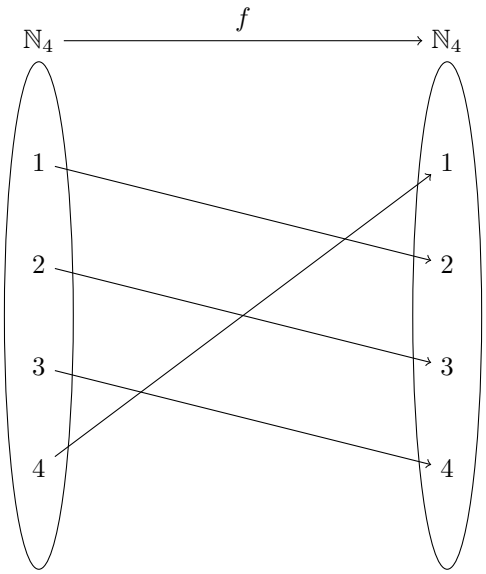
Conjuntos y Números

Miguel González

Enero 2018



Revisado en 2020

Acerca de este documento

Estos apuntes son una versión revisada de los de la asignatura Conjuntos y Números del grado en matemáticas, tomados en Enero 2018 por Miguel González. A los apuntes originales se les ha añadido esta página, una imagen de portada, y breves párrafos explicativos en las zonas menos completas. Asimismo se han revisado las erratas y completado los contenidos faltantes.

Este documento es:

- Una recopilación ordenada y directa de las definiciones y resultados más importantes del tema en cuestión, al nivel de los estudios de grado.
- Una colección de demostraciones completas de dichos resultados (salvo en los casos más básicos).
- Una *guía* para revisar de manera rápida las ideas que se han adquirido previamente, o para consultar enunciados puntuales que puedan no haberse comprendido en su totalidad.

Este documento NO es:

- Un libro de texto de la asignatura.
- Una colección de ejercicios para practicar los conceptos adquiridos.
- Un listado de ejemplos para ilustrar las ideas tratadas. A pesar de ello, en ocasiones se incluyen ejemplos puntuales que puedan ser de especial interés o curiosidad, pero se intentan reducir al mínimo en virtud del primer punto de la lista anterior.

Sobre Conjuntos y Números

En esta asignatura se introducen las herramientas generales mas básicas para el estudio de las matemáticas. Es por eso que es de vital importancia su comprensión e integración profunda, dado que las ideas que se elaboran aquí aparecerán de forma recurrente en el resto de ámbitos que se tratan en esta disciplina. A lo largo del documento, se discuten en primer lugar de nociones elementales de lógica matemática y teoría de conjuntos, y posteriormente se exploran resultados básicos de los números naturales, enteros y complejos. Finalmente se da un breve resumen de conceptos y proposiciones acerca de polinomios.

Requisitos previos

1. Nociones elementales de notación matemática.

Índice

1. Lógica matemática

Las matemáticas son un campo **formal**, cuya estructura se basa en una serie de **axiomas**, que son enunciados que se toman como ciertos, y a partir de los cuales se derivan otros mediante reglas lógicas, con el fin de ampliar el conocimiento en el ámbito correspondiente. De este modo, simplemente permitiendo que los axiomas sean hechos evidentes para nosotros, obtendremos otras ideas cuya veracidad se sustenta únicamente en estos principios evidentes, y por tanto serán también ciertas (y podremos extraer nuevos resultados de ellas). En esta sección se tratarán los aspectos más básicos de este pilar principal de las matemáticas: *la lógica*.

1.1. Proposiciones

Una proposición es una sentencia con un valor de verdad definido, es decir, de ella se puede indicar si es verdadera o falsa inequívocamente. Por ejemplo, una proposición puede ser: *todos los números naturales son pares*. Las proposiciones, en el ámbito de la lógica formal, se denotan con símbolos como $p, q, r...$ y combinándolas con operadores se obtienen otras proposiciones. Estas últimas se denominan **compuestas**.

1.2. Operadores lógicos

- **Conjunción.** Se indica con $\wedge$. La proposición $p \wedge q$ es verdadera si tanto p como q lo son.
- **Disyunción.** Se indica con $\vee$. La proposición $p \vee q$ es verdadera si al menos uno de p o q lo es.
- **Implicación.** Se indica con $\implies$. La proposición $p \implies q$ es verdadera si cuando p lo es, q también. Al ser esta la única condición, cabe destacar que si p es falsa, $p \implies q$ será verdadera siempre.
- **Equivalencia.** Se indica con $\iff$. La proposición $p \iff q$ es verdadera si el valor de verdad de p es igual que el de q.

1.3. Equivalencias, tautologías y contradicciones

Dos proposiciones son **equivalentes** lógicamente (se indica con $\equiv$) si tienen el mismo valor de verdad para cualquier interpretación, es decir, si para cualquier combinación de valores de verdad de las proposiciones atómicas que las componen, el valor de verdad resultante es igual para las dos. Si $p \equiv q$, entonces $p \iff q$ es cierto siempre. *Por ejemplo:* $p \implies q \equiv \neg p \vee q$, $(p \iff q) \wedge (q \implies p) \equiv p \implies q$.

Una proposición compuesta es una **tautología** si siempre toma el valor verdadero. Es decir, no importa qué valores de verdad tomen las proposiciones que la forman, el valor final siempre resulta en verdadero. *Por ejemplo:* $p \vee \neg p$. Compruébese que sin importar si p es verdadero o falso, la expresión se verifica.

Una proposición compuesta es una **contradicción** si siempre toma el valor falso. Es decir, no importa qué valores de verdad tomen las proposiciones que la forman, el valor final siempre resulta en falso. *Por ejemplo:* $p \wedge \neg p$. Compruébese que sin importar si p es verdadero o falso, la expresión no se verifica.

1.4. Funciones proposicionales

Las funciones proposicionales $p(x)$ no tienen un valor de verdad definido en sí, pero se convierten en proposiciones al asignar valores a sus variables, conocidas como **variables libres**. Estas pueden tomar cualquier valor. Un ejemplo de función proposicional es $p(x) = \{x^2 > 0\}$. En este caso, por ejemplo, $p(2)$ es una proposición verdadera y $p(0)$ es falsa.

Cabe destacar que, para evitar que se generen expresiones sin sentido, o para aclarar en qué ámbito debe considerarse una proposición, se suele establecer un **universo**, que muchas veces se da por entendido según el contexto, que indica los valores que pueden aceptar las variables de la función (Por ejemplo, valores de $\mathbb{N}$, de $\mathbb{R}$...).

Además de asignando valores a la función, también se obtienen proposiciones empleando **cuantificadores**.

1.4.1. Cuantificadores

- **Universal.** Se denota con $\forall$ y se expresa de la siguiente manera: $\forall x(p(x))$. Esta proposición es verdadera únicamente si todos los valores posibles x_0 de x (dentro del universo definido) hacen que la proposición $p(x_0)$ tenga valor verdadero. Por ejemplo, la proposición $\forall x(x^2 + 10x + 2 > 0)$ es falsa en el universo $\mathbb{R}$, aunque verdadera en el universo $\mathbb{N}$.

- **Existencial.** Se denota con $\exists$ y se expresa de la siguiente manera: $\exists x(p(x))$. Esta proposición es verdadera si hay algún valor x_0 de x (dentro del universo definido) que hace que la proposición $p(x_0)$ tenga valor verdadero. Por ejemplo, la proposición $\exists x(x^2 + 10x + 2 > 0)$ es verdadera en el universo $\mathbb{N}$, y por consiguiente en el universo $\mathbb{R}$.

Como dan lugar a nuevas proposiciones o funciones proposicionales, pueden en efecto combinarse entre ellos. Por ejemplo, sea la función proposicional $p(x, y) = (x^2 < y)$, entonces una proposición es (en $\mathbb{N}$) $\forall x(\exists y(x^2 < y))$. Esto es cierto dado que, sin importar el valor x_0 que tome x, si se hace $y_0 = x_0^2 + 1$, entonces $p(x_0, y_0)$ es verdadero. Nótese que $\forall x(x^2 < y)$ sigue siendo una función proposicional y no una proposición, ya que depende de y.

Es muy importante el orden de los cuantificadores, si son distintos. En el caso anterior, la proposición (en $\mathbb{N}$) $\exists y(\forall x(x^2 < y))$ es falsa. (Puesto que no importa el valor y_0 que se escoja, si se hace, por ejemplo, $x_0 = y_0$ la función $p(x_0, y_0)$ es falsa.)

Si los dos cuantificadores son iguales, se puede abreviar mediante notación: la expresión $\forall x(\forall y(p(x, y)))$ equivale a $\forall y(\forall x(p(x, y)))$ y se suele indicar $\forall x, y(p(x, y))$. Igualmente para $\exists$.

1.4.2. Negación de cuantificadores

Conviene conocer las siguientes reglas lógicas que permiten permutar la negación con los cuantificadores:

- $\neg(\forall x(p(x))) \equiv \exists x(\neg p(x))$ (Negar que siempre se cumple algo equivale a que existe un caso en el que no se cumple)

- $\neg(\exists x(p(x))) \equiv \forall x(\neg p(x))$ (Negar que existe un caso en el que se cumple algo equivale a que en todos los casos no se cumple)

1.5. Demostraciones

En lógica, las conocidas como reglas de inferencia permiten generar proposiciones ciertas a partir de otras. Por ejemplo: **Si p es cierto y p $\implies$ q es cierto, entonces q es cierto.** Con ellas se puede partir de proposiciones ciertas y extraer otras mediante **demostraciones**.

1.5.1. Demostración directa

Consiste en encadenar implicaciones como se ha descrito en la regla de inferencia anterior. Por ejemplo, si queremos demostrar la veracidad de la proposición: *el cuadrado de un natural par también es par*, o, utilizando símbolos lógicos:

$\forall x \in \mathbb{N}((x \text{ es par}) \implies (x^2 \text{ es par})$

Bastará con (asumiendo que x es un natural arbitrario) partir de la premisa ($(x$ es par) y alcanzar la conclusión (x^2 es par):
x es par $\implies x = 2k(k \in \mathbb{N})$
$x = 2k \implies x^2 = 4k^2$
$x^2 = 4k^2 \implies x^2 = 2k'(k' = 2k^2 \in \mathbb{N})$
$x^2 = 2k' \implies x^2$ es par
Luego, x es par $\implies x^2$ es par.
Lo normal es encadenar los implicadores seguidamente, sin repetir las proposiciones que se usan, es decir $p \implies r_1 \implies r_2 ... \implies r_n \implies q$. Estas demostraciones tienen la ventaja de que estos resultados parciales $p \implies r_1$, $p \implies r_2$, ... también se demuestran como verdaderos.

1.5.2. Demostraciones indirectas

Existen otros métodos de demostración que no son directos. Los más usados son los siguientes:

- **Contrapositivo.** Se basa en la siguiente equivalencia lógica: $p \implies q \equiv \neg q \implies \neg p$. Así, basta con demostrar cualquiera de las dos.

  Vamos a usarla para probar lo siguiente: *si el cuadrado de un natural es impar, dicho natural también lo es.*

  $\forall x \in \mathbb{N}(n^2 \text{ es impar}) \implies (n \text{ es impar})$

  $\equiv \neg(n \text{ es impar}) \implies \neg(n^2 \text{ es impar})$

  $\equiv (n \text{ es par}) \implies (n^2 \text{ es par})$

  Que ya se ha probado antes. Como equivale a algo cierto, ha de ser cierto.

- **Reducción al absurdo.** Se basa en suponer la negación de lo que se quiere probar, y llegar a través de equivalencias y reglas lógicas correctas a una contradicción (es decir, a una proposición que entre en conflicto con otra que se ha demostrado verdadera).

  Vamos a demostrar que *la raíz de dos no es racional*, es decir, que $\sqrt{2} \notin \mathbb{Q}$

  Suponemos lo contrario, es decir, que $\sqrt{2} \in \mathbb{Q}$. Entonces, $\sqrt{2} = \frac{p}{q}$ con $p, q \in \mathbb{Z}$, y tomamos p, q coprimos (reduciendo la fracción hasta que p y q no tengan factores en común).

  Entonces (se denota con $\rightarrow$ el salto entre pasos de la demostrafción), $2 = \frac{p^2}{q^2} \rightarrow 2q^2 = p^2 \rightarrow p = 2k(k \in \mathbb{Z})$.

  Ahora, $2 = \frac{4k^2}{q^2} \rightarrow q^2 = 2k^2 \rightarrow q = 2k'(k \in \mathbb{Z})$. Entonces p y q no son coprimos (ambos tienen el factor 2) lo que es una contradicción. Se ha usado que si el cuadrado de un número es par, entonces dicho número también lo es (puede demostrarse análogamente a lo discutido en secciones anteriores). Así, $\sqrt{2} \notin \mathbb{Q}$.

1.5.3. Principio de inducción

Otro método indirecto es el principio de inducción. Frecuentemente querremos demostrar proposiciones acerca del conjunto de los números naturales ($\mathbb{N} = \{1, 2, 3, \ldots\}$). Una de las técnicas más usadas y *naturales* de probar que una propiedad se cumple para todo $\mathbb{N}$ es la **inducción**. La idea se basa en comprobar que la proposición es cierta en un punto de partida (caso base), y que, de ser cierta en un valor natural arbitrario, lo es en el siguiente. Con demostrar estos dos hechos, la proposición se demuestra

válida a partir del caso base (puesto que al ser cierto para este valor, lo es para el sucesor, y al ser cierto el sucesor, también lo es el siguiente...)

Es decir, si una propiedad de los números naturales, $\mathcal{P}(n)$, es cierta para $n = n_0$, y cumple $\mathcal{P}(n) \implies \mathcal{P}(n+1)$, entonces se deduce $\forall n((n \geq n_0) \implies (\mathcal{P}(n)))$.

Por ejemplo: Demostrar que $1 \times 1! + 2 \times 2! + ... + n \times n! = (n+1)! - 1$ se cumple para todo $n \in \mathbb{N}$. Evidentemente, $n = 1$ satisface la propiedad: $1 \times 1! = 2! - 1 = 1$. Si ahora suponemos que n la satisface (**Hipótesis de inducción**), llegamos a que $1 \times 1! + 2 \times 2! + ... + n \times n! + (n+1) \times (n+1)! = (n+1)! - 1 + (n+1) \times (n+1)! = (n+1)! \times (n+2) - 1 = (n+2)! - 1 = ((n+1)+1)! - 1$, es decir, que $\mathcal{P}(n+1)$ es cierta y, por el principio de inducción, se ha demostrado lo que se quería. □

Cabe observar que en el paso inductivo podemos usar la propiedad $\mathcal{P}$ (que queremos probar) para todos los valores anteriores a n (a partir del caso base). Esto equivale a usar la inducción en su forma descrita anteriormente para la propiedad $\tilde{\mathcal{P}}(n) : (\forall k \leq n)(\mathcal{P}(k))$. Así, en el paso inductivo se puede usar la propiedad $\mathcal{P}(k)$ para valores de k anteriores a n, y al probar $\tilde{\mathcal{P}}$ para todo $n \in \mathbb{N}$ estamos probando también $\mathcal{P}$ (Es inmediato que $\tilde{\mathcal{P}}(n) \implies \mathcal{P}(n)$). Esto se conoce como **inducción fuerte**.

2. Conjuntos

Uno de los componentes principales de las matemáticas es el **conjunto**, que representa de manera abstracta una colección de elementos. En esta sección se describen las nociones básicas de la teoría de conjuntos.

2.1. Definir un conjunto

Un conjunto se puede definir **por extensión** o **por comprensión**. En el primer caso, se indican explícitamente sus elementos. Por ejemplo: $X = \{2, 4, 6\}$. En el segundo caso, se indica qué reglas cumplen los elementos del conjunto. Por ejemplo: $X = \{x : x \in \mathbb{N}, x \text{ es par}, x < 7\}$. Si el elemento a pertenece al conjunto X, se denota $a \in X$. El conjunto sin elementos se denota $\emptyset$.

2.2. Conceptos básicos

1. Dos conjuntos A y B son **iguales** (Denotado por $A = B$), si y solo si $\forall x(x \in A \iff x \in B)$. Es decir, si tienen los mismos elementos.

2. Dados dos conjuntos A y B, se dice que A está contenido en B o es subconjunto de B (Denotado por $A \subset B$)[1] si y solo si $\forall x(x \in A \implies x \in B)$. Obsérvese que si $A \subset B$ y $B \subset A$ entonces $A = B$.

3. Dados dos conjuntos A y B se definen:

   a) $A \backslash B := \{x \in A : x \notin B\}$ (**A menos B**)

   b) $A \cup B := \{x : x \in A \vee x \in B\}$ (**A unión B**)

   c) $A \cap B := \{x : x \in A \wedge x \in B\}$ (**A intersección B**)

   Dos conjuntos son **disjuntos** si $A \cap B = \emptyset$, es decir, si no comparten elementos.

4. Si se trabaja en un contexto o universo X (Es decir, todos los conjuntos que se consideran son subconjuntos de X), entonces se define $A^c := X \backslash A$. Se denomina **complementario** de A (*Los elementos que no están en A*).

Algunos ejemplos de estos conceptos: Sea $X = \{1, 2, 3\}$ e $Y = \{1, \{2\}, \{3\}\}$. Nótese que los elementos de X son tres números, y los elementos de Y son un número y dos conjuntos que a su vez contienen números. Se cumplen, por ejemplo, $X \neq Y$, $2 \in X$, $2 \notin Y$, $\{2\} \subset X$, $\{2\} \in Y$.

