Notas de Álgebra Superior 2

Frank Patrick Murphy Hernandez

Jaime García Villeda

Índice general

Introducción

"El álgebra es el arte de encontrar las conexiones invisibles entre los números, transformando la aritmética en una danza elegante de conceptos y estructuras que revelan la profunda simetría oculta en el corazón de las matemáticas."

Frank Murphy

En el vasto universo del álgebra, exploramos las interconexiones entre conceptos aparentemente dispares, desentrañando las complejidades matemáticas que subyacen en la estructura misma de los números. Este libro, titulado .Algebra en Acción: Un Viaje desde los Números Enteros hasta los Anillos de Polinomios", es un compendio en el que nos sumergimos en la esencia misma de la teoría algebraica.

Nuestra travesía comienza en el sólido terreno de los números enteros, esos fieles compañeros de la aritmética cotidiana. A medida que desenterramos las propiedades fundamentales de los dominios enteros, nos adentramos en la prueba del algoritmo de la división, revelando conexiones sorprendentes y aplicaciones prácticas. Este algoritmo, aparentemente simple, se convierte en la puerta de entrada a un vasto mundo de posibilidades algebraicas.

A medida que avanzamos, descubrimos que las similitudes entre el algoritmo de la división y otros conceptos algebraicos son más que meras coincidencias. Exploraremos cómo estas conexiones nos guían hacia los anillos de polinomios, introduciéndonos en un reino donde las expresiones algebraicas se elevan a un nivel superior de abstracción y generalización.

Este libro no solo busca presentar fórmulas y teoremas, sino nutrir una comprensión profunda y orgánica de la álgebra. A través de ejemplos concretos y aplicaciones prácticas, invitamos al lector a participar activamente en este viaje, donde cada paso revela nuevas perspectivas y desafíos emocionantes.

Prepárese para sumergirse en .Algebra en Acción", donde los números, algoritmos y polinomios se entrelazan en una danza matemática que despierta la mente y desafía la imaginación.

[**2**] [**4**] [**1**] [**3**]

Capítulo 1

Números Enteros

En el curso pasado vimos el concepto de número natural, así mismo estudiamos varias de sus propiedades algebraicas. Aún así, desde la intuición los naturales carecen de una operación que hoy en día se nos hace muy familiar: la resta. Aunque cabe mencionar que historicamente llegar a este concepto fue un asunto complicado para la humanidad. Así que continuamos con nuestro camino de formalizar (dentro de lo posible) estos conceptos bien conocidos, y ahora le toca el turno a los enteros.

Para poder trabajar los enteros, primero analizaremos un concepto abstracto que se llama anillo. Esto no es más que nuestra lista de deseos para los enteros, sin embargo los enteros no son los únicos que satisfacen la definición de anillo, por lo cual podremos hacer aritmetica en otros conjuntos que no sean los enteros. De hecho podemos pensar así este curso, estudiar la aritmetica en los enteros, para extenderla en los polinomios.

1. Definición de Anillo y Ejemplos

DEFINICIÓN 1.1 (Anillo). *Sea A un conjunto no vacío con dos funciones $+\colon A\times A\longrightarrow A$ y $*\colon A\times A\longrightarrow A$. Notacionalmente escribimos $a+b:=+(a,b)$ y $ab:=*(a,b)$ para $a,b\in A$. Si estas dos funciones cumplen:*

1. *Para $a,b,c\in A$, $a+(b+c)=(a+b)+c$.*
2. *Existe $0\in A$ tal que para cualquier $a\in A$, $a+0=a=0+a$.*
3. *Para todo $a\in A$, existe $b\in A$ tal que $a+b=0=b+a$.*
4. *Para $a,b\in A$, $a+b=b+a$.*
5. *Para $a,b,c\in A$, $a(bc)=(ab)c$.*
6. *Existe $1\in A$ tal que para cualquier $a\in A$, $a1=a=1a$.*
7. *Para $a,b\in A$, $ab=ba$.*
8. *Para $a,b,c\in A$, $a(b+c)=ab+ac$.*

Entonces llamamos a A un anillo.

EJEMPLO 1.1. *Los ejemplos más conocidos de anillos son:*

- *Los reales $\mathbb{Z}$*
- *Los reales $\mathbb{R}$*
- *Los racionales $\mathbb{Q}$*
- *Los complejos $\mathbb{C}$*

PROPOSICIÓN 1.1. *Sea A un anillo, entonces:*

1. *El neutro aditivo es único.*
2. *El neutro multiplicativo es único.*

DEMOSTRACIÓN.

1. Sean $0'\in A$ otro neutro aditivo. Entonces
$$0=0+0'=0'$$
Por lo que $0=0'$. Así el neutro aditivo es único.
2. Sean $1'\in A$ otro neutro multiplicativo. Entonces
$$1=11'=1'$$
Por lo que $1=1'$. Así el neutro multiplicativo es único.

□

NOTACIÓN 1.1. *Por la proposición anterior, al neutro aditivo le podemos asignar el nombre de cero,* 0*, y al neutro multiplicativo el de uno,* 1*. Dicho de otra manera, antes lo habíamos llamado así por fines pedagogicos, pero ahora sí se han ganado el nombre. Si no fueran únicos, diriamos un cero, un uno. Como son únicos, decimos el uno, el cero. Aquí la propiedad los define, por lo cual se presta a darles un nombre distinguido.*

PROPOSICIÓN 1.2. *Sea A un anillo, entonces:*

1. *Los inversos aditivos son únicos.*
2. *Los inversos multiplicativos son únicos (en caso de existir).*

DEMOSTRACIÓN. 1. Sea $a \in A$ y con inversos aditivos $b, b' \in A$. Si sumamos a b' a la igualdad $a+b=0$, entonces:

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

Por lo que $b = b'$. Así el inverso aditivo es único.

2. Sea $a \in A$ y con inversos multiplicativos $b, b' \in A$. Si multiplicamos a b' a la igualdad $ab = 1$, entonces:

$$b' = (ab)b' = (ab')b = 1b = b$$

Por lo que $b = b'$. Así el inverso multiplicativo es único.

□

NOTACIÓN 1.2. *Por la proposición anterior, si $a \in A$, a su inverso aditivo lo denotaremos por $-a$ y a su inverso multiplicativo por a^{-1}.*

PROPOSICIÓN 1.3. *Sean A un anillo y $a, b, c \in A$, entonces:*

1. $a0 = 0$
2. $(-1)a = -a$
3. $a(-b) = -(ab) = (-a)b$
4. $-(-a) = a$
5. $(-a)(-b) = ab$
6. $-(a+b) = (-a)+(-b)$
7. $a(b-c) = ab-ac$
8. *Si* $a+c = b+c$ *entonces* $a = b$

DEMOSTRACIÓN. 1. Primero consideramos que

$$a0 = a(0+0) = a0+a0$$

Sumando $-a0$ de ambos lados de la igualdad tenemos:

$$a0 = (-a0+a0)+a0 = -a0+(a0+a0) = -a0+a0 = 0$$

2. Empezamos observando:

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

Como el inverso aditivo es único concluimos que $-a = (-1)a$.

3. Tarea
4. Como $a+(-a) = 0$, entonces a es el inveros aditivo de $-a$ y como este es único concluimos que $-(-a) = a$.
5. Tarea
6. Tarea
7. Tarea
8. Tarea
9. Sumando $-c$ de ambos lados de la igualdad tenemos que:

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

10. Tarea

□

2. $\mathbb{Z}$ como Dominio Entero

DEFINICIÓN 2.1. *Sea A un anillo. Decimos que A es un dominio entero, si para todo $a,b \in A$ con $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$.*

Por contrapuesta, esto es equivalente a que si $a,b \in A$ con $ab = 0$, entonces $a = 0$ y $b = 0$.

DEFINICIÓN 2.2. *Sea A un anillo. Decimos que A tienen la propiedad de cancelación, si para todo $a,b,c \in A$ con $c \neq 0$ y $ac = bc$, entonces $a = b$.*

PROPOSICIÓN 2.1. *Sea A un anillo. Entonces A es un dominio entero si y sólo si tiene la propiedad de cancelación.*

DEMOSTRACIÓN. $\Rightarrow$)Sean $a,b,c \in A$ tales que $ac = bc$ con $c \neq 0$. Si pasamos el lado izquierdo restando, entonces tenemos

$$0 = bc - ac = (b-a)c$$

Como estamos en un dominio entero y tenemos un producto igualado a cero. Debe pasar que alguno sea cero, es decir, $b - a = 0$ o $c = 0$. Nuestra hipotesis es que $c \neq 0$. Por lo que lo que debe pasar es que $b - a = 0$. Así $a = b$ y tenemos la propiedad de cancelación.

$\Leftarrow$) Sean $a,b \in A$ con $ab = 0$. Primer caso, si $a = 0$, ya terminamos. Segundo caso, si $a \neq 0$. Entonces

$$ab = 0 = a0$$

Usando la cancelaci'on sobre a, tenemos que $b = 0$. □

Notamos que relamente son en esencia la misma propiedad, sólo que que la de dominio entero es una cancelación para un único elemento, el cero.

DEFINICIÓN 2.3. *Los enteros $\mathbb{Z}$ los definimos como un dominio entero tal que $\mathbb{N} \subseteq \mathbb{Z}$ y que todo $a \in \mathbb{Z}$ cumple una única de las siguientes:*

- $a \in \mathbb{N}^+$
- *a=0*
- $-a \in \mathbb{N}^+$

Aquí $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$. Podemos dar una definición equivalente usando los naturales en vez de los naturales positivos.

DEFINICIÓN 2.4. *Los enteros $\mathbb{Z}$ los definimos como un dominio entero tal que $\mathbb{N} \subseteq \mathbb{Z}$ y que todo $a \in \mathbb{Z}$ cumple una única de las siguientes:*

- $a \in \mathbb{N}$
- $-a \in \mathbb{N}$

3. El Orden de $\mathbb{Z}$

DEFINICIÓN 3.1. *Definimos la relación $<$ en $\mathbb{Z}$, $a < b$ para $a,b \in \mathbb{Z}$ si $b - a \in \mathbb{N}^+$*

PROPOSICIÓN 3.1. *La relacion $<$ es irreflexiva.*

DEMOSTRACIÓN. Para todo $a \in \mathbb{Z}$ tenemos que $0 = a - a \notin \mathbb{N}^+$. Así $a \not< a$. Por lo que la relación es irreflexiva □

PROPOSICIÓN 3.2. *La relacion $<$ es transitiva*

DEMOSTRACIÓN. Sean $a,b,c \in \mathbb{Z}$ tales que $a < b$ y $b < c$. Entonces $b - a \in \mathbb{N}^+$ y $c - b \in \mathbb{N}^+$. La suma de dos naturales positivos es un natural positivo, por lo que $c - a = (b-a) + (c-b) \in \mathbb{N}^+$. Por lo tanto $a < c$. □

Con estas dos propiedades podemos decir que el la relación que difinimos define un orden parcial

PROPOSICIÓN 3.3. *La relacion $<$ cumple tricotomía*

DEMOSTRACIÓN. Sea $a \in \mathbb{Z}$. Entonces a cumple una de las siguientes:

- $a \in \mathbb{N}^+$
- $a = 0$
- $-a \in \mathbb{N}^+$

Así, para en cada caso tendríamos:

- Si $a \in \mathbb{N}^+$, entonces $a > 0$.
- $a = 0$
- Si $-a \in \mathbb{N}^+$, entonces $a < 0$.

□

En este caso podemos decir que nuestro orden parcial cumple la tricotomía, o ser un orden lineal.

El orden que definimos es el menor estricto, así mismo podemos definir el menor o igual. Que como el nombre los dice, $a \leq b$ si $a < b$ o $a = b$. Si empezaramos con el menor igual $\leq$, podríamos inducir el menor esctricto, $a < b$ si $a \leq b$ y $a \neq b$.

En nuestro caso podemos hacerlo directamente de la definción, considerando la segunda definición de enteros. Por lo cual podemos dar la siguiente definción equivalente:

DEFINICIÓN 3.2. *Definimos la relación $\leq$ en $\mathbb{Z}$, $a \leq b$ para $a, b \in \mathbb{Z}$ si $b - a \in \mathbb{N}$*

PROPOSICIÓN 3.4. *Sean $a, b, c \in \mathbb{Z}$. Si $a < b$ entonces $a + c < b + c$.*

Las siguientes dos proposiciones nos dicen que la relación de orden en los enteros es compatible con las dos operaciones, suma y multiplicación.

DEMOSTRACIÓN. Si $a < b$, entonces $b - a \in \mathbb{N}^+$. Así

$$(b + c) - (c + a) = b + (c - c) - a = b + 0 - a = b - a \in \mathbb{N}^+$$

Por lo tanto $a + c < b + c$. □

PROPOSICIÓN 3.5. *Sean $a, b, c \in \mathbb{Z}$. Si $a < b$ y $c > 0$ entonces $ac < bc$.*

DEMOSTRACIÓN. Si $a < b$, entonces $b - a \in \mathbb{N}^+$. De igual manera, como $c > 0$ entonces $c = c - 0 \in \mathbb{N}^+$. Usando que el producto de naturales positivos es un natural positivo, tenemos:

$$cb - ca = c(b - a) \in \mathbb{N}^+$$

Por lo tanto $ac < bc$. □

PROPOSICIÓN 3.6. *Sean $a, b, c \in \mathbb{Z}$. Si $a > 0$ y $b > 0$ entonces $ab > 0$.*

DEMOSTRACIÓN. Como $a > 0$ y $b > 0$, entonces $a, b \in \mathbb{N}^+$. Por lo que $ab \in \mathbb{N}^+$. Por lo tanto $ab > 0$. □

PROPOSICIÓN 3.7. *Sean $a, b, c \in \mathbb{Z}$. Si $a >$ y $b < 0$ entonces $ab < 0$.*

DEMOSTRACIÓN. Como $a > 0$ y $b < 0$, entonces $a, -b \in \mathbb{N}^+$. Por lo que $-ab = a(-b) \in \mathbb{N}^+$. Por lo tanto $ab < 0$. □

PROPOSICIÓN 3.8. *Sean $a, b, c \in \mathbb{Z}$. Si $a <$ y $b < 0$ entonces $ab > 0$.*

DEMOSTRACIÓN. Como $a > 0$ y $b > 0$, entonces $-a, -b \in \mathbb{N}^+$. Por lo que $ab = (-a)(-b) \in \mathbb{N}^+$. Por lo tanto $ab > 0$. □

COROLARIO 3.1. *Sean $a, b \in \mathbb{Z}$. Si $a < b$ entonces $-b < -a$.*

4. Unidades de $\mathbb{Z}$

DEFINICIÓN 4.1. *Sea A un anillo y $a \in A$. Decimos que a es una unidad si tienen inverso multiplicativo. Al conjunto de unidades de A lo denotamos por $U(A)$.*

DEFINICIÓN 4.2. *Sea K un anillo. Decimos que K es un campo, si $U(K) = K \setminus \{0\}$ y $1 \neq 0$.*

PROPOSICIÓN 4.1. *Las unidades de $\mathbb{Z}$ son 1 y -1.*

DEMOSTRACIÓN. Sabemos que tanto 1 y -1 son unidades por que $1 * 1 = 1$ y $(-1)(-1) = 1$. Vamos a considerar el caso de una unidad distinta de estas y vamos a llegar a una contradicción para ver que 1 y -1 son las únicas unidades.

Sea u una unidad con $u \neq 1$ y $u \neq -1$. Por lo que existe $v \in \mathbb{Z}$ tal que $uv = 1$. Notamos que que $u \neq 0$, puesto que si $u = 0$ tendríamos que $0 = uv = 1$. Lo cual no puede ser.

Así podemos dividir el problema en dos casos $u > 0$ y $u < 0$.

Empecemos por $u > 0$. Ahora como $u \neq 1$, tenemos que $u > 1$. Analicemos que para con v, si $v < 0$, entonces $1 = uv < 0$. Por lo que tenemos una contradicción. Así tenemos que $v > 0$. Así multiplicar por v preserva la desiguladad $1 < u$. Por lo que tenemos:

$$1 \geq v = 1v < uv = 1$$

Lo cual es una contradicción $1 < 1$. Por lo cual no puede exisitir una unidad positiva diferente de 1.

Analogamente para -1, será la única unidad negativa. □

5. El Principio de Inducción y el Principio de Buen Orden

El principio de inducción es **la forma** de demostrar propiedades sobre los naturales, esto es debido a la construcción de los naturales. En general cuando se enuncie algún teorema sobre los naturales se demostrará usando inducción o en caso de que no, se demostrará usando resultados que ya fueron demostrados por inducción. La siguiente es la versión conjuntista del principio de inducción.

DEFINICIÓN 5.1 (Principio de Inducción C). . *Sea $A \subseteq \mathbb{N}$ tal que:*

1. $0 \in A$.
2. *Para cada $n \in \mathbb{N}$, si $n \in A$ entonces $n+1 \in A$*

Entonces $A = \mathbb{N}$

Al punto 1 se le llama la base de induccón y al punto 2 el paso inductivo. La versión más común del principio de inducción es:

DEFINICIÓN 5.2 (Principio de Inducción P). . *Sea p una propiedad, si:*

1. *$p(0)$ (0 cumple la propiedad).*
2. *Para cada $n \in \mathbb{N}$, si $p(n)$ entonces $p(n+1)$ (si n cumple la propiedad, entonces $n+1$ cumple la propiedad)*

Entonces para cada natural n, $p(n)$ (Todos los naturales cumplen la propiedad).

EJEMPLO 5.1. *Sea $A = \{n \in \mathbb{N} \mid \sum_{i=0}^{n} i = (n^2+n)/2\}$, primero $\sum_{i=0}^{0} i = 0 = (0^2+0)/2$ por lo que el paso base se cumple. Ahora supondrá que $\sum_{i=0}^{n} i = (n^2+n)/2$, a esto se le llama la hipótesis de inducción, y se suma $n+1$ de ambos lados $\sum_{i=0}^{n+1} i = (\sum_{i=0}^{n} i) + (n+1) = (n^2+n)/2 + (n+1) = ((n+1)^2 + (n+1))/2$. Por lo que si $n \in A$ entonces $n+1 \in A$ y por el principio de inducción $A = \mathbb{N}$. Lo que dice que la formula $\sum_{i=0}^{n} i = (n^2+n)/2$ se cumple para todo los naturales.*

Nótese que éstos principios son equivalentes , si se empieza con el **PIC** para llegar al **PIP** solo se considera al conjunto $A = \{n \in \mathbb{N} \mid p(n)\}$ y para el regreso se considera la propiedad $p(n) := n \in A$. Al PIC se le llamará PI a secas.

Ahora se enuncian otros principios de inducción y recuérdese que para cada $n \in \mathbb{N}$, $I_n := \{m \in \mathbb{N} \mid m < n\} = \{0, 1, \ldots, n-1\}$.

DEFINICIÓN 5.3 (Principio de Inducción Fuerte). . *Sea $A \subseteq \mathbb{N}$ tal que:*

1. $0 \in A$
2. *Para cada $n \in \mathbb{N}$, si $I_n \subseteq A$ entonces $n \in A$.*

Entonces $A = \mathbb{N}$.

DEFINICIÓN 5.4 (Principio de Inducción Generalizado). . *Sea $A \subseteq \mathbb{N}$ tal que:*
Para cada $n \in \mathbb{N}$, si $I_n \subseteq A$ entonces $n \in A$.
Entonces $A = \mathbb{N}$.

PROPOSICIÓN 5.1. *Los tres principios de inducción (PI, PIF, PIG) son equivalentes.*

Antes de empezar la demostración note que los tres principios son implicaciones y todas con el mismo consecuente, asi que lo que se busca demostrar es una proposición de lo forma $(P \Rightarrow Q) \Rightarrow (R \Rightarrow Q)$. La hipótesis es $P \Rightarrow Q$ y lo que hay que demostrar es $R \Rightarrow Q$. La forma usual de hacer esta demostración es demostrar que $R \Rightarrow P$ y por transitividad se deducirá lo deseado. Esto es una forma curiosa de demostrar que una implicaci´on implica otra implicación pues lo que se demuestra es que la hipótesis de segunda implicación implica la hipótesis de la primera implicación.

DEMOSTRACIÓN. PI $\Rightarrow$ PIF)

DEFINICIÓN 5.5. *Sea $A \subseteq \mathbb{N}$ tal que:*

1. $0 \in A$
2. *Para cada $n \in \mathbb{N}$, si $I_n \subseteq A$ entonces $n \in A$.*

Sea $m \in \mathbb{N}$ tal que $m \in A$ y se busca demostrar que $m+1 \in A$, esto se hara demostrando que $I_{m+1} \subseteq A$ y aplicando 2 se tendrá que $m+1 \in A$. Para esto defínase $A_m = \{k \in \mathbb{N} \mid k \leq m \Rightarrow I_{k+1} \subseteq A\}$. Ahora se aplicará el PI sobre A_m. Primero como $m \in \mathbb{N}$, $0 \leq m$ y por hipótesis $\{0\} \subseteq A$, entonces $0 \in A_m$. Ahora sea $k \in A_m$, hay dos casos.

Caso $m \leq k$) Si $m \leq k$ entonces $m < k+1$. Por lo que el antecedente es falso y $k+1 \in A_m$.

Caso $k < m$) Si $k < m$ entonces $k+1 \leq m$ y $I_{k+1} \in A$. Pero por 2 $k+1 \in A$, de lo que $I_{k+1} \cup \{k+1\} \subseteq A$ pero $l_{k+1} \cup \{k+1\} = I_{k+2}$. Por lo tanto $k+1 \in A_m$.

Por el PI, $A_m = \mathbb{N}$. Lo que quiere decir que $I_{m+1} \subseteq A$ y por 2 $m+1 \in A$. Por lo que A cumple 1 y 2 de PI se tiene que $A = \mathbb{N}$.

PIF$\Rightarrow$PIG) Sea $A \subseteq \mathbb{N}$ tal que para cada $n \in \mathbb{N}$, si $I_n \subseteq A$ entonces $n \in A$. Nótese que $I_0 = \varnothing$ y $I_0 \subseteq A$, entonces $0 \in A$. Entonces A cumple 1 y 2 de PIF, entonces $A = \mathbb{N}$.

DEFINICIÓN 5.6. *PIF $\Rightarrow$ PI) Sea $A \subseteq \mathbb{N}$ tal que:*

1. $0 \in A$
2. *Para cada $n \in \mathbb{N}$, si $n \in A$ entonces $n+1 \in A$.*

Sea $m \in N$ tal que $I_m \subseteq A$, y se quiere demostrar que $m \in A$. Si $m = 0$ entonces $I_0 \subseteq A$ y por 1 $0 \in A$. Si $m \neq 0$ entonces $m = k+1$ para algún $k \in \mathbb{N}$, por lo que si $I_{k+1} \subseteq A$ y en particular se tiene que $k \in A$ por los que por 2 $m = k+1 \in A$. Por el PIG se tiene que $A = \mathbb{N}$.

□

Otro principio que es equivalente al pincipio de inducción es el principio del buen orden, que dice que el orden canónico de los naturales es un buen orden.

Principio del Buen Orden. Sea $B \subseteq \mathbb{N}$, si $B \neq \varnothing$ entonces existe $b \in B$ tal que para cada $x \in B$, $b \leq x$.

El PBO dice que todo subconjunto de los naturales no vacío tiene un elemento menor.

PROPOSICIÓN 5.2. *El principio de inducción y el principio del buen orden son equivalentes*

DEMOSTRACIÓN. $\Rightarrow$) Primero la ida, el principio de inducción implica el principio del buen orden, sea $B \subseteq N$ con $B \neq \varnothing$, y se tiene que demostrar que B tiene un elemento mínimo, para hacer esto se supondrá que B no lo tiene y llegaremos a la contradicción de que B es vacío.

Se empieza suponiendo que B no tiene un mínimo y se sigue definiendo A como el conjunto de todos los naturales que son menores a todos los elementos de B, es decir, $A = \{a \in \mathbb{N} \mid a < b, \forall b \in B\}$ y se hace notar que si $a \in A$ entonces no se puede dar el caso de que $a \in B$, por que si pasase $a < a$, lo que es una contradicción, por lo cual se sigue que A es un subconjunto del complemento de B en los naturales, $A \subseteq (\mathbb{N} \setminus B)$.

Se pasa a demostrar que $A = \mathbb{N}$ por inducción, para la base se tiene que $0 \in A$, inmediatamente se observa que si $0 \in B$ entonces B tendra un mínimo contradiciendo lo supuesto, así que $0 \in \mathbb{N} \setminus B$, más aún $0 < b$ para toda $b \in B$, entonces $0 \in A$.

Para el paso inductivo, se supone que $n \in A$ y que $n+1 \notin A$, entonces negando la condición para pertencer a A se tiene que existe $b_0 \in B$ tal que $b_0 \leq n+1$, por hipótesis de inducción$n \in A$ que implica que $n < b_0$, por lo que se sigue que $n+1 \leq b_0$ y de aquí $b_0 = n+1$, nótese que esto implica que b es un mínimo de B, puesto que como $n < b$ para toda $b \in B$, entonces $n+1 \leq b$ para toda $b \in B$ y con el hecho de que $n+1 = b_0 \in B$, dice que b_0 es un mínimo, que contradice la suposición de que B no tenía elemento mínimo, por lo que $n+1 \in A$.

Por el principio de inducción $A = \mathbb{N}$, pero $A \subseteq \mathbb{N} \setminus B$ lo que implica que $\mathbb{N} = \mathbb{N} \setminus B$ y de aquí $B = \varnothing$ contraciendo el hecho de que fuese no vacío. Por lo cual B debede tener un mínimo.

$\Leftarrow$) Ahora el regreso, el principio del buen implica el principio de inducción. Sean A un subconjunto de los naturales que cumple que $0 \in A$ y si $n \in A$ entonces $n+1 \in A$, y B el complemento de A en los naturales, si se logra de demostrar que B es vacío abremos terminado pues esto último implica que $A = \mathbb{N}$.

Si B fuese distinto del vacío, por el principio del buen orden se tendría que B tiene un elemento mínimo b_0, como b_0 es distinto de 0 tiene que ser sucesor de alguien, por lo que existe k natural tal que $b_0 = k+1$, pero k no puede ser elemento de B pues b_0 es mínimo, así que k es un elemento de A, pero por hipótesis esto implica que $k+1$ es un elemento de A, pero $k+1 = b_0$ y esto es una contadicción puesto que A y B no tienen elementos en común. Esto vino de suponer que B es no vacío, por lo tanto B es vacío como se deseaba.

Otra demostración quizá más directa. Empezando con el PIG,

$$\forall A \subseteq \mathbb{N}\Big((\forall n \in \mathbb{N}, I_n \subseteq A \Rightarrow n \in A) \Rightarrow A = \mathbb{N}\Big)$$

Usando la contrapuesta se tiene que lo anterior es equivalente a:

$$\forall A \subseteq \mathbb{N}, \neg(A = \mathbb{N}) \Rightarrow \neg(\forall n \in \mathbb{N}, I_n \subseteq A \Rightarrow n \in A)$$

Negando las proposiciones, se tiene:

$$\forall A \subseteq \mathbb{N}, (A \neq \mathbb{N}) \Rightarrow (\exists n \in \mathbb{N}, I_n \subseteq A \wedge n \notin A)$$

Observando que como $A \subseteq \mathbb{N}$, se tiene que $A \neq \mathbb{N}$ si y sólo si $N \setminus A \neq \varnothing$. Poniendo $B = \mathbb{N} \setminus A$ y sustituyendo. Se observa que $I_n \subseteq A$ si y sólo si $I_n \cap B = \varnothing$. Por lo que se tiene que:

$$\forall B \subseteq \mathbb{N}, (B \neq \varnothing) \Rightarrow (\exists n \in \mathbb{N}, I_n \cap B = \varnothing \wedge n \in B)$$

Recordando I_n es el conjunto de los naturales menores que n, $I_n \cap B = \varnothing$ dice que no hay elementos menores que n en B y como $n \in B$, esto quiere decir que n es el menor elemento de B, por lo que se tiene que:

$$\forall B \subseteq \mathbb{N}, (B \neq \varnothing) \Rightarrow (\exists n \in B, \forall x \in B, n \leq x)$$

Que es el PBO. □

Lo interesante de la ultima prueba es que demuestra que el PBO es solo la contrapuesta del PIG. Más interesante aún es que la ultima proposición dice que en todo conjunto bien ordenado se puede aplicar inducción.

Ahora se tienen varias versiones del principio de inducción y se usara indiscriminadamente cualquier versión sin previo aviso.

Es común tener teoremas sobre ciertos subconjuntos de los naturales como los pares, los primos, los naturales menores ak o lo mayores a k, en este caso tambi´en se puede usar inducción. La primera forma es para $X \subseteq N$ distinto del vacío y $B \subseteq X$, se aplica el principio de inducción sobre el conjunto $A = \{n \in \mathbb{N} \mid n \in X \Rightarrow n \in B\}$. Esta forma es un poco complicada, lo que dice es que si en el conjunto X y se tiene un subconjunto B de X, entonces se puede aplicar el principio de inducción para demostrar que $B = X$, ésta forma de aplicar inducción tiene la ventaja de hacer facil de demostrar el caso base. Pero más facil de entender es el hecho de restringir la inducción vía restringir el buen orden.

Si B con la relación $\leq$ es un buen orden y se toma a C subconjunto de B, se le puede asignar la misma relación a C y ver que es un buen orden en C, ya que si X es un subconjunto de C distinto del vacío entonces X es un subconjunto de B distinto del vacío y como $\leq$ es un buen orden X tendrá un elemento menor, que es lo que se buscaba.

