# Benemérita Universidad Autónoma de Puebla

## Facultad de Ciencias Físico-Matemáticas

**Introducción a la teoría de grupos y anillos**

Tesis presentada como requisito para la obtención del título de:

Licenciado en Matemáticas

Presentada por:
Marcos Ramírez Mejía

Dirigida por:
Dr. David Villa Hernández

3 de febrero de 2015
Puebla, Puebla.

# Dedicatorias

Dedico este trabajo a mis padres:

Federico Ramírez Ordaz y Leovigilda Mejía Bonilla.

A mis hermanos:

Alejandro Ramírez Mejía, César Octavio Ramírez Mejía, Soledad Ramírez Mejía.

Y a mi hermano gemelo:

Ignacio Ramírez Mejía.

Gracias por todo su cariño y apoyo.

Este logro en mi vida jamás hubiera sido posible sin todos ustedes.

# Agradecimientos

Quiero agradecer mis compañeros Noemi Sampayo Paredes, Olivia Pozo Carranza, Pilar Macias Patraca y María Guadalupe Torres.

Al laboratorio de Lógica Matemática y a su director el Dr. José Ramón Enrique Arrazola Ramírez, gracias por su sincera amistad y por toda la ayuda que me ha prestado durante todo este tiempo. A todos los integrantes del laboratorio de lógica matemática: A Juan Manuel, Miguel Pérez, Javier Casas, Juan Pablo, Ruben Velez, Verónica Borja, Arturo Abraham, Florencio Corona, Alejandro Ramírez, Noe Tapia, Reinaldo Martínez y a Iván Martínez. No estoy seguro si falta alguien por nombrar, pero en este momento sólo alcancé a recordarlos a ustedes. Muchas gracias por todo.

A mis sinodales, la M. C. Brenda Zavala López, al Dr. César Cejudo Castilla y al Dr. José Ramón Enrique Arrazola Ramírez por revisar mi trabajo y enriquecerlo con sus correcciones y aportaciones.

Y finalmente, a mi asesor el Dr. David Villa Hernández, por darme la oportunidad de trabajar con el. Por tenerme paciencia durante estos 24 meses. Muchas gracias por todo Dr. David.

# Introducción

Uno de los principales problemas abiertos, después del descubrimiento de las fórmulas cúbicas y cuadráticas en los 1500, fue encontrar una fórmula para las raíces de polinomios de grado superior, y continuó abierto por lo menos durante 300 años. En los primeros 100 años, los matemáticos reconsideraron qué significa "número", para comprender la fórmula cúbica forzaron preguntas como, si los números negativos son en realidad números ó si los números complejos son entidades legítimas. Cerca de 1800, P. Ruffini afirmaba que no existía una fórmula quinta (que tuviera la misma forma como las cuadráticas, cúbicas o cuárticas; es decir, usando operaciones aritméticas y las raíces $n$-ésimas), pero sus contemporáneos no aceptaron su prueba (sus ideas son de hecho correctas, pero, su prueba tenía lagunas). En 1815, A. L. Cauchy introdujo la multiplicación de permutaciones y probó propiedades básicas de lo que llamamos el grupo simétrico $S_n$. En 1824, N. Abel (1802-1829) otorgó una prueba aceptable sobre el hecho de que no existe una fórmula quíntica; en su prueba, Abel construyó permutaciones de las raíces de una quíntica, usando ciertas funciones racionales introducidas por J. L. Lagrange en 1770. E. Galois (1811-1832), el joven mago quien sería asesinado antes de su cumpleaños número 21, modificó las funciones racionales pero, aún más importante, observó que la llave para entender el problema involucraba un concepto que él llamaba "grupo": subconjuntos de $S_n$ que son cerrados bajo la multiplicación (en nuestro lenguaje, subgrupos de $S_n$). Para cada polinomio $f(x)$, él asoció un grupo, ahora llamado el grupo de Galois de $f(x)$. El reconoció la conjugación, subgrupos normales, grupos cocientes y grupos simples; y él demostró, en nuestro lenguaje, que un polinomio (sobre un campo de característica 0) tiene fórmula para sus raíces, análoga a la fórmula cuadrática, si y sólo si su grupo de Galois es un grupo soluble (solubilidad es una propiedad general de la conmutatividad). Un descubrimiento tan importante que hace a Galois uno de los más destacados fundadores del álgebra moderna.

# Índice general

# Capítulo 1

# Grupos

## 1.1. Permutaciones

**Definición 1.1.1**
Una permutación de un conjunto $X$ es una biyección de $X$ en $X$. También decimos que una permutación es una reordenación de los elementos de $X$.

**Ejemplo 1**
Los reordenamientos de $X = \{1,\ 2,\ 3\}$ son:

$$\{1,\ 2,\ 3\},\ \{1,\ 3,\ 2\},\ \{2,\ 1,\ 3\},\ \{2,\ 3,\ 1\},\ \{3,\ 1,\ 2\},\ \{3,\ 2,\ 1\}$$

Sea $X = \{1,\ 2,\ 3, \ldots,\ n\}$. Un reordenamiento de $X$ es una lista sin repeticiones de todos sus elementos; y el número de permutaciones de $X$ es exactamente $n!$.

Ahora, un reordenamiento de $i_1,\ i_2, \ldots,\ i_n$ de $X$ determina una función $\alpha : X \to X$ tal que $\alpha(1) = i_1, \ldots,\ \alpha(n) = i_n$. Claramente es una biyección. En el ejemplo $\{2,\ 1,\ 3\}$ determina la función $\alpha(1) = 2,\ \alpha(2) = 1$ y $\alpha(3) = 3$. Usaremos la siguiente notación:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

Una de las ventajas de ver las permutaciones como funciones, es la posibilidad de usar la composición de funciones como operación. Lo que nos lleva a la siguiente definición.

**Definición 1.1.2**
La familia de todas las permutaciones de $X$ la denotaremos por $S_X$ (llamada el grupo de simetrías de $X$).

Cuando $X = \{1,\ 2,\ 3, \ldots,\ n\}$, $S_X$ se denota por $S_n$ (llamado el grupo simétrico de $n$ letras).

Usaremos la notación $\beta\alpha$ en lugar de $\beta \circ \alpha$ y (1) en lugar de $1_X$.

**Observación 1**
La composición en $S_3$ no es conmutativa, por ejemplo considere las permutaciones.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ y } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ entonces } \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ y}$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

**Definición 1.1.3**
Sean $i_1,\ i_2, \ldots,\ i_r$ enteros distintos de $\{1,\ 2,\ 3, \ldots,\ n\}$ si $\alpha \in S_n$ fija los otros $n - r$ elementos y

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3, \ldots,\ \alpha(i_{r-1}) = i_r,\ \alpha(i_r) = i_1$$

Entonces $\alpha$ es llamado un $r$-ciclo, o bien, un ciclo de tamaño $r$ y lo denotaremos por

$$\alpha = (i_1\ i_2 \cdots\ i_r)$$

1) Un 2-ciclo intercambia $i_1$ con $i_2$ y deja fijos el resto de los elementos. Un 2-ciclo es llamado una **transposición**.

2) Un 1-ciclo es la identidad.

3) Ciclo es del griego círculo.

En la siguiente ilustración podemos ver como una permutación puede ser representada como un círculo, con los elementos $i_n$ "girando" sobre el.

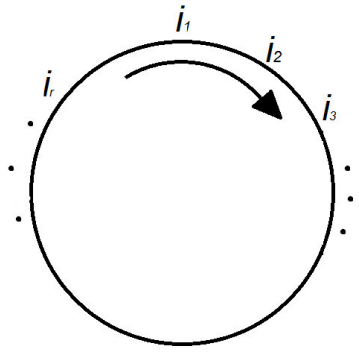



Figura 1.1: Las permutaciones de $S_n$

Hay $r$ diferentes notaciones para un $r$-ciclo.

$$(i_1\ i_2 \cdots\ i_r) = (i_2\ i_3 \cdots\ i_r\ i_1) = \ldots = (i_r\ i_1 \cdots\ i_{r-2}\ i_{r-1})$$

A continuación presentamos un algoritmo para factorizar una permutación en producto de ciclos. Sea $\alpha$ una permutación en $S_9$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$$

El primer ciclo comienza con el uno, hasta cerrar el primer ciclo, en este caso (1 6). El segundo ciclo comienza con el primer símbolo que no aparece en el primer ciclo, en este caso "2", cerramos el segundo ciclo, obteniendo en este caso (2 4). El tercer ciclo comienza con el primer símbolo que no aparece en los ciclos anteriores, en este caso "3", así sucesivamente hasta obtener una factorización de la permutación.

$$\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)$$

**Ejemplo 2**
Sea $\sigma = (1\ 2)(1\ 3\ 4\ 2\ 5)(2\ 5\ 1\ 3) \in S_5$, encontrar su notación en forma de permutación:

Primero iniciamos con el 1, y vemos que el primer ciclo lo manda al 3, luego vemos que el siguiente ciclo manda el 3 al 4 y en la transposición el cuatro queda fijo. Para el 2 vemos que el primer ciclo lo manda al 5, en el segundo vemos que el 5 va al 1 y en la transposición el 1 va al 2 y queda fijo en la permutación $\sigma$. Y así seguimos sucesivamente.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$

Usando el algoritmo para descomponer en ciclos, tenemos $\rightarrow\ \sigma = (1\ 4)(2)(3\ 5)$ y hemos factorizado en "ciclos ajenos".

**Definición 1.1.4**
Dos permutaciones $\alpha,\ \beta \in S_n$ son llamadas ajenas o disjuntas si toda $i$ que mueve una es fija bajo la otra permutación, es decir: Si $\alpha(i) \neq i\ \Rightarrow\ \beta(i) = i$ y si $\beta(j) \neq j\ \Rightarrow \alpha(j) = j$; $\beta_1,\ \ldots,\ \beta_t$ son permutaciones ajenas si dos a dos son ajenas.

**Lema 1.1.1**
Si $\alpha, \beta \in S_n$ son permutaciones ajenas, conmutan.

***Demostración.*** Por demostrar, Si $1 \leq i \leq n, \Rightarrow\ \alpha\beta(i) = \beta\alpha(i)$.
Si $\beta$ mueve a $i$, digamos $\beta(i) = j \neq i$, entonces $\beta(j) \neq j$, ya que si $\beta(j) = j$ y $j \neq i$, pero esto es una contradicción, pues $\beta$ es inyectiva como $\alpha$ y $\beta$ son

disjuntas, entonces $\alpha(i) = i$ y $\alpha(j) = j$. Por lo tanto $\beta\alpha(i) = \beta(i) = j$ y $\alpha\beta(i) = \alpha(j) = j$.

Análogamente si $\alpha$ mueve a $i$. Por último, es claro que $\beta\alpha(i) = \alpha\beta(i)$ si ambos fijan a $i$. ■

**Proposición 1.1.1**
Toda permutación $\alpha \in S_n$ es un ciclo o bien producto de ciclos ajenos.

***Demostración.*** Por inducción sobre el número de puntos que $\alpha$ mueve. Sea $k$ dicho número:

$i$)Si $k = 0$, entonces $\alpha = (1)$, por lo tanto $\alpha$ es un ciclo.

$ii$)Si $k > 0$, sea $i$ un punto que $\alpha$ mueve. Definimos $i_1 = \alpha(i), i_2 = \alpha(i_1),\ i_3 = \alpha(i_2),\ldots, i_{r+1} = \alpha(i_r)$, donde $r$ es el menor entero positivo, tal que $i_{r+1} \in \{i_1,\ \ldots,\ i_r\}$. Puesto que sólo hay $n$ elementos, la lista $i_1,\ i_2,\ldots$ eventualmente tiene que tener una repetición. Veamos que $\alpha(i_r) = i_1$. Supongamos que $\alpha(i_r) = i_j$, con $i_j \in \{i_2,\ \ldots,\ i_r\}$. Tenemos que $\alpha(i_{j-1}) = i_j$, pero esto es una contradicción, pues $\alpha$ es inyectiva y $j - 1 < r$. Denotemos por $\sigma = (i_1\ i_2 \cdots\ i_r)$ un $r$-ciclo. Si $r = n$, entonces $\alpha = \sigma$; por lo tanto $\alpha$ es ciclo. Si $r < n$, entonces $\sigma$ fija cada punto en $Y$, donde $Y$ son los otros $n - r$ puntos de $X$, y $\alpha(Y) = Y$. Definimos $\alpha'$ la permutación tal que $\alpha'(i) = \alpha(i)\ \forall i \in Y$, y deja fijo toda $i \notin Y$. Observamos que $\alpha = \sigma\alpha'$. Por hipótesis de inducción tenemos que $\alpha' = \beta_1 \cdots \beta_t$, donde $\beta_1, \ldots, \beta_t$ son ciclos disjuntos. Puesto que $\sigma,\ \alpha'$ son disjuntos, entonces $\alpha$ es producto de ciclos disjuntos. ■

**Definición 1.1.5**
Una factorización completa de una permutación $\alpha$, es una factorización $\alpha$ en ciclos disjuntos que contiene un único 1-ciclo $(i)$, para todo $i$ fijo bajo $\alpha$.

**Ejemplo 3**
La factorización completa de $\alpha = (1\ 3\ 5) \in S_5$ es $\alpha = (1\ 3\ 5)(2)(4)$

**Observación 2**
Si $\beta = (i_1\ i_2 \cdots\ i_r)$ un $r$-ciclo, entonces

$$\beta^k(i_1) = i_{k+1}, \text{ para todo } k = 1, \ldots, r-1 \text{ y } \beta^r(i_1) = i_1$$

**Teorema 1.1.1**
Sea $\alpha \in S_n$ y $\alpha = \beta_1\ \cdots\ \beta_t$ su factorización en ciclos disjuntos. Esta factorización es única salvo el orden.

***Demostración.*** Sea $\alpha = \gamma_1 \cdots \gamma_s$ otra factorización en ciclos disjuntos de tamaño mayor igual que 2 (es decir, extraemos todos los 1-ciclos).

Observemos que si $\beta_t$ mueve $i_1$, entonces $\beta_t^k(i_1) = \alpha^k(i_1),\ \forall k \geq 1$. Donde $\beta_t^k(i_1)$ representa los símbolos que mueve $\beta_t$.

Además algún $\gamma_j$ debe mover a $i_1$ y puesto que ciclos ajenos conmutan, podemos tomar $\gamma_j = \gamma_s$ y asumir que $\gamma_s$ mueve a $i_1$. En consecuencia $\beta_t^k(i_1) = \gamma_s^k(i_1)$ para todo $k \geq 1$, por lo que $\beta_t = \gamma_s$ y por lo tanto

$$\beta_1 \dots \beta_{t-1} = \gamma_1 \dots \gamma_{s-1}$$

Ahora, usando un argumento inductivo con respecto del núero de factores, se tiene que $s = t$ y los factores $\beta_i = \gamma_i$ para i=1,. . . , s. ■

**Proposición 1.1.2**
*i*) El inverso del ciclo $\alpha = (i_1\ i_2 \cdots i_r)$ es el ciclo $(i_1\ i_2 \cdots i_r)^{-1} = (i_r\ i_{r-1} \cdots i_1)$.

*ii*) Si $\gamma \in S_n$ y $\gamma = \beta_1 \cdots \beta_k$, entonces $\gamma^{-1} = \beta_k^{-1} \cdots \beta_1^{-1}$.

**Definición 1.1.6**
Dos permutaciones $\alpha,\ \beta \in S_n$ tienen la misma estructura cíclica si sus descomposiciones completas tienen el mismo número de $r$-ciclos para cada $r$.

**Observación 3**
Hay $\frac{1}{r}[n(n-1)(n-2)\dots(n-r+1)]$ $r$-ciclos en $S_n$. Esta fórmula puede usarse para contar el número de permutaciones de cierta estructura cíclica dada.

**Ejemplo 4**
El número de permutaciones en $S_4$ de la forma $(a\ b)(c\ d)$ ciclos ajenos, se cálcula como $\frac{1}{2}[\frac{1}{2}(4)(3)][\frac{1}{2}(2)(1)] = 3$; multiplicamos por $\frac{1}{2}$ para no contar $(a\ b)(c\ d) = (c\ d)(a\ b)$ dos veces.

**Ejemplo 5**
Tipos de permutaciones de $S_4$

| Estructura cíclica. | Número de permutaciones. |
|---|---|
| (1) | 1 |
| (1 2) | $6 = \frac{1}{2}(4)(3)$ |
| (1 2 3) | $8 = \frac{1}{3}(4)(3)(2)$ |
| (1 2 3 4) | $6 = \frac{1}{4}(4)(3)(2)(1)$ |
| (1 2)(3 4) | 3 |
| | Total $24 = 4!$ |

**Ejemplo 6**
$\gamma = (1\ 3)(2\ 4\ 7)(5)(6)$ y $\alpha = (2\ 5\ 6)(1\ 4\ 3)$ se puede ver que $\alpha\gamma\alpha^{-1} = (4\ 1)(5\ 3\ 7)(6)(2) = (\alpha 1\ \alpha 3)(\alpha 2\ \alpha 4\ \alpha 7)(\alpha 5)(\alpha 6)$

**Lema 1.1.2**
Si $\gamma,\ \alpha \in S_n$, entonces $\alpha\gamma\alpha^{-1}$ tiene la misma estructura cíclica que $\gamma$. Más detalladamente, si la factorización completa de $\gamma$ es

$$\gamma = \beta_1\ \beta_2 \cdots (i_1\ i_2 \cdots) \cdots \beta_t$$

entonces $\alpha\gamma\alpha^{-1}$ es la permutación obtenida de $\gamma$ por la aplicación $\alpha$ a los símbolos en los ciclos de $\gamma$.

***Demostración.*** Veamos un ejemplo numérico de $\sigma$. Sean $\gamma,\ \alpha \in S_n$ definidas como: $\gamma = (1\ 2\ 7\ 5)(4\ 3\ 6)$ y $\alpha = (1\ 3)(4\ 5)$. Entonces la permutación $\sigma$ es la permutación que obtenemos al aplicar $\alpha$ en todos los símbolos $i$ de $\gamma$.

$$\begin{array}{rccccccccc} \gamma(i) = & ( & 1 & 2 & 7 & 5 & ) & ( & 4 & 3 & 6 & ) \\ \alpha(\gamma(i)) = & ( & \alpha(1) & \alpha(2) & \alpha(7) & \alpha(5) & ) & ( & \alpha(4) & \alpha(3) & \alpha(6) & ) \\ \sigma(i) = & ( & 3 & 2 & 7 & 4 & ) & ( & 5 & 1 & 6 & ) \end{array}$$

Sea $\sigma$ la permutación definida en el enunciado anterior. Observe que si $\gamma$ deja fijo a $i$, entonces $\sigma$ deja fijo a $\alpha(i)$ ya que por definición $(\alpha(i))$ es un 1-ciclo, en la factorización de $\sigma$. Por otro lado tenemos que $\alpha\gamma\alpha^{-1}$ también deja fijo a $\alpha(i)$ pues

$$\alpha\gamma\alpha^{-1}(\alpha(i)) = \alpha\gamma(i) = \alpha(i)$$

Ahora, si $\gamma$ mueve a $i_1$, digamos $\gamma(i_1) = i_2$ esto dice que uno de los ciclos de $\gamma$ en su factorización completa es

$$(i_1\ i_2 \cdots)$$

por definición, uno de los ciclos de $\sigma$ es

$$(k\ l \cdots)$$

donde $k = \alpha(i_1)$ y $l = \alpha(i_2)$, es decir $\sigma(k) = l$; por otro lado $\alpha\gamma\alpha^{-1}(k) = \alpha\gamma\alpha^{-1}[\alpha(i_1)] = l$, entonces $\alpha\gamma\alpha^{-1}(k) = \sigma(k)$. Por lo tanto $\alpha\gamma\alpha^{-1}$ y $\sigma$ coinciden en todos los símbolos de la forma $k = \alpha(i_1)$, y puesto que $\alpha$ es sobreyectiva; todo $k$ es de esta forma, entonces $\sigma = \alpha\gamma\alpha^{-1}$. ■

**Ejemplo 7**
En $S_5$ sean

$$\beta = (1\ 2\ 3)(4)(5),$$
$$\gamma = (5\ 2\ 4)(1)(3)$$

$\beta$ y $\gamma$ tienen la misma estructura cíclica. Sea

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

además $\alpha = (1\ 5\ 3\ 4) \in S_5$ se puede ver que $\gamma = (\alpha 1\ \alpha 2\ \alpha 3)(\alpha 4)(\alpha 5)$ y por el Lema 1.1.2 se tiene

$$\alpha\beta\alpha^{-1} = \gamma$$

observamos que para $\beta = (1\ 2\ 3)(5)(4)$ se requiere un $\alpha$ distinto, es decir $\alpha(5) = 1$ y $\alpha(4) = 3$.

**Teorema 1.1.2**
Dos permutaciones $\gamma$ y $\sigma$ *en* $S_n$ tienen la misma estructura cíclica si y sólo si existe $\alpha \in S_n$ tal que $\sigma = \alpha\gamma\alpha^{-1}$.

***Demostración.*** La suficiencia se prueba con el Lema 1.1.2. Necesidad. Tomamos la factorización completa de tal forma que los ciclos que están "uno encima del otro" tienen la misma longitud

$$\gamma = \delta_1\delta_2\cdots(i_1 i_2\cdots)\cdots\delta_t$$

$$\sigma = \eta_1\eta_2\cdots(k \;\; l\cdots)\cdots\eta_t$$

definimos $\alpha(i_1) = k$ y $\alpha(i_2) = l\cdots$, se puede ver que $\sigma = \alpha\gamma\alpha^{-1}$ ■

**Proposición 1.1.3**
Si $n \geq 2$, todo $\alpha \in S_n$ es producto de transposiciones.

***Demostración.*** Es suficiente hacer la demostración para un $r$-ciclo $\beta$. Si $\beta = (1\ 2\cdots r)$, entonces $\beta = (1\ r)(1\ r-1)\cdots(1\ 3)(1\ 2)$. ■

**Observación 4**
En la factorización anterior, los ciclos (transposiciones) no son ajenas, y además la factorización no es única

$$(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3) = (1\ 3\ 2) \text{ (no conmutan)}$$

además $(1\ 2\ 3) = (2\ 3)(1\ 3)$.

**Definición 1.1.7**
Una permutación $\alpha \in S_n$ es par si esta puede factorizarse en un número par de transposiciones. En otro caso $\alpha$ es impar.

**Ejemplo 8**
$(1\ 2\ 3)$ y $(1)$ son pares ya que

$$(1\ 2\ 3) = (1\ 3)(1\ 2) \; y \; (1) = (1\ 2)(1\ 2)$$

**Definición 1.1.8**
Si $\alpha \in S_n$ *y* $\alpha = \beta_1\cdots\beta_t$ es una factorización completa en ciclos ajenos, el signo de $\alpha$ se define como

$$sgn(\alpha) = (-1)^{n-t}$$

está bien definida ya que esta factorización es única, salvo el orden.

**Observación 5**
Para todo $\tau$ un 1-ciclo, $sgn(\tau) = 1$ ya que $t = n$, luego

$$\tau = (1)(2)\ldots(n).$$

Ahora si $\tau$ es una transposición, entonces $\tau$ deja fijo a $n-2$ números para los cuales hay exactamente un 1-ciclo en la factorización completa de $\tau$, entonces $t = (n-2)+1 = n-1$. Por lo tanto $sgn(\tau) = (-1)^{n-(n-1)} = -1$.

**Teorema 1.1.3**
Para cualesquiera $\alpha,\ \beta \in S_n$, $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$

***Demostración.*** Sea $\alpha = \gamma_1 \cdots \gamma_s$ su descomposición completa en ciclos ajenos. Sea $\tau = (a\ b)$ una transposición. Vamos a demostrar que $sgn(\tau\alpha) = sgn(\tau)sgn(\alpha)$.

Caso 1. Si $(a)$ y $(b)$ son 1-ciclos en la descomposición de $\alpha$ tenemos que $\tau\alpha = (a\ b)\gamma_1 \cdots (\hat{a}) \cdots (\hat{b}) \cdots \gamma_s$ es la descomposición completa de de $\tau\alpha$ en ciclos ajenos. Por lo tanto $sgn(\tau\alpha) = (-1)sgn(\alpha)$.

Caso 2. Si $(b)$ es 1-ciclo y $(a \cdots l)$ un ciclo de orden mayor o igual a dos en la descomposición completa en ciclos ajenos de $\alpha$ tenemos que $(a\ b)(a \cdots l) = (a \cdots lb)$, entonces $\tau\alpha = (a \cdots lb)\gamma_1 \cdots (\hat{b})\widehat{(a \cdots l)} \cdots \gamma_s$ es la descomposición completa en ciclos ajenos de $\tau\alpha$. Por lo tanto $sgn(\tau\alpha) = (-1)sgn(\alpha)$.

Caso 3. Sea $(ac_1 \ldots c_k bd_1 \cdots d_l)$ con $k,\ l \geq 0$ un ciclo de tamaño mayor o igual a dos, en la descomposición completa de $\alpha$ tenemos que $(a\ b)(ac_1 \cdots c_k bd_1 \cdots d_l) = (ac_1 \ldots c_k)(bd_1 \ldots d_l)$, entonces

$$\tau\alpha = (ac_1 \cdots c_k)(bd_1 \cdots d_l)\gamma_1 \ldots (ac_1 \cdots \widehat{c_k bd_1} \cdots d_l) \cdots \gamma_s$$

es la descomposición completa de $\tau\alpha$ en ciclos ajenos. Por lo tanto

$$sgn(\tau\alpha) = (-1)sgn(\alpha).$$

De los tres casos anteriores concluimos que, para todo $\alpha \in S_n$ y $\tau \in S_n$ una transposición

$$sgn(\tau\alpha) = (-1)sgn(\alpha).$$

Por último si $\alpha = \tau_1 \cdots \tau_n$ donde cada $\tau_i$ es una transposición por inducción en $n$; podemos probar que $sgn(\alpha) = (-1)^n$, entonces

$$sgn(\alpha\beta) = (-1)^n sgn(\beta) = sgn(\alpha)sgn(\beta),\ \forall \beta \in S_n.$$

■

**Teorema 1.1.4**
Se cumplen las siguientes proposiciones:

1) Sea $\alpha \in S_n$:

i) Si $sgn(\alpha) = 1$, entonces $\alpha$ es par.

ii) Si $sgn(\alpha) = -1$, entonces $\alpha$ es impar.

2) Una permutación $\alpha$ es impar si y sólo si es producto de un número impar de transposiciones.

***Demostración.*** 1) Sea $\alpha = \tau_1 \cdots \tau_q$ su descomposición en producto de transposiciones; de la demostración del Teorema 1.1.3 $sgn(\alpha) = (-1)^q$

Si $sgn(\alpha) = 1$, entonces $q$ es par.

Si $sgn(\alpha) = -1$, entonces $q$ es impar.

donde $q$ es el número de transposiciones.

2) Necesidad. Si $\alpha$ es impar, entonces $sgn(\alpha) \neq 1$, por lo cual $sgn(\alpha) = -1$. Ahora si $\alpha = \tau_1 \ldots \tau_q$ producto de transposiciones, se sigue que $sgn(\alpha) = (-1)^q$, por lo tanto $q$ es impar.

Suficiencia. Si $\alpha = \tau_1 \cdots \tau_q$ es un producto de transposiciones y $q$ es impar, entonces $sgn(\alpha) = (-1)^q = -1$, luego por lo anterior, $\alpha$ es impar. ■

**Corolario 1.1.1**
Sea $\alpha,\ \beta \in S_n$. Si $\alpha$ y $\beta$ tienen la misma paridad, entonces $\alpha\beta$ es par, mientras que si $\alpha\ y\ \beta$ tienen paridad distinta, entonces $\alpha\beta$ es impar.

## 1.2. Monoides

**Definición 1.2.1**
Dado $S$ un conjunto no vacío, llamaremos ley de composición interna a cualquier aplicación $f : S \times S \to S$.

**Definición 1.2.2**
Enunciaremos propiedades básicas sobre aplicaciones binarias.

1) Si para cualquiera $x,\ y,\ z \in S$ se tiene que $(xy)z = x(yz)$ diremos que la ley de composición interna es **asociativa**.

2) Cualquier elemento $e \in S$ tal que $xe = ex = x$ para todo $x \in S$ será llamado **elemento neutro**.

3) El elemento neutro es único ($e = ee' = e'$ si ambos fuesen neutros).

4) Si $xy = yx$ diremos que la ley de composición interna es **conmutativa**.

Una particularidad de la Definición 1.2.2 es que si para todo $x \in S$ se tiene $xe = x$, el elemento $e$ es llamado, neutro por la derecha; y si para todo $x \in S$, se cumple $ex = x$, este elemento $e$ será llamado neutro por la izquierda. Si ambas igualdades se satisfacen para todo $x \in S$, el elemento $e$ será llamado simplemente, **elemento neutro**.

**Definición 1.2.3**
Un conjunto $S$ no vacío con una ley de composición interna " $\cdot$ " asociativa, y dotado de un elemento neutro $e$. Es llamado monoide, y se denota por $(S, \cdot)$.

**Definición 1.2.4**
Si $\{x_1, ..., x_n\} \subset S$ y $(S, \cdot)$ un monoide, definimos y denotamos

*i*)$\Pi_{k=1}^{0} x_k = e$.

*ii*)$\Pi_{k=1}^{1} x_k = x_1$.

*iii*)$\Pi_{k=1}^{n} x_k = (x_1 \cdots x_{n-1}) \cdot x_n$.

**Proposición 1.2.1**
Dado $S$ un monoide y $\{x_1, .., x_n\} \subset S$, entonces $\Pi_{k=1}^{m} x_k \cdot \Pi_{j=1}^{n} x_{m+j} = \Pi_{j=1}^{m+n} x_j$.

***Demostración.*** (Por inducción sobre $n$). Para $n = 1$ tenemos

$$\Pi_{k=1}^{m} x_k \cdot \Pi_{j=1}^{1} x_{m+j} = \Pi_{k=1}^{m} x_k \cdot x_{m+1} = \Pi_{j=1}^{m+1} x_k.$$

Supongamos que para $h < n$ tenemos $\Pi_{k=1}^{m} x_k \cdot \Pi_{j=1}^{h} x_{m+j} = \Pi_{j=1}^{m+h} x_j$.

Dado que $\Pi_{k=1}^{m} x_k, \Pi_{j=1}^{h} x_{m+j}, x_{m+h+1} \in S$ tenemos

$$\Pi_{j=1}^{m+h+1} x_j = \left(\Pi_{j=1}^{m+h} x_j\right) x_{m+h+1} = \left(\Pi_{k=1}^{m} x_k \cdot \Pi_{j=1}^{h} x_{m+j}\right) x_{m+n+1}$$

$$= \Pi_{k=1}^{m} x_k \cdot \left(\Pi_{j=1}^{h} x_{m+j} \cdot x_{m+h+1}\right) = \Pi_{k=1}^{m} x_k \cdot \left(\Pi_{j=1}^{h+1} x_{m+j}\right).$$

Luego para $h + 1 \leq n$ se cumple. ■

La proposición anterior nos garantiza que el producto de elementos de un monoide es independiente de la colocación de los paréntesis.

**Definición 1.2.5**
Sea $S$ un monoide y $n, m \in \mathbb{N} \cup \{0\}$, para $x \in S$ definimos $x^n = \Pi_{i=1}^{n} x$.

Por todo lo anterior tenemos:

*i*) $x^0 = \Pi_{k=1}^{0} x = e$

*ii*) $x^{(n+m)} = x^n \cdot x^m$

*iii*) $(x^n)^m = x^{nm}$

**Ejemplo 9**
1) $(\mathbb{N}, \cdot)$ es asociativo y 1 es el neutro.

2) $(\mathbb{Z}, \cdot)$ es asociativo y 1 es el neutro.

3) Sea $X$ un conjunto, $(P(X), \cup)$ es un monoide, como $(A \cup B) \cup C = A \cup (B \cup C)$ y el conjunto vacío "$\emptyset$" es el neutro.

4) Sea $Y$ un conjunto, $(P(Y), \cap)$ es un monoide, y claramente es asociativo, además el neutro es $Y$.

**Definición 1.2.6**
Un subconjunto $H$ del monoide $S$ es llamado submonoide, si: 1) $e \in H$, 2) $H$ es cerrado respecto a la ley de composición de $S$, y lo denotamos $(H, \cdot)$.

**Ejemplo 10**
$(\mathbb{N}, \cdot)$ submonoide de $(\mathbb{Z}, \cdot)$. Como podemos ver $(2\mathbb{N}, \cdot)$ no es submonoide de $(\mathbb{N}, \cdot)$ y por ende tampoco de $(\mathbb{Z}, \cdot)$

**Definición 1.2.7**
Sea $(S, \cdot)$ una estructura algebraica con elemento neutro, si para cualesquiera $x,\ y$ se cumple $x \cdot y = e$, entonces $x$ es llamado el **elemento inverso por la izquierda** de $y$; por otro lado a $y$ se le da el nombre de **elemento inverso por la derecha** de $x$. Si $x \cdot y = e = y \cdot x$ diremos que $x$ e $y$ son inversos.

**Proposición 1.2.2**
Sea $(S, \cdot)$ un monoide, con $e$ neutro por la izquierda. Suponga que para todo $x \in S$ existe su inverso por la izquierda, entonces $e$ es neutro y todo inverso izquierdo es inverso.

***Demostración.*** Sean $a,\ b \in S$ tales que $ba = e$, además existe $c \in S$ tal que $cb = e$. Luego tenemos que $ab = e(ab) = (cb)(ab) = c(ba)b = cb = e$. Por otro lado $ae = a(ba) = (ab)a = ea = a$. ■

**Proposición 1.2.3**
Sea $(S, \cdot)$ un monoide, si para cualquier $x \in S$ existe su inverso por ambos lados, entonces estos inversos son iguales.

***Demostración.*** Supongamos que $y \cdot x = e = xy$; luego tenemos que $y = ey = (y \cdot x)y = y \cdot (xy) = y \cdot e = y \cdot$. ■

Observe, en la prueba anterior la asociatividad fue fundamental, ya que si la quitamos el resultado anterior no se cumple.

**Definición 1.2.8**
Si en el monoide $S$, $x \in S$ tiene inversos, diremos que $x$ es invertible.

Por la Proposición 1.2.3, si $x$ es invertible en $S$ entonces su inverso es único, y lo denotaremos por $x^{-1}$. Además se tiene que $x^{-1}$ es invertible y $(x^{-1})^{-1} = x$.

**Proposición 1.2.4**
Si $(G, \cdot)$ es un monoide. Denotaremos por $G^* = \{x \in G : x \text{ es invertible}\}$, entonces $G^*$ es submonoide de $G$.

***Demostración.*** En efecto, $e \in G^*$ y si $x,\ y \in G^*$, entonces existen $x^{-1},\ y^{-1} \in G^*$, note que $(xy)^{-1} = y^{-1}x^{-1}$. Además $(xy)(y^{-1}x^{-1}) = e = (y^{-1}x^{-1})(xy)$ así que $xy \in G^*$ y $(xy)^{-1} = y^{-1}x^{-1}$. ■

## 1.3. Grupos

**Definición 1.3.1**
Diremos que $G$ es un grupo si y sólo si:

1) $G$ es un monoide.

2) $G = G^*$.

**Ejemplo 11**
Enunciamos algunos ejemplos de grupos, con sus respectivas operaciones.

1) $\langle \mathbb{Z}, + \rangle$, con $+$ suma usual.

2) $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$, con $+$ la suma usual.

3) El **grupo circular**,

$$S^1 = \{z \in \mathbb{C} : |z| = 1\},$$

es el grupo en el cual la operación es la multiplicación de números complejos; esta es una operación ya que el producto de números complejos de módulo 1 también tienen módulo 1. La multiplicación en los números complejos es asociativa, la identidad es el 1 (que tiene módulo 1), y el inverso de cualquier número complejo de módulo 1 es su conjugado complejo, que también tiene módulo 1. Por lo tanto, $S^1$ es un grupo.

4) Dado $n \in \mathbb{N}$ fijo, sea $\mu_n = \{z \in \mathbb{C} | z^n = 1\}$, entonces $\langle \mu_n, \cdot \rangle$ con $\cdot$ el producto definido en $\mathbb{C}$ es un grupo.

5) Sea $X \neq \phi$ y sea $\Im = \{f : X \to X | f \text{ es biyección}\}$. $\langle \Im, \circ \rangle$ forma un grupo.

6) $\{\pm 1, \pm\widehat{i} \pm \widehat{j} \pm \widehat{k}\}$, $\widehat{i}\widehat{j} = \widehat{k},\ \widehat{j}\widehat{i} = \widehat{k},\ \widehat{k}^2 = \widehat{i}^2 = \widehat{j}^2 = 1$ (Cuaternios de Hamilton).

7) (El cuarto Grupo de Klein) $\{e, a, b, c\},\ \ a^2 = b^2 = c^2 = e$.

Para cuando $x \in G$ y $G$ monoide tenemos definido ya $x^n$ para $n \in \mathbb{N} \cup \{0\}$. Ahora si $x \in G$ y $G$ es un grupo tiene sentido pensar en $x^n$ para $n \in \mathbb{Z}$, pues si $-n \in \mathbb{N}$, $x^n = (x^{-1})^{-\,n}$.

**Definición 1.3.2**
Si la ley de composición es conmutativa para el grupo $G$ diremos que $G$ es un grupo abeliano. Para estos grupos utilizaremos la notación aditiva, bajo ésta notación, $x^{-1}$ es sustituido por $-x$ y $x^n$ por $nx$.

**Lema 1.3.1**
Todo conjunto $G$ dotado de una ley de composición asociativa, con elemento neutro izquierdo, en el cual todo elemento de él tenga un inverso izquierdo, entonces $G$ es un grupo.

***Demostración.*** Sea $x \in G$, entonces existe $y \in G$ tal que $yx = e$ y existe $z \in G$ tal que $zy = e$ luego $xy = exy = (zy)(xy) = z(yx)y = z(ey) = zy = e$. Además $xe = x(yx) = (xy)x = ex = x$. ■

**Teorema 1.3.1**
Sea $G$ un conjunto dotado de una ley de composición asociativa. Entonces $G$ es un grupo si y sólo si para cualesquiera $a, b \in G$ existen únicos $x, y \in G$ tales que $ax = b,\ ya = b$

***Demostración.*** Necesidad. $G$ es grupo entonces $x = a^{-1}b$ y $y = ba^{-1}$ en forma unívoca.

Suficiencia. Para $a \in G$, existe $e \in G$ tal que $ea = a$ ahora dado cualquier $b \in G$, existe $x \in G$ tal que $ax = b$, entonces $eb = e(ax) = (ea)x = ax = b$, es decir, $e$ es neutro por la izquierda. Ya que para todo $a$ existe $y$ tal que $ya = e$, es decir, $a$ tiene inverso por la izquierda, se tiene que por Lema 1.3.1, $G$ es un grupo. ■

**Observación 6**
Del Teorema 1.3.1, se sigue que las dos leyes de cancelación,

$$\begin{aligned} a \cdot u &= a \cdot w \text{ implica } u = w \\ &\text{y} \\ u \cdot a &= w \cdot a \text{ implica } u = w \end{aligned}$$

se verifican en $G$.

**Ejemplo 12**
A continuación algunos ejemplos.

1) Dado que $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ son monoides, tenemos que: $(\mathbb{N}^*, \cdot)$, $(\mathbb{Z}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ son grupos.

2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ son grupos abelianos.

3) Sea $G$ el conjunto de los números reales distintos de cero y defínase para $a,\ b \in G$, $a * b = a^2 b$; de modo que $4 * 5 = 4^2(5) = 80$. ¿Cuáles axiomas de grupo en $G$ son válidos respecto a esta operación $*$ y cuáles no? Desde luego, $G$ es cerrado respecto a $*$. ¿Es asociativa $*$? Si así fuera, $(a * b) * c = a * (b * c)$, es decir, $(a * b)^2 c = a^2(b * c)$, y entonces $(a^2 b)^2 c = a^2(b^2 c)$, lo cual se reduce a $a^2 = 1$, que es válido solamente para $a = \pm 1$. Por consiguiente, en general, la ley asociativa no es válida en $G$ relativa a $*$.

4) El **grupo Booleano** $\beta(X)$ [nombrado así en honor a G. Boole (1815-1864)] es la familia de todos los subconjuntos de $X$ con la adición definida como la **diferencia simétrica** $A + B$, donde

$$A + B = (A - B) \cup (B - A)$$

la diferencia simétrica se muestra en la siguiente figura.

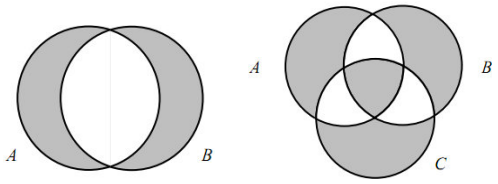



Figura 1.2: La diferencia simétrica de 2 y 3 conjuntos.

Es claro que $A + B = B + A$, entonces la diferencia simétrica es conmutativa; la identidad es el conjunto vacío $\emptyset$, y el inverso de $A$ es el mismo $A$ , es decir $A + A = \emptyset$. Es fácil verificar que $A + (B + C) = (A + B) + C$.

**Definición 1.3.3**
Sea $G$ un grupo y $a \in G$. Si $a^k = 1$ para algún $k \geq 1$, entonces el menor entero positivo es llamado el orden de $a$. Si este número $k$ no existe, diremos que $a$ tiene orden infinito.

**Observación 7**
Si $n$ es el orden de $x \in G$ y $x^m = 1$, entonces $n \leq m$.

**Ejemplo 13**
Algunos ejemplos de la definición anterior.

1) $1 \in \mathbb{Z}$ tiene orden infinito ya que $1 + 1 + 1 + \cdots + 1 \neq 0$.

2) En cualquier grupo el orden de $e$ es 1, y es el único elemento de

orden 1.

3) $a^2 = 1$, si y sólo si $a = a^{-1}$. Es decir, de orden 2.

**Teorema 1.3.2**
Si $a \in G$ es un elemento de orden $n$, entonces $a^m = 1$, si y sólo si $n|m$.

***Demostración.*** Necesidad. Asuma que $a^m = 1$. Sabemos que $m = qn + r$, donde $0 \leq r < n$. Observamos que $a^r = a^{m-qn} = 1$ y por la minimalidad de $n$, se tiene que r=0. Suficiencia. Si $n|m$, entonces $m = nk$, luego entonces $a^m = (a^n)^k = 1$. ■

**Proposición 1.3.1**
Sea $\alpha \in S_n$

i) Si $\alpha$ es un $r$-ciclo, entonces $\alpha$ tiene orden $r$.

ii) Si $\alpha = \beta_1 \cdots \beta_t$ es un producto disjunto de $r_i$-ciclos $\beta_i$, entonces $\alpha$ tiene orden $\text{mcm}\{r_1, \ldots, r_t\}$.

iii) Si $p$ es primo, entonces $\alpha$ tiene orden $p$, si y sólo si $\alpha$ es $p$-ciclo ó un producto disjunto de $p$-ciclos.

***Demostración.*** Vamos a probar una a una las proposiciones.

i) Esto ya se demostró en la Proposición 1.1.1. Pues $\alpha^r(i_1) = i_{1+r} = i_1$.

ii) Asuma que $\alpha^M = 1$, como los $\beta_i$ conmutan, se tiene que $\alpha^M = \beta_1^M \cdots \beta_t^M = 1$, $\beta_i$ disjuntos, entonces $\beta_i^M = 1$, se sigue que $r_i | M$ para todo $i$, luego entonces $M$ es común múltiplo de los $r_i$. Por otro lado si $m = \text{mcm}\{r_i\}$ es claro que $\alpha^m = \beta_1^m \cdots \beta_t^m = 1$.

iii)Necesidad; si $\alpha$ es un ciclo no hay nada que probar. Sea $\alpha = \beta_1 \cdots \beta_t$ con $\beta_1, \ldots, \beta_t$ ciclos disjuntos de orden $r_i \geq 2$ por b) $p = \text{mcm}\{r_i\}$, entonces $p = r_i l_i$ $p$ primo, por lo tanto $l_i = 1$. Suficiencia. Es claro de i) y ii) respectivamente. ■

**Ejemplo 14**
Tipos de permutaciones de $S_5$, recuerde que para calcular los $r$ ciclos de

cierto tipo usamos la fórmula $\frac{1}{r}[n(n-1)\ldots(n-r+1)]$, entonces tenemos

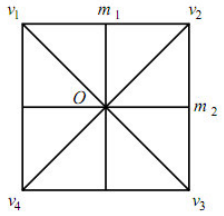
| Estructura cíclica | Número de permutaciones | Orden | Paridad |
|---|---|---|---|
| (1) | 1 | 1 | Par. |
| (1 2) | 10 | 2 | Impar. |
| (1 2 3) | 20 | 3 | Par. |
| (1 2 3 4) | 30 | 4 | Impar. |
| (1 2 3 4 5) | 24 | 5 | Par. |
| (1 2)(3 4 5) | 20 | 6 | Impar. |
| (1 2)(3 4) | 15 | 2 | Par. |
| | 120 | | |

**Proposición 1.3.2**
Si $G$ es un grupo finito, entonces todo $x \in G$ tiene orden finito.

***Demostración.*** Sea $a \in G$, consideramos el conjunto $\{1,\ a,\ a^2, \ldots,\ a^n\} \subset G$ puesto que $G$ es finito, existe $m > n$ tal que $a^m = a^n$, es decir, hay una repetición, y observe que $a^{m-n} = 1$. Por lo tanto el conjunto $\{k \in \mathbb{N} : k \geq 1,\ a^k = 1\} \neq \emptyset$ tiene elemento mínimo, y el cual es el orden de $a$. ■

**Definición 1.3.4**
Sea $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ es una mosión, si es una biyección que preserva distancias. Si $\pi$ es un polígono en $\mathbb{R}^2$, entonces $\sum(\pi)$ su grupo de simetrías, consiste de todas las mosiones $\varphi$ tales que $\varphi(\pi) = \pi$.

**Ejemplo 15**
Sea $\Pi_4$ el cuadrado con lados de tamaño 1 y vértices $v_1,\ v_2,\ v_3,\ v_4$.




Se puede ver que todo $\varphi \in \sum(\Pi_4)$ permuta los vértices de $\Pi_4$, de hecho queda determinada por $\{\varphi(v_i) : 1 \leq i \leq 4\}$. Por lo tanto, a lo más hay 4! posibles simetrías.

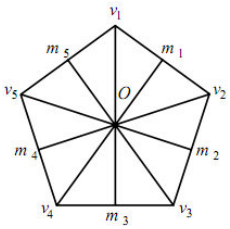
Figura 1.3: El grupo diédrico $\sum(\Pi_4)$.

Ahora, no toda permutación en $S_4$ proviene de una simetría de $\Pi_4$: Si $v_i$ y $v_j$ son adyacentes, entonces $\|v_i - v_j\| = 1$, pero $\|v_1 - v_3\| = \sqrt{2} = \|v_2 - v_4\|$. Por lo tanto, si $\varphi \in \sum(\Pi_4)$, entonces $\varphi$ preserva adyacencias.

Hay 8 simetrías de $\Pi_4$: la identidad, las tres rotaciones alrededor del $O$, es decir, $90°,\ 180°,\ 270°$; las reflexiones alrededor de los ejes "x", "y" y los ejes $v_1v_3,\ v_2v_4$.

**Observación 8**
$\sum(\Pi_4)$ es llamado el grupo diédrico $D_8$. Los elementos de $\sum(\Pi_4)$: (1), (1 2 3 4), (1 3)(2 4), (1 4 3 2), (1 2)(3 4), (1 4)(2 3), (1 3), (2 4). Se puede ver que $D_8 = \langle x,\ y : x^4 = 1,\ y^2 = 1,\ yxy = x^{-1} \rangle$, donde $x = (1\ 2\ 3\ 4)$ y $y = (2\ 4)$.

**Ejemplo 16**
El grupo diédrico $\sum(\Pi_5)$




1) 5 rotaciones. $(72j)°,\ j = 0, \ldots, 4$.
2) 5 reflexiones alrededor de los ejes $Om_k,\ k = 1, \ldots, 5$
3) $\sum(\Pi_5) = D_{10}$.

Figura 1.4: El grupo diédrico $\sum(\Pi_5)$.

**Definición 1.3.5**
Si $\Pi_n$ es el polígono regular de $n$ lados y vértices $v_1, \ldots, v_n$ y centro $O$. Entonces el grupo de simetrías es llamado $D_{2n}$ el grupo diédrico de $2n$ elementos, con $n$ rotaciones alrededor de $O$ por $(\frac{360}{n}j)^\circ,\ 0 \leq j \leq n-1$ y $n$ reflexiones:

1) $n$ impar reflexiones alrededor de $Ov_i,\ 1 \leq i \leq n$.

2) $n$ par reflexiones alrededor de $Om_i$, $m_i$ puntos medios, con $1 \leq i \leq n$

## 1.4. El teorema de Lagrange

**Definición 1.4.1**
Un subconjunto $H \leq G$ es un subgrupo de $G$ si:

1) $e \in H$

2) Si $x, y \in H$, entonces $xy \in H$.

3) Si $x \in H$, entonces $x^{-1} \in H$.

Usaremos la notación $H < G$ si $H$ está contenido propiamente en $G$.

**Observación 9**
$\{e\}$ y $G$ son los subgrupos triviales de $G$.

Si $H \leq G$ es un subgrupo, $H$ es un grupo en si. La asociatividad se hereda de $G$.

**Ejemplo 17**
El grupo 4 de Klein $V = \{(1), a = (12)(34), b = (13)(24), c = (14)(23)\} < S_4$. $1 \in V, \alpha^2 = 1$ para todo $\alpha \in V$, entonces $\alpha = \alpha^{-1}$ para todo $\alpha \in V$, además $ab = c$, $ac = b$ y $bc = a$.

**Proposición 1.4.1**
Un subconjunto $H$ de un grupo $G$ es un subgrupo si y sólo si $H \neq \emptyset$ y siempre que $x, y \in H$ entonces $xy^{-1} \in H$.

***Demostración.*** Necesidad. Como $e \in H$, entonces $H \neq \emptyset$. Además si $x, y \in H$ entonces $y^{-1} \in H$, pues $H \leq G$. Por lo tanto $xy^{-1} \in H \leq G$ cerrado bajo la operación.

Suficiencia. 1) $H \neq \emptyset$, esto implica que existe $x \in H$. Así que $x, x \in H$ por lo que $e = xx^{-1} \in H$.

2) Sea $y \in H$, como $e \in H$, entonces $y^{-1} = ey^{-1} \in H$.

3) Sea $x, y \in H$, entonces $x, y^{-1} \in H$. Por lo que $xy = x(y^{-1})^{-1} \in H$. ■

**Proposición 1.4.2**
Un subconjunto $H \neq \emptyset$ de un grupo finito $G$ es un subgrupo, si y sólo si $H$ es cerrado bajo la operación, es decir, $a, b \in H$, entonces $ab \in H$.

***Demostración.*** Necesidad. Como $H \leq G$ es un subgrupo de $G$, por definición es cerrado bajo la operación, lo tanto $ab \in H$.

Suficiencia. $G$ finito y $H \neq \emptyset$ existe $a \in H$ y el orden de $a$ es finito, digamos $n$, es decir, $a^n = e$. Como $H$ es cerrado, entonces, $a^n = e \in H$, además $a^{-1} = a^{n-1} \in H$. ■

**Observación 10**
Si $G$ no es finito, la proposición anterior puede ser falsa. Por ejemplo, $\mathbb{N} \neq \emptyset$ es cerrado bajo la suma en $\mathbb{Z}$ pero $(\mathbb{N}, +) \nleq (\mathbb{Z}, +)$ no es subgrupo.

**Ejemplo 18**
El subconjunto de todas las permutaciones pares, $A_n \leq S_n$ es un subgrupo. El subgrupo es llamado el "grupo alternante". $A_n$ es no vacío pues (1) es par, además es cerrado bajo la composición pues *(par)(par)=(par).*

**Definición 1.4.2**
$G$ grupo y $a \in G$, escribimos $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ como "todas las potencias de $a$". Es el subgrupo cíclico de $G$ generado por $a$.

Decimos que $G$ es cíclico si existe $a \in G$ tal que $G = \langle a \rangle$ y diremos que $a$ es un generador de $G$.

**Ejemplo 19**
$\mu_n$ las raíces $n$-ésimas de la unidad es cíclico y $\mu_n =< e^{\frac{2\pi i}{n}} >$.

**Definición 1.4.3**
Los enteros módulo $m$, es decir, $\mathbb{Z}_m$ es la familia de todas las clases de congruencias módulo $m$.

$[a] = [b]$ en $\mathbb{Z}_m$ si y sólo si $a \equiv b \ mod \ m$; en particular $[a] = [0]$ si y sólo si $m \big| a$.

**Observación 11**
Para $m \geq 2$; $\mathbb{Z}_m$ es cíclico generado por [1].

Un grupo cíclico puede tener varios generadores.

**Ejemplo 20**
El grupo generado por $\langle a \rangle = \left\langle a^{-1} \right\rangle$.

**Teorema 1.4.1**
Si $G = \langle a \rangle$ es el grupo cíclico de orden $n$, entonces $a^k$ es un generador de $G$ si y sólo si $(k, n) = 1$.

***Demostración.*** Si $a^k$ genera a $G$, entonces $a \in \langle a^k \rangle$ por lo que $a = a^{kt}$ para algún $t \in \mathbb{Z}$,

luego $a^{kt-1} = 1$ como el orden de $a$ es $n$, entonces $n|kt-1$. Por lo tanto $kt - 1 = vn$ para algún $v \in \mathbb{Z}$, se tiene $1 = kt - vn$ luego entonces (k,n)=1.

Ahora si $(k, n) = 1$, entonces $1 = tn + ks$ para $t, s \in \mathbb{Z}$ por lo que $a = a^{tn+sk} = a^{tn}a^{ks} = (a^k)^s \in \langle a^k \rangle$. Concluyendo que $G$ está contenido en $\langle a^k \rangle$, de donde obtenemos la igualdad. ■

**Proposición 1.4.3**
Sea $G$ un grupo finito y sea $a \in G$. Entonces el orden de $a$ es $|\langle a \rangle|$ el número de elementos en $\langle a \rangle$.

***Demostración.*** $G$ finito, entonces, existe un entero $k \geq 1$ con $1, a, a^2, \ldots, a^{k-1}$ son $k$ elementos distintos , pero, $1, a, a^2, \ldots, a^k$ tiene una repetición. Entonces $a^k = a^i$ para algún $0 \leq i < k$, si $i \geq 1$, entonces $a^{k-i} = 1$, pero esto es una contradicción, pues por hipótesis la lista $1, a, \ldots, a^{k-1}$ no tiene repeticiones, entonces $i = 0$, por lo que $a^k = 1$ . Por lo tanto $k$ es el orden de $a$ (es decir, $k$ es el menor entero positivo tal que $a^k = 1$).

Ahora sea $H = \{1, a, \ldots, a^{k-1}\}$ tal que $|H| = k$. Por demostrar $H = \langle a \rangle$. Observe que $H \subseteq \langle a \rangle$. Además para $a^i \in \langle a \rangle$, tenemos por el algoritmo de la división que $i = qk + r$ con $0 \leq r < k$, entonces $a^i = a^{qk+r} = (a^k)^q a^r = a^r \in H$ por lo cual $\langle a \rangle \subseteq H$. Por lo tanto $\langle a \rangle = H$. ■

**Definición 1.4.4**
Si $G$ es un grupo finito, el número de elementos en $G$ denotado por $|G|$, es llamado el orden de $G$.

**Proposición 1.4.4**
La intersección $\bigcap_{i \in I} H_i$ de cualquier familia de subgrupos de un grupo es nuevamente un subgrupo de $G$. En particular si $H, K \leq G$, entonces $H \cap K \leq G$.

***Demostración.*** Sean $H, K \leq G$ subgrupos de $G$; por hipótesis $e \in H$ y $e \in K$, por lo tanto $e \in H \cap K$.

Ahora; sean $x, y \in H \cap K$; por lo cual $x, y \in H$ y $x, y \in K$. Como $H$ y $K$ son subgrupos de $G$ por hipótesis tenemos que $xy \in H$ y $xy \in K$. Por lo tanto $xy \in H \cap K$.

Nuevamente, sea $x \in H \cap K$, entonces $x \in H$ y $x \in K$, y como $H$ y $K$ son subgrupos por hipótesis, tenemos que $x^{-1} \in H$ y $x^{-1} \in K$, por lo tanto $x^{-1} \in H \cap K$. Por lo tanto $H \cap K \leq G$. ■

Podemos usar el mismo argumento para probar que $\underset{i \in I}{cap} H_i$ una familia arbitraria de subgrupos es nuevamente un subgrupo de $G$.

**Corolario 1.4.1**
Si $X \subseteq G$ subconjunto, entonces, existe un subgrupo $\langle X \rangle \leq G$ de $G$ que contiene a $X$. $\langle X \rangle$ es el menor subgrupo de $G$ que contiene a $X$, es decir, si $H \leq G$ tal que $X \subseteq H$, entonces $\langle X \rangle \leq H$

***Demostración.*** Existen subgrupos de $G$ que contienen a $X$, por ejemplo $G$ mismo contiene a $X$.

Definimos $\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$, la intersección de todos los subgrupos de $G$ que contienen a $X$. Por la Proposición 1.4.4 $\langle X \rangle$ es un subgrupo de $G$; además $X \subseteq \langle X \rangle \leq H$ para todo $H$ subgrupo de $G$ que contiene a $X$. Por lo tanto $\langle X \rangle \leq H$ si $X \subseteq H$. ■

**Observación 12**
Si $X = \emptyset$; puesto que $\emptyset$ es subconjunto de cualquier conjunto, tenemos que $\emptyset \subseteq H \leq G$ subgrupo en particular $\langle \emptyset \rangle \leq \{e\}$. Por lo tanto $\langle \emptyset \rangle = \{e\}$.

