# Resúmen Matemática 4

### **Práctica 1:**

*Funciones de varias variables - Límites y Continuidad:*

- Una función real f de n variables es una regla que asigna a cada n-upla

de números reales (x1, x2, . . . , xn) un único número real f (x1, x2, . . . , xn). Donde esta n-upla es llamada Dom(f) (dominio) y los valores que toma f en la n-upla es llamada Im(f) (imagen).

*Funciones de dos variables:*

Una función real f de dos variables es una regla que asigna a cada par ordenado de números reales (x, y) un único número real f (x, y). En este caso el dominio de f (Dom(f)), que es el subconjunto de R 2 en el cual está definida la función. Por otra parte, la imagen de f es el subconjunto de R formado por los valores que toma la función f en (x, y).

*Representación gráfica de funciones:*

Se llama gráfica de una función f de dos variables al conjunto de todos los puntos del espacio con coordenadas (x, y, z) tales que (x, y) ∈ Dom(f) y z = f (x, y).

* La función nula tiene como gráfica la superficie z = 0.
* La función constante f(x, y) = c se representa gráficamente como el plano (horizontal) de ecuación z = c.

*Curvas de nivel:*

Se llama curva de nivel k de una función f de dos variables al conjunto de todos los puntos del dominio de la función con coordenadas (x, y) tales que f(x, y) = k, donde k es una constante que pertenece a la imagen de f. Llamando Ck a la curva de nivel k, entonces para cada k ∈ Im(f).

Ck = {(x, y) : (x, y) ∈ Dom(f); f(x, y) = k}

O sea, todos los pares para los cuales f evaluada en los mismos da k (siendo k, cualquier valor de la imagen).

*Límites y Continuidad:*

La idea de límite de f cuando x tiende (se acerca) a x0 es igual a L significa que a medida que x se acerca a x0 los valores que va tomando f se acercan cada vez más al valor de L.

Si el límite por la izquierda es distinto del límite por la derecha, entonces el límite de la función cuando x se acerca a x0 no existe, mientras que si ambos límites laterales existen y coinciden entonces la función tiene ese límite.

Se dice que una función de dos variables f(x, y) tiene límite L (un número real fijo) cuando (x, y) tiende a (x0, y0), si para todos los puntos (x, y) cercanos al punto (x0, y0), los valores f(x, y) son arbitrariamente próximos al número L.

Hay infinitas maneras/direcciones de acercarse a un punto en el plano.

Formalmente el límite existe si dado un número ϵ existe un número δ > 0, tal que ∀(x, y) ∈ Dom(f), entonces:

0 < p (x − x0) 2 + (y − y0) 2 ≤ δ → |f(x, y) − L| < ϵ

Entonces, la definición dice que la distancia entre f(x, y) y L es arbitrariamente pequeña siempre que la distancia entre (x, y) y (x0, y0) sea suficientemente pequeña (aunque no nula). El punto (x0, y0) puede no pertenecer al Dom(f), el único requisito es que los puntos varíen en el Dom(f).

Para determinar si una función f (x, y) tiene o no límite uno elige dos o tres caminos que nos lleven hacia el punto (x0, y0), si resulta que los valores obtenidos para ese límite son distintos según el camino elegido entonces ese límite NO existe. Sin embargo, si se prueba por varios caminos y se obtiene el mismo valor de L esto no alcanza para asegurar que el límite exista y sea ese valor pero nos permite suponer que el límite existe y toma ese valor L para luego demostrarlo efectivamente usando la definición o algunas propiedades.

Como demostrar la existencia del límite por medio de la definición es difícil, existe el teorema del Encaje o criterio del “Sandwich” que establece:

* Si existen funciones g (x, y) y h (x, y) tales que:

g (x, y) ≤ f (x, y) ≤ h (x, y) ∀ (x, y) ≠ (x0, y0)

en un disco con centro en (x0, y0), y si

lim (x,y)→(x0,y0) g(x, y) = lim (x,y)→(x0,y0) h(x, y) = L

entonces:

lim (x,y)→(x0,y0) f(x, y) = L

*Propiedad:*

* Sea c ∈ R una constante, y sean f (x, y) y g (x, y) dos funciones reales de dos variables tales que existen los siguientes límites:

lim (x,y)→(x0,y0) f(x, y) = L

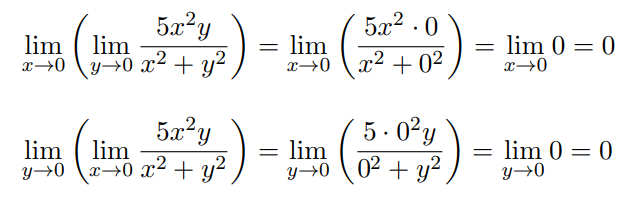
lim (x,y)→(x0,y0) g(x, y) = M

Entonces:

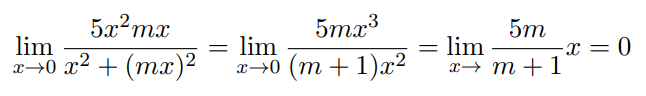
* lim (x,y)→(x0,y0) (f (x, y) + g (x, y)) = L + M
* lim (x,y)→(x0,y0) cf (x, y) = c.L
* lim (x,y)→(x0,y0) (f (x, y).g (x, y)) = L.M
* lim (x,y)→(x0,y0) f (x, y) g (x, y) = L M si M ≠ 0
* si M = 0 y L ≠ 0 entonces lim (x,y)→(x0,y0) f (x, y) g (x, y) no existe.

Se puede analizar que ocurre con la función cuando nos acercamos al punto (0,0) por diferentes caminos:

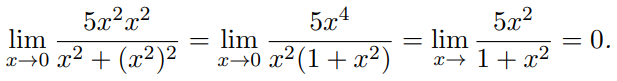
1. Límites Iterados
   1. Ej:



1. Recta ()
   1. Ej:

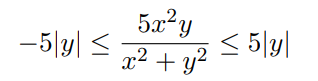


1. Curva ()
   1. Ej:



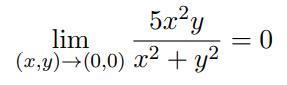
Si los límites dan el mismo resultado (0), puede probarse por el teorema del Encaje que el límite es 0.

1. Teorema del Encaje
   1. Ej:



* Luego, si tomamos g(x, y) = −5|y| y h(x, y) = 5|y| y dado que ambas tienden a

0 cuando (x, y) → (0, 0) el teorema del encaje nos asegura que:



*Coordenadas Polares:*

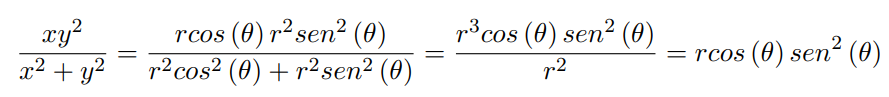
Las coordenadas polares pueden servirnos para calcular límites. En efecto, si recordamos la relación entre las coordenadas polares y las coordenadas cartesianas.

x = r cos (θ) y = r sin (θ)

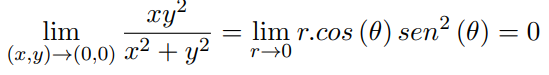
podemos decir que (x, y) → (0,0), por ejemplo, equivale a decir (en coordenadas polares)

r → 0 (independientemente del valor de θ).

Ej:



Con lo cual:



*Continuidad:*

El concepto de función continua está asociado a la idea intuitiva de una función cuya gráfica es una curva que se puede dibujar sin levantar el lápiz del papel, esto es, una curva sin saltos.

Una función real f (x, y) es continua en un punto (x0, y0) si:

* ∃f (x0, y0).
* ∃ lim (x,y)→(x0,y0) f (x, y).
* Se verifica que lim (x,y)→(x0,y0) f (x, y) = f (x0, y0).

Usando las propiedades de los límites se puede mostrar que las sumas, productos y cocientes, así como la composición, de funciones continuas son continuas en sus dominios.

Por ejemplo, una función polinomial de dos variables es continua en todo , la exponencial, seno o coseno de cualquier polinomio en x e y también son funciones continuas en .

Teorema: Si c es un número real y f y g son funciones continuas en (x0, y0), entonces las funciones siguientes son continuas en (x0, y0):

* Múltiplo escalar: c.f
* Suma (y diferencia): f + g
* Producto: f.g
* Cociente: , si g(x0, y0) ≠ 0.

Teorema: Si h es continua en (x0, y0) y g es continua en h(x0, y0), entonces la función compuesta (g ◦ h)(x, y) = g(h(x, y)) es continua en (x0, y0).

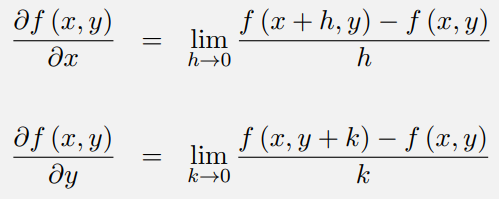
*Diferenciabilidad:*

Intuitivamente podemos ver que la gráfica de una función continua no puede estar “quebrada”, pero ¿qué pasa si la función es derivable?, ¿qué características adicionales tiene su gráfica? Sabemos que la derivada se relaciona con la pendiente de la recta tangente a la gráfica de la función.

*Derivadas Parciales:*

Consideremos una función f (x, y) definida sobre D ⊂ R 2 . Si fijamos una variable, por ejemplo y = b, y permitimos que la otra varíe nuestra función f se convierte en una función de una sola variable y podemos trazar en la curva C1 : z = f (x, b) que corresponde a la gráfica de la función F1(x) = f (x, b) de la variable x (De igual forma si fijamos x = a y la función f queda F2(x) = f (a, y) siendo gráfica de la curva C2 : z = f (a, y)).

