Álgebra II

Tijani Pakhrou

Índice general

1. Teoría de conjuntos **1**
- 1.1. Conjuntos . . . 1
- 1.2. Productos cartesianos . . . 6
- 1.3. Relaciones de equivalencia . . . 6
- 1.4. Conjunto cociente . . . 8
- 1.5. Aplicaciones . . . 10
  - 1.5.1. Correspondencias y aplicaciones . . . 10
  - 1.5.2. Imagen de una aplicación . . . 13
  - 1.5.3. Propiedades de las aplicaciones . . . 15
  - 1.5.4. Tipos de aplicaciones . . . 16
  - 1.5.5. Composición de aplicaciones . . . 18
  - 1.5.6. Restricción de una aplicación a un subconjunto . . . 19

2. Grupos **21**
- 2.1. Operaciones binarias . . . 21
- 2.2. Propiedades de las operaciones binarias . . . 22
- 2.3. Definición de grupo y propiedades . . . 24
  - 2.3.1. Grupos de matrices . . . 26
  - 2.3.2. Grupos de congruencias . . . 26
  - 2.3.3. Grupo de las biyecciones de un conjunto . . . 27
  - 2.3.4. Grupos de permutaciones . . . 27
- 2.4. Subgrupos de un grupo . . . 29
  - 2.4.1. Subgrupo generado por un subconjunto . . . 31
  - 2.4.2. Subgrupo generado por un elemento . . . 32
  - 2.4.3. Grupo cíclico . . . 32
- 2.5. Clases laterales . . . 32
- 2.6. Teorema de Lagrange . . . 35
- 2.7. Subgrupos normales y grupo cociente . . . 37
- 2.8. Homomorfismos de Grupos . . . 42
  - 2.8.1. Clasificación de homomorfismos . . . 43
  - 2.8.2. Propiedades de homomorfismos . . . 44

2.8.3. Núcleo de un homomorfismo 49
2.9. Descomposición canónica de un homomorfismo 50
2.9.1. Homomorfismo canónico 50
2.9.2. Descomposición canónica 51

3. Anillos y cuerpos **55**
3.1. Anillos 55
3.2. Elementos Invertibles y Anillos de División 56
3.3. Cuerpos 58
3.4. Divisores de cero 59
3.5. Dominio de integridad 61
3.6. Subanillos 61
3.7. Subcuerpos 63
3.8. Ideales 63
3.9. Anillo de clases de restos módulo I 65
3.10. Ideales generados 67
3.11. Ideales primos 70
3.12. Ideales maximales 71
3.13. Cuerpo de fracciones de un anillo 71
3.14. Homomorfismos de anillos 75

4. Anillos de Polinomios **81**
4.1. Definiciones 81
4.2. Operaciones en $A[X]$ 81
4.3. Anillo de polinomios 83
4.4. Teorema de la división 84
4.5. Divisor de un polinomio 85
4.6. Máximo común divisor 87
4.7. Algoritmo de Euclides (cálculo del máximo común divisor) 89
4.8. Raíces de un polinomio 93
4.9. Polinomio irreducible 94
4.9.1. Irreducibilidad en $\mathbb{C}[X]$ 95
4.9.2. Irreducibilidad en $\mathbb{R}[X]$ 95
4.9.3. Irreducibilidad en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$ 95
4.9.4. Irreducibilidad en $\mathbb{Z}_p[X]$ 96

Capítulo 1

Teoría de conjuntos

1.1. Conjuntos

Definición 1.1.1. *Un conjunto es una colección de elementos en la que no se repite ninguno.*

Notación 1. *Los conjuntos se suelen denotar con letras mayúsculas y sus elementos con letras minúsculas.*

Ejemplo 1.1.2.

- $\mathbb{N}$ es el conjunto de los números naturales.
- $\mathbb{Z}$ es el conjunto de los números enteros.
- $\mathbb{Q}$ es el conjunto de los números racionales.
- $\mathbb{R}$ es el conjunto de los números reales.

Definición 1.1.3.

- *Si x es un elemento de un conjunto X, se escribe $x \in X$, y se lee "x pertenece al conjunto X".*
- *Si x no es un elemento del conjunto X, se escribe $x \notin X$, y se lee "x no pertenece al conjunto X".*

Definición 1.1.4 (Igualdad entre conjuntos). *Dos conjuntos S y T son iguales si y sólo si*

$$\begin{cases} \forall s: \ s \in S \Longrightarrow s \in T \\ \\ \forall t: \ t \in T \Longrightarrow t \in S \end{cases}$$

Definición 1.1.5 (**Subconjuntos**). *Dados dos conjuntos S y T, se dice que S es* ***subconjunto*** *de T y se denota por $S \subset T$, si y sólo si*

$$\forall s: \ s \in S \Longrightarrow s \in T$$

Proposición 1.1.6. *Dados dos conjuntos S y T,*

$$S = T \Longleftrightarrow S \subset T \ y \ T \subset S$$

Definición 1.1.7 (**El conjunto vacío**). *El* ***conjunto vacío*** *se indica por $\emptyset$ y es un conjunto que no contiene ningún elemento, podemos definirlo del modo siguiente:*

$$\emptyset = \{n \in \mathbb{Z}: \ n \neq n\}.$$

Definición 1.1.8 (**Unión de conjuntos**). *Dados dos conjuntos S y T, se define la* ***unión*** *de los conjuntos S y T y se denota por $S \cup T$ al siguiente conjunto:*

$$S \cup T = \{x: \ x \in S \ \ ó \ \ x \in T\}$$

Ejemplo 1.1.9. Si $S = \{1, 5, 2, 6\}$ y $T = \{3, 8, 5, 9\}$, se tiene

$$S \cup T = \{1, 5, 2, 6, 3, 8, 9\}.$$

Proposición 1.1.10. *La unión posee las propiedades siguientes:*

1) $A \cup B = B \cup A$. *Conmutativa*

2) $(A \cup B) \cup C = A \cup (B \cup C)$. *Asociativa*

3) $A \subset X \ y \ B \subset X \Longleftrightarrow A \cup B \subset X$.

4) $A \subset B \Longleftrightarrow A \cup B = B$.

5) $A \cup A = A$.

6) $A \cup \emptyset = A$.

Definición 1.1.11 (**Intersección de subconjuntos**). *Dados S y T, subconjuntos de X, se define la* ***intersección*** *de los conjuntos S y T y se denota por $S \cap T$ al siguiente conjunto:*

$$S \cap T = \{x: \ x \in S \ \ y \ \ x \in T\}.$$

Si $S \cap T = \emptyset$, entonces se dice que S y T son conjuntos ***disjuntos****.*

Ejemplo 1.1.12. $S = \{1, 5, 2, 6\}$, $T = \{3, 8, 5, 9\} \Rightarrow S \cap T = \{5\}$.

Proposición 1.1.13. *La intersección posee las propiedades siguientes:*

1) $A \cap B = B \cap A$. *Conmutativa*

2) $(A \cap B) \cap C = A \cap (B \cap C)$. *Asociativa*

3) $X \subset A$ *y* $X \subset B \iff X \subset A \cap B$.

4) $A \subset B \iff A \cap B = A$.

5) $A \cap A = A$.

6) $A \cap \emptyset = \emptyset$.

Proposición 1.1.14. *La unión y la intersección tienen las propiedades siguientes:*

1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *Distributiva*

2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *Distributiva*

3) $A \cup (A \cap B) = A$. *Absorción*

4) $A \cap (A \cup B) = A$. *Absorción*

Definición 1.1.15 (**Diferencia de conjuntos).** *Dados S y T, subconjuntos de X, se define la* ***diferencia*** *de los conjuntos S y T y se denota por $T - S$ al siguiente conjunto:*

$$T - S = \{x : \ x \in T \ \ y \ \ x \notin S\}.$$

Ejemplo 1.1.16. $S = \{5\},\ T = \{3, 8, 5, 9\} \Rightarrow T - S = \{3, 8, 9\}$
Como $S \subset T \Rightarrow S \cup T = T$ y $S \cap T = S$.

Definición 1.1.17. *Si A es un subconjunto del universal X, se denomina* ***complemento*** *de A al conjunto formado por los elementos de X que no pertenecen a A. Lo indicaremos con la notación A^c, es decir,*

$$A^c = \{x \in X : \ x \notin A\}.$$

Proposición 1.1.18. *La diferencia de conjuntos cumple, entre otras, las siguientes propiedades:*

1) $A - B = A \cap B^c$.

2) $A - A = \emptyset$.

3) $A - \emptyset = A$.

4) $\emptyset - A = \emptyset$.

5) *Si* $A \subset X$, $X - A = A^c$ *y* $A - X = \emptyset$.

Proposición 1.1.19. *Las siguientes dos propiedades se conocen con el nombre de* ***leyes de De Morgan****:*

1) $(A \cup B)^c = A^c \cap B^c$.

2) $(A \cap B)^c = A^c \cup B^c$.

Definición 1.1.20 (**El conjunto de partes de un conjunto**). *Sea* X *un conjunto, se define el* ***conjunto de las partes de*** X (*conjunto potencia de* X) *como el conjunto de todos los subconjuntos o partes de* X, *y se indica por* $\mathcal{P}(X)$ *o por* 2^X, *es decir*

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

Ejemplo 1.1.21.

- Si $X = \emptyset$, entonces $\mathcal{P}(X) = \{\emptyset\}$
- Si $X = \{1\}$, entonces $\mathcal{P}(X) = \{\emptyset, X\}$
- Si $X = \{1, 2\}$, entonces

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

Observación 1.1.22.
Sea X *un conjunto, tenemos*

$$\emptyset, X \in \mathcal{P}(X).$$

Definición 1.1.23 (**Partición de un conjunto).**

- ▶ *Llamamos* ***colección*** *a todo conjunto cuyos elementos son, a su vez, conjuntos.*
- ▶ *Una* ***partición de un conjunto*** X *es una colección* $\Pi(X)$ *de subconjuntos no vacíos de* X*, que cumple las dos propiedades siguientes:*

  1) *La unión de elementos de* $\Pi(X)$ *es igual a* X*, es decir,*

  $$\bigcup \{A \subseteq X : \ A \in \Pi(X)\} = X.$$

  2) *Si* $A, B \in \Pi(X)$ *y* $A \neq B \Longrightarrow A \cap B = \emptyset$.

Ejemplo 1.1.24. Sea $X = \{1, 2, 3, 4, 5\}$.

- La colección $\Pi(X) = \big\{\{1\}, \{3, 5\}, \{2, 4\}\big\}$ es una partición de X
- La colección $\Pi(X) = \big\{\{1, 2\}, \{2, 3, 4\}, \{5\}\big\}$ no es una partición de X ya que el 2 aparece en dos subconjuntos
- La colección $\Pi(X) = \big\{\{1, 3\}, \{4, 5\}\big\}$ tampoco es una partición de X ya que el elemento 2 no aparece en ninguno de los subconjuntos

Ejemplo 1.1.25. La colección $\Pi(\mathbb{R})$ de subconjuntos de $\mathbb{R}$ definida por

$$\Pi(\mathbb{R}) = \{(-\infty, 0), \{0\}, (0, +\infty)\}$$

es una partición del conjunto $\mathbb{R}$.

Ejemplo 1.1.26. La colección $\Pi([0, 1])$ de subconjuntos de $[0, 1]$ definida por

$$\Pi([0, 1]) = \Big\{\Big[0, \frac{1}{4}\Big], \Big(\frac{1}{4}, \frac{1}{2}\Big], \Big(\frac{1}{2}, \frac{3}{4}\Big], \Big(\frac{3}{4}, 1\Big]\Big\}$$

es una partición del conjunto $[0, 1]$.

1.2. Productos cartesianos

Definición 1.2.1. *Si A y B son dos conjuntos, se define el* ***producto cartesiano de A y B****, representado por $A\times B$, como el conjunto de todos los* ***pares ordenados*** *(x, y) con $x \in A$ e $y \in B$. Así*

$$A \times B = \{(x, y) : \ x \in A \ \ e \ \ y \in B\}.$$

Nota 1.2.2. *En Teoría de conjuntos se admite que el producto cartesiano de dos conjuntos es, efectivamente, otro conjunto.*

Observación 1.2.3.

- *En general $S \times T \neq T \times S$. Además, se denota $S^2 = S \times S$.*
- *$S \times \emptyset = \emptyset \times S = \emptyset$.*

Ejemplo 1.2.4.

$$\begin{aligned}
\mathbb{N} \times \{1, 2\} &= \big\{(n, p) : \ n \in \mathbb{N} \ \text{ e } \ p \in \{1, 2\}\big\} \\
&= \Big\{(n, p) : \ n \in \mathbb{N} \ \text{ e } \ \big[\{p = 1\} \ \text{ o } \ \{p = 2\}\big]\Big\} \\
&= \Big\{(n, p) : \ n \in \mathbb{N} \ \text{ e } \ \{p = 1\}\Big\} \ \text{ o } \Big\{(n, p) : \ n \in \mathbb{N} \ \text{ e } \ \{p = 2\}\Big\} \\
&= \{(n, 1) : n \in \mathbb{N}\} \cup \{(n, 2) : n \in \mathbb{N}\}
\end{aligned}$$

Ejercicio 1.2.5. *Dados $S = \{1, 7, 5, 3\}$ y $T = \{2, 4, 5, 6\}$, calcular:*

- $S \times T$
- $T \times S$
- ¿$T \times S = S \times T$?
- ¿$(S \times T) \times S = S \times (T \times S)$?

1.3. Relaciones de equivalencia

Definición 1.3.1. *Sea X un conjunto, y sea $\mathcal{R}$ un subconjunto del producto cartesiano X^2 ($\mathcal{R} \subset X^2$).*

Decimos que $\mathcal{R}$ es una ***relación de equivalencia*** *en X si cumple las siguientes propiedades:*

1) *reflexiva:* $(x, x) \in \mathcal{R}, \forall x \in X$

2) *simétrica:* $(x,y) \in \mathcal{R} \Longrightarrow (y,x) \in \mathcal{R}$

3) *transitiva:* $(x,y) \in \mathcal{R}, (y,z) \in \mathcal{R} \Longrightarrow (x,z) \in \mathcal{R}$

Notación 2. $(x,y) \in \mathcal{R}$ *también se escribe* $x\mathcal{R}y$

Ejemplo 1.3.2.

1) Sea $X = \{1,2,3\}$, el conjunto

$$\mathcal{R} = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$$

es una relación de equivalencia en X

2) El conjunto $\mathcal{R} = \{(x,y) \in \mathbb{N} \times \mathbb{N} : \ x < y\}$ no es una relación de equivalencia en $\mathbb{N}$ ya que no cumple la propiedad reflexiva.

Ejercicio 1.3.3. *Sea* $\mathcal{R} = \{(x,y) \in \mathbb{Z}^2 : \ x - y$ *divisible por* $3\}$*, demostrar que* $\mathcal{R}$ *es una relación de equivalencia.*

1) $x\mathcal{R}x$ *ya que* $x - x = 0$ *es divisible por* 3

2) $x\mathcal{R}y \Longrightarrow y\mathcal{R}x$ *ya que si* $x - y$ *es divisible por* $3 \Longrightarrow y - x$ *también es divisible por* 3

3) $x\mathcal{R}y, y\mathcal{R}z \Longrightarrow x\mathcal{R}z$ *ya que si* $x - y$ *e* $y - z$ *son divisibles por* 3*, su suma también lo será, por lo tanto* $x - z = (x - y) + (y - z)$ *es divisible por* 3

Por lo tanto $\mathcal{R}$ *es una relación de equivalencia.*

Definición 1.3.4 (clases de equivalencia). *Sea* $\mathcal{R}$ *una relación de equivalencia definida en un conjunto* X*, y sea* $x \in X$*. Se llama* ***clase de equivalencia del elemento*** x ***para la relación*** $\mathcal{R}$*, y se denota* $[x]_{\mathcal{R}}$ *o* $\mathcal{R}(x)$*, al subconjunto de* X *definido com*

$$[x]_{\mathcal{R}} = \mathcal{R}(x) = \{y \in X : \ x\mathcal{R}y\}$$

Ejemplo 1.3.5. Sea $X = \{1,2,3\}$ y $\mathcal{R} = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$, entonces

$$\begin{aligned} [1]_{\mathcal{R}} &= \{1,2\}, \\ [2]_{\mathcal{R}} &= \{1,2\}, \\ [3]_{\mathcal{R}} &= \{3\}. \end{aligned}$$

Tenemos

$$[1]_{\mathcal{R}} \cup [2]_{\mathcal{R}} \cup [3]_{\mathcal{R}} = \{1,2\} \cup \{1,2\} \cup \{3\} = \{1,2,3\}$$

Teorema 1.3.6. *Sea $\mathcal{R}$ una relación de equivalencia definida en un conjunto X y sean $x, y \in X$. Se tiene que:*

1) $\bigcup \Big\{ [x]_{\mathcal{R}} : \ x \in X \Big\} = X$

2) $x \mathcal{R} y \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}}$

3) *Si x no está relacionado mediante la relación $\mathcal{R}$ con y, entonces*
$$[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$$

Proposición 1.3.7. *Sea $\mathcal{R}$ una relación de equivalencia definida en un conjunto X. Dados dos elementos $x, y \in X$, se cumple que*

$$x \mathcal{R} y \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}}$$

Proposición 1.3.8. *Si $\mathcal{R}$ es una relación de equivalencia definida en un conjunto X, el conjunto de todas las clases de equivalencia es una partición del conjunto X, es decir:*

1) $\bigcup \Big\{ [x]_{\mathcal{R}} : \ x \in X \Big\} = X$

2) *Si* $[x]_{\mathcal{R}}, [y]_{\mathcal{R}} \in \Big\{ [x]_{\mathcal{R}} : \ x \in X \Big\}$ *y* $[x]_{\mathcal{R}} \neq [y]_{\mathcal{R}} \Longrightarrow [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$.

1.4. Conjunto cociente

Definición 1.4.1. *Si $\mathcal{R}$ es una relación de equivalencia en un conjunto X, se llama* ***conjunto cociente de*** *X* ***por*** *$\mathcal{R}$, y se denota $X/\mathcal{R}$, al conjunto cuyos elementos son las clases de equivalencia asociadas a $\mathcal{R}$ en X.*

$$X/\mathcal{R} = \big\{ [x]_{\mathcal{R}} : \ x \in X \big\}$$

Ejemplo 1.4.2. Sean el conjunto $X = \{1, 2, 3\}$ y la relación de equivalencia $\mathcal{R} = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$, el conjunto cociente viene dado por

$$X/\mathcal{R} = \{\{1,2\}, \{3\}\} = \{[1]_{\mathcal{R}}, [3]_{\mathcal{R}}\}$$

ya que $[1]_{\mathcal{R}} = \{x \in X : (1,x) \in \mathcal{R}\} = \{1,2\} = [2]_{\mathcal{R}}$

Ejercicio 1.4.3.

1) *Demostrar que* $\mathcal{R} = \{(0,0),(1,1),(2,2),(3,3),(0,2),(1,3),(2,0),(3,1)\}$ *es una relación de equivalencia de* $X = \{0,1,2,3\}$

2) *Encontrar las clases de equivalencia de* $\mathcal{R}$.

3) *Definir el conjunto* $X/\mathcal{R}$.

Ejercicio 1.4.4. *Sea la relación de equivalencia* $\mathcal{R} = \{(x,y) \in \mathbb{Z}^2 : \ x - y$ *divisible por* $3\}$.

1) *Encontrar las clases de equivalencia de* $\mathcal{R}$.

2) *El conjunto cociente definido por esta relación de equivalencia se denotará por* $\mathbb{Z}_3$, *¿cual es dicho conjunto cociente*?

Solución:
1) Si $a \in \mathbb{Z}$ y $[a]_{\mathcal{R}}$ es su clase de equivalencia, entonces

$$\begin{aligned}[a]_{\mathcal{R}} &= \{b \in \mathbb{Z} : \ a\mathcal{R}b\} = \{b \in \mathbb{Z} : \ 3|a-b\} \\ &= \{b \in \mathbb{Z} : \ a - b = 3k, \text{ con } k \in \mathbb{Z}\} \\ &= \{a - 3k, \text{ con } k \in \mathbb{Z}\}.\end{aligned}$$

¿Cuántas clases de equivalencia distintas hay?

▶ Para saberlo, dado $a \in \mathbb{Z}$, dividimos a entre 3, se deduce, utilizando el algoritmo de la división, la existencia de números $q, r \in \mathbb{Z}$ con

$$0 \leq r \leq 3 - 1 = 2,$$

tales que

$$a = q3 + r.$$

Así que,

$$a - r = q3 \Longleftrightarrow 3|a - r \Longleftrightarrow a\mathcal{R}r \Longleftrightarrow [a]_{\mathcal{R}} = [r]_{\mathcal{R}}.$$

En resumen, hemos probado que

$$\forall\ a \in \mathbb{Z}, \ \ \exists\ r \in \{0,1,2\}, \ \ \text{tal que} \ \ [a]_{\mathcal{R}} = [r]_{\mathcal{R}}.$$

Por tanto, a lo sumo existen tres clases de equivalencia,

$$[0]_{\mathcal{R}},\ [1]_{\mathcal{R}},\ [2]_{\mathcal{R}}.$$

▶ Demostrando ahora que estas tres clases son distintas entre sí.

Si consideramos $r, s \in \{0, 1, 2\}$ con $r < s$, entonces

$$0 < s - r \leq s \leq 2 \implies s - r \in \{1, 2\}$$

Luego, $s - r$ no puede ser múltiplo de 3, y, así,

$$3 \not| \, s - r,$$

de donde las clases $[r]_{\mathcal{R}}$, $[s]_{\mathcal{R}}$ son distintas.

▶ En resumen, para la relación $\mathcal{R}$ existen exactamente 3 clases distintas, que son

$$[0]_{\mathcal{R}},\ [1]_{\mathcal{R}},\ [2]_{\mathcal{R}}.$$

Además, dado un número entero a, para saber exactamente en cuál de estas clases está situado, es suficiente dividir en los números enteros a entre 3, y si r, con $0 \leq r \leq 3 - 1 = 2$, es el resto de la división correspondiente, entonces a pertenece precisamente a la clase $[2]_{\mathcal{R}}$.

2) El conjunto cociente definido por esta relación de equivalencia es

$$\begin{aligned} \mathbb{Z}/\mathcal{R} = \mathbb{Z}_3 &= \left\{[x]_{\mathcal{R}} :\ x \in \mathbb{Z}\right\} \\ &= \left\{[0]_{\mathcal{R}}, [1]_{\mathcal{R}}, [2]_{\mathcal{R}}\right\} \end{aligned}$$

Nota 1.4.5. *Podemos generalizar el resultado de este ejercicio para cualquier número natural $m \geq 2$.*

Ejercicio 1.4.6. *Demostrar que $\mathcal{R} = S \times S$ es una relación de equivalencia en S. ¿Cuáles son las clases de equivalencia de $\mathcal{R}$?*

1.5. Aplicaciones

1.5.1. Correspondencias y aplicaciones

Definición 1.5.1. *Una **correspondencia** de un conjunto A en un conjunto B es un subconjunto arbitrario del conjunto producto cartesiano*

$$A \times B = \{(x, y) :\ x \in A \ \ e \ \ y \in B\}.$$

Definición 1.5.2. *Sean A y B dos conjuntos y $f \subset A \times B$ una correspondencia de A en B.*

*Se dice que f es una **aplicación de** A **en** B si para cada elemento x de A existe un único elemento y de B tal que $(x, y) \in f$.*

Terminología 1. *Al conjunto A se le denomina* ***dominio*** *y al conjunto B se le denomina* ***codominio****.*

Ejemplo 1.5.3. Consideremos la aplicación f, del conjunto de los números reales $\mathbb{R}$ en sí mismo, que a cada número real x le hace corresponder su cuadrado x^2, lo abreviamos así:

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longrightarrow x^2 \end{aligned}$$

El hecho de que f haga corresponder a cada x precisamente x^2 tiene una formulación matemática rigurosa, a condición *de pensar en f como en un conjunto de pares ordenados*, y de especificar que el par ordenado (x, x^2) es un elemento del conjunto f para cada número real x.