**Definición 1.4.5**
Si $X \subseteq G$ subconjunto de un grupo $G$, entonces $\langle X \rangle \leq G$ es llamado el subgrupo generado por $X$.

Si $X \neq \emptyset$ subconjunto de un grupo, definimos una "palabra" en $X$ como un elemento $g \in G$ tal que $g = x_1^{e_1} \cdots x_n^{e_n}$, donde $x_i \in X$ y $e_i = \pm 1$ para todo $i \in \{1, \ldots, n\}$.

**Proposición 1.4.5**
Si $\emptyset \neq X \subseteq G$ subconjunto de un grupo $G$, entonces $\langle X \rangle$ es el conjunto de todas las palabras en $X$.

***Demostración.*** Sea $W(X)$ el conjunto de todas las palabras de $X$, observe que $W(X) \leq G$ pues si $x \in X$, tenemos que $x^{-1} \in W(X)$, puesto que $e = xx^{-1} \in W(X)$; el producto de dos palabras en $X$ es nuevamente una palabra en $X$. Entonces $W(X) \leq G$ y además $X \subseteq W(X)$. Por lo tanto $\langle X \rangle \leq W(X)$.

Por otro lado, para todo $H \leq G$ tal que $X \subseteq H$ se cumple que $W(X) \subseteq H$ (pues es cerrado).

Puesto que $\langle X \rangle$ es la intersección de los subgrupos de $G$ que contienen a $X$, entonces $W(X) \subseteq \langle X \rangle$. ■

**Ejemplo 21**
El grupo diédrico $D_{2n} = \{\rho, \sigma : \rho^n = 1, \sigma^2 = 1, \sigma\rho\sigma = \rho^{-1}\}$ donde $\rho$ es la rotación por $\frac{360^\circ}{n}$ y $\sigma$ es una reflexión.

**Observación 13**
$G$ un grupo finito y $H \leq G$ subgrupo, tenemos que $|H| \leq |G|$; ahora para poder probar que $|H| \,\big|\, |G|$ introduciremos un nuevo concepto que llamaremos "clases laterales".

**Definición 1.4.6**
$H \leq G$ subgrupo y $a \in G$ la clase lateral $aH \subseteq G$ es el subconjunto: $aH = \{ah \ : \ h \in H\}$ "clase lateral izquierda"; $Ha = \{ha \ : \ h \in H\}$ "clase lateral derecha".

**Observación 14**
Para $(G, +)$ usaremos la notación $a + H = \{a + h : h \in H\}$ para clases laterales izquierdas y $H + a = \{h + a : h \in H\}$ para clases laterales derechas.

Las clases laterales usualmente no son subgrupos. Por ejemplo, si $a \notin H$, entonces $e \notin H$ pues de lo contrario $e = ah$, luego $a = h^{-1} \in H$, lo cual es una contradicción.

**Ejemplo 22**
$(\mathbb{R}^2, +)$ grupo abeliano. Sea $(a, b) \neq (0, 0) \in \mathbb{R}^2$.

Ahora sea $L = \{(ra, rb) : r \in \mathbb{R}\}$ es una línea recta que pasa por el origen.

Entonces $L \leq (\mathbb{R}^2, +)$. Si $\beta \in \mathbb{R}^2$ observe que si $r\alpha \in L$, entonces $\beta + r\alpha \in L'$ por "Ley del paralelogramo". $L' = \beta + L$, la cual es una recta paralela a $L$ y pasa por $\beta$.

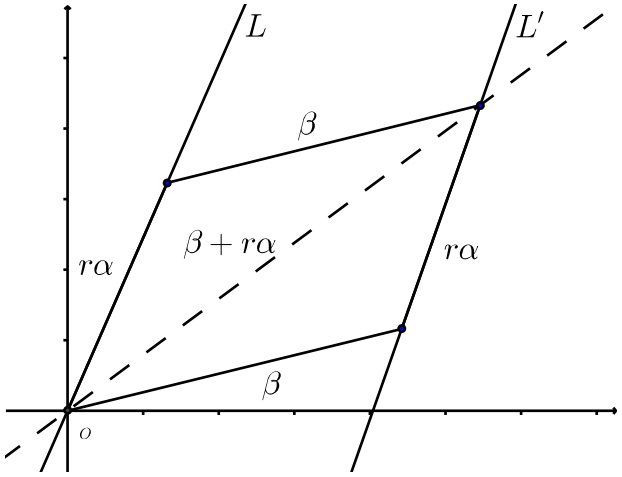



Figura 1.5: Suma de vectores.

**Ejemplo 23**
Sea $G = S_3$ y $H = \langle(1\ 2)\rangle$. Hay tres clases laterales izquierdas de H.

$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

$$\begin{aligned} H &= \{(1), (1\ 2)\} = (1\ 2)H \\ (1\ 3)H &= \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H \\ (2\ 3)H &= \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H \end{aligned}$$

Son tres clases laterales izquierdas; son disjuntas y de tamaño 2.

$$\begin{aligned} H &= \{(1), (1\ 2)\} = H(1\ 2) \\ H(1\ 3) &= \{(1\ 3), (1\ 3\ 2)\} = H(1\ 3\ 2) \\ H(2\ 3) &= \{(2\ 3), (1\ 2\ 3)\} = H(1\ 2\ 3) \end{aligned}$$

Son tres clases laterales derechas; son disjuntas y de tamaño 2.

**Lema 1.4.1**
Sea $H \leq G$ y $a, b \in G$.

i) $aH = bH$ si y sólo si $b^{-1}a \in H$. En particular, $aH = H$ si y sólo si $a \in H$.

ii) Si $aH \cap bH \neq \emptyset$, entonces $aH = bH$.

iii) $|aH| = |H|$ para todo $a \in G$.

***Demostración.*** i) Necesidad. Si $aH = bH$ tenemos que $a = ae \in aH$, por lo que $a \in bH$, luego $a = bh$ para algún $h \in H$, por lo tanto $b^{-1}a = h \in H$.

Suficiencia. Sea $b^{-1}a = h_0$ para $h_0 \in H$. Observe que $ah = (bh_0)h = b(h_0h) \in bH$, para todo $h \in H$. Por lo tanto $aH \subseteq bH$; análogamente $bh = (ah_0^{-1})h = a(h_0^{-1}h) \in aH$, para todo $h \in H$. Por lo tanto $bH \subseteq aH$.

ii) Si $aH \cap bH \neq \emptyset$, entonces $ah_1 = bh_2$ para $h_1, h_2 \in H$. Entonces $b^{-1}a = h_2h_1^{-1} \in H$. Por 1) $aH = bH$.

iii) Definimos $\varphi : H \to aH$ como $\varphi : h \mapsto ah$. Es claro que $\varphi$ es una biyección.

■

**Teorema 1.4.2 (Lagrange)**
Sea $G$ un grupo finito y $H \leq G$ un subgrupo, entonces $|H| \,\big|\, |G|$.

***Demostración.*** Sea $\{a_1H, \ldots, a_tH\}$ la familia de las distintas clases laterales de $H$ en $G$. Entonces $G = a_1H \cup a_2H \cup \cdots \cup a_tH$, ya que para todo $g \in G$, $g \in gH = a_iH$ para algún $i$; por otra parte $|G| = |a_1H| + \cdots + |a_tH|$ y por el lema anterior $|a_iH| = |H|$ para toda $i$, por lo tanto $|G| = t\,|H|$.

■

**Definición 1.4.7**
El índice de $H$ en $G$ es el número de clases laterales de $H$ en $G$, denotado por $[G : H]$.

Si $G$ es finito, entonces de la demostración del teorema de Lagrange y de la definición anterior tenemos $[G : H] = t$, es decir, $|G| = [G : H]\,|H|$. Esta fórmula muestra que $[G : H] \,\big|\, |G|$, entonces $[G : H] = |G|/|H|$.

**Ejemplo 24**
Recordemos el grupo diédrico $D_{2n} = \langle \rho, \sigma \rangle$, con $\rho$ una rotación y $\sigma$ una reflexión. Entonces, sabemos que contiene un subgrupo cíclico de orden $n$ generado por una rotación $\rho$. El subgrupo $\langle \rho \rangle$ tiene índice dos, es decir, $[D_{2n} : \langle \rho \rangle]$=2; por lo tanto tiene dos clases laterales: $\langle \rho \rangle$ y $\sigma \langle \rho \rangle$ donde $\sigma$ es cualquier reflexión que no está en $\langle \rho \rangle$. Por lo tanto, todos los elementos $\alpha \in D_{2n}$ se pueden factorizar como $\sigma^i \rho^j$ con $i = 0, 1$, y $0 \leq j \leq n$.

**Corolario 1.4.2**
Si $G$ es un grupo finito, $a \in G$, entonces el orden de $a$ es un divisor de $|G|$.

***Demostración.*** Sea $\langle a \rangle$ el subgrupo generado por $a$; sea $n$ el orden de $a$. Como podemos ver $a^n = e$, entonces el subgrupo $\langle a \rangle$ sólo tiene exactamente $n$ elementos, luego usando el teorema de Lagrange tenemos que $n \big| |G|$. ■

**Corolario 1.4.3**
Si $G$ es un grupo finito, entonces $a^{|G|} = e$, para todo $a \in G$.

***Demostración.*** Usando el corolario anterior y su notación tenemos que $n \big| |G|$ con $n$ el orden de $a$. Entonces $|G| = nm$, para algún $m \in \mathbb{Z}$, por lo que

$$a^{|G|} = a^{nm} = (a^n)^m = e^m = e$$

que es justamente lo que deseabamos probar. ■

**Corolario 1.4.4**
Si $p$ es un primo, entonces cualquier grupo $G$ de orden $p$ es cíclico.

***Demostración.*** Primero veamos que $G$ no tiene subgrupos no triviales. Sea $H \leq G$, entonces tenemos que $|H|$ tiene que dividir $|G| = p$, dejándo sólo dos posibilidades, es decir, $|H| = 1$ o $|H| = p$.

Lo primero implica que $H = \langle e \rangle$, y el segundo que $H = G$. Suponga ahora que $a \neq e \in G$, y sea $H = \langle a \rangle$ usando la observación anterior y puesto que $H$ es distinto de $e$, entonces $H$ tiene exactamente $p$ elementos. Por lo tanto $H = G$.
■

**Observación 15**
Hemos visto que $(\mathbb{Z}_m, +)$ bajo la adición es un grupo cíclico de orden $m$. Ahora definamos la multiplicación como

$$\mu : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, \text{ donde } [a][b] = [ab].$$

Como podemos ver este producto es asociativo, conmutativo, y [1] es el elemento identidad. Sin embargo no es grupo bajo esta operación, pues los inversos no existen; por ejemplo [0] no tiene inverso multiplicativo.

**Proposición 1.4.6**
El conjunto $\cup(\mathbb{Z}_m)$, definido por

$$\cup(\mathbb{Z}_m) = \{[r] \in \mathbb{Z}_m : (r, m) = 1\},$$

es un grupo multiplicativo de orden $\Phi(m)$, donde $\Phi$ es la función $\Phi$ de Euler (Definición 1.6.5). En particular, si $p$ es un primo, entonces $\cup(\mathbb{Z}_p) = \mathbb{Z}_p^*$, los elementos no nulos de $\mathbb{Z}_p$, es un grupo multiplicativo de orden $p-1$.

***Demostración.*** Observe que si $(r, m) = 1 = (r', m)$, entonces $(rr', m) = 1$ pues $rs + mt = 1$ y $r's' + mt' + 1$ para $s, t, s', t' \in \mathbb{Z}$, por lo cual $(rr')(ss') + m(tr's' + t'rs + mtt') = 1$. Por lo tanto $\cup(\mathbb{Z}_m)$ es cerrado bajo el producto. Además hemos mencionado antes es asociativo y [1] es la identidad. Ahora, si $(a, m) = 1$, entonces veamos que $[a][x] = [1]$ tiene solución $[x] \in \mathbb{Z}_m$. Como $(a, m) = 1$ entonces existen $x, s \in \mathbb{Z}$ tal que $ax + sm = 1$, entonces $(x, m) = 1$ por lo tanto $[x] \in \mathbb{Z}_m$ le cual cumple lo deseado. ■

**Corolario 1.4.5**
Si $p$ es primo y $a \in \mathbb{Z}$, entonces $a^p \equiv a \ mod \ p$.

***Demostración.*** Es suficiente con demostrar que $[a^p] = [a]$ en $\mathbb{Z}_p$. Si $[a] = [0]$, entonces $[a^p] = [a]^p = [0]^p = [0] = [a]$. Ahora, si $[a] \neq [0]$, entonces $[a] \in \mathbb{Z}_p^*$, sabemos que $|\mathbb{Z}_p^*| = p - 1$, por lo cual $[a]^{p-1} = [1]$ por lo tanto $[a]^p = [a]$. ■

**Ejemplo 25**
Es fácil ver que

$$\cup(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$$

es un grupo.

**Teorema 1.4.3**
Un entero $p$ es primo si y sólo si $(p-1)! \equiv -1 \ mod \ p$.

***Demostración.*** Necesidad. Suponga que $p$ es primo. En general para un grupo abeliano $G$. Sea $G = \{a_1, \ldots, a_n\}$, considere el producto $a_1 \cdot a_2 \cdots a_n$. Como $G$ es abeliano tenemos que $a_1 \cdot a_2 \cdot \cdots \cdot a_n = a_1' \cdot a_2' \cdot \cdots \cdot a_k'$ donde $(a_i')^2 = 1$ y $k \leq n$, es decir, cancelamos todos los elementos que no sean su propio inverso. En particular en $\mathbb{Z}_p^*$ el único elemento de orden 2 es $[-1]$, por lo cual el producto de todos los elementos de $\mathbb{Z}_p^*$ es $[(p-1)!] = [-1]$ por lo tanto $(p-1)! \equiv -1 \ mod \ p$.

Suficiencia. Ahora suponga que $m$ es un número compuesto, es decir, hay enteros $a$ y $b$ con $m = ab$ y $1 < a \leq b < m$. Si $a < b$, entonces $m = ab$ divide a $(m-1)!$, por lo tanto $(m-1)! \equiv 0 \ mod \ m$. Si $a = b$, entonces $m = a^2$. Si $a = 2$, entonces

$(a^2-1)! = 3! = 6 \equiv 2 \ mod\ 4$ y $2 \not\equiv -1 \ mod\ 4$. Si $2 < a$, entonces $2a < a^2$, y entonces $a$ y $2a$ son factores de $(a^2-1)!$; por lo que $(a^2-1)! \equiv 0 \ mod\ a^2$. Por lo tanto, $(a^2-1)! \not\equiv -1 \ mod\ a^2$. ■

## 1.5. Homomorfismos

**Definición 1.5.1**
Si $(G, *)$, $(H, \circ)$ grupos, entonces la función $f : G \to H$ es un homomorfismo de grupos. Si

$$f(x * y) = f(x) \circ f(y)$$

para todo $x, y \in G$. Si también es una biyección, entonces $f$ es llamado un isomorfismo. Dos grupos $G$ y $H$ son llamados isomorfos, denotado por $G \cong H$, si hay un isomorfismo $f : G \to H$ entre ellos.

**Definición 1.5.2**
Sea $a_1, \ldots, a_n$ la lista de elementos distintos de $G$ una tabla de multiplicación de $G$ es un arreglo de $n \times n$ en donde la entrada $ij$ es $a_i a_j$.

| $G$ | $a_1$ | $a_2$ | $\ldots$ | $a_j$ | $\ldots$ | $a_n$ |
|---|---|---|---|---|---|---|
| $a_1$ | $a_1a_1$ | $a_1a_2$ | $\ldots$ | $a_1a_j$ | $\ldots$ | $a_1a_n$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $a_i$ | $a_ia_1$ | $a_ia_2$ | $\ldots$ | $a_ia_j$ | $\ldots$ | $a_ia_n$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $a_n$ | $a_na_1$ | $a_na_2$ | $\ldots$ | $a_na_j$ | $\ldots$ | $a_na_n$ |

Esta tabla depende del orden de las $a_i$ y hay $n!$ tablas de multiplicar distintas. Si $a_1, \ldots, a_n$ es una lista de los elementos de $G$ sin repetición y si $f : G \to H$ es un isomorfismo de grupos, entonces $f(a_1), \ldots, f(a_n)$ es una lista de todos los elementos de $H$ sin repetición por ser $f$ una biyección, y esta lista determina una tabla de multiplicación para $H$.

| $H$ | $f(a_1)$ | $f(a_2)$ | $\ldots$ | $f(a_j)$ | $\ldots$ | $f(a_n)$ |
|---|---|---|---|---|---|---|
| $f(a_1)$ | $f(a_1)f(a_1)$ | $f(a_1)f(a_2)$ | $\ldots$ | $f(a_1)f(a_j)$ | $\ldots$ | $f(a_1)f(a_n)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $f(a_i)$ | $f(a_i)f(a_1)$ | $f(a_i)f(a_2)$ | $\ldots$ | $f(a_i)f(a_j)$ | $\ldots$ | $f(a_i)f(a_n)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $f(a_n)$ | $f(a_n)f(a_1)$ | $f(a_n)(a_2)$ | $\ldots$ | $f(a_n)f(a_j)$ | $\ldots$ | $f(a_n)f(a_n)$ |

Si $a_ia_j$ es la $ij$-ésima entrada en la tabla de multiplicación de $G$, entonces $f(a_i)f(a_j) = f(a_ia_j)$ es la $ij$-ésima entrada en la tabla de multiplicación de $H$. En este sentido, grupos isomorfos tienen la misma tabla de multiplicación. Por

lo tanto grupos isomorfos, son esencialmente lo mismo, difiriendo únicamente por la notación de los elementos y la operación.

**Ejemplo 26**
Sea $G = S_3$ el grupo simétrico de permutaciones de $\{1, 2, 3\}$, y $H = S_Y$, el grupo simétrico de todas las permutaciones de $Y = \{a, b, c\}$, son isomorfos. Primero, enumeramos los elementos de $G$:

$$(1),\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)$$

Después definimos la función $\varphi : S_3 \to S_Y$, entonces reemplace números por letras:

$$(1),\ (a\ b),\ (a\ c),\ (b\ c),\ (a\ b\ c),\ (a\ c\ b).$$

$\varphi : G \to H$ es un isomorfismo y se puede ver que las tablas de multiplicar coinciden.

**Lema 1.5.1**
Sea $f : G \to H$ un homomorfismo de grupos. Se cumple lo siguiente:

i) $f(1_G) = 1_H$.
ii) $f(x^{-1}) = f(x)^{-1}$.
iii) $f(x^n) = f(x)^n$, para todo $n \in \mathbb{Z}$.

***Demostración.*** Denotemos por $*$ a la operación en $G$ y por $\circ$ la operación en $H$
i) $f(1_G) = f(1_G * 1_G) = f(1) \circ f(1)$, entonces $f(1_G) = 1_H$.

ii) $1_G = x * x^{-1}$, lo que implica $1_H = f(x) \circ f(x^{-1})$ y $1_H = f(x^{-1}) \circ f(x)$, por lo tanto $f(x^{-1}) = f(x)^{-1}$.

iii) Haremos la prueba por inducción sobre $n$. Para $n \geq 0$, el punto ii) es la base de la inducción.

$$f(x^n) = f(x^{n-1} * x) = f(x^{n-1}) \circ f(x) = f(x)^{n-1} \circ f(x) = f(x)^n.$$

Ahora $x^{-n} = (x^{-1})^n$, entonces

$$f(x^{-n}) = f\left(x^{-1}\right)^n = f(x)^{-n}.$$

■

**Observación 16**
Una propiedad de un grupo $G$ que es compartida con otro grupo que es isomorfo a él es llamada un invariante de $G$. Por ejemplo, el orden de $|G|$ es un invariante de $G$, porque grupos isomorfos tienen el mismo orden. Ser abelianos es un invariante (si $f$ es un isomorfismo y $a, b$ conmutan, entonces $ab = ba$ y

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

por lo tanto, $f(a)$ y $f(b)$ conmutan). $\mathbb{Z}_6$ y $S_3$ ambos tienen orden 6, pero no son isomorfos, porque $\mathbb{Z}_6$ es abeliano y $S_3$ no lo es.

**Ejemplo 27**
Dos grupos abelianos del mismo orden que no son isomorfos

$$V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

y sea

$$\mu_4 = \{1, -i, -1, -i\}$$

si $f : v \to \mu_4$ isomorfismo, entonces existiría $x \in V$ tal que $f(x) = i$, pero todos los elementos distintos de 1 tienen orden 2, por lo cual $i^2 = f(x)^2 = f(x^2) = f((1)) = 1$, contradiciendo el hecho de que $i^2 = -1$. Por lo tanto, $V$ y $\mu_4$ no son isomorfos.

**Definición 1.5.3**
Si $f : G \to H$ es un homomorfismo, se define el núcleo y la imagen de $f$ como

$$kerf = \{x \in G : f(x) = 1\} \text{ y } imf = \{h \in H : h = f(x) \text{ para algún } x \in G\}$$

**Ejemplo 28**
Si $\mu_2$ es el grupo multiplicativo $\mu_2 = \{\pm 1\}$, entonces $sgn : S_n \to \mu_2$ es un homomorfismo. Tenemos que

$$kerf(sgn) = A_n \text{ e } imf = \mu_2.$$

**Proposición 1.5.1**
Sea $f : G \to H$ un homomorfismo.

i) $kerf$ es un subgrupo de $G$ y $imf$ es un subgrupo de $H$.

ii) Si $x \in kerf$ y si $a \in G$, entonces $axa^{-1} \in kerf$.

iii) $f$ es inyectiva si y sólo si $kerf = \{1\}$.

***Demostración.*** i) Sabemos que $f(1_G) = 1_H$, entonces $1_G \in kerf$. Si $x, y \in kerf$, se sigue que $f(xy) = f(x)f(y) = 1_H$. Finalmente; si $x \in kerf$, entonces $f(x^{-1}) = f(x)^{-1} = 1_H$ por lo tanto $x^{-1} \in kerf$.

Ahora, tenemos que $1_H = f(1_G)$, por lo que $1_H \in imf$. Si $a, b \in imf$, entonces $a = f(x)$, $b = f(y)$ para algunos $x, y \in G$, por lo cual $ab = f(x)f(y) = f(xy)$. Por lo tanto $a, b \in imf$. Luego, si $a \in imf$, entonces $a = f(x)$ para algún $x \in G$ además $f(x^{-1}) = f(x)^{-1}$, luego entonces $a^{-1} = f(x^{-1})$. Por lo tanto $a^{-1} \in imf$.

ii) $f(axa^{-1}) = f(a)f(x)f(a)^{-1} = f(a)f(a)^{-1} = 1_H$, entonces $axa^{-1} \in kerf$.

iii) Necesidad. Sea $a \in kerf$, entonces $f(a) = 1_H$, además $f(1_G) = 1_H$ y como

$f$ es inyectiva, entonces $a = 1_G$.

Suficiencia. Si $kerf = \{1_G\}$ y $f(a) = f(b)$, entonces $f(ab^{-1}) = 1_H$ por lo que $ab^{-1} = 1_G$, entonces $a = b$. ■

**Definición 1.5.4**
Un subgrupo $K \leq G$ es normal. Si $k \in K$ y $g \in G$ implica que $gkg^{-1} \in K$. Si $K$ es un subgrupo normal, escribimos $K \trianglelefteq G$.

**Observación 17**
La parte ii) de la proposición anterior nos dice que el núcleo de un homomorfismo siempre es un grupo normal.

Si $G$ es un grupo abeliano, entonces todo subgrupo $K$ es normal. Ya que, para todo $k \in K \leq G$ y $g \in G$; tenemos que $gkg^{-1} = kgg^{-1} = k \in K$.

El subgrupo cíclico $H = \langle(1\ 2)\rangle$ de $S_3$; formado por (1) y (1 2), no es es un subgrupo normal de $S_3$. Si $\alpha = (1\ 2\ 3)$, entonces $\alpha^{-1} = (3\ 2\ 1)$, y

$$\alpha(1\ 2)\alpha^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \notin H$$

por lo tanto $H$ no es normal.

**Definición 1.5.5**
Si $G$ es un grupo y $a \in G$, entonces un conjugado de $a$ es cualquier elemento en $G$ de la forma $gag^{-1}$ donde $g \in G$.

Es claro que un subgrupo $K \leq G$ es normal si y sólo si $K$ contiene todos los conjugados de sus elementos: Si $k \in K$, entonces $gkg^{-1} \in K$ para todos los $g \in G$.

**Definición 1.5.6**
Sea $G$ un grupo y $g \in G$, definimos la conjugación $\gamma_g : G \to G$ por $\gamma_g(a) = gag^{-1}$ para todo $a \in G$.

**Proposición 1.5.2**
i) Si $G$ es un grupo y $g \in G$, entonces $\gamma_g : G \to G$ es un isomorfismo.

ii) En un grupo los elementos conjugados tienen el mismo orden.

***Demostración.*** i) Observe que si $g, h \in G$, entonces

$$\begin{aligned}(\gamma_g\gamma_h)(a) &= \gamma_g(hah^{-1}) \\ &= g(hah^{-1})g^{-1} \\ &= (gh)a(h^{-1}g^{-1}) \\ &= (gh)a(gh)^{-1} \\ &= \gamma_{gh}(a)\end{aligned}$$

$\gamma_g \circ \gamma_h = \gamma_{gh}$, en particular, $\gamma_g \circ \gamma_{g^{-1}} = Id_G = \gamma_1$ así que $\gamma_g$ es una biyección. Ahora si $a, b \in G$, entonces

$$\gamma_g(ab) = g(ab)g^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b)$$

Por lo tanto $\gamma_g$ es isomorfismo.

ii) Suponga que $a, b \in G$ son conjugados, entonces existe $g \in G$ tal que $b = gag^{-1}$ esto es $b = \gamma_g(a)$, puesto que $\gamma_g$ es homomorfismo de grupos entonces si $n$ es el orden de $a$ y $m$ el orden de $b$, entonces $1 = \gamma_g(a^n) = b^n$, entonces $m \leq n$. Similarmente $a = \gamma_{g^{-1}}(b)$, $1 = \gamma_{g^{-1}}(b^m) = a^m$, entonces $n \leq m$ Por lo tanto $m = n$. ■

**Definición 1.5.7**
El centro de un grupo $G$, denotado por $Z(G)$, definido como

$$Z(G) = \{z \in G : zg = gz \text{ para todo } g \in G\}$$

esto es, $Z(G)$ contiene a todos elementos que conmutan con todos los elementos $G$. Un grupo $G$ es abeliano si y sólo si $Z(G) = G$.

**Ejemplo 29**
Si $G$ es un grupo, entonces un automorfismo de $G$ es un isomorfismo $f : G \to G$. Por ejemplo, toda conjugación $\gamma_g$ es un automorfismo de $G$. El conjunto $Aut(G)$ formado de todos los automorfismos de $G$ es un grupo, bajo la composición, y el conjunto de todas las conjugaciones,

$$\{\gamma_g : g \in G\},$$

es un subgrupo normal de $Aut(G)$. La función $\Gamma : G \to Aut(G)$ definida por $g \mapsto \gamma_g$, es un homomorfismo de grupos, además $im\Gamma = \{\gamma_g : g \in G\}$ y $ker\Gamma = Z(G)$.

Veamos que $ker\Gamma = Z(G)$. Sea $g \in G$ tal que $\gamma_g = Id$. Es decir, para cada $z \in G$ se tiene que $\gamma_g(z) = gzg^{-1} = z$, entonces $gzg^{-1}g = zg$, asociamos y tenemos $gz(g^{-1}g) = zg$, por lo cual $gz = zg$. Por lo tanto $g$ conmuta con todos los elementos de $G$. Por lo tanto $ker\Gamma \subseteq Z(G)$. La otra contención es clara.

**Ejemplo 30**
El grupo de Klein $V$ es un subgrupo normal de $S_4$. Recuerde que todos los elementos de $V$ son

$$V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

un conjugado preserva la estructura cíclica y $V$ contiene todas las estructuras cíclicas de este tipo.

**Proposición 1.5.3**
i) Si $H$ es un subgrupo de índice 2 en un grupo $G$, entonces $g^2 \in H$ para todo $g \in G$.

ii) Si $H$ es un subgrupo de índice 2 en un grupo $G$, entonces $H$ es un subgrupo normal de $G$.

***Demostración.*** i) Como $H$ tiene índice 2, es decir, $[G : H] = 2$, entonces sólo hay dos clases laterales de $H$ digamos $H$ y $aH$, recordemos que son ajenas y $a \notin H$. Sea $g \in G$, si $g \in H$, entonces $g^2$ también. Ahora si $g \notin H$, entonces $g = ah$ para algún $h \in H$. Supongamos que $g^2 \notin H$, entonces $g^2 = ah'$ observe que

$$g = g^{-1}g^2 = h^{-1}a^{-1}(ah') = h^{-1}h' \in H$$

pero esto es una contradicción.

ii) Veamos que si $h \in H$, entonces $ghg^{-1} \in H$ para todo $g \in G$, como en el inciso anterior sea $G = H \cup aH$ con $a \notin H$ las dos clases laterales de $H$. Si $g \in H$, entonces $ghg^{-1} \in H$ por ser subgrupo. Ahora, si $g \in aH$, entonces $g = ah'$ por lo cual $ghg^{-1} = ah'hh'^{-1}a^{-1} = ah''a^{-1}$ con $h'' = h'hh'$. Suponga que

$ghg^{-1} \notin H$, por lo cual $ghg^{-1} \in aH$. Por lo tanto $ah''a^{-1} = ah'''$ para algún $h''' \in H$, entonces $a = (h''')^{-1}h'' \in H$, pero esto es una contradicción. Por lo tanto $ghg^{-1} \in H$. ■

**Definición 1.5.8**
El grupo de los cuaternios es el grupo $Q$ de orden 8 definido como:

$$Q = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

donde $I$ es la matriz identidad,

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

El elemento $A \in Q$ tiene orden 4, así que $\langle A \rangle$ es un subgrupo de orden 4 y por eso de índice 2, es decir $[Q : \langle A \rangle] = 2$. Se puede ver que las clases laterales izquierdas de $A$ en $Q$, son $\langle A \rangle$ y $B\langle A \rangle = \{B, BA, BA^2, BA^3\}$. Por lo tanto, todo elemento en $Q$ tiene una expresión de la forma $B^iA^j$, donde $i = 0, 1$ y $j = 0, 1, 2, 3$.

**Ejemplo 31**
Se puede ver que $Q$ es un grupo no abeliano de orden 8 teniendo exactamente un elemento de orden 2, y por lo tanto un subgrupo de orden 2, es decir, $\langle -I \rangle$.

Veamos que todos los subgrupos de $Q$ son normales. Por el teorema de Lagrange, si $H \leq Q$ es subgrupo, entonces $|H|\big|8$. Por lo tanto $|H| = 1, 2, 4, 8$.

Para $|H| = 1$, entonces $H = \{e\}$. Si $|H| = 8$, entonces $H = Q$. Si $|H| = 2$, luego entonces $H = \langle -I \rangle = Z(Q) \trianglelefteq Q$. Ahora si $|H| = 4$, entonces $[Q : H] = 2$. Por lo tanto $H \trianglelefteq Q$ por la proposición anterior.

**Definición 1.5.9**
Un grupo finito no abeliano es llamado Hamiltoniano si todo subgrupo es normal.

**Observación 18**
El teorema de Lagrange prueba que el orden de un subgrupo de un grupo finito, divide el orden de $G$. ¿Si $d||G|$ existe $H \leq G$ tal que $|H| = d$? La respuesta es: No necesariamente.

**Proposición 1.5.4**
Sea $A_4$ el grupo alternante de orden 12, entonces no tiene subgrupos de orden 6.

***Demostración.*** Supongamos que existe $H \leq A_4$ tal que $|H| = 6$. Se tiene que $[A_4 : H] = 2$.Por lo tanto, para todo $\alpha \in A_4$ tenemos que $\alpha^2 \in H$; observe que si $\alpha$ es un 3-ciclo, entonces $\alpha = \alpha^4 = (\alpha^2)^2 \in H$. Por lo tanto $H$ contiene a todos los 3-ciclos pero esto es una contradicción, pues hay 8 3-ciclos en $A_4$. ■

## 1.6. Grupo cociente

**Definición 1.6.1**
Sea $S(G)$ el conjunto formado de todos los subconjuntos diferentes del vacío de un grupo $G$. Si $X, Y \in S(G)$ definimos: $XY = \{xy : x \in X \text{ y } y \in Y\}$.

Esta multiplicación es asociativa, ya que: $X(YZ)$ es el conjunto de todos los elementos de la forma $x(yz)$ donde $x \in X, y \in Y$ y $z \in Z$. Y por la asociatividad de $G$ tenemos que $x(yz) = (xy)z$ que es justamente un elemento en el conjunto $(XY)Z$.

**Observación 19**
En particular; si $a \in G$ y $K \leq G$ un subgrupo de $G$, tenemos que:

$$\{a\}K = aK \text{ la clase lateral izquierda de } a.$$

**Ejemplo 32**
Sea $H \leq G$ cualquier subgrupo de $G$, entonces

$$HH = H$$

Si $h, h' \in H$, entonces $hh' \in H$, ya que los subgrupos son cerrados bajo la multiplicación, por lo cual $HH \subseteq H$. Ahora; si $h \in H$, entonces $h = he \in HH$, porque $e \in H$, por lo cual $H \subseteq HH$. Por lo tanto $HH = H$. Es posible que $XY$ conmute a pesar de que sus elementos no lo hagan.

**Ejemplo 33**
Sea $G = S_3$ y $K = \langle(1\ 2\ 3)\rangle$; vea que $(1\ 2)$ no conmuta con $(1\ 2\ 3) \in K$. Pues

$$[(1\ 2\ 3)(1\ 2)](1) = 3 \text{ y } [(1\ 2)(1\ 2\ 3)](1) = 1$$

sin embargo $(1\ 2)K = K(1\ 2) = \{(1\ 2), (2\ 3), (1\ 3)\}$

**Lema 1.6.1**
Un subgrupo $K \leq G$ es normal si y sólo si $gK = Kg$ para todo $g \in G$.

***Demostración.*** Necesidad. Sea $gk \in gK$, puesto que $K \trianglelefteq G$, entonces $gkg^{-1} \in K$, es decir, $gkg^{-1} = k'$ para algún $k' \in K$, por lo que $gk = k'g \in Kg$. Por lo tanto $gK \subseteq Kg$.

Ahora $K \trianglelefteq G$, entonces $\left(g^{-1}\right)k\left(g^{-1}\right)^{-1} \in K$. Por lo tanto $g^{-1}kg = k''$ para algún $k'' \in K$, por lo cual $kg = gk''$, luego se tiene que $Kg \subseteq gK$. Por lo tanto $K \trianglelefteq G$, entonces $gK = Kg$ para todo $g \in G$.

Suficiencia. $gK = Kg$ para todo $g \in G$. Por lo tanto, para cada $k \in K$, $gk \in Kg$, entonces $gk = k'g$, implica $gkg^{-1} = k' \in K$. Por lo tanto $K \trianglelefteq G$ es normal. ■

**Observación 20**
En general, si $H, K \leq G$ subgrupos $HK$ no necesariamente es subgrupo.

**Ejemplo 34**
Si $H = \langle(1\ 2)\rangle$ y $K = \langle(1\ 3)\rangle$ en $S_3$ tenemos $HK = \{(1), (1\ 2), (1\ 3), (1\ 3\ 2)\}$ de orden $4 \nmid 6$ por lo cual $HK$ no puede ser subgrupo, de acuerdo con el teorema de Lagrange.

**Proposición 1.6.1**
Se cumplen las siguientes afirmaciones:
i) Si $H, K \leq G$, si uno de ellos es normal, entonces $HK = KH \leq G$.

ii) Si $H, K \trianglelefteq G$ son normales, entonces $HK \trianglelefteq G$.

***Demostración.***
i) Asumamos que $K \trianglelefteq G$, veamos que $HK = KH$. Para cada $k \in K \trianglelefteq G$, por definición tenemos que $gkg^{-1} \in K$ en particular para cada $h \in H$, $hkh^{-1} = k' \in K$.

Así que $hk = k'h$. Por lo tanto $HK \subseteq KH$. De forma similar $kh = h(h^{-1}kh) = hk' \in HK$. Esto implica que $KH \subseteq HK$. Por lo tanto $KH = HK$.

Ahora veamos $HK$ es subgrupo de $G$.

$1 = (1)(1) \in HK$.

Si $(hk) \in HK$, entonces $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

$(h_1k_1)(h_2k_2) \in H(KH)K = H(HK)K = (HH)(KK)$. Por lo tanto $HK$ es cerrado bajo la operación.

ii) Sea $g \in G$ arbitrario pero fijo. Entonces

$$gHK = H(gK) = HKg$$

■

**Teorema 1.6.1**
Sea $G/K = \{gK : g \in G\}$. Si $K \trianglelefteq G$, entonces $G/K$ es grupo con operación $(aK)(bK) = abK$ para todo $a, b \in G$. $G/K$ es llamado "Grupo cociente de $G$ módulo $K$".

***Demostración.*** $(aK)(bK) = a(Kb)K = abKK = (ab)K$ esto es por asociatividad en $S(G)$ (recordemos que $aK = \{a\}K$).

Por lo tanto; el producto de clases laterales izquierdas es otra vez una clase lateral izquierda. Por lo tanto la operación en $G/K$ está bien definida.

La asociatividad se hereda de $S(G)$.

$K \in G/K$ es la identidad, es decir $(gK)(K) = K(gK) = gK$.
El inverso de $aK$ es $a^{-1}K$. ■

**Observación 21**
Cuando $G$ es finito, $|G/K| = [G : K] = |G|/|K|$

**Observación 22**
El producto no depende de los representantes. Si $aK = a'K$ y $bK = b'K$, entonces existen $k, k' \in K$ tales que $a' = ak$ y $b' = bk'$, por lo que $a'b'K = a'Kb'K = akKbk'K = aKbK = abK$

**Ejemplo 35**
$(\mathbb{Z}, +)$ grupo abeliano, entonces $\langle m\rangle \trianglelefteq \mathbb{Z}$ con $m \in \mathbb{Z}$; tenemos que $\mathbb{Z}/\langle m\rangle = \mathbb{Z}_m$ y

$$a + \langle m\rangle = \{a + km : k \in \mathbb{Z}\} = [a]$$

**Observación 23**
$(a + \langle m\rangle) + (b + \langle m\rangle) = (a + b) + \langle m\rangle$ y $[a] + [b] = [a + b]$.

**Corolario 1.6.1**
Todo subgrupo normal $K \trianglelefteq G$ es el núcleo de algún homomorfismo.

***Demostración.*** Definimos el mapeo natural

$$\Pi : G \to G/K \text{ como } \Pi : g \to \Pi(g) = gK$$

observe que $(aK)(bK) = abK$, entonces $\Pi(a)\Pi(b) = \Pi(ab)$.

Por lo tanto $\Pi$ es homomorfismo de grupos y es sobreyectivo. $K$ es la identidad de $G/K$.

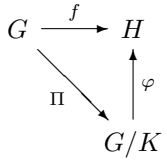
Ahora $ker\Pi = \{a \in G : \Pi(a) = \{K\}\} = \{a \in G : a\{K\} = \{K\}\} = \{K\}$. Por lo tanto $ker\Pi = \{K\}$. ■

**Teorema 1.6.2 (Primer teorema de isomorfismos)**
Si $f : G \to H$ es un homomorfismo, entonces

$$kerf \trianglelefteq G \text{ y } G/kerf \simeq imf.$$

Con más detalle, si $K = kerf$ y $\varphi : G/K \to imf \leq H$ definida como $\varphi : (aK) \mapsto f(a)$, entonces $\varphi$ es isomorfismo.

**Observación 24**
El siguiente diagrama describe la prueba del primer teorema de isomorfismos, donde $\Pi : G \to G/K$ es el mapeo natural $\Pi : a \mapsto aK$.




***Demostración.*** Sea $K = kerf \trianglelefteq G$.

Veamos que $\varphi$ está bien definida: Si $aK = bK$, entonces $a = bk$ para algún $k \in K$, entonces $f(a) = f(b)f(k)$, pero $f(k) = 1$ pues $k \in kerf$. Por lo tanto $f(a) = f(b)$. Resta demostrar que $\varphi$ es homomorfismo de grupos. Note que $f$ es homomorfismo de grupos y $\varphi(aK) = f(a)$, tenemos que

$$\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK)$$

observe que $im\varphi \leq imf$. Ahora si $y \in imf$, entonces $y = f(a)$ para $a \in G$, por lo cual $y = f(a) = \varphi(aK)$. Por lo tanto $im\varphi = imf$. Por último si $\varphi(aK) = \varphi(bK)$, entonces $f(a) = f(b)$, luego entonces $f(a^{-1}b) = 1$, entonces $a^{-1}b \in K$. Por lo tanto $a^{-1}bK = K$ si y sólo si $bK = aK$. Podemos concluir que $\varphi : G/K \to imf$ es isomorfismo. ■

**Ejemplo 36**
Sea $G = \langle a \rangle$ con $a$ de orden $m \in \mathbb{Z}$. Definimos un homomorfismo $f : \mathbb{Z} \to G$ con $f : n \mapsto a^n$, para todo $n \in \mathbb{Z}$.

Se puede ver que $f$ es homomorfismo de grupos y sobreyectivo, entonces $imf = G$. Además $kerf = \{n \in \mathbb{Z} : a^n = 1\} = \langle m \rangle$. Por lo tanto $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle \simeq G$.

**Ejemplo 37**
¿Cómo es el grupo cociente $\mathbb{R}/\mathbb{Z}$? Definimos $f : \mathbb{R} \to S'$ por $x \mapsto e^{2\pi ix}$. Tenemos que $(\mathbb{R}, +)$ y $(S', *)$, entonces $f$ es homomorfismo ya que $f(x + y) = f(x)f(y)$; además $f$ es sobreyectiva,

$$kerf = \{x \in \mathbb{R} : e^{2\pi ix} = cos(2\pi x) + isen(2\pi x) = 1\}$$

esto es $cos(2\pi x) = 1$ y $sen(2\pi x) = 0$ donde $x$ es un número entero. Puesto que $1 \in kerf$ y $\langle 1\rangle \leq kerf$ tenemos que $kerf = \mathbb{Z}$. Por lo tanto, usando el primer teorema de isomorfismos, tenemos que $\mathbb{R}/\mathbb{Z} \simeq S'$.

**Proposición 1.6.2**
Sea $G$ un grupo finito y $H, K \leq G$ subgrupos, entonces $|H||K| = |HK||H \cap K|$ donde $HK = \{hk : h \in H \text{ y } k \in K\}$.

***Demostración.*** Definimos $f : H \times K \to HK$, como $f : (h, k) \mapsto hk$. Es claro que $f$ es sobreyectiva. Observe que $H \times K$ es la unión disjunta de $\cup_{x\in HK} f^{-1}(x)$. Por lo tanto, es suficiente con ver que $|f^{-1}(x)| = |H \cap K|$, para todo $x \in HK$; en donde $f^{-1}(x) = \{(h, k) \in H \times K : hk = x\}$.

Veamos que si $x = hk$, entonces $f^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}$. Sea $(hd, d^{-1}k)$ con $d \in H \cap K$, entonces $f(hd, d^{-1}k) = (hd)(d^{-1}k) = hk = x$, por lo tanto $\{(hd, d^{-1}k)|d \in H \cap K\} \subseteq f^{-1}(x)$.

Ahora, sea $(h', k') \in f^{-1}(x)$, entonces $h'k' = hk$, luego $h^{-1}h' = kk'^{-1} \in H \cap K$; denotemos $d = h^{-1}h' = kk'^{-1}$, entonces $h' = hd$ y $k' = d^{-1}k$. Entonces $f^{-1}(x) \subseteq \{(hd, d^{-1}k)|d \in H \cap K\}$.

Por lo tanto $|f^{-1}(x)| = |\{(hd, d^{-1}k) : d \in H \cap K\}| = |H \cap K|$ ya que $d \to (hd, d^{-1}k)$ es una biyección. Por lo tanto, $|H||K| = |H \cap K||HK|$. ■

**Teorema 1.6.3 (Segundo teorema de isomorfismos)**
Si $H, K \leq G$ subgrupos y $H \trianglelefteq G$, entonces $HK$ es subgrupo, $H \cap K \trianglelefteq K$ y

$$HK/H \simeq K/H \cap K.$$

***Demostración.*** $H \trianglelefteq G$, entonces $HK$ es subgrupo. Observe que si $H \leq S \leq G$ entonces $H \trianglelefteq S$ ($ghg^{-1} \in H$ para todo $g \in G$ en particular $ghg^{-1} \in H$ para todo $g \in S$) por lo que $H \trianglelefteq HK$.

Veamos ahora que las clases $xH \in HK/H$ son de la forma $kH$ para algún $k \in K$. Por definición tenemos que $xH = hkH$ para algunos $h \in H$ y $k \in K$ además $H \trianglelefteq G$, entonces $hk = k(k^{-1}hk) = kh'$ para algún $h' \in H$. Por lo tanto $hkH = kh'H = kH$. Por lo tanto $f : K \to HK/H$, donde $k \to kH$; es sobreyectiva. Luego, $f$ es homomorfismo de grupos ya que es la restricción de

$\Pi : G \to G/H$. Observe que $ker\Pi = H$, entonces $kerf = H \cap K$ por lo que $H \cap K \trianglelefteq K$, del primer teorema de isomorfismos para $f$ obtenemos que

$$K/(H \cap K) \simeq HK/H.$$

■

**Teorema 1.6.4 (Tercer teorema de isomorfismos)**
Si $H, K \trianglelefteq G$ normales, con $K \leq H$, entonces $H/K \trianglelefteq G/K$ y

$$(G/K)/(H/K) \simeq G/H.$$

***Demostración.*** Definimos $f : G/K \to G/H$ como $aK \to aH$. $f$ está bien definida pues $aK = a'K$ si y sólo si $a^{-1}a' \in K \leq H$. Entonces $a^{-1}a' \in H$ si y sólo si $a'H = aH$. Además tenemos que $f$ es homomorfismo de grupos ya que

$$aKbK = abK \to abH = aHbH$$

y es sobreyectivo. Observe que $aH = H$ si y sólo si $a \in H$, entonces $kerf = H/K \trianglelefteq G/K$, deduciendo lo deseado por el primer teorema de isomorfismos. ■

**Teorema 1.6.5 (Teorema de correspondencia)**
Sea $G$ un grupo, $K \trianglelefteq G$ y $\Pi : G \to G/K$ el mapeo natural, entonces

$$S \to \Pi(S) = S/K$$

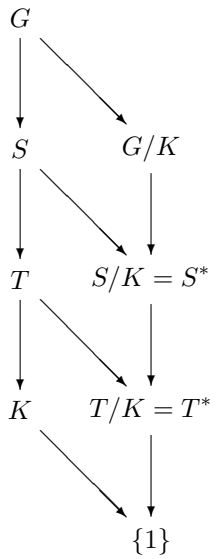
es una biyección entre $Sub(G; K)$, la familia de subgrupos de $S$ en $G$ que contienen a $K$ y $Sub(G/K)$, la familia de todos los subgrupos de $G/K$. Si denotamos $S^* = S/K$, entonces

$$T \leq S \leq G \text{ si y sólo si } T^* \leq S^* \text{ en tal caso } [S : T] = [S^* : T^*],$$

y

$$T \trianglelefteq S \text{ si y sólo si } T^* \trianglelefteq S^* \text{ en tal caso } S/T \simeq S^*/T^*$$

El siguiente diagrama nos ayudará a recordar este teorema




***Demostración.*** Definimos

$$\Phi : Sub(G;K) \to Sub(G/K), \text{ por } \Phi : S \to S/K$$

se puede ver que si $K \leq S \leq G$, entonces $S/K \in Sub(G/K)$ (ya que $K \trianglelefteq S$).

Recuerde que $\Pi$ es sobreyectiva. Veamos que $\Pi$ es inyectiva, para ello $K \leq S \leq G$, entonces $\Pi^{-1}\Pi(S) = S$. Sabemos que $S \subseteq \Pi^{-1}\Pi(S)$.

Ahora sea $a \in \Pi^{-1}\Pi(S)$, entonces $\Pi(a) = \Pi(s)$ para algún $s \in S$, por lo cual $\Pi(as^{-1}) = 1$, es decir $as^{-1} \in ker\Pi = K$, lo cual implica $a = sk$ para algún $k \in K$ con $K \subseteq S$, entonces $a = sk \in S$.

Suponga que $\Pi(S) = \Pi(S')$ para $K \leq S \leq G$ y $K \leq S' \leq G$ subgrupos, por lo cual tenemos $\Pi^{-1}\Pi(S) = \Pi^{-1}\Pi(S')$, entonces $S = S'$. Por lo tanto $\Phi$ es inyectivo.

Veamos que $\Phi$ es sobreyectivo; sea $U \leq G/K$ un subgrupo. Vamos a verificar que $\Pi^{-1}(U) \leq G$.

Tenemos que $1 \in K \subseteq \Pi^{-1}(U)$ ya que $K = \Pi^{-1}(1_{G/K})$. Ahora, si $a, b \in \Pi^{-1}(U)$, entonces $\Pi(a), \Pi(b) \in U$, por lo cual $\Pi(a)\Pi(b) = \Pi(ab) \in U$, por lo tanto $ab \in \Pi^{-1}(U)$. También si $a \in \Pi^{-1}(U)$, entonces $\Pi(a) = aK \in U$, por lo cual $\Pi(a^{-1}) = a^{-1}K \in U$, por lo tanto $a^{-1} \in \Pi^{-1}(U)$.

Es claro que $\Pi(\Pi^{-1}(a)) = U$ ($\Pi$ es sobreyectiva), es decir, $K \leq \Pi^{-1}(U) \to U$.

Por lo tanto, $\Phi$ es sobreyectiva.

Veamos que $K \leq T \leq S$ si y sólo si $T^* \leq S^*$. Suponga que $K \leq T \leq S \leq G$, entonces $\Pi(T) \leq \Pi(S)$, es decir, $T/K \leq S/K$ como podemos ver, ambos son subgrupos y la contención es clara.

Ahora suponga que $T/K \leq S/K$, si $t \in T$, entonces $tK \in S/K$. Por lo tanto $tK = sK$ para algún $s \in S$, entonces $t = sk$ para algún $k \in K \leq S$, entonces $t = sk \in S$, por lo tanto $K \leq T \leq S$.

Para ver que $[S : T] = [S^* : T^*]$ es suficiente probar que

$$sT \to \Pi(s)T^* = (sK)(T/K)$$

es una biyección.

Veamos que es inyectiva; $\Pi(s_1)T^* = \Pi(s_2)T^*$, luego $\Pi(s_1^{-1}s_2) \in T^* = T/K$.

$s_1^{-1}s_2K = tK$ para algún $t \in T$, luego, $s_1^{-1}s_2 = tk$ para algún $k \in K$, por lo cual $s_2 = s_1tk$, por lo tanto $s_2T = s_1tkT = s_1T$, pues $tk \in T$.

Ahora veamos que la aplicación inversa es inyectiva

$$(sK)(T/K) = \Pi(s)T^* \to sT,\ s \in S$$

si $s_1T = s_2T$, entonces $s_2^{-1}s_1 = t$ para algún $t \in T$, por lo cual $\Pi(s_2)^{-1}\Pi(s_1) = \Pi(s_2^{-1}s_1) = \Pi(t) \in T/K = T^*$ si y sólo si $\Pi(s_1)T^* = \Pi(s_2)T^*$. Por lo tanto $sT \leftrightarrow \Pi(s)T^*$ es una biyección.

Por último veamos que $T \trianglelefteq S$ si y sólo si $T^* \trianglelefteq S^*$ y $S/T \simeq S^*/T^*$.

Observe que $K \trianglelefteq G$ y $K \leq T \leq S$, entonces $K \trianglelefteq S$ y $T \trianglelefteq S$ por el tercer teorema de isomorfismos $T/K \trianglelefteq S/K$ y $(S/K)/(T/K) \simeq S/T$.

Si $T^* \trianglelefteq S^*$ y sea $t \in T$ y sea $s \in S$ tenemos que $\Pi(sts^{-1}) = \Pi(s)\Pi(t)\Pi(s)^{-1} \in T^*$ por ser normal, por lo tanto $(sts^{-1})K = t'K$ para algún $t' \in T$, entonces $sts^{-1} = t'k \in T$.

Es decir, los subgrupos de $G/K$ son de la forma $S/K$ donde $K \leq S \leq G$ ■

**Ejemplo 38**
Sea $G = \langle a \rangle$ un grupo cíclico de orden 30. Sea $f : \mathbb{Z} \to G$ un homomorfismo sobreyectivo definido como $f(n) = a^n$.

Observe que $kerf = \langle 30 \rangle$, luego $G \simeq \mathbb{Z}/\langle 30 \rangle$

Los subgrupos

$$\langle 30\rangle \leq \langle 15\rangle \leq \langle 5\rangle \leq \mathbb{Z}$$

corresponden a

$$\langle 1\rangle = \left\langle a^{30}\right\rangle \leq \left\langle a^{15}\right\rangle \leq \left\langle a^{5}\right\rangle \leq \langle a\rangle = G$$

$G \simeq \mathbb{Z}/\langle 30\rangle$ por el teorema de la correspondencia: $\left\langle a^{30}\right\rangle \simeq \langle 30\rangle / \langle 30\rangle, \left\langle a^{15}\right\rangle \simeq \langle 15\rangle / \langle 30\rangle, \left\langle a^{5}\right\rangle \simeq \langle 5\rangle / \langle 30\rangle, \langle a\rangle \simeq \langle 1\rangle / \langle 30\rangle$ y los cocientes

$$\frac{\left\langle a^{15}\right\rangle}{\left\langle a^{30}\right\rangle} \simeq \frac{\langle 15\rangle}{\langle 30\rangle} \simeq \mathbb{Z}_2,\ \frac{\left\langle a^{5}\right\rangle}{\left\langle a^{15}\right\rangle} \simeq \frac{\langle 5\rangle}{\langle 15\rangle} \simeq \mathbb{Z}_3,\ \frac{\langle a\rangle}{\left\langle a^{5}\right\rangle} \simeq \mathbb{Z}/\langle 5\rangle \simeq \mathbb{Z}_5$$

**Proposición 1.6.3**
Si $G$ es grupo abeliano finito y $d\big||G|$, entonces G contiene un subgrupo de orden $d$.

***Demostración.*** Haremos inducción sobre $n = |G|$ y $p$ un primo divisor de $n$. Para $n = 1$ se verifica la afirmación. Ahora sea $a \in G$ de orden $k > 1$. Si $p|k$, entonces $k = pl$, entonces $a^l$ tiene orden $p$, por lo que $\left\langle a^l\right\rangle$ es un subgrupo de orden $p$. Si $p \nmid k$ sea $H = \langle a\rangle \trianglelefteq G$ por ser abeliano, entonces $G/H$ es grupo.

Observamos que $|G/H| = n/k$ es divisible por $p$. Por hipótesis inductiva, $|G/H|$ tiene un elemento de orden $p$, digamos $bH \in G/H$ recordemos que $\Pi : G \to G/H$ es homomorfismo de grupos.

Sea $m$ el orden de $b$, entonces $b^m = 1$ por lo cual $b^m H = H$ puesto que el orden de $bH$ es $p$ implica $p|m$. Sea $m = ps$, entonces $\langle b^s\rangle$ es de orden $p$.

Ahora sea $d\big||G|$ y $p|d$ por lo anterior existe $S \leq G$ tal que $|S| = p$. Ahora $S \trianglelefteq G$ por ser abeliano y $G/S$ es grupo y $|G/S| = n/p$. Por inducción y por el teorema de la correspondencia existe $H/S \leq G/S$ de orden $d/p$; además $[G : H] = [G/S : H/S] = n/d$, entonces $|H| = d$. ■

**Definición 1.6.2**
Sean $H, K$ subgrupos, entonces definimos el producto directo $H \times K$ con

$$(h, k)(h', k') = (hh', kk')$$

la identidad es el elemento $(1_H, 1_K)$ y el inverso $(h, k)^{-1} = (h^{-1}, k^{-1})$.

**Proposición 1.6.4**
Sean $G$ y $G'$ grupos, con $K \trianglelefteq G$ y $K' \trianglelefteq G'$ normales, entonces

$$K \times K' \trianglelefteq G \times G'$$

es normal y

$$(G \times G')/(K \times K') \simeq (G/K) \times (G'/K').$$

***Demostración.*** Consideramos $\Pi : G \to G/K$ y $\Pi' : G' \to G'/K'$ se puede ver que $f : G \times G' \to (G/K) \times (G'/K')$ definido como

$$(g, g') \to (\Pi(g), \Pi'(g')) = (gK, g'K')$$

es un mapeo sobreyectivo y $kerf = K \times K'$ y el resultado se obtiene por el primer teorema de isomorfismos. ■

**Proposición 1.6.5**
Si $G$ es un grupo y $H, K \trianglelefteq G$ normales y $H \cap K = \{e\}$ y $HK = G$, entonces $G \simeq H \times K$.

***Demostración.*** Veamos que para todo $g \in G$ la factorización $g = hk$ es única. Supongamos que $hk = h'k'$, entonces $h'^{-1}h = k'k^{-1} \in H \cap K = \{e\}$, entonces $h = h'$ y $k = k'$. Ahora la función $\varphi : G \to H \times K$ como $g \mapsto (h, k)$ donde $g = hk$ está bien definida por lo anterior.

Observe que $kh = hk$. Sea $h \in H$ y $k \in K$; puesto que $K$ es normal, entonces $(hkh^{-1})k^{-1} \in K$ similarmente $h(kh^{-1}k^{-1}) \in H$ pero $H \cap K = \{e\}$, entonces $hkh^{-1}k^{-1} = 1$, entonces $hk = kh$.

