Álgebra superior II

Grupo 4083

2021-1

Universidad Nacional Autónoma de México

UNAM

Facultad de Ciencias

Índice

Operaciones binarias

Operaciones binarias

Definición: *Sea A un conjunto no vacío. Una* ***operación binaria*** *en A es una función $f : A \times A \to A$*

Observemos que:

1. El dominio de f es AxA y, al ser función debe estar bien definida, es decir, la operación asigna un elemento de A **a todo par de elementos de A**
2. Por ser función, f asigna solamente **un elemento** a cada pareja.

Decimos entonces que una operación binaria es **una regla** que asocia a cada par ordenado de elementos de A, un único elemento de A.

Las operaciones binarias son muy usadas y estudiadas en matemáticas.

Existe la convención de no denotarlas como funciones, es decir, en lugar de referirnos a la imagen de la pareja (a,b) como f(a,b), le llamamos

$$a * b$$

Aquí usamos $*$ pero puede usarse otro símbolo como: +,-,/,÷,=,|,◦, etc.

En conjuntos numéricos lo más común es usar $+$ para indicar suma y $*$ para el producto, pero aunque se usen estos símbolos, no siempre representan a la suma y el producto como los conocemos.

Otra convención, es llamarles simplemente “operaciones” esto es porque las operaciones binarias son las más comunes, aunque también existen las operaciones “unarias” -de un solo argumento-, terciarias -de tres argumentos- o, en general, n-arias -de n argumentos-. En este curso solamente estudiamos operaciones binarias por lo que generalmente les llamaremos, **operaciones.**

Recalquemos:

$$a*b \in A, \quad \forall a,b \in A$$

Esta propiedad se llama CERRADURA de la operación $*$ también se dice que la operación $*$ es **cerrada.** Observa que, al haber definido la operación como función, la cerradura se cumple por definición, así si no es cerrada, no es operación binaria.

Definición: *Sean A un conjunto no vacío, $*$ una operación en A, y $\emptyset \neq B \subseteq A$, diremos que B es* ***cerrado bajo*** $*$ *si:*

$$\forall x, y \in B \Rightarrow x * y \in B$$

Llamamos ***la restricción de*** $*$ ***sobre*** B *a la operación inducida por* $*$ *en* B

¡Cuidado!

- Observa la diferencia entre decir que $*$ es cerrada y que B es cerrado bajo $*$
- Si B no es cerrado bajo $*$ entonces su restricción sobre B no es una operación binaria en B (¿por qué?)

Veamos algunos ejemplos:

1. la suma y el producto usuales en $\mathbb{N}$, en $\mathbb{Z}$, en $\mathbb{Q}$ y en $\mathbb{R}$ son operaciones

2. la división, $\div$, en $\mathbb{R}$ no es operación pues por ejemplo $12 \div 0$, no está definido

3. la resta, $-$, en $\mathbb{N}$ no es operación pues por ejemplo $2 - 5 \notin \mathbb{N}$

4. en $\mathbb{Z}$ definamos $a * b$ como un número menor que a y b ¿esta es una operación binaria? ¿por qué?

5. en $\mathbb{Z}$ definamos $a * b = máx\{a, b\}$ ¿esta es una operación binaria? ¿por qué?

6. sea A un conjunto no vacío y definamos en $\mathcal{P}(A)$ las operaciones:

   a) $V *_{\cup} W = V \cup W$

   b) $V *_{\cap} W = V \cap W$

   ¿son operaciones binarias? ¿por qué?

Definición: *Sea A un conjunto no vacío y $*$ una operación en él. Diremos que:*

1. $*$ *es asociativa si* $\forall\ a, b, c \in A \Rightarrow (a * b) * c = a * (b * c)$
2. $*$ *es conmutativa si* $\forall\ a, b \in A \Rightarrow a * b = b * a$
3. $x \in A$ *es un* ***neutro*** *de la operación si* $\forall\ a \in A \Rightarrow x * a = a * x = a$

En los ejemplos de operaciones que hemos visto, ¿cuáles son asociativas? ¿cuáles conmutativas? ¿alguna tiene neutro?

Sobre conjuntos finitos con pocos elementos, es fácil definir operaciones binarias mediante el uso de una tabla. Así por ejemplo, si A={a}, definimos a∗a=a y la describimos con la siguiente tabla:

$*$	a
a	a

Ahora, sea $C = \{a, b, c\}$, definimos la operación $*$ con la siguiente tabla:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	a

Con esta tabla estamos indicando el resultado de la operación tomando como primer argumento la fila de la tabla, y como segundo argumento la columna, por ejemplo, $a * a = a$, $b * c = a$, $c * b = b$.

Tareita.

- Revisa si las operaciones de las tablas son asociativas, conmutativas o tienen neutro.
- Si B={a,b}, define todas las posibles operaciones binarias en B y haz las tablas correspondientes.

Ejercicios

1. Sean A un conjunto, B un subconjunto de A y $*$ una operación en A. ¿Qué es la **operación inducida** por B? ¿Bajo qué condiciones tiene sentido hablar de esta operación?

2. ¿La asignación $f(a,b) = \frac{a}{b}$ define una operación en $\mathbb{Q}$?

3. Determina si la operación definida en la última tabla es asociativa y/o conmutativa y si existe algún neutro de la operación. Argumenta.

4. Sea A un conjunto no vacío, y sea $f : A \times A \to A$ definida como $f(a,b) = a$. Determina si f es asociativa, conmutativa y si existe algún neutro para f. (Ojo, ¿qué pasa si A tiene sólo un elemento?, considera dos casos)

Tareita.

Ahora, sea $A = \{a, b, c\}$, definimos la operación $*$ con la siguiente tabla:

$*$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	a

Determinar si $*$ es conmutativa y si es asociativa.

Estructuras algebraicas

Definición: *Si A es un conjunto y $*$ es una operación binaria sobre A, llamaremos* ***estructura algebraica binaria (o magma)*** *al par* $\langle A, * \rangle$.

Nota: Un conjunto no determina una estructura algebraica por sí solo, pues con cada operación distinta que se pueda definir sobre él, se tendrá una estructura distinta.