Por lo observado anteriormente y por la proposición 2 se tiene que se puede aplicar inducción en los subconjuntos de los naturales, solo que ciertas observaciones se tienen que hacer, primero en la parte 2 del PI dice que si $n \in A$ entonces $n+1 \in A$, si se desease aplicar inducción en los pares el hecho de sumarle uno a un par lo hace un impar y deja de tener sentido, con $n+1$ se refiere al sucesor de n que en los naturales es $n+1$, pero en los pares $n+2$. Si $B \subseteq \mathbb{N}$ y $n \in B$, el sucesor de n en B, $s_B(n) = \min\{k \in B \mid k > n\}$, claro que $\{k \in B \mid k > n\}$ tiene que ser diferente para que hablar del mínimo tenga sentido. La segunda observación es que 0 no tiene por que estar en B, por ejemplo si quiero hacer inducción sobre los impares, así que en lugar de 0 en la primera se sustituye por $\min B$. Por lo que principio de inducción para subconjuntos de los naturales es:

DEFINICIÓN 5.7 (Principio de Inducción S). . *Sea $B \subseteq \mathbb{N}$ con B distinto del vacío. Si $X \subseteq B$ tal que:*

1. $\min B \in X$
2. *Para cada $n \in B$, si $n \in X$ y $s_B(n)$ existe, entonces $s_B(n) \in X$.*

Entonces $X = B$

DEFINICIÓN 5.8 (Principio de Inducción I). . *Sea $B \subseteq \mathbb{N}$ con B infinito. Si $X \subseteq B$ tal que:*

1. $\min B \in X$
2. *Para cada $n \in B$, si $n \in X$, entonces $s_B(n) \in X$.*

Entonces $X = B$

EJEMPLO 5.2. *Sean $\mathbb{P} = \{2n \mid n \in \mathbb{N}\}$ el conjunto de los pares no negativos y $A = \{n \in \mathbb{P} \mid (-1)^n = 1\}$. Como $0 \in \mathbb{P}$ es el primer elemento par, y $(-1)^0 = 1$, por lo que $0 \in A$, por lo tanto se cumple el paso base. Ahora la hipótesis de inducción es que se cumple para $n \in A$, pero ese n es de la forma $2k$ con $k \in \mathbb{N}$ asi que el sucesor de n es $n+2$ que es el siguiente par, por lo que $(-1)^{n+2} = (-1)^n(-1)^2 = 1$. Por lo tanto $A = \mathbb{P}$.*

Por último un ejemplo de cómo no usar inducción, éste ejemplo se le debe a Pólya, consideremos la siguiente afirmación, todos los caballos tienen el mismo color, para facilitar el entendimiento se considerara que hay tantos caballos como naturales, es decir, que C_n es el n-esimo caballo y que c_n es el color del n-ésimo caballo. Se demostrará que por inducción que para cualquier n natural, si se tienen n caballos entonces estos n caballos tienen el mismo color. Para el paso base $n = 0$, es claro que si no se tienen caballos, pues estos tienen el mismo color, para aclarar un poco más las cosas, se considera el caso $n = 1$, si solo se tiene un caballo pues también todos los caballos tienen el mismo color. Ahora supone valido para n, es decir, para cualquier conjunto con n caballos todos los caballos de éste conjunto tiene el mismo color. Suponemos que se tiene un conjunto con $n+1$ caballos $\{C_1, \ldots, C_n, C_{n+1}\}$ entonces para el subconjunto $\{C_1, \ldots, C_n\}$ que consta de n caballos todos sus caballos tienen el mismo color por hipótesis de inducción, de manera análoga pasa igual para $\{C_2, \ldots, C_n, C_{n+1}\}$, pero C_2 esta en ambos conjuntos por los el color de los caballos del primer subconjunto es igual al color de los caballos del segundo subconjunto, de aquí se sigue que los $n+1$ caballos tienen el mismo color. Por el principio de inducción todos los caballos tienen el mismo color.

¿Qué error tiene la prueba anterior? Considere el paso inductivo cuando se aplica de 1 para 2 los subcojuntos son $\{C_1\}$ y $\{C_2\}$ que no tienen un caballos en común para aplicar la transitividad a los colores, como es natural hemos visto dos caballos de diferentes colores y es justo lo que hace fallar la prueba, que el argumento no funciona para 2.

6. Construcción de $\mathbb{Z}$

DEFINICIÓN 6.1. *Definimos la relación $\sim$ en $\mathbb{N} \times \mathbb{N}$ como $(a,b) \sim (c,d)$, si $a+d = b+c$.*

PROPOSICIÓN 6.1. *La relación $\sim$ es una relación de equivalencia.*

DEMOSTRACIÓN.
- Sea $(a,b) \in \mathbb{N} \times \mathbb{N}$. Entonces $a+b = b+a$. Así $(a,b) \sim (a,b)$ y la relación es reflexiva.

- Sean $(a,b),(c,d) \in \mathbb{N}\times\mathbb{N}$ con $(a,b)\sim(c,d)$. Entonces $a+d=b+c$, que es lo mismo que $c+b=d+a$. De aquí $(c,d)\sim(a,b)$. Por lo que la relación es simétrica.
- Sean $(a,b),(c,d),(e,f) \in \mathbb{N}\times\mathbb{N}$ con $(a,b)\sim(c,d)$ y $(c,d)\sim(e,f)$. Entonces $a+d=b+c$ y $c+f=d+e$. Sumando f de ambos lados tenemos y sustituyendo $a+d+f=b+c+f=b+d+e$. Cancelando d, tenemos que $a+f=b+e$. Por lo que $(a,b)\sim(e,f)$ y así la relación es transitiva.

□

DEFINICIÓN 6.2. *Definimos a $\mathbb{Z}$ como $\mathbb{N}^2/\sim$*

Denotaremos a las clases de equivalencia por $[a,b]$ en vez de $[(a,b)]$.

DEFINICIÓN 6.3. *Definimos la suma y la multiplicación $+\colon \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$ y $*\colon \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$ como $[a,b]+[c,d]=[a+c,b+d]$ y $[a,b][c,d]=[ac+db,ad+bc]$*

PROPOSICIÓN 6.2. *Las operaciones estan bien definidas.*

DEMOSTRACIÓN. □

PROPOSICIÓN 6.3. *$\mathbb{Z}$ es un dominio entero con las operaciones anteriores*

DEMOSTRACIÓN. □

DEFINICIÓN 6.4. *Sean $[a,b],[c,d]\in\mathbb{Z}$. Definimos $[a,b]<[c,d]$, si $a+d<b+c$.*

PROPOSICIÓN 6.4. *La relación $<$ es irreflexiva, transitiva y lineal.*

DEMOSTRACIÓN. □

PROPOSICIÓN 6.5. *La funciíón $i\colon \mathbb{N}\longrightarrow\mathbb{Z}$ dada por $i(x)=[x,0]$ preserva suma, multiplicación y orden.*

DEMOSTRACIÓN. □

PROPOSICIÓN 6.6. *Si identificamos $\mathbb{N}$ con $im(i)$, entonces $\mathbb{Z}$ es un modelo de los enteros.*

DEMOSTRACIÓN. □

Ejercicios del capítulo

Sean A un anillo y $a,b,c,d\in A$.

EJERCICIO 6.1. *Demuestre que el neutro multiplicativo de un anillo es único.*

EJERCICIO 6.2. *Demuestre que si $a+c=b+c$ entonces $a=b$.*

EJERCICIO 6.3. *Demuestre que:*

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

EJERCICIO 6.4. *a es unidad si y sólo si $-a$ es unidad*

EJERCICIO 6.5. *Supongamos que A es un dominio entero. Demuestre que $a^2=0$ si y sólo si $a=0$.*

EJERCICIO 6.6. *Para este ejercicio supongamos que $A=\mathbb{Z}$. Demuestre lo siguiente:*

1. *$a\neq 0$ si y sólo si $a^2>0$*
2. *$a<0$ si y sólo si $-a>0$*
3. *Si $0<a<b$ entonces $a^2<b^2$*

4. *Si* $a,b > 0$ *y* $a^2 < b^2$ *entonces* $a < b$
5. *Si* $a < b$ *y* $c > d$ *entonces* $a - c < b - d$

EJERCICIO 6.7. *Supongamos que* $A = \mathbb{Z}$. *Demuestre lo siguiente:*

1. *Si* $a > 1$ *entonces* $a^2 > a$
2. *Si* $0 < a < b$ *y* $0 < c < d$ *entonces* $ac < bd$
3. *Si* $a,b > 0$ *y* $a^2 < b^2$ *entonces* $a < b$

DEFINICIÓN 6.5. *Si A es un anillo (con 1),* $S \subseteq A$ *es un subanillo si satisface las siguientes condiciones:*

1. $1 \in S$
2. *Para todo* $x,y \in S$, $x - y \in S$.
3. *Para todo* $x,y \in S$, $xy \in S$.

EJERCICIO 6.8. *Demuestra que* $\mathbb{Z}$ *es el único subanillo de* $\mathbb{Z}$.

EJERCICIO 6.9. *Demuestra que son equivalentes el Principio de Inducción y el Principio de Inducción Generalizado.*

Demuestra usando el principio de inducción las siguientes afirmaciones

EJERCICIO 6.10. *Si* $r \in \mathbb{R} \setminus \{1\}$ *entonces para todo* $n \in \mathbb{N}$, $\sum_{k=0}^{n} r^k = \frac{1-r^{n+1}}{1-r}$.

EJERCICIO 6.11. *Para todo* $n \in \mathbb{N}$, $\sum_{j=0}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1)$

EJERCICIO 6.12. *Para todo* $n \in \mathbb{N}$, $\sum_{j=0}^{n} j^3 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2$

EJERCICIO 6.13. *Para todo* $n \in \mathbb{N}$, 10^n *deja residuo* 1 *al ser dividido por* 9.

EJERCICIO 6.14. *Para todo* $n \in \mathbb{N}$, *con* $n \geq 10$, $2^n \geq n^3$.

EJERCICIO 6.15. *Para todo* $n \in \mathbb{N}^+$ *y para todo* $k \in \mathbb{N}$ *tal que* $n \geq k^2 + 1$, $n^k \leq 2^n$.

EJERCICIO 6.16. *Para todo* $n \in \mathbb{N}$ *y para todo* $x \in \mathbb{R}$ *con* $x > -1$, $(1+x)^n \geq 1 + nx$.

EJERCICIO 6.17. *Para todo* $n \in \mathbb{N}^+$ *existe un único* $k \in \mathbb{N}$ *tal que* $n = 2^k s$, *con s impar.*

EJERCICIO 6.18. *Se define la sucesión* $\{t_n\}_{n=0}^{\infty}$, *donde para todo* $n \in \mathbb{N}$, $t_n = \frac{n(n+1)}{2}$. *Demuestra lo siguiente:*

1. *Para todo* $n \in \mathbb{N}$, $t_n \in \mathbb{N}$.
2. *Para todo* $n \in \mathbb{N}^+$, $\sum_{j=1}^{n} \frac{1}{t_n} = 2 - \frac{2}{n+1}$.
3. *Todo cuadrado perfecto es suma de dos elementos de la sucesión definida.*

EJERCICIO 6.19. *Para todo $n \in \mathbb{N}^+$, el último dígito de 5^n es 5.*

EJERCICIO 6.20. *Sea $\{F_n\}_{n=1}^{\infty}$ la sucesión de Fibonacci. Demuestra que para todo $n \in \mathbb{N}$ con $n \geq 2$:*

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Utiliza este ejercicio para demostrar que bajo las mismas condiciones $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$.

EJERCICIO 6.21. *Sea $D = \{f : \mathbb{R} \to \mathbb{R} | f$ es derivable$, 0 \notin im(f)\}$.*

1. *¿Es D un anillo?*
2. *Demuestra que si $f_1, ..., f_n \in D$, entonces:*

$$\frac{(\prod_{j=1}^n f_j)'}{\prod_{j=1}^n f_j} = \sum_{j=1}^n \frac{f_j'}{f_j}$$

DEFINICIÓN 6.6. *Si X es un conjunto y $f : X \to X$ es una función, se define de manera recursiva lo siguiente:*

1. $f^0 = 1_X$.
2. *Para todo $n \in \mathbb{N}$, $f^{n+1} = f^n \circ f$.*

EJERCICIO 6.22. *Sea $f : \mathbb{N} \to \mathbb{N}$ una función tal que $f(0) = 1$ y para todo $n \in \mathbb{N}^+$, $f(n) < n$. Demuestra que para todo $n \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $f^k(n) = 1$.*

EJERCICIO 6.23. *(Principio de doble inducción) Demuestra que para todo conjunto $A \subseteq \mathbb{N} \times \mathbb{N}$ tal que:*

1. $(0,0) \in A$.
2. *Para todo $m \in \mathbb{N}$ tal que $(m,0) \in A$ entonces $(m+1,0) \in A$.*
3. *Para todo $m \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ tal que $(m,n) \in A$ entonces $(m,n+1) \in A$*

entonces $A = \mathbb{N} \times \mathbb{N}$.

EJERCICIO 6.24. *Demuestra usando el principio de doble inducción que para todo $n, m \in \mathbb{N}$, $(m+1)^n > mn$.*

Capítulo 2

Divisibilidad

1. Definición y propiedades básicas

DEFINICIÓN 1.1. *Sean $a,b \in \mathbb{Z}$. Decimos que a divide a b, lo que escribiremos $a \mid b$, si existe $c \in \mathbb{Z}$ tal que $b = ac$. Si a no divide a b, escribiremos $a \nmid b$.*

EJEMPLO 1.1.

i) $2 \mid 10$
ii) $3 \nmid 7$
iii) $17 \mid 51$
iv) $12 \mid 72$
v) $3 \nmid 101$
vi) $77 \nmid 144$
vii) $-3 \mid 6$
viii) $7 \mid -28$
ix) $-3 \mid -27$

OBSERVACIÓN 1.1. *Para cualquier $a \in \mathbb{Z}$,*

1. $1 \mid a$
2. $a \mid 0$
3. $a \mid a$

Nótese que la noción "ser divisible" define una relación en $\mathbb{Z}$. Los siguientes resultados muestran algunas propiedades de dicha relación.

PROPOSICIÓN 1.1. *Sean $a,b,c \in \mathbb{Z}$ tales que $a \mid b$ y $b \mid c$, entonces $a \mid c$.*

DEMOSTRACIÓN. Por hipótesis existen $d,e \in \mathbb{Z}$ tales que $b = ad$ y $c = be$. De esto se deduce que $c = a(de)$. □

PROPOSICIÓN 1.2. *Sean $a,b \in \mathbb{Z}$ tales que $a \mid b$ y $b \mid a$, entonces existe $u \in U(\mathbb{Z})$ tal que $a = bu$.*

DEMOSTRACIÓN. Si $b = 0$, entonces $a = 0$, pues $b \mid a$, por lo que la afirmación es cierta en este caso tomando $u = 1$. Ahora supongamos que $b \neq 0$. Dado que $a \mid b$, existe $v \in \mathbb{Z}$ tal que $b = av$, mientras que como $b \mid a$, existe $u \in \mathbb{Z}$ tal que $a = bu$. De las dos igualdades se deduce que $b = buv$. Como $b \neq 0$, por la propiedad de cancelación $uv = 1$, lo que dice que $u \in U(\mathbb{Z})$. □

COROLARIO 1.1. *Sean $a,b \in \mathbb{N}$. Si $a \mid b$ y $b \mid a$, entonces $a = b$.*

Respecto a la relación de divisibilidad, notemos que el inciso 3 de la observación 1.1 dice que esta es reflexiva. Además la proposición 1.1 dice que esta relación es transitiva. Como se puede ver en la proposición 1.2, esta relación no es simétrica, sin embargo, si nos retringumos a los naturales, esta lo es.

PROPOSICIÓN 1.3. *Sean $a,b \in \mathbb{Z}$ con $b \neq 0$. Si $a \mid b$, entonces $|a| \leq |b|$.*

DEMOSTRACIÓN. Como $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = ac$. Note que como $b \neq 0$, entonces $c \neq 0$. Además $|b| = |a||c|$ y como $|c| \geq 1$, se deduce el resultado. □

PROPOSICIÓN 1.4. *Sean $a,b,c \in \mathbb{Z}$.*

1. *Si $a \mid b$ y $a \mid c$, entonces $a \mid b+c$*
2. *Si $a \mid b$, entonces $a \mid bc$*

DEMOSTRACIÓN. Para la primera afirmación, existen $d,e \in \mathbb{Z}$ tales que $b = ad$ y $c = ae$, por lo que $b+c = a(d+e)$, de lo que se deduce el resultado.

Respecto a la segunda afirmación, como $a \mid b$, existe $d \in \mathbb{Z}$ tal que $b = ae$. De esto se deduce que $bc = a(ec)$, lo que muestra la afirmación. □

NOTACIÓN 1.1. *Dados dos enteros a,b, una combinación $\mathbb{Z}$-lineal de estos es un entero de la forma $as+bt$ para algunos $s,t \in \mathbb{Z}$.*

De la última proposición y la terminología introducida se deduce que:

COROLARIO 1.2. *Si $a,b,c \in \mathbb{Z}$ tales que $a|b$ y $a|c$, entonces a divide a cualquier combinación $\mathbb{Z}$-lineal de b y c.*

Para concluir con esta sección vamos a presentar un resultado muy importante que nos da una forma de "medir" que tanto difiere un entero de ser divisible por otro.

PROPOSICIÓN 1.5. *(Algoritmo de la división) Sean $a,b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos $q,r \in \mathbb{Z}$ tales que $a = bq+r$ con $0 \leq r < |b|$.*

DEMOSTRACIÓN. Respecto a la existencia, consideremos el conjunto $A = \{a-bm \,:\, m \in \mathbb{Z}\}$. Afirmamos que $A \cap \mathbb{N} \neq \emptyset$, para lo que procediendo por contradicción, si $A \cap \mathbb{N} = \emptyset$, entonces $A \subseteq \{n \in \mathbb{Z} \,:\, n < 0\}$. Denotemos por $-A := \{-c \,:\, c \in A\}$ y notemos que $-A \subseteq \mathbb{N}$. Como claramente $A \neq \emptyset$, entonces por el principio del buen orden existe $t_0 = \text{mín}(-A)$. Por definición existe $m_0 \in \mathbb{Z}$ tal que $t_0 = -(a-bm_0)$. Como existe $u \in U(\mathbb{Z})$ tal que $|b| = ub$, entonces se deduce que:

$$t_0 - |b| = -(a-b(m_0-u))$$

Observemos que esta igualdad muestra que $t_0 - |b| \in -A$, sin embargo, $t_0 - |b| < t_0$, lo que contradice la minimalidad de t_0. Por lo tanto se deduce que $A \cap \mathbb{N} \neq \emptyset$. Así que por el principio del buen orden existe $r = \text{mín}(A \cap \mathbb{N})$. Por definición esto dice que existe $q \in \mathbb{Z}$ tal que $r = a-bq$, de donde se deduce que $a = bq+r$ y $r \geq 0$. Lo que resta demostrar es que $r < |b|$, para lo cual, procediendo por contradicción, supongamos que $|b| \leq r$. Dado que $|b|, r \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que $|b|+n = r$. Dado que existe $u \in U(\mathbb{Z})$ tal que $|b| = ub$, entonces se deduce que:

$$a = bq+r = (q+u)b+n$$

Notemos que como $|b|+n = r$ y $b \neq 0$, entonces $n < r$, lo que contradice la minimalidad de r, por lo tanto, $r < |b|$.

Para concluir con la demostración, vamos a ver que los elementos considerados son únicos, es decir, supongamos que $q, q', r, r' \in \mathbb{Z}$ son tales que $a = bq + r = bq' + r'$ con $0 \leq r < |b|$ y $0 \leq r' < |b|$. Observe que de esto se deduce que $b(q - q') = r' - r$, lo que dice que $b|r' - r$, lo que implica que $|b| \leq |r' - r|$. Note que $|r' - r| < b$, lo que nos lleva a una contradicción a no ser que $r' - r = 0$, lo que implica que $r' = r$. Además, como $bq = bq'$ y $b \neq 0$, entonces $q = q'$. □

NOTACIÓN 1.2. *Al único r que aparece en el algoritmo de la división se le conoce como el residuo de dividir a por b.*

COROLARIO 1.3. *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Si $a = bq + r$, entonces $b \mid a$ si y sólo si $r = 0$.*

2. Máximo común divisor

NOTACIÓN 2.1. *Para $a \in \mathbb{Z}$, definimos el conjunto de divisores de a como:*

$$D_a := \{b \in \mathbb{Z} \ : \ b \mid a\}$$

El conjunto de divisores positivos de a, se define como el conjunto:

$$D_a^+ := D_a \cap \mathbb{N}^+.$$

OBSERVACIÓN 2.1. *Observemos que para $a, b \in \mathbb{Z}$, $D_a \cap D_b$ es el conjunto de divisores comunes de a y b, mientras que $D_a^+ \cap D_b^+$ es es conjunto de divisores positivos comunes de a y b. Notemos que en ambos casos estos conjuntos son no vacíos, pues 1 es un elemento en ambos. Por otro lado, $D_a^+ \cap D_b^+ \subseteq \{0, ..., a\}$ si $a \neq 0$, por lo que $D_a^+ \cap D_b^+$ es acotado superiormente. Esto implica que dicho conjunto tiene un elemento máximo.*

DEFINICIÓN 2.1. *Para a y b enteros no cero simultáneamente, definimos el máximo común divisor de a y b, como:*

$$(a, b) = \text{máx}(D_a^+ \cap D_b^+)$$

OBSERVACIÓN 2.2. *En la definición dada queda como no definido $(0,0)$, pues $D_0^+ = \mathbb{N}^+$. Algunos libros toman como convención $(0,0) := 0$.*

EJEMPLO 2.1. *Calculemos $(4,6)$. Para esto observamos que:*

$$D_4^+ = \{1, 2, 4\}$$

$$D_6^+ = \{1, 2, 3, 6\}$$

De esto se deduce que:

$$D_4^+ \cap D_6^+ = \{1, 2\}$$

Por lo tanto,

$$(4, 6) = 2.$$

La definición dada es buena para demostrar algunas propiedades del máximo común divisor, por ejemplo,

$$(a,b) = (b,a)$$

Otros ejemplos aparecen en los ejercicios.

Sin embargo, la definición no es tan calculable, sobre todo para enteros grandes, pues determinar los divisores puede ser una tarea compleja ¡y de hecho lo es! Para buscar una forma efectiva de calcular el máximo común divisor, requerimos de algunos resultados previos, entre ellos la siguiente caracterización.

PROPOSICIÓN 2.1. *Sean $a,b \in \mathbb{Z}$ no cero y $d \in \mathbb{N}^+$. Las siguientes afirmaciones son equivalentes:*

1. $d = (a,b)$
2. *d es la mínima combinación $\mathbb{Z}$-lineal positiva de a y b.*
3. i) $d \mid a$ y $d \mid b$
   ii) *d es combinación $\mathbb{Z}$-lineal de a y b.*
4. i) $d \mid a$ y $d \mid b$
   ii) *Si $c \in \mathbb{Z}$ satisface que $c \mid a$ y $c \mid b$, entonces $c \mid d$*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Definimos el conjunto $A = \{as + bt \in \mathbb{N}^+ \,:\, s,t \in \mathbb{Z}\}$, esto es el conjunto de combinaciones $\mathbb{Z}$-lineales positivas de a y b. Veamos que este conjunto es diferente del vacío, para lo cual notemos que dado que existen unidades $u,v \in \mathbb{Z}$ tales que $|a| = ua$ y $|b| = vb$, entonces $|a| + |b| \in A$.

Al aplicar el principio del buen orden, A tiene un elemento mínimo, el cual denotaremos por δ. Afirmamos que $\delta = d$, lo cual concluiría la prueba de esta implicación. En efecto, como $d \mid a$ y $d \mid b$, entonces $d \mid \delta$, lo que implica que $d \leq \delta$. Por otro lado, afirmamos que $\delta \mid a$ y $\delta \mid b$. Si demostramos esto, como $\delta > 0$, entonces $\delta \in D_a^+ \cap D_b^+$, lo que implica que $\delta \leq d$ y concluye la afirmación por antisimetría del orden. Vamos a probar que $\delta \mid a$ pues la segunda afirmación en análoga. Para esto, por el algoritmo de la división existen $q,r \in \mathbb{Z}$ tales que $a = q\delta + r$ con $0 \leq r < \delta$. Esto implica que r es una combinación lineal de a y b, lo cual implica que $r = 0$ para no contradecir la minimalidad de δ, lo que implica que $a = q\delta$, es decir, $\delta \mid a$.

$2 \Rightarrow 3$) Para la afirmación i), nuevamente probaremos una de las afirmaciones pues ambas son análogas. Veamos que $d \mid a$. Usando el algoritmo de la división, existen $q,r \in \mathbb{Z}$ tales que $a = qd + r$ con $0 \leq r < d$. Para que no se contradiga la minimalidad de d, $r = 0$, lo que muestra que $a = qd$ y por lo tanto $d \mid a$.

La segunda afirmación de 3 es obvia de la hipótesis pues d es en particular una combinación lineal de a y b.

$3 \Rightarrow 4$) No hay nada que demostrar para la afirmación i). Ahora supongamos que $c \in \mathbb{Z}$ satisface que $c \mid a$ y $c \mid b$. Como d es combinación $\mathbb{Z}$-lineal de a y b, esto implica que $c \mid d$.

$4 \Rightarrow 1$) La hipótesis del inciso i) dice que $d \in D_a^+ \cap D_b^+$. Veamos que este elemento es el máximo de dicha intersección, para lo cual, consideremos $c \in D_a^+ \cap D_b^+$. La hipótesis ii) implica que $c \mid d$, lo que implica que $c \leq d$. Por lo tanto, $d = (a,b)$. □

3. Mínimo común múltiplo

NOTACIÓN 3.1. *Para $a \in \mathbb{Z}$, definimos el conjunto de múltiplos positivos de a como:*

$$M_a^+ := \{b \in \mathbb{N}^+ \,:\, a \mid b\}$$

OBSERVACIÓN 3.1. *Observemos que para $a,b \in \mathbb{Z} \setminus \{0\}$, $M_a^+ \cap M_b^+$ es el conjunto de múltiplos positivos comunes de a y b. Además este conjunto es no vacío pues $|ab| \in M_a^+ \cap M_b^+$. El principio del buen orden implica que dicho conjunto tiene un elemento mínimo.*

DEFINICIÓN 3.1. *Para a y b enteros no cero, definimos el máximo común divisor de a y b, como:*

$$[a,b] = \text{mín}(M_a^+ \cap M_b^+)$$

OBSERVACIÓN 3.2. *En la definición dada queda como no definido $[a,b]$ si $a = 0$ o $b = 0$, pues $M_0^+ = \emptyset$. Algunos libros toman como convención $[a,b] := 0$ si $a = 0$ o $b = 0$.*

Como sucedió en el caso del máximo común divisor, hay un teorema de caracterización para el mínimo común múltiplo, el cual es menos extenso y presentamos a continuación.

PROPOSICIÓN 3.1. *Sean $a,b \in \mathbb{Z} \setminus \{0\}$ y $m \in \mathbb{N}^+$. Las siguientes afirmaciones son equivalentes:*

1. $m = [a,b]$
2. i) $a \mid m$ y $b \mid m$
   ii) *Si $c \in \mathbb{Z}$ es tal que $a \mid c$ y $b \mid c$, entonces $m \mid c$.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) La afirmación i) es obvia pues por definición $m \in M_a^+ \cap M_b^+$. Respecto a la segunda afirmación, consideremos $c \in \mathbb{Z}$ tal que $a \mid c$ y $b \mid c$. Por el algoritmo de la división existen $q,r \in \mathbb{Z}$ tales que $c = qm + r$ con $0 \leq r < m$. Notemos que como por hipótesis $a \mid m$ y $b \mid m$, entonces $a \mid c - qm$ y $b \mid c - mq$, lo que dice que $a \mid r$ y $b \mid r$. Como $0 \leq r < m$, la minimalidad de m implica que $r = 0$, por lo que $c = qm$, es decir, $m \mid c$.

$2 \Rightarrow 1$) El inciso i) y el hecho de que $m > 0$ implican que $m \in M_a^+ \cap M_b^+$. Veamos ahora que este es el mínimo de dicho conjunto, para lo que consideramos $c \in M_a^+ \cap M_b^+$. Esto dice que $a \mid c$ y $b \mid c$, por lo que ii) implica que $m \mid c$. De esto se deduce que $m \leq c$, lo que muestra que $m = \text{mín}(M_a^+ \cap M_b^+)$. □

El siguiente resultado nos da una relación aritmética entre los conceptos tratados en esta sección.

PROPOSICIÓN 3.2. *Para cualesquiera $a,b \in \mathbb{Z} \setminus \{0\}$, se tiene que:*

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

DEMOSTRACIÓN. Dado que $a \mid |ab|$ y $b \mid |ab|$, entonces por ii) de la proposición anterior se deduce que $[a,b] \mid |ab|$. De la definición se deduce que existe $d \in \mathbb{Z}$ tal que $|ab| = d[a,b]$, ecuación que implica que $d > 0$. Si demostramos que $d = (a,b)$, habremos concluido la prueba, para lo cual veremos que d cumple el inciso 4 de la proposición 2.1.

Afirmación 1: $d \mid a$ y $d \mid b$.

Probaremos únicamente la primera de estas afirmaciones pues la segunda es análoga. En efecto, del resultado anterior se deduce que existe $c \in \mathbb{Z}$ tal que $[a,b] = cb$. Además sabemos que existe $u \in \mathbb{Z}$ unidad tal que $|ab| = uab$. Por lo que tenemos las siguientes igualdades:

$$uab = |ab| = d[a,b] = dcb$$

Como $b \neq 0$, por la propiedad de cancelación respecto al producto se tiene que $ua = dc$, más aún, como u es unidad, entonces $a = (u^{-1}c)d$, lo que dice que $d \mid a$.