Demostremos que es homomorfismo; sea $g' = h'k'$, en el párrafo anterior probamos que los elementos de $H$ conmutan con los de $K$, entonces

$$\varphi(gg') = \varphi(hkh'k') = \varphi(hh'kk') = (hh', kk') = (h, k)(h', k') = \varphi(g)\varphi(g')$$

Resta demostrar que $\varphi$ es una biyección. Para ello sea $(h, k) \in H \times K$, definimos $g = hk \in G$, tenemos que $\varphi(g) = (h, k)$. Por lo tanto es sobreyectiva. Ahora si $\varphi(g) = (1, 1)$, entonces $g = (1)(1) = 1$. Por lo tanto es inyectiva. ■

**Teorema 1.6.6**
Si $(m, n) = 1$, entonces $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

***Demostración.*** Sea $a \in \mathbb{Z}$ y $[a]_m \in \mathbb{Z}_m$, se puede ver que

$f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, definida como $a \to ([a]_m, [a]_n)$ es un homomorfismo, es claro que $\langle mn \rangle \subseteq kerf$.

Ahora si $a \to (0, 0)$, entonces $m|a$ y $n|a$ y $(m, n) = 1$, entonces $mn|a$. Por lo tanto $kerf = \langle mn \rangle$.

Por el primer teorema de isomorfismos tenemos que $\mathbb{Z}/\langle mn \rangle \simeq imf \leq \mathbb{Z}_m \times \mathbb{Z}_n$. Por lo tanto $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ ya que $f$ es sobreyectiva. ■

**Ejemplo 39**
Tenemos $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$ sin embargo $\mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ pues el de la izquierda tiene elementos de orden 4 y el de la derecha no.

**Proposición 1.6.6**
Sea $G$ un grupo y $a, b \in G$ tal que $ab = ba$, donde $m$ es el orden de $a$ y $n$ el orden de $b$ y $(m, n) = 1$, entonces $ab$ tiene orden $mn$.

***Demostración.*** Como $ab = ba$, entonces $(ab)^{mn} = a^{mn}b^{mn} = 1$. Ahora suponga que $(ab)^k = 1$, entonces $a^k b^k = 1$, así que $a^k = b^{-k}$. Como $a$ tiene orden $m$, entonces $1 = a^{mk} = b^{-mk}$, y dado que $b$ tiene orden $n$, entonces $n|(-mk)$ puesto que $(m, n) = 1$, entonces $n|k$; análogamente $m|k$. Por lo tanto $mn|k$. ■

**Lema 1.6.2**
Un grupo cíclico de orden $n$ tiene un único subgrupo de orden $d$, para cada divisor de $n$ y este subgrupo es cíclico.

***Demostración.*** Sea $G = \langle a \rangle$. Si $n = cd$, sabemos que $\langle a^c \rangle$ es de orden $d$. Veamos que es único. Sea $\langle x \rangle \leq G$ de orden $d$, $x = a^m$ y $x^d = a^{dm} = 1$, entonces $n|dm$ sea $s \in \mathbb{Z}$ tal que $dm = ns$. Por lo tanto $x = a^m = (a^{n/d})^s = (a^c)^s$, por lo que $\langle x \rangle \leq \langle a^c \rangle$ puesto que ambos son de orden $d$ tenemos que $\langle x \rangle = \langle a^c \rangle$. ■

Definimos una relación de equivalencia en un grupo $G$ por $x \sim y$ si y sólo si $\langle x \rangle = \langle y \rangle$, es decir, $x, y$ generan el mismo grupo cíclico. Denotamos la clase de equivalencia de $x$ por $gen(C)$ donde $C = \langle x \rangle$; las clases de equivalencia forman una partición de $G$.

$$G = \bigcup_C gen(C)$$

donde la unión ajena corre sobre todos los subgrupos cíclicos de $G$.

Si $|C| = n$, entonces $|gen(C)| = |\{k \leq n : (k, n) = 1\}| = \Phi(n)$ es la función de Euler.

**Definición 1.6.3**
Si $n \geq 1$ un entero, $\zeta \in \mathbb{C}$ es una raíz $n$ de 1 si $\zeta^n = 1$.

**Observación 25**
Las raíces de la unidad son $e^{2\pi ik/n}$ con $k = 0, 1, 2, \ldots, n-1$.

Diremos que $\zeta$ es una raíz primitiva de 1, si $n$ es el mínimo entero positivo tal que $\zeta^n = 1$.

**Definición 1.6.4**
Si $d$ es entero positivo, entonces el $d$-ésimo polinomio ciclotómico se define por

$$\Phi_d(x) = \Pi(x - \zeta)$$

que corre sobre todas las raíces primitivas $d$ de la unidad.

**Proposición 1.6.7**
Para $n \in \mathbb{Z}$ con $n \geq 1$, entonces $x^n - 1 = \Pi_{d|n}\Phi_d(x)$.

***Demostración.*** Denotamos el producto de todas las raíces $n$-ésimas de 1 como

$$x^n - 1 = \Pi(x - \zeta)$$

este producto corre sobre todas las raíces $n$-ésimas de uno por lo que el resultado se obtiene al agrupar los factores que contienen raíces $d$-primitivas de la unidad para cada $n$. ■

**Definición 1.6.5**
La función $\Phi$ de Euler

$$\Phi(n) = grado(\Phi_n(x)).$$

**Proposición 1.6.8**
Si $n \geq 1$ entero, entonces $\Phi(n) = \{k \leq n : (k, n) = 1\}$.

***Demostración.*** Sólo necesitamos observar que $e^{2\pi ik/n}$ es raíz primitiva de 1, si y sólo si $(k, n) = 1$. ■

**Corolario 1.6.2**
Se cumple que $n = \sum_{d|n} \Phi(d)$. Observe que $\Phi(d) = grado(\Phi_d(x))$.

**Teorema 1.6.7**
Un grupo $G$ de orden $n$ es cíclico si y sólo si para cada divisor $d$ en $n$ existe a lo más un subgrupo cíclico de orden $d$.

***Demostración.*** Si $G$ es cíclico por el Lema 1.6.2 obtenemos lo deseado. Ahora; tenemos que $G = \cup_{C \leq G} gen(C)$, entonces

$$n = |G| = \sum_{C \leq G} |gen(C)| = \sum_{C \leq G} \Phi(|C|)$$

por hipótesis para cada divisor $d|n$ existen a lo más un subgrupo cíclico de orden $d$.

Por lo tanto $n = \sum\limits_{C \leq G} \Phi(|C|) \leq \sum_{d|n} \Phi(d) = n$. A lo más hay un subgrupo cíclico de orden $d$.

Por lo tanto $\sum\limits_{C \leq G} \Phi(|C|) = \sum_{d|n} \Phi(d)$. Para cada $d|n$, $\Phi(d)$ viene de $\Phi(|C|)$ donde $C$ es cíclico de orden $d$, en particular $\Phi(n)$ viene de un subgrupo cíclico $\langle a \rangle$ de orden $n$. Por lo tanto $G = \langle a \rangle$ por cardinalidad. ■

## 1.7. Acciones en grupos.

**Teorema 1.7.1 (Teorema de Cayley.)**
Todo grupo $G$ es isomorfo a un subgrupo del grupo de simetrías $S_G$. En particular, si $|G| = n$, entonces $G$ es isomorfo a un subgrupo de $S_n$.

***Demostración.*** Para cada $a \in G$ definimos

$$\tau_a : G \to G \text{ tal que } \tau_a(g) = ag \text{ para todo } g \in G$$

($\tau_a$ no es homomorfismo para $a \neq 1$).

Observe que $\tau_a \circ \tau_b = \tau_{ab}$.

$$\tau_a \circ \tau_b(g) = \tau_a(bg) = abg = \tau_{ab}(g) \text{ para todo } g \in G.$$

por lo anterior $\tau_a \circ \tau_{a^{-1}} = \tau_e = Id_G$. Luego entonces $\tau_a$ es biyección para toda $a \in G$. Por lo tanto $\tau_a \in S_G$, donde $\tau_a$ reordena los elementos en $G$ definimos $\varphi : G \to S_G$ como $a \mapsto \tau_a$. Rescribiendo $\varphi(ab) = \tau_{ab} = \tau_a\tau_b = \varphi(a)\varphi(b)$. Por lo tanto $\varphi$ es homomorfismo de grupos.

Además si $\varphi(a) = \varphi(b)$, entonces $\tau_a = \tau_b$, luego $\tau_a(x) = \tau_b(x)$ para todo $x \in G$, en particular $x = 1$ implica $a = b$. Por lo tanto $\varphi$ es inyectiva por el primer teorema de isomorfismos, tenemos que $G \simeq \frac{G}{ker\varphi} \leq im\varphi \leq S_G$. ■

**Teorema 1.7.2**
Sea $G$ un grupo y $H \leq G$, $[G : H] = n$, entonces existe un homomorfismo $\varphi : G \to S_n$ con $ker\varphi \leq H$.

***Demostración.*** Sea $G/H$ la familia de clases laterales izquierdas. Definimos para cada $a \in G$:

$$\tau_a : G/H \to G/H \text{ y } gH \mapsto agH \text{ para todo } g \in G.$$

se puede ver que $\tau_a\tau_b = \tau_{ab}$, entonces $\tau_a$ es biyectiva con inverso $\tau_{a^{-1}}$. Además $\tau_a$ es un reordenamiento de $G/H$. Por lo tanto $\tau_a \in S_{G/H}$.

Ahora, definimos $\varphi : G \to S_{G/H}$, como $a \mapsto \tau_a$. Análogamente $\varphi$ es homomorfismo de grupos. Ahora si $a \in ker\varphi$, entonces $\tau_a = Id_{G/H}$, por lo que $\tau_a(gH) = gH$ para todo $g \in G$ en particular si $g = e$ entonces $aH = H$ si y sólo si $a \in H$. Por lo tanto $ker\varphi \leq H$ y $S_{G/H} \simeq S_n$. ■

**Observación 26**
Vea que si $H = e$ obtendremos el teorema de Cayley.

Recordemos que todo grupo de orden primo es isomorfo a $\mathbb{Z}_p$ por lo que para estudiar a los grupos de orden menores a 7 sólo hace falta estudiar a los de orden 4 y 6. Ya que hasta isomorfismos sólo hay 4 grupos, uno de orden 2, otro de orden 3, 5 y 7.

**Proposición 1.7.1**
Todo grupo de orden 4 es isomorfo a $\mathbb{Z}_4$ o al grupo $V$. Por otra parte $\mathbb{Z}_4 \not\simeq V$.

***Demostración.*** Sabemos por el teorema de Lagrange que todo elemento distinto de la unidad en $G$ es de orden 2 o 4.

Si hay un elemento de orden 4, entonces $G$ es cíclico isomorfo a $\mathbb{Z}_4$. Por otra parte si $x^2 = 1$ para todo $x \in G$.

Si $g_1, g_2 \neq 1$ dos elementos distintos entre si, entonces $g_1 g_2 \notin G = \{1, g_1, g_2\}$ por lo tanto $G = \{1, g_1, g_2, g_1 g_2\}$. Ahora tenemos la biyección:

$$f : G \to V$$

definida como $f(1) = 1$, $f(g_1) = (1\ 2)(3\ 4)$, $f(g_2) = (1\ 3)(2\ 4)$ y $f(g_1 g_2) = (1\ 4)(2\ 3) = [(1\ 2)(3\ 4)][(1\ 3)(2\ 4)]$ ■

**Proposición 1.7.2**
Si $G$ es un grupo de orden 6, entonces $G \simeq (\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3)$ o $G \simeq S_3$.

***Demostración.*** Por el teorema de Lagrange si $1 \neq x \in G$, entonces $x$ tiene orden 2 o 3 o 6.

$G \simeq \mathbb{Z}_6$ si $G$ contiene un elemento de orden 6. Afirmamos que $G = \{1, g_1, \ldots, g_s\}$, existe un elemento en $G$ de orden 2. Supongamos que no, entonces $g_1$ tiene inverso distinto de $g_1$ (sin pérdida de generalidad digamos que su inverso es $g_2$), luego $g_3$ tiene inverso distinto de $g_3$, $g_1$, $g_2$ digamos $g_4$ (sin pérdida de generalidad), pero, $g_5$ queda solo y su inverso está en $G$ y además es distinto de la unidad, por lo cual $g_5$ es de orden 2. Por lo tanto $G$ contiene un elemento de orden 2, digamos $t$. Veamos los otros dos casos.

Caso 1. $G$ es abeliano. Supongamos que existe otro elemento $a$ de orden 2, entonces $at = ta$, por lo cual $H = \{1, t, a, ta\} \leq G$, pero esto es una contradicción al teorema de Lagrange, pues $4 \nmid 6$. Por lo tanto existe un elemento de orden 3, digamos $b$ y puesto que 2 y 3 son primos relativos, entonces $(t\ b)$ tiene orden 6. Por lo tanto $G \simeq \mathbb{Z}_6$.

Caso 2. $G$ no es abeliano. Si $G$ no tiene elementos de orden 3, entonces $x^2 = 1$. Para todo $x \in G$, por lo cual $G$ es abeliano ya que $yx[(xy)(xy) = 1]$, por lo tanto $xy = yx$.

De lo anterior, existe un elemento de orden 3; digamos "s". Por lo tanto

$$|\langle s \rangle| = 3, \text{ entonces } |G/\langle s \rangle| = 2, \text{ por lo cual } \langle s \rangle \trianglelefteq G \text{ es normal.}$$

por lo tanto $tst \in \langle s \rangle$, entonces $tst = s^i$ con $i = 0,\ 1,\ 2$.

Ahora si $i = 0$, entonces $tst = 1$, luego $st = t$ por lo cual $s = 1$, pero, esto es una contradicción.

Por lo cual, si $i = 1$, entonces $tst = s$, lo cual implica $st = ts$ y $st \in G$ es de orden 6, por lo tanto $G$ es cíclico. Por lo tanto $G$ es abeliano, pero también es una contradicción.

Concluimos que $tst = s^2 = s^{-1}$, es decir, $t,\ s$ no conmutan. Veamos que $G \simeq S_3$. Sea $H = \langle t \rangle$, con $t^2 = 1$. Entonces

$$\varphi : G \to S_{G/H}$$

tal que $\varphi(a) = agH$ por el teorema anterior $ker\varphi \leq H$, por lo cual $ker\varphi = \{1\}$. (Por lo tanto $\varphi$ es inyectiva) o $ker\varphi = H$.

Ahora $G/H = \{H, sH, s^2H\}$, con $H = \{1, t\}$ y

$$\varphi = \begin{pmatrix} H & sH & s^2H \\ tH & tsH & ts^2H \end{pmatrix} \text{ si } \varphi(t) \text{ es la identidad.}$$

entonces $sH = tsH$, lo cual implica $s^{-1}ts \in H$, por lo cual $s^{-1}ts = 1$, luego $t = 1$, pero esto es una contradicción; o $s^{-1}ts = t$, entonces $ts = st$, también es una contradicción, además no conmutan.

Por lo tanto $t \notin ker\varphi = \{1\}$. Por lo tanto $\varphi$ es inyectiva. Finalmente tenemos $G$ y $S_3$ de orden 6, tal que $G \simeq S_3$. Observe que $\mathbb{Z}_6 \not\simeq S_3$. ■

**Definición 1.7.1**
Sea $X$ un conjunto y $G$ un grupo. $G$ actúa en $X$ si hay una función.

$$G \times X \to X \text{ definida como } (g, x) \mapsto g \bullet x$$

tal que

i) $e \bullet x = x$ para todo $x \in X$.

ii) $(gh) \bullet x = g \bullet (h \bullet x)$ para todo $g, h \in G$ y para todo $x \in X$.
diremos que $X$ es un $G$-conjunto y $\bullet$ es una acción de $G$ en $X$.

**Observación 27**
Para cada $g \in G$ tenemos la biyección (permutación) $(\alpha_g \bullet \alpha_n) = \alpha_{gn}$ con $\alpha_g : X \to X$ con $\alpha_g : x \to gx$ con inverso $\alpha_{g^{-1}} : X \to X$ con $x \to g^{-1}x$.

Observe que $\alpha : G \to S_X$ definida como $\alpha : g \to \alpha_g$ es un homomorfismo de grupos.

**Ejemplo 40**
i) (Teorema de Cayley) Vimos que $G$ actúa en $G$ con la acción $g \bullet h = gh$.

ii) $G$ actúa en $G/H$ (el conjunto de las clases laterales) con la acción $g \bullet (aH) = (ga)H$.

iii) $G$ actúa en $G$ por conjugación, con la acción $g \bullet a = gag^{-1}$.

a) $e \bullet a = eae = a$. Para todo $a \in G$.

b) $gh \bullet a = gha(gh)^{-1} = g(hah^{-1})g^{-1} = g \bullet (hah^{-1}) = g \bullet (h \bullet a)$.

**Definición 1.7.2**
Sea $X$ un $G$-conjunto y $x \in X$. El conjunto $\mathcal{O}_G(x) = \{g \bullet x : g \in G\} = G \bullet x \subseteq X$ la llamaremos la órbita de $x$ en $G$. Al subgrupo $stab_G(x) = \{g \in G : g \bullet x = x\} \leq G$ lo llamaremos el estabilizador de $x$.

**Observación 28**
El estabilizador de $x$ es un subgrupo de $G$.

i) $e \bullet x = x$, entonces $e \in stab_G(x)$.

ii) $g \in stab_G(x)$, entonces $g \bullet x = x$, por lo cual tenemos por otro lado

$$g^{-1} \bullet (g \bullet x) = g^{-1} \bullet x = (gg^{-1}) \bullet x = e \bullet x = x.$$

por lo tanto $g^{-1} \in stab_G(x)$.

iii) Si $g_1, g_2 \in stab_G(x)$, entonces

$$g_1 g_2 \bullet x = g_1 \bullet (g_2 \bullet x) = g_1 \bullet x = x$$

por lo tanto $g_1 g_2 \in stab_G(x)$.

**Observación 29**
Tenemos una relación de equivalencia en $X$ con $x \sim y$ si $y = g \bullet x$ para $g \in G$.

***Demostración.*** i) Si $x \in X$, entonces $e \bullet x = x$, es decir, $x \sim x$.

ii) Si $x \sim y$, entonces existe $g \in G$ tal que $y = g \bullet x$, por lo que

$$g^{-1} \bullet y = g^{-1} \bullet (g \bullet x) = (g^{-1}g) \bullet x = e \bullet x = x$$

Por lo tanto $y \sim x$.

iii) Si $x \sim y$ y $y \sim z$, entonces existe $g_1, g_2 \in G$ tal que $y = g_1 \bullet x$ y $z = g_2 \bullet y$. Por lo tanto

$$z = g_2 \bullet y = g_2 \bullet (g_1 \bullet x) = (g_2 g_1) \bullet x$$

Por lo tanto $x \sim z$. ■

**Proposición 1.7.3**
Las órbitas son ajenas

***Demostración.*** Supongamos $\mathcal{O}_G(x) \cap \mathcal{O}_G(y) \neq \emptyset$, entonces existen $a, b \in G$ tal que $a \bullet x = b \bullet y$, entonces $x = a^{-1}b \bullet y$, después tenemos $g \bullet x = ga^{-1}b \bullet y \in \mathcal{O}_G(y)$, para todo $g \in G$ por lo que $\mathcal{O}_G(x) \subseteq \mathcal{O}_G(y)$ y $y = b^{-1}a \bullet x$, lo que implica , entonces $\mathcal{O}_G(y) \subseteq \mathcal{O}_G(x)$. Por lo tanto $\mathcal{O}_G(x) = \mathcal{O}_G(y)$, $g \bullet y = gb^{-1}a \bullet x \in \mathcal{O}_G(x)$ para todo $g \in G$ ■

**Corolario 1.7.1**
Sea $X = \bigcup_{x \in X} \mathcal{O}_G(x)$ la unión ajena de las órbitas, donde $\mathcal{O}_G(x) = [x]$ clase de equivalencia. Si $X$ es finito, entonces $|X| = \sum_{i=1}^{N} |\mathcal{O}_G(x_i)|$.

**Definición 1.7.3**
Sean $X, Y$ $G$-conjuntos definimos $f : X \to Y$ una función es homomorfismo de $G$-conjuntos si $f(g \bullet x) = g \bullet f(x)$, para todo $g \in G$ y $x \in X$ y diremos que $X \simeq_G Y$ como $G$-conjuntos si $f$ es biyectiva.

**Proposición 1.7.4**
Sea $X$ un $G$-conjunto y $x \in X$, entonces $\mathcal{O}_G(x) \simeq G/stab_G(x)$.

***Demostración.*** Tenemos que $\mathcal{O}_G(x) \subseteq X$ y la acción de $G$ en $\mathcal{O}_G(x)$ es la misma que $X$. Luego, $g \bullet a(stab_G(x)) = ga(stab_G(x))$ es la acción de $G$ en $G/H$, $H \leq G$, con $H = stab_G(x)$.

Vamos a definir $f : \mathcal{O}_G(x) \to G/stab_G(x)$, como $f : g \bullet x \to gH$. Veamos que $f$ está bien definida. Si $g_1 \bullet x = g_2 \bullet x$, entonces $g_1^{-1}g_2 \bullet x = x$, por lo que $g_1^{-1}g_2H = H$. Entonces $g_1^{-1}g_2 \in H$, lo que implica que $g_1H = g_2H$.

Ahora vamos a ver que $f$ es homomorfismo de $G$-conjuntos $f(a \bullet (g \bullet x)) = f(ag \bullet x) = agH = a \bullet (gH) = a \bullet f(g \bullet x)$ Es claro que es sobreyectiva. Finalmente veamos que es inyectiva. Si $g_1H = g_2H$, entonces $g_1^{-1}g_2 \in H$, por lo cual $g_1^{-1}g_2 \bullet x = x$, por lo tanto $g_1 \bullet x = g_2 \bullet x$. ■

**Corolario 1.7.2**
Sean $X$ un $G$-conjunto y $x \in X$. Entonces $|\mathcal{O}_G(x)| = [G : stab_G(x)]$.

**Observación 30**
Si $G$ es un grupo, entonces $G$ actúa en $G$ por conjugación, es decir, $g \bullet a = gag^{-1}$. Observe que, $\mathcal{O}_G(x)$ es la clase de conjugación de $x$, es decir, $\mathcal{O}_w = \{y \in G : y = axa^{-1}$ para algún $a \in G\}$.

**Definición 1.7.4**
Definamos al conjunto $\mathcal{C}_G(x) = \{g \in G : x = gxg^{-1}\}$, como el centralizador de $x$ en $G$. El centralizador está formado de todos los elementos que conmutan con $x \in G$, es decir, $gx = xg$. El centralizador es un subgrupo de $G$, es decir, $\mathcal{C}_G(x) \leq G$.

**Definición 1.7.5**
Sea $H \leq G$, el conjunto $N_G(H) = \{g \in G : gHg^{-1} = H\}$ es un subgrupo de $G$ $N_G(H) \leq G$. Lo llamaremos normalizador $H$ en $G$. $H \trianglelefteq N_G(H)$.

**Teorema 1.7.3 (Teorema de Cauchy)**
Si $G$ es un grupo finito de orden divisible por $p$ primo, entonces existe $a \in G$ de orden $p$.

***Demostración.*** Sea $|G| = pm$ con $p \nmid m$, haremos inducción sobre $m$. Sea $m = 1$ y $e \neq a \in G$, entonces $\langle a \rangle = G$, es decir, el orden de $a$ es $p$.

Ahora, recordemos que $G$ actúa en $G$ por conjugación. Sea $x \in G$, entonces $\mathcal{O}_G(x) = \{gxg^{-1} : g \in G\}$, $stab_G(x) = \mathcal{C}_G(x)$, el número de conjugados de $x$ es $|\mathcal{O}_G(x)| = [G : \mathcal{C}_G(x)]$.

Si $x \notin Z(G)$, implica que existe $g \in G$ tal que $gx \neq xg$, por lo cual $gxg^{-1} \neq x$. Por lo tanto hay al menos dos elementos en $|\mathcal{O}_G(x)|$ pues $x = exe \neq gxg^{-1} \in \mathcal{O}_G(x)$.

Por lo tanto $|\mathcal{C}_G(x)| < |G|$, entonces si $p \big| |\mathcal{C}_G(x)|$, por hipótesis inductiva existe un elemento de orden $p$, $x \in \mathcal{C}_G(x) \leq G$.

Ahora si $p \nmid |\mathcal{C}_G(x)|$ para todo $x \notin Z(G)$. Tenemos que $|G| = [G : \mathcal{C}_G(x)]|\mathcal{C}_G(x)|$, entonces $p \big| [G : \mathcal{C}_G(x)]$. Además $G = \bigcup_{i \in I} \mathcal{O}_G(x_i)$, unión disjunta. Observe que si $y \in Z(G)$, entonces $\mathcal{O}_G(y) = \{y\}$, lo que implica $|\mathcal{O}_G(y)| = 1$.

Por lo tanto

$$|G| = |Z(G)| + \sum [G : \mathcal{C}_G(x_i)]$$

entonces $p \big| |Z(G)|$ observe que $Z(G)$ es un grupo abeliano finito $p \big| |Z(G)|$ (para cada divisor $d$ del grupo, existe $H$ subgrupo tal que $|H| = d$), entonces existe $H \leq Z(G)$ de orden $p$. Por lo tanto $a \in H \leq Z(G) \trianglelefteq G$ tiene orden $p$. ■

**Definición 1.7.6**
La ecuación de clase de un grupo finito $G$ es

$$|G| = |Z(G)| + \sum_i [G : \mathcal{C}_G(x_i)]$$

donde $x_i \notin Z(G)$. (Su órbita tiene más de un elemento).

**Definición 1.7.7**
Sea $p \in \mathbb{Z}$ un entero primo $G$ es un $p$-grupo si $|G| = p^n$, para $n \geq 0$.

**Teorema 1.7.4**
Si $p$ es primo y $G$ es $p$-grupo, entonces $Z(G) \neq \{1\}$.

***Demostración.*** De la ecuación de clase

$$|G| = |Z(G)| + \sum_i [G : \mathcal{C}_G(x_i)]$$

tenemos que para $x_i \notin Z(G)$, $\mathcal{C}_G(x_i) \leq G$ es no trivial, entonces $p\big|[G : \mathcal{C}_G(x_i)]$ y $p\big||G|$, entonces $p\big||Z(G)|$. Por lo tanto $Z(G) \neq 1$. ■

**Corolario 1.7.3**
Si $p$ es primo, entonces todo grupo $G$ de orden $p^2$ es abeliano.

***Demostración.*** $G$ es abeliano, si $Z(G) = G$. Supongamos que $G$ no es abeliano, entonces $Z(G) < G$.

$$|Z(G)| = \begin{cases} 1 \text{ no puede ser pues } G \text{ es un } p\text{-grupo y } Z(G) \neq \{1\} \\ p \end{cases}$$

Por lo tanto, si $G$ es no abeliano, entonces $|Z(G)| = p$, además $Z(G) \trianglelefteq G$ , por lo cual $G/Z(G) = \langle aZ(G) \rangle$ donde $a \notin Z(G)$.

Sea $g \in G$, si $g \in Z(G)$, entonces $ag = ga$. Ahora si $g \notin Z(G)$, esto implica que $gZ(G) \neq Z(G)$. Por lo tanto $gZ(G) = a^i Z(G)$ con $i = 1, \ldots, p-1$, entonces $g = a^i z$, con $z \in Z(G)$, implica $ga = a^i za = (a^i)az = a(a^i)z = ag$. Por lo tanto $a \in Z(G)$, pero esto es una contradicción. Por lo tanto $Z(G) = G$ y es abeliano. ■

**Definición 1.7.8**
Un $G$-conjunto es transitivo si tiene una sola órbita.

**Ejemplo 41**
1. $G$ actúa en $G$ con acción $g \bullet a = ga$. Se tiene que $\mathcal{O}_G(a) = G$ y $stab_G(a) = \{1\}$.

2. G actúa en $G/H$ con acción $g \bullet aH = gaH$. Entonces $\mathcal{O}_G(aH) = G/H$ y $stab_G(aH) = aHa^{-1}$.

**Ejemplo 42**
$G$ actúa en $X$ (la familia de todos los subgrupos de $G$) por conjugación:

$$g \bullet H = gHg^{-1},\ \mathcal{O}_G(H) = \{gHg^{-1} : g \in G\},\ stab_G(H) = N_G(H)$$

**Ejemplo 43**
Sea $X = \{v_1, v_2, v_3, v_4\}$ el conjunto de los vértices de un cuadrado y $G = D_8$ actúa en $X$.

$$\text{Para todo } v_i \in X, \mathcal{O}(v_i) = X$$

Por lo tanto $X$ es transitivo. El $stab(v_i)$ es un subgrupo de orden 2.

**Proposición 1.7.5**
Sea $G$ un grupo de orden $|G| = p^n$, entonces $G$ tiene un subgrupo normal de orden $p^k$ para todo $k \leq n$.

***Demostración.*** Haremos inducción sobre $n \geq 0$. Si $e = 0$, entonces $G = \{1\}$. Ahora si, $n \geq 1$, entonces $Z(G) \leq G$ es no trivial, es decir, distinto de $\{1\}$. Observe que $Z(G)$ es un grupo finito y que $p|Z(G)$ por teorema de Cauchy, existe $a \in Z(G)$ de orden $p$, sea $Z = \langle a \rangle$.

Tenemos que $Z \leq Z(G)$, entonces $Z \trianglelefteq G$ es normal. Si $k \leq n$, entonces $k - 1 \leq n - 1$ y $p^{k-1} \leq p^{n-1} = |G/Z|$, por inducción, existe $H^* \trianglelefteq G/Z$ de orden $p^{k-1}$ por teorema de la correspondencia $H^* = H/Z$ con $H \trianglelefteq G$ de orden $p^k$. ■

**Observación 31**
Los grupos abelianos y cuaternios tienen la propiedad de que todos sus subgrupos son normales. En el otro extremo se encuentran los grupos cuyos únicos subgrupos normales son los triviales $\{1\}, G$.

**Definición 1.7.9**
Un grupo $G$ es llamado simple, si sus únicos subgrupos normales son $G$ y $\{1\}$.

**Proposición 1.7.6**
Un grupo abeliano $G$ es simple si y sólo si $G$ es finito y $G$ es de orden primo $p$.

***Demostración.*** Necesidad. Sea $G$ abeliano y simple, entonces los subgrupos de $G$ es normal. Sea $1 \neq a \in G$, entonces $\{1\} \neq \langle a \rangle \trianglelefteq G$ como $G$ es simple, entonces $G = \langle a \rangle$. Si $a$ es de orden infinito, entonces todas sus potencias son distintas. Esto implica que $\{1\} \neq \langle a^2 \rangle \lneq \langle a \rangle = G$, entonces $\langle a^2 \rangle$ es un subgrupo normal propio. Por lo tanto $a$ tiene orden finito digamos $m$.

Si $m$ no es primo, entonces $m = kl$ con $0 < k, l < m$, entonces $\{1\} \neq \langle a^k \rangle \lneq \langle a \rangle$ ($a^k$ es de orden $l$) sería un subgrupo propio normal. Por lo tanto $G$ es de orden $p$ para algún $p$-primo.

Suficiencia. Si $G$ es finito y de orden $p$ primo, sus únicos subgrupos son $\{1\}$ y $G$ (Teorema de Lagrange). ■

Denotaremos para $x \in G$, $x^G = \{gxg^{-1} : g \in G\}$. Si $x$ tiene $k$ conjugados, $|x^G| = k$. Si $H \leq G$ subgrupo, $x^H = \{hxh^{-1} : h \in H\} \subseteq x^G$. Por lo tanto $|x^H| \leq |x^G|$ los cuales son el número de conjugados de $x$ en $H$ y $G$ respectivamente.

**Observación 32**
Se puede dar la desigualdad estrica, por ejemplo:

$$H = \langle (1\ 2) \rangle < S_3, (1\ 2)^H = \{(1\ 2)\} \text{ y } (1\ 2)^{S_3} = \{(1\ 2), (1\ 3), (2\ 3)\}$$

todas las transposiciones son conjugados. Por lo tanto $1=|(1\ 2)^H|<|(1\ 2)^{S_3}|=3$. Recordemos que 2 permutaciones con la misma estructura cíclica son conjugados.

**Lema 1.7.1**
Todos los 3-ciclos son conjugados en $A_5$.

***Demostración.*** Sea $G = S_5$, $\alpha = (1\ 2\ 3)$ y $H = A_5$ sabemos que $|\alpha^G| = 20$ pues hay veinte 3-ciclos distintos (los cuales son conjugados en $S_5$). Recordemos que el número de conjugados de $\alpha$ es $|\alpha^G| = [S_5 : C_{S_5}(\alpha)]$ (donde $C_{S_5}(\alpha)$ son los elementos que conmutan con $\alpha$), entonces

$$|S_5|/|C_{S_5}(\alpha)| = 20 \text{ y } |S_5| = 120, \text{ entonces } |C_{S_5}(\alpha)| = 6$$

Por lo tanto hay exactamente 6 permutaciones que conmutan con $\alpha$ dichas permutaciones son

$$\{(1), (1\ 2\ 3), (1\ 3\ 2), (4\ 5), (4\ 5)(1\ 2\ 3), (4\ 5)(1\ 3\ 2)\} = C_{S_5}(\alpha)$$

Por lo cual concluimos $C_{A_5}(\alpha) = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, entonces $|C_{A_5}(\alpha)| = 3$, obtenemos que

$$|\alpha^{A_5}| = [A_5 : C_{A_5}(\alpha)] = \frac{|A_5|}{|C_{A_5}(\alpha)|} = \frac{60}{3} = 20$$

esto es, todos los 3-ciclos son conjugados en $A_5$. Es decir, $(i_1\ i_2\ i_3), (j_1\ j_2\ j_3) \in S_5$, entonces existe $\gamma \in A_5$ tal que

$$\gamma(i_1\ i_2\ i_3)\gamma^{-1} = j_1\ j_2\ j_3$$

. ■

**Lema 1.7.2**
Si $n \geq 3$, todo elemento en $A_n$ es un 3-ciclo o producto de 3-ciclos.

***Demostración.*** Sea $\alpha \in A_n$ para $n \geq 3$. $\alpha = \tau_1\tau_2 \cdots \tau_{2q-1}\tau_{2q}$ es producto de un número par de transposiciones además podemos asumir que los $\tau_i$ adyacentes son distintos y los podemos agrupar de 2 en 2. Digamos

$$\tau\tau' = \begin{cases} (i\ j)(j\ k) = (i\ j\ k) \text{ no ajenas} \\ (i\ j)(k\ l) = (i\ k\ j)(k\ l\ i) \end{cases}$$

■

**Lema 1.7.3**
Todos los 3-ciclos son conjugados $A_n$ para $n \geq 5$.

***Demostración.*** Sean $(1\ 2\ 3), (i\ j\ k) \in S_n$.

Caso 1. Tenemos $(1\ 2\ 3)(i\ j\ k)$ no ajenos. Sin pérdida de generalidad, $i = 1$, entonces $(1\ 2\ 3), (i\ j\ k) \in S_{\{1,2,3,j,k\}} \simeq S_5$ y por el lema anterior $(1\ 2\ 3)$ y $(i\ j\ k)$ son conjugados en $A_5$, es decir, existe $(1\ 2\ 3) = \alpha(i\ j\ k)\alpha^{-1}$ y $\alpha \in A_5 \subseteq A_n$, con $n \geq 5$.

Caso 2. $(1\ 2\ 3), (i\ j\ k)$ son ajenos. Note que $(1\ 2\ 3)$ es conjugado de $(3\ j\ k)$ y que $(3\ j\ k)$ es conjugado de $(i\ j\ k)$, por el párrafo anterior. Por lo tanto $(1\ 2\ 3)$ es conjugado de $(i\ j\ k)$. ■

**Lema 1.7.4**
Si $H \trianglelefteq A_n$ con $n \geq 5$ y $H$ contiene un 3 ciclo, entonces $H = A_n$.

***Demostración.*** Por el Lema 1.7.3 tenemos que $H$ contiene a todos los 3-ciclos, pues $H$ es cerrado bajo conjugación, por ser normal. Además todo elemento en $A_n$ es producto de 3-ciclos y $H$ cerrado bajo producto, entonces $H \supseteq A_n$. Por lo tanto $H = A_n$. ■

**Teorema 1.7.5**
$A_5$ es simple.

***Demostración.*** Sea $\{1\} \neq H \trianglelefteq A_5$ un subgrupo normal, por demostrar que $H = A_5$. Por el Lema 1.7.4, es suficiente con probar que $H$ contiene un 3-ciclo.

| Existe $(1) \neq \sigma \in H$ | Estructura de $S_5$ | Estructura de $\sigma \in A_5$ |
|---|---|---|
| | (1) | |
| | (1 2) | (1 2 3) |
| | (1 2 3) | (1 2 3 4 5) |
| | (1 2 3 4) | (1 2)(3 4) |
| | (1 2 3 4 5) | |
| | (1 2)(3 4) | |
| | (1 2)(3 4 5) | |

Si $\sigma = (1\ 2)(3\ 4)$ sea $\tau = (1\ 2)(3\ 5)$, $(\tau\sigma\tau^{-1})\sigma^{-1} \in H$ por ser normal, es decir,

$$(1\ 2)(3\ 5)(1\ 2)(3\ 4)(3\ 5)(1\ 2)(3\ 4)(1\ 2) = (3\ 5)(3\ 4)(3\ 5)(3\ 4) = (3\ 5\ 4)$$

Si $\sigma = (1\ 2\ 3\ 4\ 5)$ y $\rho = (1\ 3\ 2)$, entonces $\rho\sigma\rho^{-1}\sigma^{-1} = (1\ 3\ 4) \in H$. ■

**Lema 1.7.5**
$A_6$ es simple.

***Demostración.*** Sea $H \neq \{1\}$ un subgrupo normal de $A_6$, por demostrar que $H = A_6$. Asumimos que existe $(1) \neq \alpha \in H$ tal que $\alpha$ fija algún $i \in \{1, 2, \ldots, 6\}$, definimos $F = \{\sigma \in A_6 : \sigma(i) = i\} \simeq A_5$ simple. Observe que $\{1\} \neq \alpha \in H \cap F$ por el segundo teorema de isomorfismos $H \cap F \trianglelefteq F$. Pero $F$ simple, entonces

$H \cap F = F \subseteq H$. Además $F$ contiene un 3-ciclo (en 5 letras), por lo cual $H$ contiene un 3-ciclo, por lo tanto $H = A_6$.

Estructura de $S_6$
(1) par
(1 2)
(1 2 3) par
(1 2 3 4)
(1 2 3 4 5)par
(1 2 3 4 5 6)
(1 2)(3 4) par
(1 2)(3 4)(5 6)
(1 2)(3 4 5)
(1 2)(3 4 5 6) par
(1 2 3)(4 5 6) par

Supongamos que no existe $\alpha \in H$ con $\alpha \neq 1$ que fija algún $i \in \{1, \ldots, 6\}$, entonces $\alpha$ es de la forma.

(1 2)(3 4 5 6) ó
(1 2 3)(4 5 6)

En el primer caso $\alpha^2 \in H$, $\alpha^2 \neq 1$ y fija $\{1, 2\}$, pero, esto es una contradicción.

En el segundo caso $H$ contiene a $\alpha(\beta\alpha^{-1}\beta^{-1})$ el cual fija a 1 con $\beta = (2\ 3\ 4)$, pero, esto también es una contradicción. ■

**Teorema 1.7.6**
$A_n$ es simple, para todo $n \geq 5$.

***Demostración.*** Sea $\{1\} \neq H \trianglelefteq A_n$. Vamos a demostrar que $H = A_n$, así que basta demostrar $H$ contiene un 3-ciclo.

Sea $\beta \in H$ y $\beta \neq (1)$, entonces existe un $i \in \{1, \ldots, n\}$ tal que $\beta$ mueve a $i$, digamos $\beta(i) = j \neq i$.

Sea $\alpha$ un 3-ciclo que fija a $i$ y mueve a $j$. Observe que $\alpha, \beta$ no conmutan, pues $\alpha\beta(i) = \alpha(j) \neq i$ y $\beta\alpha(i) = \alpha(j) = j$.

Entonces $\alpha\beta \neq \beta\alpha$, luego $(1) \neq (\alpha\beta\alpha^{-1})\beta^{-1} \in H$. Como $\alpha^{-1}$ es un 3-ciclo, entonces $\beta\alpha^{-1}\beta^{-1}$ es 3-ciclo (pues conjugación preserva estructura), entonces $\gamma = [\alpha][(\beta\alpha^{-1})\beta^{-1}]$ es producto de dos 3-ciclos. Por lo tanto $\gamma$ mueve a lo más seis elementos digamos $\{i_1, \ldots, i_6\}$.

Definamos $F = \{\sigma \in A_n : \sigma \text{ fija a todo } i \neq i_1, \ldots, i_6\}$ entonces los elementos de $F$ son producto de un número par de transposiciones que mueven seis

simbolos. Por lo tanto $F \simeq A_6$ simple y $(1) \neq \gamma \in H \cap F \trianglelefteq F$ simple, entonces $H \cap F = F \trianglelefteq H$ y contiene los 3-ciclos en seis símbolos. ■

**Lema 1.7.6 (Burnside)**
Sea $G$ un grupo que actúa en un conjunto finito $X$, con $X = \cup_{i=1}^{N} \mathcal{O}_G(x_i)$ unión disjunta. Entonces

$$N = \frac{1}{|G|} \sum_{g \in G} Fix(g)$$

donde $Fix(g) = \{x \in X : g \bullet x = x\}$

***Demostración.*** Consideramos el conjunto $\mathcal{A} = \{(g, x) \in G \times X : g \bullet x = x\}$ sea $g \in G$, definimos

$$\mathcal{A}_g = \{(g, x) \in G \times X : g \bullet x = x\} = \{(g, x) \in G \times X : x \in Fix(g)\}$$

entonces $|\mathcal{A}_g| = |Fix(g)|$.

Observe que $\mathcal{A} = \cup_{g \in G} \mathcal{A}_g$ unión disjunta, por lo cual $|\mathcal{A}| = \sum_{g \in G} |Fix(g)|$.

Por otro lado sea $x \in X$, definimos

$$\mathcal{A}_x = \{(g, x) \in G \times X : g \bullet x = x\} = \{(g, x) \in G \times X : g \in stab_G(x)\}$$

observe que $\mathcal{A} = \underset{x \in X}{\cup} \mathcal{A}_x$, entonces $|\mathcal{A}| = \sum_{x \in X} |stab_G(x)|$.

Por lo tanto

$$\begin{aligned}
\sum_{g \in G} |Fix(g)| = |\mathcal{A}| = \sum_{x \in X} |stab_G(x)| &= \sum_{i=1}^{N} \sum_{x \in \mathcal{O}_G(x_i)} |stab_G(x)| \\
&= \sum_{i=1}^{N} \sum_{x \in \mathcal{O}_G(x_i)} \frac{|G|}{|\mathcal{O}_G(x_i)|} \\
&= |G| \sum_{i=1}^{N} \frac{|\mathcal{O}_G(x_i)|}{|\mathcal{O}_G(x_i)|} \\
&= |G| N
\end{aligned}$$

■

**Observación 33**
Ahora si $x \in \mathcal{O}_G(x_i)$, entonces $\mathcal{O}_G(x) = \mathcal{O}_G(x_i)$ además $\mathcal{O}_G(x) \simeq G/stab_G(x_i)$. Por lo tanto $|stab_G(x)| = \frac{|G|}{|\mathcal{O}_G(x_i)|}$

## 1.8. Teoremas de Sylow

**Definición 1.8.1**
Sea $p$ un número primo. Un $p$-subgrupo de Sylow de un grupo finito $G$ es un $p$-subgrupo máximo $P$. Es decir, si $Q$ es un $p$-subgrupo de $G$ y $P \leq Q$, entonces $P = Q$.

**Proposición 1.8.1**
Si $S$ es un $p$-subgrupo de $G$ (posiblemente $S = \{e\}$), entonces existe un $p$-subgrupo de Sylow $P$ tal que $S \leq P$.

***Demostración.*** Si no existe un $p$-subgrupo de Sylow que contiene propiamente a $S$, entonces $S$ es un $p$-subgrupo de Sylow.

En otro caso, si existe un $p$-subgrupo $p'$ que contiene propiamente a $S$. Entonces tenemos dos casos $P'$ es maximal o $P'$ no es maximal. Si $P'$ es maximal, entonces es de Sylow.

Si $P'$ no es máximo, entonces existe $P''$ $p$-subgrupo tal que $P' < P''$, este proceso continúa y es finito, el subgrupo $P^*$ de orden mayor es un $p$-subgrupo de Sylow. ■

Recordemos que para un subgrupo $H \leq G$, se tiene que
$aHa^{-1} = \{aha^{-1} : h \in H \text{ con } a \in G\}$
$N_G(H) = \{g \in G : ghg^{-1} = H\}$
el número de conjugados de $H$ es $[G : N_G(H)]$ y $H \trianglelefteq N_G(H)$, entonces $N_G(H)/H$ es grupo.

**Lema 1.8.1**
Sea $P$ un $p$-subgrupo de Sylow de un grupo finito $G$. Entonces

i) Para todo $a \in G$, $aPa^{-1}$ es un $p$-subgrupo de Sylow de G.

ii) $|N_G(P)/P|$, es primo relativo a $p$.

iii) Si $a \in G$ tiene orden una potencia de $p$ y si $aPa^{-1} = P$, entonces $a \in P$.

***Demostración.*** i) Las conjugaciones son biyecciones $|aPa^{-1}| = |P|$, entonces $aPa^{-1}$ es

un $p$-grupo. Supongamos que $aPa^{-1}$ no es maximal, lo que implica que existe $Q$ un $p$-subgrupo tal que $aPa^{-1} < Q$, entonces $P < a^{-1}Qa$, pero es una contradicción pues $a^{-1}Qa$ es un $p$-subgrupo.

ii) Si $p \big| |N_G(P)/P|$, por el Teorema de Cauchy tenemos que $N_G(P)/P$ tiene un elemento de orden $p$, digamos $aP$, entonces $S = \langle aP \rangle$ es subgrupo de $N_G(P)/P$ de orden $P$, por el teorema de la correspondencia existe $P < S < N_G(P)$ tal

que $\langle aP\rangle = S$. Notar que $\left|\frac{S}{P}\right| = \frac{|S|}{|P|} = p$, entonces $|S| = P|P|$, es decir, $S$ es un $p$-subgrupo de $G$, lo que es una contradicción con el hecho de $P$ de ser máximo.

iii) Si $aPa^{-1} = P$, entonces $a \in N_G(P)$. Si $a \notin P$, entonces $aP \neq P$ en $N_G(P)/P$. Como $a$ de orden una potencia de $p$, entonces $aP$ tiene orden una potencia de $p$ en $N_G(P)/P$, esto implica que $p\big||N_G(P)/P|$, lo que es una contradicción. ■

**Teorema 1.8.1 (Sylow)**
Sea $G$ un grupo finito de orden $p_1^{e_1}\dots p_t^{e_t}$ y sea $P$ un $p$-subgrupo de Sylow de $G$ para algún primo $p = p_j$.

i) Todo $p$-subgrupo de Sylow es conjugado a $P$.

ii) Si hay $r_j$ $p_j$-subgrupos de Sylow, entonces $r_j\big||G|/p_j^{e_j}$ y $r_j \equiv\ 1\ mod\ p_j$.

***Demostración.*** i) Sea $X = \{P_1, \dots, P_r\}$ el conjunto de conjugados de $P$ donde $P = P_1$. Si $Q$ es cualquier $p$-subgrupo de Sylow de $G$ entonces $Q$ actúa en $X$ por conjugación. Sea $P_i \in X$ y sea $q \in Q$, lo cual implica $P_i = g_iPg_i^{-1}$ y $q \bullet (g_iPg_i^{-1}) = qg_iPg_i^{-1}q^{-1} \in X$ recordemos $\mathcal{O}_G(P_i) \simeq Q/stab_Q(P_i)$, entonces $|\mathcal{O}_G(P_i)|\big||Q|$. Por lo tanto $|\mathcal{O}_G(P_i)|$ es una potencia de $p$.

Si existe una órbita de tamaño 1, entonces existe $P_i$ tal que $qP_iq^{-1} = P_i$ para todo $q \in Q$ por la parte iii) del lema anterior, entonces $q \in P_i$ para todo $q \in Q$, por lo cual $Q \leq P_i$ implica $Q = P_i$, con $Q = P_i$ el único elemento en $X$ cuya órbita sólo tiene un elemento. Pues si $P_j$ con $j \neq i$ tiene órbita de tamaño 1, similarmente tendríamos $Q = P_j$ pero esto es una contradicción, pues $Q = P_i = P_j$ con $i \neq j$. Por lo tanto, cada $P_j$ con $j \neq i$ tiene órbita de tamaño una potencia de $p$ estrictamente positiva. Si $X = \dot{\cup}_{l=1}^{r}\mathcal{O}(P_l)$, entonces

$$r = |X| = 1 + \sum_{j\neq i} |\mathcal{O}(p_j)|$$

observe que $Q = P$ satisface lo anterior. Por lo tanto $r \equiv\ 1 mod\ (p)$.

Suponga ahora que existe un $Q$ un $p$ subgrupo de Sylow de $G$ que no es conjugado a $P$, entonces $Q \neq P_i$ para todo $i$.

$$Q \text{ actúa en } X \text{ por conjugación.}$$

En este caso tenemos que no hay órbitas de tamaño 1 pues de lo contrario si $\{P_k\}$ es una órbita, entonces $Q = P_k$, lo cual es una contradicción. Por lo tanto, cada órbita tiene orden una potencia estrictamente positiva de $p$. Esto implica que $r = |X|$ es múltiplo de $p$, entonces $r \equiv 0\ mod\ p$, pero es una contradicción, pues $[r] = [1]$.

Por lo tanto, todos los $p$-subgrupos de Sylow son conjugados.

ii) Por otro lado $r_j = [G : N_G(P_j)] = |G|/|N_G(P_j)|$, entonces $r_j$ divide al orden del grupo $r_j \big| |G|$ y $r_j \equiv 1 \ mod \ p$, luego $(r_j, p_j^{e_j}) = 1$ primos relativos. Por lo tanto $r_j \big| \frac{|G|}{p_j^{e_j}}$ ■

**Corolario 1.8.1**
Un grupo finito $G$ tiene un único $p$-subgrupo de Sylow $P$ de $G$ para algún número primo $p$ si y sólo si $P \trianglelefteq G$.

***Demostración.*** Necesidad. Para cada $g \in G$, $gPg^{-1}$ es un $p$-subgrupo de Sylow pero $P$ es único, entonces $gPg^{-1} = P$ para todo $g \in G$. Por lo tanto $P \trianglelefteq G$.

Suficiencia. Si $P \trianglelefteq G$, si $Q$ es cualquier $p$-subgrupo de Sylow, entonces $Q = aPa^{-1}$
para algún $a \in G$ pero $P \trianglelefteq G$, por lo tanto $Q = P$. ■

**Teorema 1.8.2 (Sylow)**
Si $G$ es un grupo finito de orden $p^e m$, donde $p$ es un primo y $p \nmid m$, entonces todo $p$-subgrupo de Sylow $P$ de $G$ tiene orden $p^e$.

***Demostración.*** Veamos que $p \nmid [G : P]$. Tenemos

$$[G : P] = [G : N_G(P)][N_G(P) : P] = r[N_G(P) : P]$$

($r$ es el número de conjugados de $P$) recordemos que $r \equiv 1 \ mod \ p$, entonces $p \nmid r$.

Por la parte ii) del Lema 1.8.1 tenemos que $p$ y $[N_G(P) : P]$ son primos relativos, entonces $p \nmid [N_G(P) : P]$, por lo tanto $p \nmid [G : P]$.

Ahora $|P| = p^k$ para algún $k \leq e$, es decir, $[G : P] = |G|/|P| = p^e m/p^k = p^{e-k}m$, puesto que $p$ no divide a $[G : P]$, entonces $e = k$ por lo tanto $|P| = p^e$.
■

**Ejemplo 44**
Sea $G$ un grupo de orden 42, entonces $G$ no es simple. Además $|G| = 2 \times 3 \times 7$

$r_7 | \frac{|G|}{7} = 6$ por lo que $r_7 = 1,\ 2,\ 3,\ 6$ además $r_7 \equiv 1 \ mod \ 7$ obteniendo que $r_7 = 1$ concluyendo que el 7 grupo de Sylow es normal.

**Proposición 1.8.2**
Un grupo finito $G$ en el que, todos sus subgrupos de Sylow son normales, entonces $G$ es igual al producto directo de sus subgrupos de Sylow.

***Demostración.*** Sea $|G| = p_1^{e_1} \dots p_t^{e_t}$ y sea $G_{p_i}$ el $p_i$-subgrupo de Sylow de $G$. Sea $S$ el subgrupo generado por la unión de todos los subgrupos de Sylow tenemos que $G_{p_i} \leq S$, entonces $p_i^{e_i} \big| |S|$ para todo $i \in \{1, \dots, t\}$, entonces $|G| \big| |S|$.

Por lo tanto $G = S$.

Ahora sea $x \in G_{p_i} \cap \langle \cup_{j \neq i} G_{p_j} \rangle$ por lo que existe $q_i$ una potencia estrictamente positiva de $p_i$ tal que $x^{q_i} = 1$ y $x = \prod_{j \neq i} s_j$ con $s_j \in G_{p_j}$ y existen $q_j$ potencias estrictamente positiva de $p_j$ tal que $s_j^{q_j} = 1$ sea $q = \prod_{j \neq i} q_j$ y $(q_i, q) = 1$ primos relativos, es decir, existen $t, l \in \mathbb{Z}$ tal que $tq_i + lq = 1$, entonces $x = x^{q_i t} x^{ql} = 1$ ya que los $s_j$ conmutan. Por lo tanto $G$ es el producto directo de sus subgrupos de Sylow. ■

**Nota 1**
En la siguiente sección de grupos abelianos finitos, veremos el producto directo generalizado, el cual se puede aplicar en el caso no abeliano, si asumimos que los elementos de un subgrupo conmutan con los elementos de los otros subgrupos. Observemos que esto sucede en nuestra proposición: Sean $p$ y $q$ primos distintos, y $P$ el $p$-subgrupo de Sylow y $Q$ el $q$ subgrupo de Sylow. Ambos son normales, por ser únicos. Por teorema de Lagrange, tenemos que $P \cap Q = \{1\}$, y por la normalidad de $P$ y $Q$ tenemos que $(t^{-1})st(s^{-1}) = 1$, para todo $s \in P$ y $t \in Q$.

**Lema 1.8.2**
No existe $G$ grupo simple no abeliano de orden $|G| = p^e m$, donde $p$ es número primo, $p \nmid m$ y $p^e \nmid (m-1)!$.

***Demostración.*** Si $p$ es un número primo, entonces todo $p$-grupo $H$ con $|H| > p$ no es simple:

De la ecuación de clase tenemos que $Z(H) \neq \{1\}$ además sabemos que $Z(H) \trianglelefteq H$, entonces:

1. Si $Z(H)$ es subgrupo propio, entonces $H$ no es simple.

2. Si $Z(H) = H$, entonces $H$ es abeliano y H sería simple si y sólo si $|H| = p$.

Supongamos que $G$ existe. Sabemos que hay algún $P$, $p$-subgrupo de Sylow de $G$ y $|P| = p^e$, por lo que $[G : P] = m$.

Podemos asumir que $m > 1$, pues por la afirmación anterior los $p$-grupos no abelianos con $e > 1$ nunca son simples.

Sabemos por el Teorema 1.7.2 que existe

$$\varphi : G \to S_m \text{ homomorfismo de grupos}$$

tal que $ker\varphi \leq P$, puesto que $G$ es simple y $ker\varphi \trianglelefteq G$, entonces $ker\varphi = \{1\}$, $\varphi$ es inyectiva, por lo tanto $G \simeq \varphi(G) \leq S_m$ y por el teorema de Lagrange $p^e m | m!$, por lo tanto $p^e | (m-1)!$ ■

**Proposición 1.8.3**
No existen grupos simples no abelianos $G$ con $|G| < 60$.

***Demostración.*** Si $|G| = p$, G es abeliano simple.
Si $|G| = p^e$, $e > 1$ si $G$ no es abeliano, entonces no es simple, ya que el centro sería un subgrupo normal propio $\{1\} < Z(G) < G$.
Si $|G| = p^e m$, $p \nmid m$ y $p^e \nmid (m-1)!$ (por el lema anterior $G$ no puede ser simple y no abeliano).

Observe los enteros entre 2 y 59 omitiendo primos y potencias de primos, la mayoría pueden ser descartados por el lema anterior, por ejemplo para $12 = (2^2)3$ tómese $p = 2$ y $m = 3$.

Se puede ver que 30, 40, 56 son los únicos ordenes para grupos candidatos a ser no abelianos simples.

Ahora sea $|G| = 30 = 2(3)(5)$ supongamos que $G$ es simple. Sea $P$ un 5-subgrupo de Sylow de $G$, entonces $r_5$ es igual al número de conjugados de $P$. Tenemos que $r_5$ divide a 6 y $r_5 \equiv 1 \ mod\ 5$, entonces $r_5 = 1$ o 6 pero $G$ es simple, por lo cual $r_5 \neq 1$ pues de lo contrario $P \trianglelefteq G$ pero es una contradicción. Por lo tanto $r_5 = 6$.

Observe que si $P_1,\ P_2$ son 2-conjugados distintos de $P$, entonces $P_1 \cap P_2 = \{1\}$ ya que, si $P_1 \cap P_2 \neq \{1\}$ y entonces cualquier elemento distinto de la identidad, generaría tanto a $P_1$ como a $P_2$, por lo que estos serían iguales.

Por la observación anterior, los seis 5-subgrupos de Sylow solo comparten la identidad, dando origen a 4 elementos de orden 5 por cada uno, es decir, en total hay 24 elementos distintos del 1 de orden 5.

Ahora $r_3 \big| 10$ y $r_3 \equiv 1 \ mod\ 3$ y $r_3 \neq 1$, entonces $r_3 = 10$. Por lo que similarmente tenemos 20 elementos distintos de la unidad de orden 3. Como vemos $24 + 20 = 44$, lo cual excede el número total de elementos. Por lo tanto, si $|G| = 30$, entonces $G$ no es simple.