Si f (x, y) es una función de dos variables, sus derivadas parciales respecto de x y de y son las funciones definidas por:

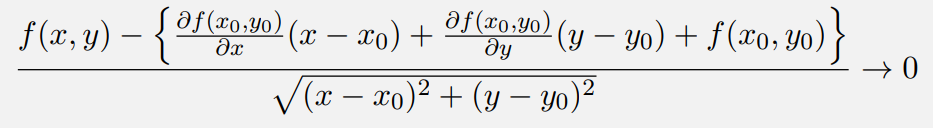


si los límites existen.

La primera representa la razón de cambio instantánea de f con respecto a x cuando y se mantiene fija, es decir cuando el punto (x, y) se mueve en la dirección del vector e1 = (1, 0), y equivalentemente, la segunda corresponde a la razón de cambio instantánea cuando el punto se mueve en la dirección de e2 = (0, 1), esto nos permite decir que las derivadas parciales de f respecto de x e y son las derivadas en las direcciones de los vectores de la base canónica de .

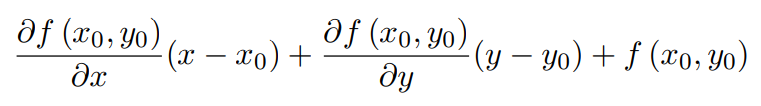
Queremos que al acercarnos suficientemente a un punto de la gráfica de una función (en ), la superficie que forma su gráfica no se distinga del plano tangente en dicho punto, y entonces podamos aproximar localmente la función (de dos variables) mediante una función lineal de dos variables (la que corresponde al plano tangente).

Sea f : D ⊂ R 2 → R y sea (x0, y0) ∈ D. Se dice que f es diferenciable en (x0, y0) ∈ D si:



cuando (x, y) tiende (x0, y0)

Entonces, si se cumple ese límite, el plano tangente



Es una buena aproximación a la función f (x, y) cuando (x, y) se acerca al punto (x0, y0).

Por lo tanto para ver si una función es diferenciable en un punto, debemos calcular las derivadas parciales y el límite, si este tiende a 0 podemos afirmar que la función es diferenciable en el punto evaluado. Además podemos decir que si es diferenciable, entonces es continua. O mediante su contrarrecíproca, si no es continua, entonces no es diferenciable.

*Condición suficiente para la diferenciabilidad:*

Sea f : D ⊂ R 2 → R y sea (x0, y0) ∈ D. Si existen las derivadas parciales y , y además estas son continuas en un entorno del punto (x0, y0), entonces f es diferenciable en (x0, y0).

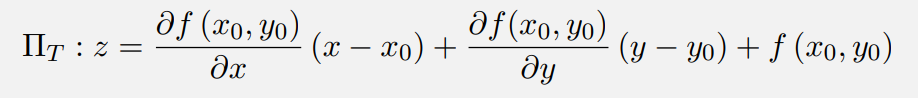
Es importante resaltar que **NO alcanza** con que existan las derivadas parciales de f en el punto dado para que sea diferenciable.

*Propiedades:* Dadas f : D ⊂ R 2 → R y g : D ⊂ R 2 → R funciones diferenciables en un entorno de (x0, y0) ∈ D entonces en ese entorno vale que:

* f + g es diferenciable
* c.f es diferenciable
* f.g es diferenciable
* f /g es diferenciable (suponemos que g nunca es 0 en D)

*Plano Tangente:*

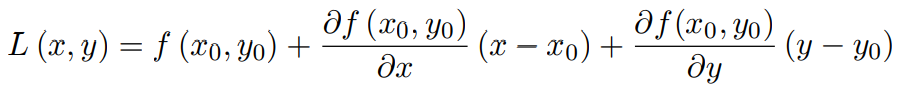
Sea f : D ⊂ → R una función diferenciable en (x0, y0) ∈ D. Una ecuación del plano tangente a la gráfica de f en el punto P0 = (x0, y0, f(x0, y0)) es :



O sea para hallar la ecuación del plano tangente debemos evaluar la función y sus derivadas parciales primeras en el punto (x0,y0).

*Linealización:*

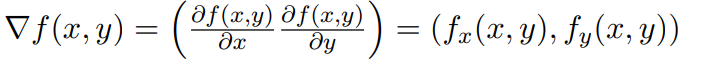
Se denomina linealización de f en el punto P0 = (x0, y0), o también polinomio de Taylor de primer orden alrededor de P0, a la siguiente función de dos variables:



cuya gráfica es el plano tangente ΠT a f en el punto P0.

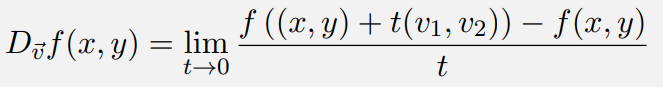
*Vector Gradiente y Derivada Direccional:*

El vector gradiente de una función de dos variables f(x, y) es el vector cuyas componentes son las derivadas parciales de la función f, se lo indica ∇f.



Así como en una variable la derivada de una función representa la dirección de crecimiento o decrecimiento, en varias variables es la derivada direccional de un vector dado la que representa la tasa de cambio de la función en la dirección de ese vector.

Sea f : U ⊂ → R la derivada direccional de f en x en la dirección del vector unitario ⃗v = (v1, v2) está dada por:



si es que el límite existe.

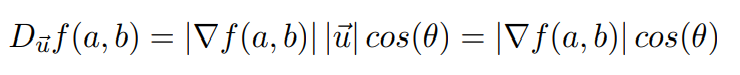
*Teorema:* Si f : D ⊂ → R es diferenciable, entonces existen todas las derivadas direccionales. La derivada direccional de f en x en la dirección de ⃗v está dada por:



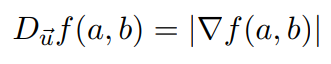
donde ∇f (x) =

*Dirección de máximo crecimiento:*

Recordando propiedades del producto escalar entre vectores, sabemos que v·w = |v| |w| cos(θ) (siendo θ el ángulo entre los dos vectores), la derivada direccional puede escribirse, usando que ⃗u = 1 como:



De la expresión anterior deducimos que la derivada direccional tendrá un valor máximo cuando cos(θ) = 1, lo que ocurre cuando θ = 0, es decir cuando ⃗u y ∇f(a, b) tienen la misma dirección, o sea:



Teorema: Si f(x, y) es diferenciable en (a,b) la dirección de máximo crecimiento de f en (a,b) está dada por la dirección del gradiente de f en (a,b).

Además, la máxima razón de cambio es |∇f(a, b)|

*Extremos de funciones de dos variables:*

Sea f : D ⊂ → R. Se dice que f tiene un máximo local o relativo en (x0, y0) ∈ D, si f(x0, y0) ≥ f(x, y) para todo punto (x, y) en algún disco centrado en (x0, y0). Si la desigualdad se verifica para todo punto del dominio de f , el máximo es absoluto o global.

Se dice que f tiene un mínimo local o relativo en (x0, y0) ∈ D si f(x0, y0) ≤ f(x, y) para todo punto (x, y) en algún disco centrado en (x0, y0). Si la desigualdad se verifica para todo punto del dominio de f , el mínimo es absoluto o global.

Los máximos y mínimos locales constituyen los extremos locales o relativos de f .

Sea f : D ⊂ → R. Un punto (x0, y0) perteneciente al dominio de f es un punto crítico de f si se cumplen algunas de las siguientes condiciones:

* Las dos derivadas parciales primeras de f se anulan en (x0, y0)
* Al menos una de las derivadas parciales primeras de f no existe en (x0, y0)

En el primer caso (o sea, cuando el gradiente de f en el punto es el vector nulo), se dice que (x0, y0) es un punto estacionario de f .

*Teorema:* Sea f : D ⊂ → R, D un conjunto abierto. Si f tiene un máximo o mínimo local en (x0, y0) ∈ D y si existen las derivadas parciales primeras de f en dicho punto, entonces fx(x0, y0) = 0 y fy(x0, y0) = 0.

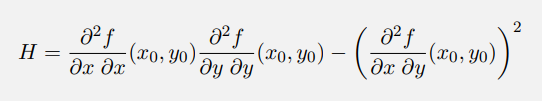
O sea todo extremo local es un punto crítico, pero no todo punto crítico es un extremo.

*Teorema de Clairaut:* Sea f : D → R una función de dos variables definida en un conjunto abierto D ⊆ R 2 , si existen las segundas derivadas cruzadas y son continuas en D, entonces estas son iguales, es decir:

=

*Criterio de las derivadas segundas:*

Sea f : D → R una función de dos variables definida en un conjunto abierto D ⊆ R 2 con segundas derivadas continuas en un entorno de un punto crítico (x0, y0), llamemos:



entonces,

* Si H > 0 y (x0, y0) > 0 entonces f(x, y) tiene un mínimo local en (x0, y0)
* Si H > 0 y (x0, y0) < 0 entonces f(x, y) tiene un máximo local en (x0, y0)
* Si H < 0 entonces f(x, y) no tiene ni un máximo ni un mínimo en (x0, y0). Diremos que f tiene un punto de ensilladura (o punto silla) en (x0, y0).
* Si H = 0 el criterio no decide.

(Obs: se puede usar en lugar de )

*Descenso del Gradiente:*

Los métodos de descenso, en general, utilizan la misma idea subyacente para conseguir una aproximación de la solución óptima: Partiendo de un punto inicial , producir una secuencia de puntos , , …, tales que se minimice cada vez más la función, es decir, f() ≥ f() ≥ f() ≥ · · · ≥ f() Suponiendo siempre que no es el punto donde la función consigue su valor mínimo. Para construir dicha secuencia de puntos partiendo de uno inicial debemos decidir, en cierta forma, para dónde debemos trasladarnos. Podríamos movernos sobre una recta (en cuando la función es de una variable) o sobre un plano (en cuando la función es de dos variables).

