N}$ *y* $\alpha \neq 1$.

Demostración.

a) $(\sqrt[n]{\alpha}\sqrt[n]{\beta})^n = (\sqrt[n]{\alpha})^n(\sqrt[n]{\beta})^n = \alpha\beta$.

b) $(\sqrt[m]{\sqrt[n]{\alpha}})^{mn} = ((\sqrt[m]{\sqrt[n]{\alpha}})^m)^n = (\sqrt[n]{\alpha})^n = \alpha$.

c) $((\sqrt[n]{\alpha})^m)^n = (\sqrt[n]{\alpha})^{mn} = ((\sqrt[n]{\alpha})^n)^m = \alpha^m$.

d) $\sqrt[n]{\alpha^m} = \sqrt[s]{\alpha^r} \Leftrightarrow (\sqrt[n]{\alpha^m})^{ns} = (\sqrt[s]{\alpha^r})^{ns} \Leftrightarrow \alpha^{ms} = \alpha^{rn} \Leftrightarrow ms = rn \Leftrightarrow$

$\frac{m}{n} = \frac{r}{s}$.

□

Este resultado se extiende a los casos $n < 0$ o $m < 0$. Por ejemplo, el caso c), si $m < 0$, tomando $p = -m$.

$$(\sqrt[n]{\alpha})^m = (\sqrt[n]{\alpha})^{-p} = \frac{1}{(\sqrt[n]{\alpha})^p} = \frac{1}{\sqrt[n]{\alpha^p}} = \sqrt[n]{\frac{1}{\alpha^p}} = \sqrt[n]{\alpha^m}.$$

El caso d) también es válido si $m, r < 0$. Esto se sigue reemplazando α por $\frac{1}{\alpha}$, ya que

$$\alpha^r = \left(\frac{1}{\alpha}\right)^{-r}, \text{ etcétera.}$$

Asimismo, nótese que el inciso c) implica que si $\alpha \in \mathbb{R}^+$ y $\frac{m}{n} \in \mathbb{Q}$, se puede definir

$$\alpha^{\frac{m}{n}} \quad \text{como} \quad \sqrt[n]{\alpha^m} \quad \text{o como} \quad (\sqrt[n]{\alpha})^m.$$

Es importante enfatizar que con la poderosa herramienta del cálculo infinitesimal esta definición se extiende a todos los reales

$$a^b = e^{b \log a}, \ a \in \mathbb{R}^+.$$

Proposición 2.6.3. $\forall\ \alpha, \beta \in \mathbb{R}^+,\ \frac{m}{n}, \frac{r}{s} \in \mathbb{Q}$, *se tiene*

a) $\alpha^{\frac{m}{n}} \beta^{\frac{m}{n}} = (\alpha\beta)^{\frac{m}{n}}$.

b) $\alpha^{\frac{m}{n}} \alpha^{\frac{r}{s}} = \alpha^{\frac{m}{n} + \frac{r}{s}}$.

c) $(\alpha^{\frac{m}{n}})^{\frac{r}{s}} = \alpha^{\frac{mr}{ns}}$.

Demostración.

a) $\alpha^{\frac{m}{n}} \beta^{\frac{m}{n}} = \sqrt[n]{\alpha^m}\sqrt[n]{\beta^m} = \sqrt[n]{\alpha^m \beta^m} = \sqrt[n]{(\alpha\beta)^m} = (\alpha\beta)^{\frac{m}{n}}$.

b) $\alpha^{\frac{m}{n}} \alpha^{\frac{r}{s}} = \alpha^{\frac{ms}{ns}} \alpha^{\frac{nr}{ns}} = \sqrt[ns]{\alpha^{ms}}\sqrt[ns]{\alpha^{nr}} = \sqrt[ns]{\alpha^{ms}\alpha^{nr}} = \sqrt[nr]{\alpha^{ms+rn}}$

$= \alpha^{\frac{ms+rn}{ns}} = \alpha^{\frac{m}{n} + \frac{r}{s}}$.

c) $(\alpha^{\frac{m}{n}})^{\frac{r}{s}} = (\sqrt[s]{\alpha^{\frac{m}{n}}})^r = (\sqrt[s]{\sqrt[n]{\alpha^m}})^r = (\sqrt[sn]{\alpha^m})^r = (\sqrt[sn]{\alpha})^{mr} = \alpha^{\frac{mr}{ns}}$.

□

2.7. Aproximación, método de Newton

Definición 26. *Si $\alpha \in \mathbb{R}$ se define su valor absoluto como*

$$|\alpha| = \begin{cases} \alpha & si\ \alpha \geqslant 0 \\ -\alpha & si\ \alpha < 0. \end{cases}$$

Observación. Son inmediatas las siguientes relaciones:

$$|-\alpha| = |\alpha|, \qquad |\alpha| \geqslant 0, \qquad \alpha \leqslant |\alpha|,$$

$$|\alpha| = 0 \Longleftrightarrow \alpha = 0 \quad \text{y} \quad |\alpha|^2 = \alpha^2.$$

Proposición 2.7.1. $\forall\ \alpha, \beta \in \mathbb{R}$,

i) $|\alpha\beta| = |\alpha||\beta|$.

ii) $|\alpha + \beta| \leqslant |\alpha| + |\beta|$.

Demostración.

i) Se tiene que

$$|\alpha\beta|^2 = (\alpha\beta)^2 = \alpha^2\beta^2 = |\alpha|^2|\beta|^2 = (|\alpha||\beta|)^2,$$

y por lo tanto $\quad |\alpha\beta| = |\alpha||\beta|$.

ii) Como

$$|\alpha+\beta|^2 = (\alpha+\beta)^2 = \alpha^2+2\alpha\beta+\beta^2 = |\alpha|^2+2\alpha\beta+|\beta|^2 \leq |\alpha|^2|+2|\alpha\beta|+|\beta|^2$$

$$= |\alpha|^2| + 2|\alpha||\beta| + |\beta|^2 = (|\alpha| + |\beta|)^2,$$

se sigue la afirmación.

□

Obsérvese que $\forall\ \alpha, \beta \in \mathbb{R}$,

$$||\alpha| - |\beta|| \leqslant |\alpha - \beta|.$$

Esto se sigue ya que

$$|\alpha| = |\alpha + \beta - \beta| \leqslant |\alpha - \beta| + |\beta|$$

y $|\alpha| - |\beta| \leqslant |\alpha - \beta|$.

Análogamente $|\beta| - |\alpha| \leqslant |\alpha - \beta|$.

Se discuten ahora algunos métodos elementales para aproximar reales. Por ejemplo, podemos aproximar $\sqrt{2}$ de la siguiente manera:

$$\begin{aligned} 1 < \ & \sqrt{2} \ < 2 \\ 1.4 < \ & \sqrt{2} \ < 1.5 = 1.4 + 10^{-1} \\ 1.41 < \ & \sqrt{2} \ < 1.42 = 1.41 + 10^{-2} \\ 1.414 < \ & \sqrt{2} \ < 1.415 = 1.414 + 10^{-3}. \end{aligned}$$

Una manera de encontrar estos valores es usando el método de Newton que se describe al final de este capítulo.

Con métodos del cálculo, se puede aproximar el número π. Como

$$\int_0^u \frac{dx}{1+x^2} = \arctan u,$$

en particular se tiene $\arctan 1 = \frac{\pi}{4}$. Usando estos hechos se puede demostrar la siguiente identidad atribuida a Leibnitz

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots,$$

cf. [5] pp. 461-462. También, al usar ciertas relaciones de arctan y polinomios de Taylor se puede obtener la siguiente aproximación de π:

$$3.14159 < \pi < 3.1416 = 3.14159 + 10^{-5},$$

cf. [13], pp. 356-357. Estas aproximaciones se pueden expresar también como

$$\begin{aligned} |\sqrt{2} - 1.414| \ &< \ 10^{-3} \\ |\pi - 3.14159| \ &< \ 10^{-5} \\ \text{o} \quad |\pi - 3.1415| \ &< \ 10^{-4}. \end{aligned}$$

Si se quiere aproximar y encontrar el margen de error del producto $\pi\sqrt{2}$ con los racionales 1.414 y 3.1415, una manera sería calcular

$$\begin{aligned} & |\sqrt{2}\pi - (3.1415)(1.414)| \\ & = |\sqrt{2}\pi - \sqrt{2}(3.1415) + \sqrt{2}(3.1415) - (3.1415)(1.414)| \\ & \leqslant \sqrt{2}(10^{-4}) + 3.1415(10^{-3}) \leqslant (1.415)10^{-4} + .0031415 \\ & = .0001415 + .0031415 \leqslant .00015 + .0032 = .00335 \leqslant .004, \end{aligned}$$

y $(1.414)(3.1415) = 4.442081$ aproxima $\sqrt{2}\pi$ con un error máximo de 4 milésimas,

$$-.004 < \sqrt{2}\pi - 4.442081 < .004.$$

También, sumando .002081 se tiene

$$\begin{aligned} -.001919 < \quad & \sqrt{2}\pi - 4.44 \quad < .006081, \\ \text{lo que implica} \quad -.01 < \quad & \sqrt{2}\pi - 4.44 \quad < .01 \end{aligned}$$

y 4.44 aproxima $\sqrt{2}\,\pi$ salvo por un error de una centésima .01=10^{-2}.

Una manera muy eficiente para calcular raíces es aplicar el método de Newton: Si $f : [x_1, x_0] \longrightarrow \mathbb{R}$ es una función con derivada continua y tal que $f(x_0)$ y $f(x_1)$ tienen signo distinto, entonces existe $r \in [x_1, x_0]$ tal que $f(r) = 0$ (teorema del valor intermedio), para aproximar r Newton formuló una algoritmo excepcionalmente útil.

Se considera la recta tangente a la gráfica en $(x_1, f(x_1))$, véase la Figura 2.2, y x_2 el punto donde esta recta intersecta a la recta real. Posteriormente se toma la recta por $(x_2, f(x_2))$ y con pendiente $f'(x_2)$, etcétera.

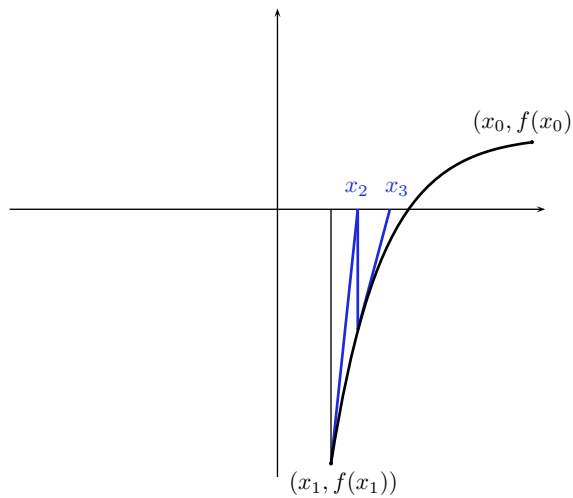


Figura 2.2: Método de Newton

Se demuestra en cálculo que si la función es de clase C^2, y su derivada no se anula, entonces $x_n \to r$, cuando $n \to \infty$. Una prueba formal se puede consultar en [5], pp. 512-514. Intuitivamente la convergencia es evidente, como se observa en la Figura 2.2.

Se encuentra ahora el valor que aproxima a la raíz, se tiene

$$\frac{f(x_n)-0}{x_n-x_{n+1}} = f'(x_n)$$

$$i.e., \quad x_n - x_{n+1} = \frac{f(x_n)}{f'(x_n)}$$

$$i.e., \quad x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Consideremos el siguiente ejemplo: $f(x) = x^2 - 5, \quad x_1 = 2,\ x_0 = 3,$

$$\begin{aligned} x_2 &= 2 - \frac{(-1)}{4} = 2.25 \\ x_3 &= 2.25 - \frac{[(2.25)^2 - 5]}{4.5} = 2.25 - \frac{[5.0625 - 5]}{4.5} \\ &= 2.25 - \frac{.0625}{4.5} = 2.25 - .01388\widehat{8} = 2.2361\widehat{.} \end{aligned}$$

Obteniéndose una aproximación a $\sqrt{5}$ con un error menor a una milésima, en efecto

$$4.9996\cdots = (2.236)^2 < 5 < (2.237)^2 = 5.004,$$

$$2.236 < \sqrt{5} < 2.237.$$

EJERCICIOS 2.7

1. Supóngase que α, β están aproximados por a, b de tal manera que se cumple, $|\alpha - a| < \varepsilon$ y $|b - \beta| < \varepsilon$. Demuestre que es válida la desigualdad $|\alpha\beta - ba| \leqslant \varepsilon^2 + \varepsilon(|\alpha| + |\beta|)$.

2. Supóngase que α, β, γ están dados con aproximación de 10^{-3} por a, b, c, números que en valor absoluto menores a 10. Pruebe que la expresión dada por $a^2 + b^2 + c^2 + ab + ac + bc$ aproxima $\alpha^2 + \beta^2 + \gamma^2 + \alpha\beta + \alpha\gamma + \beta\gamma$ con un error menor a .121.

3. Calcúlese $\sqrt{\sqrt{5} - 1}$ con una aproximación de una milésima (10^{-3}). Sugerencia: si c^2 cumple $|\sqrt{5} - 1 - c^2| < 10^{-3}$, entonces c es la aproximación buscada.

4. Calcúlese $\sqrt{2}$ y $\sqrt{3}$ con una aproximación de una milésima usando el método de Newton.

Capítulo 3

Los números complejos

3.1. Nociones básicas

3.1.1. Módulo

Definición 27. *Se define el módulo de un punto $P = (x, y)$ en el plano $\mathbb{R}^2$ como*

$$\sqrt{x^2 + y^2},$$

se denota por $|P|$. También dados 2 puntos $P, Q \in \mathbb{R}^2$, se define la distancia entre P y Q, como

$$d(P, Q) = |P - Q|.$$

Llamaremos también a los puntos en el plano vectores, y usaremos ambos términos de manera indistinta.

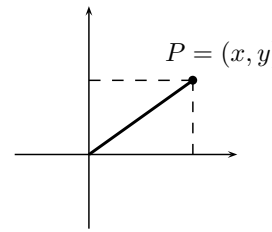


Figura 3.1: El módulo de P

Proposición 3.1.1. *Sean $r \in \mathbb{R}$ y $P, Q \in \mathbb{R}^2$. Entonces,*

i) $|rP| = |r||P|$,

ii) $|P + Q| \leqslant |P| + |Q|$ *(Desigualdad del triángulo).*

Demostración.

i) Si $r \geqslant 0$ y $P = (x, y)$, se tiene

$$|rP| = \sqrt{(rx)^2 + (ry)^2} = |r||P|.$$

Si $r < 0$, entonces

$$|rP| = \sqrt{r^2}\sqrt{x^2 + y^2} = -r\sqrt{x^2 + y^2} = |r||P|.$$

ii) Obsérvese que en un triángulo la longitud de un lado es menor que la suma de los otros dos. Este hecho se deduce fácilmente de la la Figura 3.2, o también de la desigualdad del triángulo. Por lo que

$$\begin{aligned} d(0, P+Q) &\leqslant d(0, P) + d(P, P+Q), \\ \therefore\ |P+Q| &\leqslant |P| + |(P+Q) - P| = |P| + |Q|. \end{aligned}$$

□

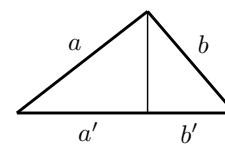


Figura 3.2: $a > a'$ y $b > b'$ por el Teorema de Pitágoras

Una prueba alternativa y más general, para la segunda parte de la proposición anterior, que usa el producto interno para vectores en $\mathbb{R}^n$, es la siguiente:

$$\begin{aligned} |a+b|^2 &= (a+b)\cdot(a+b) = |a|^2 + 2a\cdot b + |b|^2 \\ &\leqslant |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2, \end{aligned}$$

en virtud de la desigualdad de Cauchy-Schwarz, $a \cdot b \leqslant |a||b|$.

3.1.2. Argumento

Definición 28. *Se define el argumento de* $P \in \mathbb{R}^2 - \{0\}$, *tomado en el intervalo* $[0, 2\pi)$, *como la longitud del arco en la circunferencia unitaria que empieza en el punto* $e_1 = (1, 0)$ *y termina en* $P/|P|$, *moviéndose en el sentido contrario a las manecillas. A esta medida del ángulo determinado por ese arco, se le llama medición en radianes.*

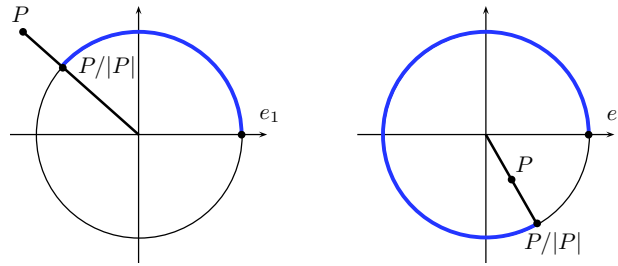


Figura 3.3: Medida de ángulos en radianes

Por ejemplo, los reales positivos tiene argumento 0, los reales negativos π. Se muestra en los cursos elementales que al tomar los polígonos regulares de n lados P_n y hacer tender $n \to \infty$, la longitud de los perímetros se aproximan a 2π. Una demostración formal se hace en cálculo, véase [13].

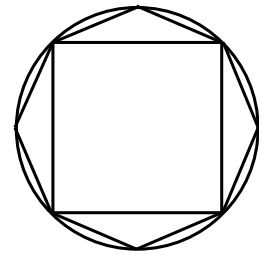


Figura 3.4: El perímetro de los polígonos regulares se aproxima a 2π

El argumento de un punto en el eje de las ordenadas positivas es $\pi/2$ (mitad de un semicírculo), y si se encuentra en la parte donde las ordenadas son negativas, es $3\pi/2$.

Definición 29. ***Sea*** $P \in \mathbb{R}^2 - \{0\}$, ***se define el argumento de*** P, ***como cualquier número de la forma*** $s + 2\pi k,\ k \in \mathbb{Z}$, ***donde*** s ***es el argumento de*** P ***tomado en*** $[0, 2\pi)$.

Esta última definición es la correcta, ya que exhibe que el argumento no está unívocamente determinado. lo cual es fundamental en la variable compleja, por ejemplo, cuando se estudia el logaritmo.

Sin embargo, si este valor se toma en $[0,\ 2\pi)$, sí lo está. En los siguientes ejemplos nos referimos solamente al argumento con valores en $[0, 2\pi)$.

1. Si el argumento de P es s, $0 \leqslant s \leqslant \pi$, el argumento de $-P$ es $s + \pi$, véase la Figura 3.6 (a).

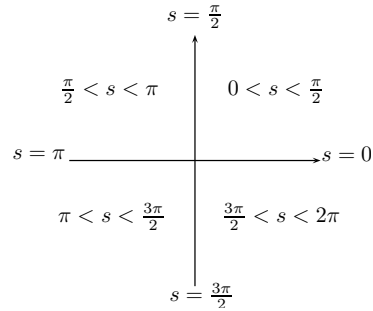
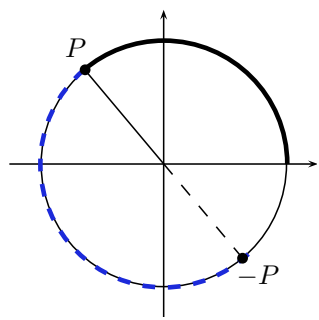
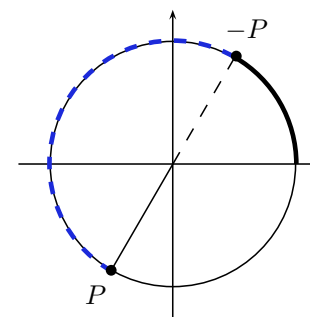


Figura 3.5: $s =$arg P tomado en $[0, 2\pi)$

2. Si $\arg P = s$, donde $\pi \leqslant s < 2\pi$, entonces $\arg(-P) = s - \pi$, véase la Figura 3.6 (b).



(a) $\arg(-P) = s + \pi$, donde $0 \leqslant s < \pi$



(b) $\arg(-P) = s - \pi$, donde $\pi \leqslant s < 2\pi$

Figura 3.6: Argumento de $-P$

3. Si $\arg P = s$, donde $P = (a, b)$ y $\overline{P} = (a, -b)$, entonces $\arg \overline{P} = 2\pi - s$, véase la Figura 3.7.

4. Si el argumento de $P = (a, b)$ es s y $b \geqslant 0$, entonces el argumento de $P' = (-a, b)$ es $\pi - s$, véase la Figura 3.8.

5. Si $P = (a, b)$, $b < 0$ y el argumento de P es s, entonces el argumento de $P' = (-a, b)$ es $3\pi - s$. Esto sucede ya que si $\arg P = 2\pi - r = s$, es decir, $r = 2\pi - s$, se tiene

$$\arg P' = \pi + r = \pi + 2\pi - s = 3\pi - s,$$

véase la Figura 3.9.

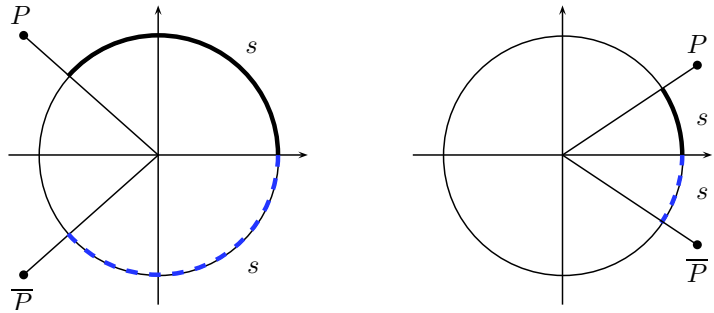


Figura 3.7: $\arg(\overline{P}) = 2\pi - s$

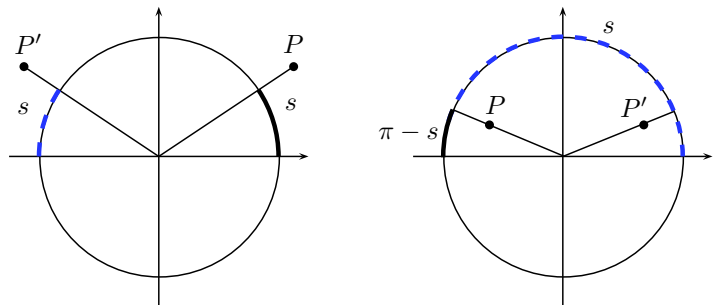


Figura 3.8: $\arg P' = \pi - s,\ P = (a, b),\ P' = (-a, b),\ b > 0$

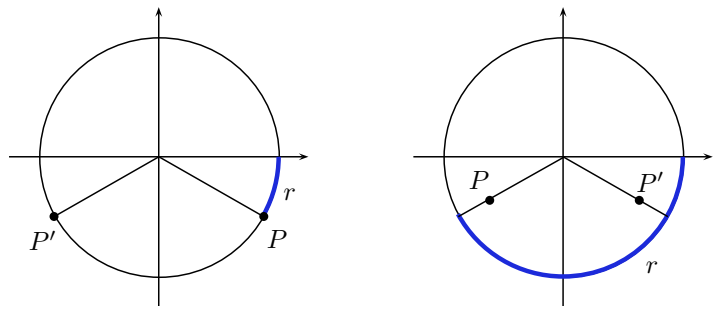


Figura 3.9: $\arg P' = 3\pi - s,\ P = (a, b),\ P' = (-a, b),\ b < 0$

Los ángulos también se miden en grados, esto es, se toma, o se define, 360° como una vuelta completa al círculo, y proporcionalmente, para otros puntos en el círculo. Por ejemplo, el ángulo entre (1,0) y (0,1) es 90°.

Obsérvese que el círculo completo de radio 1 mide 2π, lo que es $360°$, por lo que el número de grados correspondiente a x radianes está dado por

$$m = \frac{x(360)}{2\pi},$$

y a su vez m grados corresponde a x radianes

$$x = \frac{2\pi\, m}{360}.$$

Por ejemplo, si $\arg P = \pi/12$, en grados esto es

$$\frac{\pi}{12}\left(\frac{360}{2\pi}\right) = 15°,$$

y $12°$ en radianes es

$$12\left(\frac{2\pi}{360}\right) = \frac{\pi}{15},$$

o $7\pi/4$ es

$$360° - 45° = 315°.$$

Consideremos ahora el argumento como en la Definición 29. Las funciones trigonométricas $\cos : \mathbb{R} \to [-1, 1]$ y $\operatorname{sen} : \mathbb{R} \to [-1, 1]$ están determinadas bajo la siguiente regla de correspondencia:

A cada número real s, le asignamos el único punto en el círculo unitario que tiene argumento s, si escribimos $P = (x(s), y(s))$, se define $\cos s = x(s)$, y $\operatorname{sen} s = y(s)$, por lo que

$$P = (\cos s, \operatorname{sen} s)$$

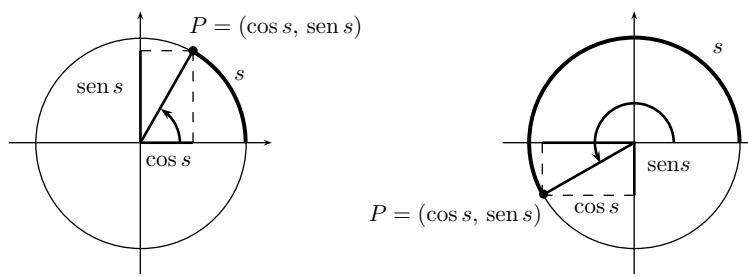


Figura 3.10: P es el único punto en el círculo unitario con argumento s

Esto se observa, en parte, de la trigonometría, véase la Figura 3.10. Sin embargo una definición formal y sus consecuencias proviene del cálculo, véase [13], pp. 256-276.

En general, si $P \in \mathbb{R}^2,\ P \neq 0$, y $\arg P = s$, entonces

$$\frac{P}{|\ P\ |} = (\cos s, \operatorname{sen} s).$$

Si $P = (a, b)$, entonces $|P|^2 = a^2 + b^2$ y se tiene

$$\cos s = \frac{a}{\sqrt{a^2 + b^2}}, \quad \operatorname{sen} s = \frac{b}{\sqrt{a^2 + b^2}}, \tag{3.1}$$

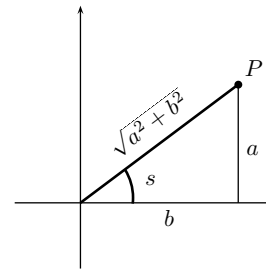


Figura 3.11: El módulo de P es $\sqrt{a^2 + b^2}$

Definición 30. *A la expresión*

$$P = r(\cos s, \operatorname{sen} s),$$

donde $r = |P|$ y s es cualquier argumento de P, se le llama forma polar de P, a r se le llama el módulo de P. .

Obsérvese que el módulo de un vector P está determinado de manera única. Y si se toma el argumento en $[0, 2\pi)$, éste también está unívocamente determinado: escribiendo

$$P = r(\cos\theta, \operatorname{sen}\theta),\ \ P = r(\cos\varphi, \operatorname{sen}\varphi),$$

entonces $\arg P = \theta = \varphi$ conforme a la manera como se definió el argumento con la longitud del arco.

Otra manera geométrica de ver esto es la siguiente:

$$\text{si} \quad \cos\varphi = \cos\theta, \quad 0 \leqslant \theta \leqslant \varphi < 2\pi,$$

entonces $\varphi = \theta$, o $\varphi = 2\pi - \theta$. Véase la Figura 3.12. La segunda igualdad acontece, salvo que $\varphi = \pi = \theta$. Puesto que $\operatorname{sen}\varphi = \operatorname{sen}(2\pi - \theta) = -\operatorname{sen}\theta$ implica $\operatorname{sen}\varphi = 0$.

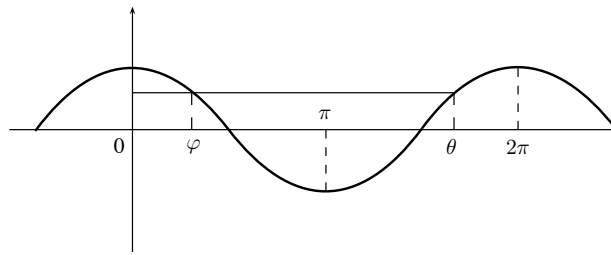


Figura 3.12: Si $\cos\varphi = \cos\theta$, entonces $\varphi = \theta$, o $\varphi = 2\pi - \theta,\ 0 \leqslant \theta,\ \varphi < 2\pi$

Ejemplos. Dados un módulo r y un argumento s encontramos las coordenadas de los puntos P que estos valores determinan:

a) $r = 3\sqrt{2}, \quad s \sim 225°$.