$|G| = 40 = 8(5)$. Sea $P$ un 5-subgrupo de Sylow de $G$, entonces $r_5 | 8$ y $r_5 \equiv 1 \ mod\ 5$, se tiene que $r_5 = 1$. Por lo tanto $P \trianglelefteq G$.

$|G| = 56 = 8(7)$. Supongamos $G$ simple. Sea $P$ un 7-subgrupo de Sylow de $G$.

$r_7 | 8$ y $r_7 \equiv 1 \ mod\ (7)$ y $G$-simple, entonces $r_7 \neq 1$ por lo tanto $r_7 = 8$.

Como anteriormente los 7-subgrupos de $G$ son cíclicos de orden primo 7, la intersección de cualesquiera dos es $\{1\}$ por lo que tenemos 48 elementos distintos de 1 de orden 7.

Además, si $Q$ es un 2-subgrupo de Sylow de $G$, tenemos que $|Q| = 8$ teniendo 56 elementos, pero $Q$ no es único pues de lo contrario $Q \trianglelefteq G$. Por lo tanto, existe $Q'$ otro 2-subgrupo de Sylow de $G$ y además tiene un elemento distinto de la unidad que no está en $Q$ lo cual excede al orden de $G$. ■

**Proposición 1.8.4**
Sea $G$ un grupo finito. Si $p$ es primo y $p^k \big| |G|$, entonces $G$ tiene un subgrupo de orden $p^k$.

***Demostración.*** $|G| = p^e m$ donde $p \nmid m$. Sea $P$ un $p$-subgrupo de Sylow de $G$, entonces $|P| = p^e$. Si $p^k \big| |G|$, se tiene que $p^k \big| \big| |P|$ y $P$ un $p$-grupo, se sigue la existencia de un subgrupo $H < P$ de orden $p^k$, por lo tanto $H < G$ de orden $p^k$. ■

## 1.9. Grupos abelianos libres.

**Definición 1.9.1**
Si $S \leq G$ y $T \leq G$ subgrupos de $G$ un grupo abeliano, entonces $G$ es la suma directa interna denotada por

$$G = S \oplus T$$

si $S+T = G$ (para cada $a \in G$, existe $s \in S$ y $t \in T$ con $a = s+t$) y $S \cap T = \{0\}$.

**Proposición 1.9.1**
Los siguientes enunciados son equivalentes para un grupo abeliano $G$ con $S$ y $T$ subgrupos de $G$.

i) $G = S \oplus T$.

ii) Todo $g \in G$ tiene una única expresión de la forma

$$g = s + t$$

donde $s \in S$ y $t \in T$.

iii) Existen homomorfismos $p : G \to S$ y $q : G \to T$, llamados proyecciones, $i : S \to G$ y $j : T \to G$, llamados inclusiones tales que

$$pi = 1_S,\ qj = 1_T,\ pj = 0,\ qi = 0 \text{ y } ip + jq = 1_G.$$

**Observación 34**
Las ecuaciones $pi = 1_S$ y $qj = 1_T$ implica que los mapeos $j$ e $i$ tienen que ser inyectivos, y los mapeos $p$ y $q$ sobreyectivos.

***Demostración.*** i) implica ii) Por hipótesis, $G = S + T$, entonces para cada $g \in G$, $g = s + t$ con $s \in S$ y $t \in T$. Verificaremos la unicidad, suponga

que $g = s_2 + t_2$ con $s_2 \in S$ y $t_2 \in T$, entonces $s + t = s_2 + t_2$, implica que $s - s_2 = t_2 - t \in S \cap T = \{0\}$. Por lo tanto $s = s_2$ $t = t_2$. Finalmente, la expresión $g = s + t$, con $s \in S$ y $t \in T$ es única.

ii) implica iii) Si $g \in G$, entonces $g = s + t$ con $s \in S$ y $t \in T$. Ahora definimos las funciones $p$ y $q$ por

$$p(g) = s \text{ y } q(g) = t$$

están bien definidas por ser $s$ y $t$ únicos. Es fácil verificar que se cumplen las ecuaciones mencionadas en donde $i$ y $j$ son las inclusiones de $S$ y $T$ en $G$ respectivamente.

iii) implica i) Si $g \in G$, de la ecuación $1_G = ip + jq$ obtenemos

$$g = ip(g) + jq(g) \in S + T,$$

ya que $S = imi$ y $T = imj$.

Ahora sea $g \in S$, por tanto tenemos que $g = ig$ y $pg = pig = g$. Si $g \in T$, entonces $g = jg$ de donde $pg = pjg = 0$, implica que $g = 0$, entonces $S \cap T = \{0\}$. Por lo tanto $G = S \oplus T$. ■

**Definición 1.9.2**
Sea $G$ un grupo abeliano y si $S,\ T \leq G$. Si $G = S \oplus T$, entonces $S \oplus T \cong S \times T$, la cual llamaremos suma directa externa.

$$(s_1, t_1) + (s_2, t_2) = (s_1 + s_2, t_1 + t_2).$$

**Corolario 1.9.1**
Sean $S$ y $T$ grupos abelianos, definimos $S' \cong S$ y $T' \cong T$ por

$$S' = \{(s, 0) : s \in S\} \text{ y } T' = \{(0, t) : t \in T\};$$

entonces $S \times T = S' \oplus T'$.

***Demostración.*** Definamos $f : S \oplus T \to S \times T$ como $f : a \mapsto (s, t)$ es una función bien definida y es un isomorfismo.

Ahora si $g = (s, t) \in S \times T$, entonces $g = (s, 0) + (0, t) \in S' + T'$ y $S' \cap T' = \{(0, 0)\}$, por lo tanto $S \times T = S' \oplus T'$. ■

**Observación 35**
En esencia no hay diferencia entre suma directa interna y suma directa externa finitas.

**Definición 1.9.3**
Si $S_1, S_2, \ldots, S_n, \ldots$ son subgrupos de un grupo abeliano $G$, definimos la suma directa finita $S_1 \oplus S_2 \oplus \cdots \oplus S_n$ de forma inductiva para $n \geq 2$

$$\sum_{i=1}^{n+1} S_i = S_1 \oplus S_2 \oplus \cdots \oplus S_{n+1} = [S_1 \oplus S_2 \oplus \cdots \oplus S_n] \oplus S_{n+1}$$

**Proposición 1.9.2**
Sea $G = S_1 + S_2 + \cdots + S_n$, donde $S_i$ son subgrupos, esto es, para cada $a \in G$, existe $s_i$ para todo $i$, con

$$a = s_1 + s_2 + \cdots + s_n.$$

Las siguientes condiciones son equivalentes:

i) $G = S_1 \oplus \cdots \oplus S_n$.

ii) Para todo $a \in G$ existe una única expresión de la forma $a = s_1 + s_2 + \cdots + s_n$, donde $s_i \in S_i$ para todo $i$.

iii) Para cada $i$,

$$S_i \cap (S_1 + S_2 + \cdots + \hat{S}_i + \cdots + S_n) = \{0\},$$

donde $\hat{S}_i$ significa que el término $S_i$ se omite de la suma.

***Demostración.*** i) implica ii) La prueba es por inducción sobre $n \geq 2$, el caso base es la proposición anterior. Para $n > 2$ definimos $T = S_1 \oplus S_2 \oplus \cdots \oplus S_n$ entonces $G = T \oplus S_{n+1}$, si $a \in G$ entonces $a = t + s_{n+1}$ con $t \in T$ y $s_{n+1} \in S_{n+1}$ donde esta expresión es única, por hipótesis inductiva $t = s_1 + \ldots s_n$, donde $s_i \in S_i$ para todo $i \leq n$, donde esta expresión es única.

ii) implica iii) Supongamos que

$$x \in S_i \cap (S_1 + S_2 + \cdots + \hat{S}_i + \cdots + S_n)$$

entonces $x = s_i \in S_i$ y $s_i = \sum_{j \neq i} s_j$ donde $s_j \in S_j$. Entonces $0 = -s_i + \sum_{j \neq i} s_j$ y $0 = 0 + 0 + \cdots + 0$ puesto que la expresión es única, entonces $s_j = 0$ para todo $j$ y $s_i = 0$.

iii) implica ii) Tenemos en particular que $S_{n+1} \cap (S_1 + S_2 + \cdots + S_n) = \{0\}$ por tanto

$$G = S_{n+1} \oplus (S_1 + S_2 + \cdots + S_n)$$

Observemos que para todo $i \leq n$ se tiene que

$$S_j \cap (S_1 + \cdots + \hat{S}_j + \cdots + S_n) \subseteq S_j \cap (S_1 + \cdots + \hat{S}_j + \cdots + S_n + S_{n+1}) = \{0\}$$

por hipótesis inductiva $S_1 + \cdots + S_n = S_1 \oplus \cdots \oplus S_n$ ■

**Corolario 1.9.2**
Sea $G = \langle y_1, \ldots, y_n \rangle$. Si para todo $m_i \in \mathbb{Z}$, tenemos que $\sum_{i=1}^{n} m_i y_i = 0$ implica que $m_i y_i = 0$, entonces

$$G = \langle y_1 \rangle \oplus \cdots \oplus \langle y_n \rangle .$$

***Demostración.*** Por la parte ii) de la proposición anterior es suficiente con probar que si $\sum_i k_i y_i = \sum_i l_i y_i$, entonces $k_i y_i = l_i y_i$ para todo $i$. Pero esto es claro ya que $\sum_i (k_i - l_i) y_i = 0$ implica que $(k_i - l_i) y_i = 0$ para todo $i$. ■

**Ejemplo 45**
Sea $V$ un espacio vectorial $n$-dimensional sobre un campo $K$, si $v_1, \ldots, v_n$ es una base, entonces

$$V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_n \rangle$$

como grupo abeliano donde

$$\langle v_i \rangle = \{ r v_i : r \in K \}$$

cada $v \in V$ tiene una única expresión de la forma $v = s_1 + \cdots + s_n$, donde $s_i = r_i v_i \in \langle v_i \rangle$, ya que $v_1, \ldots, \ v_n$ es una base.

**Proposición 1.9.3**
Si $G_1, G_2, \ldots, G_n$ son grupos abelianos y $H_i \subseteq G_i$ son subgrupos, entonces

$$(G_1 \oplus \cdots \oplus G_n)/(H_1 \oplus \cdots \oplus H_n) \cong G_1/H_1 \times \cdots \times G_n/H_n.$$

***Demostración.*** Definimos $f : G_1 \oplus \cdots \oplus G_n \to G_1/H_1 \times \cdots \times G_n/H_n$ como $(g_1, \ldots, \ g_n) \mapsto (g_1 + H_1, \ldots, \ g_n + H_n)$. $f$ es un homomorfismo sobreyectivo y $ker f = H_1 \oplus \cdots \oplus H_n$. ■

Notación. $G$ un grupo abeliano y $m$ un entero, escribimos

$$mG = \{ ma : a \in G \}$$

es fácil ver que $mG \leq G$ es subgrupo.

**Proposición 1.9.4**
Si $G$ es un grupo abeliano y $p$ es un primo, entonces $G/pG$ es un espacio vectorial sobre $\mathbb{Z}_p$.

***Demostración.*** Si $[r] \in \mathbb{Z}_p$ y $a \in G$, definimos la multiplicación por escalares como

$$[r](a + pG) = ra + pG.$$

Este producto está bien definido, pues si $k \equiv \ r \ mod \ p$, entonces $k = r + pm$ para algún $m \in \mathbb{Z}$, entonces $ka = ra + pma$ donde $pma \in pG$, por lo tanto $ka + pG = ra + pG$. ■

**Definición 1.9.4**
Sea $F = \langle x_1, \ldots, x_n \rangle$ un grupo abeliano. Si

$$F = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$$

donde cada $\langle x_i \rangle \cong \mathbb{Z}$, $F$ es llamado un grupo abeliano libre con base $x_1, \ldots, x_n$.

**Ejemplo 46**
Sea $\mathbb{Z}^m = \mathbb{Z} \times \cdots \times \mathbb{Z}$, $m$ copias de $\mathbb{Z}$

**Proposición 1.9.5**
$\mathbb{Z}^m \cong \mathbb{Z}^n$ si y sólo si $m = n$.

***Demostración.*** Necesidad. Sea $G$ un grupo abeliano, tal que $G = G_1 \oplus \cdots \oplus G_n$, entonces $2G = 2G_1 \oplus \cdots \oplus 2G_n$ . Por lo tanto

$$G/2G \cong G_1/2G_1 \oplus \cdots \oplus G_n/2G_n$$

tomando $H = \mathbb{Z}^m$, entonces $|H/2H| = |(\mathbb{Z}_2)^m| = 2^m$, similarmente $K = \mathbb{Z}^n$, entonces $|K/2K| = 2^n$, de donde $2^m = 2^n$ por lo tanto $m = n$. ■

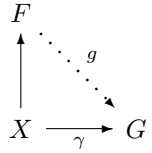
**Corolario 1.9.3**
Si $F$ es libre, dos bases de $F$ tienen el mismo número de elementos.

***Demostración.*** $\{x_1, \ldots, x_n\}$ base de $F$, entonces $F \cong \mathbb{Z}^n$, $\{y_1, \ldots, y_m\}$ base de $F$, por lo cual se tiene $F \cong \mathbb{Z}^m$, el resultado se sigue de la proposición anterior. ■

**Definición 1.9.5**
Sea $F$ un grupo abeliano libre con base $\{x_1, \ldots, x_n\}$, entonces $n$ es llamado el rango de $F$, y lo denotamos como rango($F$).

**Observación 36**
Rango($F$) está bien definido usando el Colorario 1.9.3.

**Teorema 1.9.1**
Sea $F$ un grupo libre con base $X = \{x_1, \ldots, x_n\}$. Si $G$ es un grupo abeliano arbitrario y $\gamma : X \to G$ una función, entonces existe un homomorfismo único $g : F \to G$ tal que $g(x_i) = \gamma(x_i)$ para todo $x_i \in X$.



***Demostración.*** Para todo elemento existe una única expresión de la forma

$$a = \sum_{i=1}^{n} m_i x_i$$

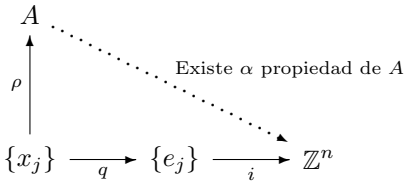
donde $m_i \in \mathbb{Z}$. Defina $g : F \to G$ por

$$g(a) = \sum_{i=1}^{n} m_i \gamma(x_i).$$

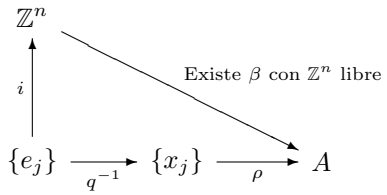
Si $h : F \to G$ es un homomorfismo con $h(x_i) = g(x_i)$ para todo $i$, entonces $h = g$, ya que ambos homomorfismos coinciden con la base. ■

**Proposición 1.9.6**
Sea $A$ un grupo abeliano y $X = \{x_1, \ldots, x_n\} \subseteq A$ con la propiedad, para todo grupo abeliano $G$ y toda función $\gamma : X \to G$ existe un único $g : A \to G$ homomorfismo tal que $g(x_i) = \gamma(x_i)$ para todo $i$, entonces $A \cong \mathbb{Z}^n$ esto es $A$ es grupo abeliano libre de rango$(n)$.

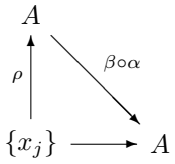
***Demostración.*** Sea $q : \{x_j\} \leftrightarrow \{e_j\}$ una biyección y $\rho, i$ inclusiones. Por la propiedad de $A$ tenemos que existe $\alpha : A \to \mathbb{Z}^n$ tal que hace conmutativo el siguiente diagrama:



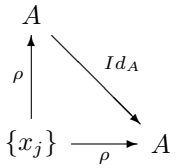

i) $\alpha \circ \rho = i \circ q$



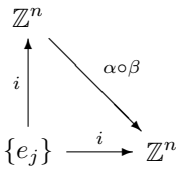

ii) $\beta \circ i = \rho \circ q^{-1}$



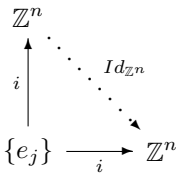
Vemos que el diagrama conmuta por i. y ii. pues $(\beta \circ \alpha) \circ \rho = \rho$. Veamos otro diagrama que conmuta




El morfismo es único $\beta \circ \alpha = Id_A$.




Este diagrama conmuta por i) y ii) además $\alpha \circ \beta \circ i = i$.




también conmuta y el morfismo es único $\alpha \circ \beta = Id_{\mathbb{Z}^n}$, entonces $A \xrightarrow{\alpha} \mathbb{Z}^n$ es isomorfismo con inverso $\mathbb{Z}^n \xrightarrow{\beta} A$. ■

**Definición 1.9.6**
Sea $p$ un número primo, decimos que un grupo abeliano $G$ es $p$-primario, si para cada $a \in G$ existe $n \geq 1$ tal que $p^n a = 0$.

Si $G$ es abeliano la componente $p$-primaria de $G$ es

$$G_p = \{a \in G : p^n a = 0 \text{ para algún } n \geq 1\} \leq G.$$

**Teorema 1.9.2 (Descomposición primaria.)**
i) Todo grupo abeliano finito $G$ es suma directa de sus componentes $p$-primarias

$$G = G_{p_1} \oplus \cdots \oplus G_{p_n}$$

ii) Dos grupos abelianos finitos $G$ y $G'$ son isomorfos si y sólo si $G_p \cong G'_p$ para todo primo $p$.

***Demostración.*** i) Sea $d$ el orden del grupo $G$ y $x \in G$ no nulo. De acuerdo con el teorema fundamental de la aritmética tenemos que

$$d = p_1^{e_1} \dots p_n^{e_n}$$

con $p_i \in \mathbb{Z}$ números primos.

Sean $r_i = d/p_i^{e_i}$ así que $d = p_i^{e_i} r_i$ puesto que $dx = 0$, por lo tanto $r_i x \in G_{p_i}$ para todo $i$; además $MCD\{r_i\} = 1$. Por lo tanto, existen $n$ enteros $s_i$ tal que $\sum s_i r_i = 1$ por lo tanto

$$x = \sum_i s_i r_i x \in G_{p_1} + \cdots + G_{p_n}.$$

Sea $H_i = G_{p_1} + G_{p_2} + \cdots + \widehat{G_{p_i}} + \cdots + G_{p_n}$. Entonces hay que probar que si $x \in G_{p_i} \cap H_i$, entonces $x = 0$.

Si $x \in G_{p_i}$, entonces $p_i^l x = 0$ para alguna $l \geq 1$; además $x \in H_i$ por lo que se tiene que $x = \sum_{j \neq i} y_j$ donde $p_j^{g_j} y_j = 0$ para $g_j \geq 1$. Sea $u = \prod_{j \neq i} p_j^{g_j}$, entonces $ux = 0$. Cómo $p_i^l$ y $u$ son primos relativos, entonces existen enteros $s$ y $t$ con $sp_i^l + tu = 1$. Por lo tanto

$$x = (sp_i^l + tu)x = sp_i^l x + tux = 0.$$

Por lo tanto $G = G_{p_1} \oplus \cdots \oplus G_{p_n}$.

ii) Si $f : G \to G'$ es un homomorfismo, si $p$-primo y $p^l a = 0$, entonces $f(p^l a) = p^l f(a) = 0$. Por lo tanto $f(G_p) \subseteq G'_p$ para todo primo $p$. Si $f$ es un isomorfismo, entonces $f^{-1}(G'_p) \subseteq G_p$ para todo $p$ primo, por lo tanto $f|_{G_p} : G_p \to G_{p'}$ es isomorfismo con inverso $f^{-1}|G'_p$.

De manera inversa, si hay un isomorfismo $f_p : G_p \to G'_p$

isomorfismo para todo $p$, entonces $\varphi : \sum_p G_p \to \sum_p G'_p$ dado por $\sum_p a_p \to \sum_p f_p(a_p)$ es isomorfismo. ■

**Definición 1.9.7**
Sea $p$-primo y sea $G$ un grupo abeliano $p$-primario. Un subgrupo $S \subseteq G$ es un subgrupo puro si para todo $n \geq 0$,

$$S \cap p^n G = p^n S.$$

**Observación 37**
La inclusión $p^n S \leq S \cap p^n G$ siempre se cumple por lo que $S \subseteq G$ es puro si dada la ecuación $s = p^n g$ para $s \in S$ y $g \in G$ existen $s' \in S$ tal que $s = p^n s'$.

**Ejemplo 47**
Todo sumando $S$ directo de $G$ es un subgrupo puro. Si $G = S \oplus T$ y $(s, 0) = p^n(u, v)$ para $u \in S$ y $v \in T$ es claro que $(s, 0) = p^n(u, 0)$.

**Ejemplo 48**
Si $G = \langle a \rangle$ es cíclico de orden $p^2$, donde $p$ es un primo, entonces $S = \langle pa \rangle$ no es un subgrupo puro pues si $s = pa \in S \cap pG$ no existe $s' \in S$ tal que $s = ps'$.

**Lema 1.9.1**
Si $p$ primo y $G$ es un grupo abeliano $p$-primario, entonces $G$ tiene un subgrupo cíclico puro no nulo.

***Demostración.*** Ya que $G$ es finito, sea $y \in G$ de orden mayor, digamos $p^l$. Veamos que $S = \langle y \rangle$ es un subgrupo puro de $G$.

Si $s \in S$, entonces $s = (mp^t)y$, donde $t \geq 0$ y $p \nmid m$ y sea para algún $a \in G$

$$s = p^n a$$

si $n \geq l$, $s = p^n a = 0$ pues $p^l g = 0$ para todo $g \in G$ ya que $y$ es de orden mayor y elegimos $s' = 0$.

Si $n < l$: Caso 1) $t \geq n$, definimos $s' = mp^{t-n}y \in S$, por lo cual $p^n s' = s$.

Caso 2) $t < n$, entonces

$$p^l a = p^{l-n}p^n a = p^{l-n}mp^t y = mp^{l-n+t}$$

y $-n + t < 0$, entonces $l - n + t < l$ y $p \nmid m$, por lo tanto $p^l a \neq 0$, pero esto es una contradicción ya que $y$ es de orden máximo. ■

**Definición 1.9.8**
Sea $p$ primo y $G$ un grupo abeliano $p$-primario, entonces

$$d(G) = dim(G/pG)$$

Observe que $d$ es aditivo sobre sumas directas,

$$d(G \oplus H) = d(G) + d(H)$$

ya que

$$G \oplus H/p(G \oplus H) = G \oplus H/pG \oplus pH \cong G/pG \oplus H/pH$$

Por lo tanto dimensión es $d(G) + d(H)$ ya que la unión de bases es una base.

**Lema 1.9.2**
Si $G \neq \{0\}$ es $p$-primario, entonces $d(G) = 1$ si y sólo si $G$ es cíclico.

***Demostración.*** Necesidad. Ahora sea $G/pG = \langle z + pG \rangle$, entonces $G/pG \cong \mathbb{Z}_p$. Cómo $\mathbb{Z}_p$ es simple, por el teorema de la correspondencia, no hay subgrupos intermedios entre $pG$ y $G$. Por lo tanto $pG \lneq G$ es subgrupo máximo propio. Veamos que $pG$ es el único subgrupo máximo propio de $G$.

Sea $L \subseteq G$ otro subgrupo máximo propio de $G$, entonces se tiene que $G/L$ es abeliano simple de orden una potencia de $p$, así que $G/L \cong \mathbb{Z}_p$ por lo que, si $a \in G$ entonces $p(a + L) = L$ en $G/L$, entonces $pa \in L$ por lo que se tiene $pG \subseteq L$ pero $pG$ es máximo, entonces $pG = L$.

Concluimos que todo subgrupo propio de $G$ está contenido en $pG$, en particular si $\langle z\rangle \lneq G$ subgrupo propio de G, entonces $\langle z\rangle \subseteq pG$, pero esto es una contradicción pues $z + pG$ genera $G/pG$. Por lo tanto $\langle z\rangle = G$ cíclico.

Suficiencia. Si $G$ es cíclico, entonces $G/pG$ es cíclico, por lo que

$$dim(G/pG) = 1.$$

■

**Lema 1.9.3**
Sea $G$ un grupo abeliano finito $p$-primario.

i) Si $S \subseteq G$, entonces $d(G/S) \leq d(G)$.

ii) Si $S$ es un subgrupo puro de $G$, entonces

$$d(G) = d(S) + d(G/S).$$

***Demostración.*** i) Por el teorema de la correspondencia, puesto que $p(G/S) \leq G/S$, entonces

$$p(G/S) = (pG + S)/S$$

entonces

$$(G/S)/p(G/S) = (G/S)/((pG + S)/S) \cong G/(pG + S)$$

puesto que $pG \subseteq pG + S$, existe un homomorfismo sobreyectivo de

$$G/pG \to G/(pG + S)$$

(de espacios vectoriales)

$$g + pG \to g + (pG + S)$$

entonces $dim(G/pG) \geq dim(G/pG + S)$, por lo que

$$d(G) \geq d(G/S)$$

ii) El núcleo del homomorfismo anterior es $(pG + S)/pG$ y por el segundo teorema de isomorfismos $(pG + S)/pG \cong S/pG \cap S$ puesto que $S$ es puro, se sigue $S \cap pG = pS$, entonces $(pG + S)/pG \cong S/pS$, por lo cual $dim((pG + S)/pG) = d(S)$.

Recordemos que si $W$ es un subespacio vectorial de V de dimensión finita sobre un campo $K$, se puede probar que $dimV = dimW + dim(V/W)$ con $V = G/pG$ y $W = (pG + S)/pG$, tenemos que

$$d(G) = d(S) + d(G/S)$$

■

**Teorema 1.9.3 (Teorema base.)**
Todo grupo abeliano finito $G$ es suma directa de grupos cíclicos de orden potencias de primos.

***Demostración.*** Por el teorema de la descomposición primaria podemos asumir que $G$ es $p$-primario para algún $p$-primo. Vemos que $G$ es suma directa de grupos cíclicos por inducción en $d(G) \geq 1$.

La base de inducción. Si $d(G) = 1$ por Lema 1.9.2 $G$ es cíclico.

Para el paso inductivo sabemos por Lema 1.9.1 que existe un subgrupo $S \subseteq G$ puro, no cero y cíclico y por el lema anterior

$$d(G/S) = d(G) - d(S) = d(G) - 1 < d(G)$$

pues $S$ es cíclico si y sólo si $d(S) = 1$, por inducción $G/S$ es suma directa de grupos cíclicos digamos

$$G/S = \sum_{i=1}^{q} \langle \overline{x_i} \rangle$$

donde $\overline{x_i} = x_i + S$.

Ahora para cada $x \in G$ y $\overline{x} = x + S$ de orden $p^l$, veamos que existe $z \in G$ tal que $z + S = \overline{x} = x + S$ tal que orden de $z$ es igual al orden de $\overline{x}$. Pero $p^l(x + S) = p^l\overline{x} = 0$, entonces $p^l x \in S$, se sigue que $p^l x = s$ para algún $s \in S$, por lo cual existe $s' \in S$ tal que $p^l x = s = p^l s'$, definimos $z = x - s'$ por lo tanto $p^l z = 0$ y $z+S = x+S$, ahora si $z$ tiene orden $p^m$ tenemos $p^m(z+S) = p^m\overline{x} = 0$ por lo que $l \leq m$ pero $p^l z = 0$, entonces $m \leq l$. Por lo tanto el orden de $z$ es $p^l$.

Para cada $i$ elegimos $z_i \in G$ con $z_i + S = \overline{x_i} = x_i + S$ con orden $z_i$ igual al orden de $\overline{x_i}$.

Definimos $T$ como $T = \langle z_1 \ldots, z_q \rangle$, ahora tenemos que $G = S + T$ ya que $G$ es generado por $S$ y los $z_i$,

$$g \in G, \text{ entonces } g + S = \sum m_i(z_i + S), \text{ por lo cual } g - \sum m_i z_i \in S$$

por último para ver que $G = S \oplus T$ hay que ver $S \cap T = \{0\}$.

Sea $y \in S \cap T$, entonces $y = \sum_i m_i z_i \in S$, se sigue $\sum m_i\overline{x_i} = 0 \in G/S$ puesto que $G/S$ es suma directa, entonces $m_i\hat{x_i} = 0$ para cada $i$ ya que $m_i\hat{x_i} = -\sum_{j\neq i} m_j\overline{x_j} \in \langle \overline{x_i} \rangle \cap [\langle \overline{x_1} \rangle + \cdots + \langle \hat{\overline{x_i}} \rangle + \cdots + \langle \overline{x_q} \rangle] = \{0\}$ , entonces $m_i z_i = 0$ para todo $i$, por lo cual $y = 0$. Por lo tanto $G = S \oplus T$, entonces

$$d(G) = d(S) + d(T) = 1 + d(T).$$

Por lo tanto $d(T) < d(G)$ por inducción $T$ es suma directa de subgrupos cíclicos.
■

Recordemos que

$$d(G) = dim(G/pG)$$

En particular

$$d(pG) = dim(pG/p^2G)$$

y más general

$$d(p^nG) = dim(p^nG/p^{n+1}G).$$

**Lema 1.9.4**
Sea $G$ un grupo abeliano finito $p$-primario, con $p$ un entero primo sea $G = \sum_j C_j$ donde cada $C_j$ es cíclico. Si $b_n \geq 0$ es el número de sumandos $C_j$ de orden $p^n$. Entonces, existe $t \geq 1$ con $d(p^nG) = b_{n+1} + b_{n+2} + \cdots + b_t$.

***Demostración.*** Sea $B_n$ la suma directa de los $C_j$ de orden $p^n$ entonces

$$G = B_1 \oplus B_2 \oplus \cdots \oplus B_t$$

para algún $t$. Ahora $p^nG = p^nB_{n+1} \oplus \cdots \oplus p^nB_t$ ya que $p^nB_j = \{0\}$ para todo $j \leq n$, ya que $p^n$ es mayor al orden de los sumandos de $B_j$. Similarmente $p^{n+1}G = (p^{n+1}B_{n+1}) \oplus \cdots \oplus p^{n+1}B_t$ usando una propiedad anterior tenemos que

$$p^nG/p^{n+1}G \cong \left[\frac{p^nB_{n+1}}{p^{n+1}B_{n+1}}\right] \oplus \cdots \oplus \left[\frac{p^nB_t}{p^{n+1}B_t}\right]$$

luego tenemos que

$$d(p^nB_m) = dim\left(\frac{p^nB_m}{p^{n+1}B_m}\right) = b_m \text{ para todo } n < m$$

ya que si $B_m = \langle x_1\rangle \oplus \cdots \oplus \langle x_{b_m}\rangle$ es suma directa de $b_m$ grupos cíclicos de orden $p^m$, entonces, si $n < m$ tenemos que $\{p^nx_i + p^{n+1}B_m\}$ es una base de $p^nB_m/p^{n+1}B_m$ y puesto que $d$ es aditivo, obtenemos que

$$d(p^nG) = b_{n+1} + b_{n+2} + \cdots + b_t.$$

■

**Definición 1.9.9**
Sea $G$ un grupo finito $p$-primario con $p$-primo para $n \geq 0$ definimos

$$U_p(n, G) = d(p^nG) - d(p^{n+1}G).$$

El lema anterior muestra que $d(p^nG) = b_{n+1} + \cdots + b_t$ y $d(p^{n+1}G) = b_{n+2} + \cdots + b_t$. Por lo tanto $U_p(n, G) = b_{n+1}$.

El cual es el número de sumandos directos de la descomposición $G = C_1 \oplus \cdots \oplus C_l$ en cíclicos de orden $p^{n+1}$.

**Teorema 1.9.4**
Si $p$ es un primo, cualesquiera dos descomposiciones de $G$ un grupo abeliano finito $p$-primario en sumas directas de grupos cíclicos, tienen el mismo número de sumandos directos de cada tipo. Más aun para cada $n \geq 0$ el número de sumandos cíclicos de orden $p^{n+1}$ es $U_p(n, G)$.

***Demostración.*** Sabemos que $G = \sum_i C_i$ con $C_i$ cíclicos por el Teorema 1.9.3 y usando el lema anterior se muestra que para cada $n \geq 0$ el número de $C_i$ de orden $p^{n+1}$ es $U_p(n, G)$ y este número fue definido independientemente de la descomposición de $G$ en suma directa de cíclicos.

Entonces si $G = \sum_j D_j$ es otra descomposición de $G$ con $D_j$ cíclicos, entonces el número de $D_j$ de orden $p^{n+1}$ es también $U_p(n, G)$. ■

**Corolario 1.9.4**
Si $G$ y $G'$ son dos grupos abelianos finitos $p$-primarios, entonces $G \cong G'$ si y sólo si $U_p(n, G) = U_p(n, G')$ para todo $n \geq 0$.

***Demostración.*** Sea $\varphi : G \to G'$, un isomorfismo de grupos. Por ser $\varphi$ un homomorfismo, tenemos que $\varphi(p^n G) \subseteq p^n G'$. Ahora, por ser $\varphi$ ismorfismo, también tenemos que $\varphi^{-1}(p^n G') \subseteq p^n G$, entonces $\varphi(p^n G) = p^n G'$ para todo $n \geq 0$, entonces $\varphi$ induce isomorfismos entre

$$p^n G/p^{n+1}G \cong p^n G'/p^{n+1}G' \text{ de } \mathbb{Z}_p$$

espacio vectorial para todo $n \geq 0$, dado por la asignación

$$p^n g + p^{n+1}G \to p^n \varphi(g) + p^{n+1}G'$$

entonces sus dimensiones son las mismas. Por lo tanto

$$dim(p^n G/p^{n+1}G) = dim(p^n G'/p^{n+1}G')$$

entonces $U_p(n, G) = U_p(n, G')$.

De forma contraria; si $U_p(n, G) = U_p(n, G')$ para todo $n \geq 0$. Si $G = \sum_i C_i$ y $G' = \sum_j C'_j$ donde $C_i$ y $C'_j$ son cíclicos.

Tenemos que $G, G'$ tienen el mismo número de sumandos cíclicos de mismo tipo. El isomorfismo de $G \to G'$ es claro. ■

**Definición 1.9.10**
Sea $G$ un grupo abeliano $p$-primario, entonces sus divisores elementales son $U_p(0, G)p's, U_p(1, G)p^{2,}s, \ldots, U_p(t-1)p^{t,}s$ con $p^t$ el orden más grande de un sumando cíclico de $G$.

**Observación 38**
Si $G$ es abeliano finito sus divisores elementales son los divisores elementales de todos sus componentes $p$-primarios.

**Teorema 1.9.5 (Fundamental de grupos abelianos finitos)**
Dos grupos abelianos $G$ y $G'$ son isomorfismos si y sólo s cualesquiera dos descomposiciones de $G$ y $G'$ en suma directa de grupos cíclicos primarios, estas tienen el mismo número de sumandos de cada orden. ($G \cong G'$ si y sólo si tienen los mismos divisores elementales.)

***Demostración.*** Por el teorema de la descomposición primaria $G \cong G'$ si y sólo si $G_p \cong G'_p$ para todo $p$; por otro lado $G_p \cong G'_p$ por el Corolario 1.9.4 si y sólo si $U_p(n, G) = U_p(n, G')$, con $n \geq 0$ es decir tienen el mismo número de sumandos del mismo tipo. ■

**Proposición 1.9.7**
Todo grupo abeliano finito $G$ es suma directa de grupos cíclos

$$G = S(C_1) \oplus \cdots \oplus S(C_t) \text{ donde } t \geq 1,\ S(C_i) \text{ cíclico de orden } C_i$$

y $C_1|C_2| \ldots |C_t$.

***Demostración.*** Sean $p_1, \ldots,\ p_n$ los divisores primos de $|G|$, luego

$$G = G_{p_1} \oplus \cdots \oplus G_{p_n}$$

por el Teorema 1.9.3 para cada $p_i$ ($G_{p_i}$ es suma de cíclicos de orden potencias de $p_i$)

$$G_{p_i} = S(p_i^{e_{i1}}) \oplus \cdots \oplus S(p_i^{e_{it}})$$

podemos asumir que $0 \leq e_{i1} \leq \cdots \leq e_{it}$ definimos $C_j = p_1^{e_{1_j}} p_2^{e_{2_j}} \ldots p_n^{e_{n_j}}$ donde algunos $e_{ij} = 0$ es claro que $C_1|C_2| \ldots |C_t$ finalmente

$$S(p_1^{e_{1j}}) \oplus S(p_2^{e_{2j}}) \oplus \cdots \oplus S(p_n^{e_{nj}}) \cong S(C_j).$$

■

**Definición 1.9.11**
Si $G$ es un grupo abeliano entonces el exponente de $G$ es el entero positivo más pequeño $m$ tal que $mG = \{0\}$

**Corolario 1.9.5**
Si $G$ es un grupo abeliano finito y $G = S(C_1) \oplus \cdots \oplus S(C_t)$ con $S(C_i)$ cíclico de orden $C_i$ y $C_1|C_2| \ldots |C_t$, entonces $C_t$ es el exponente de $G$.

***Demostración.*** Puesto que $C_i|C_t$ para todo $i$, entonces $C_t S(C_i) = \{0\}$ para todo $i$, se tiene que $C_t G = \{0\}$; por otro lado, no existe un número $1 \leq e < C_t$ tal que $eS(C_t) = \{0\}$ por lo que $C_t$ es el entero positivo más pequeño tal que $C_t G = \{0\}$ (anulador de $G$). ■

**Corolario 1.9.6**
Todo grupo abeliano finito $G$ no cíclico tiene un subgrupo isomorfo a $\mathbb{Z}_C \oplus \mathbb{Z}_C$ para algún $c > 1$.

***Demostración.*** Por la proposición anterior $G = \mathbb{Z}_{C_1} \oplus \mathbb{Z}_{C_2} \oplus \cdots \oplus \mathbb{Z}_{C_t}$ con $t \geq 2$, ya que $G$ no es cíclico; además $C_1|C_2$ el grupo cíclico $\mathbb{Z}_{C_2}$ contiene un subgrupo isomorfo a $\mathbb{Z}_{C_1}$. Por lo tanto $G$ tiene un subgrupo isomorfo $\mathbb{Z}_{C_1} \oplus \mathbb{Z}_{C_1}$. ■

**Definición 1.9.12**
Si $G$ es un grupo abeliano finito y $G = S(C_1) \oplus \cdots \oplus S(C_t)$, $t \geq 1$, $S(C_j)$ es cíclico de orden $C_j$ y $C_1|C_2|\ldots|C_t$. Entonces $C_1, \ldots, C_t$ son llamados los factores invariantes de $G$.

**Teorema 1.9.6 (Factores invariantes)**
Dos grupos abelianos finitos son isomorfos si y sólo si tienen los mismos factores invariantes.

***Demostración.*** Dados los divisores elementales de $G$ podemos construir los factores invariantes como en la proposición anterior

$$C_j = p_1^{e_{1j}} p_2^{e_{2j}} \ldots p_n^{e_{nj}}$$

donde los factores $p_i^{e_{i1}}$, $p_i^{e_{i2}}$,... que no son de la forma $p_i^0 = 1$, son los divisores elementales de la componente

$$G_{p_i}$$

entonces los factores invariantes dependen sólo de $G$ ya que son definidos en términos de los divisores elementales.

Ahora veamos que los divisores elementales se pueden calcular a partir de los factores invariantes puesto que $C_j = p_1^{e_{1j}} p_2^{e_{2j}} \ldots p_n^{e_{nj}}$ por el teorema fundamental de la aritmética $C_j$ determina todas estas potencias $p_i^{e_{ij}}$. Por lo tanto dos grupos tienen los mismos factores invariantes si y sólo si estos tienen los mismos divisores elementales si sólo si $G \cong G'$. ■

## 1.10. Ejercicios.

**Ejercicio 1.1**
i) ¿Cuántos elementos de orden 2 hay en $S_5$ y $S_6$?

ii) ¿Cuántos elementos de orden 2 hay en $S_n$?

**Ejercicio 1.2**
Si $G$ es un grupo, probar que el único elemento $g \in G$ con $g^2 = g$ es el

1.

**Ejercicio 1.3**
Sea $H$ un conjunto que contiene un elemento $e$, y suponga que hay una operación binaria asociativa $*$ sobre $H$ que cumple las siguientes propiedades:

1) $e * x = x$ para todo $x \in H$;

2) Para todo $x \in H$, existe $x' \in H$ con $x' * x = e$.

i) Probar que si $h \in H$ satisface $h * h = h$, entonces $h = e$.

ii) Para todo $x \in H$, probar que $x * x' = e$.

iii) Para todo $x \in H$, probar que $x * e = x$.

iv) Probar que si $e' \in H$ cumple $e' * x = x$ para todo $x \in H$, entonces $e' = e$.

v) Sea $x \in H$. Probar que si $x'' \in H$ cumple que $x'' * x = e$, entonces $x'' = x'$.

vi) Probar que $H$ es un grupo.

**Ejercicio 1.4**
Sea $y$ un elemento en algún grupo de orden $m$; si $m = pt$ para algún primo $p$, probar que $y^t$ tiene orden $p$.

**Ejercicio 1.5**
Sea $G$ un grupo y sea $a \in G$ de orden $k$. Si $p$ es un divisor primo de $k$, y si existe $x \in G$ con $x^p = a$, probar que $x$ tiene orden $pk$.

**Ejercicio 1.6**
Sea $G = GL(2, \mathbb{Q})$, y sea

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ y } B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

Mostrar que $A^4 = I = B^6$, pero que $(AB)^n \neq I$ para todo $n > 0$, dónde $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ es la matriz identidad. Concluya que $AB$ puede tener orden infinito aunque ambos factores $A$ y $B$ tienen orden finito (esto es imposible en un grupo finito).

**Ejercicio 1.7**
Si $G$ es un grupo en el cual $x^2 = 1$ para todo $x \in G$, probar que $G$ tiene que ser abeliano. [Los grupos Boleanos $\beta(X)$ son grupos de este tipo].

**Ejercicio 1.8**
Si $G$ es un grupo con un número par de elementos, probar que el número de elementos en $G$ de orden 2 es impar. En particular, $G$ tiene que contener un elemento de orden 2.

**Ejercicio 1.9**
¿Cuál es el orden más grande de un elemento en $S_n$, donde $n = 1, 2, \ldots, 10$?

**Ejercicio 1.10**
Sea $H$ un subgrupo de un grupo $G$.

i) Probar que las clases laterales $Ha$ y $Hb$ son iguales si y sólo si $ab^{-1} \in H$.

ii) Probar que la relación $a \equiv b$ si $ab^{-1} \in H$ es una relación de equivalencia en $G$ cuyas clases de equivalencia son clases laterales derechas de $H$.

**Ejercicio 1.11**
Definimos el grupo lineal especial por

$$SL(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : det(A) = 1\}.$$

i)Probar que $SL(2,\mathbb{R})$ es un subgrupo de $GL(2,\mathbb{R})$.

ii) Probar que $GL(2,\mathbb{Q})$ es un subgrupo de $GL(2,\mathbb{R})$.

**Ejercicio 1.12**
i) Dar un ejemplo de dos grupos $H$ y $K$ de un grupo $G$ cuya unión no sea un subgrupo de $G$.

ii) Probar que la unión $H \cup K$ de dos subgrupos es un subgrupo si y sólo si $H$ es un subconjunto de $K$ o $K$ es un subconjunto de $H$.

**Ejercicio 1.13**
Sea $G$ un grupo finito con subgrupos $H$ y $K$. Si $H \leq K$, probar que

$$[G : H] = [G : K][K : H].$$

**Ejercicio 1.14**
Si $H$ y $K$ son subgrupos de un grupo $G$ y si $|H|$ y $|K|$ son primos relativos, probar que $H \cap K = \{1\}$.

**Ejercicio 1.15**
Probar que todo subgrupo $S$ de un grupo cíclico $G = \langle a \rangle$ es cíclico.

**Ejercicio 1.16**
Probar que un grupo cíclico $G$ de orden $n$ tiene un subgrupo de orden $d$ para todo $d$ divisor de $n$.

**Ejercicio 1.17**
Sea $G$ un grupo de orden 4. Probar que $G$ es cíclico o $x^2 = 1$ para todo $x \in G$.

**Ejercicio 1.18**
Si $H$ es un subgrupo de un grupo $G$, probar que el número de clases laterales izquierdas de $H$ en $G$ es igual al número de clases laterales derechas de $H$ en $G$.

**Ejercicio 1.19**
Sea $p$ un primo impar, y sea $a_1, \ldots, a_{p-1}$ una permutación de $\{1, \ldots, p-1\}$. Probar que existe $i \neq j$ con $ia_i \equiv ja_j \ mod\ p$.

**Ejercicio 1.20**
i) Mostrar que la composición de homomorfismos es un homomorfismo.

ii) Mostrar que el inverso de un isomorfismo es un isomorfismo.

**Ejercicio 1.21**
Probar que un grupo $G$ es abeliano si y sólo si la función $f : G \to G$, dada por $f(a) = a^{-1}$, es un homomorfismo.

**Ejercicio 1.22**
En este ejercicio observaremos algunos invariantes de $G$. Sea $f : G \to H$ un isomorfismo.

Probar que si $a \in G$ tiene orden infinito, entonces también $f(a)$, y si a tiene orden finito, entonces también $f(a)$. Concluya que si $G$ tiene un elemento de algún orden $n$ y $H$ no, entonces $G \ncong H$.

**Ejercicio 1.23**
Mostrar que todo grupo $G$ con $|G| < 6$ es abeliano.

**Ejercicio 1.24**
Sea $G = \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b, \text{ donde } a \neq 0\}$. Probar que $G$ es un grupo bajo la composición que es isomorfo al subgrupo de $GL(2, \mathbb{R})$ que consiste de las matrices de la forma $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$.

**Ejercicio 1.25**
i) Si $f : G \to H$ es un homomorfismo y $x \in G$ tiene orden $k$, probar que $f(x) \in H$ tiene orden $m$, donde $m|k$.

ii) Si $f : G \to H$ es un homomorfismo y si $(|G|, |H|) = 1$, probar que $f(x) = 1$ para todo $x \in G$.

**Ejercicio 1.26**
i) Mostrar que $H$ es un subgrupo con $bH = Hb = \{hb : h \in H\}$ para todo $b \in G$, entonces $H$ tiene que ser un subgrupo normal.

ii) Si $H \leq G$ tiene índice 2, entonces $H \triangleleft G$.

**Ejercicio 1.27**
Probar que la intersección de cualquier familia de subgrupos normales de un grupo $G$ es un subgrupo normal de $G$.

**Ejercicio 1.28**
Se define $W = \langle (1\ 2)(3\ 4) \rangle$, el subgrupo cíclico de $S_4$ generado por $(1\ 2)(3\ 4)$. Mostrar que $W$ es un subgrupo normal de $V$, pero que $W$ no es un subgrupo normal de $S_4$. Concluya que la normalidad no es transitiva: $W \lhd V$ y $V \lhd G$ no implica que $W \lhd G$.

**Ejercicio 1.29**
Recuerde que el grupo de cuaternios $Q$ consiste de las ocho matrices en $GL(2, \mathbb{C})$,

$$Q = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

donde

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ y } B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

i) Probar que $-I$ es el único elemento en $Q$ de orden 2, y los otros elementos $M \neq I$ satisfacen $M^2 = -I$.

ii) Probar que $Q$ es un grupo no abeliano con la operación de multiplicación de matrices.

iii) Probar que $Q$ tiene un único subgrupo de orden 2, y es el centro de $Q$.

**Ejercicio 1.30**
Suponga que hay un grupo $G$ de orden ocho cuyos elementos

$$\pm 1, \pm i, \pm j, \pm k$$

cumplen

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,$$
$$ij = -ji,\ ik = -ki,\ jk = -kj.$$

Probar que $G \cong Q$ y, que $Q$ es un grupo de este tipo.

**Ejercicio 1.31**
i) Probar que $Aut(V) \cong S_3$ y que $Aut(S_3) \cong S_3$. Concluya que grupos no isomorfos pueden tener grupos de automorfismos isomorfos.

ii) Probar que $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$. Concluya que un grupo infinito puede tener un grupo de automorfismos finito.

**Ejercicio 1.32**
Si $G$ es un grupo para el cual $Aut(G) = \{1\}$, probar que $|G| < 2$.

**Ejercicio 1.33**
Probar que si $G$ es un grupo para el cual $G/Z(G)$ es cíclico, donde $Z(G)$ denota el centro de $G$, entonces $G$ es abeliano.

**Ejercicio 1.34**
Sea $G$ un grupo finito con $K \lhd G$. Si $(|K|, [G : K]) = 1$, probar que $K$ es el único subgrupo de $G$ que tiene orden $|K|$.

**Ejercicio 1.35**
Si $H$ y $K$ son subgrupos de un grupo $G$, probar que $HK$ es un subgrupo de $G$ si y sólo si $HK = KH$.

**Ejercicio 1.36**
Si $H$ y $K$ son subgrupos normales de un grupo $G$ con $HK = G$, probar que

$$G/(H \cap K) \cong (G/H) \times (G/K).$$

**Ejercicio 1.37**
Se define el centralizador $C_G(H)$ de un subgrupo $H \leq G$ como

$$C_G(H) = \{x \in G : xh = hx \text{ para todo } h \in H\}.$$

Para todo subgrupo $H \leq G$, probar que $C_G(H) \lhd N_G(H)$.

**Ejercicio 1.38**
Probar que $H \lhd N_G(H)$ y que $N_G(H)$ es el subgrupo más grande de $G$ que contiene a $H$ como subgrupo normal.

**Ejercicio 1.39**
Encuentra $N_G(H)$ si $G = S_4$ y $H = \langle(1\ 2\ 3)\rangle$.

**Ejercicio 1.40**
Si $H$ es un subgrupo de $G$ y si $x \in H$, probar que

$$C_H(x) = H \cap C_G(x).$$

**Ejercicio 1.41**
i) Sea $G$ un grupo arbitrario, posiblemente no abeliano, luego sea $S$ y $T$ subgrupos normales de $G$. Probar que $S \cap T = \{1\}$, entonces $st = ts$ para todo $s \in S$ y $t \in T$.

ii) Probar que la Proposición 1.9.2 se cumple para grupos no abelianos si suponemos que todos los subgrupos $S_i$ son subgrupos normales.

**Ejercicio 1.42**
Sea $G$ un grupo abeliano, no necesariamente primario. Se define un subgrupo $S \subseteq G$ como un subgrupo puro si, para todo $m \in \mathbb{Z}$,

$$S \cap mG = mS.$$

Probar que si $G$ es un grupo abeliano $p$-primario, entonces un subgrupo $S \subseteq G$ es puro justamente como se definió si y sólo si $S \cap p^n G = p^n S$ para todo $n \geq 0$.

**Ejercicio 1.43**
¿Cuántos 2-subgrupos de Sylow tiene $S_4$?

**Ejercicio 1.44**
Proporcione un ejemplo de un grupo finito $G$ que tiene $p$-subgrupos de Sylow (para algún $p$) $P, Q$ y $R$ tal que $P \cap Q = \{1\}$ y $P \cap R \neq \{1\}$.

**Ejercicio 1.45**
Un subgrupo $H$ de un grupo $G$ es llamado característico si $\varphi(H) \leq S$ para todo isomorfismo $\varphi : G \to G$. Un subgrupo $S$ de un grupo $G$ es llamado invariante completo si $\varphi(S) \leq S$ para todo homomorfismo $\varphi : G \to G$.
Probar que todo grupo invariante completo es un subgrupo característico, y que todo subgrupo característico es un subgrupo normal.

**Ejercicio 1.46**
Sea $Q$ un $p$-subgrupo normal de un grupo finito $G$. Probar que $Q \leq P$ para todo $p$-subgrupo de Sylow $P$ de $G$.

**Ejercicio 1.47**
Probar que un 2-subgrupo Sylow de $A_5$ tiene exactamente cinco conjugados.

**Ejercicio 1.48**
Probar que no hay grupos simples de orden 96, 120, 300, 312 o 1000.

**Ejercicio 1.49**
Sea $G$ un subgrupo de orden 90.

i) Si un 5-subgrupo de Sylow $P$ de $G$ no es normal, probar que este tiene seis conjugados.

ii) Probar que $G$ no es simple.

**Ejercicio 1.50**
Probar que no hay grupo simple de orden 120.

**Ejercicio 1.51**
Probar que no hay grupo simple de orden 150.

# Capítulo 2

# Anillos conmutativos

## 2.1. Anillos

**Definición 2.1.1**
Un anillo conmutativo $R$ es un conjunto con dos operaciones binarias $(R, +, *)$, digamos suma y producto, tal que

i) $R$ es un grupo abeliano con respecto a la suma;

ii) (Conmutatividad) $ab = ba$ para todo $a, b \in R$;

iii) (Asociatividad) $a(bc) = (ab)c$ para todo $a, b, c \in R$;

iv) Existe un elemento $1 \in R$ con $1a = a$ para todo $a \in R$;

v) (Distributividad) $a(b + c) = ab + ac$ para todo $a, b, c \in R$.

El elemento 1 en un anillo $R$ lo llamaremos uno, unidad o identidad en $R$.

La suma y multiplicación en un anillo conmutativo $R$ son operaciones binarias, entonces hay funciones

$$\alpha : R \times R \to R \text{ con } \alpha(r, r') = r + r' \in R$$
$$\text{y}$$
$$\mu : R \times R \to R \text{ con } \mu(r, r') = rr' \in R$$

para todo $r, r' \in R$. La ley de substitución se cumple: Si $r = r'$ y $s = s'$, entonces $r + s = r' + s'$ y $rs = r's'$.

**Ejemplo 49**
i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R},$ y $\mathbb{C}$ son anillos conmutativos con la suma usual y la multiplicación.

ii) $\mathbb{Z}_m$, los enteros módulo $m$, es un anillo conmutativo.

iii) Sea $\mathbb{Z}[i]$ el conjunto de los números complejos de la forma $a + bi$, donde $a, b \in \mathbb{Z}$ y $i^2 = -1$. Se puede verificar que $\mathbb{Z}[i]$ es un anillo conmutativo y lo llamaremos Anillo de enteros Gausianos.

iv) Consideremos el conjunto $R = \{x \in \mathbb{R} : x = a + bw \text{ con } a, b \in \mathbb{Q} \text{ y } w = \sqrt[3]{2}\}$; no es un anillo conmutativo.

Si fuese cerrado bajo el producto, entonces $w^2 \in R$. Por lo tanto $w^2 = a + bw$ tal que $a, b \in \mathbb{Q}$; multiplicando por $w$ y $b$ respectivamente obtenemos $2 = w^3 = aw + bw^2$ y $bw^2$, entonces $2 - aw = ab + b^2w$ por lo tanto

$$2 - ab = (b^2 + a)w$$

ahora si $(b^2+a) \neq 0$, entonces $w$ es racional, pero es una contradicción; de forma similar si $(b^2 + a) = 0$, entonces $2 = ab = (-b)^3$, por lo cual $\sqrt[3]{2} = -b$ es un racional pero es una contradicción.

**Proposición 2.1.1**
Sea $R$ un anillo conmutativo.
i) $0 * a = 0$ para todo $a \in R$.

ii) Si $1 = 0$, entonces $R$ consiste únicamente del elemento 0. Entonces $R$ será llamado el anillo cero.

iii) Si $-a$ es el inverso aditivo de $a$, entonces $(-1)(-a) = a$.

iv) $(-1)a = -a$ para todo $a \in R$.

v) Si $n \in \mathbb{N}$ y $n1 = 0$, entonces $na = 0$ para todo $a \in R$.

vi) El teorema del binomio se preserva. Si $a, b \in R$, entonces

$$(a + b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

***Demostración.*** i) Tenemos que $0*a = (0+0)*a = 0*a+0*a$, entonces $0*a = 0$.

ii) Sea $a \in R$, $a = 1 * a = 0 * a = 0$ para todo $a \in R$.

iii) Tenemos que $0 = (-1 + 1)(-a) = (-1)(-a) + 1(-a) = (-1)(-a) + (-a)$. Por lo que $a = (-1)(-a)$.

iv) Por iii) $(-1)(-a) = a$, entonces $(-1)(-1)(-a) = (-1)(a)$, por lo cual $(1)(-a) = (-1)(a)$.

v) Tenemos que $na = n(1 * a) = (n * 1)a = 0 * a = 0$.

vi)(Teorema del binomio) La haremos por inducción sobre $n$ mayor que cero. Sabemos que

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r} \text{ para } 0 < r < n+1$$

ahora sea $(a+b)^{n+1} = (a+b)(a+b)^n$

$$\begin{aligned}
&= \sum_{r=0}^{n} \binom{n}{r} a^{n-r+1} b^r + \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^{r+1} \\
&= a^{n+1} + \sum_{r=1}^{n} \binom{n}{r} a^{n-r+1} b^r + \sum_{r=0}^{n-1} \binom{n}{r} a^{n-r} b^{r+1} + b^{n+1} \\
&= a^{n+1} + \sum_{r=1}^{n} \binom{n}{r} a^{n-r+1} b^r + \sum_{r=1}^{n} \binom{n}{r'-1} a^{n-r'+1} b^{r'} + b^{n+1} \\
&= a^{n+1} + \sum_{r=1}^{n} \binom{n+1}{r} a^{n+1-r} b^r + b^{n+1} \\
&= \sum_{r=0}^{n+1} \binom{n+1}{r} a^{n+1-r} b^r
\end{aligned}$$

■

**Definición 2.1.2**
Un subconjunto $S$ de un anillo conmutativo $R$ es un subanillo de $R$ si:

i) $1 \in S$;

ii) Si $a, b \in S$, entonces $a - b \in S$;

iii) Si $a, b \in S$, entonces $ab \in S$.