2.3. Partes de un conjunto (Conjunto potencia)

Dado un conjunto X, se define el conjunto de partes $\mathcal{P}(X)$ (o *conjunto potencia*) como:

$$\mathcal{P}(X) := \{A : A \subset X\}$$

Es decir, se trata de todos sus subconjuntos posibles.

Tanto X (llamado *total*) como $\emptyset$ pertenecen a $\mathcal{P}(X)$. Esto es así porque ambos son subconjuntos de X. (Verifíquese que para todo x, $x \in X \implies x \in X$ y $x \in \emptyset \implies x \in X$.)

Suponiendo que X tiene un número finito n de elementos, el conjunto de partes de X tiene 2^n elementos. Esto es así porque, al construir un subconjunto de X, para cada elemento de X puede elegirse incluirlo o no. Es decir, hay 2 posibilidades para el primer elemento de X, 2 para el segundo... así n veces, luego hay 2^n subconjuntos de X diferentes (y por tanto elementos distintos de $\mathcal{P}(X)$).

Ejemplo. Sea $X = \{1, 2\}$. Entonces $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

[1] En adelante, este símbolo no excluirá la posibilidad $A = B$. Algunos autores emplean $A \subseteq B$ para designar esto.

2.4. Propiedades de conjuntos

Sean A, B, C subconjuntos de X. Se verifican (la comprobación es inmediata):

1. $A \cup B = B \cup A$, $A \cap B = B \cap A$
2. $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$. Por ello, se suele denotar sin paréntesis: $A \cup B \cup C$, $A \cap B \cap C$.
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. $A \backslash B = A \cap B^c$
5. $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$
6. $(A^c)^c = A$

Cuando se trata con n conjuntos, es habitual emplear subíndices A_1, A_2, A_3 ... A_n. Entonces, $A_1 \cup A_2 \cup ... \cup A_n$, y como el orden en el que se aplica la operación no importa gracias a la propiedad asociativa (punto 2 del listado anterior), se puede denotar $\bigcup_{i=1}^{n} A_i$. De igual manera, $A_1 \cap A_2 \cap ... \cap A_n$ se puede denotar $\bigcap_{i=1}^{n} A_i$. Se denomina **conjunto de índices** al conjunto que contiene los subíndices empleados. En este caso, sería $I = \{1, 2, 3, ..., n\}$. Si los subíndices no son números ordenados (Por ejemplo, si son letras, objetos...), las expresiones anteriores se pueden escribir $\bigcup_{i \in I} A_i$, $\bigcap_{i \in I} A_i$.

2.5. Producto cartesiano de conjuntos

El producto cartesiano permite construir un conjunto nuevo a partir de otros dos. Dados $a \in A, b \in B$, formamos (a, b), denominado *par ordenado* de A y B. Se tiene $(a, b) = (a_1, b_1)$ si y solo si $a = a_1$ y $b = b_1$.

Definición 1. Sean X, Y conjuntos. Se define el producto cartesiano como $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

2.6. Conjuntos finitos

Definición 2. Sea $\mathbb{N}_n = \{m \in \mathbb{N} : 1 \leq m \leq n\}$. Un conjunto X es **finito** si y solo si existe una biyección $f : \mathbb{N}_n \mapsto X$. Este valor n, que es único, es el número de elementos de X, y se denomina **cardinal** de X. Se denota por $|X|$.

Aunque el concepto de biyección se tratará posteriormente, esta definición quiere decir que un conjunto es finito si podemos emparejar cada uno de sus elementos con cada uno de los naturales del 1 al n, sin repetir.

2.6.1. Propiedades del cardinal

Se tienen las siguientes propiedades (verificables fácilmente):

- Sean X, Y finitos. Entonces $X \times Y$ es finito y $|X \times Y| = |X| \cdot |Y|$.
- Sean A, B disjuntos y finitos. $|A \cup B| = |A| + |B|$. Más generalmente, sean $A_1, A_2, A_3, ..., A_n$ finitos y disjuntos dos a dos (Decimos que n conjuntos son disjuntos dos a dos si todas las parejas arbitrarias que tomemos lo son, es decir, $\forall i, j \leq n \in \mathbb{N}$, $A_i \cap A_j = \emptyset$), entonces $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$.
- Sea X finito, entonces $\mathcal{P}(X)$ es finito y $|\mathcal{P}(X)| = 2^{|X|}$.

2.6.2. Principio de inclusión-exclusión

En el caso de que A, B no sean disjuntos, $|A \cup B| = |A| + |B| - |A \cap B|$, ya que la intersección ha sido contada dos veces al sumar el cardinal de cada conjunto. Si A, B, C no son disjuntos, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$, ya que al restar las intersecciones dos a dos para subsanar lo comentado anteriormente, estamos eliminando el conteo de la intersección de las tres.

Más generalmente, sean $A_1, A_2, ...A_n$ finitos.

Entonces $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{i,j:1\leq i<j\leq n} |A_i \cap A_j| + \sum_{i,j,k:1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - ... + (-1)^n |\bigcap_{k=1}^{n} A_k|$

(La demostración de esto puede hacerse por inducción. En el ámbito de estos apuntes se toma como cierta.)

3. Funciones

Una vez introducidos los conjuntos, el siguiente paso natural es introducir las *funciones*, que son asociaciones entre los elementos de dos conjuntos. Las funciones son el tema principal de esta sección.

Una función de X en Y (con X, Y conjuntos) se trata de una regla que a cada $x \in X$ le asigna un $y \in Y$ (y solo uno). Si denotamos con f a la función, esto se indica $f : X \mapsto Y$. Por ejemplo, la función $\pi(x)$ asigna a cada x de los reales positivos el número de primos menores que x. Así, $\pi : \mathbb{R}^+ \mapsto \mathbb{N} \cup \{0\}$

- El conjunto X se denomina **dominio** de f. Es una parte intrínseca de la definición de la función, y simplemente mantener la regla de asignación cambiando el dominio da lugar a una función distinta (dado que no conecta los mismos conjuntos).
- Se denomina **imagen** de f al conjunto siguiente: $Im(f) = \{y \in Y : \exists x \in X(f(x) = y)\}$. Es decir, es el conjunto de elementos de Y que pueden ser devueltos por la función.

Por ejemplo, en la función $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2 + 1$, el dominio es $\mathbb{R}$ y la imagen es $[1, \infty)$. La función no es la misma que $f : \mathbb{N} \mapsto \mathbb{R}$ dada por $f(x) = x^2 + 1$ (no conecta los mismos conjuntos).

3.1. Función inyectiva, biyectiva y sobreyectiva

Sea $f : X \mapsto Y$ una función.

- f es **sobreyectiva** si y solo si $Im(f) = Y$ (es decir, todos los elementos de Y se alcanzan partiendo de uno de X)
- f es **inyectiva** si y solo si $\forall x_1, x_2 \in X(x_1 \neq x_2 \implies f(x_1) \neq f(x_2))$ (es decir, cada elemento de Y solo se asocia con uno de X).
- f es **biyectiva** si y solo si es sobreyectiva e inyectiva.

Para demostrar que f es inyectiva, basta con ver $f(x_1) = f(x_2) \implies x_1 = x_2$ (contrapositivo de lo explicado arriba). Para probar f sobreyectiva, como $Im(f) \subset Y$, basta probar $Y \subset Im(f)$, es decir, $\forall y \in Y \exists x \in X$ t.q. $y = f(x)$.

3.2. Gráfico de una función

Sean X, Y conjuntos y $f : X \mapsto Y$ una función. Se define el gráfico de f como $G_f = \{(x, y) : x \in X, y = f(x)\}$.

3.3. Imagen y antiimagen de un conjunto

Definición 3. Sea $f : X \longrightarrow Y$ una función, y $A \subset X$. Se define la **imagen** de A a través de f como $f(A) = \{y \in Y : \exists x \in A \text{ t. q } f(x) = y\}$

Definición 4. Sea $f : X \longrightarrow Y$ una función, y $B \subset Y$. Se define la **imagen inversa o antiimagen** de B a través de f como $f^{-1}(B) = \{x \in X : f(x) \in B\}$

Atención: la notación $f^{-1}(p)$, donde p es un elemento de Y, es una manera de indicar $f^{-1}(\{p\})$. Cuando f es biyectiva, ese conjunto tiene un único elemento, lo que da lugar a una $f^{-1} : Y \mapsto X$ natural.

3.3.1. Propiedades

Las siguientes propiedades generales de funciones pueden ser verificadas fácilmente:

- $f(\emptyset) = \emptyset$
- $A \subset B \implies f(A) \subset f(B)$
- $f(A \cup B) = f(A) \cup f(B)$
  $f(A \cap B) \subset f(A) \cap f(B)$
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
  $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
- $A \subset f^{-1}(f(A))$
  $f(f^{-1}(B)) \subset B$

3.4. Composición de funciones

Dadas $f : X \mapsto Y$ y $g : Y \mapsto Z$, se define su composición $g \circ f : X \mapsto Z$ dada por $(g \circ f)(x) = g(f(x))$.

Por ejemplo, sean $f : \mathbb{R} \mapsto \mathbb{R}, f(x) = x^2 + 1$, $g : \mathbb{R} \mapsto \mathbb{R}, g(x) = cos(x)$, entonces $(f \circ g)(x) = f(g(x)) = f(cos(x)) = cos^2(x) + 1$.

Observación 1. Si g, f son inyectivas, $g \circ f$ lo es.

Si g, f son sobreyectivas $g \circ f$ lo es.

De lo anterior, si g, f son biyectivas, $g \circ f$ lo es.

3.5. Función inversa

Sea $f : X \mapsto Y$ biyectiva. Entonces, para cada $y \in Y$, existe un único $x \in X$ tal que $f(x) = y$. Es decir, podemos establecer una correspondencia entre cada valor de Y y el valor de X cuya imagen es aquel valor.

Se define **función inversa** de f como la aplicación $f^{-1} : Y \mapsto X$ que a cada $y \in Y$ hace corresponder el $x \in X$ tal que $f(x) = y$.

Observación 2. $f(x) = y \iff f^{-1}(y) = x$

3.5.1. Relación entre G_f y $G_{f^{-1}}$

Para la función biyectiva anterior:

Recordemos que $G_f = \{(x, f(x)), x \in X\}$. Además, veamos que $G_{f^{-1}} = \{(f(x), x), x \in X\}$. Entonces, los dos gráficos se diferencian en que el orden de los elementos de cada par es el opuesto. En su representación, el gráfico de una es simétrico respecto a la recta $y = x$ del gráfico de la otra.

3.5.2. Composición con la inversa y la función identidad

Teniendo en cuenta la función biyectiva anterior, consideremos $i_y : Y \mapsto Y$, $i_y(y) = y$, y además $i_x : X \mapsto X$, $i_x(x) = x$. Entonces $f \circ f^{-1} = i_y$, y $f^{-1} \circ f = i_x$.

3.6. Combinatoria de funciones

Sean X e Y conjuntos finitos de cardinales a y b respectivamente.

Observación 3. Hay b^a aplicaciones de X en Y.

Basta con observar que a cada uno de los a elementos de X debemos asociar uno de los b elementos de Y, es decir, tenemos b opciones para un elemento de X, y $b \cdot b \cdot b \cdot ... \cdot b$ (a veces) para los a elementos.

Es útil ver que existe una correspondencia entre aplicaciones de X en Y y maneras de distribuir los elementos de X en los elementos de Y. Así, existen b^a distribuciones de a elementos en otros b elementos.

Observación 4. Hay $\frac{b!}{(b-a)!}$ aplicaciones inyectivas de X en Y.

Esta vez, para el primer elemento de a tenemos b opciones, pero para el segundo no podemos repetir la que ya se ha escogido, de modo que quedan $a-1$, para el siguiente $a-2$... Así, el número de opciones totales para los a elementos es $b \cdot (b-1) \cdot (b-2) \cdot ... \cdot (b-a+1)$, que equivale a la expresión anterior.

Observación 5. Si $a = b = n$, hay $n!$ aplicaciones biyectivas de X en Y.

Es evidente que necesitamos el mismo número de elementos en ambos conjuntos para establecer una correspondencia uno a uno entre elementos. Como las aplicaciones biyectivas son inyectivas, y toda aplicación inyectiva con el mismo número de elementos en su dominio y en su conjunto de llegada es biyectiva, estamos ante el caso particular $a = b$ de la observación 3.

Observación 6. Hay $\binom{b}{a}$ conjuntos imagen posibles para aplicaciones inyectivas de X en Y. De esto sigue que hay $\binom{b}{a}$ subconjuntos posibles de a elementos tomados de uno de b.

Está claro que el tamaño del conjunto imagen de estas funciones es a (son inyectivas). Si restringimos el conjunto de llegada a un conjunto imagen determinado, tenemos $a!$ aplicaciones de X en esa imagen, ya que la función se convierte en biyectiva. Entonces, al haber $\frac{b!}{(b-a)!}$ funciones inyectivas y, sobre cada imagen, $a!$ funciones inyectivas distintas, entonces hay $\frac{b!}{(b-a)!(a!)}$ imágenes posibles, es decir, $\binom{b}{a}$. O sea, del conjunto de b elementos inicial (el conjunto de llegada), podemos tomar $\binom{b}{a}$ subconjuntos de a elementos.

Proposición 1. *Hay* $\sum_{k=0}^{b} (-1)^k \binom{b}{k} (b-k)^a$ *aplicaciones sobreyectivas de* X *en* Y.

El número de aplicaciones sobreyectivas es igual al número de aplicaciones totales menos las no sobreyectivas. Numeremos los elementos del conjunto de llegada con $y_1, y_2, ..., y_b$. Sea $A_i = \{f : y_i \notin f(X)\}$. Entonces, el conjunto de funciones no sobreyectivas es $\bigcup_{k=1}^{b} A_i$. Efectivamente, todas las funciones en ese conjunto carecen de algún elemento de Y en su imagen. Ahora debemos aplicar el principio de inclusión-exclusión, observando que $\sum_{1 \le i_1 < i_2 < ... < i_j \le b} |\bigcap_{k=1}^{j} A_{i_k}| = \binom{b}{j} \cdot (b-j)^a$, porque hay $(b-j)^a$ aplicaciones posibles de X en Y que no contengan j elementos prefijados del conjunto de llegada en su imagen, y $\binom{b}{j}$ maneras de prefijar esos elementos. Una vez aplicado el principio de inclusión-exclusión, y restado el resultado al número de aplicaciones totales, b^a, se obtiene la expresión del enunciado.

3.7. Principio del palomar

Una interesante pero potente observación es que si un conjunto A tiene más elementos que otro B y tratamos de distribuir los elementos del primero sobre el segundo, habrá elementos del segundo con más de un elemento de A. Esto se conoce como **principio del palomar**.

Proposición 2. *Sean* X *e* Y *conjuntos finitos de cardinales* a *y* b *respectivamente. Si* $a > b$, $f : X \mapsto Y$ *no puede ser inyectiva. Es decir,* $\exists y \in Y$ *t.q.* $|f^{-1}(\{y\})| \ge 2$.

Por ejemplo: Se tienen los números $1, 2, 3, ..., 2n$. Se escogen $n + 1$ de ellos. Hay dos números a y b entre los escogidos tales que a divide a b.

Para demostrarlo, veamos que si $x_1, x_2, ...x_{n+1}$ son los números escogidos, podemos escribirlos de la forma $x_j = 2^{m_j} \cdot a_j$, donde a_j es un impar, que además se halla entre 1 y $2n$. En ese conjunto hay n impares, pero tenemos $n + 1$ impares $a_1, a_2, ...a_j$, de modo que al menos dos de los a_j son iguales. Esto se traduce en que hay dos x_j con el mismo factor, de modo que uno divide al otro.

4. Relaciones de orden

Otro elemento básico de la teoría de conjuntos es el **orden**: la noción de establecer relaciones entre los elementos de un conjunto para enriquecer su estructura. En esta sección se estudian los conceptos básicos sobre este tema.

Sea X un conjunto. Una **relación de orden** en X es un subconjunto R de $X \times X$ que cumple:

- $(a, a) \in R$ (Propiedad reflexiva)
- $(a, b) \in R$ y $(b, a) \in R \implies a = b$ (Propiedad antisimétrica)
- $(a, b) \in R$ y $(b, c) \in R \implies (a, c) \in R$. (Propiedad transitiva)

Cuando $(a, b) \in R$, se denota por aRb o $a \preceq b$.

Ejemplos de estas relaciones son $\geq$ en $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Z}$..., $|$ (divide a) en $\mathbb{N}$, $\subset$ en $\mathcal{P}(X)$...

Sea cual sea X, un ejemplo de relación de orden es la trivial $R = \{(a, a) : a \in X\}$.

Definición 5. Sea X y un conjunto y R una relación de orden en ese conjunto. R es una **relación de orden total** si $\forall a, b \in X$, o bien aRb o bien bRa.

Por ejemplo, $\leq$ en $\mathbb{N}$ es de orden total, pero $|$ no, puesto que por ejemplo 3 y 7 no se relacionan.

Un conjunto **ordenado** es aquel con una relación de orden. Si es total, se dice que el conjunto es **totalmente ordenado**.