Afirmación 2: Si $c \in \mathbb{Z}$ es tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Sea un tal $c \in \mathbb{Z}$. De la hipótesis se deduce que existen $e,f \in \mathbb{Z}$ tales que:

$$a = ec$$
$$b = fc$$

Consideremos el elemento $m \in \mathbb{Z}$ definido mediante $m := efc$. Dado que $m = af = eb$, entonces $a \mid m$ y $b \mid m$. Por la proposición anterior $[a,b] \mid m$, por lo que existe $g \in \mathbb{Z}$ tal que $m = g[a,b]$. Luego tenemos las siguientes igualdades:

$$g[a,b]c = mc = (efc)c = ab$$

Además sabemos que existe $u \in \mathbb{Z}$ unidad tal que $ab = u|ab|$, por lo que $ab = ud[a,b]$, de donde se deduce que:

$$g[a,b]c = ud[a,b]$$

Como $[a,b] \neq 0$, entonces de la ecuación anterior se deduce que $gc = ud$, que al usar el hecho de que u es unidad implica que $d = (u^{-1}g)c$, es decir, $c \mid d$. Esto concluye la prueba de la afirmación y de la proposición. □

4. Algoritmo de Euclides

En esta sección daremos un algoritmo para calcular el máximo común divisor de un par de enteros. Dicho algoritmo se basa en el siguiente resultado.

PROPOSICIÓN 4.1. *Sean $a,b,q,r \in \mathbb{Z}$ tales que $a = bq + r$. Entonces, $D_a \cap D_b = D_b \cap D_r$. Más aún,*

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

DEMOSTRACIÓN. Para la primera afirmación demostraremos una doble contención.
$\subseteq$) Sea $c \in D_a \cap D_b$. Por definición $c \mid a$ y $c \mid b$, de donde se deduce que $c \mid r$ pues $r = a - bq$. De esto se deduce que $c \in D_r$ y además $c \in D_b$, lo que prueba esta contención.

$\supseteq$) Sea $c \in D_b \cap D_r$. Por definición se tiene que $c \mid b$ y $c \mid r$, por lo que $c \mid a$ pues $a = bq + r$. Además claramente $c \mid b$, por lo que $c \in D_a \cap D_b$.

Respecto a la siguiente afirmación se tiene que:

$$(a,b) = \text{máx}(D_a^+ \cap D_b^+) = \text{máx}(D_a \cap D_b \cap \mathbb{N}^+) = \text{máx}(D_b \cap D_r \cap \mathbb{N}^+) = \text{máx}(D_b^+ \cap D_r^+) = (b,r)$$

□

A continuación explicaremos el algoritmo que buscamos. Comenzamos con $a,b \in \mathbb{Z} \setminus \{0\}$. Por el algoritmo de la división existen $q,r \in \mathbb{Z}$ tales que:

$$a = bq + r, \qquad \text{con} \quad 0 \leq r < |b|$$

La proposición anterior implica que

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

Al considerar $b,r \in \mathbb{Z}$, por el algoritmo de la división existen $q_1, r_1 \in \mathbb{Z}$ tales que:

$$b = rq_1 + r_1, \qquad \text{con} \quad 0 \leq r_1 < r$$

La proposición anterior implica que

$$(b,r) = (r,r_1)$$

Si en este proceso $r_1 = 0$, entonces $r = (a,b)$ y además el hecho de que $a + b(-q) = r$, nos da una expresión del máximo común divisor de a y b como combinación lineal. En caso contrario, al considerar $r, r_1 \in \mathbb{Z}$, el algoritmo de la división dice que existen $q_2, r_2 \in \mathbb{Z}$ tales que:

$$r = r_1 q_2 + r_2, \qquad \text{con} \quad 0 \leq r_2 < r_1$$

Además $(r, r_1) = (r_1, r_2)$. Nuevamente, si $r_2 = 0$, entonces $r_1 = (a,b)$ y por sustitución podemos obtener una combinación $\mathbb{Z}$-lineal de $r_1 = (a,b)$ en términos de a y b haciendo sustituciones sucesivas en las ecuaciones obtenidas. En caso contrario podemos aplicar el mismo proceso a $r_1, r_2 \in \mathbb{Z}$. Esto produce una sucesión de ecuaciones y una sucesión decreciente de enteros $\cdots < r_3 < r_2 < r_1 < |b|$ la cual debe ser eventualmente cero, donde el último residuo no cero es el máximo común divisor de a y b. Además por sustituciones sucesivas se puede obtener la expresión como combinación $\mathbb{Z}$-lineal de a y b a (a,b). Este proceso se conoce como el **algoritmo de Euclides**.

EJEMPLO 4.1. *Encontrar usando el algoritmo de Euclides* $(17,26)$ *y expresar dicho entero como combinación* $\mathbb{Z}$*-lineal de* 17 *y* 26*.*

SOLUCIÓN. *Aplicamos el algoritmo de la división a* 26 *y* 17*, por lo que tenemos:*

$$26 = 17(1) + 9 \tag{1}$$

Como el residuo es distinto de cero, continuamos aplicando el algoritmo de la división a 17 *y* 9*, entonces:*

$$17 = 9(1) + 8 \tag{2}$$

Como el residuo es no cero, aplicamos el algoritmo de la división a 9 *y* 8*, por lo que:*

$$9 = 8(1) + 1 \tag{3}$$

El residuo nuevamente es no cero, por lo que aplicamos el algoritmo a 8 *y* 1*, de donde* $8 = 8(1)$ *y el residuo es cero, por lo tanto, concluimos que:*

$$(26,17) = 1$$

Para expresar $(26,17)$ *como combinación lineal, notemos que por la ecuación (2) tenemos que* $8 = 17 + 9(-1)$*, por lo que al sustituir esto en la ecuación (3) y reducir se tiene que:*

$$(26,17) = 1 = 9 + 8(-1) = 9(2) + 17(-1) \tag{4}$$

De la ecuación (1) se tiene que $9 = 26 + 17(-1)$*, por lo que al sustituir esto en la ecuación (4) se tiene que:*

$$(26,17) = 1 = 26(2) + 17(-3)$$

Esto último da la combinación buscada.

5. Ecuaciones diofantinas lineales

DEFINICIÓN 5.1. *Sean* $a, b \in \mathbb{Z}$*. Decimos que a y b son* ***primos relativos*** *si* $(a,b) = 1$*.*

OBSERVACIÓN 5.1. *Sean* $a, b \in \mathbb{Z}$*. Si existen* $s, t \in \mathbb{Z}$ *tales que* $as + bt = 1$*, entonces* $(a,b) = 1$*, pues el máximo común divisor es la mínima combinación lineal positiva de a y b.*

EJEMPLO 5.1. *Dado que* $2(-1) + 3(1) = 1$*, entonces* $(2,3) = 1$*.*

Un resultado importante se presenta a continuación.

LEMA 5.1. *(Euclides) Sean $a,b,c \in \mathbb{Z}$ con $b \neq 0$. Si $a \mid bc$ y $(a,b) = 1$, entonces $a \mid c$.*

DEMOSTRACIÓN. Por hipótesis existe $k \in \mathbb{Z}$ tal que $ka = bc$. Además existen $s,t \in \mathbb{Z}$ tal que $sa+tb = 1$, por lo que:

$$c = c(sa+tb) = csa+t(bc) = csa+ka = (cs+k)a$$

De esto se deduce el resultado. □

DEFINICIÓN 5.2. *Sean $a,b,c \in \mathbb{Z}$ con $a,b \neq 0$. Una **ecuación diofantina lineal** es una ecuación sobre los enteros de la forma:*

$$ax+by = c$$

El ejemplo más simple de ecuación diofantina se da cuando $c = 0$. En este caso tenemos el siguiente resultado previo.

LEMA 5.2. *Sean $a,b \in \mathbb{Z} \setminus \{0\}$ tales que $(a,b) = 1$. Las soluciones de la ecuación $ax+by = 0$ son de la forma*

$$\begin{cases} x = bt \\ y = -at, \end{cases} \qquad \text{para } t \in \mathbb{Z}.$$

DEMOSTRACIÓN. Como primer paso veamos que las x y y propuestas son en efecto soluciones pues para $t \in \mathbb{Z}$, se tiene que:

$$a(tr)+b(-at) = 0$$

Ahora veamos que todas las soluciones de dicha ecuación son de la forma propuesta. Para esto, si $x,y \in \mathbb{Z}$ satisfacen que $ax+by = 0$, entonces $ax = -by$, entonces $b \mid ax$, dado que $(a,b) = 1$, entonces $b \mid x$, por lo que existe $t \in \mathbb{Z}$ tal que $x = bt$. Al sustituir esto en la ecuación, se tiene que:

$$0 = ax+by = abt+by = b(at+y)$$

Dado que $b \neq 0$, entonces $at+y = 0$, de donde se deduce que $y = -at$. □

Usando el resultado anterior se puede resolver el caso general, es decir, aquel que no pide que $(a,b) = 1$. Para hacer esto requerimos introducir una notación.

NOTACIÓN 5.1. *Si $a,b \in \mathbb{Z}$ son tales que $a \neq 0$ y $a \mid b$, entonces existe un único $c \in \mathbb{Z}$ tal que $b = ca$. A dicho c lo denotaremos por $\frac{b}{a}$.*

PROPOSICIÓN 5.1. *Sean $a,b \in \mathbb{Z} \setminus \{0\}$. Las soluciones de la ecuación $ax+by = 0$ son de la forma:*

$$\begin{cases} x = \frac{b}{(a,b)}t \\ y = -\frac{a}{(a,b)}t, \end{cases} \qquad \text{para } t \in \mathbb{Z}.$$

DEMOSTRACIÓN. Es consecuencia directa del ejercicio 5.9 y el lema anterior. □

Ahora tratemos la solución de una ecuación diofantina lineal general. Tenemos el siguiente resultado de existencia de soluciones.

PROPOSICIÓN 5.2. *Sean $a,b,c \in \mathbb{Z}$ con $a,b \neq 0$. La ecuación $ax+by = c$ tiene solución si y sólo si $(a,b) \mid c$.*

DEMOSTRACIÓN. $\Rightarrow$) Dado que existen $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0 + by_0 = c$ y además $(a,b) \mid a$ y $(a,b) \mid b$, entonces $(a,b) \mid c$.

$\Leftarrow$) Sabemos que existen $s,t \in \mathbb{Z}$ tales que $sa+tb = (a,b)$. Por otro lado, la hipótesis dice que existe $k \in \mathbb{Z}$ tal que $c = k(a,b)$. De esto se deduce que $a(sk) + b(tk) = c$, por lo que la solución buscada es $x = sk$ y $y = tk$. □

Ya que tenemos una forma de saber cuando una ecuación diofantina lineal tiene solución, vamos a pasar a cómo obtenerlas. Respecto a esto note que el regreso de la afirmación anterior nos dice como construir una solución de la ecuación diofantina tratada. Sin embargo, nos gustaría ver si estas son todas las soluciones. El siguiente resultado dice que dicho proceso pasa por el caso de tomar $c = 0$.

PROPOSICIÓN 5.3. *Sean $a,b,c \in \mathbb{Z}$ con $a,b \neq 0$. Supongamos que $x_1, y_1 \in \mathbb{Z}$ satisfacen que $ax_1 + by_1 = c$. Entonces toda solución de la ecuación $ax+by = c$ tiene la forma:*

$$\begin{cases} x = x_0 + x_1 \\ y = y_0 + y_1 \end{cases}$$

Donde $ax_0 + by_0 = 0$.

DEMOSTRACIÓN. Primero notemos que en efecto tal forma de las soluciones es válida pues:

$$a(x_0+x_1) + b(y_0+y_1) = (ax_0+by_0) + (ax_1+by_1) = c$$

Ahora veamos que toda solución de la ecuación diofantina se puede escribir así. En efecto, si $x,y \in \mathbb{Z}$ satisfacen que $ax+by = c$, entonces notemos que como $ax_1 + by_1 = c$, entonces $a(x-x_1) + b(y-y_1) = 0$. Por lo tanto, al tomar $x_0 := x - x_1$ y $y_0 := y - y_1$, se tiene el resultado deseado. □

En virtud al resultado anterior tenemos lo siguiente:

DEFINICIÓN 5.3. *Dada la ecuación diofantina lineal $ax+by = c$, la ecuación diofantina $ax+by = 0$ se conoce como la ecuación homogénea asociada a $ax+by = c$.*

OBSERVACIÓN 5.2. *Con la terminología anterior podemos interpretar la última proposición diciendo que las soluciones de una ecuación diofantina (siempre que estas existan) se pueden escribir mediante una solución particular de esta y las soluciones de la ecuación homogénea asociada.*

Dado que conocemos como son todas las soluciones generales de la ecuación homogénea asociada a una ecuación diofantina, podemos parafrasear la proposición para dar de forma explícita todas las soluciones de una ecuación diofantina lineal.

COROLARIO 5.1. *Sean $a,b,c \in \mathbb{Z}$ con $a,b \neq 0$. Supongamos que $x_1, y_1 \in \mathbb{Z}$ satisfacen que $ax_1 + by_1 = c$. Entonces toda solución de la ecuación $ax+by = c$ tiene la forma:*

$$\begin{cases} x = x_1 + \frac{b}{(a,b)}t \\ y = y_1 - \frac{a}{(a,b)}t, \end{cases} \qquad \text{Para } t \in \mathbb{Z}.$$

Terminamos esta sección presentando un par de ejemplos.

EJEMPLO 5.2. *Resolver la ecuación diofantina*

$$4x + 6y = 3$$

SOLUCIÓN. *Notemos que $(4,6) = 2$ y como $2 \nmid 3$, la ecuación dada no tiene solución.*

EJEMPLO 5.3. *Resolver la ecuación diofantina*

$$26x - 17y = -2$$

SOLUCIÓN. *En el ejemplo 4.1 vimos que* $(26,17) = 1$, *por lo que* $(26,-17) = 1$. *De esto se deduce que dicha ecuación tiene solución. Para obtener una solución particular recordemos que en dicho ejemplo se expresó el máximo común divisor de* 26 *y* 17 *como combimación* $\mathbb{Z}$*-lineal, obteniendo:*

$$26(2) + 17(-3) = 1$$

De esto se deduce que:

$$26(-4) - 17(-6) = -2$$

Por lo que una solución particular de la ecuación dada es $x_1 = -4$ *y* $y_1 = -6$.

Por otro lado, respecto a las soluciones de la ecuación homogénea asociada, que es $26x - 17y = 0$, *estas tienen la forma* $x = 17t$ *y* $y = 26t$ *para* $t \in \mathbb{Z}$. *Por lo tanto, el corolario 5.1 dice que las soluciones de la ecuación dada son:*

$$\begin{cases} x = -4 + 17t \\ y = -6 + 26t, \end{cases} \qquad \textit{Para } t \in \mathbb{Z}.$$

Ejercicios del capítulo

Sean $a,b,c,p,q,s,t,k \in \mathbb{Z}$.

Demuestre las siguientes afirmaciones

EJERCICIO 5.1. *Para todo $k,n \in \mathbb{N}$, $k!n!$ divide a $(k+n)!$*

EJERCICIO 5.2. *Si $\{a_0,...,a_n\} \subseteq \mathbb{Z}$ entonces $\prod_{k=0}^{n} k!$ divide a $\prod_{i<j}(a_i - a_j)$.*

EJERCICIO 5.3. *Si $a|b$ entonces $a|-b$, $-a|b$ y $-a|-b$.*

EJERCICIO 5.4. *$a|b$ si y sólo si $|a| \mid |b|$.*

EJERCICIO 5.5. *Si $a|b$ y $b|a$ entonces $a = \pm b$.*

EJERCICIO 5.6. *Si $\{b_1,...,b_n\} \subseteq \mathbb{Z}$ entonces a divide a $b_1,...,b_n$ si y sólo si a divide a cualquier combinación lineal de $b_1,...,b_n$.*

EJERCICIO 5.7. *Si $b \neq 0$, entonces existen únicos $q,r \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq r < |b|$. Usa el principio de buen orden.*

EJERCICIO 5.8. *Si $d = (a,b)$ y $d = as + bt$ entonces $(d,s) = 1$.*

EJERCICIO 5.9. *Si $d = (a,b)$, $a = ds$ y $b = dt$ entonces $(s,t) = 1$.*

EJERCICIO 5.10. *Si $c|a$ y $(a,b) = 1$ entonces $(b,c) = 1$.*

EJERCICIO 5.11. *Si $a,b \in \mathbb{Z}^*$, entonces son equivalentes:*

1. $a|b$
2. $(a,b) = |a|$
3. $[a,b] = |b|$

¿Puede a o b ser cero en este resultado?

EJERCICIO 5.12. *Si $(a,b) = 1$, $a|c$ y $b|c$ entonces $ab|c$.*

EJERCICIO 5.13. *Si $k \neq 0$ entonces:*

1. $(ka,kb) = |k|(a,b)$.
2. $[ka,kb] = |k|[a,b]$.

EJERCICIO 5.14. $(a,b) = (a,b-a)$

EJERCICIO 5.15. *Si* $(a,b) = (c,b) = 1$ *entonces* $(ac,b) = 1$.

EJERCICIO 5.16. *Si* $\{F_n\}_{n=1}^{\infty}$ *es la sucesión de Fibonacci entonces* $(F_n, F_{n+1}) = 1$

EJERCICIO 5.17. $(a,a+1) = 1$ *y* $[a,a+1] = |a(a+1)|$.

EJERCICIO 5.18. *Si* $(a,b) = 1$ *entonces para todo* $n,m \in \mathbb{N}$, $(a^n, b^m) = 1$.

EJERCICIO 5.19. *Si* $(a,b) = 1$ *y existe* $n \in \mathbb{N}$ *tal que* $a|b^n$ *entonces* $a = 1$ *ó* $a = -1$.

EJERCICIO 5.20. *Todo entero al cuadrado es de la forma* $4k+1$ *ó* $4k$.

EJERCICIO 5.21. *Usando el algoritmo de Euclides expresa el máximo común divisor como combinación lineal de:*

1. $513, 24$.
2. $225, 717$.
3. $2n+1, 4n$.
4. $4n^2+2n-40, 2n+7$.

NOTA 5.1. *Al definir de manera conjuntista el máximo común divisor de dos números, es sencillo generalizar este concepto para una cantidad arbitraria de números. En el siguiente ejercicio se utiliza esta generalización y se denota por* $mcd\{a_j | j \in J\}$ *al máximo común divisor de conjunto* $\{a_j | j \in J\} \subseteq \mathbb{Z}$, *donde* J *es un conjunto indicador.*

EJERCICIO 5.22. *Calcula lo siguiente:*

1. $mcd\{x^5 + x | x \in \mathbb{Z}\}$
2. $mcd\{1000x^5 + 1000x | x \in \mathbb{Z}\}$
3. $mcd\{ax^5 + ax | x \in \mathbb{Z}\}$, *donde* $a \in \mathbb{Z}^*$.

EJERCICIO 5.23. *Si* s,t *son una solución de la ecuación* $ax+by = d$. *Encuentra todas las soluciones enteras de dicha ecuación.*

EJERCICIO 5.24. *Realiza lo siguiente:*

1. *Encuentra las soluciones enteras de la ecuación* $5x+3y = 1$.
2. *Encuentra las soluciones enteras de la ecuación* $2x+3y = 1$.
3. *Usa los resultados anteriores para demostrar que el sistema de ecuaciones*
$$\begin{cases} 5x+3y = 1 \\ 2x+3y = 1 \end{cases}$$
no tiene solución en $\mathbb{Z}$ *de forma simultánea.*

EJERCICIO 5.25. *Encuentra el conjunto de soluciones enteras de las siguientes ecuaciones diofantinas.*

1. $789x+79y = 764$.
2. $561x+568y = 1891$.

3. $1569x + 3574y = 546235$.
4. $(6n+1)x + (3n)y = 12$.

En los siguientes dos ejercicios x, y, z serán incógnitas en los enteros.

EJERCICIO 5.26. *Encuentra todas las soluciones enteras de las siguientes ecuaciones:*
1. $x^2 + y^2 = 2xy$.
2. $x^2 + y^2 + z^2 = 2xyz$.

EJERCICIO 5.27. *Resolver la ecuación sobre $\mathbb{Z}$,*

$$x + xy + y = 54$$

Demuestre que todas las soluciones satisfacen que $x + y = 14$.

EJERCICIO 5.28. *Sean $m, d \in \mathbb{N}^+$ y recuerda que $b \in \mathbb{Z}$.*
1. *Demuestra que el sistema de ecuaciones*
$$\begin{cases} x + y = b \\ (x, y) = d \end{cases}$$
tiene solución si y sólo si $d|b$.
2. *Demuestra que el sistema de ecuaciones*
$$\begin{cases} (x, y) = d \\ [x, y] = m \end{cases}$$
tiene solución si y sólo si $d|m$.
3. *Demuestra que el sistema de ecuaciones*
$$\begin{cases} xy = b \\ (x, y) = d \end{cases}$$
tiene solución si y sólo si $d^2|b$.

EJERCICIO 5.29. *Demuestra que si p, q son primos entonces $[p, q] = |pq|$. ¿Es cierto el regreso de esta afirmación?*

EJERCICIO 5.30. *Considera la sucesión $\{p_k\}_{k=1}^{\infty}$ de números primos positivos ordenados de forma creciente, es decir, $p_1 = 2$, $p_2 = 3$, ... Encuentra el primer término para el cual $f_k = p_1 \cdot \ldots \cdot p_k + 1$ no es primo.*

Demuestra las siguientes afirmaciones.

EJERCICIO 5.31. *Si $a > 2$ entonces a es un cuadrado perfecto si y sólo si todo factor primo en la descomposición de a tiene una potencia par.*

EJERCICIO 5.32. *Demuestra lo siguiente:*
1. *Si $a, b \in \mathbb{N}$ son cuadrados perfectos entonces ab es un cuadrado perfecto.*
2. *Si $(a, b) = 1$ y ab es un cuadrado perfecto entonces a y b son cuadrados perfectos.*

EJERCICIO 5.33. *Si $n > 1$ y n es no es primo entonces existe un primo p tal que $p < n^2$.*

EJERCICIO 5.34. *Si $2^n - 1$ es primo y $n \in \mathbb{N}$ entonces n es primo.*

EJERCICIO 5.35. *Si $n \in \mathbb{N}$ y $2^n + 1$ es primo entonces n es potencia de dos.*

EJERCICIO 5.36. *Si $p \in \mathbb{N}$ es primo entonces $p|(a+b)^p - (a^p + b^p)$.*

EJERCICIO 5.37. *Para todo natural n existen n naturales consecutivos no primos.*

EJERCICIO 5.38. *Si $a = up_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ y $b = vp_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ donde $u, v \in \mathbb{Z}$ son unidades, $p_1, \ldots, p_n$ son números primos positivos y $k_1, .., k_n, r_1, .., r_n \in \mathbb{N}$, entonces:*

$$(a,b) = p_1^{f_1} \cdot \ldots \cdot p_n^{f_n}$$

$$[a,b] = p_1^{g_1} \cdot \ldots \cdot p_n^{g_n}$$

donde $f_i = \min\{k_i, r_i\}$ y $g_i = \max\{k_i, r_i\}$.

EJERCICIO 5.39. *Sea $a \in \mathbb{Z}$ y D_a es el conjunto de sus divisores. Entonces, se define una función $D : \mathbb{Z}^* \to \mathbb{N}$, mediante $D(a) = |D_a|$.*

1. *Demuestra que $D_a \subseteq D_b$ si y sólo si $a|b$.*
2. *Demuestra que $D_a = D_{|a|}$.*
3. *Para todo $a \in \mathbb{Z}$ calcula de forma explícita $|D_a|$. ¿Está D bien definida?*
4. *¿Es D una función inyectiva?, ¿es suprayectiva? Argumenta.*

EJERCICIO 5.40. *Sea $n \in \mathbb{N}^+$. Usando el teorema fundamental de la aritmética construye una función inyectiva $\phi : \mathbb{N}^n \to \mathbb{N}$.*

EJERCICIO 5.41. *Discutir lo que pasa con la proposición 2.1 si a o b es cero. Discutir también qué sucede con la proposición 3.1 si $a = 0$ o $b = 0$.*

Capítulo 3

Congruencias

Primos

DEFINICIÓN 0.1. *Sea $p \in \mathbb{Z}$ con $p \neq 0$ y que no sea unidad. Decimos que p es irreducible, si $p = ab$ entonces a es unidad o b es unidad.*

Lo que quiere decir esto interpreta en los enteros, es que los divisores de p son $-p, -1, 1$ y p. Observemos que no pedimos que p sea positivo, por lo cual tenemos $-2, 3, -5, 7, -11$ como ejemplos de irreducibles.

Observamos que esta es la definición más conocida de primo (que tenga 2 divisores, 4 si considerarmos los negativos), pero sin embargo no es la verdadera desde un punto de vista tecnico

DEFINICIÓN 0.2. *Sea $p \in \mathbb{Z}$ con $p \neq 0$ y que no sea unidad. Decimos que p es primo, si $p \mid ab$ entonces $p \mid a$ o $p \mid b$.*

Esta es la correcta defincón de primo desde un punto de vista técnico.

PROPOSICIÓN 0.1. *Sea $p \in \mathbb{Z}$. Entonces p es primo si y sólo si p es irreducible*

Sin embargo, en el caso de los enteros no hay problema, amabas definciones son equivalentes.

PROPOSICIÓN 0.2 (Teorema fundamental de la Aritmética). *Sea n un natural. Entonces existe únicos primos $p_1, \dots p_k$ y enteros positivos $n_1, \dots n_k$ tales que $n = p_1^{n_1} \dots p_k^{n_k}$*

PROPOSICIÓN 0.3. *Existen una infinidad de primos.*

DEMOSTRACIÓN. Supongamos que existe una cantidad finita de primos, digamos $p_1, \dots, p_n$. Ponemos $M = p_1 \dots p_n + 1$. Ahora por el teorema fundamental de la aritmética M tiene una descomposición en primos, $M = q_1 \dots q_s$. De las dos formas de ver a M tenemos la siguiente combinación lineal:

$$(-1)p_1 \dots p_n + q_1 \dots q_s = 1$$

De aquí tenemos que $(p_i, q_j) = 1$, por lo que $p_i \neq q_j$. Por lo que los q_j son nuevos primos.

□

Congruencias

DEFINICIÓN 0.3. *Sea n un entero. Decimos que dos enteros x es congruente con y módulo n, si $n \mid x - y$. Este hecho lo denotamos por $x \equiv y mod n$*

PROPOSICIÓN 0.4. *Sea n un entero. La relación $* \equiv * mod n$ es una relación de equivalencia sobre los enteros.*

PROPOSICIÓN 0.5. *Sea n un entero. La relación $* \equiv * mod n$ es una relación de congruencia sobre los enteros.*

DEFINICIÓN 0.4. *Sea n un entero. Definimos los enteros módulo n, como los enteros cociente la relación de equivalencia $* \equiv * mod n$. A este conjunto lo denotamos por $\mathbb{Z}_n$.*

DEFINICIÓN 0.5. *Sea n un entero. Definimos dos funciones $+ \colon \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ y $* \colon \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ dadas por $[x] + [y] = [x + y]$ y $[x][y] = [xy]$.*

DEFINICIÓN 0.6. *Sea n un entero. Las funciones definidas anteriormente estan bien definidas y brindan a $\mathbb{Z}_n$ de estructura de anillo*

PROPOSICIÓN 0.6. *Sea n un entero. Son equivalentes:*

- *n es un primo.*
- $\mathbb{Z}_n$ *es un dominio entero.*
- $\mathbb{Z}_n$ *es un campo.*

PROPOSICIÓN 0.7. *Sea n un entero. Entonces* $[x] \in \mathbb{Z}_n$ *es una unidad si y sólo si* $(x,n) = 1$

DEFINICIÓN 0.7. *Definimos la función* $\phi : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$ *dada por* $\phi(n) = |\{k = 1,\ldots,n-1 \mid (k,n) = 1\}|$. *Esta función la llamaremos la función* ϕ *de Euler.*

PROPOSICIÓN 0.8. *Sea p un primo. Entonces* $\phi(p^n) = p^{n-1}(p-1)$

PROPOSICIÓN 0.9. *Sean a y b primos relativos. Entonces* $\phi(ab) = \phi(a)\phi(b)$

PROPOSICIÓN 0.10. *Existen una infinidad de primos de la forma* $4k+3$.

DEMOSTRACIÓN. Supongamos que existe una cantidad finita de primos de la forma $4k+3$, digamos $p_1,\ldots,p_n$. Ponemos $M = 4p_1 \ldots p_n + 3$, notamos que $M \equiv 3 mod 4$. Así tenemos que $M \equiv -1 mod 4$. Por lo que M es de la forma $4s-1$. Ahora por el teorema fundamental de la aritmética M tiene una descomposición en primos, $M = q_1 \ldots q_s$. De las dos formas de ver a M tenemos la siguiente combinación lineal:

$$4p_1 \ldots p_n + (-1)q_1 \ldots q_s = 1$$

De aquí tenemos que $(p_i, q_j) = 1$, por lo que $p_i \neq q_j$. Es decir, los primos q_j son nuevos primos.
Ahora

$$[M] = [4k+3] = [3] = [4][k] + [3] = [4][0] + [3] = [3]$$

Por otro lado:

$$[M] = [q_1 \ldots q_s] = [q_1] \ldots [q_s]$$

Si tuviesemos que todos los $[q_j] = 1$, llegariamos a que $[M] = [1]$. Por lo que debe existir al menos un $[q_{j_0}] = [3]$. Este es un nuevo primo de la forma $4k+3$ que no estaba en la lista original

□

PROPOSICIÓN 0.11 (Teorema del Binomio del Tonto). *Sea p un primo. Para* $a,b \in \mathbb{Z}_p$, $(a+b)^p = a^p + b^p$.

PROPOSICIÓN 0.12 (Pequeño Teorema de Fermat). *Sea p un primo. Entonces* $a^p \equiv a mod p$ *para todo* $a \in \mathbb{Z}$

PROPOSICIÓN 0.13. *Sea p un primo impar. Entonces* $b^2 \equiv -1 mod p$ *si y sólo si* $p \equiv 1 mod 4$.