Contrario a la teoría de grupos, el uso de $H \leq G$ para denotar subgrupos; usaremos en teoría de anillos la siguiente notación: $S \subseteq R$ para subanillos. También escribiremos $S \subsetneq R$ para denotar un subanillo propio; esto es $S \subseteq R$ y $S \neq R$.

**Proposición 2.1.2**
Un subanillo $S$ de un anillo conmutativo $R$ es un anillo conmutativo.

***Demostración.*** Tenemos que $(S,+) \leq (R,+)$ pues $1 \in S$ usando ii) en la definición, tenemos $1-1=0 \in S$ además $0-1=-1 \in S$, entonces si $a \in S$, se tiene que $(-1)(a) = -a \in S$ por último $a-(-b) = a+b \in S$. Las demás propiedades del producto se heredan de $R$. ■

**Ejemplo 50**
Si $n \geq 3$ es un entero, sea $\zeta_n = e^{2\pi i/n}$ la $n$-ésima raíz primitiva de la unidad, y defina

$$\mathbb{Z}[\zeta_n] = \{z \in \mathbb{C} : z = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1} : a_i \in \mathbb{Z}\}$$

Cuando $n=4$, entonces $\mathbb{Z}[\zeta_4]$ es el conjunto de los enteros Gausianos $\mathbb{Z}[i]$. Es fácil verificar que $\mathbb{Z}[\zeta_n]$ es un subanillo de $\mathbb{C}$, para probar que $\mathbb{Z}[\zeta_n]$ es cerrado bajo la multiplicación, note que si $m \geq n$, entonces $m = qn+r$, donde $0 \leq r < n$, y $\zeta_n^m = \zeta_n^r$.

**Definición 2.1.3**
Un dominio (dominio entero) es un anillo conmutativo $R$ que cumple dos axiomas extras: primero,

$$1 \neq 0;$$

segundo, la ley de cancelación para la multiplicación: Para todo $a, b, c \in R$

$$\text{Si } ca = cb \text{ y } c \neq 0, \text{ entonces } a = b.$$

**Ejemplo 51**
Los anillos conmutativos, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son dominios; el anillo cero 0 no es un dominio.

**Proposición 2.1.3**
Un anillo conmutativo $R$ distinto del cero es un dominio si y sólo si el producto de cualesquiera dos elementos distintos del cero en $R$ es distinto del cero.

***Demostración.*** Necesidad. Sea $a, b \in R$ y $0 \neq c \in R$, tenemos que $ca = cb$ si y sólo si $c(a-b) = 0$. Si $c \neq 0$ y $c(a-b) = 0$, entonces $(a-b) = 0$ por lo que $a = b$.

Suficiencia. Ahora si $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$ pues de lo contrario $a * 0 = 0 = ab$ con $a \neq 0$, por lo tanto $b = 0$. ■

**Proposición 2.1.4**
El anillo conmutativo $\mathbb{Z}_m$ es un dominio si y sólo si $m$ es primo.

***Demostración.*** Necesidad. Si $m = ab$ con $1 < a, b < m$, entonces $[a] \neq 0$ y $[b] \neq 0$, pero sin embargo $[a][b] = [m] = 0$.

Suficiencia. Si $m$ es primo y $[ab] = [a][b] = [0]$, entonces $p|ab$, por lo cual o $p|a$ o $p|b$; por lo tanto $[a] = 0$ o $[b] = 0$. ■

**Ejemplo 52**
Sea $\mathcal{F}(\mathbb{R})$ el conjunto de todas las funciones $\mathbb{R} \to \mathbb{R}$, dado $f, g \in \mathcal{F}(\mathbb{R})$ definimos la suma de funciones $f + g$ y el producto de funciones $fg$ como:

$$f + g : a \to f(a) + g(a) \text{ y } fg : a \to f(a)g(a)$$

observe que $fg$ no es su composición. $\mathcal{F}(\mathbb{R})$ es anillo conmutativo donde 0 es la función constante cero que denotaremos por $Z$, es decir $Z(a) = 0$ para toda $a \in \mathbb{R}$; de manera similar el 1 es la función constante uno que denotaremos por $\epsilon$, es decir, $\epsilon(a) = 1$ para todo $a \in \mathbb{R}$. Mostraremos que $\mathcal{F}(\mathbb{R})$ no es dominio.

$$f(a) = \begin{cases} a \text{ si } a \leq 0 \\ 0 \text{ si } a \geq 0; \end{cases} \qquad g(a) = \begin{cases} 0 \text{ si } a \leq 0 \\ a \text{ si } a \geq 0. \end{cases}$$

Así definidas, $f$ y $g$ son distintos de $Z$ pero $fg = Z$.

**Definición 2.1.4**
Sea $a$ y $b$ elementos del anillo conmutativo $R$. Entonces $a$ divide a $b \in R$ ($a$ es un divisor de $b$ ó $b$ es un múltiplo de $a$), denotado por $a|b$, si existe un elemento $c \in R$ con $b = ca$.

**Observación 39**
Como un caso extremo, si $0|a$, entonces $a = 0b$. Por lo tanto, 0 divide a $a$ si y sólo si $a = 0$.

Que $a|b$ no depende únicamente de los elementos $a$ y $b$ sino también del anillo $R$. Por ejemplo, 3 divide a 2 en $\mathbb{Q}$, pues $2 = 3 \times \frac{2}{3}$, y $\frac{2}{3} \in \mathbb{Q}$, pero, 3 no divide a 2 en $\mathbb{Z}$, porque no existe entero $c$ tal que $3c = 2$.

**Definición 2.1.5**
Un elemento $u$ en un anillo conmutativo $R$ es llamado una unidad si $u|1 \in R$, esto es, si existe $v \in R$ con $uv = 1$; el elemento $v$ es llamado el inverso de $u$ y $v$; usualmente lo denotamos por $u^{-1}$.

**Observación 40**
Una propiedad interesante es que siempre podemos dividir entre ellas: Si $a \in R$ y $u$ es una unidad en $R$ (entonces existe un $v \in$ R tal que $uv = 1$) , entonces

$$a = u(va)$$

es una factorización de $a \in R$, por $va \in R$; por lo tanto podemos definir el cociente $a/u$ como $va = u^{-1}a$.

Igual que en la definición anterior, dados elementos $a$ y $b$, nuevamente que $a|b$ no sólo depende de los elementos sino también del anillo $R$ donde esté definido; similarmente que un elemento $u \in R$ sea una unidad depende del anillo donde

esté definido. Por ejemplo, el número 2 es una unidad en $\mathbb{Q}$, para $\frac{1}{2}$ es un elemento de $\mathbb{Q}$ y $2 \times \frac{1}{2} = 1$, pero 2 no es una unidad en $\mathbb{Z}$, pues no existe entero $v$ con $2v = 1$. Las únicas unidades en $\mathbb{Z}$ son 1 y $-1$.

**Proposición 2.1.5**
Sea $R$ un dominio, y sea $a, b \in R$ distintos del cero. Entonces $a|b$ y $b|a$ si y sólo si $b = ua$ para alguna unidad $u \in R$.

***Demostración.*** Necesidad. Si $a|b$, se tiene que $b = ua$ para $u \in R$, de forma similar si $b|a$, entonces $a = vb$ para algún $v \in R$, por lo que se tiene $vb = vua = a$ y como $R$ es dominio, entonces $vu = 1$. Por lo tanto $u \in R$ es unidad.

Suficiencia. Si $b = ua$ para $u \in R$ unidad (es decir $a|b$). Sea $v \in R$ tal que $vu = 1$, entonces $vb = a$. Por lo tanto $b|a$. ■

**Proposición 2.1.6**
Si $a$ es un entero, entonces $[a]$ es una unidad en $\mathbb{Z}_m$ si y sólo si $a$ y $m$ son primos relativos.

***Demostración.*** Si $a$ y $m$ son primos relativos, entonces existen enteros $s$ y $t$ tales que, $sa + tm = 1$, entonces $[a]^{-1} = [s]$. Si $sa \equiv 1 \ mod \ m$ entonces si $sa + mt = 1$ para $s, t \in \mathbb{Z}$. Por lo que $a$ y $m$ son primos relativos. ■

**Corolario 2.1.1**
Si $p$ es un primo, entonces todo $0 \neq [a] \in \mathbb{Z}_p$ es una unidad.

***Demostración.***
Tenemos que $[a] \neq [0]$, si y sólo si $1 \leq a < p$, entonces $(a, p) = 1$. ■

**Definición 2.1.6**
Si $R$ es un anillo conmutativo, entonces el grupo de las unidades de $R$ es

$$U(R) = \{\text{Todas las unidades en } R\}.$$

Se puede verificar que $U(R)$ es un grupo multiplicativo.

**Definición 2.1.7**
Un campo $F$ es un anillo conmutativo en el cual $1 \neq 0$ y para todo elemento no nulo $a$ este es una unidad; es decir, $a^{-1} \in F$ con $a^{-1}a = 1$.

Los ejemplos más naturales que conocemos son los campos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

La definición de campo puede ser expresada en términos del grupo de las unidades; un anillo conmutativo $R$ es un campo si y sólo si $U(R) = R^*$, el conjunto de los elementos no nulos de $R$. Es decir, $R$ es un campo si y sólo si $R^*$ es un grupo multiplicativo. Vea que $U(R^*) \neq \emptyset$ pues por definición $1 \neq 0$.

**Proposición 2.1.7**
Todo campo es un dominio.

***Demostración.*** Si $c \neq 0$ y $ca = cb$ al multiplicarlo por $c^{-1}$, entonces $a = b$. ■

**Observación 41**
El recíproco de esta proposición es falso. Por ejemplo tome $\mathbb{Z}$ y sabemos que es dominio entero pero no es un campo.

**Proposición 2.1.8**
El anillo conmutativo $\mathbb{Z}_m$ es un campo si y sólo si $m$ es un número primo.

***Demostración.*** Necesidad. Si $\mathbb{Z}_m$ es campo, entonces es dominio entero si y sólo si $m$ es primo.

Suficiencia. Si $m$ es primo todos los elementos en $\mathbb{Z}_m^*$ son unidades ■

**Teorema 2.1.1**
Si $R$ es un dominio, entonces existe un campo $F$ que contiene a $R$ como un subanillo. Por otra parte, $F$ puede ser elegido de modo que, para cada $f \in F$, existen $a, b \in R$ con $b \neq 0$ y $f = ab^{-1}$.

***Demostración.*** Sea $X = \{(a, b) \in R \times R : b \neq 0\}$ un conjunto. Definimos una relación de equivalencia "$\equiv$" en $X$ por:

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

reflexiva, simétrica, transitiva y conmutativa.

Veamos que es transitiva. Si $(c, d) = (e, f)$, entonces $cf = de$ por definición. Tenemos que $afd = bfc = bed$ cancelando $d$ tenemos que $af = be$, entonces $(a, b) = (e, f)$.

Denotaremos la clase de equivalencia de $(a, b)$ por $[a, b]$. Definimos $F = \{[a, b] : (a, b) \in X\}$, $F$ es $X$ módulo la equivalencia y la equipamos con la siguientes operaciones binarias:

$$[a, b] + [c, d] = [ad + bc, bd]$$

y

$$[a, b][c, d] = [ac, bd]$$

Tenemos que $b \neq 0$ y $d \neq 0$ por ser $R$ dominio entero, entonces $bd \neq 0$, por lo que $(ad + bc, bd), (ac, bd) \in X$.

La suma está bien definida. Ya que si $[a, b] = [a', b']$ y $[c, d] = [c', d']$ ya que $(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd$.

De manera similar se puede ver que la multiplicación está bien definida.

Con estas operaciones se puede ver que $R$ tiene estructura de anillo conmutativo, en el cual el cero es $[0,1]$, el uno es $[1,1]$; el inverso aditivo es $-[a,b] = [-a,b]$.

Definimos $R' = \{[a,1] : a \in R\} \subseteq F$ es subanillo; identificamos $a \in R$ con $[a,1] \in R'$.

$F$ es campo pues si $[a,b] \neq [0,1]$, entonces $a \neq 0$ y $[a,b]^{-1} = [b,a]$.

Por último si $b \neq 0$, entonces $[b,1]^{-1} = [1,b]$ y $[a,b] = [a,1][b,1]$. ■

**Definición 2.1.8**
El campo $F$ construido en el teorema anterior a partir de $R$ es llamado el campo de las fracciones de $R$; y lo denotaremos por $Frac(R)$, y sus elementos los denotaremos como $[a,b] \in Frac(R)$ por $a/b$; en particular los elementos $[a,1] \in Frac(R)$ son denotados por $a/1$ o más simplemente, por $a$.

Observe que el campo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$; esto es, $Frac(\mathbb{Z}) = \mathbb{Q}$.

**Definición 2.1.9**
Un subcampo de un campo $K$ es un subanillo $k$ de $K$ que también es campo.

Podemos ver que un subconjunto $k$ de un campo $K$ es un subcampo si y sólo si $k$ es un subanillo que es cerrado bajo inversos; esto es, si $a \in k$ y $a \neq 0$, entonces $a^{-1} \in k$. Otra cosa común es verificar que la intersección de subcampos de $K$ es un subcampo de $K$ (la intersección no es igual al vacío porque el 1 está en todos los subcampos).

## 2.2. Polinomios.

**Definición 2.2.1**
Si $R$ es un anillo conmutativo, una sucesión en $R$ es:

$$\sigma = (s_0, s_1, \dots, s_i, \dots)$$

donde las entradas $s_i \in R$ para todo $i \geq 0$; donde los $s_i$ son los coeficientes de $\sigma$.

$\sigma$ la definimos como $\sigma : \mathbb{N} \to R$ es una función donde $i \to \sigma(i) = s_i$. Ahora si $\tau : \mathbb{N} \to R$ tal que $\tau = (t_0, t_1, t_2, \dots, t_i, \dots)$ una sucesión, entonces $\sigma = \tau$ si y sólo si $\sigma(i) = \tau(i)$ para todo $i \geq 0$; es decir, $\sigma = \tau$ si y sólo si $s_i = t_i$ para todo $i \geq 0$.

**Definición 2.2.2**
Una sucesión $\sigma = (s_0, s_1, \dots, s_i, \dots)$ en un anillo conmutativo $R$ es llamado un

polinomio, si existe $m \in \mathbb{N}$ tal que $s_i = 0$ para todo $i > m$, esto es

$$\sigma = (s_0, \dots, s_m, 0, \dots)$$

un polinomio tiene sólo un número finito de coeficientes distintos de cero. El polinomio cero lo definimos como $(0, \dots, 0, \dots)$.

**Definición 2.2.3**
Si $\sigma = (s_0, \dots, s_n, 0, 0, \dots) \neq 0$ es un polinomio, entonces hay $s_n \neq 0$ con $s_i = 0$ para todo $i > n$ llamamos a $n$ el grado de $\sigma$ y lo denotaremos por $deg(\sigma)$. $s_n$ es el coeficiente principal.

El polinomio cero no tiene grado pues no tiene coeficientes no nulos.

$R[x]$ es el conjunto de todos los polinomios con coeficientes en $R$.

**Proposición 2.2.1**
Si $R$ es un anillo conmutativo, entonces $R[x]$ también, además $R \subseteq R[x]$.

Sea $\sigma = (s_0, s_1, \dots)$ y $\tau = (t_0, t_1, \dots)$ definimos

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \dots, s_n + t_n, \dots)$$

y

$$\sigma\tau = (c_0, c_1, c_2, \dots) \text{ donde } c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$$

con $i, j = 0, \dots, k$ y $R = \{(r, 0, 0, \dots) : r \in R\}$.

***Demostración.*** Sean $\sigma = (s_0, s_1, \dots), \tau = (t_0, t_1, \dots)$ y $\gamma = (d_0, d_1, \dots)$ en $R[x]$. Vemos que $(R[x], +)$ grupo abeliano, entonces

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, s_2 + t_2, \dots)$$

entrada a entrada. Tenemos el polinimo cero por $(0, 0, 0, \dots)$. Es fácil ver que $\sigma + \tau = \tau + \sigma$, y además $\sigma + (\tau + \gamma) = (\sigma + \tau) + \gamma$; pues $s_i + t_i = t_i + s_i$ y $s_i + (t_i + d_i) = (s_i + t_i) + d_i$ respectivamente, y esto se cumple para todo $i$. Definimos $-\sigma = (-s_0, -s_1, -s_2, \dots)$.

Definimos la unidad como $(1, 0, 0, \dots)$, tenemos que $\sigma\tau = \tau\sigma$ puesto que

$$\sum_{i+j=k} s_i t_j = \sum_{j+i=k} t_j s_i$$

las entradas $k$-ésimas coinciden, para toda $k$. Ahora tenemos $\gamma(\sigma+\tau) = \gamma\sigma+\gamma\tau$, donde las $k$-ésimas entradas son

$$\sum_{i+j=k} d_i(s_j + t_j) = \sum_{i+j=k} d_i s_j + \sum_{i+j=k} d_i t_j$$

Asociatividad del producto; sea $0 \leq l$, observe que

$$\sum_{i+j+k} s_i t_j d_k = \sum \text{ con } i, j, k = 0, \ldots, l.$$

Fijemos $i$ y agrupamos todos los términos que contengan a $s_i$ obtenemos

$$s_i \left( \sum_{j+k=m} t_i d_k \right) \text{ donde } i + m = l,$$

por lo que

$$\sum = \sum_{i+m=l} s_i \left( \sum_{j+k=m} t_j d_k \right)_m \text{ donde es la } l\text{-ésima entrada de } \sigma(\tau * \delta).$$

Ahora si fijamos $k$ y agrupamos todos los términos que contengan $d_k$ obtenemos

$$\left( \sum_{i+j=n} s_i t_j \right) d_k \text{ donde } n + k = l,$$

por lo que

$$\sum = \sum_{n+k=l} \left( \sum_{i+j=n} s_i t_i \right)_n d_k \text{ es la entrada } l\text{-ésima de } (\sigma * \tau)\delta.$$

■

**Lema 2.2.1**
Sea $R$ un anillo conmutativo y sean $\sigma, \tau \in R[x]$ polinomios distintos de cero.

i) $\sigma\tau = 0$ ó $deg(\sigma\tau) \leq deg(\sigma) + deg(\tau)$.

ii) Si $R$ es un dominio entero, entonces $\sigma\tau \neq 0$ y $deg(\sigma\tau) = deg(\sigma) + deg(\tau)$.

iii) Si $R$ es un dominio entero, entonces $R[x]$ es un dominio entero.

***Demostración.*** Observemos que ii) implica iii)

i) Sean $m = deg(\sigma)$ y $n = deg(\tau)$, entonces para $k > m + n$ tenemos que $c_k = \sum_{i=0}^{k} s_i t_{k-i}$.

Si $i > m$, entonces $s_i = 0$, entonces $s_i t_{k-i} = 0$. Si $i \leq m$, entonces $k - i > n$, se tiene que $t_{k-i} = 0$, por lo tanto $s_i t_{k-i} = 0$.

Por lo tanto $c_k = 0$ para $k > m + n$. Por lo tanto $deg(\sigma\tau) \leq deg\sigma + deg(\tau)$.

ii) Cada término en $\sum_{i=0}^{m+n} s_i t_{m+n-i}$ es cero (Si $i > m$, entonces $s_i = 0$, si $i < m$, entonces $t_{m+n-i} = 0$) con la excepción de $s_m t_n$ puesto que $R$ es dominio entero y $s_m \neq 0$ y $t_n \neq 0$, entonces $(s_m)(t_n) \neq 0$. Por lo tanto $deg(\sigma\tau) = m+n$. ■

**Definición 2.2.4**
Si $R$ es un anillo conmutativo, entonces $R[x]$ es llamado el anillo de polinomios sobre $R$.

**Definición 2.2.5**
Definimos el elemento $x \in R[x]$ por

$$x = (0, 1, 0, 0, \dots).$$

**Lema 2.2.2**
Se cumplen las siguientes propiedades.

i) Si $\sigma = (s_0, s_1, \dots)$, entonces $x\sigma = (0, s_0, s_1, \dots)$.

ii) Si $n \geq 1$, entonces $x^n = (0, 0, \dots, 0, 1, 0, \dots)$, con $1 = t_n$.

iii) Si $r \in R$, entonces $(r, 0, 0, \dots)(s_0, s_1, \dots, s_j, \dots) = (rs_0, rs_1, \dots, rs_j, \dots)$.

***Demostración.*** i) Observemos que la $k$-ésima entrada de $(\sigma)x$ es $c_k = s_{k-1}\tau_1 = s_{k-1}$; $k = 1, \dots, m+1$ y $c_0 = s_0\tau_0 = 0$, en donde los $(\tau)i$ son los coeficientes de $x$.

ii) Usando inducción en i.

iii) Sean los $(\sigma_i)$ los coeficientes de $(r, 0, 0, 0, \dots)$, entonces el coeficiente $k$-ésimo del producto es $c_k = \sum_{i=0}^{k} \sigma_i s_{k-i} = \sigma_0 s_k = rs_k$.

Identificando a $r$ con $(r, 0, 0, \dots)$ tenemos que $r(s_0, s_1, \dots) = (rs_0, rs_1, \dots)$. ■

**Proposición 2.2.2**
Si $\sigma = (s_0, s_1, \dots, s_n, 0, 0, \dots)$, entonces $\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$ en donde cada $s \in R$ lo identificamos con $(s, 0, 0, \dots, ...)$.

***Demostración.*** Tenemos

$$\begin{aligned}\sigma &= (s_0, 0, 0, \dots) + (0, s_1, 0, 0, \dots) + (0, 0, s_2, 0, \dots) + \cdots + (0, \dots, 0, s_n) \\ &= s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n\end{aligned}$$

■

En adelante identificaremos a $\sigma$ con

$$f(x) = s_0 + s_1x + \cdots + s_nx^n$$

donde $s_0$ es el término constante y $s_n$ el coeficiente principal. Si $s_n = 1$ $f(x)$ se llamará polinomio mónico. Un polinomio constante es el polinomio 0 ó un polinomio de grado 0; si es de grado 1 es llamado polinomio lineal $a + bx$ con $b \neq 0$.

**Corolario 2.2.1**
Dos polinomios $f(x) = s_0 + s_1x + \cdots + s_nx^n$ y $g(x) = t_0 + t_1x + \cdots + t_mx^m$ son iguales si y sólo si $m = n$ y $s_i = t_i$ para todo $i$.

***Demostración.*** Es clara de la definición. ■

**Observación 42**
Si $R$ es un anillo conmutativo cada polinomio $f(x) = s_0+s_1x+\cdots+s_nx^n \in R[x]$ define una función polinomial. $f : R \to R$ tal que $f(a) = s_0+s_1a+\cdots+s_na^n \in R$; las funciones polinomiales y los polinomios son distintos.

**Ejemplo 53**
En $\mathbb{Z}_2$ solo hay un número finito de funciones de

$$\mathbb{Z}_2 \to \mathbb{Z}_2$$

sin embargo hay una infinidad de polinomios en $\mathbb{Z}_2[x]$ por ejemplo

$$1, x, x^2, x^3, \ldots, x^n, \ldots$$

**Definición 2.2.6**
Sea $k$ un campo, el campo de fracciones de $k[x]$ lo denotaremos por $k(x)$, y es llamado el campo de funciones racionales sobre $k$.

**Proposición 2.2.3**
Si $k$ es un campo, entonces los elementos de $k(x)$ tienen la forma $f(x)/g(x)$ para $f(x), g(x) \in k[x]$ y $g(x) \neq 0$.

***Demostración.*** La prueba se deduce del Teorema 2.1.1 cuando se construyó el campo de fracciones de un dominio entero. ■

**Proposición 2.2.4**
Si $p$ es un primo, entonces $\mathbb{Z}_p(x)$ es un campo infinito que contiene a $\mathbb{Z}_p$.

***Demostración.*** $\mathbb{Z}_p[x]$ es un dominio entero infinito, para las potencias $x^n$, con $n \in \mathbb{N}$, entonces $\mathbb{Z}_p[x] \subseteq \mathbb{Z}_p(x)$ el campo de fracciones infinito y $\mathbb{Z}_p[x]$ es subanillo. Además $\mathbb{Z}_p \subseteq \mathbb{Z}_p[x]$ subanillo. ■

$R[x]$ es comunmente llamado el anillo de todos los polinomios sobre $R$ en una variable si $A = R[x]$, entonces $A[y]$ es llamado el anillo de todos los polinomios

sobre $R$ en dos variables $x$ e $y$ y es denotado por $R[x, y]$.

Por inducción se puede formar el anillo conmutativo $R[x_1, \ldots, x_n]$ de todos los polinomios en $n$ variables con coeficientes en $R$. Además como $R$ es dominio entero, entonces $R[x_1, \ldots, x_n]$ también lo será.

## 2.3. Máximo común divisor.

**Teorema 2.3.1 (Algoritmo de la división.)**
Si $K$ es un campo y $f(x), g(x) \in K[x]$ con $f(x) \neq 0$ entonces existen polinomios $q(x), r(x) \in K[x]$ tal que

$$g(x) = q(x)f(x) + r(x) \text{ tal que } r(x) = 0 \text{ o } grad(r) < grad(f).$$

***Demostración.***

Existencia de $q(x)$ y $r(x)$.

a) Si $f(x)|g(x)$, entonces $g(x) = q(x)f(x)$ y definimos $r(x) = 0$.

b) Si $f(x) \nmid g(x)$ considere el conjunto {De todos los polinomios no cero de la forma $g(x) - q(x)f(x)$ donde $q \in K[x]$}; ahora por último axioma de los números enteros existe un polinomio $r$ tal que el grado de $r$ es menor que el grado de todos los elementos de este conjunto. $r(x) = g(x) - q(x)f(x)$, entonces $g(x) = q(x)f(x) + r(x)$, entonces por demostrar $grad(r) < grad(f)$.

Sea $f(x) = s_n x^n + \cdots + s_1 x + s_0$ y $r(x) = t_m x^m + \cdots + t_0$ sabemos que $s_n \neq 0$ en $K$. Por lo tanto es unidad, entonces existe $s_n^{-1} \in K$.

Suponga $grad(r) \geq grad(f)$, definimos

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x) \in K[x].$$

Observemos que $h(x) = 0$ ó $grad(g) < grad(r)$. Si $h(x) = 0$, entonces $g = (t_m s_n^{-1} x^{m-n})f(x)$ pero eso es una contradicción ya que $f$ no divide a $g$. Pero si $h \neq 0$, tenemos que $grad(h) < grad(r)$ además $g(x) - q(x)f(x) = r(x) = h(x) + t_m s_n^{-1} x^{m-n} f(x)$, entonces $h(x) = g(x) - (q(x) + t_m s_n^{-1} x^{m-n})f(x) \in \{g(x) - q(x)f(x) \neq 0 : q \in K[x]\}$ pero esto contradice la minimalidad de $r(x)$. Por lo tanto $grad(r) < grad(f)$.

Unicidad. Sea $g(x) = q'(x)f(x) + r'(x)$ donde el $grad(r') < grad(f)$, entonces $(q(x) - q'(x))f(x) = r'(x) - r(x)$ si $r'(x) \neq r(x)$ tenemos que:

$$grad[(q(x) - q'(x))f(x)] = grad(q(x) - q'(x)) + grad(f) \geq grad(f)$$

pero $grad(r'(x) - r(x)) \leq max\{grad(r'), grad(r)\} < grad(f)$, pero esto es una contradicción.

Por lo tanto $r'(x) = r(x)$, entonces $(q(x) - q'(x))f(x) = 0$, con $f(x) \neq 0$ por ser dominio entero tenemos que $q(x) - q'(x) = 0$, por lo tanto $q'(x) = q(x)$. ■

**Definición 2.3.1**
Si $f(x)$ y $g(x)$ son polinomios en $K[x]$, donde $K$ es un campo, los polinomios $q(x)$ y $r(x)$ son llamados cociente y residuo de dividir $g(x)$ entre $f(x)$.

**Corolario 2.3.1**
Sea $R$ un anillo conmutativo y sea $f(x) \in R[x]$ mónico, si $g(x) \in R[x]$, entonces existen $q(x), r(x) \in R[x]$ con

$$g(x) = q(x)f(x) + r(x)$$

donde $r(x) = 0$ o $grad(r(x)) < grad(f(x))$.

***Demostración.*** En el teorema anterior se usó el hecho de que el coeficiente principal de $f(x)$ ($s_n \neq 0$) y de que además tenía inverso, pero como $f$ es mónico, entonces $s_n = 1$. Por lo tanto $t_m s_n^{-1} \in R$ y la demostración se sigue de la misma forma. ■

**Definición 2.3.2**
Si $f(x) \in K[x]$, $K$ campo, entonces una raíz de $f(x)$ en $K$, es un elemento $a \in K$ tal que $f(a) = 0$.

**Ejemplo 54**
Si $f(x), g(x) \in R[x]$ con $R$ anillo conmutativo. Sea $a(x) = f(x) + g(x)$ y $m(x) = f(x)g(x)$ la evaluación $a(a) = f(a) + g(a)$ y $m(a) = f(a)g(a)$.

**Lema 2.3.1**
Sea $f(x) \in K[x]$, donde $K$ es un campo y sea $a \in K$, existe un $q(x) \in K[x]$ tal que

$$f(x) = q(x)(x - a) + f(a).$$

***Demostración.*** Por el algoritmo de la división, existe $q(x)$ y $r(x)$ tal que

$$f(x) = q(x)(x - a) + r(x) \text{ y } grad(r(x)) < grad(f(x)) \text{ o } r(x) = 0$$

por lo tanto $r(x) = 0$ o el grado de $r(x)$ es cero, por lo tanto $r(x)$ es un polinomio constante; ahora $f(a) = r(a)$, entonces $r(x) = f(a)$ es constante. Por lo tanto

$$f(x) = q(x)(x - a) + f(a).$$

■

**Proposición 2.3.1**
Si $f(x) \in K[x]$, $K$ campo, entonces $a$ es raíz de $f(x)$ en $K$ si y sólo si $(x-a)|f(x)$ en $K[x]$.

***Demostración.*** Directa del lema anterior. ■

**Teorema 2.3.2**
Sea $K$-campo, $f(x) \in K[x]$, entonces si $f(x)$ tiene grado $n$, entonces $f(x)$ tiene a lo más $n$-raíces en $K$.

***Demostración.*** Por inducción sobre $n \geq 0$. En el caso base tenemos que si $n = 0$, entonces $f(x)$ es una constante distinta de cero. Por lo tanto el número de raíces es cero.

Si $f(x)$ no tiene raíces en $K$, tenemos que $0 \leq n$.

Supongamos que existe $a \in K$ tal que $f(a) = 0$ si y sólo si $f(x) = q(x)(x - a)$ más aun $q(x) \in K[x]$ es de grado $(n - 1)$.

Si hay una raíz $b \in K$ de $f(x)$ con $b \neq a$, entonces

$$0 = f(b) = q(b)(b - a), \text{ entonces } q(b) = 0$$

Por lo tanto $b$ es raíz $q(x)$ y a lo más hay $(n-1)$ raíces de $q$ en $K$, por hipótesis de inducción. Por lo que $f(x)$ tiene a lo más $n$-raíces en $K$. ■

**Ejemplo 55**
El teorema es falso si $R$ es un anillo conmutativo arbitrario.

$$x^2 - 1 \in \mathbb{Z}_8[x] \text{ tiene 4 raíces y estas son } [1], [3], [5], [7].$$

**Corolario 2.3.2**
Sea $K$ un campo infinito y sean $f(x)$ y $g(x)$ polinomios en $K[x]$. Si $f(x)$ y $g(x)$ determinan la misma función polinomial ($f(a) = g(a)$ para todo $a \in K$), entonces $f(x) = g(x)$.

***Demostración.*** Si $f(x) \neq g(x)$, entonces $h(x) = f(x) - g(x) \neq 0$. Sea $n = grad(h(x))$, con $f(a) = g(a)$ para todo $a \in K$, y tenemos que $a$ es raíz de $h(x)$ para todo $a \in K$ y puesto que es infinito, entonces $h(x)$ tiene más raíces de $n$, pero es una contradicción. Por lo tanto $f(x) = g(x)$ como polinomios en $K[x]$. ■

**Corolario 2.3.3**
Sea $K$ un campo (probablemente finito). Si $f(x), g(x) \in K[x]$, si $grad(f) \leq grad(g) \leq n$ y si $f(a) = g(a)$ para $n+1$ elementos $a \in K$, entonces $f(x) = g(x)$ en $K[x]$, lo cual no puede ser.

***Demostración.*** Si $f(x) \neq g(x)$, entonces $grad(f(x) - g(x))$ está definido y $grad(f(x) - g(x)) \leq n$ y tiene $n + 1$ raíces en $K$, lo cual no puede ser. ■

**Observación 43**
Un grupo finito es cíclico si y sólo si para cada divisor de $|G|$ hay a lo más un subgrupo de ese orden.

**Teorema 2.3.3**
Si $K$ es un campo y $G$ es un subgrupo finito del grupo multiplicativo $K^\times$, entonces $G$ es cíclico. En particular, si $K = \mathbb{Z}_p$, entonces $K^\times$ es cíclico.

***Demostración.*** Sea $d\big||G|$. Sean $S$ y $T$ dos subgrupos de $G$ de orden $d$ distintos, entonces $|S \cup T| > d$, además para toda $a \in S \cup T$ $a^d = 1$ por lo tanto el polinomio $x^d - 1 \in K[x]$ tiene más de $d$ raíces, pero es una contradicción. Por lo tanto para cada divisor $d\big||G|$ a lo más hay un subgrupo de $G$ con ese orden. ■

**Definición 2.3.3**
Si $K$ es campo finito, un generador del grupo $K^\times$ es llamado elemento primitivo de $K$.

**Definición 2.3.4**
Si $f(x), g(x) \in K[x]$, $K$ campo, entonces $c \in K[x]$ es un divisor común si tenemos que $c(x)|f(x)$ y $c(x)|g(x)$. Si $f(x)$ y $g(x)$ en $K[x]$ no son ambos cero, definimos el máximo común divisor, abreviado como MCD, como el polinomio mónico que es común divisor de mayor grado. La notación que usaremos será $\text{MCD}\{f, g\} := (f, g)$. Si $f = 0 = g$, $(f, g) = 0$.

**Teorema 2.3.4**
Sea $K$ campo y $f(x), g(x) \in K[x]$, entonces su MCD $d(x)$ es una combinación lineal de $f(x)$ y $g(x)$; es decir, hay $s(x), t(x) \in K[x]$ con

$$d(x) = s(x)f(x) + t(x)g(x).$$

La demostración se verá en Dominios de Ideales Principales.

**Corolario 2.3.4**
Sea $K$ un campo y sea $f(x), g(x) \in K[x]$. Un divisor mónico común $d(x)$ es el MCD si y sólo si es divisible por cualquier divisor común; esto es, $c(x)$ es un divisor común, entonces $c(x)|d(x)$. Más aun el MCD es único.

***Demostración.*** Tenemos que $d(x) = s(x)f(x) + t(x)g(x)$. Ahora si $c(x)|f(x)$ y $c(x)|g(x)$ en $K[x]$, entonces $c(x)|d(x)$. La suficiencia por la definición queda probado. Para demostrar la unicidad tenemos que $d'(x)|d(x)$ y $d(x)|d'(x)$, entonces $d(x) = v(x)d'(x)$ y $d'(x) = u(x)d(x)$, por lo que $d'(x) = u(x)v(x)d'(x)$, luego $u(x)v(x) = 1$. Por lo que $u$ y $v$ son unidades. Finalmente y puesto que $d$ y $d'$ son mónicos, tenemos que $u = v = 1$, por lo que $d = d'$. ■

**Definición 2.3.5**
Un elemento $p$ en un dominio es irreducible si $p$ ni es 0 ni es unidad, en cualquier factorización $p = uv \in R$, $u$ es unidad o $v$ es unidad. Los elementos $a, b \in R$ son asociados si hay una unidad $u \in R$ con $b = ua$.

**Proposición 2.3.2**
Si $K$ es campo, entonces un polinomio $p(x) \in K[x]$ es irreducible si y sólo si $grad(p) = n \geq 1$ y no tiene factorización en $K[x]$ de la forma $p(x) = g(x)h(x)$ donde los grados de $h(x)$ y $g(x)$ son ambos menores que $n$.

***Demostración.*** Veamos que $h(x) \in K[x]$ es unidad si y sólo si $grad(h(x)) = 0$. Si $h(x)u(x) = 1$, entonces $grad(h(x))+grad(u(x)) = 0$, por lo cual $grad(h(x)) = 0$. Si $grad(h(x)) = 0$, entonces $h(x)$ es una constante no cero en $K$ y es una unidad.

Si $p$ es irreducible y $p(x) = g(x)h(x)$, entonces $g$ es unidad ó $h$ es unidad, por lo que $grad(h) = n$ ó $grad(g) = n$.

Ahora, si $p$ no es irreducible, entonces $p(x) = g(x)h(x)$ para el cual $g(x)$ y $h(x)$ no son unidades, entonces $g(x)$ y $h(x)$ no tienen grado cero; por lo tanto tienen grado positivo menores que $n$. ■

**Ejemplo 56**
Como podemos ver

$$2x - 2 = 2(x - 1) \in \mathbb{Z}[x]$$

no es irreducible ya que 2 no es unidad en $\mathbb{Z}$.

**Ejemplo 57**
El polinomio $x^2 + 1 \in \mathbb{R}[x]$ es irreducible pero en $\mathbb{C}[x]$ tenemos que $x^2 - 1 = (x - i)(x + i)$.

**Corolario 2.3.5**
Sea $K$ un campo y sea $f(x) \in K[x]$ un polinomio cuadrático o cúbico. Entonces $f(x)$ es irreducible en $K[x]$ si y sólo si $f(x)$ no tiene raíces en $K$.

***Demostración.*** Si $f(x) = g(x)h(x)$ y $g, h$ son ambos de grado menor que $f(x)$ si y sólo si al menos uno de los dos tiene grado 1 si y sólo si $f(x)$ tiene al menos una raíz en $K$. ■

**Ejemplo 58**
Esto es falso para el polinomio de grado 4.

$$(x^2 + 1)^2 = x^4 + 2x^2 + 1$$

no tiene raíces en $\mathbb{R}[x]$

**Lema 2.3.2**
Sea $K$ un campo y $p(x), f(x) \in K[x]$, y sea $d(x) = (p, f)$ su MCD. Si $p(x)$ es un polinomio mónico irreducible, entonces

$$d(x) = \begin{cases} 1 \text{ si } p(x) \nmid f(x) \\ p(x) \text{ si } p(x)|f(x). \end{cases}$$

***Demostración.*** Si $d|p$ con $d = (p, f)$ mónico y $p(x)$ también mónico. Sea $p = dq$, si $d$ es unidad, entonces $d = 1$ por ser mónico. Si $q$ es unidad, puesto que $p$ y $d$ son mónicos, comparando los coeficientes principales, tenemos que $q = 1$ de donde $d = p$. Por lo que, entonces $d = 1$ ó $d = p$.

Si $p \nmid f$, entonces $q$ no es unidad, pues de lo contrario $p|d|f$, pero es una contradicción. Por lo tanto $d$ es una unidad y $d = 1$.

Ahora si, $p|f$, entonces $p|d$ lo cual implica $d$ no es una unidad. Por lo tanto $q$ es unidad, entonces $d = p$. ■

**Teorema 2.3.5 (Lema de Euclides)**
Sea $K$ un campo, y sean $f(x), g(x) \in K[x]$. Si $p(x)$ es un polinomio irreducible en $K[x]$, y $p(x)|f(x)g(x)$, entonces

$$p(x)|f(x) \text{ o } p(x)|g(x)$$

más generalmente, si $p(x)|f_1 \dots f_n$,entonces $p(x)|f_i$ para algún $i$.

***Demostración.*** Suponga que $p|fg$ y $p \nmid f$, entonces $(p, f) = 1$ luego entonces $1 = sp + tf$ para algún $s, t \in K[x]$. Por lo tanto

$$g = spg + t(fg) = spg + ph$$

para $h \in K[g]$, por lo tanto $p|g$. ■

**Definición 2.3.6**
Si $f, g \in K[x]$ con $K$ campo son llamados primos relativos si $(f, g) = 1$.

**Corolario 2.3.6**
Sean $f, g, h \in K[x]$ con $K$ un campo, si $f$ y $h$ son primos relativos y $h|fg$, entonces $h|g$.

***Demostración.*** Tenemos que $(h, f) = 1$, entonces $1 = hs + ft$ para $s, t \in K[x]$ luego entonces $g = hsg + fgt$ como $h|fg$, por lo tanto $h|g$. ■

**Definición 2.3.7**
Si $K$ es un campo, una función racional $f/g \in K(x)$ es la fracción reducida si $f, g$ son primos relativos.

**Proposición 2.3.3**
Sea $K$ un campo, con $0 \neq f/g \in K(x)$. $f/g$ se puede reducir a su mínima expresión (fracción reducida).

***Demostración.*** Sea $d = (f, g)$, entonces $f = df'$ y $g = dg'$. Observe que $d = sdf' + tdg'$, por lo cual $1 = sf' + tg'$ en $K(x)$, por lo tanto $(f', g') = 1$ y $f'/g'$ es la fracción reducida. ■

**Teorema 2.3.6 (Algoritmo de Euclides.)**
Sea $K$-campo y $f(x), g(x) \in K[x]$. Existen algoritmos para calcular $(f, g)$ y para encontrar $s(x), t(x) \in K[x]$ tal que

$$d(x) = s(x)f(x) + t(x)g(x)$$

***Demostración.***

$$\begin{aligned}
g &= q_1 f + r_1 \\
f &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Los grados de los residuos son estrictamente decrecientes, el procedimiento se termina en un número finito de pasos. Se asegura que $d = r_n$ una vez que se hace mónico. Por sustitución hacia atrás se puede observar que $d|f$ y $d|g$. Sea $c$ divisor común de $f, g$ por sustitución de arriba hacia abajo podemos observar que $c|r_i$ para todo $i$, en particular $c$ divide a $r_n$.

Para hallar $s$ y $t$ sustituimos de abajo hacia arriba. Es decir:

$$\begin{aligned}
r_n = r_{n-2} - q_n r_{n-1} =& r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) \\
=& (1 - q_{n-1}) r_{n-2} - q_n r_{n-3} \\
=& (1 - q_{n-1})(r_{n-4} - q_{n-2} r_{n-3}) - q_n r_{rn-3} \\
&\vdots \\
=& sf + tg
\end{aligned}$$

■

**Corolario 2.3.7**
Sea $k$ un subcampo de $K$, entonces $k[x]$ es subanillo de $K[x]$. Si $f, g \in k[x]$, entonces $(f, g) \in k[x]$ es igual al $(f, g) \in K[x]$.

***Demostración.*** Observe que existen únicos $Q, R \in K[x]$, $g = Qf + R$ (algoritmo de la división) en $K[x]$, analogamente existen únicos $q, r \in k[x]$ tal que $g = qf + r$ (algoritmo de la división) en $k[x]$, pero $g = qf + r$ es válido en $K[x]$ y por la unicidad de $Q$ y $R$, entonces $q = Q$ y $r = R$ ambos en K[x].

Por lo que las ecuaciones del algoritmo de Euclides en $K[x]$ son las mismas que $k[x]$. Por lo tanto En ambos anillos se obtiene el mismo $(f, g)$. ■

**Teorema 2.3.7 (Unicidad de la factorización.)**
Si $K$ es campo todo polinomio $f(x) \in K[x]$ de grado mayor o igual a 1 es producto de constantes diferentes del cero y polinomios irreducibles mónicos. Más aun si $f(x)$ tiene 2 factorizaciones $f(x) = ap_1(x)\cdots p_m(x)$ y $f(x) = bq_1(x)\cdots q_n(x)$, entonces $a = b$, $m = n$ y $p_i = q_i$ para todo $i$.

***Demostración.*** Existencia. Por inducción en $grad(f) \geq 1$. En el caso base tenemos que si $grad(f) = 1$, entonces $f(x) = ax + b = a(x + ba^{-1})$. Ahora vamos a asumir que $grad(f) \geq 1$. Si $f(x)$ es irreducible y $a$ es su coeficiente principal, entonces $f(x) = a(a^{-1}f(x))$ en donde el último factor es mónico e irreducilbe.

Si $f(x)$ no irreducible, entonces $f(x) = g(x)h(x)$ en donde $grad(g)$, $grad(h) < grad(f)$ ambos por inducción, tienen factorizaciones $g(x) = bp_1(x)\cdots p_m(x)$ y $cq_1(x)\cdots q_n(x)$ donde $p, q$ son mónicos irreducibles, entonces

$$f(x) = (bc)p_1(x)\cdots p_m(x)q_1(x)\ldots q_n(x).$$

Unicidad. Por inducción en $M = max\{m, n\}$

$$f(x) = ap_1(x)\cdots p_m(x) = bq_1(x)\cdots q_n(x)$$

Para el caso base tenemos que si $M = 1$ entonces el polinomio $f(x) = ap_1(x) = bq_1(x)$.

$f(x) = ap_1(x)$, entonces el coeficiente principal de $f$ es $a$; $f(x) = bq_1(x)$, entonces el coeficiente principal de $f$ es $b$; entonces por lo anterior $a = b$ por lo tanto $p_1 = q_1$.

Para $M \geq 1$. Observe que $p_m|q_1\ldots q_n$. Por lema de Euclides se tiene que existe un $i$ tal que $p_m|q_i$ pero $q_i$ es mónico irreducible, entonces $p_m = q_i$ reindexando, podemos escribir $p_m = q_n$ y cancelando obtenemos que

$$ap_1(x)\ldots p_{m-1}(x) = bq_1(x)\ldots q_{n-1}$$

por hipótesis inductiva $a = b$ y $m-1 = n-1$ por lo tanto $m = n$ y reindexando $p_i = q_i$ con $i = 1\ldots m-1$. ■

Sea $K$ campo, asumimos que existen $a_1, r_1, \ldots, r_n \in K$ tales que

$$f(x) = a\prod_{i=1}^{n}(x - r_i)$$

si $r_1, \ldots, r_s$ con $s \leq n$ son las raíces distintas de $f$ entonces $f(x) = a(x - r_1)^{e_1}\ldots(x - r_s)^{e_s}$ con $r_j$ raíces distintas, $e_j \geq 1$ con $e_j$ multiplicidad de la raíz

$r_j$. Por la factorización única la multiplicidad de raíces está bien definida.

Sabemos que si $f(x) \in K[x]$ tiene una raíz $r \in K$, entonces $f(x) = (x-r)g(x) \in K[x]$. Por lo tanto $f$ no es irreducible. En el caso de polinomios de grado 2 y 3 ($f$ es irreducible si y sólo si no tiene raíces en $K[x]$).

**Teorema 2.3.8**
Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Toda raíz racional de $f$ tiene la forma $\frac{b}{c} \in \mathbb{Q}$ en donde $b|a_0$ y $c|a_n$.

***Demostración.*** Sea $r = \frac{b}{c}$ tal que $(b, c) = 1$ sustituyendo $r$ obtenemos que

$$0 = f(r) = a_0 + a_1\left(\frac{b}{c}\right) + \cdots + a_n\left(\frac{b}{c}\right)^n$$

multiplicado por $c^n$,

$$0 = a_0c^n + a_1bc^{n-1} + a_2b^2c^{n-2} + \cdots + a_{n-1}b^{n-1}c + a_nb^n$$

entonces $a_nb^n = -(a_0c^{n-1} + a_1bc^{n-2} + a_2b^2c^{n-3} + \cdots + a_{n-1}b^{n-1})c$ entonces $c|a_nb^n$. $(b, c) = 1$, luego $(b^n, c) = 1$, entonces tenemos que $c|a_n$; además $a_0c^n = -(a_1c^{n-1} + c_2bc^{n-2} + \cdots + a_{n-1}b^{n-2}c + a_nb^{n-1})b$ por lo tanto $b|a_0c^n$. Ahora $(b, c) = -1$, luego $(b, c^n) = 1$, por lo tanto $b|a_0$. ■

**Definición 2.3.8**
Un número complejo $\alpha \in \mathbb{C}$ es llamado entero algebraico si $\alpha$ es raíz de un polinomio mónico $f(x) \in \mathbb{Z}[x]$.

Es claro que cualquier número algebraico $z \in \mathbb{C}$ que es raíz de $g \in \mathbb{Q}[x]$ es necesariamente una raíz de un polinomio $h(x) \in \mathbb{Z}[x]$.

Por supuesto, cualquier $z \in \mathbb{Z}$ es un entero algebraico pues es raíz de $x - z \in \mathbb{Z}[x]$ para contrastar los elementos en $\mathbb{Z}$ con los enteros algebraicos en general, llamaremos a los elementos de $\mathbb{Z}$ enteros racionales.

**Corolario 2.3.8**
Un número racional $z$, que es un entero algebraico debe estar en $\mathbb{Z}$. Es decir, si $f \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ es mónico, toda raíz racional de $f$ es un entero que divide al término constante.

***Demostración.*** Si $f = a_0 + a_1x + \cdots + a_nx^n$ es mónico, entonces $a_n = 1$ por el teorema anterior, las raíces racionales de $f$ son los divisores de $a_0$. ■

**Ejemplo 59**
$f(x) = x^3 + 4x^2 - 2x - 1 \in \mathbb{Q}[x]$ (es irreducible si y sólo si no tiene raíces racionales) las únicas posibles raíces son $\pm 1$ pero $f(1) = 2$ y $f(-1) = 4$. Por lo tanto $f$ no tiene raíces en $\mathbb{Q}$, entonces $f$ es irreducible en $\mathbb{Q}[x]$.

## 2.4. Homomorfismos

Al igual que en grupos, los homomorfismos son utilizados para comparar anillos conmutativos.

**Definición 2.4.1**
Si $A, R$ anillos conmutativos. Entonces $f : A \to R$ una función es homomorfismo de anillos si:

i) $f(1) = 1$.

ii) $f(a + a') = f(a) + f(a')$, para todo $a, a' \in A$.

iii) $f(aa') = f(a)f(a')$, para todo $a, a' \in A$.

**Observación 44**
Si $f : A \to R$ es biyección decimos que $f$ es un isomorfismo de anillos y $A \cong R$ son isomorfos como anillos.

**Ejemplo 60**
Sea $R$ un dominio entero y $F$ su campo de fracciones. Se dijo que $R$ es subanillo de $F$ (lo cual no es cierto).

$$F = \{[a, b] : a, b \in R \text{ y } b \neq 0\}$$

Recordemos que $[a, b] = [c, d]$ si y sólo si $ad = bc$, $\hat{1} = [1, 1]$, $[a, b] + [c, d] = [ad + bc, bd]$,$[a, b][c, d] = [ac, bd]$. Y $R$ se identificó con $R' = \{[a, 1] : a \in R\} \subseteq F$. Se puede ver facilmente que la función $f : R \to R'$ dada por $f(a) = [a, 1]$ es un isomorfismo.

**Ejemplo 61**
Cuando un elemento en un anillo conmutativo $R$ es identificado con un polinomio constante, esto es, $r$ es identificado con $(r, 0, 0, \dots)$, implicamos que $R$ es un subanillo de $R[x]$. El subconjunto $R' = \{(r, 0, 0, \dots) : r \in R\}$ es un subanillo de $R[x]$, como podemos ver la función $f : R \to R' \subseteq R[x]$, definida por $f(r) = (r, 0, 0, \dots)$, es un isomorfismo.

**Lema 2.4.1**
Si $f : A \to R$ es un homomorfismo de anillos, entonces para todo $a \in A$, con $a$ diferente de cero, se tiene que:

i) $f(a^n) = f(a)^n$ para todo $n \geq 0$;

ii) Si $a$ es una unidad, entonces $f(a)$ es una unidad y $f(a^{-1}) = f(a)^{-1}$; es una unidad, entonces $f(a^{-n}) = f(a)^{-n}$ para todo $n \geq 1$;

iii) Si $f : A \to R$ es un homomorfismo de anillos, entonces

$$f(U(A)) \leq U(R),$$

donde $U(A)$ es el grupo de las unidades de $A$; si $f$ es un isomorfismo, entonces

$$U(A) \cong U(R).$$

***Demostración.*** i) Por inducción en $n \geq 0$. ii) Si $a$ una unidad en $A$, entonces existe $b = a^{-1}$ tal que $ab = 1$ por lo cual $1 = f(1) = f(ab) = f(a)f(b)$ por lo tanto $f(b) = f(a)^{-1}$. La segunda parte es por inducción sobre $n \geq 1$. ii) implica iii) ya que si $a \in U(A)$, entonces $f(a) \in U(R)$, si $f$ es isomorfismo, sabemos que $f(U(A)) \subseteq U(R)$. Si $r \in U(R)$ existe un $r' \in R$ tal que $rr' = 1$ y como $f$ es sobreyectiva, entonces existen $a, a' \in A$ tal que $f(a) = r$ y $f(a') = r'$ además $f(aa') = f(a)f(a') = 1$, entonces $aa' = 1$ por ser $f$ inyectiva. Por lo tanto $a \in U(A)$. Por lo tanto $f(U(A)) = U(R)$. ■

**Proposición 2.4.1**
Si $R$ y $S$ anillos conmutativos y $\varphi : R \to S$ homomorfismo de anillos. Entonces existe un homomorfismo de anillos $\varphi^* : R[x] \to S[x]$ dado por

$$\varphi^* : r_0 + r_1x + r_2x^2 + \ldots \mapsto \varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \ldots$$

**Definición 2.4.2**
Si $f : A \to R$ es un homomorfismo de anillos, entonces el núcleo está definido como

$$kerf = \{a \in A \text{ con } f(a) = 0\}$$

y su imagen es

$$imf = \{r \in R : r = f(a) \text{ para algún } a \in A\}.$$

**Observación 45**
Si omitimos las multiplicaciones en los anillos; $A$ y $R$ son grupos abelianos con respecto a la suma y las definiciones coinciden con la teoría de grupos.

**Ejemplo 62**
Sea $e_a : K[x] \to K$ definida como $f(x) \to f(a)$. Podemos ver que es homomorfismo de anillos; es sobreyectiva dado $b \in K$ y $f(x) = x - a + b \to b$ y

$$ker\ e_a = \{f(x) : f(a) = 0\}; \text{ es decir polinomios donde } a \text{ es una raíz.}$$

Si $f : H \to G$ es homomorfismo de grupos, entonces $kerf \trianglelefteq H$.

Si $f : A \to R$ es de anillos $kerf$ es casi un subanillo; sin embargo si $R \neq 0$, entonces $1 \notin kerf$ ya que $f(1_A) = 1_R \neq 0$. $kerf$ es cerrado bajo multiplicación.

**Definición 2.4.3**
Un ideal $I \leq R$ en un anillo conmutativo $R$:

i) $0 \in I$;

ii) Si $a, b \in I$, entonces $a + b \in I$;

iii) Si $a \in I$ y $r \in R$, entonces $ra \in I$.

**Ejemplo 63**
Los anillos $\{0\}$ y $R$ son ideales triviales de $R$.

Si $I \neq R$, diremos que $I$ es un ideal propio.

**Ejemplo 64**
Sean $b_1, \ldots, b_n \in R$ un anillo conmutativo. Y sea

$$I = \{r_1 b_1 + \cdots + r_n b_n : r_i \in R \text{ para todo } i\}$$

las combinaciones lineales de $b_i$ en $R$. Entonces, $I \leq R$ ideal, decimos que $I = \langle b_1, \ldots, b_n \rangle$ el ideal generado por $b_i$.

**Definición 2.4.4**
En particular si $I = \langle b \rangle = \{rb : r \in R\}$ este será llamado ideal principal.

**Observación 46**
$R = (1)$ y $\{0\} = (0)$

**Ejemplo 65**
El subconjunto $\{z \in \mathbb{Z} : z \text{ es un número par}\} \leq \mathbb{Z}$ es un ideal principal.

**Proposición 2.4.2**
Si $f : A \to R$ es homomorfismo de anillos, entonces $kerf \leq A$ es un ideal y $imf \subseteq R$ subanillo; además si $A \neq 0 \neq R$, entonces $kerf \lneqq A$ propio.

***Demostración.*** i) $kerf \leq A$ es subgrupo aditivo de $A$; por lo tanto contiene al cero y es cerrado, además si $a \in A$ y $b \in kerf$, entonces $f(ab) = f(a)f(b) = f(a)f(0) = 0$ , por lo tanto $ab \in kerf$. Además si $A \neq 0 \neq R$, entonces $1 \neq 0$ y $1 \neq kerf$. Por lo tanto es ideal propio.

ii) $imf \leq R$ es subanillo. Tenemos $f(1_A) = 1_R \in imf$. Ahora si $r_1, r_2 \in imf$, entonces $r_1 = f(a_1)$ y $r_2 = f(a_2)$, entonces $r_1 r_2 = f(a_1)f(a_2) = f(a_1 a_2) \in imf$, además

$$r_1 - r_2 = f(a_1) - f(a_2) = f(a_1) + f(-a_2) = f(a_1 - a_2) \in imf.$$

Observe que $f(0) = f(0+0) = f(0)+f(0)$, entonces $f(0) = 0$ y $0 = f(a+(-a)) = f(a) + (f(-a))$ por lo tanto $f(-a) = -f(a)$ ■

**Proposición 2.4.3**
Sea $R$ un anillo conmutativo. Si $I \leq R$ es un ideal tal que $u \in I$ para $u \in R$ una unidad, entonces $I = R$.

***Demostración.*** Si $u \in R$ unidad, entonces existe $v \in R$ tal que $uv = 1 \in I$ además para todo $r \in R$ tenemos que $r = r1 \in I$, por lo tanto $R \subseteq I$. ■

**Proposición 2.4.4**
Sea $K$ un anillo conmutativo. $K$ es campo si y sólo si sus únicos ideales son los ideales triviales.

***Demostración.*** Necesidad. Si $K$ es un campo. Sea $I \leq K$ un ideal, si $I = 0$ no hay nada que probar. Ahora supongamos $I \neq \{0\}$, entonces existe $0 \neq a \in I \subseteq K$ con $K$ un campo, entonces $a$ es una unidad por lo tanto $I = K$.