En esta línea de pensamiento, f se definirá con rigor como

$$f = \{(x, x^2) : \ x \in \mathbb{R}\}$$

o equivalentemente como

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = x^2\}.$$

Ejemplo 1.5.4. El conjunto

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^2 + 1\}$$

es una correspondencia de $\mathbb{R}$ en $\mathbb{R}$, pero *no* es una aplicación, puesto que para cada número real x, el número real $x^2 + 1$ es positivo, resulta que si fijamos $x \in \mathbb{R}$, la ecuación

$$y^2 = x^2 + 1$$

tiene exactamente dos soluciones en el conjunto $\mathbb{R}$ de los números reales:

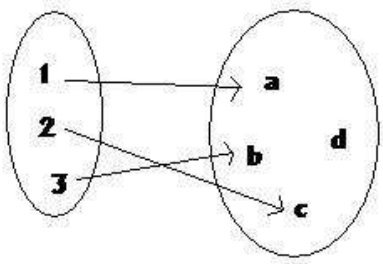
$$\begin{aligned} y_1 &= \sqrt{x^2 + 1} > 0 \\ y_2 &= -\sqrt{x^2 + 1} < 0 \end{aligned}$$

Por tanto, no se da la unicidad del elemento que la correspondencia C asigna a cada elemento x del conjunto $\mathbb{R}$, es decir,

$$(x, y_1), (x, y_2) \in C.$$

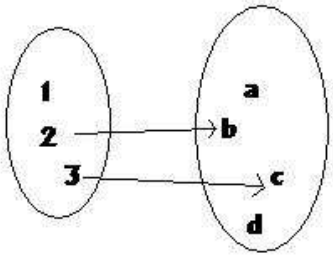
Ejemplo 1.5.5. Sean $A = \{1, 2, 3\}$ y $B = \{a, b, c, d\}$

1)



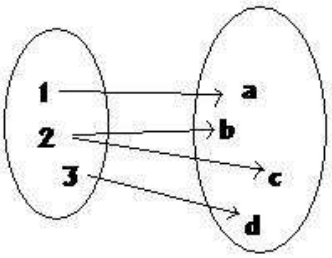
Sí es aplicación.

2)



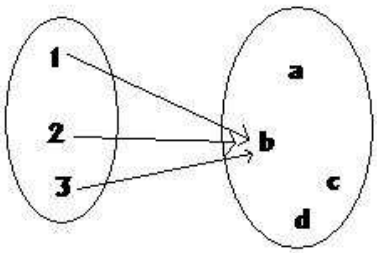
No, todos los elementos del conjunto A deben tener imagen en B.

3)



No, la imagen debe ser única

4)



Sí

1.5.2. Imagen de una aplicación

Definición 1.5.6. *Sea f es una aplicación de A en B y sea $x \in A$, el único elemento $y \in B$ tal que $(x, y) \in f$ recibe el nombre de* ***imagen del elemento*** *x* ***mediante la aplicación*** *f.*

Esto se suele expresar de alguna de las formas siguientes:

$$f : x \longrightarrow y \quad o \quad f(x) = y$$

Por tanto, escribir $f(x) = y$ es equivalente a escribir $(x, y) \in f$.

Ejemplo 1.5.7. La aplicación seno es la aplicación f de $\mathbb{R}$ en sí mismo definida por

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = \sin(x)\}.$$

En este caso, la imagen del número real x mediante f es $f(x) = \sin(x)$.

Si hacemos, en particular, $x = 2\pi$, tenemos

$$f(2\pi) = \sin(2\pi) = 0$$

es decir, $(2\pi, 0) \in f$, y decimos que 0 es la imagen de 2π mediante f.

Terminología 2. *Sea f es una aplicación de A en B.*

1) *Al elemento x tal que $f(x) = y$ se le denomina* ***contraimagen*** *de y.*

2) *El subconjunto de elementos del codominio B que son imagen de algún elemento del dominio A, recibe el nombre de* ***recorrido de la aplicación*** *f o* ***imagen de la aplicación*** *f, y se denota $f(A)$ o $\mathrm{Im}(f)$, es decir,*

$$f(A) = \mathrm{Im}(f) = \{f(a) : \ a \in A\}.$$

Definición 1.5.8. *Sea f una aplicación de A en B. Si M es un subconjunto no vacío de A, se define la* ***imagen de*** *M* ***por*** *f, y se escribe $f(M)$, como el subconjunto de B formado por las imágenes mediante f de todos los elementos de M, es decir,*

$$f(M) = \{f(x) : \ x \in M\}.$$

Si $M = \emptyset$, definimos $f(\emptyset) = \emptyset$.

Ejemplo 1.5.9. Sea

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \sin(x) \end{array}$$

- $\mathrm{Im}(f) = f(\mathbb{R}) = \{y \in \mathbb{R} : \ -1 \leq y \leq 1\} = [-1, 1]$.
- Si $M = \{k\pi : \ k \in \mathbb{Z}\}$, entonces

$$f(M) = \{0\}$$

ya que $\sin(k\pi) = 0$, para todo número entero k.

Definición 1.5.10. *Sea f una aplicación de A en B. La* ***imagen inversa*** *de un subconjunto $S \subseteq B$ por f es el conjunto de todos los elementos de A cuya imagen mediante f es un elemento de S, y se denota $f^{-1}(S)$, es decir,*

$$f^{-1}(S) = \{x \in A : \ f(x) \in S\}.$$

Ejemplo 1.5.11. Sea

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & x^2 \end{array}$$

- Si $S = (-\infty, 0)$, entonces

$$f^{-1}(S) = \{x \in \mathbb{R} : \ f(x) \in S\} = \emptyset$$

puesto que no existe ningún número real cuyo cuadrado sea un número real negativo.

- Si $I = [4, 9]$, entonces

$$\begin{aligned} f^{-1}(I) &= [-3, -2] \cup [2, 3] \\ &= \{x \in \mathbb{R} : \ (-3 \leq x \leq -2) \ \text{ o } \ (2 \leq x \leq 3)\} \end{aligned}$$

ya que los cuadrados de todos los números reales que forman parte de los intervalos $[-3, -2]$ y $[2, 3]$ están en el intervalo $[4, 9]$.

1.5.3. Propiedades de las aplicaciones

Proposición 1.5.12. *Sea f una aplicación de un conjunto A en otro conjunto B, entonces se verifica que:*

1) $\quad Si \ \ L \subset M \subset A \Longrightarrow f(L) \subset f(M)$

2) $\quad f(L \cup M) = f(L) \cup f(M), \ \forall\, L, M \in \mathcal{P}(A)$

3) $\quad f(L \cap M) \subset f(L) \cap f(M), \ \forall\, L, M \in \mathcal{P}(A)$

4) $\quad Si \ \ S \subset T \subset B \Longrightarrow f^{-1}(S) \subset f^{-1}(T)$

5) $\quad f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T), \ \forall\, S, T \in \mathcal{P}(B)$

6) $\quad f^{-1}(S \cap T) \subset f^{-1}(S) \cap f^{-1}(T), \ \forall\, S, T \in \mathcal{P}(B)$

Ejemplo 1.5.13. Sea la aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$. Consideremos los subconjuntos de $\mathbb{R}$ dados por

$$L = (-\infty, 0), \quad M = (0, +\infty)$$

Observamos que $f(L) = f(M) = (0, +\infty)$, pero $L \cap M = \emptyset$, de modo que

$$f(L \cap M) = \emptyset \neq (0, +\infty) = f(L) \cap f(M)$$

Así, en este caso, no se cumple la igualdad entre $f(L \cap M)$ y $f(L) \cap f(M)$.

1.5.4. Tipos de aplicaciones

Definición 1.5.14 (**Aplicación inyectiva**). *Sea f una aplicación de A en B. Decimos que f es* ***inyectiva*** *(o uno a uno) si*

$$\forall \;\; x_1, x_2 \in A, \;\; x_1 \neq x_2 \;\; \Longrightarrow \;\; f(x_1) \neq f(x_2).$$

O, equivalentemente,

$$\forall \;\; x_1, x_2 \in A, \;\; f(x_1) = f(x_2) \;\; \Longrightarrow \;\; x_1 = x_2.$$

Ejemplo 1.5.15. Sea

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & x^2 \end{array}$$

Si $x \neq 0$, entonces

$$f(x) = x^2 \;\; \text{y} \;\; f(-x) = (-x)^2 = x^2$$

Es decir, los elementos $x, -x \in \mathbb{R}$ son distintos y, sin embargo, tienen la misma imagen mediante f.

Por tanto, la aplicación f no es inyectiva.

Ejemplo 1.5.16. Sea

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longrightarrow & n^2 \end{array}$$

Sean $n, m \in \mathbb{N}$ tal que $f(n) = f(m)$. Entonces

$$n^2 = m^2 \;\; \Longrightarrow \;\; 0 = n^2 - m^2 = (n-m)(n+m)$$

Dado que estamos suponiendo que n y m son números enteros positivos, se deduce fácilmente que

$$n + m \geq 2\,, \;\; \forall \; n, m \in \mathbb{N}$$

Si el producto $(n-m)(n+m)$ es igual a cero, el factor $n - m$ ha de ser igual a cero, lo que es tanto como decir que

$$n = m.$$

Por tanto, la aplicación f es inyectiva.

Definición 1.5.17 (**Aplicación sobreyectiva**). *Sea f una aplicación de A en B. Se dice que f es* ***sobreyectiva****, cuando cada elemento $y \in B$ es la imagen mediante f de algún elemento $x \in A$, es decir,*

$$\forall \; y \in B, \;\; \exists \; x \in A \;\; \textit{tal que} \;\; f(x) = y$$

Proposición 1.5.18. *Sea f una aplicación de A en B. Entonces*

$$f \text{ es sobreyectiva} \iff \mathrm{Im}(f) = B$$

Ejemplo 1.5.19. La aplicación

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & x^2 \end{array}$$

no es sobreyectiva, ya que no existe número real x cuya imagen $f(x) = x^2$ sea el número real -1.

Ejemplo 1.5.20. Sea

$$\begin{array}{rccc} f: & \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ & (x,y) & \longrightarrow & 2x+3y \end{array}$$

Veamos que $\mathrm{Im}(f) = \mathbb{R}$

Para ello, es suficiente demostrar que cada elemento z de $\mathbb{R}$ está en $Im(f)$. Pero, para cada elemento z de $\mathbb{R}$, se cumple

$$2(-z) + 3z = 3z - 2z = z$$

Por tanto, $z = f(-z, z)$, con $(-z, z) \in \mathbb{R}\times\mathbb{R}$

Así, hemos comprobado que $\mathrm{Im}(f) = \mathbb{R}$, y, en consecuencia, que f es una aplicación sobreyectiva de $\mathbb{R}\times\mathbb{R}$ en $\mathbb{R}$.

Definición 1.5.21 (Aplicación biyectiva). *Sea f una aplicación de A en B. Se dice que f es **biyectiva** si es inyectiva y sobreyectiva.*

O, equivalentemente,

$$\forall\ y \in B,\ \ \exists!\ (\textit{existe un único})\ \ x \in A\ \ \textit{tal que}\ \ f(x) = y.$$

Ejemplo 1.5.22. La aplicación

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & 2x+3 \end{array}$$

es biyectiva. Probémoslo.

- En primer lugar, f es inyectiva, porque dados los números reales x, t, si $f(x) = f(t)$, tenemos que

  $$2x + 3 = 2t + 3 \Longrightarrow 2x = 2t \Longrightarrow x = t$$

  Queda así demostrado que f es inyectiva.

- En segundo lugar, f es sobreyectiva, es decir,

$$\mathrm{Im}(f) = f(\mathbb{R}) = \mathbb{R}$$

En efecto, para cada número real y, buscamos otro x tal que

$$2x + 3 = y.$$

Necesariamente ha de ser $x = \frac{y-3}{2}$. En efecto,

$$f\Big(\frac{y-3}{2}\Big) = 2 \cdot \frac{y-3}{2} + 3 = (y-3) + 3 = y$$

siendo $\frac{y-3}{2}$ un número real.

Así, $\mathrm{Im}(f) = \mathbb{R}$, luego f es sobreyectiva.

Por tanto, f es biyectiva.

C.Q.D (Como Queríamos Demostrar)

Ejemplo 1.5.23. La aplicación

$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longrightarrow & (x^2-y^2, 2xy) \end{array}$$

es suprayectiva, ya que un sistema de ecuaciones de la forma

$$\left\{ \begin{array}{ll} x^2 - y^2 & = a \\ 2xy & = b \end{array} \right.$$

tiene solución para cualquier par de valores a y b reales.

Sin embargo la aplicación no es inyectiva, dado que si

$$\left\{ \begin{array}{ll} x^2 - y^2 & = x'^2 - y'^2 \\ 2xy & = 2x'y' \end{array} \right. \not\Rightarrow \left\{ \begin{array}{l} x = x' \\ y = y' \end{array} \right.$$

Basta tomar $(x,y) = (1,1)$, $(x',y') = (-1,-1)$.

1.5.5. Composición de aplicaciones

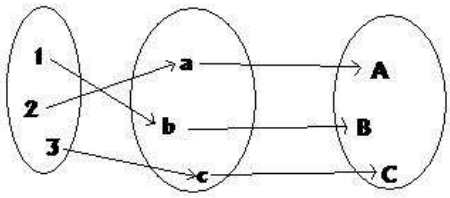
Definición 1.5.24. *Sean f una aplicación del conjunto A en el conjunto B y g una aplicación del conjunto B en el conjunto C.*

Se llama ***composición de f con g, o f compuesta con g****, y se denota $g \circ f$, en este orden, a la aplicación*

$$\begin{array}{rccc} h = g \circ f: & A & \longrightarrow & C \\ & x & \longrightarrow & h(x) = g \circ f(x) = g\big(f(x)\big). \end{array}$$

Ejemplo 1.5.25. $S = \{1, 2, 3\},\ T = \{a, b, c\},\ V = \{A, B, C\}$

$$\left\{\begin{array}{ll} f(1) = b, & g(a) = A \\ f(2) = a, & g(b) = B \\ f(3) = c, & g(c) = C \end{array}\right. \Longrightarrow \left\{\begin{array}{l} (g \circ f)(1) = B \\ (g \circ f)(2) = A \\ (g \circ f)(3) = C \end{array}\right.$$



Nota 1.5.26 (¡Atención!). *En general* $f \circ g \neq g \circ f$.

En el ejemplo anterior, no podemos calcular $f \circ g$ *dado que el codominio de* g *no coincide con el dominio de* f.

Ejemplo 1.5.27. Dados las siguientes aplicaciones

$$\begin{array}{rccc} f: & \mathbb{R} - \{1\} & \longrightarrow & \mathbb{R} - \{0\} \\ & x & \longrightarrow & \frac{1}{x-1} \end{array} \qquad \begin{array}{rccc} g: & \mathbb{R} - \{0\} & \longrightarrow & \mathbb{R} - \{0\} \\ & x & \longrightarrow & \frac{1}{y} \end{array}$$

su composición $g \circ f$ se define como

$$\begin{array}{rccc} g \circ f: & \mathbb{R} - \{1\} & \longrightarrow & \mathbb{R} - \{0\} \\ & x & \longrightarrow & g \circ f(x) = g\big(f(x)\big) = \frac{1}{f(x)} = \frac{1}{\frac{1}{x-1}} = x - 1 \end{array}$$

1.5.6. Restricción de una aplicación a un subconjunto

Definición 1.5.28. *Sea* $f : X \longrightarrow Y$ *una aplicación y sea* $A \subset X$.

Definimos f ***restringida a*** A, *y denotamos por* $f|_A$, *a la aplicación que cumple que*

$$\begin{array}{rccc} f|_A: & A & \longrightarrow & Y \\ & a & \longrightarrow & f|_A(a) = f(a) \end{array}$$

Capítulo 2

Grupos

2.1. Operaciones binarias

Definición 2.1.1. *Una* ***operación binaria*** (*ley de composición interna*) "$*$" *en un conjunto no vacío A es una aplicación*

$$\begin{array}{rccl} * : & A \times A & \longrightarrow & A \\ & (a,b) & \longrightarrow & *(a,b) \end{array}$$

Escribiremos $a * b$ en lugar de $*(a,b)$, y se lee "a multiplicado por b" o "a por b"

Ejemplo 2.1.2. La suma "+" y el producto "$\cdot$" son operaciones binarias en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$

Ejemplo 2.1.3. La aplicación

$$\begin{array}{rccl} * : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n,p) & \longrightarrow & n * p = n^2 \end{array}$$

es una operación binaria.

Ejemplo 2.1.4. La aplicación

$$\begin{array}{rccl} * : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n,p) & \longrightarrow & n * p = n - p \end{array}$$

no es una operación binaria, ya que, por ejemplo, $2 - 3 = -1 \notin \mathbb{N}$

Ejemplo 2.1.5. La aplicación

$$\begin{array}{rccl} * : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n,p) & \longrightarrow & n * p = \frac{n}{p} \end{array}$$

no es una operación binaria, ya que, por ejemplo, $\frac{2}{3} \notin \mathbb{N}$

2.2. Propiedades de las operaciones binarias

Sea $*$ una operación binaria sobre un conjunto A.

1) Asociativa: *Se dice que* $*$ *es* ***asociativa*** *si*

$$(a * b) * c = a * (b * c) \quad \textit{para cualesquiera} \quad a, b, c \in A$$

2) Conmutativa: *Se dice que* $*$ *es* ***conmutativa*** *si*

$$a * b = b * a \quad \textit{para todo} \quad a, b \in A$$

3) Elemento neutro por la izquierda: *Un elemento* $e \in A$ *se dice un* ***neutro por la izquierda*** *si*

$$e * a = a \quad \textit{para todo} \quad a \in A$$

4) Elemento neutro por la derecha: *Un elemento* $e \in A$ *se dice un* ***neutro por la derecha*** *si*

$$a * e = a \quad \textit{para todo} \quad a \in A$$

5) Elemento neutro: *Si un elemento* $e \in A$ *es simultáneamente neutro por la derecha y por la izquierda,* e *se llama simplemente* ***neutro***.

6) Elemento inverso por la izquierda: *Si* $e \in A$ *es un neutro para* $*$, $b \in A$ *se dice un* ***inverso de*** $a \in A$ ***por la izquierda*** *si*

$$b * a = e$$

7) Elemento inverso por la derecha: *Si* $e \in A$ *es un neutro para* $*$, $b \in A$ *se dice un* ***inverso de*** $a \in A$ ***por la derecha*** *si*

$$a * b = e$$

8) Elemento inverso: *Si el elemento inverso por la izquierda y por la derecha es el mismo, se denomina* ***inverso de*** $a \in A$ *y se simboliza por*

$$a^{-1}$$

Teorema 2.2.1. *El elemento neutro, si existe, de un conjunto* A *con respecto a una operación binaria* $*$ *es único.*

Teorema 2.2.2. *Sea* $*$ *una operación binaria sobre un conjunto* A. *Si* $*$ *es asociativa, el inverso de* $a \in A$, *si existe es único.*

Demostración. Sean b y c inversos de a, tenemos que

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b$$

□

Ejemplo 2.2.3. La suma "+" y el producto "·" en $\mathbb{R}$ son asociativas, conmutativas, todo $x \in \mathbb{R}$ tiene al elemento $-x$ como inverso aditivo, y si $x \neq 0$, $\frac{1}{x}$ es su inverso multiplicativo.

Ejemplo 2.2.4. En el conjunto $\mathcal{M}_2(\mathbb{R})$ de las matrices 2×2 el producto de matrices es asociativo, pero no conmutativo; la matriz identidad

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

es el neutro y por el álgebra lineal sabemos que una matriz $A \in \mathcal{M}_2(\mathbb{R})$ tiene un inverso multiplicativo si y sólo si su determinante es distinto de 0.

Ejemplo 2.2.5. Sea $*$ una operación binaria sobre $\mathbb{R}$, definida por

$$a * b = a + 2b \quad \text{para cualesquiera} \quad a, b \in \mathbb{R}.$$

Como

$$(a * b) * c = (a + 2b) * c = a + 2b + 2c$$

y

$$a * (b * c) = a * (b + 2c) = a + 2(b + 2c) = a + 2b + 4c,$$

entonces la operación $*$ no es asociativa.

Ejemplo 2.2.6. La operación binaria en $\mathbb{R}$, definida como

$$a * b = a^2 + b^2$$

es conmutativa pero no es asociativa.

Nota 2.2.7 (Tabla de multiplicar). *La mejor manera de representar una operación binaria es mediante una tabla de multiplicar*

Ejemplo 2.2.8. Si A es un conjunto finito, una operación binaria $*$ se puede describir dando su tabla de multiplicar.

Se colocará sobre el eje OX los elementos de A y sobre el eje OY de nuevo los elementos de A.

En los puntos de intersección de la fila de un elemento con la columna de otro elemento, colocaremos los resultados de multiplicar los correspondientes elementos.

Esto es, si $S = \{a, b, c\}$, tendremos,

$2^o elemento$

$1^{er} elemento$ $*$	**a**	**b**	**c**
a	$a * a$	$a * b$	$a * c$
b	$b * a$	$b * b$	$b * c$
c	$c * a$	$c * b$	$c * c$

2.3. Definición de grupo y propiedades

Definición 2.3.1. *Un **grupo** es un conjunto G no vacío en que está definida una operación binaria, $* : G \times G \longrightarrow G$, con las siguientes propiedades:*

1) *Cerrada:* $\forall\ a, b \in G, \quad a * b \in G$

2) *Asociativa:* $\forall\ a, b, c \in G, \quad (a * b) * c = a * (b * c)$

3) *Elemento neutro:* $\exists\ e \in G :\ \forall\ a \in G,\ a * e = e * a = a$

4) *Elemento inverso:* $\forall\ a \in G,\ \exists\ a^{-1} \in G :\ a * a^{-1} = a^{-1} * a = e$

Ejemplo 2.3.2. Los conjuntos

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +),$$
$$(\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot), (\mathbb{Q}^+, \cdot), (\mathbb{R}^+, \cdot), (\mathbb{C} - \{0\}, \cdot),$$

son grupos.

Ejemplo 2.3.3. El conjunto $\big(\{2n+1 :\ n \in \mathbb{Z}\}, +\big)$ no es un grupo, porque la suma no es una operación binaria cerrada en el conjunto de los números impares.

Proposición 2.3.4. *El elemento neutro de un grupo $(G, *)$ es único.*

Demostración. Supongamos que e y e' son elementos neutros en el grupo dado.

Como e es un elemento neutro, $e * a = a$ para todo $a \in G$; en particular

$$e * e' = e'.$$

Como $e * e' = e$ por ser e' también elemento neutro, se tiene $e = e'$ □

Proposición 2.3.5. *El elemento inverso de un elemento a de un grupo $(G, *)$ es único.*

Proposición 2.3.6 (Simplificar). *Si $(G,*)$ es un grupo, se tienen las siguientes propiedades: para todo $a,b,c \in G$*

$$\begin{cases} 1) \quad Si\ a*b = a*c \Rightarrow b = c \\ \\ 2) \quad Si\ a*b = c*b \Rightarrow a = c \end{cases}$$

Proposición 2.3.7. *Sea $(G,*)$ un grupo y $a \in G$, se tiene que*

$$\left(a^{-1}\right)^{-1} = a$$

Proposición 2.3.8. *En un grupo $(G,*)$ se tiene que*

$$(a*b)^{-1} = b^{-1}*a^{-1}$$

para todo $a,b \in G$.

Definición 2.3.9. *Un $(G,*)$ un grupo es* ***conmutativo o abeliano*** *si,*

$$a*b = b*a$$

para todo $a,b \in G$.