DEMOSTRACIÓN. $\Rightarrow$) Como p es un primo impar tenemos que $p \equiv 1 mod 4$ o $p \equiv 3 mod 4$. Supongamos que $p \equiv 3 mod 4$, es decir, que $p = 4k+3$ para algun entero k.
Así,

$$\begin{aligned} b^p &= b^{4k+3} \\ &= b^{2(2k+1)+1} \\ &= (b^2)^{2k+1} b \end{aligned}$$

Usando la hipotesis tenemos que

$$b^p \equiv (-1)^{2k-1} b mod p$$

Así aplicando el pequeño teorema de Fermat tenemos que

$$b \equiv -b mod p$$

Lo cual es una contradicción a menos que $p = 2$, pero este no es el caso.
$\Leftarrow$)

□

PROPOSICIÓN 0.14. *Existen una infinidad de primos de la forma* $4k+1$.

DEMOSTRACIÓN. Supongamos que existe una cantidad finita de primos positivos de la forma $4k+1$, digamos $p_1,\ldots,p_n$. Ponemos $N = p_1 \ldots p_n$ y $M = (2N)^2+1$. Ahora por el teorema fundamental de la aritmética M tiene una descomposición en primos positivos, $M = q_1 \ldots q_s$. De las dos formas de ver a M tenemos la siguiente combinación lineal:

$$(-1)4p_1^2 \ldots p_n^2 + (-1)q_1 \ldots q_s = 1$$

De aquí tenemos que $(p_i, q_j) = 1$, por lo que $p_i \neq q_j$. Es decir, los primos q_j son nuevos primos. Tomamos cualquier q_j y lo llamamos q. Como $M = (2N)^2+1$. Tenemos que $q \mid (2N)^2+1$. Lo que quiere decir:

$$(2N)^2 \equiv -1 mod q$$

Por otro lado notamos que q tiene que ser impar, caso contrario M sería par. Por lo que $\frac{q-1}{2}$ es un natural. La congruencis pasada la elevamos a $\frac{q-1}{2}$, por lo que tenemos:

$$(2N)^{q-1} \equiv (-1)^{\frac{q-1}{2}} mod q$$

Podemos aplicar el pequeño Teorema de Fermat, así tendríamos:

$$(2N))^{q-1} \equiv 1 mod q$$

Usando que la relacion es transitiva, obtenemos:

$$1 \equiv (-1)^{\frac{q-1}{2}} mod q$$

Si q fuera de la forma $4w+3$, tendríamos que:

$$1 \equiv (-1)^{2w+1} mod q$$

O lo que es equivalente:

$$1 \equiv -1 mod q$$

Esto solo pasa cuando $q = 2$. Lo que es una contradicción. Así q es de la forma $4k+1$.

□

PROPOSICIÓN 0.15 (Teorema Chino de Residuo). *Sean* $n_1,\ldots,n_k$ *naturales tales que* $(n_i,n_j) = 1$ *con* $i \neq j$ *y* $a_1,\ldots,a_k$ *enteros. Entonces el sistema de ecuaciones tiene solución:*

$$\begin{cases} x & \equiv a_1 mod n_1 \\ x & \equiv a_2 mod n_2 \\ \vdots & \\ x & \equiv a_k mod n_k \end{cases}$$

Ejercicios del capítulo

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

EJERCICIO 0.1. *Demuestre que* $\mathbb{Z}_n = \mathbb{Z}_{-n}$.

EJERCICIO 0.2. *Sean* $f : \mathbb{Z}_3 \to \mathbb{Z}_6$ *y* $g : \mathbb{Z}_6 \to \mathbb{Z}_3$ *cuya regla de correspondencia es* $f([a]_3) = [a]_6$ *y* $g([a]_6) = [a]_3$.

1. *¿Están estas funciones bien definidas? Es decir, no dependen de representantes*
2. *En caso de que ser alguna de ellas función ¿es inyectiva o suprayectiva?*

EJERCICIO 0.3. *Demuestre que si* p *es primo y* $p \equiv 1 \mod 3$, *entonces* $p \equiv 1 \mod 6$.

EJERCICIO 0.4. *Demuestre que si* $2^n - 1$ *es primo y* $n \in \mathbb{N}$ *entonces* n *es primo.*

Sugerencia: Recuerde que $a^k - b^k = (a-b)(\sum_{i=0}^{k-1} a^{k-1-i}b^i)$ *cunado* $k \in \mathbb{N}^+$.

EJERCICIO 0.5. *Supongamos que* p *es primo y* $p > 0$. *Demuestre que* $(p-1)! \equiv -1 \mod p$.

Sugerencia: Calcular $(p-1)!$ *en* $\mathbb{Z}_p$ *recordando que* $\mathbb{Z}_p$ *es un campo.*

EJERCICIO 0.6. *Si* $a = up_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ *y* $b = vp_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ *donde* $u, v \in \mathbb{Z}$ *son unidades,* $p_1, \ldots, p_n$ *son números primos positivos y* $k_1, .., k_n, r_1, .., r_n \in \mathbb{N}$, *son las descomposiciones según el teorema fundamental de la aritmética de a y b, entonces:*

$$(a,b) = p_1^{f_1} \cdot \ldots \cdot p_n^{f_n}$$

$$[a,b] = p_1^{g_1} \cdot \ldots \cdot p_n^{g_n}$$

donde $f_i = \min\{k_i, r_i\}$ *y* $g_i = \max\{k_i, r_i\}$.

EJERCICIO 0.7. *Demuestre que si* $p \in \mathbb{N}^+$ *es primo, entonces* $p \mid (a+b)^p - (a^p + b^p)$.

Sugerencia: Notar que el teorema del binomio es válido sobre los enteros y aplicarlo, analizando la divisibilidad de los coeficientes binomiales con p.

EJERCICIO 0.8. *Supongamos que* p *es primo y* $p > 0$. *Demuestre que para todo* $a \in \mathbb{Z}$,

1. $a^p \equiv a \mod p$.
2. *Si* $(a,p) = 1$ *entonces* $a^{p-1} \equiv 1 \mod p$.

Sugerencia: Para el primer caso aplicar inducción y extender el resultado a los enteros. Para el segundo usar el lema de Euclides.

EJERCICIO 0.9. *Supongamos que* $p \in \mathbb{N}$ *es primo impar y* $p = x^2 + y^2$ *con* $x, y \in \mathbb{Z}$. *Demuestre que* $p \equiv 1 \mod 4$.

Sugerencia: Analizar la paridad de x, y.

EJERCICIO 0.10. *Si $n = 2p$ con p un primo impar, demuestre que existe $[x] \in \mathbb{Z}_n$ con $[x] \neq [0]$ y $[x] \neq [1]$ tal que $[x]^2 = [x]$.*

Sugerencia: Encontrar un número impar adecuado.

EJERCICIO 0.11. *Encuentra las soluciones del siguiente sistema de congruencias usando el teorema chino del residuo:*

$$\begin{cases} x \equiv 34 \mod 2 \\ x \equiv 5 \mod 29 \end{cases}$$

EJERCICIO 0.12. *Encuentra las soluciones del siguiente sistema de congruencias usando el teorema chino del residuo:*

$$\begin{cases} x \equiv 7 \mod 125 \\ x \equiv 9 \mod 36 \\ x \equiv 78 \mod 64 \end{cases}$$

EJERCICIO 0.13. *Demuestre que ningun siglo empieza con martes, jueves o domingo.*

Capítulo 4

Racionales y Reales

En la antigua matemática griega, la justificación de los números racionales se fundamentaría en su capacidad para representar proporciones y relaciones armoniosas en la naturaleza y la música. Los números racionales, como fracciones, permiten expresar divisiones de unidades de manera precisa, lo que es fundamental para comprender la geometría y la aritmética básica. Además, su aplicación práctica en la división de recursos y la distribución equitativa en la sociedad refleja su importancia en la vida cotidiana. Desde esta perspectiva, los números racionales son más que meras abstracciones matemáticas; son herramientas fundamentales para comprender y relacionarse con el mundo que nos rodea, desde las leyes de la física hasta las estructuras sociales y culturales.

1. Construcción de los racionales

De manera analoga a como los enteros se construyen a partir de los naturales, construiremos los racionales a partir de los enteros. Nos gustaría que los enteros tengan inversos multiplicativos, es decir, buscamos un campo $\mathbb{Q}$ que contenga a los enteros. Así mismo, esta definición es bastante laxa. Puesto que de lo que conocemos también los reales son un campo que contienen a los enteros.

DEFINICIÓN 1.1. *Los racionales $\mathbb{Q}$ son un campo tal que $\mathbb{Z} \subseteq \mathbb{Q}$ y para todo $x \in \mathbb{Q}$ existen $n, m \in \mathbb{Z}$ con $m \neq 0$ tales que $x = nm^{-1}$.*

Otra forma de decirlo es que los racionales son el mínimo campo que contiene a los enteros. Pero no nos centraremos en esta descripción.

Procedamos a hacer este proceso de manera intuitiva. Comunmente, expresamos un racional como una fracción $\frac{n}{m}$ donde $n, m \in \mathbb{Z}$ con $m \neq 0$. Tenemos muchas combinaciones de dos enteros que representan la misma fraccion, por ejemplo:

$$\frac{1}{2} = \frac{2}{4} = \frac{-1}{-2} = \frac{5}{10}$$

Bien sabemos que dos fracciones $\frac{a}{b}$ y $\frac{c}{d}$ son iguales cuando $ad = bc$. Como mencionamos anteriormente haremos analoga a la de los enteros, ponemos $Q = \mathbb{Z} \times \mathbb{N}^+$ y definimos la siguiente relación:

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

PROPOSICIÓN 1.1. *La relación definida es de equivalencia.*

DEMOSTRACIÓN. La reflexividad y simetría son claras, únicamente demostraremos la transitividad: sean $(a,b),(c,d),(e,f) \in \mathbb{Z} \times \mathbb{Z}^*$ tales que $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, es decir, $ad = bc$ y $cf = de$. Ahora observemos que se tienen las siguientes igualdades:

$$(af)d = (ad)f = (bc)f = b(cf) = b(de) = (be)d$$

Dado que $d \neq 0$, por la propiedad de cancelación se deduce que $af = be$, lo que dice que $(a,b) \sim (e,f)$. □

De la intuición que nos da la motivación dada al inicio de la sección, la clase de la pareja (a,b) representa el cociente $\frac{a}{b}$. Esto nos lleva a lo siguiente:

DEFINICIÓN 1.2. *El conjunto de números racionales, $\mathbb{Q}$, se define como el conjunto cociente $(\mathbb{Z}\times\mathbb{Z}^*)/\sim$. Además denotamos,*

$$\frac{a}{b} := [(a,b)]$$

De la definición se puede ver que se cumple lo siguiente:

OBSERVACIÓN 1.1.

1. *Para cualquier $a \neq 0$, $\frac{0}{1} = \frac{0}{a}$.*
2. *Para cualquier $c \neq 0$, $\frac{a}{b} = \frac{ac}{bc}$*

El siguiente paso es definir dos operaciones en $\mathbb{Q}$; una suma y un producto. Para definir estas, usaremos nuevamente la intuición que nos da identificar una pareja $(a,b) \in \mathbb{Z}\times\mathbb{Z}^*$ con la ecuación $bx = a$. Para esto sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Para definir $\frac{a}{b} + \frac{c}{d}$, consideremos las ecuaciones que definen las fracciones consideradas:

$$\begin{cases} bx = a \\ dy = c \end{cases}$$

De las ecuaciones anteriores se deduce que,

$$bd(x+y) = d(bx) + b(dy) = da + bc$$

Dado que $bd \neq 0$, esto nos dice que podríamos definir:

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

Respecto a definir $\frac{a}{b} \cdot \frac{c}{d}$, tenemos que del sistema

$$\begin{cases} bx = a \\ dy = c \end{cases}$$

se deduce que:

$$(bd)xy = (bx)(dy) = ac$$

Esto nos dice que podemos definir,

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

Lo anterior dice que tenemos asignaciones:

$$+, \cdot : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$$

Dado que las asignaciones anteriores están definidas en un conjunto cociente, tenemos que ver que estas no dependen de representantes.

PROPOSICIÓN 1.2. *Las asignaciones definidas no dependen de representantes.*

DEMOSTRACIÓN. Vamos a hacer el caso de la suma pues el del producto es análogo. Para esto supongamos que $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$, es decir, $ab' = ba'$ y $cd' = dc'$. De esto se deduce que:

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

De esto se deduce que

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

De esto se deduce que

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$$

□

Para los cálculos es muy útil la siguiente propiedad:

OBSERVACIÓN 1.2.

$$\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$$

Además con estas funciones podemos darle una estructura algebraica a $\mathbb{Q}$.

PROPOSICIÓN 1.3. *$\mathbb{Q}$ es un campo con las operaciones definidas.*

DEMOSTRACIÓN. Todas las propiedades se siguen de cálculos directos, simplemente indicaremos los elementos distinguidos. Respecto a la estructura aditiva, el neutro aditivo es la clase $\frac{0}{1}$ y $-\frac{a}{b} = \frac{-a}{b}$. Respecto a la estructura multiplicativa, el neutro multiplicativo es la clase $\frac{1}{1}$ y dado que $\frac{a}{b} = \frac{0}{1}$ si y sólo si $a = 0$, entonces para $\frac{a}{b} \neq \frac{0}{1}$, se tiene que $(\frac{a}{b})^{-1} = \frac{b}{a}$. □

2. El orden en los racionales

Para definir un orden en los racionales usaremos un resultado preliminar.

LEMA 2.1. *Si $q \in \mathbb{Q}$, entonces existen $a, b \in \mathbb{Z}$ con $b > 0$ tales que:*

$$q = \frac{a}{b}.$$

DEMOSTRACIÓN. Por definición existen $c, d \in \mathbb{Z}$ con $d \neq 0$ tales que $q = \frac{c}{d}$. Si $d > 0$, no hay nada que probar, pero si $d < 0$, tenemos que $q = \frac{-c}{-d}$, de donde se deduce la afirmación. □

Supongamos que tenemos racionales $\frac{a}{b}, \frac{c}{d}$ tales que $b, d > 0$. Si cada uno de estos representa la ecuación $bx = a$ y $dy = c$ y suponemos que $x < y$, entonces observemos que:

$$ad = (bx)d = (bd)x < (bd)y = bc$$

Esto nos lleva a definir lo siguiente.

DEFINICIÓN 2.1. *Dados $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ con $b, d > 0$, decimos que $\frac{a}{b} < \frac{c}{d}$ si $ad < bc$.*

Dado que la definición anterior es para clases de equivalencia, tenemos que probar que esta no depende de representantes.

PROPOSICIÓN 2.1. *La relación $<$ definida no depende de representantes.*

Más aún, esta nos permite definir un orden.

PROPOSICIÓN 2.2. *La relación $<$ definida es un orden estricto en $\mathbb{Q}$.*

DEMOSTRACIÓN. La relación es claramente irreflexiva. Para la transitividad supongamos que $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ con $b,d,f > 0$ tales que $\frac{a}{b} < \frac{c}{d}$ y $\frac{c}{d} < \frac{e}{f}$. Estas hipótesis implican que:

$$ad < bc$$
$$cf < de$$

Al hacer el producto de la primera desigualdad con f y la segunda con b, se tiene que:

$$(af)d = (ad)f < (bc)f = b(cf) < b(de) = (be)d$$

Como $d > 0$, se deduce de la desigualdad $(af)d < (be)d$ que $af < be$, lo que dice que $\frac{a}{b} < \frac{e}{f}$. □

Más aún, el orden definido cumple la propiedad de tricotomia.

PROPOSICIÓN 2.3. *Si $q_1, q_2 \in \mathbb{Q}$, entonces se cumple una y sólo una de las siguientes afirmaciones:*

1. $q_1 < q_2$
2. $q_1 = q_2$
3. $q_1 > q_2$

DEMOSTRACIÓN. Supongamos que $q_1 = \frac{a}{b}$ y $q_2 = \frac{c}{d}$ con $b,d > 0$. La propiedad se aplica de la propiedad de tricotomía aplicada a los enteros ad y bc. □

Las propiedades de compatibilidad del orden respecto a las operaciones de $\mathbb{Q}$ se muestran en el ejercicio 5.6.

Recapitulando lo trabajado hasta el momento, la motivación de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ era para poder resolver todas las ecuaciones de la forma $ax = b$ con $a,b \in \mathbb{Z}$ y $a \neq 0$. Lo único que faltaría justificar es a qué nos referimos con extender $\mathbb{Z}$ a $\mathbb{Q}$. Esta idea se escribe de manera formal en el siguiente resultado.

PROPOSICIÓN 2.4. *La función $\iota : \mathbb{Z} \to \mathbb{Q}$ que tiene por regla de correspondencia $\iota(a) = \frac{a}{1}$, es inyectiva, respeta las operaciones y elementos distinguidos. Además esta preserva el orden.*

Con esto queda claro que de verdad en $\mathbb{Q}$ podemos resolver todas las ecuaciones de la forma $bx = a$ para $a,b \in \mathbb{Z}$ y $b \neq 0$.

3. El anillo de números decimales finitos

Consideremos el conjunto

$$D = \left\{ \frac{a}{10^n} \ : \ a \in \mathbb{Z},\ n \in \mathbb{N} \right\}$$

Por definición es claro que $D \subseteq \mathbb{Q}$. Más aún, como $\frac{1}{3} \in \mathbb{Q} \setminus D$, dicha contención es propia.

Además las operaciones de $\mathbb{Q}$ permiten darle estructura de anillo a D.

PROPOSICIÓN 3.1. *$D \subseteq \mathbb{Q}$ es un subanillo, por lo tanto, D es un anillo con la suma y producto de racionales.*

DEFINICIÓN 3.1. *El anillo D se conoce como el **anillo de números decimales (finitos)**.*

El siguiente resultado que buscamos es caracterizar los elementos de D mediante una expansión. Esto se hace en el siguiente resultado.

PROPOSICIÓN 3.2. *Para cualquier $q \in D \setminus \{0\}$, existen únicos $m \in \mathbb{Z}$ y $r_0, ..., r_n \in \{0, ..., 9\}$ con $r_n \neq 0$ tales que:*

$$q = m + \sum_{k=0}^{n} \frac{r_k}{10^k}$$

NOTA 3.1. *Para q como en el resultado anterior, escribiremos:*

$$q = r_0.r_1 r_2 \cdots r_n$$

*A esta expresión la llamaremos la **expansión decimal** de q.*

Mediante estas expresiones podemos recuperar la forma de operar decimales bien conocidas de los cursos básicos. Vamos a mostrar un ejemplo.

EJEMPLO 3.1. *Calcular* $1.261 + 1.04$.

Solución: *Recordando la notación, tenemos que:*

$$1.261 = 1 + \frac{2}{10} + \frac{6}{10^2} + \frac{1}{10^3}$$

$$1.04 = 1 + \frac{4}{10^2}$$

Por lo tanto, hacemos la suma mediante términos semejantes según las potencias de 10, reduciendo de ser necesario, siempre manteniendo las potencias de 10 en los denominadores:

$$\begin{aligned}
1.261+1.04 &= \left(1+\frac{2}{10}+\frac{6}{10^2}+\frac{1}{10^3}\right)+\left(1+\frac{4}{10^2}\right)\\
&= (1+1)+\frac{2}{10}+\left(\frac{6}{10^2}+\frac{4}{10^2}\right)+\frac{1}{10^3}\\
&= 2+\frac{2}{10}+\frac{10}{10^2}+\frac{1}{10^3}\\
&= 2+\frac{2}{10}+\frac{1}{10}+\frac{1}{10^3}\\
&= 2+\frac{3}{10}+\frac{1}{10^3}\\
&= 2.301
\end{aligned}$$

Esta forma de operar corresponde al conocido algoritmo estudiado en cursos básicos.

$$\begin{array}{rr}
 & 1\\
 & 1.261\\
+ & \\
\hline
 & 2.301
\end{array}$$

Por otro lado, de las expresiones decimales podemos obtener un criterio de comparación de decimales gracias a la compatibilidad de las operaciones con el orden. Para esto observemos que cualesquiera dos expresiones decimales de un par de números, se pueden escribir con la misma longitud agregando ceros a la derecha del punto de ser necesario. De esto se deduce lo siguiente:

PROPOSICIÓN 3.3. *Sean $a = a_0.a_1\cdots a_n$ y $b = b_0.b_1\cdots b_n$ dos decimales. Entonces, $a < b$ si y sólo si existe $i \in \{0,...,n\}$ tal que $a_i < b_i$ y para cualquier $j \in \{0,...,i-1\}$, $a_j = b_j$.*

4. Los números reales

A diferencia de los sistemas numéricos introducidos en los capítulos anteriores, dar una motivación ecuacional de los números reales no es posible, la motivación viene de la completez de los números racionales. Una posible motivación en este sentido aparece en el ejercicio 5.14.

Tomando como motivación la proposición 3.2 podemos definir un número real como una expresión de la forma:

$$r = r_0.r_1r_2\cdots$$

donde $r_0 \in \mathbb{Z}$ y para cualquier $n \in \mathbb{N}^+$, $r_n \in \{0,...,9\}$. Sin embargo hay que imponer una relación pues la experiencia indica que hay ciertas expresiones que tenemos que identificar. Por ejemplo, para una expresión que tiene una cola de ceros o colas de 9. Vamos a poner esto de manera formal.

DEFINICIÓN 4.1. *Sea $m \in \mathbb{Z}$. Una sucesión $\{a_n\}_{n=0}^{\infty}$ tiene una cola de m's, si existe $n_0 \in \mathbb{N}$ tal que para cualquier $n \geq n_0$, $a_n = m$.*

Para las colas de cero es claro que hay que identificar todos los reales que debe representar la sucesión con aquel que tiene la última entrada distinta de cero. Por ejemplo,

$$1.2 \sim 1.20 \sim 1.200 \sim 1.2000 \sim \cdots$$

Notemos que los elementos con colas de 0's, son precisamente los números decimales por la proposición 3.2.

Por otro lado, para las colas de 9's la situación es mas interesante. Para esto recordemos que es un hecho conocido de cálculo que para $n_0 \in \mathbb{N}^+$,

$$\sum_{n=n_0}^{\infty} \frac{9}{10^n} = \frac{1}{10^{n_0-1}}$$

Esto nos dice que hay que identificar expresiones como:

$$0.999999\cdots \sim 1$$
$$1.8799999\cdots \sim 1.88$$

Por lo tanto, podemos definir al conjunto de números reales, $\mathbb{R}$, como el conjunto de sucesiones $\mathbb{Z} \times \{0,...,9\}^{\mathbb{N}}$ donde identificamos sucesiones que tengan colas de 0's y 9's de acuerdo a las reglas anteriores. Notacionalmente escribiremos para $(r_0, \{r_n\}_{n=1}^{\infty}) \in \mathbb{Z} \times \{0,...,9\}^{\mathbb{N}}$ mediante $r_0.r_1r_2\cdots$, sin hacer explícito que esto es una clase de equivalencia.

Esta claro que todo decimal es un numero real por la proposición 3.2. Por otro lado, de esta descripción notemos que cualquier real r, se puede aproximar por decimales. Esto pues si $r = r_0.r_1r_2\cdots$, entonces los decimales $\sum_{k=0}^{n} \frac{r_k}{10^k}$, aproximan a dicho real hasta el decimal n. Para formalizar esto, notemos que podemos definir un orden en $\mathbb{R}$, que extiende de forma obvia al orden que estaba inducido por $\mathbb{Q}$ en D, a saber:

DEFINICIÓN 4.2. *Sean $a, b \in \mathbb{R}$ tales que $a = a_0.a_1a_2\cdots$ y $b = b_0.b_1b_2\cdots$. Decimos que $a < b$, si existe $i \in \{0,...,n\}$ tal que $a_i < b_i$ y para cualquier $j \in \{0,...,i-1\}$, $a_j = b_j$.*

Tenemos el resultado que se espera.

PROPOSICIÓN 4.1. *La relación $< \subseteq \mathbb{R}^2$ define un orden estricto en $\mathbb{R}$.*

Con la proposición anterior, la idea de aproximación de un real por decimales, está dada por el siguiente resultado:

PROPOSICIÓN 4.2. *Para cualquier $r \in \mathbb{R}$ y $n \in \mathbb{N}$, existen $a_0 \in \mathbb{Z}$ y $a_1, ..., a_n \in \{0,...,9\}$ tales que:*

$$a_0.a_1\cdots a_n \leq r \leq a_0.a_1\cdots a_n + \frac{1}{10^n}$$

Respecto a las operaciones, podemos usar la intuición que da la proposición anterior. Para esto introduciremos una familia de funciones que truncan un número real en el n-ésimo término de su expansión. Sea $n \in \mathbb{N}$. Definimos la función:

$$x_n : \mathbb{R} \to D$$

con regla de correspondencia:

$$x_n(r_0.r_1r_2\cdots) = r_0.r_1\cdots r_n$$

El siguiente ingrediente tiene que ver con introducir un postulado conocido como el axioma del supremo, cuya prueba omitiremos pues es técnica, pero que se puede consultar en el teorema 1 en [**2**, pp 220].

PROPOSICIÓN 4.3. *(Axioma del supremo) Todo subconjunto no vacío de $\mathbb{R}$ que es acotado superiormente, tiene un supremo, esto es, una mínima cota superior.*

Como es bien sabido, del axioma del supremo se obtiene la correspondiente propiedad para ínfimos (ver ejercicio 5.15).

Con esto en mente, respecto a la suma notemos que si $r,s \in \mathbb{R}$, entonces el truncamiento n-ésimo de ambos reales puede sumarse con las operaciones de D, obteniendo $x_n(r)+x_n(s)$, y esto intuitivamente es una buena aproximación de la suma que de hecho coincide si $r,s \in D$ con decimales con m enteros a la derecha si $m \leq n$. Esto nos lleva a considerar el conjunto:

$$\{x_n(r)+x_n(s) \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$$

Este conjunto es claramente no vacío y además acotado superiormente, esto pues notemos que individualmente, tenemos que para r, tenemos que si $r > 0$, entonces para cualquier $n \in \mathbb{N}$, se tiene que $x_n(r) < r_0 + 1$ y $r_0 + 1 \in \mathbb{Z}$. Por otro lado, si $r < 0$, claramente esto acota superiormente a todos los $x_n(r)$. Por lo tanto, hemos probado que existe $a \in \mathbb{Z}$ tal que para cualquier $n \in \mathbb{N}$, $x_n(r) < a$. De forma análoga, existe $b \in \mathbb{Z}$ tal que para cualquier $n \in \mathbb{N}$, $x_n(s) < b$. De esto se deduce que para cualquier $n \in \mathbb{N}$,

$$x_n(r)+x_n(s) < a+b$$

Por lo que el conjunto mencionado es acotado. Por lo tanto podemos tomar su supremo y definir:

$$r+s := \sup\{x_n(r)+x_n(s) \mid n \in \mathbb{N}\}$$

De manera completamente análoga podemos definir el producto de reales mediante:

$$rs := \sup\{x_n(r)x_n(s) \mid n \in \mathbb{N}\}$$

Al definir estas operaciones tenemos el resultado buscado respecto a la estructura algebraica en $\mathbb{R}$.

PROPOSICIÓN 4.4. *Los reales con las operaciones definidas forman un campo.*

5. Encaje de los racionales en los reales

Ya sabemos que podemos encajar D en $\mathbb{R}$ y es claro de la definición que $D \subseteq \mathbb{Q}$. La meta de esta sección es ver que de hecho podemos encajar $\mathbb{Q}$ en $\mathbb{R}$. Esto se puede hacer de manera puramente formal como lo muestra el siguiente resultado.

PROPOSICIÓN 5.1. *Definamos la asignación $\iota : \mathbb{Q} \to \mathbb{R}$ mediante la regla de correspondencia:*

$$\iota(\frac{a}{b}) = ab^{-1}$$

La asignación anterior no depende de representantes, es una función inyectiva, preserva las operaciones y los neutros de ellas, así como el orden.

La desventaja de la proposición anterior es que no damos de manera explícita como expresar cualquier racional mediante una expansión infinita, pues para definir la imagen de ι usamos el hecho de que $\mathbb{R}$ es un campo y que los enteros tienen una expresión como números reales canónica. Esto tiene sus ventajas desde el punto de vista abstracto pues permite ver de forma sencilla las propiedades algebraicas de ι, sin embargo, vamos a ver como expresar a cualquier racional mediante una expansión decimal infinita. Para esto requerimos de un concepto previo.

DEFINICIÓN 5.1. *Sea $r \in \mathbb{R}$ con $r = r_0.r_1r_2\cdots$. Decimos que r es **periódico** con periodo $r_{n+1}\cdots r_{n+p}$, si para cualquier $m \in \mathbb{N}$ y $k \in \{1,...,p\}$,*

$$r_{n+k+mp} = r_{n+k}$$

En tal caso escribiremos:

$$r = r_0.r_1\cdots r_n\overline{r_{n+1}\cdots r_{n+p}}$$

EJEMPLO 5.1.

$$\frac{1}{3} = 0.\overline{3}$$

EJEMPLO 5.2.

$$\frac{8}{7} = 1.\overline{142857}$$

Veamos como dar la expansión de un racional cualquiera no cero. Sea $q \in \mathbb{Q}\setminus\{0\}$. Entonces existen $a,b \in \mathbb{Z}$ con $b > 0$ tales que:

$$q = \frac{a}{b}$$

Al aplicar el algoritmo de la división, existen $q_0, r_0 \in \mathbb{Z}$ tales que $a = bq_0 + r_0$ con $0 \leq r_0 < b$. Note que si $r_0 = 0$ no hay nada que probar pues de hecho $q \in \mathbb{Z}$, así que supongamos que $r_0 \neq 0$. De esto se deduce que:

$$q = q_0 + \frac{r_0}{b} \tag{5}$$

Respecto a los residuos, notemos que al aplicar al conjunto $\{10^n r_0\}_{n=0}^{\infty}$ con b, notemos los residuos deben ser una cantidad finita, por lo tanto deben existir $s,t \in \mathbb{N}$ tales que $10^{s+t}r_0$ y $10^t r_0$ tienen el mismo residuo, de donde se deduce que existe $r_1 \in \{0,...,9\}$ tal que:

$$\frac{10^{s+t}r_0}{b} - \frac{10^t r_0}{b} = r_1$$

Esto implica que:

$$\frac{r_0}{b} = \frac{r_0}{10^t}\frac{1}{10^s-1} = \frac{r_0}{10^{s+t}}\frac{1}{1-\frac{1}{10^s}} \tag{6}$$

Notemos que como tenemos que $\frac{1}{1-\frac{1}{10^s}} = 0.\overline{0\cdots 1}$ con 1 en la posición s. De esto se deduce usando la ecuación 6 que:

$$\frac{r_0}{b} = 0.0\cdots r_1\overline{0\cdots r_1}$$

con el primer r_1 en posición $s+t$ y el segundo en posición s respecto al periodo. De la ecuación 5 se deduce que:

$$q = .0\cdots r_1\overline{0\cdots r_1}$$

Esto muestra que:

PROPOSICIÓN 5.2. *$q \in \mathbb{Q}$, entonces q es periódico.*

El regreso del resultado anterior también es cierto (ver ejercicio 5.13).