Tenemos que $225° \sim 5\pi/4$ y

$$\cos\frac{\pi}{4} = \frac{1}{\sqrt{2}} = \operatorname{sen}\frac{\pi}{4},$$

$$\therefore \quad P = 3\sqrt{2}\left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) = (-3, -3).$$

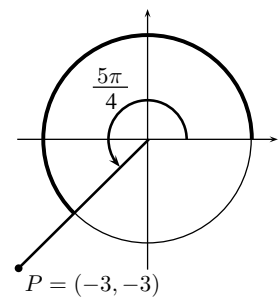


Figura 3.13: $r = 3\sqrt{2}, \quad s \sim 225°$

b) $r = 2, \quad s \sim 300°$.

Se toma un triángulo equilátero, y se denota por y a la longitud de la mediatriz como en la Figura 3.14.

Como $y^2 + 1/4 = 1$, se sigue que $y = \sqrt{3}/2$, y

$$\cos\frac{\pi}{3} = \frac{1}{2} = \operatorname{sen}\frac{\pi}{6}, \quad \cos\frac{\pi}{6} = \frac{\sqrt{3}}{2} = \operatorname{sen}\frac{\pi}{3},$$

por lo tanto, geométricamente se sigue que

$$P = 2\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) = (1, -\sqrt{3}),$$

donde la primera igualdad se da pues el lado opuesto a $\pi/6$ mide $1/2$ (ver Figura 3.15).

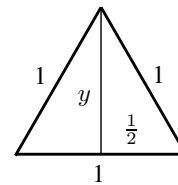


Figura 3.14: $y = \sqrt{3}/2$ es la longitud de la mediatriz

Otra manera (algebraica):

$$s = \frac{3\pi}{2} + \frac{\pi}{6} = \frac{10\pi}{6} = \frac{5\pi}{3},$$

y

$$\cos\frac{5\pi}{3} = \cos\left(-\frac{\pi}{3}\right) = \cos\frac{\pi}{3} = \frac{1}{2},$$

$$\operatorname{sen}\frac{5\pi}{3} = \operatorname{sen}\left(-\frac{\pi}{3}\right) = -\operatorname{sen}\frac{\pi}{3} = -\frac{\sqrt{3}}{2}.$$

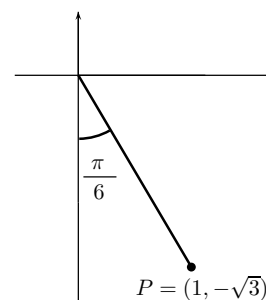


Figura 3.15: $r = 2, \quad s \sim 300°$.

Localizamos en qué cuadrantes aparecen los puntos en el círculo unitario con argumentos 1,2,3,4,5 y 6. Véase la Figura 3.16. Se tiene

$$0 < 1 < \frac{\pi}{2} < 2 < 3 < \pi < 4 < \frac{3\pi}{2} < 5 < 6 < 2\pi,$$

ya que como $8 < 3\pi$, se tiene $4 < 3\pi/2$, y dado que $3\pi < 10$, se cumple la siguiente desigualdad, etcétera. Obsérvese que dichos números están distribuidos a la misma distancia en el círculo.

Si se quiere localizar los puntos con estos argumentos $s = 1, 2$ ó 3, basta calcular $\cos s$ y $\operatorname{sen} s$. Sin usar programas o calculadoras, estos se pueden aproximar también usando los residuos de Taylor, cf. [13], pp. 345-361.

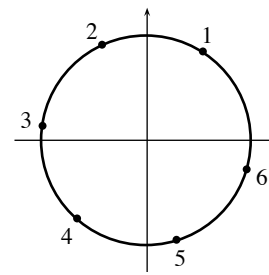


Figura 3.16: Los puntos en el círculo unitario con argumentos $1, 2, 3, 4, 5, 6$

Usando propiedades de las funciones trigonométricas se pueden localizar argumentos de vectores. Por ejemplo, el argumento de (3,1) está entre 0 y $\pi/6$. Esto se puede corroborar tomando la función seno, que es creciente en el intervalo $[0, \pi/2]$: si arg(3,1)=s,, entonces

$$\operatorname{sen} 0 = 0 < \operatorname{sen} s = \frac{1}{\sqrt{10}} \quad \text{y} \quad \frac{1}{\sqrt{10}} < \frac{1}{2} = \operatorname{sen} \frac{\pi}{6} \quad (2 < \sqrt{10}).$$

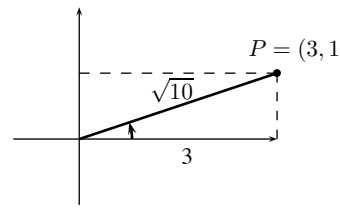


Figura 3.17: El argumento de (3,1) es menor a $\pi/6$

Se prueba también que el argumento de $(-3, -4)$ está entre $7\pi/6$ y $4\pi/3$. Si $s = \arg(-3, -4)$ se tiene que

$$s - \pi = \arg(3, 4),$$

y hay que probar que $\pi/6 < \arg(3,4) < \pi/3$, o equivalentemente (usando el hecho de que el seno es creciente en el 1er cuadrante),

$$\frac{1}{2} = \operatorname{sen}\frac{\pi}{6} < \frac{4}{5} < \operatorname{sen}\frac{\pi}{3} = \frac{\sqrt{3}}{2}.$$

Esto se sigue ya que $8 < 5\sqrt{3}$ $(64 < 25 \cdot 3)$.

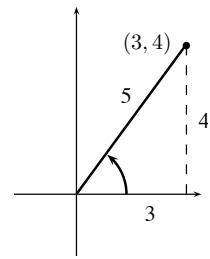


Figura 3.18: El argumento de (3,4) está entre $\pi/6$ y $\pi/3$

Un método para encontrar el argumento de un vector dado es usar la función inversa de la tangente, si escribimos

$$\tan s = \frac{y}{x},$$

entonces $s = \arctan(y/x)$, véase la Figura 3.19. Además del uso de una calculadora, es muy ilustrativo conocer métodos del cálculo.

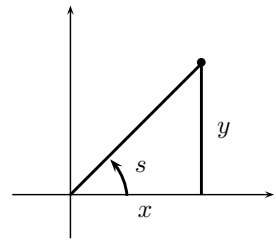


Figura 3.19: $\arctan(y/x) = s$

Es conveniente transladar el problema al primer cuadrante ya que

$$\tan|(0,\pi/2) \longrightarrow \mathbb{R}^+$$

es una biyección bicontinua.

Con la ayuda del cálculo se pueden obtener finas aproximaciones. Por ejemplo, si se quiere aproximar el valor $\operatorname{sen}(1/2)$ con un error menor a 10^{-5}, es útil usar el siguiente resultado.

Teorema 3.1.2. (Teorema de Taylor) *Sean $f : (a, b) \longrightarrow \mathbb{R}$ una función de clase C^{n+1}, y $x_0 \in (a, b)$. Entonces $\forall\ x \in (a, b)$, $\exists\, c \in (x_0, x) \cup (x, x_0)$, tal que*

$$f(x) = \sum_{k=0}^{n} \frac{f^k(x_0)}{k!}(x - x_0)^k + \frac{f^{n+1}(c)}{(n+1)!}(x - x_0)^{n+1}.$$

Al término $\frac{f^{n+1}(c)}{(n+1)!}(x - x_0)^{n+1}$ se le conoce como el residuo de Lagrange. Una prueba de este teorema se puede consultar en [7], pp 703-708. Usando este resultado, aproximamos $\operatorname{sen} x$ en el intervalo $(-\frac{\pi}{4}, \frac{\pi}{4})$ por un polinomio, al tomar su desarrollo alrededor de $x_0 = 0$. Lo que nos permite encontrar $\operatorname{sen} 1/2$ con un error de truncamiento menor a 10^{-5}.

El residuo toma una de las formas

$$\pm\frac{\operatorname{sen} c}{(n+1)!}x^{n+1},\ \pm\frac{\cos c}{(n+1)!}x^{n+1}, \qquad c \in (0, x)\ \text{ o }\ c \in (x, 0).$$

por lo que el error de truncamiento es menor o igual a

$$\frac{|x|^{n+1}}{(n+1)!} \leqslant \frac{(\pi/4)}{(n+1)!} < \frac{1}{(n+1)!}.$$

Si $n + 1 = 9$, se tiene

$$\frac{1}{(n+1)!} < .000002756 < 3 \cdot 10^{-6}.$$

Por lo que, para este valor la fórmula de Taylor establece la aproximación

$$\operatorname{sen} x = \operatorname{sen} 0 + x\cos 0 - \frac{x^2}{2!}\operatorname{sen} 0 - \frac{x^3}{3!}\cos 0 + \frac{x^4}{4!}\operatorname{sen} 0 + \frac{x^5}{5!}\cos 0$$

$$-\frac{x^6}{6!}\operatorname{sen} 0 - \frac{x^7}{7!}\cos 0 + \frac{x^8}{8!}\operatorname{sen} 0 + \frac{x^9}{9!}\cos c, \qquad c \in (0, x)\ \text{o}\ c \in (x, 0).$$

Por lo tanto

$$P(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!}$$

es el polinomio requerido. En $1/2$ se tiene

$$\begin{aligned} P\left(\frac{1}{2}\right) &= \frac{1}{2} - \frac{1}{2^3 \cdot 3!} + \frac{1}{2^5 \cdot 5!} - \frac{1}{2^7 \cdot 7!} \\ &= \frac{2^2 \cdot 3! - 1}{2^3 \cdot 3!} + \frac{2^2 \cdot 7 \cdot 6 - 1}{2^7 \cdot 7!} = \frac{23}{2^3 \cdot 3!} + \frac{167}{2^7 \cdot 7!} \\ &= \frac{23 \cdot 2^4 \cdot 7 \cdot 6 \cdot 5 \cdot 4 + 167}{2^7 \cdot 7!} = \frac{23(16)(840) + 167}{(128)(5040)} \end{aligned}$$

$$= \frac{309287}{645120} = .479425533.$$

Tomando $\alpha_1 = .479425$, se tiene

$$\left|\alpha_1 - P\left(\frac{1}{2}\right)\right| < 6 \cdot 10^{-7} < 10^{-6}.$$

$$\therefore \quad \left|\alpha_1 - \operatorname{sen}\frac{1}{2}\right| \leqslant \left|\alpha_1 - P\left(\frac{1}{2}\right)\right| + \left|P\left(\frac{1}{2}\right) - \operatorname{sen}\frac{1}{2}\right|$$

$$< 10^{-6} + 3 \cdot 10^{-6} = 4 \cdot 10^{-6} < 10^{-5}.$$

EJERCICIOS 3.1

1. Encuentre las coordenadas del vector P para $r = 3$ y $s = 150°$, $r = 5$ y $s = 30°$, $r = \sqrt{2}$ y $s = 135°$.

2. Calcule las coordenadas de los vectores de módulo 1, con argumento s, para $s = 2$, $s = 4$ y $s = 6$, con aproximación de 2 decimales.

3. Determine el argumento de los siguientes vectores, con aproximación de 2 decimales: (3,4) y $(-1, 2)$.

4. Escriba los vectores del ejercicio anterior en su forma polar.

3.2. Multiplicación de complejos

Se identifica a los reales con los puntos del eje de las abscisas en $\mathbb{R}^2$

$$\mathbb{R} \longleftrightarrow \{(x, y) \in \mathbb{R}^2 \mid y = 0\}.$$

Definición 31. *Los números complejos, denotados por* $\mathbb{C}$, *son los puntos del plano* $\mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R},\ y \in \mathbb{R}\}$.

Definición 32. *La suma de complejos se define exactamente como en el espacio vectorial* $\mathbb{R}^2$

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

obsérvese que esta suma extiende la suma en $\mathbb{R}$:

$$\begin{array}{ccccc} (a,0) & + & (b,0) & = & (a+b,0) \\ a & + & b & = & a+b. \end{array}$$

Para definir el producto, primero lo definimos para complejos de norma 1.

Definición 33. *Si* $z_1 = (\cos s_1, \operatorname{sen} s_1)$ *y* $z_2 = (\cos s_2, \operatorname{sen} s_2)$, *entonces*

$$z_1 z_2 = (\cos(s_1 + s_2),\ \operatorname{sen}(s_1 + s_2)).$$

Resulta que $z_1 z_2$ es el complejo en el círculo unitario cuyo argumento es la suma de s_1 y s_2, los argumentos de z_1 y z_2.

Obsérvese que si $s_1 + s_2 > 2\pi$, $z_1 z_2$ también se puede escribir como

$$(\cos(s_1 + s_2 - 2\pi)\,, \operatorname{sen}(s_1 + s_2 - 2\pi))\,.$$

La definición no depende del argumento tomado, ya que si $s_1' = s_1 + 2k_1\pi$ y $s_2' = s_2 + 2k_2\pi$, entonces $s_1' + s_2' = s_1 + s_2 + 2(k_1 + k_2)\pi$, y por consiguiente $\cos(s_1' + s_2') = \cos(s_1 + s_2)$, $\operatorname{sen}(s_1' + s_2') = \operatorname{sen}(s_1 + s_2)$, véase la Figura 3.20.

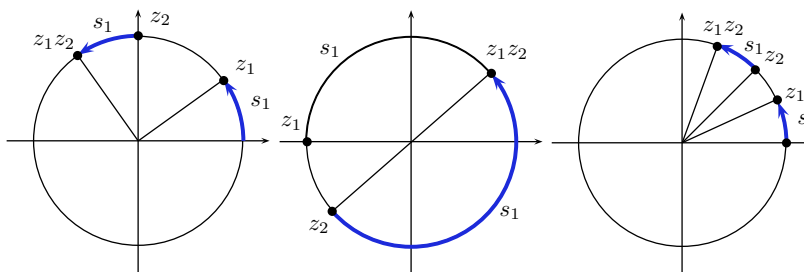


Figura 3.20: El argumento del producto es la suma de los argumentos

Ejemplos.

1. $$(0,1)(-1,0) = (0,-1).$$

   Como $\arg(0,1) = \frac{\pi}{2}$ y $\arg(-1,0) = \pi$, se sigue que

   $$\arg[(0,1)(-1,0)] = \frac{3\pi}{2}$$

   (véase la Figura 3.21).

2. $$(-1,0)(0,-1) = (0,1).$$

   Como $\arg(-1,0) = \pi$ y $\arg(0,-1) = \frac{3\pi}{2}$, se tiene

   $$\arg[(-1,0)(0,-1)] = \frac{5\pi}{2}$$

   (véase la Figura 3.22).

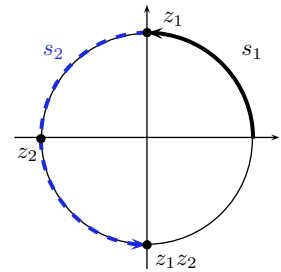


Figura 3.21: (0,1)(−1,0)=(0,−1)

3.
$$\left(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\left(\frac{-1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}\right) = (1, 0)$$

La igualdad se sigue ya que

$$\arg z_1 = \frac{\pi}{2} + \frac{\pi}{4} = \frac{3\pi}{4}, \quad \text{y} \quad \arg z_2 = \pi + \frac{\pi}{4} = \frac{5\pi}{4}$$

(véase la Figura 3.23).

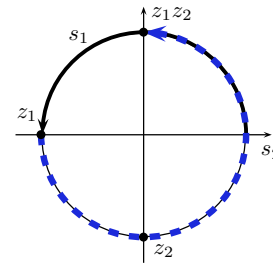


Figura 3.22: (−1,0)(0,−1)=(0,1)

4.
$$(1, 0)(a, b) = (a, b),$$

donde $\sqrt{a^2 + b^2} = 1$: si s es el argumento de (a, b),

$$\arg[(1, 0)(a, b)] = 0 + s = s = \arg(a, b).$$

5. $(\cos 4, \operatorname{sen} 4)(\cos 3, \operatorname{sen} 3) = (\cos 7, \operatorname{sen} 7) = (\cos(7 - 2\pi), \operatorname{sen}(7 - 2\pi))$.

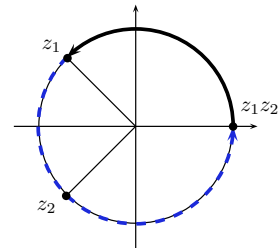


Figura 3.23: $(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}})(\frac{-1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}) = (1, 0)$

Definimos ahora el producto de manera general.

Definición 34. *Sean* $z_1 = r_1(\cos s_1, \operatorname{sen} s_1)$ *y* $z_2 = r_2(\cos s_2, \operatorname{sen} s_2)$, *se define su producto como*

$$z_1 z_2 = r_1 r_2(\cos(s_1 + s_2), \operatorname{sen}(s_1 + s_2)).$$

Es decir, ***multiplicar complejos es multiplicar sus módulos y sumar sus argumentos.***

Como en el caso anterior, se sigue directamente que la multiplicación no depende de la elección del argumento.

Ejemplos.

1. Multiplicamos $(\sqrt{3}, 1)$ por $(-3, -3)$.

   Para esto,

   $$|(\sqrt{3}, 1)| = \sqrt{3+1} = 2 \quad \text{y} \quad (\sqrt{3}, 1) = 2\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) = 2\left(\cos\frac{\pi}{6}, \operatorname{sen}\frac{\pi}{6}\right).$$

   Además, $|(-3, -3)| = 3\sqrt{2}$, por lo que

   $$|(-3, -3)| = 3\sqrt{2}\left(\frac{-1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}\right) = 3\sqrt{2}\left(\cos\frac{5\pi}{4}, \operatorname{sen}\frac{5\pi}{4}\right),$$

   por lo cual

   $$(\sqrt{3}, 1)(-3, -3) = 6\sqrt{2}\left(\cos\frac{34\pi}{24}, \operatorname{sen}\frac{34\pi}{24}\right) = 6\sqrt{2}\left(\cos\frac{17\pi}{12}, \operatorname{sen}\frac{17\pi}{12}\right),$$

   (véase la Figura 3.24).

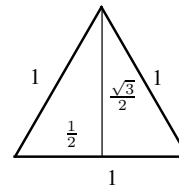


Figura 3.24: Argumentos $\frac{\pi}{6}$ y $\frac{\pi}{3}$

2. Calculamos $(-2\sqrt{3}, 2)(5\sqrt{3}, 5)$.

   Se tiene $|(-2\sqrt{3}, 2)| = \sqrt{12+4} = 4$ y $|(5\sqrt{3}, 5)| = \sqrt{100} = 10$, por lo que

$$\begin{aligned}(-2\sqrt{3}, 2)(5\sqrt{3}, 5) &= \left[4\left(-\frac{\sqrt{3}}{2}, \frac{1}{2}\right)\right]\left[10\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)\right] \\ &= 40\left(\cos\left(\pi - \frac{\pi}{6}\right), \operatorname{sen}\left(\pi - \frac{\pi}{6}\right)\right)\left(\cos\frac{\pi}{6}, \operatorname{sen}\frac{\pi}{6}\right) \\ &= -40\end{aligned}$$

   (véase la Figura 3.25).

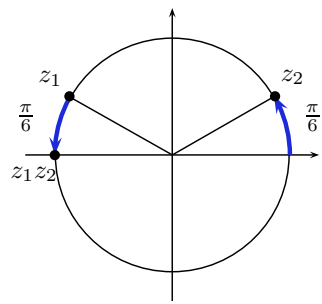


Figura 3.25: $(\cos(\pi - \frac{\pi}{6}), \operatorname{sen}(\pi - \frac{\pi}{6}))(\cos\frac{\pi}{6}, \operatorname{sen}\frac{\pi}{6}) = (-1, 0)$

3. Hacemos el producto $(2, -2)(-3, 3)$.

$$(2, -2) = 2\sqrt{2}\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$$

y

$$(-3,3) = 3\sqrt{2}\left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right),$$

por lo tanto

$$\begin{aligned}(2,-2)(-3,3) &= 12\left(\cos\frac{7\pi}{4}, \operatorname{sen}\frac{7\pi}{4}\right)\left(\cos\frac{3\pi}{4}, \operatorname{sen}\frac{3\pi}{4}\right)\\ &= 12\left(\cos\frac{2\pi}{4}, \operatorname{sen}\frac{2\pi}{4}\right) = (0,12).\end{aligned}$$

EJERCICIOS 3.2

1. Calcule el producto de $(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$ por $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$.
2. Pruebe que $(\cos 115°, \operatorname{sen} 115°)(\cos 65°, \operatorname{sen} 65°) = (-1, 0)$.
3. Calcule el producto $(0,8)(0,3)$.
4. Determine el producto de los siguientes números complejos:

   a) $(2, 2\sqrt{3})(-5\sqrt{3}, -5)$.

   b) $-2\,(\cos 2, \operatorname{sen} 2)\ 3\,(\cos 3, \operatorname{sen} 3)$.

   c) $\sqrt{3}\,(\cos(-35), \operatorname{sen}(-35))\ \sqrt{3}\,(\cos 15, \operatorname{sen} 15)$.

3.3. Los complejos son un campo

El complejo (0,1) se denota por i y a los complejos de la forma $(0, b)$, por $b\,i$. También a los reales $(a, 0)$ se les denota simplemente por a. De esta manera al complejo

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

se le denota por

$$a + ib.$$

Obsérvese que $a + ib = a' + ib' \iff a = a'$ y $b = b'$, ya que se tiene una correspondencia biunívoca

$$(a, b) \longleftrightarrow (a + i\,b).$$

Definición 35. *Dado $z = a + i\,b \in \mathbb{C}$, se dice que a es la parte real de z, y se escribe* $\operatorname{Re} z = a$, *y que b es la parte imaginaria de z, se escribe* $\operatorname{Im} z = b$.

Al eje de las ordenadas se le llama el eje imaginario. Obsérvese que

$$i^2 = -1,$$

puesto que

$$i \longleftrightarrow \left(\cos\frac{\pi}{2}, \operatorname{sen}\frac{\pi}{2}\right).$$

Teorema 3.3.1. *Sean $z = a + ib$ y $w = c + id$ números complejos, entonces*

$$zw = ac - bd + i(ad + bc).$$

Demostración. Escribimos a z y w en su forma polar,

$$z = r_1\cos\theta_1 + i\, r_1 \operatorname{sen}\theta_1 \quad \text{y} \quad w = r_2\cos\theta_2 + i\, r_2 \operatorname{sen}\theta_2,$$

por lo que

$$\begin{aligned} zw &= r_1 r_2[\cos(\theta_1+\theta_2) + i\ \operatorname{sen}(\theta_1+\theta_2)] \\ &= r_1 r_2[\cos\theta_1\cos\theta_2 - \operatorname{sen}\theta_1\operatorname{sen}\theta_2] \\ &\qquad + i\, r_1 r_2[\operatorname{sen}\theta_1\cos\theta_2 + \operatorname{sen}\theta_2\cos\theta_1] \\ &= r_1\cos\theta_1 r_2\cos\theta_2 - r_1\operatorname{sen}\theta_1 r_2\operatorname{sen}\theta_2 \\ &\qquad + i\,[r_1\operatorname{sen}\theta_1 r_2\cos\theta_2 + r_1\cos\theta_1 r_2\operatorname{sen}\theta_2] \\ &= ac - bd + i\,[bc + ad]. \end{aligned}$$

□

Se usaron las identidades $\cos(\theta_1+\theta_2) = \cos\theta_1\cos\theta_2 - \operatorname{sen}\theta_1\operatorname{sen}\theta_2$, y la correspondiente para la función seno. Estas conocidas igualdades se pueden probar de manera geométrica (véase, por ejemplo, [11] pp. 38, 39), o usando el cálculo (véase, por ejemplo, [13] pp. 266, 267).

Una manera de recordar la fórmula del teorema es usar la distributividad y el hecho $i^2 = -1$. En casi todos los casos, ésta es la manera de multiplicar, por ejemplo,

$$(\sqrt{3} + i)(-3 - 3i) = -3\sqrt{3} + 3 + i(-3 - 3\sqrt{3}).$$

Sin embargo, en algunos casos es más adecuado usar la idea geométrica mencionada en los ejemplos de la sección anterior.

Obsérvese que si $c \in \mathbb{R}$,

$$c(a + ib) = (c + i \cdot 0)(a + ib) = ca + icb,$$

esta operación se puede interpretar como el producto de un escalar por un vector o como el producto de dos complejos.

Proposición 3.3.2. *El producto de complejos cumple las leyes asociativa, conmutativa y distributiva.*

Demostración. Dejamos como ejercicio la prueba de la asociatividad. Probamos las otras 2 leyes:

Sean $z = (a + ib),\ w = (c + id)$ y $u = (e + if)$, entonces

$$zw = ac - bd + i(ad + bc) = ca - db + i(cb + da) = wz.$$

También

$$\begin{aligned} z(w + u) &= (a + ib)[c + e + i(d + f)] \\ &= a(c + e) - b(d + f) + i[a(d + f) + b(c + e)] \\ &= ac - bd + i(ad + bc) + ae - bf + i[af + be] \\ &= zw + zu. \end{aligned}$$

□

Definición 36. *Se define el conjugado de un complejo $z = a + ib$ como el complejo $a - ib$.*

El conjugado de z se denota por $\overline{z}$, nótese que este punto es el reflejado de z con respecto al eje real, véase la Figura 3.26.

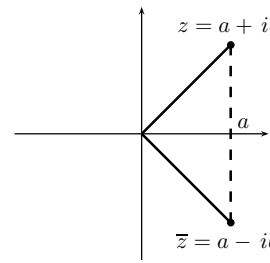


Figura 3.26: El conjugado de $z = a + ib$

Evidentemente $\overline{(\overline{z})} = z$:

$$(\overline{a - ib}) = a - (-ib) = a + ib.$$

Obsérvese que

$$z + \overline{z} = 2\,\mathrm{Re}\, z \quad \text{y} \quad z - \overline{z} = (2\,\mathrm{Im}\, z)i :$$

si $z = a + ib,\ \overline{z} = a - ib$, entonces

$$z + \overline{z} = 2a \quad \text{y} \quad z - \overline{z} = 2ib.$$

También, $z = \overline{z} \Longleftrightarrow z \in \mathbb{R}$, ya que $a + ib = a - ib \Leftrightarrow b = -b \Leftrightarrow b = 0$.

Proposición 3.3.3. *Sean $z, w \in \mathbb{C}$, entonces*

i) $\overline{z+w} = \overline{z} + \overline{w}$.

ii) $\overline{z}\,\overline{w} = \overline{zw}$.

iii) $z\overline{z} = |z|^2$.

Demostración.

i) Es claro de la definición. Para probar *ii)* si $z = a + ib$ y $w = c + id$,

$$\overline{z}\,\overline{w} = (a - ib)(c - id) = ac - bd + i\,[-ad - bc]$$

$$= \overline{(a + ib)(c + id)} = \overline{zw}.$$

La propiedad *iii)* es inmediata ya que $(a + ib)(a - ib) = a^2 + b^2$. □

Proposición 3.3.4. *Sea $z \in \mathbb{C}$, $z \neq 0$, entonces existe $w \in \mathbb{C}$ único tal que $wz = 1$, a w se le denota por $1/z$ o por z^{-1}.*

Demostración. Sea $z = a + ib$, se quiere encontrar $w = x + iy$ tal que

$$(a + ib)(x + iy) = ax - by + i\,(ay + bx) = 1,$$

i.e.,

$$\begin{cases} ax - by = 1 \\ bx + ay = 0, \end{cases} \tag{3.2}$$

si $a, b \neq 0$, se tiene

$$\begin{pmatrix} a & -b & 1 \\ b & a & 0 \end{pmatrix} \sim \begin{pmatrix} ab & -b^2 & b \\ -ab & -a^2 & 0 \end{pmatrix} \sim \begin{pmatrix} ab & -b^2 & b \\ 0 & -b^2 - a^2 & b \end{pmatrix}$$

$$\therefore \quad y = \frac{-b}{a^2 + b^2} \quad \text{y}$$

$$x = \frac{1}{b}(-ay) = \frac{a}{a^2 + b^2}.$$

$$\therefore \quad \frac{1}{z} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2},$$

si $a = 0$ o $b = 0$, esta expresión también satisface (3.2). □

Notése que el inciso iii) de la Proposición 3.3.3 prueba la Proposición 3.3.4 de manera inmediata sin ningún cálculo, ya que esta identidad establece que $1/z = \overline{z}/|z|^2$. Se tiene también una simple interpretación geométrica:

$$z^{-1} = \frac{1}{z}$$

es el número que tiene argumento $-s$ y módulo $1/|z|$, donde $s = \arg z$. Esto se sigue ya que multiplicar complejos es sumar sus argumentos y multiplicar sus normas, *i.e.*, si

$$z = r\cos\theta + i\, r\,\mathrm{sen}\,\theta,$$
$$\frac{1}{z} = \frac{1}{r}(\cos\theta - i\ \mathrm{sen}\,\theta).$$

Y el inverso se obtiene por una doble inversión: sobre la recta real y sobre el círculo unitario (o al revés), esto es,

$$z \longrightarrow \overline{z} \longrightarrow \frac{\overline{z}}{|\overline{z}|^2} \ = \ \frac{\overline{z}}{\overline{z}z} \ = \ \frac{1}{z},$$

(véase la Figura 3.27).