Haremos modificaciones utilizando un vector, que funcionará como una brújula y se ajustará a cada paso para indicar nuestro camino hacia el “norte” (la solución óptima). Llamando ∆x a dicho vector indicador:



El factor η (eta) indica un escalamiento del vector de direccionamiento y lo llamaremos tamaño de paso (también conocido como tasa de aprendizaje en el contexto del Deep Learning).

Para mínimo crecimiento, la función queda:



Notemos que cuando la función tome valores muy similares en dos aproximaciones consecutivas, como trataremos con funciones continuas, sería sensato pensar que la actualización fue muy pequeña y por ende nos encontramos cerca de la solución. Esta condición de corte tendrá la forma:



El parámetro ε lo llamaremos tolerancia.

### **Práctica 2:**

*Regresión Lineal:*

La regresión es el estudio de la dependencia entre diferentes aspectos de una situación o experimento. Esta herramienta matemática intenta determinar cuáles de dichos aspectos pueden influenciar en el comportamiento del resto y de qué forma lo hacen.

*Regresión Lineal Simple:*

Como sabemos, una función lineal tiene por gráfica a una recta y una ecuación de la siguiente forma:

y = β0 + β1x

donde β0 es la ordenada al origen y β1 la pendiente.

Sean x1, x2, . . . , xn los valores de la variable independiente para las que se realizarán las observaciones y sean i e yi , respectivamente, la variable aleatoria y el valor observado asociado con xi . Entonces los datos se componen entonces por los n pares ordenados (x1, y1),(x2, y2), . . . ,(xn, yn).

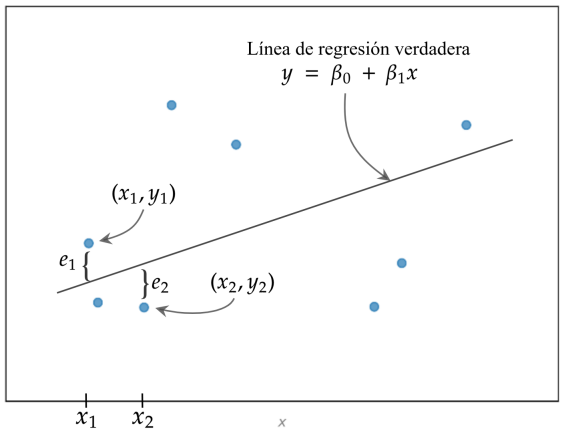
*Modelo de Regresión Lineal Simple:*

Existen parámetros β0, β1 y de tal suerte que con cualquier valor fijo de la variable independiente x, la variable dependiente está relacionada con x por medio de la ecuación de modelo

Y = β0 + β1x + e

La cantidad e en la ecuación de modelo es una variable aleatoria, que se supone está normalmente distribuida con E(e) = 0 y V (e) =

Notemos que sin la presencia del error e, cualquier par observado (x, y) correspondería a un punto que cae exactamente sobre la recta y = β0+β1x, llamada línea de regresión verdadera. Al incluir el término de error aleatorio es posible encontrar puntos (x, y) por encima de la línea de regresión verdadera (cuando e > 0) o por debajo (cuando e < 0). Esta variación en el valor del error se le atribuye precisamente al parámetro que suele ser mayor a 0 y representa la varianza de la variable aleatoria e.



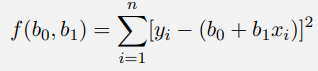
*Método de mínimos cuadrados:*

El método de mínimos cuadrados determina que la recta de mejor ajuste es aquella tal que las distancias verticales de los puntos observados hasta la recta sean las mínimas posibles. La medida que tomará el método es la suma de los cuadrados de estas desviaciones.

La desviación vertical del punto (xi , yi) con respecto a la línea y = β0 + β1x es

la altura del punto - altura de la lÍnea = yi − (β0 + β1x)

La suma de las desviaciones verticales al cuadrado de los puntos (x1, y1), . . . ,(xn, yn) a la lÍnea es entonces



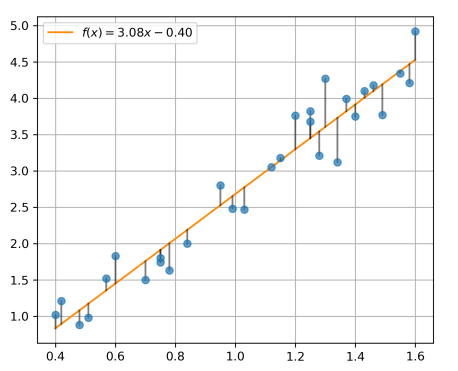
Las estimaciones puntuales de β0 y β1, denotadas por 0 y 1 llamadas estimaciones de mínimos cuadrados, son aquellos valores que reducen al mínimo a f(b0, b1).

Es decir, 0 y 1 son tales que

f(0, 1) ≤ f(b0, b1) ∀ b0, b1

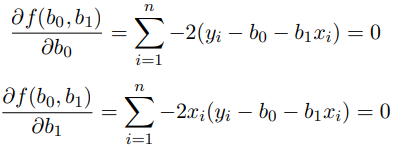
La línea de regresión estimada o línea de mínimos cuadrados es entonces la línea cuya ecuación es:

= 0 + 1x

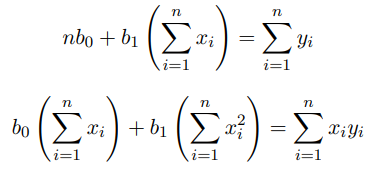


Luego, el método de mínimos cuadrados toma cada una de dichas desviaciones, las eleva al cuadrado y las suma. Aquella recta que minimice la suma será la que se considerará la recta de ajuste.

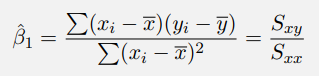
Si calculamos las derivadas parciales de f(b0, b1) con respecto a b0 y b1, y luego las igualamos a 0, podremos hallar los valores minimizantes de estos parámetros:



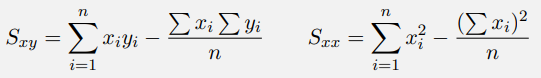
Realizando algunas operaciones algebraicas y reordenando términos se obtiene el siguiente sistema de ecuaciones, llamadas **ecuaciones normales**:



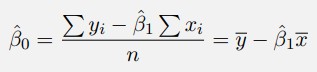
La estimación de mínimos cuadrados de la pendiente β1 de la recta de regresión verdadera será entonces



Otra forma de expresar a Sxy y Sxy es:



La estimación de mínimos cuadrados de la ordenada al origen β0 es:



*Estimación de :*

El parámetro determina la cantidad de variabilidad en el modelo de regresión. Un valor grande de conducirá a (xi , yi) observados que están bastante dispersos en torno a la línea de regresión verdadera, mientras que sea pequeña los puntos observados tenderán a quedar cerca de la línea verdadera.

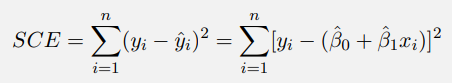
Las desviaciones verticales entre los valores observados y valores ajustados.



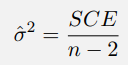
recibirán el nombre de **residuos**.

Los residuos son cantidades que determinan directamente la variabilidad del modelo. Representan los errores que se generan al ajustar una recta a puntos que no siguen una relación totalmente determinística.

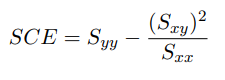
La suma de cuadrados de error o residuales denotada por **SCE**, es:



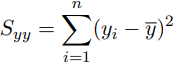
Luego, el estimador insesgado de es:



Forma alternativa:



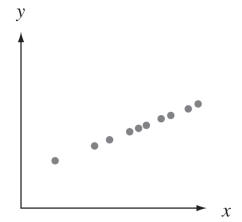
donde



*Coeficiente de determinación:*

Nos indicará cuán bien se ajustó la recta a los datos observados.

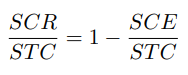
Variación explicada:



La variación total de la variable y denotada por STC podemos escribirla como la suma de la variabilidad explicada SCR y la no explicada SCE. Luego:

STC = SCR + SCE

Si movemos un poco los términos y dividimos a ambos miembros por la variabilidad total (STC) obtenemos la proporción o porcentaje de explicación de la variación por parte del modelo:



Este recibe el nombre de Coeficiente de Determinación, denotado por , está dado por:



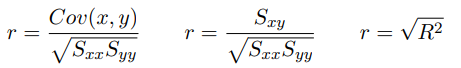
Se interpreta como la proporción de variación y observada que puede ser explicada por el modelo de regresión lineal simple.

tomará valores entre 0 y 1.

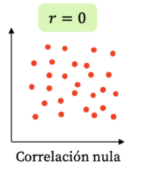
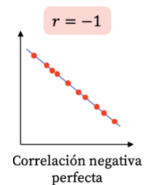
*Coeficiente de correlación lineal:*

El coeficiente de correlación es la medida que podemos usar para describir qué tan fuerte es la relación lineal entre dos variables x e y.

Hay diferentes fórmulas:



r tomará valores entre -1 y 1.

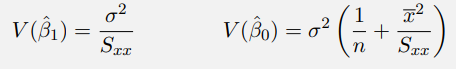


*Inferencias estadísticas:*

Tanto 0 como 1 son estimadores insesgados, es decir:



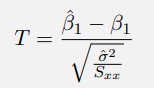
Las varianzas de los estimadores son de la forma



Tanto 0 como 1 están normalmente distribuidas con las varianzas y valores medios mencionados en los puntos anteriores.