Ejercicios del capítulo

Sean $a,b,c,d,c',d' \in \mathbb{Z}$ con $b,d,d' \neq 0$.

EJERCICIO 5.1. *Concluir la demostración de la proposición 1.2.*

EJERCICIO 5.2. *Supongamos que $[b,d] = sb$ y $[b,d] = td$. Demuestre que:*

$$\frac{a}{b} + \frac{c}{d} = \frac{as+bt}{[b,d]}$$

EJERCICIO 5.3. *Supongamos que $\frac{a}{b} < \frac{c}{d}$ y que $(c,d) \sim (c',d')$ con $b,d,d' > 0$. Demuestre que $\frac{a}{b} < \frac{c'}{d'}$, en otras palabras, que el orden no depende de representantes por la derecha.*

DEFINICIÓN 5.2. *El conjunto de números racionales positivos se define como:*

$$\mathbb{Q}^+ = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; ab > 0 \right\}$$

EJERCICIO 5.4. *Demuestre que la relación de pertenencia en el conjunto $\mathbb{Q}^+$ no depende de representantes, esto es, que si $\frac{a}{b} \in \mathbb{Q}$ y $(a,b) \sim (c,d)$, entonces $\frac{c}{d} \in \mathbb{Q}^+$*

EJERCICIO 5.5. *Sean que $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ tales que $b,d > 0$. Demuestre que $\frac{a}{b} < \frac{c}{d}$ si y sólo si $\frac{c}{d} - \frac{a}{b} \in \mathbb{Q}^+$.*

EJERCICIO 5.6. *Sean $q_1, q_2, q_3 \in \mathbb{Q}$. Demuestre lo siguiente:*

1. *Si $q_1 < q_2$, entonces $q_1 + q_3 < q_2 + q_3$*
2. *Si $q_1 < q_2$ y $q_3 \in \mathbb{Q}^+$, entonces $q_1 q_3 < q_2 q_3$*

EJERCICIO 5.7. *Realice el producto de los elementos 1.261 y 1.04 usando las operaciones del anillo de decimales finitos. Discuta por qué esta forma de operar es compatible con el algoritmo que se enseña en los cursos básicos.*

EJERCICIO 5.8. *Recordemos que D es el anillo de números decimales. Demuestre que si $x \in D$, existen únicos $a_0 \in \mathbb{Z}$, así como $a_1, ..., a_n \in \{0, ..., 9\}$ tales que:*

$$x = \sum_{i=0}^{n} \frac{a_i}{10^i}$$

EJERCICIO 5.9. *Demuestre que para cualquier $n \in \mathbb{N}^+$, existen únicos $r_0, ..., r_n \in \{0, ...9\}$ con $r_n \neq 0$ tales que*

$$n = \sum_{k=1}^{n} r_k 10^k$$

EJERCICIO 5.10. *Demuestre que para cualquier $a \in \mathbb{R}$ y $n \in \mathbb{N}$, existen $a_0 \in \mathbb{Z}$ y $a_1, ..., a_n \in \{0, ..., 9\}$ tales que:*

$$a_0.a_1 \cdots a_n \leq x \leq a_0.a_1 \cdots a_n + \frac{1}{10^n}$$

EJERCICIO 5.11. *Demuestre la proposición 3.3.*

EJERCICIO 5.12. *Pruebe que la expansión decimal de $\frac{1}{3}$ está dada por $0.\overline{3}$.*

EJERCICIO 5.13. *Demuestre que si $r \in \mathbb{R}$ es periódico, entonces $r \in \mathbb{Q}$*

EJERCICIO 5.14. *Sea $p \in \mathbb{N}$ un primo. Supongamos que existe $a_p \in \mathbb{R}$ tal que $a_p^2 = p$. Demuestre que $a_p \notin \mathbb{Q}$*

EJERCICIO 5.15. *Suponiendo como válido el axioma del supremo, demuestre lo siguiente: Todo subconjunto no vacío de $\mathbb{R}$ que es acotado inferiormente, tiene una máxima cota inferior, esto es, un ínfimo.*

Capítulo 5

Complejos

1. Álgebra de los Complejos

Los complejos nacen históricamente de la pregunta de si existe un "número" x tal que $x^2+1=0$. Dicho de otro modo, $x^2=-1<0$. Ahora bien, es bien sabido que si $x\in\mathbb{R}$, entonces $x^2\geq 0$ por lo que este número que buscamos no puede ser un un número real. Ahora bien, este número en caso de existir se le suele denotar por "i". Así continuando con el relato, viendo que no puede ser parte de los reales nos gustaría que i perteneciese a un conjunto con cierta estructura algebraica y más aún que dicha estructura algebraica contenga los reales y preseverme muchas de sus propiedades. Entonces a este conjunto que buscamos lo denotaremos por $\mathbb{C}$ y lo llamaremos el conjunto de los números complejos. De manera todavía un poco ambigua solicitaremos que:

- $i\in\mathbb{C}$
- $\mathbb{R}\subseteq\mathbb{C}$
- $\mathbb{C}$ sea un campo.

Como recordatorio damos la definición de campo.

DEFINICIÓN 1.1 (Campo). *Sea K un conjunto no vacío con dos funciones $+\colon K\times K\longrightarrow K$ y $*\colon K\times K\longrightarrow K$. Notacionalmente escribimos $\lambda+\mu:=+(\lambda,\mu)$ y $\lambda\mu:=*(\lambda,\mu)$ para $\lambda,\mu\in K$. Si estas dos funciones cumplen:*

1. *Para $\lambda,\mu,\nu\in K$, $\lambda+(\mu+\nu)=(\lambda+\mu)+\nu$.*
2. *Existe $0\in K$ tal que para cualquier $\lambda\in K$, $\lambda+0=\lambda=0+\lambda$.*
3. *Para todo $\lambda\in K$, existe $-\lambda\in K$ tal que $\lambda+(-\lambda)=0=(-\lambda)+\lambda$.*
4. *Para $\lambda,\mu\in K$, $\lambda+\mu=\mu+\lambda$.*
5. *Para $\lambda,\mu,\nu\in K$, $\lambda(\mu\nu)=(\lambda\mu)\nu$.*
6. *Existe $1\in K$ tal que para cualquier $\lambda\in K$, $\lambda 1=\lambda=1\lambda$.*
7. *Para todo $\lambda\in K$ con $\lambda\neq 0$, existe $\lambda^{-1}\in K$ tal que $\lambda\lambda^{-1}=1=\lambda^{-1}\lambda$.*
8. *Para $\lambda,\mu\in K$, $\lambda\mu=\mu\lambda$.*
9. *Para $\lambda,\mu,\nu\in K$, $\lambda(\mu+\nu)=\lambda\mu+\lambda\nu$.*

Entonces llamamos a K un campo.

Realmente lo que haremos es dar un modelo de $\mathbb{C}$ por que hay varias formas de construirlos, y realmente se obtienen las mismas propiedades.

El modelo clásico de $\mathbb{C}$ es definirlo a nivel de conjunto con $\mathbb{R}^2$. Ahora la suma será la misma que $\mathbb{R}^2$, es decir, entrada a entrada. El producto lo definiremos de la siguiente manera:

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

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

Lo primero que vamos a ver es que realmente $\mathbb{C}$ es un campo. De álgebra lineal sabemos que cumple los primeros 4 axiomas, entonces nos enfocaremos en los siguientes.

PROPOSICIÓN 1.1. *$\mathbb{C}$ es un campo*

DEMOSTRACIÓN.

- Sean $(a,b),(c,d),(e,f) \in \mathbb{C}$. Entonces:

$$\begin{aligned}[(a,b)*(c,d)]*(e,f) &= (ac-bd, ad+bc)*(e,f)\\ &= ((ac-bd)e-(ad+bc)f, (ac-bd)f+(ad+bc)e)\\ &= (ace-bde-adf-bcf, acf-bdf+ade+bce)\\ &= (a(ce-df)-b(cf+de), a(cf+de)+b(ce-df))\\ &= (a,b)*(ce-df, cf+de)\\ &= (a,b)*[(c,d)*(e,f)]\end{aligned}$$

  Por lo tanto el producto es asociativo.
- Sea $(a,b) \in \mathbb{C}$. Entonces

$$(a,b)*(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b)$$

  y

$$(1,0)*(a,b) = (1\cdot a - 0\cdot b, 1\cdot b + 0\cdot a) = (a,b)$$

  Por lo tanto el producto tiene identidad.
- Sea $(a,b) \in \mathbb{C}$ con $(a,b) \neq 0$. Entonces $a \neq 0$ o $b \neq 0$. Así buscamos $(c,d) \in \mathbb{C}$ tal que $(a,b)*(c,d) = (1,0)$. Realmente, esto es, $(ac-bd, ad+bc) = (1,0)$. Como dos vectores son iguales si y sólo si son iguales entrada a entrada, tenemos el siguiente sistema de ecuaciones:

$$\begin{cases} 1 &= ac-bd \\ 0 &= ad+bc \end{cases}$$

  donde las incógnitas son c y d. Por la regla de Cramer vemos que la solución es $c = \frac{a}{a^2+b^2}$ y $d = \frac{-b}{a^2+b^2}$. Notamos que aquí usamos que $a^2+b^2 \neq 0$, para que la fracción este bien definida. Veamos que efectivamente es la inversa:

$$\begin{aligned}(a,b)*(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) &= (a\frac{a}{a^2+b^2} - b\frac{-b}{a^2+b^2}, a\frac{-b}{a^2+b^2} + b\frac{a}{a^2+b^2})\\ &= (\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2})\\ &= (\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2})\\ &= (1,0)\end{aligned}$$

  Analogamente $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})*(a,b) = (1,0)$.
- Sean $(a,b),(c,d) \in \mathbb{C}$. Entonces:

$$(a,b)*(c,d) = (ac-bd, ad+bc) = (c,d)*(a,b)$$

  Por lo tanto la multiplicación es commutativa.
- Sean $(a,b),(c,d),(e,f) \in \mathbb{C}$. Entonces:

$$\begin{aligned}(a,b)*[(c,d)+(e,f)] &= (a,b)*(c+e, d+f)\\ &= (a(c+e)-b(d+f), a(d+f)+b(c+e))\\ &= (ac+ae-bd-bf, ad+af+bc+be)\\ &= (ac-bd, ad+bd)+(ae-bf, af+be)\\ &= (a,b)*(c,d)+(a,b)*(e,f)\end{aligned}$$

  Por lo tanto las operaciones distribuyen.

De aquí que $\mathbb{C}$ es un campo. □

Con nuestro modelo de los complejos $\mathbb{C}$ que es el plano real $\mathbb{R}^2$ no podemos decir que $\mathbb{R} \subseteq \mathbb{R}^2$. Así que tenemos que buscar una forma de darle sentido a esta propiedad. La solución es relativamente sencilla, hacerlo por medio de una función inyectiva. Así es que tenemos la siguiente proposición.

PROPOSICIÓN 1.2. *Sea* $i\colon \mathbb{R} \longrightarrow \mathbb{C}$ *dado por* $i(x) = (x,0)$. *Entonces* i *preserva las operaciones algebraicas y es una función inyectiva.*

DEMOSTRACIÓN. Sean $a, b \in \mathbb{R}$. Entonces para la suma tenemos:

$$\begin{aligned} i(a+b) &= (a+b,0) \\ &= (a,0)+(b,0) \\ &= i(a)+i(b) \end{aligned}$$

y para el producto tenemos:

$$\begin{aligned} i(ab) &= (ab,0) \\ &= (ab-0\cdot 0, a\cdot 0+b\cdot 0) \\ &= (a,0)*(b,0) \\ &= i(a)i(b) \end{aligned}$$

Ahora notemos que $i(1) = (1,0)$, es decir, manda unidades en unidades.

Por último si $i(x) = i(y)$, entonces $(x,0) = (y,0)$. Por definición de par ordenado, tenemos que $x = y$. Así la función es inyectiva. □

Intepretando el resultado, podemos identificar a los reales como el subconjunto de los complejos de la forma $(x,0)$ con $\mathbb{R}$, es decir, con la imagen de i.

Con esto en mente procedemos al último punto. Buscamos un complejo $(x,y) \in \mathbb{C}$ tal que $(x,y)^2 = (-1,0)$. Simplemente proponemos $(x,y) = (0,1)$, verifiquemos:

$$(0,1)^2 = (0,1)*(0,1) = (0\cdot 0 - 1\cdot 1, 1\cdot 0 + 0\cdot 1) = (-1,0)$$

Ahora bien, nuestro modelo de los complejos cumple con las propiedades deseadas. Vamos a proceder a mejorar la notación. En vez de escribir $(x,y) \in \mathbb{C}$, escribiremos $x+iy$. Notamos que con esta notación 1 corresponde a $(1,0)$ e i corresponde a $(0,1)$. Con esta notación la suma resulta:

$$(a+ib)+(c+di) = (a+c)+i(b+d)$$

y el producto resulta:

$$(a+ib)(c+di) = (ac-bd)+i(ad+bc)$$

Ahora algunas cuestiones notacionales, en vez de $a+i0$, simplemente escribiremos a. A su vez, en el caso de $0+ib$, escribiremos ib. Así, en el caso $0+i0$, siguiendo la notación, simplemente escribiremos 0. Para terminar, en el caso de $a+i1$, escribiremos $a+i$.

EJEMPLO 1.1. *A continuación unos ejemplos númericos de las operaciones complejas:*

- $$(1+7i)+(-3+4i) = -2+11i$$
- $$(1+i)(1-i) = (1\cdot 1 - 1(-1)) + i(1\cdot 1 + 1(-1)) = (1+1)+i0 = 2$$
- $$i^2 = ii = (0\cdot 0 - 1\cdot 1) + i(1\cdot 0 + 0\cdot 1) = -1$$
- $$(2-i)^{-1} = \frac{2}{2^2+(-1)^2} + i\frac{-(-1)}{2^2+(-1)^2} = \frac{2}{5} + i\frac{1}{5}$$

■

$$\begin{aligned}\frac{-1+2i}{1+i} &= (-1+2i)(1+i)^{-1}\\ &= (-1+2i)(\frac{1}{1^2+1^2}+\frac{-i}{1^2+1^2})\\ &= (-1+2i)(\frac{1}{2}+\frac{-i}{2})\\ &= (-1\frac{1}{2}-2\frac{-1}{2})+i(-1\frac{-1}{2}+2\frac{1}{2})\\ &= \frac{1}{2}+i\frac{3}{2}\end{aligned}$$

A continuación vamos a una construcción alternativa de los complejos. Ahora pongamos:

$$\mathbb{C} := \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,b \in \mathbb{R}\}$$

Lo primero que observamos es que $\mathbb{C}$ es un subconjunto de las matrices de dos por dos con coeficientes reales $M_2(\mathbb{R})$. Procedemos con la misma ruta que la anterior para ver que esto también es un modelo de los complejos.

PROPOSICIÓN 1.3. *$\mathbb{C}$ es un campo.*

DEMOSTRACIÓN. La suma y multiplicación son la de las matrices.

Tenemos que ver que estas operaciones están bien definidas, por lo que tomamos dos elementos $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathbb{C}$. Primero la suma:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} \in \mathbb{C}$$

Ahora para la multiplicación:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \in \mathbb{C}$$

De nuevo, nos valdremos de ciertos resultados de álgebra lineal. Observamos que $\begin{pmatrix} 0 & -0 \\ 0 & 0 \end{pmatrix} \in \mathbb{C}$. Por último, si $\lambda \in \mathbb{R}$

$$\lambda\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{pmatrix} \in \mathbb{C}$$

Por lo cual $\mathbb{C}$ es un subespacio de $M_2(\mathbb{R})$. De esto se sigue que cumple los primeros cuatro axiomas de campo.

Ahora la asociatividad se sigue de la asociatividad de la multiplicación de matrices, y de igual manera también tenemos la distributividad.

Para la existencia de unidad, es fácil ver la unidad de $M_2(\mathbb{R})$ es un complejo, esto es,

$$\begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} \in \mathbb{C}$$

De nuevo, lo más complicado sería ver que existen los inversos. Sea $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}$ con $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \neq 0$. Así $a \neq 0$ o $b \neq 0$. Calculamos

$$det\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2+b^2 \neq 0$$

Así de álgebra lineal sabemos que esta matriz es invertible. Más aún, sabemos que la inversa es la matriz coadjugada por el inverso del determinante, es decir:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{C}$$

Por lo tanto $\mathbb{C}$ es un campo. □

De igual manera veamos que los reales están contenidos en este modelo de los complejos.

PROPOSICIÓN 1.4. *Sea* $\eta : \mathbb{R} \longrightarrow \mathbb{C}$ *dado por* $\eta(x) = \begin{pmatrix} x & 0 \\ -0 & x \end{pmatrix}$. *Entonces* η *preserva las operaciones algebraicas y es una función inyectiva.*

DEMOSTRACIÓN. Sean $a, b \in \mathbb{R}$. Entonces para la suma tenemos:

$$\begin{aligned} \eta(a+b) &= \begin{pmatrix} a+b & 0 \\ -0 & a+b \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ -0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ -0 & b \end{pmatrix} \\ &= \eta(a) + \eta(b) \end{aligned}$$

y para el producto tenemos:

$$\begin{aligned} \eta(ab) &= \begin{pmatrix} ab & 0 \\ -0 & ab \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ -0 & a \end{pmatrix}\begin{pmatrix} b & 0 \\ -0 & b \end{pmatrix} \\ &= \eta(a)\eta(b) \end{aligned}$$

Ahora notemos que $\eta(1) = \begin{pmatrix} 1 & 0 \\ -0 & 1 \end{pmatrix}$, es decir, manda unidades en unidades.

Por último si $\eta(x) = \eta(y)$, entonces $\begin{pmatrix} x & 0 \\ -0 & x \end{pmatrix} = \begin{pmatrix} y & 0 \\ -0 & y \end{pmatrix}$. Sabemos que dos matrices son iguales si y sólo si son iguales en todas sus entradas., tenemos que $x = y$. Así la función es inyectiva. □

De igual manera tenemos que para este modelo $\mathbb{R} \subseteq \mathbb{C}$.

Finalmente, verifiquemos que existe i,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -0 & -1 \end{pmatrix}$$

Vamos a comparar los dos modelos, en el segundo modelo podemos plantear un segundo i:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -0 & -1 \end{pmatrix}$$

Lo que esta sucediendo es que si $i^2 = -1$ también tenemos que $(-i)^2 = -1$. En el caso de las matrices no tenemos una forma (muy intuitiva) de elegir cual de las dos posibilidades poner como i. Pero en el caso del plano cartesiano es bastante intuitivo elegir a $(0,1)$.

Vale la pena hacer una aclaración sobre la notación, comunmente se suelen usar z y w para denotar complejos, en cuyo caso nos estaremos refiriendo a que son de la forma $z = z_1 + iz_2$ o $w = w_1 + iw_2$.

Para finalizar esta sección analizaremos el problema de encontrar la raíz cuadrada de un número complejo $z = a + bi \in \mathbb{C}$. Buscamos un complejo $w = x + iy \in \mathbb{C}$ tal que $w^2 = z$, esto es:

$$a + bi = (x + yi)^2 = x^2 - y^2 + 2xyi$$

Ahora tenemos el siguiente sistema de ecuaciones:

$$\begin{cases} a &= x^2 - y^2 \\ b &= 2xy \end{cases}$$

Procedemos a elevar al cuadrado ambas ecuaciones;

$$\begin{cases} a^2 &= x^4 - 2x^2y^2 + y^4 \\ b^2 &= 4x^2y^2 \end{cases}$$

Para luego sumarlas

$$a^2 + b^2 = x^4 + 2x^2y^2 + y^4 = (x^2 + y^2)^2$$

De aquí

$$x^2 + y^2 = \sqrt{a^2 + b^2}$$

Sumandole a esta última ecuación, la primer ecuación del sistema de ecuaciones, $a = x^2 - y^2$, tenemos:

$$2x^2 = a + \sqrt{a^2 + b^2}$$

Despejando llegamos a que:

$$x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$$

Por otro lado, si en vez de sumar restamos, tenemos que:

$$2y^2 = \sqrt{a^2 + b^2} - a$$

De nuevo, despejando:

$$y = \pm\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}$$

Finalmente para las raíces podemos elegir la positiva o la negativa. Ahora bien, como tenemos a x y a y esto nos da 4 posibles combinaciones. De las cuales sólo 2 son correctas. Para saber cuales son recordamos la segunda ecuación $b = 2xy$. Esto nos dice que si $b > 0$ entonces elegimos x y y con el mismo signo, y en caso de que $b < 0$ entonces elegimos a x y y con signo contrario.

EJEMPLO 1.2. *Obtener $\sqrt{i}$.*

SOLUCIÓN. *Usaremos las fórmulas obtenidas anteriormente para $a = 0$ y $b = 1$:*

$$x = \pm\sqrt{\frac{0 + \sqrt{0^2 + 1^2}}{2}} = \frac{1}{\sqrt{2}}$$

$$y = \pm\sqrt{\frac{\sqrt{0^2 + 1^2} - 0}{2}} = \frac{1}{\sqrt{2}}$$

Dado que $b > 0$, las raíces cuadradas son:

$$\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

$$-\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$$

EJEMPLO 1.3. *Obtener* $\sqrt{-i}$.

SOLUCIÓN. *Lo único que difiere este ejemplo con el anterior es en los signos de x y y, ya que* $b<0$ *tenemos que los signos de x y y deben ser opuestos, por lo tanto las raíces son:*

$$\frac{1}{\sqrt{2}}-i\frac{1}{\sqrt{2}}$$
$$-\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}}$$

Formalmente lo que sería un modelo de los complejos es $\mathbb{C}$ es:

- $\mathbb{C}$ es un campo.
- Existe un morfismo de campos $\eta:\mathbb{R}\longrightarrow\mathbb{C}$ (que sea morfismo de campos quiere decir que abre sumas, multiplicaciones y manda al uno en el uno).
- La ecuación $x^2+1=0$ tiene solución.
- Si existe otro campo K donde la ecuación tiene solución y cuenta con un morfismo de campos $\varepsilon:\ :\mathbb{R}\longrightarrow K$, entonces existe un único $\theta:\mathbb{C}\longrightarrow K$ tal que $\theta\eta=\varepsilon$.

PROPOSICIÓN 1.5. *Ambos modelos de los complejos propuestos cumplen lo anterior.*

2. Geometría subyacente de la estructura algebraica de $\mathbb{C}$

2.1. El plano complejo. Recordaremos que el modelo básico que tomamos de $\mathbb{C}$ tiene como conjunto subyacente a $\mathbb{R}^2$, por lo que a todo $z\in\mathbb{C}$ se le puede identificar con la pareja ordenada $(x,y)\in\mathbb{R}^2$ si $z=x+iy$. De aquí en adelante llamaremos a $\mathbb{R}^2$ el **plano complejo**, en el cual llamaremos al eje x como el **eje real** y al eje y como el **eje imaginario**. Esto se muestra en la figura 1.

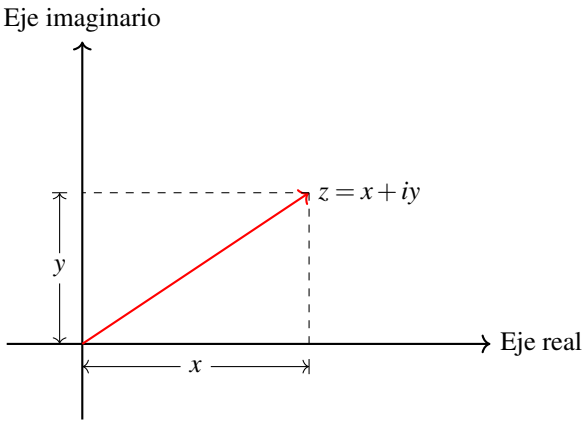

FIGURA 1. El plano complejo.

Note que esto da lugar a un par de funciones, a saber las proyecciones en la primera y segunda coordenada, las cuales llamaremos la **parte real** y la **parte imaginaria** respectivamente, y que denotaremos por

$$Re, Im:\mathbb{C}\to\mathbb{R}.$$

Escribiendo esto de forma ecuacional, por definición se tiene que:

$$Re(x+iy)=x$$

$$Im(x+iy) = y$$

Algunas propiedades básicas de estas funciones se encuentran en el siguiente resultado.

PROPOSICIÓN 2.1.

1. *Las funciones parte real e imaginaria son $\mathbb{R}$-lineales. Es decir, para cualesquiera $z, w \in \mathbb{C}$ y $\lambda \in \mathbb{R}$, se cumple que:*
$$Re(\lambda z + w) = \lambda Re(z) + Re(w)$$
$$Im(\lambda z + w) = \lambda Im(z) + Im(w)$$
Además, las matrices asociadas respectivas son $\begin{pmatrix} 1 & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 1 \end{pmatrix}$. Más aún, estas funciones son suprayectivas pero no inyectivas.
2. *Para cualquier $z \in \mathbb{C}$:*
$$(Re \circ Re)(z) = Re(z)$$
$$(Re \circ Im)(z) = Im(z)$$
$$(Im \circ Re)(z) = 0$$
$$(Im \circ Im)(z) = 0$$
$$z = Re(z) + i \cdot Im(z)$$
3. *Para cualesquiera $z, w \in \mathbb{C}$ se cumple que:*
$$Re(zw) = Re(z)Re(w) - Im(z)Im(w)$$
$$Im(zw) = Re(z)Im(w) + Im(z)Re(w)$$

DEMOSTRACIÓN. Para la primera afirmación supongamos que $z = z_1 + iz_2$ y $w = w_1 + iw_2$. Entonces, dado $\lambda \in \mathbb{R}$ se tiene que

$$\lambda z + w = (\lambda z_1 + w_1) + i(\lambda z_2 + w_2)$$

De esto se deduce que

$$Re(\lambda z + w) = \lambda z_1 + w_1 = \lambda Re(z) + Re(w)$$
$$Im(\lambda z + w) = \lambda z_2 + w_2 = \lambda Im(z) + Im(w)$$

Para la matriz asociada, si $\beta = \{1 = e_1, i = e_2\} \subseteq \mathbb{C}$ es la base canónica de $\mathbb{C}$ como $\mathbb{R}$-espacio, entonces $Re(1) = 1$ y $Re(i) = 0$. Así, para la parte real la matriz asociada es

$$\begin{pmatrix} Re(1) & | & Re(i) \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

De forma análoga notemos que $Im(1) = 0$ y $Im(i) = 1$, por lo que la matriz asociada a la parte imaginaria es:

$$\begin{pmatrix} Im(1) & | & Im(i) \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix}.$$

Además note que dado $\lambda \in \mathbb{R}$, $Re(\lambda) = \lambda$ y $Im(\lambda i) = \lambda$, por lo que ambas funciones son suprayectivas. Además note que $Re(0) = Re(i) = 0$ y $Im(0) = Im(1) = 0$, por lo que ambas funciones no son inyectvas.

La afirmación 2 es clara de las definiciones pues para $x + iy \in \mathbb{C}$,

$$(Re \circ Re)(x+iy) = Re(x) = x = Re(x+iy)$$
$$(Re \circ Im)(x+iy) = Re(y) = y = Im(x+iy)$$
$$(Im \circ Re)(x+iy) = Im(x) = 0$$
$$(Im \circ Im)(x+iy) = Im(y) = 0$$
$$Re(x+iy) + i\, Im(x+iy) = x + iy$$

Para la última afirmación note que si escribimos $z = Re(z) + i\, Im(z)$ y $w = Re(w) + i\, Im(w)$, entonces al realizar el producto de z y w, por definición se tiene que

$$zw = (Re(z)Re(w) - Im(z)Im(w)) + i(Re(z)Im(w) + Im(z)Re(w)),$$

de lo que se sigue el resultado buscado. □

Con la terminología definida vamos a definir una nueva función de variable compleja con valores en $\mathbb{C}$,

$$\overline{\square} : \mathbb{C} \to \mathbb{C}$$

$$\overline{Re(z) + iIm(z)} = Re(z) - iIm(z)$$

Esta función se conoce como la **conjugación compleja** y note que esta es geométricamente la reflexión respecto al eje real como lo muestra la figura 2.