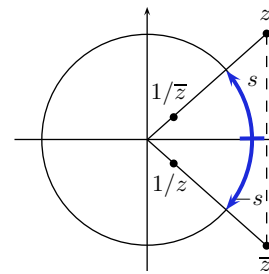


Figura 3.27: Interpretación geométrica de $1/z$

Nótese que $1(a + ib) = a + ib$, por lo que el siguiente resultado es consecuencia de las observaciones anteriores.

Teorema 3.3.5. ***Los números complejos son un campo.***

El cociente se define como

$$\frac{z}{w} = zw^{-1}, \text{ donde } w \neq 0.$$

Obsérvese que

$$\frac{z}{w} = \frac{z}{w} \cdot 1 = \frac{z \cdot \overline{w}}{w \cdot \overline{w}} = \frac{z\overline{w}}{|w|^2},$$

lo cual exhibe una manera inmediata para calcular cocientes:

Si $z = a + ib$ y $w = c + id$, entonces

$$\frac{z}{w} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd+i(bc-ad)}{c^2+d^2}.$$

Ejemplo.

$$\frac{2+5i}{4-3i} = \frac{(2+5i)(4+3i)}{25} = -\frac{7}{25} + \frac{26}{25}i.$$

Obsérvese también que

$$\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}},$$

esto se sigue ya que

$$\overline{z} = \overline{\left(\frac{z}{w} \cdot w\right)} = \overline{\left(\frac{z}{w}\right)}\,\overline{w}.$$

EJERCICIOS 3.3

1. Realice las siguientes operaciones de números complejos.
   a) $\overline{2-4i/(5-5i)}$ *c)* $(2-3i)/(1+5i)$
   b) $(4+i)/(6-i)$ *d)* $(-1+6i)(3+5i)-2i$.

2. Pruebe que el producto de números complejos cumple la ley asociativa.

3. Calcule $(\frac{\sqrt{3}}{2} + \frac{1}{2}\,i)^{205}$ y $(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i)^{56}$.

4. Sea $z = 6 - 8i$, para que número z' se cumple $zz' = 100$.

5. Encuentre las parejas u, v de números complejos para las cuales sucede que: *a)* $u\,\overline{(\overline{v}u)} = v$ *b)* $v + iu = -\overline{v} + i\overline{u}$ *c)* $|u/v| = |u|/|v|$.

3.4. Raíz cuadrada

Los reales positivos tienen 2 raíces cuadradas; si $a \in \mathbb{R}^+$ y $b \in \mathbb{R}^+$ son tales que $b^2 = a$, también $(-b)^2 = a$. Esto también se extiende a los complejos, sin embargo los reales negativos no tienen raíces en $\mathbb{R}$ (Leyes de los signos) pero sí en $\mathbb{C}$.

Teorema 3.4.1. *Sea $z \in \mathbb{C}$, $z \neq 0$, entonces la ecuación $w^2 = z$ tiene exactamente 2 soluciones en $\mathbb{C}$.*

Por ejemplo, si $z = -3$, entonces $w_1 = \sqrt{3}i$ y $w_2 = -\sqrt{3}i$ son sus raíces cuadradas. Antes de probar el teorema exhibimos otro ejemplo, sea $z = 5 - 12i$. Si $w = x + iy$ cumple $w^2 = z$, se tiene

$$x^2 - y^2 = 5, \tag{3.3}$$

$$2xy = -12.$$

Elevando al cuadrado ambas ecuaciones se tiene

$$\begin{aligned} x^4 - 2x^2y^2 + y^4 &= 25 \\ 4x^2y^2 &= 144. \end{aligned}$$

Sumándolas

$$x^4 + 2x^2y^2 + y^4 = 169,$$

$$i.e., \quad (x^2 + y^2)^2 = 169$$

y

$$x^2 + y^2 = 13$$

(como $x^2+y^2 \geqslant 0,\ -13$ no es solución). Sumando (3.3) a esta última ecuación se tiene

$$2x^2 = 18 \quad \text{y} \quad x = \pm 3,$$

restando tenemos

$$2y^2 = 8 \quad \text{y} \quad y = \pm 2.$$

Como $2xy = -12,\ x, y$ tienen distinto signo, y entonces

$$w_1 = -3 + 2i, \qquad w_2 = 3 - 2i$$

son las únicas raíces.

DEMOSTRACIÓN. (Del Teorema 3.4.1) Sea $z = a + ib,\ z \neq 0$. Entonces $w = x + iy$ es una raíz cuadrada de z

$$\iff (x + iy)^2 = a + ib,$$

i.e.,

$$x^2 - y^2 = a, \tag{3.4}$$

$$2xy = b. \tag{3.5}$$

Elevando al cuadrado ambas ecuaciones se tiene

$$\begin{aligned} x^4 - 2x^2y^2 + y^4 &= a^2 \\ 4x^2y^2 &= b^2, \end{aligned}$$

y sumándolas se tiene

$$\begin{aligned} x^4 + 2x^2y^2 + y^4 &= a^2 + b^2 \\ i.e., \quad (x^2 + y^2)^2 &= a^2 + b^2. \end{aligned}$$

Necesariamente

$$x^2 + y^2 = \sqrt{a^2 + b^2} \qquad (\text{ya que } x^2 + y^2 \geqslant 0).$$

Sumando y restando de esta última ecuación, la ecuación que aparece en (3.4) se tiene

$$\begin{aligned} 2x^2 &= a + \sqrt{a^2 + b^2}, \\ 2y^2 &= -a + \sqrt{a^2 + b^2}, \end{aligned}$$

esto es,

$$\begin{aligned} x &= \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}, \\ y &= \pm\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}. \end{aligned}$$

Aparentemente, hay cuatro soluciones, sin embargo usando la ecuación (3.5) se sigue que si $b > 0$ x, y son del mismo signo y si $b < 0$, estos números son de signos opuestos. □

Obsérvese que si z es real las raíces se encuentran de manera más rápida, por ejemplo si $z = a,\ a < 0$, se debe resolver

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b = 0. \end{cases}$$

Por lo tanto, $x = 0$ o $y = 0$. Si $y = 0$,

$$x^2 = a \Rightarrow x^2 < 0,$$

por lo que $x = 0$ y $y^2 = -a,\ i.e.,\ y = \pm\sqrt{-a},$ y

$$w = \pm\sqrt{-a}\, i.$$

Más aún, estas raíces se deducen directamente de la interpretación geométrica del producto, sin hacer ninguna cuenta. Esta interpretación nos permitirá probar fácilmente que todo complejo distinto de cero tiene n raíces n-ésimas.

Interpretación geométrica

Sea $z \in \mathbb{C}$, $|z| = r$ y $\arg z = s$, donde $0 \leqslant s < 2\pi$. Entonces si $w \in \mathbb{C}$ cumple $w^2 = z$, se sigue de la interpretación geométrica del producto que si

$$|w| = \sqrt{r} \quad \text{y} \quad \arg w = \frac{s}{2},$$

necesariamente $w^2 = z$, y también $(-w)^2 = z$. Nótese que

$$-w = \sqrt{r}\left[\cos\left(\frac{s}{2} + \pi\right) + i\,\text{sen}\left(\frac{s}{2} + \pi\right)\right],$$

(véase la Figura 3.28).

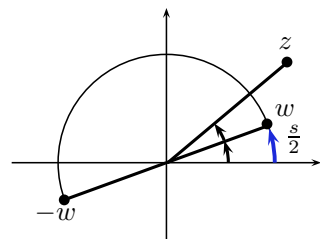


Figura 3.28: Interpretación geométrica de la raíz cuadrada de z

Ejemplo. Si

$$z = 9\left(\cos\frac{\pi}{3} + i\,\text{sen}\,\frac{\pi}{3}\right),$$

sus raíces cuadradas son

$$w = \pm 3\left(\cos\frac{\pi}{6} + i\,\text{sen}\,\frac{\pi}{6}\right).$$

Ecuaciones de 2o grado

Como en los cursos elementales, se puede completar cuadrados en la fórmula cuadrática

$$ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{C}$$

$$x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a},$$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{(2a)^2},$$

y las soluciones son

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Al número $d = b^2 - 4ac$ se le llama el discriminante. En particular, si $a, b, c \in \mathbb{R}$ y $d < 0$ no hay solución real, pero compleja sí. Obsérvese primero que si $\alpha, \beta \in \mathbb{C} - \{0\}$, $\sqrt{\alpha}$ es una raíz de α y $\sqrt{\beta}$ lo es de β, entonces todas las raíces de $\alpha\beta$ son

$$\pm(\sqrt{\alpha}\sqrt{\beta}),$$

ya que $(\pm\sqrt{\alpha}\sqrt{\beta})^2 = \alpha\beta$ y sólo hay 2 raíces.

Volviendo a las soluciones de la ecuación cuadrática con coeficientes reales, si $d < 0$, escribiendo

$$d = (-1)(d'), \quad d' > 0,$$

las soluciones son

$$\frac{-b \pm \sqrt{(-1)}\sqrt{d'}}{2a} = \frac{-b \pm i\sqrt{d'}}{2a}.$$

Ejemplo.

$$x^2 + 5x + 9,$$

tiene como raíces

$$\frac{-5 \pm \sqrt{25 - 36}}{2} = -\frac{5}{2} \pm i\frac{\sqrt{11}}{2}.$$

EJERCICIOS 3.4

1. Calcule las raíces cuadradas de $z = 3 + 4i$.
2. Encuentre las raíces cuadradadas de:
   a) $z = 1 + 2i$ *b)* $w = 12(\cos\frac{5\pi}{2} + i\,\mathrm{sen}\,\frac{5\pi}{2})$.
3. Halle las soluciones de las siguientes ecuaciones:
   a) $x^2 - x + 1 = 0$ *b)* $3x^2 + 3x + 2 = 0$ *c)* $x^2 + ix - 1 = 0$.

3.5. Raíces n-ésimas

La misma idea geométrica para encontrar raíces cuadradas se aplica para las raíces n-ésimas. Obsérvese que en esta caso es muy importante considerar todos los posibles argumentos, por ejemplo,

$$\left(\cos\frac{\pi}{7} + i\,\mathrm{sen}\,\frac{\pi}{7}\right)^{120} = \cos\frac{120\pi}{7} + i\,\mathrm{sen}\,\frac{120\pi}{7}$$

$$= \cos\left[\frac{(16\cdot 7+8)\pi}{7}\right] + i\,\mathrm{sen}\left[\frac{(16\cdot 7+8)\pi}{7}\right] = \cos\frac{8\pi}{7} + i\,\mathrm{sen}\,\frac{8\pi}{7}.$$

Es decir, al sumar argumentos, éstos pueden dar *muchas vueltas* al círculo.

Teorema 3.5.1. *Sea* $z \in \mathbb{C},\ z \neq 0,\ z = r(\cos s + i\,\mathrm{sen}\,s),\ 0 \leqslant s < 2\pi$, *entonces* z *tiene exactamente* n *raíces* n*-ésimas dadas por*

$$w_k = \sqrt[n]{r}\left[\cos\left(\frac{2k\pi+s}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi+s}{n}\right)\right],$$

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

Demostración. Sea $w = \rho(\cos\sigma + i\,\mathrm{sen}\,\sigma)$ tal que $w^n = z$, entonces

$$w^n = \rho^n[\cos(n\sigma) + i\,\mathrm{sen}(n\sigma) \quad \textbf{(Fórmula de De Moivre)}$$

$$\therefore \quad \rho^n = r \quad \text{y} \quad \rho = \sqrt[n]{r}.$$

También, $n\sigma - s = 2k\pi,\ k \in \mathbb{Z}$, por lo que

$$\sigma = \frac{2k\pi+s}{n}, \quad k \in \mathbb{Z}.$$

Se afirma que tomando $k = 0, 1, \ldots, n-1$ se obtienen todas las raíces distintas:

Dos enteros k_1, k_2 determinan la misma solución si y sólo si

$$\frac{2k_1\pi+s}{n} - \frac{2k_2\pi+s}{n} = 2k\pi, \quad \text{para alguna } k \in \mathbb{Z}$$

$$\begin{aligned} &\Leftrightarrow \quad \frac{2k_1\pi}{n} - \frac{2k_2\pi}{n} = 2k\pi \\ &\Leftrightarrow \quad k_1 - k_2 = kn \\ &\Leftrightarrow \quad k_1 \equiv k_2 \quad \text{mód } n. \end{aligned}$$

El resultado se sigue ya que $\mathbb{Z}_n$ tiene exactamente n elementos distintos representados por las clases $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. □

Obsérvese que la elección $0 \leqslant s < 2\pi$ en el enunciado del teorema, sólo fue tomada para evitar complicaciones innecesarias, sin embargo el resultado es cierto para cualquier elección.

Ejemplos.

1. Calculamos las raíces sextas de -27.

$$z = 27(\cos\pi + i\,\mathrm{sen}\,\pi) \quad \text{y} \quad \sqrt[6]{27} = \sqrt{3}.$$

$$\text{Entonces} \qquad w_k = \sqrt[6]{3}\left[\cos\left(\frac{\pi + 2k\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{\pi + 2k\pi}{6}\right)\right],$$

$k = 0, 1, \ldots, 5$. Por lo cual

$$\begin{aligned}
w_0 &= \sqrt{3}\left(\cos\frac{\pi}{6} + i\,\mathrm{sen}\,\frac{\pi}{6}\right),\\
w_1 &= \sqrt{3}\left[\cos\left(\frac{\pi}{6} + \frac{2\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{\pi}{6} + \frac{2\pi}{6}\right)\right]\\
&= \sqrt{3}\left(\cos\frac{3\pi}{6} + i\,\mathrm{sen}\,\frac{3\pi}{6}\right) = \sqrt{3}\,i,\\
w_2 &= \sqrt{3}\left(\cos\frac{5\pi}{6} + i\,\mathrm{sen}\,\frac{5\pi}{6}\right),\\
w_3 &= \sqrt{3}\left(\cos\frac{7\pi}{6} + i\,\mathrm{sen}\,\frac{7\pi}{6}\right),\\
w_4 &= \sqrt{3}\left(\cos\frac{9\pi}{6} + i\,\mathrm{sen}\,\frac{9\pi}{6}\right) = \sqrt{3}(-i),\\
w_5 &= \sqrt{3}\left(\cos\frac{11\pi}{6} + i\,\mathrm{sen}\,\frac{11\pi}{6}\right).
\end{aligned}$$

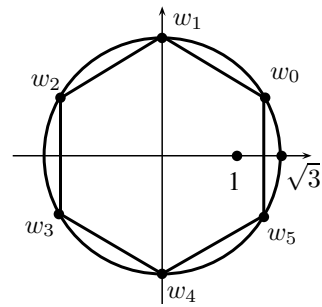


Figura 3.29: Raíces sextas de -3

Obsérvese que habiendo obtenido la primera raíz, las otras se obtienen sumando al argumento $2\pi/n$, consecutivamente, lo cual describe un polígono regular de n lados, como en las Figuras 3.29 y 3.30.

2. Calculamos las raíces quintas de 25.

$$z = 25(\cos 0 + i \operatorname{sen} 0),$$

$$w_k = \sqrt[5]{25}\left(\cos\frac{2k\pi}{5} + i \operatorname{sen}\frac{2k\pi}{5}\right)$$

$k = 0, 1, \ldots, 4$.

$$\begin{aligned}
w_0 &= \sqrt[5]{25}, \\
w_1 &= \sqrt[5]{25}\left(\cos\frac{2\pi}{5} + i \operatorname{sen}\frac{2\pi}{5}\right), \\
w_2 &= \sqrt[5]{25}\left(\cos\frac{4\pi}{5} + i \operatorname{sen}\frac{4\pi}{5}\right), \\
w_3 &= \sqrt[5]{25}\left(\cos\frac{6\pi}{5} + i \operatorname{sen}\frac{6\pi}{5}\right), \\
w_4 &= \sqrt[5]{25}\left(\cos\frac{8\pi}{5} + i \operatorname{sen}\frac{8\pi}{5}\right).
\end{aligned}$$

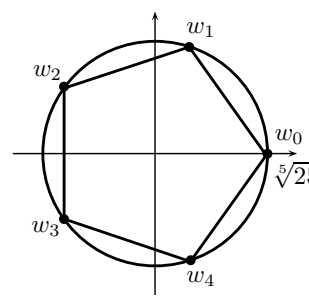


Figura 3.30: Raíces quintas de 25

En el siguiente capítulo usaremos un hecho fundamental de la matemática:

Teorema 3.5.2. (Teorema fundamental del álgebra) *Sea*

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$$

un polinomio con coeficientes complejos, entonces existe $z_0 \in \mathbb{C}$ *tal que* $P(z_0) = 0$.

En este libro no se demuestra este resultado. Una prueba simple y elegante se sigue del teorema de Liouville de la variable compleja. Una prueba que no usa variable compleja, se puede consultar en [2] pp. 96-98.

Obsérvese que este teorema es falso en los reales, por ejemplo, el polinomio

$$P(x) = x^2 + 1,$$

no tiene raíces reales, sus raices complejas son $\pm i$.

Así como los reales son un campo ordenado, los complejos no lo son. Resulta que no existe un orden en $\mathbb{C}$ compatible con la suma y el producto y que extienda el orden en los reales (ejercicio).

Por ejemplo, si ordenamos $\mathbb{C}$ de tal manera que $a + ib \leqslant c + id$, si se cumple

i) $a < c$,

ii) $a = c,\ b \leqslant d$,

es fácil checar que este orden cumple las propiedades de la tricotomía y la transitividad, sin embargo no es compatible con el producto. Una manera de verificar esto es al tomar los valores $u = 1$, $v = 1+i$ y $z = i$. Ya que entonces $0 < z$ y $u < v$, pero uz no es menor a zv, dado que $i > i(1 + i) = -1 + i$ (véase la Figura 3.31).

Otra manera más breve de mostrar que este definición de orden no es compatible con el producto, es tomar $i > 0$, ya que entonces $i^2 > 0$, pero $-1 < 0$.

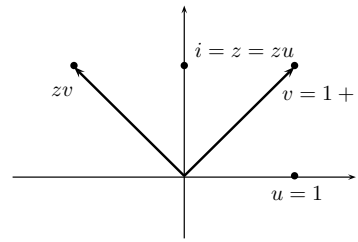


Figura 3.31: Los complejos no son un campo ordenado

EJERCICIOS 3.5

1. Calcule las raíces cuartas de -16, y las raíces cúbicas de $27i$.

2. Probar que no existe un orden en $\mathbb{C}$ que sea compatible con la suma y el producto y que extienda el orden de los reales. Sugerencia: mostrar que suponer $0 < -i$ implica incompatibilidad con las hipótesis.

Capítulo 4

El anillo de los polinomios

4.1. Definiciones

Definición 37. *Un polinomio es una expresión de la forma*

$$a_0 + a_1 x + \cdots + a_n x^n,$$

donde $a_i \in K$ y K es un campo ($\mathbb{C}$, $\mathbb{R}$, o $\mathbb{Q}$). Al símbolo x se le llama la indeterminada.

Escribiremos también $a_0 + a_1 z + \cdots + a_n z^n$, en este caso la indeterminada es z, y usaremos ambas expresiones de manera indistinta.

Ejemplo. $2 + 3x^2 + x^5$ (si el coeficiente es cero se omite).

El término de grado i es $a_i x^i$, a éste se le conoce también como un monomio. Al polinomio 0 se le llama el polinomio nulo.

Definición 38. *El grado de un polinomio es el mayor de los grados de los términos con coeficiente distinto de cero.*

Ejemplos. $P(x) = 2 - 5x^3 + 6x^4$ tiene grado cuatro. El polinomio constante $P(x) = 5$ tiene grado cero. El polinomio $P(x) = x^n$ tiene grado n.

Se tiene por acuerdo que el polinomio 0 tiene grado $-\infty$ (esto se motivará más tarde). En múltiples instancias es muy conveniente interpretar un polinomio como una función

$$P : K \longrightarrow K,$$

con regla de correspondencia $z \mapsto a_0 + a_1 z + \cdots + a_n z^n$. Por ejemplo, si los coeficientes son reales se puede interpretar como una función $P : \mathbb{R} \longrightarrow \mathbb{R}$ con la misma regla de correspondencia.

En particular, el polinomio $P(z) = 1 + z + z^3$, induce una función real $P : \mathbb{R} \longrightarrow \mathbb{R}$ definida como $P(x) = 1 + x + x^3$. Nótese que si $x = 2$, entonces $P(2) = 11$.

Obsérvese que si se tiene un polinomio $f(x) = a + bx + cx^2$, tal que se anula en $0, 1$ y -1, necesariamente se trata del polinomio nulo. Esto se sigue, ya que estas condiciones implican $a = 0$, y también

$$\begin{aligned} b + c &= 0, \\ -b + c &= 0. \end{aligned}$$

Por lo que

$$b = c = 0.$$

También, nótese que si $f_1(x) = a_1x^2 + b_1x + c_1$ y $f_2(x) = a_2x^2 + b_2x + c_2$ son dos polinomios que satisfacen $f_1(x) = f_2(x)\ \forall\ x \in \mathbb{C}$, entonces $a_1 = a_2$, $b_1 = b_2,\ c_1 = c_2$.

Esto se deriva, ya que como $f_1(0) = f_2(0)$, se tiene $c_1 = c_2$, también evaluando en 1 y -1 se tiene

$$\begin{aligned} a_1 + b_1 &= a_2 + b_2 \\ \text{y} \quad a_1 - b_1 &= a_2 - b_2, \end{aligned}$$

por lo que $a_1 = a_2$ y $b_1 = b_2$.

EJERCICIOS 4.1

1. Sea $f(z) = z^3 - 3z^2 - 1$. Encuentre el polinomio $g(z)$ para el cual se cumple $g(z) = f(z - 1)\ \forall\ z \in \mathbb{C}$.

2. Exhiba un polinomio de grado 5 con coeficientes reales que se anule en las raíces cúbicas complejas de la unidad.

4.2. El dominio entero $A[z]$

Un polinomio $a_0 + a_1x + \cdots + a_nx^n$ se puede escribir como

$$\sum_{i=0}^{\infty} a_ix^i,$$

simplemente escribiendo $a_m = 0$ si $m > n$. Esta convención nos permite definir la suma, escribiendo la expresión anterior como $a_0 + a_1x + a_2x^2 + \cdots$.

Definición 39. *La suma de polinomios está dada por*

$$(a_0 + a_1x + a_2x^2 + \cdots) + (b_0 + b_1x + b_2x^2 + \cdots)$$

$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots .$$

Definición 40. *El producto de polinomios está dado por*

$$\begin{aligned}&(a_0 + a_1x + a_2x_2 + \cdots)(b_0 + b_1x + b_2x_2 + \cdots)\\ &= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots\\ &+ \left(\sum_{j=0}^{k} a_jb_{k-j}\right)x^k + \cdots .\end{aligned}$$

Ejemplos.

1. $(2 + 3x + 5x^5) + (3x^2 + 6x^5) = 2 + 3x + 3x^2 + 11x^5.$

2. $$\begin{aligned}&(2 + 3x + 2x^2)(5 + x + x^2 + x^3)\\ &= 10 + (2 + 3 \cdot 5)x + (2 + 3 + 2 \cdot 5)x^2 + (2 + 3 + 2)x^3\\ &\quad +(3 + 2)x^4 + 2x^5\\ &= 10 + 17x + 15x^2 + 7x^3 + 5x^4 + 2x^5.\end{aligned}$$

Obsérvese que si

$$g(x) = f_1(x) + f_2(x) \quad \text{y} \quad h(x) = f_1(x)f_2(x),$$

entonces $\forall\ \alpha \in \mathbb{C}$ se tiene que

$$g(\alpha) = f_1(\alpha) + f_2(\alpha) \quad \text{y} \quad h(\alpha) = f_1(\alpha)f_2(\alpha).$$

Esto se sigue ya que la definición está basada en tratar a la indeterminada x como un elemento del campo y usar las propiedades distributiva y asociativa.

Evidentemente si $f_1(x)$ tiene grado m y $f_2(x)$ tiene grado n, el grado de $f_1(x) + f_2(x)$ es menor o igual al máximo de m y n.

Ejemplos.

1. $(2 + x) + (-2 - x) = 0.$
2. $(2 + 3x^5) + (1 + x + x^9) = 3 + x + 3x^5 + x^9.$

Proposición 4.2.1. *Si $P(z)$ tiene grado n y $Q(z)$ tiene grado m, entonces el grado de $P(z)Q(z)$ es $n + m$.*

Demostración. Si alguno de los dos polinomios es nulo, el producto también. Por convención $(-\infty) + n = -\infty$.

En los demás casos, si el polinomio $P(z) = a_0 + a_1z + \cdots + a_nz^n$ y $Q(z) = b_0 + b_1z + \cdots + b_mz^m$, $a_n \neq 0$ y $b_m \neq 0$, el término de grado máximo en $P(z)Q(z)$ es $b_ma_nz^{n+m}$: tomando $s > m + n$, $s = i + j$, entonces $i > m$ o $j > n$, en estos casos $a_i = 0$ o $b_j = 0$. □

Ejemplo.

$$(2-3x+x^3)(3-x) = 6-11x+3x^2+3x^3-x^4.$$

Denotaremos por $A[z]$, o por $A[x]$, al conjunto de polinomios con una indeterminada (z o x) sobre el anillo A (A puede ser $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). *Diremos que dos polinomios $p(z)$ y $q(z)$ son iguales si tienen los mismos coeficientes.*

Teorema 4.2.2. *El conjunto $A[z]$ es un anillo conmutativo con unidad.*

Demostración. Se sigue directamente de la definición que la suma de polinomios es conmutativa y asociativa. También, si $p(z) = a_n z^n + \cdots + a_0$, $a_i \in A$, entonces $p(z) + 0 = p(z)$, esto es, el neutro aditivo es el polinomio constante 0, y el inverso aditivo es $-p(z) = -a_n z^n - \cdots - a_1 z - a_0$, ya que $p(z) + (-p(z)) = 0$.

En cuanto al producto, la conmutatividad se sigue de la definición, y un argumento simple muestra que $p(z) \cdot 1 = p(z)$, para todo polinomio $p(z)$. Para la asociatividad, si tenemos $p(z) = \sum_{j=0}^{\infty} a_j z^j$, $q(z) = \sum_{j=0}^{\infty} b_j z^j$ y $h(z) = \sum_{j=0}^{\infty} c_j z^j$, el coeficiente de grado m en $[p(z)q(z)]h(z)$ está dado por

$$\sum_{l+k=m} \left(\sum_{i+j=k} a_i b_j \right) c_l,$$

esta doble suma se puede expresar también como

$$\sum_{i+j+l=m} a_i b_j c_l.$$

Por consiguiente, este coeficiente es también el de grado m en $p(z)[q(z)h(z)]$, y por lo tanto el producto es asociativo. Finalmente, el coeficiente del término de grado k en $p(z)[q(z) + h(z)]$ es

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

que es precisamente el coeficiente del término de grado k en el polinomio $p(z)q(z) + p(z)h(z)$, por lo que vale la ley distributiva. □

De hecho $A[z]$ es un dominio entero, ésto es consecuencia inmediata de la Proposición 4.2.1, ya que si

$$p(z)q(z) = 0,$$

entonces el grado de $p(z)$ o de $q(z)$ es $-\infty$.

En particular es válida la ley de la cancelación para el producto, ya que si $p(z) \neq 0$ y $p(z)q(z) = p(z)h(z)$, entonces $q(z) = h(z)$.

Definición 41. *Sea $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ una función, se dice que φ es polinomial si existe $f \in \mathbb{C}[z]$ tal que $f(n) = \varphi(n)\ \forall\ n \in \mathbb{N}$.*

Ejemplo.

La función $\varphi(n) = 1 + 3 + 5 + 7 + \cdots + 2n - 1$, es polinomial.

En efecto, como

$$\begin{aligned}\varphi(n) &= 1 + 2 + \cdots 2n - (2 + 4 + 6 + \cdots + 2n) \\ &= \frac{2n(2n+1)}{2} - 2(1 + 2 + 3 + \cdots + n) \\ &= n(2n+1) - 2\,\frac{n(n+1)}{2} \\ &= n(2n + 1 - n - 1) = n^2,\end{aligned}$$

tenemos que $\varphi(n) = f(n)$, donde $f(z) = z^2$.