Observación 7. Si X es un conjunto ordenado por la relación $\mathcal{R}$, entonces esa relación también es de orden en $Y \subset X$.

En efecto, si $\mathcal{R}$ es relación de X, como las tres propiedades se cumplen para cualesquiera elementos de X, y todo elemento de Y está en X, también se cumplen para elementos de Y.

4.1. Máximo, mínimo, maximal y minimal

Sea X un conjunto ordenado por la relación $\preceq$, y sea $A \subset X$.

- Se dice que $a \in A$ es **máximo** de A si $\forall b \in A, b \preceq a$. Si existe máximo, es único. (Por la propiedad antisimétrica).
- Se dice que $a \in A$ es **mínimo** de A si $\forall b \in A, a \preceq b$. Si existe mínimo, es único. (Por la propiedad antisimétrica).
- Se dice que $a \in A$ es **elemento maximal** de A si $\nexists b \in A$ t.q. $a \preceq b$ y $a \neq b$.
- Se dice que $a \in A$ es **elemento minimal** de A si $\nexists b \in A$ t.q. $b \preceq A$ y $a \neq b$.

Por ejemplo, consideremos el conjunto $\mathbb{R}$, la relación $\leq$ y el siguiente subconjunto $A = \{x \in R : 0 \leq x < 2\}$. El 0 es mínimo puesto que por la definición del conjunto, $0 \leq x \ \forall x \in A$. Se puede demostrar que no existe máximo, puesto que $\forall a \in A \ \exists b \in A$, $b = \frac{a+2}{2}$ t.q. $a < b$. Efectivamente, si $a \geq b$, se tiene $a \geq \frac{a+2}{2} \implies a \geq 2$ contradiciendo $a \in A$.

Si consideramos $\mathbb{N}$, la relación 'divide a' ($|$), y el subconjunto $A = \{2, 5, 6, 10, 12, 30\}$, veremos que no hay máximo, puesto que $\forall a \in A$, si $a \neq 30$, entonces $30|a$ no se cumple, y si $a = 30$, $12|a$ no se cumple. Sin embargo, 30 es elemento maximal, puesto que no hay otro elemento $b \in A$ tal que $30|b$.

Una forma de visualizar esto es realizar un **grafo dirigido** con vértices los elementos del conjunto, y aristas que van desde a hasta b si aRb. Aquel vértice m al que no lleguen flechas será minimal, pues no habrá casos en los que aRm para algún a, y aquel del que no partan flechas será maximal.

Observemos que en esta relación (| en $\mathbb{N}$), el 1 es mínimo en todo subconjunto $A \subset \mathbb{N}$ que lo contenga, y si un conjunto no contiene al 1, los primos son minimales, y el menor número de acuerdo al orden habitual ($\leq$) sera mínimo.

Observación 8. En un conjunto ordenado, un máximo es además elemento maximal, y un mínimo es elemento minimal. Además, si el orden es total, todo minimal es mínimo y todo maximal es máximo.

Es decir, en orden total, máximo y maximal coinciden, así como mínimo y minimal. Vamos a probarlo para maximales y máximos. Efectivamente, si M es máximo, como $\forall a \in A$, $a \preceq M$, entonces está claro que $\nexists a \neq M$ t.q. $M \preceq a$, ya que en ese caso, por la propiedad antisimétrica, tendríamos que $M = a$. Si el orden es total, y M' es maximal, tenemos que $\nexists a \neq M'$ t.q. $M' \preceq a$, es decir, $\forall a \in A$, $\neg(M' \preceq a)$, y al ser el orden total, $a \preceq M'$, luego también es máximo.

4.2. Cotas, supremo e ínfimo

Sea $(X, \preceq)$ un conjunto ordenado y $A \subset X$.

Definición 6. $x \in X$ es **cota superior** de A en X si y solo si $\forall a \in A$, se verifica $a \preceq x$.

Definición 7. $x \in X$ es **cota inferior** de A en X si y solo si $\forall a \in A$, se verifica $x \preceq a$.

Definición 8. $s \in X$ es **supremo** de A si y solo si s es cota superior de A, y $\forall y \in X$ t.q. y es cota superior de A, se tiene $s \preceq y$. El supremo, si existe, es único. También se conoce como çota superior mínima". Se denota por $\sup(A)$.

Definición 9. $i \in X$ es **ínfimo** de A si y solo si i es cota inferior de A, y $\forall y \in X$ t.q. y es cota inferior de A, se tiene $y \preceq i$. El ínfimo, si existe, es único. También se conoce como çota inferior máxima". Se denota por $\text{ínf}(A)$.

Por ejemplo, en $\mathbb{R}$ con el orden habitual, el conjunto $A = \{\frac{1}{n} : n \in \mathbb{N}\}$ tiene máximo 1, supremo 1, ínfimo 0 y no tiene mínimo.

En $\mathbb{N}$ con el orden |, el conjunto $A = \{2, 5, 6, 10, 12, 30\}$ tiene ínfimo 1, puesto que la única cota inferior del conjunto es 1 (el único valor $b \in \mathbb{N}$ tal que $\forall a \in A$, se tiene $b|a$ es 1). Además, tiene supremo 60, ya que las cotas superiores del conjunto son los múltiplos de 60, que es múltiplo de todos ellos, y 60 divide a todos sus múltiplos luego es el 'menor' en este orden.

4.2.1. Buen orden

Definición 10. Se dice que una relación de orden $\mathcal{R}$ en X es un **buen orden** si y solo si para todo subconjunto de X, existe un mínimo con ese orden. Es decir, $\forall A \subset X$, $\exists a \in A$ t.q. $a \preceq b$ $\forall b \in A$.

Por ejemplo, el orden habitual $\leq$ en $\mathbb{N}$ es buen orden, pero no lo es en $\mathbb{Z}$ o $\mathbb{R}$, ya que en el primero el conjunto no está acotado inferiormente, de modo que no tiene mínimo, y en el segundo, además de esto, existen multitud de conjuntos acotados sin mínimo, como $A = \{\frac{1}{n} : n \in \mathbb{N}\}$.

5. Relaciones de equivalencia

Otro tipo de relaciones naturales son las de equivalencia. La importancia de las relaciones de equivalencia (extensión de la relación de igualdad, $=$) es que permiten generar nuevos conjuntos *agrupando* elementos que son *equivalentes*. El conjunto de *agrupaciones* resultante es el nuevo conjunto (llamado *cociente*). Antes, vamos a definir, en general, lo que es una relación:

Definición 11. Una **relación** en un conjunto X es un conjunto $R \subset X \times X$.

Si $(a, b) \in R$, se dice que «a se relaciona con b», o aRb.

Ya conocemos la relaciones de orden, que son aquellas que verifican las propiedades transitiva, antisimétrica y reflexiva. Otro ejemplo de relaciones son las funciones usuales $f : X \mapsto X$, que deben cumplir ciertas propiedades, como $aRb \wedge aRb_1 \implies b = b_1$, o $\forall a \in X$, $\exists b \in X$ t.q. aRb.

Definición 12. Una relación R en X es **relación de equivalencia** en X si cumple las siguientes propiedades:

- Reflexiva. $aRa \ \forall a \in X$
- Simétrica. $aRb \implies bRa \ \forall a, b \in X$
- Transitiva. $aRb \wedge bRc \implies aRc \ \forall a, b, c \in X$

Por ejemplo, la siguiente relación en $\mathbb{R}$ es de equivalencia: $aRb \iff a - b \in \mathbb{Z}$. Veamos que efectivamente, si $a, b, c \in \mathbb{R}$, $aRa \implies a - a = 0 \in \mathbb{Z}$, lo cual es cierto, $aRb \implies a - b \in \mathbb{Z} \implies (-1)(a-b) = b - a \in \mathbb{Z} \implies bRa$, y además $aRb \wedge bRc \implies a - b \in \mathbb{Z} \wedge b - c \in \mathbb{Z} \implies (a-b) + (b-c) = a - c \in \mathbb{Z} \implies aRc$.

5.1. Clases de equivalencia

Definición 13. Sea X un conjunto con una relación $\mathcal{R}$ de equivalencia. Dado $x \in X$, su clase de equivalencia se define: $[x] := y \in X : xRy$. x se conoce como *representante* de la clase.

Tiene las siguientes propiedades:

- $xRy \implies [x] = [y]$
- $[x] \cap [y] \neq \emptyset \implies [x] = [y]$
- $xRy \iff [x] = [y] \iff [x] \cap [y] \neq \emptyset$

Que se pueden demostrar de manera sencilla. Por ejemplo, para la primera, $z \in [x] \iff xRz \iff yRz \iff z \in [y]$. (A causa de las propiedades simétrica, transitiva, y la condición xRy).

Estas propiedades indican que dos clases de equivalencia, o son disjuntas, o son la misma, y la unión de todas es X, luego constituyen **particiones** de X. La relación de equivalencia *trocea* el conjunto en distintas *agrupaciones* de elementos equivalentes.

En general se escoge un representante significativo para cada clase. Por ejemplo, en la relación descrita con anterioridad (En $\mathbb{R}$, con $aRb \iff a - b \in \mathbb{Z}$), dos elementos son equivalentes si y solo si su parte decimal es la misma, de modo que podemos escoger el representante de la clase de equivalencia como un número en $[0, 1)$, que tenga la misma parte decimal que los de esa clase.

5.2. Congruencia módulo m

Vamos a definir una útil relación de equivalencia en $\mathbb{Z}$, prefijado un $m \in \mathbb{N}$. Se define: $aRb \iff m|b-a \iff \exists k \in \mathbb{Z}$ tal que $b-a=mk \iff b=a+mk$.

Es decir, equivalen si su resto al dividir por m es el mismo. Veamos que se trata de una relación de equivalencia, pues $aRa \iff m|0 \iff \exists k$ tal que $0=km$ lo que se verifica con $k=0$. Además, si se tiene $aRb \implies b=a+km \implies a=b-km \implies m|a-b \implies bRa$. Por último, $aRb \wedge bRc \implies b=km+a \wedge c=lm+b$, de modo que $c=(l+k)m+a \implies aRc$.

Esta relación se denota $a \equiv b \mod m$, y se lee «a es congruente con b módulo m». Las clases de equivalencia son $[a]=\{mk+a : k \in \mathbb{Z}\}$. Así, el conjunto de clases de equivalencia es $\{[0],[1],[2],...[m-1]\}$, dado que cualquier otro número entra en alguna de las clases de estos números. Por ejemplo, $m+7 \in [7]$ dado que es un número de la forma $mk+7$. Los representantes habituales de las clases son, como se ha comentado antes, los restos de dividir por m los valores de cada clase.

Esto da lugar a una serie de propiedades, conocidas como **aritmética modular**, muy sencillas de probar teniendo en cuenta la definición de la relación. Estas son:

Sean $a,b,c,d \in \mathbb{Z}$ y $m \in \mathbb{N}$ tales que $a \equiv b \mod m$ y $c \equiv d \mod m$

- $a+c \equiv b+d \mod m$
- $ac \equiv bd \mod m$

5.3. Particiones de un conjunto

Definición 14. Una **partición** de X es una familia de subconjuntos $A_i \subset X$, $\{A_i\}_{i\in I}$ donde I es el conjunto de índices, tal que:

- $\forall i \in I$, $A_i \neq \emptyset$ (No vacíos)
- $\forall i,j \in I$, $A_i \cap A_j = \emptyset$ (Disjuntos entre sí)
- $\bigcup_{i\in I} A_i = X$ (Su unión es el total)

Además, como es un conjunto de subconjuntos de X, tenemos que $\{A_i\}_{i\in I} \subset \mathcal{P}(X)$.

Está claro que cada elemento de X pertenece a alguna de las particiones, puesto que está en la unión de todas ellas. Además pertenece solo a una de ellas, puesto que de pertenecer a dos de ellas no serían disjuntas.

Un ejemplo de partición, de $\mathbb{R}^2$ es el conjunto de rectas verticales que pasan por un determinado punto del eje X, es decir, $\{A_r\}_{r\in\mathbb{R}}$ donde $A_r=\{(r,y) : y \in \mathbb{R}\}$.

5.3.1. Equivalencia entre particiones de un conjunto y relaciones de equivalencia

Vamos a comprobar que una relación de equivalencia equivale a una partición. Es decir:

Observación 9. Sea $\{A_i\}_{i\in I}$ una partición de X. Si definimos en X la relación $xRy \iff \exists j \in I$ tal que $x,y \in A_j$, entonces:

1. R es una relación de equivalencia en X.
2. Las clases de equivalencia de R son cada una de las particiones A_i.

Demostración. R cumple la propiedad reflexiva, dado que $xRx \implies \exists j$ tal que $x \in A_j$, y como sabemos que $\bigcup_{i\in I} A_i = X$, esto es cierto. También cumple la simétrica: $xRy \implies \exists j$ tal que $x,y \in A_j$, luego

también yRx. La transitiva también se cumple: $xRy \wedge yRz \implies \exists j_1, j_2$ tales que $x, y \in A_{j_1}$ y $y, z \in A_{j_2}$, y puesto que los conjuntos de la partición son disjuntos dos a dos, $j_1 = j_2 = j$ (en caso contrario no lo serían porque y estaría en dos conjuntos distintos de la partición), de modo que $x, y, z \in A_j \implies xRz$.

Para demostrar 2, vamos a ver que las clases de equivalencia forman una partición. Sean $x, y \in X$, no relacionados, es decir, sus clases de equivalencia son distintas. Supongamos $[x] \cap [y] \neq \emptyset$, es decir, que no son disjuntas. Entonces, sea $c \in [x] \cap [y]$. $cRx \wedge cRy \implies xRy$, llegando a una contradicción. Por tanto, dos clases distintas son disjuntas. Además, la unión de todas las clases es el total, es decir $\forall x \in X$, $\exists [x]$ tal que $x \in [x]$, lo que es evidente porque es su propia clase y debe darse xRx. Como cada clase de equivalencia la podemos definir como «elementos que pertenecen a una misma A_j», hay una clara biyección entre cada clase y el A_j al que pertenecen todos los de la clase. □

5.4. Conjunto cociente

Dado X y una relación de equivalencia $\mathcal{R}$:

Definición 15. Se define el **conjunto cociente** $(X/\mathcal{R})$ como el conjunto cuyos elementos son las clases de equivalencia de los elementos de X con la relación $\mathcal{R}$.

En algunos casos particulares existen notaciones específicas para el conjunto cociente. Por ejemplo, en la relación $xRy \iff x - y \in \mathbb{Z}$ de $\mathbb{R}$, el conjunto cociente se suele escribir $\mathbb{R}/\mathbb{Z}$, y lo podemos describir como $\mathbb{R}/\mathbb{Z} = \{[r] : 0 \leq r < 1\}$, escogiendo como representante de cada clase la parte decimal de los miembros de la misma. También, en la congruencia módulo m, se expresa el conjunto cociente como $\mathbb{Z}_m$, y como ya se vio con anterioridad, $\mathbb{Z}_m = \{[x]_m : 0 \leq x < m, x \in \mathbb{Z}\}$.

5.4.1. Funciones en el conjunto cociente

Al intentar definir funciones en X/R como *reglas* aplicadas en sus representantes, se debe comprobar que la función definida no dependa del representante escogido en cada clase, puesto que este no es único. Para ilustrar esta idea, intentemos definir funciones sobre $\mathbb{R}/\mathbb{Z}$:

1. $f : \mathbb{R}/\mathbb{Z} \mapsto \mathbb{R}$, $f([x]) = x^2$. Está mal definida, puesto que una misma clase tiene varias imágenes. Efectivamente, $[0] = [7]$, pero si aplicamos la regla que hemos escrito para f obtenemos tanto 0 como 49, luego la función no está bien definida.

2. $f : \mathbb{R}/\mathbb{Z} \mapsto \mathbb{R}$, $f([x]) = x^2$ con $0 \leq x < 1$. Está bien definida, puesto que estamos eligiendo solo los representantes en $[0, 1)$, que abarcan todas las clases del conjunto cociente pero no repiten clase dando lugar a imágenes dobles.

3. $f : \mathbb{R}/\mathbb{Z} \mapsto \mathbb{R}^2$, $f([x]) = (\cos(2\pi x), \sin(2\pi x))$. Está bien definida, porque como el periodo de cada una de estas funciones trigonométricas es 2π, no dependen del representante tomado. Puesto que en esta relación, los miembros de una clase $[x]$ son todos los reales de la forma $x + k, k \in \mathbb{Z}$, tomemos el que tomemos como reprsentante, obtenemos $(\cos(2\pi(x+k)), \sin(2\pi(x+k))) = (\cos(2\pi x), \sin(2\pi x))$, es decir, un mismo resultado siempre. Esta función tiene particular interés, dado que a cada clase de equivalencia le asigna un punto distinto de la circunferencia de radio 1, de manera biyectiva (los ángulos van entre 0 y 2π, sin incluir este último y sin repetir). De algún modo, el conjunto $\mathbb{R}/\mathbb{Z}$ es equivalente a una circunferencia.

6. Cardinales y numerabilidad

En esta sección nos centramos en la cantidad de elementos que tiene un conjunto. Cuando este es finito no hay mucho problema, pero es interesante observar cómo se comportan los distintos tipos de conjunto infinito.

Definición 16. Dos conjuntos A y B son **equipotentes** (tienen el mismo cardinal) $\iff \exists f : A \mapsto B$, con f biyectiva.