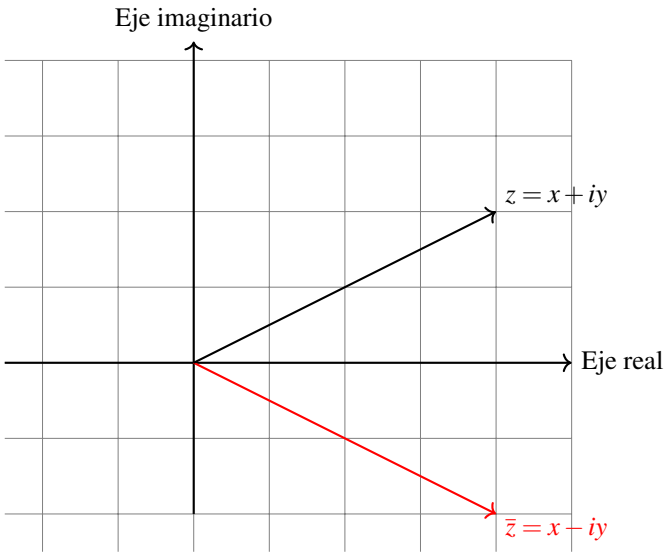

FIGURA 2. La conjugación vista como reflexión.

Algunas propiedades algebraicas básicas de la conjugación compleja se encuentran en el siguiente resultado.

PROPOSICIÓN 2.2. *Sean $z, w \in \mathbb{C}$.*

1. *$z = \overline{z}$ si y sólo si $z \in \mathbb{R}$.*
2. *La conjugación es $\mathbb{R}$-lineal con matriz asociada*
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
3. *$\overline{zw} = \overline{z}\,\overline{w}$*
4. *Si $w \neq 0$, entonces $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$*
5. *$Re(z) = \frac{z+\overline{z}}{2}$ y $Im(z) = \frac{z-\overline{z}}{2i}$*
6. *$Re(\overline{z}) = Re(z)$ y $Im(\overline{z}) = -Im(z)$*
7. *La conjugación es una involución, es decir, $\overline{\overline{z}} = z$. En particular la conjugación es biyectiva.*

DEMOSTRACIÓN. Para 1 el regreso es claro. Para la ida, si $z = \overline{z}$, entonces $Re(z) + i\,Im(z) = Re(z) - i\,Im(z)$. Esto implica que $2i\,Im(z) = 0$, por lo que $Im(z) = 0$, luego, $z \in \mathbb{R}$.

Respecto a 2, si $\lambda \in \mathbb{R}$ y $z, w \in \mathbb{C}$, entonces note que como $\lambda z + w = (\lambda Re(z) + Re(w)) + i(\lambda Im(z) + Im(w))$, entonces

$$\overline{\lambda z + w} = (\lambda Re(z) + Re(w)) - i(\lambda Im(z) + Im(w)) = \lambda(Re(z) - i\,Im(z)) + (Re(w) - i\,Im(w)) = \lambda\overline{z} + \overline{w},$$

que es lo que se quería probar respecto a la linealidad. Respecto a la matriz asociada se deduce que dado que en la base canónica estándar (como $\mathbb{R}$-espacio) $\{1,i\} \subseteq \mathbb{C}$ se tiene que $\overline{1} = 1$ y $\overline{i} = -i$, entonces la matriz buscada es

$$\begin{pmatrix} \overline{1} & | & \overline{i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Para 3, como $zw = (Re(z)Re(w) - Im(z)Im(w)) + i(Re(z)Im(w) + Im(z)Re(w))$, entonces

$$\overline{zw} = (Re(z)Re(w) - Im(z)Im(w)) - i(Re(z)Im(w) + Im(z)Re(w)) = \overline{z}\,\overline{w}$$

Respecto a 4 note que como $z = \frac{z}{w}w$, al usar 3 se tiene que $\overline{z} = \overline{(\frac{z}{w})}\overline{w}$, de lo que se deduce el resultado buscado.

Para 5 observemos que si escribimos $z = Re(z) + i\ Im(z)$, entonces $\overline{z} = Re(z) - i\ Im(z)$, de donde $z + \overline{z} = 2Re(z)$, mientras que $z - \overline{z} = 2i\ Im(z)$, de donde se deduce el resultado claramente. Además, de esto mismo se ve que 6 también es válido.

La afirmación 7 es clara. □

Para continuar, dado un vector cualquiera en el plano complejo, a este se le puede asociar su longitud, que no es más que la distancia de este al origen. Esto nos permite definir una función

$$|\square| : \mathbb{C} \to \mathbb{R},$$

que no es más que la norma usual de $\mathbb{R}^2$. En este contexto, a esta función la llamaremos la **norma compleja** y esta cumple las siguientes propiedades.

PROPOSICIÓN 2.3. *La norma compleja satisface:*

1. *Es una norma real, es decir,*
   - *Para todo $z \in \mathbb{C}$, $|z| \geq 0$*
   - *$|z| = 0$ si y sólo si $z = 0$*
   - *Para cualquier $\lambda \in \mathbb{R}$ y $z \in \mathbb{C}$, $|\lambda z| = abs(\lambda)|z|$, con $abs(\lambda)$ el valor absoluto de λ.*
   - *(Desigualdad del triángulo) Para cualesquiera $z, w \in \mathbb{C}$ se tiene que*

$$|z + w| \leq |z| + |w|$$

2. *Es un valor absoluto sobre $\mathbb{C}$, es decir, para cualesquiera $z, w \in \mathbb{C}$, $|zw| = |z||w|$*
3. *Extiende al valor absoluto real, es decir, para cualquier $\lambda \in \mathbb{R}$, $|\lambda| = abs(\lambda)$. Por tal razón, de ahora en adelante no usaremos la notación abs.*
4. *Para cualquier $z \in \mathbb{C}$, $|Re(z)| \leq |z|$, $|Im(z)| \leq |z|$ y $|z| \leq |Re(z)| + |Im(z)|$*
5. *Para cualquier $z \in \mathbb{C}$, $z\overline{z} = |z|^2$. Por lo tanto, si $z \neq 0$, entonces $z^{-1} = \frac{\overline{z}}{|z|^2}$*
6. *Para cualquier $z \in \mathbb{C}$, $|z| = |\overline{z}|$*
7. *Para cualesquiera $z, w \in \mathbb{C}$, $||z| - |w|| \leq |z - w|$*
8. *Se cumple la desigualdad de Cachy-Schwartz, es decir,*

$$\left| \sum_{k=1}^{n} z_k w_k \right| \leq \sqrt{\sum_{k=1}^{n} |z_k|^2} \sqrt{\sum_{k=1}^{n} |w_k|^2}$$

DEMOSTRACIÓN. Todas las propiedades salvo 2, 5 y 6 se ven en Cálculo o Álgebra Lineal. 1 Note que 5 es un cálculo directo pues

$$z\overline{z} = (Re(z) + i\,Im(z))(Re(z) - i\,Im(z)) = Re(z)^2 - i^2 Im(z)^2 = |z|^2$$

Además, si $z \neq 0$, entonces $|z| \neq 0$. Así, $z(\frac{\overline{z}}{|z|^2}) = 1$. Por unicidad del inverso multiplicativo se sigue el resultado.

La propiedad 6 es obvia de 5 (o la definición directa de la norma) y 2 también es obvia de la primera afirmación de 5. □

2.2. Estructura aditiva de $\mathbb{C}$. Ahora trataremos la interpretación geométrica de las operaciones en los complejos. Respecto a la suma y diferencia esta proviene de la identificación $\mathbb{C} = \mathbb{R}^2$, de donde se heredaron estas operaciones. Para esto considere $z, w \in \mathbb{C}$ con $z = z_1 + iz_2$ y $w = w_1 + iw_2$. Consideremos la representación vectorial de z y w mediante flechas que unen el origen de $\mathbb{R}^2$ con los puntos (z_1, z_2) y (w_1, w_2) respectivamente. Para esto nos apoyaremos en la figura 3.

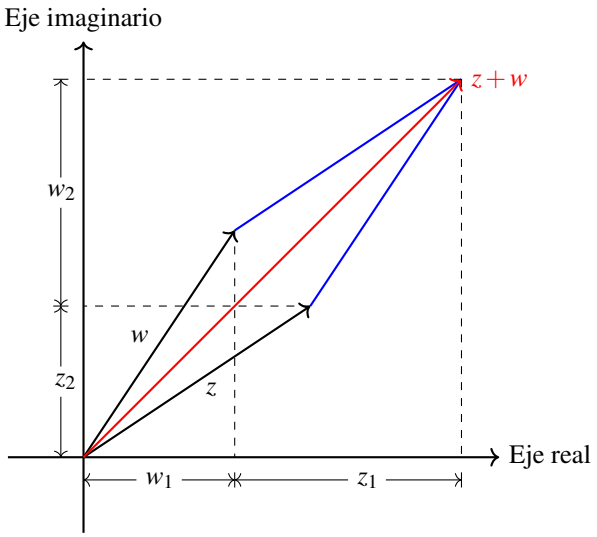

FIGURA 3. Geometría de la suma de complejos

Esto muestra que la suma de z y w se obtiene por medio de la **ley del paralelogramo** y corresponde a la diagonal del paralelogramo formado por los vectores z y w. Además note que de esta figura se puede ver que se cumple la desigualdad del triángulo, $|z+w| \leq |z| + |w|$, pues en geometría euclidiana la mínima distancia entre dos puntos se da a partir de una línea recta entre estos.

Por otro lado, dado que la diferencia de complejos es realmente una suma pues $z - w = z + (-w)$, esta también se obtiene por la ley del paralelogramo como se observa en la figura 4. Note que dado que la longitud de $z - w$ es medida con la norma compleja, esta es la misma que la de la segunda diagonal del paralelogramo en la figura 3 pues podemos trasladar $z - w$ a dicha diagonal o por el criterio LAL de congruencia.[1] Es importante observar que el tomar inversos aditivos en los complejos corresponde trivialmente a una reflexión respecto al origen del plano complejo.

Ya que hemos interpretado las operaciones que provienen de la estructura aditiva de $\mathbb{C}$, vamos a hacer lo propio con el producto de complejos. Para esto requerimos recordar algunas ideas de geometría analítica, a saber, la de coordenadas polares. Esto se presentará en la siguiente subsección.

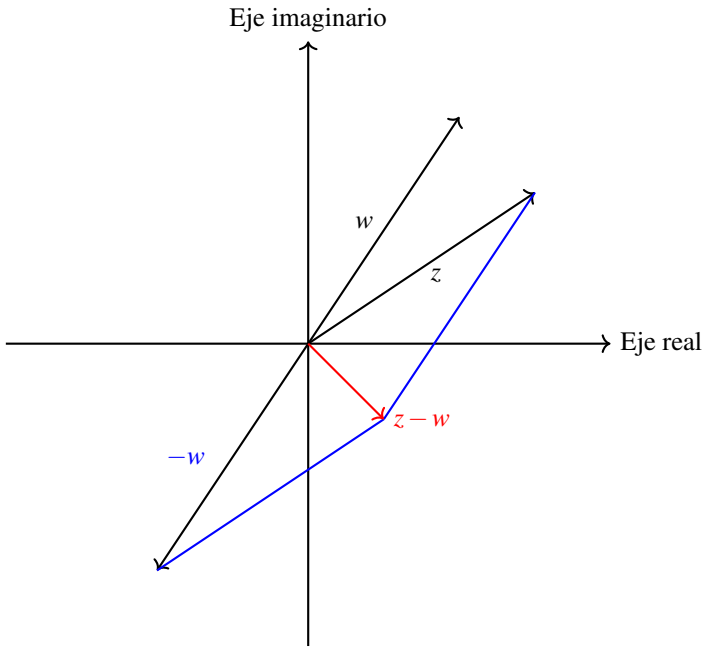

FIGURA 4. Geometría de la resta de complejos

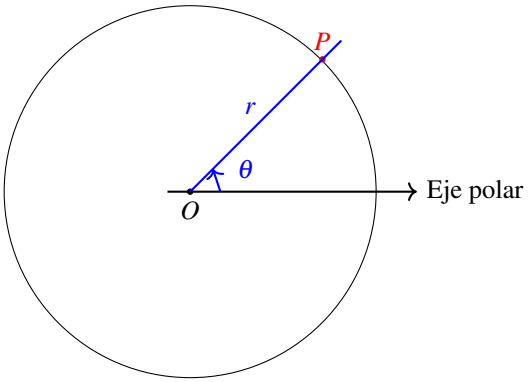

FIGURA 5. Sistema polar

2.3. Representación polar. Comencemos con considerar un plano, un punto distinguido al cual llamaremos el origen y denotaremos por O, y tracemos una recta a partir de dicho punto la cual tomaremos como horizontal por comodidad y que llamaremos el eje polar. Esta situación se muestra en la figura 5.

Note que por cualquier punto en el plano que no es el origen, digamos P, podemos trazar una única circunferencia con centro en O y que pasa por el punto P. Con el radio de dicha circunferencia y el ángulo entre la recta que une a O y P y el eje polar, podemos determinar la ubicación del punto P, además note que este proceso puede hacerse para cualquier punto que no es el origen. A dicho radio r lo llamaremos la **norma** del punto P y a dicho ángulo como **un argumento** del punto P. Además, por completez al punto O le

[1]Este criterio es el "lado ángulo lado" en los triángulos $\Delta 0wz$ y $\Delta 0z(z-w)$ pues estos comparten un lado (vector z), los lados w y el formado por el segmento $z-w$ y z tienen la misma magnitud, y los ángulos entre los lados correspondientes son los mismos.

asignamos norma cero, pero no le asignamos ningún argumento.[2] Así, a la pareja (r,θ) descrita anteriormente la llamaremos las **coordenadas polares** del punto $P \neq O$. Es importante notar que nos referimos a θ como **un** argumento y no como "el argumento" pues este no está unívocamente determinado pues dado un ángulo, al sumar a este un múltiplo entero de 2π obtenemos la misma representación del ángulo original.

Podemos ahora realizar esta construcción sintética en el plano complejo, donde O será el cero complejo y el eje polar el eje real positivo. Esto nos permite por trigonometría básica ver que si $P = x+iy \neq 0$, entonces existen $r > 0$ y $\theta \in \mathbb{R}$ tales que $x = r\cos\theta$ y $y = r\operatorname{sen}\theta$, por lo que

$$P = r(\cos\theta + i\operatorname{sen}\theta) =: r\ cis\theta$$

A esta última expresión de le conoce como la **representación polar del complejo** $x+iy$. Además note que trivialmente $r = |x+iy| = \sqrt{x^2+y^2}$.

EJEMPLO 2.1. *Encontrar la representación polar del complejo* $\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

SOLUCIÓN. *Note que* $r = |\frac{1}{2} + i\frac{\sqrt{3}}{2}| = \sqrt{(\frac{1}{2})^2 + (\frac{\sqrt{3}}{2})^2} = 1$. *Por otro lado como este complejo no es puramente imaginario, el argumento se obtiene de la ecuación* $\tan\theta = \frac{y}{x} = \sqrt{3}$, *por lo que* $\theta = \frac{\pi}{3} + 2\pi k$, $k \in \mathbb{Z}$. *Geométricamente tenemos la situación de la figura 6.*

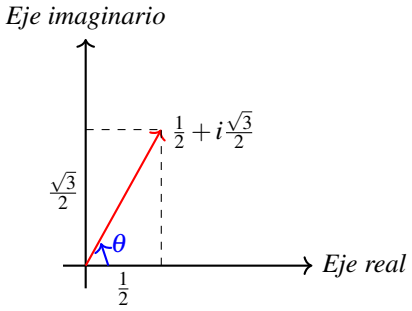

FIGURA 6. Representación polar del complejo $\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Por lo tanto,

$$\begin{aligned}\frac{1}{2} + i\frac{\sqrt{3}}{2} &= 1(\cos\frac{\pi}{3} + i\operatorname{sen}\frac{\pi}{3}) \\ &= \cos\frac{\pi}{3} + i\operatorname{sen}\frac{\pi}{3} \\ &=: cis\frac{\pi}{3}\end{aligned}$$

En esta última representación estamos tomando un argumento "estándar" pues estamos restringiendo los valores de este al intervalo $[0,2\pi)$, *pero la elección en cualquier otro intervalo es perfectamente válida.*

Podemos recapitular la cuestión del ángulo estudiada diciendo que tenemos una relación

$$\arg : \mathbb{C}^* \to \mathbb{R},$$

donde $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, que a cada complejo le asigna un argumento de este. Usamos el término relación pues como comentamos el argumento está bien definido salvo múltiplos enteros de 2π. Algunos textos llaman a esto

[2] Esto último pues si pensamos a un punto como una circunferencia degenerada, tendríamos problemas con la construcción mencionada en la asignación de un argumento para este caso.

funciones multivaluadas, sin embargo, nosotros no usaremos esta última terminologia pues conjuntistamente arg es una relación pues esta permite asociar a $x+iy$ el conjunto $\{\theta+2\pi k \ : \ k\in\mathbb{Z},\ \tan\theta=\frac{y}{x}\}$.

El especificar un rango particular en el codominio donde arg sea una función[3] como por ejemplo los intervalos $[0,2\pi)$, $[-\pi,\pi)$ y $(-\pi,\pi]$ se conoce como tomar una **rama del argumento**. Este último concepto se entenderá en las secciones posteriores.

Aprovecharemos la teoría desarrollada para demostrar un resultado clásico. Para esto note que si $z,w\in\mathbb{C}$ son diferentes de cero, entonces representamos ambos complejos usando coordenadas polares

$$z = r_1\ cis\theta_1$$

$$w = r_2\ cis\theta_2$$

Entonces realicemos el producto de estos mediante estas representaciones coordenadas, con lo que tenemos que:

$$\begin{aligned} zw &= r_1r_2(\cos\theta_1+i\,\mathrm{sen}\,\theta_1)(\cos\theta_2+i\,\mathrm{sen}\,\theta_2)\\ &= r_1r_2((\cos\theta_1\cos\theta_2-\mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2)+i(\mathrm{sen}\,\theta_1\cos\theta_2+\cos\theta_1\,\mathrm{sen}\,\theta_2))\\ &= r_1r_2(\cos(\theta_1+\theta_2)+i\,\mathrm{sen}(\theta_1+\theta_2)) \end{aligned}$$

Esto da pie a lo siguiente.

PROPOSICIÓN 2.4. *Para cualesquiera $z,w\in\mathbb{C}^*$,*

$$\arg(zw)=\arg(z)+\arg(w)+2\pi k,$$

con $k\in\mathbb{Z}$. Por lo que tomando una rama del argumento específica,

$$\arg(zw)=\arg(z)+\arg(w)$$

Además tenemos el siguiente interesante resultado.

PROPOSICIÓN 2.5. *(De Moivre) Si $z\in\mathbb{C}$ se escribe de la forma polar como $z=r\ cis\theta$, entonces para cualquier $n\in\mathbb{Z}$ se cumple que:*

$$z^n = r^n cis(n\theta)$$

DEMOSTRACIÓN. Por inducción entera: La base de la inducción es cuando $n=0$, en cuyo caso no hay nada que probar. Para el paso inductivo, si suponemos que el resultado vale para n, notemos que dado que $z^{n+1}=z^nz$, el cálculo realizado anteriormente aunado al hecho de que $z=r\ cis\theta$ y $z^n=r^ncis(n\theta)$ implica que

$$z^{n+1}=r^nr\ cis(n\theta+\theta)=r^{n+1}cis((n+1)\theta)$$

Para concluir, si $n<0$, entonces existe $m>0$ tal que $n=-m$. Note que entonces $z^n=(z^m)^{-1}=(r^m\ cis(m\theta))^{-1}=r^{-m}\ cis(m\theta)^{-1}=r^n\ cis(m\theta)^{-1}$. Ahora observe que

$$cis(m\theta)^{-1}=\frac{\overline{cis(m\theta)}}{|cis(m\theta)|^2}=\cos(m\theta)-i\,\mathrm{sen}(m\theta)=\cos(-m\theta)+i\,\mathrm{sen}(-m\theta)=cis(n\theta),$$

lo que concluye la prueba. □

[3]De hecho note que esta restricción no solo hace que arg se función, sino que hasta es biyectiva.

Una de las aplicaciones básicas de este resultado que tiene que ver con la obtención de raíces n-esimas en $\mathbb{C}$. Para esto supongamos que $n \in \mathbb{N}^+$ y queremos hallar las raíces n-esimas de un complejo $w \in \mathbb{C}$ dado, el cual es no cero para no trivializar la pregunta. Esto es equivalente a resolver la ecuación

$$z^n = w,$$

donde la incógnita en z. Note que por el Teorema Fundamental del Álgebra esa ecuación siempre se puede resolver y además podemos encontrar n raíces contando mutiplicidades. Así que para resolverla expresamos en forma polar a $w = r\ cis\theta$ y supongamos que $z \in \mathbb{C}$ es una solución, por lo que esta la expresamos usando coordenadas polares como $z = \rho\ cis\phi$. El hecho de que $z^n = w$ implica usando el teorema de De Moivre que:

$$\rho^n\ cis(n\phi) = r\ cis(\theta) \tag{7}$$

Al tomar la norma en esta ecuación se deduce que $\rho^n = r$; como $r, \rho \in \mathbb{R}$ y son positivos, entonces deducimos que $\rho = \sqrt[n]{r}$. Además, al usar esto en la ecuación (7)se deduce que $cis(n\phi) = cis(\theta)$, lo que sucede si y sólo si existe $k \in \mathbb{Z}$ tal que $n\phi = \theta + 2\pi k$. Con esto hemos encontrado las raíces buscadas y así prácticamente hemos demostrado el siguiente resultado.

PROPOSICIÓN 2.6. *Dado $w \in \mathbb{C}$ no cero expresado de forma polar como $w = r\ cis(\theta)$, las raíces n-esimas de este complejo están dadas por*

$$z_k = \sqrt[n]{r}\ cis\left(\frac{\theta + 2\pi k}{n}\right),$$

donde $k \in \{0, ..., n-1\}$.

DEMOSTRACIÓN. Lo único que falta argumentar son los valores que toma k, pero esto es consecuencia de la periodicidad de las funciones coseno y seno. □

EJEMPLO 2.2. *Como caso particular el resultado anterior nos permite calcular las raíces n-ésimas de la unidad para $n > 1$, las cuales están dadas por*

$$z_k = cis\left(\frac{2\pi k}{n}\right),$$

con $k \in \{0, ..., n-1\}$.

Note que todas estas raíces tienen norma uno, por lo que todas se encuentran sobre el círculo unitario. Si $n = 2$ estas claramente son $z_1 = 1$ y $z_2 = -1$. Cuando $n > 2$ las notemos que las raíces sucesivas forman un ángulo de $\frac{2\pi}{n}$, por lo que con estas podemos construir un polígono regular de n lados inscrito en la circunferencia unitaria donde los vértices son las raíces. Este hecho no es particular de nuestro ejemplo y recomendamos el ejercicio **??** *para ver un caso más general. Por otro lado, este ejemplo muestra un modelo como grupo multiplicativo del grupo $(\mathbb{Z}/n, +)$.*

2.4. Interpretación del producto en $\mathbb{C}$. Regresando a nuestro problema de dar una interpretación del producto complejo, note que si $z, w \in \mathbb{C}$ son diferentes de cero, entonces representamos ambos complejos usando coordenadas polares

$$z = r_1\ cis\theta_1$$
$$w = r_2\ cis\theta_2$$

En la subsección anterior demostramos que esto implica que:

$$zw = r_1 r_2\ cis(\theta_1 + \theta_2)$$

Este cálculo nos esta diciendo que si tomamos el complejo w y hacemos el producto con z, el complejo resultante se obtiene al multiplicar el módulo de w por el de z y hacer una rotación por θ_1 grados al vector que representa a w. Esto se muestra en la figura **??**.

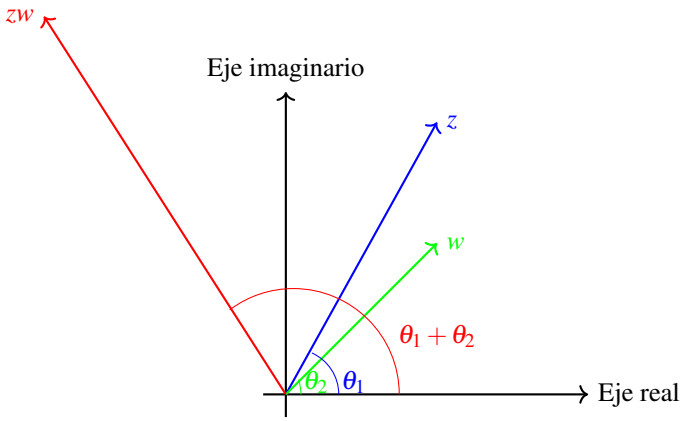

FIGURA 7. Interpretación del producto de complejos

Veamos esto mediante un ejemplo concreto.

EJEMPLO 2.3. *Consideremos $z = w = i$. En representación polar $z = w = cis(\frac{\pi}{2})$. Entonces zw tiene norma 1 y el ángulo que le corresponde respecto al eje real es $\frac{\pi}{2} + \frac{\pi}{2} = \pi$. Es decir,*

$$zw = cis(\pi) = -1$$

¡Lo que justamente nos muestra que $i^2 = -1$!

Ejercicios del capítulo

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

EJERCICIO 2.1. *Calcule i^n para cualquier $n \in \mathbb{Z}$.*

EJERCICIO 2.2. *Calcula las raíces sextas de -64 y las raíces cúbicas de $8i$.*

EJERCICIO 2.3. *Demuestre que si $z \in \mathbb{C}$ es una raíz n-ésima de la unidad con $z \neq 1$, entonces $\sum_{k=0}^{n-1} z^k = 0$.*

EJERCICIO 2.4. *Demuestre que $z \in \mathbb{R}$ si y sólo si $z = \bar{z}$.*

EJERCICIO 2.5. *Demuestre que $z \in \mathbb{R}$ o z es imaginario puro si y sólo si $z^2 = \overline{(z)}^2$.*

EJERCICIO 2.6. *Demuestre que $|z+w|^2 = |z|^2 + 2Re(z\overline{w}) + |w|^2$.*

EJERCICIO 2.7. *Demuestre que $|z+w|^2 + |z-w|^2 = 2(|z|^2 + |w|^2)$.*

EJERCICIO 2.8. *Demuestre que si $|z| = 1$ o $|w| = 1$ y $\bar{z}w \neq 1$, entonces*

$$\left| \frac{z-w}{1-\bar{z}w} \right| = 1$$

EJERCICIO 2.9. *Supongamos que $n \in \mathbb{N}$ con $n \geq 2$. Demuestre que las raíces del polinomio $x^n - 1$ son los vértices de un polígono regular en el plano complejo.*

EJERCICIO 2.10. *Definimos el conjunto*

$$\mathbb{C}_1^+ = \{z \in \mathbb{C} \,:\, Re(z) > 0\}$$

Dí si las siguientes afirmaciones son verdaderas ó falsas dando una demostración o contraejemplo según sea el caso.

1. *Si $z, w \in \mathbb{C}_1^+$ entonces $z + w \in \mathbb{C}_1^+$.*
2. *Si $z, w \in \mathbb{C}_1^+$ entonces $zw \in \mathbb{C}_1^+$.*
3. *Para todo $z \in \mathbb{C}$ se satisface una y sólo una de las siguientes afirmaciones: $z \in \mathbb{C}_1^+$, $z = 0$ ó $-z \in \mathbb{C}_1^+$.*

DEFINICIÓN 2.1. *Sea K un campo, decimos que un orden total $\leq$ sobre K respeta las operaciones (de K) si:*

1. *Para todo $a, b, c \in K$ tal que $a \leq b$, $a + c \leq b + c$.*
2. *Para todo $a, b \in K$ tal que $0 \leq a$ y $0 \leq b$, $0 \leq ab$.*

EJERCICIO 2.11. *Demuestra que no existe orden total en $\mathbb{C}$ que respete las operaciones de dicho campo.*

EJERCICIO 2.12. *Considere la función* $g : \mathbb{C}^* \to \mathbb{C}^*$ *con regla de correspondencia:*

$$g(z) = \frac{1}{z}.$$

Demuestre que esta función manda circunferencias en el plano complejo centradas en el origen en circunferencias en el plano complejo centradas en el origen.[4] *Discutir lo que sucede con el radio en esta transformación.*

[4]Por circunferencias nos referimos a circunferencias no degeneradas.

Capítulo 6

Polinomios

En este capítulo introduciremos la noción de polinomio con coeficientes en un campo (en una variable), para la cual daremos una definición formal, y veremos como es que esta nos permite recuperar las expresiones de la forma $\sum_{j=0}^{n} a_j x^j$. Además probaremos que el conjunto de dichos polinomios tiene estructura de anillo y que este cumple algunas propiedades que tiene el anillo de los números enteros.

1. Definiciones básicas

En todo este capítulo K denotará un campo arbitrario, a no ser que se diga lo contrario.

Denotemos por $K^{\mathbb{N}}$ al conjunto de sucesiones con dominio $\mathbb{N}$ y codominio el campo K. Recordemos que un elemento $f \in K^{\mathbb{N}}$ queda determinado por sus valores, $f(0), f(1), f(2), ...$, los cuales pueden darnos una cantidad infinita de elementos en K, uno por cada natural. Así que tomaremos un subconjunto del conjunto de sucesiones, para lo cual notemos que dado que K tiene un elemento distinguido, a saber el cero, podemos definir el **soporte de una sucesión**, el que denotaremos por $sop(f)$, como el conjunto:

$$\{n \in \mathbb{N} \,:\, f(n) \neq 0\}.$$

Decimos que una sucesión $f \in K^{\mathbb{N}}$ tiene **soporte finito**, si $|sop(f)| < \infty$, esto es, sólo existen una cantidad finita de elementos cuya imagen es no cero. Esto es equivalente a decir que existe $m \in \mathbb{N}$ tal que para cualquier $n \geq m$, $f(n) = 0$. Por lo tanto, si tomamos una función $f \in K^{\mathbb{N}}$ tal que m cumple la condición anterior, los valores posiblemente no cero de f están dados por la m-ada:

$$(f(0), ..., f(m)) \in K^m$$

A una de estas m-adas le podemos asociar la expresión formal:

$$\sum_{j=0}^{m} f(j)x^j.$$

En lo que sigue identificaremos al elemento f con dicha expresión formal. Así que definimos el conjunto de polinomios con coeficientes en el campo K, el que denotaremos por $K[x]$, como el conjunto de todas las funciones $K^{\mathbb{N}}$ con soporte finito, las cuales escribiremos según la convención anterior.