Ejemplo 2.3.10. $(\mathbb{Z},+),(\mathbb{R},+),(\mathbb{R}-\{0\},\cdot),...$

Proposición 2.3.11. *Sea $(G,*)$ un grupo. Las siguientes propiedades son equivalentes:*

1) *$(G,*)$ es abeliano*

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

Nota 2.3.12. *Sea $(G,*)$ un grupo. Para cualquier $a \in G$ y cualquier $n \in \mathbb{N}$, se define*

- $a^n = a*a*a*\cdots*a$ *de n factores*
- $a^{-n} = a^{-1}*a^{-1}*a^{-1}*\cdots*a^{-1}$ *de n factores*
- $a^0 = e$, *el elemento neutro de G*

Proposición 2.3.13. *Sea $(G,*)$ un grupo*

1) *Si $\forall\ x \in G,\ x^2 = x*x = e$, entonces G es abeliano*

2) *Si $\forall\ a,b \in G,\ (a*b)^2 = a^2*b^2$, entonces G es abeliano*

Definición 2.3.14 (Orden de un grupo). *Si $(G,*)$ es un grupo y G posee un número finito de elementos se define el* ***orden de*** *G, que se simboliza mediante $|G|$, $\text{card}(G)$ o $\mathcal{O}(G)$, como el número de elementos de G y se dice que $(G,*)$ es un grupo finito. En caso contrario diremos que $(G,*)$ es un grupo infinito.*

2.3.1. Grupos de matrices

Ejemplo 2.3.15. El conjunto $GL_n(\mathbb{R}) \subset \mathcal{M}_{n\times n}(\mathbb{R})$ de las matrices de orden n con determinante distinto de 0, con la operación producto de matrices, es un grupo. En efecto:

1) Operación interna: el producto de dos matrices de orden n con determinante distinto de 0 es otra matriz de orden n con determinante distinto de 0.

2) Propiedad asociativa: el producto de matrices es asociativo

3) Elemento neutro: la matriz identidad de orden n es una matriz con determinante no nulo que es el elemento neutro del producto

4) Elemento inverso: para todas las matrices de orden n con determinante no nulo existe otra matriz de orden n con determinante no nulo, donde el producto de ambas es la matriz identidad.

2.3.2. Grupos de congruencias

Definición 2.3.16. *Sea $m \in \mathbb{N}$ y sea $a, b \in \mathbb{Z}$, se dice que a es congruentes con b módulo m si y sólo si m divide a $(a-b)$, $\big($es decir, $a-b = k\cdot m$ para algún $k \in \mathbb{Z}\big)$, y lo representamos por*

$$a \equiv b \bmod(m)$$

Nota 2.3.17. *Sabemos que la relación de congruencia definida en el conjunto $\mathbb{Z}$ es una relación de equivalencia.*

Por lo tanto, la clase de equivalencia del elemento $a \in \mathbb{Z}$, que se denota $[a]$, es

$$[a] = \{b \in \mathbb{Z} : \ a \equiv b \bmod(m)\},$$

y el conjunto cociente de $\mathbb{Z}$ mediante esta relación de equivalencia se define como:

$$\mathbb{Z}_m = \big\{[0], [1], \ldots, [m-1]\big\}$$

Definición 2.3.18. *En el conjunto $\mathbb{Z}_m$ se define una suma "$\oplus$" y un producto "$\otimes$" de clases de equivalencias como:*

$$\begin{aligned} [a] \ \oplus \ [b] &= [a+b] \\ [a] \ \otimes \ [b] &= [a\cdot b] \end{aligned}$$

Proposición 2.3.19. *Sea $m \in \mathbb{N}$, entonces $(\mathbb{Z}_m, \oplus)$ es un grupo abeliano*

2.3.3. Grupo de las biyecciones de un conjunto

Sea $X \neq \emptyset$ un conjunto, y sea

$$\mathrm{Biy}(X) = \{f \text{ aplicación de } X \text{ en } X : f \text{ es biyectiva } \}$$

Sea $\circ$ la operación composición de aplicaciones.
El conjunto $(\mathrm{Biy}(X), \circ)$ es un grupo. En efecto,

1) Operación cerrada (interna):

   $f, g \in \mathrm{Biy}(X) \Rightarrow f \circ g \in \mathrm{Biy}(X)$ (visto en ejercicio 9 del tema 1)

2) Propiedad asociativa:

   $f, g, h \in \mathrm{Biy}(X) \Longrightarrow (f \circ g) \circ h = f \circ (g \circ h)$, ya que

$$\begin{aligned}\big((f \circ g) \circ h\big)(x) &= (f \circ g)(h(x)) = f\big(g(h(x))\big) \\ &= f\big((g \circ h)(x)\big) = \big(f \circ (g \circ h)\big)(x)\end{aligned}$$

3) Elemento neutro:

   Sea la aplicación $i : X \longrightarrow X$ tal que $\forall x \in X,\ i(x) = x$, por lo tanto

   $\left.\begin{array}{l}(i \circ f)(x) = i(f(x)) = f(x) \\ (f \circ i)(x) = f(i(x)) = f(x)\end{array}\right\} \Longrightarrow i$ es el elemento neutro

4) Elemento inverso:

   Si $f : X \longrightarrow X$, definimos $f^{-1} : X \longrightarrow X$, de modo que si

$$f(x) = y \Longrightarrow f^{-1}(y) = x.$$

   Tendremos que f^{-1} es una aplicación biyectiva dado que f también lo es.

   $\left.\begin{array}{l}(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = i(x) \\ (f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = i(y)\end{array}\right\} \Longrightarrow f^{-1}$ es el elemento inverso de f

2.3.4. Grupos de permutaciones

Definición 2.3.20. *Sea $S = \{1, 2, 3, \ldots, n\}$ el conjunto de los n primeros números naturales.*

*Una **permutación de** n **elementos** es una biyección $\sigma : S \longrightarrow S$ que se escribe de la forma*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

El conjunto de todas las permutaciones del conjunto $\{1, 2, \ldots, n\}$ *se denotará por* S_n.

En S_n *definimos una operación binaria interna* $*$ *como la composición de aplicaciones, esto es:*

$$\sigma * \tau = \sigma \circ \tau, \ \forall \ \sigma, \tau \in S_n$$

Ejemplo 2.3.21. Sean σ y τ dos permutaciones de S_3 dadas por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Entonces

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

mientras que

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Observación 2.3.22. *El número de elementos de* S_n *es* $n!$*, es decir,*

$$|S_n| = \text{card}(S_n) = n!$$

Nota 2.3.23. *Denotaremos por* e *la permutación correspondiente a la aplicación identidad, esto es,*

$$e(i) = i, \quad i = 1, 2, ..., n,$$

o en la notación anterior

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

Claramente

$$\sigma \circ e = e \circ \sigma = e, \ \forall \ \sigma \in S_n,$$

Definición 2.3.24. *El conjunto* S_n *con la operación de composición de aplicaciones* $\circ$*, se llama* ***grupo de*** n ***permutaciones***

Ejemplo 2.3.25. Escribiremos la tabla del grupo $(S_3, \circ)$

$$S_3 = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \right.$$
$$\left. \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

La tabla de multiplicar es:

$\circ$	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_2	τ_3	τ_1
σ_2	σ_2	e	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	e	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	e	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	e

Observación 2.3.26.

- *Se observa fácilmente que* $\tau_i^{-1} = \tau_i$, $i = 1,2,3$ *y* $\sigma_1^{-1} = \sigma_2$.
- *El grupo* $(S_3, \circ)$ *no es abeliano*

Proposición 2.3.27.

- *El grupo* $(S_2, \circ)$ *es abeliano*
- *Si* $n \geq 3$, *el grupo* $(S_n, \circ)$ *no es abeliano*

2.4. Subgrupos de un grupo

Definición 2.4.1. *Sea* $(G, *)$ *y un subconjunto* $H \neq \emptyset$ *de* G. *Se dice que* H *es un* ***subgrupo*** *de* $(G, *)$, *y se escribe* $(H, *) \leq (G, *)$, *si* H *es un grupo con respecto a la operación* $*$ *definida en* G.

Observación 2.4.2. *Si* $(H, *) \leq (G, *)$, *entonces*

1) *El elemento neutro de* G *pertenece a* H.
2) *Si* $a \in H$, *su inverso,* a^{-1} *pertenece a* H.

Ejemplo 2.4.3. $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ y este, a su vez, es un subgrupo de $(\mathbb{R}, +)$.

Ejemplo 2.4.4. $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$ es un subgrupo de $(\mathbb{R}^* = \mathbb{R} - \{0\}, \cdot)$.

Ejemplo 2.4.5. Los enteros pares son un subgrupo de $(\mathbb{Z}, +)$. Sin embargo, los enteros impares no forman un subgrupo.

Nota 2.4.6. $\{e\}$ *y* G *con la operación* $*$ *son subgrupos de* $(G, *)$. *A estos subgrupos se les denomina* ***impropios***. *Al resto de subgrupos de un grupo se les denomina* ***propios***.

Proposición 2.4.7. *Sea $(G, *)$ un grupo y H un subconjunto de G, con $H \neq \emptyset$. H es un subgrupo de $(G, *)$ si y sólo si para todo $x, y \in H$, $x * y^{-1} \in H$*

Demostración.

- $\boxed{\Rightarrow}$

  Supongamos que $(H, *)$ es un subgrupo de $(G, *)$. Dados $x, y \in H$, tenemos $y^{-1} \in H$, y por tanto $x * y^{-1} \in H$.

- $\boxed{\Leftarrow}$

  Supongamos que $x * y^{-1} \in H$ para todo $x, y \in H$,

  1) Elemento neutro:
     Si $x = y \Rightarrow x^{-1} = y^{-1} \Longrightarrow x * y^{-1} = x * x^{-1} \in H \Longrightarrow e \in H$.
  2) Elemento inverso:
     Sea $x \in H$. Como para todo $x, y \in H$, se tiene que $x * y^{-1} \in H$, entonces
     $$e * x^{-1} = x^{-1} \in H$$
  3) Operación interna:
     Sean $x, y \in H$, entonces $y^{-1} \in H$, luego $(y^{-1})^{-1} \in H$. Por hipótesis tenemos que $x * (y^{-1})^{-1} \in H$. Por tanto $x * y \in H$.
  4) Asociativa:
     $(x * y) * z = x * (y * z)$, $\forall x, y, z \in H$ ya que $x, y, z \in G$ y G es un grupo con la propiedad asociativa.

□

Proposición 2.4.8. *Dado un grupo $(G, *)$, la intersección de dos subgrupos de G, H_1 y H_2, es un subgrupo de G.*

Demostración. $H = H_1 \cap H_2 \neq \emptyset$ ya que $e \in H_1$ y $e \in H_2$

$$\begin{aligned} \forall x, y \in H &\Longrightarrow x \in H_1, y \in H_1, \quad x \in H_2, y \in H_2 \\ &\Longrightarrow x * y^{-1} \in H_1, \quad x * y^{-1} \in H_2 \\ &\Longrightarrow x * y^{-1} \in H_1 \cap H_2 = H \end{aligned}$$

por lo tanto, por la proposición anterior, H es un subgrupo. □

2.4.1. Subgrupo generado por un subconjunto

Definición 2.4.9. *Dado un subconjunto S de un grupo $(G,*)$, se llama* ***subgrupo generado por*** *S, y se denota $\langle S\rangle$, al más pequeño de los subgrupos de $(G,*)$ que contienen a S, es decir:*

$$\langle S\rangle = \bigcap_{\substack{H\leq G\\ H\supset S}} H.$$

Proposición 2.4.10. *Si $(G,*)$ es un grupo y S es un subconjunto de G, se tiene que*

$$\langle S\rangle = \left\{ s_1^{k_1} * s_2^{k_2} * \cdots * s_n^{k_n} :\ n\in\mathbb{N} : s_1, s_2, \ldots, s_n \in S,\ k_1, k_2, \ldots, k_n \in \mathbb{Z}\right\}$$

Demostración. Sea

$$H_s = \left\{ s_1^{k_1} * s_2^{k_2} * \cdots * s_n^{k_n} :\ s_1, s_2, \ldots, s_n \in S,\ k_1, k_2, \ldots, k_n \in \mathbb{Z}\right\}.$$

1) H_s es un subgrupo de $(G,*)$. En efecto:

   ▶ $H_s \neq \emptyset$ ya que $\forall s\in S, s = s^1 \in H_s$, es decir, $S\subset H_s$.

   ▶ Si $x, y \in H_s$, con

   $$x = s_1^{k_1} * \cdots * s_n^{k_n} \ \text{ siendo } \ s_1, ..., s_n \in S \ \text{ y } \ k_1, ..., k_n \in \mathbb{Z},$$

   y con

   $$y = t_1^{l_1} * \cdots * t_m^{l_m} \ \text{ siendo } \ t_1, ..., t_m \in S \ \text{ y } l_1, ..., l_m \in \mathbb{Z},$$

   como

   $$y^{-1} = t_m^{-l_m} * \cdots * t_1^{-l_1},$$

   tendremos que

   $$x * y^{-1} = s_1^{k_1} * \cdots * s_n^{k_n} * t_m^{-l_m} * \cdots * t_1^{-l_1} \in H_s.$$

2) Probamos que $\langle S\rangle = H_s$.

   Como $\langle S\rangle$ es el más pequeño de los subgrupos que contiene a S y $S\subset H_s$ se tiene que

   $$\langle S\rangle \subseteq H_s.$$

   Falta probar la inclusión contraria: Sea $x = s_1^{k_1} * \cdots * s_n^{k_n} \in H_s$, done $s_i \in S$ y $k_i \in \mathbb{Z}$ para todo $i = 1, 2, \ldots, n$.

Puesto que $S \subset \langle S \rangle$ y $\langle S \rangle$ es un subgrupo de $(G, *)$, se tiene que $s_i^{k_i} \in \langle S \rangle$ para todo $i = 1, 2, \ldots, n$, con lo cual

$$x = s_1^{k_1} * \cdots * s_n^{k_n} \in \langle S \rangle$$

Por tanto

$$H_s \subseteq \langle S \rangle.$$

□

Ejemplo 2.4.11. Tomemos el subconjunto $S = \{\sigma_1, \sigma_2\}$ del grupo S_3 de permutaciones de tres elementos. En este caso, el subgrupo generado es $\langle S \rangle = \{e, \sigma_1, \sigma_2\}$.

2.4.2. Subgrupo generado por un elemento

Definición 2.4.12. *Sea $(G, *)$ un grupo y sea $a \in G$. Denotaremos $\langle a \rangle$ y lo llamaremos* ***subgrupo generado por el elemento*** *a al subgrupo*

$$\langle a \rangle = \{a^k : \ k \in \mathbb{Z}\}$$

Ejemplo 2.4.13. Tomemos el elemento τ_2 del grupo S_3. El subgrupo generado será $\langle \tau_2 \rangle = \{e, \tau_2\}$

2.4.3. Grupo cíclico

Definición 2.4.14. *Un grupo G se dice que es un* ***grupo cíclico*** *si existe al menos un elemento $x \in G$ tal que el subgrupo generado por x es G, es decir, $\langle x \rangle = G$.*

Ejemplo 2.4.15. $(\mathbb{Z}, +)$ y $(\mathbb{Z}_m, \oplus)$ son grupos cíclicos con generadores 1 y [1], respectivamente.

2.5. Clases laterales

Definición 2.5.1. *Sea H un subgrupo del grupo $(G, *)$ y sea a un elemento de G, se llama* ***clase lateral por la izquierda de*** *H al conjunto*

$$aH = \{a * h \in G : \ \forall h \in H\}$$

Análogamente definimos ***clase lateral por la derecha*** *al conjunto*

$$Ha = \{h * a \in G : \ \forall h \in H\}$$

Ejemplo 2.5.2.

1) Dado el grupo de las permutaciones de tres elementos S_3 y dado el subgrupo $H = \{e, \sigma_1, \sigma_2\}$, las clases laterales por la izquierda y por la derecha de dicho subgrupo son:

$$\begin{array}{ll} eH = H, & He = H \\ \sigma_2 H = H, & H\sigma_2 = H \\ \sigma_1 H = H, & H\sigma_1 = H \\ \tau_1 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_1 = \{\tau_1, \tau_2, \tau_3\} \\ \tau_2 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_2 = \{\tau_1, \tau_2, \tau_3\} \\ \tau_3 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_3 = \{\tau_1, \tau_2, \tau_3\} \end{array}$$

2) Dado el grupo de las permutaciones de tres elementos S_3 y dado el subgrupo $H = \{e, \tau_1\}$, las clases laterales por la izquierda y por la derecha de dicho subgrupo son:

$$\begin{array}{ll} eH = H, & He = H \\ \sigma_2 H = \{\sigma_2, \tau_3\}, & H\sigma_2 = \{\sigma_2, \tau_2\} \\ \sigma_1 H = \{\sigma_1, \tau_2\}, & H\sigma_1 = \{\sigma_1, \tau_3\} \\ \tau_1 H = H, & H\tau_1 = H \\ \tau_2 H = \{\sigma_1, \tau_2\}, & H\tau_2 = \{\sigma_2, \tau_2\} \\ \tau_3 H = \{\sigma_2, \tau_3\}, & H\tau_3 = \{\sigma_1, \tau_3\} \end{array}$$

Observación 2.5.3.

1) *La clase lateral por la izquierda aH no tiene por qué coincidir con la clase lateral por la derecha Ha (ejemplo 2).*

2) *La igualdad de clases no se refiere a los productos individuales sino a conjuntos completos (en el ejemplo 2, $eH = \tau_1 H$)*

3) *El elemento que define la clase está en la clase.*

Teorema 2.5.4. *Sea G un grupo y H un subgrupo de $(G, *)$. Entonces las clases laterales derechas (respectivamente: izquierdas) de H en G constituyen una partición de G.*

Demostración. Demostramos el caso por la derecha, el otro es análogo.

1) Probamos que $G = \bigcup_{g \in G} Hg$

   ▶ Sea $x \in G$, entonces

   $$x \in Hx = \{h * x \in G : \ \forall h \in H\}$$

   ya que $x = e * x$ donde $e \in H$. Luego $x \in Hx \subset \bigcup_{g \in G} Hg$.

Por tanto

$$G \subseteq \bigcup_{g \in G} Hg.$$

- Sea $x \in \bigcup_{g \in G} Hg$, entonces existe un $g_0 \in G$ tal que $x \in Hg_0$.

  Puesto que $Hg_0 \subset G$, se tiene que $x \in G$.

  Luego

$$\bigcup_{g \in G} Hg \subseteq G.$$

Por tanto

$$G = \bigcup_{g \in G} Hg.$$

2) Probamos que si dos clases laterales derechas se intersecan, deben ser iguales.

   Sean Ha y Hb dos clases de H en G, supongamos que

$$Ha \cap Hb \neq \emptyset$$

   entonces existe $x \in Ha \cap Hb$, por lo que

$$x = h * a = h' * b$$

   con $h, h' \in H$.

   La ecuación $h * a = h' * b$ implica que $a = h^{-1} * h' * b$, como $h^{-1} * h' \in H$ por ser subgrupo, se tiene que $a \in Hb$.

   Sea ahora $y \in Ha$, entonces existe $h'' \in H$ tal que $y = h'' * a$.

   Como $a = h^{-1} * h' * b$ tenemos que

$$y = h'' * h^{-1} * h' * b,$$

   es decir $y \in Hb$

   Luego

$$Ha \subset Hb.$$

   De la misma forma se demuestra que $Hb \subset Ha$, por lo tanto

$$Ha = Hb.$$

Como todo elemento de G está en alguna clase y las clases o son iguales o son disjuntas formarán una partición de G. □

2.6. Teorema de Lagrange

Teorema 2.6.1 (Lagrange). *Si G es un grupo finito y H un subgrupo de G, entonces el orden de H divide el orden de G*

Demostración. Supongamos que $G = \{g_1, g_2, \ldots, g_n\}$.

Sean $Hg_1, ..., Hg_n$ las clases por la derecha de H en G que formen una partición de G, es decir

$$G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_n$$

donde $Hg_i \cap Hg_j = \emptyset$ si $i \neq j$ con $i, j = 1, 2, \ldots, n$.

Definimos la aplicación

$$\begin{array}{rccc} \varphi_g : & H & \longrightarrow & Hg \\ & a & \longrightarrow & a * g \end{array}$$

dicha aplicación es biyectiva, ya que es suprayectiva (por definición de clase) e inyectiva porque si

$$\varphi_g(a) = \varphi_g(b) \Longrightarrow a * g = b * g \Longrightarrow a = b.$$

Por lo tanto, $\text{card}(Hg) = \text{card}(H)$ por ser biyectiva. En este caso tendremos que

$$\text{card}(G) = \text{card}(Hg_1) + \cdots + \text{card}(Hg_n) = n \cdot \text{card}(H).$$

Por tanto, $\text{card}(H)$ divide $\text{card}(G)$. □

Ejemplo 2.6.2. $G = \{1, 2, 3, 4, 5\}, H = \{1, 2\}$ no puede ser nunca un subgrupo de G aunque no conozcamos la operación definida en G

Corolario 2.6.3. *Si G es un grupo de orden p, con p primo, entonces G es cíclico.*

Demostración. Sea $x \in G$ con $x \neq e$, el subgrupo $\langle x \rangle$ es distinto de $\{e\}$.

Por el Teorema de Lagrange, $\text{card}(\langle x \rangle)$ divide a p, puesto que p es primo, entonces sus únicos divisores son 1 y p.

Como $\text{card}(\langle x \rangle) > 1$ se ha de tener $\text{card}(\langle x \rangle) = p$ y por tanto x es un generador de G. □

Observación 2.6.4. *Si el orden de G es primo, entonces G no tiene subgrupos propios, tendrá solamente los impropios: $\{e\}, G$*

Ejemplo 2.6.5.

1) Determinar los subgrupos del grupo cuya tabla de multiplicar es:

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

(Grupo de Klein)

Los subgrupos serán de orden 1, 2 ó 4.

Orden 1:$\{I\}$

Orden 2: $\{I, A\}, \{I, B\}, \{I, C\}$

Orden 4: $G = \{I, A, B, C\}$

2) Determinar los subgrupos del grupo C_5 cuya tabla de multiplicar es:

	I	A	B	C	D
I	I	A	B	C	D
A	A	B	C	D	I
B	B	C	D	I	A
C	C	D	I	A	B
D	D	I	A	B	C

(Grupo cíclico de orden 5)

Este grupo no tiene ningún subgrupo propio.

3) Determinar los subgrupos del grupo de permutaciones de tres elementos S_3

Como card$(S_3) = 6$, podemos tener subgrupos de orden 1, 2, 3 ó 6

Orden 1: $\{e\}$

Orden 2: $\{e, \tau_1\}, \{e, \tau_2\}, \{e, \tau_3\}$

Orden 3: $\{e, \sigma_1, \sigma_2\}$

Orden 6: S_3

4) Determinar los subgrupos del grupo C_4 cuya tabla de multiplicar es:

$*$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

(Grupo cíclico de orden 4)

Los subgrupos serán de orden 1, 2 ó 4:

Orden 1: $\{I\}$

Orden 2: $\{I, B\}$

Orden 4: $\{I, A, B, C\}$

2.7. Subgrupos normales y grupo cociente

Definición 2.7.1. *Sea $(G, *)$ un grupo y H un subgrupo de G. Se dice que dos elementos $x, y \in G$ están relacionados mediante H, y escribimos $x \equiv y(H)$, si y sólo si $x^{-1} * y \in H$.*

Proposición 2.7.2. *Sea $(G, *)$ un grupo y H un subgrupo de G. La relación definida en* 2.7.1 *es una relación de equivalencia y la clase de equivalencia de un elemento x de G en esta relación coincide con:*

$$xH = \{x * h : \ h \in H\}$$

(*clase lateral por la izquierda de H*)

Nota 2.7.3. *El conjunto de las clases de equivalencia* (*conjunto cociente*) *que se obtienen al definir en G la relación de equivalencia módulo H dada en la definición* 2.7.1*, es el siguiente conjunto:*

$$G/H = \{gH : \ g \in G\},$$

(*conjunto de particiones formado por las clases laterales por la izquierda de H*).

Es natural preguntarse si al conjunto G/H se le puede dotar de una estructura de grupo, cuya operación esté relacionada con la operación de G.

En este sentido lo más lógico que cabe esperar del resultado de operar las clases de equivalencia xH e yH en G/H es la clase de equivalencia $(x * y)H$. Pero esto no sucede para cualquier subgrupo de un grupo dado como se muestra en el ejemplo siguiente.

Ejemplo 2.7.4. Sea $H = \{e, b\}$ un subgrupo del siguiente grupo.