Por ejemplo, son equipotentes $\mathbb{N}$ y $2\mathbb{N}$, donde $2\mathbb{N}$ es el conjunto de naturales múltiplos de 2. La biyección es $f : \mathbb{N} \mapsto 2\mathbb{N}$ dada por $f(n) = 2n$. Asimismo, son equipotentes $\mathbb{N}$ y $\mathbb{Z}$, con la función dada por $f(2n) = n$, con $n \geq 1$, $f(1) = 0$ y $f(2n+1) = -n$ con $n \geq 1$.

Observación 10. «Ser equipotentes» es una relación de equivalencia.

Razón. La propiedad reflexiva se cumple, puesto que la biyección $f : A \mapsto A$ con $f(a) = a$ asegura que A es equipotente con A. Para la simétrica, $ARB \implies \exists f : A \mapsto B$ biyectiva, luego $f^{-1} : B \mapsto A$, la inversa, es biyectiva, de modo que BRA. Finalmente, $ARB \wedge BRC \implies \exists f : A \mapsto B$, $g : B \mapsto C$ biyectivas, luego $g \circ f : A \mapsto C$ es biyectiva así que ARC.

Las clases de equivalencia de esta relación las denominamos **cardinales** (generalización del concepto «número de elementos del conjunto» en conjuntos finitos), de modo que A y B son equipotentes $\iff$ $card(A) = card(B)$, es decir, si su clase de equivalencia bajo esa relación (cardinal) es la misma (en otras palabras, si son equipotentes).

Definición 17. Un conjunto $A \neq \emptyset$ es finito si y solo si $\exists n$ tal que hay una $f : \{1, 2, 3, ..., n\} \mapsto A$ biyectiva. n es el número de elementos, único para ese conjunto, y los elementos pueden escribirse $A = \{a_1, a_2, ...a_n\}$ con los a_i distintos. Por definición, $\emptyset$ es finito y de 0 elementos.

6.1. Conjuntos infinitos y numerables

Definición 18. Un conjunto es **infinito** $\iff$ no es finito. Un conjunto A es **numerable** si es equipotente con $\mathbb{N}$, es decir, si $card(A) = card(\mathbb{N})$, luego $\exists f : \mathbb{N} \mapsto A$ biyectiva.

Por ejemplo, como se vio antes, $2\mathbb{N}$ y $\mathbb{Z}$ son numerables.

Proposición 3. *$\mathbb{N} \times \mathbb{N}$ es numerable, y por tanto lo es $A \times B$ si A y B lo son.*

Se puede describir una biyección entre pares de naturales con los naturales, si se cuentan de esta forma: $(1,1), (1,2), (2,2), (2,1), (1,3), (2,3), (3,3), (3,2), (3,1), ...$, es decir, tomando en orden cada diagonal en la representación gráfica de los puntos de $\mathbb{N} \times \mathbb{N}$ como rejilla. Ahora, si A, B son numerables, $\exists f : \mathbb{N} \mapsto A$, $g : \mathbb{N} \mapsto B$ biyectivas, y entonces la siguiente función $h : \mathbb{N} \times \mathbb{N} \mapsto A \times B$, definida por $h(n, m) \mapsto (f(n), g(m))$, es biyectiva, y como $\mathbb{N} \times \mathbb{N}$ es numerable, lo es $A \times B$.

Proposición 4. *Si $B \subset \mathbb{N}$ es infinito, es numerable. Asimismo, si A es numerable y $C \subset A$ es infinito, es numerable.*

Para comprobarlo, vamos a numerar B. Como B es infinito, sabemos que $B \neq \emptyset$, y al ser un subconjunto de $\mathbb{N}$, que se trata de un buen orden, podemos tomar $b_1 = min(B)$. De hecho, seguiremos tomando elementos de esta forma: $b_{n+1} = min(B \backslash \{b_1, b_2, b_3...b_n\})$. Sabemos que este mínimo existe porque $B \backslash \{b_1, b_2, b_3...b_n\} \neq \emptyset$ ya que en caso contrario $B = \{b_1, b_2, ..., b_n\}$ y sería finito. Hemos definido recursivamente una sucesión $\{b_n\}_{n \in \mathbb{N}}$ que se trata de la función entre $\mathbb{N}$ y B buscada. Queda probar que dicha función es sobreyectiva (está claro que es inyectiva por la forma en que hemos tomado los elementos). Para ello, supongamos que hay algún $b \in B$ tal que $\nexists m \in \mathbb{N}$ t.q. $b_m = b$. Entonces el conjunto

F de los b de estas características es no vacío. Sea $a = min(F)$, y $j = max(\{n \in \mathbb{N} : b_n < a\})$. Pero entonces, el paso $j \to j+1$ de la recurrencia se debe tomar a para b_n, dado que todos los menores que él han sido tomados ya. Entonces, $a \notin F$ contradiciendo que es mínimo.

Proposición 5. $\mathbb{Q}$ *es numerable.*

Para demostrarlo, comprobaremos que si $q \in \mathbb{Q}$, entonces $\exists! a_q \in \mathbb{Z}$ y $\exists! b_q \in \mathbb{N}$ tales que $q = \frac{a_q}{b_q}$ con ambos coprimos. Sea $f : \mathbb{Q} \mapsto \mathbb{Z} \times \mathbb{Z}$, de manera que $f(q) = (a_n, b_n)$. f es inyectiva, dado que si $f(q) = f(q')$, es porque $(a_q, b_q) = (a_{q'}, b_{q'})$, de donde se tiene que $\frac{a_q}{b_q} = \frac{a_{q'}}{b_{q'}} \implies q = q'$. Entonces, $f : \mathbb{Q} \mapsto f(\mathbb{Q})$ es biyectiva. Sabemos que $f(\mathbb{Q}) \subset \mathbb{Z} \times \mathbb{Z}$ no es finito porque no lo es, por ejemplo $\{(n, 1) : n \in \mathbb{N}\} \subset f(\mathbb{Q})$. Como, por lo visto anteriormente, $\mathbb{Z} \times \mathbb{Z}$ es numerable, ocurre que $f(\mathbb{Q})$ es numerable, luego debe serlo $\mathbb{Q}$.

Proposición 6. $\mathbb{R}$ *no es numerable.*

Demostración. Primero supongamos que $[0, 1)$ es numerable. Cualquier $x \in [0, 1)$ se puede representar decimalmente como $0.x_1x_2x_3x_4...$, para que $x = \sum_{i=1}^{\infty} \frac{x_i}{10^i}$. Tomaremos dicha representación en su forma terminada en 0s en caso de ambigüedad (por ejemplo, en lugar del 0,23999999.. tomaremos el 0,240000....). Como hemos dicho que se pueden numerar, denotaremos x^j al j-ésimo término de la numeración. Ahora podemos formar un elemento que no está en la numeración, contradiciendo que sea numerable. Sea $r_n = 1$ si $x_n^n \neq 1$, y $r_n = 2$ en caso contrario. Entonces, el número $r = r_1r_2r_3... = \sum_{i=1}^{\infty} \frac{r_i}{10^i}$ no está en la numeración, puesto que para cada término n de la numeración, su n-ésimo decimal difiere con el n-ésimo decimal de r, luego no hay ninguno igual que él. Esto se conoce como **proceso diagonal de Cantor**. Como $[0, 1) \subset \mathbb{R}$, y todo subconjunto infinito de uno numerable ha de ser numerable, deducimos que $\mathbb{R}$ no es numerable.

6.2. Orden del cardinal

En el conjunto de las clases de equivalencia de la relación de equipotencia (es decir, el de los cardinales), definimos la siguiente relación:

Definición 19. Sean A, B conjuntos. $card(A) \preceq_c card(B) \iff \exists f : A \mapsto B$ con f inyectiva.

Obsérvese que la relación no depende del representante elegido, puesto que si tomamos otro (sea C equipotente a A), se sigue teniendo $card(C) \preceq_c card(B)$ dado que podemos componer la biyectiva entre C y A con la inyectiva f para dar lugar a una inyectiva de C a B.

Proposición 7. $\preceq_c$ *es relación de orden.*

Las propiedades transitiva y reflexiva se comprueban fácilmente. La propiedad antisimétrica, esto es, dados A, B con $f : A \mapsto B$ inyectiva y $g : B \mapsto A$ inyectiva, se tiene que existe $h : A \mapsto B$ biyectiva, se conoce como **teorema de Cantor-Bernstein**, y aquí, por el momento, se admite sin demostración.

Este teorema se puede probar, en su caso principal, ($B \subset A$, $f : A \mapsto B$ inyectiva (la de B a A es la inclusión)), considerando $D_1 := A \backslash B$, $D_{n+1} = f(D_n)$ si $n \geq 1$ y $C = B \backslash \bigcup_{n \geq 2} D_n$, observando que los D_n son disjuntos y no vacíos, y definiendo $h : A \mapsto B$ como $h(c) = c$ si $c \in C$, y $h(d) = f(d)$ si $d \in \bigcup_{n \geq 1} D_n$. h es biyectiva.

Proposición 8. *Una unión finita de conjuntos finitos es finita. Una unión numerable de conjuntos numerables es numerable.*

Vamos a ver por qué se cumple lo segundo, que es el caso menos trivial. Tenemos una familia de conjuntos $\{A_i\}_{i\in I}$, todos ellos numerables, con I numerable. Entonces lo que se afirma es que $\bigcup_{i\in I} A_i$ es numerable. Vamos a suponer $I = \mathbb{N}$ puesto que como es numerable podemos transformarlo en $\mathbb{N}$ a través de la biyección correspondiente. Sea entonces B la unión que estamos considerando. Veamos que $A_1 \subset B$ y A_1 numerable, luego $card(A_1) \preceq_c card(B)$. Ahora veremos que $card(B) \preceq_c card(A_1) = card(\mathbb{N}) = card(\mathbb{N}^2)$. Para ello construiremos $f : B \mapsto \mathbb{N}^2$ inyectiva. Sabemos que $\forall A_n, \exists g_n : A_n \mapsto \mathbb{N}$, todas ellas biyectivas. Supongamos que los A_n son disjuntos todos entre sí. Sea $f : B \mapsto \mathbb{N}^2$ la definida por $b \mapsto f(b) = (n, g_n(b))$, es decir, a cada elemento de b se asigna el índice del conjunto al que pertenece y su imagen a través de la g_n biyectiva del mismo. Es fácil ver que f es inyectiva.

Para el caso general, en el que los A_n no tienen porque ser disjuntos, haremos f de esta forma: $b \mapsto (min(B'), g_{min(B')}(b))$, donde B' es el conjunto de los índices de los A_n a los que pertenece b, evidentemente no vacíos puesto que b pertenece a alguno, lo que asegura la existencia de mínimo por el buen orden. □

Lema 1. *El cardinal de cualquier intervalo de $\mathbb{R}$ es igual al cardinal de $\mathbb{R}$. Por ejemplo, $card([0,1]) = card(\mathbb{R})$.*

Demostración. Usaremos el teorema de Cantor-Bernstein. En primer lugar, está claro que $card([0,1]) \leq card(\mathbb{R})$ puesto que la función de inclusión $x \mapsto x$ entre esos conjuntos es inyectiva. Ahora veremos que $card(\mathbb{R}) \leq card([0,1])$. La función inyectiva entre esos dos conjuntos es, por ejemplo, una sigmoide: $f(x) = \frac{1}{1+e^x}$.

Proposición 9. *$card(\mathcal{P}(\mathbb{N})) = card(\mathbb{R})$.*

Para probar $\leq$, la función inyectiva es: $A \mapsto 0.a_1a_2a_3a_4...$ donde cada decimal a_n es 1 si $n \in A$, o 0 si no (por ejemplo). Para probar $\geq$, podemos hacer que la función inyectiva sea de $[0,1)$ en las partes de $\mathbb{N}$, de acuerdo con el lema anterior. Entonces, la función será: $x \mapsto A$, donde si el desarrollo decimal de x es $x = 0.x_1x_2x_3...$ con la periodicidad en 0 si hay ambigüedad entre 0 o 9, entonces $A = \{x_n + 10^n : n \in \mathbb{N}\}$.

Observación 11. $card(A) < card(\mathbb{N}) < card(\mathbb{R})$, donde A es un conjunto finito.

La **hipótesis del continuo** indica que no existe un conjunto B cuyo cardinal esté entre el de $\mathbb{N}$ y el de $\mathbb{R}$. Se ha demostrado que esta afirmación es indecidible y su veracidad o falsedad no altera la consistencia de la teoría de conjuntos.

Proposición 10. *Sea cual sea X, $card(X) < card(\mathcal{P}(X))$.*

Se probará primero que $X \leq card(\mathcal{P}(X))$. La función inyectiva puede ser esta: $x \mapsto \{x\}$. Ahora se va a ver que $X \neq card(\mathcal{P}(X))$. Supongamos el caso contrario, entonces existe $f : X \mapsto \mathcal{P}(X)$ biyectiva. Se define $B = \{x \in X : x \notin f(x)\}$. Como f es sobreyectiva, y B es subconjunto de X, $\exists b \in X$ tal que $f(b) = B$. Ahora tenemos las siguientes equivalencias: $b \in B \iff b \notin f(b) \iff b \notin B$, contradictorias. Por tanto, no existe tal biyección.

Proposición 11. *Sean A, B conjuntos. Se tiene que si $\exists f : A \mapsto B$ sobreyectiva, $card(A) \geq card(B)$.*

Hay que encontrar $g : B \mapsto A$ inyectiva. Podemos hacer que $g(b) = a_b \in f^{-1}(\{b\})$, donde a_b es un elemento arbitrario de ese conjunto, puesto que sabemos que f es sobreyectiva así que las imágenes inversas de cada elemento de b son no vacías. Es inyectiva, porque si $g(c) = g(b) \implies a_c = a_b \implies f(a_c) = f(a_b) \implies c = b$.

Se ha usado el **axioma de elección**, por el cual se puede formar un nuevo conjunto a partir de una familia de conjuntos, tomando un elemento arbitrario de cada uno de ellos.

7. Números naturales y enteros

En esta sección se discuten conceptos básicos acerca de los números naturales ($\mathbb{N} = \{1, 2, \ldots\}$) y los enteros ($\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$).

7.1. Los naturales

Divisibilidad. La relación $a|b$, que indica que a divide a b, tiene lugar si y solo si $\exists m \in \mathbb{N}$ tal que $b = a \cdot m$. Es relación de orden, y cumple que si $n|a$ y $n|b$, entonces $n|a + b$ y si $n|a$, $n|ab$. Asimismo, si $n|a$ y $n|a + b$, se verifica que $n|b$.

Números primos y compuestos. p es primo si y solo si sus únicos divisores son 1 y p, y además $p \neq 1$. c es compuesto si y solo si no es primo y $c \neq 1$. Esto es, $\exists m, n \in \mathbb{N}$, $m, n \neq 1$, tales que $mn = c$.

Para hallar los primos hasta un límite n, se puede usar el algoritmo conocido como **criba de eratóstenes**, que consiste en listar los números del 2 al n, tomar el primero como primo, eliminar sus múltiplos de la lista, tomar el siguiente no tachado como primo e iterar hasta pasar el elemento $\sqrt{n}$, a partir del cual todos los elementos no eliminados son primos. (Puesto que de ser $n' \leq n$ compuesto, alguno de sus divisores ha de ser menor o igual que $\sqrt{n}$, en caso contrario, $n' > \sqrt{n} \cdot \sqrt{n} = n$, contradictorio).

MCD y MCM. El MCD (máximo común divisor) de un conjunto $A \in \mathbb{N}$ no vacío de números es el máximo del conjunto de divisores comunes a todos los elementos de A. Podemos asegurar que dicho máximo existe, porque ese conjunto es no vacío (tiene al 1) y es finito ya que hay a lo sumo mín A divisores comunes. Así, debe tener máximo.

El MCM (mínimo común múltiplo) de un conjunto A no vacío es el mínimo del conjunto de múltiplos comunes. Podemos asegurar que existe, porque $\prod_{a \in A} a$ es múltiplo común, así que el conjunto de múltiplos comunes es no vacío y por el buen orden existe.

Veremos el **algoritmo de euclides** para hallar el MCD de dos números. Primero, es necesario conocer el siguiente resultado básico:

Proposición 12 (División euclídea)**.** *Sean $a, b \in \mathbb{N}$. Se tiene que $\exists c, r \in \mathbb{N} \cup \{0\}$ tales que $b = ac + r$, con $0 \leq r < a$.*

El algoritmo de Euclides es el siguiente. Sean $a, b \in \mathbb{N}$ y $b > a$ sin perder en generalidad. Para hallar $mcd(a, b)$:

1. En primer lugar, sean $r_0 = b, r_1 = a$. $\exists c_1, r_2$ tales que $r_0 = r_1 c_1 + r_2$, con $0 \leq r_2 < r_1 < r_0$.
2. Si tenemos m números con $0 \leq r_m < r_{m-1} < \ldots < r_2 < r_1 < r_0$, construimos el siguiente por división euclídea: $r_{m-1} = c_m r_m + r_{m+1}$, y se tiene $0 \leq r_{m+1} < r_m$.
3. El algoritmo se detiene cuando se encuentra $r_t = 0$. En ese caso, r_{t-1} es el mcd buscado. El algoritmo siempre se detiene dado que para cualquier r_j se tiene que el siguiente es menor en 1 por lo menos, así que se llegará eventualmente al 0.