Al ser los polinomios funciones, hay una noción de igualdad que proviene de la igualdad de funciones, la cual simplemente se reduce a que los valores en la imagen del polinomio en cuestión, sean los mismos. Es decir, dados $f, g \in K[x]$, se tiene que $f = g$ si y sólo si para cualquier $j \in \mathbb{N}$, $f(n) = g(n)$. Cuando escribimos $f = \sum_{j=0}^{n} a_j x^j$, llamaremos a los elemento $a_0, ..., a_j \in K$, los **coeficientes** del polinomio f.

Consideremos $f \in K[x]$ no cero. Dado que existe $m \in \mathbb{N}$ tal que para cualquier $n \geq m$, $f(n) = 0$. Esto dice que el conjunto $\{k \in \mathbb{N} \,:\, \forall n \geq k(f(n) = 0)\} \neq \emptyset$, por lo que el principio del buen orden nos asegura que este tiene un elemento mínimo. Esto nos llega al siguiente concepto.

DEFINICIÓN 1.1. *Para $f \in K[x]$ no cero, definimos el **grado** del polinomio f, como:*

$$\partial(f) = \text{mín}\{k \in \mathbb{N} \ : \ \forall n \geq k(f(n) = 0)\}$$

Además definimos $\partial(0) = -\infty$.

Como consecuencia de la definición de polinomios, para cualquier $m \geq \partial(f)$, se tiene que:

$$\sum_{j=0}^{m} f(j)x^j = \sum_{j=0}^{\partial(f)} f(j)x^j.$$

Al coeficiente correspondiente al grado, se le conoce como **coeficiente principal** del polinomio en cuestión.

OBSERVACIÓN 1.1. *Los polinomios de grado 0, con aquellos que están dados por un elemento no cero del campo. A estos polinomios los llamaremos **polinomios constantes**.*

Nuestra siguiente meta es definir operaciones en el conjunto de polinomios. Para definir una suma, usamos la idea que viene directamente de la suma de funciones, esto es, la definición se hace de forma puntual. En términos de la notación introducida, si $f, g \in K[x]$ y escribimos $f = \sum_{j=0}^{n} f(j)x^j$ y $g = \sum_{j=0}^{m} g(j)x^j$, definimos:

$$f + g := \sum_{j=0}^{\text{máx}\{n,m\}} (f(j) + g(j))x^j$$

Veamos que esta definición nos permite obtener un polinomio de dos polinomios dados, esto es que hemos definido una función:

$$+ : K[x] \times K[x] \longrightarrow K[x]$$

Antes de hacer esto, vamos a dar una convención, para la cual notemos que por definición el grado de un polinomio nos da una función:

$$\partial : K[x] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

En el conjunto $\mathbb{N} \cup \{-\infty\}$, podemos definir un orden que extiende al de los naturales, simplemente poniendo que para cualquier $n \in \mathbb{N} \cup \{-\infty\}$,

$$-\infty \leq n.$$

Con esto en mente, planteamos el resultado buscado.

PROPOSICIÓN 1.1. *Para $f, g \in K[x]$,*

$$f + g \in K[x].$$

Además,

$$\partial(f + g) \leq \text{máx}\{\partial f, \partial g\}.$$

DEMOSTRACIÓN. Para la primera afirmación, notemos que si demostramos que $sop(f+g) \subseteq sop(f) \cup sop(g)$, entonces $sop(f+g)$ es finito pues $f,g \in K[x]$. Para esto, al considerar $n \in sop(f+g)$, se tiene que $0 \neq (f+g)(n) = f(n)+g(n)$. Esto implica que $f(n) \neq 0$ o $g(n) \neq 0$, es decir, que $n \in sop(f) \cup sop(g)$, como se quería probar.

Para la segunda afirmación, esta es obvia si alguno de los polinomios es el polinomio cero, y también lo es si $g = \sum_{j=0}^{\partial(f)} -f(j)x^j$. Dejando estos casos, si $n = \partial(f+g)$, entonces $0 \neq (f+g)(n) = f(n)+g(n)$, así que como antes $f(n) \neq 0$ o $g(n) \neq 0$. El primero de estos casos dice que $n \leq \partial(f)$ y el segundo que $n \leq \partial(g)$. En cualquiera de los casos se deduce que $n \leq \text{máx}\{\partial(f), \partial(g)\}$, lo que concluye la prueba de la afirmación. □

OBSERVACIÓN 1.2. *La desigualdad respecto a los grados en la afirmación anterior puede ser estricta, pues al considerar $f,g \in K[x]$ definidos por $f = 1-x$ y $g = x$, se tiene que $f+g = 1$. Luego $\partial(f+g) <$ $\text{máx}\{\partial(f), \partial(g)\}$.*

Ya que hemos definido una primer operación en $K[x]$, vamos a definir una segunda operación, que jugará el papel del producto en $K[x]$. A diferencia del caso de la suma, para definir dicha operación, nuestra motivación es que se cumpla la ley de los exponentes que se cumple en cualquier anillo, esto es, que $a^n a^m = a^{n+m}$, por lo que la definición no se dará de forma puntual. Para obtener la definición mencionada, dados $f,g \in K[x]$, con $f = \sum_{j=0}^{n} f(j)x^j$ y $g = \sum_{j=0}^{m} g(j)x^j$, definimos fg, para que su j-ésimo coeficiente esté dado mediante la fórmula:

$$(fg)(j) := \sum_{k+l=j} f(k)g(l)$$

OBSERVACIÓN 1.3. *Para $f,g \in K[x]$, podemos calcular el j-ésimo coeficiente del producto mediante las fórmulas:*

$$(fg)(j) = \sum_{k=0}^{j} f(k)g(j-k) = \sum_{k=0}^{j} f(j-k)g(k).$$

Como antes, veamos que con lo anterior obtenemos un polinomio. Esto es, que lo que hemos definido da lugar a una función:

$$\cdot : K[x] \times K[x] \longrightarrow K[x]$$

Nuevamente, para incluir el caso del polinomio cero, requerimos introducir una convención en el conjunto $\mathbb{N} \cup \{-\infty\}$. En este conjunto, extenderemos la suma, definiendo para $n \in \mathbb{N} \cup \{-\infty\}$,

$$-\infty + n := n + (-\infty) := \infty$$

Note que esta definición está de acuerdo con la teoría de límites de sucesiones reales.

Con lo anterior en mente, el resultado buscado es:

PROPOSICIÓN 1.2. *Para $f,g \in K[x]$,*

$$fg \in K[x].$$

Además,

$$\partial(fg) = \partial(f) + \partial(g).$$

DEMOSTRACIÓN. En el caso en que algún polinomio sea cero, ambas afirmaciones son obvias, así que supongamos que $n = \partial(f)$ y $m = \partial(g)$, ambos números naturales. Afirmamos que para $k > n+m$, el coeficiente de fg es cero. En efecto, de la definición tenemos que:

$$(fg)(k) = \sum_{j=0}^{k} f(j)g(k-j) \tag{8}$$

Notemos que si $j > n$, entonces $f(j) = 0$, por lo tanto, en la suma anterior únicamente hay que analizar lo que sucede con los sumandos que corresponden a los índices $j \in \{0,...,n\}$, pues los restantes son cero. Pero para estos, tenemos que $k-j \geq k-n$, pero como $k-n > (n+m)-n = m$, entonces $g(k-j) = 0$, por lo que hemos probado que todos los sumandos en la ecuación (8) son cero. Esto muestra que $fg \in K[x]$. Más aún, para concluir con la demostración, notemos que el coeficiente $n+m$ de fg es no cero. En efecto, al tomar $k = n+m$ en la ecuación (8), y hacer el mismo análisis anterior, se tienen la serie de igualdades:

$$(fg)(n+m) = \sum_{j=0}^{n+m} f(j)g(n+m-j) = \sum_{j=0}^{n} f(j)g(n+m-j) = f(n)g(m).$$

Dado que por definición $f(n), g(m) \neq 0$ y K es un campo, entonces $f(n)g(m) \neq 0$, lo que prueba que $\partial(fg) = n+m$. □

A manera de recapitulación, hemos definido en el conjunto de polinomios $K[x]$, dos funciones:

$$+, \cdot : K[x] \times K[x] \longrightarrow K[x]$$

Dichas funciones, permiten darle una estructura algebraica al conjunto de polinomios.

PROPOSICIÓN 1.3. *$K[x]$ con las operaciones definidas es un anillo.*

DEMOSTRACIÓN. La propiedad asociativa para la suma es obvia. Además el polinomio constante cero es el neutro aditivo, y es claro que para $f \in K[x]$, el polinomio $\sum_{j=0}^{\partial(f)} -f(j)x^j$ es su inverso aditivo. Además claramente la suma es conmutativa.

Para las propiedades del producto, respecto a la asociatividad, sean $f, g, h \in K[x]$. Veamos que $f(gh)$ y $(fg)h$ tienen los mismos coeficientes, lo cual implica que son iguales. En efecto, dado $n \in \mathbb{N}$, se tiene que:

$$\begin{aligned}
(f(gh))(n) :&= \sum_{j+k=n} f(j)(gh)(k) \\
&= \sum_{j+k=n} f(j)\left(\sum_{l+r=k} g(j)h(r)\right) \\
&= \sum_{j+l+r=n} f(j)(g(l)h(r)) \\
&= \sum_{j+l+r=n} (f(j)g(l))h(r) \\
&= \sum_{k+r=n} \left(\sum_{j+l=k} f(j)g(l)\right)h(r) \\
&= \sum_{k+r=n} (fg)(k)h(r) \\
&=: ((fg)h)(n)
\end{aligned}$$

Para las propiedades que faltan, es claro de la definición que el polinomio constante con valor 1 es el neutro del producto. Además la conmutatividad se deduce de la definición nuevamente. Respecto a la

propiedad distributiva, esta es un cálculo sencillo que se sigue de que esta propiedad se sigue de la propiedad correspondiente para el campo. □

El siguiente paso es estudiar algunas propiedades de este anillo. La primera tiene que ver con que no todos los elementos en el anillo de polinomios son unidades, pues por ejemplo el polinomio $f = x \in K[x]$, no tiene un inverso, ya que si existiera dicha inverso, digamos $g \in K[x]$, se tendría que $xg = 1$. Al calcular el grado se tendría que cumplir que $1 + \partial(g) = 0$, lo cual es imposible.

Ya que sabemos que no todos los elementos del anillo de polinomios son unidades, el siguiente paso es ver si podemos caracterizar los elementos que los son. El resultado buscado es:

PROPOSICIÓN 1.4. *Sea $f \in K[x]$. Entonces f es una unidad si y sólo si $\partial(f) = 0$.*

DEMOSTRACIÓN. $\Rightarrow$) Por hipótesis existe $g \in K[x]$ tal que $fg = 1$. Al calcular el grado se tiene que $\partial(f) + \partial(g) = 0$. Esto dice que los polinomios f y g son no cero, por lo que su grado es un número natural, y así $\partial(f) = \partial(g) = 0$, de donde se deduce el resultado.

$\Leftarrow$) Por hipótesis existe $c \in K \setminus \{0\}$ tal que $f = c$. Definamos $g = c^{-1} \in K[x]$, y notemos que $fg = 1$, por lo que f es unidad. □

De forma análoga a lo que pasó con $\mathbb{Z}$, si bien dicho anillo no es un campo, este no tiene divisores de cero. Nuevamente tenemos esta propiedad para $K[x]$.

PROPOSICIÓN 1.5. *$K[x]$ es dominio entero.*

DEMOSTRACIÓN. Supongamos que $f, g \in K[x]$ son no cero. Por lo tanto $\partial(f), \partial(g) \in \mathbb{N}$, así que $\partial(fg) = \partial(f) + \partial(g) \in \mathbb{N}$, lo que dice que $fg \neq 0$. □

Para concluir los resultado básicos de esta sección, vamos a ver que todo polinomio tiene asociada una función polinomial. Hay que tener cuidado pues estos dos conceptos suelen confundirse, y no son lo mismo (ver ejercicio 5.11). Así, para $f \in K[x]$, definimos su **función polinomial asociada**, $Pol(f) : K \to K$, mediante la regla de correspondencia:

$$Pol(f)(a) := f(a).$$

Al elemento $f(a) \in K$ obtenido de sustituir todas las ocurrencias de la variable x en f, se le conoce como la **evaluación** de f en a. De forma explícita, si $f = \sum_{j=0}^{n} b_j x^j$, entonces:

$$f(a) := \sum_{j=0}^{n} b_j a^j.$$

En lo que sigue de estas notas escribiremos a los polinomios mediante expresiones de la forma $f = \sum_{j=0}^{n} a_j x^j$, eliminando la notación para los coeficientes mediante los elementos $f(0), ..., f(n)$, con el fin de no confundir la notación con la evaluación de un polinomio en un elemento del campo en cuestión.

EJEMPLO 1.1. *Considere $f \in \mathbb{Z}_2[x]$ definido mediante $f = x^2 + x$. Calculemos las posibles evaluaciones del polinomio anterior en los únicos dos elementos de $\mathbb{Z}_2$. Estas son:*

$$f(0) := 0^2 + 0 = 0$$
$$f(1) := 1^2 + 1 = 0$$

Esto dice que la función polinomial definida por f, es la función constante cero, es decir, $Pol(f) = 0$. Sin embargo, note que f no es el polinomio cero. Esto muestra que pueden existir distintos polinomios que induzcan la misma función polinomial.

2. Algoritmo de la división

Uno de los resultados mas importantes en $\mathbb{Z}$ es el algoritmo de la división. Para el anillo de polinomios se cumple un resultado análogo, el cual se muestra a continuación.

PROPOSICIÓN 2.1. *(Algoritmo de la división) Sean $f,g \in K[x]$ con $g \neq 0$. Entonces existen únicos $q,r \in K[x]$ tales que $f = qg + r$ con $\partial(r) < \partial(g)$.*

DEMOSTRACIÓN. Para $g \in K[x]$ no cero, veremos que para cualquier $f \in K[x]$ se cumple el resultado mencionado. Respecto a la existencia de la descomposición, primero notemos que si $\partial(f) < \partial(g)$, entonces $f = 0g + f$, así que en este caso no hay nada que probar. Por lo tanto, vamos a suponer que $\partial(f) \geq \partial(g)$, para lo cual probaremos el resultado por inducción generalizada sobre $n := \partial(f)$. Dado que el paso base es obvio, supongamos que el resultado vale para polinomios con grado menor a n. Ahora definimos $h \in K[x]$ mediante:

$$h := f - a_n b_m^{-1} x^{n-m} g,$$

donde $a_n \in K$ es el coeficiente principal de f y $b_m \in K$ es el coeficiente principal de g. Notemos que obviamente $\partial(h) < \partial(f)$, por lo que existen $q_1, r \in K[x]$ tales que:

$$h = q_1 g + r, \quad \text{con } \partial(r) < \partial(g).$$

De esto se deduce que:

$$f = (a_n b_m^{-1} x^{n-m} + q_1)g + r.$$

Esto prueba la existencia de la descomposición.

Para la unicidad, supongamos que existen $q_1, q_2, r_1, r_2 \in K[x]$ tales que:

$$f = q_1 g + r_1, \quad \text{con } \partial(r_1) < \partial(g)$$
$$f = q_2 g + r_2, \quad \text{con } \partial(r_2) < \partial(g)$$

De esto se deduce que $(q_1 - q_2)g = r_2 - r_1$. Notemos que esta igualdad implica que $\partial(r_2 - r_1) = \partial(q_1 - q_2) + \partial(g)$. Pero como por hipótesis se tiene que $\partial(r_2 - r_1) < \partial(g)$, esto sólo puede suceder si $r_2 - r_1 = q_1 - q_2 = 0$, lo que prueba la unicidad. □

A continuación trataremos algunos resultados que se derivan del anterior.

PROPOSICIÓN 2.2. *(Teorema del residuo) Para $f \in K[x]$ y $a \in K$, existe un único $q \in K[x]$, tal que $f = (x-a)q + f(a)$.*

DEMOSTRACIÓN. Al aplicar el algoritmo de la división entre f y $x - a \neq 0$, existen únicos $q, r \in K[x]$ tales que:

$$f = (x-a)q + r, \quad \text{con } \partial(r) < \partial(x-a) = 1.$$

La condición en los grados dice que $r \in K[x]$ es un polinomio constante, por lo que el valor de este se puede calcular al evaluar en cualquier elemento del campo. Así que al evaluar en $a \in K$ la igualdad anterior, se tiene que $f(a) = r(a) = r$, de donde se deduce la descomposición buscada. □

Para el siguiente resultado requerimos presentar alguna terminología previa, pues como en el caso de $\mathbb{Z}$, podemos definir una noción de divisibilidad en el conjunto de polinomios.

DEFINICIÓN 2.1. *Sean $f,g \in K[x]$. Decimos que f **divide** a g, lo que se denota por $f \mid g$, si existe $h \in K[x]$ tal que $g = fh$.*

Las propiedades básicas de la noción de divisibilidad aparecen en el ejercicio 5.3. Como en el caso de los números enteros, dichas propiedades dicen que la divisibilidad define un pre-orden en el anillo de polinomios.

COROLARIO 2.1. *Para $f \in K[x]$ y $a \in K$, son equivalentes:*

1. $f(a) = 0$
2. $(x-a) \mid f$

DEMOSTRACIÓN. Directa del teorema del residuo. □

3. Irreducibilidad

DEFINICIÓN 3.1. *Sea $f \in K[x]$ no unidad. Decimos que f es:*

1. ***irreducible** si siempre que $f = gh$ con $g,h \in K[x]$, se tiene que $g \in U(K[x])$ ó $h \in U(K[x])$.*
2. ***primo** si siempre que $f \mid gh$ con $g,h \in K[x]$, se tiene que $f \mid g$ o $f \mid h$.*

OBSERVACIÓN 3.1. *El hecho de que $K[x]$ sea un dominio entero, permite probar de la misma forma a como se hizo en el caso de los enteros que todo elemento irreducible es primo. El regreso de esta afirmación también es cierto (ver ejercicio 5.16).*

EJEMPLO 3.1. *Todo polinomio de grado 1 es irreducible.*

EJEMPLO 3.2. *El polinomio $f = x^2 - 2$ es irreducible sobre los racionales, pero no es irreducible sobre los reales.*

EJEMPLO 3.3. *Si $f \in K[x]$ tiene una raíz y $\partial(f) \geq 2$, entonces f no es irreducible.*

El siguiente resultado es un análogo al teorema fundamental de la aritmética para el caso de $\mathbb{Z}$. Únicamente presentamos la prueba de la existencia pues la unicidad en la descomposición, es el mismo argumento de la prueba que se hizo para los enteros.

PROPOSICIÓN 3.1. *Todo polinomio no constante es producto de polinomios irreducibles.*

DEMOSTRACIÓN. Consideremos $S = \{f \in K[x] \ : \ \partial(f) \geq 1 \text{ y } f \text{ no es producto de irreducibles}\}$. Lo que queremos demostrar es que $S = \emptyset$, así que procediendo por contradicción, supongamos que $S \neq \emptyset$. Consideremos el conjunto $R = \{n \in \mathbb{N} \ : \ \exists f \in S(n = \partial f)\}$, el cual es no vacío por hipótesis y un subconjunto de los números naturales, así que el principio del buen orden implica que existe $\min R$, y sea $p \in S$ tal que $\partial p = \min R$. Notemos que p no puede ser irreducible y además $\partial p \geq 1$, luego existen $f,g \in K[x]$ tales que $p = fg$ y $\partial f, \partial g \geq 1$. Dado que esto implica que $\partial p > \partial f, \partial g$, entonces $f,g \notin S$, lo que implica que f y g son productos de polinomios irreducibles, lo cual es una contradicción pues esto implicaría que p también lo es. Esto concluye la prueba de la afirmación. □

4. Máximo común divisor

DEFINICIÓN 4.1. *Sean $f,g \in K[x]$. Decimos que $p \in K[x]$ es el **máximo común divisor** de f y g, si se cumple lo siguiente:*

1. *$p \mid f$ y $p \mid g$.*
2. *Si $h \in K[x]$ satisface que $h \mid f$ y $h \mid g$, entonces $h \mid p$.*
3. *p es mónico, es decir, tiene coeficiente principal uno.*

OBSERVACIÓN 4.1. *La última condición en la definición anterior asegura la unicidad del máximo común divisor (ver ejercicio 5.2). Por tal razón denotaremos al máximo común divisor de f y g, mediante (f,g).*

La existencia del máximo común divisor se puede probar adaptando las ideas del concepto correspondiente a los enteros. En particular, con la teoría desarrollada, podemos garantizar su existencia del algoritmo de Euclides, el cual podemos obtener pues se deduce del algoritmo de la división. Para esto comencemos por considerar $f,g \in K[x]$ con $g \neq 0$. Por el algoritmo de la división existen únicos $q_1, r_1 \in K[x]$ tales que:

$$f = gq_1 + r_1, \quad \text{con } \partial(r_1) < \partial(g).$$

Si $r_1 = 0$, entonces $g \mid f$, y tomamos $(f,g) = b_n^{-1} g$, donde $b_n \in K$ es el coeficiente principal de g. En caso contrario, aplicamos el algoritmo de la división a los elementos $g, r_1 \in K[x]$, por lo que existen únicos $q_2, r_2 \in K[x]$ tales que:

$$g = r_1 q_2 + r_2, \quad \text{con } \partial(r_2) < \partial(r_1).$$

Si $r_2 = 0$, entonces $r_1 \mid g$, y tomamos $(f,g) = c_m^{-1} r_1$, donde $c_m \in K$ es el coeficiente principal de r_1. En caso contrario, aplicamos el algoritmo de la división a los elementos $r_1, r_2 \in K[x]$, por lo que existen único $q_3, r_3 \in K[x]$ tales que:

$$r_1 = r_2 q_3 + r_3, \quad \text{con } \partial(r_3) < \partial(r_2).$$

Podemos continuar con este argumento de forma sucesiva, y notemos que dado que la sucesión de polinomios que son residuos en alguna aplicación del algoritmo de la división satisfacen que:

$$\cdots < \partial(r_3) < \partial(r_2) < \partial(r_1) < \partial(g),$$

debe existir algún $k \in \mathbb{N}^+$ tal que $r_k = 0$. Luego, $(f,g) = d_l^{-1} r_{k-1}$, donde $d_l \in K$ es el coeficiente principal de r_{k-1}. La discusión anterior podemos enunciarla en el siguiente resultado, cuya prueba es análoga a la de los enteros, por lo tanto, la omitiremos:

PROPOSICIÓN 4.1. *Para $f,g \in K[x]$ con $g \neq 0$, el último residuo no cero de aplicar sucesivamente el algoritmo de la división calcula (f,g) al multiplicarlo por el inverso de su coeficiente principal.*

Vamos a mostrar un ejemplo del uso del resultado anterior.

EJEMPLO 4.1. *Calcular el máximo común divisor de* $x^2+1,\ x^5+1 \in \mathbb{Z}_3[x]$.

Solución. *Aplicaremos el algoritmo de la división. Notemos que:*

$$\begin{aligned} x^5+1 &= (x^2+1)(x^3-x)+(x+1) \\ x^2+1 &= (x+1)(x-1)+2 \\ x+1 &= 2(2x+2)+0 \end{aligned}$$

El último residuo no cero es el polinomio constante $2 \in \mathbb{Z}_3[x]$*, y dado que el coeficiente principal es* 2*, al multiplicar por su inverso multiplicativo, que es él mismo, se tiene que:*

$$(x^2+1, x^5+1) = 1.$$

Tal y como sucedió en el caso de los enteros, para $K[x]$ se tiene que el máximo común divisor se expresa como combinación de los polinomios en cuestión, resultado que también se puede deducir del algoritmo de Euclides.

PROPOSICIÓN 4.2. *Sean* $f, g \in K[x]$ *no cero. Entonces existen* $r, s \in K[x]$ *tales que:*

$$(f,g) = rf + sg.$$

Nuevamente vamos a intercambiar la prueba del resultado anterior, por un ejemplo, con el objetivo de mostrar que la teoría y los ejemplos trabajan igual que en el caso de los enteros.

EJEMPLO 4.2. *Expresar* $(x^2+1, x^5+1) \in \mathbb{Z}_3[x]$ *como combinación lineal de los polinomios* $x^2+1, x^5+1 \in \mathbb{Z}_3[x]$.

Solución: *Usaremos las igualdades obtenidas en el cálculo de* (x^2+1, x^5+1) *que aparecen en el ejemplo 4.1. Del último residuo no cero, se tiene que:*

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

Al multiplicar por el inverso multiplicativo de $2 \in \mathbb{Z}_3$*, que es el mismo elemento, se tiene que:*

$$2(x^2+1) - 2(x+1)(x-1) = 1 = (x^2+1, x^5+1) \tag{9}$$

Dado que $x^5+1 = (x^2+1)(x^3-x)+(x+1)$*, se tiene que* $x+1 = (x^5+1)-(x^2+1)(x^3-x)$*, que al sustituir en la ecuación (9) nos lleva a la igualdad:*

$$2(x^2+1) - 2((x^5+1)-(x^2+1)(x^3-x))(x-1) = (x^2+1, x^5+1)$$

Reducimos el primer miembro de esta ecuación recordando que estamos trabajando en $\mathbb{Z}_3[x]$*:*

$$(x^2+1)(2x^4-2x^3-2x^2+2x+2)+(x^5+1)(x-1) = (x^2+1, x^5+1).$$

Para concluir con esta sección, tal y como sucede en el caso de los enteros, también podemos hacer ecuaciones diofantinas lineales. Tenemos nuevamente un teorema de existencia de estas:

PROPOSICIÓN 4.3. *Sean $f,g,h \in K[x]$. Entonces la ecuación $Xf+Yg=h$ con $X,Y \in K[x]$ incógnitas polinomiales, tiene solución, si y sólo si $(f,g) \mid h$. Además, si $X_0,Y_0 \in K[x]$ son soluciones particulares de la ecuación mencionada, las soluciones de la ecuación planteada están dadas por:*

$$\begin{cases} X &= X_0 + \frac{g}{(f,g)}t \\ Y &= Y_0 - \frac{f}{(f,g)}t, \end{cases}$$

donde $t \in K[x]$ es cualquier polinomio.

La prueba del resultado anterior se obtiene de adaptar la del caso entero. En lugar de realizarla, haremos un ejemplo.

EJEMPLO 4.3. *Resolver la ecuación diofantina en $\mathbb{Z}_3[x]$:*

$$X(x^5+1)+Y(x^2+1)=x$$

Solución: *Dado que $(x^5+1,x^2+1)=1$, la ecuación anterior tiene solución. Como se vio en el ejercicio anterior, se tiene la igualdad:*

$$(x^2+1)(x^4-x^3-x)+(x^5+1)(x-1)=(x^2+1,x^5+1)=1$$

Esto implica que:

$$(x^2+1)(x^5-x^4-x^2)+(x^5+1)(x^2-x)=x$$

Luego, una solución particular está dada por:

$$\begin{cases} X_0 &= (x^2-x) \\ Y_0 &= (2x^5-2x^4-2x^3+2x^2+2x), \end{cases}$$

Por lo tanto, todas las soluciones de la ecuación dada, son:

$$\begin{cases} X &= (x^2-x)+(x^2+1)t \\ Y &= (2x^5-2x^4-2x^3+2x^2+2x)-(x^5+1)t, \end{cases}$$

con $t \in K[x]$.

5. Multiplicidad de raíces

Saber si un polinomio dado tiene una raíz o no, es complicado de saber. Por ejemplo, sobre los números reales no todo polinomio tiene una raíz, por ejemplo, el polinomio $x^2+1 \in \mathbb{R}[x]$. En el caso de los complejos, siempre es posible encontrar al menos una raíz, cosa que se conoce como el Teorema Fundamental del Álgebra, hecho que históricamente recibe este nombre por lo que se entendía por Álgebra en la matemática anterior a la moderna. Dicho sea de paso, la prueba de este resultado queda fuera de los alcances de estas notas.

PROPOSICIÓN 5.1. *Todo polinomio no constante sobre los complejos, tiene al menos una raíz compleja.*

Respecto al número de raíces, hay un resultado en cualquier campo que se debe a D'Alembert (ver ejercicio 5.14). Así que contando multiplicidades de la soluciones, un polinomio no cero sobre los complejos tiene tantas raíces como su grado. En esta sección discutiremos un proceso para determinar la **multiplicidad de una raíz**, esto es, el número de veces que dicha raíz se repite. Esto se puede ver de forma ecuacional como sigue: Si $f \in K[x]$ tiene una raíz $a \in K$ con multiplicidad $n \in \mathbb{N}^+$, entonces existe $g \in K[x]$ tal que:

$$f=(x-a)^n g$$

y además $g(a) \neq 0$.

Nuestra siguiente meta es obtener un resultado que permita saber cuando la multiplicidad de una raíz es mayor uno. Para esto, sea $f \in K[x]$ y supongamos que $f = \sum_{j=0}^{n} a_j x^j$. Definimos la derivada del polinomio f, denotada por $f' \in K[x]$, mediante:

$$f' = \sum_{j=0}^{n} j a_j x^{j-1}$$

Esta derivada cumple todas las propiedades de la noción de derivada usual. Algunas propiedades relevantes aparecen en los ejercicios 5.39 y 5.40.

El resultado es:

PROPOSICIÓN 5.2. *Sea $f \in K[x]$. Entonces,*

1. *Si f tiene una raíz múltiple, entonces f y f' no son primos relativos.*
2. *Si f y f' no son primos relativos, entonces f tiene una raíz múltiple.*

DEMOSTRACIÓN. Para la primera afirmación, si f tiene una raíz múltiple, digamos $a \in K$, entonces existe $n \in \mathbb{N}$ con $n \geq 2$, tal que $f = (x-a)^n g$. Notemos que $f' = n(x-a)^{n-1} g + (x-a)^n g$. Por lo tanto, $(x-a) \mid f$ y $(x-a) \mid f'$, lo que implica que $(x-a) \mid (f, f')$, por lo que f y f' no pueden ser primos relativos.

La segunda afirmación queda como ejercicio. □

Notemos que podemos dar una definición recursiva de derivada de un polinomio, como sigue:

DEFINICIÓN 5.1. *Sea $f \in K[x]$. Definimos la n-ésima derivada de f, la que denotaremos por $f^{(n)}$, mediante la definición recursiva:*

1. $f^{(0)} := f$
2. *Para $n \in \mathbb{N}$, $f^{(n+1)} := (f^{(n)})'$*

Para una multiplicidad específica, en el caso complejo tenemos el siguiente resultado.

PROPOSICIÓN 5.3. *Sea $f \in \mathbb{C}[x]$ y $a \in \mathbb{C}$ una raíz de f. La raíz a tiene multiplicidad $m > 0$ si y sólo si:*

1. $f(a) = \cdots = f^{(m-1)}(a) = 0$.
2. $f^{(m)}(a) \neq 0$.

DEMOSTRACIÓN. $\Rightarrow$) Usaremos inducción sobre m. Para la base, que es $m = 1$, la raíz $a \in \mathbb{C}$ de f tiene multiplicidad 1, lo que dice que $f = (x-a)g$ con $g(a) \neq 0$. Notemos que $f' = g + (x-a)g'$. Como $f'(a) = g(a) \neq 0$, esto muestra que se cumplen las dos condiciones de la conclusión.

Respecto al paso inductivo, si este vale para m, supongamos que $f = (x-a)^{m+1} g$, es decir, f tiene a $a \in \mathbb{C}$ como raíz de multiplicidad $m+1$. Al tomar la derivada,

$$f' = (m+1)(x-a)^m g + (x-a)^{m+1} g' = (x-a)^m ((m+1)g + (x-a)g)$$

Dado que $((m+1)g + (x-a)g)(a) = (m+1)g(a) \neq 0$, entonces f' tiene como raíz con multiplicidad m a $a \in \mathbb{C}$. Entonces la hipótesis de inducción implica que:

1. $f'(a) = \cdots = (f')^{(m-1)}(a) = 0$
2. $(f')^{(m)}(a) \neq 0$

Dado que $a \in \mathbb{C}$ es raíz de f, entonces las condiciones anteriores y esta observación implican el resultado.

$\Leftarrow$) Nuevamente aplicaremos inducción sobre m. El paso base, $m = 1$, es claro. Para el paso inductivo, supongamos que el resultado vale para m, y queremos demostrarlo para $m+1$. El considerar $f' \in K[x]$, este cumple que:

1. $f'(a) = \cdots = (f')^{(m)}(a) = 0$
2. $(f')^{(m+1)}(a) \neq 0$

Por lo tanto f' tiene a $a \in \mathbb{C}$ como raíz de multiplicidad m, así que existe $g \in \mathbb{C}[x]$ tal que $f' = (x-a)^m g$ con $g(a) \neq 0$. Por otro lado, como $f(a) = 0$, sabemos que podemos descomponer $f = (x-a)^n h$, con $h \in K[x]$ tal que $h(a) \neq 0$, es decir, n es la multiplicidad de a, la cual cumple que $n \geq 1$. Al derivar, tenemos que $f' = n(x-a)^{n-1}h + (x-a)^n h'$. Comparando las dos expresiones en para f', tenemos que:

$$(x-a)^m g = (x-a)^{n-1}(nh + (x-a)h')$$

De esto se deduce que $m = n-1$, es decir, $n = m+1$, lo que dice que $f = (x-a)^{m+1}h$, y así, a tiene multiplicidad $m+1$ en f.

□

EJEMPLO 5.1. *Demuestre que el polinomio $f = x^5 - ix^4 + 2x^3 - 2ix^2 + x - i \in \mathbb{C}[x]$, tiene únicamente por raíces a i y $-i$.*

Solución. *Dado que el polinomio dado tiene coeficientes complejos, este tiene 5 raíces, contando la multiplicidad. Primero notemos que obviamente $i, -i \in \mathbb{C}$ son raíces de f. Luego, nuestra meta será demostrar que estas raíces tienen multiplicidades cuya suma son 5. Para esto notemos que:*

$$\begin{aligned} f' &= 5x^4 - 4ix^3 + 6x^2 - 4ix + 1 \\ f^{(2)} &= 20x^3 - 12ix^2 + 12x - 4i \\ f^{(3)} &= 60x^2 - 24ix + 12 \end{aligned}$$

Además se tiene que $f'(i) = f^{(2)}(i) = 0$ y $f^{(3)}(i) = -24$, por lo que i tiene multiplicidad 3. Por otro lado, $f'(-i) = 0$, pero $f^{(2)}(-i) = 16i$, por lo que $-i$ tiene multiplicidad 2. Por lo tanto, los complejos dados son las únicas raíces de f.

Ejercicios del capítulo

Sean K un campo arbitrario y $f,g,h \in K[x]$.

EJERCICIO 5.1. *Calcula:*

1. $(x+1)(x-1)$.
2. $(a_0x^2+a_1x+a_2)(b_0x^3+b_1x^2+b_2x+b_3)$.
3. $[(ax^3+bx^2+cx+d)^2+(ex+f)^3](gx^2+hx+j)$.

EJERCICIO 5.2. *Sea $f \in K[x]$ no cero. Demuestre que:*

$$\partial(f) = \text{máx}\{n \in \mathbb{N} \,:\, f(n) \neq 0\}$$

EJERCICIO 5.3. *Sean $f,g,h \in K[x]$. Demuestre las siguientes afirmaciones:*

1. $f \mid f$
2. *Si $f \mid g$ y $g \mid f$ con $f \neq 0$, entonces existe $c \in K \setminus \{0\}$ tal que $f = cg$.*
3. *Si $f \mid g$ y $g \mid h$, entonces $f \mid h$.*

EJERCICIO 5.4. *Sea $f = x^3+3x^2+4x+1 \in \mathbb{Q}[x]$. Encuentra todos los $a \in \mathbb{C}$ tales que $f(a) = 0$.*

EJERCICIO 5.5. *Sea $f = x^4+x^3-2x^2+3x+1 \in \mathbb{Q}[x]$. Encuentra todos los $a \in \mathbb{C}$ tales que $f(a) = 0$.*

EJERCICIO 5.6. *Encuentra un polinomio racional f de grado dos que cumpla las condiciones: $f(0) = 1$, $f(2) = 1$ y $f(-3) = 0$. ¿Es único este polinomio?*

EJERCICIO 5.7. *Expresa el polinomio $f = x^2+2 \in \mathbb{Q}[x]$ como producto de polinomios complejos de grado 1 y demuestra que este no puede expresarse con producto de polinomios racionales de grado 1.*

EJERCICIO 5.8. *Sean $f,g \in \mathbb{R}[x]$. Usa el algoritmo de la división para expresar f en terminos de g para cada uno de los siguientes casos:*

1. $f = x^2-2x+1$ y $g = x-1$.
2. $f = x^3+x-1$ y $g = x^2+1$.
3. $f = x^3+x$ y $g = x$.
4. $f = x^3-1$ y $g = x-1$.

EJERCICIO 5.9. *Sean $f,g \in \mathbb{Z}_2[x]$ definidos mediante $f = x^5+1$ y $g = x^3+1$.*

1. *Calcula (f,g).*
2. *Expresa (f,g) como combinación lineal.*
3. *Considera la ecuación diofantina $Xf+Yg = x^2-1$, donde $X,Y \in \mathbb{Z}_2[x]$ son incógnitas. ¿Tiene esta ecuación solución? De ser la respuesta anterior afirmativa calcula todas las soluciones de dicha ecuación.*

EJERCICIO 5.10. *Demuestra que los siguientes polinomios en $\mathbb{C}[x]$ no tienen raíces múltiples en $\mathbb{C}$:*

1. x^4+1.
2. x^5-5x+1.

3. x^2+bx+c, *si* $b^2-4c\neq 0$.

EJERCICIO 5.11. *Sean* $f,g\in\mathbb{Z}_2[x]$ *definidos mediante* $f=x+1$ *y* $g=x^3+1$. *Demuestra que* $f\neq g$ *en* $\mathbb{Z}_2[x]$ *pero que* $Pol(f)=Pol(g)$.

DEFINICIÓN 5.2. *Una función* $\phi:\mathbb{N}\to\mathbb{N}$ *se llama polinomial sobre* $\mathbb{Q}$ *si existe* $f\in\mathbb{Q}[x]$ *tal que para todo* $n\in\mathbb{N}$, $\phi(n)=f(n)$.

EJERCICIO 5.12. *Demuestra que las funciones* $\phi,\psi:\mathbb{N}\to\mathbb{N}$ *cuya regla de correspondencia es* $\phi(n)=\sum_{k=1}^{n}2k-1$ *y* $\psi(n)=\sum_{k=1}^{n}k^2$ *son polinomiales.*

EJERCICIO 5.13.

1. *Demuestra que* $K[x]$ *es un dominio entero.*
2. *¿Es* $K[x]$ *un campo? Argumenta tu respuesta.*
3. *Encuentra todos los elementos idempotentes en* $K[x]$ *y demuestra tu respuesta.*

EJERCICIO 5.14. *Sea* $f\in K[x]$. *Demuestre que si* $\partial(f)=n\in\mathbb{N}$, *entonces* f *tiene a los más n raíces distintas en K.*

Sugerencia: Usar inducción sobre n.

EJERCICIO 5.15. *Supongamos que* f *tiene grado* 9 *y que* $f=f_1f_2f_3f_4$ *donde los polinomios* f_i *tienen grado positivo para* $i=1,..,4$. *Demuestra que al menos dos de los* f_i *tienen el mismo grado.*

EJERCICIO 5.16. *Sea* $f\in K[x]$. *Demuestra que* f *es irreducible en* $K[x]$ *si y sólo si primo.*

EJERCICIO 5.17. *Demuestre que la descomposición como producto de polinomios irreducibles en la proposición 3.1 es única salvo el orden de los factores.*

EJERCICIO 5.18. *Demuestra las siguientes afirmaciones:*

1. *Si* $f=x^2+bx+c\in\mathbb{R}[x]$ *entonces* f *es irreducible en* $\mathbb{R}[x]$ *si y sólo si* $b^2-4c<0$.
2. *Si* $f\in\mathbb{R}[x]$ *es mónico e irreducible con* $\partial(f)=2$. *Entonces existen* $a,b\in\mathbb{R}$ *tales que* $f=(x-a)^2+b^2$.

EJERCICIO 5.19. *Para toda* $n\in\mathbb{N}$ *se define:*

$$T_n=\frac{(x+\sqrt{x^2-1})^n+(x-\sqrt{x^2-1})^n}{2}$$

Demuestra que para toda n impar:

1. $x|T_n$.
2. *El coeficiente principal de* T_n *es* 2^{n-1}.
3. *El coeficiente lineal es* $(-1)^{\frac{n-1}{2}}n$.
4. *Si* $p\in\mathbb{N}$ *es un primo impar entonces* $T_p\equiv x^p \mod p$.

EJERCICIO 5.20. *Sean $f,g \in \mathbb{Q}[x]$ definidos mediante $f = x^3 - kx^2 - 2x + k + 3$ y $g = x - k$. ¿Para qué valores $k \in \mathbb{Q}$ se tiene que $g|f$?*

EJERCICIO 5.21. *Dí si la siguiente afirmación es verdadera ó falsa dando una demostración ó un contraejemplo según sea el caso: Si $f|gh$ entonces $f|(f,g)(f,h)$.*

EJERCICIO 5.22. *Demuestra que para todo $n,m \in \mathbb{N}^+$, $(x^n - 1, x^m - 1) = x^{(n,m)} - 1$ y expresa el máximo común divisor como combinación lineal.*

EJERCICIO 5.23. *Demuestra que los polinomios $x^4 + x^2 + r^2$ y $x^2 + x + r$ son primos relativos para toda $r \in \mathbb{R} \setminus \{0,1\}$.*

EJERCICIO 5.24. *Enuncia y demuestra el Teorema Fundamental de la Aritmética en $K[x]$.*

EJERCICIO 5.25. *Demuestra que $t^4 + 4$ se puede expresar como producto de dos polinomios de grado dos con coeficientes enteros.*

EJERCICIO 5.26. *Demuestra que todo polinomio real se puede factorizar como producto de polinomios reales con grado a lo más dos.*

EJERCICIO 5.27. *Supongamos que los complejos con algebraicamente cerrados. Sea $f \in \mathbb{R}[x]$ con $\partial(f) \geq 1$. Demuestra que si f es irreducible entonces $\partial(f) = 1$ ó $\partial(f) = 2$.*

EJERCICIO 5.28. *Sean $f,g \in K[x]$ con K campo. Si f se descompone como $f = ap_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ y g se descomponen como $g = bp_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ donde $a,b \in K[x]$ son unidades y $p_1, \ldots, p_n$ son polinomios mónicos irreducibles, entonces:*

$$(f,g) = p_1^{s_1} \cdot \ldots \cdot p_n^{s_n}$$

$$[f,g] = p_1^{t_1} \cdot \ldots \cdot p_n^{t_n}$$

donde $s_i = \min\{k_i, r_i\}$ y $t_i = \max\{k_i, r_i\}$.

EJERCICIO 5.29. *Determine el mínimo común múltiplo y el máximo común divisor de las siguientes parejas de polinomios complejos:*

1. $(x-2)^3(x-3)^4(x-i)$ y $(x-1)(x-2)(x-3)^3$.
2. $(x^2-1)(x^2+1)$ y $(x+i)^3(x^3-1)$.

EJERCICIO 5.30. *Sea $f \in K[x]$ con K un campo. Demuestre que son equivalentes:*

1. *f es mónico, $f(a) = 0$ y f es el polinomio de grado mínimo con esta propiedad*
2. *f es mónico, $f(a) = 0$ y f es irreducible.*

EJERCICIO 5.31. *Sea $f \in \mathbb{C}[x]$ tal que $f = u(x-a_1)^{k_1} \cdot \ldots \cdot (x-a_n)^{k_n}$ donde $u \in \mathbb{C}^*$, $a_1, \ldots, a_n \in \mathbb{C}$ con $a_i \neq a_j$ si $i \neq j$, y $k_1, \ldots, k_n \in \mathbb{N}^+$. Demuestra lo siguiente:*

1. *Si $m(a_i)$ denota la multiplicidad de a_i en f entonces para todo $i \in \{1, .., n\}$, $m(a_i) = k_i$.*

2. $\partial(f) = \sum_{i=1}^{n} m(a_i)$.

EJERCICIO 5.32. *Sea $f \in \mathbb{C}[x]$ con la forma $f = \sum_{k=0}^{n} a_k z^k$, con $a_n \neq 0$. Demuestre lo siguiente:*

1. *La suma de las raíces de f es $-\frac{a_{n-1}}{a_n}$*
2. *El producto de las raíces de f es $(-1)^n \frac{a_0}{a_n}$*

EJERCICIO 5.33. *Para $p \in \mathbb{N}$ primo, sea $f \in \mathbb{Z}_p[x]$. Demuestre que $f' = 0$ si y sólo si para todo $k \in \mathbb{N}$ tal que $p \nmid k$, $a_k = 0$ en $\mathbb{Z}$.*

EJERCICIO 5.34. *Si f y g son polinomios enteros mónicos, demuestra que al expresar $f = gq + r$ con $\partial(r) < \partial(g)$, entonces q y r tienen coeficientes enteros.*

EJERCICIO 5.35. *Si $f \in \mathbb{C}[x]$ y este tiene la forma $f = \sum_{k=0}^{n} a_k x^k$, se define una función $\_^* : \mathbb{C}[x] \to \mathbb{C}[x]$ mediante $f^* = \sum_{k=0}^{n} a_k x^k$. Demuestra lo siguiente:*

1. *Si $g := ff^*$ entonces $g \in \mathbb{R}[x]$.*
2. *Si $a \in \mathbb{C}$ es raíz de g entonces a es raíz de f o $\overline{a}$ es raíz de f.*

EJERCICIO 5.36.

1. *Demuestra que para toda $n \in \mathbb{N}$, $x - 1 | x^n - 1$.*
2. *Si $n \in \mathbb{N}$ es impar, encuentra $g \in \mathbb{R}[x]$ tal que $(x+1)g = x^n + 1$.*
3. *¿Qué sucede con la afirmación anterior si n es un número par no cero?*
4. *¿Qué sucede con la afirmación 2 si $x+1, x^n+1, g \in \mathbb{Z}_p[x]$ con $p \in \mathbb{N}$ primo?*

EJERCICIO 5.37. *Sea $f \in K[x]$ tal que $x - a | f$. Demuestra que $(x-a)^2 | f$ si y sólo si $f'(a) = 0$.*

EJERCICIO 5.38. *Sea $a \in K^*$. Demuestra que:*

1. *Si $f' = af$ entonces $f = 0$.*
2. *Si $f'' + af = 0$ entonces $f = 0$.*

EJERCICIO 5.39. *Demuestra que $(fg)' = f'g + fg'$.*

EJERCICIO 5.40. *Sea $f \in K[x]$ y $m \in \mathbb{N}^+$. Definamos $g \in K[x]$ mediante $g := f^m$, esto es, f elevado a la m. Demuestre que:*

$$g' = mf^{m-1}f'.$$

EJERCICIO 5.41. *Sean $\{a_0, ..., a_n\}, \{b_0, ..., b_n\} \subseteq \mathbb{C}$. Demuestra que existe $f \in \mathbb{C}[x]$ tal que $f(a_k) = b_k$, para todo $k = 0, ..., n$.*

DEFINICIÓN 5.3. *Si $f \in K[x]$ se define $V(f) = \{a \in K | f(a) = 0\}$.*

EJERCICIO 5.42. *Suponiendo que K es algebraicamente cerrado, demuestra las siguientes propiedades:*

1. *$V(0) = K$.*
2. *$V(f) = \emptyset$ si y sólo si $\partial(f) = 0$.*

3. $V(fg) = V(f) \cup V(g)$.
4. *Si* $\partial(f) \in \mathbb{N}$ *entonces* $|V(f)| \leq \partial(f)$.

DEFINICIÓN 5.4. *Para* $c \in \mathbb{R}^+$, *se define una función* $\| \ \|_c : \mathbb{C}[x] \to \mathbb{R}^+ \cup \{0\}$ *mediante la regla de correspondencia:*

$$\|f\|_c = \max_{k \in \mathbb{N}} \{|f(k)|c^k\}$$

EJERCICIO 5.43. *Demuestra las siguientes propiedades:*

1. *La función* $\| \ \|_c$ *está bien definida, es decir, para todo* $f \in \mathbb{R}[x]$ *se tiene que* $\|f\|_c \in \mathbb{R}^+ \cup \{0\}$.
2. $\|f\|_c = 0$ *si y sólo si* $f = 0$.
3. *Para todo* $f, g \in \mathbb{C}[x]$, $\|f+g\|_c \leq \|f\|_c + \|g\|_c$.
4. *Para todo* $f, g \in \mathbb{C}[x]$, $\|fg\|_c = \|f\|_c \|g\|_c$.

EJERCICIO 5.44. *Sea* $p \in \mathbb{N}$ *un primo. Demuestra que para todo* $a \in \mathbb{Z}_p$ *se tiene que* $|V(x^p - a)| = 1$. *¿Qué sucede en* $\mathbb{Z}_n$ *para* $n \in \mathbb{N}^+$*?*

DEFINICIÓN 5.5. *Sea* $Q \in \mathbb{R}^+ \setminus \{1\}$. *Si* $x \in \mathbb{R}$ *se define el Q-número x, denotado por* $[x]_Q$, *de la siguiente forma:*

$$[x]_Q = \frac{Q^x - 1}{Q - 1}$$

Así, se define también para $n \in \mathbb{N}$ *el Q-factorial de manera recursiva como:*

1. $[0]_Q! = 1$.
2. *Para todo* $n \in \mathbb{N}$, $[n+1]_Q! = [n+1]_Q \cdot [n]_Q!$

Y por lo tanto para todo $n, k \in \mathbb{N}$, *tales que* $0 \leq k \leq n$, *las Q-combinaciones de n en k, mediante la relación.*

$$\binom{n}{k}_Q = \frac{[n]_Q!}{[k]_Q! \cdot [n-k]_Q!}$$

DEFINICIÓN 5.6. *Si* $f \in \mathbb{R}[x]$ *se define la Q-derivada respecto a x, la que denotamos por* $D_x^Q(f)$, *mediante:*

$$D_x^Q(f) = \frac{f(Qx) - f(x)}{(Q-1)x}$$

EJERCICIO 5.45. *Demuestra las siguientes afirmaciones:*

1. *La función* D_x^Q *está bien definida, es decir,* $im(D_x^Q) \subseteq \mathbb{R}[x]$.
2. *Para todo* $n \in \mathbb{N}^+$, $D_x^Q(x^n) = [n]_Q \, x^{n-1}$.
3. *Para todo* $f, g \in \mathbb{R}[x]$ *se cumplen:*

$$D_x^Q(fg) = D_x^Q(f)g(Qx) + fD_x^Q(g)$$
$$D_x^Q(fg) = D_x^Q(f)g + f(Qx)D_x^Q(g)$$

EJERCICIO 5.46. *Demuestra las siguientes afirmaciones:*

1. $\lim_{Q\to 1} D_x^Q(f) = f'$.
2. *Para todo* $n \in \mathbb{N}$

$$(D_x^Q)^n(f) = (Q-1)^n Q^{-\frac{n(n-1)}{2}} x^{-n} \sum_{k=0}^{n} \binom{n}{k}_Q (-1)^k Q^{\frac{k(k-1)}{2}} f(Q^{n-k}x)$$

"Algebra is generous; she often gives more than is asked of her"

D'Alembert

Anexos

6. Naturales

Los naturales $\mathbb{N}$ son un conjunto que cumple con los axiomas de Peano

DEFINICIÓN 6.1 (Axiomas de Peano). *Un sistema de Peano, es una pareja (N,s,e) donde N es un conjunto, $e \in N$ es un elemento de N, y $s\colon N \to N$ una función que cumple:*

- *Para todo $n \in N$, $s(n) \neq e$.*
- *Para todo $n \in N$ con $n \neq e$, existe $m \in N$ tal que $s(m) = n$.*
- *Para todo $m,n \in N$, si $s(m) = s(n)$ entonces $m = n$.*
- *Axioma de Inducción) Si $A \subseteq N$, $e \in A$ y si $n \in A$ entonces $s(n) \in A$, entonces $A = N$.*

En general, usamos la notación $((N),0,s)$ donde la función s esta dada por $s(n) = n+1$. Con una noción adecuada se puede demostrar que sólo existe un sistema de Peano. Quedemonos en mente que no hay riesgo en decir que los naturales son únicos. Por último la existencia de estos es un axioma de nuestro sistema matemático.

Una forma alternativa y la más común de presentar a los axiomas de Peano es:

- Cero es un natural.
- Si n es un natural, el sucesor de n es un natural
- Cero no es sucesor de algún natural
- Si dos naturales tienen el mismo sucesor entonces son iguales.
- Si un subconjunto de los naturales tiene al cero y cada vez que un elemento pertenece a el su sucesor también, entonces ese subconjunto son los naturales.

7. Ordenes Parciales

DEFINICIÓN 7.1. *Sea P un conjunto y R una relación sobre P. Decimos que P con R es un conjunto parcialmente ordenado, si se cumple*

1. *Reflexividad) Para toda $x \in P$, xRx*
2. *Antisimetría)Para todo $x, y \in P$, si xRy e yRx, entonces $x = y$*
3. *Transitividad) Para todo $x, y, z \in P$, si xRy e $y \leq z$, entonces xRz*

La relación es lo que llamamos el orden.

Esencialmente lo que estamos planteando es que la relación R se podría entender o modelaría el menor o igual $\leq$.

EJEMPLO 7.1. *Sea X un conjunto. Entonces el conjunto potencia $\mathscr{P}(X)$ es un conjunto parcialmente ordenado con la contención $\subseteq$.*

EJEMPLO 7.2. *Los naturales $\mathbb{N}$ con su orden $\leq$ son un conjunto parcialmente ordenado.*

Ahora bien, si pensamos en $\leq$ una pregunta natural sería, ¿Por qué no $<$?.

La respuesta es rápida es sencilla, por que ambos nos dan el mismo resultado. Uno es menor y otro es menor o igual.

Empecemos modelando el menor (o menor estricto)

DEFINICIÓN 7.2. *Sea P un conjunto y R una relación sobre P. Decimos que P con R es un conjunto parcialmente ordenado, si se cumple*

1. *Irreflexividad) Para toda $x \in P$, $\neq xRx$*
2. *Transitividad) Para todo $x, y, z \in P$, si xRy e $y \leq z$, entonces xRz*

A este llamemoslo un orden estricto.

DEFINICIÓN 7.3. *Sea X un conjunto con un orden estricto R. Definamos una nueva relación R^* en X. Para $x, y \in X$, xR^*y si xRy o $x = y$. Dicho en lenguaje de coonjuntos $R^* = R \cup \Delta_X$.*

8. Relaciones de Equivalencia y Particiones

Una relación R sobre un conjunto X es un subconjunto de R del conjunto $X \times X$. Obsevamos que notacionalmente escribimos xRy en vez de $(x,y) \in R$. Consideremos los dos grandes ejemplos de relaciones $=$ y $\leq$, en ambos caso se nos hace extraño ver $= \subseteq X \times X$ o $\leq \subseteq X \times X$.

Dentro de las relaciones que más se estudian son los ordenes y la relaciones de equivalencia.

DEFINICIÓN 8.1. *Sea X un conjunto y R una relación sobre X ($R \subseteq X \times X$). Decimos que:*

- *R es reflexiva, si para todo $x \in X$ tenemos que xRx.*
- *R es simétrica, si xRy implica que yRx.*
- *R es transitiva, si xRy y yRz, entonces xRz.*

El ejemplo por excelencia de relación de equivalencia es la igualdad. Pero no es el caso así de los ordenes, que tienen la propiedad de la antisimétria. Notemos que un conjunto paracialmente ordenado que el orden una relación de equivalencia no es más que la igualdad.

Ahora bien, una relación de equivalencia $\sim$ induce una relación de igualdad, por lo que de alguna manera podemos pensar las relaciones de equivalencia como igualdades o preigualdades.

DEFINICIÓN 8.2. *Sea X un conjunto y $\sim$ una relación de equivalencia sobre X. Definimos $[x]_\sim = \{y \in X \mid y \sim x\}$. Si la relación de equivalencia se sobre entiende simplemente escribiremos $[x]$. Por otor lado también es importante notar que $[x] \subseteq X$. Al conjunto $[x]$ lo llamaremos la clase de equivalencia de x*

PROPOSICIÓN 8.1. *un conjunto y $\sim$ una relación de equivalencia sobre X. Para $x, y \in X$ son equivalentes:*

1. $[x] = [y]$.
2. $x \sim y$.

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Notemos que $x \in [x]$ puesto que la relación es reflexiva, y así tenemos que $x \sim x$. Por hipotesis $x \in [x] = [y]$. Así $x \in [y]$. De donde de $x \sim y$.

2) $\Rightarrow$ 1) Sea $z \in [x]$, entonces $x \sim z$. Por lo que usando la hipotesis $x \sim y$, concluimos que $y \sim z$. Así $z \in [y]$. La otra contención es análoga. □

La proposición anteiror nos dice que efectivamente las relaciones de equivalencia se comportan como igualdades con ciertos elementos. Solo falta tener un conjunto donde se defina y es lo que procederemos a hacer.

DEFINICIÓN 8.3. *Sea X un conjunto y $\sim$ una relación de equivalencia sobre X. Definimos $X/\sim$ como la familia de clases de equivalencia de X, es decir, $\{[x] \mid x \in X\}$.*

Notamos que la relación de equivalencia $\sim$ induce una igualdad en $X/\sim$.

PROPOSICIÓN 8.2. *Sea X un conjunto y $\sim$ una relación de equivalencia sobre X. Entonces:*

1. $\emptyset \notin X/\sim$
2. $[x] \cap [y] = \emptyset$ *si* $[x] \neq [y]$
3. $\bigcup_{x \in X} [x] = X$

DEMOSTRACIÓN.

1. Se sigue de que $x \in [x]$ para toda $x \in X$
2. Si $[x] \cap [y] \neq \emptyset$ entonces existe $z \in [x] \cap [y]$. Sea $w \in [x]$, entonces $w \sim x$ y $x \sim z$. Por lo que $w \sim z$ y $z \sim y$. Así $w \sim z$. Por lo que $[x] \subseteq [y]$. De forma analoga $[y] \subseteq [x]$. Por lo que $[x] = [y]$.
3. Como $x \in [x]$, tenemos que $X \subseteq \bigcup_{x \in X} [x]$.

□

DEFINICIÓN 8.4. *Sea X un conjunto, y $\mathfrak{A}$ una familia de subconjuntos de X. Diremos que $\mathfrak{A}$ es una partición de X si:*

1. $\emptyset \notin \mathfrak{A}$
2. $A \cap B = \emptyset$ *si* $A \neq B$ *para* $A, B \in \mathfrak{A}$
3. $\bigcup_{A \in \mathfrak{A}} A = X$

Como vimos en la proposición pasada, las relaciones de equivalencia inducen particiones.

Bibliografía

[1] Albert Cuoco and Joseph Rotman. *Learning modern algebra*, volume 23. MAA, 2013.

[2] Humberto Cárdenas, Lluis Emilio, Raggi Franciso, and Tomás Franciso. *Álgebra Superior*. Editorial trillas, 1995.

[3] Joseph J Rotman. A first course in abstract algebra: with applications. *(No Title)*, 2006.

[4] Murray R Spiegel et al. Algebra superior. 1986.