$*$	e	a	a^2	b	$a*b$	a^2*b
e	e	a	a^2	b	$a*b$	a^2*b
a	a	a^2	e	$a*b$	a^2*b	b
a^2	a^2	e	a	a^2*b	b	$a*b$
b	b	a^2*b	$a*b$	e	a^2	a
$a*b$	$a*b$	b	a^2*b	a	e	a^2
a^2*b	a^2*b	$a*b$	b	a^2	a	e

D_6 (Grupo diédrico de orden 6)

Tenemos

$$aH = \{a, a*b\} \text{ y } a^2H = \{a^2, a^2*b\}$$

con lo que

$$(aH)\cdot(a^2H) = \{e, b, a*b*a^2, a*b*a^2*b\} = \{e, b, a^2*b, a^2\}$$

mientras

$$(a*a^2)H = a^3H = eH = H.$$

Observación 2.7.5. *El ejemplo anterior sugiere que únicamente para algunos subgrupos distinguidos de G puede definirse una operación en el conjunto cociente. Tales subgrupos reciben el nombre de* **"normales"**.

Definición 2.7.6. *Un subgrupo H de un grupo $(G, *)$ se dice* ***normal****, y escribiremos $H \lhd G$, si $gH = Hg$ para todo $g \in G$.*

Ejemplo 2.7.7. Todo subgrupo de un grupo abeliano es normal.

En efecto: Sea H es subgrupo de $(G, *)$ (abeliano), y sea $g \in G$. Tenemos que

$$g*h = h*g, \ \forall h \in H \subset G.$$

Por tanto $gH = Hg$.

Ejemplo 2.7.8. En el grupo de las permutaciones de tres elementos, S_3, el subgrupo $H = \{e, \sigma_1, \sigma_2\}$ es normal. Sin embargo, los subgrupos $H_1 = \{e, \tau_1\}, H_2 = \{e, \tau_2\}$ y $H_3 = \{e, \tau_3\}$ no lo son.

Ejemplo 2.7.9. Los subgrupos impropios son normales.

En efecto: Dado el subgrupo impropio $H = \{e\}$, como $e*g = g = g*e$, tenemos que

$$gH = Hg, \forall g \in G$$

Dado el subgrupo impropio $H = G$, tenemos que

$$gH = G = Hg, \forall g \in G$$

Proposición 2.7.10. *Sea $(G, *)$ un grupo y H un subgrupo de G, las siguientes condiciones son equivalentes*

1) *H es un subgrupo normal de G.*

2) *$x * h * x^{-1} \in H$ para todo $x \in G$ y para todo $h \in H$*

3) *$xH = Hx$ para todo $x \in G$, es decir, las clases laterales por la izquierda y por la derecha de H coinciden.*

Demostración. Demostraremos que 1) $\Rightarrow$ 2), 2) $\Rightarrow$ 3) y 3) $\Rightarrow$ 1), con lo cual quedará demostrada la proposición.

- $\boxed{1) \Rightarrow 2)}$ Sea $x \in G$ y $h \in H$.

  Como H es normal, es decir $xH = Hx$, entonces $x * h = h * x$.

  Así que $x * h * x^{-1} = h \in H$

- $\boxed{2) \Rightarrow 3)}$ Sea $x \in G$.

  - ⊙ Si $y \in xH$ entonces existe $h \in H$ tal que $y = x * h$. Como $x * h * x^{-1} \in H$, operando con x por la derecha se obtiene $x * h \in Hx$, es decir, $y \in Hx$.

    Luego
    $$xH \subset Hx.$$

  - ⊙ Si $y \in Hx$ entonces existe $h \in H$ tal que $y = h * x$.

    Puesto que $x^{-1} * h * (x^{-1})^{-1} \in H$, se obtiene que $h * x \in xH$, así que $y \in xH$.

    Luego
    $$Hx \subset xH.$$

  Por tanto $xH = Hx$.

- $\boxed{3) \Rightarrow 1)}$ Por la definición del subgrupo normal.

C.Q.D

□

Observación 2.7.11. *Sea $(G, *)$ un grupo y H un subgrupo normal de G. Entonces,*

$$\{gH : \ g \in G\} = \{Hg : \ g \in G\}.$$

Por tanto, los conjuntos de clases laterales izquierda y derecha proporcionen la misma partición del grupo G.

Proposición 2.7.12. *Sea $(G, *)$ un grupo y H un subgrupo normal de G. Si $aH = a'H$ y $bH = b'H$, entonces $(a * b)H = (a' * b')H$.*

Demostración. Sea $aH = a'H$, tenemos que $a \in a'H$, entonces existe $h' \in H$ tal que $a = a' * h'$.

De igual modo si $bH = b'H \Longrightarrow b \in b'H \Longrightarrow$ existe $h'' \in H$ tal que $b = b' * h''$

Por lo tanto,

$$\begin{aligned} a * b = a' * h' * b' * h'' &= a' * b' * \Big[\overbrace{\big(b'^{-1} * h' * b' \big)}^{\in H \text{ por ser normal}} * h'' \Big]^{=h''' \in H} \\ &= a' * b' * h'''. \end{aligned}$$

Así que

$$a * b \in (a' * b')H.$$

Luego

$$(a * b)H \subset (a' * b')H$$

Como las clases laterales forman una partición, entonces

$$\begin{aligned} (a * b)H \subset (a' * b')H &\Longrightarrow (a * b)H \cap (a' * b')H \neq \emptyset \\ &\Longrightarrow (a * b)H = (a' * b')H \end{aligned}$$

□

Observación 2.7.13. *La proposición anterior muestra que la operación producto de dos clases de equivalencia en G/H definida de la forma siguiente:*

$$\begin{array}{rccl} \cdot & : & G/H \times G/H & \longrightarrow G/H \\ & & (aH, bH) & \longrightarrow \cdot(aH, bH) = aH \cdot bH = (a * b)H \end{array}$$

está bien definida, es decir, el producto de las clases del conjunto cociente G/H es independiente de los elementos elegidos para calcularlo si el subgrupo es normal.

Teorema 2.7.14 (Grupo cociente). *Sea $(G, *)$ un grupo y H un subgrupo normal de G. Sean $x, y \in G$, la operación*

$$(xH) \cdot (yH) = (x * y)H$$

define en el conjunto cociente G/H una estructura de grupo. Este grupo se llama ***grupo cociente de*** *G* ***sobre*** *H.*

Demostración.

1) Operación interna:

   Si $a, b \in G$, entonces $(aH)\cdot(bH) \in G/H$ ya que $(a*b)H$ es uno de los elementos de la partición definida por el subgrupo H.

2) Propiedad asociativa:

   Sean $a, b, c \in G$, tenemos que

$$\big((aH)\cdot(bH)\big)\cdot(cH) = \big((a*b)H\big)\cdot cH = \big((a*b)*c\big)H.$$

   Como G es un grupo, entonces $(a*b)*c = a*(b*c)$.

   Así que

$$\begin{aligned}\big((a*b)*c\big)H = \big(a*(b*c)\big)H &= (aH)*\big((b*c)H\big)\\ &= (aH)\cdot\big((bH)\cdot(cH)\big).\end{aligned}$$

3) Elemento neutro:

   La clase $eH = H$ es el elemento neutro del producto de clases ya que $(aH)\cdot(eH) = (a*e)H = aH$.

4) Elemento inverso:

   Dada una clase aH existe una clase inversa $a^{-1}H$, tal que su producto es el elemento neutro, ya que

$$(aH)\cdot(a^{-1}H) = (a*a^{-1})H = eH = H.$$

□

Ejemplo 2.7.15. Sea el grupo S_3 de las permutaciones de tres elementos y el subgrupo normal $H = \{e, \sigma_1, \sigma_2\}$, definimos las clases

$$E = eH = \{e, \sigma_1, \sigma_2\} = \sigma_1 H = \sigma_2 H$$
$$A = \tau_1 H = \tau_2 H = \tau_3 H = \{\tau_1, \tau_2, \tau_3\}$$

Tenemos que
$E\cdot E = (eH)\cdot(eH) = (e*e)H = eH = E$
$E\cdot A = (eH)\cdot(\tau_1 H) = (e*\tau_1)H = \tau_1 H = A$
$A\cdot A = (\tau_1 H)\cdot(\tau_1 H) = (\tau_1*\tau_1)H = eH = E$
Por lo tanto, la tabla de multiplicar es:

$(G/H,\cdot)$	E	A
E	E	A
A	A	E

Podemos ver que dicho conjunto de clases con la operación producto de clases es un grupo.

Ejemplo 2.7.16. Sea el grupo S_3 de las permutaciones de tres elementos y el subgrupo $H = \{e, \tau_1\}$.

Como H no es un subgrupo normal, no podemos definir el grupo cociente G/H, ya que, por ejemplo $\sigma_2 H = \tau_3 H$, pero

$$(\sigma_2 H) \cdot (\sigma_1 H) = (\sigma_2 * \sigma_1)H = eH = H = \{e, \tau_1\},$$

sin embargo

$$(\tau_3 H) \cdot (\sigma_1 H) = (\tau_3 * \sigma_1)H = \tau_2 H = \{\tau_2, \sigma_1\}.$$

Como vemos $H \neq \tau_2 H$, por lo que la operación entre clases no está bien definida, es decir,

$$\big(\sigma_2 H, \sigma_1 H\big) = \big(\tau_3 H, \sigma_1 H\big) \text{ no implica } (\sigma_2 H) \cdot (\sigma_1 H) = (\tau_3 H) \cdot (\sigma_1 H)$$

Esto es debido a que el subgrupo utilizado no es normal.

2.8. Homomorfismos de Grupos

Definición 2.8.1. *Sean $(G_1, *)$ y $(G_2, \circ)$ dos grupos y f una aplicación de G_1 en G_2, $f : G_1 \longrightarrow G_2$. La aplicación f es un* ***homomorfismo de grupos*** *si para todo $x, y \in G_1$, tenemos que*

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

Ejemplo 2.8.2. La aplicación

$$\begin{array}{rccc} f: & (\mathbb{R}, +) & \longrightarrow & (\mathbb{R} - \{0\}, \cdot) \\ & x & \longrightarrow & e^x \end{array}$$

es un monomorfismo, ya que

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

para todo $x, y \in \mathbb{R}$.

Ejemplo 2.8.3. Si $(G, *)$ es un grupo abeliano, entonces la aplicación

$$\begin{array}{rccc} f: & (G, *) & \longrightarrow & (G, *) \\ & x & \longrightarrow & x^2 \end{array}$$

es un monomorfismo, ya que

$$f(x * y) = (x * y)^2 = x * y * x * y = (x * x) * (y * y) = f(x) * f(y)$$

para todo $x, y \in G$.

2.8.1. Clasificación de homomorfismos

Definición 2.8.4. *Sea f un homomorfismo entre grupos, tenemos que:*

1) *Si f es inyectiva, entonces f es un* ***monomorfismo***
2) *Si f es sobreyectiva, entonces f es un* ***epimorfismo***
3) *Si f es biyectiva, entonces f es un* ***isomorfismo***
4) *Un isomorfismos entre un mismo grupo se llama* ***automorfismos****.*
5) *Dos grupos son* ***isomorfos*** *si se puede establecer un isomorfismo entre ellos.*

Ejemplo 2.8.5. La aplicación

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}-\{0\},\cdot) \\ & x & \longrightarrow & e^x \end{array}$$

es un homomorfismo y como además f es inyectiva, entonces es un monomorfismo.

Ejemplo 2.8.6. La aplicación

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^+,\cdot) \\ & x & \longrightarrow & e^x \end{array}$$

tenemos que f es biyectiva y por tanto es un isomorfismo.

Ejemplo 2.8.7. Sean los grupos $G_1 = (\mathbb{R}-\{0\},\cdot)$ y $G_2 = (\mathbb{R}-\{0\},\cdot)$. Consideremos la aplicación $f(x) = x^2$.

Como $f(x\cdot y) = (x\cdot y)^2 = x^2\cdot y^2 = f(x)\cdot f(y)$, entonces f es un homomorfismo, pero en este caso f no es ni sobreyectiva ni inyectiva.

Ejemplo 2.8.8. Sea $G_1 = (GL_2(\mathbb{R}),\cdot)$, donde

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}): \quad ad-bc \neq 0 \right\}$$

y " $\cdot$ " es el producto de matrices habitual, y sea $G_2 = (\mathbb{R}-\{0\},\cdot)$, definimos la aplicación

$$\begin{array}{rl} f: & GL_2(\mathbb{R}) \longrightarrow \mathbb{R}-\{0\} \\ & \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow ad-bc. \end{array}$$

Por lo tanto es una aplicación que calcula el determinante de la matriz. Como sabemos que

$$f(A\cdot B) = \det(A\cdot B) = \det(A)\cdot\det(B) = f(A)\cdot f(B),$$

entonces f es un homomorfismo.

2.8.2. Propiedades de homomorfismos

Proposición 2.8.9. *Sea $(G_1, *)$ un grupo y $(G_2, \cdot)$ sólo un conjunto con una operación interna. Si la aplicación $f : G_1 \longrightarrow G_2$ cumple que*

$$f(g_1 * g_2) = f(g_1) \cdot f(g_2) \quad \forall g_1, g_2 \in G_1,$$

entonces $(f(G_1), \cdot)$ es un grupo, donde $f(G_1) = \{f(g) \in G_2 : \ g \in G_1\}$.

Demostración. Demostramos que cumple las propiedades de grupo:

1) Operación interna:

   Si $f(g_1), f(g_2) \in f(G_1)$, entonces $f(g_1) \cdot f(g_2) \in f(G_1) \subset G_2$ ya que $f(g_1) \cdot f(g_2) = f(g_1 * g_2)$ y $g_1 * g_2 \in G_1$ puesto que $(G_1, *)$ es un grupo.

2) Propiedad asociativa:

$$\begin{aligned}\big(f(g_1) \cdot f(g_2)\big) \cdot f(g_3) &= f(g_1 * g_2) \cdot f(g_3) = f\big((g_1 * g_2) * g_3\big) \\ &= f\big(g_1 * (g_2 * g_3)\big) = f(g_1) \cdot f(g_2 * g_3) \\ &= f(g_1) \cdot \big(f(g_2) \cdot f(g_3)\big).\end{aligned}$$

3) Elemento neutro:

   Tomamos $\widetilde{e} = f(e)$. Sea $g \in G_1$, tenemos que

$$f(g) \cdot \widetilde{e} = f(g) \cdot f(e) = f(g * e) = f(g)$$

   y

$$\widetilde{e} \cdot f(g) = f(e) \cdot f(g) = f(e * g) = f(g).$$

   Por tanto $\widetilde{e}$ es el elemento neutro de $(f(G_1), \cdot)$.

4) Elemento inverso:

   Sea $g \in G_1$. Si tomamos $h = f(g^{-1})$ donde $g^{-1} \in G_1$ es el inverso de g en $(G_1, *)$ tendremos que

$$f(g) \cdot h = f(g) \cdot f(g^{-1}) = f(g * g^{-1}) = f(e) = \widetilde{e}$$

   y

$$h \cdot f(g) = f(g^{-1}) \cdot f(g) = f(g^{-1} * g) = f(e) = \widetilde{e}$$

   Luego $f(g^{-1})$ es el inverso de $f(g)$ en $(f(G_1), \cdot)$.

Por lo tanto $(f(G_1), \cdot)$ es un grupo. □

Proposición 2.8.10. *Si f es un homomorfismo entre los grupos $(G_1, *)$ y $(G_2, \cdot)$, se tiene que:*

1) *$f(e_1) = e_2$, donde e_1 es el elemento neutro de G_1 y e_2 es el elemento neutro de G_2.*

2) *$f(g^{-1}) = (f(g))^{-1}$ para todo g de G_1.*

Demostración.

1) $f(g_1) \cdot f(e_1) = f(g_1 * e_1) = f(g_1) = f(g_1) \cdot e_2 \Longrightarrow f(e_1) = e_2$.

2) $\forall g \in G_1, \quad f(g) \cdot f(g^{-1}) = f(g * g^{-1}) = f(e_1) = e_2.$
$$\Longrightarrow f(g^{-1}) = \big(f(g)\big)^{-1}.$$

□

Ejemplo 2.8.11. Sean los grupos $G_1 = (\mathbb{R}, +)$ y $G_2 = (\mathbb{R} - \{0\}, \cdot)$ y sea $f(x) = e^x$.
Tenemos que $e_1 = 0 \Longrightarrow f(e_1) = f(0) = e^0 = 1 = e_2$.
Además

$$\begin{aligned} \forall x \in G_1,\ x^{-1} = -x \Longrightarrow f(x^{-1}) = f(-x) &= e^{-x} \\ &= \frac{1}{e^x} = \frac{1}{f(x)} = \big(f(x)\big)^{-1}. \end{aligned}$$

Proposición 2.8.12. *Sea f un homomorfismo entre los grupos $(G_1, *)$ y $(G_2, \cdot)$, se tiene:*

1) *Si H_1 es un subgrupo de G_1, entonces $f(H_1)$ es un subgrupo de G_2.*

2) *Si H_2 es un subgrupo de G_2, entonces $f^{-1}(H_2)$ es un subgrupo de G_1.*

Demostración.

1) Como $e_1 \in H_1$ implica que
$$f(e_1) = e_2 \in f(H_1)$$
se tiene que $f(H_1) \neq \emptyset$.
Sean $x, y \in f(H_1)$, entonces existen $a, b \in H_1$ tales que
$$x = f(a), \quad y = f(b).$$
Así que
$$x \cdot y^{-1} = f(a) \cdot \big(f(b)\big)^{-1} = f(a) \cdot f(b^{-1}) = f(a * b^{-1}) \in f(H_1).$$
ya que $a * b^{-1} \in H_1$.

2) Como $f(e_1) = e_2 \in H_2$ se tiene que $e_1 \in f^{-1}(H_2)$.
Sean $x, y \in f^{-1}(H_2) = \{a \in G_1 : f(a) \in H_2\}$ entonces

$$f(x), f(y) \in H_2$$

por lo tanto, $f(x) \cdot (f(y))^{-1} \in H_2$ ya que H_2 es un subgrupo.
Así que

$$f(x) \cdot (f(y))^{-1} = f(x) \cdot f(y^{-1}) = f(x * y^{-1})$$

Luego $x * y^{-1} \in f^{-1}(H_2)$.

□

Ejemplo 2.8.13. Sean $G_1 = (GL_2(\mathbb{R}), \cdot)$ con

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ ad - bc \neq 0 \right\},$$

$f(A) = ad - bc$ con $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y $G_2 = (\mathbb{R} - \{0\}, \cdot)$.

Tomemos el subconjunto

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ b \in \mathbb{R} \right\} \subset GL_2(R).$$

Dicho subconjunto con la operación producto de matrices es subgrupo de G_1, ya que dadas las matrices

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in H \ \text{ y } \ B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H,$$

tenemos que $B^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in H$ y además

$$AB^{-1} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in H.$$

Por otro lado, dada una matriz $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in H$ podemos construir el conjunto formado por todas las imágenes de matrices de H, y tendríamos $f(A) = 1 \cdot 1 - a \cdot 0 = 1 = e_2$, por lo tanto el conjunto $f(H) = \{e_2\}$ es subgrupo de G_2.

Proposición 2.8.14. *Sea f un homomorfismo entre los grupos $(G_1, *)$ y $(G_2, \cdot)$, tenemos que*

1) *Si H_2 es un subgrupo normal de G_2, entonces $f^{-1}(H_2)$ es un subgrupo normal de G_1.*

2) *Si H_1 es un subgrupo normal de G_1 y f es sobreyectiva, entonces $f(H_1)$ es un subgrupo normal de G_2.*

Demostración.

1) Por el apartado 2) de la Proposición 2.8.12, sabemos que

$$f^{-1}(H_2) = \{h \in G_1 : \ f(h) \in H_2\}$$

es un subgrupo, falta probar que es normal.

Sea $g \in G_1$ y sea $h \in f^{-1}(H_2)$. Tenemos

$$f(g * h * g^{-1}) = f(g) \cdot f(h) \cdot f(g^{-1}) = f(g) \cdot h \cdot \big(f(g)\big)^{-1} \in H_2,$$

ya que H_2 es un subgrupo normal en G_2.

Así que

$$g * h * g^{-1} \in f^{-1}(H_2).$$

Por lo tanto $f^{-1}(H_2)$ es normal.

2) Tenemos que demostrar que si $g_2 \in G_2$, $g_2 f(H_1) g_2^{-1} \subset f(H_1)$.

Puesto que f es sobreyectiva ($f(G_1) = G_2$), existe un $g_1 \in G_1$ tal que $f(g_1) = g_2$. De aquí se deduce que para todo $h_1 \in H_1$, se tiene que:

$$\begin{aligned} g_2 \cdot f(h_1) \cdot g_2^{-1} &= f(g_1) \cdot f(h_1) \cdot (f(g))^{-1} \\ &= f(g_1) \cdot f(h_1) \cdot f(g_1^{-1}) \\ &= f(g_1 * h_1 * g_1^{-1}). \end{aligned}$$

Como H_1 es normal de G_1, se cumple que $g_1 * h_1 * g_1^{-1} \in H_1$.

Así que $f(g_1 * h_1 * g_1^{-1}) \in f(H_1)$.

Por lo tanto el subgrupo $f(H_1)$ es subgrupo normal ya que

$$g_2 f(H_1) g_2^{-1} \in f(H_1) \ \ \forall g_2 \in G_2.$$

□

Proposición 2.8.15. *Sea f un isomorfismo entre los grupos $(G_1, *)$ y $(G_2, \cdot)$, se tiene que:*

1) *G_1 es abeliano si y sólo si G_2 es abeliano.*

2) *G_1 es cíclico si y sólo si G_2 es cíclico.*

Demostración.

1) $\boxed{\Rightarrow}$ Supongamos que G_1 es abeliano.

Sean $g_2, h_2 \in G_2$ como f es sobreyectiva (por ser isomorfismo) se cumple que existen $g_1, h_1 \in G_1$ tales que

$$f(g_1) = g_2,\ f(h_1) = h_2.$$

Así que

$$g_2 \cdot h_2 = f(g_1) \cdot f(h_1) = f(g_1 * h_1)$$

como G_1 es abeliano, tenemos que

$$f(g_1 * h_1) = f(h_1 * g_1) = f(h_1) \cdot f(g_1) = h_2 \cdot g_2$$

por tanto G_2 es abeliano.

$\boxed{\Leftarrow}$ Como f es un isomorfismo, entonces f^{-1} también lo será, por lo tanto, para todo $g_1, h_1 \in G_1$ podemos escribir

$$g_1 = f^{-1}(g_2), \quad h_1 = f^{-1}(h_2) \quad \text{con} \quad g_2, h_2 \in G_2.$$

Así que

$$\begin{aligned} g_1 * h_1 = f^{-1}(g_2) * f^{-1}(h_2) &= f^{-1}(g_2 \cdot h_2) \ \ (f^{-1} \ \text{ es un isomorfismo}) \\ &= f^{-1}(h_2 \cdot g_2) \ \ (G_2 \ \text{ es abeliano}) \\ &= f^{-1}(h_2) * f^{-1}(g_2) \\ &= h_1 * g_1 \end{aligned}$$

Por tanto G_1 es abeliano.

2) $\boxed{\Rightarrow}$ Supongamos que G_1 es cíclico, entonces existe $x \in G_1$ tal que $\langle x \rangle = G_1$. Sea $g_2 \in G_2$, como f es sobreyectiva (por ser isomorfismo), tenemos que $f^{-1}(g_2) \in G_1$.

Así que, existe $n \in \mathbb{Z}$ tal que

$$f^{-1}(g_2) = g_1 = x^n.$$

Luego

$$g_2 = f(x^n) = (f(x))^n.$$

Por tanto G_2 es cíclico.

$\boxed{\Leftarrow}$ Se demuestra igual aplicando el resultado a f^{-1} (ya que f es un isomorfismo).

□

Ejemplo 2.8.16. El grupo S_3 no puede ser isomorfo a $\mathbb{Z}_6$ ya que éste es abeliano mientras que el primero no lo es.

2.8.3. Núcleo de un homomorfismo

Definición 2.8.17. *Dado un homomorfismo f entre los grupos G_1 y G_2 ($f : G_1 \longrightarrow G_2$), definimos el* ***núcleo*** *de f como el conjunto*

$$\ker(f) = \{x \in G_1 : \ f(x) = e_2\},$$

donde e_2 es el elemento neutro de G_2.