*Inferencias sobre β1:*

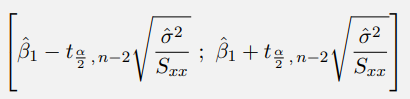
La suposición del modelo de regresión lineal simple implica que la variable estándar (o estadístico)



tiene una distribución t Student con n − 2 grados de libertad.

*Intervalo de confianza para β1:*

Un intervalo de confianza de 100(1 − α)% para la pendiente β1 de la línea de regresión verdadera es:

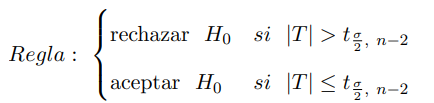


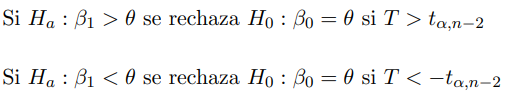
*Tests de Hipótesis sobre β1:*

En este caso deseamos probar la hipótesis de que la pendiente β1 es igual a una constante, por ejemplo θ. Entonces supongamos las hipótesis:

H0 : β1 = θ Ha : β1 ≠ θ

Hay que fijar la regla de decisión:





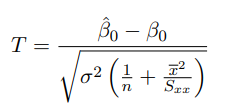
Notemos que aceptar H0 : β1 = 0 implica aceptar que la pendiente de la recta de regresión verdadera es nula, lo que es equivalente a concluir que no existe ninguna relación lineal entre las variables x e Y .

Por otro lado, si se rechaza esta hipótesis nula, significaría que x tiene cierta importancia al explicar la variabilidad de Y .

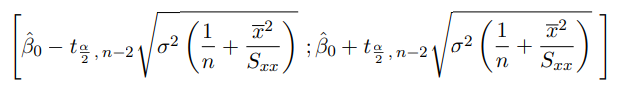
*Inferencias sobre β0:*

*Intervalo de confianza para β0:*

Intervalos de confianza de nivel (1 − α) se deducen de manera análoga a lo visto para β1. En este caso utilizamos el estadístico:



El cual tiene distribución student con n − 2 grados de libertad. Luego, el intervalo es:

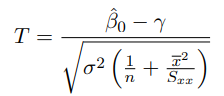


*Tests de Hipótesis sobre β0:*

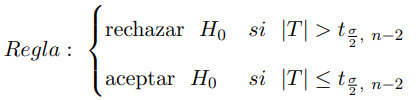
De manera similar a lo visto sobre β1, se puede realizar tests de hipótesis sobre β0. Específicamente si tenemos las hipótesis

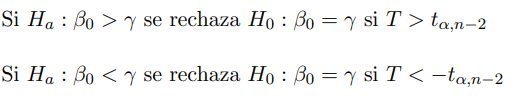
H0 : β0 = γ Ha : β0 ≠ γ

y el estadístico de prueba es:



que bajo H0 : β0 = γ tiene distribución student con n − 2 grados de libertad. Finalmente, la regla de decisión de la prueba es igual a la de β1:





*Intervalo de confianza para la respuesta media:*

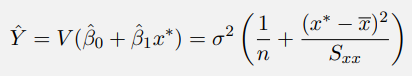
Sea = 0 + 1 , donde es un valor fijo de x. Entonces

La esperanza de es



De forma tal que 0 + 1 es un estimador puntual insesgado de β0 + β1.

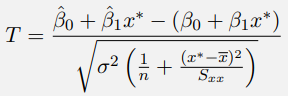
La varianza de es



y la desviación estándar es la raíz cuadrada de esta expresión.

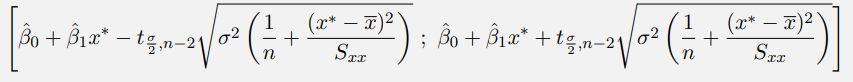
tiene distribución normal con esperanza y varianza anteriores.

*Teorema:* La variable aleatoria



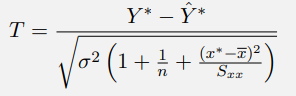
tiene distribución student con n − 2 grados de libertad.

Un intervalo de confianza de 100(1 − α)% para β0 + β1 de la línea de regresión verdadera es:



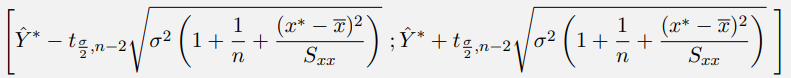
*Intervalo de predicción para valores futuros de Y:*

*Teorema:* La variable aleatoria



tiene distribución student con n − 2 grados de libertad.

Un intervalo de predicción del 100(1 − α)% para es:



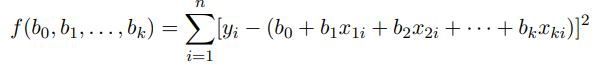
*Regresión Lineal Múltiple:*

La principal ventaja de la regresión múltiple es que nos permite utilizar más información disponible para estimar la variable dependiente.

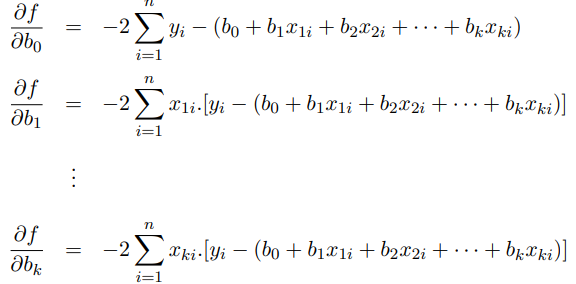
*Modelo de Regresión Lineal Múltiple:*

y = β0 + β1x1 + β2x2 + · · · + βkxk + ε

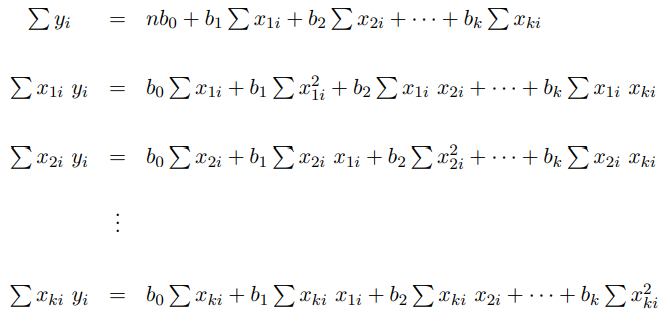
Los coeficientes β0, . . . , βk se estimarán de manera similar que la regresión lineal simple, por el método de mínimos cuadrados buscando minimizar una función de error:



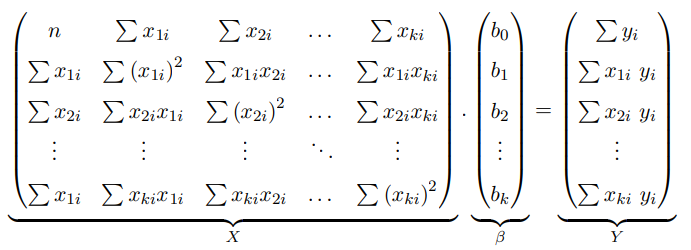
Para hallar las estimaciones de mínimos cuadrados, es decir, los valores bi que hacen mínima a la función f(b0, b1, . . . , bk), debemos calcular las derivadas parciales de f con respecto a cada variable bi.



Igualando cada una de ellas a 0 (para obtener el punto estacionario de la función), obtenemos el siguiente sistema de ecuaciones normales:



El sistema de ecuaciones anterior puede disponerse en forma matricial de la siguiente manera:



La solución del sistema para encontrar los estimadores de los coeficiente será:



La estimación queda de la forma:



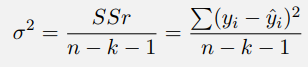
*Varianza y Coeficiente de Determinación:*

Si bien la forma de la estimación de la varianza del modelo y el coeficiente de determinación son similares a aquellas que se utilizan para la regresión lineal simple, sufren algunas modificaciones en el caso de la regresión múltiple.

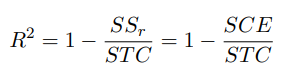
La estimación de la varianza del modelo está basada en la suma de residuos al cuadrado:



*Estimación de la Varianza:*



Por otro lado, considerando al coeficiente de determinación , la forma de calcularlo es idéntica a como lo hacemos para el modelo de regresión simple:



*Coeficiente de Determinación Ajustado:*



Finalmente, la raÍz cuadrada del coeficiente de determinación múltiple se denomina coeficiente de correlación múltiple r:



### **Práctica 3:**

*Los números enteros:*

Un número entero es cualquier elemento del conjunto formado por los números naturales, sus opuestos (versiones negativas de los naturales) y el cero.

El conjunto de los enteros se designa por Z. Z = {.... − 3, −2, −1, 0, 1, 2, 3, .....}

Una característica de los números enteros es que están ordenados:

* El de menor valor absoluto, si el signo común es +.
* El de mayor valor absoluto, si el signo común es −.
* El cero, 0, es menor que todos los positivos y mayor que todos los negativos.

*Operaciones en Z:*

***Suma:***

* Cerrada: Es decir, la suma de dos números enteros da como resultado otro número entero.
* Asociativa: Dados tres números enteros a, b y c, las sumas (a + b) + c y a + (b + c) son iguales.
* Conmutativa: Dados dos números enteros a y b, las sumas a+b y b+a son iguales.
* Elemento neutro: Todos los números enteros a quedan inalterados al sumarles 0: a + 0 = a. para todo a entero.
* Ley de Monotonía de la suma: Dados tres números enteros a, b y c,vale que si a ≤ b entonces a + c ≤ b + c.