Demostración. En cada paso, $r_{i-1} = c_i r_i + r_{i+1}$, se tiene que $mcd(r_{i-1}, r_i) = mcd(r_i, r_{i+1})$, porque si $n|r_{i+1}$ y $n|r_i$, se tiene de las propiedades de la divisibilidad que $n|r_{i-1}$, e igualmente, si $n|r_{i-1}$ y $n|r_i$, entonces $n|r_{i+1}$. Es decir, que los divisores comunes a dos restos consecutivos son los mismos. Entonces, $mcd(a, b) = mcd(r_{t-2}, r_{t-1})$, y como $r_{t-2} = c_{t-1} r_{t-1} + 0 = c_{t-1} r_{t-1}$, dicho mcd es r_{t-1}.

7.1.1. Identidad de Bézout

Un importante resultado en teoría de números es el siguiente:

Proposición 13. *Sean $a, b \in \mathbb{N}$, y $d = mcd(a, b)$. Entonces, $\exists x, y \in \mathbb{Z}$ tales que $ax + by = d$. Además, hay infinitos de estos x, y.*

Demostración. La prueba será por inducción. Usaremos la notación y conceptos empleados para el algoritmo de Euclides. Se va a probar que si $k < t$, donde t era el paso en el que se paraba de iterar, $\exists x_k, y_k \in \mathbb{Z}$ con $r_k = x_k a + y_k b$. Por inducción, el caso base será $k = 0$ y $k = 1$. Es evidente que $r_0 = b = 1 \cdot b + 0 \cdot a$ y que $r_1 = a = 0 \cdot b + 1 \cdot a$.

Para el paso inductivo, supondremos que la afirmación tiene lugar si $k < m$, con $m < t$ y probaremos que en ese caso también se cumple si $k = m$. Observemos que $r_{m-2} = c_{m-1} r_{m-1} + r_m$, luego $r_m = r_{m-2} - c_{m-1} r_{m-1}$. Por hipótesis de inducción, $r_m = x_{m-2}a + y_{m-2}b - c_{m-1}x_{m-1}a - c_{m-1}y_{m-1}b = (x_{m-2} - c_{m-1}x_{m-1})a + (y_{m-2} - c_{m-1}y_{m-1})b$, como se quería probar, pues los términos entre paréntesis son enteros.

Ahora que hemos probado esa propiedad, veamos que si $k = t - 1$ se tiene la identidad de Bézout, puesto que $\exists x, y \in \mathbb{Z}$ tales que $r_{t-1} = d = ax + by$.

Finalmente, sabiendo que existen tales x, y, notemos que $\forall k \in \mathbb{Z}$, si $x' = -kb$ y $y' = ka$, tenemos que $(x + x')a + (y + y')b = d$, puesto que $(x + x')a + (y + y')b = xa + yb - kba + kab = xa + yb = d$, luego hay infinitas soluciones. □

Asimismo cabe observar que la expresión $ax + by$ es divisible por todos los divisores comunes de a y b, por lo tanto lo es también por el *mcd*. De esta manera, si $ax + by = d$, ha de ser que $mcd(a, b)|d$. Combinando estas dos ideas, sabemos que expresiones como $2x + 3y = 1$ tienen solución (¡infinitas!), pero no $2x + 4y = 1$, por ejemplo.

7.1.2. Primos relativos

Definición 20. $a, b \in \mathbb{N}$ son **primos entre sí** si y solo si $mcd(a, b) = 1$. También se emplea la terminología **coprimos** o **primos relativos**.

Proposición 14. *Sean $a, b, c \in \mathbb{N}$. Si $c|ab$ y además a y c son coprimos, entonces $c|b$. De esto se deduce que:*

1. *Si p es primo y $p|ab$, o bien $p|a$ o $p|b$.*
2. *Si p es primo y $p|a_1a_2a_3...a_k$, $\exists i \in \mathbb{N}$, $1 \leq i \leq k$, tal que $p|a_i$.*

Demostración. Por la identidad de Bézout, se tiene que $\exists x, y \in \mathbb{Z}$ tales que $xa + yc = 1$, es decir, $x \cdot ab + yb \cdot c = b$. Como $c|ab$ y $c|c$, entonces $c|b$. Para el primer corolario, sin perder en generalidad, digamos que $p \nmid a$. Entonces se tiene que p, a son coprimos y se aplica el lema. Para el segundo corolario, se aplica inducción sobre k y el primer corolario. □

7.1.3. Teorema fundamental de la aritmética

Teorema 1. *Todo $n \in \mathbb{N}$, $n \geq 2$, puede expresarse como producto de números primos, y de una única forma (Ignorando el orden de los factores).*

Demostración. Para probar que todo número se puede expresar de esta forma, procederemos por inducción. Evidentemente, 2 es el producto de 2, que es primo. Sea n natural. Supongamos que si t verifica $2 \leq t < n$, t se puede expresar como producto de primos. Vamos a probar que entonces n también puede expresarse de esta forma. Si n es primo, hemos acabado. Si n es compuesto, $\exists a, b \in \mathbb{N}$ tales que $n = ab$, con $a > 1$, $b > 1$. Entonces, por hipótesis, tanto a como b se pueden expresar como producto de primos, así que ab también, multiplicando ambos productos de primos.

Para probar que esta distribución es única, supongamos que hay algún n' tal que $n' = p_1p_2...p_k = q_1q_2...q_m$, con los conjuntos $\{p_i : 1 \leq i \leq k\}$ y $\{q_j : 1 \leq j \leq m\}$ distintos, y cada p_i o q_j primo. Sea n el mínimo del conjunto de tales n'. Entonces, $p_1|n$, de modo que por la proposición 14, corolario 2, $\exists j \in \mathbb{N}$ tal que $p_1|q_j$. Pero como ambos dos son primos, sigue que $p_1 = q_j$. Así pues, dividiendo n por $p_1 = q_j$, queda que $p_2...p_k = q_1q_2...q_{j-1}q_{j+1}...q_m = n''$, y este valor se puede expresar de dos formas como producto de primos, y es menor que n, contradiciendo que n fuese el mínimo. □

Observación 12. La forma habitual de escribir una factorización en primos es $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$, con los $\alpha_i > 0$ y $p_1 < p_2 < ... < p_k$.

7.2. Los enteros

7.2.1. Propiedades del conjunto. Grupos y anillos

En el conjunto de los números enteros, $\mathbb{Z}$, se definen las operaciones binarias internas que denotaremos $+$ y $\cdot$ (suma o adición y producto o multiplicación). Satisfacen las siguientes propiedades:

1. $\forall z, w, v \in \mathbb{Z}$, $z + (v + w) = (z + v) + w$ (Asociativa de la adición)
2. $\exists 0 \in \mathbb{Z}$, $\forall z \in \mathbb{Z}$, $z + 0 = z = 0 + z$. (Existencia de elemento neutro aditivo)
3. $\forall z \in \mathbb{Z}$, $\exists -z \in \mathbb{Z}$, $z + (-z) = 0$. (Existencia de elemento inverso aditivo (también denominado opuesto)).
4. $\forall z, w \in \mathbb{Z}$, $z + w = w + z$ (Conmutativa de la adición)
5. $\forall z, w, v \in \mathbb{Z}$, $z \cdot (v \cdot w) = (z \cdot v) \cdot w$ (Asociativa del producto)
6. $\forall z, w, v \in \mathbb{Z}$, $z \cdot (v + w) = zv + zw$ (Distributiva del producto respecto de la adición)
7. $\forall z, w \in \mathbb{Z}$, $zw = wz$ (Conmutativa del producto)
8. $\exists 1 \in \mathbb{Z}$ $\forall z \in \mathbb{Z}$, $z1 = 1z = z$. (Existencia del elemento neutro multiplicativo, o elemento unidad)
9. $\forall z, w \in \mathbb{Z}$, $zw = 0 \implies z = 0 \vee w = 0$.

Definición 21. Un conjunto A en el que se define una operación $+$ se conoce como **grupo** si la operación satisface las propiedades $1, 2, 3$. Si además satisface la 4, se conoce como **grupo conmutativo o abeliano**.

Definición 22. Un conjunto A en el que se definen dos operaciones, $+$ y $\cdot$, se conoce como **anillo** si estas satisfacen las propiedades $1, 2, 3, 4, 5, 6$. Si además la segunda operación satisface la 7, se trata de un **anillo conmutativo**. Si satisface la 8, se trata de un **anillo unitario**.

Así pues, $\mathbb{Z}$ con $+$ y $\cdot$ se trata de un anillo conmutativo unitario.

Además existe la relación de orden total $'\leq'$ en $\mathbb{Z}$ lo que lo convierte en un anillo ordenado. Se cumple que si $a, b, c \in \mathbb{Z}$ y $a \leq b$, entonces $a + c \leq b + c$ y si además $c > 0$, entonces $ac \leq bc$.

7.2.2. Divisibilidad

La divisibilidad en $\mathbb{Z}$ se comporta de igual manera que en $\mathbb{N}$: $a|b \iff \exists c \in \mathbb{Z}$ t.q. $ca = b$. Cumple las propiedades de suma y producto ya mencionadas en $\mathbb{N}$. Se cumple la división euclídea: $\forall a, b \in \mathbb{Z}, a \neq 0$, $\exists c, r \in \mathbb{Z}$, $0 \leq r < |a|$ tales que $b = ac + r$.

Se aplica de igual forma el algoritmo de euclides y la identidad de Bézout: $\forall a, b \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ tales que $ax + by = mcd(a, b)$.

7.2.3. Ecuaciones diofánticas

Teorema 2. *Dados $a, b, c \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ tales que $ax + by = c$ (ecuación diofántica) si y solo si $mcd(a, b)|c$, esto es, c es múltiplo de $mcd(a, b)$.*

Demostración. Vamos a probar que, dados $a, b \in \mathbb{Z}$, se tiene: $\{ax + by : x, y \in \mathbb{Z}\} = \{md : m \in \mathbb{Z}\}$ con $d = mcd(a, b)$. En primer lugar, está claro que como $d|a$ y $d|b$, $d|xa$ y $d|yb$ luego $d|(xa + yb)$, es decir, $xa + yb = dm$ para algún $m \in \mathbb{Z}$. Además, como $\exists x, y \in \mathbb{Z}$ tales que $xa + yb = d$, entonces $xam + ybm = dm$, luego $\forall m \in \mathbb{Z}$, dm se expresa como elemento del primer conjunto para los enteros xm y ym. □

Por ejemplo, no hay soluciones enteras para $20x + 14y = 7$, dado que $mcd(20, 14) = 2$, que no divide a 7. Sin embargo, sí hay para $164 = 20x + 28y$. El procedimiento para hallarlas puede ser, en primer lugar, dividir por el mcd: $41 = 5x + 7y$, y ahora se puede encontrar una de las soluciones, x_0, y_0, y hallar las demás considerando que si x, y son soluciones, se tiene que $41 = 5x + 7y$ y como sabemos que $41 = 5x_0 + 7y_0$, restando, $5(x - x_0) + 7(y - y_0) = 0$, la cual es fácil de resolver.

7.3. Congruencias

Recordemos que si $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, existe una relación de equivalencia llamada **congruencia módulo m**:

$a \equiv b \mod m \iff m|(b - a)$

Proposición 15. *Sean $a, b, c, d \in \mathbb{Z}, m \in \mathbb{N}$. Si $a \equiv b \mod m$ y $c \equiv d \mod m$, entonces $a + c \equiv b + d \mod m$, $ac \equiv bd \mod m$.*

Esto se vio anteriormente, en la sección de relaciones de equivalencia. De aquí se deduce que, siendo $a, b, c \in \mathbb{Z}$, $m, n \in \mathbb{N}$, se tiene que si $a \equiv b \mod m$, entonces $a + c \equiv b + c \mod m$, $ac \equiv bc \mod m$ y $a^n \equiv b^n \mod m$. Esto se deduce de que $c \equiv c \mod m$, y de aplicar sucesivas veces la segunda propiedad del lema en el caso de las potencias.

Por ejemplo, si queremos resolver $3x \equiv 4 \mod 5$, podemos valernos de que $6x \equiv 8 \equiv 3 \mod 5$, y como $6 \equiv 1 \mod 5$, sigue que $6x \equiv x \mod 5$, luego $x \equiv 3 \mod 5$, así que la solución es $x = 5k + 3$, $k \in \mathbb{Z}$.

7.3.1. Operaciones en el conjunto cociente. Congruencias y anillos.

Recordemos que $\mathbb{Z}_m$ es el conjunto cociente para la relación de congruencia las propiedades vistas anteriormente, se tiene que si $\overline{a_1} = \overline{a_2}$ y $\overline{b_1} = \overline{b_2}$, entonces $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ y además $\overline{a_1 b_1} = \overline{a_2 b_2}$.

Así pues, tiene sentido definir los siguientes operadores binarios internos: $+, \cdot : \mathbb{Z}_m \times \mathbb{Z}_m \mapsto \mathbb{Z}_m$, que vienen dados por $\overline{a} + \overline{b} = \overline{a + b}$, y $\overline{a} \cdot \overline{b} = \overline{ab}$. Estos operadores están bien definidos (no importa qué representante se tome para aplicar la regla), dado que si tomamos dos representantes diferentes, tales que $\overline{a} = \overline{a'}$, entonces, según se vio antes, $\overline{a} + \overline{b} = \overline{a + b} = \overline{a' + b} = \overline{a'} + \overline{b}$, e igual para el producto.

Proposición 16. $(\mathbb{Z}_m, +, \cdot)$ *es un anillo conmutativo unitario.*

Visto lo anterior, es sencillo demostrar cada una de las propiedades que definen un anillo conmutativo unitario, por ejemplo la existencia de elemento unidad (en este caso $\overline{1}$), neutro aditivo ($\overline{0}$), o la distributiva, que se probará a continuación:

$\overline{a}(\overline{b} + \overline{c}) = \overline{a}(\overline{b + c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Análogamente se prueban las demás. Observemos que se cumple que el opuesto aditivo de una clase es la clase del opuesto aditivo en $\mathbb{Z}$ de su elemento: $-\overline{a} = \overline{-a}$.

Proposición 17. *Si $m \in \mathbb{N}$ es compuesto y $m = ab$, $a > 1$, $b > 1$, entonces en $\mathbb{Z}_m$ se tiene que $\overline{a}\overline{b} = \overline{0}$ (pese a que ni $\overline{a} = \overline{0}$ ni $\overline{b} = \overline{0}$). Se dice entonces que $\overline{a}$ y $\overline{b}$ son **divisores de cero**.*

Si $p \in \mathbb{N}$ es primo, entonces en $\mathbb{Z}_p$ se tiene que si $\overline{a}\overline{b} = \overline{0}$, o bien $\overline{a} = \overline{0}$, o bien $\overline{b} = \overline{0}$. En este caso, por tanto, no hay divisores de cero.

El primer caso es trivial, y en el segundo, como $\overline{0} = \overline{a}\overline{b} = \overline{ab}$, entonces $p|ab \implies p|a \vee p|b$, esto es, la clase de alguno de los dos es la de 0.

En adelante se usará esta notación: $\mathbb{Z}_m^* = \mathbb{Z}_m \backslash \{\overline{0}\}$

Proposición 18. *$(\mathbb{Z}_p^*, +, \cdot)$, con p primo, es un **cuerpo conmutativo unitario**, esto es, un anillo conmutativo unitario tal que $\forall \overline{a} \in \mathbb{Z}_p^*$, $\exists \overline{a}^{-1} \in \mathbb{Z}_p^*$ t.q. $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$.*

Demostración. Sea $\overline{a} \in \mathbb{Z}_p$, $\overline{a} \neq \overline{0}$. Entonces, $p \nmid a$, de modo que $mcd(p, a) = 1$, así que $\exists x, y \in \mathbb{Z}$ t.q. $ax + py = 1$, de modo que $\overline{ax + py} = \overline{1}$, luego $\overline{a} \cdot \overline{x} + \overline{p} \cdot \overline{y} = \overline{1}$. Como $\overline{p} = \overline{0}$, entonces, $\overline{a} \cdot \overline{x} = \overline{1}$, de modo que $\overline{x}$ es el inverso buscado. □

Por ejemplo, para resolver la congruencia $8x \equiv 7 \mod 11$, podemos escribir $\overline{8} \cdot \overline{x} = \overline{7}$, luego $\overline{x} = \overline{7} \cdot \overline{8}^{-1}$. Se puede calcular (por ejemplo por algoritmo de Euclides para hallar la solución a la identidad de Bézout correspondiente) que ese inverso es $\overline{-4}$, de modo que $\overline{x} = \overline{-28} = \overline{5}$, luego $x = 11k + 5$, $k \in \mathbb{Z}$.

Observación 13. Veamos que $(\mathbb{Z}_p^*, \cdot)$ es un grupo conmutativo con $p - 1$ elementos, y podemos denotar $\overline{a}^n$ como el producto de $\overline{a}$ por sí mismo n veces ($n \in \mathbb{N}$), así como $\overline{a}^0 = \overline{1}$, y $\overline{a}^{-n} = \overline{a}^{-1^n}$.