Ejemplo 2.8.18. Sean $G_1 = (\mathbb{R}, +)$ y $G_2 = (\mathbb{R} - \{0\}, \cdot)$, con el homomorfismo $f(x) = e^x$, tenemos que

$$\ker(f) = \{x \in \mathbb{R} : \ f(x) = 1\} = \{x \in \mathbb{R} : \ e^x = 1\} = \{0\}.$$

Ejemplo 2.8.19. Sean $G_1 = (GL_2(\mathbb{R}), \cdot)$ con

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ ad - bc \neq 0 \right\}$$

y $G_2 = (\mathbb{R}^*, \cdot)$, con $f(A) = ad - bc$ siendo $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Tenemos que

$$\ker(f) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ ad - bc = 1 \right\}.$$

Por lo tanto el núcleo serán la matrices de orden 2 con determinante igual a 1.

Proposición 2.8.20. *Sea f un homomorfismo entre los grupos $(G_1, *)$ y $(G_2, \cdot)$, se tiene que:*

1) *El núcleo de f es un subgrupo normal de G_1.*
2) *f es un monomorfismo si y sólo si $\ker(f) = \{e_1\}$, donde e_1 es el elemento neutro de G_1.*

Demostración.

1) $\odot$ ▶ Como $f(e_1) = e_2$, tenemos que $e_1 \in \mathrm{Ker}(f)$, es decir

$$\mathrm{Ker}(f) \neq \emptyset.$$

▶ Sean $x, y \in \ker(f)$ entonces

$$f(x * y^{-1}) = f(x) \cdot f(y^{-1}) = e_2 \cdot \big(f(y)\big)^{-1} = \big(f(y)\big)^{-1} = e_2^{-1} = e_2.$$

Esto significa que $x * y^{-1} \in \ker(f)$, por lo tanto $\ker(f)$ es un subgrupo de G_1.

⊙ Probamos que Ker(f) es normal. Sea $g \in G_1$ y $x \in \ker(f)$, y comprobar que $g * x * g^{-1} \in \ker(f)$. Tenemos que

$$\begin{aligned} f(g * x * g^{-1}) &= f(g) \cdot f(x) \cdot f(g^{-1}) \\ &= f(g) \cdot e_2 \cdot \big(f(g)\big)^{-1} = f(g) \cdot \big(f(g)\big)^{-1} = e_2. \end{aligned}$$

Así que $g * x * g^{-1} \in \ker(f)$.

Por lo tanto $\ker(f)$ es un subgrupo normal.

2) $\boxed{\Rightarrow}$ Supongamos que f es inyectiva.

Si $x \in \ker(f)$ entonces $f(x) = e_2$. Además sabemos que $f(e_1) = e_2$.

Como f es inyectiva y $f(x) = f(e_1) = e_2$, entonces $x = e_1$.

Luego $\ker(f) = \{e_1\}$.

$\boxed{\Leftarrow}$ Supongamos que $\ker(f) = \{e_1\}$.

Sean $x, y \in G_1$ tales que $f(x) = f(y)$ entonces

$$f(x) \cdot \big(f(y)\big)^{-1} = e_2 \Longrightarrow f(x) \cdot f(y^{-1}) = e_2 \Longrightarrow f(x * y^{-1}) = e_2.$$

Como $\ker(f) = \{e_1\}$ se tiene que $x * y^{-1} = e_1$ luego $x = y$,por lo tanto f es inyectiva.

□

2.9. Descomposición canónica de un homomorfismo

2.9.1. Homomorfismo canónico

Lema 2.9.1. *Si H es un subgrupo normal de $(G, *)$, la aplicación*

$$\begin{array}{rccc} \pi: & G & \longrightarrow & G/H \\ & g & \longrightarrow & gH \end{array}$$

es un epimorfismo, es decir, es un homomorfismo sobreyectivo.

Demostración. Sean $a, b \in G$, tenemos que

$$\pi(a * b) = (a * b)H = (aH) \cdot (bH) = \pi(a) \cdot \pi(b).$$

Además es una aplicación sobreyectiva por construcción, ya que el codominio es el conjunto de elementos que tienen contraimagen. □

Definición 2.9.2 (**Proyección canónica).** *Si H es un subgrupo normal de G, la aplicación definida por*

$$\begin{array}{rccc} \pi: & G & \longrightarrow & G/H \\ & g & \longrightarrow & gH \end{array}$$

se llama, ***homomorfismo canónico, o proyección canónica****, de núcleo H.*

2.9.2. Descomposición canónica

Definición 2.9.3. *Sea f un homomorfismo entre los grupos G y G'.*

El homomorfismo canónico de núcleo $\mathrm{Ker}(f)$ *definido de la siguiente manera*

$$\begin{array}{rccc} \pi_f: & G & \longrightarrow & G/\mathrm{Ker}(f) \\ & g & \longrightarrow & \pi_f(g) = g\mathrm{Ker}(f) \end{array}$$

se denomina ***descomposición canónica del homomorfismo****.*

Proposición 2.9.4. *Sea f un homomorfismo entre los grupos $(G_1, *)$ y $(G_2, \odot)$, entonces*

$$\begin{array}{rccc} \rho: & G_1/\mathrm{Ker}(f) & \longrightarrow & G_2 \\ & g\mathrm{Ker}(f) & \longrightarrow & f(g) \end{array}$$

es un homomorfismo inyectivo.

Además, f se descompone en dos homomorfismos π y ρ, es decir, $f = \rho \circ \pi$

$$G_1 \xrightarrow{\pi} G_1/\mathrm{Ker}(f) \xrightarrow{\rho} G_2 \qquad (f: G_1 \longrightarrow G_2)$$

donde

$$\begin{array}{rccc} \pi: & G_1 & \longrightarrow & G_1/\mathrm{Ker}(f) \\ & g & \longrightarrow & g\mathrm{Ker}(f) \end{array}$$

es un homomorfismo sobreyectivo.

Demostración.

■ Hay que probar que la correspondencia ρ es un homomorfismo inyectivo.

▶ Probamos que ρ es un aplicación, es decir, se cumple que

$$\text{Si } \; g\mathrm{Ker}(f) = g'\mathrm{Ker}(f) \text{ entonces } \; \rho(g) = \rho(g').$$

Esto es debido a que si $g\mathrm{Ker}(f) = g'\mathrm{Ker}(f)$, entonces $g' = g * h$ con $h \in \ker(f)$. Como f es un aplicación, tenemos que

$$f(g') = f(g * h)$$

así que

$$f(g') = f(g) \odot f(h) = f(g) \odot e_2 = f(g),$$

es decir,

$$\rho(g) = f(g) = \rho(g') = f(g').$$

Por lo tanto

$$\begin{array}{rccc} \rho: & G_1/\mathrm{Ker}(f) & \longrightarrow & G_2 \\ & g\mathrm{Ker}(f) & \longrightarrow & f(g) \end{array}$$

es una aplicación.

- ▶ La aplicación ρ es un homomorfismo ya que

$$\begin{aligned} \rho\big(g\mathrm{Ker}(f) \cdot g'\mathrm{Ker}(f)\big) &= \rho\big((g * g')\mathrm{Ker}(f)\big) \\ &= f(g * g') = f(g) \odot f(g') \\ &= \rho\big(g\mathrm{Ker}(f)\big) \cdot \rho\big(g'\mathrm{Ker}(f)\big). \end{aligned}$$

- ▶ La aplicación ρ es inyectivo ya que si tomamos un elemento $g\mathrm{Ker}(f)$ del núcleo de ρ, tendremos que $\rho\big(g\mathrm{Ker}(f)\big) = e_2$, entonces

$$f(g) = e_2$$

así que

$$g \in \mathrm{Ker}(f)$$

luego

$$g\mathrm{Ker}(f) = \mathrm{Ker}(f).$$

por lo tanto vemos que el único elemento que pertenece al núcleo de ρ es el elemento neutro del grupo $G_1/\mathrm{Ker}(f)$, esto es $\mathrm{Ker}(f)$, por lo tanto ρ es inyectiva $\Big(\ker(\rho) = \big\{\mathrm{Ker}(f)\big\}\Big)$.

- ■ Ya hemos visto que π es un homomorfismo sobreyectivo.
- ■ Por la definición de π y ρ se tiene que f se descompone en dos homomorfismos π y ρ, es decir, $f = \rho \circ \pi$.

□

Observación 2.9.5.

1) *Si f es sobreyectiva, entonces ρ también lo es, ya que si $g_2 \in G_2$, podemos tomar $g_1 \in G_1$ tal que $f(g_1) = g_2$ entonces*

$$\rho\big(g_1\mathrm{Ker}(f)\big) = f(g_1) = g_2.$$

Por tanto, para todo $g_2 \in G_2$, existe $g_1\mathrm{Ker}(f) \in G_1/\mathrm{Ker}(f)$ tal que

$$\rho\big(g_1\mathrm{Ker}(f)\big) = g_2.$$

2) *Si* $f : G_1 \longrightarrow G_2$ *un homomorfismo sobreyectivo entre los grupos* G_1 *y* G_2 *con núcleo* $\mathrm{Ker}(f)$*, entonces* $G_1/\mathrm{Ker}(f)$ *es isomorfo a* G_2*.*

Ejemplo 2.9.6. Sea $\begin{array}{rccl} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}-\{0\},\cdot) \\ & x & \longrightarrow & e^x \end{array}$, tenemos que

$$\mathrm{Ker}(f) = \{x : \ f(x) = 1\} = \{0\}$$

por tanto

$$(\mathbb{R},+)/\mathrm{Ker}(f) = \{x\mathrm{Ker}(f) : \ x \in \mathbb{R}\} = \{\{x\} : \ x \in \mathbb{R}\} = \mathbb{R}$$

$$\begin{array}{rccl} \pi: & \mathbb{R} & \longrightarrow & (\mathbb{R},+)/\mathrm{Ker}(f) \\ & x & \longrightarrow & \{x\} \end{array} \qquad \begin{array}{rccl} \rho: & (\mathbb{R},+)/\mathrm{Ker}(f) & \longrightarrow & (\mathbb{R}-\{0\},\cdot) \\ & \{x\} & \longrightarrow & e^x \end{array}$$

Ejemplo 2.9.7. Sean $G_1 = (GL_2(\mathbb{R}),\cdot)$, $G_2 = (\mathbb{R}-\{0\},\cdot)$ con

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ |A| = ad - bc \neq 0 \right\}$$

y $f(A) = ad - bc = |A|$ donde $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

En este caso

$$\ker(f) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ |A| = ad - bc = 1 \right\},$$

por lo tanto

$$G_1/\mathrm{Ker}(f) = \big\{M\mathrm{Ker}(f) : \ M \in GL_2(\mathbb{R})\big\}.$$

Como $|B| = 1$ para todo $B \in \ker(f)$, tenemos que

$$M\mathrm{Ker}(f) = \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ |A| = |M|\},$$

por lo tanto

$$G_1/\mathrm{Ker}(f) = \big\{\{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ |A| = m\}, \forall m \in \mathbb{R}\big\},$$

o sea, el conjunto cociente está construído con conjuntos de matrices que tienen el mismo determinante.

$$\begin{array}{rccl} \pi: & G_1 & \longrightarrow & G_1/\mathrm{Ker}(f) \\ & M & \longrightarrow & \big\{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) : \ |A| = |M|\big\} = M\mathrm{Ker}(f) \end{array}$$

$$\begin{array}{rccl} \rho: & G_1/\mathrm{Ker}(f) & \longrightarrow & (\mathbb{R}-\{0\},\cdot) \\ & M\mathrm{Ker}(f) & \longrightarrow & |M| \end{array}$$

$$G_1 \overset{\text{sobreyectia}}{\underset{\pi}{\longrightarrow}} G_1/\mathrm{Ker}(f) \overset{\text{biyectiva}}{\underset{\rho}{\longrightarrow}} \mathbb{R}-\{0\}$$

$$M \overset{\text{sobreyecta}}{\underset{f}{\longrightarrow}} \text{matrices con determinante} |M| \to |M|$$

Ejemplo 2.9.8. Tomemos $G_1 = (\mathbb{R}, +)$ y $G_2 = (GL_2(\mathbb{R}), \cdot)$ con

$$f(x) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix},$$

tenemos que

$$\ker(f) = \{2\pi k : \ k \in \mathbb{Z}\},$$

por lo tanto,

$$G_1/\mathrm{Ker}(f) = \big\{\{x + 2\pi k : \ k \in \mathbb{Z}\}, \ 0 \leq x < 2\pi\big\}$$

$$\begin{array}{rccl} \pi : & G_1 & \longrightarrow & G_1/\mathrm{Ker}(f) \\ & y & \longrightarrow & y\mathrm{Ker}(f) = \{y + 2\pi k : \ k \in \mathbb{Z}\} \end{array}$$

Por otra parte tenemos que

$$y = x + 2\pi n \quad \text{con} \quad n \in \mathbb{Z}, \ 0 \leq x < 2\pi.$$

Así que

$$\begin{aligned} \pi(y) = \{y + 2\pi k : \ k \in \mathbb{Z}\} &= \{x + 2\pi n + 2\pi k : \ n, k \in \mathbb{Z}, \ 0 \leq x < 2\pi\} \\ &= \{x + 2\pi(n + k) : \ n, k \in \mathbb{Z}, \ 0 \leq x < 2\pi\} \\ &= \{x + 2\pi l : \ l \in \mathbb{Z}, \ 0 \leq x < 2\pi\} \end{aligned}$$

es decir,

$$\pi(y) = y\mathrm{Ker}(f) = x\mathrm{Ker}(f), \ x \in [0, 2\pi].$$

$$\begin{array}{rccl} \rho : & G_1/\mathrm{Ker}(f) & \longrightarrow & (GL_2(\mathbb{R}), \cdot) \\ & x\mathrm{Ker}(f) & \longrightarrow & \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}. \end{array}$$

Capítulo 3

Anillos y cuerpos

3.1. Anillos

Definición 3.1.1. *Un conjunto A dotado de dos operaciones binarias cerradas que escribiremos $+$ (suma) y $\cdot$ (producto) se llama* ***anillo*** *si se cumplen las siguientes propiedades:*

1) $(A, +)$ *es un grupo abeliano.*

2) *El producto $\cdot$ es asociativo.*

3) *Se cumple la propiedad distributiva*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a,$$

para todo $a, b, c \in A$.

Definiciones 3.1.2.

1) *El inverso respecto a la suma se llama* ***opuesto****. Por notación, al opuesto de un elemento dado $a \in A$ lo representaremos por $-a$.*

2) *El elemento neutro de la suma lo denotaremos por 0 y lo denominaremos* ***elemento cero****.*

3) *Si el producto es conmutativo, se dice que $(A, +, \cdot)$ es un* ***anillo conmutativo****.*

4) *Si existe un elemento, que denotaremos 1, tal que*

$$a \cdot 1 = 1 \cdot a = a, \quad \forall\, a \in A$$

diremos que $(A, +, \cdot)$ es un ***anillo con unidad****.*

En este caso, el elemento 1 recibe el nombre de ***elemento unidad****.*

Proposición 3.1.3. *El elemento unidad, si existe, es único.*

Demostración. Si $a, b, c \in A$ y verifican que $a \cdot b = a$ y $a \cdot c = a$ tendremos que $a \cdot b = a \cdot c \quad \forall a \in A$, por lo tanto $b = c = 1$. □

Ejemplos 3.1.4.

1) $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.

2) $(2\mathbb{Z}, +, \cdot)$ (conjunto de todos los enteros pares) es un anillo conmutativo sin unidad.

3) Las matrices de orden n con coeficientes reales $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ es un anillo no conmutativo con unidad.

3.2. Elementos Invertibles y Anillos de División

Definición 3.2.1. *Sea $(A, +, \cdot)$ un anillo con unidad 1 y $1 \neq 0$. Un elemento a de A se dice que es **invertible** si existe un elemento $b \in A$ tal que*

$$a \cdot b = b \cdot a = 1.$$

Observación 3.2.2. *Si a es un elemento invertible de un anillo, entonces b también lo es.*

Proposición 3.2.3. *Si existe el inverso de un elemento a lo denotaremos por a^{-1} y es único.*

Demostración. Si $a, b, c \in A$ y $a \cdot b = a \cdot c = b \cdot a = c \cdot a = 1$, tenemos que

$$c = c \cdot (\overbrace{a \cdot b}^{=1})$$

por asociatividad del producto, ya que es un anillo, se tiene que

$$c = (c \cdot a) \cdot b = 1 \cdot b = b \Rightarrow c = b.$$

□

Notación 3. *Al conjunto de los elementos invertibles de A lo denotaremos por $U(A)$.*

Ejemplo 3.2.4.

1) $U(\mathbb{Z}) = \{-1, 1\}$.

2) $U(\mathbb{Z}_{12}) = \{[1], [5], [7], [11]\}$.

3) $U(\mathbb{Z}_5) = \{[1], [2], [3], [4]\}$.

Definición 3.2.5. *Los elementos invertibles de un anillo* $(A, +, \cdot)$ *se llaman* ***unidades*** *de* A.

Proposición 3.2.6. *Sea* $(A, +, \cdot)$ *un anillo con unidad. Si* $U(A)$ *es el conjunto de los elementos invertibles de* A*, entonces* $(U(A), \cdot)$ *es un grupo.*

Demostración.

1) La asociatividad se cumple siempre ya que son elementos de un anillo.

2) Los elementos de $U(A)$ tienen inverso.

3) $1 \in U(A)$ ya que $1 \cdot 1 = 1$ (el 1 es su propio inverso), por lo tanto tiene elemento neutro.

4) Si $a, b \in U(A) \Rightarrow a \cdot b \in U(A)$, ya que

$$(a \cdot b) \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = 1,$$

por lo tanto $(a \cdot b)$ tiene inverso y al tener inverso pertenece a $U(A)$, por lo que la operación es cerrada.

□

Ejemplo 3.2.7. Dadas las matrices de orden n con la suma y el producto de matrices, $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, son un anillo con unidad. La unidades de $\mathcal{M}_n(\mathbb{R})$ serán aquellas matrices que tienen determinante distinto de cero $GL_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \text{ tal que } |A| \neq 0\}$, $(GL_n(\mathbb{R}), \cdot)$ es un grupo.

Observación 3.2.8. *Si* $(A, +, \cdot)$ *es un anillo unitario* (*anillo con unidad* 1)*, se tiene que*

$$0 \neq 1,$$

ya que $\forall a \in A, a \cdot 0 = 0$ *y* $a \cdot 1 = a$

Definición 3.2.9. *Un anillo unitario* $(A, +, \cdot)$*, con* $1 \neq 0$*, se dice que es un* ***anillo de división*** *si*

$$U(A) = A^* = A - \{0\}.$$

Observación 3.2.10. *Si* $(A, +, \cdot)$ *es un anillo unitario, se tiene que* $U(A) \subset A^*$*, donde* A^* *denota el conjunto* A *excluido el elemento neutro de la suma.*

Proposición 3.2.11. *Sea* $(A, +, \cdot)$ *un anillo, se tiene que:*

1) $\forall a \in A \;\; a \cdot 0 = 0 \cdot a = 0$.

2) *Si* $(-a)$ *es el elemento opuesto de* a *para la suma se tiene que:*

- $(-a) \cdot b = -(a \cdot b)$,
- $a \cdot (-b) = -(a \cdot b)$,
- $(-a) \cdot (-b) = a \cdot b$,

para todo $a, b \in A$

Demostración. 1) Sea $a \in A$, puesto que $0 + 0 = 0$, entonces

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0,$$

por tanto $a \cdot 0 = 0$ ya que el elemento neutro de un grupo es único.

2) como

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

se tiene que $(-a) \cdot b$ es el opuesto de $(a \cdot b)$.

De manera similar se demuestra la segunda igualdad.

Para demostrar la última usamos la primera y la propiedad distributiva para obtener

$$\begin{aligned}(-a) \cdot (-b) - (a \cdot b) &= (-a) \cdot (-b) + (-a) \cdot b \\ &= (-a) \cdot \big((-b) + b\big) = (-a) \cdot 0 = 0.\end{aligned}$$

□

3.3. Cuerpos

Definición 3.3.1. *Un conjunto* A *dotado de dos operaciones binarias internas* $+, \cdot$ *se dice que es un* ***cuerpo*** *si*

1) $(A, +, \cdot)$ *es un anillo conmutativo con unidad,*

2) *todo elemento* $x \in A$*, con* $x \neq 0$*, tiene inverso* x^{-1} *respecto al producto.*

Observación 3.3.2.

1) *Si* $(A, +, \cdot)$ *es un anillo conmutativo y* $(A^*, \cdot)$ *es un grupo, entonces* $(A, +, \cdot)$ *es un cuerpo.*

2) *Si* $(A, +, \cdot)$ *es un cuerpo, entonces* $(A, +, \cdot)$ *es un anillo conmutativo con unidad y además* $U(A) = A^*$.

Ejemplo 3.3.3. $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z}_p,+,\cdot)$ con p primo, son cuerpos.

Nota 3.3.4. *Un cuerpo se suele decir que es un* ***anillo de división conmutativo****.*

Observación 3.3.5. *Existen anillos de división que no son conmutativos (no son cuerpos), véase el ejemplo siguiente.*

Ejemplo 3.3.6. Sea

$$H(\mathbb{R}) = \{a + bi + cj + dk : \ a, b, c, d \in \mathbb{R}\}$$

donde

$$\begin{aligned} &i^2 = j^2 = k^2 = -1, \\ &i1 = 1i = i, \ j1 = 1j = j, \ k1 = 1k = k, \\ &ij = k, \ jk = i, \ ki = j, \end{aligned}$$

estas condiciones implican que

$$ji = -k, \ kj = -i, \ ik = -j.$$

La suma se define componente a componente:

$$(a + bi + cj + dk) + (r + si + tj + uk) = (a + r) + (b + s)i + (c + t)j + (d + u)k$$

y el producto se realiza multiplicando los términos y utilizando las relaciones anteriores:

$$\begin{aligned} (a + bi + cj + dk) \cdot (r + si + tj + uk) \\ &= ar - bs - ct - du + (as + br + cu - dt)i \\ &+ (at + cr + ds - bu)j + (au + dr + bt - cs)k \end{aligned}$$

Por tanto $(H(\mathbb{R}),+,\cdot)$ es un anillo. Además todo elemento es invertible, por lo que es un anillo de división, pero no un cuerpo, al no ser conmutativo.

3.4. Divisores de cero

Definición 3.4.1. *Si $(A,+,\cdot)$ es un anillo, un elemento $a \in A$ con $a \neq 0$, se dice que es un* ***divisor de cero*** *si existe un elemento $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$ ó $b \cdot a = 0$.*

Ejemplo 3.4.2. En $\mathbb{Z}_{12}$, [3] y [4] son divisores de cero ya que

$$[3] \cdot [4] = [12] = [0];$$

también lo son $[2], [6], [8], [9]$ y $[10]$.

Ejemplo 3.4.3. En el conjunto

$$\mathcal{C}(\mathbb{R}, \mathbb{R}) = \big\{ f : \mathbb{R} \longrightarrow \mathbb{R} : \ f \text{ continua} \big\},$$

definimos una suma y un producto mediante

$$\begin{cases} (f+g)(x) = f(x) + g(x) \\ (f \cdot g)(x) = f(x) \cdot g(x) \end{cases}$$

con $f, g \in \mathcal{C}(\mathbb{R}, \mathbb{R}), x \in \mathbb{R}$.

$\big(\mathcal{C}(\mathbb{R}, \mathbb{R}), +, \cdot\big)$ es un anillo conmutativo (ya que $f \cdot g = g \cdot f$), unitario (el elemento unidad es la función $i(x) = 1$ para todo $x \in \mathbb{R}$).

Tomemos $f(x) = x - |x|$ y $g(x) = x + |x|$, se tiene que

$$(f \cdot g)(x) = 0, \quad \forall x \in \mathbb{R},$$

así que $f(x)$ y $g(x)$ son divisores de cero.

Observación 3.4.4. *Un cuerpo C no tiene divisores de cero, ya que si $a \neq 0$ y $a \cdot b = 0$, multiplicando por a^{-1}, el inverso de a, se tiene que*

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Nota 3.4.5. *Aunque hay anillos que sin ser cuerpos tampoco tienen divisores de cero.*

Por ejemplo, en el anillo $(\mathbb{Z}, +, \cdot)$ no hay divisores de cero, aunque si $a = 0$ se tiene que $0 \cdot b = 0$ para todo b, 0 no se considera un divisor de cero.

Proposición 3.4.6. *En un anillo $(A, +, \cdot)$, sea a un elemento de A que no es un divisor de cero. Entonces:*

1) *Si $a \cdot b = a \cdot c$, con $b, c \in A$, entonces $b = c$.*

2) *Si $b \cdot a = c \cdot a$, con $b, c \in A$, entonces $b = c$.*

Demostración.

1) Supongamos que $a \cdot b = a \cdot c$; esto es equivalente a $a \cdot (b - c) = 0$. Como a no es un divisor de cero, $b - c$ tiene que ser 0, de donde se deduce el resultado deseado.

2) Análogo.

□

3.5. Dominio de integridad

Definición 3.5.1. *Un anillo A sin divisores de cero se denomina* ***dominio de integridad****.*

Observación 3.5.2. *En un dominio de integridad, el producto de dos elementos no nulos, es distinto de* 0*.*

Ejemplos 3.5.3.

1) $(\mathbb{Z}, +, \cdot)$ es un dominio de integridad.

2) Todos los cuerpos son dominios de integridad.

3) $(\mathbb{Z}_p, +, \cdot)$ es dominio de integridad si p es primo.

4) Sea $\mathcal{M}_2(\mathbb{R})$ el conjunto de todas las matrices de orden 2 con coeficientes reales. Con la suma y el producto este conjunto es un anillo. Pero no es dominio de integridad, ya que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

3.6. Subanillos

Definición 3.6.1. *Sea subconjunto $S \subset A$ con $(A, +, \cdot)$ un anillo, se dice que $(S, +, \cdot)$ es un* ***subanillo*** *de $(A, +, \cdot)$, si*

1) *$(S, +)$ es un subgrupo de $(A, +)$,*

2) *el producto $\cdot$ restringido a S es cerrado;*

de forma equivalente, la suma y el producto son operaciones cerradas en S, y $(S, +, \cdot)$ es un anillo.

Ejemplo 3.6.2. $(\mathbb{Z}, +, \cdot)$ es subanillo de $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ es subanillo de $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ es subanillo de $(\mathbb{C}, +, \cdot)$.

Observación 3.6.3.

1) *Los subanillos de un anillo unitario no tienen por qué ser unitarios e incluso si son unitarios, el elemento neutro del subanillo puede ser distinto del elemento neutro del anillo.*

2) *Los divisores de cero de un subanillo lo son también del anillo, pero puede suceder que un anillo tenga divisores de cero y el subanillo no.*

Ejemplo 3.6.4. Sea $\mathbb{R} \times \mathbb{R}$ con las operaciones:

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b) \cdot (c,d) = (a \cdot c, b \cdot d), \ \ \forall (a,b),(c,d) \in \mathbb{R} \times \mathbb{R}$$

y sea $H = \{(h,0) \text{ tal que } h \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}$

1) $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ es un anillo unitario.

2) $(H, +, \cdot)$ es un subanillo unitario

3) Los elementos $(n,0) \in \mathbb{R} \times \mathbb{R}$ son divisores de cero en $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ pero no en $(H, +, \cdot)$.

Demostración.

1) $(\mathbb{R} \times \mathbb{R}, +)$ es un grupo conmutativo, con elemento cero $(0,0)$.
$((\mathbb{R} \times \mathbb{R})^*, \cdot)$ cumple que:

   1,1) Es una operación interna pues $(a \cdot c, b \cdot d) \in \mathbb{R} \times \mathbb{R}$

   1,2) Es asociativa ya que $[(a,b) \cdot (c,d)] \cdot (e,f) = (a \cdot c, b \cdot d) \cdot (e,f) = (a \cdot c \cdot e, b \cdot d \cdot f) = (a,b) \cdot (c \cdot e, d \cdot f) = (a,b) \cdot [(c,d) \cdot (e,f)]$

   1,3) Tiene elemento neutro, que es $(1,1)$, ya que $(a,b) \cdot (1,1) = (a,b)$

   1,4) Tiene elemento unidad (invertible), ya que $\forall (a,b) \in (\mathbb{R} \times \mathbb{R})^*$ se cumple que $(a,b) \cdot \left(\frac{1}{a}, \frac{1}{b}\right) = (1,1)$

   Por lo tanto, $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ es un anillo con unidad con unidad $(1,1)$. Además es conmutativo respecto al producto.

2) $(H, +, \cdot)$ es un subanillo unitario, ya que:

   2,1) Sean $(a,0),(b,0) \in H$, entonces $(a,0) - (b,0) = (a-b,0) \in H$, por lo que $(H, +)$ es un subgrupo de $(\mathbb{R} \times \mathbb{R}, +)$

   2,2) Sean $(a,0),(b,0) \in H$, entonces $(a,0) \cdot (b,0) = (a \cdot b, 0) \in H$, por lo que $\cdot$ es una operación cerrada en H

   Por lo tanto $(H, +, \cdot)$ es subanillo. Además tiene unidad, ya que $(1,0) \in H$ cumple que

   $$(a,0) \cdot (1,0) = (a,0), \ \forall (a,0) \in H,$$

   por lo tanto $(1,0)$ es el elemento neutro del producto en H, pero no del producto en $\mathbb{R} \times \mathbb{R}$.

   Esto significa que $(H, +, \cdot)$ es subanillo unitario.

3) Los elementos de la forma $(a, 0)$ con $a \neq 0$ son divisores de cero en $\mathbb{R} \times \mathbb{R}$, ya que $(a, 0) \cdot (0, b) = (0, 0)$ aunque $a, b \neq 0$.

   Sin embargo, en H un elemento de la forma $(a, 0)$ con $a \neq 0$ no es divisor de cero, ya que si $(a, 0) \cdot (b, 0) = (0, 0)$ y $a \neq 0$, entonces $b = 0$

□

3.7. Subcuerpos

Definición 3.7.1. *Sea $S \subset C$ con $(C, +, \cdot)$ un cuerpo, se dice que $(S, +, \cdot)$ es un **subcuerpo** de $(C, +, \cdot)$ si*

1) *$(S, +)$ es un subgrupo de $(C, +)$,*

2) *$(S^*, \cdot)$ es un subgrupo de $(C^*, \cdot)$.*

De manera equivalente, la suma y el producto son operaciones cerradas en S, y $(S, +, \cdot)$ es un cuerpo.

Observación 3.7.2. *La terna $(S, +, \cdot)$ es subcuerpo de $(C, +, \cdot)$ si*

1) *$S \subset C$ con $S \neq \emptyset$,*

2) *$x - y \in S,\ \forall x, y \in S$,*

3) *$x \cdot y^{-1} \in S,\ \forall x, y \in S^*$.*

Ejemplos 3.7.3. *$(\mathbb{Q}, +, \cdot)$ es subcuerpo de $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ es subcuerpo de $(\mathbb{C}, +, \cdot)$*

3.8. Ideales

Definición 3.8.1. *Un subanillo I de un anillo A se dice que es un **ideal** de A si para todo $i \in I$ y para todo $a \in A$ se cumple que $i \cdot a \in I$ y $a \cdot i \in I$.*

Observación 3.8.2. *Para probar que un subconjunto I de A es un ideal de un anillo $(A, +, \cdot)$ baste con demostrar que:*

1) *Para todo $i, j \in I$ se cumple que $i - j \in I$.*

2) *Para todo $i \in I$ y para todo $a \in A$ se cumple que $i \cdot a \in I$ y $a \cdot i \in I$.*

Ejemplo 3.8.3. El subanillo trivial $\{0\}$ de cualquier anillo A es ideal, ya que

$$a \cdot 0 = 0 \cdot a = 0, \quad \forall a \in A.$$

Ejemplo 3.8.4. Otro subanillo trivial es el propio A y también es ideal de si mismo.

Ejemplo 3.8.5. Sea

$$\mathcal{C}[0,1] = \{f : [0,1] \longrightarrow \mathbb{R} \text{ tal que } f \text{ es continua}\}$$

con $(f+g)(x) = f(x) + g(x), (f \cdot g)(x) = f(x) \cdot g(x)$.

Dado $r \in [0,1]$, el subconjunto M_r de $\mathcal{C}[0,1]$ definido por

$$M_r = \{f \in \mathcal{C}[0,1] \text{ tal que } f(r) = 0\}$$

es un ideal de $(\mathcal{C}[0,1], +, \cdot)$.

Ejemplo 3.8.6. El conjunto $m\mathbb{Z}$ con $m \in \mathbb{N}$ definido como

$$m\mathbb{Z} = \{m\,k \text{ tal que } k \in \mathbb{Z}\}$$

es un ideal de $(\mathbb{Z}, +, \cdot)$ ya que se cumple que:

1) $\forall i = m\,k, j = m\,k' \in m\mathbb{Z},\ i - j = m\,(k - k') \in m\mathbb{Z}$ ya que $k - k' \in \mathbb{Z}$.

2) $\forall i = m\,k \in m\mathbb{Z}, \forall a \in \mathbb{Z},\ i\,a = m\,(k\,a) \in m\mathbb{Z}$ ya que $k\,a \in \mathbb{Z}$.

Proposición 3.8.7. *Si A es un anillo con unidad 1 e I es un ideal de A tal que $1 \in I$, entonces I coincide con A.*

Demostración. $\forall a \in A, a \cdot 1 = a \in I \Longrightarrow A = I$. □

Proposición 3.8.8. *Si A es un anillo de división, los únicos ideales de A son $\{0\}$ y el propio A (los ideales impropios).*

Demostración. Sea I un ideal de A con $I \neq \{0\}$ y sea $i \in I$ con $i \neq 0$, tomamos $a = i^{-1} \in A$, por lo tanto $i \cdot a = i \cdot i^{-1} \in I$ ya que I es ideal, además $i \cdot i^{-1} = 1 \in I \Longrightarrow I = A$ por la propiedad anterior. □

Proposición 3.8.9. *Un cuerpo $(C, +, \cdot)$ no tiene ideales propios.*

Demostración. Sea I ideal de C con $I \neq \{0\}$, si $a \neq 0 \in I$ entonces $x \cdot a \in I$ para todo $x \in C$.

Tomemos $x = a^{-1}$ (sabemos que a^{-1} existe ya que C es un cuerpo), entonces $x \cdot a = a^{-1} \cdot a = 1 \in I$, así que $I = C$. □

3.9. Anillo de clases de restos módulo I

El papel de los ideales en un anillo es similar al de los subgrupos normales en la teoría de grupos.

Proposición 3.9.1. *Si I es un ideal de un anillo A, la relación*

$$x\mathcal{R}y \Longleftrightarrow x - y \in I \text{ para } x, y \in A$$

es una relación de equivalencia.

Demostración.

1) Propiedad reflexiva: $x\mathcal{R}x$, ya que $x - x = 0 \in I$

2) Propiedad simétrica: $x\mathcal{R}y \Rightarrow y\mathcal{R}x$, ya que

$$x - y \in I \Longrightarrow -(x - y) = y - x \in I$$

porque es un subgrupo aditivo de A y, por tanto, si un elemento pertenece a I, su opuesto también pertenece a I.

3) Propiedad transitiva: $x\mathcal{R}y, y\mathcal{R}z \Longrightarrow x\mathcal{R}z$, ya que

$$x - y \in I, y - z \in I \Rightarrow x - y + y - z = x - z \in I$$

porque I es un subgrupo aditivo y la suma de dos elementos del subgrupo es otro elemento del subgrupo.

□

Nota 3.9.2. *El subgrupo $(I, +)$ es normal de A. Por lo tanto podemos definir el grupo cociente A/I respecto a la suma de clases*

▶

$$[r + I] + [s + I] = [(r + s) + I]$$

donde la clase de equivalencia de $x \in A$ será

$$[x + I] = \{x + a \text{ tal que } a \in I\}.$$

Expresaremos la relación $[x + I] = [y + I]$ como $x \equiv y \mod I$.

▶ *En analogía con la suma de clases podemos escribir el producto de clases como*

$$[r + I] \cdot [s + I] = [(r \cdot s) + I]$$

siempre y cuando este bien definida, es decir, sea independiente del representante.

Proposición 3.9.3. *Sea I un ideal de un anillo A; la suma y el producto de clases en el cociente A/I están bien definidas, y con estas, A/I posee estructura de anillo. Dicho anillo recibe el nombre de* ***anillo de clases de restos módulo*** *I.*

Demostración.

- $(A/I, +)$ es un grupo con respecto a la suma de clases definida anteriormente dado que $(I, +)$ es un subgrupo normal de $(A, +)$ y, por tanto, como quedó demostrado en el tema de Grupos (tema 2) podemos definir el conjunto cociente A/I, que con la suma de clases tiene estructura de grupo.

- Vamos a ver que en el conjunto cociente A/I el producto de clases definido anteriormente, $[x + I] \cdot [y + I] = [(x \cdot y) + I],\ \forall\, x, y \in A$, es independiente de los representantes elegidos, y por tanto está bien definido, ya que si

$$\left.\begin{array}{l}[x + I] = [x' + I] \\ [y + I] = [y' + I]\end{array}\right\} \Rightarrow [x + I] \cdot [y + I] = [(x \cdot y) + I] = [(x' \cdot y') + I],$$

  puesto que

$$x \cdot y - x' \cdot y' = x \cdot y - x \cdot y' + x \cdot y' - x' \cdot y' = x \cdot (y - y') + (x - x') \cdot y'$$

  y como $y - y' \in I$ y $x - x' \in I$ ya que $[y + I] = [y' + I]$ y $[x + I] = [x' + I]$ tendremos que

$$x \cdot y - x' \cdot y' = x \cdot y'' + x'' \cdot y',$$

  como $y'' \in I \Rightarrow x \cdot y'' \in I$ y como $x'' \in I \Rightarrow x'' \cdot y' \in I$ por definición de ideal, por tanto $x \cdot y'' + x'' \cdot y' = a + b$ con $a, b \in I$. Como $(I, +)$ es un grupo aditivo $a + b \in I$, así que $x \cdot y - x' \cdot y' \in I$ y por tanto $x \cdot y$ y $x' \cdot y'$ definen la misma clase de equivalencia.

- Como las operaciones suma y producto de clases están bien definidas es fácil demostrar que los elementos de A/I, esto es, las clases $[x + I]$ tal que $x \in A$, forman estructura de anillo puesto que A tiene estructura de anillo.

□

Observación 3.9.4. *Supongamos que I es un ideal de un anillo A, y que $I \neq A$.*

Es fácil comprobar que si A es conmutativo, también lo es A/I, y que si 1 es el elemento unidad de A, entonces $[1 + I]$ es el elemento unidad de A/I.

Ejemplo 3.9.5. En el anillo $(\mathbb{Z}, +, \cdot)$ podemos definir una relación de equivalencia dados $a, b \in \mathbb{Z}$, de modo que

$$a \mathcal{R} b \Longleftrightarrow a - b = k \cdot m$$

para algún $k \in \mathbb{Z}$ con $m \in \mathbb{N}$.

Hemos visto que $m\mathbb{Z}$ será un ideal de $(\mathbb{Z}, +, \cdot)$. La relación de equivalencia que hemos definido es lo mismo que decir que

$$a - b \in I = m\mathbb{Z}.$$

Podemos definir el conjunto cociente

$$\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z}) = \mathbb{Z}/I$$

que estará formado por las clases de equivalencia de la forma:

$$[a]_m = \big\{b \in \mathbb{Z} : \ b - a = m\,k \text{ con } k \in \mathbb{Z}\big\} = \big\{b \in \mathbb{Z} : \quad b \equiv a \bmod(m)\big\}.$$

Por lo tanto, las clases de equivalencia de $\mathbb{Z}_m$ serán

$$\mathbb{Z}_m = \big\{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\big\},$$

que son las clases de restos módulo m.

Observación 3.9.6.

1) $(\mathbb{Z}_n, +)$ *es cíclico, ya que* $\overbrace{[1]_n + [1]_n + \cdots + [1]_n}^{(n} = [n]_n = [0]_n$.

2) $[-1]_n = [n-1]_n$ *ya que*

$$[1]_n - [1]_n = [0]_n = [n]_n = [n - 1 + 1]_n = [1]_n + [n-1]_n,$$

así que

$$[-1]_n = [n-1]_n.$$

3.10. Ideales generados

Definición 3.10.1. *Dado un anillo A y un subconjunto $S \subset A$, el* ***ideal generado por*** *S, que denotaremos por $\langle S \rangle$, se define como el mínimo ideal que contiene a S, esto es, el ideal I tal que $S \subset I$ y si J es otro ideal, se cumple que si $S \subset J$, entonces $I \subset J$.*

O equivalentemente

$$\langle S \rangle = \bigcap_{\substack{I \text{ es un ideal de } A \\ I \supset S}} I.$$

Proposición 3.10.2. *Sea A un anillo conmutativo con unidad y S un subconjunto de A. El ideal generado por S es*

$$\langle S\rangle = \big\{r_1\cdot s_1+\cdots+r_n\cdot s_n:\ r_i\in A, s_i\in S, n\in\mathbb{N}\big\}.$$

Demostración. Sea

$$I = \big\{r_1\cdot s_1+\cdots+r_n\cdot s_n:\ r_i\in A, s_i\in S, n\in\mathbb{N}\big\},$$

como $s_i = 1\cdot s_i$ para todo $s_i\in S$, se tiene que $S\subset I$.

Además si J es un ideal que contiene a S y $s_i\in S$, entonces

$$r_i\cdot s_i\in J \quad \forall\, r_i\in A,$$

por definición de ideal.

Del mismo modo cualquier combinación lineal del tipo

$$r_1\cdot s_1+\cdots+r_n\cdot s_n\in J$$

para cualquier J tal que $S\subset J$.

Por tanto

$$I\subset J.$$

Falta demostrar que I es un ideal, para ello tomamos

$$\begin{aligned} p &= r_1\cdot s_1+\cdots+r_n\cdot s_n\in I\\ p' &= r_1'\cdot s_1+\cdots+r_n'\cdot s_n\in I \end{aligned}$$

se tiene que:

1) Es un grupo con respecto a la suma:

$$\begin{aligned} p-p' &= r_1\cdot s_1+\cdots+r_n\cdot s_n+(-r_1'\cdot s_1)+\cdots+(-r_n'\cdot s_n)\\ &= (r_1-r_1')\cdot s_1+\cdots+(r_n-r_n')\cdot s_n\\ &= r_1''\cdot s_1+\cdots+r_n''\cdot s_n\in I \end{aligned}$$

2) Cumple la propiedad de absorción con respecto al producto:

$\forall\, r\in A$

$$\begin{aligned} r\cdot p &= r\cdot(r_1\cdot s_1+\cdots+r_n\cdot s_n)\\ &= r\cdot r_1\cdot s_1+\cdots+r\cdot r_n\cdot s_n\\ &= r_1'\cdot s_1+\cdots+r_n'\cdot s_n\ \in I. \end{aligned}$$

Por lo tanto, I es un ideal. □

Ejemplo 3.10.3. Si $S = \{s\}$ tiene un sólo elemento, tenemos que

$$\langle S \rangle = \langle s \rangle = \{r \cdot s : \ r \in A\} = As$$

si A es conmutativo

$$\langle S \rangle = As = sA.$$

Por ejemplo, si $m \in \mathbb{Z}$ entonces

$$\langle m \rangle = \{m \cdot a : \ a \in \mathbb{Z}\} = m\mathbb{Z}.$$

Proposición 3.10.4. *Todos los ideales de* $(\mathbb{Z}, +, \cdot)$ *son de la forma*

$$\langle m \rangle = m\mathbb{Z}.$$

Demostración. Sea I un ideal de $(\mathbb{Z}, +, \cdot)$ y m el menor entero positivo de I, entonces tenemos que

$$\langle m \rangle = \{a \cdot m : \ a \in \mathbb{Z}\} \subset I,$$

ya que I es un ideal (y hemos visto que el generado por m es el menor que contiene a m).

Además si $i \in I$, por el algoritmo de la división en $\mathbb{Z}$ tenemos que

$$i = c \cdot m + r$$

donde $c, r \in \mathbb{Z}$ tal que $0 \leq r < m$.

Por tanto

$$r = i - c \cdot m \in I + \langle m \rangle \subset I.$$

Pero como m es el menor entero positivo de I (lo hemos elegido así), tendrá que cumplirse que $r = 0$, ya que r no puede ser un entero positivo menor que m.

Así que

$$i = c \cdot m \in \langle m \rangle.$$

Por lo tanto, todo ideal del anillo $(\mathbb{Z}, +, \cdot)$ está generado por un sólo elemento. □

3.11. Ideales primos

Definición 3.11.1. *Un ideal I de un anillo conmutativo A es un* ***ideal primo*** *si dados dos elementos cualesquiera a y b de A tales que $a \cdot b \in I$, se tiene que o bien $a \in I$ o bien $b \in I$.*

Ejemplo 3.11.2. Sea p un número entero positivo primo y consideremos $p\mathbb{Z}$, que es un ideal de $(\mathbb{Z}, +, \cdot)$.

Si a y b son dos números enteros tales que $a \cdot b \in p\mathbb{Z}$, entonces p divide a $a \cdot b$ y como p es primo, entonces p divide a a o p divide a b, por lo tanto, o bien $a \in p\mathbb{Z}$ o bien $b \in p\mathbb{Z}$, así que $p\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$.

Ejemplo 3.11.3. $3\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ ya que $\forall\, a, b \in \mathbb{Z}$ tal que $a \cdot b \in 3\mathbb{Z}$, por tanto, o bien $a = 3 \cdot s$ o bien $b = 3 \cdot s$ con $s \in \mathbb{Z}$.

Ejemplo 3.11.4. $6\mathbb{Z}$ no es un ideal primo de $\mathbb{Z}$ ya que puede existir $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ tales que $a \cdot b \in 6\mathbb{Z}$ con $a \notin 6\mathbb{Z}$ y $b \notin 6\mathbb{Z}$, por ejemplo, si tomamos $a = 3$ y $b = 2$, tenemos $a \cdot b = 6 \in 6\mathbb{Z}$ pero $a = 3 \notin 6\mathbb{Z}$ y $b = 2 \notin 6\mathbb{Z}$.

Proposición 3.11.5. *Sea A un anillo conmutativo e I un ideal de A con $I \neq A$. El anillo cociente A/I es un dominio de integridad si y sólo si I es un ideal primo de A.*

Demostración.

$\boxed{\Rightarrow}$ A/I dominio de integridad $\Longrightarrow$ I ideal primo de A:

Tomamos $a, b \in A$ tal que $a \cdot b \in I$ entonces

$$[a + I] \cdot [b + I] = [a \cdot b + I] = I$$

(sabiendo que I es el elemento neutro del anillo A/I).

Como A/I es dominio de integridad, entonces, o bien $[a + I] = I$ o bien $[b + I] = I$, por lo tanto, o bien $a \in I$ o bien $b \in I$, o sea, I es un ideal primo.

$\boxed{\Leftarrow}$ I es un ideal primo de $A \Longrightarrow A/I$ es dominio de integridad:

Sea $[a + I] \cdot [b + I] = I$ para un par de elementos $[a + I]$ y $[b + I]$ de A/I, por tanto

$$I = [a + I] \cdot [b + I] = [a \cdot b + I] \Longrightarrow a \cdot b \in I$$

y como I es primo, tendremos que o bien $a \in I$ o bien $b \in I$, por tanto, o bien $[a + I] = I$ o bien $[b + I] = I$, o sea, A/I es dominio de integridad.

□

3.12. Ideales maximales

Definición 3.12.1. *Sea A un anillo conmutativo con unidad, e I un ideal de A con $I \neq A$. El ideal I se llama* ***maximal*** *si no existe otro ideal J de A tal que $I \subset J \subset A$ con $I \neq J$ y $J \neq A$.*

Teorema 3.12.2. *Sea A un anillo conmutativo con unidad e I un ideal de A. El anillo cociente A/I es un cuerpo si y sólo si I es un ideal maximal.*

Corolario 3.12.3. *Todo ideal maximal en un anillo conmutativo con unidad es un ideal primo.*

Demostración. Si I es maximal, A/I es un cuerpo por el Teorema 3.12.2, por lo que también es un dominio de integridad, y por la Proposición 3.11.5, I es primo. □

3.13. Cuerpo de fracciones de un anillo

Sea A un dominio de integridad conmutativo con unidad 1. En el producto cartesiano

$$A \times A^* = \{(a, b) \text{ tal que } a \in A, b \in A^*\}$$

definimos la relación

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow a \cdot d = b \cdot c$$

que es una relación de equivalencia, dado que cumple las propiedades:

1) Reflexiva: $(a, b)\mathcal{R}(a, b)$ ya que $a \cdot b = b \cdot a$

2) Simétrica: $(a, b)\mathcal{R}(a', b') \Longrightarrow (a', b')\mathcal{R}(a, b)$ ya que

$$a \cdot b' = b \cdot a' \Longrightarrow a' \cdot b = b' \cdot a$$

3) Transitiva: $(a, b)\mathcal{R}(a', b'), (a', b')\mathcal{R}(a'', b'') \Longrightarrow (a, b)\mathcal{R}(a'', b'')$, ya que

$$\begin{cases} a \cdot b' = b \cdot a' \\ a' \cdot b'' = b' \cdot a'' \end{cases} \Longrightarrow \begin{cases} a \cdot b' \cdot b'' = b \cdot a' \cdot b'' \\ a' \cdot b'' = b' \cdot a'' \end{cases}$$

$$\begin{aligned} &\Longrightarrow a \cdot b' \cdot b'' = b \cdot b' \cdot a'' \\ &\Longrightarrow b' \cdot a \cdot b'' = b' \cdot b \cdot a'' \\ &\Longrightarrow a \cdot b'' = b \cdot a'' \end{aligned}$$

La clase del elemento $(a, b) \in A \times A^*$ la simbolizaremos mediante

$$[(a, b)]$$

y al conjunto cociente de las clases de equivalencia lo denotaremos por

$$C = (A \times A^*)/\mathcal{R}.$$

En C definimos una suma y un producto como

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)]$$

Teorema 3.13.1. $(C, +, \cdot)$ *es un cuerpo con las operaciones anteriores, y se llama* ***cuerpo de las fracciones del anillo*** A.

Demostración.

1) Grupo aditivo:

   1,1) Operación cerrada: Por definición, se puede ver fácilmente que es una operación cerrada

   1,2) Propiedad asociativa:

$$\begin{aligned}\big([x, y] + [x', y']\big) + [x'', y''] &= [x \cdot y' + y \cdot x', y \cdot y'] + [x'', y''] \\ &= [(x \cdot y' + y \cdot x') \cdot y'' + x'' \cdot (y \cdot y'), (y \cdot y') \cdot y''] \\ &= [x \cdot (y' \cdot y'') + y \cdot (x' \cdot y'' + x'' \cdot y'), y \cdot (y' \cdot y'')] \\ &= [x, y] + [x' \cdot y'' + y' \cdot x'', y' \cdot y''] \\ &= [x, y] + \big([x', y'] + [x'', y'']\big)\end{aligned}$$

   1,3) Elemento neutro $e_0 = [0, 1]$:

$$[x, y] + [0, a] = [x \cdot a + 0 \cdot y, y \cdot a] = [a \cdot x, a \cdot y] = [x, y]$$

   1,4) Elemento opuesto $[x, y]_+^{-1} = [-x, y]$:

$$[x, y] + [-x, y] = [x \cdot y - x \cdot y, y \cdot y] = [0, y \cdot y] = e_0$$

2) Grupo multiplicativo:

   2,1) Operación cerrada: Por definición, se puede ver fácilmente que es una operación cerrada

2,2) Propiedad asociativa:

$$\begin{aligned}\big([x,y]\cdot[x',y']\big)\cdot[x'',y''] &= [x\cdot x', y\cdot y']\cdot[x'',y'']\\ &= [(x\cdot x')\cdot x'', (y\cdot y')\cdot y'']\\ &= [x\cdot(x'\cdot x''), y\cdot(y'\cdot y'')]\\ &= [x,y]\cdot[x'\cdot x'', y'\cdot y'']\\ &= [x,y]\cdot\big([x',y']\cdot[x'',y'']\big)\end{aligned}$$

2,3) Elemento neutro $e_1 = [1,1]$:

$$[x,y]\cdot[a,a] = [x\cdot a, y\cdot a] = [x,y]$$

2,4) Elemento inverso $[x,y]^{-1} = [y,x]$:

$$[x,y]\cdot[y,x] = [x\cdot y, y\cdot x] = [1,1] = e_1$$

3) Distributividad:

$$\begin{aligned}[x,y]\cdot\big([x',y']+[x'',y'']\big) &= [x,y]\cdot[x'\cdot y''+y'\cdot x'', y'\cdot y'']\\ &= [x\cdot(x'\cdot y''+y'\cdot x''), y\cdot(y'\cdot y'')]\\ &= [(x\cdot x')\cdot(y''\cdot y)+(x\cdot x'')\cdot(y'\cdot y), (y\cdot y')\cdot(y''\cdot y)]\\ &= [x\cdot x', y\cdot y'] + [x\cdot x'', y\cdot y'']\\ &= [x,y]\cdot[x',y'] + [x,y]\cdot[x'',y'']\end{aligned}$$

Por lo tanto, C es un cuerpo y además es conmutativo ya que

$$[x,y]\cdot[x',y'] = [x',y']\cdot[x,y].$$

□

Ejemplo 3.13.2. A partir del anillo $(\mathbb{Z},+,\cdot)$ generamos un cuerpo $(\mathbb{Q},+,\cdot)$, donde

$$\mathbb{Q} = \mathbb{Z}\times\mathbb{Z}^*/\mathcal{R}$$

es el conjunto de las clases de equivalencia con la relación definida antes, es decir,

$$(a,b)\mathcal{R}(x,y) \Leftrightarrow a\cdot y = b\cdot x.$$

Tenemos que

$$[(a,b)]\in\mathbb{Q} \Longrightarrow [(a,b)] = \left\{(x,y) = \frac{x}{y} :\ x\in\mathbb{Z},\ y\in\mathbb{Z}^*,\quad a\cdot y = b\cdot x\right\}$$

esto es, el conjunto de las fracciones equivalentes $\frac{a}{b} = \frac{x}{y}$.

Además la suma de fracciones es

$$[x, y] + [x' + y'] = [x \cdot y' + y \cdot x', y \cdot y']$$

o de forma equivalente

$$\frac{x}{y} + \frac{x'}{y'} = \frac{x \cdot y' + y \cdot x'}{y \cdot y'}.$$

Y el producto de fracciones es

$$[x, y] \cdot [x', y'] = [x \cdot x', y \cdot y']$$

o de forma equivalente

$$\frac{x}{y} \cdot \frac{x'}{y'} = \frac{x \cdot x'}{y \cdot y'}$$

Observación 3.13.3. *Es necesario que A sea un dominio de integridad conmutativo con unidad.*

Si no fuese así no podríamos definir una relación de equivalencia como la que hemos definido

$$(x, y)\mathcal{R}(x', y') \Longleftrightarrow x \cdot y' = y \cdot x'.$$

Véase el ejemplo siguiente:

Ejemplo 3.13.4. El conjunto de funciones reales de variable real $\mathcal{C}(\mathbb{R}, \mathbb{R})$ no es un dominio de integridad. Si tomamos

$$\begin{aligned} &f_1(x) = x + |x|, \qquad f_2(x) = f_3(x) = 0, \\ &g_1(x) = x, \qquad g_2(x) = x - |x|, \qquad g_3(x) = -x, \end{aligned}$$

y según la relación anterior tenemos que:

$$(f_1, g_1)\mathcal{R}(f_2, g_2) \text{ ya que } f_1 \cdot g_2 = g_1 \cdot f_2$$

y

$$(f_2, g_2)\mathcal{R}(f_3, g_3) \text{ ya que } f_2 \cdot g_3 = g_2 \cdot f_3$$

Sin embargo,

$$(f_1, g_1)\not\mathcal{R}(f_3, g_3)$$

ya que

$$f_1 \cdot g_3 \neq f_3 \cdot g_1,$$

por lo tanto no es un relación de equivalencia ya que no cumple la propiedad transitiva.

Nota 3.13.5. *En sentido estricto, A no es un subanillo de C; sin embargo identificaremos A con su anillo isomorfo $\mathcal{A}$ (ver sección que viene a continuación), y con un cierto abuso del lenguaje, diremos que C contiene a A (esto equivale a identificar los enteros $\mathbb{Z}$ con el conjunto de las fracciones de la forma $\frac{p}{1}$, con $p \in \mathbb{Z}$).*

3.14. Homomorfismos de anillos

Definición 3.14.1. *Dados dos anillos A, A', una función $f : A \to A'$ se dice que es un* ***homomorfismo de anillos*** *si para todo par de elementos r y s de A, se tiene que*

$$f(r+s) = f(r) + f(s),$$
$$f(rs) = f(r)f(s).$$

Observación 3.14.2. *En particular f es un homomorfismo entre los grupos $(A, +)$ y $(A', +)$.*

Definición 3.14.3. *Una aplicación f entre dos cuerpos C y C' con las propiedades anteriores se dice que es un* ***homomorfismo de cuerpos****. En este caso, f define un homomorfismo entre los grupos aditivos $(C, +)$ y $(C', +)$, y también entre los grupos multiplicativos $(C^*, \cdot)$ y $(C'^*, \cdot)$.*

Definición 3.14.4. *Si un homomorfismo f de anillos es una biyección, se dice que f es un* ***isomorfismo de anillos****, y A y A' se dice que son* ***isomorfos****. En este caso f^{-1} es también un isomorfismo de anillos.*

Definición 3.14.5. *Un homomorfismo $f : A \longrightarrow B$ entre anillos unitarios conmutativos es:*

1) ***Epimorfismo*** *si f es una aplicación sobreyectiva.*

2) ***Monomorfismo*** *si f es una aplicación inyectiva.*

3) ***Isomorfismo*** *si f es una aplicación biyectiva.*

Ejemplo 3.14.6. La siguiente aplicación f es un homomorfismo entre los cuerpos $(\mathbb{R}^2, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$

$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ & (a,b) & \longrightarrow & a+bi \end{array}$$

con

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b) \cdot (c,d) = (a \cdot d - b \cdot d, a \cdot d + b \cdot c).$$

Ejemplo 3.14.7. La siguiente aplicación π es un homomorfismo entre anillos (homomorfismo canónico):

$$\begin{array}{rccc} \pi: & A & \longrightarrow & A/I \\ & a & \longrightarrow & [a+I] \end{array}$$

Dicho homomorfismo π es sobreyectivo.

Proposición 3.14.8. *Sea $f : A \to A'$ un homomorfismo de anillos, entonces se tienen las siguientes propiedades:*

1) *$f(0_A) = 0_{A'}$ y $f(-x) = -f(x)$, donde 0_A y $0_{A'}$ son los elementos neutros de A y A', respectivamente, con respecto a la primera operación.*

2) *Si S es un subanillo de A, $f(S) = \{f(s) : \ s \in S\}$ es un subanillo de A'.*

3) *Si S' es un subanillo de A', $f^{-1}(S') = \{s \in A : \ f(s) \in S'\}$ es un subanillo de A.*

4) *Si I' es un ideal de A', $f^{-1}(I')$ es un ideal de A.*

5) *Si f es sobreyectiva e I es un ideal de A, $f(I)$ es un ideal de A'.*

6) *Si A es un anillo con unidad 1_A y f es sobreyectiva, entonces A' es un anillo con unidad*
$$1_{A'} = f(1_A).$$

Demostración.

1) ▶ Si $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, entonces $f(0_A) = 0_{A'}$ ya que el elemento neutro del grupo $(A', +)$ es único.

   ▶ Si $f(0_A) = f(x + (-x)) = f(x) + f(-x)$, entonces
   $$f(x) + f(-x) = 0_{A'}.$$
   Por tanto
   $$f(-x) = -f(x).$$

2) Si S es un subanillo de A, entonces $(S, +)$ es un subgrupo de $(A, +)$.

   Como f es un homomorfismo entre grupos $(A, +)$ y $(A', +)$, entonces $(f(S), +)$ es un subgrupo de $(A', +)$ (véase, Proposición 2.8.12).

   Demostramos que el producto es una operación cerrada en $f(S)$: Sean $x, y \in S$, tenemos que
   $$f(x) \cdot f(y) = f(x \cdot y)$$
   por ser un homomorfismo.

   Como x e y son elementos del subanillo S, entonces $x \cdot y \in S$, por lo tanto $f(x \cdot y) \in f(S)$.

   Luego $f(S)$ es subanillo de A'.

3) Por la Proposición 2.8.12 se tiene que, si S' es subgrupo de $(A', +)$, entonces $f^{-1}(S')$ es subgrupo de $(A, +)$.

   Por lo tanto, para demostrar que $f^{-1}(S')$ es subanillo de A, sólo tenemos que demostrar que en $f^{-1}(S')$ el producto es una operación cerrada.

   Para ello consideremos $x, y \in f^{-1}(S')$ entonces existen $x', y' \in S'$ tales que

   $$f(x) = x', f(y) = y'.$$

   Por lo tanto,

   $$f(x) \cdot f(y) = f(x \cdot y) = x' \cdot y' \in S',$$

   ya que S' es un subanillo, así que $x \cdot y \in f^{-1}(S')$.

   Esto significa que $f^{-1}(S')$ es subanillo de A.

4) Hemos demostrado anteriormente que la contraimagen de un subanillo de A' es un subanillo de A, así que sólo tenemos que demostrar que la contraimagen de un ideal cumple la propiedad de absorción con el producto.

   Tomemos $x \in f^{-1}(I')$, por lo tanto existe $x' \in I'$ tal que

   $$f(x) = x'.$$

   Sea $a \in A$ tenemos que $f(a) \in A'$, entonces

   $$f(a) \cdot x' = f(a) \cdot f(x) \in I',$$

   ya que I' es un ideal de A'.

   Como f es un homomorfismo, se tiene que

   $$f(a) \cdot f(x) = f(a \cdot x) \in I',$$

   por lo tanto $a \cdot x \in f^{-1}(I')$, así que $f^{-1}(I')$ es un ideal de A.

5) Al igual que en el apartado anterior, para demostrar que la imagen de un ideal I de A es un ideal de A' si f es sobreyectiva, basta demostrar que en $f(I)$ el producto cumple la propiedad de absorción.

   Como f es sobreyectiva, entonces

   $$\forall\, b \in A', \exists\, a \in A \quad \text{tal que} \quad f(a) = b.$$

   Por lo tanto, $\forall y \in f(I)$, existe $x \in I$ tal que

   $$y = f(x).$$

Así que

$$b \cdot y = f(a) \cdot f(x) = f(a \cdot x).$$

Como I es un ideal $a \cdot x \in I$, así $f(a \cdot x) \in f(I)$, por lo que $f(I)$ es un ideal de A'.

6) Si $a' \in A'$, existe un $a \in A$ tal que $a' = f(a)$ y por tanto

$$a' \cdot f(1_A) = f(a) \cdot f(1_A) = f(a \cdot 1_A) = f(a) = a',$$

y también $f(1_A) \cdot a' = a'$, lo que prueba que

$$1_{A'} = f(1_A).$$

□

Proposición 3.14.9. *Sea $f : A \longrightarrow A'$ un homomorfismo de anillos. Entonces* $\ker(f) = \{x \in A : \ f(x) = 0_{A'}\}$*, el* ***núcleo*** *de f, es un conjunto no vacío, y es un ideal de A.*

Demostración. Tenemos $\ker(f) \neq \emptyset$ ya que $f(0_A) = 0_{A'} \Longrightarrow 0_A \in \ker(f)$. Vamos a probar que $\ker(f)$ es un ideal:

1) Sean $x, y \in \ker(f)$ entonces $f(x) = f(y) = 0$, por tanto

$$f(x) - f(y) = f(x) + f(-y) = 0,$$

luego

$$f(x - y) = 0,$$

así que

$$x - y \in \ker(f),$$

por lo tanto, $\ker(f)$ es un subgrupo aditivo.

2) Sean $x \in \ker(f)$ y $a \in A$, entonces

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0_{A'} = 0_{A'},$$

así que

$$a \cdot x \in \ker(f),$$

por lo tanto $\ker(f)$ cumple la propiedad de absorción.

Por lo tanto $\ker(f)$ es un ideal. □

Proposición 3.14.10. *Un homomorfismo $f : A \longrightarrow A'$ es inyectivo si y sólo si* $\ker(f) = \{0_A\}$.

Demostración.

$\boxed{\Rightarrow}$ Supongamos que f es inyectiva, si $x \in \ker(f)$ entonces $f(x) = 0_{A'}$. Como además sabemos que $f(0_A) = 0_{A'}$, entonces, al ser f inyectiva si $f(x) = f(0_A)$ se tiene que $x = 0_A$, por lo tanto

$$\ker(f) = \{0_A\}.$$

$\boxed{\Leftarrow}$ Supongamos que $\ker(f) = \{0_A\}$. Tomemos $f(x) = f(y)$ entonces

$$f(x) - f(y) = 0_{A'} \Longrightarrow f(x) + f(-y) = 0_{A'},$$

así que

$$f(x - y) = 0_{A'}.$$

Como $\ker(f) = \{0_A\}$, entonces

$$x - y = 0_A \Longrightarrow x = y,$$

por lo tanto f es inyectiva.

□

Capítulo 4

Anillos de Polinomios

4.1. Definiciones

Definición 4.1.1 (**Polinomio**). *Sea A un anillo. Se llama* ***polinomio en la indeterminada*** *X* ***con coeficientes en*** *A a una expresión formal de la forma*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0,$$

con $a_i \in A$ para todo $i = 1, \ldots, n$, donde $n \in \mathbb{N}$. El elemento a_i se llama coeficiente de X^i o de grado i en $P(X)$.

Notación 4. *Notaremos por $A[X]$ al conjunto de los polinomios en la indeterminada X con coeficientes en el anillo A.*

Definición 4.1.2 (**Grado**). *El grado de $P(X)$ es el mayor número entero positivo n tal que $a_n \neq 0$ y se denota* $\text{grado}(P(X)) = n$.

El coeficiente a_n se llama ***coeficiente líder de*** *$P(X)$. Si $a_n = 1$, decimos que $P(X)$ es un* ***polinomio mónico****.*

4.2. Operaciones en $A[X]$

1) **Igualdad de polinomios.**

   Dos polinomios

$$P(X) = a_n X^n + \cdots + a_1 X + a_0 \quad \text{y} \quad Q(X) = b_m X^m + \cdots + b_1 X + b_0$$

   son *iguales*, $P(X) = Q(X)$, si $n = m$ y $a_i = b_i, \forall i \geq 0$.

2) **Suma de polinomios.**

Dados dos polinomios

$$P(X) = a_n X^n + \cdots + a_1 X + a_0 \quad \text{y} \quad Q(X) = b_m X^m + \cdots + b_1 X + b_0,$$

denominamos *polinomio suma* al polinomio

$$S(X) = P(X) + Q(X) = c_n X^n + \cdots + c_1 X + c_0$$

con $c_i = a_i + b_i, \forall i \geq 0$.

3) **Producto de polinomios.**

Dados dos polinomios

$$P(X) = a_n X^n + \cdots + a_1 X + a_0 \quad \text{y} \quad Q(X) = b_m X^m + \cdots + b_1 X + b_0,$$

denominamos *polinomio producto* al polinomio

$$M(X) = d_{n+m} X^{n+m} + \cdots + d_1 X + d_0,$$

con

$$d_i = \sum_{\substack{k=0 \\ k \leq n,\ i-k \leq m}}^{i} a_k b_{i-k}$$

Ejemplo 4.2.1.

1) En $\mathbb{R}[X]$: $P(X) = 1 + 2X + X^2 + X^3$

$Q(X) = 2 + X^3$

$P(X) + Q(X) = 3 + 2X + X^2 + 2X^3$

$P(X) \cdot Q(X) = 2 + 4X + 2X^2 + 3X^3 + 2X^4 + X^5 + X^6$

2) En $\mathbb{Z}_3[X]$: $P(X) = \overline{1} + \overline{2}X^2 + \overline{1}X^3$

$Q(X) = \overline{1}X + \overline{2}X^3$

$P(X) + Q(X) = \overline{1} + \overline{1}X + \overline{2}X^2$

$P(X) \cdot Q(X) = \overline{1} + \overline{1}X + \overline{1}X^3 + \overline{1}X^4 + \overline{1}X^5 + \overline{2}X^6$

Nota 4.2.2. *Para simplificar la notación, a partir de ahora, las clases $\overline{n} = [n]_p$ del anillo $\mathbb{Z}_p$ las denotaremos como $\overline{n} \equiv n$.*

4.3. Anillo de polinomios

Definición 4.3.1. *Sea A un anillo conmutativo con unidad, el conjunto $A[X]$ con la suma y el producto definidos anteriormente, $(A[X], +, \cdot)$, es un anillo conmutativo con unidad y se denomina* ***anillo de polinomios de*** *A.*

- *El elemento neutro de la suma de polinomios es $0(X) = 0_A$ (elemento cero).*
- *El elemento neutro del producto de polinomios es $1(X) = 1_A$ (elemento identidad).*
- *El elemento opuesto de $P(X) = a_0 + a_1X + \cdots + a_nX^n$ de la suma de polinomios es $-P(X) = -a_0 + (-a_1)X + \cdots + (-a_n)X^n$.*
- *El polinomio $0(X)$ no tiene grado y los polinomios de la forma $P(X) = a_0$ tienen grado 0.*

Proposición 4.3.2. *Si A es un dominio de integridad, su anillo de polinomios $A[X]$ también es un dominio de integridad.*

Demostración. Sea A dominio de integridad y sean

$$P(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X], \quad \text{con} \quad a_n \neq 0$$

$$Q(X) = b_0 + b_1X + \cdots + b_mX^m \in A[X], \quad \text{con} \quad b_m \neq 0$$

entonces,

$$P(X) \cdot Q(X) = c_0 + c_1X + \cdots + c_{n+m}X^{n+m} \neq 0$$

con $c_{n+m} = a_nb_m \neq 0$ ya que A es dominio de integridad. □

Proposición 4.3.3. *Dados dos polinomios $P(X)$ y $Q(X)$ pertenecientes a un dominio de integridad, tenemos que:*

1) $\text{grado}\big(P(X) \cdot Q(X)\big) = \text{grado}(P(X)) + \text{grado}(Q(X))$.
2) $\text{grado}(P(X) + Q(X)) \leq \text{máx}\big\{\text{grado}(P(X)),\ \text{grado}(Q(X))\big\}$.

Demostración.

1) Si $\text{grado}(P(X)) = n$ y $\text{grado}(Q(X)) = m$, entonces

$$\text{grado}(P(X) \cdot Q(X)) = m + n$$

ya que $a_n \neq 0, b_m \neq 0 \Rightarrow a_n \cdot b_m \neq 0$ porque A es dominio de integridad.

Esto no sería cierto si no es un dominio de integridad, por ejemplo, $\mathbb{Z}_6[X]$ no lo es y podemos tomar $P(X) = 3X, Q(X) = 2X \Rightarrow Q(X) \cdot Q(X) = 3X \cdot 2X = (3 \cdot 2)X^2 = 6X^2 = 0X^2 = 0$

2) Si $m \neq n \Rightarrow P(X) + Q(X) \neq 0$ entonces

$$\text{grado}(P(X) + Q(X)) = \text{máx}(m, n)$$

$$\left.\begin{array}{l} \text{Si } m = n \text{ y } a_n \neq -b_n \Rightarrow \text{grado}(P(X) + Q(X)) = n \\ \text{Si } m = n \text{ y } a_n = -b_n \Rightarrow \text{grado}(P(X) + Q(X)) < n \end{array}\right\}$$

se tiene que,

$$\text{grado}(P(X) + Q(X)) \leq n = \text{máx}(n, m).$$

Por lo tanto, siempre se cumplirá que

$$\text{grado}(P(X) + Q(X)) = \text{máx}\left\{\text{grado}(P(X)), \text{grado}(Q(X))\right\}.$$

□

Proposición 4.3.4. *Si A es un dominio de integridad conmutativo con unidad, los elementos invertibles de $A[X]$ coinciden con los elementos invertibles de A, $U(A) = U(A[X])$.*

Demostración. Si $P(X) \neq 0, Q(X) \neq 0$ y $P(X) \cdot Q(X) = 1$ entonces

$$\text{grado}(P(X) \cdot Q(X)) = \text{grado}(P(X)) + \text{grado}(Q(X)) = 0$$

por tanto

$$\text{grado}(P(X)) = 0, \quad \text{grado}(Q(X)) = 0$$

ya que es un dominio de integridad, por lo tanto los únicos elementos invertibles de $A[X]$ son de la forma $P(X) = a_0$. □

Ejemplo 4.3.5. $U(\mathbb{Z}) = \{\pm 1\} = U(\mathbb{Z}[X])$.

4.4. Teorema de la división

Dado un cuerpo C, el conjunto $C[X]$ de polinomios con coeficientes en C forma un anillo respecto a la suma y el producto de polinomios. Además, $C[X]$ es un dominio de integridad conmutativo con unidad.

Teorema 4.4.1 (Algoritmo de división). *Sea C un cuerpo y $P(X)$ y $Q(X)$ dos polinomios de $C[X]$, con $P \neq 0$. Entonces existen dos polinomios $S(X)$ y $R(X)$ también del anillo $C[X]$ tales que*

$$P(X) = Q(X)S(X) + R(X)$$

y $R(X) = 0$ o $\text{grado}\big(R(X)\big) < \text{grado}\big(Q(X)\big)$

Ejemplo 4.4.2.

1) En $\mathbb{Q}[X]$ tomamos $P(X) = X^4 - X^2 + 1, Q(X) = 2X^2 + 1$ entonces $P(X) = Q(X) \cdot S(X) + R(X)$ con $S(X), R(X) \in \mathbb{Q}[X]$

$$\begin{array}{l|l} X^4 - X^2 + 1 & 2X^2 + 1 \\ \hline -X^4 - \frac{1}{2}X^2 & \frac{1}{2}X^2 - \frac{3}{4} \\ \hline -\frac{3}{2}X^2 + 1 & \\ \frac{3}{2}X^2 + \frac{3}{4} & \\ \hline \frac{7}{4} & \end{array}$$

Por lo tanto

$$S(X) = \frac{1}{2}X^2 - \frac{3}{4}, R(X) = \frac{7}{4}, \text{grado}(R(X)) = 0 < \text{grado}(Q(X)) = 2.$$

Esta propiedad está definida en $\mathbb{Q}[X]$ (ya que $\mathbb{Q}$ es un cuerpo), pero no en $\mathbb{Z}[X]$ (ya que $\mathbb{Z}$ no es cuerpo).

2) En $\mathbb{Z}_5[X]$ tomamos $P(X) = 3X^3 + 2X + 4, Q(X) = 1X^2 + 2$ entonces $P(X) = Q(X) \cdot S(X) + R(X)$ con $S(X), R(X) \in \mathbb{Z}_5[X]$

$$\begin{array}{l|l} 3X^3 + 2X + 4 & 1X^2 + 2 \\ \hline -3X^3 - 6X & 3X \\ \hline -4X + 4 & \\ \hline 1X + 4 & \end{array}$$

Por lo tanto $S(X) = 3X, R(X) = 1X + 4$.

Proposición 4.4.3. *Los polinomios cociente, $S(X)$, y resto, $R(X)$, son únicos.*

4.5. Divisor de un polinomio

Definición 4.5.1. *Sean $P(X), Q(X) \in A[X]$ con $Q(X) \neq 0$, se dice que $Q(X)$* ***divide a*** *$P(X)$ o que $Q(X)$ es* ***divisor*** *de $P(X)$ si*

$$P(X) = Q(X) \cdot S(X)$$

para algún $S(X) \in A[X]$ y se denota $Q(X) \big| P(X)$.

Ejemplo 4.5.2. En $\mathbb{R}[X]$ tomamos

$$P(X) = X^3 + X^2 + X + 1,\ Q(X) = X + 1,$$

$Q(X)$ divide a $P(X)$ ya que existe $S(X) = X^2 + 1 \in \mathbb{R}[X]$ con

$$P(X) = Q(X) \cdot S(X).$$

Ejemplo 4.5.3. En $\mathbb{Z}_3[X]$ tomamos

$$P(X) = 2X^3 + 1,\ Q(X) = 2X + 1,$$

$Q(X)$ divide a $P(X)$ ya que existe $S(X) = X^2 + X + 1 \in \mathbb{Z}_3[X]$ con

$$P(X) = Q(X) \cdot S(X).$$

Proposición 4.5.4. *Sea C un cuerpo. Si $P \in C[X]$ y $a \in C$, entonces $X - a$ divide a $P(X)$ si y sólo si $P(a) = 0$.*

Demostración.

$\boxed{\Rightarrow}$

Si $(X - a)|P(X)$ entonces existe $S(X) \in C[X]$ tal que

$$P(X) = S(X) \cdot (X - a)$$

y por tanto

$$P(a) = S(a) \cdot (a - a) = 0.$$

$\boxed{\Leftarrow}$

Por el teorema de la división entera podemos escribir

$$P(X) = S(X) \cdot Q(X) + R(X)$$

con $\text{grado}(R(X)) < \text{grado}(Q(X))$ ó $R(X) = 0$.
Si tomamos $Q(X) = X - a$ entonces

$$P(X) = S(X) \cdot (X - a) + R(X)$$

con $\text{grado}(R(X)) < \text{grado}(Q(X)) = 1$.
Así que

$$\text{grado}(R(X)) = 0.$$

Por tanto

$$R(X) = b \in C.$$

Luego

$$P(X) = S(X) \cdot (X - a) + b$$

entonces

$$P(a) = S(a) \cdot (a - a) + b = b.$$

Como además hemos supuesto que $P(a) = 0$ se tiene que

$$P(a) = b = 0.$$

Por tanto $Q(X) = X - a$ divide a $P(X)$.

□

Ejemplo 4.5.5. El polinomio $X - [3]$ divide a $P(X) = X^2 + X + [1]$ en $\mathbb{Z}_{13}[X]$ ya que $P([3]) = [13] = [0]$ en $\mathbb{Z}_{13}$.

De hecho $P(X) = (X - [9])(X - [3])$.

Sin embargo $X-3$ no divide a $P(X) = X^2+X+1$ en $\mathbb{Q}[X]$ ya que $P(3) = 13 \neq 0$ en $\mathbb{Q}$.

4.6. Máximo común divisor

Definición 4.6.1. *Se dice que $D(X) \in A[X]$, donde A es un cuerpo, es el* ***máximo común divisor*** *de $P(X)$ y $Q(X)$ y se escribe*

$$\text{mcd}\big(P(X), Q(X)\big) = D(X)$$

si, y sólo si, satisface las condiciones siguientes:

1) *$D(X)$ es mónico.*

2) *$D(X)|P(X)$ y $D(X)|Q(X)$.*

3) *Si $\forall\ H(X) \in A[X]$ tal que $H(X)|P(X)$ y $H(X)|Q(X)$, entonces $H(X)|D(X)$.*

Observación 4.6.2. *El máximo común divisor de dos polinomios es el polinomio mónico de grado más alto que divide a ambos polinomios.*

Nota 4.6.3.

- *Exigimos que el máximo común divisor sea mónico para que sea único.*
- *Si A no fuese cuerpo no podríamos simplificar para obtener un polinomio mónico, ya que puede ocurrir que $A[X]$ tenga divisores de cero (y por tanto no se pueda simplificar).*

Proposición 4.6.4. *Sean $P(X), Q(X) \in A[X]$ dos polinomios fijos, entonces*

$$I = \{P(X) \cdot R(X) + Q(X) \cdot S(X), \forall\ R(X), S(X) \in A[X]\}$$

es un ideal de $A[X]$ y lo denotaremos por $[P(X), Q(X)]$.

Demostración. Dados

$$A_1(X) = P(X) \cdot R_1(X) + Q(X) \cdot S_1(X) \in I$$

y

$$A_2(X) = P(X) \cdot R_2(X) + Q(X) \cdot S_2(X) \in I,$$

tenemos que

1)

$$\begin{aligned} A_1(X) - A_2(X) = &(R_1(X) - R_2(X)) \cdot P(X) \\ &+ (S_1(X) - S_2(X)) \cdot Q(X) \in I. \end{aligned}$$

2) Para todo $H(X) \in A[X]$,

$$\begin{aligned} A_1(X) \cdot H(X) = &P(X) \cdot (R_1(X) \cdot H(X)) \\ &+ Q(X) \cdot (S_1(X) \cdot H(X)) \in I. \end{aligned}$$

Por lo tanto I es un ideal. □

Observación 4.6.5. *Si I es un ideal generado por $P(X)$ y $Q(X)$, o sea,*

$$I = \{P(X) \cdot R(X) + Q(X) \cdot S(X)\ , \forall\ R(X), S(X) \in A[X]\}\,,$$

existirá un polinomio $D(X)$ tal que

$$I = [D(X)]\,.$$

Por tanto, $D(X)|P(X)$ y $D(X)|Q(X)$ ya que

$$D(X)|P(X) \cdot R(X) + Q(X) \cdot S(X).$$

Además, como $D(X) \in I$, tendremos que

$$D(X) = P(X) \cdot A(X) + Q(X) \cdot B(X).$$

Si $H(X)$ divide a $P(X)$ y a $Q(X)$ se cumplirá que $H(X)|D(X)$, ya que

$$P(X) = M_1(X) \cdot H(X),\ Q(X) = M_2(X) \cdot H(X).$$

Entonces

$$D(X) = H(X) \cdot [A(X) \cdot M_1(X) + B(X) \cdot M_2(X)].$$

Por lo tanto, $D(X)$ es el máximo común divisor de $P(X)$ y $Q(X)$.

4.7. Algoritmo de Euclides (cálculo del máximo común divisor)

Proposición 4.7.1. *Si $P(X) = Q(X) \cdot S(X) + R(X)$ es la división de $P(X)$ por $Q(X) \neq 0$, entonces los ideales $[P(X), Q(X)]$ y $[Q(X), R(X)]$ coinciden.*

Demostración.

1) Sea $F(X) \in [P(X), Q(X)]$ entonces existen $A_1(X), A_2(X) \in A[X]$ tal que

$$F(X) = A_1(X) \cdot P(X) + A_2(X) \cdot Q(X)$$

Como además $P(X) = Q(X) \cdot S(X) + R(X)$ entonces

$$F(X) = A_1(X) \cdot [Q(X) \cdot S(X) + R(X)] + A_2(X) \cdot Q$$
$$(X = [A_1(X) \cdot S(X) + A_2(X)] \cdot Q(X) + A_1(X) \cdot R(X)$$

Así que

$$F(X) \in [Q(X), R(X)]$$

Por tanto

$$[P(X), Q(X)] \subset [Q(X), R(X)]$$

2) Por otro lado, si $G(X) \in [Q(X), R(X)]$ entonces existen $B_1(X), B_2(X) \in A[X]$ tal que

$$G(X) = B_1(X) \cdot Q(X) + B_2(X) \cdot R(X).$$

Como $P(X) = Q(X) \cdot S(X) + R(X)$ entonces

$$R(X) = P(X) - Q(X) \cdot S(X).$$

Así que

$$\begin{aligned} G(X) &= B_1(X) \cdot Q(X) + B_2(X) \cdot [P(X) - Q(X) \cdot S(X)] \\ &= B_2(X) \cdot P(X) + [B_1(X) - B_2(X) \cdot S(X)] \cdot Q. \end{aligned}$$

Por tanto

$$G(X) \in [P(X), Q(X)] .$$

Luego

$$[Q(X), R(X)] \subset [P(X), Q(X)]$$

Teniendo en cuenta que

$$[P(X), Q(X)] \subset [Q(X), R(X)]$$

y que

$$[Q(X), R(X)] \subset [P(X), Q(X)] ,$$

entonces

$$[P(X), Q(X)] = [Q(X), R(X)] .$$

□

Nota 4.7.2. *Si seguimos con este procedimiento llegamos a obtener resto nulo y, por tanto, el polinomio generador del ideal.*

Además hemos visto que dicho polinomio es el máximo común divisor. Si $D(X)$ es el máximo común divisor de $P(X)$ y $Q(X)$, entonces

$$[D(X)] = [P(X), Q(X)] .$$

Por tanto

$$P(X) = Q(X) \cdot S_0(X) + R_0(X) \Longrightarrow [P(X), Q(X)] = [Q(X), R_0(X)]$$

$$Q(X) = R_0(X) \cdot S_1(X) + R_1(X) \Longrightarrow [Q(X), R_0(X)] = [R_0(X), R_1(X)]$$

$$R_0(X) = R_1(X) \cdot S_2(X) + R_2(X) \Longrightarrow [R_0(X), R_1(X)] = [R_1(X), R_2(X)]$$

$$\vdots \qquad\qquad \vdots$$

$$\begin{aligned} R_{i-1}(X) = R_i(X) \cdot S_{i+1}(X) + R_{i+1}(X) \Longrightarrow \\ [R_{i-1}(X), R_i(X)] = [R_i(X), R_{i+1}(X)] \end{aligned}$$

$$R_i(X) = R_{i+1}(X) \cdot S_{i+2}(X) + 0 \Longrightarrow$$
$$[R_i(X), R_{i+1}(X)] = [R_{i+1}(X)] = [P(X), Q(X)]\,.$$

Entonces $R_{i+1}(X)$ es el máximo común divisor de $P(X)$ y $Q(X)$.

Observación 4.7.3. *El procedimiento es equivalente al algoritmo de Euclides para números enteros.*

Ejemplo 4.7.4. Calcular $\mathrm{mcd}(480, 324)$. Tenemos que

$$480 = 1 \cdot 324 + 156$$
$$324 = 2 \cdot 156 + 12$$
$$156 = 13 \cdot 12 + 0$$

Por tanto

$$\mathrm{mcd}(480, 324) = 12.$$

Ejemplo 4.7.5. Calcular $\mathrm{mcd}(X^4 + 3X^3 + 3X^2 + X + 2, X^3 + 2X^2 + 1)$ en $\mathbb{Q}[X]$. Tenemos que

$$X^4 + 3X^3 + 3X^2 + X + 2 = (X + 1) \cdot (X^3 + 2X^2 + 1) + (X^2 + 1)$$

$$X^3 + 2X^2 + 1 = (X + 2) \cdot (X^2 + 1) + (-X - 1)$$

$$X^2 + 1 = (-X + 1) \cdot (-X - 1) + 2$$

$$-X - 1 = \Big(-\frac{1}{2}X - \frac{1}{2}\Big) \cdot 2 + 0$$

Por lo tanto, tenemos

$$\mathrm{mcd}(X^4 + 3X^3 + 3X^2 + X + 2, X^3 + 2X^2 + 1) = 2,$$

como $\mathbb{Q}$ es un cuerpo, podemos normalizar para obtener el polinomio mónico, así que

$$\mathrm{mcd}(X^4 + 3X^3 + 3X^2 + X + 2, X^3 + 2X^2 + 1) = 1.$$

Ejemplo 4.7.6. Calcular $\mathrm{mcd}(X^3 + X^2 + X + 1, X^2 + 2)$ en $\mathbb{Z}_3[X]$. Tenemos que

$$X^3 + X^2 + X + 1 = (X + 1) \cdot (X^2 + 2) + (2X + 2)$$

$$X^2 + 2 = (2X + 1) \cdot (2X + 2) + 0$$

Por tanto

$$\mathrm{mcd}(X^3+X^2+X+1, X^2+2) = X+1,$$

lo hemos hecho mónico (normalizado), ya que $\mathbb{Z}_3$ es cuerpo. Para normalizarlo hemos multiplicado por 2.

Observación 4.7.7. *Si $D(X)$ es el máximo común divisor de $P(X)$ y $Q(X)$, entonces*

$$[D(X)] = [P(X), Q(X)]\,.$$

Por lo tanto

$$D(X) \in [P(X), Q(X)]\,.$$

Así que existen $A_1(X), A_2(X) \in A[X]$ tales que

$$D(X) = A_1(X)\cdot P(X) + A_2(X)\cdot Q(X).$$

Ejemplo 4.7.8. Usando los polinomios del ejemplo anterior:

1) $X^3+X^2+X+1 = (X+1)(X^2+2)+2X+2$ entonces

$$X^3+X^2+X+1-(X+1)(X^2+2) = 2X+2.$$

Por tanto

$$X+1 = 2\cdot\overbrace{(X^3+X^2+X+1)}^{P(X)} + (X+1)\cdot\overbrace{(X^2+2)}^{Q(X)}$$

2) $X^2+2 = (2X+1)\cdot(2X+2) = 2X\cdot(2X+2)+(2X+2)$, entonces

$$X^2+2-2X\cdot(2X+2) = 2X+2.$$

Por tanto

$$\begin{aligned} 2X+2 &= X^2+2+X(2X+2)\\ &= X^2+2+X[(X^3+X^2+X+1)+2(X+1)(X^2+2)]\\ &= (X^2+2)[1+2X(X+1)]+(X^3+X^2+X+1)X \end{aligned}$$

Así que

$$X+1 = [2+X(X+1)](X^2+2)+2X(X^3+X^2+X+1).$$

Luego

$$X+1 = (X^2+X+2)\overbrace{(X^2+2)}^{Q(X)} + 2X\overbrace{(X^3+X^2+X+1)}^{P(X)}$$

Podemos ver que la descomposición no es única.

4.8. Raíces de un polinomio

Definición 4.8.1. *Sea A un anillo y $P \in A[X]$, se dice que $a \in A$ es una **raíz** de $P(X)$ si $P(a) = 0$.*

Definición 4.8.2 (**Multiplicidad de un raíz**). *Sea C un cuerpo y $P \in C[X]$. Si $(X-a)^n$ con $n \in \mathbb{N}$ divide a $P(X)$ y $(X-a)^{n+1}$ no divide a $P(X)$, se dice que la raíz a tiene **multiplicidad** n.*

Ejemplo 4.8.3. $a = 1$ tiene multiplicidad 1 para $P(X) = X^2 - 1$ en $\mathbb{Q}[X]$ y multiplicidad 2 para $Q(X) = X^2 - 2X + 1$ en $\mathbb{Q}[X]$.

Proposición 4.8.4. *Sea A un cuerpo, dado el polinomio $P(X) \in A[X]$ con* $\text{grado}(P(X)) = n \geq 1$*, entonces $P(X)$ tiene a lo sumo n raíces en $A[X]$ contando cada raíz tantas veces como indica su multiplicidad.*

Demostración. Supongamos que $P(X)$ tiene m raíces, $a_1, a_2, \cdots, a_m$, por lo tanto $(X - a_i)|P(X), i = 1, \ldots, m$ entones

$$P(X) = (X - a_1) \cdot (X - a_2) \cdots (X - a_m) \cdot B(X)$$

con $B(X) \in A[X]$, como

$$\text{grado}(P(X)) = m + \text{grado}(B(X))$$

se tiene que

$$n = m + \text{grado}(B(X))$$

por tanto

$$n \geq m.$$

Luego, el número de raíces es menor o igual que el grado. □

Observación 4.8.5. *Es necesario imponer que A sea un cuerpo para que se cumpla la proposición anterior ya que, por ejemplo,*

$$P(X) = (X - 2)(X - 3)$$

en $\mathbb{Z}_6[X]$ tiene como raíces 2 y 3 pero también 0 y 5, mientras que $\text{grado}(P(X)) = 2$ *(esto es debido a que $\mathbb{Z}_6$ no es un cuerpo, por tanto $\mathbb{Z}_6[X]$ no es dominio de integridad).*

4.9. Polinomio irreducible

Definición 4.9.1. *Sea A un anillo conmutativo con unidad, un polinomio $P(X) \in A[X]$ que no sea invertible en $A[X]$ se dice que es* ***irreducible*** *en $A[X]$ si para toda descomposición de la forma*

$$P(X) = Q(X) \cdot S(X)$$

con $Q(X), S(X) \in A[X]$, se tiene que o bien $Q(X)$ o bien $S(X)$ son una unidad de $A[X]$.

Un polinomio que no es irreducible, se dice ***reducible****.*

Ejemplo 4.9.2. $P(X) = X^2 - 2$ es irreducible en $\mathbb{Q}[X]$, pero no en $\mathbb{R}[X]$, ya que

$$P(X) = (X - \sqrt{2})(X + \sqrt{2}).$$

Ejemplo 4.9.3. $P(X) = X^2 + 1$ es irreducible en $\mathbb{Q}[X]$ y en $\mathbb{R}[X]$, pero no $\mathbb{C}[X]$, ya que podemos escribir

$$P(X) = (X + i)(X - i),$$

ni en $\mathbb{Z}_5[X]$ ya que

$$P(X) = (X - 2)(X + 2)$$

en $\mathbb{Z}_5[X]$.

Observación 4.9.4. *Los polinomios irreducibles en un anillo de polinomios juegan el mismo papel que los números primos.*

Proposición 4.9.5. *Todo polinomio $P(X) \in A[X]$ de grado mayor que 0 es producto de polinomios irreducibles.*

Demostración.

1) Si $P(X)$ es irreducible, ya está hecha la factorización.

2) Si $P(X)$ es reducible, tiene divisores de grado menor, entonces $P(X) = A_1(X) \cdot P_1(X)$.

   Se repite el proceso hasta obtener un producto de polinomios irreducibles.

□

4.9.1. Irreducibilidad en $\mathbb{C}[X]$

Teorema 4.9.6 (Teorema fundamental del Álgebra). *Todo polinomio $P(X) \in \mathbb{C}[X]$ no constante tiene al menos una raíz en $\mathbb{C}$.*

Proposición 4.9.7. *Todo polinomio $P(X) \in \mathbb{C}[X]$ con $\text{grado}(P(X)) = n \geq 1$ tiene n raíces en $\mathbb{C}[X]$ (contando multiplicidad).*

Proposición 4.9.8. *Un polinomio $P(X) \in \mathbb{C}[X]$ es irreducible en $\mathbb{C}[X]$ si y sólo si tiene grado 1.*

Observación 4.9.9. *Dado $P(X) \in \mathbb{C}[X]$ con $\text{grado}(P(X)) = n$, entonces $P(X) = k(X - a_1)(X - a_2)\cdots(X - a_n)$ con $k \in \mathbb{C}$ y $a_i \in \mathbb{C}, i = 1, \ldots, n$ raíces de $P(X)$.*

4.9.2. Irreducibilidad en $\mathbb{R}[X]$

Proposición 4.9.10. *Si $P(X) \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$, su grado es 1 ó 2. Además si su grado es 2 y $P(X)$ es irreducible, entonces $P(X) = aX^2 + bX + c$ cumple que $\Delta = b^2 - 4ac < 0$.*

Ejemplo 4.9.11.

1) $P(X) = X^2 + 2X + 1$ es reducible en $\mathbb{R}[X]$ ya que $b^2 - 4ac > 0$ entonces $P(X) = (X + 1)^2$.

2) $P(X) = X^2 - 2X + 2$ es irreducible en $\mathbb{R}[X]$ ya que $b^2 - 4ac < 0$ entonces $P(X) = [X - (1 + i)][X - (1 - i)]$.

4.9.3. Irreducibilidad en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$

Proposición 4.9.12. *Sea $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Q}[X]$ un polinomio con coeficientes en $\mathbb{Z}$.*

Si $\dfrac{a}{b}$ es una raíz de $P(X)$ con a y b primos entre sí ($a, b \in \mathbb{Z}$), entonces $a|a_0$ y $b|a_n$.

Observación 4.9.13. *Si a es una raíz entera de $P(X)$, entonces $a|a_0$.*

Observación 4.9.14. *Un polinomio $P(X)$ mónico ($a_n = 1$) con coeficientes enteros no tiene raíces fraccionarias.*

4.9.4. Irreducibilidad en $\mathbb{Z}_p[X]$

Proposición 4.9.15. *Existen p polinomios lineales irreducibles mónico en $\mathbb{Z}_p[X]$ (con p primo) de la forma $X + a$.*

Ejemplo 4.9.16. En $\mathbb{Z}_3[X]$ los polinomios lineales irreducibles mónicos son $X, X + 1, X + 2$.

Proposición 4.9.17. *Existen $\dfrac{p^2 - p}{2}$ polinomios cuadráticos mónicos irreducibles en $\mathbb{Z}_p[X]$ (con p primo).*

Ejemplo 4.9.18. En $\mathbb{Z}_3[X]$ habrá $\dfrac{9-3}{2} = 3$ polinomios cuadráticos irreducibles: $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$.