***Resta:***

* La resta de dos enteros a − b se realiza sumando el opuesto del entero que quiero restar, es decir: a + (−b)

***Multiplicación:***

* Cerrada: Es decir, la multiplicación de dos números enteros da como resultado otro número entero.
* Asociativa: Dados tres enteros a, b y c, los productos (a.b).c y a.(b.c) son iguales.
* Conmutativa: Dados dos números enteros a y b, los productos a.b y b.a son iguales.
* Elemento neutro: Existe un número entero especial 1 tal que todos los números enteros a quedan inalterados al multiplicarlos por él, a.1 = 1.a = a para cualquier a entero.
* Ley de Monotonía del producto: Dados números enteros a, b,vale que si a ≤ b entonces a.c ≤ b.c si c es positivo y a.c ≥ b.c si c es un número negativo.

*Propiedad distributiva:* Dados tres números enteros a, b y c, el producto a.(b+c) y la suma de productos (a.b)+ (a.c) son idénticos. Es decir, a(b + c) = ab + ac

*Divisibilidad en Z:*

Se dice que está parcialmente definida ya que no siempre es posible efectuarla entre dos enteros cualesquiera. O sea no es cerrada ya que no siempre da como resultado otro entero.

Dados dos números enteros a y b, con b no nulo. Se dice que b divide a a, y se escribe b|a, si existe un entero c tal que:

a = b.c

En este caso se dice que b es un divisor de a, a es divisible por b o que a es múltiplo de b.

*Propiedades básicas:*

* a|a
* 1|a
* a|0
* a|b entonces a| − b, −a|b y −a| − b
* a|b entonces a|bc
* a|b y b|c entonces a|c
* a|b y a|c entonces a|b + c

*Algoritmo de la División:*

Dados a, b ∈ Z con b ≠ 0, cuando no existe el entero c que haga valer la igualdad a = bc, se trata de realizar la división inexacta entre a y b.

Dados a, b ∈ Z con b ≠ 0, existen y son únicos c (cociente) y r (resto) enteros tales que:

a = bc + r con 0 ≤ r < |b|

*Enteros Primos:*

Un número entero p ≠ 1 se dice primo si sus únicos divisores son los triviales (esto es el propio número, su opuesto, 1 y −1). Caso contrario se dice que el número es compuesto. Ej: 2, 3, 5, 7, .... son primos.

*Criba de Eratóstenes:*

La Criba de Eratóstenes es un método algorítmico para encontrar y/o enumerar los primos (positivos) menores que un natural fijo dado.

*Teorema Fundamental de la Aritmética:*

Todo número entero distinto de 0, 1, −1 es producto finito de números primos y esa factorización es única salvo el orden.

*Máximo Común Divisor:*

*Dados a, b ∈ Z no simultáneamente nulos, existe un único entero d > 0 que satisface:*

* *d|a y d|b*
* *Si existe D tal que D|a y D|b entonces D|d*

*Este entero d es el denominado máximo común divisor entre a y b y se lo denota (a, b) o m.c.d(a, b).*

*Algoritmo de Euclides:*

Permite calcular el MCD, su versión extendida, además permite expresarlo como combinación lineal.

Dados a, b ∈ Z, supongamos a ≥ b con b ≠ 0.

Por el algoritmo de la división existen c1 y r1 tales que a = c1b + r1 con 0 ≤ r1 < b.

Si r1 = 0, (a, b) = (b, r1) = (b, 0) = b

Si r1 ≠ 0, podemos decir que existen c2 y r2 tales que b = c2r1 + r2 con 0 ≤ r2 < r1.

Si r2 es cero, ya está, el mcd es r1, si no es cero repetimos el proceso.

Y así sucesivamente.

Concluímos: (a, b) = (b, r1) = (r1, r2) = (r2, r3) = ....... = (rn−1, rn) = (rn, 0) = rn siendo rn el último resto no nulo.

Ej: (60, 45) = (45, 15) = (15, 0) = 15

*Identidad de Bézout:*

Dados a, b ∈ Z y d su m.c.d, existen enteros m y n tales que:

d = ma + nb

Si (a, b) = 1 se dice que a y b son coprimos.

*Mínimo Común Múltiplo:*

Dados a, b ∈ Z, existe un único entero m que satisface:

* a|m y b|m
* Si existe M tal que a|M y b|M entonces m|M

Este entero m se denomina mínimo común múltiplo entre a y b y se lo denota [a, b] o mcm[a, b]

*Números Reales:*

Con los números reales pueden realizarse todo tipo de operaciones básicas (suma, resta, producto, división y además potencias y raíces) con diversas excepciones importantes:

1. No existen raíces de orden par (cuadradas, cuartas, sextas, etc.) de números negativos en números reales.

2. La división por cero no está definida (pues cero no posee inverso multiplicativo)

3. No se puede hallar el logaritmo de un número real negativo, cualquiera sea la base de logaritmos.

El conjunto de los números reales junto con la suma y el producto usual, dotado del orden habitual que es compatible con estas operaciones, tiene estructura de cuerpo.

*Números Racionales:*

Un número racional es todo número que puede representarse como el cociente de dos números enteros (o más precisamente, un entero y un natural positivo, o sea, podemos considerar que el denominador nunca es negativo) Es decir, una fracción común con numerador a y denominador b distinto de cero.

*Equivalencia entre fracciones:*

*= si y sólo si ad = bc*

*Orden de los números racionales:*

Cuando ambos denominadores son positivos < si y sólo si ad < bc

*Operaciones entre Números Racionales:*

***Suma:***

******

* Bien Definida y Cerrada.
* Asociativa.
* Conmutativa.
* Elemento Neutro.

***Resta:***

* El inverso aditivo u opuesto existe y está dado por: −() = =

***Multiplicación:***

* La multiplicación o producto de dos números racionales está dado por:

. =

* Cerrada.
* Asociativa.
* Conmutativa.
* Elemento Neutro.

***División:***

* El inverso multiplicativo existe en los números racionales y está dado por: = con a ≠ 0.
* Se define la división o cociente de dos racionales r entre s distinto de 0, al producto de r por el inverso de s, esto es:

: = .

*Densidad de los racionales:*

Para cualquier par de números racionales existe otro número racional situado entre ellos, propiedad que no está presente en los números naturales ni en los números enteros.

x < < y

*Números Irracionales:*

Un número irracional es un número que no puede ser expresado como cociente de dos enteros, es decir que no puede ser una fracción donde m y n sean enteros (con n diferente de cero)

*Propiedades:*

* La suma y la diferencia de un número racional y de un número irracional es un número irracional.
* El producto de un racional diferente de cero por un irracional es un número irracional.
* El cociente entre un racional no nulo y un irracional, es un número irracional.
* El inverso de un número irracional es número irracional.

La suma y el producto de irracionales no son operaciones cerradas.

*Números Complejos:*

***Forma binómica:***

Definimos al número i (unidad imaginaria) como aquel número que satisface la siguiente igualdad:

i 2 = −1

Esto nos permite ampliar al conjunto de los números reales y por lo tanto escribiremos a un número complejo z de la siguiente forma:

z = a + ib, a, b ∈ R

Al conjunto de números complejos, al que denotaremos como C, se define por comprensión de la siguiente forma: C = {z = a + ib; a, b ∈ R; = −1}

Si tenemos b = 0 “recuperamos” a los números reales.

Si a = 0 decimos que el número complejo es un imaginario puro.

Dado un número complejo z = a + ib, se definen la parte real y la parte imaginaria de z como:

Re(z) = a Im(z) = b

siendo a, b ∈ R.

Dos números complejos son iguales si lo son las partes reales e imaginarias respectivamente.

Es decir, dados dos números complejos z1 y z2, vale la igualdad si :

Re(z1) = Re(z2) y Im(z1) = Im(z2)

*Conjugado:*

El conjugado de un número complejo z = a + ib se lo denota como o y se lo define como: = a − ib

*Operaciones Aritméticas entre Números Complejos:*

***Suma:***

Dados dos números complejos z1 = a1 + ib1 y z2 = a2 + ib2, se define la suma de estos dos números como:

z1 + z2 = (a1 + a2) + i(b1 + b2)

Sumamos “parte real con parte real” y “parte imaginario con parte imaginaria”.

* Cerrada.
* Asociativa.
* Conmutativa.
* Elemento Neutro. (0 = 0 + i0)

***Opuesto y Resta:***

Dado un número complejo z = a + ib se define el opuesto de z y se lo denota como −z al complejo

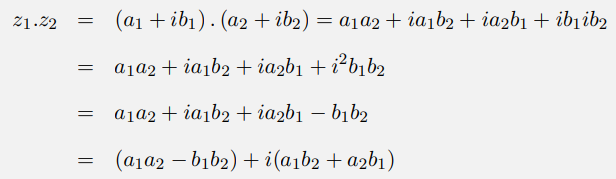
−z = −a − ib.