Suficiencia. Sea $0 \neq a \in K$, entonces $\langle a \rangle \neq 0$ por lo tanto $\{ka : k \in K\} = \langle a \rangle = K$ y $1 \in K$ por lo cual existe $k \in K$ tal que $ka = 1$, por lo tanto $a$ es unidad, entonces $K$ es campo. ■

**Proposición 2.4.5**
Sea $f : A \to R$ homomorfismo de anillos, $f$ es inyectiva si y sólo si $kerf = \{0\}$.

***Demostración.*** Necesidad. Si $f$ es inyectiva. Sea $a \in kerf$, entonces $f(a) = 0$ además $f(0) = 0$ por lo tanto $f(a) = f(0)$, por lo tanto $a = 0$.

Suficiencia. Si $kerf = \{0\}$; sea $f(a) = f(b)$, entonces $f(a-b) = f(a) - f(b) = 0$, entonces $a - b = 0$ por lo tanto $a = b$. ■

**Corolario 2.4.1**
Si $f : K \to R$ homomorfismo de anillos. K un campo y $R \neq 0$ un anillo conmutativo, entonces $f$ es inyectivo.

***Demostración.*** Si $kerf = \{0\}$ ó $kerf = \{K\}$ pero $R \neq 0$, entonces $kerf \lneqq K$ propio. Por lo tanto $kerf = \{0\}$ si y sólo si $f$ es inyectivo. ■

**Teorema 2.4.1**
Si $K$ es un campo, todo ideal $I$ de $K[x]$ son ideales principales. Además, si $I \neq \{0\}$, existe un polinomio mónico que genera a $I$.

***Demostración.*** Sea $K$ un campo, entonces $K[x]$ es un dominio entero euclidiano. En la siguiente sección se demostrará que dominio euclidiano implica dominio de ideales principales. ■

**Definición 2.4.5**
Sea $R$ un dominio entero esté será llamado un dominio de ideales principales si todos los ideales de $R$ son principales.

**Ejemplo 66**
Los conjuntos $\mathbb{Z}$ y $K[x]$ son ejemplos de dominios de ideales principales.

***Demostración.*** $\mathbb{Z}$ es dominio de ideales principales.

Sea $0 \neq I \neq \mathbb{Z}$ un ideal propio y sea $n = min\{m \in I : 0 < m\}$. Afirmamos que $I = \langle n \rangle$. Es claro que $\langle n \rangle = n\mathbb{Z} \subseteq I$.

Sea $a \in I$, ahora por el algoritmo de la división tenemos que $a = ln + r$ con $0 \leq r < n$, observe que $r = a - ln \in I$ y por la minimalidad de $n$ se tiene que $r = 0$. Por lo tanto $a = ln$ para algún $l \in \mathbb{Z}$, entonces $a \in \langle n \rangle$ por lo tanto $I = \langle n \rangle$ es ideal principal. ■

**Definición 2.4.6**
Un dominio euclidiano es un dominio entero con algoritmo de la división.

**Ejemplo 67**
Sea $I = \{f \in \mathbb{Z}[x] : \text{El término constante es par.}\} \leq \mathbb{Z}[x]$ es un ideal no principal. Observemos que $I$ es un ideal, $0 \in I$, $f + g \in I$ y $ag \in I$. Para $f, g \in I$ y $a \in Z[x]$.

Ahora suponga que $I = \langle d(x) \rangle$, tenemos que $2 \in I$, por lo cual existe $f(x) \in \mathbb{Z}[x]$ tal que $2 = f(x)d(x)$ y ahora comprobando los grados tenemos que $0 = grad(f) + grad(d)$, de aquí tenemos que $grad(d) = 0$, por lo tanto $d(x)$ es constante; y sólo tenemos como posibilidad $d = \pm 1$ y $d = \pm 2$.

Suponga $d(x) = \pm 2$, puesto que $x \in I$, entonces existe $g \in \mathbb{Z}[x]$ tal que $x = d(x)g(x) = \pm 2g(x)$ donde el coeficiente de $x$ es 1 pero del lado derecho todos los coeficientes son pares, pero esto es una contradicción. Por lo tanto $d = \pm 1$, entonces $1 \in I$, tenemos que $I = \mathbb{Z}[x]$, pero también es una contradicción. Por lo tanto $I$ no es principal.

**Definición 2.4.7**
Un elemento $\delta$ en $R$ anillo conmutativo es máximo común divisor de $\alpha, \beta \in R$ si:

i) Si $\delta$ es un divisor común de $\alpha, \beta$.

ii) Si $\gamma$ es común divisor de $\alpha$ y $\beta$, entonces $\gamma | \delta$.

$\delta$ no es único ya que $u\delta$ también es $MCD$ con $u \in U(R)$. En $\mathbb{Z}$ este es único ya que $\delta$ se exige que sea positivo y en $R[x]$ se forza a ser mónico.

**Observación 47**
Sea $R$ un dominio de ideales principales y $\pi, \alpha \in R$ con $\pi$ irreducible. Sea $\delta$ un $MCD$ de $\alpha, \pi$. En particular $\delta | \pi$ , entonces $\pi = \delta\epsilon$ irreducible, por lo tanto $\delta$ es unidad o $\epsilon$ es unidad. Por otro lado, $\alpha = \delta\beta$. Si $\delta$ no es unidad, entonces $\epsilon$ es una unidad y tenemos $\delta = \pi\epsilon^{-1}$ por lo cual $\alpha = \pi\epsilon^{-1}\beta$. Por otro lado, si $\delta$ es una unidad, entonces 1 es un $MCD$ de $\{\alpha, \pi\}$. Por lo tanto, si $R$ es un dominio de ideales principales y $\pi \in R$ es irreducible y $\alpha \in R$, entonces $\pi | \alpha$ ó 1 es un $MCD$ de $\{\alpha, \pi\}$.

**Teorema 2.4.2**
Sea $R$ un dominio de ideales principales. Entonces:

i) Cualquier $\alpha, \beta \in R$ tiene un MCD, digamos $\delta$, y $\delta = \sigma\alpha + \tau\beta$ para $\sigma, \tau \in R$.

ii)Si un elemento $\pi \in R$ irreducible divide a $\alpha\beta$, entonces $\pi|\alpha$ o $\pi|\beta$.

***Demostración.*** i) Supongamos que al menos uno de los dos ($\alpha$ o $\beta$) es distinto de cero.

Sea $I = \{\sigma\alpha + \tau\beta : \sigma, \tau \in R\}$, observemos que $\alpha, \beta \in I$, entonces $I \neq \{0\}$. Se puede ver que $I \leq R$ es ideal.

Como $R$ es un dominio de ideales principales, tenemos que $I = \langle\delta\rangle$ para $\delta \in I$, entonces por demostrar que $\delta$ es un MCD de $\{\alpha, \beta\}$ puesto que $\alpha, \beta \in I$, por lo cual $\alpha = p_1\delta$ para $p_1 \in R$ y $\beta = p_2\delta$ para $p_2 \in R$. Por lo tanto $\delta$ es un divisor común, puesto que $\delta \in I$, entonces $\delta = \sigma\alpha + \tau\beta$ para $\sigma, \tau \in R$ finalmente si $\delta$ es cualquier divisor común de $\alpha, \beta$, entonces $\alpha = \gamma\alpha'$, $\beta = \gamma\beta'$, entonces $\delta = \sigma\gamma\alpha' + \tau\gamma\beta'$ de aquí $\gamma|\delta$. Por lo tanto $\delta$ es un MCD de $\{\alpha, \beta\}$.

ii) Si $\pi|\alpha$ no hay nada que probar. Ahora si $\pi \nmid \alpha$, entonces 1 es MCD de $\{\pi, \alpha\}$, por lo cual tenemos $1 = \sigma\pi + \tau\alpha$ para $\sigma, \tau \in R$ luego de aquí $\beta = \sigma\pi\beta + \tau\alpha\beta$ entonces $\pi|\alpha\beta$ por lo tanto $\pi|\beta$. ■

Si $I, J \leq R$ son ideales, entonces $I \cap J \leq R$ es un ideal; se puede verificar que $0 \in I \cap J$, $a + b \in I \cap J$ y $ra \in I \cap J$ esto es para $a, b \in I$ y $r \in R$. En general la intersección de cualquier familia de ideales es un ideal.

**Definición 2.4.8**
Si $f, g$ son elementos en $R$, entonces un común múltiplo de $f, g$ es un elemento $m \in R$ tal que $f|m$ y $g|m$. Si $f, g$ no son ambos cero, definimos

$$c = [f, g] = MCM\{f, g\}$$

donde $c$ es un común múltiplo tal que $c|m$ para $m$ cualquier común múltiplo si $f = 0 = g$, entonces $[0, 0] = 0$.

Vea que MCM no es único si $c = [f, g]$ entonces $cu$ con $u \in U(R)$ también será MCM. Si $R$ es un dominio de ideales principales y $a, b \in R$, entonces existe $[a, b]$. Si $a = 0$, $b = 0$, entonces $[a, b] = 0$. Ahora sean $\langle a\rangle, \langle b\rangle \leq R$ ideales, con $\langle a\rangle \cap \langle b\rangle \leq R$ ideal, entonces $\langle a\rangle \cap \langle b\rangle = \langle c\rangle$. Se puede ver que $c = [a, b]$.

## 2.5. Dominios Euclidianos

**Definición 2.5.1**
Un dominio euclidiano es: Un dominio entero $R$ donde se ha definido una función

$$\partial : R - \{0\} \to \mathbb{N},$$

llamada función grado, tal que:

i) $\partial(f) \leq \partial(fg)$ para todo $f, g \in R$ con $f, g \neq 0$;

ii) Para todo $f, g \in R$ con $f \neq 0$, existe $q, r \in R$ con

$$g = qf + r,$$

donde $r = 0$ ó $\partial(r) < \partial(f)$.

Note que si $R$ tiene función grado $\partial$ que es identicamente 0, entonce $r = 0$, y tomando $g = 1$, entonces todo elemento tiene inverso. Por lo tanto $R$ es un campo.

**Ejemplo 68**
Los enteros $\mathbb{Z}$ es un dominio euclidiano con función grado $\partial(m) = |m|$. En $\mathbb{Z}$, tenemos

$$\partial(mn) = |mn| = |m||n| = \partial(m)\partial(n)$$

**Ejemplo 69**
Cuando $k$ es un campo, el dominio $k[x]$ es un dominio euclidiano con la función usual grado para polinomios no nulos. En $k[x]$, tenemos

$$\begin{aligned} \partial(fg) &= deg(fg) \\ &= deg(f) + deg(g) \\ &= \partial(f) + \partial(g). \end{aligned}$$

Si $\partial$ es multiplicativa, como sucedió en el caso de $\mathbb{Z}$, $\partial$ recibe el nombre de norma.

**Ejemplo 70**
En los enteros Gaussianos $\mathbb{Z}[i]$ forman un dominio euclidiano cuya función grado:

$$\partial(a + bi) = a^2 + b^2 \text{ es una norma.}$$

Para ver que $\partial$ es una norma, primero observe si $\alpha = a + bi$, entonces

$$\partial(\alpha) = \alpha\overline{\alpha},$$

donde $\overline{\alpha} = a - bi$ es el conjugado complejo de $\alpha$, entonces $\partial(\alpha\beta) = \partial(\alpha)\partial(\beta)$ para todo $\alpha, \beta \in \mathbb{Z}[i]$, pues

$$\partial(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \partial(\alpha)\partial(\beta);$$

Ahora tenemos que si $\beta = c + id \in \mathbb{Z}[i]$, y si $\beta \neq 0$, entonces $1 \leq \partial(\beta)$, por lo tanto $\partial(\alpha) \leq \partial(\alpha)\partial(\beta) = \partial(\alpha\beta)$.
Si $\alpha, \beta \in \mathbb{Z}[i]$ y $\beta \neq 0$ observe que

$$\alpha/\beta = \alpha\overline{\beta}/\partial(\beta) = x + iy$$

para $x, y \in \mathbb{Q}$.

Sean $x = a+u$ y $y = b+v$ en donde $a, b \in \mathbb{Z}$ son los enteros más cercanos a $x, y$ respectivamente, es decir $|u|, |v| \leq \frac{1}{2}$. Observe que $\alpha = \beta(a + bi) + \beta(u + vi)$, luego tenemos que $\beta(u + vi) = \alpha - \beta(a + bi) \in \mathbb{Z}[i]$, finalmente $\partial(\beta(u + vi)) = \partial(\beta)\partial(u + vi)$; por lo que basta ver que $\partial(u + vi) < 1$; observemos que $|u| \leq \frac{1}{2}$ y $|v| \leq \frac{1}{2}$, entonces $u^2 \leq \frac{1}{4}$ y $v^2 \leq \frac{1}{4}$, por lo tanto $u^2 + v^2 \leq \frac{1}{2} < 1$.

Por lo tanto $\partial(\beta(u + vi)) < \partial(\beta)$, entonces $\mathbb{Z}[i]$ dominio euclidiano. Puede ocurrir que el cociente y el residuo no sean únicos.

Por ejemplo, para $\alpha = 3 + 5i$ y $\beta = 2$, entonces

$$\alpha/\beta = \frac{3}{2} + \frac{5}{2}i$$

además $\frac{3}{2} = 1 + \frac{1}{2}$ ó $2 - \frac{1}{2}$; también $\frac{5}{2} = 2 + \frac{1}{2}$ ó $3 - \frac{1}{2}$; por lo tanto hay cuatro residuos y cuatro cocientes.

$$3 + 5i = \begin{cases} 2(1 + 2i) + (1 + i) \\ 2(1 + 3i) + (1 - i) \\ 2(2 + 2i) + (-1 + i) \\ 2(2 + 3i) + (-1 - i) \end{cases}$$

**Teorema 2.5.1**
Si $R$ es un dominio euclidiano, entonces $R$ es un dominio de ideales principales.

***Demostración.*** Sea $I$ un ideal de $R$. Si $I = \{0\}$ éste es ideal principal generado por el 0. Si $I \neq \{0\}$. Consideramos $d \in I$ un elemento de grado mínimo en $I$. Claramente $\langle d \rangle \subseteq I$. Ahora, sea $a \in I$, existe $q, r \in R$ , tales que $a = qd + r$ con $r = 0$ ó $\partial(r) < \partial(d)$, suponiendo que $r \neq 0$, tendríamos que $r \in I$ es de grado menor que $d$, lo cual es una contradicción, por lo que $a = qd$, obteniendo la otra contención. ■

**Corolario 2.5.1**
$\mathbb{Z}[i]$ es dominio de ideales principales.

Observe que, dominio de ideales principales no implica dominio euclidiano. Como contraejemplo tenemos $R = \{a + b\alpha : a, b \in \mathbb{Z}, \alpha = \frac{(1+\sqrt{-1}a)}{2}\}$

**Proposición 2.5.1**
i) Sea $R$ un anillo euclidiano tal que $R$ no es campo. Si la función grado $\partial$ es una norma, entonces $\alpha$ es unidad si y sólo si $\partial(\alpha) = 1$.

ii) Sea $R$ un anillo euclidiano tal que $R$ no es campo. Si la función grado $\partial$ es una norma y $\partial(\alpha) = p$ con $P$ primo, entonces $\alpha$ es irreducible.

iii) Las únicas unidades en $\mathbb{Z}[i]$ son $\pm 1$ y $\pm i$.

***Demostración.*** i) Necesidad. Observemos que $1_R^2 = 1_R$, entonces $[\partial(1_R)]^2 = \partial(1_R) \in \mathbb{N}$, entonces $\partial(1_R) = 0$ ó $\partial(1_R) = 1$.

Si $\partial(1_R) = 0$, entonces para todo $a \in R$ tenemos $\partial(a) = \partial(a1_R) = \partial(a)\partial(1_R) = 0$, entonces $R$ es un campo, pero eso es una contradicción. Concluimos que $\partial(1_R) = 1$.

Si $\alpha \in U(R)$, entonces existe un $\beta \in R$ tal que $\alpha\beta = 1_R$, $\partial(\alpha)\partial(\beta) = 1$, por lo tanto $\partial(\alpha) = 1$. Veremos que no existen elementos $\beta \in R$ tal que $\partial(\beta) = 0$.

Por el algoritmo de la división, si $0 \neq \beta \in R$ es tal que $\delta(\beta) = 0$, entonces tendríamos $1_R = q\beta + r$ con $r = 0$ ó $(\partial(r) < \partial(\beta) = 0)$. Por lo tanto $r = 0$ y $1_R = q\beta$, entonces $\partial(\beta)\partial(q) = 1$ entonces $0 = 1$ pero es una contradicción. Por lo tanto para todo $\alpha \in R$ tenemos que $\partial(\alpha) > 0$

Ahora si $\partial(\alpha) = 1$ del algoritmo de la división tenemos que $\alpha = q\alpha^2 + r$ con $r = 0$ ó $\partial(\alpha) < 1$, y por lo anterior $\partial(r)$ no puede ser cero, por lo tanto $\alpha = q\alpha^2$ y por ser dominio entero $1 = q\alpha$. Entonces $\alpha$ es unidad.

ii) Sea $\alpha = \beta\gamma$ donde ni $\beta$ ni $\gamma$ son unidades, entonces $p = \delta(\alpha) = \delta(\beta)\delta(\gamma)$. Con $p$-primo, entonces $\partial(\beta) = 1$ ó $\partial(\gamma) = 1$, por i) tenemos que $\beta$ es unidad ó $\gamma$ es unidad, pero es una contradicción. Por lo tanto $\alpha$ es irreducible.

iii) Si $\alpha = a + bi \in \mathbb{Z}[i]$ es unidad, entonces $a^2 + b^2 = 1$, $(a^2 = 1$ y $b^2 = 0)$ ó $(a^2 = 0$ y $b^2 = 1)$, entonces $\alpha = \pm 1$ ó $\alpha = \pm i$. ■

**Lema 2.5.1**
Sea $p \in \mathbb{Z}$ primo tal que $p \equiv 1 \ mod\ 4$, entonces existe $m \in \mathbb{Z}$ tal que $m^2 \equiv -1 \ mod\ p$.

***Demostración.*** Sea $G = \mathbb{Z}_p^*$, entonces $|G| = p$–1 por hipótesis $p-1 \equiv 0 \ mod\ 4$. Por lo tanto $4\big||G|$, puesto $G$ es cíclico finito , existe $H \leq G$ cíclico tal que $|H| = 4$.

Sea $|H| = \langle m \rangle$ tenemos que $\left[m^4\right] = 1$. Por lo tanto el orden de $m^2$ es 2, pero el único elemento en $\mathbb{Z}_p$ de orden 2 es el $-1$. Por lo tanto $[m^2] = [-1]$, entonces $m^2 \equiv -1 \ mod\ p$. ■

**Teorema 2.5.2 (Fermat)**
Si $p$ es un número primo impar, entonces $p = a^2 + b^2$ para $a, b \in \mathbb{Z}$ si y sólo si $p \equiv 1 \ mod\ 4$.

***Demostración.*** Necesidad. Supongamos que $p = a^2+b^2$, puesto que $p$ es impar tenemos que $a$ y $b$ tienen diferente paridad, digamos, $a$ par y $b$ impar, entonces $a = 2m$ y $b = 2n + 1$. Entonces

$$p = a^2 + b^2 = 4m^2 + 4n^2 + 4n + 1 \equiv 1 \ mod\ 4.$$

Suficiencia. Supongamos que $p \equiv 1 \ mod\ 4$, entonces existe $m \in \mathbb{Z}$ tal que $p|(m^2 + 1) = (m + i)(m - i) \in \mathbb{Z}[i]$.

Si $p|(m \pm i) \in \mathbb{Z}[i]$, entonces $m \pm i = p(u + iv)$ con $u, v \in \mathbb{Z}$, por lo tanto $pu = m$ y $pv = 1$, pero esto es una contradicción. Por lo tanto, $p$ no satisface el lema de Euclides.

$\mathbb{Z}[i]$ es un dominio de ideales principales. Recuerde que en un dominio de ideales principales es $\pi$ es irreducible y $\pi|\alpha\beta$, entonces $\pi|\alpha$ ó $\pi|\beta$. Por lo tanto, $p$ no es irreducible en $\mathbb{Z}[i]$. Entonces existe una factorización $p = \alpha\beta \in \mathbb{Z}[i]$ en donde $\alpha = a + ib$ y $\beta = c + id$ no son unidades.

Tomando normas

$$p^2 = \partial(p) = \partial(\alpha)\partial(\beta) = (a^2 + b^2)(c^2 + d^2) \in \mathbb{Z}$$

$\alpha, \beta$ no unidades de $\mathbb{Z}[i]$, entonces $a^2+b^2 \neq 1 \neq c^2+d^2$, entonces por el lema de Euclides, tenemos $p|(a^2+b^2)$ ó $p|(c^2+d^2)$; ahora usando el teorema fundamental de la aritmética y factorización única en $\mathbb{Z}$, $p = a^2 + b^2$ y $p = c^2 + d^2$. ■

## 2.6. Espacios Vectoriales

**Definición 2.6.1**
Si $k$ es un campo, entonces un espacio vectorial sobre $k$ es un grupo abeliano $(V, +)$ con una multiplicación por escalares, es decir, una función $k \times V \to V$ denotada por $(a, v) \mapsto av$ que satisface para todo $a, b, 1 \in k$, $u, v \in V$:

i) $a(u + v) = au + av$.

ii) $(a + b)v = av + bv$.

iii) $(ab)v = a(bv)$.

iv) $1v = v$.

Los elementos de $V$ son llamados vectores y los elementos en $k$ son llamados escalares.

**Ejemplo 71**
1) El espacio euclidiano $V = \mathbb{R}^n$ es un espacio vectorial sobre $\mathbb{R}$, en este espacio los vectores son $n$-adas $(a_1, \ldots, a_n)$ donde $a_i \in \mathbb{R}$ para todo $i$. La suma está definida como

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_2) = (a_1 + b_1, \ldots, a_n + b_n)$$

geométricamente la suma de vectores está descrita por la ley del paralelogramo. La multiplicación por escalares está definida por

$$av = a(a_1, \ldots, a_n) = (aa_1, \ldots, aa_n).$$

2) Una generalización del ejemplo anterior sería $V = K^n$ para $K$ un campo, decir,

$$v = (a_1, \ldots, a_n) \text{ donde } a_i \in K \text{ para todo } i.$$

3) Sea $R$ un anillo conmutativo y $K$ un subanillo $K \leq R$ que sea un campo, entonces $R$ es un espacio vectorial sobre $K$. Tomando los elementos de $R$ como vectores y los elementos de $K$ como escalares, y ahora definimos $av$ como la multiplicación por escalares con $a \in K$ y $v \in R$. Observe que los axiomas de espacio vectorial son un caso particular de los axiomas de anillo conmutativo.

4) Si $K$ es un campo, el anillo de polinomios $R = K[x]$ es un espacio vectorial sobre $K$. Los vectores son polinomios de la forma $f(x) = b_n x^n + \cdots + b_1 x + b_0$ y los escalares de la forma $a \in K$, y la multiplicación por escalares como $af(x)$; esto es

$$af(x) = ab_n x^n + \cdots + ab_1 x + ab_0$$

en particular, si un campo $K$ es subcampo de un campo $E$ más grande, entonces $E$ es un espacio vectorial sobre $K$.

**Definición 2.6.2**
Si $V$ es un espacio vectorial sobre $K$, entonces un subespacio de $V$ es un subconjunto $U \subseteq V$ tal que

i) $0 \in U$

ii) $u, u' \in U$, entonces $u + u' \in U$

iii) $u \in U$ y $a \in K$, entonces $au \in U$.

**Ejemplo 72**
1) Si $v = (a_1, \ldots, a_n) \neq 0$ un vector en $\mathbb{R}^n$, entonces la recta que pasa por el origen

$$l = \{av : a \in \mathbb{R}\} \subseteq \mathbb{R}^n$$

es un subespacio de $\mathbb{R}^n$. Similarmente el plano generado por dos vectores $v_1, v_2$ no colineales, es decir,

$$\{av_1 + bv_2 : a, b \in \mathbb{R}\} \subseteq \mathbb{R}^n \text{ es subespacio.}$$

2) Si $m \leq n$, $\mathbb{R}^m$ son los vectores en $R^n$ tales que las últimas $n-m$ coordenadas son cero, entonces $\mathbb{R}^m \subseteq \mathbb{R}^n$. Por ejemplo, podemos ver a $\mathbb{R}^2$ como los puntos $(x, y, 0) \in \mathbb{R}^3$.

3) Si $K$ es un campo; un sistema lineal homogéneo sobre $K$ de $m$ ecuaciones con $n$ incógnitas es un conjunto de ecuaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

donde $a_{ij} \in K$. Una solución del sistema es un vector $(c_1, \ldots, c_n) \in K^n$ donde se cumple $\sum_i a_{ji}c_i = 0$ para todo $j$. La solución es no trivial si algún $c_i \neq 0$. El conjunto de soluciones forman un subespacio de $K^n$, llamado el espacio solución.

**Definición 2.6.3**
Una lista en un espacio vectorial $V$ es un conjunto ordenado $v_1, \ldots, v_n$ de vectores en $V$, es decir, existe algún $n \geq 1$ y una función

$$\varphi : \{1, 2, \ldots, n\} \to V \text{ tal que } \varphi(i) = v_i \text{ para todo } i$$

entonces $X = im\varphi$; $X$ es ordenado en el sentido de que existe un primer vector $v_1$, un segundo vector $v_2$ y así sucesivamente. Un vector puede aparecer muchas veces en una lista, esto es; $\varphi$ no necesariamente es inyectiva.

**Definición 2.6.4**
Sea $V$ un espacio vectorial sobre $K$ un campo. Una $K$-combinación lineal de una lista $v_1, \ldots, v_n$ en $V$ es un vector $v$ de la forma

$$v = a_1v_1 + \cdots + a_nv_n \text{ donde } a_i \in K \text{ para todo } i.$$

**Definición 2.6.5**
Si $X : v_n, \ldots, v_m$ es una lista en $V$, entonces $\langle v_1, \ldots, v_m \rangle \leq V$ el conjunto de todas las combinaciones lineales de $v_1, \ldots, v_m$.

**Lema 2.6.1**
Sea $V$ un espacio vectorial sobre $K$ campo.

i) La intersección de subespacios en $V$ es un subespacio en $V$.

ii) Si $X = v_1, \ldots, v_m$ es una lista en $V$, entonces la intersección de todos los subespacios de $V$ que contienen a $X$ es es $\langle v_1, \ldots, v_m \rangle$, es decir, $\langle v_1, \ldots, v_m \rangle$ es el subespacio más pequeño (mínimo) de $V$ que contiene a $X$.

***Demostración.*** i) La demostración es clara usando la definición de subespacio.

ii) Sea $\mathcal{S}$ la familia de todos los subespacios de $V$ que contienen a $X$. Por demostrar; $\bigcap_{s \in \mathcal{S}} s = \langle v_1, \ldots, v_m \rangle$.

Sabemos que $X \subseteq \langle v_1, \ldots, v_m \rangle$, entonces $\langle v_1, \ldots, v_m \rangle \in \mathcal{S}$. Por lo tanto $\bigcap_{s \in \mathcal{S}} s \subseteq \langle v_1, \ldots, v_m \rangle$.

Ahora $s \in \mathcal{S}$ tenemos que $X \subset s$, entonces $\langle v_1, \ldots, v_m \rangle \subset s$. Por lo tanto $\langle v_1, \ldots, v_m \rangle \subseteq \bigcap_{s \in \mathcal{S}} s$. ■

**Observación 48**
Si $X = \emptyset$, entonces $\langle X \rangle = \bigcap_{s \in \mathcal{S}} s$

donde $\mathcal{S}$ la familia de subespacios de $V$ que contienen a $X$. Cualquier subespacio contiene al $\emptyset$, en particular $\{0\}$, entonces $\langle \emptyset \rangle = \bigcap_{s \subseteq V} s = \{0\}$.

**Ejemplo 73**
1) Si $V = \mathbb{R}^2$. Sea $e_1 = (1, 0), e_2 = (0, 1)$, entonces $V = \langle e_1, e_2 \rangle$.

$$v = (a, b) = ae_1 + be_2.$$

2) Si $V = K^n$ para $K$ un campo definimos $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ donde 1 es la $i$-ésima entrada, entonces $V = \langle e_i : i = 1, \ldots, n \rangle$

**Observación 49**
Un espacio vectorial. No necesariamente está generado por una lista finita de vectores. Cómo ejemplo tenemos $V = K[x]$. Suponga que $V$ está generado por $X = f_1(x), \ldots, f_m(x)$.

Sea $d = max\{\partial(f_i(x)) : i = 1, \ldots, m\}$ cualquier combinación lineal de $f_1, \ldots, f_m$ tendría grado a lo más $d$, pero, $x^{d+1}$ no es combinación lineal de los elementos en $X$.

**Definición 2.6.6**
Un espacio vectorial $V$ es llamado de dimensión finita si está generado por una lista finita de vectores.

**Ejemplo 74**
$K^n$ es de dimensión finita pues está generado por $e_i$ con $i = 1, \ldots, n$. Por lo tanto $K[x]$ es dimensión infinita.

Si $v_1, \ldots, v_m$ es una lista, entonces escribiremos $v_1, \ldots, \hat{v_i}, \ldots, v_m$ es una lista más corta donde hemos quitado $v_i$.

**Proposición 2.6.1**
Si $V$ es un espacio vectorial, entonces las siguientes condiciones en una lista $X = v_1, \ldots, v_m$ que genera a $V$ son equivalentes.

i) $X$ no es la lista más corta que genera a $V$.
ii) Algún $v_i$ está en lo generado por los otros generadores, es decir,

$$v_i \in \langle v_1, \ldots, \hat{v_i}, \ldots, v_m \rangle .$$

iii) Existen escalares $a_1, \ldots, a_m$ no todos cero, con

$$\sum_{l=1}^{m} a_l v_l = 0.$$

***Demostración.*** i) implica ii). Si $X$ no es la lista más corta de generadores entonces al menos podemos extraer un $v_i \in \langle v_1, \ldots, \hat{v_i}, \ldots, v_m \rangle$ y estos generarán a $V$.

ii) implica iii). $v_i \in \langle v_1, \ldots, \hat{v_i}, \ldots, v_m \rangle$, entonces $v_i = \sum_{j \neq i} c_j v_j$, definimos $a_i = -1$ y $a_j = c_j$ con $j \neq i$. Por lo tanto

$$\sum_{l=1}^{m} a_l v_l = 0.$$

iii) implica i). La ecuación $\sum_{l=1}^{m} a_l v_l = 0$ para la cual existe un $a_i \neq 0$, y por lo tanto al menos un $v_i \in \langle v_1, \ldots, \hat{v_i}, \ldots, v_m \rangle$, la cual es una lista más corta en comparación a $X$. ■

**Definición 2.6.7**
Una lista $X = v_1, \ldots, v_m$ en un espacio vectorial es linealmente dependiente si existen $a_i$ no todos iguales a cero tal que $\sum_{l=1}^{m} a_l v_l = 0$. De lo contrario $X$ es linealmente independiente.

El conjunto vacío $\emptyset$ es una lista de tamaño cero, por lo tanto $\emptyset$ es linealmente independiente.

**Ejemplo 75**
1) Cualquier lista que contiene al vector cero es linealmente dependiente. Es decir,

$$X = v_1, \ldots, v_m \text{ si } v_i = 0, \text{ entonces } \sum_{l=1}^{m} a_l v_l = 0$$

definimos $a_i \neq 0$ y $a_j = 0$ para todo $j \neq i$.
2) La lista $X = v_1$ es linealmente independiente si y sólo si $v_1 \neq 0$.

3) La lista $X = v_1, v_2$ es linealmente dependiente si y sólo si uno es múltiplo escalar del otro.
4) Si existe una repetición en la lista $v_1, \ldots, v_m$ (es decir, si $v_i = v_j$ para algún $i \neq j$), entonces $v_1, \ldots, v_m$ es linealmente dependiente. Definimos $a_i = -1$, $a_j = 1$ y al resto de los $a_k = 0$ para $k \neq i, j$.

Entonces una condición necesaria más no suficiente para que la lista $v_1, \ldots, v_m$ sea linealmente independiente, es que los $v_i$ sean distintos.

**Corolario 2.6.1**
Si $X = v_1, \ldots, v_m$ es una lista tal que $V = \langle v_1, \ldots, v_m \rangle$, entonces $X$ es la lista más pequeña de generadores si y sólo si $X$ es linealmente independiente.

**Definición 2.6.8**
Una lista $X = v_1, \ldots, v_m$ es linealmente independiente si cada vez que la combinación

$$\sum_{l=1}^{m} a_l v_l = 0, \text{ entonces } a_i = 0 \text{ para todo } i.$$

Observe que una sublista de una lista linealmente independiente es linealmente independiente.

**Definición 2.6.9**
Una base de $V$ es una lista $X$ linealmente independiente y que genera a $V$. Una base es una lista más corta de generadores.

**Ejemplo 76**
$K^n = \langle e_1, \ldots, e_n \rangle$. El conjunto $\{e_1, \ldots, e_n\}$ es la base estándar de $K^n$.

**Proposición 2.6.2**
Sea $X = v_1, \ldots, v_m$ una lista en un espacio vectorial $V$ sobre un campo $K$. $X$ es una base si y sólo si cada vector en $V$ tiene una única expresión como $K$-combinación lineal de vectores en $X$.

***Demostración.*** Necesidad. Si un vector $v = \sum a_i vi = \sum b_i v_i$, entonces $\sum(a_i - b_i)v_i = 0$ por la independencia lineal, tenemos que $a_i = b_i$. Suficiencia. Todo vector en $V$ es combinación lineal de $v_i$, entonces, los $v_i$ generan a $V$. Si $0 = \sum a_i v_i$ y si los $a_i$ no todos cero, entonces $0 = \sum o v_i$ tiene dos expresiones como combinación lineal de los $v_i$, lo cual es una contradicción, por lo tanto $a_i = 0$ para todo $i$, lo cual implica que los $v_i$ son linealmente independientes. ■

**Definición 2.6.10**
Si $X = v_1, \ldots, v_n$ es una base de $V$. Si $v \in V$, entonces existen escalares únicos $a_1, \ldots, a_n$ con $V = \sum_{i=1}^{n} a_i v_i$. Entonces $(a_1, \ldots, a_n)$ son las coordenadas de $v \in V$, con respecto a la base $X$.

**Teorema 2.6.1**
Todo espacio vectorial $V$ de dimensión finita tiene una base.

***Demostración.*** Sabemos que existe $X$ una lista finita que genera a $V$ por ser $V$ de dimensión finita. Si los elementos en $X$ son linealmente independientes, entonces $X$ es una base.

Si no, $X$ se puede reducir a una sublista más corta $X'$ que genera. Si $X'$ es linealmente independiente $X'$ es base. Si no, $X'$ se puede reducir a una sublista $X''$ que genera. Usando este proceso y como $X$ es un conjunto finito , entonces eventualmente llegaremos a una sublista que genera y linealmente independiente, dicho de otra forma, esta sublista es una base. ■

**Lema 2.6.2**
Sea $u_1, \ldots, u_n$ elementos en un espacio vectorial $V$ y $v_1, \ldots, v_m \in \langle u_1, \ldots, u_n \rangle$. Si $m > n$, entonces $v_1, \ldots, v_m$ son linealmente dependientes.

***Demostración.*** Haremos inducción sobre $n$. Si $n = 1$, entonces hay al menos dos vectores $v_1, v_2 \in \langle u_1 \rangle$, de aquí $v_1 = au_1$ y $v_2 = bu_1$. Si $u_1 = 0$, entonces $v_1 = 0$. Por lo tanto $\{v_1, v_2\}$ es linealmente dependiente. Ahora suponga que $u_1 \neq 0$. Podemos asumir que $v_1 \neq 0$, entonces $a \neq 0$. Por lo tanto $v_2 - ba^{-1}v_1 = 0$. Por lo tanto $v_1, \ldots, v_m$ son linealmente dependientes.

Ahora tenemos que $v_i = a_{i1}u_1 + \cdots + a_{in}u_n$ podemos asumir que algún $a_{i1} \neq 0$ pues de lo contrario $v_i \in \langle u_2, \ldots, u_n \rangle$ al cual aplica la hipótesis de inducción. Reordenando podemos asumir que $a_{11} \neq 0$. Para $i \geq 2$, definimos $v_i' = v_i - a_{i1}a_{11}^{-1}v_1 \in \langle u_2, \ldots, u_n \rangle$ puesto que $m-1 > n-1$, por hipótesis de inducción existen escalares $b_2, \ldots, b_m$ no todos cero tal que

$$b_2v_2' + \cdots + b_mv_m' = 0, \text{ entonces } (-\sum_{i\geq 2} b_i a_{i1} a_{11}^{-1})v_1 + b_2v_2 + \cdots + b_mv_m = 0$$

En donde no todos los coeficientes son cero, por lo tanto $v_1, \ldots, v_m$ son linealmente dependientes. ■

**Corolario 2.6.2**
Un sistema homogéneo de ecuaciones lineales, sobre un campo $K$ con más incógnitas que ecuaciones tiene una solución no trivial.

***Demostración.*** Suponga que $(B_1, \ldots, B_n)$ es solución del sistema

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

si $a_{i1}B_1 + \cdots + a_{in}B_n = 0$ para todo $i = 1, \ldots, m$. Ahora si $c_1, \ldots, c_n$ son las columnas de $A = [a_{ij}]_{m\times n}$, entonces

$$B_1c_1 + \cdots + B_nc_n = 0 \text{ observemos que } c_i \in K^m$$

ahora $K^m$ está generado por $m$-vectores y $n > m$; por lo tanto los $c_i$ son linealmente dependientes, por lo tanto, existen escalares no todos cero $\gamma_1, \ldots, \gamma_n$ tal que $\gamma_1c_1 + \cdots + \gamma_nc_n = 0$ ; por lo tanto $(\gamma_1, \ldots, \gamma_n)$ es una solución no trivial. ■

**Teorema 2.6.2 (Invariancia de la dimensión.)**
Si $X = x_1, \ldots, x_n$ y $Y = y_1, \ldots, y_m$ bases de $V$, entonces $m = n$.

***Demostración.*** Si $m \neq n$, tenemos que $n < m$ o $m < n$. Primer caso, $n < m$; $y_1, \ldots, y_m \in \langle x_1, \ldots, x_n\rangle$ ya que $X$ genera a $V$; por lo tanto $y_1, \ldots, y_m$ son linealmente dependientes. Pero es una contradicción, $y_1, \ldots, y_m$ forman una base de $V$. Similarmente si $m < n$, tenemos que $x_1, \ldots, x_n \in \langle y_1, \ldots, y_m\rangle$, entonces $x_1, \ldots, x_n$ son linealmente dependiente. Pero es una contradicción. ■

**Definición 2.6.11**
Si $V$ es un espacio vectorial de dimensión finita sobre $K$, la dimensión de $V$ será igual al número de elementos de una base de $V$.

**Ejemplo 77**
1) El conjunto $\emptyset$ es una base de $V = \{0\}$. Po lo tanto $dim\{0\} = 0$, pues el conjunto vacío $\emptyset$ no tiene elementos.

Sea $X = \{x_1, \ldots, x_n\}$; definimos

$$K^X = \{\text{Funciones } f : X \to K\}$$

$K^X$ tiene estructura de espacio vectorial si definimos

$$[f + f'](x) = f(x) + f'(x)$$

como la suma de vectores y

$$[af](x) = af(x)$$

como el producto de escalares. Se puede ver que la lista

$$\left\{ f_{x_i}(y) = \begin{cases} 1 \text{ si } y = x_i \\ 0 \text{ si } y \neq x_i \end{cases} : x_i \in X \right.$$

forma una base, por lo tanto $dimK^X = n$. Observe que $f(x_i) = y_i$, de aquí $f = \sum_{i=1}^n y_i f_{x_i}$ generan. Si $\sum_{i=1}^n a_i f_{x_i} = 0$ evaluando en $x_i$, entonces $a_i = 0$. Por lo tanto es linealmente independiente.

**Lema 2.6.3**
Si $X = v_1, \ldots, v_m$ es una lista linealmente dependiente en $V$, entonces existe $v_r$ con $r \geq 1$ y $v_r \in \langle v_1, \ldots, v_{r-1} \rangle$. Cuando $r = 1$ interpretamos $\langle v_1, \ldots, v_{r-1} \rangle = \{0\}$.

***Demostración.*** Sea $r$ el máximo entero tal que $v_1, \ldots, v_{r-1}$ sean linealmente independientes. Si $v_1 = 0$, entonces $v_1 \in \{0\}$, tomamos $r = 1$. Ahora si $v_1 \neq 0$, entonces $r \geq 2$ puesto que $v_1, \ldots, v_m$ son linealmente dependientes, entonces $r - 1 < m$, además existen $a_1, \ldots, a_r$ no todos cero tal que

$$a_1 v_1 + \cdots + a_r v_r = 0$$

observe que $a_r \neq 0$ por la independencia lineal de $v_1, \ldots, v_{r-1}$, por lo tanto $v_r \in \langle v_1, \ldots, v_{r-1} \rangle$. ■

**Lema 2.6.4 (Cambio.)**
Si $X = x_1, \ldots, x_m$ es una base de vectores de $V$ y $y_1, \ldots, y_n$ es un subconjunto linealmente independiente de $V$, entonces $n \leq m$.

***Demostración.*** Veamos primero que podemos reemplazar un elemento de $X$ por $y_n \in \langle X \rangle$ ya que $X$ es base de $V$, la lista $y_n, x_1, \ldots, x_n$ es linealmente dependiente.

$y_1, \ldots, y_n$ linealmente independiente, entonces $y_n \notin \{0\}$ por el lema anterior, existe $i$ tal que $x_i = a y_n + \sum_{j<i} a_j x_j$, por lo que el conjunto

$$X' = \{y_n, x_1, \ldots, \hat{x_i}, \ldots, x_m\} \text{ generan a } V.$$

ahora repetimos el argumento para la lista

$$y_{n-1}, y_n, x_1, \ldots, \hat{x_i}, \ldots, x_m$$

por el lema anterior podemos tener:

$$y_n \in \langle y_{n-1} \rangle\,,\ x_1 \in \langle y_{n-1}, y_n \rangle\,, x_2 \in \langle y_{n-1}, y_n, x_1 \rangle\,, \ldots$$

tenemos que los $y_i$ son linealmente independientes, entonces, cualquier sublista es linealmente independiente, entonces $y_n \notin \langle y_{n-1} \rangle$. Por lo tanto, del lema anterior, el elemento reemplazable debe ser algún $x$, digamos un $x_j$. Por lo cual reemplazando $x_j$ por $y_{n-1}$ obtenemos una nueva lista de generadores $X''$; repitiendo este procedimiento. Cada vez que adjuntamos un vector $y$ al principio de la lista y quitamos un $x$, la opción de elegir los $y_i \in \{y_{i+1}, \ldots, y_n\}$ no es posible, por la independencia lineal de los elementos $y$.

Si $n > m$, implicaría que son mas elementos $y$ que elementos $x$, por lo cual el procedimiento anterior termina con una lista de $m$ elementos $y$ (es decir, una $y$ por cada $x$ reemplazada) y ninguna $x$.

Por lo tanto una sublista de $y$ genera a $V$, lo cual contradice la independencia lineal de los elementos $y$. Por lo tanto $n \leq m$. ■

**Teorema 2.6.3 (Invariancia de la dimensión.)**
Si $X = x_1, \ldots, x_m$ y $Y = y_1, \ldots, y_n$ son bases de un espacio vectorial $V$, entonces $m = n$.

***Demostración.*** Tenemos que $X$ es una base y $Y$ es linealmente independiente, entonces $n \leq m$. Además $Y$ es una base y $X$ es linealmente independiente, entonces $m \leq n$. Por lo tanto $n = m$. ■

**Definición 2.6.12**
Una lista linealmente independiente $u_1, \ldots, u_m$ es maximal si no existe $v \in V$ tal que $u_1, \ldots, u_m, v$ es linealmente independiente.

**Lema 2.6.5**
Si $V$ es un espacio vectorial de dimensión finita, entonces una lista linealmente independiente $v_1, \ldots, v_n$ maximal es una base de $V$.

***Demostración.*** Si una lista no es base, entonces no genera a $V$, por lo tanto existe $w \in V$ tal que $w \notin \langle v_1, \ldots, v_n \rangle$, entonces $v_1, \ldots, v_n, w$ es linealmente independiente. Pero esto es una contradicción. ■

**Proposición 2.6.3**
Sea $Z = u_1, \ldots, u_m$ una lista linealmente independiente en un espacio $V$ de dimensión $n$, entonces $Z$ se puede extender a una base, es decir, existen vectores $v_{m+1}, \ldots, v_n$ tal que $u_1, \ldots, u_m, v_{m+1}, \ldots, v_n$ es base de $V$.

***Demostración.*** Si $Z$ no genera, entonces existe $w_1 \in V$ tal que $w_1 \notin \langle Z \rangle$ y $u_1, \ldots, u_m, w_1$ linealmente independiente, ya que si, $a_1 w_1 + \sum b_i u_i = 0$ si $a_i \neq 0$, entonces $w_1 \in \langle Z \rangle$, lo cual es una contradicción, por lo que $a_i = 0$, lo cual a su vez implica que $b_i = 0$

Si $Z, w_1$ no genera, entonces existen un $w_2 \in V$ tal que $w_2 \notin \langle Z, w_1 \rangle$. $Z, w_1, w_2$ son linealmente independientes puesto que $dim\ V = n$, este proceso es finito ya que el tamaño de la lista no puede exceder a $n$. ■

**Corolario 2.6.3**
Si $dim\ V = n$, entonces cualquier lista de $n + 1$ elementos o más es linealmente dependientes.

**Corolario 2.6.4**
Sea $V$ un espacio vectorial con $dim\ V = n$.

i) Una lista de $n$ vectores que generan a $V$ es linealmente independientes.

ii) Una lista linealmente independiente de $n$ vectores, generan a $V$.

***Demostración.*** i) Si la lista es linealmente dependiente, entonces esta se puede recortar para dar una base, pero esta base sería de tamaño menor a $n$. Esto es una contradicción.

ii) Si la lista no genera, entonces esta se puede extender a una base, de tamaño mayor a $n$. También es una contradicción. ■

**Corolario 2.6.5**
Sea $U$ un subespacio vectorial de $V$ con $dim\ V = n$, entonces

i) $U$ es de dimensión finita y $dim\ U \leq dim\ V$.

ii) Si $dim\ U = dim\ V =$, entonces $U = V$.

***Demostración.*** i) Tomamos $u_1 \in U$. Si $U = \langle u_1 \rangle$, entonces $U$ es de dimensión finita, si no fuera así, existiría $u_2 \in U$ tal que $u_2 \notin \langle u_1 \rangle$ y $\{u_1, u_2\}$ linealmente independiente. Si $U = \langle u_1, u_2 \rangle$ hemos terminado. Este procedimiento no se puede repertir $n+1$ veces; pues encontramos $u_1, \ldots, u_{n+1}$ vectores linealmente independientes en $U \subseteq V$, pero esto es una contradicción.

Ahora una base de $U$ que es linealmente independiente se puede extender a una base de $V$, entonces $dim\ U \leq dim\ V$.

ii) Si $dim\ U = dim\ V$, entonces una base de $U$ es una lista de tamaño $n$ linealmente independiente en $V$, por lo cual esta base es una base de $V$, por lo cual $V \subseteq U$, por lo tanto $U = V$. ■

## 2.7. Transformaciones lineales.

Los homomorfismos entre espacios vectoriales sobre un campo $K$ son llamados transformaciones lineales. Si $V, W$ son espacios vectoriales sobre un campo $K$:

$$T : V \to W \text{ es transformación lineal.}$$

Si para todo $u, v \in V$ y $a \in K$ se tiene que:

i) $T(u + v) = T(u) + T(v)$,

ii) $T(av) = aT(v)$.

Decimos que una transformación lineal es no singular (o un isomorfismo) si $T$ es una biyección. En este caso $V \cong W$ como espacio vectorial. Observe que $T(\sum_{i=1}^{n} a_i v_i) = \sum_{i=1}^{n} a_i T(v_i)$.

**Definición 2.7.1**
Si $V$ es un espacio vectorial sobre $K$. El conjunto $\mathrm{GL}(V)$ grupo general lineal formado por todas las transformaciones no singulares $V \to V$. Es un grupo bajo la composición de transformaciones; ya que la composición de transformaciones no singulares es nuevamente una transformación no singular; por último la inversa de una transformación no singular es una transformación no singular.

**Teorema 2.7.1**
Sea $v_1, \ldots, v_n$ una base de un espacio vectorial $V$ sobre un campo $K$ . Ahora sea $W$ un espacio vectorial sobre $K$ y $w_1, \ldots, w_n$ una lista en $W$. Entonces existe una única transformación lineal $T : V \to W$ tal que $T(v_i) = w_i$ para todo $i$.

***Demostración.*** Para $v \in V$ la expresión $v = \sum a_i v_i$ es única, por lo cual $T(v) = \sum_{i=1}^{n} a_i w_i$ está bien definida (transformación lineal). Ahora suponga que $S : V \to W$ es tal que $S(v_i) = w_i$. Tenemos que para todo $v \in V$, $v = \sum a_i v_i$, por lo tanto $S(v) = \sum a_i w_i = T(v)$. ■

**Corolario 2.7.1**
Si dos transformaciones lineales $S, T : V \to W$ y $v_1, \ldots, v_n$ una base de $V$ con $T(v_i) = S(v_i)$ para todo $i$, entonces $T = S$.

**Proposición 2.7.1**
Si $T : K^n \to K^m$ es una transformación lineal, entonces existe $A_{m\times n}$ tal que

$$T(y) = Ay.$$

***Demostración.*** Sea $[e_1, \ldots, e_n]$ la base estándar de $K^n$ y $[e'_1, \ldots, e'_m]$ base estándar de $K^m$. Definimos $A = [a_{ij}]$ (las columnas son coordenadas de $e_j$ en la base $e'_i$) en donde $T(e_j) = \sum_{i=1}^{m} a_{ij} e'_i$; observe que si $S(y) = Ay$, entonces $T = S$ pues coinciden en la base. ■

**Observación 50**
En general. Si $X = v_1, \ldots, v_n$ base de $V$ y $Y = w_1, \ldots, w_n$ base de $W$ la matriz asociada a $T : V \to W$ (transformación lineal) es $A = [a_{ij}]$ tal que $T(v_j) = \sum_{i=1}^{m} a_{ij} w_j$ para $j = 1, \ldots, n$, la cual denotaremos por $A =_Y [T]_X$.

**Ejemplo 78**
Sea $T : \mathbb{R}^2 \to \mathbb{R}^2$ la transformación rotación por $90°$ y $X = \{(1, 0), (0, 1)\}$ la base estándar. Entonces:

$$_X[T]_X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

ya que $T(1, 0) = 0(1, 0) + 1(0, 1)$, $T(0, 1) = -1(1, 0) + 0(0, 1)$.

**Proposición 2.7.2**
Sean $V, W$ espacios vectoriales sobre un campo $K$, y sean $X = v_1, \ldots, v_n$ y $Y = w_1, \ldots, w_m$ bases de $V$ y $W$ respectivamente. Denotamos por $\mathrm{Hom}_K(V, W)$

al conjunto de todas las transformaciones lineales de $V \to W$; también denotaremos por $\mathrm{Mat}_{m\times n}(K)$ al conjunto de todas las matrices de tamaño $m \times n$ con entradas $K$, entonces la función $T \to {}_Y[T]_X$ es una biyección entre $\mathrm{Hom}_K(V,W) \to \mathrm{Mat}_{m\times n}(K)$.

***Demostración.*** Sea $A \in M_{m\times n}(K)$, y

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

la $j$-ésima columna de la matriz, entonces definimos $z_j = \sum_{i=1}^{m} a_{ij}w_i$. Ahora definimos $T(v_j) = z_j$, por lo tanto $A =_Y [T]_X$ teniendo la sobreyectividad. Para la inyectividad, sean $T$ y $S$ en $\mathrm{Hom}_K(V,W)$ tales que ${}_Y[T]_X = A =_Y [S]_X$ entonces $T$ y $S$ coinciden en la base y por tanto son iguales. ■

**Proposición 2.7.3**
Sean $T : V \to W$ y $S : W \to U$ transformaciones lineales, y ahora sean $X = x_1, \ldots, x_n$ y $Y = y_1, \ldots, y_m$ y $Z = z_1, \ldots, z_l$ bases de $V, U$ y $W$ respectivamente, entonces

$${}_Z[S \circ T]_X =_Z [S]_{YY}[T]_X.$$

***Demostración.*** Tenemos que ${}_Y[T]_X = [a_{pj}]$, por lo cual $T(x_j) = \sum_p a_{pj}y_p$ y ${}_Z[S]_Y = [b_{qp}]$, entonces $S(y_p) = \sum_q b_{qp}z_q$, por lo tanto

$$S \circ T(x_j) = S(T(x_j)) = \sum_p \sum_q a_{pj}b_{qp}z_q = \sum_q c_{qj}z_q$$

en donde $c_{qj} = \sum_p b_{qp}a_{pj}$ la cual es la entrada $qj$ de $[b_{qp}][a_{pj}]$. ■

**Corolario 2.7.2**
El producto de matrices es asociativo.

**Corolario 2.7.3**
Sea $T : V \to W$ una transformación lineal y $X$ una base de $V$, $Y$ una base de $W$, entonces si $T$ es no singular ${}_X[T^{-1}]_Y = ({}_Y[T]_X)^{-1}$.

***Demostración.*** Tenemos que $I =_Y [1_W]_Y =_Y [T]_X \ {}_X[T^{-1}]_Y$ y
$I =_X [1_V]_X =_X [T^{-1}]_Y \ {}_Y[T]_X$. ■

**Corolario 2.7.4**
Sea $T : V \to V$ una transformación lineal, $X, Y$ bases de $V$, entonces existe una matriz no singular $P$ con entradas en $K$ tal que

$${}_Y[T]_Y = P_X[T]_X P^{-1}.$$

***Demostración.*** Tenemos que ${}_Y[T]_Y =_Y [1_V T 1_V]_Y =_Y [1_V]_X \ {}_X[T]_X \ {}_X[1_V]_Y$ defina $P =_Y [1_V]_X$ y observe que $P^{-1} =_X [1_V]_Y$. ■

**Proposición 2.7.4**
Si $B = PAP^{-1}$ para $A, B, P \in M_{n\times n}[K]$ y $P$ no singular, entonces existe $T : K^n \to K^n$ y bases $X$ e $Y$ de $K^n$ tal que $B =_Y [T]_Y$ y $A =_X [T]_X$.

***Demostración.*** Sea $E = \{e_1, \ldots, e_n\}$ base estándar de $K^n$. Definimos, $T : K^n \to K^n$ tal que $T(e_j) = Ae_j$ es la $j$-ésima columna de $A$. Entonces tenemos $A =_E [T]_E$, ahora vamos a definir $y_j = P^{-1}e_j$ ($y_j$ es la columna $j$-ésima de $P^{-1}$); observe que el conjunto $Y = \{y_j\}$ es base ya que $P^{-1}$ no es singular si $\sum_j a_j y_j = 0$, entonces $\sum_j a_j P^{-1}e_j = P^{-1}(\sum_j a_j e_j) = 0$, aplicando $P$ en ambos lados, obtenemos que $\sum_j a_j e_j = 0$ de donde $a_j = 0$ para todo $j$. Es suficiente con probar que $B =_Y [T]_Y$; esto es, $T(y_j) = \sum b_{ij} y_i$, donde $B = [b_{ij}]$. Tenemos

$$\begin{aligned} T(y_j) &= Ay_j \\ &= AP^{-1}e_j \\ &= P^{-1}Be_j \\ &= P^{-1}\sum_i b_{ij}e_i \\ &= \sum_i b_{ij}P^{-1}e_i \\ &= \sum_i b_{ij}y_i \end{aligned}$$

■

**Definición 2.7.2**
Si $T : V \to W$ es una transformación lineal, entonces el núcleo (o espacio nulo) de $T$ es

$$kerT = \{v \in V : T(v) = 0\},$$

y la imagen de $T$ es

$$imT = \{w \in W : w = T(v) \text{ para algún } v \in V\}.$$

**Proposición 2.7.5**
Sea $T : V \to W$ una transformación lineal.

i) $kerT$ es un subespacio de $V$, $imT$ es un subespacio de $W$.

ii) $T$ es inyectiva si y sólo si $kerT = \{0\}$.

De la teoría de grupos, la prueba del inciso ii) es clara. Para el inciso i) se sabe que $kerT$ e $ImT$ son subgrupos abelianos por lo que resta probar que son cerrados bajo la multiplicación escalar.

**Lema 2.7.1**
Sea $T : V \to W$ una transformación lineal.

i) Si $T$ no es singular. Entonces para toda base $X = v_1, \ldots, v_n$ de $V$ tenemos que $T(v_1), \ldots, T(v_n)$ base de $W$.

ii) Si existe una base $X = v_1, \ldots, v_n$ de $V$ tal que $T(v_1), \ldots, T(v_n)$ es base de $W$, entonces $T$ es no singular.

***Demostración.*** i) Si $T(\sum a_i v_i) = \sum a_i T(v_i) = 0$ si y sólo si $\sum a_i v_i \in kerT = \{0\}$, entonces $a_i = 0$ para todo $i$ teniendo que $T(v_1), \ldots, T(v_n)$ es linealmente independiente. Ahora $T$ es no singular, por lo que para todo $w \in W$ existe $v \in V$ tal que $w \in T(v) = T(\sum b_i v_i) = \sum b_i T(v_i)$. Por lo tanto $T(v_i)$ generan a $W$.

ii) Para todo $w \in W$ tenemos $w = \sum b_i T(v_i) = T(\sum b_i v_i) \in imT$. Por lo tanto $T$ es sobreyectiva.