Definición: *Si A es un conjunto y $*$ es una operación binaria sobre A, diremos que $\langle A, * \rangle$ es un* ***semigrupo*** *si $*$ es una operación asociativa.*

tareita:

Ejercicio: Para los siguientes pares $\langle A, * \rangle$, determina cuáles son semigrupos.

1. Sean $A = \mathbb{N}$, y $* : A \times A \to A$ definida como $n * m = 2n + m \quad \forall n, m \in \mathbb{N}$
2. Sean X un conjunto, $A = P(X)$ y $*$ definida como $B * C = B \cap C \quad \forall\, B, C \in P(X)$.
3. Sean X un conjunto y $A = \{f \subseteq X \times X \mid f \text{ es una función}\}$ y sea $*$ definida como la composición entre funciones $(f * g = f \circ g)$.

Definición: *Si A es un conjunto y $*$ es una operación binaria sobre A, diremos que $\langle A, * \rangle$ es un* ***monoide*** *si:*

- $*$ *es una operación asociativa*
- $\exists\, \boldsymbol{e} \in A$ *tal que* $\boldsymbol{e} * a = a * \boldsymbol{e} = a \quad \forall a \in A$, $\boldsymbol{e}$ *se llama* ***neutro de*** $*$ ***en*** A

Un monoide es un semigrupo con elemento neutro.

Tareita: determina cuáles son monoides

1. Sean $A = \mathbb{N} \setminus \{0\}$, y $* : A \times A \to A$ definida como $n * m = n \cdot m \quad \forall n, m \in \mathbb{N}$ (el producto usual en $\mathbb{N}$)
2. Sean X un conjunto, $A = P(X)$ y $*$ definida como $B * C = B \cup C \quad \forall B, C \in P(X)$.
3. Sea $A = \mathbb{R}$ y sea $*$ definida como $a * b = 0 \quad \forall a, b \in \mathbb{R}$.
4. Define un magma que no sea semigrupo y un semigrupo que no sea monoide.

Definición: *Si A es un conjunto y $*$ es una operación binaria sobre A, diremos que $\langle A, * \rangle$ es un* ***grupo*** *si:*

- $*$ es una operación asociativa
- $\exists\, \mathbf{e} \in A$ tal que $\mathbf{e} * a = a * \mathbf{e} = a \quad \forall a \in A$, $\mathbf{e}$ se llama **neutro de $*$ en A**
- $\forall x \in A$, $\exists\, y \in A$ tal que $x * y = y * x = \mathbf{e}$

Además, diremos que el grupo es ***abeliano*** *si la operación $*$ es conmutativa.*

Si sucede que $x * y = \mathbf{e}$ decimos que y es un **inverso derecho** de x, y que x es un **inverso izquierdo** de y. Cuando $x * y = y * x = \mathbf{e}$, decimos que y es un **inverso de** x (y, evidentemente, x es un inverso de y.) Observa que un grupo es un monoide en donde cada elemento tiene un inverso.

Ejemplos:

1. Si A es un conjunto cualquiera, el conjunto de todas las funciones biyectivas de A en A forma un grupo con la composición de funciones. La función identidad en A sería un elemento neutro (y es una función biyectiva), y para cada función biyectiva f, f^{-1} sería el inverso de f en el grupo. ¿Es un grupo abeliano?

2. El conjunto de los números enteros forma un grupo abeliano con la suma: la suma en $\mathbb{Z}$ es asociativa y conmutativa. El cero sería un neutro y para cada número entero a, $-a$ es su inverso respecto a la suma, pues $a + (-a) = 0$.

3. Sea $A = \{0, 1\}$, y definimos $\bigoplus$ como $1 \bigoplus 1 = 0,\ 0 \bigoplus 0 = 0,\ 1 \bigoplus 0 = 0 \bigoplus 1 = 1$
   Entonces $\langle A, \bigoplus \rangle$ es un grupo abeliano. El 0 es el neutro del grupo y 1 es su propio inverso, la operación es claramente conmutativa.

Teorema 1. *Sea $\langle G, * \rangle$ un grupo. Entonces, existe un único elemento neutro del grupo.*

Demostración: Por definición, sabemos que existe al menos un elemento neutro $x_0 \in G$. Supongamos que $y_0 \in G$ es otro neutro del grupo, y nuestro objetivo será demostrar que $x_0 = y_0$. Como x_0 es un neutro de $*$ en G y $y_0 \in G$, tenemos que

$$x_0 * y_0 = y_0 * x_0 = y_0 \text{ en particular } y_0 = x_0 * y_0 \quad (1)$$

De forma análoga, y_0 también es neutro en G y x_0 es un elemento de G, entonces:

$$x_0 = x_0 * y_0 \quad (2)$$

Por lo tanto, de (1) y (2) tenemos que:

$$x_0 = x_0 * y_0 = y_0 \qquad \therefore x_0 = y_0 \quad \blacktriangle$$

Tareita: demostrar el siguiente teorema.

Teorema 2. *El inverso de cada elemento de un grupo es único.*

Definición: *Sea $\langle G, * \rangle$ un grupo. Diremos que $H \subseteq G$ es un* ***subgrupo*** *si $\langle H, *|_H \rangle$ es un grupo. Denotamos como $H \leq G$ la proposición "H es un subgrupo de G".*

Un **subgrupo** de un grupo G es un subconjunto H de G de forma que H es **cerrado** bajo $*$ y $\langle H, * \rangle$ es un grupo con la misma operación $*$ restringida a H.

Notemos que en caso de que H no fuera cerrado bajo $*$, la restricción $*|_H$ no sería una función de $H \times H$ en H, pues habría un par de elementos $a, b \in H$ tales que $a * b \notin H$, por lo que $*|_H$ no sería una operación binaria en H, y entonces $\langle H, *|_H \rangle$ no podría ser grupo. Entonces, decir que H es cerrado bajo $*$ es equivalente a decir que $*|_H$ es una operación binaria en H.

En todas las estructuras algebraicas podemos definir lo que es una ***subestructura*** de la misma forma. Por ejemplo, un *submonoide* de un monoide M, sería un subconjunto de M que sea cerrado bajo la operación del monoide, y que a su vez cumpla la definición de monoide con la misma operación.
El trabajo con subestructuras es muy común en el estudio de las estructuras algebraicas (y en las matemáticas en general), y analizando su comportamiento y características se obtiene mucha información sobre la estructura algebraica.

Ejemplos:

1. Sabemos que $\langle \mathbb{N}, \cdot \rangle$ es un monoide, entonces $A = \{2^k | k \in \mathbb{N}\}$ sería un submonoide de $\mathbb{N}$.

   Demostración: 1 es el único elemento neutro del producto en $\mathbb{N}$, por lo que cualquier submonoide de $\mathbb{N}$ debe tener al 1 como elemento, en este caso, $1 = 2^0$ por lo que $1 \in A$. Por otro lado, sean $a = 2^k$ y $b = 2^l$ dos elementos arbitrarios de A, entonces:

   $$a \cdot b = (2^k)(2^l) = 2^{k+l} \quad \text{en donde } k + l \in \mathbb{N}$$

   por lo tanto, para cualquier par de elementos a, b de A, tenemos que $a \cdot b \in A$, y por lo tanto, A es cerrado bajo el producto usual. Esto demuestra que A es un submonoide de $\mathbb{N}$. ▲

2. Sabemos que $\langle \mathbb{Z}, + \rangle$ es un grupo abeliano. Entonces $A = \{3k \mid k \in \mathbb{Z}\}$ es un subgrupo (abeliano) de $\langle \mathbb{Z}, + \rangle$.

3. Sea G el grupo de todas las funciones biyectivas $\mathbb{R}$ en $\mathbb{R}$ usando la composición de funciones como operación. Entonces el conjunto $A = \{f \in G | f(0) = 0\}$ es un subgrupo de G.

Demostración: La función identidad, I, es el elemento neutro de G, por lo que debemos comprobar que la identidad es elemento de A. Claramente $I(0) = 0$, por lo que $I \in A$.

Ahora, sean $f, g \in A$, entonces:

$$(f \circ g)(0) = f(g(0)) = f(0) = 0 \ \therefore f \circ g \in A$$

así, A es cerrado bajo la composición de funciones.

Por último, debemos verificar que para cada elemento de A, su inverso respecto a $\circ$ es también elemento de A. Sea $f \in A$, entonces f es una función biyectiva de $\mathbb{R}$ en $\mathbb{R}$ que deja fijo al cero, pero esto quiere decir que f^{-1} también deja fijo al cero pues:

$$0 = I(0) = (f^{-1} \circ f)(0) = f^{-1}(f(0)) = f^{-1}(0)$$

Por lo tanto, $\langle A, \circ \rangle$ es un grupo, es decir, que A es un subgrupo de G ▲

Ejercicios

1. Sea X un conjunto. Sea $G = \mathcal{P}(X)$, el conjutnos potencia de X. Sea $* : G \times G \to G$ definida como:

$$A * B = A \cap B \quad \forall A, B \in P(X)$$

¿Qué tipo de estructura forma el par $\langle G, * \rangle$? Describe todas las propiedades que encuentres.

2. Sea $\langle G, * \rangle$ un grupo abeliano y sea $x \in G$. Demuestra que el inverso de x respecto a $*$ es único. ¿Existen grupos en donde los inversos no sean únicos?

3. Sea $G = \{a, b\}$. ¿Cuántos grupos distintos se pueden definir en G?

4. Sea $G = \{a, b, c\}$. Define un par de operaciones $*_1$ y $*_2$ de forma que $\langle G, *_1 \rangle$ sea un grupo abeliano pero $\langle G, *_2 \rangle$ sea un grupo no abeliano, y que a sea el neutro en ambos grupos.

De aquí en adelante, denotaremos simplemente ab en lugar de $a * b$ para referirnos a una operación binaria genérica, es decir, la trataremos como si fuera un producto sin que esto suponga que nos referimos al producto usual de los grupos numéricos conocidos. Esta regla se omitirá en algunos casos específicos en los que se describirá explícitamente de qué operación hablamos.

El siguiente resultado demuestra las *reglas de cancelación* de la operación de un grupo.

Teorema 3. *Sean G un grupo, $a, b, c \in G$ entonces,*

1. $ab = ac \Rightarrow b = c$
2. $ba = ca \Rightarrow b = c$

Demostración.

1. Sabemos que en un grupo, todo elemento tiene inverso, en particular a, entonces:

$$\begin{aligned} & ab = ac \\ \Rightarrow\ & a^{-1}(ab) = a^{-1}(ac) \\ \Rightarrow\ & (a^{-1}a)b = (a^{-1}a)c \\ \Rightarrow\ & \mathbf{e}b = \mathbf{e}c \\ \Rightarrow\ & b = c \qquad \therefore ab = ac \Rightarrow b = c \end{aligned}$$

2. La demostración es análoga. ▲

Teorema 4. *Sean G un grupo, $a, b \in G$ entonces,*

1. *la ecuación $ax = b$ tiene solución única en G*
2. *la ecuación $ya = b$ tiene solución única en G*

Demostración.

1. Sea $x = a^{-1}b$, claramente $x \in G$. Entonces,

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

Por lo tanto, $x = a^{-1}b$ es una solución de la ecuación $ax = b$

2. La demostración es análoga. ▲

Teorema 5. *Sean G un grupo, $a, b \in G$ entonces,*

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

Demostración.

1. Sabemos que:

$$aa^{-1} = a^{-1}a = \mathbf{e}$$

Es decir, a cumple con ser un inverso de a^{-1}, y por el ***Teorema 2***, a es el único inverso de a^{-1}. Por lo tanto, $(a^{-1})^{-1} = a$.

2. Observemos que:

$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(\mathbf{e})a^{-1} = aa^{-1} = \mathbf{e}$$

y por otro lado,

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = \mathbf{e}$$

Entonces, $b^{-1}a^{-1}$ es un inverso de ab, y por el ***Teorema 2***, es el único inverso de ab. Por lo tanto,

$$(ab)^{-1} = b^{-1}a^{-1} \quad \blacktriangle$$

Inducción Matemática

Principio de Inducción Completa.

Sea $A \subseteq \mathbb{N}$ *tal que*

1. $0 \in A$
2. $n \in A \Rightarrow n+1 \in A$

entonces $A = \mathbb{N}$.

Este principio es el quinto de los axiomas de Peano, que definen al conjunto de los números naturales.

Principio del Buen Orden.

Sea $A \subseteq \mathbb{N}$, $A \neq \emptyset$, entonces A tiene mínimo.

Principio de Inducción Modificado.

Sea $A \subseteq \mathbb{N}$ tal que

1. $0 \in A$
2. $k \in A \forall k \in \{0, 1, 2, ..., n\} \Rightarrow n + 1 \in A$

entonces $A = \mathbb{N}$.

Teorema.

Los tres principios son equivalentes.

1. **PIM $\Rightarrow$ PBO**

Demostración. Sabemos que se cumple PIM y debemos demostrar que se cumple PBO, es decir que cualquier subconjunto no vacío de $\mathbb{N}$ tiene mínimo. Procederemos por contradicción, suponiendo que existe un subconjunto que no tiene mínimo.

Sea $A \subseteq \mathbb{N}$, $A \neq \emptyset$, que no tiene mínimo. Sea $B = \mathbb{N} \setminus A$ notemos que $0 \in B$ pues de otro modo 0 sería el mínimo de A.

Supongamos que $\{0, 1, 2, .., n\} \subseteq B$ entonces $n+1 \notin A$ pues sería su mínimo. Por lo tanto $n+1 \in B$ y como se cumple PIM concluimos que $B = \mathbb{N}$!!!

Esto contradice que $A \neq \emptyset$ por lo que la suposición inicial es falsa, no existe tal subconjunto y por tanto se cumple PBO.

2. **PBO $\Rightarrow$ PIC**

Demostración. Ahora suponemos que se cumple PBO y debemos demostrar que se cumple PIC.

Consideremos $A \subseteq \mathbb{N}$ tal que $0 \in A$ y si $n \in A \Rightarrow n+1 \in A$. Debemos demostrar que $A = \mathbb{N}$.

Sea $B = \mathbb{N} \setminus A$, si $B = \emptyset$, entonces $A = \mathbb{N}$ y acabamos. Supongamos entonces que $B \neq \emptyset$ y así $A \neq \mathbb{N}$. Como se cumple PBO, B tiene mínimo. Sea b tal mínimo, sabemos que $b > 0$ porque $0 \in A$ entonces $b-1 \in \mathbb{N}$ y $b-1 \notin B$ pues es menor que b.

Entonces como A y B son complementarios, $b-1 \in A$ y por las hipótesis se tiene que $(b-1)+1 = b \in A$ contradiciendo la construcción de B.

Por lo tanto $B = \emptyset$ y $A = \mathbb{N}$, es decir se cumple PIC.

3. **PIC $\Rightarrow$ PIM**

Demostración. Supongamos que el PIC se cumple en $\mathbb{N}$ y consideremos $A \subseteq \mathbb{N}$ que satisface las hipótesis del PIM, es decir, $0 \in A$ y $\{0, 1, 2, ..., n\} \subset A \Rightarrow n+1 \in A$. Debemos demostrar que $A = \mathbb{N}$, es decir, que se cumple PIM.

Anillos, dominios enteros y campos

Definición. *Sea A un conjunto y $+, \cdot$ dos operaciones binarias definidas en A. Diremos que la terna $\langle A, +, \cdot \rangle$ es un* ***anillo*** *si:*

1. $\langle A, + \rangle$ *es un grupo abeliano.*
2. $\langle A, \cdot \rangle$ *es un semigrupo.*
3. $(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in A$ *(distributividad por la derecha)*
4. $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in A$ *(distributividad por la izquierda)*

Definición. *Sea* $\langle A, +, \cdot \rangle$ *un anillo diremos que:*

1. $\langle A, +, \cdot \rangle$ ***anillo conmutativo*** *si* $\cdot$ *es una operación conmutativa.*

2. $\langle A, +, \cdot \rangle$ *es un* ***anillo con unitario****, si*

$$\exists x \in A \text{ tal que } a \cdot x = x \cdot a = a \quad \forall a \in A$$

x se llama ***el uno o elemento unitario*** *del anillo.*

Tareita: demostrar que el unitario de un anillo es único.

Ejemplos

1. ¿Cómo sería el anillo trivial? Intenta crear las operaciones que le den esta estructura al conjunto de un solo elemento.

2. Definamos sobre el conjunto $A = \{a, b\}$ las operaciones de suma y producto de acuerdo a las siguientes tablas:

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

   Comprueba que A con estas operaciones es un anillo ¿es conmutativo? ¿tiene unitario?

3. $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ con la suma y producto usuales son anillos conmutativos con unitario.

4. $n\mathbb{Z}$ para $n \in \mathbb{N}, n > 1$ con la suma y producto usuales ¿es anillo? ¿conmutativo? ¿con unitario?

5. Las matrices de $n \times n$ con coeficientes en $\mathbb{R}$, forman un anillo. ¿Conmutativo? ¿con unitario?

Notación: en cualquier grupo aditivo, la expresión $a - b$ significa $a + (-b)$.

Sabemos que en un grupo se cumplen las leyes de cancelación por ambos lados entonces, si $\langle A, +, \cdot \rangle$ es un anillo, estas leyes también son válidas pues $\langle A, + \rangle$ es grupo abeliano. De aquí, se obtienen varios corolarios:

Corolarios. Si $\langle A, +, \cdot \rangle$ es un anillo y 0 su neutro aditivo, se cumplen,

1. $a + b = a \Rightarrow b = 0$
2. $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in A$
3. $-(-a) = a$
4. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
5. $(-a) \cdot (-b) = a \cdot b$

Tareita: demostrarlos

Definición. *Si dos elementos de un anillo son ambos distintos de cero y su producto es cero, les llamamos* ***divisores de cero.***

¿En $\mathbb{Z}$ hay divisores de cero?

Definición. *Un anillo conmutativo con unitario que no tiene divisores de cero se llama* ***dominio entero.***

Tareita: ¿cuáles de los ejemplos de anillos que dimos son dominios enteros?

Con frecuencia, en lugar de escribir $a \cdot b$ escribiremos solamente ab y DE para dominio entero.

Tenemos entonces que si A, es DE, entonces $\forall\, a, b \in A$,

$$ab = 0 \quad \Leftrightarrow \quad a = 0 \ \text{ ó } \ b = 0$$

Proposición. *En un dominio entero se cumple la ley de la cancelación para el producto.*

Demostración. Sean A un dominio entero y $a, b, c \in A$, $a \neq 0$ tales que $ab = ac$ entonces,

$$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$$

Como A es dominio entero y $a \neq 0$ entonces $b - c = 0 \ \therefore b = c.$ ■

La demostración de la cancelación por la derecha es totalmente análoga.

Tareita: demostrarlos

Observación: El regreso de esta proposición también es válido. Tenemos así, una caracterización de DE.

Definición. *Sea $\langle A, +, \cdot \rangle$ un anillo con unitario 1. Si $a \in A$ y $\exists x \in A$ tal que*

$$ax = xa = 1$$

decimos que x es ***el inverso multiplicativo de*** *a y lo denotamos como a^{-1}.*

No todos los elementos de un anillo tienen inverso multiplicativo.

Definición. *Sea $\langle A, +, \cdot \rangle$ un anillo con unitario 1. Los elementos que tienen inverso multiplicativo se llaman* ***unidades.***

¿El unitario de un anillo es unidad? ¿su inverso aditivo, es unidad? ¿cuáles son las unidades en $\mathbb{Z}$? ¿y en $\mathbb{Q}$?

Definición. *Sea K un conjunto y $+, \cdot$ dos operaciones binarias definidas en K, $\langle K, +, \cdot \rangle$ es un* ***campo*** *si:*

1. *$\langle K, +, \cdot \rangle$ es anillo conmutativo con unitario.*

   Si 0 es su neutro aditivo, llamamos $K^* = K \setminus \{0\}$

2. *$\langle K^*, \cdot \rangle$ es un grupo abeliano.*

Al campo genérico así definido lo denotamos como $\mathbb{K}$.

Tareita: ¿Cuáles de los anillos que hemos dado, son también campos?

Un par de teoremas sobre dominios enteros

Teorema. *Todo campo es dominio entero.*

Demostración. Sean $\mathbb{K}$ un campo y $a, b \in \mathbb{K}$ tales que $ab = 0$ y supongamos que $a \neq 0$. Como todo campo es un anillo conmutativo con uno en el que los elementos no nulos forman un grupo con el producto, entonces a tiene inverso multiplicativo: a^{-1}. Así,

$$ab = 0 \quad \Leftrightarrow \quad (a^{-1}a)b = (a^{-1})0 \quad \Leftrightarrow \quad 1b = 0 \quad \Leftrightarrow \quad b = 0 \quad \therefore \mathbb{K} \text{ es dominio entero.} \quad \blacktriangle$$

Teorema. *Todo dominio entero finito es un campo.*

Teorema. *Todo dominio entero finito es un campo.*

Demostración. Sea D un dominio entero finito. Sabemos que todo dominio entero es un anillo conmutativo con uno, por lo que sólo debemos verificar que los elementos distintos de cero tienen inverso multiplicativo. Si $|D| = 2$ entonces $D = \mathbb{Z}_2$ que es campo y terminamos.
Supongamos que $|D| > 2$ y sea $a \in D$, $a \neq 0$, $a \neq 1$, pues 1 es su propio inverso multiplicativo. Digamos que $|D| = n$. Recordemos que $D^* = D \setminus \{0\}$. Consideremos el conjunto $A = \{a, a^2, ..., a^n\}$.

Como $a \neq 0$ y D es dominio entero, entonces $a^i \neq 0 \; \forall \; i \in \{1, ..., n\}$. Es decir, $A \subseteq D^*$ y como $|D^*| = n - 1$, existe un par de *elementos repetidos* en A. Sean $k_1 \neq k_2$ tales que $a^{k_1} = a^{k_2}$, s.p.g. supongamos que $k_1 < k_2$. Observemos que $k_2 - k_1 \geq 2$ pues si $k_2 - k_1 = 1$, entonces $k_2 = k_1 + 1$, y tendríamos que

$$a^{k_1} = a^{k_2} = a^{k_1+1} = a \cdot a^{k_1} \;\; \Rightarrow \;\; a^{k_1} = a \cdot a^{k_1} \;\; \therefore \;\; a = 1!!!$$

Entonces $k_2 - k_1 \geq 2$ y así,

$$a^{k_1} = a^{k_2} \Rightarrow a^{k_1} = a^{k_1} \cdot a^{k_2-k_1}$$

$$\Rightarrow a^{k_1} - a^{k_1} \cdot a^{k_2-k_1} = 0$$

$$\Rightarrow a^{k_1}(1 - a^{k_2-k_1}) = 0$$

Como D es dominio entero y $a^{k_1} \neq 0$, necesariamente $1 - a^{k_2-k_1} = 0$, es decir,

$$1 = a^{k_2-k_1} \Rightarrow 1 = a \cdot a^{k_2-k_1-1}$$

Por lo que $a^{k_2-k_1-1}$ es el inverso multiplicativo de a y por tanto, todos los elementos distintos de cero tienen inverso multiplicativo, es decir D es un campo. ▲

El anillo de los enteros.
Divisibilidad

Definición. *Sea A un anillo. Una* ***clase positiva*** *en A, es un subconjunto $P \subset A$ a cuyos elementos llamamos* ***positivos*** *y que satisface:*

1. *Si $a, b \in P \Rightarrow a + b \in P$ es decir, es cerrado bajo la suma*
2. *Si $a, b \in P \Rightarrow ab \in P$ es decir, es cerrado bajo el producto*
3. *Si $a \in A$, una y solamente una de las siguientes se cumple: $a \in P$ ó $-a \in P$ ó $a = 0$.*

A un anillo con clase positiva, le llamamos **anillo ordenado** y si además es dominio entero, le llamamos **dominio ordenado.**

Definición. *Sea A un anillo (o dominio) ordenado con clase positiva P y sean $a, b \in A$,* ***si*** $b - a \in P$, ***decimos que*** *"a* ***es menor que*** *b" y lo denotamos:*

$$a < b$$

Notemos que esta es una relación definida sobre los elementos del anillo. Resulta que esta relación es un *orden lineal* sobre el anillo, es decir, cumple que es: antirreflexiva, transitiva y tricotómica.

Propiedades del orden. *Sea A un anillo ordenado y $a, b, c \in A$ entonces,*

1. $a < b \Rightarrow a + c < b + c$
2. $a < b$ *y* $c \in P \Rightarrow ac < bc$
3. *Se cumple una y solamente una de las siguientes:* $a < b$ *ó* $a = b$ *ó* $b < a$
4. *Si* $a < b$ *y* $b < c \Rightarrow a < c$
5. *Si* $a \neq 0 \Rightarrow a^2 \in P$

Tareita. demostrarlas.

Y como corolarios inmediatos:

Corolarios. *Sea A un anillo ordenado y $a, b, c \in A$ entonces,*

1. *Se cumple una y solamente una de las siguientes:* $0 < a$ *ó* $a = 0$ *ó* $a < 0$
2. *Si* $a < b$ *y* $c < 0 \Rightarrow bc < ac$
3. *Si* $a < 0$ *y* $b < 0 \Rightarrow 0 < ab$

Tareita. demostrarlo.

Notas:

1. Si $a < b$ también podemos expresarlo como $b > a$
2. Denotamos $a \leq b$ si $a < b$ ó $a = b$
3. y análogamente $a \geq b$ si $a > b$ ó $a = b$
4. $\mathbb{Z}$ es un dominio entero ordenado

Valor absoluto. *Si* $a \in \mathbb{Z}$ *definimos*

$$|a| = \begin{cases} a & si\ a \geq 0 \\ -a & si\ a < 0 \end{cases}$$

Desigualdad del triángulo. $|a+b| \leq |a| + |b|$

Demostración. Procedemos por casos.

1. Si $a \geq 0,\ \ b \geq 0$ entonces,

$$|a+b| = a+b = |a| + |b|$$

2. Si $a < 0,\ \ b < 0$ entonces, $a+b < 0$ por lo que

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

3. Si $a \geq 0,\ b < 0$ demostraremos que $|a+b| < a-b$ porque $a-b = a+(-b) = |a|+|b|$ y concluimos.
   Para demostrar que $|a+b| \leq a-b$ analizaremos dos casos posibles:

   3.1 Si $a+b \geq 0$ entonces,

   $$|a+b| = a+b < a-b \Leftrightarrow b < -b$$

   y esto es cierto porque $b < 0 \quad \therefore |a+b| < a-b.$

   3.2 Si $a+b < 0$ entonces,

   $$|a+b| = -(a+b) = -a+(-b) \leq a-b \Leftrightarrow -a \leq a$$

   y esto es cierto porque $a \geq 0 \quad \therefore |a+b| \leq a-b.$

4. Si $a < 0,\ b \geq 0$ es análogo a (3). ■

Definición. *Sean* $a, b \in \mathbb{Z}$ *decimos que* b ***divide a*** a *si* $\exists q \in \mathbb{Z}$ *tal que* $a = bq$ *y lo denotamos así*

$$b \mid a$$

Si b ***no divide a*** a*, denotamos* $b \nmid a$

Otras formas de decir que b **divide a** a son:

1. a es divisible por b
2. a es divisible entre b
3. b es divisor de a
4. b es factor de a
5. a es múltiplo de b

$$b \mid a \text{ si } \exists q \in \mathbb{Z} \text{ tal que } a = bq$$

De la definición se desprende inmediatamente que:

1. $1 \mid a$
2. $a \mid a$
3. $a \mid 0$
4. Si $b \mid a \Rightarrow -b \mid a$

Definición. *Un* ***divisor propio de*** a *es un entero* b *tal que* $b \mid a$ *pero* $b \neq a$.

Definición. $a \in \mathbb{N}$ *es un número* ***perfecto*** *si es la suma de sus divisores propios.*

Teorema. *Si* $b \mid a$ *y* $a \neq 0$ *entonces* $|b| \leq |a|$.

Demostración. Si $b \mid a$ entonces $a = bq$ p.a. $q \in \mathbb{Z}$, $q \neq 0$ de donde

$$|a| = |bq| = |b||q| \geq |b| \qquad \blacksquare$$

Definición. *Si* $a, b \in \mathbb{Z}$, *una* ***combinación lineal de*** a ***y*** b *es un número de la forma* $ax + by$ *con* $x, y \in \mathbb{Z}$.

Teorema. *Si* $c \mid a$ *y* $c \mid b$ *entonces* $c \mid ax + by \; \forall x, y \in \mathbb{Z}$.

Corolario. *Si* $a \mid c_1$ *y* $a \mid c_2$ *y* $a \mid c_3 \ldots$ *y* $a \mid c_n$ *entonces* $a \mid c_1x_1 + c_2x_2 + c_3x_3 + \ldots + c_nx_n \; \forall \, x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Tareita: demostrarlos

Teorema (del algoritmo de la división)

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos, tales que

$$a = qb + r \text{ con } 0 \leq r < |b|$$

Demostración.

Tareita: demostrar la unicidad, revisar otra demostración (y entender ambas)

El anillo $\mathbb{Z}_m$

Definición. *Sea $m \in \mathbb{Z}$. Definimos el* ***conjunto de los múltiplos de m*** *como el conjunto:*

$$m\mathbb{Z} \quad = \quad \{mn \mid n \in \mathbb{Z}\}$$

Proposición. *El conjunto $m\mathbb{Z}$ cumple las siguientes propiedades:*

1. $0 \in m\mathbb{Z}$.
2. $m\mathbb{Z}$ *es cerrado bajo la suma de* $\mathbb{Z}$.
3. *Si* $a \in m\mathbb{Z}$, *entonces* $qa \in m\mathbb{Z} \quad \forall q \in \mathbb{Z}$.

Sea $m \in \mathbb{Z}$. Definimos la relación $\sim$ en $\mathbb{Z}$ de la siguiente forma:

$$a \sim b \iff \exists k \in \mathbb{Z}\,(b - a = mk)$$

o de forma equivalente:

$$a \sim b \iff b - a \in m\mathbb{Z}$$

No es difícil demostrar que esta es una relación de equivalencia en $\mathbb{Z}$. ¿Cuál es la partición que induce? Observemos que:

$$0 \sim b \iff b - 0 \in m\mathbb{Z} \iff \exists k \in \mathbb{Z}\,(b = mk)$$

Entonces, un número b está en la clase del 0 si y sólo si es un múltiplo de m, por lo que

$$[0] = m\mathbb{Z}$$

Ahora, si $b \in \mathbb{Z}$, por el **algoritmo de la división**, sabemos que existen $q, r \in \mathbb{Z}$ únicos, tales que $0 \leq r < m$, y $b = mq + r$. Entonces $r \sim b$, pues

$$b - r = (mq + r) - r = mq \in m\mathbb{Z}$$

Entonces, todos los enteros de la forma $mq + r$ están relacionados con r, y de hecho

$$[r] = \{mq + r \mid q \in \mathbb{Z}\}$$

Esto quiere decir que el conjunto $\{0, 1, 2, ..., m-1\}$ es un conjunto mínimo de representantes de las clases de equivalencia. Además, es el conjunto de todos los posibles residuos que puede dejar un número al dividirse entre m, y todos los números que dejan el mismo residuo pertenecen a la misma clase de equivalencia. Así,

$$\mathbb{Z}/\sim = \{[0], [1], [2], ..., [m-1]\}$$

A este conjunto también lo denotamos como $\mathbb{Z}/m\mathbb{Z}$.

Dotaremos a $\mathbb{Z}/m\mathbb{Z}$ con una estructura de anillo. Definimos la suma de la siguiente forma:

$$[a] + [b] = [a + b]$$

Esta definición parece bastante razonable, sin embargo, debemos verificar que ***está bien definida***, pues como cada clase de equivalencia tiene varios representantes, el resultado de la suma podría ser distinto si se usaran otros representantes de la misma clase de equivalencia. Comprobar que la suma está bien definida, es comprobar que no depende del representante elegido, veamos:

Sean $a \sim a'$ y $b \sim b'$. Debemos verificar que $a + b \sim a' + b'$. Como $a \sim a'$ y $b \sim b'$ entonces, $\exists\, k_1, k_2 \in \mathbb{Z}(a' - a = mk_1 \ \wedge\ b' - b = mk_2)$ es decir, $a = a' - mk_1 \quad \wedge \quad b = b' - mk_2$

$$\Rightarrow a + b = (a' - mk_1) + (b' - mk_2) = a' + b' + m(-k_1 - k_2)$$

$$\Rightarrow (a + b) - (a' + b') = m(-k_1 - k_2) \Rightarrow (a' + b') - (a + b) = m(k_1 + k_2) \quad \text{tomando } k = k_1 + k_2$$

$$\Rightarrow a + b \sim a' + b' \quad \blacktriangle$$

Así, $[a' + b'] = [a + b]$. Por lo tanto, $[a] + [b] = [a'] + [b']$. Entonces, la suma en $\mathbb{Z}/m\mathbb{Z}$ está bien definida.

Ahora definimos el producto de la siguiente forma:

$$[a] \cdot [b] = [ab]$$

De forma similar a la suma, se puede demostrar que el producto está bien definido. Dejaremos como ejercicio demostrar que para cualquier entero m distinto de cero, $\langle \mathbb{Z}/m\mathbb{Z}, +, \cdot \rangle$ es un anillo conmutativo con uno, y a este anillo lo denotaremos como $\mathbb{Z}_m$.
Para hacernos la vida más fácil, escribiremos $\bar{a}$ para denotar $[a]$. Entonces

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$$

Y decimos que es **el anillo de clases residuales módulo** m**.**

Ejemplo 1. Consideremos el anillo $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

Observemos que $\bar{2} + \bar{2} = \bar{4} = \bar{0}$, entonces, $\bar{2}$ es su propio inverso aditivo. Por otro lado, $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$. Es decir, $\mathbb{Z}_4$ no es un dominio entero.

Ejemplo 2. Consideremos el anillo $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

Observemos que $\bar{2} + \bar{1} = \bar{3} = \bar{0}$, entonces, $\bar{2}$ es el inverso aditivo de $\bar{1}$.
Por otro lado, $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{1} \cdot \bar{2} = \bar{2}$, $\bar{2} \cdot \bar{2} = \bar{4} = \bar{1}$. Es decir, $\mathbb{Z}_3$ sí es un dominio entero, y de hecho, es un campo.

¿Es $\mathbb{Z}_6$ un dominio entero?... ¿$\mathbb{Z}_5$ es dominio entero?

Con la misma relación de equivalencia, ¿qué conjuntos serían $\mathbb{Z}/0\mathbb{Z}$ y $\mathbb{Z}/1\mathbb{Z}$? ¿Qué tipo de estructuras serían $\mathbb{Z}_0$ y $\mathbb{Z}_1$?

Primos. Teorema fundamental de la aritmética

Definición: *Diremos que un número natural* $p > 1$ *es un* ***número primo*** *si*

$$\forall n \in \mathbb{N} \; (\; n|p \;\; \Rightarrow \;\; (\; n = 1 \;\; \vee \;\; n = p \;) \;)$$

Un número primo p, es un número natural cuyos únicos divisores (positivos) son 1 y p. El concepto de número primo se considera únicamente en el contexto de los números naturales. Por definición, 1 no es un número primo, aunque cumple con la propiedad que define a estos números.

Definición. *Diremos que un número natural $p > 1$ es un* ***número primo*** *si*

$$\forall n \in \mathbb{N}\ (n \mid p \ \Rightarrow\ (n = 1 \ \vee\ n = p\ ))$$

Definición. *Diremos que un número natural m es un* ***número compuesto*** *si no es un número primo. Es decir, si*

$$\exists n \in \mathbb{N}\ (n \mid m \ \wedge\ (n \neq 1 \ \wedge\ n \neq m\ ))$$

Notemos que, de acuerdo a estas definiciones, cualquier número natural $n > 1$ es un número primo o un número compuesto, por lo que podemos clasificar a todos los números naturales en estas dos categorías.

Criba de Eratóstenes

1. Hacer una lista (o tabla) de todos los números entre 2 y n.
2. Marcar el primer número de la lista que no esté tachado (el primero en marcarse sería el 2).
3. Tachar todos los múltiplos del número marcado en el paso anterior.
4. Regresar al paso 2.

El algoritmo termina cuando todos los números de la lista están marcados o tachados. Los números marcados son primos y el resto son compuestos.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	~~47~~	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

El Teorema Fundamental de la Aritmética

Teorema. *Todos los números naturales mayores a 1 se escriben de forma única como producto de potencias de números primos.*

Demostración. Veamos que tal factorización existe, lo haremos por inducción fuerte sobre $n \geq 2$.

Caso base. $n = 2$

Sabemos que si $m \in \mathbb{N}$ y $m \mid 2$, entonces $m \leq 2$. Los únicos números naturales menores a 2 son 0 y 1, y como $0 \nmid 2$ tenemos que 2 es un número primo, por lo tanto cumple el teorema (de hecho, todos los primos lo cumplen trivialmente). ▲

Hipótesis de inducción. Sea $n \in \mathbb{N}, n > 2$ y supongamos que $\forall m < n$, m se escribe como producto de potencias de números primos.

Paso inductivo. Demostremos que n se escribe como producto de potencias de números primos.

Si n es un número primo, cumple el teorema y no hay nada que hacer. Supongamos que n es compuesto. Entonces $\exists a, b \in \mathbb{N}$ tales que $ab = n$ con $a, b > 1$, es decir, a y b son divisores de n, por lo que $1 < a < n$ y $1 < b < n$. Por hipótesis de inducción, a y b se escriben como producto de potencias de números primos. Es decir,

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{y} \quad b = q_1^{l_1} q_2^{l_2} \cdots q_s^{l_s} \quad \text{donde los } p_i \text{ y los } q_i \text{ son primos}$$

$$\therefore n = ab = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})(q_1^{l_1} q_2^{l_2} \cdots q_s^{l_s})$$

Demostremos ahora la unicidad de tal factorización.

Supongamos que hay números que tienen dos representaciones distintas como producto de potencias de primos, sea n el menor de tales números, o sea que todos los enteros entre 2 y $n-1$ sí tienen una factorización única como producto de potencias de primos. Entonces,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1^{l_1} q_2^{l_2} \cdots q_s^{l_s}$$

Notemos que $r > 1$ y $s > 1$, además los primos $p_1, p_2, ...p_r$ son todos distintos a los primos $q_1, q_2 ... q_s$ porque si por ejemplo, p_1 fuera un elemento común a ambas colecciones, entonces podrían dividirse las dos factorizaciones entre p_1 y obtendríamos dos factorizaciones distintas del entero $\frac{n}{p_1}$, pero, este número es menor que n y los números menores a n sí son unívocamente factorizables en primos.
Sin pérdida de generalidad, supongamos que $p_1 < q_1$ y definamos al entero positivo N como,

$$N = (q_1 - p_1) q_2 q_3 ... q_s = p_1 (p_2 p_3 ... p_r - q_2 q_3 ... q_s) \qquad (*)$$

$$N = (q_1 - p_1)q_2q_3...q_s = p_1(p_2p_3...p_r - q_2q_3...q_s) \qquad (*)$$

Evidentemente $N < n$ por lo que N es unívocamente factorizable en primos. Pero $p_1 \nmid (q_1 - p_1)$, por lo que (*) expresa dos factorizaciones distintas de N !!! (una contiene a p_1 y la otra no). La contradicción surge de haber supuesto la existencia de tales números.

Concluimos entonces que tal factorización es única, es decir, todos los números naturales mayores a 1 se escriben de forma única como producto de potencias de números primos. ▲

Teorema. *Un número entero p es primo si y solamente si* $\forall\ 1 < n \leq \sqrt{p},\ n \nmid p$

Demostración.

$\Rightarrow$) Sea p primo, entonces su único divisor menor que p es $1 \therefore \forall\ 1 < n \leq \sqrt{p},\ n \nmid p$.

$\Leftarrow$) Sea $p \in \mathbb{N}$ y supongamos que $\forall\ 1 < n \leq \sqrt{p},\ n \nmid p$, demostremos que p es primo.

Supongamos que no lo es, es decir $p = ab$. Como todo $1 < n \leq \sqrt{p}$, no divide a p y como $a \mid p$ y $b \mid p$, entonces $a > \sqrt{p}$ y $b > \sqrt{p} \Rightarrow ab > p \Rightarrow p = ab > p$!!!

Por lo tanto p es primo. ▲

Corolario. *Un número entero p es primo si y solamente si p no es divisible por algún primo $q \leq \sqrt{p}$*

Demostración. Es inmediato del teorema anterior y del Teorema Fundamental de la Aritmética pues todo compuesto menor que $\sqrt{p}$ tiene divisores primos menores que $\sqrt{p}$.

Lema. *Todo número $n \in \mathbb{N}, n > 1$, tiene un divisor primo.*

Demostración. Sea $A = \{n \in \mathbb{N}, n > 1 \mid n \text{ no tiene divisores primos}\}$ y supongamos que $A \neq \emptyset$ entonces por PBO hay un mínimo m. Claramente m no puede ser primo, pues él mismo sería su divisor primo, entonces es compuesto $m = ab$ con $1 < a \leq b < m$, como $a < m$ entonces $a \notin A$ por lo que $\exists p$ primo, tal que $p \mid a$ pero $p \mid ab = m$!!!

Por lo tanto $A = \emptyset$ es decir, todo $n \in \mathbb{N}, n > 1$, tiene un divisor primo. ▲

Teorema. *Hay una infinidad de números primos*

Demostración. Supongamos que hay un número finito de primos, digamos n y sean todos ellos, el conjunto

$$\{p_1, p_2, ...p_n\}$$

Consideremos el número $N = p_1p_2...p_n + 1$. Por el algoritmo de la división N no es divisible por ningún primo pues el residuo dal dividir N entre cualquier primo p_j es 1, pero esto contradice al lema por lo tanto hay una infinidad de primos. ▲

Nuestro sistema numérico es posicional de base 10 y nos permite representar cada entero mediante los diez dígitos que conocemos. En realidad podríamos representarlos usando otra base, esta es una de las aplicaciones del algoritmo de la división y se demuestra en el siguiente teorema.

Teorema. *Sean* $b, n \in \mathbb{Z}, b > 1, n > 0$, *existen* $k \in \mathbb{N}$ *y enteros* $0 \leq a_j < b$, $j = 1, 2, ..., k$, *tales que*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

y $a_k \neq 0$. *Además esta representación es única.*

Tareita: buscar la demostración de este teorema y verificar cómo se usa. (por ejemplo en el Grimaldi o el Espinosa)

Máximo común divisor. Algoritmo de Euclides