Esto nos permite definir la operación resta entre dos complejos z1 = a1+ib1 y z2 = a2+ib2 como sigue:

z1 − z2 = (a1 + ib1) − (a2 + ib2) = (a1 + ib1) + (−a2 − ib2)

***Producto:***

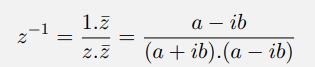
Dados dos números complejos z1 = a1 + ib1 y z2 = a2 + ib2, se define el producto de estos dos números como:



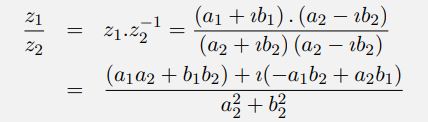
1. Cerrado.
2. Asociativo.
3. Conmutativo.
4. Elemento Neutro. (1 = 1 +i0)

***Inverso y Cociente:***

Dado el número complejo z = a+ib ≠ 0 +i0, se define el inverso de z y se lo denota como al siguiente número:



Dados dos números complejos z1 = a1+ib1 y z2 = a2+ib2 ≠ 0+ı0, se define el cociente de estos dos números y se lo denota como z1 z2 , al producto de z1 con el inverso de z2 es decir:



***Potencias:***

Potencias del número i:

* = 1
* = i
* = −1
* = i = −1.i
* = . = −1. −1 = 1

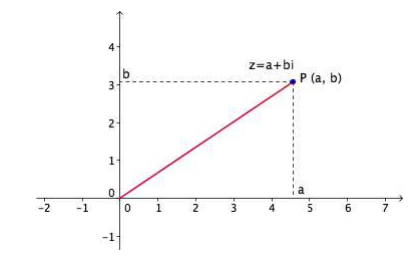
Esto nos permite inferir que = siendo m = 4q + r; 0 ≤ r < 4 ya que:

= = . = . = . = 1. =

*Representación en par ordenado:*

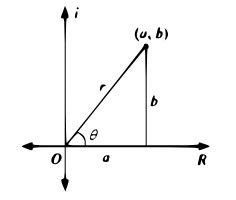
Un número complejo z sería un par ordenado (a, b) donde a es la parte real y b la parte imaginaria de mi complejo.

El concepto de número complejo extiende así la recta real a un espacio bidimensional, el llamado Plano Complejo.



*Módulo y Argumento:*

De la representación en el plano complejo de un número z se puede ver que hay asociado a cada número complejo un número real que es su distancia al origen y llamaremos módulo del complejo y al que denotaremos como |z|, y un ángulo θ, que es el que forma el segmento de recta |z| con el eje real positivo, al que llamaremos argumento de z y se definen de la siguiente forma:



módulo de z = |z| =

argumento de z = θ = arctan(b/a)

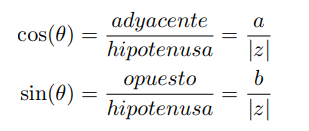
Observemos que hay infinitos ángulos equivalentes a θ (es decir, ángulos que satisfacen que su tangente es igual a b a ) por eso tenemos que elegir el rango para que no haya confusión. (0 ≤ θ < 2π)

En términos de estos valores diremos que dos complejos z y w son iguales si :

módulo de z = |z| = |w| = módulo de w

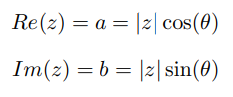
θ = argumento de z = argumento de w = α + 2kπ

Observando el gráfico y recordando propiedades y definiciones trigonométricas:



se puede expresar la parte real y la parte imaginaria de cada complejo en forma binómica

z = a + ib como:



***Forma Trigonométrica:***



***Forma Exponencial:***

Usando la fórmula de Euler:



y la forma trigonométrica de un número complejo, obtenemos una forma cómoda de escribir a un número complejo z que se conoce como forma exponencial del complejo y se la define como:



***Forma Polar:***

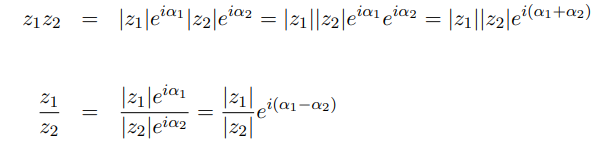
La muy usada forma polar toma los elementos básicos, módulo y argumento. Es muy sencilla y práctica pero no es muy intuitiva para realizar operaciones.



*Operaciones en forma exponencial:*

La forma polar, trigonométrica o exponencial de un complejo resulta muy conveniente para el producto y cociente, y por ende para las potencias (que ya vimos eran tediosas para la forma binómicas).

*Producto y cociente de complejos en forma exponencial:*

**

*Potencias de un número Complejo:*



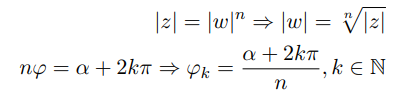
*Raíces n-ésimas de un complejo:*

Dado un número complejo z = |z|, se define a las raíces n-ésimas de z (y se las denota como ), como los números complejos w que satisfacen la siguiente ecuación = z

Luego, dado z = |z| y n ∈ N las raíces n-ésimas de z, las w = |w| tales que = z, cumplen que :



Entonces:



Las raíces n-ésimas de z están dadas por la siguiente expresión:



### **Práctica 4:**

*Relaciones Binarias:*

Dados dos conjuntos no vacíos A y B, una relación binaria definida entre los mismos es un subconjunto del producto cartesiano A × B, caracterizado por alguna propiedad común a sus elementos:

R = {(x, y)/(x, y) ∈ A × B} ⊂ A × B

Muchas veces cuando (x, y) ∈ R escribiremos xRy y diremos que x está relacionado por R con y.

*Dominio e Imagen de una Relación:*

Sea R una relación de A en B.

Se llama dominio de R al conjunto de elementos x de A tales que (x, y) ∈ R

DomR = {x ∈ A : (x, y) ∈ R}

Se llama imagen de R al conjunto de elementos y de B tales que (x, y) ∈ R

ImR = {y ∈ B : (x, y) ∈ R}

*Relación Inversa:*

Sea R una relación de A en B. Se llama relación inversa de R al subconjunto de B × A definido por

= {(y, x) : (x, y) ∈ R}

Ej:

R = {(−8, −2); (−1, −1); (0, 0); (1, 1); (8, 2); (27, 3)}

= {(−2, −8); (−1, −1); (0, 0); (1, 1); (2, 8); (3, 27)}

*Composición:*

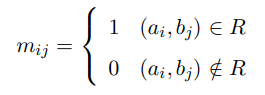
Dadas las relaciones R en A × B y S en B × C se puede construir la relación composición:

SoR = {(x, z) : (x, y) ∈ R,(y, z) ∈ S} ⊂ A × C

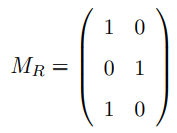
*La matriz de una relación:*

Es posible representar una relación entre dos conjuntos finitos con una matriz.

Sea R una relación entre A = {a1, ....am} y B = {b1, ....bn}, la matriz de representación MR de la relación está dada por:



Ej: Sea R = {(1, r); (2, s); (3, r)} una relación entre A = {1, 2, 3} y B = {r, s}



*Relaciones Binarias en un conjunto:*

*Propiedades:*

* **Reflexividad:** R será reflexiva si para todo x ∈ A vale que xRx
* **Simetría:** R será simétrica si para todo x, y en A vale que xRy implica yRx
* **Antisimetría:** R será antisimétrica si para todo x, y en A vale que xRy e yRx implican que x = y
* **Transitividad:** R será transitiva si para todo x, y, z en A vale que xRy e yRz implican que xRz

*Relaciones de Orden:*

Una relación binaria R definida sobre un conjunto A es un **Preorden** en A si es reflexiva y transitiva.

Y es una relación de **Orden** (o un orden sobre A) si es reflexiva, antisimétrica y transitiva.

*Orden:*

* **Parcial:** refiere a una relación donde hay elementos que no son comparables.
* **Total/Lineal:** Si cada par de elementos en un conjunto es comparable.

*Relación Orden Producto:*

Se llama relación orden producto (estándar) a la relación R ⊂ A1 × A2 × × An definida por: (x1, x2, , xn)R(y1, y2, , yn) si y sólo si x1R1y1, x2R2y2 · · · xnRnyn para todo i = 1....n

Relación Producto Lexicográfico:

Se llama relación producto lexicográfico a la relación L ⊂ A1 × A2 × × An definida por: (x1, x2, , xn)L(y1, y2, , yn) si y sólo si xi = yi para todo i = 1....n, o xjRjyj siendo j el primer índice tal que xj ≠ yj.

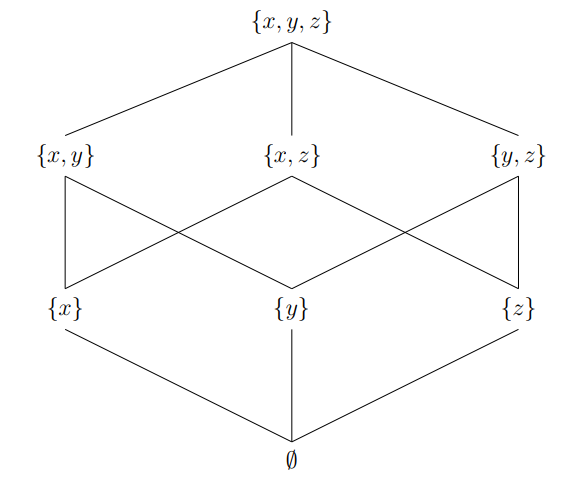
*Conjuntos Ordenados:*

Un conjunto A junto con un orden (parcial/total) R es un conjunto ordenado. (conjunto parcialmente/totalmente ordenado). Generalmente se dice que R ordena al conjunto A y se denota (A, R).

*Diagramas de Hasse:*

Un diagrama de Hasse es una versión simplificada de un digrafo. Es una herramienta muy útil ya que describe completamente el orden asociado.

Ej: Veamos el diagrama de Hasse para un ejemplo particular de S = {x, y, z} .



*Elementos extremos de conjuntos (parcialmente) ordenados:*

Sea (A, <) un conjunto ordenado cualquiera.

Diremos que un elemento a ∈ A es un elemento máximo de A si x < a para todo x ∈ A. De manera dual, un elemento a ∈ A es un elemento mínimo de A si a < x para todo x ∈ A.

Sean (A, <) un conjunto ordenado cualquiera y B un subconjunto de A.