Ahora sea $v \in V$ tal que $T(v) = 0$, si $v = \sum_i a_i v_i$, entonces $T(v) = \sum_i a_i T(v_i) = 0$ por lo que $a_i = 0$ para todo $i$ por lo que $v = 0$, y entonces $kerT = \{0\}$. ■

**Teorema 2.7.2**
Si $V$ es un espacio vectorial de dimensión $n$ sobre $K$. Entonces $V \simeq K^n$.

***Demostración.*** Tomamos una base de $\{v_1, \ldots, v_n\}$ de $V$ y definimos $T : V \to K^n$ como $v_i \to e_i$ para todo $i$. $T$ se extiende de manera lineal y por ii) del lema anterior es no singular. ■

**Corolario 2.7.5**
Dos espacios vectoriales de dimensión finita $V, W$ sobre $K$ son isomorfos si y sólo si $dimV = dimW$.

***Demostración.*** Necesidad. Si $T : V \to W$ es no singular y $v_1, \ldots, v_n$ es base de $V$ entonces $T(v_1), \ldots, T(v_n)$ es base de $W$ por lo tanto $dimV = dimW$.

Suficiencia. $dimV = dimW = n$, por lo tanto $V \cong K^n$ y $W \cong K^n$. ■

**Definición 2.7.3**
$\mathrm{GL}(n, K)$ es el conjunto de todas las matrices no singulares $n \times n$ con entradas en $K$.

**Proposición 2.7.6**
Sea $V$ un espacio vectorial de dimensión $n$ y $X$ base de $V$, entonces

$$\mu : \mathrm{GL}(V) \to \mathrm{GL}(n, K)$$

definido como $T \mapsto [T] =_X [T]_X$ es un isomorfismo de grupos.

***Demostración.*** Anteriormente definimos la biyección $\mu : \mathrm{Hom}_X(V,V) \to \mathrm{Mat}_n(K)$ como $T \mapsto [T] =_X [T]_X$, y se probó que $T \circ S \to [T \circ S] = [T][S]$, además se vio que si $T \in \mathrm{GL}(V)$, entonces $[T]$ es no singular. Por lo tanto $\mu\big|_{GL(V)} : \mathrm{GL}(V) \to \mathrm{GL}(n,K)$ es homomorfismo inyectivo de grupos.

Por último veamos que es sobreyectiva. Sea $A \in \mathrm{GL}(n,K)$, puesto que $\mu$ es sobreyectiva, existen $S,T$ en $Hom(V,V)$ tales que $A = [T]$ y $A^{-1} = [S]$, luego $[T \circ S] = [T][S] = I_{n\times n}$, por lo tanto $T \circ S = 1_V$. Por lo tanto $T \in \mathrm{GL}(V)$. ■

## 2.8. Anillo cociente y campos finitos

Recordemos que un ideal $I \subseteq R$ de un anillo conmutativo, como subgrupo es normal en $R$, entonces $R/I$ está definido. Y definimos el mapeo natural:

$$\pi : R \to R/I$$
$$a \mapsto \pi(a) = a + I$$
$$a + I = b + I \text{ en } R/I \text{ si y sólo si } b - a \in I$$

**Teorema 2.8.1**
Si $I < R$ ideal y $R$ anillo conmutativo $R/I$ es un anillo conmutativo y

$$\pi : R \to R/I \text{ es un homomorfismo sobreyectivo de anillos.}$$

Definimos $(a+I)(b+I) = ab + I$ como la multiplicación.

***Demostración.*** Sólo veremos que las operaciones de suma y producto están bien definidas, pues si $a + I = a' + I$ y $b + I = b' + I$, entonces $a - a' \in I$ y $b - b' \in I$, $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + (b - b')a' \in I$, por lo cual $(a + I)(b + I) = (ab) + I = (a'b') + I = (a' + I)(b' + I)$. Por otro lado,

$(a + I) + (b + I) = (a + b) + I$, ahora si $(a - a') \in I$ y $b - b' \in I$, entonces $(a+b)-(a'+b') \in I$, por lo tanto $(a+I)+(b+I) = (a+b)+I = (a'+b')+I = (a' + I) + (b' + I)$. Además las propiedades de R/I de anillo, se heredan $R$.

Observemos que $\pi(a) = a+I$, entonces $\pi(a)\pi(b) = \pi(ab)$ y $\pi(a)+\pi(b) = \pi(a+b)$. Además $\pi(1_R) = 1_{R/I}$. Por lo tanto $\pi$ es homomorfismo de anillos. ■

**Definición 2.8.1**
$R/I$ es llamado el anillo cociente de $R$ módulo $I$.

**Ejemplo 79**
Sea $\mathbb{Z}/(m)$, con $m$ un ideal principal generado por $m$; este coincide con el anillo conmutativo $\mathbb{Z}_m$.

$$(a + (m))(b + (m)) = ab + (m) = [ab] = [a][b].$$

**Corolario 2.8.1**
$R$ anillo conmutativo, con $I \leq R$ un ideal. Existe un anillo conmutativo $A$ y un homomorfismo de anillos $\pi : R \to A$ tal que $ker\pi = I$.

***Demostración.*** Tenemos que $\pi : R \to R/I$ es tal que $ker\pi = I$. ■

**Teorema 2.8.2 (Primer teorema de isomorfismos.)**
Si $f : R \to A$ es homomorfismo de anillos, entonces $kerf \leq R$ ideal y $imf \subseteq A$ subanillo y $R/kerf \cong imf$.

***Demostración.*** Sea $\varphi : R/I \to A$, con $I = kerf$ definida como $r + I \to \varphi(r + I) = f(r)$. Así definida $\varphi$ es un isomorfismo de grupos abelianos, para el cual $\varphi(1 + r) = f(1_R) = 1_A$. Además

$$\varphi(r + I)\varphi(s + I) = f(r)f(s) = f(rs) = \varphi(rs + I) = (\varphi(r + I)\varphi(s + I)).$$

■

**Definición 2.8.2**
Si $K$ es un campo. La intersección de todos los subcampos de $K$ es llamado el campo primo de $K$.

Cualquier subcampo de $\mathbb{C}$ contiene a $\mathbb{Q}$. Entonces el campo primo de $\mathbb{C}$ y $\mathbb{R}$ es $\mathbb{Q}$.

**Proposición 2.8.1**
Si $K$ es un campo, entonces su campo primo es isomorfo a $\mathbb{Q}$ ó $\mathbb{Z}_p$. Para algún primo $p$.

***Demostración.*** Consideremos $\mathcal{X} : \mathbb{Z} \to K$, un homomorfismo de anillos definido como $n \to \mathcal{X}(n) = n\epsilon$; donde $\epsilon$ es la unidad en $K$.

Como $\mathbb{Z}$ es dominio de ideales principales, entonces existe $m \in \mathbb{Z}$ tal que tal que $ker\mathcal{X} = (m)$.

Si $m = 0$, entonces $\mathcal{X}$ es inyectivo por lo cual debe existir una copia isomorfica de $\mathbb{Z}$ que es un subanillo de $K$; Sea esta copia $\mathcal{Z}$ y $\mathcal{Q} = Frac(\mathcal{Z})$, entonces $\mathcal{Q} \subseteq K$ y $\mathcal{Q} \simeq \mathbb{Q}$.

Observe que $im\mathcal{X} \subseteq \mathcal{Q} \subseteq K$. Puesto que cualquier subcampo de $K$ contiene a $\epsilon$, entonces contiene a $im\chi$ por lo cual contiene a $\mathcal{Q} \simeq \mathbb{Q}$. Si $m \neq 0$, tenemos que $im\chi \simeq \mathbb{Z}/(m) = \mathbb{Z}_m$ puesto que $K$ es campo tenemos que $im\chi$ es un dominio entero, por lo tanto $m$ es primo. Además $im\chi = \{0, \epsilon, 2\epsilon, \ldots, (p-1)\,\epsilon\} \simeq \mathbb{Z}_p$ es un subcampo de $K$. Claramente, $im\chi$ es el campo primo de $K$, ya que para cualquier subcampo de $K$ que contiene a $\epsilon$ contiene a $im\chi$, por lo tanto $im\chi \simeq \mathbb{Z}_p$ es el campo primo de $K$. ■

**Definición 2.8.3**
Un campo $k$ tiene característica 0 si su campo primo es isomorfo a $\mathbb{Q}$; un campo $k$ tiene característica $p$ si tiene campo primo isomorfo a $\mathbb{Z}_p$ para algún primo $p$.

Los campos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ tienen característica 0, cualquier campo finito tiene característica $p$.

**Proposición 2.8.2**
Si $k$ es un campo de característica $p > 0$, entonces $pa = 0$ para todo $a \in k$.

***Demostración.*** Como $k$ es de característica $p$, tenemos que $p \cdot 1 = 0$ pero $1 \in k$, además $1 \cdot a = a$, por lo tanto $pa = p(1a) = (p1) \cdot a = 0 \cdot a = 0$. ■

**Proposición 2.8.3**
Si $k$ es un campo finito, entonces $|k| = p^n$ para algún primo $p$ y $n \geq 1$.

***Demostración.*** El campo primo de $k$, $P$ es finito, por lo que no puede ser isomorfo a el campo primo infinito $\mathbb{Q}$, por lo cual $P \simeq \mathbb{Z}_p$ para algún primo $p$.Recordemos que $k$ es espacio vectorial sobre $P$, $k$ es finitamente dimensional, y $dim_{\mathbb{Z}_p} k = n$, por lo tanto $|k| = p^n$. ■

**Proposición 2.8.4**
Sea $k$ un campo e $I = (p(x))$ un ideal principal, con $p(x)$ un polinomio no cero en $k[x]$, entonces los siguiente es equivalente:

i) $p(x)$ es irreducible;

ii) $k[x]/I$ es un campo;

iii) $k[x]/I$ es un dominio.

***Demostración.*** i) implica ii). Suponga $p(x)$ irreducible. Observe que $I = (p(x))$ es un ideal propio, así que $0 + I \neq 1 + I \in k[x]/I$. Si $f(x) + I \in k[x]/I$ no es cero, por lo tanto $f(x) \notin I$; por lo que, $f(x)$ no es múltiplo de $p(x)$, es decir $p(x) \nmid f(x)$, por lo que $p$ y $f$ son primos relativos, es decir, $(p(x), f(x)) = 1$ por lo tanto existen polinomios $s$ y $t$ con $1 = sf + tp$, por lo tanto $1 - sf \in I$ luego entonces $1 + I = sf + I = (s + I)(f + I)$. Por lo tanto todo elemento distinto de cero en $k[x]/I$ tiene inverso. Por lo tanto $k[x]/I$ es campo. ii) implica iii); por supuesto todo campo es un dominio entero.

iii) implica i) Si $k[x]/I$ es un dominio. Si $p(x)$ no es un polinomio irreducible en $k[x]$, entonces existe una factorización $p(x) = g(x)h(x)$ en $k[x]$ con $grad(g), grad(h) < grad(p)$; de aquí se sigue que $g(x) \notin I$ y $h(x) \notin I$ es decir $g(x) + I \neq 0 \neq h(x) + I$ pero

$$(g(x) + I)(h(x) + I) = p(x) + I = I$$

lo cual es una contradicción y por lo tanto $p(x)$ es irreducible. ■

**Proposición 2.8.5**
Sea $k$ un campo, sea $p(x) \in k[x]$ mónico irreducible de grado $d$, sea $K = k[x]/I$, donde $I = (p(x))$ y además $\beta = x + I \in K$:

i) Si $K$ es un campo y $k' = \{a + I : a \in k\}$ es un subcampo de $K$ isomorfo a $k$. Por lo tanto, si $k'$ se identifica con $k$. $k$ puede expresarse como subcampo de $K$.

ii) $\beta$ es una raíz de $p(x)$ en $K$.

iii) Si $g(x) \in k[x]$ y $\beta$ es una raíz de $g(x)$, entonces $p(x)|g(x)$ en $k[x]$.

iv) $p(x)$ es el único polinomio mónico irreducible con raíz $\beta$.

v) La lista $1, \beta, \beta^2, \ldots, \beta^{d-1}$ es una base de $K$ espacio vectorial sobre el campo $k$, por lo tanto $dim_k(K) = d$.

***Demostración.*** i) El anillo cociente $K = k[x]$ es un campo por proposición anterior. Además observe que $\pi : k[x] \to k[x]/I = K$ es homomorfismo de anillos. Ahora tomando la restricción $\pi|_k : k \mapsto K$, definida como $a \mapsto a + I$ es isomorfo entre $k \simeq k'$. Recordemos que $k[x]$ es dominio entero. El grado de 0 no está definido; es inyectiva pues $a + I = b + I$, entonces $a - b \in I$ si $a - b \neq 0$, entonces $a - b \in k$ sería unidad, pero es una contradicción pues $I$ es propio. Por lo tanto $a - b = 0$.

ii) Sea $p(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$, donde $a_i \in k$ para todo $i$. En $K = k[x]/I$ tenemos que

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1x + I) + \cdots + (1x^d + I) \\ &= a_0 + a_1x + \cdots + x^d + I \\ &= p(x) + I = I, \end{aligned}$$

porque $p(x) \in I = (p(x))$. Pero como $I = 0+I$ es el elemento cero de $K = k[x]/I$, por lo tanto $\beta$ es una raíz de $p(x)$.

iii) Si $p(x) \nmid g(x)$ en $k[x]$, entonces su máximo común divisor es 1, ya que $p(x)$ es irreducible. Por lo tanto, existen $s(x), t(x) \in k[x]$ tal que

$$1 = s(x)p(x) + t(x)g(x)$$

puesto que $k[x] \subseteq K[x]$, podemos considerar esta ecuación en $K[x]$. Evaluando en $\beta$ nos llevará a la contradicción de que $1_K = 0_K$.

iv) Sea $h(x) \in k[x]$ un polinomio mónico ireducible con $\beta$ como raíz. Por la parte anterior, tenemos que $p(x)|h(x)$. Cómo $h(x)$ es irreducible, tenemos que $h(x) = cp(x)$ para alguna constante $c \in k$; luego como $h(x)$ y $p(x)$ son mónicos, tenemos que $c = 1$ por lo tanto $h(x) = p(x)$.

Todos los elementos de $K$ son de la forma $f(x) + I$, donde $f(x) \in k[x]$. Por el algoritmo de la división, existen polinomios $q(x), r(x) \in k[x]$ con $f(x) = q(x)p(x) + r(x)$ y $r(x) = 0$ ó $deg(r) < d = deg(p)$. Ahora como $f - r = qp \in I$ se tiene que $f(x) + I = r(x) + I$. Si $r(x) = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$, con $b_i \in k$ para todo $i$, luego podemos ver que $r(x) + I = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$, por lo tanto $\{1, \beta, \ldots, \beta^{d-1}\}$ generan a $K$.

Para probar la unicidad, suponga que

$$b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1} = c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}$$

definimos $g(x) \in k[x]$ por $g(x) = \sum_{i=0}^{d-1}(b_i - c_i)x^i$; si $g(x) = 0$ hemos terminado. Suponga que $g(x) \neq 0$, observe que $g(\beta) = 0$, entonces $p|g$, entonces $grad(p) < grad(g)$ pero es una contradicción. Por lo tanto $g(x) = 0$, entonces $b_i = c_i$ para todo $i$; de aquí se sigue que $\{1, \beta, \beta^2, \ldots, \beta^{d-1}\}$ es base de $K$. ■

**Definición 2.8.4**
Si $K$ es un campo que contiene a $k$ como un subcampo, entonces $K$ es llamado un (campo) extensión de $k$ y lo escribiremos $K/k$ es una extensión de campo.

Una extensión de campo $K$ de un campo $k$ es una extensión finita de $k$ si $K$ es un espacio vectorial de dimensión finita sobre $k$. La dimensión de $K$, denotado por $[K : k]$, es llamado grado de la extensión $K/k$.

**Ejemplo 80**
El polinomio $x^2 + 1 \in \mathbb{R}[x]$ es irreducible luego entonces $K = \mathbb{R}[x]/(x^2 + 1)$ es un campo de extensión de $\mathbb{R}$ de grado 2. Si $\beta$ es una raíz de $x^2 + 1$, entonces $\beta^2 = -1$; por otro lado , todo elemento de $K$ tiene una única expresión de la forma $a+b\beta$, donde $a, b \in \mathbb{R}$, como podemos ver esta es una forma de construir $\mathbb{C}$.

Para ver que existe un isomorfismo $K \to \mathbb{C}$. Considere la evaluación $\varphi : \mathbb{R}[x] \to \mathbb{C}$, definido como $f(x) \mapsto f(i)$.

Primero; $\varphi$ es sobreyectiva, pues $a + bi = \varphi(a + bx) \in im\varphi$. Segundo; tenemos que $ker\varphi = \{f(x) \in \mathbb{R}[x] : f(i) = 0\}$, el conjunto de todos los polinomios que tienen $i$ como raíz. Sabemos que $x^2+1 \in ker\varphi$, así que $(x^2+1) \subseteq ker\varphi$. Por otro lado, ahora si tomamos $g(x) \in ker\varphi$. Si $i$ es una raíz de $g(x)$ y su máximo común divisor $(g, x^2+1) \neq 1$ en $\mathbb{C}[x]$; por lo tanto $(g, x^2+1) \neq 1$ en $\mathbb{R}[x]$ por la irreductibilidad de $x^2 + 1$ en $\mathbb{R}[x]$ da $x^2 + 1|g(x)$, y por lo tanto $g(x) \in (x^2 + 1)$ por lo tanto $ker\varphi = (x^2 + 1)$. Por último el primer terema de isomorfismos nos da que $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$

**Definición 2.8.5**
Sea $K/k$ una extensión de campo. Un elemento $\alpha \in K$ es algebraico sobre $k$ si existe un polinomio no cero $f(x) \in k[x]$ tal que $\alpha$ es una de sus raíces; en caso contrario decimos, $\alpha$ es trascendental sobre $k$. Una extensión es algebraica si todo $\alpha \in K$ es algebraico sobre $k$.

**Proposición 2.8.6**
Si $K/k$ es una extensión de campo finita, entonces $K/k$ es una extensión algebraica.

***Demostración.*** Por definición, $K/k$ finito significa que $[K : k] = n < \infty$; esto es, $K$ es un espacio vectorial sobre $k$ que tiene dimensión $n$. La lista de $n+1$ vectores $1, \alpha, \alpha^2, \ldots, \alpha^n$ es linealmente dependiente. Para todo $\alpha \in K$, entonces existen $c_0, c_1, \ldots, c_n \in k$ no todos cero, tal que $\sum c_i \alpha^i = 0$. Por lo tanto el polinomio $f(x) = \sum c_i x^i$ es distinto de cero, y $\alpha$ es una raíz de $f(x)$ por lo tanto, $\alpha$ es algebraico sobre $k$. ■

**Definición 2.8.6**
Si $K/k$ es una extensión y $\alpha \in K$, entonces $k(\alpha)$ es la intersección de todos los subcampos de $K$ que contienen a $k$ y a $\alpha$.

$k(\alpha)$ es el subcampo de $K$ que se obtiene de $k$ adjuntando $\alpha$ en $k$.

Análogamente si $A \subseteq K$ subconjunto no necesariamente finito; $k(A)$ es el subcampo de $K$ que se obtiene de $k$ adjuntando $A$ en $k$.

En particular si $A = \{z_1, \ldots, z_n\}$ es un subconjunto finito, entonces $k(A)$ es el subcampo más chico de $K$ que contiene a $A$ y $k$.

**Teorema 2.8.3**
i) Si $K/k$ es una extensión y $\alpha \in K$ es algebraico sobre $k$, entonces existe un polinomio irreducible y mónico único $p(x) \in k[x]$ que tiene $\alpha$ como una raíz. Más aun, si $I = (p(x))$, entonces $k[x]/I \simeq k(\alpha)$; de hecho existe un isomorfismo

$$\varphi : k[x]/I \to k(\alpha)$$

tal que $\varphi(x + I) = \alpha$ y $\varphi(c + I) = c$ para todo $c \in k$.

ii) Si $\alpha' \in K$ es otra raíz de $p(x)$, entonces hay un isomorfismo

$$\theta : k(\alpha) \to k(\alpha').$$

tal que $\theta(\alpha) = \alpha'$ y $\theta(c) = c$ para todo $c \in k$.

***Demostración.*** i) Considere la evaluación, el homomorfismo de anillos $\varphi : k[x] \to K$ definido como

$$\varphi : f(x) \mapsto f(\alpha).$$

recordemos que $im\varphi \subseteq K$ subanillo, que consiste de todos los polinomios en $\alpha$. Además el $ker\varphi \leq k[x]$ es un ideal que consiste de todos los polinomios $f(x) \in k[x]$ que tienen a $\alpha$ como raíz. Como todo ideal en $k[x]$ es un ideal principal, tenemos que $ker\varphi = (p(x))$ para algún polinomio mónico en $k[x]$. Pero $k[x]/(p(x)) \simeq im\varphi$ el cual es un dominio, entonces $p(x)$ es irreducible, por lo anterior $k[x]/p(x)$ es un campo, por lo tanto $im\varphi$ es subcampo de $K$ que contiene a $k$ y $\alpha$.

Ahora cualquier subcampo que contiene a $k$ y $\alpha$ contiene $im\varphi$, entonces $im\varphi = k(\alpha)$. La unicidad de $p(x)$ está dada por la Proposición 2.8.5

ii) Tenemos de la parte anterior i), que existen isomorfismos $\varphi : k[x]/I \to k(\alpha)$ y $\Phi : k[x]/I \to k(\alpha')$ tales que $\varphi(c + I) = c$ y $\Phi(c) = c + I$ para toda $c \in k$; además $\varphi : x + I \mapsto \alpha$ y $\Phi : x + I \mapsto \alpha'$, entonces la composición $\theta = \Phi\varphi^{-1}$ es el isomorfismo deseado. ■

**Definición 2.8.7**
Si $K/k$ es una extensión de campo y $\alpha \in K$ es algebraico sobre $k$, entonces el único polinomio mónico irreducible $p(x) \in k[x]$ que tiene $\alpha$ como una raíz es llamado polinomio mínimo de $\alpha$ sobre $k$ y se denota como

$$irr(\alpha, k) = p(x).$$

Por ejemplo $irr(i, \mathbb{R}) = x^2 + 1$, mientras que $irr(i, \mathbb{C}) = x - i$.

**Teorema 2.8.4**
Sea $k \subseteq E \subseteq K$ campos, con $E$ extensión finita de $k$ y $K$ extensión finita de $E$. Entonces $K$ es extensión finita de $k$ y

$$[K : k] = [K : E][E : k].$$

***Demostración.*** Si $A = \{a_1, \ldots, a_n\}$ es base de $E$ sobre $k$ y si $B = \{b_1, \ldots, b_m\}$ es una base de $K$ sobre $E$, entonces es suficiente con probar que una lista $X$ de todo $a_i b_j$ es una base de $K$ sobre $k$.

Sea $u \in K$, puesto que $B$ es una base de $K$ sobre $E$, existen escalares $\lambda_i \in E$ tales que $u = \sum_j \lambda_j b_j$. Puesto que $A$ es base de $E$ sobre $k$, existen escalares $\mu_{ji} \in k$ con $\lambda_j = \sum_i \mu_{ji} a_i$. Por lo tanto $u = \sum_{ij} m_{ji} a_i b_j$. Por lo tanto $\{a_i bj\}$ generan a $K$ sobre $k$.

Veamos la independencia lineal. Suponga que existen $\mu_{ji} \in k$ con

$$\sum_{ij} \mu_{ji} a_i b_j = 0.$$

Si definimos, $\lambda_j = \sum_i \mu_{ji} a_i \in E$ y $\sum_j \lambda_j b_j = 0$, entonces, por la independencia lineal de $B$, $\lambda_j = 0$ para todo $j$ de donde, por la independencia lineal de $A$, obtenemos que $\mu_{ji} = 0$. ■

**Ejemplo 81**
Sea $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Las posibles raíces racionales de $f(x)$ son $\pm 1$, pero $f(\pm 1) = -8 \neq 0$. Por lo tanto $f(x)$ no tiene factores lineales.

Observe que las raíces reales de $f(x)$ son:

$\beta^2 = 5 \pm 2\sqrt{6} = 2 \pm 2\sqrt{2}\sqrt{3} + 3$; también observe que $(\sqrt{a} \pm \sqrt{b})^2 = a \pm 2\sqrt{a}\sqrt{b} + b$, entonces $\beta = \pm\sqrt{2} \pm \sqrt{3}$ son las raíces reales de $f(x)$.

Sea $g(x)$ un factor cuadrático de $f(x)$, entonces $g(x) = (x - a\sqrt{2} - b\sqrt{3})(x - c\sqrt{2} - d\sqrt{3})$ con $a, b, c, d \in \{\pm 1\}$, luego entonces $g(x) = x^2 - ((a+c)\sqrt{2} + (b+d)\sqrt{3})x + 2ac + 3bd + (ad + bc)\sqrt{6}$.

Ahora, $(a+c)\sqrt{2} + (b+d)\sqrt{3}$ es racional si y sólo si $a + c = 0$ y $b + d = 0$, luego entonces $ad + cd = 0$ y $cb + cd = 0$, por lo cual $ad + cb = -2cd \neq 0$ por lo tanto el término constante de $g(x)$ es irracional. Por lo tanto $g(x) \notin \mathbb{Q}[x]$.

Por lo tanto $f(x)$ es irreducible en $\mathbb{Q}[x]$; por lo que $E = \mathbb{Q}(\beta) \simeq \mathbb{Q}[x]/(f(x))$. Si $\beta = \sqrt{2} + \sqrt{3}$, entonces $irr(\beta, \mathbb{Q}) = f(x)$.

Por otro lado sea $E = \mathbb{Q}(\beta)$ y sea $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , entonces $\mathbb{Q} \subseteq E \subseteq F$ extensiones de campo y

$$[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}]$$

Observe que $[E : \mathbb{Q}] = 4$. Además $[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$; puesto que $\sqrt{2}$ es raíz del polinomio mónico irreducible $x^2 - 2$ en $\mathbb{Q}[x]$, tenemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Por otro lado $[F : \mathbb{Q}(\sqrt{2})] \leq 2$, ya que si $\sqrt{3}$ pertenece a $\mathbb{Q}(\sqrt{2})$, entonces el grado de esta extensión es 1, o el polinomio $x^2 - 3$ es irreducible en $\mathbb{Q}(\sqrt{2})[x]$ por lo tanto $[F : \mathbb{Q}] \leq 4$, pero $[E : \mathbb{Q}] = 4$, luego entonces $[F : \mathbb{Q}] = 4$, de aquí tenemos $[F : E] = 1$, por lo tanto $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Es decir $F$ se obtiene de $\mathbb{Q}$ adjuntando las raíces de $f$ pero también adjuntando las raíces de $(x^2 - 2)(x^2 - 3)$.

**Teorema 2.8.5 (Kronecker)**
Si $k$ es un campo y $f(x) \in k[x]$, entonces existe un campo $K$ tal que $k \subseteq K$ como subcampo en el cual $f(x)$ se descompone como producto de polinomios lineales en $K[x]$.

***Demostración.*** La prueba será por inducción sobre $grad(f)$. Si $grad(f) = 1$, entonces $f(x)$ es lineal, es decir, $K = k$. Si $grad(f) > 1$, tenemos $f(x) = p(x)g(x)$, con $p(x)$ irreducible; sea $z$ una raíz de $p(x)$, sabemos que existe un campo $F$ que contiene a $K$ y $z$. Entonces en $F[x]$, $p(x) = (x - z)h(x)$ y $f(x) = (x - z)h(x)g(x)$. Por inducción existe $K$ un campo que contiene a $F$ en el cual $h(x)g(x)$, y por lo tanto $f(x)$ son productos de factores lineales en $K[x]$. ■

**Definición 2.8.8**
Sea $k \subseteq K$ y sea $f(x) \in k[x]$. Diremos que $f(x)$ divide sobre $K$ si

$$f(x) = a(x - z_1) \dots (x - z_n),$$

con $z_1, \dots, z_z \in K$ y $a \in k$ distinto de cero.

$K$ es el campo de descomposición de $f/k$. Si $f$ no se descompone sobre ningún subcampo propio de $K$.

Por ejemplo, considere $x^2+1 \in \mathbb{Q}[x]$ se descompone totalmente en $\mathbb{C}$ sin embargo el campo de descomposición es $\mathbb{Q}(i)$; el campo de descomposición de $x^2+1 \in \mathbb{R}[x]$ es $\mathbb{R}(i) = \mathbb{C}$. En un ejemplo anterior vimos que $E = (\sqrt{2} + \sqrt{3})$ es campo de descomposición de los polinomios $f(x) = x^4 - 10x^2 + 1$ y $g(x) = (x^2 - 2)(x^2 - 3)$. La existencia de un campo de descomposición es una consecuencia del teorema de Kronecker

**Corolario 2.8.2**
Sea $k$ un campo, y sea $f(x) \in k[x]$. Entonces un campo de descomposición de $f(x)$ sobre $k$ existe.

***Demostración.*** Por el teorema de Kronecker existe $K/k$ tal que $f(x)$ se descompone en $K[x]$; es decir, $f(x) = a(x - \alpha_1) \dots (x - \alpha_n)$. El subcampo $E = k(\alpha_1, \dots, \alpha_n)$ de $K$ es el campo de descomposición de $f$ sobre $k$. ■

**Proposición 2.8.7**
Sea $p$ un primo, y sea $k$ un campo. Si $f(x) = x^p - c \in k[x]$ y $\alpha$ es una raíz $p$-ésima de $c$ (en algún campo de descomposición), entonces $f(x)$ es irreducible en $k[x]$ ó $c$ tiene una raíz $p$-ésima en $k$. En cualquier caso, si $k$ contiene las raíces $p$-ésimas de la unidad, entonces $k(\alpha)$ es un campo de descomposición de $f(x)$.

***Demostración.*** Por el teorema de Kronecker existe una extensión de campo $K/k$ que contiene a todas las raíces de $f(x)$. Si $\alpha^p = c$, entonces cualquier raíz $p$-ésima de $c$ es de la forma $w\alpha$, donde $w$ es una raíz $p$-ésima de 1, es decir, $w$ es raíz de $x^p - 1$.

Si $f(x)$ no es irreducible en $k[x]$, entonces existe una factorización $f(x) = g(x)h(x)$ en $k[x]$ con $g(x)$ no constante y $d = grad(g) < p$.

Sea $\beta$ el término constante de $g(x)$, es el producto de algunas de las raíces de $f(x)$:

$$\pm b = \alpha^d w \text{ con alguna raíz } p\text{-ésima de 1,}$$

observe que $(\pm b)^p = (\alpha^d w)^p = c^d$.

Ahora $p$ es primo y $d < p$, luego entonces $(d, p) = 1$, entonces existen $s, t \in \mathbb{Z}$ tal que $1 = sd + tp$, entonces

$$c = c^{sd+tp} = c^{sd} c^{tp} = (\pm b)^{ps} c^{tp} = (\pm b^s c^t)^p$$

y $\pm b^s c^t \in k$. Por lo tanto $k$ contiene una raíz $p$-ésima de $c$.

Si $\alpha$ es una raíz $p$-ésima de $c$, entonces $f(x) = \prod_w (x - w\alpha)$, $w$ corre sobre las raíces $p$-ésimas de la unidad. Asumiendo que $w \in k$, para toda raíz $p$-ésima de 1, entonces $k(\alpha)$ es campo de descomposición de $f(x)$. ■

**Ejemplo 82**
Para todo primo $p$, $x^p - 2$ es irreducible en $\mathbb{Q}[x]$.

**Teorema 2.8.6 (Galois.)**
Si $p$ es primo y $n \in \mathbb{N}$, entonces existe un campo que contiene exactamente $p^n$ elementos.

***Demostración.*** Consideramos $q = p^n$, y el polinomio

$$g(x) = x^q - x \in \mathbb{F}_p[x]$$

por el teorema de Kronecker, existe un campo $K$ que contiene a $\mathbb{F}_p$ tal que $g(x)$ es un producto factores lineales en $K[x]$ (se descompone totalmente). Se define

$$E = \{\alpha \in K : g(x) = 0\} \subseteq K;\ \mathbb{F}_p \subseteq K$$

$K$ campo de característica $p$, entonces $pa = 0$ para todo $a \in K$. Observe que $g'(x) = p^n x^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$, luego entonces tenemos que $(g, g') = 1$, por lo cual todas las raíces de $g(x)$ son distintas, por lo tanto $|E| = p^n$.

Veamos que $E$ es campo. Sean $a, b \in E$, entonces $a^q = a$ y $b^q = b$. Por lo tanto $(ab)^q = ab \in E$. Luego tenemos que $(a - b)^q = a^q - b^q \in K$. Finalmente, $a \neq 0$, entonces $a^q = a$, por lo tanto $a^{q-1} = 1$. Por lo tanto $a^{-1} = a^{q-2} \in E$.
■

**Notación 1**
Denotaremos un campo finito con $q = p^n$ elementos para $p$ primo por $\mathbb{F}_q$.

**Corolario 2.8.3**
Para todo primo $p$ y todo entero $n \geq 1$, existe un polinomio irreducible $g(x) \in \mathbb{F}_p[x]$ de grado $n$. De hecho, si $\alpha$ es un elemento primitivo de $\mathbb{F}_{p^n}$, entonces su polinomio mínimo $g(x) = irr(\alpha, \mathbb{F}_p)$ tiene grado $n$.

***Demostración.*** Sea $E/\mathbb{F}_p$ una extensión finita con $p^n$ elementos, y sea $\alpha \in E$ un elemento primitivo. Entonces $E = \mathbb{F}_p(\alpha)$, observemos que $g(x) = irr(\alpha, \mathbb{F}_p) \in \mathbb{F}_p[x]$, con $g(\alpha) = 0$ es irreducible. Si $grad(g) = d$, entonces $[\mathbb{F}_p[x]/(g(x)) : \mathbb{F}_p] = d$, pero, $\mathbb{F}_p[x]/(g(x)) \simeq \mathbb{F}_p(\alpha) = E$ y $[E : \mathbb{F}_p] = n$, por lo tanto $n = d$, por lo tanto $g(x)$ es irreducible de grado $n$ en $\mathbb{F}_p[x]$. ■

**Ejemplo 83**
Si

$$k = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{Z}_2 \right\} \text{ es campo y } |k| = 4$$

ahora sea $q(x) = x^2+x+1 \in \mathbb{F}_2[x]$ irreducible mónico, entonces $F = \mathbb{F}_2[x]/(q(x))$ campo con base $\{1 + \langle q(x)\rangle, x + \langle q(x)\rangle\}$; por lo tanto los elemntos de $F$ son de la forma $a + bz$ y $a, b \in \mathbb{Z}_2$, con $z = x + \langle q(x)\rangle$.

Observe que $z$ es raíz de $q(x)$ en $F$, entonces $0 = z^2 + z + 1 \in F$ y $z^3 = zz^2 = z(z + 1) = z^2 + z = 1$. Por lo tanto $z^2 = z + 1$ y $z^3 = 1$.

Se puede ver que

$$\varphi : k \to F \text{ es isomorfismo de anillos}$$

con

$$\varphi\left( \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} \right) = a + bz.$$

**Lema 2.8.1**
Sea $f(x) \in k[x]$, donde $k$ es un campo y sea $E$ campo de descomposición de $f(x)$ sobre $k$. Sea $\varphi : k \to k'$ un isomorfismo de campos, sea $\varphi^* : k[x] \to k'[x]$ el isomorfismo

$$g(x) = a_0 + a_1x + \cdots + a_nx^n \to g^*(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

Sea $E'$ el campo de descomposición de $f^*(x)$ sobre $k'$, entonces existe un isomorfismo $\Phi : E \to E'$ que extiende $\varphi$.

$$\begin{array}{ccc} E & \overset{\Phi}{\cdots\cdots\blacktriangleright} & E' \\ \vert & & \vert \\ k & \xrightarrow[\varphi]{} & k' \end{array}$$

***Demostración.*** Por inducción en $d = [E, k]$. Si $d = 1$, entonces $f(x)$ se descompone en factores lineales en $k[x]$, entonces se sigue que $f^*(x)$ se descompone en factores lineales en $k'[x]$. Por lo tanto $\Phi = \varphi$ y $k = E \to k' = E'$.

Ahora sea $d > 1$ y $\varphi : k \to k'$ isomorfismo, entonces $\varphi^* : k[x] \to k'[x]$ isomorfismo de anillos. Sea $f(x) = p(x)g(x)$ con $p(x) \in k[x]$ irreducible mónico por lo tanto $f^*(x) = p^*(x)g^*(x)$ y $p^*(x) \in k'[x]$.

Sea $z$ raíz de $p(x)$ y $z'$ raíz de $p^*(x)$, entonces

$$k(z) \simeq \frac{k[x]}{(p(x))} \simeq \frac{k'[x]}{(p^*(x))} \simeq k'(z').$$

Para el paso inductivo, sea $z$ raíz de $f(x)$ en $E$ sobre $k$ y sea $p(x) = irr(z, k)$. Observe que $grad(p) > 1$ pues $z \notin k$. Además $[k(z) : k] = grad(p)$.

Sea $z'$ una raíz de $f^*(x)$ en $E'$ sobre $k'$ y $p^* = irr(z', k')$ el correspondiente polinomio mónico irreducible en $k'[x]$. Entonces existe un isomorfismo entre

$$\widetilde{\varphi} : k(z) \to k'(z')$$

$\widetilde{\varphi}$ extiende $\varphi$ con $\widetilde{\varphi}(z) = z'$ observe que $f(x)$ es un polinomio con coeficientes en $k(z)$ pues $k \subseteq k(z)$ y $k[x] \subseteq k(z)[x]$ podemos decir que $E$ es campo de descomposición sobre $k(z)$; esto es

$$E = k(z)(z_1, \ldots, z_n)$$

donde $z_1, \ldots, z_n$ son raíces de $f(x)/(x - z)$; después de todo

$$E = k(z, z_1, \ldots, z_n) = k(z)(z_1, \ldots, z_n).$$

Similarmente, $E'$ es campo de descomposición $f^*(x)$ sobre $k'(z')$. Pero $[E : k(z)] < [E : k]$ por hipótesis de inducción existe $\Phi : E \to E'$ isomorfismo que extiende $\widetilde{\varphi}$ y entonces extiende a $\varphi$. ■

**Teorema 2.8.7**
Si $k$ es un campo y $f(x) \in k[x]$, entonces cualesquiera dos campos de descomposición de $f(x)$ sobre $k$ son isomorfos con un isomorfismo que fija $k$ punto a punto.

***Demostración.*** Sea $E$ y $E'$ campos de descomposición de $f(x)$ sobre $k$ tomando $\varphi = k \to k$, definido como $a \to a$; la identidad del lema anterior, se obtiene el resultado. ■

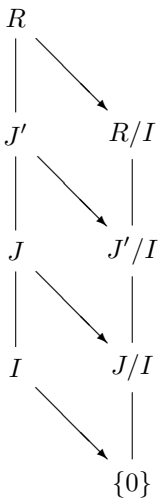
**Corolario 2.8.4**
Cualesquiera dos campos finitos de $p^n$ elementos, son isomorfos.

***Demostración.*** Si $E$ es un campo con $q = p^n$ elementos , el teorema de Lagrange aplicado en $E^*$, entonces cualquier elemento de $E$ es raíz del polinomio $f(x) = x^q - x \in \mathbb{F}_p[x]$. Por lo tanto $E$ es campo de descomposición de $f(x)$. Cualquier campo de $p^n$ elementos es campo de descomposición de $f(x)$ y por teorema anterior cualesquiera dos campos de $p^n$ elementos son isomorfos. ■

## 2.9. Ideales primos y maximales.

**Proposición 2.9.1 (Teorema de la correspondencia.)**
Si $I$ es un ideal propio en un anillo conmutativo $R$, entonces existe una biyección que conserva inclusión, es decir, $\{J \leq R \text{ ideales} : I \subseteq J \subseteq R\} \leftrightarrow$

{Ideales de $R/I$} donde $\pi : R \to R/I$ es el mapeo natural y $\varphi : J \mapsto \pi(J) = J/I = \{a + I : a \in J\}$.




***Demostración.*** Consideremos a $(R, +)$ sólo como grupo abeliano y $I \subseteq R$ como subgrupo. El teorema de correspondencia de grupos nos proporciona una biyección que preserva inclusión. Sea $\Phi$:{Todos los subgrupos de $R$ que contienen a $I$}$\to$ {todos los subgrupos de $R/I$}; donde $\Phi(J) = \Pi(J) = J/I$.

Si $J \subseteq R$ es un ideal, entonces $\Phi(J) \leq R/I$ ideal. Para todo $r \in R$ y $a \in J$ tenemos que $ra \in J$, por lo tanto $(r + I)(a + I) = ra + I \in J/I$. Sea

$$\varphi = \Phi|_{\text{Todos los ideales en } I \leq J \leq R}$$

note que $\varphi$ es inyectiva por que $\Phi$ también lo es. Para mostrar que $\varphi$ es sobreyectiva; sea $J^* \leq R/I$ un ideal.

Ahora $\Pi^{-1}(J^*)$ es un ideal entre $I$ y $R$ ($\Pi^{-1}(J^*)$ contiene a $I = \Pi^{-1}(\{\overline{0}\}) \subseteq \Pi^{-1}(J)$). Además $\varphi(\Pi^{-1}(J^*)) = \Pi(\Pi^{-1}(J^*)) = J^*$. Por lo tanto es sobreyectiva. Es decir, cualquier ideal de $R/I$ tiene la forma $J/I$ para algún $J$ con $I \subseteq J \subseteq R$ ideal. ■

**Ejemplo 84**
Sea $I = (m)$ un ideal no nulo y $m \in \mathbb{Z}$. Si $J$ es un ideal en $\mathbb{Z}$ que contiene a $I$. Sabemos que $J = (a)$ para algún $a \in \mathbb{Z}$ pues $\mathbb{Z}$ es dominio de ideales principales y $(m) \subseteq (a)$, entonces $a|m$. Por el teorema de la correspondencia, cualquier ideal en $\mathbb{Z}_m$ tiene la forma $([a])$ para algún divisor $a$ de $m$.

**Definición 2.9.1**
Un ideal $I$ en un anillo conmutativo $R$ es llamado un ideal primo, si $I \nleq R$ y $ab \in I$, entonces $a \in I$ o $b \in I$.

**Ejemplo 85**
Algunos ejemplos de ideales primos.

1) $R$ anillo conmutativo no cero es un dominio entero si y sólo si $ab = 0$, entonces $a = 0$ o $b = 0$. Por lo tanto el ideal $(0) = \{0\} \leq R$ es un ideal primo si y sólo si $R$ es dominio entero.

2) Los ideales primos de $\mathbb{Z}$ son $(p)$ con $p$ un primo o $p = 0$. Observe que $(m) = (-m)$ generan el mismo ideal principal; así que restringimos nuestra atención a generadores no negativos. Si $p = 0$, el resultado se sigue de 1) para $\mathbb{Z}$ un dominio.

Si $p > 0$ primo, observe que $(p)$ es un ideal propio pues de lo contrario $1 \in (p)$, entonces existe $ap = 1$, pero esto es una contradicción. Ahora si $ab \in (p)$, entonces $p|ab$; por el lema de Euclides $p|a$ o $p|b$, esto es $a \in (p)$ o $b \in (p)$. Por lo tanto $(p)$ es un ideal primo.

Contrariamente, si $m > 1$ no es primo, entonces $m = ab$ para $0 < a < m$ y $0 < b < m$; entonces ni $a$ ni $b$ son múltiplos de $m$ y por lo tanto $a \notin (m)$ y $b \notin (m)$. Pero $ab = m \in (m)$. Por lo tanto $(m)$ no es ideal primo.

**Proposición 2.9.2**
Un ideal $I$ en un anillo conmutativo $R$ es un ideal primo si y sólo si $R/I$ es un dominio.

***Demostración.*** Necesidad. Sea $I$ un ideal primo. Como $I$ es un ideal propio, entonces tenemos que $1 \notin I$ y por lo tanto $1 + I \neq 0 + I$ en $R/I$.

Si $(a + I)(b + I) = 0 + I$, entonces $ab \in I$. Como $I$ es un ideal primo, entonces $a \in I$ o $b \in I$, entonces $a + I = 0 + I$ o $b + I = 0 + I$. Por lo tanto $I$ es primo, entonces $R/I$ es dominio entero.

Suficiencia. Si $R/I$ es dominio entero, tenemos que $1 + I$ es distinto de $0 + I$, por lo que 1 no pertenece a $I$, entonces $I$ es un ideal propio en $R$. Ahora, sean $a, b \in R$ tales que $ab \in I$, entonces $ab + I = 0 + I$ por lo que $a + I = 0 + I$ o $b + I = 0 + I$, con lo cual $a \in I$ o $b \in I$. ■

**Proposición 2.9.3**
Si $k$ es un campo, entonces un polinomio no cero $p(x) \in k[x]$ es irreducible si y sólo si $(p(x))$ es un ideal primo.

***Demostración.*** Tenemos que $p(x) \in k[x]$ es irreducible si y sólo si $k[x]/(p(x))$ dominio entero si y sólo si $(p(x))$ es ideal primo. ■

**Definición 2.9.2**
Un ideal $I$ en un anillo conmutativo es ideal máximo si es un ideal propio y no existe un ideal $J$ tal que $I \subsetneq J \subsetneq R$.

**Ejemplo 86**
El ideal $\{0\}$ es máximo si y sólo si $R$ es campo.

**Proposición 2.9.4**
Un ideal propio $I$ en un anillo conmutativo no cero $R$ es ideal máximo si y sólo si $R/I$ es un campo.

***Demostración.*** Por el teorema de la correspondencia para anillos se puede ver que $I$ es máximo si y sólo si $R/I$ no tiene otros ideales más que $I/I$ y $R/I$ si y sólo si $R/I$ es campo. ■

**Corolario 2.9.1**
Todo ideal maximal $I$ en un anillo conmutativo $R$ es un ideal primo.

***Demostración.*** Si $I$ es un ideal máximo, entonces $R/I$ es un campo. Luego, como todo campo es dominio entero, $R/I$ es un dominio entero, y por lo tanto $I$ es un ideal primo. ■

**Ejemplo 87**
El inverso del corolario anterior es falso. Por ejemplo; considere el ideal principal $(x) \in \mathbb{Z}$, observe que $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$; donde $\mathbb{Z}$ es dominio entero, entonces $(x)$ es ideal primo en $\mathbb{Z}[x]$. Sin embargo $\mathbb{Z}$ no es campo, entonces $(x)$ no es ideal máximo.

**Ejemplo 88**
Sea $k$ un campo y $a = (a_1, \ldots, a_n) \in k^n$. Definimos el mapeo evaluación como

$$e_a : k[x_1, \ldots, x_n] \to k$$

por

$$e_a : f(x_1, \ldots, x_n) = f(a_1, \ldots, a_n).$$

Tenemos que $e_a$ es homomorfismo sobreyectivo de anillos, entonces

$$k \simeq \frac{k[x_1, \ldots, x_n]}{ker\ e_a}$$

por lo tanto $ker\ e_a$ es máximo.

**Teorema 2.9.1**
Si $R$ es un dominio de ideales principales, entonces cualquier ideal primo no nulo $I$ es un ideal máximo.

***Demostración.*** Asuma que existe un ideal propio $J$ tal que $I \subseteq J$. Como $R$ es dominio de ideales principales, $I = (a)$ y $J = (b)$ para $a, b \in R$. Ahora $a \in J$, entonces $a = rb$ para algún $r \in R$, entonces $rb \in I$; pero, $I$ es un ideal primo por lo tanto $r \in I$ o $b \in I$.

Si $r \in I$, entonces $r = sa$ para algún $s \in R$ y $a = sab$, entonces $sb = 1$ pertenece a $J$, por lo tanto $J = R$. Si $b \in I$, entonces $J \subseteq I$, por lo tanto $I = J$. ■

**Proposición 2.9.5**
Sea $R$ un anillo conmutativo y $P$ un ideal primo. Si $I, J$ son ideales con $IJ \subseteq P$, entonces $I \subseteq P$ o $J \subseteq P$.

***Demostración.*** Suponga que $I \not\subseteq P$ y $J \not\subseteq P$, entonces existe $a \in I$ y $b \in J$ con $a, b \notin P$. Pero $ab \in IJ \subseteq P$, lo cual contradice el hecho de que $P$ es primo. ■

**Proposición 2.9.6**
Sea $B$ un subconjunto de un anillo conmutativo $R$ el cual es cerrado bajo suma y producto:

i) Sea $J_1, \ldots, J_n$ ideales en $R$, y por lo menos $n-2$ de ellos son primos. Si $B \subseteq J_1 \cup \cdots \cup J_n$, entonces $B$ está contenido en algún $J_i$.

ii) Sea $I$ un ideal en $R$ con $I \subsetneq B$. Si hay ideales primos $P_1, \ldots, P_n$ tal que $B - I \subseteq P_1 \cup \cdots \cup P_n$, entonces $B \subseteq P_i$ para algún $i$.

***Demostración.*** i) Por inducción sobre $n \geq 2$. Para el caso base tenemos que $n = 2$, entonces ninguno de los ideales $J_1$ o $J_2$ necesita ser primo. Si $B \not\subseteq J_2$, entonces existe $b_1 \in B$ tal que $b_1 \notin J_2$; como $B \subseteq J_1 \cup J_2$, entonces $b_1 \in J_1$. Similarmente, si $B \not\subseteq J_1$, existe $b_2 \in B$ con $b_2 \notin J_1$ y $b_2 \in J_2$. Sin embargo, si $y = b_1 + b_2 \in B$, entonces $y \notin J_1$ de otro modo, $b_2 = y - b_1 \in J_1$ (porque ambos $y$ y $b_1$ están en $J_1$). De forma similar, $y \notin J_2$, lo cual contradice el hecho de que $B \subseteq J_1 \cup J_2$.

Para el paso inductivo, asuma que $B \subseteq J_1 \cup \cdots \cup J_{n+1}$, donde al menos $n - 1 = (n+1) - 2$ para algún $J_i$ son ideales primos. Sea

$$D_i = J_1 \cup \cdots \cup \widehat{J_i} \cup \cdots \cup J_{n+1}.$$

Como $D_i$ es una unión de $n$ ideales al menos $(n-1) - 1 = n - 2$ de ellos es primo, supongamos que $B \not\subseteq D_i$ para todo $i$. Por lo tanto, para todo $i$ existe $b_i \in B$ con $b_i \notin D_i$; como $B \subseteq D_i \cup J_i$, tendremos que $b_i \in J_i$. Ahora sea $n \geq 3$, entonces al menos uno de los $J_i$ es un ideal primo; por notación asuma que $J_1$ es primo. Considere el elemento

$$y = b_1 + b_2 b_3 \cdots b_{n+1}.$$

Como todos los $b_i \in B$ y $B$ es cerrado bajo la suma y producto, $y \in B$. Ahora $y \notin J_1$; sino de otra forma $b_2 b_3 \cdots b_{n+1} = y - b_1 \in J_1$. Como $J_1$ es primo, algún $b_i \in J_1$ para $i \neq 1$. Esto es una contradicción, pues $b_i \notin D_i \supseteq J_1$. Si $i > 1$ y $y \in J_i$, entonces $b_2 b_3 \cdots b_{n+1} \in J_i$ para $i \neq 1$, porque $J_i$ es un ideal, por lo tanto $b_1 = y - b_2 b_3 \cdots b_{n+1} \in J_i$. Esto no puede ser, ya que $b_1 \notin D_1 \supseteq J_i$. Por lo tanto, $y \notin J_i$ para cualquier $i$, contradiciendo el hecho de que $B \subseteq J_1 \cup \cdots \cup J_{n+1}$. Por lo anterior, obtenemos que existe un $i$ tal que $B$ está contenido en $D_i$, obteniendo el resultado por hipótesis inductiva

ii) La hipótesis nos dice que $B \subseteq I \cup P_1 \cdots \cup P_n$, así que de la parte anterior tenemos que $B \subseteq I$ o $B \subseteq P_i$. Y como $I$ es un subconjunto propio de $B$, la primera posibilidad no puede ocurrir. ■

## 2.10. Dominios de factorización única

**Definición 2.10.1**
Dos elementos $a, b$ en un anillo conmutativo $R$ serán llamado asociados si existe una unidad $u \in R$ con $b = ua$.

**Ejemplo 89**
Las unidades en $\mathbb{Z}$ son $\{1, -1\}$, y por lo tanto, los únicos asociados a cualquier entero $m \in \mathbb{Z}$ son $\{m, -m\}$; en $k[x]$ con $k$ un campo, las unidades son las constantes distintas de cero, por lo tanto los únicos asociados para el polinomio $f(x) \in k[x]$ son los polinomios $uf(x)$, con $u \in k$ y $u \neq 0$. Las únicas unidaddes en $\mathbb{Z}[x]$ son $\pm 1$, por lo tanto los únicos asociados de un polinomio $f(x) \in \mathbb{Z}[x]$ son $\pm f(x)$.

En un anillo conmutativo $R$, si $a$ y $b$ son asociados, entonces generan el mismo ideal principal; el caso contrario puede ser falso si $R$ no es un dominio.

**Proposición 2.10.1**
Sea $R$ un dominio y sean $a, b \in R$;

i) $a|b$ y $b|a$ si y sólo si $a$ y $b$ son asociados.

ii) Los ideales principales son $(a)$ y $(b)$ son iguales si sólo si $a$ y $b$ son asociados.

***Demostración.*** i) Si $a|b$ y $b|a$, entonces existen $r, s \in R$ tal que $b = ra$ y $a = sb$, por lo tanto $b = ra = rsb$. Si $b = 0$, entonces $a = 0$; si $b \neq 0$, entonces podemos cancelarlo (recuerde que $R$ es un dominio) para obtener $1 = rs$. Ahora $a = ub$ para $u \in R$ una unidad, entonces $b|a$. Similarmente $u^{-1}a = b$ para $u^{-1}$ unidad, entonces $a|b$.

ii) Necesidad. Si $(a) = (b)$, entonces $a \in (b)$; como, $a = rb$ para algún $r \in R$, y por lo tanto $b|a$. Similarmente, $b \in (a)$ implica que $a|b$, y por i) vemos que que

$a$ y $b$ son asociados.

Suficiencia. Si $a = ub$, con $u$ una unidad, entonces $a \in (b)$ y $(a) \subseteq (b)$. De forma similar $b = u^{-1}a$ implica $(b) \subseteq (a)$, y por lo tanto $(a) = (b)$. ■

**Observación 51**
Recuerde que un elemento $p$ en un dominio entero $R$ es irreducible si es distinto de 0, no unidad y sus únicos factores son unidades o asociados.

**Corolario 2.10.1**
Si $R$ es un dominio de ideales principales y $p \in R$ es irreducible, entonces $(p)$ es un ideal primo.

***Demostración.*** Veamos que $(p)$ es máximo. Sea $I$ un ideal tal que $(p) \subseteq I$. Como $R$ es dominio de ideales principales, existe un $q \in R$ tal que $I = (q)$. Además como $p \in (q)$, entonces $p = qr$ para algún $r \in R$. Como $p$ es irreducuble nos dice que $q$ es un asociado o una unidad.En el primer caso, $(p) = (q)$; ahora en el segundo caso $(q) = R$. Se sigue que $(p)$ es un ideal máximo, y por lo tanto es un ideal primo. ■

**Definición 2.10.2**
Un dominio $R$ es un dominio de factorización única si:

i) Si para todo $r \in R$ distinto de cero y no es una unidad, es producto de irreducibles;

ii) Si $up_1 \cdots p_m = vq_1 \cdots q_n$, con $u$ y $v$ unidades y todo $p_i$ y $q_j$ irreducibles, entonces $m = n$ y existe una permutación $\sigma \in S_n$ con $p_i$ y $q_{\sigma(i)}$ asociados para todo $i$.

**Proposición 2.10.2**
Sea $R$ un dominio en el cual todo $r \in R$ no cero y no unidad, es un producto de irreducibles. Entonces $R$ es un dominio de factorización única si y sólo si $(p)$ es un ideal primo en $R$ para todo elemento irreducible $p \in R$.

***Demostración.*** Suponga que $R$ es un dominio de factorización única. Si $a, b \in R$ y $ab \in (p)$, entonces existe $r \in R$ tal que

$$ab = rp.$$

Factorizando cada $a, b$ y $r$ en irreducibles; por factorización única, el lado izquierdo de la ecuación tiene que involucrar un asociado a $p$, este surge como un factor de $a$ o $b$, y por lo tanto $a \in (p)$ o $b \in (p)$.

Ahora asuma que $up_1 \cdots p_m = vq_1 \cdots q_n$ con $u, v$ unidades y $p_i$, $q_i$ irreducibles. La demostración será por inducción sobre el $max\{m, n\}$.

Si $max\{m,n\} = 1$, entonces $up_1 = vq_1$, por lo tanto $p_1, q_1$ son asociados. Para el paso inductivo, la ecuación original nos muestra que $p_1|q_1 \cdots q_n$. Por hipótesis inductiva, $(p_1)$ es un ideal primo, existe algún $q_j$ con $p_1|q_j$. Pero $q_j$, es irreducible y no tiene divisores más que las unidades y los asociados, por lo tanto $q_j$ y $p_1$ son asociados y $q_j = up_1$ para alguna unidad $u$. Cancelando $p_1$ por ambos lados, tenemos $p_2 \cdots p_m = uq_1 \cdots \widehat{q_j} \cdots q_n$. Por hipótesis inductiva, $m-1 = n-1$ (así que $m = n$) y después del posible reacomodo de índices, $q_i$ y $p_i$ son asociados para todo $i$. ■

**Lema 2.10.1**
i) Si $R$ es un anillo conmutativo y

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

es una cadena ascendente de ideales en $R$. Entonces $J = \cup_{1 \leq n} I_n$ es un ideal en $R$.

ii) Si $R$ es un dominio de ideales principales, entonces no existen cadenas infinitas ascendentes de ideales

$$I_1 \subsetneq I_2 \subsetneq \cdots \subseteq I_n \subsetneq I_{n+1} \subsetneq \ldots$$

iii) Sea $R$ un dominio de ideales principales. Si $r \in R$ no es 0 o una unidad, entonces $r$ es un producto de irreducibles.

***Demostración.*** i) Afirmamos que $J$ es un ideal. Si $a \in J$, entonces $a \in I_n$ para algún $n$; si $r \in R$, entonces $ra \in I_n$, porque $I_n$ es un ideal; por lo tanto $ra \in J$. Si $a, b \in J$, entonces existe ideales $I_n$ y $I_m$ con $a \in I_n$ y $b \in I_m$; ya que la cadena es ascendente, podemos asumir que $I_n \subseteq I_m$, entonces $a, b \in I_m$. Como $I_m$ es un ideal, $a + b \in I_m$ y $a + b \in J$. Por lo tanto $J$ es un ideal.

ii) Si por el contrario, existe una cadena estrictamente ascendente infinita, entonces definimos $J = \cup_{n \geq 1} I_n$. Por i), $J$ es un ideal; y como $R$ es dominio de ideales principales, tenemos $J = (d)$ para algún $d \in J$. Ahora $d$ está dentro de $J$ por lo que $d$ pertenece a $I_n$ para algún $n$. Por lo tanto

$$J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J,$$

pero esto es una contradicción.

iii) Un divisor $r$ de un elemento $a \in R$ es llamado divisor propio de $a$ si $r$ no es unidad o no es un asociado de $a$. Si $r$ es un divisor de $a$, entonces $(a) \subseteq (r)$; si $r$ es un divisor propio, entonces $(a) \subsetneq (r)$, pues si la inecuación no es estricta, entonces $(a) = (r)$, y esto forza $a$ y $r$ ser asociados.

Vamos a llamar a un elemento no unidad y distinto de cero $a \in R$ bueno si es un producto de irreducibles; de otro modo, llamaremos al elemento $a$ malo. Mostraremos que no hay malos elementos. Si $a$ es malo, este no es irreducible,

y por lo tanto $a = rs$, donde ambos $r$ y $s$ son divisores propios. Pero el producto de buenos elementos es un buen elemento, y por lo tanto al menos uno de los factores, digamos $r$ es malo. Por lo anterior vemos que $(a) \subsetneq (r)$. Luego seguimos por inducción, que existe una sucesión $a_1 = a$, $a_2 = r$, $a_3, \ldots, a_n, \ldots$ de malos elementos con cada $a_{n+1}$ un divisor propio de $a_n$, y esto produce una cadena infinita estrictammente creciente

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \ldots,$$

contradiciendo la parte ii) de este lema. ■

**Teorema 2.10.1**
Si $R$ es un dominio de ideales principales, entonces $R$ es un dominio de factorización única. En particular, todo anillo euclidiano es un dominio de factorización única.

***Demostración.*** Tenemos que $R$ es dominio de ideales principales y $p$ es irreducible, entonces $(p)$ es primo. Además como $R$ es dominio de ideales principales, entonces para $r \neq 0$ y no unidad, por lema anterior parte iii), $r$ se descompone como producto de irreducibles, entonces $R$ es dominio de factorización única. ■

**Proposición 2.10.3**
Si $R$ es dominio de factorización única, entonces un máximo común divisor de cualquier conjunto finito de elementos $a_1, \ldots, a_n \in R$ existe.

***Demostración.*** La prueba será por inducción sobre el número de elementos. Es suficiente con probar la existencia para $a, b \in R$. Sean

$$a = up_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

y

$$b = vp_1^{f_1} p_2^{f_2} \cdots p_t^{f_t},$$

con $u, v$ unidades y $e_i \geq 0$ y $f_i \geq 0$ para todo $i$. Es fácil ver que si $c|a$, entonces la factorización de $c$ en irreducibles es $c = wp_1^{g_1} p_2^{g_2} \cdots p_3^{g_t}$, con $w$ una unidad y $0 \leq g_i \leq e_i$ para todo $i$. Por lo tanto, $c$ es un divisor común de $a$ y $b$ si y sólo si $g_i \leq m_i$ para todo $i$, con

$$m_i = min\{e_i, f_i\}.$$

Ahora es claro que $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ es máximo común divisor de $a$ y $b$. ■

**Definición 2.10.3**
Elementos $a_1, \ldots, a_n$ en un dominio de factorización única son llamados primos relativos si el máximo común divisor de ellos es una unidad; esto es, todo divisor común de $a_1, \ldots, a_n$ es una unidad.

**Definición 2.10.4**
Un polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, donde $R$ es un dominio de factorización única, es llamado primitivo si sus coeficientes son primos relativos; esto es, el único divisor común de $a_n, \ldots, a_1, a_0$ son unidades.

**Observación 52**
Si $R$ es un dominio de factorización única, y $p(x) \in R[x]$ un polinomio irreducible de grado positivo es primitivo. Si no, entonces existe un irreducible $q \in R$ que divide cada uno de sus coeficientes: $p(x) = qg(x)$ puesto que $p(x)$ es irreducible y $q$ es un factor no unidad, tenemos que $q$ es asociado a $p(x)$, sin embargo polinomios asociados tienen el mismo grado, teniendo una contradicción ya que el grado de $q$ es cero, concluyendo que todo polinomio irreducible con coeficientes en un dominio de factorización única es primitivo.

**Lema 2.10.2 (Lema de Gauss)**
Si $R$ es un dominio de factorización única y $f(x), g(x) \in R[x]$ ambos primitivos, entonces su producto $f(x)g(x)$ es también primitivo.

***Demostración.*** Sea $\pi : R \to R/(p)$ el mapeo natural definido como $\pi : a \mapsto a+(p)$, es homomorfismo de anillos. Sea $\tilde{\pi} : R[x] \to R/(p)[x]$ el mapeo que reemplaza cada coeficiente $c$ de un polinomio en $R[x]$ por $\pi(c)$, es un homomorfismo de anillos. Si un polinomio $h(x) \in R[x]$ no es primitivo, existe algún irreducible $p \in R$ tal que los coeficientes de $\tilde{\pi}(h(x))$ son 0 en $R/(p)$; es decir $\tilde{\pi}(h) = 0$ en $(R/(p))[x]$. Por lo tanto, si el producto $f(x)g(x)$ no es primitivo, existe algún irreducible $p$ con $0 = \tilde{\pi}(fg) = \tilde{\pi}(f)\tilde{\pi}(g)$ en $(R/(p))[x]$. Ahora como $(p)$ es un ideal primo, $R/(p)$ es un dominio, y por lo tanto $(R/(p))[x]$ es también un dominio. Pero, ni $\tilde{\pi}(f)$ ni $\tilde{\pi}(g)$ es 0 en $(R/(p))[x]$, porque $f$ y $g$ son primitivos, y esto contradice que $(R/(p))[x]$ sea un dominio. ■

**Lema 2.10.3**
Sea $R$ un dominio de factorización única, sea $\mathcal{Q} = Frac(R)$, y sea $f(x) \in \mathcal{Q}[x]$ distinto de cero.

i) Existe una factorización

$$f(x) = c(f)f^*(x),$$

con $c(f) \in \mathcal{Q}$ y $f^*(x) \in R[x]$ es primitivo. La factorización es única en el sentido de que si $f(x) = qg^*$, con $q \in \mathbb{Q}$ y $g^*(x) \in R[x]$ es primitivo, entonces existe una unidad $w \in R$ con $q = wc(f)$ y $g^* = w^{-1}f^*(x)$.

ii) Si $f(x), g(x) \in R[x]$, entonces $c(fg)$ y $c(f)c(g)$ son asociados en $R$ y $(fg)^*$, $f^*g^*$ son asociados en $R[x]$.

iii) Sea $f(x) \in \mathcal{Q}[x]$ tiene una factorización $f(x) = qg^*(x)$, donde $q \in \mathcal{Q}$ y $g^*(x) \in R[x]$ primitivo. Entonces $f(x) \in R[x]$ si y sólo si $q \in R$.

iv) Sea $g^*(x), f(x) \in R[x]$. Si $g^*(x)$ es primitivo y $g^*(x)|bf(x)$, con $b \in R$ y $b \neq 0$, entonces $g^*|f(x)$.

***Demostración.*** i) Sea $f(x) \in \mathcal{Q}[x]$, entonces existe $b \in R$ tal que $bf(x) \in R[x]$. Si $d$ es el máximo común divisor de todos los coeficientes de $bf(x)$, entonces $(b/d)\, f(x) \in R[x]$ es un polinomio primitivo. Si definimos $c(f) = d/b$ y $f^*(x) = (b/d)f(x)$, entonces $f^*(*)$ es primitivo y $f(x) = c(f)f^*(x)$.

Para probar la unicidad, supongamos que $c(f)f^*(x) = f(x) = qg^*$, con $c(f), q \in \mathcal{Q}$ y $f^*(x), g^*(x) \in R[x]$. Ahora tomemos $q/c(f) = u/v$ tal que $u, v$ son primos relativos en $R$. La ecuación $vf^*(x) = ug^*(x)$ está en $R[x]$; igualado coeficientes, $v$ es un divisor común de cada coeficiente de $ug^*(x)$. Como $u$ y $v$ son primos relativos, entonces $v$ divide a los coeficientes de $g^*(x)$. Pero $g^*(x)$ es primitivo, y por lo tanto $v$ es una unidad. Un argumento similar muestra que $u$ es una unidad. Por lo tanto, $q/c(f) = u/v$ es una unidad en $R$, llamémoslo $w$; tenemos $wc(f) = q$ y $f^*(x) = wg^*$.

ii) Existen dos factorizaciones de $f(x)g(x)$ en $R[x]$: $f(x)g(x) = c(fg)(f(x)g(x))^*$ y $f(x)g(x) = c(f)f^*(x)c(g)g^*(x) = c(f)c(g)f^*(x)g^*(x)$. Como el producto de polinomios primitivos es primitivo, cada uno de estos es una factorización y tenemos que $c(fg)$ un asociado de $c(f)c(g)$ y $(fg)^*$ un asociado de $f^*g^*$.

iii) Si $q \in R$, entonces es obvio que $f(x) = qg^*(x) \in R[x]$. Contrariamente, si $f(x) \in R[x]$, entonces no hay necesidad de despejar los denominadores, por lo tanto $c(f) = d \in R$, con $d$ el máximo común divisor de los coeficientes de $f(x)$. Por lo tanto, $f(x) = df^*(x)$. Por la unicidad, existe una unidad $w \in R$ con $q = wd \in R$.

iv) Como $bf = hg^*$, tenemos que $bc(f)f^* = c(h)h^*g^* = c(h)(hg)^*$. Luego por la unicidad de $f^*$, $(hg)^*$, y $h^*g^*$ son asociados, y por lo tanto $g^*|f^*$. Pero $f = c(f)f^*$, y por lo tanto $g^*|f$. ■

**Definición 2.10.5**
Sea $R$ un dominio de factorización única con $\mathcal{Q} = Frac(R)$. Si $f(x) \in \mathcal{Q}[x]$, existe una factorización $f(x) = c(f)f^*(x)$, con $c(f) \in \mathcal{Q}$ y $f^*(x) \in R[x]$ es primitivo. Llamaremos $c(f)$ el contenido de $f(x)$ y $f^*(x)$ el polinomio primitivo asociado.

Del lema anterior ambos $c(f)$ y $f^*(x)$ son únicos salvo por el producto por unidades de $R$.

**Teorema 2.10.2 (Gauss)**
Si $R$ es dominio de factorización única, entonces $R[x]$ es también dominio de factorización única.

***Demostración.*** Primero será por inducción sobre el $grad(f)$, veamos que todo $f(x) \in R[x]$, no cero ni unidad, es producto de irreducibles. Si $grad(f) = 0$, entonces $f(x)$ es una constante, por lo tanto está en $R$. Como $R$ es un dominio de factorización única, $f$ es un producto de irreducibles. Si $grad(f) > 0$, entonces $f(x) = c(f)f^*(x)$, con $c(f) \in R$ y $f^*(x)$ es primitivo. Ahora $c(f)$ es o bien una unidad o un producto de irreducibles, por la base de la inducción. Si $f^*$ es irreducible, no hay nada que probar, por otro lado si $f^*(x) = g(x)h(x)$ con $g(x)$ y $h(x)$ ambos no unidades. Como $f^*(x)$ es primitivo, sin embargo, ni $g$ ni $h$ son constantes; entonces cada uno tiene grado menor que $grad(f^*) = grad(f)$, y por lo tanto cada uno es producto de irreducibles, por hipótesis inductiva.

Para demostrar que $R[x]$ es dominio de factorización única falta demostrar que $(p(x))$ es ideal primo de $R[x]$ para todo $p(x) \in R[x]$ irreducible. Es decir, basta con ver que si $p|fg$, entonces $p|f$ o $p|g$.

Supongamos que $p \nmid f$. Caso i) Si $grad(p) = 0$. Escribimos

$$f(x) = c(f)f^*(x) \text{ y } g(x) = c(g)g^*(x),$$

con $c(f), c(g) \in R$, y $f^*(x), g^*(x)$ primitivos. Ahora $p|fg$, por lo tanto

$$p|c(f)c(g)f^*(x)g^*(x).$$

Como $f^*g^*$ es primitivo, tenemos que $c(f)c(g)$ un asociado de $c(fg)$. Sin embargo, si $p|f(x)g(x)$, entonces $p$ divide cada coeficiente de $fg$; esto es, $p$ es un divisor común de todos lo coeficientes de $fg$, por lo tanto en $R$, el cual es un dominio de factorización única, $p$ divide a los asociados $c(fg)$ y $c(f)c(g)$. Observe que $(p)$ es un ideal primo en $R$, por lo tanto $p|c(f)$ o $p|c(g)$. Si $p|c(f)$, entonces $p$ divide $c(f)f^*(x) = f(x)$, lo cual es una contradicción. Por lo tanto, $p|c(g)$ y $p|g(x)$.

Caso ii) Suponga que $grad(p) > 0$. Sea

$$(p, f) = \{s(x)p(x) + t(x)f(x) : s(x), t(x) \in R[x]\};$$

por supuesto, $(p, f)$ es un ideal que contiene a $p(x)$ y $f(x)$. Eliga $m(x) \in (p, f)$ de grado mínimo. Si $\mathcal{Q} = Frac(R)$ es el campo de fracciones de $R$, entonces el algoritmo de división en $\mathcal{Q}[x]$ nos da polinomios $q'(x), r'(x) \in \mathcal{Q}[x]$ con

$$f(x) = m(x)q'(x) + r'(x),$$

con $r'(x) = 0$ o $grad(r') < grad(m)$. Despejando denominadores, existen polinomios $q(x), r(x) \in R[x]$ y una constante $b \in R$ con

$$bf(x) = q(x)m(x) + r(x),$$

con $r(x) = 0$ o $grad(r) < grad(m)$. Como $m \in (p, f)$, existen polinomios $s(x), t(x) \in R[x]$ con $m(x) = s(x)p(x) + t(x)f(x)$; por lo tanto $r = bf - qm \in (p, f)$. Como $m$ tiene grado mínimo en $(p, f)$, tendremos que $r = 0$; esto es,

$bf(x) = m(x)q(x)$, y por lo tanto $bf(x) = c(m)m^*(x)q(x)$. Pero $m^*$ es primitivo, y $m^*(x)|bf(x)$, por lo cual $m^*(x)|f(x)$. Usando un argumento similar, cambiando $f(x)$ por $p(x)$ (esto es, iniciando con una ecuación $b''p(x) = q''(x)m(x)+r''(x)$ para alguna constante $b''$), nos da $m^*(x)|p(x)$. Como $p(x)$ es irreducible, los únicos factores son unidades y asociados. Si $m^*(x)$ fuera un asociado de $p(x)$, entonces $p(x)|f(x)$ (puesto que $p(x)|m^*|f(x)$), contrario a la hipótesis. Por lo tanto, $m^*$ tiene que ser una unidad; esto es, $m(x) = c(m) \in R$, y $(p, f)$ contiene a la constante $c(m) \neq 0$. Ahora sea $c(m) = sp + tf$, y por lo tanto

$$c(m)g(x) = s(x)p(x)g(x) + t(x)f(x)g(x).$$

Como $p(x)|f(x)g(x)$, tenemos que $p(x)|c(m)g(x)$. Pero $p(x)$ es primitivo, porque este es un irreducible y entonces que $p(x)|g(x)$. ■

**Corolario 2.10.2**
Si $k$ es un campo, entonces $k[x_1, \ldots, x_n]$ es un dominio de factorización única.

***Demostración.*** La prueba es por inducción sobre $n \geq 1$. Se demostró que si $k$ es campo, el anillo de polinomios $k[x_1]$ en una variable es un dominio de factorización única. Para el paso inductivo, recuerde que

$k[x_1, \ldots, x_n, x_{n+1}] = R[x_{n+1}]$, con $R = k[x_1, \ldots, x_n]$. Por inducción, $R$ es un dominio de factorización única, por lo tanto es $R[x_{n+1}]$. ■

**Corolario 2.10.3 (Gauss.)**
Sea $R$ un dominio de factorización única, sea $\mathcal{Q} = FracR$, y sea $f(x) \in R[x]$. Si

$$f(x) = G(x)H(x) \text{ en } \mathcal{Q}[x],$$

entonces existe una factorización

$$f(x) = g(x)h(x) \text{ en } R[x],$$

con $grad(g) = grad(G)$ y $grad(h) = grad(H)$; de hecho, $G(x)$ es un múltiplo constante de $g(x)$ y $H(x)$ es un múltiplo constante de $h(x)$. Por lo tanto, si $f(x)$ no tiene factores de grado menor en $R[x]$, entonces $f(x)$ es irreducible en $\mathcal{Q}[x]$.

***Demostración.*** La factorización $f(x) = G(x)H(x)$ en $\mathcal{Q}[x]$ nos da $q, q' \in \mathcal{Q}$ con

$$f(x) = qG^*(x)q'H^*(x) \text{ en } \mathcal{Q}[x],$$

con $G^*(x)$, $H^*(x) \in R[x]$ son primitivos. Pero $G^*(x)H^*(x)$ es primitivo, por Lema 2.10.2. Como $f(x) \in R[x]$, por lema anterior tenemos que la ecuación $f(x) = qq'[G^*(x)H^*(x)]$ implica que $qq' \in R$. Por lo tanto, $qq'G^*(x) \in R[x]$, y una factorización de $f(x)$ en $R[x]$ es $f(x) = [qq'G^*(x)]H^*(x)$. ■

**Corolario 2.10.4**
Si $\alpha$ es un entero algebraico, entonces $irr(\alpha, \mathbb{Q})$ es un elemento en $\mathbb{Z}[x]$.

***Demostración.*** Sea $p(x) \in \mathbb{Z}[x]$ el polinomio mónico de grado mínimo que tiene a $\alpha$ como raíz. Si $p(x) = G(x)H(x)$ en $\mathbb{Q}[x]$, con $grad(G) < grad(p)$ y $grad(H) < grad(p)$, entonces $\alpha$ es una raíz de $G(x)$ o $H(x)$. Por el Teorema 2.10.2, existe una factorización $p(x) = g(x)h(x)$ en $\mathbb{Z}[x]$ con $grad(g) = grad(G)$ y $grad(h) = grad(H)$; de hecho, existen racionales $c$ y $d$ con $g(x) = cG(x)$ y $h(x) = dH(x)$. Si $a$ es el coeficiente principal de $g(x)$ y $b$ es el coeficiente principal de $h(x)$, entonces $ab = 1$, para $p(x)$. Por lo tanto, podemos asumir que $a = 1 = b$, para $a, b \in \mathbb{Z}$; esto es, podemos suponer que ambos $g(x)$ y $h(x)$ son mónicos. Como $\alpha$ es una raíz de $g(x)$ o $h(x)$, es una contradicción al hecho de que $p(x)$ es un polinomio mónico en $\mathbb{Z}[x]$ de grado mínimo que tiene a $\alpha$ como una raíz. Se sigue que $p(x) = irr(\alpha, \mathbb{Q})$, este último es el único polinomio irreducible mónico en $\mathbb{Q}[x]$ que tiene $\alpha$ como una raíz. ■

**Definición 2.10.6**
Si $\alpha$ es un entero algebraico, entonces su polinomio mínimo es el polinomio mónico en $\mathbb{Z}[x]$ de grado mínimo con $\alpha$ como raíz.

Por el corolario anterior; todo entero algebraico $\alpha$ tiene un polinomio mínimo único $m(x) \in \mathbb{Z}[x]$, denotado por, $m(x) = irr(\alpha, \mathbb{Q})$, con $m(x)$ es irreducible en $\mathbb{Q}[x]$.

**Teorema 2.10.3**
Sea $f(x) = a_0 + a_1x + a_2x^2 + \cdots + x^n \in \mathbb{Z}[x]$ mónico, y sea $p$ un primo. Si $f(x)$ es irreducible *mod* $p$, esto es, si

$$\tilde{f}(x) = [a_0] + [a_1]x + [a_2]x^2 + \cdots + x^n \in \mathbb{Z}_p[x]$$

es irreducible, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

***Demostración.*** El mapeo natural $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ define un homomorfismo $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ por

$$\tilde{\varphi}(b_0 + b_1x + b_2x^2 + \dots) = [b_0] + [b_1]x + [b_2]x^2 + \dots;$$

tal que, reduce todos los coeficientes *mod* $p$. Si $g(x) \in \mathbb{Z}[x]$, denotamos su imagen $\tilde{\varphi}(g(x)) \in \mathbb{Z}_p[x]$ por $\tilde{g(x)}$. Suponga que $f(x)$ se factoriza en $\mathbb{Z}[x]$; es decir, $f(x) = g(x)h(x)$, con $grad(g) < grad(f)$ y $grad(h) < grad(f)$; por supuesto, $grad(f) = grad(g) + grad(h)$. Ahora $\tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$, ya que $\tilde{\varphi}$ es un homomorfismo de anillos, por lo tanto $grad\,(\varphi f) = grad\,(\tilde{g}) + grad\left(\tilde{h}\right)$. Como $f(x)$ es mónico, $\tilde{f}(x)$ también es mónico, entonces $grad(\tilde{f}) = grad(f)$. Por lo tanto, ambos $\tilde{g}(x)$ y $\tilde{h}(x)$ tienen grados menores que $grad(\tilde{f})$, contradiciendo la irreductibilidad de $\tilde{f}(x)$. Por lo tanto, $f(x)$ es irreducible en $\mathbb{Z}[x]$, y por Teorema 2.10.2 y corolario de Gauss, $f(x)$ es irreducible en $\mathbb{Q}[x]$. ■

**Ejemplo 90**
El reciproco del teorema anterior es falso.

Tome $f(x) = x^4 + 1$. Veamos que $f(x)$ es irreducible en $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Las posibles raíces racionales $\pm 1$ y $f(\pm 1) = 2$. Ahora si $x^4+1 = (x^2+ax+b)(x^2-ax+c)$.

Multiplicando e igualando los coeficientes tenemos

$$\begin{aligned} c + b - a^2 &= 0 \\ a(c-b) &= 0 \\ bc &= 1. \end{aligned}$$

Si $a = 0$, se tiene $c+b = 0$, luego entonces $-b^2 = 1$. Por lo que no hay soluciones en $\mathbb{Q}$. Si $c = b$, tenemos que $b^2 = 1$, por lo cual $b = \pm 1$ por lo tanto $a^2 = \pm 2$ y tampoco hay solución en $\mathbb{Q}$.

Veamos que $f(x) \in \mathbb{Z}_p[x]$ no es irreducible para todo $p$ primo. Si $p = 2$, entonces $f(x) = (x+1)^4$. Ahora sea $p$ primo impar ($p = 2n+1$, entonces $p^2 = 4n^2 + 4n + 1) = 4n(n+1) + 1)$. Observamos que $p^2 \equiv 1 \; mod \; 8$.

Además $|(\mathbb{F}_{p^2})^*| = p^2 - 1$ es divisible por ocho. $(\mathbb{F}_{p^2})^*$ es cíclico, entonces tiene un subgrupo cíclico de orden ocho. Por lo tanto $\mathbb{F}_{p^2}$ contiene todas las raíces octavas de la unidad en particular $\mathbb{F}_{p^2}$ contiene todas las raíces de $f(x) = x^4+1$, es decir, $\mathbb{F}_{p^2}$ es campo de descomposición de $x^4+1$ sobre $\mathbb{F}_p$ y $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$. Si fuera irreducible en $\mathbb{F}_p[x]$, entonces $4|[\mathbb{F}_{p^2} : \mathbb{F}_p]$. Por lo tanto, $x^4+1$ se factoriza en $\mathbb{F}_p$ para todo primo $p$.

**Ejemplo 91**
1) Mostraremos que $f(x) = x^4 - 5x^3 + 2x + 3$ es un polinomio irreducible en $\mathbb{Q}[x]$. Basta encontrar un primo $p$ tal que $\tilde{f}(x)$ es irreducible en $\mathbb{F}_p[x]$.

Observe que $\tilde{f}(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ es irreducible. Pues no tiene raíces en $\mathbb{F}_2$. Si $x^4 + x^3 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$, entonces $a = b = 1$, pero, esto es una contradicción. Por lo tanto $x^4-5x+2x+3$ es irreducible en $\mathbb{Q}[x]$.

2) Recordemos que si $n$ es un entero positivo el $n$ polinomio ciclotómico es

$$\Phi_n(x) = \prod (x - \zeta),$$

con $\zeta$ recorriendo todas las $n$ raíces primitivas de la unidad.

Sabemos que, para todo entero $n > 1$,

$$x^n - 1 = \prod_{d|n} \Phi_{d(x)},$$

con $d$ recorriendo sobre todos los divisores $d$ de $n$. Ahora $\Phi_1(x) = x - 1$. Para $p$ primo se tiene que

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x),$$

y por lo tanto

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

**Lema 2.10.4**
Sea $g(x) \in \mathbb{Z}[x]$. Si existe $c \in \mathbb{Z}$ con $g(x + c)$ irreducible en $\mathbb{Z}[x]$, entonces $g(x)$ es irreducible en $\mathbb{Q}[x]$.

***Demostración.*** La función $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$, dado por $f(x) \to f(x + c)$, es un isomorfismo. Si $g(x) = s(x)t(x)$, entonces $g(x+c) = \varphi(g(x)) = \varphi(st) = \varphi(s)\varphi(t)$ sería una factorización de $g(x + c)$. Por lo tanto, $g(x)$ es irreducible en $\mathbb{Z}[x]$ y por el corolario del Teorema 2.10.3, $g(x)$ es irreducible en $\mathbb{Q}[x]$. ■

**Teorema 2.10.4 (Criterio de Eisenstein.)**
Sea $R$ un dominio de factorización única con $\mathcal{Q} = Frac(R)$, y sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Si existe un elemento irreducible $p \in R$ con $p|a_i$ para todo $i < n$ pero con $p \nmid a_n$ y $p^2 \nmid a_0$, entonces $f(x)$ es irreducible en $\mathcal{Q}[x]$.

***Demostración.*** Sea $\Pi : R[x] \to R/(p)[x]$ un homomorfismo de anillos definido como

$$\sum \alpha_i x_i \to \sum \pi(\alpha_i)x^i,$$

suponga que $f(x) \in \mathcal{Q}[x]$ no es irreducibe por corolario de Gauss, $f(x) \in R[x]$ tiene una factorización propia digamos

$$f(x) = g(x)h(x)$$

con $g(x), h(x) \in R(x)$, $m = grad(g) < grad(f)$ y $k = grad(h) < grad(f)$. Sea $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$ y $h(x) = c_kx^k + c_{k-1}x^{k-1} + \cdots + c_0$, $\tilde{\pi}$ es homomorfismo, entonces $[a_n]x^n = \tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$ , por lo tanto $[b_0][c_0] = [0]$, por lo tanto $c_0b_0 \in (p)$, entonces $b_0 \in (p)$ o $c_0 \in (p)$, por lo tanto $p|b_0$ o $p|c_0$ pero $a_0 = c_0b_0$ y $p^2 \nmid a_0$, entonces $p$ sólo divide uno de los dos, digamos $p|c_0$ y $p \nmid b_0$.

Ahora $p \nmid a_n = b_mc_k$, entonces $p \nmid b_m$ y $p \nmid c_k$. Sea $r$ el índice menor $i$ tal que $p \nmid c_i$ por lo anterior $0 < r \leq k < n$ observe que $p|c_0, \ldots, p|c_{r-1}$, entonces $\tilde{h} = [c_k]x^k + [c_{k-1}]x^{k-1} + \cdots + [c_r]x^r$. Ahora observe que $a_r = b_0c_r + b_1c_{r-1} + \cdots + b_rc_0$, por lo tanto $[a_r] = [b_0c_r] \neq [0]$, ya que $p \nmid b_0$ y $p \nmid c_r$, pero esto implica que $a_r = a_n$ ya que $[a_i] \neq 0$ sólo para $i = n$, por lo que tenemos una contradicción. ■

**Corolario 2.10.5 (Gauss.)**
Para todo primo, el polinomio ciclotómico de orden $n$, $\Phi_p(x)$ es irreducible en $\mathbb{Q}[x]$.

***Demostración.*** $\Phi_p(x) = (x^p - 1)/(x - 1)$, tendríamos

$$\begin{aligned}\Phi_p(x+1) &= [(x+1)^p - 1]/x \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p.\end{aligned}$$

por lo tanto $\Phi_p(x+1)$ es irreducible por el criterio de Eisenstein y por lema anterior $\Phi_p(x)$ es irreducible. ■

## 2.11. Ejercicios

**Ejercicio 2.1**
i) Si $R$ es un dominio y $a \in R$ satisface $a^2 = a$, probar que $a = 0$ o $a = 1$.

ii) Mostrar que el anillo conmutativo $\mathcal{F}(\mathbb{R})$ contiene un número infinito de elementos $f \neq 0, 1$ con $f^2 = f$.

**Ejercicio 2.2**
i) Si $R$ es un dominio y $S$ es un subanillo de $R$, entonces $S$ es un dominio.

ii) Probar que $\mathbb{C}$ es un dominio, y concluya que el anillo de los enteros Gausianos es un dominio.

**Ejercicio 2.3**
i) Probar que $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ es un dominio.

ii) Probar que $R = \{\frac{1}{2}(a + b\sqrt{2}) : a, b \in \mathbb{Z}\}$ no es un dominio.

iii) Usando el hecho de que $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ es una raíz de $x^2 - x + 5$, probar que $R = \{a + b\alpha : a, b \in \mathbb{Z}\}$ es un dominio.

**Ejercicio 2.4**
i) Si $R$ es un anillo conmutativo, se define la operación círculo $a \circ b$ por

$$a \circ b = a + b - ab$$

probar que la operación círculo es asociativa y que $0 \circ\ a = a$ para todo $a \in R$.

ii) Probar que un anillo conmutativo $R$ es un campo si y sólo si $\{r \in R : r \neq 1\}$ es un grupo abeliano bajo la operación círculo.

**Ejercicio 2.5**
Definimos $\mathbb{F}_4$ como el conjunto de todas las matrices de la forma

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

con $a, b \in \mathbb{Z}_2$.

i) Probar que $\mathbb{F}_4$ es un anillo conmutativo bajo la suma y producto usual de matrices.

ii) Probar que $\mathbb{F}_4$ es un campo con exactamente cuatro elementos.

**Ejercicio 2.6**
Probar que todo dominio $R$ con un número finito de elementos tiene que ser un campo.

**Ejercicio 2.7**
Si $R$ es un anillo conmutativo, se define la relación $\equiv$ en $R$ por $a \equiv b$ si existe una unidad $u \in R$ tal que $b = ua$. Probar que si $a \equiv b$, entonces $(a) = (b)$, con $(a) = \{ra : r \in R\}$. Por el contrario, probar que si $R$ es un dominio, entonces $(a) = (b)$, implica $a \equiv b$.

**Ejercicio 2.8**
i) Si $R$ es un dominio, mostrar que si un polinomio en $R[x]$ es una unidad en $R[x]$, entonces es una constante no cero (el caso contrario es verdadero si $R$ es un campo).

ii) Mostrar que $(2x + 1)^2 = 1$ en $\mathbb{Z}_4[x]$. Concluir que la hipótesis en la parte i. donde $R$ es un dominio es necesaria.

**Ejercicio 2.9**
Mostrar que la función polinomial definida por $f(x) = x^p - x \in \mathbb{Z}_p$ es identicamente cero.

**Ejercicio 2.10**
Si $R$ es un anillo conmutativo y $f(x) = \sum_{i=0}^{n} s_i x^i \in R[x]$ tiene grado $n \geq 1$, definimos su derivada $f'(x) \in R[x]$ por

$$f'(x) = s_1 + 2s_2x + 3s_3x^2 + \cdots + ns_nx^{n-1} :$$

si $f(x)$ es un polinomio constante, se define la derivada como el polinomio cero. Probar que las reglas usuales del cálculo se conservan:

$$\begin{aligned}
(f + g)' &= f' + g';\\
(rf)' &= r(f') \text{ si } r \in R;\\
(fg)' &= fg' + f'g;\\
(f^n)' &= nf^{n-1}f' \text{ para todo } n \geq 1.
\end{aligned}$$

**Ejercicio 2.11**
Sea $R$ un anillo conmutativo y sea $f(x) \in R[x]$.

i) Probar que si $(x - a)^2 | f(x)$, entonces $x - a | f'(x)$ en $R[x]$.

ii) Probar que si $x-a|f(x)$ y $x-a|f'(x)$, entonces $(x-a)^2|f(x)$.

**Ejercicio 2.12**
i) Si $f(x)=ax^{2p}+bx^p+c\in\mathbb{Z}_p[x]$, probar que $f'(x)=0$.

ii) Probar que un polinomio $f(x)\in\mathbb{Z}_p[x]$ tiene $f'(x)=0$ si y sólo si existe un polinomio $g(x)=\sum a_nx^n$ con $f(x)=g(x^p)$; esto es, $f(x)=\sum a_nx^{np}\in\mathbb{Z}_p[x^p]$.

**Ejercicio 2.13**
Si $R$ es un anillo conmutativo, se define $R[[x]]$ como el conjunto de todas las sucesiones $(s_0,s_1,\dots)$ con $s_i\in R$ para todo $i$ (aquí no asumiremos que $s_i=0$ para $i$ grandes).

i) Muestre que las fórmulas que definen la suma y multiplicación sobre $R[x]$ tienen sentido para $R[[x]]$, y pruebe que $R[[x]]$ es un anillo conmutativo bajo estas operaciones ($R[[x]]$ es llamado el anillo formal de las series de potencias sobre $R$).

ii) Probar que $R[x]$ es un subanillo de $R[[x]]$.

iii) Probar que si $R$ es un dominio, entonces $R[[x]]$ es un dominio.

**Ejercicio 2.14**
i) Denote una serie formal de potencias $\sigma=(s_0,s_1,s_2,\dots,s_n,\dots)$ por

$$\sigma=s_0+s_1x+s_2x^2+\dots.$$

Probar que si $\sigma=1+x+x^2+\dots$, entonces $\sigma=1/(1-x)$ en $R[[x]]$; esto es, $(1-x)\sigma=1$.

ii) Probar que si $k$ es un campo, entonces una serie formal de potencias $\sigma\in k[[x]]$ es una unidad si y sólo si su término constante es distinto de cero; esto es, $ord(\sigma)=0$.

iii) Probar que si $\sigma\in k[[x]]$ y $ord(\sigma)=n$, entonces

$$\sigma=x^nu$$

con $u$ una unidad en $k[[x]]$.

**Ejercicio 2.15**
Encontrar el máximo común divisor de $x^2-x-2$ y $x^3-7x+6$ en $\mathbb{Z}_5[x]$, y expresalo como una combinación lineal de ellos.

**Ejercicio 2.16**
Sea $R$ un dominio. Si $f(x)\in R[x]$ tiene grado $n$, probar que $f(x)$ tiene a lo más $n$ raíces en $R$.

**Ejercicio 2.17**
Sea $f(x), g(x) \in R[x]$, donde $R$ es un dominio. Si el coeficiente principal de $f(x)$ es una unidad en $R$, entonces el algoritmo de la división nos da un cociente $q(x)$ y un residuo $r(x)$ después de dividir $g(x)$ por $f(x)$. Probar que $q(x)$ y $r(x)$ son únicos determinados por $g(x)$ y $f(x)$.

**Ejercicio 2.18**
Sea $k$ un campo, y sea $f(x), g(x) \in k[x]$ primos relativos. Si $h(x) \in k[x]$, probar que $f(x)|h(x)$ y $g(x)|h(x)$ implica $f(x)g(x)|h(x)$.

**Ejercicio 2.19**
Si $k$ es un campo, probar que $\sqrt{1-x^2} \notin k(x)$, con $k(x)$ es el campo de las funciones racionales.

**Ejercicio 2.20**
i) Sea $f(x) = (x-a_1)\dots(x-a_n) \in k[x]$, con $k$ un campo. Mostrar que $f(x)$ no tiene raíces repetidas (esto es, todos los $a_i$ son elementos distintos de $k$) si y sólo si el máximo común divisor $(f, f') = 1$, con $f'(x)$ es la derivada de $f$.

ii) Probar que si $p(x) \in \mathbb{Q}[x]$ es un polinomio irreducible, entonces $p(x)$ no tiene raíces repetidas en $\mathbb{C}$.

**Ejercicio 2.21**
Sea $\zeta = e^{2\pi i/n}$.
i) Probar que

$$x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)\dots(x-\zeta^{n-1})$$

y, si $n$ es impar, entonces

$$x^n + 1 = (x+1)(x+\zeta)(x+\zeta^2)\dots(x+\zeta^{n-1}).$$

ii) Para los números $a$ y $b$, probar que

$$a^n - b^n = (a-b)(a-\zeta b)(a-\zeta^2 b)\dots(a-\zeta^{n-1}b)$$

y, si $n$ es impar, entonces

$$a^n + b^n = (a+b)(a+\zeta b)(a+\zeta^2 b)\dots(a+\zeta^{n-1}b).$$

**Ejercicio 2.22**
i) Mostrar que todo elemento $a \in \mathbb{Z}_p$ tiene una $p$-ésima raíz (es decir, existe $b \in \mathbb{Z}_p$ con $a = b^p$).

ii) Sea $k$ un campo que contiene a $\mathbb{Z}_p$ como un subcampo (por ejemplo, $k = \mathbb{Z}_p$). Para todo entero positivo $n$, mostrar que la función $\varphi_n : k \to k$, dado por $\varphi(a) = a^{p^n}$, es un homomorfismo de anillos.

**Ejercicio 2.23**
Si $R$ es un campo, mostrar que $R \simeq Frac(R)$. Más precisamente, mostrar que los homomorfismos $f : R \to Frac(R)$ definido como $r \to [r, 1]$, es un isomorfismo.

**Ejercicio 2.24**
i) Si $R$ y $S$ son anillos conmutativos, mostrar que su producto directo $R \times S$ es también un anillo conmutativo, donde la suma y el producto en $R \times S$ están definidas como:

$$(r, s) + (r', s') = (r + r', s + s') \text{ y } (r, s)(r', s') = (rr', ss').$$

ii) Mostrar que si $m$ y $n$ son primos relativos, entonces $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ como anillos.

iii) Mostrar que si ninguno de $R$ o $S$ es el anillo cero, entonces $R \times S$ no es un dominio.

iv) Mostrar que $R \times \{0\}$ es un ideal en $R \times S$.

v) Mostrar que $R \times \{0\}$ es un anillo isomorfo a $R$, pero no es un subanillo de $R \times S$.

**Ejercicio 2.25**
Sea $F$ el conjunto de todas las matrices $2 \times 2$ con coeficientes reales, de la forma

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Probar que $F$ es un campo (con la suma y producto usual de matrices), además probar que existe un isomorfismo $\varphi : F \to \mathbb{C}$ con $det(A) = \varphi(A)\overline{\varphi(A)}$.

**Ejercicio 2.26**
Si $k$ es un campo y $[f, g]$ denota el mínimo común múltiplo los polinomios mónicos $f(x), g(x) \in k[x]$, mostrar que

$$[f, g](f, g) = fg.$$

**Ejercicio 2.27**
Si $R$ es un dominio de ideales principales y $a, b \in R$, probar que su mínimo común múltiplo existe.

**Ejercicio 2.28**
i) Si $k$ es un campo, probar que el anillo de las series formales de potencias $k[[x]]$ es un dominio de ideales principales.

ii) Probar que todo ideal no cero en $k[[x]]$ es igual a $(x^n)$ para algún $n \geq 0$.

**Ejercicio 2.29**
Si $k$ es un campo, mostrar que el ideal $(x, y)$ en $k[x, y]$ no es un ideal principal.

**Ejercicio 2.30**
Para todo $m \geq 1$, probar que todo ideal en $\mathbb{Z}_m$ es un ideal principal. (Si $m$ es compuesto, entonces $\mathbb{Z}_m$ no es un dominio de ideales principales ya que no es un dominio).

**Ejercicio 2.31**
Necesitaremos una definición previa para este ejercicio.

**Definición 2.11.1**
Sea $k$ un campo. Un divisor común de $a_1(x), a_2(x), \ldots, a_n(x)$ en $k[x]$ es un polinomio $c(x) \in k[x]$ con $c(x)|a_i(x)$ para todo $i$; el máximo común divisor es el común divisor mónico de grado máximo. Escribimos $c(x) = (a_1, a_2, \ldots, a_n)$.

Sea $k$ un campo, y sean los polinomios $a_1, a_2, \ldots, a_n$ en $k[x]$:
i) Mostrar que el máximo común divisor $d(x)$ de estos polinomios tienen la forma $\sum t_i(x)a_i(x)$, con $t_i(x) \in k[x]$ para $1 \leq i \leq n$.

ii) Probar que $c(x)|d(x)$ para todo divisor común mónico $c(x)$ de los $a_i(x)$.

**Ejercicio 2.32**
i) Mostrar que $x, y \in k[x, y]$ son primos relativos, pero tal que 1 no es combinación de ellos [es decir, no existe $s(x, y), t(x, y) \in k[x, y]$ con $1 = xs(x, y) + yt(x, y)$].

ii) Mostrar que 2 y $x$ son primos relativos en $\mathbb{Z}[x]$, pero que 1 no es combinación lineal de ellos; esto es, no existe $s(x), t(x) \in \mathbb{Z}[x]$ con $1 = 2s(x) + xt(x)$.

**Ejercicio 2.33**
Probar que existen dominios $R$ que contienen un par de elementos que no tienen máximo común divisor.

**Ejercicio 2.34**
Sea $\partial$ la función grado de un anillo euclidiano $R$. Si $m, n \in \mathbb{N}$ y $m \geq 1$, probar que $\partial'$ también es una función grado sobre $R$, con

$$\partial'(x) = m\partial(x) + n$$

para todo $x \in R$. Concluya que un anillo euclidiano puede no tener elementos de grado 0 o de grado 1.

**Ejercicio 2.35**
Sea $R$ un anillo euclidiano con función grado $\partial$.
i) Probar que $\partial(1) \leq \partial(a)$ para todos los $a \in R$ no ceros.

ii) Probar que un $u \in R$ no cero es una unidad si y sólo si $\partial(u) = \partial(1)$.

**Ejercicio 2.36**
Sea $R$ un anillo euclidiano, y asuma que $b \in R$ no es cero y no es unidad. Probar, para todo $i \geq 0$, que: $\partial(b^i) < \partial(b^{i+1})$.

**Ejercicio 2.37**
Probar, con todos los axiomas de la definición de espacio vectorial, que la ley conmutativa de la adición de vectores es redundante; es decir, si $V$ satisface los demás axiomas, entonces $u + v = v + u$ para todo $u, v \in V$.

**Ejercicio 2.38**
Si $V$ es un espacio vectorial sobre $\mathbb{Z}_2$ y si $v_1 \neq v_2$ son vectores no cero en $V$, probar que $v_1,\ v_2$ es linealmente independiente. ¿Esto será verdad para espacios vectoriales sobre cualquier otro campo?

**Ejercicio 2.39**
Probar que las columnas de una matriz A de $m \times n$ sobre un campo $k$ son linealmente dependientes en $k^m$ si y sólo si el sistema homogéneo $Ax = 0$ tiene una solución no trivial.

**Ejercicio 2.40**
Si $U$ es un subespacio de un espacio vectorial $V$ sobre un campo $k$, definimos la multiplicación escalar sobre el grupo cociente $V/U$ por

$$\alpha(v + U) = \alpha v + U,$$

con $\alpha \in k$ y $v \in V$. Probar que esta es una función bien definida que hace $V/U$ un espacio vectorial sobre $k$ ($V/U$ es llamado un espacio cociente).

**Ejercicio 2.41**
Si $V$ es un espacio vectorial de dimension finita y $U$ es un subespacio, probar que

$$dim(U) + dim(V/U) = dim(V).$$

**Ejercicio 2.42**
Necesitamos una definición previa.

**Definición 2.11.2**
Si $U$ y $W$ son subespacios de un espacio vectorial $V$, definimos

$$U + W = \{u + w : u \in U \text{ y } w \in W\}.$$

i) Probar que $U + W$ es un subespacio de $V$.

ii) Si $U$ y $U'$ son subespacios de un espacio vectorial de dimensión finita $V$, probar que

$$dim(U) + dim(U') = dim(U \cap U') + dim(U + U').$$

**Ejercicio 2.43**
Necesitamos una definición previa.

**Definición 2.11.3**
Si $U$ y $W$ son espacios vectoriales sobre un campo $k$, entonces su suma directa es el conjunto de todos los pares ordenados,

$$U \oplus W = \{(u, w) : u \in U \text{ y } w \in W\},$$

con suma

$$(u, w) + (u', w') = (u + u', w + w')$$

y multiplicación escalar

$$\alpha(u, w) = (\alpha u, \alpha w).$$

Si $U$ y $W$ son espacios vectoriales de dimensión finita sobre un campo $k$, probar que

$$dim(U \oplus W) = dim(U) + dim(W).$$

**Ejercicio 2.44**
Sea $V$ y $W$ un espacio vectorial sobre un campo $k$, y sea $S, T : V \to W$ una transformación lineal.

i) Si $V$ y $W$ son de dimensión finita, probar que

$$dim(Hom_k(V, W)) = dim(V)dim(W).$$

ii) El espacio dual $V^*$ de un espacio vectorial $V$ sobre un campo $k$ está definida por

$$V^* = Hom_k(V, k).$$

Si $dim(V) = n$, probar que $dim(V^*) = n$, y por lo tanto $V^* \simeq V$.

iii) Si $X = v_1, \ldots, v_n$ es una base de $V$, definir $\delta_1, \ldots \delta_n \in V^*$ por

$$\delta_i(v_j) = \begin{cases} 0 & \text{y} \quad j \neq i \\ 1 & \text{y} \quad j = i. \end{cases}$$

Probar que $\delta_1, \ldots, \delta_n$ es una base de $V^*$ (esta es llamada la base dual que surge de $v_1, \ldots v_n$).

**Ejercicio 2.45**
Si tenemos que

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

defina $det(A) = ad - bc$. Si $V$ es un espacio vectorial con base $X = v_1, v_2$, definimos $T : V \to V$ por $T(v_1) = av_1 + bv_2$ y $T(v_2) = cv_1 + dv_2$. Probar que $T$ es una transformación lineal no singular si y sólo si $det({}_X[T]_X) \neq 0$.

**Ejercicio 2.46**
Sea $U$ un subespacio de un espacio vectorial $V$.

i) Probar que el mapeo natural $\Pi : V \to V/U$, dado por $v \to v + U$, es una transformación lineal con kernel $U$.

ii) Establecer y probar el primer teorema de isomorfismos para espacios vectoriales.

**Ejercicio 2.47**
Sea $\mathcal{V}$ un espacio vectorial de dimensión finita sobre un campo $k$, y sea $\mathcal{B}$ el conjunto de todas las bases de $\mathcal{V}$. Probar que $\mathcal{B}$ es un conjunto $GL(\mathcal{V})$ transitivo.

**Ejercicio 2.48**
Probar que si $I = \{0\}$, entonces $R/I \simeq R$.

**Ejercicio 2.49**
(Tercer teorema de isomorfismos para anillos) Si $R$ es un anillo conmutativo que tiene ideales $I \subseteq J$, entonces $J/I$ es un ideal en $R/I$ y existe un isomorfismo de anillos $(R/I)/(J/I) \simeq R/I$.

**Ejercicio 2.50**
Para todo anillo conmutativo $R$, probar que $R[x]/(x) \simeq R$.

**Ejercicio 2.51**
Probar que $\mathbb{Z}_3/(x^3 - x^2 + 1) \simeq \mathbb{Z}_3/(x^3 - x^2 + x + 1)$.

**Ejercicio 2.52**
Si $X$ es un subconjunto de un anillo conmutativo $R$, definimos $\mathcal{L}(X)$ como la intersección de todos estos ideales $I$ en $R$ que contienen a $X$. Probar que $\mathcal{L}(X)$ es el conjunto de todos los elementos $a \in R$ para los cuales existen un número finito de elementos $x_1, \ldots, x_n \in X$ y elementos $r_i \in R$ con $a = r_1x_1 + \cdots + r_nx_n$.

**Ejercicio 2.53**
Sean $h(x), p(x) \in k[x]$ polinomios mónicos, con $k$ un campo. Si $p(x)$ es irreducible y si toda raíz de $h(x)$ (en un campo de descomposición apropiado) es también una raíz de $p(x)$, probar que $h(x) = p(x)^m$ para algún entero $m \geq 1$.

**Ejercicio 2.54**
Teorema del residuo chino.
i) Probar que si $k$ es un campo y $f(x), f'(x) \in k[x]$ son primos relativos, entonces dados $b(x), b'(x) \in k[x]$, entonces existe $c(x) \in k[x]$ con

$$c - b \in (f) \text{ y } c - b' \in (f') :$$

por otra parte, si $d(x)$ es otra solución común, entonces $c - d \in (ff')$.

ii) Probar que si $k$ es un campo y $f(x), g(x) \in k[x]$ son primos relativos, entonces

$$k[x]/(f(x)g(x)) \simeq k[x]/(f(x)) \times k[x]/(g(x)).$$

**Ejercicio 2.55**
i) Probar que un campo $K$ no puede tener subcampos $k'$ y $k''$ con $k' \simeq \mathbb{Q}$ y $k'' \simeq \mathbb{Z}_p$ para algún primo $p$.

ii) Probar que un campo $K$ no puede tener subcampos $k'$ y $k''$ con $k' \simeq \mathbb{Z}_p$ y $k'' \simeq \mathbb{Z}_q$, con $p \neq q$ primos.

**Ejercicio 2.56**
Probar que el grupo estocástico $\sum(2, \mathbb{F}_4) \simeq A_4$.

**Ejercicio 2.57**
Sea $f(x) = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} + x^n \in k[x]$, con $k$ un campo, y suponga que $f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$. Probar qie $s_{n-1} = -(\alpha_1+\alpha_2+\cdots+\alpha_n)$ y que $s_0 = (-1)^n\alpha_1\alpha_2\ldots\alpha_n$. Concluya que la suma y producto de todas las raíces de $f(x)$ están en $k$.

**Ejercicio 2.58**
Escriba las tablas de suma y multiplicación para el campo $\mathbb{F}_8$ con ocho elementos.

**Ejercicio 2.59**
Sea $k \subseteq K \subseteq E$ campos. Probar que si $E$ es una extensión finita sobre $k$, entonces $E$ es extensión finita sobre $K$ y $K$ es una extensión finita de $k$.

**Ejercicio 2.60**
Sea $k \subseteq F \subseteq K$ una torre de campos, y sea $z \in K$. Probar que si $k(z)/k$ es finito, entonces $[F(z) : F] \leq [k(z) : k]$. En particular, $[F(z) : F]$ es finito.

**Ejercicio 2.61**
i) ¿Es $\mathbb{F}_4$ un subcampo $\mathbb{F}_8$?

ii) Para cualquier $p$, probar que si $\mathbb{F}_{p^n}$ es un subcampo de $\mathbb{F}_{p^n}$, entonces $n|m$.

**Ejercicio 2.62**
Sea $K/k$ una extensión de campo. Si $A \subseteq K$ y $u \in k(A)$, probar que existen $a_1, \ldots, a_n \in A$ con $u \in k(a_1, \ldots, a_n)$.

**Ejercicio 2.63**
Sea $I$ un ideal en un anillo conmutativo $R$. Si $J^*$ y $L^*$ son ideales en $R/I$ , probar que existen ideales $J$ y $L$ en $R$ que contienen a $I$ tal que $J/I = J^*$, $L/I = L^*$, y $(J \cap L)/I = J^* \cap L^*$. Concluya que si $J^* \cap L^* = \{0\}$, entonces $J \cap L = I$.

**Ejercicio 2.64**
Sea $f : A \to R$ un anillo de homomorfismos, cuando $A$ y $R$ son anillos conmutativos distintos de cero. Proporcione un ejemplo de un ideal primo $P$ y $A$ con $f(P)$ no un ideal primo en $R$.

**Ejercicio 2.65**
Sea $f : A \to R$ un anillo de de homomorfismos. Si $\mathcal{Q}$ es un ideal primo en $R$, probar que $f^{-1}(\mathcal{Q})$ es un ideal primo en $A$. Concluya que si $J/I$ es un ideal primo en $R/I$, cuando $I \subseteq J \subseteq R$, entonces $J$ es un ideal primo en $R$.

**Ejercicio 2.66**
Probar que si $P$ es un ideal primo en un anillo conmutativo $R$ y si $r^n \in P$ para algún $r \in R$ y $n \geq 1$, entonces $r \in P$.

**Ejercicio 2.67**
Si $I$ y $J$ son ideales en un anillo conmuatativo $R$, definimos

$$IJ = \{\text{Todas las sumas finitas} \sum_l a_l b_l : a_l \in I \text{ y } b_l \in J\}.$$

i) Probar que $IJ$ es un ideal en $R$ y que $IJ \subseteq I \cap J$.

ii) Si $I = (2)$ es el ideal de los enteros pares en $\mathbb{Z}$, probar que si $I^2 = II \subset I \cap I = I$

**Ejercicio 2.68**
Sean $I$ y $J$ ideales en un anillo conmutativo $R$.
i) Probar que el mapeo $R/(I \cap J) \to R/I \times R/J$, dado $\varphi : r \to (r + I, r + J)$, es una función inyectiva.

ii) Llame $I$ y $J$ coprimos si $I + J = R$. Probar que si $I$ y $J$ son coprimos, entonces el homomorfismos de anillos $\varphi : R/(I \cap J) \to R/I \times R/J$ en la parte i. es una función sobreyectiva.

iii) Generalizar el teorema del residuo chino Como sigue. Sea $R$ un anillo conmutativo y sea $I_1, \ldots, I_n$ coprimos dos a dos; esto es, $I_i$ e $I_j$ son coprimos para todo $i \neq j$. Probar que si $a_1, \ldots, a_n \in R$, entonces existe $r \in R$ con $r + I_i = a_i + I_i$ para todo $i$.

**Ejercicio 2.69**
Si $I$ y $J$ son ideales coprimos en un anillo conmutativo $R$, probar que

$$I \cap J = IJ.$$

**Ejercicio 2.70**
Sea $R$ un dominio de factorización única y sea $\mathcal{Q} = Frac(R)$ un campo de fracciones. Probar que cada $a/b \in \mathcal{Q}$ distinto de cero tiene una expresión de la forma $u/v$ con $u$ y $v$ primos relativos.

**Ejercicio 2.71**
Si $R$ es un dominio, probar que las únicas unidades en $R[x_1, \ldots, x_n]$ son unidades en $R$. Por otra parte, probar que $2x + 1$ es una unidad en $\mathbb{Z}_4[x]$.

**Ejercicio 2.72**
i) Probar que $x$ e $y$ son primos relativos en $k[x, y]$, donde $k$ es un campo.

ii) Probar que 1 no es una combinación lineal de $x$ e $y$ en $k[x, y]$.

**Ejercicio 2.73**
i) Probar que $\mathbb{Z}[x_1, \ldots, x_n]$ es un dominio de factorización única para todo $n \geq 1$.

ii) Si $k$ es un campo, probar que el anillo de polinomios en una infinidad de variables, $R = k[x_1, x_2, \ldots, x_n, \ldots]$, es también un dominio de factorización única.

**Ejercicio 2.74**
i) Si $a$ es un entero libre de cuadrados, probar que $x^n - a$ es irreducible en $\mathbb{Q}[x]$ para todo $n \geq 1$. Concluya que existen polinomios irreducibles en $\mathbb{Q}[x]$ para todo grado $n \geq 1$.

ii) Si $a$ es un entero libre de cuadrados, probar que $\sqrt[n]{a}$ es irracional para todo $n \geq 2$.

**Ejercicio 2.75**
Sea $R$ un dominio de factorización única con $\mathcal{Q} = Frac(R)$. Si $f(x) \in R[x]$, probar que $f(x)$ es irreducible en $R[x]$ si y sólo si $f(x)$ es primitivo y $f(x)$ es irreducible en $\mathcal{Q}[x]$.

# Bibliografía


[1] Rotman, J. J. 2003. *Advanced Modern Algebra*, segunda edición, Prentice Hall, New Jersey, EUA

[2] Gentile, E. R. 1967. *Estructuras Algebraicas I*, Unión Panamericana, Washington, D. C., EUA

[3] Gentile, E. R. 1973. *Estructuras Algebraicas III*, Organización de los Estados Americanos, Washington, D. C., EUA

[4] Herstein, I. N. 1975. *Topics in Algebra*, segunda edición, John Wiley & Sons, New York, EUA

[5] Herstein, I. N. 1996. *Abstract Algebra*, tercera edición, Prentice Hall, New Jersey, EUA

[6] Jacobson, N. 1985. *Basic Algebra I*, segunda edición, W. H. Freeman, San Francisco, EUA

[7] Fraleigh, J. B. 1988. *Algebra Abstracta*, Addison Wesley Iberoamericana, México D. F.

[8] Friedberg, S. H., Insel, A. J., Spence, L. E. 2003. *Linear Algebra*, cuarta edición, Prentice Hall, New Jersey, EUA

[9] Grossman S., S. I. 2008. *Álgebra lineal*, sexta edición, McGraw Hill Interamericana, México, D. F.