En general, se puede obtener una expresión para $\sum_{k=1}^{n} k^j$ si se conoce $\sum_{k=1}^{n} k^{j-1}$. Por ejemplo, si queremos obtener una expresión para la suma de los primeros n cuadrados $1 + 2^2 + \cdots + n^2$ el truco es tomar

$$(k+1)^3 - k^3 = 3k^2 + 3k + 1.$$

Esta igualdad aplicada n veces, para $k = 1, 2, \ldots n$, establece que

$$\sum_{k=1}^{n} \left[(k+1)^3 - k^3\right] = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + n,$$

obteniéndose

$$(n+1)^3 - 1 = 3\sum_{k=1}^{n} k^2 + 3\frac{n(n+1)}{2} + n,$$

esto es

$$(n+1)^3 - (n+1) - 3\frac{n(n+1)}{2} = 3\sum_{k=1}^{n} k^2,$$

o

$$(n+1)\left[(n+1)^2 - 1 - \frac{3n}{2}\right] = 3\sum_{k=1}^{n} k^2$$

i.e.,

$$\frac{n+1}{3}\left(n^2 + 2n - \frac{3n}{2}\right) = \sum_{k=1}^{n} k^2$$

$$\therefore \quad \frac{n(n+1)}{3}\left(\frac{2n+1}{2}\right) = \frac{n(n+1)(2n+1)}{6} = \sum_{k=1}^{n} k^2.$$

Por consiguiente $\varphi(n) = \sum_{k=1}^{n} k^2$ es polinomial, *i.e.*, $\varphi(n) = f(n)$, donde

$$f(z) = \frac{z(z+1)(2z+1)}{6}.$$

Asimismo, este método muestra que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$:

$$(n+1)^2 - 1 = \sum_{k=1}^{n} \left[(k+1)^2 - k^2\right] = 2\sum_{k=1}^{n} k + n$$

$$\text{y} \quad \sum_{k=1}^{n} k = \frac{(n+1)^2 - 1 - n}{2} = \frac{n(n+1)}{2}.$$

EJERCICIOS 4.2

1. Demuestre que no existen $f(x)$ y $g(x)$ polinomios con coeficientes racionales de grado 1 tales que $f(x)g(x) = 2x^2 + 1$.

2. Considere $f(x)$, $g(x)$ y $h(x)$ polinomios con coeficientes enteros, y suponga que $f(x) = g(x)h(x)$ y $f(0) = 54321$. ¿Es posible que $g(0) = 4$? Explique.

3. Encuentre el polinomio de grado 2 $f(x)$ que toma los siguientes valores: $f(-2) = 0$, $f(-1) = -4$ y $f(0) = -6$.

4. Sea $f(x) = f_1(x)f_2(x)f_3(x)f_4(x)$ un polinomio de grado 9 donde el grado de $f_i(x)$ es positivo, para $i = 1, \ldots, 4$. Pruebe que al menos dos de los polinomios $f_i(x)$ tienen el mismo grado.

4.3. División con residuo

En el anillo de los polinomios sobre un campo, a semejanza de los enteros, el algoritmo de la división también es válido. Denotamos por $\operatorname{gr}(f(x))$ al grado de un polinomio $f(x)$, y por $K[x]$ el conjunto de los polinomios con una indeterminada sobre un campo K, que por lo general será $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$.

Teorema 4.3.1. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, donde $g(x)$ es no nulo, entonces existe otros 2 únicos polinomios $q(x)$ y $r(x)$ en $K[x]$ tales que*

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

ii) $\operatorname{gr}(r(x)) < \operatorname{gr}(g(x))$.

A $f(x)$ se le llama el dividendo, a $g(x)$ el divisor, a $q(x)$ el cociente y a $r(x)$ el residuo. Obsérvese que en $\mathbb{Z}$, si $a, b \in \mathbb{Z}$, $b \neq 0$ y $a = bq + r$, donde $0 \leqslant r < |b|$, el valor absoluto juega el papel del grado.

Ejemplo.

Si $f(x) = x^2 - 2$ y $g(x) = x - 1$, entonces $q(x) = x + 1$ y $r(x) = -1$, ya que

$$x^2 - 2 = (x + 1)(x - 1) - 1.$$

Demostración. (Del Teorema 4.3.1)

Unicidad

Si

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x),$$

donde $\operatorname{gr}(r_i(x)) < \operatorname{gr}(g(x)),\ i = 1, 2$, se tiene

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Si $q_1(x) \neq q_2(x)$, entonces $g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x)$ es un polinomio no nulo de grado mayor o igual a $\operatorname{gr}(g(x))$. Esto se sigue, ya que

$$\operatorname{gr}(q_1(x) - q_2(x)) = t \geqslant 0 \quad \text{y} \quad \operatorname{gr}(g(x)) = m \geqslant 0,$$

por lo cual

$$\operatorname{gr}(r_2(x) - r_1(x)) = m + t \geqslant m.$$

Sin embargo,

$$\operatorname{gr}(r_2(x) - r_1(x)) \leqslant \text{máx}\{\operatorname{gr}(r_1), \operatorname{gr}(r_2(x))\} < \operatorname{gr}(g(x)) = m.$$

Esta contradicción garantiza que $q_1(x) = q_2(x)$, y entonces $r_2(x) = r_1(x)$.

Existencia

El algoritmo consiste en tomar una sucesión de parejas de polinomios $q_i(x)$ y $r_i(x)$ tales que

$$f(x) = g(x)q_i(x) + r_i(x), \quad i = 1, 2, \ldots,$$

donde $\operatorname{gr}(f(x)) > \operatorname{gr}(r_1(x)) > \operatorname{gr}(r_2(x)) > \cdots$, por lo que después de un número finito de pasos se tiene que $\operatorname{gr}(r_t(x)) < \operatorname{gr}(g(x))$, para alguna t. Específicamente:

a) Si $\operatorname{gr}(f(x)) < \operatorname{gr}(g(x))$, se tiene

$$f(x) = g(x) \cdot 0 + f(x), \quad \text{en tal caso} \quad r(x) = f(x) \quad \text{y terminamos.}$$

b) Si $\operatorname{gr}(f(x)) > \operatorname{gr}(g(x))$, donde $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ y $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$, se procede de la siguiente manera:

i) Sean

$$q_1(x) = \frac{a_m}{b_n}\, x^{m-n} \quad \text{y} \quad r_1(x) = f(x) - g(x)q_1(x),$$

entonces $\operatorname{gr}(r_1(x)) < \operatorname{gr}(f(x))$ (véase el ejemplo a continuación).

ii) Habiendo obtenido $q_i(x)$ y $r_i(x)$, si $\operatorname{gr}(r_i(x)) \geqslant n$ (de otra manera, ya terminamos), escribimos $\operatorname{gr}(r_i(x)) = m_i$ y

$$r_i(x) = a_{i,m_i}x^{m_i} + a_{i,m_i-1}x^{m_i-1} + \cdots + a_{i,m_0},$$

se toma

$$q_{i+1}(x) = q_i(x) + a_{i,m_i}\, b_n^{-1}x^{m_i-n},$$

por lo que

$$\begin{aligned} & f(x) - q_{i+1}(x)g(x) \\ = \;& f(x) - q_i(x)g(x) - a_{i,m_i}\, b_n^{-1}x^{m_i-n}(g(x)) \\ = \;& r_i(x) - a_{i,m_i}\, b_n^{-1}x^{m_i-n}(g(x)) = r_{i+1}(x) \end{aligned}$$

es un polinomio de grado menor a $r_i(x)$ (ver ejemplo).

Como los grados de los polinomios decrecen, después de un número finito de pasos, para alguna t.

$$\operatorname{gr}(r_t(x)) < \operatorname{gr}(g(x))$$

y

$$f(x) = g(x)q_t(x) + r_t(x).$$

□

Obsérvese que la prueba del teorema radica en ir tomando a los residuos como dividendos, lo cual funciona gracias a la propiedad distributiva.

Ejemplo. Sea $f(x) = x^4+5x^3-2x^2+x-1$ y $g(x) = 2x^2-x+3$. Calculamos el cociente y el residuo de $f(x)$ entre $g(x)$.

En este caso se sigue de la Figura 4.1 que

$$\begin{aligned} q_1(x) &= \frac{1}{2}x^2, \\ q_2(x) &= \frac{1}{2}x^2 + \frac{11}{4}x, \qquad \text{y} \\ q(x) &= \frac{1}{2}x^2 + \frac{11}{4}x - \frac{3}{8}. \end{aligned}$$

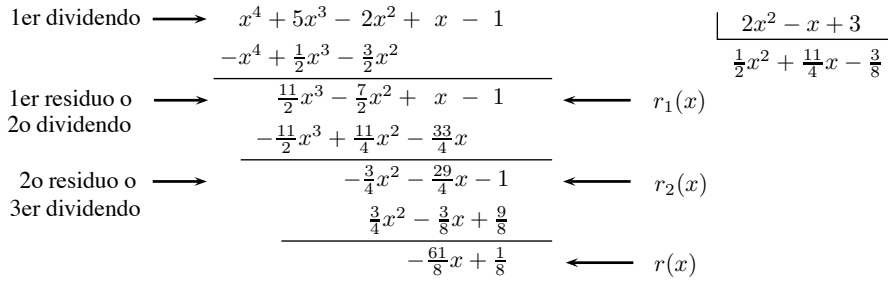


Figura 4.1: División con residuo

Obsérvese que en el Teorema 4.3.1, si $f(x)$ y $g(x)$ tienen coeficientes reales (o racionales), entonces también el cociente $q(x)$ y residuo el $r(x)$ tienen coeficientes reales (o racionales). Esto se sigue ya que $q(x)$ y $r(x)$ se obtienen de divisiones, sumas, restas y multiplicaciones de elementos en $f(x)$ y en $g(x)$, que son reales (o racionales).

Como en los enteros se tiene el concepto de divisibilidad. Se dice que $g(x)$ divide a $f(x)$, si

$$g(x)h(x) = f(x),$$

para alguna $h(x) \in K[x]$, se escribe $g(x)|f(x)$.

Evidentemente

$$g(x)|f(x) \Longleftrightarrow r(x) = 0,$$

donde $f(x) = g(x)q(x) + r(x)$ y $\operatorname{gr}(r(x)) < \operatorname{gr}(g(x))$.

Proposición 4.3.2. *Sea $f(x) \in K[x]$, entonces las siguientes afirmaciones son equivalentes:*

i) $f(x)$ *tiene un inverso multiplicativo.*

ii) $f(x)|1$.

iii) $f(x)$ *es de grado cero.*

Demostración. *i)* $\Leftrightarrow$ *ii)* es evidente ($\exists\ g(x)$ tal que $f(x)g(x) = 1$).

Ahora, si $f(x)$ es de grado 0, $f(x)$ es un escalar distinto de 0, por lo que tiene un inverso multiplicativo que es otro polinomio de grado 0 y se cumple *i)* (y por consiguiente *ii)*).

Finalmente si se cumple *ii)*, tomando en cuenta que los grados se suman en el producto y que $1 = f(x)g(x)$ se tiene

$$-\infty < \operatorname{gr}(f(x)) \leqslant 0.$$

□

Obsérvese que

$$(x-a)|(x-b) \Longleftrightarrow a=b,$$

ya que si $(x-a)q(x) = x-b$, entonces $-\infty < \operatorname{gr}(q(x)) = 0$ y $q(x) \in K$, digamos $q(x) = \alpha$, por lo que

$$\alpha x - \alpha a = x - b, \quad \text{luego} \quad \alpha = 1, \quad \text{de donde} \quad a = b.$$

Ya que por definición dos polinomios son iguales si y sólo si sus coeficientes son iguales.

Definición 42. *Dados dos polinomios $g(x)$ y $f(x)$ en $K[x]$, se dice que son asociados si $g(x)|f(x)$ y $f(x)|g(x)$.*

Claramente se sigue de la Proposición 4.2.1, que en este caso se tiene $f(x) = \alpha g(x)$, para alguna $\alpha \in K - \{0\}$, y viceversa, esta condición implica que $f(x)$ y $g(x)$ son asociados.

EJERCICIOS 4.3

1. Calcule el cociente y el residuo al dividir los siguientes polinomios:

   a) $x^3 - 3x + 2$ entre $x^2 + 2$.

   b) $2x - 1$ entre $-x^2 + 1$.

   c) $x^3 + 2x^2 - x + 4$ entre $3x + 1$.

4.4. Teoremas del residuo y del factor

Definición 43. *Sea $f(x) \in \mathbb{C}[x]$, se dice que a es una raíz (o un cero) del polinomio $f(x)$, si $f(a) = 0$.*

Es decir, las raíces son las soluciones de la ecuación

$$f(x) = 0.$$

Se sigue directamente del Teorema 4.3.1 (de la división con residuo), el siguiente resultado.

Corolario 4.4.1. *Si $f(x) \in \mathbb{C}[x]$, y $a \in \mathbb{C}$, entonces existen $q(x) \in \mathbb{C}[x]$ y $r \in \mathbb{C}$ únicos tales que*

$$f(x) = q(x)(x-a) + r.$$

Esta ecuación tiene consecuencias fundamentales.

Teorema 4.4.2. (Teorema del residuo) *Bajo las hipótesis del corolario anterior, se tiene*

$$r = f(a).$$

Demostración. La prueba ciertamente es simple,

$$f(a) = q(a)(a-a) + r = r.$$

□

Corolario 4.4.3. (Teorema del factor) $a \in \mathbb{C}$ *es raíz del polinomio* $f(x)$ *si y sólo si* $(x-a) \mid f(x)$.

Demostración. En efecto, como $f(a) = r$,

$$f(a) = 0 \Leftrightarrow (x-a) \mid f(x).$$

□

Corolario 4.4.4. *Bajo la notación del Corolario 4.4.1, se tiene*

$$(x-a) \mid [f(x) - f(a)].$$

Demostración. Esto se sigue, ya que

$$f(x) - f(a) = g(x)(x-a) + f(a) - f(a).$$

□

Corolario 4.4.5. *Si* $(x-a) \mid [f(x)g(x)]$, *entonces*

$$(x-a) \mid f(x) \quad o \quad (x-a) \mid g(x).$$

Demostración. La hipótesis implica

$$f(a)g(a) = 0,$$

$$\therefore \quad f(a) = 0 \quad \text{y} \quad (x-a) \mid f(x),$$

$$\text{o} \quad g(a) = 0 \quad \text{y} \quad (x-a) \mid g(x).$$

□

En este contexto es importante destacar de nuevo el teorema fundamental del álgebra, que establece que todo polinomio en $\mathbb{C}[x]$ de grado positivo tiene al menos una raíz en $\mathbb{C}$.

Por ejemplo, podemos expresar $x^3 - 1$ como polinomios de grado 1 de la siguiente manera: si

$$\alpha = \cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right),$$

entonces $\alpha^3 = 1$, y también

$$\alpha^2 = \overline{\alpha} = \cos\left(\frac{4\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{4\pi}{3}\right)$$

cumple $(\overline{\alpha})^3 = 1$ (véase la Figura 4.2).

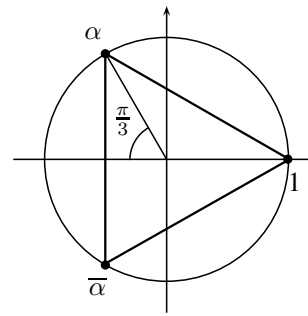


Figura 4.2: Raíces de $x^3 - 1$

La tercera raíz claramente es 1, por lo que usando el Corolario 4.4.3 se tiene

$$(x-1) \mid (x^3 - 1),$$

en efecto $x^3 - 1 = (x^2 + x + 1)(x - 1)$.

Ahora $x - \alpha$ y $x - \overline{\alpha}$ son factores de $x^3 - 1$, por lo que usando dos veces el Corolario 4.4.5, se tiene

$$x^2 + x + 1 = (x - \alpha)(x - \overline{\alpha}).$$

En efecto,

$$\begin{aligned}(x-\alpha)(x-\overline{\alpha}) &= x^2 - \alpha x - \overline{\alpha} x + |\alpha|^2 \\ &= x^2 - x(\alpha + \overline{\alpha}) + 1 \\ &= x^2 - 2\cos\left(\frac{2\pi}{3}\right) x + 1\end{aligned}$$

$$= x^2 + x + 1,$$

y por lo tanto

$$x^3 - 1 = (x-1)(x-\alpha)(x-\overline{\alpha}).$$

Obsérvese que el polinomio cero tiene una infinidad de raíces.

Teorema 4.4.6. *En los polinomios con coeficientes reales, $\mathbb{R}[x]$, las raíces complejas aparecen por parejas de conjugados, i.e., si $f(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$, entonces*

$$f(\alpha) = 0 \Longleftrightarrow f(\overline{\alpha}) = 0.$$

Demostración. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, si $\alpha \in \mathbb{C}$ es una raíz de $f(x)$, entonces

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

conjugando la ecuación tenemos

$$\overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0} = \overline{0} = 0,$$

por lo que usando las propiedades de la conjugación

$$f(\overline{\alpha}) = 0.$$

La misma prueba muestra la afirmación recíproca. □

Algunos resultados sobre polinomios en $\mathbb{Z}[x]$ se establecen a continuación.

Teorema 4.4.7. *Sea $f(x) \in \mathbb{Z}[x]$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Si $a/b \in \mathbb{Q}$, $(a,b) = 1$, es una raíz de $f(x)$, entonces*

$$a \,|\, a_0 \quad y \quad b \,|\, a_n.$$

Demostración. Si

$$a_0 + a_1\left(\frac{a}{b}\right) + \cdots + a_n\left(\frac{a}{b}\right)^n = 0,$$

entonces

$$b^n a_0 + a_1 a b^{n-1} + \cdots + a_{n-1}a^{n-1}b + a_n a^n = 0.$$

Finalmente, como $(a,b) = 1$, se sigue el resultado

$$b \,|\, a_n \quad \text{y} \quad a \,|\, a_0.$$

□

Por ejemplo, el polinomio

$$f(x) = 2x^3 + x^2 - 2$$

no tiene raíces racionales, ya que si $f(a/b) = 0$, entonces $a \,|\, 2$ y $b \,|\, 2$. Las únicas posibles raíces son $\pm 1,\ \pm 2$ y $\pm 1/2$, sin embargo

$$f(1) = 1, \quad f(-1) = -3,$$

$$f(2) = 18, \quad f(-2) = -14,$$

$$f\left(\frac{1}{2}\right) = \frac{2}{2^3} + \frac{1}{2^2} - 2 = -\frac{3}{2} \quad \text{y} \quad f\left(-\frac{1}{2}\right) = -\frac{1}{2^2} + \frac{1}{2^2} - 2 = -2.$$

Como caso particular del Teorema 4.4.7, se tiene que si

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

es un polinomio en $\mathbb{Z}[x]$ que tiene raíces racionales, éstas son enteras. Esto se cumple, ya que si

$$f\left(\frac{a}{b}\right) = 0 \quad \text{y} \quad (a, b) = 1,$$

entonces $b \,|\, 1$, *i.e.*, $b = \pm 1$, y $\frac{a}{b}$ es entero.

Analizamos ahora el polinomio

$$f(x) = x^3 + x - 3,$$

su derivada es $f'(x) = 3x^2 + 1$, obsérvese que $f'(x) > 0 \ \forall\ x \in \mathbb{R}$, también el mínimo de $f'(x)$ es 1 en $x = 0$ (véase la Figura 4.3).

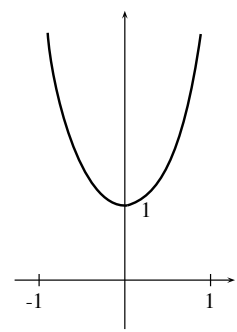


Figura 4.3: Gráfica de $f'(x) = 3x^2 + 1$

Es decir, la gráfica de $f(x) = x^3 + x - 3$ es creciente, además la derivada decrece a 1 en 0 para luego crecer, *i.e.*, 0 es un punto de inflexión. También $f(1) = -1$ y $f(2) = 7$, por lo que f tiene una única raíz real en el intervalo (1,2) (véase la Figura 4.4).

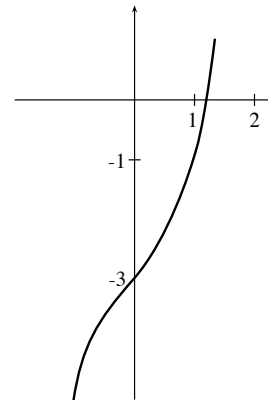


Figura 4.4: Gráfica de $f(x) = x^3 + x - 3$

EJERCICIOS 4.4

1. Encuentre las raíces de $x^6 - 1 = 0$.

2. Exprese $x^8 - 1$ como producto de polinomios con coeficientes reales.

3. Demuestre que si $f(x) \mid g(x)$, entonces la raíces de $f(x)$ también lo son de $g(x)$.

4. Demuestre que si $f(x) \neq 0$ y a, b, c son raíces distintas de $f(x)$, entonces $\text{gr}\,(f(x)) \geqslant 3$.

5. Sean $f(x)$ y $g(x)$ polinomios tales que $(x - a) \mid f(x)$ y $(x - a) \nmid g(x)$. Demuestre que $(x - a) \nmid f(x) + g(x)$.

6. Si $f(z) = z^3 + 2z^2 - z - 2$. Determine los números $z \in \mathbb{C}$ tales que $f(z) = 0$.

4.5. Polinomios de grado 2

Sea

$$f(z) = az^2 + bz + c,\ a, b, c \in \mathbb{C}, \quad a \neq 0,$$

se quiera factorizar $f(z)$ y encontrar sus raíces, completando cuadrados se tiene

$$az^2 + bz + c = a\left[z^2 + \frac{b}{a}z + \frac{c}{a}\right]$$

$$= a\left[z^2 + 2\,\frac{b}{2a}z + \left(\frac{b}{2a}\right)^2 + \frac{c}{a} - \left(\frac{b}{2a}\right)^2\right]$$

$$= a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right]. \tag{4.1}$$

Denotamos

$$\alpha = \frac{b^2 - 4ac}{4a^2}$$

Si $b^2 = 4ac$, entonces $\alpha = 0$, y

$$f(z) = a\left(z + \frac{b}{2a}\right)^2.$$

Si $b^2 \neq 4ac$, entonces , $\alpha \neq 0$. Tomando $\sqrt{\alpha}$ una raíz cuadrada de α, $-\sqrt{\alpha}$ es la otra, y se sigue de (4.1) que

$$f(z) = a\left(z + \frac{b}{2a} - \sqrt{\alpha}\right)\left(z + \frac{b}{2a} + \sqrt{\alpha}\right),$$

tomando $z_1 = -(b/2a) + \sqrt{\alpha}$ y $z_2 = -(b/2a) - \sqrt{\alpha}$ se tiene

$$f(z) = a(z - z_1)(z - z_2),$$

por lo que z_1, z_2 son las raíces de $f(z)$. Nótese que si β es una raíz de $f(z)$, entonces $(z - \beta) \mid f(z)$ y se sigue del Corolario 4.4.5 que $\beta = z_1$ o $\beta = z_2$.

Obsérvese que

$$z_1 = -\frac{b}{2a} + \sqrt{\frac{b^2 - 4ac}{4a^2}} = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

y

$$z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

donde $\sqrt{b^2 - 4ac}$ es cualquier raíz de $b^2 - 4ac$.

Ejemplo. Factorizamos $z^2 + i$.

En este caso tenemos $b = 0$, $a = 1$ y $c = i$, por lo que $b^2 - 4ac = -4i$. Por lo cual

$$z_1 = \frac{\sqrt{-4i}}{2} = \sqrt{-i} = \cos\frac{3\pi}{4} + i\,\mathrm{sen}\,\frac{3\pi}{4} \quad \text{y} \quad z_2 = -\cos\frac{3\pi}{4} - i\,\mathrm{sen}\,\frac{3\pi}{4}.$$

Si $\beta = \cos(3\pi/4) + i\,\mathrm{sen}(3\pi/4)$, entonces $z^2 + i = (z - \beta)(z + \beta)$.

EJERCICIOS 4.5

1. Encuentre un polinomio de grado 4 con coeficientes reales que no tenga ninguna raíz real.

2. Sea $f(x) = ax^2 + bx + c$ un polinomio de grado 2 con coeficientes reales, recordamos que el discriminante Δ de $f(x)$ es $\Delta = b^2 - 4ac$. Demuestre que:

i) $f(x)$ tiene dos raíces reales distintas, si $\Delta > 0$.

ii) $f(x)$ tiene dos raíces reales iguales, si $\Delta = 0$.

iii) $f(x)$ tiene dos raíces complejas no reales, que son conjugadas entre sí, si $\Delta < 0$.

4.6. División sintética

El proceso de dividir un polinomio por un divisor de la forma $x - a$ se puede simplificar sustancialmente. Este proceso permite también obtener una expresión para polinomios de la forma $\sum a_i(x-a)^i$.

Veamos el siguiente ejemplo, dividimos $4x^4 - 3x^3 + 2x^2 - x + 1$ entre $x + 1$.

$$
\begin{array}{rrcrrcr}
4x^4 & -3x^3 & + & 2x^2 & -x & + & 1 \\
-4x^4 & -4x^3 & & & & & \\
\hline
 & -7x^3 & + & 2x^2 & -x & + & 1 \\
 & 7x^3 & + & 7x^2 & & & \\
\hline
 & & & 9x^2 & -x & + & 1 \\
 & & & -9x^2 & -9x & & \\
\hline
 & & & & -10x & + & 1 \\
 & & & & 10x & + & 10 \\
\hline
 & & & & & & 11
\end{array}
\qquad
\begin{array}{r|l}
 & x + 1 \\
\hline
 & 4x^3 - 7x^2 + 9x - 10
\end{array}
$$

Este proceso se puede escribir de manera más esquemática.

$$\begin{array}{ccccc|l} 4 & -3 & 2 & -1 & 1 & -1 \\ & -4 & & & & \hline \\ \hline & -7 & & & & 4-7+9-10 \\ & & 7 & & & \\ \hline & & 9 & & & \\ & & & -9 & & \\ \hline & & & -10 & & \\ & & & & 10 & \\ \hline & & & & 11 & \end{array}$$

Obsérvese que los coeficientes del cociente son el 1er número del 1er renglón y los números que aparecen debajo de las rayas horizontales, exceptuando el último, que es el residuo. Los números arriba de las líneas horizontales, se obtienen al multiplicar a (en el ejemplo $a = -1$) por los coeficientes del cociente. Obsérvese también que los números debajo de las líneas horizontales se obtienen sumando los números de arriba.

Sintetizando aún más, se escribe simplemente

$$\begin{array}{ccccc|l} 4 & -3 & 2 & -1 & 1 & -1 \\ & -4 & 7 & -9 & 10 & \hline \\ \hline 4 & -7 & 9 & -10 & 11 & \end{array}$$

Obteniéndose un algoritmo muy simple: bajar 4 debajo de la raya, multiplicarlo por -1 y ponerlo arriba de la raya, sumar y el resultado es el siguiente coeficiente del cociente. Posteriormente, multiplicar este número por -1 y ponerlo arriba de la raya en la siguiente columna, etcétera.

Veamos otro ejemplo:

$$\begin{array}{cccccc|l} 1 & 1 & 2 & 3 & 5 & -6 & 2 \\ & 2 & 6 & 16 & 38 & 86 & \hline \\ \hline 1 & 3 & 8 & 19 & 43 & 80 & \end{array}$$

por lo cual

$$x^5 + x^4 + 2x^3 + 3x^2 + 5x - 6 = (x^4 + 3x^3 + 8x^2 + 19x + 43)(x - 2) + 80.$$

A este rápido algoritmo se le llama división sintética. A continuación observamos que este método permite expresar rápidamente un polinomio de la forma $\sum a_i(x-a)^i$.

Si $f(x)$ es un polinomio de grado n y $a \in \mathbb{C}$, entonces

$$\begin{aligned} f(x) &= (x-a)f_1(x) + b_0 \\ f_1(x) &= (x-a)f_2(x) + b_1 \\ &\vdots \\ f_{n-1}(x) &= (x-a)f_n(x) + b_{n-1}, \end{aligned}$$

como el grado de $f_i(x)$ es $n-i$, $f_n(x)$ es de grado 0 (o $-\infty$), *i.e.*, $f_n(x) \in \mathbb{C}$, se puede escribir como $f_n(x) = b_n$ y se tiene

$$\begin{aligned} f(x) &= b_0 + f_1(x)(x-a) \\ &= b_0 + b_1(x-a) + f_2(x)(x-a)^2 \\ &= b_0 + b_1(x-a) + b_2(x-a)^2 + f_3(x)(x-a)^3 \\ &\vdots \\ &= b_0 + b_1(x-a) + b_2(x-a)^2 + b_3(x-a)^3 + \cdots + b_n(x-a)^n, \end{aligned}$$

obteniéndose

$$f(x) = \sum_{i=0}^{n} b_i(x-a)^i,$$

donde b_0 es el residuo de $f(x)$ al dividirlo por $x-a$, b_1 es el residuo de $f_1(x)$ al dividirlo por $x-a$, etcétera. Usando la división sintética se obtienen rápidamente los b_i : por ejemplo, si se quiere expresar $x^4+3x^3+x^2-2x-1$ en la forma $\sum a_i(x+2)^i$, hacemos lo siguiente:

$$\begin{array}{rcrrrrrl} f(x) & \longrightarrow & 1 & 3 & 1 & -2 & -1 & \big| \, -2 \\ & & & -2 & -2 & 2 & 0 & \\ \cline{3-7} f_1(x) & \longrightarrow & 1 & 1 & -1 & 0 & \big| \; -1 & \\ & & & -2 & 2 & -2 & & \\ \cline{3-6} f_2(x) & \longrightarrow & 1 & -1 & 1 & \big| \; -2 & & \\ & & & -2 & 6 & & & \\ \cline{3-5} f_3(x) & \longrightarrow & 1 & -3 & \big| \; 7 & & & \\ & & & -2 & & & & \\ \cline{3-4} f_4(x) & \longrightarrow & 1 & \big| \; -5 & & & & \end{array}$$

y se tiene

$$\begin{aligned} &x^4+3x^3+x^2-2x-1 \\ &= (x+2)^4 - 5(x+2)^3 + 7(x+2)^2 - 2(x+2) - 1, \end{aligned}$$

obsérvese que el coeficiente del término de grado máximo coincide con el correspondiente en $\sum(x-a)^i$.

EJERCICIOS 4.6

1. Muestre que $2x^7 - 3x^5 + 2x^4 - x^3 + 7x - 2$ no tiene raíces racionales.

2. Aproxime la raíz real de $f(x) = x^3 + x - 3$ con una aproximación de una centésima usando el método de Newton.

3. Encuentre la expresión de $x^3 - 2x^2 + x + 2$ en la forma $\sum_{i=0}^{3} b_i(x-1)^i$.

4.7. Aproximaciones a raíces en polinomios reales

Se sigue del teorema del valor intermedio que si $f(x)$ es un polinomio real, tal que $f(a) < 0$ y $f(b) > 0$, donde $a < b$, entonces existe $c \in [a, b]$, tal que $f(c) = 0$.

Bisectando iteradamente el intervalo $[a, b]$ se puede aproximar la raíz (eligiendo el intervalo donde se cambia el signo). Sin embargo este método no es eficiente, por ejemplo, si $a = 3,\ b = 7$ y se quiere aproximar con milésimas a un punto en el intervalo, el número n de etapas debe cumplir

$$\frac{7-3}{2^n} \leqslant .001, \qquad i.e., \quad 4 < \frac{2^n}{1000},$$

o

$$4000 < 2^n, \qquad i.e. \quad n > \frac{\log 4000}{\log 2} \sim \frac{8.3}{.7} \sim 12.$$

Ciertamente el método de Newton es uno de los más eficientes, como ya se ha ilustrado.

Otro método interesante desde el punto de vista teórico es el de Horner. Esencialmente este método consiste en ir trasladando sucesivamente el problema a intervalos con un extremo en el origen. Sea

$$\alpha = A.a_1a_2a_3\ldots,$$

una raíz aislada de un polinomio $f(x)$ en el intervalo $[A, A+1]$, $A \in \mathbb{N} \cup \{0\}$, el algoritmo es el siguiente.

1. Se expresa $f(x) = \sum_j a_{0,j}(x-A)^j$, mediante la división sintética iterada, y se define

$$f_0(x) = \sum_j a_{0,j}\, x^j,$$

obsérvese que

$$f(x) = f_0(x - A), \tag{4.2}$$

es decir, el valor de f_0 en el "traslado" de x al intervalo $(0, 1)$ es el mismo del valor de f en x (véase la Figura 4.5).

Nótese que para encontrar el primer decimal de α, *i.e.*, a_1, hay que checar que $f(A.a_1)$ y $f(A.a_1^*)$ tienen signo distinto, donde $a_1^* = a_1 + 1$, y para esto basta checar que $f_0(.a_1)$ y $f_0(.a_1^*)$ lo tienen. Esto se sigue ya que usando (4.2)

$$f_0(.t) = f_0(A.t - A) = f(A.t).$$

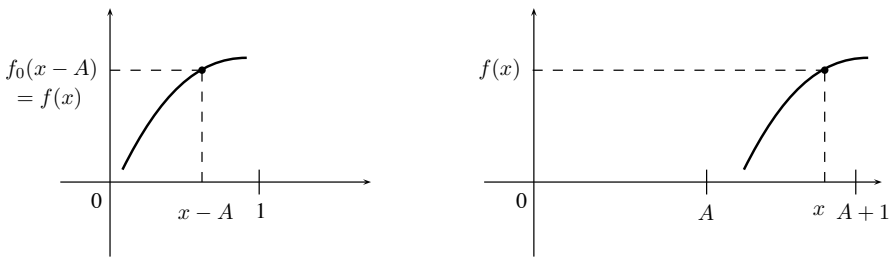


Figura 4.5: Método de Horner

2. Se calcula $f_0(.1), f_0(.2), \ldots$ etcétera, para obtener el cambio de signo, obteniéndose a_1. Lo cual se puede hacer rápidamente encontrando el residuo al dividir por $x - .t$ (usando división sintética).

3. Se define $f_i(x)$ inductivamente, si

$$f(x) = f_{i-1}(x - A.a_1a_2 \ldots a_{i-1}),$$

(como en (4.2)), habiendo encontrado el valor a_i y se expresa

$$f_{i-1}(x) = \sum_j a_{i,j}(x - 10^{-i}a_i)^j,$$

y se define

$$f_i(x) = \sum_j a_{i,j}x^j.$$

Obsérvese que

$$f_{i-1}(x) = f_i(x - 10^{-i}a_i).$$

Se tiene entonces que

$$\begin{aligned} f(x) &= f_{i-1}(x - A.a_1a_2\cdots a_{i-1}) \\ &= f_i(x - A.a_1a_2\cdots a_{i-1} - 10^{-i}a_i) \\ &= f_i(x - A.a_1a_2\ldots a_i). \end{aligned} \tag{4.3}$$

4. El siguiente paso es calcular a_{i+1}, para lo que basta calcular el polinomio f_i en $t \times 10^{-(i+1)}$, donde $t \in \{0, 1, \ldots, 9\}$, ya que

$$f(A.a_1a_2\cdots a_it) = f_i(A.a_1, \cdots a_it - A.a_1a_2\cdots a_i) = f_i(t \times 10^{-(i+1)}),$$

usando (4.3).

Es posible que en algún momento se encuentre la raíz exacta. El método también se aplica si $\alpha \in (-(A+1), -A),\ A \in \mathbb{N} \cup \{0\}$ y

$$\alpha = -A.a_1a_2\ldots.$$

Para esto es necesario anteponer el signo menos a $A, A.a_1, \ldots, A.a_1a_2\ldots a_i$ y a $t \times 10^{-i}$ en el método (por ejemplo al dividir sintéticamente por el divisor $x - (-.1) = x + .1$ se escribe $-,1$).

Consideremos el mismo ejemplo de la sección 4.4,

$$f(x) = x^3 + x - 3,$$

como se mostró hay una sola raíz en el intervalo $(1, 2)$. A continuación se calcula $f_0(x)$.

1	0	1	−3	| 1
	1	1	2	
1	1	2	−1	
	1	2		
1	2	4		
	1			
1	3 .			

Por lo tanto

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

y

$$f_0(x) = x^3 + 3x^2 + 4x - 1.$$

Calculamos ahora a_1, el residuo de $f_0(x)$ al dividir por $x - .t$ es $f_0(.t)$ (teorema del residuo).

$$\begin{array}{cccc|l} 1 & 3 & 4 & -1 & \vert\ .1 \\ & .1 & .31 & .431 & \\ \hline 1 & 3.1 & 4.31 & -.569 & < 0 \end{array}$$

$$\begin{array}{cccc|l} 1 & 3 & 4 & -1 & \vert\ .2 \\ & .2 & .64 & .928 & \\ \hline 1 & 3.2 & 4.64 & -.072 & < 0 \end{array}$$

$$\begin{array}{cccc|l} 1 & 3 & 4 & -1 & \vert\ .3 \\ & .3 & .99 & 1.497 & \\ \hline 1 & 3.3 & 4.99 & .497 & > 0. \end{array}$$

Por lo tanto $a_1 = 2$.

Ahora se calcula $f_1(x)$:

$$\begin{array}{cccc|l} 1 & 3 & 4 & -1 & \vert\ .2 \\ & .2 & .64 & .928 & \\ \hline 1 & 3.2 & 4.64 & -.072 & \\ & .2 & .68 & & \\ \hline 1 & 3.4 & 5.32 & & \\ & .2 & & & \\ \hline 1 & 3.6, & & & \end{array}$$

de donde

$$f_0(x) = (x - .2)^3 + 3.6(x - .2)^2 + 5.32(x - .2) - .072$$

y

$$f_1(x) = x^3 + 3.6\,x^2 + 5.32\,x - .072.$$

Ahora calculamos a_2 :

$$\begin{array}{cccc|l} 1 & 3.6 & 5.32 & -.072 & \vert\ .01 \\ & .01 & .0361 & .053561 & \\ \hline 1 & 3.61 & 5.3561 & -.018439 & < 0 \end{array}$$

1	3.6	5.32	$-.072$	$\vert$ .02
	.02	.0724	.107848	
1	3.62	5.3924 $\vert$	.035848	> 0.

Por lo tanto $\alpha = 1.21\cdots$.

En el siguiente ejemplo calculamos las raíces de

$$f(x) = x^3 - 2x^2 + 2.$$

Su derivada es

$$f'(x) = 3x^2 - 4x,$$

cuyos puntos críticos son $x_1 = 0$ y $x_2 = 4/3$. Calculando su segunda derivada tenemos $f''(x) = 6x - 4$, por lo que 0 es un máximo ($f''(0) < 0$) y $4/3$ es un mínimo ($f''(4/3) = 4 > 0$) (véase la Figura 4.6).

Evaluando $f(x)$ en $-1, 0, 4/3$ se tiene

$$f(-1) = -1, \quad f(0) = 2 \quad \text{y} \quad f\left(\frac{4}{3}\right) = 2 - \frac{32}{27} > 0,$$

por lo que la raíz tiene la forma

$$\alpha = -0.a_1a_2\cdots,$$

y $f_0(x) = f(x)$, ya que en este caso $A = 0$. Se calcula a_1.

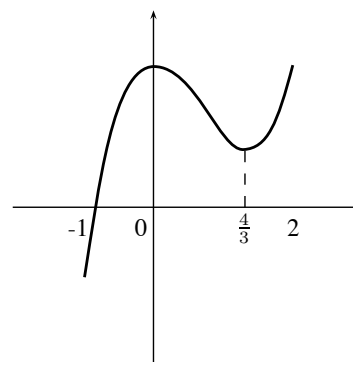


Figura 4.6: Gráfica de $f(x) = x^3 - 2x^2 + 2$

$$\begin{array}{cccc|l} 1 & -2 & 0 & 2 & -.9 \\ & -.9 & 2.61 & -2.349 & \\ \hline 1 & -2.9 & 2.61 & -.349 & \end{array} \quad < 0,$$

$$\begin{array}{cccc|l} 1 & -2 & 0 & 2 & -.8 \\ & -.8 & 2.24 & -1.792 & \\ \hline 1 & -2.8 & 2.24 & .208 & \end{array} \quad > 0,$$

Por lo que $\alpha = -0.8$.

El siguiente paso es calcular $f_1(x)$:

$$\begin{array}{cccc|l} 1 & -2 & 0 & 2 & -.8 \\ & -.8 & 2.24 & -1.792 & \\ \hline 1 & -2.8 & 2.24 & .208 & \\ & -.8 & 2.88 & & \\ \hline 1 & -3.6 & 5.12 & & \\ & -.8 & & & \\ \hline 1 & -4.4 & & & \end{array}$$

de donde

$$f_0(x) = (x + .8)^3 - 4.4(x + .8)^2 + 5.12(x + .8) + .208$$

y

$$f_1(x) = x^3 - 4.4\,x^2 + 5.12\,x + .208,$$

etcétera. Ciertamente, el método de Newton es más eficiente.

EJERCICIOS 4.7

1. Haga una aproximación de una centésima de $\sqrt[n]{3}$, donde $n = 2, 3, 4$, usando el método de Newton y luego el método de Horner.

2. Aproxime las raíces del polinomio $2x^3 + 2x^2 - 1$ con un error de una centésima.

4.8. Factorización de polinomios

Teorema 4.8.1. (Teorema del factorización) *Sea $f(z)$ un polinomio de grado n, $n > 0$ con coeficientes en $\mathbb{C}$, entonces existen k números complejos distintos dos a dos: $z_1, z_2, \ldots, z_k$ tales que*

$$f(z) = b(z - z_1)^{s_1}(z - z_2)^{s_2} \cdots (z - z_k)^{s_k},$$

donde $s_i \in \mathbb{N}\ \forall\ i$ y $b \in \mathbb{C}$. Además, esta descomposición es única salvo permutación de los factores.

Obsérvese que $k \leqslant n$. Veamos 2 ejemplos:

$$x^2 + 1 = (x - i)(x + i),$$

$$x^3 + 2x^2 - 4x - 8 = (x^2 - 4)(x + 2) = (x - 2)(x + 2)^2.$$

Demostración. (Del Teorema 4.8.1) Esencialmente el resultado es consecuencia del teorema fundamental del álgebra.

Existencia

Lo probamos por inducción sobre el grado: si $f(z) = a_1 z + a_0,\ a_1 \neq 0$, entonces $\operatorname{gr}(f(z)) = 1$, y se tiene

$$f(z) = a_1 \left(z - \frac{a_0}{a_1} \right).$$

Suponiendo cierto el resultado para polinomios de grado $n - 1$, por el teorema fundamental del álgebra, existe $\alpha \in \mathbb{C}$, tal que

$$f(\alpha) = 0,$$

y por el Corolario 4.4.3, tenemos que

$$(z - \alpha) \mid f(z),$$

i.e.,

$$f(z) = (z - \alpha)q(z), \tag{4.4}$$

donde $q(z)$ es un polinomio de grado $n - 1$. Por hipótesis de inducción

$$q(z) = b(z - z_1)^{s_1}(z - z_2)^{s_2} \cdots (z - z_k)^{s_k}.$$

Obteniéndose el resultado, al integrar la descomposición de $q(z)$ a la expresión (4.4). Ya sea que $\alpha = z_i$ para alguna i, o que $\alpha \neq z_i\ \forall\ i$.

Unicidad

También la probamos inductivamente sobre el grado de f: si $n = 1$,

$$f(z) = b(z - a) = b'(z - a'),$$

entonces por definición $b = b',\ ba = ba'$, y por lo tanto $a = a'$.

Suponiendo cierto para $n - 1$, si

$$f(z) = b(z - z_1)^{s_1} \cdots (z - z_k)^{s_k} = b'(z - w_1)^{t_1} \cdots (z - w_m)^{t_m},$$

al considerar el coeficiente del término de grado máximo, se tiene que $b = b'$.

Ahora $(z - z_1) \mid f(z)$, por lo que usando el Corolario 4.4.5,

$$(z - z_1) \mid z - w_i,$$

para alguna i, y sin perder generalidad (permutando los factores y renombrando si es necesario) se tiene

$$(z - z_1) \mid z - w_1,$$

i.e., $z_1 = w_1$. Finalmente como el anillo de polinomios es un dominio entero, se obtiene

$$(z - z_1)^{s_1 - 1}(z - z_2)^{s_2} \cdots (z - z_k)^{s_k} = (z - w_1)^{t_1 - 1}(z - w_2)^{t_2} \cdots (z - w_m)^{t_m},$$

que son polinomios de grado $n - 1$, por lo que aplicando la hipótesis de inducción $s_1 - 1 = t_1 - 1$, y salvo una permutación, los factores $(z - z_j)^{s_j}$ son los factores $(z - w_j)^{t_j}$. □

Definición 44. *Sea $f(z)$ un polinomio en $\mathbb{C}[z]$ y α una raíz de $f(z)$, se dice que α es una raíz de multiplicidad m, si $(z-\alpha)^m \mid f(z)$, pero $(z-\alpha)^{m+1} \nmid f(z)$.*

Por ejemplo, si

$$f(z) = (z - 1)^2(z + 2)(z - i)^3,$$

1 es de multiplicidad 2, y i es de multiplicidad 3 ¿por qué?

Proposición 4.8.2. *Sean $f(z)$ y $g(z)$ dos polinomios en $\mathbb{C}[z]$, tales que $f(\alpha) = g(\alpha)\ \forall\ \alpha \in \mathbb{C}$, entonces son iguales como polinomios.*

Demostración. Lo probamos por inducción sobre el menor de los grados. Si $\operatorname{gr}(f(z)) \leqslant 0$, $f(z)$ es constante y $g(z)$ también, por lo que son iguales.

Si $\operatorname{gr}(f(z)) = n$ y z_0 es una raíz de $f(z)$, entonces también lo es de $g(z)$, por lo que

$$f(z) = (z - z_0)h(z),$$

$$g(z) = (z - z_0)h_1(z),$$

y $h(z)$ tiene grado $n-1$, de donde

$$h(\alpha) = h_1(\alpha) \quad \forall\ \alpha \neq z_0.$$

Finalmente se demuestra de manera idéntica que al caso real que los polinomios como funciones de $\mathbb{C}$ en $\mathbb{C}$ son continuas, por lo que si coinciden en $\mathbb{C}$, salvo quizá en un punto, deben coincidir también en dicho punto ($f(x)$ es continua en $x_0 \Leftrightarrow \forall$ sucesión $x_n \to x_0$, $f(x_n) \to f(x_0)$), por lo que

$$h(\alpha) = h_1(\alpha) \quad \forall\ \alpha \in \mathbb{C},$$

y se sigue de la hipótesis de inducción que $h(z)$ y $h_1(z)$ son el mismo polinomio, y en consecuencia $f(z)$ y $g(z)$ también. □

Obsérvese que en la última parte de la demostración se usó variable compleja, pero muy elemental.

EJERCICIOS 4.8

1. Sean $\alpha_1, \alpha_2, \ldots, \alpha_t$ todas las raíces de $f(x)$, $\alpha_i \neq \alpha_j$ si $i \neq j$, y m_i la multiplicidad de α_i. Muestre que

$$m_1 + \cdots + m_t = \operatorname{gr}(f(x)).$$

2. ¿Qué polinomio de grado 4 tiene como raíces a $0, \pi, 2$ y -1?

3. Sean α es raíz de multiplicidad m_i de $f_i(x)$, $i = 1, 2$, y $g_1(x), g_2(x)$ polinomios no nulos cualesquiera. Demuestre que α es raíz de multiplicidad mayor o igual al mínimo de m_1 y m_2, para $f_1(x)g_1(x) + f_2(x)g_2(x)$. Pruébese también que si $m_1 > m_2$, α es raíz de multiplicidad m_2 de $f_1(x) + f_2(x)$.

4. Pruebe que α es raíz de multiplicidad 0 de $f(x)$ si y sólo si α no es raíz de $f(x)$.

5. Suponga que α es raíz de multiplicidad m_i de $g_i(x)$, para $i = 1, 2$. Si

$$f(x) = g_1(x)g_2(x),$$

muestre que α es raíz de multiplicidad $m_1 + m_2$ de $f(x)$.

6. Determine la multiplicidad de 1 como raíz de los siguientes polinomios:

i) $-x^4 + 3x^3 + 2x^2 - 4$,

ii) $3x^4 - x^3 - x - 1$.

7. Demuestre de manera breve la Proposición 4.8.2, observando que $f - g$ no puede ser un polinomio de grado finito, al tener una infinidad de raíces.

4.9. Raíces múltiples, derivadas

A todo polinomio

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n$$

se le asocia otro polinomio que es su derivada

$$f'(z) = a_1 + 2a_2 z + 3a_3 z^2 + \cdots + n a_n z^{n-1}.$$

Obsérvese que si $f(x) \in \mathbb{R}[x]$, $f'(x)$ es como en cálculo, su derivada. Dada la estructura de campo de $\mathbb{C}$, esta situación se generaliza fácilmente a funciones de $\mathbb{C}$ en $\mathbb{C}$. Se pueden discutir ciertas propiedades de la derivada de polinomios en $\mathbb{C}$ sin usar cálculo complejo (derivadas).

Definición 45. *Sea*

$$f(z) = \sum_{k=0}^{\infty} a_k z^k,$$

donde $a_j = 0 \ \forall \ j > N$, *se define la derivada de* $f(z)$ *como el polinomio*

$$f'(z) = \sum_{k=0}^{\infty} (k+1) a_{k+1} z^k.$$

Inductivamente se define también

$$f^{n+1}(z) = (f^n)'(z).$$

Probamos ahora, sin usar cálculo, la regla de Leibnitz.

Proposición 4.9.1. *Si* $f(z) = g(z)h(z)$, *entonces*

$$f'(z) = g'(z)h(z) + g(z)h'(z).$$

Obsérvese que el cálculo real no es suficiente para probar esta identidad, sin embargo, los mismos métodos que muestran este hecho en cálculo real, se aplican al caso complejo.

Demostración. (De la Proposición 4.9.1) Dada $z \in \mathbb{C}$,

$$g(z) = \sum_{i=0}^{\infty} a_i z^i \quad \text{y} \quad h(z) = \sum_{j=0}^{\infty} b_j z^j,$$

se sigue de la definición del producto que

$$f(z) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) z^k = \sum_{k=0}^{\infty} c_k z^k.$$

Ahora

$$f'(z) = \sum_{k=0}^{\infty}(k+1)c_{k+1}z^k = \sum_{k=0}^{\infty}\left((k+1)\sum_{i+j=k+1}a_ib_j\right)z^k. \qquad (4.5)$$

También

$$g'(z) = \sum_{k=0}^{\infty}(k+1)a_{k+1}z^k = \sum_{k=0}^{\infty}a'_kz^k,$$

donde $a'_k = (k+1)a_{k+1}\ \forall\ k$, análogamente

$$h'(z) = \sum_{k=0}^{\infty}b'_kz^k,$$

donde $b'_k = (k+1)b_{k+1}\ \forall\ k$.

Bajo esta notación

$$\begin{aligned} g(z)h'(z) &= \sum_{k=0}^{\infty}\left(\sum_{i+j=k}a_ib'_j\right)z^k = \sum_{k=0}^{\infty}\left(\sum_{i+j=k}(j+1)a_ib_{j+1}\right)z^k \\ &= \sum_{k=0}^{\infty}\left(\sum_{i+s-1=k}sa_ib_s\right)z^k = \sum_{k=0}^{\infty}\left(\sum_{i+s=k+1}sa_ib_s\right)z^k, \end{aligned}$$

donde $s = j+1$.

Invirtiendo los papeles de $g(z)$ y $h(z)$, se tiene también

$$h(z)g'(z) = \sum_{k=0}^{\infty}\left(\sum_{i+s=k+1}ia_ib_s\right)z^k.$$

Finalmente, usando (4.5) se tiene que

$$\begin{aligned} g(z)h'(z) + g'(z)h(z) &= \sum_{k=0}^{\infty}\left(\sum_{i+s=k+1}(i+s)a_ib_s\right)z^k \\ &= \sum_{k=0}^{\infty}\left(\sum_{i+s=k+1}(k+1)a_ib_s\right)z^k = f'(z). \end{aligned}$$

□

Corolario 4.9.2. *Si* $f(z) = [g(z)]^m$, *entonces*

$$f'(z) = m[g(z)]^{m-1}g'(z),$$

donde $f(z), g(z) \in \mathbb{C}[z]$.

Demostración. Por inducción, si $m = 1$, no hay nada que probar.

Suponiendo cierto para $m-1$ y usando la Proposición 4.9.1, como

$$f(z) = [g(z)]^{m-1} g(z),$$

se sigue que

$$\begin{aligned} f'(z) &= (m-1)[g(z)]^{m-2} g'(z) g(z) + g'(z)[g(z)]^{m-1} \\ &= [g(z)]^{m-1} g'(z)[m-1+1] = m[g(z)]^{m-1} g'(z). \end{aligned}$$

□

Lema 4.9.3. *Si α es raíz de multiplicidad m de $f(z)$, entonces α es raíz de multiplicidad $m-1$ de $f'(z)$.*

Demostración. Se tiene $f(z) = (z-\alpha)^m g(z)$, donde $(z-\alpha) \nmid g(z)$. Ahora

$$f'(z) = m(z-\alpha)^{m-1} g(z) + (z-\alpha)^m g'(z) = (z-\alpha)^{m-1}[m\, g(z) + (z-\alpha) g'(z)],$$

como $z-\alpha$ no es factor de

$$m\, g(z) + (z-\alpha) g'(z),$$

α es raíz de multiplicidad $m-1$ de $f'(z)$. □

Establecemos ahora condiciones para encontrar la multiplicidad de las raíces.

Teorema 4.9.4. *Sea $f(z)$ un polinomio de grado positivo y $m \in \mathbb{N}$, entonces α es una raíz de multiplicidad m de $f(z)$ si y sólo si se cumplen las siguientes 2 condiciones:*

a) $f(\alpha) = f'(\alpha) = \cdots = f^{m-1}(\alpha) = 0$,

b) $f^m(\alpha) \neq 0$.

Por ejemplo, si $f(z) = z^5$, entonces 0 es una raíz de multiplicidad 5, ya que $f'(0) = f^2(0) = f^3(0) = f^4(0) = 0$, pero $f^5(0) \neq 0$:

$$\begin{aligned} f'(z) &= 5z^4, \\ f^2(z) &= 5 \cdot 4z^3, \\ f^3(z) &= 5 \cdot 4 \cdot 3z^2, \\ f^4(z) &= 5!z, \\ f^5(z) &= 5!. \end{aligned}$$

Demostración. (Del Teorema 4.9.4) $\Rightarrow$) Hacemos inducción sobre la multiplicidad. Si α es de multiplicidad 1 de $f(z)$, se sigue del Lema 4.9.3 que tiene multiplicidad 0 para $f'(z)$, por lo que

$$f(\alpha) = 0 \quad \text{y} \quad f'(\alpha) \neq 0$$

(si α es de multiplicidad 0 para $f'(z)$, entonces $(z-\alpha) \nmid f'(z)$ y $f'(\alpha) \neq 0$).

Suponiendo cierto para raíces de multiplicidad m, sea α raíz de multiplicidad $m+1$ en $f(z)$, entonces por el Lema 4.9.3, α es de multiplicidad m de $f'(z)$ y por hipótesis de inducción

$$f'(\alpha) = f^2(\alpha) = \cdots = f^m(\alpha) = 0,$$

pero $f^{m+1}(\alpha) \neq 0$, como $f(\alpha) = 0$, se sigue el resultado.

$\Leftarrow$) Inducción sobre el número m definido por a) y b).

Si $m = 1$, $f(\alpha) = 0$ y $f'(\alpha) \neq 0$, entonces

$$(z-\alpha) \mid f(z),$$

pero α no es raíz de $f'(z)$, por lo que α es de multiplicidad 1 (usando de nuevo el lema).

Suponiendo cierto para m, probamos para $m+1$. Sea $f(z) \in \mathbb{C}[z]$ tal que

$$f(\alpha) = f'(\alpha) = \cdots = f^m(\alpha) = 0$$

y

$$f^{m+1}(\alpha) \neq 0,$$

entonces (por hipótesis de inducción) α es de multiplicidad m de $f'(z)$, por lo que es de multiplicidad $m+1$ de $f(z)$. □

En algunos casos de raíces de multiplicidad mayor a 1, derivando se pueden encontrar las ceros de los polinomios, por ejemplo, si

$$\begin{aligned} f(z) &= z^4 - 3z^3 - 6z^2 + 28z - 24, \\ f'(z) &= 4z^3 - 9z^2 - 12z + 28 \\ \text{y} \quad f''(z) &= 12z^2 - 18z - 12. \end{aligned}$$

Las raíces de $f''(z)$ son las de $2x^2 - 3x - 2 = 0$, éstas son

$$\frac{3 \pm \sqrt{9+16}}{4} = 2, -\frac{1}{2}.$$

También, $f(2) = 0$, ya que

$$\begin{array}{ccccc|c} 1 & -3 & -6 & 28 & -24 & 2 \\ & 2 & -2 & -16 & 24 & \\ \hline 1 & -1 & -8 & 12 & 0 & \end{array}$$

y como

$$\begin{array}{cccc|c} 4 & -9 & -12 & 28 & 2 \\ & 8 & -2 & -28 & \\ \hline 4 & -1 & -14 & 0 & \end{array}$$

$f'(2) = 0$.

Ahora $f^3(z) = 24x - 18$ y $f^3(2) \neq 0$, por lo que se sigue del Corolario 4.4.3 que 2 es una raíz de multiplicidad 3 y

$$(z-2)^3 \mid f(z).$$

EJERCICIOS 4.9

1. Determine la otra raíz de $f(z) = z^4 - 3z^3 - 6z^2 + 28z - 24$, y escriba su factorización. Sugerencia: usar división sintética iterada.

2. Factorice $f(x) = x^5 - 4x^4 + 4x^3 + 2x^2 - 5x + 2$.

3. Muestre que las únicas raíces de $x^4 - 2ix^3 - 2ix - 1$ son i y $-i$.

4. Demuestre que $2x^5 - 3x^4 + 1$ no tiene ninguna raíz de multiplicidad 4.

4.10. Coeficientes, raíces y polinomios simétricos

Definición 46. *A un polinomio se le llama mónico si el coeficiente del término de grado máximo es 1.*

Por ejemplo $f(x) = x^5 - 2x^2 + 1$. Es importante relacionar los coeficientes de un polinomio con sus raíces. Por ejemplo, en un polinomio mónico de grado 3 con raíces $\alpha_1, \alpha_2, \alpha_3$, no necesariamente distintas, se tiene

$$\begin{aligned} (z-\alpha_1)(z-\alpha_2)(z-\alpha_3) &= z^3 + a_1 z^2 + a_2 z + a_3 \\ &= z^3 + (-\alpha_1 - \alpha_2 - \alpha_3) z^2 \\ &\quad + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) z - \alpha_1\alpha_2\alpha_3. \end{aligned}$$

En consecuencia

$$\begin{aligned} a_1 &= -\alpha_1 - \alpha_2 - \alpha_3, \\ a_2 &= \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3, \\ a_3 &= -\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Esta situación es válida para cualquier polinomio como se muestra en el siguiente teorema. Las relaciones obtenidas (4.6) se les conoce como ecuaciones de Vieta.

Teorema 4.10.1. *Sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de un polinomio mónico contadas con su multiplicidad, entonces si*

$$f(z) = z^n + a_1 z^{n-1} + \cdots + a_n = (z - \alpha_1)\cdots(z - \alpha_n),$$

se tiene

$$a_i = \sum_{1 \leqslant r_1 < \cdots < r_i \leqslant n} \left(\prod_{j=1}^{i} (-\alpha_{r_j}) \right), \tag{4.6}$$

donde la suma es tomada de tal manera que para toda colección de i naturales distintos $r_1, r_2, \ldots, r_i$ menores a n, aparece el sumando

$$\prod_{j=1}^{i} (-\alpha_{r_j}) = (-\alpha_{r_1})(-\alpha_{r_2})\cdots(-\alpha_{r_i}), \quad \textit{correspondiente a } r_1, \ldots, r_i.$$

Demostración. (Del Teorema 4.10.1)

Al efectuar todos los productos en

$$(z - \alpha_1)(z - \alpha_2)\cdots(z - \alpha_n),$$

los términos de grado $n-i$ son precisamente aquéllos obtenidos al multiplicar i números de la forma

$$(-\alpha_{r_1}), (-\alpha_{r_2}), \ldots, (-\alpha_{r_i}),$$

(donde $1 \leqslant r_1 < r_2 < \cdots < r_i \leqslant n$), por $n - i$ indeterminadas z. □

Obsérvese que el número de sumandos que definen el coeficiente a_i (del término de grado $n - i$) es C_n^i. En el ejemplo, previo al teorema se tiene $C_3^1 = 3,\ C_3^2 = 3,\ C_3^3 = 1$.

Nótese que en la discusión en el teorema anterior se considera una raíz de multiplicidad k, como k raíces, por ejemplo

$$\begin{aligned} (z-2)^2 &= z^2 - 4z + 4 = (z-2)(z-2) \\ &= z^2 + (-2-2)z + (-2)(-2) \end{aligned}$$

o

$$(z-2)^3 = z^3 + (-2-2-2)z^2 +$$

$$[(-2)(-2)+(-2)(-2)+(-2)(-2)]z + (-2)(-2)(-2).$$

Los coeficientes de los polinomios expresados en términos de raíces tienen propiedades interesantes.

Teorema 4.10.2. *Sean $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$ números complejos,*

$$a_{n,i} = \sum_{1 \leqslant r_1 < \cdots < r_i \leqslant n} \left(\prod_{j=1}^{i} -\alpha_{r_j} \right) \qquad y \qquad s_{n,i} = \sum_{j=1}^{n} \alpha_j^i,$$

donde $i \leqslant n$, $i, n \in \mathbb{N}$, entonces

a) $a_{n,1} + s_{n,1} = 0 \quad \forall\ n \geqslant 1.$

b) $2a_{n,2} + a_{n,1}s_{n,1} + s_{n,2} = 0 \quad \forall\ n \geqslant 2.$

c) $3a_{n,3} + a_{n,2}s_{n,1} + a_{n,1}s_{n,2} + s_{n,3} = 0 \quad \forall\ n \geqslant 3.$

Demostración. Obsérvese que $\forall\ n$ $a_{n,i}$ y $s_{n,i}$ se pueden pensar también como polinomios simétricos en n variables (*i.e.*, no varían los valores de la función al permutar el orden de las α_i).

a)

$$\sum_{i=1}^{n}(-\alpha_i) + \sum_{j=1}^{n}\alpha_j = 0.$$

b) Por ejemplo, si $n = 3$ se tiene

$$2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_3\alpha_2) + (\alpha_1 + \alpha_2 + \alpha_3)(-\alpha_1 - \alpha_2 - \alpha_3)$$

$$+\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0.$$

En general

$$2\sum_{1 \leqslant r_1 < r_2 \leqslant n} (-\alpha_{r_1})(-\alpha_{r_2}) + \left(-\sum_{i=1}^{n}\alpha_i\right)\left(\sum_{i=1}^{n}\alpha_i\right) + \sum_{i=1}^{n}\alpha_i^2 = 0,$$

ya que en el segundo término los productos $\alpha_i\alpha_j$, donde $i \neq j$, aparecen 2 veces y se cancelan todos con los del primer término. Se generan también cuadrados que se cancelan con el último término.

c)

$$3\sum_{1\leqslant r_1<r_2<r_3\leqslant n}\left(\prod_{j=1}^{3}(-\alpha_{r_j})\right)+\left(\sum_{1\leqslant r_1<r_2\leqslant n}(-\alpha_{r_1})(-\alpha_{r_2})\right)[\alpha_1+\alpha_2+\cdots+\alpha_n]$$

$$-(\alpha_1+\cdots+\alpha_n)(\alpha_1^2+\cdots+\alpha_n^2)+(\alpha_1^3+\cdots+\alpha_n^3)=0.$$

El primer *término* se puede interpretar como 3 veces la suma de los coeficientes de los términos de grado $n-3$ (*i.e.*, suma de todos los productos de la forma $(-\alpha_i)(-\alpha_j)(-\alpha_k)$, i,j,k distintos).

El segundo *término* contiene de nuevo todos estos coeficientes repetidos 3 veces por lo que se cancelan, pero también aparecen sumandos de la forma $\alpha_i^2\alpha_j$ $i\neq j$, los cuales se cancelan con los del tercer *término,* con excepción de los sumandos $-(\alpha_i)^3$ del tercer *término* que se cancelan con la expresión del cuarto *término.* □

EJERCICIOS 4.10

1. Demuestre el Teorema 4.10.1 para el caso $n=2$ usando la fórmula de las raíces de la ecuación cuadrática.

2. Bajo la notación del Teorema 4.10.2, exprese $a_{2,1}$ y $a_{2,2}$ en términos de $s_{2,1}$ y $s_{2,2}$, y viceversa.

3. Exprese $a_{3,1}, a_{3,2}$ y $a_{3,3}$ en términos de $s_{3,1}, s_{3,2}$ y $s_{3,3}$, y viceversa.

4. Demuestre el Teorema 4.10.2 cuando $n=2$ y $n=3$.

5. Si $f(x)=x^2+bx+c$, demuestre que $(\alpha_1-\alpha_2)(\alpha_2-\alpha_1)=4c-b^2$, donde α_1,α_2 son sus raíces,

4.11. Factorización en polinomios reales

Teorema 4.11.1. *Sea $f(x)\in\mathbb{R}[x]$, entonces f se puede factorizar como el producto de una constante por polinomios mónicos de grados 1 y 2, en algunos casos los polinomios de grado 2 no se pueden descomponer en polinomios reales de grado 1.*

Demostración. Se sigue del teorema de factorización que

$$f(x)=b(x-\alpha_1)^{t_1}(x-\alpha_2)^{t_2}\cdots(x-\alpha_k)^{t_k},$$

$b\in\mathbb{R}$, ya que es el coeficiente del término de grado máximo. Ahora se sigue del Teorema 4.4.6 que si $\alpha\notin\mathbb{R}$ y $f(\alpha)=0$, entonces $f(\overline{\alpha})=0$, por lo que

en la descomposición de $f(x)$ aparecen los factores $(x-\alpha)$ y $(x-\overline{\alpha})$. Ahora, como

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - \alpha x - \overline{\alpha}x + |\alpha|^2 = x^2 - 2\,\mathrm{Re}\,(\alpha)x + |\alpha|^2,$$

es un polinomio en $\mathbb{R}[x]$, se pueden remplazar todas las raíces complejas para formar polinomios reales de grado 2. Las potencias son iguales. Esto se prueba por inducción, dividiendo $f(x)$ entre $x^2 - 2\,\mathrm{Re}\,(\alpha)x + |\alpha|^2$ se obtiene un polinomio real, etcétera. □

Ejemplo

$$x^3 - 1 = (x-1)(x-w)(x-w^2),$$

donde $w = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$ y $w^2 = \overline{w}$, por lo que

$$x^3-1 = (x-1)(x-w)(x-\overline{w}) = (x-1)(x^2-2\,\mathrm{Re}\,(w)x+|w|^2) = (x-1)(x^2+x+1).$$

Definición 47. *Dado* $f(z) \in \mathbb{C}[z]$, $f(z) = a_0z^n + \cdots + a_n$, *se define su conjugado* $\overline{f}(z) = \overline{a}_0z^n + \cdots + \overline{a}_n$.

Proposición 4.11.2. *Sean* $f(z), g(z), h(z) \in \mathbb{C}[z]$. *Entonces,*

a) si $f(z) = g(z)h(z)$, *se tiene que* $\overline{f}(z) = \overline{g}(z)\overline{h}(z)$,

b) si $g(z) \mid f(z)$, *se tiene que* $\overline{g}(z) \mid \overline{f}(z)$,

c) si $f(x) \in \mathbb{R}[x]$, *se tiene que*

$$g(x) \mid f(x) \Longleftrightarrow \overline{g}(x) \mid f(x),$$

en particular

$$(x-\alpha)^m \mid f(x) \Longleftrightarrow (x-\overline{\alpha})^m \mid f(x).$$

Demostración.

a) Si

$$g(z) = \sum_{i=1}^{n} a_iz^i \quad \text{y} \quad h(z) = \sum_{i=1}^{n} b_iz^i,$$

el coeficiente del término de grado k de f está dado por

$$\sum_{i+j=k} a_ib_j,$$

y el de $\overline{f}$ por

$$\overline{\left(\sum_{i+j=k} a_i b_j\right)} = \sum_{i+j=k} \overline{a}_i \overline{b}_j.$$

b) Si $f(z) = g(z)h(z)$, se sigue de *a*) que $\overline{f}(z) = \overline{g}(z)\overline{h}(z)$.

c) Como $f(x) \in \mathbb{R}[x]$, usando a) se tiene que $f(x) = g(x)h(x)$ si y sólo si $\overline{f}(x) = f(x) = \overline{g}(x)\overline{h}(x)$. □

EJERCICIOS 4.11

1. Factorice $x^4 + 16$ y $x^6 + 1$ como productos de polinomios con coeficientes reales de grado 1 y 2. Encuentre también la factorización en productos de polinomios de grado 1, algunos complejos.

2. Demuestre que $1/4(-1 + \sqrt{5} + \sqrt{10 + 2\sqrt{5}}\ i)$ es una raíz quinta de la unidad. Sugerencia: factorice $x^4+x^3+x^2+x+1$ como producto de 2 polinomios de grado 2 reales.

4.12. El máximo común divisor

Como $\mathbb{Z}$, los polinomios $K[x]$ son una anillo euclidiano. El Algoritmo de Euclides (Capítulo 1, sección 1.4) también se aplica a los polinomios gracias al concepto de grado, y se obtienen máximos comunes divisores.

Lema 4.12.1. *Sean $f_1(x), f_2(x) \in K[x]$ y consideremos $g(x)$ otro polinomio tal que $g(x) \mid f_i(x)$, $i = 1, 2$, entonces $g(x)$ divide a toda combinación lineal de $f_1(x)$ y $f_2(x)$, i.e.*

$$g(x) \mid (h_1(x)f_1(x) + h_2(x)f_2(x)),$$

$\forall\ h_1(x), h_2(x) \in K[x]$.

Demostración. Se puede escribir

$$h_i(x)f_i(x) = g(x)\varphi_i(x), \quad i = 1, 2,$$

sumando y factorizando se obtiene el resultado. □

Proposición 4.12.2. *Consideremos $f_1(x), f_2(x) \in K[x]$ no nulos y una combinación lineal de grado mínimo $d(x) = f_1(x)g_1(x) + f_2(x)g_2(x)$, entonces $d(x) \mid f_i(x)$, $i = 1, 2$ y por lo tanto a cualquier combinación lineal de ellos (por el Lema 4.12.1).*

Demostración. Igual que en los enteros. Si

$$f_1(x) = d(x)q_1(x) + r_1(x),$$

$\operatorname{gr}(r_1(x)) \leqslant \operatorname{gr}(d(x))$. Necesariamente $r_1(x) = 0$, ya que si $r_1(x) \neq 0$, sustituyendo $d(x)$, se tendría que $r_1(x)$ es una combinación lineal de menor grado. Análogamente, $d(x) \mid f_2(x)$. □

Definición 48. *Un máximo común divisor MCD de dos polinomios no nulos $f_1(x)$ y $f_2(x)$ es un divisor común de grado máximo.*

Proposición 4.12.3. *Si $d_1(x), d_2(x)$ son máximos divisores comunes de $f_1(x)$ y $f_2(x)$, entonces $d_1(x), d_2(x)$ son asociados.*

Demostración. Se hace exactamente como en el caso de los enteros, aplicando el algoritmo de Euclides a $f_1(x), f_2(x)$, se obtiene un divisor común $g(x)$. Este algoritmo muestra que todo divisor común divide a $g(x)$. En particular, si $d(x)$ es un MCD, $d(x) \mid g(x)$,

$$\therefore \quad \operatorname{gr}(g(x)) \geqslant \operatorname{gr}(d(x)).$$

Como también $\operatorname{gr}(g(x)) \leqslant \operatorname{gr}(d(x))$, $g(x)$ es asociado con $d(x)$. En consecuencia, cualesquiera 2 MCDs son asociados entre sí, y se sigue el resultado (ya que ser asociado es una relación de equivalencia). □

Teorema 4.12.4. *Cualquier combinación lineal de grado mínimo de $f_1(x)$ y $f_2(x)$ es un* MCD *de ellos.*

Demostración. Sea $e(x)$ una combinación lineal de grado mínimo y $d(x)$ un MCD. Entonces, por la Proposición 4.12.2 $e(x)$ es un divisor común, por lo que $\operatorname{gr}(e(x)) \leqslant \operatorname{gr}(d(x))$, y por el Lema 4.12.1 $d(x) \mid e(x)$,

$$\therefore \quad \operatorname{gr}(e(x)) = \operatorname{gr}(d(x)).$$

□

Corolario 4.12.5. *Cualquier* MCD *de $f_1(x)$ y $f_2(x)$ es una combinación lineal de grado mínimo de ellos.*

Demostración. Si $d(x)$ es un MCD, entonces es asociado a una combinación lineal de grado mínimo y por lo tanto también es combinación lineal de grado mínimo. □

Corolario 4.12.6. *Todo divisor común de $f_1(x)$ y $f_2(x)$ es un divisor de cualquier* MCD

Demostración. Un MCD es combinación lineal de $f_1(x)$ y $f_2(x)$, etcétera. □

Corolario 4.12.7. *Sea $e(x)$ un divisor común de $f_1(x)$ y $f_2(x)$ tal que para todo divisor $g(x)$ de $f_1(x), f_2(x)$ se tiene $g(x) \mid e(x)$, entonces $e(x)$ es un* MCD

Demostración. Si $d(x)$ es un MCD, por hipótesis $d(x) \mid e(x)$, por lo tanto $\operatorname{gr}(d(x)) \leqslant \operatorname{gr}(e(x))$, también $\operatorname{gr}(d(x)) \geqslant \operatorname{gr}(e(x))$. □

Definición 49. *Sean $f_1(x), f_2(x) \in K[x]$ no nulos, se define el máximo común divisor como su único MCD mónico. Se escribe sin ambigüedad*

$$d(x) = (f_1(x), f_2(x)).$$

Obsérvese que si $f_1(x)$ o $f_2(x)$ es nulo, digamos $f_1(x)$, entonces

$$d(x) = kf_2(x),$$

(si $f_2(x) = a_n x^n + \cdots + a_0$, entonces $k = 1/a_n$).

Teorema 4.12.8. *Sea $f(z) \in K[z]$, entonces $f(z)$ tiene una raíz de multiplicidad > 1 si y sólo si*

$$(f(z), f'(z)) \neq 1.$$

Demostración. $\Rightarrow$) Sea α una raíz de multiplicidad m de $f(z)$, entonces α es una raíz de multiplicidad $m-1$ de $f'(z)$, *i.e.*, $m - 1 > 0$. Como

$$(z - \alpha) \mid f'(z) \quad \text{y} \quad (z - \alpha) \mid f(z),$$

se sigue que

$$(f(z), f'(z)) \neq 1.$$

$\Leftarrow$) Sea $q(z) = (f(z), f'(z))$, donde $\operatorname{gr}(q(z)) > 0$, y α es una raíz de $q(z)$, por lo tanto α es una raíz de $f(z)$ y de $f'(z)$, y si α es raíz de multiplicidad m de $f(z)$, lo es de multiplicidad $m-1$ de $f'(z)$ y $m - 1 > 0$. □

EJERCICIOS 4.12

1. Sea $\{\alpha_1, \ldots, \alpha_k\}$ el conjunto de raíces comunes de dos polinomios no nulos $f(z), g(z) \in K[z]$, donde m_i y n_i son las multiplicidades de α_i como raices de $f(z)$ y $g(z)$, respectivamente, demuestre que

$$(f(z), g(z)) = \prod_{i=1}^{k} (z - \alpha_i)^{\min(m_i, n_i)}.$$

2. Sea $f_1(z)$ el cociente de $f(z)$ y de $(f(z), f'(z))$, donde $f(z)$ es no nulo. Demuestre que $f_1(z)$ tiene las mismas raíces que $f(z)$, pero todas con multiplicidad 1.

3. Calcule el MCD de $f(x) = x^7 + x^3 + 1$ y su derivada, compruebe que $f(x)$ no tiene raíces de multiplicidad > 1.

4. Factorice el polinomio $f(z) = z^3 + (-6 - 3i)\, z^2 + (9 + 12i)\, z + (-2 - 11i)$.

4.13. Método de Sturm

Este método sirve para localizar las raíces reales de polinomios reales. Usando el Ejercicio 2 de la sección anterior, se puede suponer que todas las raíces son de multiplicidad uno, remplazando $f(x)$ por

$$f_1(x) = \frac{f(x)}{(f(x), f'(x))},$$

si es necesario.

Aplicando el algoritmo de Euclides a $f(x)$ y $f'(x)$ se tiene

$$\begin{array}{rcl} f(x) & = & f'(x)q_1(x) + r_2(x) \\ f'(x) & = & r_2(x)q_2(x) + r_3(x) \\ r_2(x) & = & r_3(x)q_3(x) + r_4(x) \\ & \vdots & \\ r_{n-2}(x) & = & r_{n-1}(x)q_{n-1}(x) + r_n(x), \end{array} \tag{4.7}$$

donde $r_n(x)$ es una constante $\neq 0$, ya que $(f(x), f'(x)) = 1$ (pues el último residuo $\neq 0$ es el MCD y por hipótesis tiene grado $\leqslant 0$).

Ahora, escribimos

$$\begin{array}{llll} f_2(x) = -r_2(x), & f_3(x) = -r_3(x), & f_4(x) = r_4(x), & f_5(x) = r_5(x), \\ f_6(x) = -r_6(x), & f_7(x) = -r_7(x), & f_8(x) = r_8(x), & f_9(x) = r_9(x), \end{array}$$

etcétera (por parejas) y

$$f(x) = f_0(x), \quad f'(x) = f_1(x).$$

Si $c \in \mathbb{R}$, denotamos por $V(c)$ el número de cambios de signo de la sucesión $f_0(c), f_1(c), \ldots$, etcétera. Por ejemplo, si $f_0(c) = 2$, $f_1(c) = -1$, $f_2(c) = -2$, $f_3(c) = 4$ y $f_4(c) = 3$, entonces $V(c) = 2$.

Teorema 4.13.1. (Sturm) *Sea $f(x) \in \mathbb{R}[x]$ y $f_0(x), \ldots, f_n(x)$ los polinomios descritos antes, entonces si $a, b \in \mathbb{R}$ no son raíces de ninguna $f_i(x)$, $a < b$, el número de raíces de $f(x)$ en (a, b) es*

$$V(a) - V(b).$$

Demostración. Si $\forall\ x \in [a, b]$, x no es raíz de ningún $f_i(x)$, cada $f_i(x)$ tiene el mismo signo en $[a, b]$ y $V(a) = V(b)$.

Sean $\rho_1, \rho_2, \ldots, \rho_k$ los puntos en $[a, b]$ que son raíces de algún

$$f_i(x)$$

en orden creciente, tomando $a_0 = a, a_1, a_2, \ldots, a_{k-1}, a_k = b$, tales que

$$a_0 < \rho_1 < a_1 < \rho_2 < a_2 < \cdots < \rho_k < a_k,$$

se tiene

$$V(a) - V(b) = \sum_{i=0}^{k-1} [v(a_i) - v(a_{i+1})].$$

Por lo tanto, basta probar que

$$V(a_i) - V(a_{i+1}) = \begin{cases} 0 & \text{si } f(\rho) \neq 0 \\ 1 & \text{si } f(\rho) = 0. \end{cases}$$

Para esto se puede suponer que hay un solo $\rho \in [a, b]$ tal que es raíz de algún $f_i(x)$, y hay que probar que

$$V(a) - V(b) = \begin{cases} 0 & \text{si } f(\rho) \neq 0 \\ 1 & \text{si } f(\rho) = 0. \end{cases}$$

Caso 1: $f(\rho) \neq 0$.

En este caso ρ es una raíz de $f_{j_1}(x), \ldots, f_{j_t}(x)$, y no hay 2 de estos índices que sean consecutivos, ya que en este caso ρ sería raíz de 2 residuos consecutivos en el algoritmo de Euclides para $f(x)$ y $f'(x)$, y $f(x)$ y $f'(x)$ tendrían una raíz en común.

También al contar $V(a)$ y $V(b)$ se pueden ignorar los cambios de signo entre $f_j(x)$ y $f_{j+1}(x)$ si $j, j+1 \notin \{j_1, j_2, \ldots, j_t\}$, ya que estas funciones tienen signo constante en $[a, b]$, por lo que si cambian de signo en a, también lo hacen en b.

Falta probar que $\forall\ j_i,\ i = 1, 2, \ldots, t$, el número de cambios en $f_{j_i-1}(a)$, $f_{j_i}(a), f_{j_i+1}(a)$ es el mismo que en $f_{j_i-1}(b), f_{j_i}(b), f_{j_i+1}(b)$. Para esto obsérvese que si $r_0(x) = f(x),\ r_1(x) = f_1(x)$ en la notación de (4.7), entonces

$$r_i(x) \,|\, r_{i-1}(x) - r_{i+1}(x) \quad \forall\ i,$$

por lo que $f_i(x) \,|\, f_{i-1}(x) + f_{i+1}(x)$:

Si $r_{i-1}(x) = f_{i-1}(x)$, entonces $r_{i+1}(x) = -f_{i+1}(x)$, y si $r_{i-1}(x) = -f_{i-1}(x)$ se tiene $r_{i+1}(x) = f_{i+1}(x)$.

En consecuencia

$$f_{j_i-1}(\rho) + f_{j_i+1}(\rho) = 0 \quad \forall\ i,$$

y f_{j_i-1}, f_{j_i+1} tienen signos opuestos y las posibilidades se describen en las siguientes figuras.

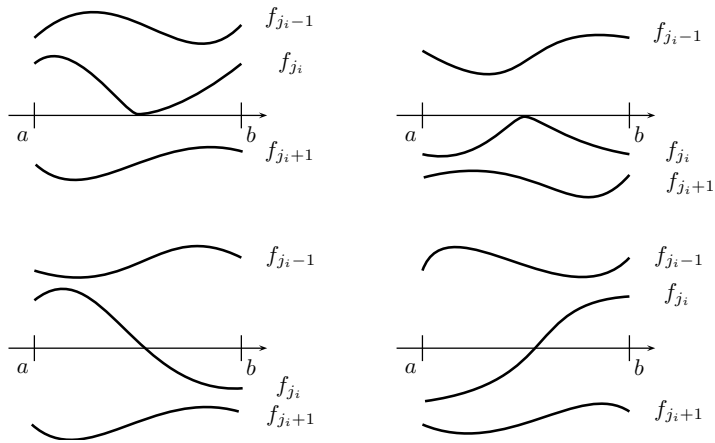


Figura 4.7: Cambios de signo de los polinomios de Sturm f_{j_i}

En cualquiera de estos casos hay un cambio de signo en a y otro en b, la misma situación sucede invirtiendo (en la Figura 4.7) las posiciones de f_{j_i-1} y f_{j_1+1}, por lo cual

$$V(a) - V(b) = 0.$$

Caso 2: $f(\rho) = 0$.

El mismo razonamiento anterior se aplica a los cambios de signo en las secuencias $f_1(a), \ldots, f_n(a)$ y $f_1(b), \ldots, f_n(b)$.

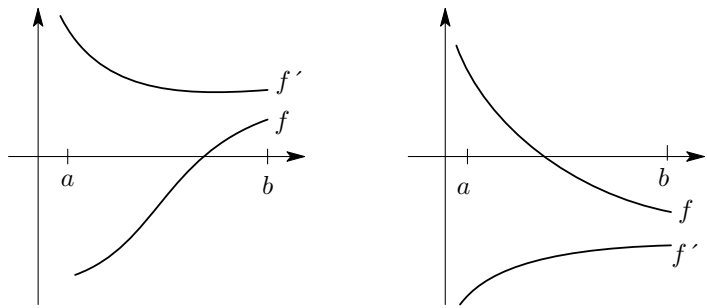


Figura 4.8: Caso 2 en la prueba del teorema de Sturm, cambios de signo de f y f'

Ahora $f(a)$ y $f(b)$ tienen signos opuestos, ya que ρ no es un punto crítico, *i.e.* $f'(\rho) \neq 0$. Por lo que basta probar que $f(b)$ y $f'(b)$ tienen el mismo signo,

ya que esto implica que $f(a)$ y $f'(a)$ tienen signos contrarios y

$$V(a) - V(b) = 1,$$

véase la Figura (4.8).

Para demostrar esto se expresa

$$f(x) = a_0 + a_1(x-\rho) + a_2(x-\rho)^2 + \cdots,$$

y se tiene $a_0 = f(\rho) = 0$ y $a_1 = f'(\rho)$. Por lo cual

$$\text{signo de } a_1 = \text{signo de } f',$$

y basta probar que para alguna $\sigma \in (\rho, b)$

$$\text{signo de } f(\sigma) = \text{signo de } a_1$$

(f tiene signo constante en $(\rho, b]$). Como el signo de a_1 es el signo de $a_1(\sigma-\rho)$, basta probar

$$|a_1(\sigma-\rho)| > |a_2(\sigma-\rho)^2 + \cdots + a_m(\sigma-\rho)^m|.$$

Finalmente, si σ es suficientemente cercana a ρ, de tal manera que

$$|\sigma - \rho| < 1$$

y

$$(\sigma-\rho) < \frac{|a_1|}{|a_i(m-1)|} \quad \forall\ i,\ a_i \neq 0,$$

se tiene

$$|a_2(\sigma-\rho)^2 + \cdots + a_m(\sigma-\rho)^m| < \sum_{i=2}^{m} |a_i|(\sigma-\rho)^i \leqslant \sum_{i=2}^{m} |a_i|(\sigma-\rho)^2$$

$$< (\sigma-\rho)\sum_{i=2}^{m} \frac{|a_i||a_1|}{|a_i|(m-1)} \leq (\sigma-\rho)|a_1|$$

(los sumandos donde $a_i = 0$ se omiten). □

La filosofía es que si $\sigma-\rho$ es muy pequeño, el término de grado 1 domina. Antes de mostrar un ejemplo, obsérvese que si

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{R}[x]$$

y

$$A = \text{máx}\{1, |a_1| + |a_2| + \cdots + |a_n|\},$$

entonces f no tiene raíces en $[-A, A]^c$:

Esto se sigue, ya que si $x \in [-A, A]^c$,

$$|x^n| > (|a_1| + |a_2| + \cdots + |a_n|)\,|x^{n-1}|$$

$$\geqslant |a_1||x|^{n-1} + |a_2||x|^{n-2} + \cdots + |a_n||x^{n-n}| \geqslant |a_1 x^{n-1} + \cdots + a_n|.$$

Ejemplo.

Sea

$$f(x) = x^4 - x - 3,$$

por la observación anterior las raíces de f están en el intervalo $[-4, 4]$. Más aún, si $|x| > 2$, entonces

$$x^4 > 2^3|x| = 4|x|(1+1) = 4|x| + 4|x| > |x| + 3 \geqslant |x+3|,$$

y las raíces están en $[-2, 2]$.

Aplicamos el teorema de Sturm para aislarlas,

$$f'(x) = 4x^3 - 1,$$

$$\begin{array}{llll} x^4 & -x & -3 & \\ -x^4 & +\frac{x}{4} & & \\ \hline & -\frac{3}{4}x & -3 & \end{array} \qquad \begin{array}{l|l} 4x^3 - 1 & \\ \hline \frac{x}{4} & \end{array}$$

Por lo tanto

$$f_2(x) = \frac{3}{4}(x+4), \qquad r_2(x) = -\frac{3}{4}(x+4),$$

y como

$$\begin{array}{llll|l} 4 & 0 & 0 & -1 & -4 \\ & -16 & 64 & -256 & \\ \hline 4 & -16 & 64 & -257\,, & \end{array}$$

se tiene

$$4x^3 - 1 = \left(-\frac{3}{4}\right)(x+4)\left(-\frac{4}{3}\right)(4x^2 - 16x + 64) - 257,$$

$$\text{por lo cual} \qquad (f(x), f'(x)) = 1.$$

También

$$f_3(x) = 257.$$

Ahora, $f_0(2) > 0$ y $f_0(-2) > 0$, también $f_0(0)$, $f_0(1)$ y $f_0(-1)$ son negativos. Así mismo $f_1(2)$ y $f_1(1)$ son positivos y f_1 en $-2, -1$ y 0 toman valores negativos, por lo que se tiene la siguiente tabla.

	-2	2	0	1	-1
$f_0(x)$	+	+	-	-	-
$f_1(x)$	-	+	-	+	-
$f_2(x)$	+	+	+	+	+
$f_3(x)$	+	+	+	+	+

Las 2 primeras columnas muestran que hay 2 raíces en $(-2, 2)$, y las otras 3 refinan el resultado probando que hay una en $(-2, 1)$ y otra en (1,2). Nótese que las otras dos raíces son dos complejos conjugados entre sí.

Gráficamente, $x = \sqrt[3]{1/4} < 1$ es el único punto crítico, que es un mínimo, ya que $f''(x) = 12x^2$ (véase la Figura 4.9).

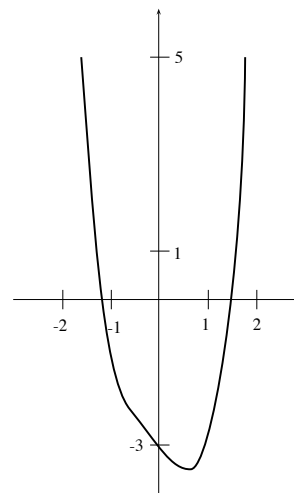


Figura 4.9: Gráfica de $f(x) = x^4 - x - 3$

EJERCICIO 4.13 1. Usando el método de Sturm, aislar las raíces de $x^3 - 4x + 1$, y probar que $x^4 + x^3 + 2x^2 + x + 1$ no tiene raíces reales.

4.14. Funciones racionales, fracciones parciales

Se define una relación de equivalencia entre las expresiones de la forma

$$\frac{f(x)}{g(x)},$$

donde $f(x), g(x)$ son polinomios y $g(x) \neq 0$, de la siguiente manera:

$$\frac{f_1(x)}{g_1(x)} \sim \frac{f_2(x)}{g_2(x)}$$

si $f_1(x)g_2(x) = f_2(x)g_1(x)$.

Esta relación es evidentemente reflexiva y simétrica. También es transitiva, esto se demuestra igual que con los racionales, si

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \quad \text{y} \quad \frac{a_2}{b_2} \sim \frac{a_3}{b_3},$$

entonces $a_1b_2 = a_2b_1$, $a_2b_3 = a_3b_2$ y $a_1b_2b_3 = a_3b_2b_1$, etcétera.

Definición 50. *Las clases de equivalencia obtenidas bajo la relación anterior se llaman funciones racionales.*

Igual que en $\mathbb{Q}$ se definen 2 operaciones:

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)}$$

y

$$\frac{f_1(x)}{g_1(x)} \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}.$$

Es fácil probar que estas operaciones no dependen del representante, de hecho la misma prueba en $\mathbb{Q}$ se aplica a este caso. Mostraremos como se descomponen estas funciones en fracciones parciales, lo cual es de utilidad al resolver integrales.

Lema 4.14.1. *Si $g(x) = h(x)k(x)$ y $(h(x), k(x)) = 1$, entonces para todo $f(x)$ existen polinomios $s(x), t(x)$ tales que*

$$\frac{f(x)}{g(x)} = \frac{s(x)}{h(x)} + \frac{t(x)}{k(x)}.$$

Además, si $f(x), h(x), k(x) \in \mathbb{R}[x]$, entonces $s(x), t(x) \in \mathbb{R}[x]$.

Demostración. Aplicando el algoritmo de Euclides se pueden encontrar $h_1(x), k_1(x)$ (reales si $h(x)$ y $k(x)$ lo son) tales que

$$1 = h(x)h_1(x) + k(x)k_1(x),$$

por lo cual

$$\frac{f(x)}{g(x)} = \frac{f(x)\left[h(x)h_1(x) + k(x)k_1(x)\right]}{g(x)} = \frac{f(x)h_1(x)}{k(x)} + \frac{f(x)k_1(x)}{h(x)}.$$

□

Nótese que la descomposición en el Lema 4.14.1 no es única (ejercicio).

Lema 4.14.2. *Sean $h(x), f(x)$ polinomios tales que $\operatorname{gr}(f(x)) < \operatorname{gr}(h(x))^m$, y $\operatorname{gr}(h(x)) > 0$, entonces existen polinomios $s_1(x), s_2(x), \ldots, s_m(x)$ tales que $\operatorname{gr}(s_i(x)) < \operatorname{gr}(h(x))\ \forall\ i$, y*

$$\frac{f(x)}{[h(x)]^m} = \frac{s_1(x)}{h(x)} + \cdots + \frac{s_m(x)}{[h(x)]^m}.$$

Además, si $h(x), f(x) \in \mathbb{R}[x]$, los polinomios $s_i(x)$ también.

Demostración. Sea $n = \operatorname{gr}(h(x))$, se aplica el algoritmo de la división a los siguientes cocientes:

$$\begin{aligned}
f(x) &= h(x)q_1(x) + r_1(x),\\
q_1(x) &= h(x)q_2(x) + r_2(x),\\
q_2(x) &= h(x)q_3(x) + r_3(x),\\
&\vdots\\
q_{k-2}(x) &= h(x)q_{k-1}(x) + r_{k-1}(x),\\
q_{k-1}(x) &= h(x)q_k(x) + r_k(x),
\end{aligned}$$

donde $\operatorname{gr}(r_i(x)) < n\ \forall\ i$, $\operatorname{gr}(q_k(x)) < n$ y $\operatorname{gr}(q_{k-1}(x)) \geqslant n$.

Esto se puede lograr: si $\operatorname{gr}(f(x)) < \operatorname{gr}(h(x))$, no hay nada que probar; de otra manera: $\operatorname{gr}(f(x)) > \operatorname{gr}(q_1(x))$ $(\operatorname{gr}(f(x)) = \operatorname{gr}(h(x)) + \operatorname{gr}(q_1(x)))$ y los grados de los q_i van disminuyendo, por lo que el proceso se termina en la primera k tal que

$$\operatorname{gr}(q_k(x)) < \operatorname{gr}(h(x)) = n.$$

Finalmente sustituyendo $q_{k-1}(x)$ en la ecuación anterior, e iterando este proceso se tiene

$$\begin{aligned}
q_{k-2}(x) &= h(x)[h(x)q_k(x) + r_k(x)] + r_{k-1}(x)\\
&= [h(x)]^2 q_k(x) + h(x)r_k(x) + r_{k-1}(x)
\end{aligned}$$

y

$$\begin{aligned} q_{k-3}(x) &= h(x)q_{k-2}(x) + r_{k-2}(x) \\ &= [h(x)]^3 q_k(x) + [h(x)]^2 r_k(x) + h(x)r_{k-1}(x) + r_{k-2}(x), \end{aligned}$$

hasta obtener después de k pasos,

$$q_0(x) = f(x) = [h(x)]^k q_k(x) + [h(x)]^{k-1} r_k(x) + \cdots + h(x)r_2(x) + r_1(x). \quad (4.8)$$

Se tiene $k < m$. De otra manera, si $k \geqslant m$, usando la ecuación (4.8), se concluye que $\operatorname{gr}(f(x)) = \operatorname{gr}(h(x)^k) + \operatorname{gr}(q_k(x)) \geqslant \operatorname{gr}(h(x)^m)$, lo cual contradice la hipótesis sobre los grados. Finalmente, dividiendo por $[h(x)]^m$ se sigue el resultado. □

Obsérvese que si $\operatorname{gr}(f(x)) > \operatorname{gr}(h(x))^m$ en el Lema 4.14.2 se sigue un resultado análogo, aplicando dicho lema a $r(x)$, donde

$$f(x) = g(x)[h(x)]^m + r(x),$$

y $\operatorname{gr}(r(x)) < \operatorname{gr}(h(x))^m$, obteniéndose en este caso una parte polinomial.

Teorema 4.14.3. *Sea*

$$g(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_n)^{r_n},$$

donde $\alpha_i \neq \alpha_j$, *si* $i \neq j$, *entonces*

$$\frac{f(x)}{g(x)} = s(x) + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{a_{ij}}{(x - \alpha_i)^j}.$$

Demostración. Aplicando el Lema 4.14.1 se tiene

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{n} \frac{f_i(x)}{(x - \alpha_i)^{r_i}},$$

y por el Lema 4.14.2, $\forall\ i$

$$\frac{f_i(x)}{(x - \alpha_i)^{r_i}} = s_i(x) + \sum_{j=1}^{r_i} \frac{a_{ij}}{(x - \alpha_i)^j},$$

ya que $\operatorname{gr}(x - \alpha_i) = 1$, escribiendo $s(x) = \sum_{i=1}^{n} s_i(x)$ se sigue el resultado. □

Teorema 4.14.4. *Sea*

$$g(x) = \left(\prod_{i=1}^{n}(x-\alpha_i)^{r_i}\right)\left(\prod_{i=1}^{m}(x^2+a_ix+b_i)^{s_i}\right)$$

donde los factores son distintos dos a dos, $a_i, b_i, \alpha_i \in \mathbb{R}\ \forall\ i$ *y los polinomios de grado 2 son irreducibles en* $\mathbb{R}[x]$*, entonces si* $f(x) \in \mathbb{R}[x]$

$$\frac{f(x)}{g(x)} = s(x) + \sum_{i=1}^{n}\sum_{j=1}^{r_i}\frac{a_{ij}}{(x-\alpha_i)^j} + \sum_{i=1}^{m}\sum_{j=1}^{s_i}\frac{A_{ij}x+B_{ij}}{(x^2+a_ix+b_i)^j},$$

donde $s(x) \in \mathbb{R}[x],\ a_{ij}, A_{ij}, B_{ij} \in \mathbb{R}\ \forall\ i, j.$

Demostración. De nuevo como en el teorema anterior el resultado es consecuencia inmediata de los Lemas 4.14.1 y 4.14.2: usando el primero

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{n}\frac{f_i(x)}{(x-\alpha_i)^{r_i}} + \sum_{i=1}^{m}\frac{g_i(x)}{(x^2+a_ix+b_i)^{s_i}},$$

y usando el segundo se obtiene la expresión del enunciado. □

En la práctica se encuentra la descomposición del Teorema 4.14.4 de una manera un poco distinta: si $\operatorname{gr}(f(x)) > \operatorname{gr}(g(x))$, por el algoritmo de la división

$$f(x) = g(x)h(x) + r(x), \quad \text{donde } \operatorname{gr}(r(x)) < \operatorname{gr}(g(x)),$$

y

$$\frac{f(x)}{g(x)} = h(x) + \frac{r(x)}{g(x)}. \tag{4.9}$$

Por otra parte, usando el Teorema 4.14.4 y sumando toda la parte no polinomial se tiene

$$\frac{f(x)}{g(x)} = k(x) + \frac{q(x)}{g(x)},$$

donde $\operatorname{gr}(q(x)) < \operatorname{gr}(g(x))$. Esto se sigue, ya que al sumar dos funciones racionales, donde los grados de los numeradores son menores a los de los denominadores, se obtiene una función racional con estas características. Por lo cual

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

y se sigue entonces por unicidad que

$$k(x) = h(x) \quad \text{y} \quad r(x) = q(x).$$

Por consiguiente, para encontrar la expresión del Teorema 4.14.4, primero se puede aplicar el algoritmo de la división para obtener (4.9) y después encontrar a_{ij}, A_{ij}, B_{ij} sumando las expresiones no polinomiales y resolviendo para $r(x)$ mediante un sistema de ecuaciones. Las observaciones y resultados anteriores garantizan la la existencia de las soluciones ($r(x) = q(x)$).

Ejemplo.

Sea

$$R(x) = \frac{2x^7 + 5x^6 + x^5 - x^4 - 7x^3 + x^2 + x + 7}{x^6 - 2x^3 + 1}.$$

Primero se encuentra la parte polinomial

$$\begin{array}{rrrrrrrr|l}
2x^7 & +5x^6 & +\,x^5 & -x^4 & -7x^3 & +x^2 & +x & +7 & \multicolumn{1}{|l}{x^6 - 2x^3 + 1} \\
\cline{9-9}
-2x^7 & & & 4x^4 & & & -2x & & 2x + 5 \\
\cline{1-8}
 & 5x^6 & +x^5 & +3x^4 & -7x^3 & +x^2 & -x & +7 & \\
 & -5x^6 & & & 10x^3 & & & -5 & \\
\cline{2-8}
 & & x^5 & +3x^4 & +3x^3 & +x^2 & -x & +2, &
\end{array}$$

por lo que

$$R(x) = 2x + 5 + \frac{x^5 + 3x^4 + 3x^3 + x^2 - x + 2}{x^6 - 2x^3 + 1}.$$

Si $x^3 = y$, el denominador de la parte no polinomial es $y^2 - 2y + 1 = (y-1)^2$, por lo tanto $x^6 - 2x^3 + 1 = (x^3 - 1)^2 = [(x-1)^2(x^2 + x + 1)]^2$.

Si $R_1(x)$ denota la parte no polinomial en $R(x)$, se tiene

$$\begin{aligned}
R_1(x) &= \frac{a_1}{x-1} + \frac{a_2}{(x-1)^2} + \frac{a_3x + a_4}{x^2 + x + 1} + \frac{a_5x + a_6}{(x^2 + x + 1)^2} \\
&= \frac{a_1(x-1)(x^2 + x + 1)^2 + a_2(x^2 + x + 1)^2}{x^6 - 2x^3 + 1} \\
&\quad + \frac{(a_3x + a_4)(x-1)^2(x^2 + x + 1) + (a_5x + a_6)(x-1)^2}{x^6 - 2x^3 + 1}.
\end{aligned}$$

Como

$$\begin{aligned}
(x^2 + x + 1)^2 &= x^4 + 2x^3 + 3x^2 + 2x + 1, \\
(x-1)^2(x^2 + x + 1) &= (x^2 - 2x + 1)(x^2 + x + 1) = x^4 - x^3 - x + 1, \\
\text{y} \quad (x^2 + x + 1)^2(x-1) &= x^5 + x^4 + x^3 - x^2 - x - 1;
\end{aligned}$$

el numerador de $R_1(x)$ es

$$\begin{aligned}
&a_1(x^5+x^4+x^3-x^2-x-1)+a_2(x^4+2x^3+3x^2+2x+1)\\
&\quad +(a_3x+a_4)(x^4-x^3-x+1)+(a_5x+a_6)(x^2-2x+1)\\
&=(a_1+a_3)x^5+(a_1+a_2-a_3+a_4)x^4+(a_1+2a_2-a_4+a_5)x^3\\
&\quad +(-a_1+3a_2-a_3-2a_5+a_6)x^2+(-a_1+2a_2+a_3-a_4+a_5-2a_6)x\\
&\quad -a_1+a_2+a_4+a_6.
\end{aligned}$$

Por lo que se obtiene el siguiente sistema de ecuaciones

$$\left\{\begin{array}{rcl}
1 &=& a_1+a_3\\
3 &=& a_1+a_2-a_3+a_4\\
3 &=& a_1+2a_2-a_4+a_5\\
1 &=& -a_1+3a_2-a_3-2a_5+a_6\\
-1 &=& -a_1+2a_2+a_3-a_4+a_5-2a_6\\
2 &=& -a_1+a_2+a_4+a_6.
\end{array}\right.$$

Resolvemos ahora el sistema

$$\begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1\\
1 & 1 & -1 & 1 & 0 & 0 & 3\\
1 & 2 & 0 & -1 & 1 & 0 & 3\\
-1 & 3 & -1 & 0 & -2 & 1 & 1\\
-1 & 2 & 1 & -1 & 1 & -2 & -1\\
-1 & 1 & 0 & 1 & 0 & 1 & 2
\end{pmatrix}\sim
\begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1\\
0 & 1 & -2 & 1 & 0 & 0 & 2\\
0 & 2 & -1 & -1 & 1 & 0 & 2\\
0 & 3 & 0 & 0 & -2 & 1 & 2\\
0 & 2 & 2 & -1 & 1 & -2 & 0\\
0 & 1 & 1 & 1 & 0 & 1 & 3
\end{pmatrix}$$

$$\begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1\\
0 & 1 & -2 & 1 & 0 & 0 & 2\\
0 & 0 & 3 & -3 & 1 & 0 & -2\\
0 & 0 & 6 & -3 & -2 & 1 & -4\\
0 & 0 & 6 & -3 & 1 & -2 & -4\\
0 & 0 & 3 & 0 & 0 & 1 & 1
\end{pmatrix}\sim
\begin{pmatrix}
 & \cdots & & & & \\
\vdots & 3 & -3 & 1 & 0 & -2\\
 & 0 & 3 & -4 & 1 & 0\\
 & 0 & 3 & -1 & -2 & 0\\
 & 0 & 3 & -1 & 1 & 3
\end{pmatrix}$$

$$\begin{pmatrix}
 & \cdots & & & & \\
\vdots & 3 & \cdots & & & \\
 & \vdots & 3 & -4 & 1 & 0\\
 & & 0 & 3 & -3 & 0\\
 & & 0 & 3 & 0 & 3
\end{pmatrix}\sim
\begin{pmatrix}
 & \cdots & & & \\
\vdots & 3 & \cdots & & \\
 & \vdots & 3 & \cdots & \\
 & & \vdots & 3 & -3 & 0\\
 & & & 0 & 3 & 3
\end{pmatrix}$$

Por lo tanto $a_6=1$ y también $a_5=1$. Luego $3a_4-4+1=0$, *i.e.* $a_4=1$. Dado que $3a_3-3+1=-2$, se tiene que $a_3=0$. Tomado la 2a ecuación (en

la matriz escalonada), se tiene que $a_2+1=2$, por lo que $a_2=1$. Finalmente, se sigue de la primera ecuación que $a_1=1$.

Por consiguiente

$$a_1=a_2=a_4=a_5=a_6=1 \quad \text{y} \quad a_3=0,$$

por lo cual

$$R(x)=2x+5+\frac{1}{x-1}+\frac{1}{(x-1)^2}+\frac{1}{x^2+x+1}+\frac{x+1}{(x^2+x+1)^2}.$$

EJERCICIOS 4.14

1. Demuestre que la descomposición en el Lema 4.14.1 no es única.
2. Encuentre la descomposición en fracciones parciales de las funciones

$$\frac{x^5+x^3+x+1}{x^3-6x^2+11x-6}, \quad \frac{x^5-x^4+1}{x^4-x^3-x+1}.$$

4.15. Teorema de Cardano-Ferro-Tartaglia

Como se observó en los ejemplos de la sección del teorema de Sturm, si

$$f(x)=x^3+bx^2+cx+d, \qquad b,c,d\in\mathbb{R},$$

se tiene que $|x|^3>|bx^2+cx+d|$, en $(-M,M)^c$, donde

$$M=\text{máx}\{1,|b|+|c|+|d|\},$$

por lo que las raíces de f están en $(-M,M)$.

Al final de la edad media en la universidad de Boloña se descubrió la solución al problema de encontrar las raíces de polinomios de grado 3, el método se atribuye a Cardano, Ferro y Tartaglia. Éste es un interesante episodio de la historia de la matemática (cf. [3]).

Obsérvese primero que basta solucionar una ecuación de la forma

$$z^3+pz+q=0. \tag{4.10}$$

Esto se sigue, ya que al hacer un cambio de variable $y=z-b/3$, en la ecuación

$$y^3+by^2+cy+d=0,$$

se tiene

$$\left(z-\frac{b}{3}\right)^3+b\left(z-\frac{b}{3}\right)^2+c\left(z-\frac{b}{3}\right)+d$$

$$= z^3 - 3z^2\frac{b}{3} + 3z\frac{b^2}{9} - \frac{b^3}{27} + bz^2 - 2z\frac{b^2}{3} + \frac{b^3}{9} + cz - \frac{cb}{3} + d,$$

y esta nueva ecuación es de la forma (4.10).

La expresión

$$\Delta = \frac{q^2}{2^2} + \frac{p^3}{3^3}$$

es muy importante, se le llama el *discriminante* del polinomio. Nótese que si $p = 0$ la solución de (4.10) es trivial.

Teorema 4.15.1. (Cardano, Ferro, Tartaglia) *Si $p \neq 0$, al menos una de las soluciones de (4.10) es de la forma*

$$z = \left(-\frac{q}{2} + \sqrt{\Delta}\right)^{1/3} + \left(-\frac{q}{2} - \sqrt{\Delta}\right)^{1/3},$$

donde $(-q/2 + \sqrt{\Delta})^{1/3}$ es una de las tres raíces cúbicas de $-q/2 + \sqrt{\Delta}$ y $(-q/2 - \sqrt{\Delta})^{1/3}$ es a su vez una las tres raíces cúbicas de $-q/2 - \sqrt{\Delta}$.

Demostración. Se puede escribir

$$z = s + t,$$

$s, t \in \mathbb{C}$, mostraremos que z es solución si se toman s y t adecuados.

Ahora,

$$(s+t)^3 + p(s+t) + q = 0,$$

esto es

$$s^3 + 3s^2t + 3st^2 + t^3 + ps + pt + q = 0.$$

La esencia de la prueba es exhibir que existen $s, t \in \mathbb{C}$ tales que

$$\begin{cases} s^3 + t^3 = -q & (4.11) \\ 3st = -p, & (4.12) \end{cases}$$

lo cual prueba que z es solución.

Resolvemos el sistema (4.11) (4.12). Despejando

$$s^3 + \left(-\frac{p}{3s}\right)^3 = -q,$$

y

$$(s^3)^2 + qs^3 - \left(\frac{p}{3}\right)^3 = 0,$$

que es cuadrática, tomando $\alpha = s^3$, se tiene

$$\alpha^2 + \alpha q - \left(\frac{p}{3}\right)^3 = 0,$$

la cual tiene soluciones

$$s^3 = \alpha = -\frac{q}{2} \pm \sqrt{\frac{q^2}{2^2} + \frac{p^3}{27}}.$$

Se puede hacer lo mismo con t y siendo simétricas las ecuaciones se tiene

$$t^3 = \beta = -\frac{q}{2} \pm \sqrt{\frac{q^2}{2^2} + \frac{p^3}{27}},$$

obsérvese que $s \neq 0$ y $t \neq 0$, ya que $p \neq 0$ (por la ecuación (4.12)). Tomando

$$s^3 = -\frac{q}{2} + \sqrt{\Delta} \tag{4.13}$$

$$\text{y} \quad t^3 = -\frac{q}{2} - \sqrt{\Delta}, \tag{4.14}$$

(o al revés, lo cual es la misma solución) se cumple la ecuación (4.11), *i.e.,* s es una de las raíces cúbicas de $-q/2 + \sqrt{\Delta}$ y t de $-q/2 - \sqrt{\Delta}$.

Recordamos que al tomar las raíces cúbicas de un complejo w, si γ es una de ellas las otras son $\gamma\alpha$ y $\gamma\overline{\alpha}$, donde $\alpha = \cos(2\pi/3) + i\,\mathrm{sen}(2\pi/3)$. También, tomando todos los posibles valores de dichas s y t, los productos st (que son a los más nueve) resultan ser las raíces cúbicas de $\frac{-p^3}{27}$, ya que

$$\sqrt[3]{\left(-\frac{q}{2} + \sqrt{\Delta}\right)\left(-\frac{q}{2} - \sqrt{\Delta}\right)} = \sqrt[3]{\frac{q^2}{4} - \frac{q^2}{4} - \frac{p^3}{27}} = \sqrt[3]{-\frac{p^3}{27}}.$$

Fijando entonces una raíz cúbica cualquiera de $-q/2 - \sqrt{\Delta}$ y *rotando* las 3 raíces de $-q/2 + \sqrt{\Delta}$ se obtienen las 3 raíces de

$$\sqrt[3]{-\frac{p^3}{27}}.$$

Una de éstas es precisamente $-p/3$, por lo que para estos valores se cumple la ecuación (4.12). □

Ejemplo.

Resolvemos

$$f(x) = x^3 - 3x + 1,$$

se tiene $p = -3$ y $q = 1$. Entonces

$$x = \left(-\frac{1}{2} + \sqrt{\frac{1}{4} - 1}\right)^{1/3} + \left(-\frac{1}{2} - \sqrt{\frac{1}{4} - 1}\right)^{1/3}$$

$$= \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^{1/3} + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)^{1/3}.$$

Obsérvese que al tomar la raíz cuadrada, como aparece ésta y su inversa, no importa cual se tome, se presentan las dos por simetría.

Una raíz cúbica de

$$-\frac{1}{2} + \frac{\sqrt{3}}{2}i = \cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right) = \alpha$$

es $\beta = \cos(2\pi/9) + i\,\mathrm{sen}(2\pi/9) \sim 40°$, y de

$$-\frac{1}{2} - \frac{\sqrt{3}}{2}i = \cos\left(\frac{4\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{4\pi}{3}\right)$$

es $\cos(4\pi/9) + i\,\mathrm{sen}(4\pi/9) = \beta^2$. En este caso hay 3 raíces reales dadas por

$$\beta + \overline{\beta}, \quad \beta\alpha + \overline{\beta\alpha} \quad \text{y} \quad \beta\alpha^2 + \overline{\beta\alpha^2}.$$

Esto se sigue, ya que la ecuación (4.12) en nuestro caso está dada por

$$3st = -p \quad i.e., \quad st = -3/3 = 1,$$

y si s, t son complejos unitarios, esto se satisface si y sólo si s y t son conjugados (véase la Figura 4.10). Nótese que $\overline{\beta} = \beta^2\alpha^2$, $\overline{\beta\alpha} = \beta^2\alpha$, $\overline{\beta\alpha^2} = \beta^2$.

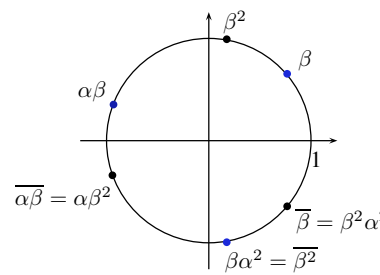


Figura 4.10: Las soluciones de $f(x) = x^3 - 3x + 1$ están dadas por $s + t$, donde $s = \beta,\ \beta\alpha,\ \beta\alpha^2$ y $t = \overline{s}$

Además tomando algunos valores:

$$f(-2) = -1, \quad f(-1) = 3, \quad f(0) = 1, \quad f(1) = -1 \quad \text{y} \quad f(2) = 3,$$

se sigue que una de la raíces está entre -2 y -1, otra entre 0 y 1, y la tercera entre 1 y 2 (véase la Figura 4.11).

Obsérvese que no todos los apareamientos de s y t producen raíces, por ejemplo $\beta + \beta^2$ no es raíz, ya que tienen parte imaginaria y sólo hay 3 raíces reales. Los cálculos parecen amables, pero éste es un caso excepcional, en general esto es muy laborioso, por lo que en muchos casos es más adecuado usar métodos del cálculo y posiblemente el método de Sturm. El siguiente resultado muestra que el signo del discriminante Δ determina si existen 3 raíces reales o no.

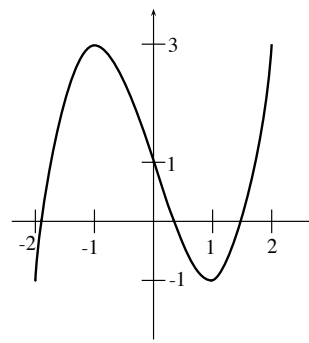


Figura 4.11: Gráfica de $f(x) = x^3 - 3x + 1$

Teorema 4.15.2. *Sea*

$$f(x) = x^3 + px + q,$$

un polinomio real sin raíces múltiples, $p, q \neq 0$, entonces f tiene 3 raíces reales distintas si y sólo si $\Delta < 0$.

Nótese que los casos $p = 0$ o $q = 0$ son triviales, tanto en polinomios reales como en complejos.

Demostración.

Caso 1: $p < 0$.

Se tiene

$$\begin{aligned} f'(x) &= 3x^2 + p \\ f''(x) &= 6x, \end{aligned}$$

por lo cual $f'(x) = 0$ en $-\sqrt{-p/3} \in \mathbb{R}^-$ y en $\sqrt{-p/3} \in \mathbb{R}^+$, y se tiene un máximo local en $x = -\sqrt{-p/3}$, y un mínimo local en $x = \sqrt{-p/3}$.

Obsérvese que hay 3 raíces reales si y sólo si $f(-\sqrt{-p/3})$ y $f(\sqrt{-p/3})$, esto es los valores que toma la función en los puntos críticos, son de signo distinto (véase la Figura 4.12).

El caso en que $\sqrt{-p/3}$ o $-\sqrt{-p/3}$ sean raíces de f no acontece, pues éstas serían raíces de multiplicidad mayor a 1.

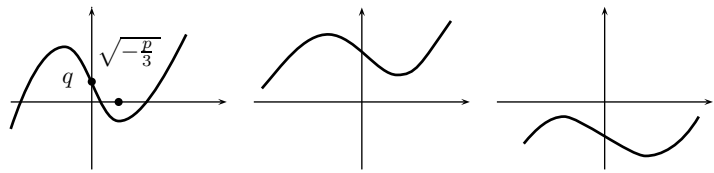


Figura 4.12: Demostración del Teorema 4.15.2

Por lo tanto, el teorema en este caso se sigue de la siguiente afirmación:

$$f(-\sqrt{-p/3})f(\sqrt{-p/3}) = 4\Delta. \tag{4.15}$$

Probamos ahora la afirmación (4.15):

$$\begin{aligned} f\left(-\sqrt{-\frac{p}{3}}\right) &= \left(-\sqrt{-\frac{p}{3}}\right)^3 + p\left(-\sqrt{-\frac{p}{3}}\right) + q \\ &= -\left(-\frac{p}{3}\sqrt{-\frac{p}{3}}\right) - p\left(\sqrt{-\frac{p}{3}}\right) + q = -\frac{2}{3}p\sqrt{-\frac{p}{3}} + q, \end{aligned}$$

$$f\left(\sqrt{-\frac{p}{3}}\right) = \sqrt{-\frac{p}{3}}\left(-\frac{p}{3}\right) + p\sqrt{-\frac{p}{3}} + q = \frac{2}{3}p\sqrt{-\frac{p}{3}} + q,$$

y

$$\begin{aligned} f\left(-\sqrt{-\frac{p}{3}}\right) f\left(\sqrt{-\frac{p}{3}}\right) &= \left(q - \frac{2}{3}p\sqrt{-\frac{p}{3}}\right)\left(q + \frac{2}{3}p\sqrt{-\frac{p}{3}}\right) \\ &= q^2 - \frac{2^2}{3^2}p^2\left(-\frac{p}{3}\right) = 2^2\left(\frac{q^2}{2^2} + \frac{p^3}{3^3}\right) = 4\Delta. \end{aligned}$$

Caso 2: $p \geqslant 0$.

Se tiene que

$$f'(x) = 3x^2 + p > 0$$

y la gráfica es creciente, por lo que hay una sola raíz real. Además el discriminante es

$$\frac{q^2}{2^2} + \frac{p^3}{3^3} > 0.$$

□

Corolario 4.15.3. *Sea $f(x) = x^3 + px + q$ un polinomio real, $p, q \neq 0$, entonces $\Delta = 0$ si y sólo si f tiene raíces reales que son de multiplicidad mayor a 1.*

Demostración. $\Rightarrow$) Si $p < 0$, como

$$f\left(\sqrt{-\frac{p}{3}}\right) f\left(-\sqrt{-\frac{p}{3}}\right) = 4\Delta,$$

se sigue que si $\Delta = 0$, entonces $\sqrt{-p/3}$ o $-\sqrt{-p/3}$ son raíces de f, y necesariamente son de multiplicidad mayor a 1.

Si $p > 0$, se tiene

$$\frac{q^2}{2^2} + \frac{p^3}{3^3} > 0.$$

$\Leftarrow$) Si $p < 0$ y si f tiene una raíz α de multiplicidad mayor a 1, entonces $f'(\alpha) = 0$, lo cual implica que

$$\alpha = \pm\sqrt{-\frac{p}{3}} \quad \text{y} \quad \Delta = 0.$$

Si $p > 0$, como la derivada es positiva, f es creciente, tiene solamente una raíz real y no tiene puntos críticos reales. □

Ejemplos.

1) Si

$$f(x) = x^3 - 3x + 1,$$

el discriminante es

$$\Delta = \frac{1}{4} - \frac{3^3}{3^3} < 0,$$

y hay 3 raíces reales, véase la Figura 4.11.

2) Sea

$$f(x) = x^3 - x + 3.$$

Como el discriminante es

$$\Delta = \frac{3^2}{2^2} - \frac{1}{3^3} > 0,$$

hay una única raíz real, véase la Figura 4.13.

Al conocer la raíz de un polinomio de 3er grado, digamos α, se tiene

$$(z-\alpha)\,|\,f(z) \quad \text{y} \quad \frac{f(z)}{z-\alpha}$$

es un polinomio de grado 2 que se puede resolver. Como se mostró, si α es una raíz compleja no real, $\overline{\alpha}$ también lo es.

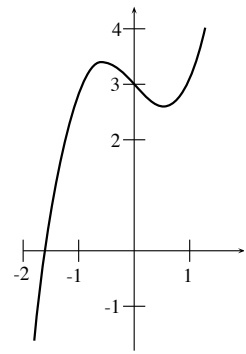


Figura 4.13: Gráfica de $f(x) = x^3 - x + 3$

En general, usando los métodos de Sturm, Newton y Horner se pueden localizar las raíces de un polinomio como se muestra en el siguiente ejemplo.

Consideremos el polinomio

$$f(x) = x^3 + 3x^2 - 2x - 5.$$

Las raíces de $f(x)$ están en $(-10, 10)$, para aislarlas podemos aplicar el método de Sturm y posteriormente Newton o Horner.

Aplicamos el algoritmo de la división al polinomio y su derivada

$$f'(x) = 3x^2 + 6x - 2,$$

$$\begin{array}{rrrr|l}
x^3 & +3x^2 & -2x & -5 & \big|\ 3x^2+6x-2 \\
\cline{5-5}
-x^3 & -2x^2 & +\frac{2}{3}x & & x/3+1/3 \\
\cline{1-3}
 & x^2 & -\frac{4}{3}x & -5 & \\
 & -x^2 & -2x & +\frac{2}{3} & \\
\cline{2-4}
 & & -\frac{10}{3}x & -\frac{13}{3} &
\end{array}$$

por lo que $f_2(x) = \dfrac{1}{3}(10x + 13)$. Además, se puede escribir

$$r_2(x) = -\frac{10}{3}x - \frac{13}{3} = -\frac{10}{3}\left(x + \frac{13}{10}\right)$$

y

$$\begin{array}{cccc} 3 & 6 & -2 & \\ & -\frac{39}{10} & \frac{21(-13)}{100} & \quad \big| -13/10 \\ \hline 3 & \frac{21}{10} & \big| & < 0 \end{array}$$

por lo que $f_3(x) > 0$.

Usando división sintética calculamos algunos valores del polinomio

$$\begin{array}{cccccc} 1 & 3 & -2 & -5 & \big| -4 & \\ & -4 & 4 & -8 & & \\ \hline 1 & -1 & 2 & \big| -13 & = f(-4), & \end{array} \qquad \begin{array}{cccccc} 1 & 3 & -2 & -5 & \big| -2 & \\ & -2 & -2 & 8 & & \\ \hline 1 & 1 & -4 & \big| 3 & = f(-2), & \end{array}$$

$$\begin{array}{cccccc} 1 & 3 & -2 & -5 & \big| 2 & \\ & 2 & 10 & 16 & & \\ \hline 1 & 5 & 8 & \big| 11 & = f(2), & \end{array} \qquad \begin{array}{cccccc} 1 & 3 & -2 & -5 & \big| -3 & \\ & -3 & 0 & 6 & & \\ \hline 1 & 0 & -2 & \big| 1 & = f(1), & \end{array}$$

y

$$f(1) = -3 \quad \text{y} \quad f(-1) = -1,$$

obteniéndose la siguiente tabla

	-4	-2	0	2	-3	1	-1
$f(x)$	$-$	$+$	$-$	$+$	$+$	$-$	$-$
$f'(x)$	$+$	$-$	$-$	$+$	$+$	$+$	$-$
$f_2(x)$	$-$	$-$	$+$	$+$	$-$	$+$	$+$
$f_3(x)$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
	3	2	1	0	2	1	1

Las primeras columnas indican que hay una raíz entre -4 y -2, otra entre -2 y 0, y otra entre 0 y 2. Las siguientes refinan esta información: hay una entre -4 y -3, otra entre -2 y -1 y otra entre 1 y 2. Los ceros de la derivada son

$$\frac{-6 \pm \sqrt{36+24}}{6} = -1 \pm \sqrt{\frac{2^2 \cdot 3 \cdot 5}{2^2 \cdot 3^2}} = -1 \pm \sqrt{\frac{5}{3}}.$$

Ahora $f''(x) = 6x + 6$, y $6(-1 + \sqrt{5/3}) + 6 > 0$, por lo que $-1 + \sqrt{5/3}$ es un mínimo, también $6(-1 - \sqrt{5/3}) + 6 < 0$, por lo que $-1 - \sqrt{5/3}$ es un máximo. También $x = -1$ es un punto crítico de la derivada, *i.e.*, es un punto de inflexión (véase la Figura 4.14).

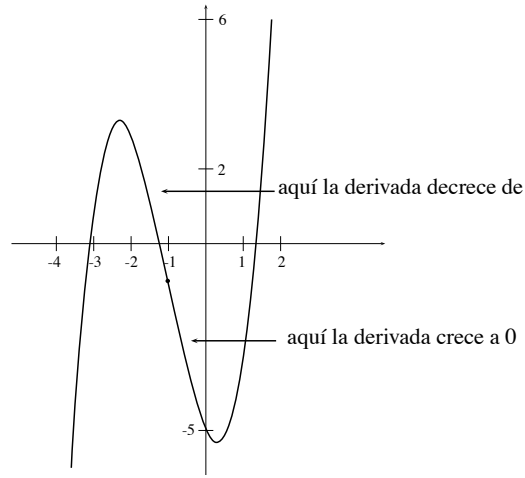


Figura 4.14: Gráfica de $f(x) = x^3 + 3x^2 - 2x - 5$

EJERCICIOS 4.15

1. Exhiba una familia no numerable de polinomios reales, cada uno de los cuales tiene una raíz real y una raíz compleja de multiplicidad 2.

2. Determine el número de raíces reales de los siguientes polinomios.

   a) $x^3 - 3x + 5$,

   b) $x^3 - 5x + 3$.

4.16. Método de Ferrari

Sea

$$f(x) = x^4 + bx^3 + cx^2 + dx + e, \qquad b, c, d, e \in \mathbb{R}.$$

Ferrari observó que si se completaban cuadrados en los términos de grado máximo, se le podía asociar a f un polinomio de grado 3 que de poder resolverse, la solución permitía resolver el polinomio original. Específicamente si x es una raíz de f, se puede escribir:

$$x^4 + bx^3 = -cx^2 - dx - e$$
$$\iff x^4 + bx^3 + \frac{b^2x^2}{4} = -cx^2 - dx - e + \frac{b^2x^2}{4}$$

$$\iff \left(x^2+\frac{b}{2}x\right)^2=\left(\frac{b^2}{4}-c\right)x^2-dx-e. \tag{4.16}$$

La eficacia del método estriba en introducir una nueva variable t que permite completar cuadrados (de nuevo) en el miembro izquierdo de (4.16), mientras que en el derecho se genera una ecuación cuadrática en x con coeficientes en t, b, c, d, e.

Específicamente (4.16) se cumple si y sólo si

$$\left(x^2+\frac{b}{2}x\right)^2+\left(x^2+\frac{b}{2}x\right)t+\frac{t^2}{4}=\left(\frac{b^2}{4}-c\right)x^2-dx-e+\left(x^2+\frac{b}{2}x\right)t+\frac{t^2}{4}$$

$$\iff$$

$$\left(x^2+\frac{b}{2}x+\frac{t}{2}\right)^2=\left(\frac{b^2}{4}-c+t\right)x^2+\left(-d+\frac{b}{2}t\right)x+\left(\frac{t^2}{4}-e\right). \tag{4.17}$$

Obsérvese que si el miembro derecho en (4.17) es de la forma $(Ax+B)^2$, se tendría, conociendo t, que

$$x^2+\frac{b}{2}x+\frac{t}{2}=\begin{cases}(Ax+B)\\ -(Ax+B),\end{cases} \tag{4.18}$$

que ciertamente se puede resolver.

Nótese que el miembro derecho en (4.17) es de la forma

$$(Ax+B)^2=A^2x^2+2ABx+B^2$$

$$\iff$$

$$\left(-d+\frac{b}{2}t\right)^2-4\left(\frac{b^2}{4}-c+t\right)\left(\frac{t^2}{4}-e\right)=0. \tag{4.19}$$

Finalmente, esta ecuación es de 3er grado en la variable t, por lo que se puede resolver y por ende la original. Simplificamos (4.19).

$$d^2-dbt+\frac{b^2t^2}{4}-\frac{b^2t^2}{4}+b^2e+ct^2-4ce-t^3+4te=0$$

o

$$-[t^3-ct^2+(bd-4e)t+(4ce-b^2e-d^2)]=0.$$

Al polinomio

$$g(t)=t^3-ct^2+(bd-4e)t+4ce-b^2e-d^2$$

se le llama el polinomio auxiliar (y es claro que al encontrar una raíz t de g, se puede resolver el polinomio original).

Obsérvese que para escribir el miembro derecho en la expresión (4.17) como

$$A^2x^2 + 2ABx + B^2,$$

los valores A^2, B^2 quedan unívocamente determinados. Para las dos raíces de A^2 y las dos de B^2, se tienen 2 expresiones para $2AB$, la elección lo determina $-d + bt/2$. Se puede fijar A arbitrariamente, y la elección de B o $-B$, la determina el signo de $-d + bt/2$.

Ejemplos.

1) Sea

$$f(x) = x^4 + 4x^3 + x + 1,$$

el polinomio auxiliar es

$$t^3 - ct^2 + (bd - 4e)t + 4ce - b^2e - d^2,$$

como $b = 4,\ c = 0$, y $d, e = 1$ esta expresión es

$$t^3 - 17,$$

que fácilmente se puede resolver.

Se toma $t = (17)^{1/3}$, nótese que $2 < t < 3$, como

$$-d + \frac{bt}{2} = -1 + \frac{4 \cdot 17^{\,1/3}}{2} > 0,$$

$$\begin{aligned} Ax + B &= \sqrt{\frac{b^2}{4} - c + t}\ \ x + \sqrt{\frac{t^2}{4} - e} \\ &= \sqrt{4 + \sqrt[3]{17}}\ \ x + \sqrt{\frac{17^{\,2/3}}{4} - 1}, \end{aligned}$$

y la ecuación original se puede resolver encontrando la solución de

$$x^2 + 2x + \frac{17^{\,1/3}}{2} = \pm\left(\sqrt{4 + 17^{\,1/3}}\, x + \sqrt{\frac{17^{\,2/3}}{4} - 1}\right), \tag{4.20}$$

véase (4.18). Tomando el valor positivo, si

$$\alpha = (4 + 17^{\,1/3})^{1/2} \quad \text{y} \quad \beta = \sqrt{\frac{17^{\,2/3}}{4} - 1},$$

se obtienen dos de las soluciones del polinomio de grado 4 al resolver

$$x^2 + (2-\alpha)x + \frac{17^{\,1/3}}{2} - \beta.$$

Éstas son

$$\frac{-2 + \sqrt{4 + 17^{\,1/3}} \pm \sqrt{8 - 2\sqrt{4+17^{1/3}} + 17^{\,1/3} - 4\left(\frac{17^{1/3}}{2} - \sqrt{\frac{17^{2/3}}{4} - 1}\right)}}{2}$$

etcétera. Nótese que las soluciones pueden ser números complejos, posteriormente se toman los valores negativos en (4.20) obteniéndose las otras dos raíces.

2) Sea

$$f(x) = x^4 + \sqrt{6}x + \frac{1}{4},$$

en este caso $b = c = 0,\ d = \sqrt{6}$ y $e = 1/4$, el polinomio auxiliar es

$$t^3 - ct^2 + (bd - 4e)t + 4ce - b^2e - d^2 = t^3 - t - 6,$$

y $t = 2$ es una solución, por lo tanto las soluciones de $f(x)$ son las de

$$x^2 + \frac{b}{2}x + \frac{t}{2} = \pm(Ax + B).$$

Como

$$A = \pm\sqrt{b^2/4 - c + t} \quad \text{y} \quad B = \pm\sqrt{t^2/4 - e},$$

$A = \pm\sqrt{2},\ B = \sqrt{3}/2,\ 2AB = -d + bt/2 = -\sqrt{6}$, se toma $A = -\sqrt{2}$. Por lo cual hay que resolver

$$x^2 + 1 = \pm\left(-\sqrt{2}x + \frac{\sqrt{3}}{2}\right).$$

Las soluciones de

$$x^2 + \sqrt{2}x + 1 - \frac{\sqrt{3}}{2} \quad \text{y} \quad x^2 - \sqrt{2}x + 1 + \frac{\sqrt{3}}{2},$$

son

$$\frac{-\sqrt{2} \pm \sqrt{2 - 4\left(1 - \frac{\sqrt{3}}{2}\right)}}{2} = -\frac{1}{\sqrt{2}} \pm \sqrt{\frac{1}{2} - 1 + \frac{\sqrt{3}}{2}} = -\frac{1}{\sqrt{2}} \pm \sqrt{-\frac{1}{2} + \frac{\sqrt{3}}{2}}$$

y

$$\frac{\sqrt{2}\pm\sqrt{2-4\left(1+\frac{\sqrt{3}}{2}\right)}}{2}=\frac{1}{\sqrt{2}}\pm\sqrt{\frac{1}{2}-1-\frac{\sqrt{3}}{2}}=\frac{1}{\sqrt{2}}\pm\sqrt{-\frac{1}{2}-\frac{\sqrt{3}}{2}}.$$

Podemos revisar que éstas son las 4 raíces de $f(x)=x^4+\sqrt{6}x+1/4$, si denotamos

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

como aparecen α y $\overline{\alpha}$, el polinomio $x^2-(\alpha+\overline{\alpha})x+|\alpha|^2$ debe ser un factor de $f(x)$, esto es

$$x^2-\sqrt{2}x+\frac{1}{2}+\frac{1}{2}+\frac{\sqrt{3}}{2},$$

y

$$\begin{array}{rrrrr|l}
x^4 & 0 & 0 & \sqrt{6}x & \frac{1}{4} & x^2-\sqrt{2}x+1+\frac{\sqrt{3}}{2} \\
\cline{6-6}
-x^4 & \sqrt{2}x^3 & -(1+\frac{\sqrt{3}}{2})x^2 & & & x^2+\sqrt{2}x+1-\frac{\sqrt{3}}{2} \\
\cline{1-3}
 & \sqrt{2}x^3 & -(1+\frac{\sqrt{3}}{2})x^2 & & & \\
 & -\sqrt{2}x^3 & 2x^2 & -(\frac{\sqrt{3}\sqrt{2}}{2}+\sqrt{2})x & & \\
\cline{2-4}
 & & (1-\frac{\sqrt{3}}{2})x^2 & \sqrt{2}(\frac{\sqrt{3}}{2}-1)x & \frac{1}{4} & \\
 & & & \sqrt{2}(1-\frac{\sqrt{3}}{2})x & -\frac{1}{4} & \\
\cline{3-5}
 & & 0 & 0 & 0 &
\end{array}$$

El cociente es precisamente $x^2+\sqrt{2}x+1-\sqrt{3}/2$ cuyas raíces son reales y son las otras dos raíces de $f(x)=x^4+\sqrt{6}x+\frac{1}{4}$.

Glosario de símbolos

$A[z]$	el anillo de polinomios sobre el anillo A
$\arg z$	argumento del complejo z
C_n^k	número de combinaciones de n elementos tomados de k en k, coeficiente binomial
$\mathbb{C}$	los números complejos
$\mathbb{C}[z]$	el anillo de polinomios sobre los complejos
$a \equiv b \mod m$	a congruente con b módulo m
$\overline{z}$	el conjugado del complejo z
$\supset$	contiene a
D	números decimales
Δ	el discriminante de un polinomio de grado 2 o 3
$a \mid b$	a es un factor de b
$\therefore$	de dónde, por lo tanto
$\sim$	equivalente a, relacionado con
$\in$	pertenece a, es elemento de
$\notin$	no pertenece a, no es elemento de
$\exists$	existe
$\nexists$	no existe
$f'(x)$	derivada de la función $f(x)$
$\mathrm{gr}(p(x))$	grado del polinomio $p(x)$
$g(x) \mid f(x)$	el polinomio $g(x)$ es un factor del polinomio $f(x)$
$\cap$	intersección (de conjuntos)

$K[z]$	el anillo de polinomios sobre el campo K
$\mathbb{N}$	los números naturales
$\neq$	diferente a, no igual a
(a, b)	máximo común divisor de a y b
$[a, b]$	mínimo común múltiplo de a y b
MCD	máximo común divisor
MCM	mínimo común múltiplo
$\prod_{j=1}^{n} a_j$	$a_1\, a_2\, \cdots a_n$
$\forall$	para todo
$\mathbb{Q}$	los números racionales
$\mathbb{R}$	los números reales
$\mathbb{R}[x]$	el anillo de polinomios sobre los reales
$\subset$	subconjunto de
$\sum$	sumatoria
$\sum_{k=0}^{n} a_k$	$a_0 + a_1 + a_2 + a_3 + \cdots + a_n$
$\Longleftrightarrow$	si y sólo si
$\ni$	tal que
$\mid$	tal que, para especificar pertenencia a un conjunto
$\cup$	unión (de conjuntos)
$\emptyset$	el conjunto vacío
$\mathbb{Z}$	los números enteros
$\mathbb{Z}[x]$	el anillo de polinomios sobre los números enteros
$\mathbb{Z}_p$	los campos $\mathbb{Z}_p$, clases de equivalencia en $\mathbb{Z}$ módulo p, p primo

Bibliografía

[1] Bravo A., Rincón H. y Rincón C., *Álgebra Superior*, México, Las Prensas de Ciencias, UNAM, 2008.

[2] Bulaich R., Gómez Ortega J.A. y Váldez R., *Álgebra*, 3a edición, México, Cuadernos de Olimpiadas de Matemáticas, UNAM, Instituto de Matemáticas, 2017.

[3] Cano Figueroa, C., *Notas de Variable Compleja*, Tesis de licenciatura, UNAM, Facultad de Ciencias, 2003.

[4] Cárdenas, H., Lluis, E., Raggi, F., Tomás. F., *Álgebra Superior*, México, Trillas, 1973.

[5] Courant, R., John F., Introducción al Cálculo y al Análisis Matemático, México, Limusa, 2001.

[6] Gómez Laveaga, C., *Álgebra Superior, Curso Completo*, México, Las prensas de Ciencias, UNAM, 2015.

[7] Haaser, N. La Salle J., Sullivan J., *Curso de Análisis Matemático,* Segunda edición, vol. I, México, Trillas, 1970.

[8] Koblitz N. *A Course in Number Theory and Cryptography,* Second Edition, Springer Verlag, New York, 1994.

[9] Lascurain Orive, A., *Álgebra Superior I,* 2a edición, México, Las Prensas de Ciencias, UNAM, 2017.

[10] Maclachan C. and Reed A. *The Arithmetic of Hyperbolic 3-Manifolds,* Springer Verlag GTM, New York, 2003.

[11] Ramírez Galarza A.I., *Geometría Analítica,* 2a edición, México, Las Prensas de Ciencias, UNAM, 2006.

[12] Rudin W. *Principios de Análisis Matemático,* tercera edición, México, McGraw Hill, 1980.

[13] Spivak, M., *Calculus*, W.A. Benjamin, United States of America, 1967.

Índice analítico

algoritmo de Euclides, 13
algoritmo de la división, 4
argumento, 72
Aritmética
    teorema fundamental de la, 19

Cardano-Ferro-Tartaglia
    teorema de, 156
cociente, 4
combinación lineal, 3, 4
congruencia, 23
conjunto
    acotado, 44
cota
    inferior, 44
    superior, 44

De Moivre
    fórmula de, 98
Del factor
    teorema del, 112
Del residuo
    teorema del, 112
discriminante, 97, 156
división sintética, 119
divisibilidad, 1
divisor, 1
    común, 3

ecuaciones diofantinas, 15

Ferrari
    método de, 164
fracciones racionales, 149

ínfimo, 44

Leibnitz
    regla de, 131

mínima combinación lineal, 7
máximo común divisor, 7, 11
método de Horner, 122
método de Newton, 68
método de Sturm, 143
mínimo común múltiplo, 9, 11
módulo, 71
multiplicidad, 129

números complejos, 83
    cociente de, 92
    conjugado, 90
    parte imaginaria, 88
    parte real, 88
    producto de, 86
    raíz cuadrada de, 93
    raices n-ésimas de, 98
    suma de, 83
números racionales, 34
números reales, 41

orden, 41

polinomial
    función, 107
polinomio
    derivada de un, 131
    conjugado, 139
    definición, 103
    factorización de un, 128

grado de un, 103
mónico, 135
raíz de un, 112
polinomios
asociados, 112
irreducibles, 152
máximo común divisor, 141, 142
producto de, 105
simétricos, 137
suma de, 104
primo
número, 18
relativo, 9

residuo, 4

supremo, 44

teorema chino del residuo, 27
transitividad, 41
tricotomía, 41

Álgebra superior II
editado por la Facultad de Ciencias
de la Universidad Nacional Autónoma de México,
se terminó de imprimir el 2 de febrero de 2019
en los talleres de Amy Soluciones Gráficas, S. A. de C. V.
Corregidora 79, Santa Anita, Iztacalco
C.P. 8300. Ciudad de México.

El tiraje fue de 500 ejemplares.
Está impreso en papel cremy book de 60 g.
En su composición se utilizó tipografía
computer modern de 11/13 puntos de pica.

Tipo de impresión: offset

El cuidado de la edición estuvo a cargo de
Patricia Magaña Rueda