* Un elemento a ∈ A es una cota superior de B si b < a para todo b ∈ B.
* Un elemento a ∈ A es una cota inferior de B si a < b para todo b ∈ B.
* Un elemento a ∈ A se llama supremo de B (mínima cota superior de B) si a es cota superior de B y a < c para toda c cota superior de B.
* Un elemento a ∈ A se llama ínfimo de B (máxima cota inferior de B) si a es cota inferior de B y c < a para toda c cota inferior de B.

*Reticulado:* Un reticulado es un conjunto ordenado (L, <) tal que cada subconjunto {a, b} de dos elementos tiene supremo e ínfimo.

*Relaciones de Equivalencia:*

Diremos que una relación R definida sobre un conjunto A reflexiva, simétrica y transitiva es una relación de equivalencia (∼, ≈ o ≡).

La idea de equivalencia sobre un conjunto permite establecer una relación entre los elementos del conjunto que comparten cierta característica o propiedad. Esto permitirá reagrupar dichos elementos.

*Clases de Equivalencia, Conjunto Cociente y Particiones:*

*Clase de Equivalencia:* Dada una relación de equivalencia R sobre A y un elemento a ∈ A se denominará clase de equivalencia de a por R y se denotará (o R(a)) al conjunto de todos los elementos de A que están relacionados con a por R. Es decir, = {x ∈ A : xRa}

Cualquier elemento de se llama representante de la clase, y en particular, como la relación es reflexiva se da que a ∈ , luego a es representante de la clase para todo a ∈ A.

*Conjunto Cociente:* Al conjunto formado por todas las clases de equivalencia de elementos del conjunto A respecto de la relación R se lo llamará conjunto cociente de A respecto de la relación R y se lo denotará: A/R = { : a ∈ A}

*Partición:* Una partición de un conjunto A es un conjunto de partes no vacías de A, disjuntas dos a dos y tales que su unión coincide con A.

Esto es, dado A un conjunto, y P = {Ai} con i ∈ I (una familia de subconjuntos de A). Se dice que P es una partición de A si y sólo si se verifican:

* Si Ai ∈ P entonces Ai ≠ ∅
* Si Ai , Aj ∈ P entonces Ai ∩ Aj = ∅ para i ≠ j
* i∈I Ai = A

*Lema:* Sea R una relación de equivalencia en un conjunto A, entonces para todos par a, b de elementos de A vale que = si y sólo si aRb

*Teorema:* Si R es una relación de equivalencia en un conjunto A, el conjunto cociente A/R es una partición de A.

*Relación de Congruencia:*

Dados los enteros a, b y m, se dice que a es congruente con b módulo m y se escribe a ≡ b (mod m) (o a ≡m b o a ≡ b (m) ) si y sólo si m|a − b, es decir, existe k ∈ Z tal que a − b = k.m

*Teorema:* Todo entero es congruente módulo m con su resto en la división por m.

*Teorema:* Dos enteros son congruentes módulo m si y sólo si los respectivos restos en su división por m son iguales.

*Teorema:* Sea m ∈ N, Zm = Zm = Z/ ≡m , el conjunto cociente, tiene m clases de equivalencias.

### **Práctica 5:**

*Estructuras Algebraicas:*

Una Estructura Algebraica es un conjunto no vacío dotado con una o más operaciones. Si a cada elemento del producto cartesiano se le asigna únicamente un elemento del conjunto diremos que la operación está bien definida, o que es una operación n-aria en el conjunto.

El nombre de una estructura algebraica (A, ∗) (conjunto A dotado de una operación ∗) indica qué propiedades verifica la operación y permite asegurar que se cumplirán ciertos resultados, sin importar los elementos o la operación en particular de que se trate.

*Propiedades:*

* **Grupoide:** Se dirá que (A, ∗) tiene estructura de grupoide si la operación ∗ es una operación binaria.
* **Semigrupo:** Se dirá que (A, ∗) tiene estructura de semigrupo si ∗ es asociativa. Si además ∗ es conmutativa se dirá un semigrupo conmutativo.
* **Monoide:** Se dirá que (A, ∗) tiene estructura de monoide si ∗ es asociativa y existe en A elemento neutro para ∗ . Será monoide conmutativo si ∗ es además conmutativa.
* **Grupo:** Se dirá que (A, ∗) tiene estructura de grupo si ∗ es asociativa, existe en A elemento neutro para ∗ y cada elemento de A tiene inverso. Si ∗ es además conmutativa se llamará grupo conmutativo (o Abeliano)

***Anillo:***

Si tengo dos operaciones binarias, que en general se llaman suma y producto, la terna ordenada (A, +, .) tiene estructura de anillo si (A, +) es un grupo conmutativo, el producto es asociativo y se satisfacen:

* Distributividad por la izquierda: para cualesquiera a, b, c a(b + c) = ab + ac
* Distributividad por la derecha: para cualesquiera a, b, c (a + b)c = ac + bc

*Observación:*

Cualquiera sea n ∈ N se indicará con a n el resultado de operar a consigo mismo n veces, esto es a ∗ a ∗ · · · ∗ a = a · . . . a

*Leyes de los exponentes:* Dado un semigrupo (S, ∗), a ∈ S y m, n naturales, valen:

*Grupos:*

Podemos asegurar que en cualquier grupo:

* el elemento neutro es único
* todo elemento tiene un único inverso
* valen las propiedades cancelativas

*Otras Propiedades:*

* Cualquiera sea a ∈ G,
* Cualesquiera sean a, b ∈ G,

*Grupo Cíclico:*

Un grupo G se dice que es cíclico si existe a ∈ G tal que para todo elemento b ∈ G existe un entero k tal que b = a k . En este caso decimos que a es un generador de G y escribimos

G =< a >

*Teorema:* Todo grupo cíclico es abeliano

*Grupos cíclicos finitos:* Si G es un grupo cíclico de orden m, entonces G = {e, a, , ...., }

*Subgrupos:*

Dado un grupo (G, ∗) y dado H ⊂ G, si (H, ∗) constituye en sí mismo un grupo se dice que es un subgrupo de G.

Al heredar la operación del grupo se heredan sus propiedades. Es decir, la asociatividad de ∗ en H está garantizada pues se cumple para todos los elementos de G , en particular se cumple para los de H. También si ∗ es conmutativa en G será conmutativa en H.

Luego, para que H sea subgrupo (o sea, un grupo) solo será es necesario que:

* e ∈ H, el elemento neutro de ∗ en G debe estar en H (recordemos que el neutro es único)
* a, b ∈ H → a ∗ b ∈ H, la operación debe ser cerrada en H (era cerrada en G)
* a ∈ H → a −1 ∈ H, cada elemento de H tiene su inverso en H (sabemos que el inverso existe pero en G, hay que asegurar que esté en H)

*Otra forma de probar que es un subgrupo (más sencilla):*

Dado un grupo (G, ∗), un subconjunto H ⊂ G resultará un subgrupo de G si y sólo si :

* e ∈ H
* si a, b ∈ H entonces ∈ H

*Teorema:* Si (G, ∗), es un grupo cíclico y (H, ∗) es un subgrupo de (G, ∗), entonces (H, ∗) es cíclico.

*Aritmética modular:*

La aritmética modular es una forma de representar números para que su valor nunca exceda un cierto límite, llamado módulo.

Por ser la congruencia una relación de equivalencia en Z, determina una partición del conjunto de los números enteros en clases de equivalencia que se denominan clases de congruencia módulo m .

La clase de congruencia módulo m de un número x será el conjunto x = {y ∈ Z : y ≡m x}

*Teorema:* Sea m ∈ N, Zm = Zm = Z/ ≡m , el conjunto cociente, tiene m clases de equivalencias.

*Aritmética en Zm:*

La relación de congruencia es compatible con la suma y el producto.

Dados a, b, c, d ∈ Z tales que a ≡m b y c ≡m d. Entonces se cumple que:

* a + c ≡m b + d
* a · c ≡m b · d

*Operaciones en Zm:*

Suma:

* Asociatividad
* Conmutatividad
* Existencia del neutro
* Todo elemento tiene opuesto

Producto:

* Asociatividad
* Conmutatividad
* Existencia del neutro
* El producto se distribuye en la suma

*Elementos invertibles:*

Dado ∈ Zm, decimos que es invertible (o divisor de la unidad), si: existe ∈ Zm tal que · =

*Teorema:* Sea ∈ Zm, es invertible si y sólo si (a, m) = 1

Dado ∈ Zm no nulo, decimos que es divisor de 0 si: existe ∈ Zm,≠ 0 tal que · =

*Corolario:* Si m ∈ Z es primo, Zm es un cuerpo

*Teorema:* Dado a ∈ Zm, a es invertible si y sólo si a NO es divisor de 0

*Aplicaciones a la criptografía:*

*Cifrado de César:*

Es un tipo de cifrado por sustitución en el que una letra de un texto es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D(situada 3 lugares más abajo o a la derecha de la A, depende de cómo organicemos el alfabeto), la B sería reemplazada por la E, y así siguiendo.

*El cifrado RSA:*

Aquí está el algoritmo de generación de claves públicas:

1. Elegir 2 números primos (muy grandes), p y q

2. Calcular el módulo r donde r = p · q (esto es fácil de calcular, pero puede ser difícil de revertir) (Utilizaremos luego este módulo en el proceso de encriptación y desencriptación)

3. Calcular la función de Euler ϕ = (p − 1) · (q − 1)

4. Elegir un número mayor que 1 y menor que ϕ que sea coprimo con ϕ (es decir cualquier número menor (si se elige mayor se vuelve a ajustar por el módulo) que ϕ que no tenga divisor común con él). Llamar a este número e

5. e es el exponente público Las claves públicas para RSA vienen en un par: una mitad es el módulo RSA y la otra un exponente. Por ejemplo, si el módulo RSA r fuera 183 y el exponente e fuera 97, la clave quedaría así: {183, 97}.