7.3.2. Pequeño teorema de Fermat

Teorema 3 (Pequeño teorema de Fermat)**.** *Sea $p \in \mathbb{N}$ un número primo. En $\mathbb{Z}_p$:*

1. *Si $\overline{a} \neq \overline{0}$, entonces $\overline{a}^{p-1} = \overline{1}$. Esto es, si $a \in \mathbb{Z}$, $p \nmid a$, entonces $a^{p-1} \equiv 1 \mod p$*
2. *$\overline{a}^p = \overline{a}$. Es decir, si $a \in \mathbb{Z}$, entonces $a^p \equiv a \mod p$.*

La demostración se omite en estos apuntes. Es consecuencia inmediata del teorema de Lagrange que se discute en los apuntes de *Estructuras Algebraicas*.

Por ejemplo, para saber qué resto deja 10^{1000} al dividir por 13, ahora sabemos que $10^{12} \equiv 1 \mod 13 \iff (10^{12})^{83} \equiv 1^{83} \equiv 1 \mod 13 \iff (10^{12})^{83} \cdot 10^4 = 10^{1000} \equiv 10^4 \mod 13$, así que basta con calcular este resto.

Para saber si una ecuación como $ax \equiv c \mod m$ tiene soluciones, basta con observar que esta equivale a $ax - c = mk$ para algún $k \in \mathbb{Z}$, es decir, $ax + m(-k) = c$. Sabemos que $\exists x \in \mathbb{Z}$ que satisface esto si $mcd(a, m)|c$, puesto que se trata de una ecuación diofántica. Es decir:

Proposición 19. *Sea $m \in \mathbb{N}$, y sean $a, c \in \mathbb{Z}$.*
$\exists x \in \mathbb{Z}$ tal que $ax \equiv c \mod m \iff mcd(a, m)|c$.

Esto explica que en $\mathbb{Z}_p$, con p primo, todos los elementos distintos de $\overline{0}$ tengan inverso multiplicativo, puesto que para que este exista para un elemento $\overline{a}$, debe tenerse que $\exists x \in \mathbb{Z}$ t.q. $\overline{a} \cdot \overline{x} = \overline{1}$, esto es, que $ax \equiv 1 \mod p$. Como $mcd(a, p) = 1|1$, existe tal inverso.

De hecho, como el único número que divide al 1 es el propio 1, podemos decir en general:

Proposición 20. *Sea $m \in \mathbb{N}$, $a \in \mathbb{Z}$. En $\mathbb{Z}_m$, si $\overline{a} \neq \overline{0}$:*
$\overline{a}$ tiene inverso multiplicativo $\iff mcd(a, m) = 1$.

Es decir, si a es coprimo con m. Cabe observar también que en $\mathbb{Z}_m$, si dos elementos $\overline{a}$ y $\overline{b}$, distintos de $\overline{1}$, cumplen que $\overline{a}\overline{b} = \overline{0}$, esto es, que $ab = km$, entonces no pueden tener inverso porque $mcd(a, m) \neq 1$ y $mcd(b, m) \neq 1$. (Puesto que $a|km$ y $b|km$).

Además es evidente que $\overline{1}$ siempre tiene inverso (y este es $\overline{1}$).

Definición 23. Se define el conjunto $\mathcal{U}(Z_m)$, o **unidades de** $\mathbb{Z}_m$, como el conjunto de elementos que tienen inverso: $\mathcal{U}(Z_m) = \{\overline{a} \in \mathbb{Z}_m : mcd(a, m) = 1\}$.

Su cardinal se conoce como **función indicatriz de Euler** o función ϕ de Euler: $\phi(m) = |\mathcal{U}(Z_m)|$

Así, si pensamos en los representantes de cada clase de $\mathbb{Z}_m$ como los que van de 0 a $m-1$, entonces podemos decir que el valor de $\phi(m)$ es el número de coprimos con m entre 1 y $m-1$. (coprimos anteriores a m), puesto que $\overline{0}$ nunca tiene inverso.

Por ejemplo, $\phi(6) = 2$, dado que $\mathcal{U}(\mathbb{Z}_6) = \{\overline{1}, \overline{5}\}$. Las demás clases, $\overline{2}, \overline{3}, \overline{4}$ no tienen inverso puesto que sus representantes no son coprimos con 6 y, por supuesto, $\overline{0}$ tampoco.

Cabe observar que, como $\mathbb{Z}_p^*$, con p primo, es un cuerpo, sus $p-1$ elementos tienen inverso, luego $\phi(p) = p-1$ si p es primo.

Observación 14. $\mathcal{U}(\mathbb{Z}_m)$, con el producto de $\mathbb{Z}_m$, es un grupo conmutativo.

Cumple la propiedad asociativa y conmutativa dado que el producto de $\mathbb{Z}_m$ la cumple para cualquier clase de $\mathbb{Z}_m$. Asimismo, el conjunto de unidades es cerrado al producto, ya que si $\overline{a} \in \mathcal{U}(\mathbb{Z}_m)$ y $\overline{b} \in \mathcal{U}(\mathbb{Z}_m)$ $\exists \overline{x}, \overline{y} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{x} = \overline{1}$, y $\overline{b} \cdot \overline{y} = \overline{1}$, luego $\overline{ab} \cdot \overline{xy} = \overline{1}$ así que $\overline{ab}$ tiene inverso luego $\overline{ab} \in \mathcal{U}(\mathbb{Z}_m)$. Además existe elemento neutro, $\overline{1}$, que evidentemente está en el conjunto puesto que $\overline{1}$ es su inverso, y, por último, cada elemento $\overline{a} \in \mathcal{U}(\mathbb{Z}_m)$ tiene un opuesto respecto a esta operación, por definición de $\mathcal{U}(\mathbb{Z}_m)$, y dicho opuesto está en el conjunto dado que $\overline{a}$ es su inverso multiplicativo.

7.3.3. Propiedades de la función phi y Teorema de Euler

Proposición 21. *La función ϕ tiene las siguientes propiedades que permiten su cálculo:*

1. *Si m_1, m_2 son coprimos, entonces $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$.*

   Inductivamente, si $m_1, m_2, ..., m_n$ son coprimos dos a dos, entonces $\phi(\prod_{i=1}^n m_i) = \prod_{i=1}^n \phi(m_i)$.

2. *Si p es primo, y $k \in \mathbb{N}$, entonces $\phi(p^k) = p^{k-1}(p-1)$.*

La prueba de *1* está fuera del ámbito de estos apuntes, pero se explora en profundidad en los de *Estructuras Algebraicas*. Vamos a probar *2*. Desde 1 hasta p^k hay p^k números, de los cuales p^{k-1} son múltiplos de p: $p, 2p, 3p, ..., p^{k-1}p = p^k$. Los demás son coprimos con p, al ser p primo, y por tanto son coprimos con p^k. Es decir, entre 1 y p^k hay $p^k - p^{k-1}$ coprimos con p^k, luego $\phi(p^k) = p^k - p^{k-1}$ de donde sigue la expresión buscada.

Con esto podemos calcular el valor de la función fácilmente para cualquier valor n natural, a través de su descomposición en primos, puesto que si $n = \prod_{i=1}^k p_i^{\alpha_i}$, con cada $\alpha_i \in \mathbb{N}$ y cada p_i primo diferente a los demás, entonces $\phi(n) = \prod_{i=1}^n p_i^{\alpha_i - 1}(p_i - 1)$, hecho que sigue de aplicar las propiedades anteriores, dado que cada potencia de primos es coprimo con las demás.

Teorema 4 (Euler)**.** *Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$.*
Si $mcd(a, m) = 1$, entonces $\overline{a}^{\phi(m)} = \overline{1}$ en $\mathbb{Z}_m$, esto es, $a^{\phi(m)} \equiv 1 \mod m$.

Podemos observar que el pequeño teorema de Fermat es un caso particular de este teorema. Una vez más, la demostración es consecuencia del teorema de Lagrange que se discute en los apuntes de *Estructuras Algebraicas*.

Teorema 5 (Wilson)**.** *Si p es primo, entonces $(p-1)! \equiv -1 \equiv p-1 \mod p$.*

Demostración. Supondremos que p es impar dado que si $p = 2$ se verifica inmediatamente la proposición. Veamos que $\overline{a}$, con $1 \leq a \leq p-1$ es inverso de si mismo en $\mathbb{Z}_p$ si y solo si $a = p-1$ o si $a = 1$. Efectivamente, $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{-1} \cdot \overline{-1} = \overline{1}$, y si se tiene que $a^2 \equiv 1 \mod p$, entonces $(a-1)(a+1) \equiv 0 \mod p$, y como p es primo, debe ser porque $a - 1 \equiv 0 \mod p \implies a \equiv 1 \mod p$ o bien $a + 1 \equiv 0 \mod p \implies a \equiv -1 \mod p$.

Ahora, veamos que $\overline{(p-1)!} = \overline{1} \cdot \overline{2 \cdot 3 \cdot ... \cdot (p-2)} \cdot \overline{p-1}$, pero el segundo factor debe ser $\overline{1}$ dado que se tiene un número par de clases que deben ser parejas elemento-inverso, dado que ninguno puede ser inverso de sí mismo como se vio antes. Entonces, se tiene $\overline{(p-1)!} = \overline{-1}$. □

Teorema 6 (Teorema chino del resto)**.** *Sean los naturales* $m1$*,* $m2$*,* $m3$ *...* m_i *coprimos dos a dos y sean* $a_1, a_2, ..., a_i$ *enteros. Entonces el sistema* $x \equiv a_j \mod m_j$ *para* $1 \leq j \leq i$ *tiene solución, que además es única módulo* $m_1 m_2 m_3 ... m_i$*.*

Veremos la demostración con dos ecuaciones. Sean a_1, $a_2 \in \mathbb{Z}$ m_1 y $m_2 \in nset$. Consideramos el sistema $x \equiv a_1 \mod m_1$ y $x \equiv a_2 \mod m_2$. Si existen M_1, M_2 que satisfagan $M_1 \equiv 1 \mod m_1$ y $M_1 \equiv 0 \mod m_2$, y $M_2 \equiv 0 \mod m_1$, $M_2 \equiv 1 \mod m_2$, entonces el valor $z = a_1 M_1 + a_2 M_2$ es solución del sistema original, dado que tendríamos que $z \equiv a_1 \cdot 1 + 0 \mod m_1$ y $z \equiv 0 + a_2 \cdot 1 \mod m_2$. Como m_1 y m_2 son coprimos, $\exists x, y \in \mathbb{Z}$ tales que $m_1 a + m_2 b = 1$. Veamos que $M_1 = m_2 b$ y $M_2 = m_1 a$ satisfacen las ecuaciones anteriores, luego el sistema tiene solución.

Para ver que es única módulo el producto, veamos que todas las soluciones r del sistema deben satisfacer que $z \equiv r \mod m_i$ para $i = 1, 2$, donde z es la solución descrita con anterioridad. Entonces, $m_1 | (z - r)$ y $m_2 | (z - r)$. Como m_1, m_2 son coprimos, debe tenerse que $m_1 m_2 | (z - r)$, luego $r \equiv z$ mód $m1m2$.

Con n ecuaciones, basta con ver que cada uno de los sistemas que permiten obtener los M_i que dan la solución $x = \sum_{i=1}^{n} a_i M_i$, son equivalentes al sistema $M_i \equiv 1 \mod m_i$, $M_j \equiv 0 \mod \prod_{i \neq k, 1 \leq k \leq n} m_k$, que es un sistema de 2 ecuaciones con las bases de las congruencias coprimas, que ya se vio antes como resolver.

8. Números complejos

En esta sección se discuten las bases de los números complejos. El siguiente paso tras los enteros hubiese sido (además de los racionales) el conjunto de números reales, pero este cuerpo ya es objeto de estudio detallado en otras muchas asignaturas, empezando desde *cálculo I*. Por tanto, se da el salto a cómo construir el cuerpo de complejos a partir de $\mathbb{R}$. La siguiente subsección profundiza brevemente en este aspecto:

8.1. Construcción de los números

- $\mathbb{N}$ se construye a través de distintos axiomas, como por ejemplo $1 \in \mathbb{N}$, $\forall n \in \mathbb{N}, s(n) \in \mathbb{N}$ (donde $s(n)$ denota el 'siguiente' a n, y devuelve un número distinto de n tal que $\forall n, m \in \mathbb{N}$, $n \neq m$, se tiene que $s(n) \neq s(m)$)... Se define la operación suma como la aplicación reiteradas veces de $s(n)$ y el producto como la aplicación reiteradas veces de la suma.

- Para resolver ecuaciones como $3 + x = 2$, al no bastar con los elementos de $\mathbb{N}$, se define $\mathbb{Z}$ como el conjunto cociente de la relación $(a, b)\mathcal{R}(c, d) \iff a + d = b + c$ en $\mathbb{N} \times \mathbb{N}$, y las aplicaciones definidas son suma: $[(a, b)] + [(c, d)] = [(a + c, b + d)]$, y producto: $[(a, b)][(c, d)] = [(ac + bd, ad + bc)]$. Es un anillo conmutativo unitario.

- Para resolver ecuaciones como $3x = 2$, al no bastar con los elementos de $\mathbb{Z}$, se define $\mathbb{Q}$ como el conjunto cociente de la relación $(a, b)\mathcal{R}(c, d) \iff ad = bc$ en $\mathbb{Z} \times \mathbb{Z}^*$, y las aplicaciones definidas son suma: $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$, y producto: $[(a, b)][(c, d)] = [(ac, bd)]$. Es un cuerpo.

- Muchos conjuntos de racionales como $A = \{q \in \mathbb{Q} : q^2 < 5\}$, acotados superiormente, carecen de supremo en $\mathbb{Q}$, así que se construye $\mathbb{R}$ como el conjunto de los elementos de $\mathbb{Q}$ más los supremos de todos los conjuntos. Es decir, el conjunto $\mathbb{R}$ verifica la **propiedad del supremo o de completitud**, es decir, que todo subconjunto no vacío acotado superiormente de $\mathbb{R}$ tiene supremo en $\mathbb{R}$.

- Muchas ecuaciones como $x^2 + 1 = 0$ quedan sin definir en $\mathbb{R}$. Por ello, se define un objeto, i, como la solución a esta ecuación, esto es, se verifica $i^2 + 1 = 0$. Así, podemos construir nuevos números, de la forma $z = a + ib \in \mathbb{C}$, con $a, b \in \mathbb{R}$, denominados **complejos**. Formalmente se define este nuevo conjunto como $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, es decir, son el producto cartesiano de los reales con ellos mismos, y las operaciones definidas son $(a, b) + (c, d) = (a + c, b + d)$ y $(a, b)(c, d) = (ac - bd, ad + bc)$. Este conjunto con estas operaciones constituye un cuerpo conmutativo, y todo par $(a, b) = (a, 0) + (b, 0) \cdot (0, 1)$, así que se representan los pares de la forma $(x, 0)$ por x, y $(0, 1)$ por i.

  Como ya se ha visto, estos elementos y operaciones se denotan: $(a + ib) + (c + id) = (a + c) + i(b + d)$, $(a + ib)(c + id) = (ac - bd) + i(bc + da)$.

8.2. Representación de $\mathbb{C}$ y terminología

Los complejos se representan en el **plano complejo**, en el que el eje X o eje real ($\mathbb{R}$) representa los números reales, el eje Y o eje imaginario ($i\mathbb{R}$) representa los imaginarios puros (de la forma bi con $b \in \mathbb{R}$), y cualquier punto del plano representa, a través de sus coordenadas (a, b), el complejo $a + ib$.

También se pueden considerar los complejos como un vector $\vec{Oz}$, que va desde el origen hasta el punto correspondiente.

Definición 24. Sea $z = a + ib \in \mathbb{C}$. Se define su **parte real** por $Re(z) = a$, su **parte imaginaria** por $Im(z) = b$, y su **módulo** por $|z| = \sqrt{a^2 + b^2}$, es decir, el tamaño del vector correspondiente al número.

Podemos considerar las ecuaciones de distintas regiones del plano complejo. Por ejemplo, la ecuación del eje X es $Im(z) = 0$, y el segundo cuadrante es $Im(z) > 0$, $Re(z) < 0$.

8.2.1. Forma polar

Los complejos también se pueden representar en su **forma polar**, $z = |z|cs(\theta)$, donde $cs(\theta) = \cos(\theta) + i\sin(\theta)$, y θ es un **argumento** de z, es decir, uno de los posibles ángulos medidos entre $\vec{Oz}$ y el eje X.

Veamos el razonamiento detrás de la forma polar. Vamos a considerar el complejo $w = a + ib$, con el mismo argumento θ que z y en la circunferencia unidad (por lo que $a = \cos(\theta)$ y $b = \sin(\theta)$, dado que así su módulo es $\sqrt{\cos^2(\theta) + \sin^2(\theta)} = 1$). Como el argumento de w y z es el mismo, los vectores $\vec{Oz}$ y $\vec{Ow}$ son paralelos y podemos encontrar $\lambda \in \mathbb{R}$ tal que $z = \lambda w$, por lo que $|z|^2 = |\lambda(a + ib)|^2 = |a\lambda + ib\lambda|^2 = a^2\lambda^2 + b^2\lambda^2 = \lambda^2(a^2 + b^2)$, de modo que $|z| = \lambda \cdot 1$ (suponiendo $\lambda > 0$). Así, $z = |z|w$, es decir, $z = |z|cs(\theta)$.

De hecho, si θ es argumento de z, entonces todos los números de la forma $\theta + 2k\pi$, $k \in \mathbb{Z}$, son argumentos de z, dada la periodicidad 2π de las funciones sin y cos. Además una forma de calcular un argumento de $z = a + ib$ es a través de $\arctan\frac{b}{a}$, teniendo en cuenta tomar el valor devuelto para el cuadrante apropiado donde se halla el número. Esto se explica a través de la interpretación geométrica del argumento como ángulo entre OX y $\vec{Oz}$.

Observación 15. Si $z = a(\cos(\theta) + i\sin(\theta))$ y $a \in \mathbb{R}$, $a \geq 0$, entonces $a = |z|$.

Puesto que $|z|^2 = |a(\cos(\theta) + i\sin(\theta))|^2 = a^2\cos^2(\theta) + a^2\sin^2(\theta) = a^2(1) = a^2$, luego $|z| = |a|$ pero $a \geq 0$.

Teorema 7 (Euler)**.** *Sea* $\theta \in \mathbb{R}$. $e^{i\theta} = \cos\theta + i\sin\theta$

A partir de ahora se denotará así $cs(\theta)$. La demostración de este hecho se puede realizar con los desarrollos en serie de Taylor de e^x, $\cos(x)$ y $\sin(x)$. Se puede también comprobar fácilmente que propiedades importantes de e^{ix} son verificadas por $cs(x)$, en concreto: $cs(a + b) = cs(a)cs(b)$, $cs(0) = 1$ y $cs'(x) = ics(x)$, lo que permite intuir que ambas funciones sean las mismas sin necesidad de utilizar las series de Taylor.

De aquí también se deduce fácilmente la identidad de Euler: $e^{i\pi} + 1 = 0$.

Es importante observar que los números de la forma $e^{i\theta}$, $\theta \in \mathbb{R}$, son los de la circunferencia unidad.

8.2.2. Conjugado complejo

Definición 25. Sea $z = a + ib$, $a, b \in \mathbb{R}$. Se define el **conjugado** de z por $\overline{z} = a - ib$.

Geométricamente se trata del simétrico de z respecto de OX.

Proposición 22. *Sea* $z \in \mathbb{C}$.

1. $Re(z) = \frac{z+\overline{z}}{2}$, *luego* $z \in \mathbb{R} \iff z = \overline{z}$.
2. $Im(z) = \frac{z-\overline{z}}{2i}$, *luego* $z \in i\mathbb{R} \iff z = -\overline{z}$.
3. $\overline{z + w} = \overline{z} + \overline{w}$
4. $\overline{zw} = \overline{z}\,\overline{w}$
5. $|z|^2 = z\overline{z}$
6. $|z| = |\overline{z}|$.
7. $\overline{e^{i\theta}} = e^{-i\theta}$

Todas estas se prueban fácilmente a través de la definición.

Conviene observar además que $\frac{z}{w} = \frac{z\overline{w}}{|w|^2}$, y más particularmente, $\frac{1}{w} = \frac{\overline{w}}{|w|^2}$.

8.2.3. Producto y cociente en forma polar

Sean $z, w \in \mathbb{C}$, $z = re^{i\alpha}$, $w = se^{i\beta}$, con $r, s \in \mathbb{R}$ $r, s \geq 0$. Como $zw = rse^{i(\alpha+\beta)}$, entonces observamos que $|zw| = rs = |z||w|$ por la observación 15, y $\arg(zw) = \alpha + \beta = \arg(z) + \arg(w)$.

Asimismo, como $\frac{1}{w} = \frac{\overline{w}}{|w|^2} = \frac{se^{i\beta}}{s^2} = \frac{e^{-i\beta}}{s}$, entonces $\frac{z}{w} = \frac{r}{s}e^{i(\alpha-\beta)}$, luego el número resultante tiene módulo $|\frac{z}{w}| = \frac{|z|}{|w|}$ y argumento $\arg(\frac{z}{w}) = \alpha - \beta = \arg z - \arg w$.

Es fácil deducir también que $z^n = \prod_{k_1}^{n}(re^{i\alpha}) = r^n e^{i(\sum_{k=1}^{n}\alpha)} = r^n e^{in\alpha}$, $\forall n \in \mathbb{N}$, y $\forall n \in \mathbb{Z}$ si $r \neq 0$, teniendo en cuenta que $z^{-1} = \frac{1}{z}$.

Con esto es fácil resolver raíces de un número complejo. Por ejemplo, para resolver $z^3 = 2 + 2i$, es decir, las raíces cúbicas de $2 + 2i$, basta con tener en cuenta que si $z = re^{i\theta}$ y $2 + 2i = \sqrt{8}e^{i\frac{\pi}{4}}$, entonces como $z^3 = r^3 e^{3i\theta}$, debe tenerse que $r^3 = \sqrt{8} \implies r = \sqrt[6]{8}$ y $\theta = \frac{\frac{\pi}{4}}{3} = \frac{\pi}{12}$. Además hay otras dos raíces, que se obtienen similarmente considerando que $2 + 2i$ tiene por argumento $\frac{\pi}{4} + 2\pi$ y $\frac{\pi}{4} + 4\pi$. (También se habría podido operar con coordenadas cartesianas, aunque suele ser menos cómodo).

Con esto se observa que las tres soluciones obtenidas anteriormente verifican que $z_2 = e^{i\frac{2\pi}{3}}z_1$, $z_3 = e^{i\frac{2\pi}{3}}z_2$. Es decir, basta con conocer una de ellas y luego aplicar un giro de $\frac{2\pi}{3}$ a la misma. De hecho, las raíces n-ésimas de un número son todas de igual módulo y se convierten una en otra con giros de $\frac{2\pi}{n}$, de ahí que haya n de ellas.

8.3. Raíces de la unidad

Veamos primero que $e^{i\theta} = 1 \iff \theta = 2k\pi, k \in \mathbb{Z}$, para que $\cos\theta = 1$ y $\sin\theta = 0$. Además, se deduce de esto que $e^{ia} = e^{ib} \iff a - b \in 2\pi\mathbb{Z}$, es decir, $\frac{a}{2\pi} \equiv \frac{b}{2\pi}$ mód $\mathbb{Z}$.

Las raíces n-ésimas de la unidad son los números que satisfacen $z^n = 1$. Si escribimos $z = re^{i\theta}$, $z^n = r^n e^{in\theta}$ y $1 = e^{k2\pi}$, $k \in \mathbb{Z}$, podemos observar que $r^n = 1 \implies r = 1$, y $\theta = \frac{2k\pi}{n}$.

Sea $\omega_k = e^{i\frac{2k\pi}{n}}$. Estas son las **raíces enésimas de 1**. Podemos establecer las siguientes propiedades:

1. ω_k, $k \in \mathbb{Z}$ son raíces de la unidad, es decir, $\omega_k^n = 1$.
2. $\omega_k = \omega_l \iff k \equiv l$ mód n. De hecho, las raíces únicas distintas son $\omega_0, \omega_1, ..., \omega_{n-1}$, y luego se repiten cíclicamente.
3. $\omega_{k+1} = e^{i\frac{2\pi}{n}}\omega_k$.
4. $\overline{\omega k} = \omega{-k}$.
5. Las raíces n-ésimas de la unidad forman un grupo conmutativo respecto del producto de $\mathbb{C}$, dado que:

   $\omega_k\omega_l = \omega_{k+l}$ (Cerrado al producto)

   $\omega_0\omega k = \omega_k$ (Elemento neutro)

   $\omega_k\omega_{-k} = \omega_0$ (Elemento opuesto)

   Estas propiedades son fáciles de comprobar teniendo en cuenta la definición de ω_k y el producto en $\mathbb{C}$. Además, se comprueba que $z^n = 1 \implies \overline{z^n} = \overline{1} = 1 \implies \overline{z}^n = 1$, es decir, el conjugado de una raíz también lo es.

8.4. Raíces n-ésimas de un complejo

Si $w \in \mathbb{C}$. Sus raíces n-ésimas son las soluciones z_i de la ecuación $z_i^n = w$. Como ya vimos en el caso de las raíces cúbicas, las soluciones se pueden convertir una en otra a través de giros de $\frac{2\pi}{n}$. De hecho:

Proposición 23. *Si z_1 es raíz $n-sima$ de w, todas las raíces distintas (incluyendo multiplicidades) son $z_i = z_1\omega_i$, con $0 \leq i < n$.*

Demostración. Vamos a denotar $z = rei\theta$ y $w = |w|e^{i(\alpha+2k\pi)}$, $k \in \mathbb{Z}$. Entonces, $z^n = r^n e^{in\theta}$, de modo que debe tenerse $r = \sqrt[n]{|w|}$ y $\theta = \frac{2k\pi+\alpha}{n}$. De este modo, si $z_1 = se^{\frac{\alpha}{n}i}$, las soluciones son $z_1\omega_k = se^{\frac{\alpha}{n}i}e^{i\frac{2k\pi}{n}} = se^{\frac{2k\pi+\alpha}{n}i}$, como se quería. De hecho, en general, z_1 es de la forma $z_1 = se^{\frac{\alpha+2m\pi}{n}i}$ con algún $m \in \mathbb{Z}$ y también se verifica que al girarlo multiplicándolo por una raíz de la unidad se obtiene otra solución: $z_1\omega_k = se^{\frac{\alpha+2m\pi}{n}i}e^{i\frac{2k\pi}{n}} = se^{\frac{2(m+k)\pi+alpha}{n}i}$

8.5. Desigualdades útiles

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

1. $Re(z) \leq |Re(z)| \leq |z|$
2. $Im(z) \leq |Im(z)| \leq |z|$
3. $|z + w| \leq |z| + |w|$ (Triangular)

Demostración: En 1, la primera desigualdad es trivial. Para la segunda, veamos que si $z = a + ib$, entonces $|a|^2 = a^2 \leq a^2 + b^2 = |z|^2$, de manera que $|a| \leq |z|$. Análogamente para 2. También se puede comprobar que $ze^{i\frac{3\pi}{2}}$ tiene como parte real la imaginaria de z y su mismo módulo, de manera que aplicando 1 para este número sigue inmediatamente 2.

Para 3, observemos que $|z + w|^2 = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} = |z|^2 + z\overline{w} + \overline{z\overline{w}} + |w|^2 = |z|^2 + 2Re(z\overline{w}) + |w|^2 \leq |z|^2 + |w|^2 + 2|z||\overline{w}| = |z|^2 + |w|^2 + 2|z||w| = (|z| + |w|)^2$. Con esta relación y teniendo en cuenta que los términos son positivos, sigue 3. □

9. Polinomios

Durante esta sección, sea $\mathbb{K}$ un conjunto y $+, \cdot$ operadores binarios internos de $\mathbb{K}$ tales que $(\mathbb{K}, +, \cdot)$ es un cuerpo conmutativo. Esto es, $(\mathbb{K}, +)$ es grupo conmutativo y también lo es $(\mathbb{K}^*, \cdot)$. El elemento neutro de $+$ en $\mathbb{K}$ se denotará 0 y el de $\cdot$ se indicará con 1.

Definición 26. Un **polinomio** de grado n (con $n \in \mathbb{N} \cup \{0\}$) en $\mathbb{K}$ es una expresión de la forma $P(X) = \sum_{i=0}^{n} a_i X^i$, con $a_i \in \mathbb{K}$, $a_n \neq 0$. Se dice que n es el **grado** del polinomio, $gr(P) = n$, y además a_n es el **coeficiente principal**.

Además se debe incluir a esta defínción el polinomio 0, $P(X) = 0$. Por convención, $gr(0) = -\infty$.
Se denota $\mathbb{K}[X]$ el conjunto de los polinomios con coeficientes en $\mathbb{K}$.

Definición 27 (Suma y producto de polinomios)**.** Sea $P(X)$ un polinomio de grado n y $Q(X)$ uno de grado m, con $m \geq n$ sin perder en generalidad, y además denotamos $\{a_i\}_{0 \leq i \leq n} \subset \mathbb{K}$ los coeficientes de $P(X)$ y $\{b_i\}_{0 \leq i \leq m} \subset \mathbb{K}$ los coeficientes de $Q(X)$. Se definen las operaciones internas de $\mathbb{K}[X]$:

- $P(X)+Q(X) = b_m X^m + b_{m-1} X^{m-1} + ... + b_{n+1} X^{n+1} + (a_n + b_n) X^n + (a_{n-1} b_{n-1}) X^{n-1} + ... + (a_0 + b_0)$.
- $P(X)Q(X) = \sum_{i=0}^{n+m} c_i X^i$, con $c_i = \sum_{k=0}^{i} a_{i-k} b_k$, donde $a_r = 0$ si $r > n$ y $b_s = 0$ si $s > n$.

Además, $P + 0 = 0 + P = P$, y $P0 = 0P = 0$.

Observación 16. $gr(P+Q) = max(gr(P), gr(Q))$ salvo que $gr(P) = gr(Q) = n$ y $a_n = -b_n$, cancelándose y dando un grado menor.
En el caso de la multiplicación, $gr(PQ) = gr(P) + gr(Q)$.

Lema 2. *$\mathbb{K}[X]$ con estas operaciones es un anillo conmutativo unitario. La unidad es $P(X) = 1$.*

Las operaciones se han elegido así para que verifiquen las características de anillo conmutativo unitario. Se pueden comprobar una a una.

Lema 3. *Las unidades de $\mathbb{K}[X]$ son los polinomios de grado 0, es decir, los $P(X) = a_0$, con $a_0 \in \mathbb{K}^*$.*

Demostración. Es muy fácil comprobar que el inverso de $P(X) = a_0$ se trata de $P^{-1}(X) = a_0^{-1}$, donde a_0 es el inverso en el grupo $(K^*, \cdot)$. En efecto, $P(X)P^{-1}(X) = a_0 a_0^{-1} = 1$. Ahora veamos que si un polinomio cualquiera $P(X)$ tiene inverso, $P^{-1}(X)$, debe ser que $gr(P(X)) = 0$. De otro modo, $gr(P(X)P^{-1}(X)) = gr(P(X)) + gr(P^{-1}(X)) > 0$, luego ese producto no puede ser la unidad.

9.1. Divisibilidad

Definición 28. Sean $P, Q \in \mathbb{K}[X]$. Se dice que P **divide a** Q si $\exists R \in \mathbb{K}[X]$ tal que $RP = Q$. Se denota $P|Q$.

Estas son algunas propiedades:

- Si $P|Q$ y $Q \neq 0$, entonces $gr(P) \leq gr(Q)$.
- Si $P|Q$ entonces $P|RQ$ $\forall R \in \mathbb{K}[X]$.
- Si $P|Q$ y $P|R$, $P|Q + R$.
- Sean $C_1, C_2 \in \mathbb{K}[X]$. Si $P|Q$ y $P|R$, entonces $P|(C_1 Q + C_2 R)$.

Que se demuestran fácilmente a través de la definición, del mismo modo que se hizo para números enteros. Asimismo siguen los resultados ya familiares:

Teorema 8 (División euclídea)**.** *Sean $P(X)$, $Q(X) \in \mathbb{K}[X]$, $Q \neq 0$. Entonces, $\exists C(X), R(X) \in \mathbb{K}[X]$ tales que $gr(R) < gr(Q)$ y $P = CQ + R$. Además son únicos.*

Demostración. Se hará por inducción sobre el grado de P, para un Q dado. a_i denota los coeficientes de P y b_i los de Q. Veamos que si $gr(P) < gr(Q)$, sencillamente: $P = Q \cdot 0 + P$. Para el paso inductivo, supongamos que se verifica para $gr(P) < n$, con $gr(P) \geq gr(Q)$. Entonces también lo hace si $gr(P) = n$. Para probarlo, sea $\hat{P} = P - \frac{a_n}{b_m} X^{n-m} Q(X)$, donde $m = gr(Q)$. Entonces, $\hat{P} = a_n X^n + a_{n-1} X^{n-1} + ... + a_0 - \frac{a_n}{b_m} X^{n-m}(b_m X^m + b_{m-1} X^{m-1} + ... + b_0) = (a_{n-1} - \frac{a_n}{b_m} b_{m-1}) X^{n-1} + (a_{n-2} - \frac{a_n}{b_m} b_{m-2}) X^{n-2} + ... + (a_0 - \frac{a_n}{b_m} b_0)$, que es de grado menor a n. Por hipótesis, $\exists \hat{C}, \hat{R} \in \mathbb{K}[X]$ tales que $\hat{P} = Q\hat{C} + \hat{R}$. Entonces, $P = Q\hat{C} + \hat{R} + \frac{a_n}{b_m} X^{n-m} Q = Q(\frac{a_n}{b_m} X^{n-m} + \hat{C}) + \hat{R}$, probando lo que se quería puesto que además por hipótesis $gr(\hat{R}) < gr(Q)$.

Para la probar la unicidad, veamos que si $P = C_1 Q + R_1$ y $P = C_2 Q + R_2$, entonces, restando, $(C_1 - C_2)Q = R_2 - R_1$. Pero $gr(R_2 - R_1) < gr(Q)$, luego el único modo de que se verifique esta igualdad es que $C_1 - C_2 = 0 \implies C_1 = C_2$. □

Proposición 24. *Si $P|Q$ y $Q|P$, entonces $Q = aP$ con $a \in \mathbb{K}^*$.*

Demostración. Tenemos que para unos $R, S \in \mathbb{K}[X]$, se tiene que $PR = Q$ y $QS = P$, de modo que $PRS = P$, luego $gr(PRS) = gr(P) \implies gr(RS) = 0 \implies gr(R) = 0$. Así pues, $R = a$ con $a \in \mathbb{K}^*$, y $P \cdot a = Q$.

Definición 29. Un polinomio es **mónico** si su coeficiente principal es 1.

Teorema 9 (Máximo común divisor)**.** *Sean $P, Q \in \mathbb{K}[X]$, con al menos uno distinto de 0. Entonces, $\exists! D(X) \in \mathbb{K}[X]$ que verifique:*

1. *$D|P$ y $D|Q$*
2. *$\exists U, V \in \mathbb{K}[X]$ tales que $D = UP + VQ$*
3. *D es mónico*

*D se denomina **máximo común divisor**, y además verifica que si $S \in \mathbb{K}[X]$ cumple $S|P$ y $S|Q$, entonces $S|D$.*

Demostración. Será por inducción sobre mín$(gr(P), gr(Q))$. Para el caso base, supongamos que tal mínimo es $-\infty$, y sin perder en generalidad, que es $Q = 0$. Entonces, $D = \frac{P}{a}$, donde a es el coeficiente principal de P. En efecto, $D|0$ y $D|P$ ($0D = 0$ y $aD = P$). Además, satisface la identidad de Bézout: $D = \frac{1}{a} P + 1 \cdot 0$, y es mónico puesto que se ha dividido P por su coeficiente principal.

Ahora supongamos que se cumple si mín$(gr(P), gr(Q)) < n$. Veremos que también lo hace para tal mínimo igual a n. Sin perder en generalidad, sea Q el de menor grado. Por división euclídea, $\exists C, R \in \mathbb{K}[X]$ con $gr(R) < gr(Q)$, tales que $P = CQ + R$. Como mín$(gr(Q), gr(R)) < n$, por hipótesis de inducción, $\exists \hat{D}$ con las propiedades de *mcd* para Q y R. Pero entonces:

1. Como $\hat{D}|Q \wedge \hat{D}|R \implies \hat{D}|(CQ + R) \implies \hat{D}|P$.
2. Como $\exists \hat{U}, \hat{V} \in \mathbb{K}[X]$ tales que $\hat{D} = \hat{U}Q + \hat{V}R$, entonces $\hat{D} = \hat{U}Q + \hat{V}(P - CQ) = (\hat{U} - \hat{V}C)Q + \hat{V}P$, luego también se verifica la identidad de Bézout con P y Q.
3. Evidentemente, por hipótesis, $\hat{D}$ es mónico.

Entonces, $\exists mcd(P, Q) = \hat{D}$. □

De la demostración se desprende que si $P = CQ + R$, $gr(R) < gr(Q)$, entonces $mcd(R, Q) = mcd(P, Q)$, luego se aplica también el algoritmo de euclides.

Definición 30 (Polinomios irreducibles)**.** Sea $P \in \mathbb{K}[X], P \neq 0$. P es reducible si $\exists Q, R \in \mathbb{K}[X]$, con $gr(Q), gr(R) < gr(P)$, tales que $P = RQ$. P es **irreducible** si no es reducible, es decir, si $P = RQ \implies gr(R) = 0 \vee gr(Q) = 0$.

Proposición 25. *Sea $P \in \mathbb{K}[X]$ irreducible tal que $P|QR$. Entonces, $P|Q \vee P|R$. Inductivamente, si $P|Q_1Q_2...Q_r$, entonces, $\exists j \in \mathbb{N}$, $1 \leq j \leq r$ tal que $P|Q_j$.*

Para probar lo primero, veamos que si $P|Q$ hemos acabado. Si $P \nmid Q$, entonces $mcd(P, Q) = 1$ puesto que P es irreducible, así que solo lo dividen unidades o él mismo. Como $P \nmid Q$, el máximo divisor común ha de ser una unidad, y como debe ser mónico, será el 1. Entonces, por Bézout, $\exists A, B \in \mathbb{K}[X]$ tales que $AP + BQ = 1$, de modo que $APR + BQR = R$. Como $P|APR$ y $P|BQR$ por hipótesis, entonces $P|R$. □

Proposición 26. *Sea $Q \in \mathbb{K}[X]$, con $gr(Q) \geq 1$. Entonces, $\exists c \in \mathbb{K}^*$ y $P_1, P_2, ...P_r$ mónicos irreducibles tales que $Q = cP_1P_2...P_r$, y son únicos salvo el orden.*

La prueba es análoga a la del teorema fundamental de la aritmética para $\mathbb{N}$.

9.2. Raíces de un polinomio

Definición 31. Si $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, se define su **función polinómica** por $f_p : \mathbb{K} \mapsto \mathbb{K}$, con $f(x) = \sum_{k=0}^{n} a_k x^k$. Muchas veces se denota directamente por $p(x)$.

Definición 32. $a \in \mathbb{K}$ es **raíz** de $P(X)$ si y solo si $p(a) = 0$, es decir, si su función polinómica se anula en ese punto.

Proposición 27. *Sea $a \in \mathbb{K}$, y $P(X) \in \mathbb{K}[X]$. Entonces, el resto de dividir $P(X)$ por $(X - a)$ es $P(a)$. Por tanto, $(X - a)|P \iff p(a) = 0$.*

Demostración. Veamos que $P(X) = (X - a)C(X) + R(X)$ es la división euclídea, y $gr(R(X)) < 1$, luego $R(X) = r \in \mathbb{K}$. Evaluando las funciones polinómicas: $p(a) = (a - a)C(a) + r \implies p(a) = r$.

Observación 17. Sea $P \in \mathbb{K}[X]$, con $gr(P) \geq 2$. Entonces, si tiene una raíz $a \in \mathbb{K}$, es reducible, dado que es divisible por $X - a$ de grado menor.

Proposición 28. *Si $P(X)$ es de grado impar mayor que uno, en $\mathbb{R}$ tiene una raíz y por tanto es reducible.*

Se puede aplicar el teorema de los valores intermedios (ver más en los apuntes de *Cálculo I*). La función polinómica es continua, y como $p(x) = x^n(a^n + \frac{a^{n-1}}{x} + ... + \frac{a_0}{x^n})$, entonces, si $a_n > 0$, $\lim_{x \to +\infty} p(x) = +\infty$ y $\lim_{x \to -\infty} p(x) = -\infty$, de modo que hay valores en los que $p(x) > 0$ y otros en los que $p(x) < 0$, luego $\exists c \in \mathbb{R}$ tal que $p(c) = 0$. Si $a_n < 0$ el procedimiento es análogo.

Proposición 29. *Sea $P(X) = \sum_{k=0}^{n} a_k X^k$, con $a_k \in \mathbb{Z}$ $\forall k \in \mathbb{N}$, $0 \leq k \leq n$. Sea también $q = \frac{u}{v}$, ambos coprimos, es decir, la fracción en forma irreducible, y con $u \in \mathbb{Z}$ y $v \in \mathbb{N}$. Entonces, $p(q) = 0 \implies u|a_0 \wedge v|a_n$.*

Así, por ejemplo, el polinomio $P(X) = 2X^2 - 3X + 1$ no puede tener raíz 2, dado que $2 \nmid 1$.

Demostración. $0 = p(q) = \sum_{k=0}^{n} a_j(\frac{u^j}{v^j})$. Podemos multiplicar ambos lados por v^n: $0 = \sum_{k=0}^{n} a_j u^j v^{n-j}$. Como $v| \sum_{k=0}^{n-1} a_j u^j v^{n-j}$, despejando de la igualdad anterior con 0, se tiene que $v| - a_n u^n$, pero como v es coprimo con u, se tiene que $v| - a_n \implies v|a_n$, y de manera análoga se prueba para $u|a_0$.

Observación 18. Si $P \in \mathbb{K}[X]$ y $a \in \mathbb{K}$ es raíz de P, entonces $P(X) = (X - a)Q(X)$, con $gr(Q) = gr(P) - 1$.

Repitiendo inductivamente:

Proposición 30. *Si $P(X) \in \mathbb{K}[X]$, $\exists a_1, a_2, ...a_m \in \mathbb{K}$ y $U(X) \in \mathbb{K}[X]$ tales que $P(X) = U(X) \prod_{i=1}^{m}(X - a_i)$, con $gr(U) = gr(P) - m$ y U irreducible.*

Una consecuencia es que si P es de grado n, entonces tiene a lo sumo n raíces. Se conoce como **multiplicidad** de una raíz al número de veces que aparece en la lista mencionada anteriormente, (a_1, a_2, ... a_m). Alternativamente, a es raíz de multiplicidad k si $(X - a)^k|P$ y $(X - a)^{k+1} \nmid P$.

9.3. Irreducibilidad en los diferentes cuerpos

Para los cuerpos de coeficientes $\mathbb{C}$ y $\mathbb{R}$ es inmediato distinguir qué polinomios son irreducibles y cuales no:

Teorema 10 (Fundamental del álgebra)**.** *Sea $P \in \mathbb{C}[X]$, con $gr(P) \geq 1$. Entonces, P tiene una raíz en $\mathbb{C}$ y por tanto es reducible.*

Como consecuencia, se tiene que si $P \in \mathbb{C}[X]$ de grado n y de coeficiente principal $c \in \mathbb{C}$, entonces $\exists z_1, z_2, ...z_n \in \mathbb{C}$ tales que $P = c\prod_{i=1}^{n}(X - z_i)$. Así, **los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1**. Este corolario se prueba por inducción en n y usando el teorema fundamental.

Proposición 31. *Sea $P \in \mathbb{R}[X]$, y $z \in \mathbb{C}$ una raíz de P considerado en $\mathbb{C}[X]$. Entonces también es raíz $\overline{z}$.*

Demostración. Está claro que $0 = \sum_{i=1}^{n} a_i z^i$, donde $P(X) = \sum_{i=1}^{n} a_i X^i$. Tomando conjugados, $\overline{0} = 0 = \overline{\sum_{i=1}^{n} a_i z^i} = \sum_{i=1}^{n} \overline{a_i z^i} = \sum_{i=1}^{n} a_i \overline{z}^i$ dado que los a_i son reales luego sus conjugados son ellos mismos.

Como consecuencia, las raíces complejas no reales de P aparecen por pares, luego todas las raíces son $\alpha_1, \alpha_2, ...\alpha_m \in \mathbb{R}$, y $\beta_1, \overline{\beta_1}, ...\beta_r, \overline{\beta_m} \in \mathbb{C}\backslash\mathbb{R}$. Como se tiene que $\forall \beta \in \mathbb{C}$, $(X - \beta)(X - \overline{\beta}) = X^2 - 2XRe(\beta) + |\beta|^2$, entonces:

Proposición 32. *Sea $P \in \mathbb{R}[X]$, con las raíces indicadas arriba y coeficiente principal c entonces $P = c\prod_{i=1}^{m}(X - \alpha_i)\prod_{i=1}^{r}(X^2 - 2Re(\beta_i) + |\beta_i|^2)$ es su descomposición en factores **irreducibles**.*

Esto es así dado que, como se ha visto, los factores se pueden escribir de esta manera, y ademas los factores cuadráticos son irreducibles en $\mathbb{R}$ porque como se ha visto sus 2 raíces son complejas no-reales. Por tanto, **los polinomios irreducibles en $\mathbb{R}[X]$ son los de grado 1 y los de grado 2 sin raíces reales**, es decir, los de forma $aX^2 + bX + c$ con $a \neq 0$ y $b^2 < 4ac$.

Ahora vamos a estudiar una serie de criterios para irreducibilidad en $\mathbb{Q}[X]$, que no es tan sencillo. Para ello, antes:

Definición 33. Se dice que $P \in \mathbb{Z}[X]$ es **primitivo** si y solo si $mcd(\{a_i\}_{i=0}^{n}) = 1$, es decir, si no hay un factor común a todos sus coeficientes.

Lema 4 (Gauss)**.** *Sea $P \in \mathbb{Z}[X]$ primitivo. P es irreducible en $\mathbb{Z}[X]$ $\iff$ P es irreducible en $\mathbb{Q}[X]$.*

Demostración. Se va a probar, equivalentemente, que P es reducible en $\mathbb{Q}[X]$ $\iff$ P es reducible en $\mathbb{Z}[X]$. Evidentemente se tiene $\Longleftarrow$ al ser $\mathbb{Z} \subset \mathbb{Q}$.

Ahora, como lema previo, observemos que **si $A, B \in \mathbb{Z}[X]$ son primitivos también lo es $C = AB$.** Si no lo fuese, $\exists d | c_k$ $\forall 0 \leq k \leq n$. Si p es primo tal que $p|d$, entonces $p|c_k$. Ahora, sea l el menor número tal que $p \nmid a_l$. Entonces, $p|a_k$ si $k \leq l$. Asimismo, sea r el menor tal que $p \nmid b_r$. Entonces, $p|b_k$ si $k \leq r$. Como $c_{l+r} = a_l b_r + \{a_k b_m\}_{k+m=l+r}$, y $p|c_{l+r}$, $p|\{a_k b_m\}_{k+m=l+r}$, se tiene que $p|a_l b_r$, contradiciendo el hecho de que no divida a ninguno.

Visto este lema, se procede a probar $\Longrightarrow$. Supongamos que $P = Q_1 Q_2$, $Q_i \in \mathbb{Q}[X]$ y $gr(Q_i) \geq 1$. Sabemos que $\exists q_i \in \mathbb{Q}$ tal que $Q_i = q_i A_i$ con A_i primitivo (para obtenerlo, sacar los factores correspondientes de Q_i hasta que quede con coeficientes enteros sin factores comunes). Entonces, $P = q_1 q_2 A_1 A_2 = \frac{a}{b} A_1 A_2$, con a, b coprimos. También podemos suponer $a, b > 0$, si no, basta con introducir el signo negativo en A_1. Así, $bP = aA_1A_2$. Como A_1A_2 es primitivo por el lema anterior, sigue que $mcd(\{\text{coeficientes de } aA_1A_2\})$ $= a$, y además, como P es primitivo, $mcd(\{\text{coeficientes de } bP\}) = b$. Como son exactamente los mismos polinomios, sigue que $a = b$, de manera que $P = A_1A_2$, luego es reducible en $\mathbb{Z}[X]$. $\square$

Teorema 11 (Criterio de Eisenstein)**.** *Sea $P(X) = \sum_{i=0}^{n} a_i X^i$ primitivo (luego en $\mathbb{Z}[X]$), y supongamos que $\exists p \in \mathbb{N}$ primo tal que $p|a_i$ $\forall i \in \mathbb{N}$, $0 \leq i \leq n-1$, $p \nmid a_n$ y $p^2 \nmid a_0$. Entonces P es irreducible en $\mathbb{Z}[X]$, y por el lema de Gauss en $\mathbb{Q}[X]$.*

Demostración. Por reducción al absurdo. Supongamos que $P(X) = B(X)C(X)$, con $grB, grC \geq 1$. Denotamos $grB = r$, $grC = s$, luego $grP = r+s = n$. También denotamos a_i los coeficientes de P, y b_i, c_i los de B y C. Sabemos entonces que $a_0 = b_0c_0$, $a_1 = b_0c_1 + b_1c_0$, $a_2 = b_0c_2 + b_1c_1 + b_2c_0$, ... Tomando clases en $\mathbb{Z}_p$, se obtiene que $\overline{a_0} = \overline{b_0}\overline{c_0}$, $\overline{a_1} = \overline{b_0}\overline{c_1} + \overline{b_1}c_0$... Es decir, que si denotamos $\overline{P}(X) = \sum_{i=0}^{n} \overline{a_i} X^i$, $\overline{B}(X) = \sum_{i=0}^{n} \overline{b_i} X^i$, $\overline{C}(X) = \sum_{i=0}^{n} \overline{c_i} X^i$, se verifica que $\overline{P} = \overline{BC}$. Ahora bien, sabemos que $\overline{a_j} = \overline{0}$ si $0 \leq j \leq n-1$, y $\overline{a_n} \neq \overline{0}$. Así, $\overline{P} = \overline{a_n} X^n = \overline{BC}$. Debe ser entonces que $\overline{B} = \overline{b_r} X^r$ y $\overline{C} = \overline{c_s} X^s$. Entonces se tiene $p|b_0$ y $p|c_0$ para que no haya término de grado 0 en $\overline{B}$ ni en $\overline{C}$. Así, $p^2|b_0c_0$ luego $p^2|a_0$, lo cual es contradictorio. □

De esta prueba se extrae una importante observación:

Observación 19. $\overline{AB} = \overline{A} \cdot \overline{B}$ con $A, B \in \mathbb{Z}[X]$.

Que ya hemos probado durante la demostración anterior. Entonces se deduce otro criterio de irreducibiliad:

Proposición 33. *Si $P \in \mathbb{Z}[X]$ es primitivo, reducible en $\mathbb{Z}[X]$, entonces $\overline{P}$ es reducible en $\mathbb{Z}_p[X]$ ($p \nmid a_n$ para evitar que se anule al tomar clases). Como consecuencia, si $\exists p \in \mathbb{N}$ primo, con $p \nmid a_n$, tal que $\overline{P}$ es irreducible en $\mathbb{Z}_p[X]$, entonces es irreducible en $\mathbb{Z}[X]$ y por tanto en $\mathbb{Q}[X]$.*

En efecto, si $P = AB$ con $grA, grB \geq 1$, entonces como $\overline{P} = \overline{A} \cdot \overline{B}$, se tiene que es reducible también en $\mathbb{Z}_p$. □