6. El exponente privado d es la inversa de e módulo ϕ (es decir, e · d ≡ϕ 1

7. Producir la clave privada encontrando la inversa modular de la pública utilizando ϕ como módulo.

*Morfismos de grupos:*

Dados dos grupos (G1, ∗) y (G2, ⊗) se dirá que una función f : G1 → G2 es un morfismo de grupos si y sólo si “respeta” las operaciones, en la siguiente forma:

f(a ∗ b) = f(a) ⊗ f(b) para todo a, b ∈ G1

**Monomorfismo:** cuando es inyectivo

**Epimorfismo:** cuando es sobreyectivo

**Isomorfismo:** cuando es biyectivo (o sea, inyectivo y sobreyectivo)

* Sean los grupos (G1, ∗) y (G2, ⊗) y f : G1 → G2 un morfismo entre ellos, entonces f(e1) = e2 (siendo e1 y e2 los neutros respectivos a cada grupo).
* Además para cualquier a ∈ G1, f() =

Se denomina núcleo del morfismo f al conjunto Nu(f) = {a ∈ G1 : f(a) = e2} es decir al subconjunto del dominio formado por todos los elementos cuya imagen es el neutro del codominio.

Se denomina imagen del morfismo f al conjunto Im(f) = {b ∈ G2 : ∃a ∈ G1, f(a) = b}

Sean los grupos (G1, ∗) y (G2, ⊗). Si f : G1 → G2 un morfismo de grupos entonces es Nu(f) e Im(f) son subgrupos de G1 y G2 respectivamente.

### **Práctica 6:**

*Espacios Vectoriales:*

Un Espacio Vectorial sobre el cuerpo K es una estructura algebraica (V,+,.) creada a partir de un conjunto no vacío V , una operación interna “+” llamada suma (definida sobre los elementos del conjunto V ), y una operación externa “.” llamada producto por escalar (definida entre dicho conjunto y el cuerpo matemático K, que serán los reales o los complejos).

*Propiedades:*

*Clausura:*

* “+” es cerrado en V , es decir, ∀v1, v2 ∈ V, v1 + v2 ∈ V .
* “.” es cerrado en V , es decir, ∀v ∈ V y ∀k ∈ K, k.v ∈ V .

*Suma:*

* “+” debe ser conmutativa, es decir: ∀v1, v2 ∈ V ; v1 + v2 = v2 + v1.
* “+” debe ser asociativa: ∀v1, v2, v3 ∈ V ; (v1 + v2) + v3 = v1 + (v2 + v3).
* Existencia del elemento neutro para “+”, es decir, ∃0 ∈ V : v + 0 = v, ∀v ∈ V .
* Existencia del opuesto, es decir, ∀v ∈ V, ∃ − v ∈ V : v + (−v) = 0.

*Producto:*

* “.” sea asociativa: ∀α, β ∈ K y ∀v ∈ V ; (αβ).v = α(β.v).
* “.” sea distributiva respecto de la suma de escalares ∀α, β ∈ K y ∀v ∈ V ; (α + β).v = α.v + β.v.
* “.” sea distributiva respecto de la suma de vectores: ∀α ∈ K y ∀v1, v2 ∈ V ; α.(v1 + v2) = α.v1 + α.v2.
* ∀v ∈ V, ∃1 ∈ K : 1.v = v.

*Teorema:* Sea V un espacio vectorial. Entonces:

* Para todo escalar α vale que α.0 = 0
* Para todo v ∈ V , se cumple 0.v = 0
* Si α.v = 0 entonces α = 0 o v = 0 (o ambos son nulos)
* Para todo v ∈ V vale que −1v = -v

*Subespacios Vectoriales:*

Un subespacio S de un espacio vectorial V es cualquier subconjunto (no vacío) S de V tal que él mismo es un espacio vectorial. Esto es, un subconjunto S de V que es cerrado bajo las operaciones de suma de vectores y multiplicación por un escalar.

Sea V espacio vectorial, y sea S ⊂ V . Entonces S es un subespacio de V si y sólo si se satisfacen las siguientes condiciones:

* S ≠ ∅
* ∀s1, s2 ∈ S → s1 + s2 ∈ S.
* Dado k ∈ K y ∀s ∈ S → k.s ∈ S.

*Conjunto Generador - Espacio Generado:*

Dado un conjunto de vectores S = {v1, v2, . . . , vr} del espacio vectorial V , se llama combinación lineal de los vectores de S, a los vectores v de la forma v = c1v1 + c2v2 + · · · + crvr, donde los coeficientes c1, c2 . . . , cr son escalares.

Al conjunto de todos los vectores que se obtienen como combinación lineal de los vectores de S se lo denomina el espacio generado por S.

*Independencia Lineal:*

Nuestro propósito será encontrar al conjunto generador “más pequeño” posible de un espacio vectorial V, es decir, conjuntos generadores de V con la menor cantidad posible de vectores.

Un conjunto de generadores minimal para V será aquel conjunto S de vectores que no tenga elementos redundantes o innecesarios, es decir, todos los vectores del conjunto S deben ser necesarios para generar V.

Los vectores v1, v2, . . . , vp de un espacio vectorial V se dicen linealmente independientes si la combinación c1v1 + c2v2 + · · · + crvr = 0 implica que todos los ci son nulos. Si no todos los escalares son nulos, serán linealmente dependientes.

*Base y Dimensión:*

Un conjunto de vectores v1, v2, . . . , vr forma una base del espacio vectorial V , si y sólo si:

* {v1, v2, . . . , vr} son linealmente independientes
* {v1, v2, . . . , vr} generan V .

*Teorema:* Si B = {v1, ...., vn} es una base de un espacio vectorial V, todo conjunto

M = {u1....um} de m > n vectores de V es linealmente dependiente.

*Corolario:* Si B = {v1, ...., vn} y B′ = {u1....um} son dos bases de un espacio vectorial V, entonces m = n.

Es decir, todas las bases de un espacio vectorial V (finitamente generado) tienen el mismo número de elementos.

*Dimensión:* Si una base de un espacio vectorial V tiene n vectores, se dice que V tiene dimensión n.

*Dato:* El subespacio {0} se dice que tiene dimensión 0.

*Teorema:* Si V es un espacio vectorial de “dimensión n” (n > 0) entonces:

* Cualquier conjunto de n vectores “linealmente independientes” de V genera todo V (forman una base de V ).
* Todo conjunto de n vectores que generan V son “linealmente independientes” (o sea, forman una base de V ).

Esto dice que si sabemos la dimensión del espacio y tenemos la cantidad necesaria de vectores no hace falta probar las dos condiciones para ser base, con alguna de las dos bastará.

*Transformaciones Lineales:*

Una transformación lineal es una aplicación de un espacio vectorial V en otro espacio vectorial W, y se la denota como L : V → W, si satisface:

* ∀v1, v2 ∈ V, L(v1 + v2) = L(v1) + L(v2)
* ∀α ∈ K y ∀v ∈ V, L(α.v) = α.L(v).

O, equivalentemente, ∀α, β ∈ K y ∀v1, v2 ∈ V, L(αv1 + βv2) = αL(v1) + βL(v2)

La transformación Identidad ∀v ∈ V, I : V → V definida por I(v) = v.

La transformación Nula ∀v ∈ V, N : V → V definida por N(v) = .

*Propiedades:*

Dada una transformación lineal L : V → W, se cumplen las siguientes propiedades:

* L(0v) = 0w.
* ∀v ∈ V, L(−v) = −L(v).
* Si v1, . . . , vn ∈ V entonces L(α1v1 + · · · + αnvn) = α1L(v1) + · · · + αnL(vn).

*Imagen y Núcleo de una transformación lineal:*

El Núcleo de una transformación lineal L es el conjunto de vectores v ∈ V que son transformados o “enviados” al vector nulo 0w de W. Es decir,

Nu(L) = {v ∈ V : L(v) = 0w}

La Imagen de la transformación lineal L es el conjunto de vectores w ∈ W que son imagen por L de elementos v ∈ V y se denota como Im(L) o L(V).

Im(L) = {w ∈ W : ∃v ∈ V w = L(v)}

*Teorema:* Si L : V → W es una transformación lineal entre los espacios vectoriales V y W, entonces el Núcleo es un subespacio de V y la Imagen es un subespacio de W.

*Teorema:* Si L : V → W es una transformación lineal entre los espacios vectoriales V y W de dimensión finita, entonces:

dim(Nu(L)) + dim(Im(L)) = dim(V )

*Corolario:*

* Una transformación lineal inyectiva conserva la independencia lineal.
* Una transformación lineal sobreyectiva cubre todo el codominio.

*Representación matricial-Matriz asociada:*

Consideremos una transformación L : V → W, con V un espacio vectorial de dimensión n y W otro espacio vectorial (que eventualmente puede ser igual a V ) de dimensión m, y sean BV = {v1, v2, . . . , vn} y BW = {w1, w2, . . . , wm} bases de V y W respectivamente.

Primeramente evaluamos cómo actúa L sobre cada vector de la base BV y luego escribiremos al vector resultante (que pertenece al subespacio W) en términos de los vectores de la base BW .

En efecto,

L(vj ) = w = a1jw1 + a2jw2 + · · · + aijwi + · · · + amjwm

Entonces, con las coordenadas aij formamos la columna j de la matriz A que representar´a a L en las bases BV y BW , es decir:

