

# Álgebra

José Cuevas Barrientos

3 de mayo de 2021



---

## Índice general

---

	INTRODUCCIÓN . . . . .	V
<b>I</b>	<b>Álgebra abstracta</b>	<b>1</b>
1	TEORÍA DE GRUPOS . . . . .	3
1.1	Teoría elemental de números . . . . .	3
1.2	Estructuras algebraicas . . . . .	10
1.3	Representaciones de grupos finitos . . . . .	18
1.3.1	Productos de grupos . . . . .	19
1.3.2	Teoremas de isomorfismos y categorías . . . . .	21
1.3.3	Ecuación de clases y $p$ -grupos . . . . .	24
1.4	Teoremas de Sylow . . . . .	25
1.4.1	Acciones . . . . .	25
1.4.2	Teoremas de Sylow . . . . .	28
1.5	Grupos resolubles . . . . .	31
1.6	Grupo simétrico . . . . .	33
1.6.1	Signo de una permutación . . . . .	35
1.6.2	Grupos alternantes y diedrales . . . . .	37
2	ANILLOS Y CUERPOS . . . . .	41
2.1	Definiciones elementales . . . . .	41
2.2	Divisibilidad en anillos . . . . .	48
2.3	Polinomios . . . . .	53
2.4	Divisibilidad de polinomios . . . . .	59
2.4.1	Raíces básicas . . . . .	63
2.5	Números complejos . . . . .	64
2.5.1	El teorema fundamental del álgebra I . . . . .	67

<b>II</b>	<b>Álgebra lineal</b>	<b>69</b>
3	MÓDULOS . . . . .	71
	3.1 Módulos y vectores . . . . .	71
	3.2 Módulos libres y bases . . . . .	75
	3.2.1 Finitamente generados . . . . .	75
	3.2.2 Espacios de dimensión infinita . . . . .	77
	3.2.3 Fórmulas con la dimensión . . . . .	79
	3.3 Matrices y transformaciones lineales . . . . .	81
	3.4 Determinante . . . . .	86
4	EXTENSIONES DE CUERPO . . . . .	91
	4.1 Extensiones algebraicas y transcendentales . . . . .	91
5	ÁLGEBRA LINEAL . . . . .	97
	5.1 Diagonalización . . . . .	97
	ÍNDICE DE NOTACIÓN . . . . .	101
	ÍNDICE ALFABÉTICO . . . . .	105
	BIBLIOGRAFÍA . . . . .	109
	Álgebra abstracta . . . . .	109
	Álgebra lineal . . . . .	109
	Artículos . . . . .	110

---

## Introducción

---

El álgebra es el estudio de las estructuras matemáticas, esto es, conjuntos dotados de relaciones y/u operaciones que satisfacen una serie de condiciones que lo dotan de una *forma*. Ésto tal vez en principio difiera con la imagen que uno pueda tener del álgebra, pero hay varias consideraciones que tener de esta sentencia, por ejemplo, las estructuras son bastante comunes, los conjuntos numéricos son el ejemplo más importante, de hecho, abren la puerta a una pregunta más fundamental: ¿qué es un número? El lector puede creer que esto es una pregunta trivial ya que conoce números como 1, 0,  $\pi$  o  $\sqrt{2}$ . ¿Y qué hay de  $\emptyset$ ? No, ésto es un conjunto. Sin embargo, von Neumann propone construir el conjunto de los naturales usando al conjunto vacío  $\emptyset$  como sinónimo del 0. En efecto, la teoría de conjuntos nos otorga “materiales” bajo los cuales construimos todo nuestro universo de objetos, en consecuencia los números como tal no han de ser más que conjuntos, luego no es la “composición” del objeto lo que determina su cualidad de número o no.

Veamos otra característica, podríamos decir que el 1 se define como el sucesor del 0 en los naturales. Ésta definición es independiente de cómo definamos 0 o 1, ya sea con conjuntos conocidos o raros, pero sino de cómo se relacionan los elementos de éste conjunto. En este sentido, el conjunto  $S := \{1, 0, \pi, \sqrt{2}\}$  no es numérico, ya que carece de propiedades básicas como que  $\pi + \pi = 2\pi \notin S$  (a menos claro que redefinamos  $+$  para  $S$ ). Pero ésto conlleva a una apreciación elemental,  $S$  puede ser numérico dependiendo de cómo se definen sus operaciones; a ésto es lo que se le dice una *estructura*. Ésto también nos obliga a definir una manera de decir que dos estructuras tienen la misma forma, pero pueden definir en composición, un ejemplo sería encontrar un método para señalar que los conjuntos  $\{0, 1, 2, \dots\}$  y  $\{\text{cero},$

uno, dos, ... } son, en esencia, la misma estructura. La sentencia empleada para señalar este hecho es “las estructuras son isomorfas”. Por supuesto cabe preguntarse ¿la misma estructura en qué sentido? Pues los conjuntos pueden “concordar” en la suma, pero “diferir” en el producto, a lo que se le añade un apellido al término de isomorfismo, por ejemplo: son isomorfas en orden, o isomorfas como espacios vectoriales, etc. Con éste preámbulo, el rol del álgebra se ve más claro, y también se comprende una división del álgebra respecto de las estructuras que estudia.

Para muchos fines, una de las estructuras más básicas (en términos de condiciones) son los *grupos* al que dedicamos un largo capítulo para ver en detalle. Algo de lo que el lector se va a percatar es que mientras más básicas sean las estructuras, más libertades poseen de modo que su estudio suele o verse fragmentado (según añadir más condiciones, como finitud o conmutatividad) o simplemente no puede profundizar demasiado; como es el caso con la teoría nativa de conjuntos, que eventualmente rota entre otros temas más específicos como números ordinales o cardinales para tener más información, pero es aún muy amplia en contextos genéricos, como el axioma de elección demuestra. Al igual que la teoría de conjuntos es vital para comprender o leer otros conceptos en matemáticas, la teoría de grupos es vital para escribir el resto del álgebra. A veces puede sentirse como innecesaria, pero vuelve en contextos inesperados, como en el grupo especial en la teoría de matrices, o el grupo de Galois en la teoría de extensión de cuerpos.

Parte I.

---

# ÁLGEBRA ABSTRACTA

---





# 1

---

## Teoría de grupos

---

Comenzaremos el capítulo con dar una breve introducción a la teoría de números, la cual servirá tanto para ilustrar como para poder definir ciertos conceptos que nos serán útiles.

### 1.1. Teoría elemental de números

Comenzaremos por una aplicación directa del principio del buen ordenamiento de  $\mathbb{N}$ :

**Teorema 1.1 – Algoritmo de la división:** Dados cualesquiera  $a, b \in \mathbb{Z}$  con  $a > 0$ , existen unos únicos números  $q, r \in \mathbb{Z}$  tales que

$$b = aq + r, \quad 0 \leq r < a$$

DEMOSTRACIÓN: Vamos a definir un conjunto

$$S = \{x \in \mathbb{N} : x = b - an, \quad n \in \mathbb{Z}\}$$

y veremos que es no vacío.

Si  $b \geq 0$  entonces para  $n = 0$  se obtiene  $x = b - a \cdot 0 = b \geq 0$  luego  $b \in S$ .

Si  $b < 0$  entonces, como  $a$  es entero positivo, luego  $a \geq 1$ , multiplicando por  $-b$  obtenemos

$$-ab \geq -b \implies x = b - ab \geq 0,$$

finalmente  $x \in S$ , es decir,  $S$  es siempre no vacío.

Por axioma del buen orden,  $S$  posee mínimo al que denotaremos como

$$r = b - aq.$$

Ahora hemos de probar la desigualdad con  $r$ . Supongamos que (como  $r$  es natural) por contradicción  $r \geq a$ , luego  $r - a = b - aq - a = b - a(q + 1) \geq 0$ , por lo tanto,  $r - a \in S$ , lo que contradice el que nuestro  $r$  sea el mínimo elemento.

Finalmente probaremos la unicidad suponiendo que existen múltiples  $r_1, r_2$  y  $q_1, q_2$  que satisfacen, la ecuación, luego

$$aq_1 + r_1 = aq_2 + r_2,$$

supongamos que  $r_2 \geq r_1$  es positivo, luego

$$r_2 - r_1 = a(q_1 - q_2)$$

como  $a$  es positivo y entero,  $q_1 - q_2$  debe ser también entero positivo. Luego  $r_2 - r_1$  debe ser múltiplo de  $a$ , sin embargo, como

$$0 \leq r_1 \leq r_2 < a,$$

entonces debe ser cero; con lo cual se concluye que  $q_1 = q_2$ .  $\square$

A tal  $q$  en el algoritmo se le dice “cociente”, mientras que a  $r$  se le denomina “resto”.

**Definición 1.2 – Divisibilidad:** Sean  $a, b \in \mathbb{Z}$  (léase “ $a$  y  $b$  enteros”), escribiremos  $a \mid b$  (léase “ $a$  divide a  $b$ ”, “ $b$  es múltiplo de  $a$ ” o “ $a$  es un divisor de  $b$ ”) si y sólo si existe un entero  $q$  tal que  $b = aq$ .

**Teorema 1.3:** La divisibilidad en los naturales es una relación de orden parcial.

DEMOSTRACIÓN: Es claro que es reflexiva. La transitividad es sencilla, pues

$$a \mid b \wedge b \mid c \iff b = aq_1 \wedge c = bq_2 \implies c = (aq_1)q_2 = a(q_1q_2) \implies a \mid c.$$

La antisimetría es la más difícil, pero nótese que si  $b = aq_1$  con  $q_1 \in \mathbb{N}$ , entonces  $b \geq a$  y  $\leq$  (y  $\geq$  también) es una relación de orden total, lo que significa que es antisimétrica.

También podemos ver que no es de orden total puesto que  $2 \nmid 3$  y  $3 \nmid 2$ .  $\square$

Por ejemplo  $2 \mid 10$  o  $3 \mid 6$ .

**Teorema 1.4:** Sean  $a, b, c \in \mathbb{Z}$  con  $a \neq 0$  entonces:

1.  $a \mid 0$ ,  $a \mid ka$  y  $1 \mid a$  para todo  $k \in \mathbb{Z}$ .
2.  $a \mid b$  y  $c \mid d$  implican  $ac \mid bd$ .
3.  $a \mid b$  y  $b \mid c$  implican  $a \mid c$ .
4.  $a \mid b$  y  $a \mid c$  implican  $a \mid ub + vc$ , donde  $u, v \in \mathbb{Z}$ .
5.  $a \mid b$  con  $a, b$  positivos implica  $a \leq b$ .
6.  $a \mid b$  y  $b \mid a$  implican  $|a| = |b|$ .

DEMOSTRACIÓN: Probaremos el 4:

Por construcción existen  $q_1, q_2 \in \mathbb{Z}$  tales que  $b = aq_1$  y  $c = aq_2$ , finalmente  $ub + vc = uaq_1 + vaq_2 = a(uq_1 + vq_2)$ .  $\square$

**Definición 1.5 – Máximo común divisor.** Dados  $a, b \in \mathbb{Z}$  definimos el máximo común divisor  $M = (a; b)$  (a veces denotado como  $\text{mcd}(a, b)$ ) como aquel que satisface:

- a)  $M \mid a$  y  $M \mid b$ .
- b) Si  $c \mid a$  y  $c \mid b$  entonces  $c \leq M$ .

Cabe destacar que el máximo común divisor no es una *función ordenada*, es decir,  $(a; b) = (b; a)$ .

**Teorema 1.6:** Sean  $a, b, k \in \mathbb{Z}$  no nulos, entonces

- a)  $(a; b) = (-a; b) = (-a; -b) = (|a|; |b|)$ .
- b)  $(ak; bk) = |k|(a; b)$ .
- c)  $(a; b) = d$ .  $(a/d; b/d) = 1$ .

**Lema 1.7:** Sean  $a, b \in \mathbb{Z}$  tales que  $b = aq + r$ , entonces  $(a; b) = (a; r)$ .

DEMOSTRACIÓN: Sean  $k = (a; b)$  y  $l = (a; r)$ . Es fácil ver que como  $r = b - aq$ , entonces  $k \mid r$  por definición  $k \leq l$ . Asimismo, se deduce que  $k \geq l$ ; con lo cual  $k = l$ .  $\square$

**Teorema 1.8 (Algoritmo de Euclides):** Sean  $a, b \in \mathbb{Z}$ , una forma de calcular  $(a; b)$  es a través del siguiente método:

$$\begin{aligned} b &= aq_1 + r_1, & 0 < r_1 < a \\ a &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_n &= r_{n+1}q_{n+2}, \end{aligned}$$

dónde  $r_{n+1} = (a; b)$ .

Tomemos dos números cualesquiera: 288 y 560, e intentemos aplicar al método de Euclides:

$$560 = 288 \cdot 1 + 272$$

$$288 = 272 \cdot 1 + 16$$

$$272 = 16 \cdot 17$$

por lo tanto  $16 = (288; 560)$ .

**Teorema 1.9 – Identidad de Bézout:** Para todo  $a, b \in \mathbb{Z}$  existen  $x, y \in \mathbb{Z}$  tales que  $(a; b) = ax + by$ .

DEMOSTRACIÓN: Definamos el conjunto

$$S = \{z > 0 : z = ax + by, \quad x, y \in \mathbb{Z}\}$$

veamos que no es vacío. Pues  $a^2 + b^2 \in S$ . Por principio del buen ordenamiento posee mínimo  $g = ax_0 + by_0$ .

Podemos ver que  $g$  divide a  $a$  y a  $b$  pues

$$a = qg + r, \quad 0 \leq r < g$$

con lo cual

$$\begin{aligned} r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + by_0 \in S \end{aligned}$$

Si  $r \neq 0$  entonces se contradice con que  $g$  era el menor.

Como  $g$  es un divisor común de  $a, b$  se concluye que  $g \leq d = (a; b)$ .

Como  $d \mid a$ ,  $d \mid b$ , entonces  $d \mid ax_0 + by_0 = g$ . Al ser ambos positivos,  $d \leq g$ . Por antisimetría  $d = g$ . □

**Definición 1.10 – Números coprimos y primos:** Decimos que  $a, b \in \mathbb{Z}$  son *coprimos* si  $(a; b) = 1$ . Un número primo  $p$  es aquel que es positivo y sólo posee dos divisores naturales: el 1 y  $p$ . Los números que son el producto de números primos son llamados *compuestos*.

Nótese que como los números primos por definición poseen dos divisores, el 1 no es primo, pero tampoco cumple con la condición para ser compuesto. Más adelante veremos que es el único natural que posee esta propiedad.

**Teorema 1.11:** Sea  $p$  un número primo tal que  $p \nmid a$  entonces  $p, a$  son coprimos.

DEMOSTRACIÓN: Por definición  $d = (p; a)$  cumple  $d \mid p$ , luego  $d \mid 1$  o  $d \mid p$ . Como  $d \mid a$  y  $p \nmid a$  entonces  $d \nmid p$ , es decir,  $d \mid 1$ .  $\square$

Esto podríamos haberlo utilizado como definición auxiliar de *primo*.

**Teorema 1.12:** Si se encuentran  $u, v \in \mathbb{Z}$  tales que

$$ua + vb = 1,$$

entonces  $a, b$  son coprimos.

DEMOSTRACIÓN: Considere la prueba anterior, demostramos que el mínimo del conjunto equivale al máximo común divisor, como dicho conjunto admite únicamente valores positivos, el mínimo valor posible es 1, de ser obtenido, es inmediato que equivale al mcd.  $\square$

**Teorema 1.13 – Lema de Euclides:** Sea  $a \mid bc$  con  $a, b$  coprimos; entonces  $a \mid c$ .

DEMOSTRACIÓN: Por identidad de Bézout,  $1 = ax_0 + by_0$ , por lo tanto,  $c = ax_0c + by_0c$ . Evidentemente  $a \mid ax_0c$  y por construcción  $a \mid y_0bc$ , luego  $a \mid ax_0c + by_0c = c$ .  $\square$

Más adelante nos referiremos a esta propiedad como “ley de cancelación”.

**Teorema 1.14:** Sea  $(a; b) = 1$  y  $(a; c) = 1$ , entonces  $(a; bc) = 1$ .

DEMOSTRACIÓN: Digamos que  $d = (a; bc)$ . Como  $d \mid a$  y  $(a; b) = 1$ , se obtiene que  $(d; b) = 1$ . Por lema de Euclides  $d \mid c$ . Y como  $(a; c) = 1$  entonces  $d = 1$ .  $\square$

**Teorema 1.15:** Sea  $p$  primo tal que  $p \mid ab$  entonces  $p \mid a$  o  $p \mid b$ . Más aún, si  $p \mid a_1 \cdots a_n$ , entonces divide a por lo menos uno de los  $a_i$ .

DEMOSTRACIÓN: Probaremos la primera proposición. Si  $p \mid ab$  pero  $p \nmid a$ , lo que implica  $(p; a) = 1$ , por lema de Euclides,  $p \mid b$ . El resto es por inducción.  $\square$

**Teorema 1.16 – Teorema fundamental de la aritmética:** Todo número natural mayor que 1 es o primo o compuesto y puede escribirse como un único producto de números de primos (descomposición prima).

DEMOSTRACIÓN: Primero probaremos que todo número o es primo o es compuesto. Supongamos que tenemos el siguiente conjunto

$$S = \{n \in \mathbb{N} : n > 1 \text{ y } n \text{ es primo o compuesto}\},$$

probaremos que contiene a todo  $n > 1$  por inducción. Evidentemente  $2 \in S$ . Si  $n + 1$  es primo entonces pertenece a  $S$ , sino, puede escribirse como  $n + 1 = ab$  donde como  $a \mid n + 1$  se cumple que  $a \leq n + 1$  y  $b \leq n + 1$ , luego  $a, b \in S$ ; es decir,  $a, b$  o son primos o son producto de primos, por lo tanto,  $n + 1$  es compuesto.

Ahora probaremos que la descomposición prima es única. Supongamos que no lo fuese y hubiesen dos posibles descomposiciones primas:

$$n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n$$

donde  $p_1 \leq p_2 \leq \cdots \leq p_n$  y  $q_1 \leq q_2 \leq \cdots \leq q_n$ . Luego  $p_1 \mid q_1 q_2 \cdots q_n$ . Por ser primo,  $p_1 \mid q_i$  para algún  $1 \leq i \leq n$ , es decir,  $p_1 \leq q_i$ . Por simetría  $q_1 \mid p_1 \cdots p_n$  y  $q_1 \leq p_1$ . Como  $p_1 = q_1$ . Luego podemos aplicar el mismo método sobre

$$\frac{n}{p_1} = p_2 \cdots p_n = q_2 \cdots q_n$$

para ver que, por inducción,  $p_1 = q_1, p_2 = q_2, \dots, p_n = q_n$ . Es decir, la factorización es única.  $\square$

**Teorema 1.17:** Los números primos son infinitos.

DEMOSTRACIÓN: Supongamos por contradicción que los primos fueran finitos, entonces podríamos hacer una lista de todos ellos como prosigue:

$$P := \{p_1, p_2, \dots, p_n\},$$

como nos hemos asegurado que  $p_i$  es positivo y mayor que 1, es fácil ver que si  $p_i \mid c$  entonces  $p_i \nmid c + 1$ . Finalmente el número

$$c = p_1 \cdot p_2 \cdots p_n + 1$$

no sería divisible por ningún de los primos en nuestra lista, y por lo tanto, por ningún otro número más que si mismo y el 1; es decir,  $c$  sería primo, contradiciendo que los habíamos organizado en una lista.  $\square$

También, suele ser necesario tener que confirmar si un número es primo, por lo cual, hay varias formas, la primera es **la criba de Eratóstenes** que consiste en denotar los números de 2 hasta  $n$  y comenzar tachando los múltiplos de los primos, los no tachados resultan ser primos:

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

pero considera que si queremos ver si  $n$  es primo debemos comprobar que no sea divisible por ningún número entre 2 y  $n - 1$  (lo cuál es un proceso terriblemente ineficiente). Por lo cuál, el truco está en probar **sólo** los números primos, del 2 hasta  $\sqrt{n}$ .

**Definición 1.18 – Orden  $p$ -ádico:** Sea  $n$  un número mayor a 1 y  $p$  un número primo, entonces diremos que su orden  $p$ -ádico  $\nu_p(n)$  es el natural tal que  $p^\nu \mid n$ , pero  $p^{\nu+1} \nmid n$ .

Una identidad muy interesante, y que puede ser de mucho uso es que si  $\tau(n)$  es la función que calcula la cantidad de divisores que tiene un natural  $n$ .

**Teorema 1.19:** Sea  $n > 1$  un número natural, divisible por los primos  $p_1, \dots, p_m$ . Entonces

$$\tau(n) = (\nu_{p_1}(n) + 1)(\nu_{p_2}(n) + 1) \cdots (\nu_{p_m}(n) + 1) = \prod_{p \mid n} (\nu_p(n) + 1).$$

DEMOSTRACIÓN: Nótese que todos los divisores de  $n$  resultan ser combinaciones de la forma

$$\prod_{i=1}^m p_i^{\beta_i}$$

dónde  $0 \leq \beta_i \leq \nu_{p_i}(n)$ . Por lo que es fácil ver que  $\beta_i$  posee  $(\nu_{p_i}(n) + 1)$  posibles valores, por ende, la fórmula del enunciado.  $\square$

**Definición 1.20 – Congruencia modular:** Se dice que dos enteros  $a, b$  son congruentes en módulo  $n \geq 2$  natural syss  $a - b \mid n$ , en cuyo caso demotaremos  $a \equiv b \pmod{n}$ . En general escribiremos  $\mathbb{Z}_n$  o  $\mathbb{Z}/n\mathbb{Z}$  al conjunto cociente dado por la congruencia en módulo  $n$ .

Cabe destacar que con lo que hemos probado sigue que la congruencia es una relación de equivalencia sin importar el  $n$  elegido. Nótese que bajo la misma definición las congruencias en módulo  $n$  o  $-n$  concuerdan. ¿Por qué excluir al 1 y al 0 entonces?

**Proposición 1.21:** Sean  $a \equiv b, c \equiv d$  en módulo  $n$  y  $m \in \mathbb{N}$  entonces:

1.  $a + c \equiv b + d$ .
2.  $ac \equiv bd$ .
3.  $a^m \equiv b^m$ .

Además, si el módulo es  $p$  primo y  $a \neq 0$  entonces existe  $b$  tal que  $ab \equiv 1$ .

HINT: El último sale con la identidad de Bézout.

De ahora en adelante se admite que  $\mathbb{Z}_p$  representa  $\mathbb{Z}/p\mathbb{Z}$  con  $p$  primo. Esta distinción es por la propiedad de que los elementos no nulos de  $\mathbb{Z}_p$  poseen inverso multiplicativo.

## 1.2. Estructuras algebraicas

En el libro sobre teoría de conjuntos vimos como mediante variados modelos se pueden formalizar las matemáticas mediante el objeto de los conjuntos (o las clases). No obstante, varios matemáticos (incluidos Cantor mismo) describen a estos elementos como *amorfos* en el sentido de que podrían ser o representar cualquier cosa sin ninguna clase de patrón e importancia. En este sentido surge el concepto de las *estructuras algebraicas*, como conjuntos



dotados de propiedades que generan objetos que resultan de interés y que son manejables. Se comenzará este libro analizando una de las estructuras más básicas (pero no menos importantes o interesantes):

**Definición 1.22 – Grupos:** Una función  $\cdot : G^2 \rightarrow G$  sobre un conjunto  $G$  se dice que cumple:

**Asociatividad** Para todo  $x, y, z \in G$  se cumple  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

**Elemento neutro** Existe  $e \in G$  tal que para todo  $x \in G$  se cumple  $e \cdot x = x \cdot e = x$ .

**Conmutatividad** Para todo  $x, y \in G$  se cumple  $x \cdot y = y \cdot x$ .

Además se dice que un elemento  $x \in G$  es *invertible* (donde  $G$  posee neutro  $e$ ) si existe  $y \in G$  tal que  $x \cdot y = y \cdot x = e$ , en cuyo caso al  $y$  le decimos una *inversa* de  $x$ .

Un par  $(G, \cdot)$  se dice:

**Semigrupo** Si  $\cdot$  es asociativa.

**Monoide** Si  $(G, \cdot)$  es semigrupo y posee neutro.

**Grupo** Si  $(G, \cdot)$  es monoide y todo elemento es invertible.

Además se agrega el sufijo *conmutativo* o *abeliano* si  $(G, \cdot)$  es conmutativo.

De aquí en adelante abreviaremos  $xy = x \cdot y$ .

Dentro del libro de teoría de conjuntos se demuestra que  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$  y  $(\mathbb{Q}_{\neq 0}, \cdot)$  son grupos abelianos. En la sección anterior vimos que  $(\mathbb{Z}_n, +)$  también lo es y que  $(\mathbb{Z}_p \setminus \{0\}, \cdot)$  también (¿por qué importa en el último caso que  $p$  sea primo?).

Además dado un conjunto  $X$  no vacío, el conjunto de las biyecciones de  $X$  es también un grupo (¿por qué?).

**Teorema 1.23:** Sea  $(G, \cdot)$  una estructura algebraica:

1. Si posee elemento neutro es único.

Si es semigrupo:

2. La inversa de un elemento invertible es única, por lo que le denotamos como  $a^{-1}$ .

3. La inversa de un elemento  $a$  invertible es invertible y  $(a^{-1})^{-1} = a$ .

4. El producto de invertibles es invertible y

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

Si es grupo entonces:

5. Posee *cancelación* por la izquierda y derecha:

$$ab = ac \iff b = c, \quad ab = cb \iff a = c.$$

En virtud de este teorema, denotaremos 1 al neutro de un grupo en general para mantener la notación multiplicativa (excepto en ejemplos concretos claro).

**Proposición 1.24:** Sea  $(S, \cdot)$  un semigrupo tal que

1. Si para todo  $a, b \in S$  existen  $x, y \in S$  tales que  $ax = b$  e  $ya = b$ , entonces  $S$  es un grupo.
2. Si es finito entonces es grupo syss posee cancelación por la izquierda y la derecha.

**Definición 1.25 – Subgrupo:** Sea  $S \subseteq G$  un grupo. Se dice que  $S$  es subgrupo si  $(S, \cdot|_{S^2})$  es grupo. Si  $S$  es subgrupo de  $G$  escribiremos  $S \leq G$ .

Notemos que  $\{1\}$  siempre cumple ser un subgrupo, a éste le llamaremos subgrupo *trivial*.  $G$  mismo también es un subgrupo de  $G$ . A los subgrupos de  $G$  distintos de  $G$  y de  $\{1\}$  les diremos *propios*.

En general, dada cualquier tipo de estructura añadiremos el prefijo *sub* para indicar que es subconjunto de otra estructura con la que comparte propiedades.

**Teorema 1.26 (Criterio de subgrupos):**  $S \leq G$  syss es no vacío y para todo  $x, y \in S$  se cumple que  $xy^{-1} \in S$ .

**Corolario 1.27:** La intersección arbitraria de subgrupos es un subgrupo. Además nunca es vacía pues 1 siempre pertenece a la intersección de subgrupos.

**Definición 1.28 – Subgrupo generado:** Dado  $S \subseteq G$  se denota  $\langle S \rangle$  a

$$\langle S \rangle := \bigcap \{H : S \subseteq H \leq G\}$$

Es decir, al mínimo subgrupo (bajo la inclusión) de  $G$  que le contiene. Si  $S = \{x_1, \dots, x_n\}$  nos permitiremos abreviar  $\langle x_1, \dots, x_n \rangle := \langle S \rangle$ .

**Corolario 1.29:**  $S \leq G$  syss  $\langle S \rangle = S$ .

**Proposición 1.30:** Para todo  $x \in \langle S \rangle$ , se cumple que

$$x = x_1 x_2 \cdots x_n$$

donde para todo  $i \leq n$  se cumple que  $x_i$  o  $x_i^{-1}$  pertenece a  $S$ .

**Teorema 1.31:** Sean  $A, B \leq G$ , tales que  $A \cup B \leq G$ , entonces  $A \subseteq B$  o  $B \subseteq A$ .

DEMOSTRACIÓN: Si son iguales, entonces el resultado está probado. De lo contrario, sin pérdida de generalidad supongamos que  $a \in A \setminus B$ , demostraremos que  $B \subset A$ .

Sea  $b \in B$ , como  $A \cup B$  es grupo, entonces  $ab \in A \cup B$ , ergo,  $ab \in A$  o  $ab \in B$ . No obstante,  $ab \notin B$  pues de lo contrario como  $b^{-1} \in B$  entonces  $a \in B$ , lo que es absurdo. Como  $ab, a^{-1} \in A$  entonces  $b \in A$ .  $\square$

**Proposición 1.32:** Si  $\{H_i : i \in I\}$  es una familia de subgrupos linealmente ordenado por inclusión<sup>1</sup> entonces  $H := \bigcup_{i \in I} H_i$  es un subgrupo, y de hecho es el mínimo subgrupo que contiene a todos los  $H_i$ .

DEMOSTRACIÓN: Sea  $x, y \in H$ , por definición hay un par de subgrupos  $H_x$  y  $H_y$  en la familia tales que  $x \in H_x$  e  $y \in H_y$ . Luego como es linealmente ordenado, entonces  $H_x \subseteq H_y$  o  $H_y \subseteq H_x$ , luego  $H_z := H_x \cup H_y$  pertenece a la familia y contiene a  $x, y$ , luego  $xy^{-1} \in H_z \subseteq H$ , por lo que  $H \leq G$  por el criterio.

La parte de ser “el mínimo que contiene a la familia” queda al lector.  $\square$

<sup>1</sup>Es decir, tal que para todo  $i, j \in I$  se cumple que  $H_i \subseteq H_j$  o  $H_j \subseteq H_i$ .

**Definición 1.33 – Potencias y generadores:** Sea  $x \in G$  y  $n \in \mathbb{Z}$ , entonces se le llama  $n$ -ésima potencia de  $x$  a:

$$x^n = \begin{cases} \underbrace{x \cdot x \cdots x}_n & n > 0 \\ 1 & n = 0 \\ (x^{-1})^{-n} & n < 0 \end{cases}$$

En ciertos casos, también se denota  $nx$  en lugar de  $x^n$ . En general denotaremos  $x^n$  si la operación es  $\cdot$  y  $nx$  si la operación es  $+$ .

Se dice que  $B$  es una base si genera a  $G$ , i.e., si  $\langle B \rangle = G$ . Un grupo se dice *cíclico* si posee una base singular, cabe destacar que los grupos cíclicos son abelianos. Se define el orden de un grupo cíclico  $\langle x \rangle$  como el mínimo natural  $n$  tal que  $x^n = 1$ , de no existir ningún natural que satisfaga dicha condición se dice de orden 0. Denotaremos  $\text{ord } x$  al orden de  $x$ .

Otros textos definen el orden como el cardinal del conjunto, reflexione, por qué ambas son equivalentes para grupos cíclicos finitos.  $(\mathbb{Z}, +)$  es un ejemplo de grupo cíclico de generador 1 y de orden 0, de hecho,  $(\mathbb{Z}_n, +)$  también es cíclico de generador 1 y orden  $n$ . Nótese que  $e$  es el único elemento de orden 1.

**Teorema (AE) 1.34:** Si  $G$  tiene una base finita, entonces todo subgrupo propio está contenido en un subgrupo maximal.

DEMOSTRACIÓN: La demostración aplica el lema de Zorn. Sea  $S \subsetneq G$  y  $B := \{g_1, \dots, g_n\}$  base de  $G$ , entonces sea  $S_k := \langle S, g_1, g_2, \dots, g_k \rangle$  de modo que

$$S = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n = G.$$

Elijamos  $S_m$  como el subgrupo más grande distinto de  $G$ , luego sea

$$\mathcal{F} := \{H : S_m \leq H \subsetneq G \wedge g_{m+1} \notin H\}$$

entonces  $\mathcal{F}$  es un conjunto parcialmente ordenado por la inclusión, y toda cadena tiene supremo por la proposición anterior (1.32), luego por el lema de Zorn tiene un elemento maximal  $M$  que es subgrupo no tiene a  $g_{m+1}$  (de modo que es distinto de  $G$ ), contiene a  $S$  y es trivial ver que  $M$  es un subgrupo maximal.  $\square$

**Proposición 1.35:** Dado  $a \in G$  y  $n \in \mathbb{Z}_{\neq 0}$ , se cumple que

$$\text{ord}(a^n) = \frac{\text{ord } a}{\text{mcd}(\text{ord } a, n)} = \frac{\text{mcm}(\text{ord } a, n)}{n}.$$

**Definición 1.36 – Morfismos:** Decimos que una aplicación  $\varphi : (G, \cdot) \rightarrow (H, \star)$  entre grupos es un *morfismo* de grupos si para todo  $a, b \in G$ :

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$$

A esto se le agrega el prefijo *mono-*, *epi-* e *iso-* si es inyectiva, suprayectiva y biyectiva resp. Dos grupos se dicen *isomorfos* si existe un isomorfismo entre ambos, lo que se escribe como  $G \cong H$ . Cuando queramos decir que un morfismo es un mono- o epimorfismo diremos que es mónico o épico resp.

Si  $\varphi : G \rightarrow G$  se le añade el prefijo *endo-* y si además resulta ser biyectiva, entonces se le añade el prefijo *auto-*. Esta nomenclatura se aplica a todos los otros morfismos en álgebra.

Visualmente denotamos los monomorfismos por  $\hookrightarrow$ , los epimorfismos por  $\twoheadrightarrow$  y los isomorfismos por  $\cong$  (algunos usan  $\xrightarrow{\sim}$ ).

Es claro que la identidad es un automorfismo, y en un grupo, la función  $f(x) = x^{-1}$  lo es también. En  $(\mathbb{R}, +)$  se cumple que  $f(x) = kx$  con  $k \neq 0$  es también un automorfismo. En  $(\mathbb{Z}, +)$  la función  $f(x) = 2x$  es un endomorfismo mónico pero no épico, pues 1 no tendría preimagen.

**Teorema 1.37:** Sea  $G = \langle g \rangle$ , entonces:

1. Si es finito y  $|G| = m$ , entonces  $G = \{1, g, g^2, \dots, g^{m-1}\}$  y  $g^n = e$  syss  $m \mid n$ .
2. Si  $G$  es infinito, entonces  $(G, \cdot) \cong (\mathbb{Z}, +)$ .
3. Si  $G$  es finito, entonces  $G \cong \mathbb{Z}_m$

**Definición 1.38 – Clases laterales:** Dados dos subconjuntos  $A, B$  de  $G$ , se define

$$AB := \{xy : x \in A, y \in B\}$$

Si alguno es el conjunto singular  $A = \{a\}$ , omitiremos las llaves, de modo que  $aB := \{a\} \cdot B$  y  $Ab := A \cdot \{b\}$ .

**Lema 1.39:** Sea  $H \leq G$  y  $a, b \in G$ , entonces

1.  $a \in aH$ .
2.  $aH = bH$  o  $aH \cap bH = \emptyset$ .
3.  $a \equiv b$  (mód  $H$ ) dado por  $a^{-1}b \in H$  es una relación de equivalencia.
4.  $|aH| = |bH|$ .

DEMOSTRACIÓN: Probaremos la segunda, esto es que si no son disjuntos entonces son iguales. Sea  $c \in aH \cap bH$ , por definición,  $c = ax = by$  con  $x, y \in H$ , luego  $b = a(xy^{-1})$  donde  $xy^{-1} \in H$  por el criterio de subgrupo.  $\square$

Denotaremos  $G/H$  al conjunto cociente de  $G$  bajo la relación de equivalencia que es la congruencia módulo  $H$ . Notemos que bajo estas definiciones, la notación  $\mathbb{Z}_n$  tiene sentido.

**Teorema 1.40 – Teorema de Lagrange:** Sea  $H \leq G$  con  $G$  finito, entonces

$$|G/H| = \frac{|G|}{|H|}.$$

En base al teorema de Lagrange, llamamos *índice* de un subgrupo  $H$  al valor de  $|G/H|$ .

**Corolario 1.41:** El orden de todo elemento de un grupo finito es un divisor de su cardinal.

**Corolario 1.42:** Todo grupo de cardinal  $p$  primo es cíclico y, en consecuencia, isomorfo a  $\mathbb{Z}_p$ .

**Definición 1.43:** Denotamos por  $\mathbb{Z}_n^\times$  (léase “grupo multiplicativo” o “unidades de  $n$ ”) al conjunto de todos los elementos coprimos a  $n$  de  $\mathbb{Z}_n$ . Queda al lector demostrar que  $(\mathbb{Z}_n^\times, \cdot)$  es un grupo abeliano de neutro 1. Llamamos  $\phi : \mathbb{N}_{\geq 2} \rightarrow \mathbb{N}$  a la función  $\phi$  o indicatriz de Euler que

mide el cardinal del grupo multiplicativo de  $m$ , es decir:

$$\phi(n) := |\mathbb{Z}_n^\times|$$

**Teorema 1.44 (Euler-Fermat):** Si  $a$  coprimo a  $n$ , entonces

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

**Corolario 1.45 (Pequeño teorema de Fermat):** Sea  $a \in \mathbb{Z}_p$  no nulo, entonces

$$a^{p-1} \equiv 1, \quad a^p \equiv a \pmod{p}.$$

**Teorema 1.46 – Teorema chino del resto:** Si  $(n; m) = 1$ , entonces

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm},$$

donde un isomorfismo  $f$  es de la siguiente forma: dados  $p, q$  tales que  $pn + qm = 1$ , entonces

$$f(x, y) := ypn + xqm.$$

DEMOSTRACIÓN: Probemos que la función propuesta es, en efecto, un isomorfismo. La construcción utiliza la identidad de Bézout que requiere que los valores sean coprimos, veamos que  $f$  está bien definida: si  $x' = x + an$  e  $y' = y + bm$ , entonces

$$\begin{aligned} f(x', y') &= (y + bm)pn + (x + an)qm \\ &= ypn + xqm + nm(aq + bp) \equiv f(x, y) \pmod{nm}. \end{aligned}$$

Ahora veamos que  $f$  es inyectiva: Si

$$\begin{aligned} f(a, b) &\equiv f(c, d) \\ aqm + bpn &\equiv cqm + dpn \\ (a - c)qm &\equiv np(d - b) \pmod{nm}. \end{aligned}$$

Osea  $(a - c)qm = np(d - b) + snm = n(p(d - b) + sm)$ , luego  $n \mid (a - c)qm$ , pero  $(n; qm) = 1$ , luego por lema de Euclides,  $n \mid a - c$  lo que equivale a que  $a \equiv c \pmod{n}$ . Es análogo que  $b \equiv d \pmod{m}$ , que es lo que se quería probar.

Como  $f$  es inyectiva entre dos conjuntos finitos equipotentes, entonces es biyectiva, luego es isomorfismo.  $\square$

**Corolario 1.47:** Si  $(n; m) = 1$ , entonces

$$\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times,$$

en particular  $\phi(n)\phi(m) = \phi(nm)$ .

**Proposición 1.48:** Si  $p$  primo entonces  $\phi(p^k) = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right)$ .  
Luego, si  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ , entonces

$$\phi(n) = n \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right).$$

### 1.3. Representaciones de grupos finitos

Hemos visto ya que todo grupo finito de cardinal primo es isomorfo a un grupo cíclico  $\mathbb{Z}_p$ , entonces nos interesa ver si podemos usar otros grupos conocidos, como el simétrico y el diedral, para poder representar ciertos grupos finitos.

**Definición 1.49 – Conjugado, subgrupo normal, centro:** Dos elementos de un grupo  $a, b \in G$  se dicen *conjugados* si existe  $c \in G$  tal que  $c^{-1}ac = b$  (y por ende, con  $d := c^{-1}$  se cumple  $d^{-1}bd = a$ ).

Se dice que un subgrupo  $N \leq G$  es *normal* syss, para todo  $x \in G$  se cumple que  $xN = Nx$ , en cuyo caso denotaremos  $N \trianglelefteq G$ . Esto es equivalente a decir que todos los conjugados de  $N$  pertenecen a  $N$ , i.e., para todo  $x \in G$  se cumple  $x^{-1}Nx = N$ .

Se le llama *centralizador*  $Z(S)$  de  $S$  al conjunto de todos los elementos que conmutan con todos los elementos de  $S$ , i.e.

$$Z(S) := \{x \in G : \forall g \in S (xg = gx)\},$$

al centralizador de todo  $G$ , se le dice el *centro*. Llamamos *normalizador*  $N(S)$  de un conjunto  $S$  a los elementos que fijan al conjunto bajo conjugación, i.e.,

$$N(S) := \{x \in G : x^{-1}Sx = S\}.$$

Llamamos clase de conjugación  $C_G(S)$  de  $S$  al conjunto de todos los conjugados de  $S$ .

**Proposición 1.50:** Todo subgrupo de índice dos es normal.



**Proposición 1.51:** Se cumple:

1.  $N \trianglelefteq G$  syss  $N(N) = G$  syss  $C_G(N) = \{N\}$ .
2. Si  $S, T \subseteq G$ , entonces  $Z(S \cup T) = Z(S) \cap Z(T)$ , en particular,

$$Z(S) = \bigcap_{g \in S} Z(g).$$

3.  $H \leq G$  es abeliano syss  $H \subseteq Z(H)$ . Esto aplica también para  $G$  mismo.
4.  $Z(g) = N(g)$ .
5. Si  $S \subseteq G$  entonces  $Z(S) \leq N(S) \leq G$ .
6. Si  $H \leq G$  entonces  $H \trianglelefteq N(H) \leq G$ .
7.  $N \leq Z(G)$  implica  $N \trianglelefteq G$ , en particular,  $Z(G) \trianglelefteq G$ .
8.  $C_G(x) = \{x\}$  syss  $x \in Z(G)$ . Más generalmente  $C_G(S) = \{S\}$  syss  $S \subseteq Z(G)$ .

### §1.3.1 Productos de grupos.

**Proposición 1.52:** Se cumple:

1. Para todo  $S \subseteq G$  se cumple que  $|C_G(S)| = |G/N(S)|$ .
2. El conjugado de la inversa es la inversa del conjugado. Más generalmente las potencias del conjugado son el conjugado de la potencia.
3. El orden se preserva bajo conjugados.

DEMOSTRACIÓN: 1. Veamos que  $x \equiv y \pmod{Z(g)}$  implica  $x^{-1}y \in Z(g)$ , ergo

$$(x^{-1}y)g = g(x^{-1}y) \iff xgx^{-1} = ygy^{-1}.$$

Esto se traduce a decir que las clases de equivalencia determinadas por  $Z(g)$  se componen de los elementos que generan el mismo conjugado. Es claro que todo conjugado puede escribirse como  $x^{-1}gx$ , y lo anterior prueba que se determinásemos una aplicación entre ambos conjuntos esta sería inyectiva y suprayectiva, i.e., biyectiva, luego los conjuntos son equipotentes.

2. Sea  $a \in G$  y  $c \in G$  arbitrario, de forma que  $b := c^{-1}ac$ , luego por la propiedad anterior se cumple que  $b^k = c^{-1}a^k c$ , por lo que si  $n := \text{ord } a$ , entonces  $b^n = c^{-1}a^n c = c^{-1}ec = e$ . Por lo que  $\text{ord } b \leq \text{ord } a$ . Pero notemos que  $a = (c^{-1})^{-1}bc^{-1}$ , por lo que  $\text{ord } a \leq \text{ord } b$ . En conclusión,  $\text{ord } a = \text{ord } b$ .

□

**Proposición 1.53:** Para  $n \geq 3$  se cumple que  $Z(S_n) = 1$  y que  $Z(D_{2n}) = 1$  si  $n$  impar, y  $Z(D_{2n}) = r^{n/2}$  si  $n$  par.

DEMOSTRACIÓN: El centro de los grupos diedrales queda al lector. Sea  $\sigma \in S_n$  no unitario, luego existe un par  $i \neq j$  tales que  $\sigma(i) = j$ . Como  $n \geq 3$  existe un  $k$  distinto de ambos, luego  $(j, k)\sigma \neq \sigma(j, k)$ , pues basta considerar la imagen de  $i$  en cada caso.

□

**Teorema 1.54:** Sean  $H, K \leq G$ , entonces:

1.  $HK \leq G$  syss  $HK = KH$ .
2.  $H \trianglelefteq G$  o  $K \trianglelefteq G$  implica  $HK \leq G$ .
3.  $H \trianglelefteq G$  y  $K \trianglelefteq G$  implica  $HK \trianglelefteq G$ .

DEMOSTRACIÓN: 1.  $\implies$ . Sea  $hk \in HK$ , como  $H, K, HK \leq G$ ; entonces  $h^{-1} \in H, k^{-1} \in G$  y  $(h^{-1}k^{-1})^{-1} = kh \in HK$ , luego  $KH \subseteq HK$ . Análogamente se prueba la otra implicancia y por doble contención los conjuntos son iguales.

$\Leftarrow$ . Sean  $x, y \in HK$  por ende existen  $h_1, h_2 \in H$  y  $k_1, k_2 \in K$  tales que  $x = h_1k_1$  e  $y = h_2k_2$ . Luego  $xy^{-1} = h_1(k_1k_2^{-1})h_2^{-1}$ . Se cumple que  $(k_1k_2^{-1})h_2 \in KH = HK$ , por ende  $(k_1k_2^{-1})h_2 = h_3k_3$ , finalmente como  $H \leq G$  entonces  $h_1h_3 \in H$  y  $xy^{-1} = h_1(k_1k_2^{-1})h_2 = h_1h_3k_3 \in HK$  que es el criterio del subgrupo.

2. Sin pérdida de generalidad supongamos que  $H \trianglelefteq G$ , entonces  $kh = khk^{-1}k = h'k$  con  $h' \in H$  por ser conjugado de un elemento de  $H$ , luego  $KH = HK$ .
3. Por el inciso anterior se cumple que  $HK \leq G$  y para todo  $x \in G$  se cumple que  $x^{-1}h k x = (x^{-1}h x)(x^{-1}k x)$ .

□

**Definición 1.55 – Conmutador:** Definamos el conmutador  $[x, y] := x^{-1}y^{-1}xy$ , que satisface que  $xy = yx[x, y]$ , luego  $xy = yx$  si y sólo si  $[x, y] = 1$ . Llamaremos *subgrupo derivado*  $G'$  al conjunto de todos los conmutadores de  $G$ . Queda al lector probar que  $G' \leq G$ .

**Teorema 1.56:** Si  $N, M \leq G$  tales que  $N \cap M = \{1\}$ , entonces  $nm = mn$  con  $n \in N$  y  $m \in M$ .

DEMOSTRACIÓN: Notemos que  $[n, m] = (n^{-1}m^{-1}n)m = n^{-1}(m^{-1}nm)$ , donde  $n^{-1}mn \in M$  y  $m^{-1}nm \in N$  por ser normales. Como  $[n, m] \in N \cap M = \{1\}$ , entonces  $[n, m] = 1$ , luego conmutan.  $\square$

**Definición 1.57 – Producto de subgrupos:** Decimos que  $G$  es un producto de los subgrupos  $N_1, N_2, \dots, N_m$  si  $G = N_1 \cdots N_m$  y las intersecciones de los subgrupos son triviales dos a dos. En este caso, denotaremos  $G = N_1 \times \cdots \times N_m$ .

Además dados  $(H, \star), (G, *)$  grupos se define la operación  $\cdot$  sobre  $H \times G$ :

$$(h_1, g_1) \cdot (h_2, g_2) := (h_1 \star h_2, g_1 * g_2)$$

**Teorema 1.58:** Si  $G = N_1 \times \cdots \times N_m$ , entonces todo  $g \in G$  cumple que se escribe de forma única como  $g = n_1 \cdots n_m$  con  $n_i \in N_i$ .

**Teorema 1.59 – Teorema fundamental de los grupos abelianos finitos:** Todo grupo abeliano finito es isomorfo a un producto de grupos cíclicos.

**Corolario 1.60:** Todo grupo abeliano posee subgrupos de todos los divisores de su cardinal.

**§1.3.2 Teoremas de isomorfismos y categorías.** Éstos teoremas son herramientas casi-universales en el álgebra. Realizaremos la demostración en el contexto de teoría de grupos, pero no la repetiremos en el contexto de anillos ni módulos, pues son análogas.

**Definición 1.61 – Sucesión exacta:** Si se tiene una sucesión de morfismos:

$$\cdots \longrightarrow G_i \xrightarrow{\varphi_i} G_{i+1} \xrightarrow{\varphi_{i+1}} G_{i+2} \longrightarrow \cdots$$

es *exacta* si  $\text{Im} \varphi_i = \ker \varphi_{i+1}$  para todo  $i \in \mathbb{Z}$  (para el cuál estén definidos). Una sucesión exacta se dice *corta* si es finita.

**Proposición 1.62:** Se cumple:

1. Si  $H \trianglelefteq G$ , entonces

$$H \xhookrightarrow{\iota} G \twoheadrightarrow^{\pi} G/H$$

es una sucesión exacta corta.

2.  $f : G \rightarrow G'$  es inyectiva syss  $0 \longrightarrow G \xrightarrow{f} G' \longrightarrow 0$  es exacta
3.  $f : G \rightarrow G'$  es suprayectiva syss  $G \xrightarrow{f} G' \longrightarrow 0$  es exacta
4. Dados  $f : G' \rightarrow G$  y  $g : G \rightarrow G''$  morfismos de grupos, se cumple que

$$0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$$

es exacta syss existe  $H \trianglelefteq G$  tal que el siguiente diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & G' & \xrightarrow{f} & G & \xrightarrow{g} & G'' \longrightarrow 0 \\ & & \downarrow & & \downarrow \text{Id} & & \downarrow \\ 0 & \longrightarrow & H & \xhookrightarrow{\iota} & G & \twoheadrightarrow^{\pi} & G/H \longrightarrow 0 \end{array}$$

**Teorema 1.63 – Primer teorema de isomorfismos:** Sea  $\varphi : G \rightarrow H$  un morfismo de grupos con  $N := \ker \varphi \trianglelefteq G$ , entonces  $\bar{\varphi} : G/N \rightarrow \text{Im} \varphi$  dado por  $\bar{\varphi}(x) := \varphi(xN)$  resulta ser un isomorfismo.

En figura de diagrama conmutativo:

**Corolario 1.64:** Si  $\varphi : G \rightarrow H$  es un epimorfismo, entonces  $G/\ker \varphi \cong H$ .

$$\begin{array}{ccc}
G & \xrightarrow{\varphi} & H \\
\pi \downarrow & & \uparrow \iota \\
G/\ker \varphi & \xrightarrow[\varphi]{\sim} & \text{Im} \varphi
\end{array}$$

**Teorema 1.65 – Segundo teorema de isomorfismos:** Sean  $H \leq G$  y  $K \trianglelefteq K$ , entonces

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

DEMOSTRACIÓN: Sea  $\varphi : H \rightarrow HK/K$  definida por  $\varphi(h) := hK$  es un epimorfismo de grupos pues  $hkK \in HK/K$ , pero  $hkK = hK = \varphi(h)$ .

Luego, busquemos el kernel de  $\varphi$ . Notemos que  $1 \in \ker \varphi$  y  $\varphi(1) = K$ , asimismo, para todo  $k \in K$  se cumple que  $\varphi(k) = K$ , luego  $H \cap K \subseteq \ker \varphi$  y ya hemos visto que la otra implicancia también se da, luego por el primer teorema de isomorfismos se cumple el enunciado.  $\square$

**Teorema 1.66 – Tercer teorema de isomorfismos:** Sean  $K \leq H \trianglelefteq G$  y  $K \trianglelefteq G$ , entonces

$$\frac{G}{H} \cong \frac{G/K}{H/K}.$$

DEMOSTRACIÓN: Al igual que con la demostración del segundo teorema, vamos a tratar de aplicar el primer teorema:

Los elementos de  $(G/K)/(H/K)$  son de la forma  $gK(H/K)$ , luego  $\varphi : G \rightarrow (G/K)/(H/K)$  dado por  $\varphi(g) := (gK)(H/K)$  es un epimorfismo de grupos, donde el  $x \in G$  pertenece al kernel si y sólo si  $gK \in H/K$ , i.e,  $g \in H$ .  $\square$

Si bien el segundo teorema de isomorfismos no se aplica en casos más generales, la relación entre cardinales si es generalizable:

**Teorema 1.67:** Sean,  $H, K \leq G$  finito, entonces

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

DEMOSTRACIÓN: Sea  $f : H \times K \rightarrow HK$  dada por  $f(h, k) = hk$ . Claramente  $f$  es suprayectiva. Sean  $(h_1, k_1), (h_2, k_2) \in H \times K$ , luego  $f(h_1, k_1) = f(h_2, k_2)$

implica que  $u := k_1 k_2^{-1} = h_1^{-1} h_2 \in H \cap K$ . Luego es trivial probar que  $hk = h'k'$  syss existe  $u \in H \cap K$  tal que  $h' = hu$  y  $k' = u^{-1}k$ . Con lo que  $|f^{-1}[hk]| = |(hu, u^{-1}k) : u \in H \cap K| = |H \cap K|$ .

Luego se cumple que

$$H \times K = \bigcup_{x \in HK} f^{-1}[x] \implies |H||K| = |HK||H \cap K|.$$

□

**Proposición 1.68:** Si  $H_1 \trianglelefteq G_1$  y  $H_2 \trianglelefteq G_2$ , entonces

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$

DEMOSTRACIÓN: Se comienzan por definir los siguientes epimorfismos en base al siguiente diagrama conmutativo:

$$\begin{array}{ccccc} & & \pi_1 & & \\ & \searrow & & \searrow & \\ G_1 \times G_2 & \longrightarrow & G_1 & \longrightarrow & \frac{G_1}{H_1} \end{array}$$

y análogamente con  $\pi_2 : G_1 \times G_2 \rightarrow G_2/H_2$ . Luego  $\pi := (\pi_1, \pi_2)$  es un epimorfismo de kernel  $H_1 \times H_2$  que por el primer teorema de isomorfismos prueba el enunciado. □

### §1.3.3 Ecuación de clases y $p$ -grupos.

**Lema 1.69:** Dos clases de conjugación o son iguales o son disjuntas.

DEMOSTRACIÓN: Sean  $x, y \in G$  y sea  $z \in C_G(x) \cap C_G(y)$ , luego, existen  $g_1, g_2 \in G$  tales que  $g_1^{-1}xg_1 = g_2^{-1}yg_2$ , ergo  $y = (g_1g_2^{-1})^{-1}x(g_1g_2^{-1})$  y por ende  $C_G(y) \subseteq C_G(x)$ . El caso converso es análogo y por doble inclusión se concluye que los conjuntos son iguales. □

**Teorema 1.70 – Ecuación de clases:** Para todo grupo finito  $G$ , existen  $g_1, \dots, g_k \in G \setminus Z(G)$  tales que

$$|G| = |Z(G)| + \sum_{i=1}^k |G : Z(g_i)|.$$

DEMOSTRACIÓN: Por el lema anterior, el conjunto de clases de conjugación de un grupo determina una partición estricta de él, luego, en un caso finito, hay finitos conjuntos no vacíos, ergo elegimos representantes aleatorios de cada clase. Para toda clase de conjugación puede darse que  $|C_G(x)| = 1$ , o  $|C_G(x)| > 1$ , el primer caso equivale a pertenecer al centro, mientras que el segundo equivale a no pertenecer al centro. Luego como las clases determinan una partición estricta, basta sumar los cardinales de las clases de conjugación, y notemos que todos los elementos cuya clase es singular pertenecen al centro, ergo se cumple la fórmula del enunciado.  $\square$

**Definición 1.71 –  $p$ -grupo:** Se dice que  $G$  es un  $p$ -grupo si posee de cardinal alguna potencia de  $p$ . También se dice que  $H$  es un  $p$ -subgrupo de  $G$  si  $H \leq G$  y  $H$  es un  $p$ -grupo.

**Corolario 1.72:** Todo  $p$ -grupo posee centro no trivial.

**Teorema 1.73:** Si  $G/Z(G)$  es cíclico entonces  $G$  es abeliano. Luego  $|G/Z(G)|$  no es primo.

DEMOSTRACIÓN: Si  $G/Z(G)$  es cíclico, entonces todos sus elementos son de la forma  $g^n Z(G)$  con un  $g$  fijo, luego todo  $x \in G$  se escribe como  $g^n z$  con  $z \in Z(G)$ . Luego es fácil comprobar que  $x$  conmuta con todo elemento de  $G$ .  $\square$

**Teorema 1.74:** Todo grupo finito de cardinal  $p$  o  $p^2$  es abeliano. Luego todo grupo de cardinal  $p^2$  es isomorfo a  $\mathbb{Z}_{p^2}$  o a  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

## 1.4. Teoremas de Sylow

### §1.4.1 Acciones.

**Definición 1.75 – Acción:** Una acción de un grupo  $G$  sobre un conjunto  $S$  no vacío arbitrario es un morfismo  $\tau : G \rightarrow \text{Sym}(S)$ . Es decir  $\tau_g$  con  $g \in G$  es una permutación de  $S$ , y cumplen que

$$\tau_{xy} = \tau_x \circ \tau_y,$$

de esto se deduce que  $\tau_1 = \text{Id}_S$ .

Diremos que una acción es *fiel* si  $\tau$  es inyectiva.

Dada una acción  $\tau$  de  $G$  sobre  $S$ , entonces definimos los siguientes conjuntos:

$$\text{Orb}_a := \{\tau_g(a) : g \in G\}, \quad \text{Stab}_a := \{g \in G : \tau_g(a) = a\}$$

a los que llamamos órbita y estabilizador de  $a$  resp.

Decimos que una acción es *transitiva* si para todo  $a \in S$  se cumple que  $\text{Orb}_a = S$ .

En un grupo finito  $\tau_g : G \rightarrow G$  dado por  $\tau_g(x) = xg$  es una acción, y es de hecho la acción fiel que prueba el teorema de Cayley.  $\tau_g := g^{-1}xg$  es también una acción fiel.

**Teorema 1.76:** Si  $G$  actúa sobre  $S$ , entonces:

1.  $\text{Stab}_a \leq G$ .
2. El conjunto de órbitas de los elementos forman una partición estricta de  $S$ .
3. Para todo  $a \in S$  y  $g \in G$  se cumple que

$$\text{Stab}_{\tau_g(a)} = g^{-1}\text{Stab}_a g$$

Ergo, los estabilizadores son conjugados.

4. Existe una biyección entre  $G/\text{Stab}_a$  y  $\text{Orb}_a$ , en particular si  $G$  es finito, entonces

$$|G| = |\text{Orb}_a| |\text{Stab}_a|$$

DEMOSTRACIÓN: 1. Ejercicio para el lector.

2. Basta ver que si dos órbitas no son disjuntos entonces son iguales, para ello si  $a, b \in S$  basta probar que  $\text{Orb}_a \subseteq \text{Orb}_b$ . Sea  $c \in \text{Orb}_a \cap \text{Orb}_b$ , de forma que existen  $g_1, g_2 \in G$  tales que

$$c = \tau_{g_1}(a) = \tau_{g_2}(b)$$

Ahora, sea  $d := \tau_g(a)$ , entonces  $d = \tau_g(\tau_{g_1}^{-1}(c)) = \tau_{gg_1^{-1}g_2}(b)$ , ergo  $d \in \text{Orb}_b$ .

3. Ejercicio para el lector.



4. Prefijado un  $a \in S$ , vamos a definir  $H := \text{Stab}_a$ ,  $K := \text{Orb}_a$  y  $\varphi : G/H \rightarrow K$  como  $\varphi(gH) = \tau_g(a)$ . En primer lugar, veamos que está bien definida, si  $x \equiv y \pmod{H}$ , entonces existe  $h \in H$  tal que  $xh = y$ , luego

$$\tau_y(a) = \tau_{xh}(a) = \tau_x(\tau_h(a)) = \tau_x(a).$$

Queda al lector probar que  $\varphi$  es una biyección. □

**Corolario 1.77:** Si  $G$  actúa sobre  $S$ , donde  $S$  es finito, entonces existen  $x_1, \dots, x_n$  tales que

$$|S| = \sum_{i=1}^n |\text{Orb}_{x_i}| = \sum_{i=1}^n |G/\text{Stab}_{x_i}|.$$

**Definición 1.78 – Puntos fijos:** En general, se dice que  $x$  es un punto fijo de una endo-función  $f$  si  $f(x) = x$ . Si  $G$  actúa sobre  $S$ , entonces se denota  $\text{Fix}_g(S)$  al conjunto de puntos fijos de la permutación  $\tau_g$ . Denotamos  $\text{Fix}_G(S)$  al conjunto de puntos fijos bajo cualquier permutación de la acción, es decir:

$$\text{Fix}_g(S) := \{x \in S : \tau_g(x) = x\}, \quad \text{Fix}_G(S) := \bigcap_{g \in G} \text{Fix}_g(S).$$

**Teorema 1.79:** Si  $G$  es un  $p$ -grupo que actúa sobre  $S$  finito, entonces

$$|S| \equiv |\text{Fix}_G(S)| \pmod{p}$$

DEMOSTRACIÓN: Por la ecuación de órbitas se cumple que

$$|S| = \sum_{i=1}^n |\text{Orb}_{x_i}|,$$

nótese que como  $G$  es un  $p$ -grupo y  $\text{Stab}_{x_i}$  un  $p$ -subgrupo, entonces  $|\text{Orb}_x| = |G/\text{Stab}_x|$  siempre es una potencia de  $p$  (que incluye  $p^0 = 1$ ). Si es una potencia no nula entonces  $|\text{Orb}_x| \equiv 0 \pmod{p}$ , si  $|\text{Orb}_x| = 1$  entonces es un punto fijo global y  $x \in \text{Fix}_G(S)$ . □

**Corolario 1.80:** Si  $G$ , un  $p$ -grupo, actúa sobre  $S$  que no es de cardinal múltiplo de  $p$ , entonces  $S$  posee al menos un punto fijo global.

**§1.4.2 Teoremas de Sylow.** Los teoremas de Sylow son un conjunto de cuatro teoremas<sup>2</sup> bastante importantes para la teoría de grupos finitos. De antemano advierto que la mayoría de demostraciones de los teoremas hace uso de las acciones de grupos, así que relea dicha sección las veces necesarias para entenderlos mejor.

Además nos referiremos a los teoremas de Sylow por números romanos, e.g., Sylow I.

**Teorema 1.81 – Teorema de Cauchy:** Si  $p$  divide al cardinal de  $G$ , entonces  $G$  contiene un elemento de orden  $p$ , y por ende, un subgrupo de cardinal  $p$ .

DEMOSTRACIÓN: Si  $G$  es abeliano, entonces ya hemos probado que posee subgrupos de todos los divisores de su cardinal.

Si  $G$  no es abeliano: Supongamos por contradicción que esto no pasa, entonces sea  $G$  el grupo de cardinalidad mínima tal que contradice el enunciado. Notemos que todos sus subgrupos deben tener cardinal que no es divisible por  $p$ , de lo contrario, poseen un elemento de orden  $p$  por la minimalidad del cardinal de  $G$ . Por el teorema de Lagrange, para todo  $H \leq G$  se cumple que  $|G| = |H| |G/H|$ , luego  $p$  divide a  $|G/H|$  para todo subgrupo  $H$  de  $G$ . Luego por ecuación de clases, se cumple que  $p$  divide a  $|G/Z(g_i)|$ , luego divide al cardinal del centro, pero como asumimos que  $G$  no posee subgrupos propios cuyo cardinal sea un múltiplo de  $p$ , entonces  $Z(G) = G$ , luego  $G$  es abeliano, lo que es absurdo.  $\square$

**Corolario 1.82:** Si todos los elementos no-neutros de un grupo  $G$  tienen orden  $p$ , entonces  $G$  es un  $p$ -grupo.

**Definición 1.83 –  $p$ -subgrupo de Sylow:** Dado un grupo de cardinal  $n$  y un primo  $p$  tal que  $p \mid n$  se dice que un subgrupo  $H \leq G$  es un  $p$ -subgrupo de Sylow si  $|H| = p^m$  con  $m := \nu_p(n)$ . Denotaremos  $\text{Syl}_p(G)$  al conjunto de  $p$ -subgrupos de Sylow de  $G$ .

**Teorema 1.84 – Primer teorema de Sylow:** Todo grupo finito  $G$  contiene un  $p$ -subgrupo de Sylow para todo  $p$  primo. Osea,  $\text{Syl}_p(G) \neq \emptyset$ .

---

<sup>2</sup>A veces el cuarto se considera una variación del tercero.

DEMOSTRACIÓN: Lo demostraremos por inducción fuerte sobre el cardinal de  $G$ . El cual es de la forma  $p^\alpha m$  con  $p \nmid m$ . También asumiremos que  $\alpha > 0$ , pues dicho caso es trivial.

**Caso 1 ( $p$  divide a  $Z(G)$ ).** Luego  $Z(G)$  como es abeliano, posee un elemento de orden  $p$  que genera un subgrupo cíclico  $N$  que es normal (por ser subgrupo del centro), ergo  $G/N$  es grupo de cardinal  $p^{\alpha-1}m$ . Luego, por inducción  $G/N$  contiene un  $p$ -subgrupo de Sylow que denotaremos por  $\bar{P}$ . Luego sea  $P := \{g \in G : gN \in \bar{P}\}$ . Probaremos que  $P$  es un  $p$ -subgrupo de Sylow:

**$P$  es subgrupo:** Es claro que  $1 \in P$ , luego no es vacío. Sean  $u, v \in P$ , luego  $uv^{-1} \in P$ , pues  $\bar{P}$  es un subgrupo de  $G/N$ .  **$P$  es de Sylow:** Sea  $\varphi : P \rightarrow \bar{P}$  tal que  $\varphi(g) = gN$ , como  $\varphi$  es un epimorfismo, por el primer teorema de isomorfismos se cumple que  $|P/\ker \varphi| = |\bar{P}|$  y  $\ker \varphi = N \cap P = N$ , luego  $|P| = |N| |\bar{P}| = p \cdot p^{\alpha-1} = p^\alpha$ .

**Caso 2 ( $p$  no divide a  $Z(G)$ ).** Por la ecuación de clases se cumple que hay alguna clase de conjugación no trivial cuyo cardinal no es múltiplo de  $p$  y como son de la forma  $|G/Z(g)|$  entonces hay algún  $|Z(g)| = p^\alpha n$  y por inducción fuerte, contiene un  $p$ -subconjunto de Sylow que lo es de  $G$ .  $\square$

**Teorema 1.85:** Todo grupo no abeliano de orden  $2p$  con  $p$  primo impar es isomorfo a  $D_{2p}$ .

DEMOSTRACIÓN: Por el primer teorema de Sylow  $G$  posee un 2-subconjunto y un  $p$ -subconjunto de Sylow, que son cíclicos, ergo se escriben como  $\langle x \rangle$  y  $\langle y \rangle$ , y se cumple que

$$|\langle x \rangle \langle y \rangle| = \frac{\text{ord}(x) \cdot \text{ord}(y)}{|\langle x \rangle \cap \langle y \rangle|}$$

Como los valores son enteros, la intersección sólo puede tener cardinalidad 1, 2,  $p$  o  $2p$ , por contención, debe tener cardinalidad 1 o 2, y queda al lector probar que el otro caso es imposible. Luego  $G = \langle x, y \rangle$  y por ende es isomorfo a  $D_{2p}$ .  $\square$

**Teorema 1.86 – Segundo teorema de Sylow:** Todos los  $p$ -subgrupos de Sylow de un grupo finito son conjugados. En consecuencia, si  $P$ , es un  $p$ -subgrupo de Sylow, entonces

$$|\text{Syl}_p(G)| = |G/Z(P)|.$$

DEMOSTRACIÓN: Sea  $Q$  otro  $p$ -subgrupo de Sylow, entonces consideremos la acción del producto por la derecha de  $Q$  (un  $p$ -grupo) sobre  $G/P$  (un grupo cuyo cardinal no es múltiplo de  $p$ ), luego  $\text{Fix}_Q(G/P)$  es no vacío, es decir, existe un  $g \in G$  tal que para todo  $q \in Q$  se cumple que  $Pgq = Pg$ , o más bien, que  $qg \in Pg$  para todo  $q \in Q$ . Luego  $Q \subseteq g^{-1}Pg$  y por cardinalidad se comprueba que ambos conjuntos son iguales.  $\square$

**Corolario 1.87:**  $G$  posee un único  $p$ -subgrupo de Sylow si y sólo si éste es normal.

**Definición 1.88 – Grupo simple:** Se dice que un grupo es *simple* si su único subgrupo normal impropio es el trivial.

**Ejemplo.** Los grupos cíclicos de orden primo son simples.

**Corolario 1.89:** Un grupo de cardinal  $mp$  con  $p$  primo y  $p \nmid m$  no es simple.

**Teorema 1.90 – Tercer teorema de Sylow:** Si  $|G| = p^k m$  con  $p \nmid m$ , entonces

$$n_p \equiv 1 \pmod{p} \quad \text{y} \quad n_p \mid m$$

donde  $n_p := |\text{Syl}_p(G)|$ .

DEMOSTRACIÓN: Consideremos la acción de  $P \in \text{Syl}_p(G)$  (un  $p$ -grupo) sobre  $\text{Syl}_p(G)$  por conjugación. Luego se tiene que

$$|\text{Syl}_p(G)| = n_p \equiv |\text{Fix}_P(\text{Syl}_p(G))| \pmod{p}$$

Probaremos ahora, por contradicción, que  $P$  es el único punto fijo de su acción. Sea  $Q \in \text{Syl}_p(G)$  distinto de  $P$  tal que es punto fijo. Por definición, para todo  $g \in P$  se cumple que  $g^{-1}Qg = Q$ , luego  $P \leq N(Q) \leq G$ . Luego, podemos ver que  $Q$  y  $P$  son  $p$ -subgrupos de Sylow de  $N(Q)$ , y  $Q$  es normal, luego por el corolario anterior  $P = Q$ . En conclusión  $|\text{Fix}_P(\text{Syl}_p(G))| = 1$ .

Consideremos la acción de  $G$  sobre  $\text{Syl}_p(G)$  por conjugación. Luego  $n_p \mid p^k m = |G|$  y  $n_p$  es coprimo a  $p$  (por el inciso anterior), por ende, por lema de Euclides,  $n_p \mid m$ .  $\square$

En general  $n_p$  representará a la cantidad de  $p$ -subgrupos de Sylow de un grupo finito prefijado.

**Teorema 1.91 – Cuarto teorema de Sylow:** Se cumple que  $n_p := |G/N(P)|$  donde  $P \in \text{Syl}_p(G)$ .

HINT: Relea el último paso en la demostración anterior.

## 1.5. Grupos resolubles

**Definición 1.92 – Series de grupos:** Dado un grupo  $G$  se le dice *serie normal* de subgrupos a una cadena de inclusiones estrictas

$$G =: G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}.$$

En una serie se le llama *factores* a los términos  $G_{i+1}/G_i$ . Una serie es estricta si  $G_i \neq G_j$  para todo  $i \neq j$ . Una serie se dice abeliana (resp. cíclica) si todos los factores lo son.

Una serie se dice *de composición* si es estricta y los factores son simples (lo que equivale a ver que  $G_i$  es un subgrupo normal maximal en  $G_{i+1}$ ). La máxima longitud de una serie de composición se denota por  $\ell(G)$ . Nótese que si  $G$  es no trivial y simple, entonces  $\ell(G) = 1$ .

**Lema 1.93 (Zassenhaus):** Sea  $G$  un grupo, tal que  $H' \trianglelefteq H \leq G$  y  $K' \trianglelefteq K \leq G$ , entonces  $H'(H \cap K') \trianglelefteq H'(H \cap K)$  y  $K'(K \cap H') \trianglelefteq K'(K \cap H)$ , y

$$\frac{H'(H \cap K)}{H'(H \cap K')} \cong \frac{K'(K \cap H)}{K'(K \cap H')}$$

DEMOSTRACIÓN: Como  $H \cap K' \leq H$  (por intersección de subgrupos) y  $H'(H \cap K') \leq H \leq G$  pues el producto de subgrupo normal con subgrupo es subgrupo; este argumento sirve para todos los términos.  $\square$

**Teorema 1.94 – Teorema de Jordan-Hölder:** Si un grupo finito  $G$  posee dos series de composición

$$\begin{aligned} G &\triangleright G_1 \triangleright \cdots \triangleright G_p = \{1\} \\ G &\triangleright H_1 \triangleright \cdots \triangleright H_q = \{1\} \end{aligned}$$

entonces  $p = q$  y los factores son respectivamente isomorfos tras una permutación de índices.

DEMOSTRACIÓN: Si dos series de composición cumplen el enunciado diremos que son JH-equivalentes, en contexto de ésta demostración. Además llamaremos serie G a la serie de los  $G_i$ s y serie H a la serie de los  $H_i$ s.

La demostración es por inducción fuerte sobre el cardinal  $n$  de  $G$ : El caso  $n = 2$  es trivial.

Si  $G_1 = H_1$ , entonces como  $|G_1| < n$  se deduce el resto. Si  $G_1 \neq H_1$ , entonces como  $G_1 H_1$  es normal y contiene estrictamente a  $G_1$ , entonces  $G_1 H_1 = G$ . Luego sea  $K := G_1 \cap H_1$ , y sea

$$K \triangleright K_1 \triangleright \cdots \triangleright K_r = \{1\}.$$

Por ende, nos queda que

$$\begin{aligned} G_1 &\triangleright K \triangleright K_1 \triangleright \cdots \triangleright K_r, \\ H_1 &\triangleright K \triangleright K_1 \triangleright \cdots \triangleright K_r, \end{aligned}$$

son series de composición para  $G_1$  y  $H_1$ . Nuevamente, como  $|G_1| < n$  entonces todas las series de composición de  $G_1$  son JH-equivalentes, luego es equivalente a la de arriba; y lo mismo aplica para todas las serie de  $H_1$ . Pero además, el tercer teorema de isomorfismos que dice que  $G/G_1 \cong H_1/K$  y  $G/H_1 \cong G_1/K$ , por lo que se demuestra que la series G y H son JH-equivalentes.  $\square$

Al definir conmutadores, decimos que se define el *derivado* de un grupo como el conjunto de todos los conmutadores.

**Lema 1.95:** Si  $G$  es finito, entonces son equivalentes:

1. Todas las series de composición de  $G$  son abelianas.
2.  $G$  posee una serie cíclica.
3.  $G$  posee una serie abeliana.
4. Existe un  $n$  tal que el  $n$ -ésimo derivado de  $G$  es trivial.

DEMOSTRACIÓN: Es claro que (1)  $\implies$  (2)  $\implies$  (3).

(3)  $\implies$  (1). ...  $\square$

**Definición 1.96 – Grupo resoluble:** Un grupo es resoluble si cumple las condiciones del lema anterior.

**Teorema 1.97:** Se cumple:

1. Si  $G$  es resoluble y  $H \leq G$ , entonces  $H$  es resoluble.
2. Si  $G$  es resoluble y  $N \trianglelefteq G$ , entonces  $G/N$  es resoluble.
3. Si  $N \trianglelefteq G$  es tal que  $N$  y  $G/N$  son resolubles, entonces  $G$  también lo es.
4. Si  $H, K \leq G$  son resolubles y  $H \trianglelefteq G$ , entonces  $HK$  es resoluble.

DEMOSTRACIÓN: 1. Sea  $G \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$  una serie abeliana, veremos que

$$G \cap H = H \triangleright G_1 \cap H \triangleright \cdots \triangleright \{1\}$$

es una serie abeliana. Nótese que

$$\frac{G_i \cap H}{G_{i+1} \cap H} = \frac{G_i \cap H}{G_{i+1} \cap (G_i \cap H)} \cong \frac{G_{i+1}(G_i \cap H)}{G_{i+1}} \leq \frac{G_i}{G_{i+1}},$$

donde el último es abeliano, y la equivalencia viene dada por el segundo teorema de isomorfismos.

□

## 1.6. Grupo simétrico

Dados nuestros conocimientos en teoría de conjuntos debería de ser fácil probar que  $(\text{Func}(S), \circ)$  es siempre un monoide y para que cumpla ser un grupo debemos considerar el subgrupo de los elementos invertibles, es decir, el conjunto de las permutaciones de  $S$ , el cual denotamos por  $\text{Sym}(S)$ .

Es fácil probar que  $\text{Sym}(S) \cong \text{Sym}(T)$  syss  $|S| = |T|$ , así que como representante general denotaremos  $S_n$  al grupo simétrico sobre  $\{1, 2, \dots, n\}$ .

**Proposición 1.98:** Se cumple:

1.  $|S_n| = n!$ .
2.  $S_n$  no es abeliano con  $n \geq 3$ .

3.  $S_i \leq S_j$  para todo  $i < j$ .

**Teorema 1.99 – Teorema de Cayley:** Para todo grupo finito  $G$  de cardinal  $n$  se cumple que

$$G \cong H \leq S_n.$$

DEMOSTRACIÓN: Vamos a definir  $\varphi_a : G \rightarrow G$  como  $f_a(x) = xa$ . Sigue que

$$(f_a \circ f_b)(x) = f_b(f_a(x)) = f_b(xa) = (xa)b = x(ab) = f_{ab}(x).$$

Es decir, que  $f_{ab} = f_a \circ f_b$ . Nótese que las aplicaciones  $f_a$  son biyectivas pues admiten inversa  $f_a^{-1}$ . Finalmente  $\varphi(a) = f_a$  es un monomorfismo cuya imagen forma un subgrupo de  $S_n$ , que es lo que se quería probar.  $\square$

La importancia del teorema de Cayley, también y apropiadamente llamado teorema de representación de grupos finitos, es que nos permite describir a los grupos finitos en término de los grupos simétricos, destacando la importancia de éstos últimos.

**Definición 1.100 – Órbitas y ciclos:** Dado  $\sigma \in \text{Sym}(S)$  y  $a \in S$ , diremos que la órbita de  $a$  es la tupla ordenada

$$(a, \sigma(a), \sigma^2(a), \dots)$$

En particular, como  $\text{Sym}(S)$  es siempre de cardinal finito, entonces toda permutación es de orden finito, por ende, todas las órbitas lo son. Diremos que una órbita es trivial si posee un único elemento. Los elementos de órbitas triviales se llaman *puntos fijos*.

Diremos que una permutación es un *ciclo* si todas sus órbitas son triviales excepto una. En cuyo caso, denotaremos a la permutación mediante su órbita no-trivial, por ejemplo, la permutación

$$\{(1, 1), (2, 3), (3, 5), (4, 4), (5, 2), (6, 6)\} \in \text{Sym}(6)$$

se denotará como  $(2, 3, 5)$ ,  $(3, 5, 2)$  o  $(5, 2, 3)$ . **Ojo:** los ciclos están ordenados, no es lo mismo  $(2, 3, 5)$  que  $(5, 3, 2)$ . Los ciclos de orden 2 se denominarán *trasposiciones*.

Dos ciclos se dicen *disjuntos* si sus órbitas no-triviales lo son.

**Teorema 1.101:** Se cumplen:



1. El orden de los ciclos es el cardinal de su órbita no trivial.
2. La inversa de un ciclo  $(a_1, a_2, \dots, a_{n-1}, a_n)$  es  $(a_n, a_{n-1}, \dots, a_2, a_1)$ .
3. Dos ciclos disjuntos conmutan.
4. Toda permutación de  $S_n$  excepto Id, puede escribirse como el producto de ciclos disjuntos dos a dos.
5. El orden de un producto de ciclos disjuntos dos a dos es el mínimo común múltiplo de todos sus ordenes.
6. Las trasposiciones forman una base para  $S_n$ .
7. Si  $\sigma \in S_n$  y  $(a_1, \dots, a_n)$  es un ciclo, entonces

$$\sigma^{-1}(a_1, \dots, a_n)\sigma = (\sigma(a_1), \dots, \sigma(a_n)).$$

DEMOSTRACIÓN: 4. Dada una permutación de  $S_n$  distinta de la identidad, luego posee alguna órbita no trivial. Finalmente se deduce que se puede escribir como la composición de todos los ciclos derivados de sus órbitas no triviales, los cuales son disjuntos dos a dos.

5. Queda al lector.
6. Por la 4, basta probar que todo ciclo está generado por trasposiciones, lo que se hace notando que

$$(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_n).$$

□

### §1.6.1 Signo de una permutación.

**Lema 1.102:** Si  $\sigma \in S_n$  cumple que

$$\sigma = \prod_{i=1}^n \tau_{1,i} = \prod_{i=1}^m \tau_{2,i}$$

donde  $\tau_{j,i}$  es una trasposición, entonces  $n \equiv m \pmod{2}$ .

DEMOSTRACIÓN: En dicha situación podemos mover todo de un lado al otro y escribir:

$$1 = \left( \prod_{i=1}^n \tau_{1,i} \right) \left( \prod_{i=1}^m \tau_{2,(m-i+1)}^{-1} \right) = \tau_{1,1} \tau_{1,2} \cdots \tau_{1,n} \tau_{2,m}^{-1} \tau_{2,m-1}^{-1} \cdots \tau_{2,1}^{-1}.$$

Por ende, se reduce a probar que el producto de impares trasposiciones nunca es 1.

Supongamos que 1 puede ser el producto de un número impar de trasposiciones, entonces sea  $n$  el mínimo impar que lo cumpla. Es claro que  $n$  no puede ser 1, luego sea  $(\tau_i)_{i=1}^n$  una sucesión de trasposiciones cuyo producto es 1, luego sean  $(a_i, b_i) := \tau_i$  donde  $a_i < b_i$  para que esté bien definido. Notemos que la primera trasposición mueve a  $a_1$  a  $b_1$ , así que alguna otra debe mover a  $b_1$ , es decir,  $b_1 = a_i$  o  $b_i$  para algún  $i > 1$ . Así usaremos que

$$(a, b)(c, d) = (c, d)(a, b), \quad (a, b)(b, c) = (b, c)(a, b)$$

Para mover ese  $a_i$  o  $b_i$  a la segunda trasposición, y de paso, renombraremos  $a_2 := b_1$  y  $b_2$  como aquél que le acompañaba. Ahora tenemos que

$$1 = (a_1, b_1)(b_1, b_2)\tau_3 \cdots \tau_n.$$

**Caso 1** ( $b_2 = a_1$ ): En este caso  $\tau_1 = \tau_2$  y luego se cancelan pues las trasposiciones son de orden dos, luego 1 se escribe con  $n - 2$  trasposiciones con  $n - 2$  impar, lo que contradice la minimalidad de  $n$ .

**Caso 2** ( $b_2 \neq a_1$ ): Aquí utilizamos una de las propiedades señaladas para ver que

$$1 = (b_1, b_2)(a_1, b_2)\tau_3 \cdots \tau_n$$

luego iteramos el paso anterior y reordenamos de forma que  $\tau_3 = (b_2, b_3)$ . Como el producto es la identidad, podemos reordenar e iterar el proceso varias veces pero llega un punto en el que  $b_i = a_1$  en cuyo caso las dos trasposiciones se cancelaran y contradicen la minimalidad de  $n$ .  $\square$

**Definición 1.103 – Signo de una permutación:** Si una permutación  $\sigma$  se puede escribir como un producto de  $n$  trasposiciones, entonces  $\text{sgn } \sigma := (-1)^n$ . Las permutaciones de signo 1 se dicen *pares* y el resto *impares*.

Notemos que la identidad es par, y las trasposiciones pares. Un ciclo de longitud  $n$  es de paridad  $(-1)^{n+1}$ .

**Proposición 1.104:** Se cumple que  $\text{sgn} : S_n \rightarrow (\{\pm 1\}, \cdot)$  es un homomorfismo, es decir,  $\text{sgn}(\sigma\tau) = \text{sgn} \sigma \cdot \text{sgn} \tau$ .

**Corolario 1.105:** El signo se conserva entre inversas y conjugados.

**§1.6.2 Grupos alternantes y diedrales. Grupo alternante.** Como vimos, el signo es un morfismo de grupos, esto es importante porque significa que el kernel del signo, es decir el conjunto de permutaciones pares, es un subgrupo normal del simétrico. Luego denotamos

$$A_n := \{\sigma \in S_n : \text{sgn} \sigma = 1\}.$$

**Proposición 1.106:** Se cumple:

1. Para  $n > 2$ , se cumple que  $|A_n| = \frac{n!}{2}$ .
2.  $A_i \leq A_j$  para todo  $2 < i < j$ .
3.  $A_4$  es no abeliano y en consecuencia todo  $A_n$  con  $n \geq 4$  lo es.

Una característica es que veremos que los grupos alternantes son simples, pero para demostrarlo bastan varios lemas:

**Lema 1.107:** Si  $n \geq 3$ , entonces  $A_n$  está generado por los ciclos de longitud 3.

DEMOSTRACIÓN: Por definición todo elemento de  $A_n$  es una permutación par, que podemos separar en productos de dos trasposiciones. Luego o  $(a, b)(a, c) = (a, b, c)$  o  $(a, b)(c, d) = (a, b, c)(c, a, d)$ .  $\square$

**Lema 1.108:** Si  $n \geq 5$ , y  $N \trianglelefteq A_n$  contiene un ciclo de longitud 3, entonces  $N = A_n$ .

DEMOSTRACIÓN: Sea  $\tau$  un ciclo de longitud 3 en  $N$ , luego existe  $\sigma \in S_n$  tal que

$$\sigma^{-1}\tau\sigma = (1, 2, 3).$$

Si  $\sigma \in A_n$ , entonces  $(1, 2, 3) \in N$ , de lo contrario  $\sigma' := \sigma(4, 5) \in A_n$  y

$$\sigma'^{-1}\tau\sigma' = (4, 5)\sigma^{-1}\tau\sigma(4, 5) = (4, 5)(1, 2, 3)(4, 5) = (1, 2, 3).$$

Luego es fácil deducir que todos los otros ciclos de longitud 3 están en  $N$ , luego  $N = A_n$ .  $\square$

**Teorema 1.109:** Si  $n \geq 5$ , entonces  $A_n$  es simple.

DEMOSTRACIÓN: Primero veamos que  $A_5$  es **simple**: Si  $\{1\} \neq N \trianglelefteq A_5$ , entonces un elemento no neutro de  $N$  es de la forma  $(a, b, c)$ ,  $(a, b)(c, d)$  o  $(a, b, c, d, e)$ .

En el primer caso el lema prueba que  $N = A_5$ .

Si  $(a, b)(c, d) \in N$ , entonces con  $\sigma := (a, b, e)$  se cumple

$$\sigma^{-1}(a, b)(c, d)\sigma = (b, e)(c, d) \in N,$$

luego  $(a, b)(c, d) \cdot (b, e)(c, d) = (b, a, e) \in N$  y  $N = A_5$ .

Si  $(a, b, c, d, e) \in N$ , entonces con  $\sigma := (a, b)(d, e)$  se cumple

$$\sigma^{-1}(a, b, c, d, e)\sigma = (a, c, e, d, b) \in N,$$

luego  $(a, b, c, d, e)(a, c, e, d, b) = (b, e, c) \in N$  y  $N = A_5$ .

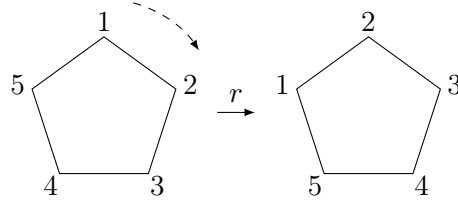
Ahora veamos que si  $n \geq 5$  entonces  $A_n$  es **simple**: Será por inducción sobre  $n$ , donde el caso base está probado. En primer lugar identificaremos  $A_n$  con el subgrupo de  $A_{n+1}$  de las permutaciones que tienen al  $n+1$  como punto fijo. De este modo si  $N \trianglelefteq A_{n+1}$ , entonces  $N \cap A_n \trianglelefteq A_n$ . Si  $N \cap A_n = A_n$ , entonces  $N$  contiene a un ciclo de longitud 3 y  $N = A_{n+1}$ . Si  $N \cap A_n = \{1\}$ , entonces si  $\sigma \in N_{\neq 1}$  entonces  $\sigma(n+1) =: p \neq n+1$ . Como  $\sigma$  no puede ser una trasposición (pues sería impar), y tampoco puede ser un 3-ciclo, entonces existen  $q, r$ ; distintos entre sí y distintos de  $p, n+1$ ; tales que  $\sigma(q) = r$ . Sean  $u, v$  distintos entre sí y distintos de  $p, q, r, n+1$ . Luego si  $\tau := (p, n+1)(q, r, u, v)$  entonces  $\eta := \tau^{-1}\sigma\tau$ . Nótese que  $\eta(p) = n+1$ , de modo que  $\sigma\eta \in N \cap A_n$ , pero  $\eta(r) = u$ , luego  $(\sigma\eta)(q) = u$  con lo que  $\sigma\eta \neq 1$ , por lo que  $N = \{1\}$ , completando la minimalidad de  $A_{n+1}$ .  $\square$

**Corolario 1.110:** Si  $n \geq 5$ , entonces  $A_n$  no resoluble y, en consecuencia,  $S_n$  tampoco lo es.

Queda de ejercicio probar que  $S_1, S_2, S_3$  y  $S_4$  sí son resolubles.

**Grupo diedral.** Consideremos un polígono de  $n$  lados (o  $n$ -gono) regular y enumeremos sus vértices. Pongamos reglas: claramente no admitimos la posibilidad de deformar el polígono, de manera que, por ejemplo, el vértice 2 siempre está entre el vértice 1 y el vértice 3. Los vértices se “leen” en sentido horario y siempre hay un vértice líder o principal por el cuál se comienzan a

enumerar el resto. Así, llamamos grupo diedral al conjunto de todas las isometrías posibles en el polígono, en particular, como indicamos que lo que nos interesa es el ordenamiento de los vértices, entonces traslaciones no afectan a la figura, sino que sólo lo hacen las rotaciones y las reflexiones:



**Figura 1.1.** Ejemplo con un pentágono.

En esencia esto representa a un grupo, sin embargo, hay que formalizar esta idea, y para ello, definiremos:

**Definición 1.111 – Grupo diedral o diédrico:** Fijado un  $n > 2$ , se define un grupo donde  $r$  es un elemento de orden  $n$ ,  $s$  de orden 2 no generado por  $r$  tales que  $srs = r^{-1}$ . Finalmente  $D_{2n} := \langle r, s \rangle$ .

**Proposición 1.112:** Para todo grupo diedral se cumple:

1. En  $D_{2n}$  se cumple que  $\text{ord } r = n$  y  $\text{ord } s = 2$ .
2.  $rs = sr^{-1}$  y más generalmente  $r^k s = sr^{-k}$ . Esto equivale a que  $srs^{-1} = r^{-1}$  y que  $\text{ord}(rs) = 2$ .
3. El grupo no es abeliano, por ende tampoco es cíclico.
4.  $|D_{2n}| = 2n$ .

**Observación.** El lector puede argüir que, en teoría, nuestra definición es informal y no permite construir ningún grupo en lo absoluto. A esto yo respondo de dos posibles maneras: en primer lugar podemos usar los métodos de la demostración del teorema de Cayley para formar, de manera rigurosa, los grupos diedrales como subgrupos de uno simétrico. En segundo lugar, como los isomorfismos nos señalan que no importan los objetos de un grupo sino las relaciones entre ellos, y como se puede deducir de antemano que los grupos diedrales poseen  $2n$  elementos, puedes tomar  $2n$  elementos cualesquiera de nuestra teoría y definir la operación de tal modo que cumpla con lo pedido. En ambos casos, se ahorrará esta discusión en las definiciones de grupos posteriores.



## 2

---

# Anillos y Cuerpos

---

La teoría de anillos y cuerpos es bastante importante para el álgebra, en ciertos aspectos comparte similitudes con la teoría de grupos, sin embargo, a diferencia de ésta, la gran mayoría de la literatura no concuerda sobre temas como las definiciones básicas en la teoría de anillos. Ésto se debe a una inconclusa batalla entre aplicaciones y similitudes, algunas definiciones permiten mayor fuerza entre los resultados obtenidos, mientras que las otras hacen ligeros sacrificios para conservar una clara simetría entre los anillos y los grupos; en éste texto se opta por la segunda.

Una de las cosas que más difieren es en si considerar la inclusión de la unidad en un anillo como fundamental. Libros como [1] definen anillo con neutro multiplicativo y “anillo” (en inglés, *rng*), sin *i*, a dichas estructuras sin inversos. Ésta no es práctica de éste libro, pero se le señala al lector tenerla en cuenta.

### 2.1. Definiciones elementales

**Definición 2.1 – Anillo, cuerpo, dominio:** Se dice que una terna  $(A, +, \cdot)$  es un anillo si  $(A, +)$  es un grupo abeliano (cuyo neutro denotaremos “0”, y donde el inverso de  $a$  le denotaremos  $-a$ ),  $(A_{\neq 0}, \cdot)$  un semigrupo (cuyo posible neutro se denota “1”, y donde el inverso de  $a$

se denota  $a^{-1}$ ) y para todo  $x, y, z$  se cumple que

$$x(y + z) = xy + xz.$$

(distributividad de  $\cdot$  respecto de  $+$ ).

Si  $(A_{\neq 0}, \cdot)$  posee neutro o es conmutativo le diremos anillo unitario o conmutativo resp. Si  $x \in A$  posee inverso respecto de  $\cdot$ , entonces diremos que es *invertible* o que es una *unidad*. Denotaremos por  $A^\times$  al conjunto de elementos invertibles de un anillo unitario  $A$ . Si  $A$  es un anillo unitario, y además  $A^\times = A_{\neq 0}$ , entonces diremos que es un anillo de división.

Si  $A$  es un anillo unitario conmutativo, entonces diremos que es un *dominio*; y si es de división conmutativo, entonces diremos que es un *cuerpo*.

Si  $x, y \in A$  son no nulos y  $xy = 0$  entonces diremos que  $x, y$  son *divisores de cero*.  $A$  se dice un *dominio íntegro* si es un dominio sin divisores de cero.

Cabe destacar que como se exige que  $(A_{\neq 0}, \cdot)$  sea un semigrupo y dijimos que el conjunto vacío no cuenta como estructura algebraica estamos exigiendo a que todo anillo tenga al menos dos elementos y que en todo cuerpo  $1 \neq 0$ . Ejemplos de cuerpos lo son  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  y  $(\mathbb{Z}_p, +, \cdot)$ . Nótese que  $(\mathbb{Z}_n, +, \cdot)$  es anillo, pero no siempre cuerpo, pues si  $n$  posee divisores propios  $p, q$  entonces  $p, q$  son divisores de cero.

**Teorema 2.2:** En todo anillo se cumple:

1.  $a0 = 0a = 0$  (aniquilador o absorbente).
2.  $a(-b) = (-a)b = -ab$  (ley de signos).
3.  $(-a)(-b) = ab$ .
4.  $-(a + b) = -a + (-b)$

**Teorema 2.3:** Si  $A$  es un anillo unitario, entonces:

1.  $(A^\times, \cdot)$  es un grupo.
2. Los divisores de cero (si los posee) no son invertibles.

**Corolario 2.4:** Todo cuerpo es un dominio íntegro.



De ahora en adelante se supondrá que  $\mathbb{k}$  representa un cuerpo con operaciones  $+$ ,  $\cdot$ , neutro aditivo  $0$  y multiplicativo  $1$ .

**Definición 2.5 – Anillo ordenado:** Se dice que una cuádrupla  $(A, +, \cdot, \leq)$  es un *anillo ordenado* si  $(A, +, \cdot)$  es un anillo linealmente ordenado por  $\leq$  tal que

- $a \leq b \implies a + c \leq b + d.$
- $a, c \geq 0 \implies ac \geq 0.$

Se les dice *positivos* (resp. *negativos*) a los elementos mayores (resp. menores) o iguales al  $0$ . Denotaremos  $A_{\geq 0}$  a los elementos de  $A$  positivos para ser consistentes con nuestra notación. Algunos libros denotan  $A^+$ ,  $A^-$  al conjunto de elementos positivos y negativos resp. Se le añade el prefijo *estrictamente* si son distintos del cero.

**Teorema 2.6:** Sea  $A$  un anillo ordenado, entonces se cumple:

1.  $a \leq b$  syss  $b - a \geq 0$ .
2.  $a \leq b$  y  $c \leq d$  implica  $a + c \leq b + d$ .
3.  $a < b$  y  $c \leq d$  implica  $a + c < b + d$ .
4.  $a \leq b$  syss  $-b \leq -a$ .
5.  $a \geq 0$  syss  $-a \leq 0$ .
6.  $a \leq b$  y  $c \geq 0$  implica  $ac \leq bc$ .
7.  $a \leq b$  y  $c \leq 0$  implica  $bc \leq ac$ .
8.  $a^2 \geq 0$ .
9.  $1 > 0$ .

**Definición 2.7 – Subanillo, ideal:** Se dice que  $\emptyset \neq B \subseteq A$  es un *subanillo* de  $A$  (denotado  $B \leq A$ ) si  $B$  es cerrado bajo las operaciones de  $A$  y sus elementos poseen inverso aditivo. Se dice que un subanillo  $I$  de  $A$  es un *ideal* (denotado  $I \trianglelefteq A$ ) si para todo  $x \in I$  y todo  $a \in A$ , se cumple que  $ax, xa \in I$  (también denotado como que  $AI, IA \subseteq I$ ).

Para todo anillo  $A$  se cumple que  $\{0\} \leq A$ , a él le diremos subanillo trivial; cabe notar que todo subanillo no trivial de  $A$  es un anillo. Además  $\{0\}, A \trianglelefteq A$ , a éstos le decimos *ideales impropios*.

**Proposición 2.8:** Si  $1 \in B \leq A$ , entonces  $B^\times \leq A^\times$ .

**Proposición 2.9 (Criterio del subanillo):**  $B \subseteq A$  es un subanillo syss para todo  $x, y \in B$  se cumple:

- $x - y \in B$ .
- $xy \in B$ .

**Lema 2.10:** La intersección arbitraria de subanillos (resp. ideales) es un subanillo (resp. ideal).

**Definición 2.11:** Luego, dado un conjunto  $S \subseteq A$  se denota:

$$\langle S \rangle := \bigcap \{B : S \subseteq B \leq A\}, \quad (S) := \bigcap \{I : S \subseteq I \trianglelefteq A\}.$$

A los ideales de la forma  $(x)$  se les dice *principales*. Es fácil ver que  $(0) = \{0\}$ , y si  $A$  es unitario entonces  $(1) = A$ . Le llamamos *dominio de ideales principales* (abreviado DIP) a un dominio cuyos ideales sean todos principales.

**Proposición 2.12:** Si  $\mathcal{F}$  es una familia no vacía de subanillos (resp. ideales) linealmente ordenado por inclusión, entonces  $S := \bigcup \mathcal{F}$  es un subanillo (resp. ideal).

DEMOSTRACIÓN: Sean  $x, y \in S$ , luego  $x \in S_x \in \mathcal{F}$  e  $y \in S_y \in \mathcal{F}$ , luego  $S_x \subseteq S_y$  o  $S_y \subseteq S_x$ , en particular  $S_z := S_x \cup S_y \in \mathcal{F}$  y contiene a ambos  $x, y$ . Como  $S_z$  es un subanillo, entonces  $x - y \in S_z \subseteq S$  y  $xy \in S_z \subseteq S$ , luego  $S$  es subanillo por el criterio.

En el caso de ideales, también es trivial ver que si  $x \in S_x \subseteq S$ , entonces  $\lambda x, x\lambda \in S_x \subseteq S$ , de modo que  $S$  es también ideal.  $\square$

**Proposición 2.13:** Si  $\emptyset \neq S \subseteq A$  conmutativo, entonces

$$(S) = \left\{ \sum_{i=1}^n \lambda_i s_i : \forall i (s_i \in S, \lambda_i \in A) \right\}.$$

En general, si tenemos un conjunto finito  $(x_i)_{i=1}^n$  y unos valores arbitrarios  $\lambda_i \in A$  a los que llamamos *ponderaciones*, entonces a los elementos de la forma

$$\sum_{i=1}^n \lambda_i x_i = \lambda_1 x_1 + \cdots + \lambda_n x_n,$$

les decimos *combinaciones lineales* de los  $x_i$ . Éstos van a ser, sobretodo, importantes en el álgebra lineal, ésto también forja un paralelo entre éste y aquél capítulo.

La proposición anterior dice que el ideal generado por un subconjunto  $S$  no vacío de un anillo es el conjunto de todas las posibles combinaciones lineales de elementos de  $S$ .

**Proposición 2.14:** Todo ideal  $I$  de un anillo unitario  $A$  es propio syss no contiene elementos invertibles.

**Corolario 2.15:** Un dominio  $A$  es un cuerpo syss no posee ideales propios. En particular, todo cuerpo es un DIP.

**Definición 2.16 – Morfismos:** Una aplicación  $\varphi : A \rightarrow B$  entre anillos se dice un *morfismo* si para todo  $a, b \in A$

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Definimos el kernel de un morfismo de anillos como  $\ker \varphi := \varphi^{-1}[0]$ .

**Proposición 2.17:** Si  $\varphi$  es un morfismo de anillos entre  $A$  y  $B$ . Entonces

1.  $\varphi(0_A) = 0_B$ .
2. Si  $\varphi$  es suprayectiva y  $A$  es unitario, entonces  $B$  también y  $\varphi(1_A) = 1_B$ .
3. Se cumple que  $\text{Img } \varphi \leq B$  y  $\ker \varphi \trianglelefteq A$ .
4.  $\varphi[A^\times] \subseteq B^\times$ .

De esta forma se cumple una especial reciprocidad entre la teoría de grupos y la de anillos. Los subgrupos son como los subanillos, y los subgrupos normales son como los ideales.

**Lema 2.18:** Dado  $I \trianglelefteq A$  propio, se cumple que  $a \equiv b \pmod{I}$  dado por  $(b-a) \in I$  es una relación de equivalencia. Esta relación cumple que si  $a \equiv c$  y  $b \equiv d \pmod{I}$ , entonces  $a + b \equiv c + d$  y  $ab \equiv cd \pmod{I}$ .

**Teorema 2.19:** Dado  $I \trianglelefteq A$  propio, entonces  $(A/I, +, \cdot)$  es también un anillo.

**Teorema 2.20 – Teoremas de isomorfismos:** Sean  $A, B$  anillos y  $\varphi : A \rightarrow B$  un morfismo, luego:

- I  $A/\ker \varphi \cong \text{Img } \varphi$ .
- II Si...
- III Si  $J \trianglelefteq I \trianglelefteq A$  y  $J \trianglelefteq A$ , entonces

$$\frac{A}{I} \cong \frac{A/J}{I/J}.$$

**Corolario 2.21:** Si  $\varphi : A \rightarrow B$  es morfismo, entonces:

1.  $\varphi$  inyectiva syss  $\ker \varphi = \{0\}$ .
2.  $\varphi$  suprayectiva syss  $A/\ker \varphi \cong B$ .

**Definición 2.22 – Dominio euclídeo:** Sea  $A$  un dominio íntegro ordenado es un *dominio euclídeo* syss existe una función  $d : A_{\neq 0} \rightarrow \mathbb{N}$ , llamada *norma euclídea*, si cumple los siguientes axiomas:

1. Si  $a, b \in A$  entonces  $d(a) \leq d(a, b)$ .
2. Si  $a, b \in A$  existen  $q, r \in A$  tales que  $b = aq + r$ , con  $d(r) < d(a)$  o  $r = 0$ .

Obsérvese que  $\mathbb{Z}$  es un dominio euclídeo, donde la norma euclídea es evidentemente el valor absoluto.

**Teorema 2.23:** Todo dominio euclídeo es un DIP.

DEMOSTRACIÓN: Sea  $A$  un dominio euclídeo de norma  $d$ . Sea  $I$  un ideal no-trivial de  $A$  y  $a \in I$  el elemento tal que  $d(a) = \min(d[I])$ .

Si  $b \in I$ , existen  $q, r \in A$  tales que  $b = aq + r$ , con  $d(r) < d(a)$  o  $r = 0$  por definición de norma euclídea. Como  $I$  es ideal,  $aq \in I$ , por ende,  $r = b - aq \in I$ . Como  $a$  es el mínimo de  $d$  en  $I$ , nos queda que  $r = 0$ ; es decir,  $b = aq \in I$ , luego  $I = (a)$ .  $\square$

**Teorema 2.24:** Sea  $A$  un dominio íntegro, entonces son equivalentes:

- (1) Todo ideal de  $A$  está finitamente generado.
- (2) Para toda cadena ascendente de ideales de  $A$

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

existe  $n$  tal que para todo  $m \geq n$  se da  $I_n = I_m$ .

- (3) Toda familia no-vacía de ideales de  $A$  admite un maximal<sup>1</sup> por inclusión ( $\subseteq$ ).

DEMOSTRACIÓN: (1)  $\implies$  (2). Sea  $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$  una cadena ascendente de ideales de  $A$ , entonces,  $I := \bigcup_{i=0}^{\infty} I_i$  (la unión de los ideales) es también un ideal, por (1),  $I$  posee un generador finito  $X$ . Luego, todo elemento de  $X$  pertenece a algún  $I_i$ , por ende, eventualmente se cumple que  $X \subseteq I_n$ , no obstante,  $I = (X) \subseteq I_n$ , por lo tanto se cumple el enunciado de (2) como se quería.

(2)  $\implies$  (3). Veamos que dicho  $I_n$  en la cadena de la prop. (2) corresponde al elemento máximo (en particular, el maximal) de dicha cadena, por ende, ambas expresiones son equivalentes.

(3)  $\implies$  (1). Si el ideal  $I$  de  $A$  no fuese finitamente generado, podríamos considerar  $a_0 \in I$  y ver que  $(a_0) \subset I$ , luego, podríamos extraer  $a_1 \in I \setminus (a_0)$  tal que  $(a_0, a_1) \subset I$  y así sucesivamente para obtener una cadena infinita sin un elemento maximal.  $\square$

**Definición 2.25 – Anillo noetheriano:** Un dominio íntegro es un *anillo noetheriano* si cumple con las condiciones del teorema 2.24.

Nótese que todo DIP es trivialmente noetheriano, por ende, todo cuerpo lo es también.

---

<sup>1</sup>Vea la expresión [TdC 2.7].

## 2.2. Divisibilidad en anillos

Curiosamente ya hemos visto como el conjunto de números enteros admite las ideas de divisibilidad, y en la siguiente sección sobre como esta propiedad se mantiene en polinomios racionales. El objetivo de esta sección es generalizar dicha propiedad en términos del álgebra moderna, también se pretende profundizar en teoría de números en el reino de la aritmética modular; por supuesto, comencemos con una definición:

**Definición 2.26 – Divisibilidad:** Sea  $A$  un dominio con  $a, b \in A$ . Escribimos  $a \mid b$  cuando existe  $q \in A$  tal que  $b = aq$ . Si dos elementos cumplen que  $a \mid b$  y  $b \mid a$ , diremos que son **asociados**.

Todas las propiedades de divisibilidad en enteros se conservan. Cabe destacar que podemos generalizar una propiedad de los enteros y notar que toda unidad  $u$  divide a todo elemento de  $A$ . Asimismo, dos elementos son asociados syss el segundo es el producto del primero por una unidad.

Los divisores de un elemento se clasifican en: *impropios* que son las unidades y los asociados de si mismo; y *propios*.

**Definición 2.27 – Irreducibles y primos:** Sea  $A$  un dominio. Diremos que un elemento es *irreducible* (resp. *reducible*) syss es no es nulo, ni una unidad, ni posee (resp. sí posee) divisores propios.

Diremos también que un elemento  $p$  es *primo* syss  $p \mid ab$  implica  $p \mid a$  o  $p \mid b$ .

De esta forma, podemos ver que todo dominio  $A$  se divide en su elemento nulo, sus unidades, sus elementos reducibles y sus irreducibles.

En caso de los enteros podemos ver que la noción de primo e irreducible concuerdan, pero ese no es siempre el caso.

**Teorema 2.28:** En un dominio íntegro  $A$  todo primo es irreducible.

DEMOSTRACIÓN: Sea  $p = xy$  un primo de  $A$  con  $x, y \in A$ . Por construcción,  $xy \mid p$ , lo que implica,  $x \mid p$  e  $y \mid p$ . También  $p \mid xy$ , por definición,  $p \mid x$  o  $p \mid y$ . Luego, alguno de los dos ( $x$  o  $y$ ) está asociado con  $p$ , por ende, el otro es una unidad; es decir,  $p$  es irreducible.  $\square$

**Definición 2.29:** Un dominio  $A$  se dice que posee la *propiedad de factorización*, cuando todo elemento reducible puede expresarse como un producto de elementos irreducibles. Dicho dominio será llamado un *dominio de factorización única* (DFU) cuando posee dicha propiedad, pero con elementos primos en su lugar y cuando todo par de factorizaciones:

$$n = p_1 \cdots p_n = q_1 \cdots q_m$$

satisfacen que  $n = m$  y que existe una permutación  $\sigma \in S_n$  tal que  $p_i$  y  $q_{\sigma(i)}$  son asociados (unicidad de la factorización).

Si no comprende la unicidad, déjeme aclarárselo con un ejemplo. El número 6 puede descomponerse en factores irreducibles como

$$6 = 2 \cdot 3 = (-3) \cdot (-2),$$

nótese que podemos reordenar los elementos (por medio de la permutación) y ver que el 2 y el  $-2$  son asociados, por tanto, no corresponde a una “factorización distinta”. En general, si  $A$  es DFU entonces todo elemento podrá escribirse de la forma

$$n = u \prod_{i=0}^k p_i^{\alpha_i},$$

donde  $u$  es una unidad,  $p_i$  es un elemento irreducible y para  $i \neq j$  se da que  $p_i$  no está asociado con  $p_j$ .

El teorema fundamental de la aritmética señala que  $\mathbb{Z}$  es un DFU.

**Teorema 2.30:** Sea  $A$  un anillo noetheriano, entonces, posee la propiedad de factorización. Si además todo irreducible es primo, entonces  $A$  es DFU.

**DEMOSTRACIÓN:** Lo probaremos por negación de la implicación, i.e., probaremos que si  $A$  no posee la propiedad de factorización entonces  $A$  no sería noetheriano.

Comencemos por construir un conjunto  $S$  que contiene: el cero, las unidades de  $A$ , sus elementos irreducibles y los productos **finitos** entre irreducibles. Luego, supongamos que  $B := A \setminus S$  fuese no-vacío, de manera que existe  $x \in B$ ; como  $x$  es reducible, existen  $y, z \in A$  no-unitarios tales que  $x = yz$ , y por lo menos alguno pertenece a  $B$ .

Utilizando esta información, crearemos una secuencia de elementos de  $B$  tales que  $x_0 = x$  y  $x_{n+1} \mid x_n$  con ambos siempre en  $B$ . En general, para  $m > n$  se tiene que  $x_m \mid x_n$ , pero  $x_n \nmid x_m$ .

Luego, el conjunto  $I = \{a : \exists n \in \mathbb{N} \ x_n \mid a\}$  es un ideal y veremos que no puede ser finitamente generado. Para ello, consideremos que los elementos  $y_0, \dots, y_k$  son pertenecientes a  $I$ . Por lo tanto, debe existir un  $m \in \mathbb{N}$  tal que  $x_m \mid y_i$  para todo  $0 \leq i \leq k$ . Dicho conjunto no puede generar el conjunto, pues de lo contrario  $x_m \mid x_n$  para todo  $n \in \mathbb{N}$  lo que es una contradicción.

Para la segunda afirmación, supondremos que  $n$  es un elemento con dos factorizaciones

$$n = \prod_{i=0}^j p_i = \prod_{i=0}^k q_i,$$

como las factorizaciones son iguales, podemos decir que se dividen entre sí, por ende,  $p_0 \mid \prod_{i=0}^k q_i$  y, como  $p_0$  es primo,  $p_0 \mid q_i$  para algún  $i = 0, \dots, k$ . Construyamos la permutación  $\sigma$  tal que  $p_0 \mid q_{\sigma(0)}$ , pero como ambos son irreducibles, son asociados. Por cancelación, nos queda que  $\prod_{i=1}^j p_i = \prod_{i=1}^k q_{\sigma(i)}$  y repetimos la operación  $j$  veces para comprobar el teorema.  $\square$

**Definición 2.31:** Sea  $A$  un anillo. Diremos que un ideal  $P$  en  $A$  es *primo* syss  $P \neq A$  y si  $I, J$  son ideales de  $A$  tales que  $IJ \subseteq P$  entonces  $I \subseteq P$  o  $J \subseteq P$ .

Diremos que un ideal  $M$  en  $A$  es *maximal* syss  $M \subseteq I \subseteq A$  implica que  $M = I$  o  $I = A$ .

**Teorema 2.32:** Un ideal  $P$  en un dominio  $A$  es primo syss  $A/P$  es un dominio íntegro.

DEMOSTRACIÓN:  $\implies$ . Nótese que como  $P \neq A$ , entonces  $1 \notin P$ , luego  $[1] \neq 0$ , es decir,  $A/P$  es un dominio. Si  $a, b \in A/P$  cumplen que  $[a][b] = [ab] = 0$ , entonces  $ab \in P$  lo que implica que  $a \in P$  o  $b \in P$  por definición, por tanto es íntegro.

$\impliedby$ . Es análogo.  $\square$

**Teorema 2.33:** Un ideal  $M$  en un dominio  $A$  es maximal syss  $A/M$  es un cuerpo.

DEMOSTRACIÓN:  $\implies$ . Como  $M \neq A$ ,  $A/M$  es un dominio. Supongamos que  $I$  es un ideal de  $A/M$  y  $f : A \rightarrow A/M$  es un homomorfismo de anillos, entonces  $J := f^{-1}(I)$  es un ideal que satisface que  $M \subseteq J \subseteq A$ , luego  $M = J$  o  $J = A$ . En el primer caso,  $I$  corresponde al ideal trivial  $(0)$ . En el segundo, corresponde al ideal  $(1)$ . Luego por el corolario ?? es un cuerpo.



$\Leftarrow$ . Es análogo. □

**Corolario 2.34:** En un dominio  $A$ , todo ideal maximal es primo.

**Teorema 2.35:** Son equivalentes:

1. **El axioma de elección.**
2. Todo ideal propio de un dominio está contenido en un ideal maximal.
3. **Teorema de Krull:** Todo dominio tiene un ideal maximal.

DEMOSTRACIÓN: (1)  $\Rightarrow$  (2). Sea  $\mathcal{F}$  la familia de los ideales propios de un dominio  $D$  que contienen a un ideal  $I$  fijo. Como  $I \in \mathcal{F}$  se da que es una familia no vacía parcialmente ordenada y toda cadena tiene supremo (su unión, por la proposición 2.12) luego  $\mathcal{F}$  tiene un elemento maximal que es un ideal.

(2)  $\Rightarrow$  (3). Basta notar que  $(0)$  es un ideal propio en todo dominio.

(3)  $\Rightarrow$  (1). En particular veremos que el teorema de Krull equivale a la siguiente proposición:

Si  $\mathcal{F}$  es una familia de conjuntos no vacíos, entonces existe  $K$  tal que para todo  $S \in \mathcal{F}$  se cumple que  $S \cap K$  es singular.

Generalizando la descripción de  $K$  diremos que es una *dispersión* de  $\mathcal{F}$  y en particular el AE equivale a que toda familia de conjuntos no vacíos posee una dispersión maximal.

<++> □

**Lema 2.36:** Sea  $A$  un dominio íntegro y  $p \in A$  no nulo, entonces:

1.  $(p)$  es primo syss  $p$  lo es.
2.  $p$  es irreducible syss  $(p)$  es maximal entre los ideales principales.

Como un DIP es un dominio, vemos que efectivamente todo irreducible es primo. Lo que sumado al teorema 2.30 nos da:

**Teorema 2.37:** Todo DIP es un DFU.

**Definición 2.38:** Sea  $A$  un DFU, entonces definiremos un *máximo común divisor* (mcd) entre dos números  $a, b \in A$  como el producto de todos los primos que dividen a ambos elevados al mínimo exponente en cada caso. Análogamente definimos un *mínimo común múltiplo* (mcm) entre ambos como el producto de todos los primos que dividen a cualquiera de los dos elevados al máximo exponente en cada caso.

Nótese que siempre, todos los mcd's y mcm's resp. son asociados entre sí.

**Teorema 2.39 – Identidad de Bézout:** Sea  $A$  un DIP con  $a_0, \dots, a_n \in A$ ; luego sea  $m$  un mcd, entonces

$$(m) = \sum_{i=0}^n (a_i) = (a_0, \dots, a_n);$$

en particular, existen  $\lambda_0, \dots, \lambda_n \in A$  tales que

$$\sum_{i=0}^n \lambda_i a_i = m.$$

DEMOSTRACIÓN: Definamos que  $(m) = \sum_{i=0}^n (a_i)$ , probaremos que  $m$  es un mcd de dicha secuencia. Evidentemente  $m \mid a_i$  para  $i = 0, \dots, n$  y si  $d$  es un divisor común, entonces  $(m) \subseteq (d)$  lo que implica  $m \mid d$ . Como el resto de mcd's son asociados, también están contenidos en  $(m)$ ; por simetría, el ideal de todos los mcd's concuerda y es el mismo.  $\square$

Nótese que conceptos como los de coprimos se mantienen igualmente.

Otro concepto, que nos será de especial utilidad en la sección sobre divisibilidad polinómica, es la de cuerpo de cocientes:

**Teorema 2.40:** Sea  $A$  un dominio, entonces, denotaremos por  $\sim$  a la relación en  $A^2$  tal que

$$(a, b) \sim (c, d) \iff ad = bc.$$

Luego  $\sim$  resulta ser una relación de equivalencia, con la cual definimos  $K := A^2 / \sim$  como el conjunto de las clases de equivalencia de  $A$ ; a  $K$  le llamamos su *cuerpo de cocientes* (también llamado *anillo o cuerpo de fracciones*), pues efectivamente resulta ser un cuerpo y posee todos los elementos de  $A$ .

## 2.3. Polinomios

Un polinomio viene a representar objetos de la forma

$$2x + 1; \quad 5xy + 6z^3; \quad 15x^2 + 3y + 2x$$

y así, y para ello surgen dos representaciones incompatibles: la analítica y la algebraica.

Para explicarlo en términos sencillos me serviré de una analogía: imagina que queremos definir el concepto de un platillo gastronómico, para ello podrías definirlo o en base a una receta o en base al resultado final. La primera es la visión de los algebristas sobre los polinomios, la segunda la de los analistas. Ambas son útiles dentro de sus contextos. Dado que la receta corresponde a una manipulación de los ingredientes, y nuestros *ingredientes* son los números de nuestras estructuras, puede darse que queramos modificar una estructura, ya sea extendiéndola o contrayéndola, lo que equivale a cambiar los ingredientes. Ésto es fatal para el platillo final, ya que es muy difícil extraer la receta del resultado para permitirnos encontrar una manera *natural* de ver la transformación del platillo; sin embargo, la receta no tiene problema, ya que basta con re-ejecutar el proceso para obtener el platillo modificado sin mayores esfuerzos.

**Ejemplo (informal).** Consideremos que trabajamos en  $\mathbb{F}_p$  y se define el polinomio  $f(x) := x^{p^2} - x^p$ . Por el pequeño teorema de Fermat es fácil ver que toma 0 en todo punto, ¿deberíamos entonces extender el polinomio como el constante 0? Consideremos  $\mathbb{F}_i := \{a + ib : a, b \in \mathbb{F}_p\}$  donde  $i^2 = -1$  y para tomar un ejemplo en concreto, sea  $p = 3$ ; luego  $f(i) = i^9 - i^3 = i - (-i) = 2i \neq 0$ . Queda al lector explicar cuándo se replica este fenómeno.

**Definición formal.** Aquí haremos un enredado ejercicio para poder definir a los polinomios como *recetas*, debido a su complejidad se deja como opcional. Para la construcción de los polinomios, primero construiremos una versión más rudimentaria: los *monomios*. El término “-nomio” significa adecuadamente “término”, de manera que queremos algo de la forma  $x^2y$ , por ejemplificar, sin preocuparse aún de “los números que acompañan los monomios”, llamados *coeficientes*.

Definiremos  $S$  como un conjunto cualquiera que contiene a las indeterminadas (usualmente denotadas  $x, y$ , etc.). Y denotaremos  $\eta : S \rightarrow \mathbb{N}$  a una función que representará un monomio, que a cada indeterminada le asigna

su exponente. Luego algo como  $x^2y$  se representa por la función

$$\eta(s) := \begin{cases} 2, & s = x \\ 1, & s = y \\ 0, & s \notin \{x, y\} \end{cases}$$

Si se admite que  $\epsilon_x$  es la función que da 1 cuando la indeterminada del argumento y del índice son iguales, y cero en otro caso, entonces podemos denotar  $\eta = 2\epsilon_x + 1\epsilon_y$ . Denotamos  $M$  al conjunto de todos los monomios.

**Definición 2.41 – Polinomio:** Finalmente, dado un anillo  $A$  y un conjunto de indeterminadas  $S$ , denotaremos  $A[S]$  al conjunto de todas las aplicaciones  $f : M \rightarrow A$  tal que  $M \setminus f^{-1}[0]$  es finito, es decir, tal que tan sólo finitos monomios poseen coeficientes no nulos. En definitiva  $f$  representa a la expresión

$$f(u_1)x_1^{u_1(x_1)} \cdots x_n^{u_1(x_n)} + \cdots + f(u_m)x_1^{u_m(x_1)} \cdots x_n^{u_m(x_n)}.$$

Definimos el grado (en inglés, *degree*) de un polinomio, como la mayor suma de exponentes por término, formalmente

$$\deg f = \max\{u(x_1) + \cdots + u(x_n) : f(u) \neq 0\}$$

Digamos que el grado de  $f$  es  $d$ , si hay un sólo término de  $f$  de grado  $d$  diremos que el coeficiente de dicho término es llamado *coeficiente director* o *lider*. Si el coeficiente director es 1, se dice que el polinomio es *mónico*.

Además definimos  $+, \cdot$  sobre  $A[S]$  de la siguiente forma, para todo  $\eta \in M$

$$(f + g)(\eta) := f(\eta) + g(\eta), \quad (f \cdot g)(\eta) := \sum_{\substack{\kappa, \lambda \in M \\ \kappa + \lambda = \eta}} f(\kappa) \cdot g(\lambda).$$

Cabe destacar que puede darse el caso que dado un polinomio no-constante de una sola indeterminada  $f$  exista un  $x \in A$  tal que  $f(x) = 0$ , en ese caso decimos que  $x$  es una *raíz* del polinomio.

En realidad, todo este proceso corresponde a una formalidad para la construcción absoluta de los polinomios, en lo sucesivo, sólo los denotaremos mediante sus representaciones, por ejemplo

$$f(x) = \sum_{i \geq 0} a_i x^i$$

el cual pertenece a  $A[x]$ . Por lo general se suelen usar polinomios de una única variable por su simpleza, cabe destacar que si estos poseen un grado digamos  $n$ , entonces es por que el término  $x^n$  es el mayor con coeficiente no nulo.

Sean  $f, g \in A[x]$ , entonces

$$(f + g)(x) := f(x) + g(x) = \sum_{i \geq 0} (a_i + b_i) x^i$$

$$(f \cdot g)(x) := f(x) \cdot g(x) = \sum_{k \geq 0} \left( \sum_{i+j=k} a_i b_j \right) x^k.$$

**Teorema 2.42:** Sea  $A$  un anillo, entonces  $(A[x], +, \cdot)$  lo es. Si  $A$  es unitario,  $A[x]$  también lo es. Si  $A$  es conmutativo,  $A[x]$  también lo es.

DEMOSTRACIÓN: Es evidente que  $(A[x], +)$  es un grupo abeliano, la asociatividad del producto se demuestra con

$$\begin{aligned} (fg)h &= \sum_{v \geq 0} \left( \sum_{u+k=v} \left( \sum_{i+j=u} a_i b_j \right) c_k \right) x^v = \sum_{v \geq 0} \left( \sum_{i+j+k=v} a_i b_j c_k \right) x^v \\ &= \sum_{v \geq 0} \left( \sum_{i+w=v} a_i \sum_{j+k=w} b_j c_k \right) x^v = f(gh), \end{aligned}$$

la distributividad es simple, puede comprobarla manualmente. Si  $A$  es unitario, entonces  $1(x) := 1 \in A[x]$  que es, asimismo, una unidad. La conmutatividad es trivial.  $\square$

Podemos afirmar sencillamente que  $\deg(f + g) \leq \max(\deg f, \deg g)$  y  $\deg(fg) \leq \deg f + \deg g$ .

**Teorema 2.43:** Sean  $f, g \in A[x]$  no nulos, de grados  $n$  y  $m$  respectivamente, tales que  $a_n, b_m$  **no** son divisores de cero, entonces

$$\deg(fg) = \deg f + \deg g.$$

DEMOSTRACIÓN: Notemos que como  $a_n, b_m$  son no nulos y no divisores de cero, se da  $\sum_{i+j=n+m} a_i b_j = a_n b_m \neq 0$ , pues para todo  $i > n$  y  $j > m$  ocurre  $a_i = b_j = 0$ , es decir,  $\deg(fg) \leq \deg f + \deg g$ , por tricotomía,  $\deg(fg) = \deg f + \deg g$ .  $\square$

Cabe destacar que como todo polinomio de una indeterminada posee coeficientes en el anillo, todo polinomio de  $(n + 1)$  indeterminadas es realmente un polinomio de una con coeficiente en el anillo de polinomios de  $n$  indeterminadas, es decir,  $A[x_1, \dots, x_n, x_{n+1}] = A[x_1, \dots, x_n][x_{n+1}]$ .

Notemos que si  $f \in A[x_1, \dots, x_n]$  entonces se escribe como prosigue

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n};$$

evidentemente,  $A[x_1, \dots, x_n]$  es siempre un anillo por inducción.

**Teorema 2.44:** Sea  $A$  un dominio íntegro, entonces  $A[x_1, \dots, x_n]$  es un dominio íntegro.

DEMOSTRACIÓN: Por el teorema anterior, sabemos que multiplicar dos polinomios no nulos incrementa su grado y por definición de grado en polinomios de múltiples variables este siempre crece, por tanto, no puede ser nulo a menos que uno de ellos sea nulo, osea, es un dominio íntegro. Para formalismos, el argumento se aplica con inducción.  $\square$

**Teorema 2.45:** Todas las unidades de un dominio íntegro  $A$  lo son también de  $A[x_1, \dots, x_n]$ .

DEMOSTRACIÓN: Por el teorema 2.43 vemos que multiplicar polinomios sólo incrementa el grado de éste, por ende, el polinomio debe ser constante para ser invertible, luego, debe ser una unidad de  $A$ .  $\square$

Similar a como en la sección 1.3 introducimos la división de números mediante un algoritmo, veremos que los polinomios comparten dicha propiedad:

**Teorema 2.46 – Algoritmo de división polinómica:** Sea  $A$  un anillo con  $\alpha \in A[x]$  un polinomio no nulo cuyo coeficiente director es una unidad de  $A$  y  $\beta \in A[x]$  cualquiera. Existen unos únicos polinomios  $q, r \in A[x]$  tales que

$$\beta(x) = \alpha(x) \cdot q(x) + r(x), \quad 0 \leq \deg r < \deg \alpha$$

DEMOSTRACIÓN: Diremos que  $n := \deg \alpha$  y  $m := \deg \beta$ . Si  $n > m$  entonces  $q = 0$  y  $r = \beta$ . De caso contrario ( $n \leq m$ ), lo probaremos por inducción sobre  $m$ .

Caso  $m = 0$ : ocurre con  $\beta(x) = b_0$  y  $\alpha(x) = a_0$ , con  $a_0$  unidad, por tanto,  $q(x) = a_0^{-1}b_0$ .

Caso  $m$ : Consideremos que  $\beta(x) = b_0 + \cdots + b_mx^m$  y  $\alpha(x) = a_0 + \cdots + a_nx^n$ , luego  $\alpha a_n^{-1}b_mx^{m-n} = \sum_{i=0}^n a_ia_n^{-1}b_mx^{m-n+i}$  posee mismo término director, por ende, existen  $q, r \in A[x]$  tales que:

$$\beta - \alpha a_n^{-1}b_mx^{m-n} = \alpha q + r$$

(por hipótesis inductiva, pues el polinomio de la izquierda tiene grado a lo más  $m-1$ ). Finalmente, pasamos el término de  $\alpha$  a la derecha para obtener que

$$\beta(x) = \alpha(x) \cdot (a_n^{-1}b_mx^{m-n} + q(x)) + r(x)$$

que satisface todas nuestras restricciones.

La unicidad de  $q, r$  se produce pues si existiese otro par  $q', r' \in A[x]$  se tendría que

$$\alpha q + r = \alpha q' + r' \iff \alpha(q - q') = r' - r$$

como son distintos, son no nulos, por lo tanto,  $\deg(r' - r) < \deg \alpha \leq \deg \alpha + \deg(q - q')$  lo que es absurdo.  $\square$

Nuevamente, a  $q(x), r(x)$  les llamamos *cociente* y *resto* resp. De igual forma, si el resto en la división entre  $\beta(x)$  sobre  $\alpha(x)$  escribiremos  $\alpha(x) \mid \beta(x)$  como si de números enteros se tratase.

**Corolario 2.47:** Si  $A$  es un cuerpo, entonces  $A[x]$  es un dominio euclídeo cuya norma es el grado.

**Teorema 2.48 – Regla de Ruffini:** Sea  $A$  un anillo con  $p(x) \in A[x]$  y  $a \in A$ . Luego la división de  $p(x)$  con  $(x - a)$  es la constante  $p(a)$ . Una consecuencia es que  $(x - a) \mid p(x)$  si y sólo si  $a$  es una raíz de  $p$ .

**Teorema 2.49:** Sea  $A$  un anillo con  $p(x) \in A[x]$  de grado  $n$ , entonces  $p$  tiene, a lo sumo,  $n$  raíces.

**Teorema 2.50 (Algoritmo de Horner-Ruffini):** Sean  $A$  un dominio íntegro con  $x_0 \in R$  y  $p(x) \in A[x]$  un polinomio de la forma  $p(x) = a_0 + \cdots + a_nx^n$ . Definase la secuencia, de forma inductiva (a la inversa):

$$b_n := a_n, \quad b_i = a_i + b_{i+1}x_0;$$

entonces se cumple que

$$p(x) = (x - x_0)(b_n x^{n-1} + \cdots + b_1) + b_0$$

DEMOSTRACIÓN: Para ver el funcionamiento del algoritmo, nótese que el polinomio puede escribirse como

$$p(x) = a_0 + x(a_1 + \cdots x(a_{n-1} + xa_n) \cdots).$$

□

Un ejemplo rápido de aplicación es dividir el polinomio  $3x^2 + 2x + 1$  sobre  $x + 1 = x - (-1)$ :

$$\begin{array}{r|rrr} & 3 & 2 & 1 \\ -1 & & 3 \cdot -1 = -3 & -1 \cdot -1 = 1 \\ \hline & 3 & 2 + (-3) = -1 & 1 + 1 = 2 \end{array}$$

**Figura 2.1.** Aplicación del algoritmo de Horner-Ruffini.

Podemos ver que es correcto, pues

$$(x - (-1))(3x + (-1)) + 2 = 3x^2 - x + 3x - 1 + 2 = 3x^2 + 2x + 1.$$

**Teorema 2.51 – Polinomio de interpolación de Lagrange:** Sea  $A$  un cuerpo con  $a_1, \dots, a_n, b_1, \dots, b_n \in A$ . Existe un único polinomio  $f \in A[x]$  de grado menor a  $n$  tal que  $f(a_i) = b_i$  para todo  $i = 1, \dots, n$ ; y está dado por la fórmula<sup>a</sup>

$$f(x) = \sum_{i=1}^n b_i \frac{P_i(x)}{P_i(a_i)}, \quad P_i(x) = \frac{\prod_{j=1}^n (x - a_j)}{x - a_i}. \quad (2.1)$$

<sup>a</sup>En análisis matemático, la expresión  $P_i(a_i)$  estaría indeterminada por ser del tipo “0/0”, no obstante, aquí, se realiza la división polinómica primero y luego se efectúa la aplicación en el punto  $a_i$ . Dicho de otro modo, no se indetermina y se entiende que se erradica el factor  $x - a_i$  del producto.

DEMOSTRACIÓN: Es fácil ver que  $P_i(a_j) = 0$  cuando  $i \neq j$ , por lo que, el polinomio de Lagrange efectivamente cumple con las condiciones indicadas. Para ver que es el único de grado menor a  $n$ , consideremos que  $g(x) \in A[x]$  también cumpliera con las condiciones, luego  $(f - g)(x)$  sería un polinomio de grado menor que  $n$  con  $n$  raíces, lo que es imposible por el teorema 2.49. □



**Teorema 2.52 – Teorema de bases de Hilbert:** Si  $A$  es un anillo noetheriano, entonces  $A[x_1, \dots, x_n]$  lo es.

DEMOSTRACIÓN: Esencialmente sólo nos basta probar que si  $A$  es noetheriano,  $A[x]$  lo es. Pues la generalización se reduce a simple inducción.

Sea  $I$  un ideal de  $A[x]$ , entonces definiremos  $I_i$  como el conjunto compuesto por todos los coeficientes directores de los polinomios de  $I$  de grado  $i$  (más el cero).

Es fácil ver que  $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$  (pues basta multiplicar por  $x$  el polinomio que justifica que  $a_i \in I_i$  para ver que pertenece también a  $I_{i+1}$ ). Aplicando la definición de noetheriano, existe un  $n$  tal que  $I_n$  es el maximal.

Sea  $I_i = (a_{i0}, \dots, a_{im})$  (nótese que si  $I_i$  se puede generar con menos de  $i$  elementos, podemos rellenar con generadores redundantes).

Luego sea  $p_{ij}$  un polinomio en  $I$  de grado  $i$  tal que todo coeficiente de grado  $k$  sea  $a_{kj}$ . Definamos  $J := (p_{ij} : i = 0, \dots, n; j = 0, \dots, m)$ . Evidentemente  $J \subseteq I$ .

Sea  $f$  un polinomio de grado  $k$  contenido en  $I$ , probaremos que  $f \in J$  por inducción sobre  $k$ . Si  $k > n$ , vemos que el coeficiente director de los polinomios  $x^{k-n}p_{n0}, \dots, x^{k-n}p_{nm}$  son  $a_{n0}, \dots, a_{nm}$  que definen  $I_k = I_n$ , luego, existen  $b_0, \dots, b_m \in A$  tales que

$$q := b_0x^{k-n}a_{n0} + \dots + b_mx^{k-n}a_{nm}$$

es un polinomio que comparte coeficiente director y grado con  $f$  (y además pertenece a  $I$ ), luego,  $f - q$  es de grado menor que  $q$  y por hipótesis inductiva, pertenece a  $J$ . El argumento es análogo si  $k \leq n$ . Con esta información se concluye que  $I \subseteq J$  lo que, por tricotomía, implica que  $I = J$ . Más concretamente, demostramos que todo ideal de  $A[x]$  está finitamente generado.  $\square$

## 2.4. Divisibilidad de polinomios

**Definición 2.53 – Contenido:** Sea  $A$  un DFU, definimos la aplicación  $c : A[x] \rightarrow \mathcal{P}(A)$ , llamada *contenido del polinomio*, como aquella tal que sea  $d$  el mcd de los coeficientes no-nulos de  $f \in A[x]$ , entonces  $c(f) = (d)$ . Definimos que  $c(0) = (0)$ .

Decimos que un polinomio es *primitivo* si  $c(f) = (1)$ , es decir, si

sus coeficientes no-nulos son coprimos. En particular, todo polinomio mónico es primitivo.

**Lema 2.54 (Lema de Gauss):** Sea  $A$  un DFU con  $f, g \in A[x]$  primitivos, entonces  $f \cdot g$  es primitivo.

DEMOSTRACIÓN: Sean  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  y  $g(x) = b_0 + \cdots + b_mx^m$ , entonces  $f \cdot g(x) = c_0 + \cdots + c_{n+m}x^{n+m}$ . Sea  $p$  un número primo y digamos que divide a todos los  $a_i$  con  $i < u$  y los  $b_i$  con  $i < v$ , entonces

$$p \mid c_{u+v} - a_ub_v = \sum_{i=0}^{u-1} b_i c_{u+v-i} + \sum_{i=0}^{v-1} b_{u+v-i} c_i$$

debido a que  $p$  divide los términos en rojo. Pero como  $p \nmid a_u, b_v$  concluimos que  $p \nmid c_{u+v}$ .  $\square$

**Teorema 2.55:** Sean  $f, g \in A[x]$  y  $k \in A$ , entonces

- a)  $c(kf) = (k)c(f)$ .
- b)  $c(fg) = c(f)c(g)$ .

DEMOSTRACIÓN: a) Por propiedades del mcd.

- b) Consideremos que  $c(f) = a$ ,  $c(g) = b$ ; por lo que  $f = af^*$ ,  $g = bg^*$  con  $f^*, g^*$  primitivas. Entonces  $c(fg) = c((ab)f^*g^*) = (ab)c(f^*g^*)$ . Pero por lema de primitividad de Gauss,  $f^*g^*$  es primitiva, por ende el teorema.  $\square$

**Lema 2.56:** Sea  $A$  un DFU con  $K$  su cuerpo de cocientes y  $f, g \in A[x]$  polinomios primitivos no-constantos.  $f$  y  $g$  son asociados en  $K[x]$  syss lo son en  $A[x]$ .

DEMOSTRACIÓN: Si lo son, entonces existen  $a, b \in A$  no-nulos tales que  $f = (a/b)g$ , es decir,  $af = bg$ . Observe que

$$(a) = (a)c(f) = c(af) = c(bg) = (b)c(g) = (b),$$

por lo que  $a, b$  son asociados y existe una unidad  $u \in A$  tal que  $b = au$ . Con esto  $af = bg = aug$ , por cancelación, nos queda que, efectivamente,  $f, g$  son asociados en  $A[x]$ .  $\square$

**Teorema 2.57:** Si  $f \in \mathbb{k}[x]$  es de grado 2 o 3, entonces es irreducible syss no posee raíces.

DEMOSTRACIÓN: Por regla de Ruffini es claro que si es irreducible no posee raíces. Para el caso recíproco basta considerar que toda posible factorización incluye un término de grado 1.  $\square$

**Teorema 2.58 – Criterio de Irreducibilidad de Gauss:** Sea  $A$  un DFU,  $K$  su cuerpo de cocientes y  $f \in A[x]$  un polinomio primitivo no-constante.  $f$  es irreducible en  $A[x]$  syss lo es en  $K[x]$ .

DEMOSTRACIÓN:  $\Leftarrow$ . Éste caso es trivial.

$\Rightarrow$ . Supongamos que  $f$  es reducible en  $K[x]$ , pero no en  $A[x]$ , por lo que  $f = gh$  con  $g, h \in K[x]$ . Esto significa que

$$g(x) = \sum_{i=0}^n \frac{a_i}{b_i} x^i, \quad h(x) = \sum_{i=0}^m \frac{c_i}{d_i} x^i$$

con  $b_i, c_i$  no-nulos. Definamos  $b := \prod_{i=0}^n b_i$  y  $\tilde{b}_i := b/b_i$  con lo que  $g_1(x) = \sum_{i=0}^n a_i \tilde{b}_i x^i$  de contenido  $u$ , por lo que  $g_2 := g_1/u$ . Por lo que  $g = (b/u)g_2$  y  $h = (d/v)h_2$ , es decir,

$$f = \frac{bd}{uv} g_2 h_2$$

como  $u, v$  son no-nulos,  $f$  y  $g_2 h_2$  son primitivos asociados en  $K[x]$ , luego lo son en  $A[x]$ .  $\square$

**Teorema 2.59 – Criterio de Irreducibilidad de Eisenstein:** Sean  $A$  un DFU,  $K$  su cuerpo de cocientes y  $f = \sum_{i=0}^n a_i x^i \in A[x]$  no-constante. Sea  $p \in A$  un primo, luego  $f$  es irreducible en  $K$  si:

1.  $p \nmid a_n$ .
2.  $p \mid a_i$  para  $i = 0, 1, \dots, n-1$ .
3.  $p^2 \nmid a_0$ .

DEMOSTRACIÓN: Supondremos que  $f = af^*$  con  $f^*$  primitiva ( $a$  es una unidad en  $K$ ), de modo que si fuese reducible en  $K$  existirían  $g = \sum_{i=0}^r b_i x^i, h = \sum_{i=0}^s c_i x^i \in A[x]$  primitivos, no-constantes, tales que  $f^* = gh$ . Nótese que

$a_0^* = b_0 c_0$ , por lo que  $p \mid b_0$  o  $p \mid c_0$ , pero no ambos (restricción por construcción), por ello supondremos el primer caso.

$p$  no puede dividir todos los  $b_i$  por ser  $g$  primitiva, así que digamos que sea  $k$  el primer índice tal que  $p \nmid b_k$  con  $0 < k \leq r < n$ . Sabemos que  $p \mid a_k = \sum_{i+j=k} b_i c_j$ , además de dividir todos los términos individualmente a excepción del último, por lo que,  $p$  divide a la resta (que da como resultado  $b_k c_0$ ), pero  $p \nmid b_k$  y  $p \nmid c_0$ , lo que sería absurdo.  $\square$

**Teorema 2.60:** Sea  $A$  un dominio con  $a \in A$  invertible y  $b \in A$  cualquiera, entonces  $p(x)$  es irreducible syss  $p(ax + b)$  lo es.

DEMOSTRACIÓN: Para demostrarlo veremos que  $f : A[x] \rightarrow A[x]$  donde  $f(p(x)) = p(ax + b)$  es un isomorfismo de anillos. Es claro que es un homomorfismo, y como  $g(x) = ax + b$  es una biyección, comprobamos el enunciado.  $\square$

**Corolario 2.61:** Para todo  $p$  primo, llamamos polinomio ciclotómico  $p$ -ésimo a

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1},$$

los cuales son irreducibles en  $\mathbb{Q}[x]$ .

DEMOSTRACIÓN: Es una aplicación directa del criterio de Eisenstein usando la composición

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k.$$

Nótese que el polinomio es mónico, así que  $p$  no divide al coeficiente director, mientras que el término constante es  $p$  así que  $p^2 \nmid p$ , y para el resto basta notar que el denominador es de la forma  $n!$  con  $n < p$ , así que no “cancela” el término con  $p$ , luego  $p \mid \binom{p}{n}$ .  $\square$

Usualmente se suelen aplicar en conjunto el criterio de Eisenstein con el teorema anterior para demostrar la irreducibilidad de un polinomio. Por ejemplo, utilizando el mismo polinomio que en la aplicación del algoritmo de Horner-Ruffini,  $p(x) = 3x^2 + 2x + 1$ , probaremos que es irreducible en  $\mathbb{Q}$ , primero multiplicamos todos los términos por 3 para obtener  $3p(x) = 9x^2 + 6x + 3$ , luego consideremos el polinomio

$$3p\left(\frac{1}{3}(x+1)\right) = (x+1)^2 + 2(x+1) + 3 = x^2 + 2x + 1 + 2x + 2 + 3 = x^2 + 4x + 6$$

que es irreducible por criterio de Eisenstein. Recuerde que 3 es una unidad de  $\mathbb{Q}$  y como el polinomio original es primitivo, entonces es irreducible también en  $\mathbb{Z}$ .

**Teorema 2.62 – Teorema de las raíces racionales:** Sea  $A$  un DFU,  $K$  su cuerpo de cocientes y  $p(x) \in A[x]$  un polinomio no-constante:

$$p(x) = \sum_{i=0}^n c_i x^i.$$

Si  $\alpha = a/b$ , con  $a, b \in A$  coprimos, es una raíz de  $p(x)$ , entonces  $a \mid c_0$  y  $b \mid c_n$ .

DEMOSTRACIÓN: Como  $\alpha = a/b$  es una solución

$$\sum_{i=0}^n \frac{a^i}{b^i} c_i = 0,$$

multiplicando por  $b^n$  y aplicando técnicas de despeje obtenemos las dos ecuaciones siguientes:

$$\begin{aligned} a^n c_n &= -b \sum_{i=0}^{n-1} a^i b^{n-1-i} c_i \\ b^n c_0 &= -a \sum_{i=1}^{n-1} a^{i-1} b^{n-i} c_i, \end{aligned}$$

en las cuales, evidentemente los factores resultan ser elementos de  $A$ , por lo que,  $b \mid a^n c_n$  y  $a \mid b^n c_0$ , pero como  $a, b$  son coprimos, nos resulta que  $b \mid c_n$  y  $a \mid c_0$  tal como lo indica el enunciado.  $\square$

Esto es útil tanto para buscar raíces racionales que con aplicar la regla de Ruffini simplifican los polinomios, como para comprobar la irracionalidad de ciertas raíces, en particular para otorgar otra demostración que  $\sqrt{2} \notin \mathbb{Q}$ , pero que se generaliza a que para todo primo  $p$  se cumple que  $\sqrt{p} \notin \mathbb{Q}$ .

**Corolario 2.63:** Sea  $A$  un DFU,  $K$  su cuerpo de cocientes y  $p(x) \in A[x]$  un polinomio no-constante mónico, entonces  $\alpha \in K$  es una raíz de  $p$  si y sólo si  $\alpha \in A$ .

### §2.4.1 Raíces básicas.

**Definición 2.64:** Dado  $\alpha \in \mathbb{k}$ , decimos que  $\beta$  es una  $n$ -ésima raíz de  $\alpha$  si  $\beta^n = \alpha$  o alternativamente si  $\beta$  es raíz del polinomio  $x^n - \alpha$ .

**Lema 2.65:** Si  $\beta$  es una raíz cuadrada de  $\alpha$ , entonces  $-\beta$  y  $\beta$  son todas las raíces cuadradas de  $\alpha$ .

**Teorema 2.66 (Fórmula cuadrática):** Si  $p(x) = x^2 + rx + s$ , entonces llamamos definimos  $\Delta := r^2 - 4s$  como el *discriminante* de  $p(x)$ . Finalmente  $p$  tiene raíces syss existe  $\alpha$  raíz cuadrada de  $\Delta$ , en cuyo caso las raíces de  $p$  son

$$\frac{-r + \alpha}{2}, \quad \frac{-r - \alpha}{2}.$$

DEMOSTRACIÓN: Es fácil comprobar que éste es el caso, pero la deducción viene de que si

$$\begin{aligned} x^2 + rx + s = 0 &\iff x^2 + 2x \cdot \frac{r}{2} = -s \\ &\iff x^2 + 2x \cdot \frac{r}{2} + \frac{r^2}{4} = \left(x - \frac{r}{2}\right)^2 = \frac{r^2}{4} - s = \frac{\Delta}{4} \end{aligned}$$

Luego si  $\alpha$  es raíz de  $\Delta$ , entonces  $\pm\alpha/2 = x - r/2$  y así se deduce el enunciado.  $\square$

**Corolario 2.67:** Un polinomio de grado 2 es irreducible syss su discriminante no posee raíces cuadradas.

## 2.5. Números complejos

Rigurosamente los números complejos emergen por las llamadas extensiones de Kronecker, que se ven más adelante, de modo que se introduce la unidad imaginaria  $i$  como raíz del polinomio real irreducible  $x^2 + 1$ . Aquí haremos una definición alternativa de los números complejos que permitirá al lector acostumbrarse a ellos.

**Definición 2.68 – Números complejos:** Se define  $\mathbb{C}$  como el conjunto  $\mathbb{R}^2$  con las operaciones:

$$(a, b) + (c, d) := (a + c, b + d), \quad (a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Usualmente denotamos  $(a, b) = a + ib$ . Pues  $(1, 0)$  se comporta como

el neutro multiplicativo,  $(0, 0)$  como el neutro aditivo e  $i^2 = (0, 1)^2 = (-1, 0) = -1$ . También se definen las funciones  $\text{Re}, \text{Im} : \mathbb{C} \rightarrow \mathbb{R}$  como

$$\text{Re}(a + ib) = a, \quad \text{Im}(a + ib) = b,$$

las que se llaman *parte real* e *imaginaria*, resp.

También, denotamos

$$|a + ib| := \sqrt{a^2 + b^2}, \quad \overline{a + ib} := a - ib,$$

donde a  $|z|$  se le dice el *módulo*<sup>a</sup> de  $z$  y a  $\bar{z}$  el *conjugado* de  $z$ .

<sup>a</sup>Algunos textos prefieren usar  $\|\cdot\|$  para los complejos y dejar  $|\cdot|$  para los reales. Mi convenio es usar  $\|\cdot\|$  para sus espacios vectoriales.

**Proposición 2.69:** Para todo  $z, w \in \mathbb{C}$  se cumple:

1.  $|z| = 0$  syss  $z = 0$ .
2.  $\bar{\bar{z}} = z$ .
3.  $|\bar{z}| = |z|$ .
4.  $z + \bar{z} = 2 \text{Re } z$  y  $z - \bar{z} = 2i \text{Im } z$ .
5.  $\overline{z + w} = \bar{z} + \bar{w}$  y  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$ . En otras palabras,  $\bar{\cdot}$  es un automorfismo de cuerpos.
6.  $x \in \mathbb{R}$  syss  $\bar{x} = x$  syss  $i\bar{x} = -x$ .
7.  $z \cdot \bar{z} = |z|^2$ .
8.  $|zw| = |z| |w|$ .

**Teorema 2.70:**  $(\mathbb{C}, +, \cdot)$  es un cuerpo.

DEMOSTRACIÓN: Lo único que no es obvio es que la existencia de los inversos multiplicativos, lo cual se consigue notando que si  $z \in \mathbb{C}_{\neq 0}$ , entonces  $z^{-1} = \bar{z}/|z|^2$  mediante las propiedades anteriores.  $\square$

**Teorema 2.71:** La aplicación  $x \mapsto (x, 0)$  es un monomorfismo de cuerpos. Esto se interpreta como que  $\mathbb{C}$  contiene un subcuerpo isomorfo a  $\mathbb{R}$ .

**Proposición 2.72:** Todo complejo tiene raíz cuadrada. En consecuencia, todo polinomio cuadrático es reductible en los complejos.

**Proposición 2.73:** Si  $P, Q \in \mathbb{C}[x]$ , entonces:

1. Para todo  $z \in \mathbb{C}$  que  $\overline{P}(\bar{z}) = \overline{P(z)}$ .
2.  $P \in \mathbb{R}[x]$  syss  $P(z) = \overline{P(z)}$ .
3. Si  $R := P \cdot Q$ , entonces  $\overline{R} = \overline{P} \cdot \overline{Q}$ .
4. Si  $P \in \mathbb{R}[x]$  tiene raíz compleja  $z$ , entonces  $\bar{z}$  también es raíz.
5.  $P \cdot \overline{P} \in \mathbb{R}[x]$ .

**Definición 2.74:** Se define la función  $\text{cis} : \mathbb{R} \rightarrow \mathbb{C}$  tal que

$$\text{cis } \theta := \cos \theta + i \sin \theta.$$

Y se define  $\arg : \mathbb{C}_{\neq 0} \rightarrow (-\pi, \pi]$  así:

$$\arg(x + iy) = \begin{cases} \arctan(y/x), & x > 0 \\ \arctan(y/x) + \pi, & x < 0 \wedge y \geq 0 \\ \arctan(y/x) - \pi, & x < 0 \wedge y < 0 \\ \pi/2, & x = 0 \wedge y > 0 \\ -\pi/2, & x = 0 \wedge y < 0 \end{cases}$$

**Proposición 2.75:** Si  $z \in \mathbb{C}_{\neq 0}$ , entonces  $z = |z| \text{cis}(\arg z)$ .

**Teorema 2.76 – Teorema de De Moivre:** Si  $u = r \text{cis } \alpha$  y  $v = s \text{cis } \beta$ , entonces

$$u \cdot v = rs \text{cis}(\alpha + \beta). \quad (2.2)$$

En particular

$$u^n = r^n \text{cis}(n\alpha). \quad (2.3)$$

DEMOSTRACIÓN: Basta notar que

$$\begin{aligned} u \cdot v &= rs(\text{cis } \alpha \cdot \text{cis } \beta) \\ &= rs(\cos \alpha \cos \beta - \sin \alpha \sin \beta + i(\sin \alpha \cos \beta + \cos \alpha \sin \beta)) \end{aligned}$$



$$= rs(\cos(\alpha + \beta) + i \sin(\alpha + \beta)) = rs \operatorname{cis}(\alpha + \beta)$$

como se quería probar.  $\square$

**Corolario 2.77:** Todo  $z \in \mathbb{C}$  tiene una raíz  $n$ -ésima compleja, dada por

$$|z|^{1/n} \operatorname{cis}\left(\frac{\arg z}{n}\right).$$

**§2.5.1 El teorema fundamental del álgebra I.** Usando un poco de cálculo diferencial de una variable se otorga una demostración al teorema fundamental del álgebra.

**Lema 2.78:** Si  $f \in \mathbb{C}[x]$  es no constante, entonces  $|f(z)| \rightarrow \infty$  si  $|z| \rightarrow \infty$ . Dicho de otro modo, para todo  $R > 0$  existe  $r > 0$  tal que para todo  $|z| \geq r$  se cumple que  $|f(z)| \geq R$ .

DEMOSTRACIÓN: En particular probaremos que

$$\lim_{|z| \rightarrow \infty} \frac{|f(z)|}{|z|^n} = |c_n|$$

Esto se cumple pues si

$$f(z) = c_n z^n + \cdots + c_1 z + c_0$$

entonces

$$\frac{|f(z)|}{|z|^n} \geq |c_n| + |c_{n-1}| |z|^{-1} + \cdots + |c_0| |z|^{-n}$$

lo que converge a  $|c_n|$  y que

$$|f(z)| \geq |c_n| |z|^n - |z|^{n-1}(|c_{n-1}| + \cdots + |c_0| |z|^{1-n})$$

Luego, basta exigir que  $|z| > 1$  para ver que

$$\frac{|f(z)|}{|z|^n} \geq |c_n| - \frac{1}{|z|}(|c_{n-1}| + \cdots + |c_1| + |c_0|)$$

de lo que se concluye el enunciado.  $\square$

**Lema 2.79:** Para todo  $f \in \mathbb{C}[x]$  no constante, existe  $x_0$  que minimiza  $|f(x_0)|$ .

DEMOSTRACIÓN: Sea  $R := |f(0)| + 1$ , por el lema anterior existe  $r$  tal que para todo  $|z| \leq r$  se cumple que  $|f(z)| \leq R$ . Luego como la imagen continua de compactos es compacta, entonces  $|f|$  alcanza su mínimo en  $\overline{B}_r(0)$ , que es mínimo en todo el dominio.  $\square$

**Teorema 2.80 – Teorema fundamental del álgebra:** Todo polinomio no constante en  $\mathbb{C}$  tiene al menos una raíz.

DEMOSTRACIÓN: Por el lema anterior todo polinomio alcanza su mínimo en módulo, así que probaremos que ese mínimo no puede ser no nulo. Sea  $f \in \mathbb{C}[x]$  y  $x_0$  el punto que le minimiza a un valor no nulo. Reemplazando  $g(x) := f(x_0 + x)/|f(x_0)|$  se obtiene que  $g(0) = 1$ , basta probar que el mínimo de  $g$  no es 1. Sea  $k$  el mínimo natural no nulo tal que  $g$  posee un término no nulo con  $z^k$ , es decir, que  $g$  es de la forma

$$g(z) = 1 + az^k + \dots,$$

luego, si  $\alpha$  es una  $k$ -ésima raíz de  $a$ , entonces

$$g(\alpha z) = 1 - z^k + z^{k+1}h(z)$$

donde  $h \in \mathbb{C}[x]$ .

Por desigualdad triangular

$$|g(\alpha z)| \leq |1 - z^k| + |z|^{k+1}|h(z)|,$$

luego si  $x$  es un real tal que  $x \in [0, 1)$ , entonces

$$|g(\alpha x)| \leq 1 - x^k(1 - x|h(x)|)$$

por lo que, por límites existe un  $x_1 \in (0, 1)$  tal que  $x_1|h(x_1)| < 1$ , por ende,  $|g(\alpha x_1)| < 1$  contradiciendo la minimalidad de  $g(0) = 1$ .  $\square$

Parte II.

---

# ÁLGEBRA LINEAL

---



## 3

---

### Módulos

---

Uno de los objetivos del álgebra lineal es el de poder desarrollar las llamadas ecuaciones lineales, para las cuales introduciremos objetos vitales bajo los nombres de *vectores* y *matrices* que se vuelven fundamentales en el contexto del álgebra lineal.

#### 3.1. Módulos y vectores

**Definición 3.1 – Módulos y vectores:** Dado un anillo unitario  $A$ , diremos que una terna  $(M, +, \cdot)$  es un  $A$ -módulo izquierdo (resp. derecho) si  $+$  :  $M^2 \rightarrow M$  y  $\cdot$  :  $A \times M \rightarrow M$  tales que  $(M, +)$  es un grupo abeliano (de neutro  $\vec{0}$ ) y para todo  $\vec{u}, \vec{v} \in M$  y  $\alpha, \beta \in A$  se cumple:

1.  $\alpha(\beta\vec{u}) = (\alpha\beta)\vec{u}$ .
2.  $1\vec{u} = \vec{u}$ .
3.  $\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$ .
4.  $(\alpha + \beta)\vec{u} = \alpha\vec{u} + \beta\vec{u}$ .

Si  $A$  es un anillo de división entonces diremos que  $M$  es un  $A$ -espacio vectorial, a los elementos de  $M$  les diremos *vectores* y a los de  $A$  *escalares*.

**Proposición 3.2:** Si  $M$  es un  $A$ -módulo, entonces:

1. Para todo  $\alpha \in A$  se cumple que  $\alpha \cdot \vec{0} = \vec{0}$ .
2. Para todo  $\vec{v} \in M$  se cumple que  $0 \cdot \vec{v} = \vec{0}$ .
3. Para todo  $\vec{v} \in M$  se cumple que  $(-1)\vec{v} = -\vec{v}$ .

**Definición 3.3 – Morfismos de módulos:** Una aplicación  $f : M \rightarrow N$  se dice un morfismo de  $A$ -módulos si para todo  $\vec{u}, \vec{v} \in M$  y  $\lambda \in A$  se comprueba

$$f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v}), \quad f(\lambda \vec{u}) = \lambda f(\vec{u}).$$

Nuevamente la nomenclatura categórica se extiende a morfismos de módulos. El espacio de morfismos de  $A$ -módulos desde  $M$  a  $N$  se denota por  $\text{Hom}_A(M, N)$ . Las funciones de  $\text{Hom}_A(U, A)$  se dicen *funcionales*.

Un morfismo entre espacios vectoriales se dice una *función lineal*.

**Ejemplos.** Son  $A$ -módulos:

- $A^n$  con la suma y el producto por escalar coordenada a coordenada.
- $\text{Func}(S; A)$  con  $(f + g)(s) := f(s) + g(s)$  y  $(\alpha f)(s) := \alpha \cdot f(s)$  para  $\alpha \in A$  y  $s \in S$ .
- $A[S]$  de forma análoga a  $\text{Func}(S; A)$ .
- $I$  con la suma y el producto, donde  $I$  es ideal de  $A$ .
- $B$ , donde  $B$  es un anillo tal que  $A$  es subanillo de  $B$ .
- $\text{Hom}_A(U, V)$  de forma análoga a  $\text{Func}(S; A)$ .

**Proposición 3.4:** Dados  $X, Y$  no vacíos se cumple que  $\text{Func}(X; A) \cong \text{Func}(Y; A)$  si y sólo si  $|X| = |Y|$ . Luego, dado un cardinal  $\kappa$  denotamos  $A^\kappa$  a un  $A$ -módulo  $\text{Func}(S; A)$  genérico<sup>1</sup> con  $|S| = \kappa$ .

<sup>1</sup>En particular consideramos la representación ordinal-conjuntista de  $\kappa$ .

**Definición 3.5 – Submódulo:** Dado  $M$  un  $A$ -módulo, se dice que  $N$  es submódulo de  $M$  (denotado  $N \leq M$ ) si  $N$  es también un  $A$ -módulo. Trivialmente,  $M$  y  $\{0\}$  son submódulos de  $M$  y se dicen *impropios*. Un submódulo se dice *simple* (o *irreducible*) si no admite submódulos propios.

**Teorema 3.6 (Criterio del submódulo):**  $N$  es submódulo del  $A$ -módulo  $M$  si y sólo si  $N$  es no vacío y para todo  $\vec{u}, \vec{v} \in N$  y todo  $\lambda \in A$  se cumple que  $\lambda\vec{u} + \vec{v} \in N$ .

**Lema 3.7:** La intersección de submódulos es un submódulo.

**Definición 3.8:** Si  $S \subseteq M$  donde  $M$  es un  $A$ -módulo, se le llama *submódulo generado por  $S$*  a

$$\langle S \rangle := \bigcap \{N : S \subseteq N \leq M\}.$$

Se dice que  $S$  es un *sistema generador* de  $M$  si  $\langle S \rangle = M$ .

**Proposición 3.9:** Se cumple que

$$\langle S \rangle = \left\{ \sum_{i=1}^n \lambda_i x_i : \forall i (\lambda_i \in A \wedge x_i \in S) \right\}.$$

**Definición 3.10 – Suma de submódulos:** Si  $\{N_i\}_{i \in I}$  son submódulos de  $M$ , entonces se define su suma como

$$\sum_{i \in I} N_i := \left\langle \bigcup_{i \in I} N_i \right\rangle,$$

en particular  $S + T := \langle S \cup T \rangle$ .

Se dice que una familia de submódulos  $\{N_i\}_{i \in I}$  es *independiente* si para todo  $i \in I$  se cumple que  $N_i \cap \sum_{j \neq i} N_j = \{0\}$ . La suma de una familia independiente de submódulos se dice *directa* y se denota como  $\bigoplus_{i \in I} N_i$ .

**Proposición 3.11:** Si  $N$  es un submódulo del  $A$ -módulo  $M$ , entonces  $x \equiv y \pmod{N}$  definido porque  $x - y \in N$  es una relación de equivalencia,

bajo la cuál se denota por  $M/N$  al conjunto cociente que también resulta ser un  $A$ -módulo.

**Teorema 3.12 – Teoremas de isomorfismos:** Se cumple:

I Si  $M, N$  son  $A$ -módulos y  $\varphi : M \rightarrow N$  un morfismo, entonces

$$\frac{M}{\ker \varphi} \cong \text{Img } \varphi.$$

II Si  $S, T$  son submódulos del  $A$ -módulo  $M$ , entonces

$$\frac{S}{S \cap T} \cong \frac{S+T}{T}.$$

III Si  $S \leq T \leq M$ , entonces

$$\frac{M}{T} \cong \frac{M/S}{T/S}.$$

**Teorema 3.13:** Sea  $M$  un  $A$ -módulo y  $\{N_i\}_{i \in I}$  una familia de submódulos tales que  $M = \sum_{i \in I} N_i$ , son equivalentes:

- a)  $M = \bigoplus_{i \in I} N_i$ .
- b) Si  $\sum_{i \in I} m_i = 0$  con  $m_i \in N_i$  para todo  $i \in I$ , entonces  $m_i = 0$ .
- c) Para todo  $m \in M$  existen unos únicos  $m_i \in N_i$  para cada  $i \in I$  tales que

$$m = \sum_{i \in I} m_i.$$

DEMOSTRACIÓN: a)  $\implies$  b). Procedemos a demostrarlo por contradicción, supongamos que existe un subconjunto  $J \subseteq I$  tal que

$$\sum_{j \in J} m_j = 0$$

con  $m_j \neq 0$  para todo  $j \in J$ . Tomemos un  $j_0 \in J$  tal que  $m_{j_0} \neq 0$ , evidentemente  $m_{j_0} = \sum_{j \in J \setminus \{j_0\}} -m_j$ . Luego

$$m_{j_0} \in N_{j_0} \cap \sum_{j \in J \setminus \{j_0\}} N_j \subseteq N_{j_0} \cap \sum_{i \in I \setminus \{j_0\}} N_i.$$



b)  $\implies$  c). Consideraremos el siguiente homomorfismo

$$\begin{aligned} f : \prod_{i \in I} N_i &\longrightarrow M \\ (m_i)_{i \in I} &\longmapsto \sum_{i \in I} m_i, \end{aligned}$$

por construcción, sabemos que corresponde a un epimorfismo, y la propiedad b) nos asegura que  $\ker f = (0)_{i \in I}$ , por ende es un monomorfismo.

c)  $\implies$  a). También por contradicción, sea  $m \in M$  con dos descomposiciones

$$m = \sum_{i \in I} m_i = \sum_{i \in I} n_i.$$

Luego para algún  $i \in I$  ha de darse que  $m_i \neq n_i$ , luego

$$0 \neq m_i - n_i = \sum_{j \neq i} n_j - m_j$$

luego  $m_i - n_i \in N_i \cap \sum_{j \neq i} N_j$  que es absurdo.  $\square$

## 3.2. Módulos libres y bases

**Definición 3.14:** Sea  $M$  un  $A$ -módulo con  $X \subseteq M$ . Diremos que  $X$  es *libre* o que sus elementos son *linealmente independientes* si la ecuación

$$\lambda_0 x_0 + \cdots + \lambda_n x_n = 0$$

se da con  $x_i \in X$  distintos dos a dos y  $\lambda_i \in A$  siempre que  $\lambda_i = 0$  para todo  $i = 0, \dots, n$ . De lo contrario decimos que el conjunto está *ligado* o que hay elementos que son *linealmente dependientes* entre sí.

Si,  $X$  es un conjunto libre y además es un sistema generador, diremos que  $X$  es una *base* de dicho módulo. Si  $M$  posee alguna base, entonces, se dice que es *libre*.

**Ejemplo.** Es fácil notar que con la suma y producto normal  $\mathbb{Q}$  es un  $\mathbb{Z}$ -módulo, sin embargo, no es libre (¿por qué?).

**§3.2.1 Finitamente generados.** De momento nos referiremos a módulos finitamente generados como aquellos que poseen un sistema generador finito. Ciertamente hay algunos que no lo poseen, pero sus resultados suelen ser más complicados.

**Teorema 3.15:** Sea  $M$  un  $A$ -módulo, entonces  $M \cong A^n$  syss posee una base de cardinal  $n$ .

DEMOSTRACIÓN: Notemos que si  $X$  es una base cualquiera de  $M$ , entonces

$$M = \bigoplus_{x \in X} \langle x \rangle;$$

luego es isomorfo a  $\prod_{x \in X} \langle x \rangle$  y  $\langle x \rangle \cong A$  trivialmente para todo  $x \in X$ .  $\square$

**Lema 3.16:** Si  $S$  es ligado en un espacio vectorial, entonces existe un  $\vec{v} \in S$  que es generado por el resto, es decir, tal que  $\vec{v} \in \langle S \setminus \{\vec{v}\} \rangle$ .

**Teorema 3.17:** Si  $G$  es un sistema generador ligado, entonces  $\vec{v} \in G$  está generado por el resto de  $G$  syss  $G \setminus \{\vec{v}\}$  es un sistema generador. Si  $S$  es libre en un espacio vectorial y  $\vec{v}$  no es generado por  $S$ , entonces  $S \cup \{\vec{v}\}$  es libre.

**Corolario 3.18:** Todo sistema generador finito contiene una base, en consecuencia, todo espacio vectorial finitamente generado es libre.

**Teorema 3.19:** Todo par de bases de un espacio vectorial finitamente generado posee el mismo cardinal.

DEMOSTRACIÓN: Sean  $X := \{x_1, \dots, x_n\}$  e  $Y$  bases tal que  $|X| \leq |Y|$  (en principio,  $Y$  podría ser infinito). Sea  $y_1 \in Y$  cualquiera, como  $y_1 \in V = \langle X \rangle$ , entonces existen  $\alpha_{1,i} \in \mathbb{k}$  tales que

$$y_1 = \sum_{i=1}^n \alpha_{1,i} x_i$$

como  $y_1 \neq 0$  algún  $\alpha_{1,i}$  ha de ser no nulo y reordenando supongamos que  $\alpha_{1,1} \neq 0$ , luego

$$x_1 = \frac{1}{\alpha_{1,1}} y_1 - \sum_{i=2}^n \frac{\alpha_{1,i}}{\alpha_{1,1}} x_i,$$

llamando  $B_0 := X$  y  $B_1 := B_0 \setminus \{x_1\} \cup \{y_1\}$ , como  $X \subseteq \langle B_1 \rangle$ , entonces  $B_1$  es base y posee  $n$  elementos.

Análogamente se escoge  $y_2 \in Y \subseteq V = \langle B_1 \rangle$ , luego existen  $\alpha_{2,i} \in \mathbb{k}$  tales que

$$y_2 = \alpha_{2,1} y_1 + \sum_{i=2}^n \alpha_{2,i} x_i$$

notamos que algún  $\alpha_{2,i}$  con  $i > 1$  ha de ser no nulo y reordenamos para que  $\alpha_{2,2} \neq 0$ , luego

$$x_2 = \frac{1}{\alpha_{2,2}} - \left( \frac{\alpha_{2,1}}{\alpha_{2,2}} y_1 + \sum_{i=3}^n \frac{\alpha_{2,i}}{\alpha_{2,2}} x_i \right),$$

de modo que si  $B_2 := B_1 \setminus \{x_2\} \cup \{y_2\}$  entonces  $B_2$  es base.

Iterando el proceso anterior,  $B_n$  resulta ser base y estar formado solamente a partir de elementos de  $Y$ , luego  $Y = B_n$  pues de tener elementos aparte sería ligado y es claro que  $B_n$  posee  $n$  elementos.  $\square$

**Corolario 3.20:** Todo conjunto libre en un espacio vectorial finitamente generado se puede extender a una base.

**Definición 3.21 – Dimensión:** Si  $V$  es un  $\mathbb{k}$ -espacio vectorial y sus bases son equipotentes, entonces denotamos por  $\dim_{\mathbb{k}} V$  al cardinal de cualquiera de ellas.

**Corolario 3.22:** Si  $S$  es libre en un espacio vectorial de dimensión finita  $n$  y  $S$  posee  $n$  elementos, entonces  $S$  es base.

**§3.2.2 Espacios de dimensión infinita.** Es sencillo notar que para todo cuerpo  $\mathbb{k}$  se cumple que  $\mathbb{k}[x]$  es un  $\mathbb{k}$ -espacio vectorial y que  $\{1, x, x^2, \dots\}$  es una base, sin embargo, generalizar sus propiedades es mucho más difícil que en el caso finito e inevitablemente hay que recurrir al axioma de elección.

**Teorema 3.23:** Son equivalentes:

1. **El axioma de elección.**
2. Todo conjunto libre en un espacio vectorial está contenido en una base.
3. Todo espacio vectorial es un módulo libre.

DEMOSTRACIÓN: (1)  $\implies$  (2). Aplicamos el lema de Zorn: Sea  $S$  un conjunto libre, luego se define  $\mathcal{F}$  como la familia de conjuntos libres que contienen a  $S$ , es claro que  $\mathcal{F}$  está parcialmente ordenado por la inclusión, y por el lema anterior un elemento maximal de  $\mathcal{F}$  sería una base que contenera a  $S$ . Sea  $\mathcal{C}$  una cadena de  $\mathcal{F}$  hay que probar que  $T := \bigcup \mathcal{C} \in \mathcal{F}$  para poder aplicar el

lema de Zorn, y es claro que  $S \subseteq T$ , luego sólo falta probar que  $T$  es libre, lo que queda al lector (HINT: Use prueba por contradicción).

(2)  $\implies$  (3). Trivial.

(3)  $\implies$  (1). Probaremos que implica el axioma de elecciones múltiples, que es equivalente al AE: Sea  $\{X_i : i \in I\}$  una familia de conjuntos no vacíos, hemos de probar que existe  $\{F_i : i \in I\}$  tal que  $F_i \subseteq X_i$  y los  $F_i$  son finitos. Definamos  $X := \bigcup_{i \in I} X_i$ , si  $\mathbb{k}$  es un cuerpo arbitrario, entonces  $\mathbb{k}(X)$  es el cuerpo de polinomios con indeterminadas en  $X$ . Se le llama  $i$ -grado de un monomio a la suma de exponentes de las indeterminadas de  $X_i$ . Se dice que una función racional  $f \in \mathbb{k}(X)$  es  $i$ -homogéneo de grado  $d$  si todos los monomios del denominador tienen un  $i$ -grado común de  $n$  y los del numerador un  $i$ -grado común de  $n+d$ . Denotamos  $K$  al subconjunto de  $\mathbb{k}(X)$  conformado por las funciones racionales  $i$ -homogéneas de grado 0 para todo  $i \in I$ ;  $K$  resulta ser un subcuerpo estricto de  $\mathbb{k}(X)$  (¿por qué?), luego  $\mathbb{k}(X)$  es un  $K$ -espacio vectorial. Finalmente denotamos por  $V$  al  $K$ -subespacio de  $\mathbb{k}(X)$  generado por  $X$ , y por  $B$  a una base de  $V$ . Por definición de  $B$  y en particular para  $x \in X_i$  existe un subconjunto finito  $B(x)$  de  $B$  tal que

$$x = \sum_{v \in B(x)} \lambda_{v,x} v$$

donde  $\lambda_{v,x} \in K_{\neq 0}$ . Nótese que si  $y \in X_i$  es distinto de  $x$ , entonces

$$y = (y/x)x = \sum_{v \in B(x)} (y/x \cdot \lambda_{v,x})v$$

donde  $y/x \cdot \lambda_{v,x} \in K_{\neq 0}$ , luego los  $B(x)$  y los  $\lambda_{v,x}/x$  son fijos para un  $X_i$  fijo, por lo que le denotamos por  $B_i$  y  $\beta_{v,i}$  resp.

Finalmente  $\beta_{v,i}$  es  $i$ -homogéneo de grado  $-1$  y  $j$ -homogéneo de grado 0 para todo  $j \neq i$ . Así que  $\beta_{v,i}$  debe tener finitos términos de  $X_i$ , luego llamamos  $F_i$  al subconjunto de  $X_i$  que tienen términos en algún  $\beta_{v,i}$  para algún  $v \in B_i$ .  $\square$

**Teorema 3.24:** Son equivalentes:

1. El axioma de elección.
2. En un espacio vectorial, todo generador contiene una base.

HINT: Siga la prueba anterior.

**Ejemplo (bases de Hamel).** Si se asume el AE,  $\mathbb{R}$  como  $\mathbb{Q}$ -espacio vectorial tiene una base  $H$ , usualmente llamada *de Hamel*. Queda al lector

probar que todas las bases de Hamel no son ni finitas ni numerables. No sólo es complejo, sino imposible construir manualmente una base de Hamel, puesto que se ha demostrado que la existencia de esta base es independiente a la teoría elemental ZF. Algunos textos prueban que las bases de Hamel son conjuntos tan “raros” que las hay tanto Lebesgue-medibles como no.

**Teorema (AE) 3.25:** Todo par de bases de un espacio vectorial son equipotentes.

DEMOSTRACIÓN: Sean  $X, Y$  bases del espacio, podemos suponer que ambas son infinitas, pues el caso restante ya fue probado. Para todo  $x \in X$  admitamos que  $Y_x$  es un subconjunto finito de  $Y$  tal que  $x \in \langle Y_x \rangle$ , notemos que  $Y' := \bigcup_{x \in X} Y_x$  cumple que  $X \subseteq \langle Y' \rangle$ , de modo que  $Y'$  es base, luego  $Y = Y'$ . Como se asume AE cada  $Y_x$  puede ser enumerado y como son finitos los índices han de ser naturales, de modo que se puede definir  $f : Y \rightarrow X \times \mathbb{N}$  tal que  $f(y)$  es un par  $(x, i)$  donde  $y$  es el  $i$ -ésimo elemento de  $Y_x$ . Nótese que  $f$  es inyectiva, para finalizar, como  $X$  es infinito y se asume AE se cumple que  $\aleph_0 \leq |X|$  de modo que  $|X \times \mathbb{N}| = |X|$  y existe una biyección  $g : X \times \mathbb{N} \rightarrow X$ , luego  $f \circ g : Y \rightarrow X$  es una inyección, y análogamente se construye otra inyección desde  $X$  a  $Y$ . Finalmente, por el teorema de Cantor-Schröder-Bernstein, existe una biyección entre  $X$  e  $Y$ , que es lo que se quería probar.  $\square$

Observe que, al contrario del caso finito, un conjunto libre puede tener cardinal la dimensión y no ser base. En efecto, basta tomar una base de cardinal infinito y quitarle un elemento cualquiera como ejemplo.

### §3.2.3 Fórmulas con la dimensión.

**Teorema 3.26:** Si  $W$  es un  $V$ -espacio vectorial y  $V$  un  $\mathbb{k}$ -espacio vectorial, entonces  $W$  es un  $\mathbb{k}$ -espacio vectorial y

$$\dim_{\mathbb{k}}(W) = \dim_{\mathbb{k}}(V) \cdot \dim_V(W).$$

DEMOSTRACIÓN: Sea  $B_W$  una base de  $W$  como  $V$ -espacio vectorial y  $B_V$  una base de  $V$  como  $\mathbb{k}$ -espacio vectorial, luego

$$B := B_W \cdot B_V = \{bc : b \in B_W, c \in B_V\}$$

debe ser una base de  $W$  como  $\mathbb{k}$ -espacio vectorial.

En efecto, si  $w \in W$ , entonces existen  $x_i \in B_W$  y  $\alpha_i \in V$  tales que

$$w = \sum_{i=1}^n \alpha_i x_i,$$

además, para todo  $\alpha_i \in V$  existen  $y_i \in B_V$  y  $\beta_{ij} \in \mathbb{k}$  tal que

$$\alpha_i = \sum_{j=1}^{m_i} \beta_{ij} y_i,$$

luego

$$w = \sum_{i=1}^n \sum_{j=1}^{m_i} \beta_{ij} (y_j x_i)$$

donde  $\beta_{ij} \in \mathbb{k}$  y  $z_{ij} := y_j x_i \in B$ . Luego  $B$  es un sistema generador.

Sean  $\beta_{ij} \in \mathbb{k}, x_i \in B_W, y_j \in B_V$  tales que

$$\sum_{i=1}^n \sum_{j=1}^{m_i} \beta_{ij} (y_j x_i) = 0.$$

Notemos que

$$\sum_{i=1}^n \left( \sum_{j=1}^{m_i} \beta_{ij} y_j \right) x_i = 0.$$

donde  $\sum_{j=1}^{m_i} \beta_{ij} y_j \in V$ . Como  $B_W$  es libre, entonces los coeficientes de los  $x_i$  han de ser nulos, es decir,

$$\sum_{j=1}^{m_i} \beta_{ij} y_j = 0$$

razonamos análogamente para concluir que  $\beta_{ij} = 0$  para todo par de índices, que es lo que se quería probar.  $\square$

**Teorema 3.27:** Si  $V$  es un espacio vectorial y  $W \leq V$ , entonces:

1.  $\dim V = \dim W + \dim(V/W)$ .
2. Si  $\dim V = \dim W$  y es finito, entonces  $V = W$ .

DEMOSTRACIÓN: 1. Sea  $B_W$  una base de  $W$ , sabemos que se puede extender a una base  $B_V$  de  $V$ , simplemente basta ver que  $B := \{[\vec{v}] : \vec{v} \in B_V \setminus B_W\}$  conserva el cardinal deseado y que es base de  $V/W$ . Sean

$\vec{u}, \vec{v} \in B_V \setminus B_W$ , si  $[\vec{u}] = [\vec{v}]$  entonces  $\vec{u} - \vec{v} \in W$ , luego  $B_V$  sería ligado lo que es absurdo, análogamente se prueba que  $B$  es libre. Para notar que  $B$  es un sistema generador, basta considerar que todo  $[\vec{v}] \in V/W$  se escribe como

$$\vec{v} = \sum_{i=1}^n \lambda_i \vec{e}_i$$

donde  $e_i \in B_V$ , luego

$$[\vec{v}] = \sum_{i=1}^n \lambda_i [\vec{e}_i],$$

donde  $[\vec{e}_i]$  o pertenece a  $B$ , o es nulo, en cuyo caso podemos omitirlo. De este modo, es claro que  $B$  es base.

2. Si  $B$  es base de  $W$  y tiene el mismo cardinal de  $\dim V$  que es finito, entonces es base de  $V$ , de modo que  $V = \langle B \rangle = W$ .

□

**Teorema 3.28 – Fórmula de Grossman:** Si  $A, B \leq V$  con  $V$  un espacio vectorial, entonces

$$\dim A + \dim B = \dim(A + B) + \dim(A \cap B).$$

**Teorema 3.29:** Si  $f : V \rightarrow W$  es lineal, entonces

$$\dim V = \dim(\ker f) + \dim(\text{Img } f).$$

### 3.3. Matrices y transformaciones lineales

**Teorema 3.30:** Sea  $f : X \rightarrow N$  donde  $X$  es base de un  $A$ -módulo  $M$  y  $N$  es otro  $A$ -módulo. Entonces existe un único homomorfismo de módulos  $\bar{f} : M \rightarrow N$  tal que  $\bar{f}|_X = f$ .

**Teorema 3.31:** Si  $f \in L(V, W)$ , entonces:

1.  $f$  es inyectiva syss  $\ker f = \{0\}$ .
2.  $f$  es suprayectiva syss su imagen contiene a alguna base, y por ende a todas ellas.

3. En particular, si  $n := \dim V = \dim W < +\infty$  entonces  $f$  es un isomorfismo de módulos syss es inyectiva o suprayectiva, lo que se reduce a ver que  $\dim \ker f = 0$  o  $\dim \text{Im} f = n$ .

**Corolario 3.32:** Dos espacios vectoriales son isomorfos syss comparten dimensión.

**Definición 3.33:** Si  $B := (e_i)_{i \in I}$  es una base (ordenada) de un  $A$ -módulo  $M$ , entonces  $\pi_i^B : M \rightarrow A$  son la serie de aplicaciones tal que para todo  $v \in M$  se cumple que

$$v = \sum_{i \in I} \pi_i^B(v) e_i.$$

Sabemos que para cada  $i \in I$ , las proyecciones  $\pi_i^B$  están bien definidas. Se define  $\pi^B : M \rightarrow A^I$  la función tal que  $\pi^B(v) := (\pi_i^B(v))_{i \in I}$ .

De este modo si  $v = 2e_1 + 3e_2 - 1e_3$  donde  $B := (e_1, e_2, e_3)$  es una base ordenada de un módulo que contiene a  $v$ , entonces  $\pi^B(v) = (2, 3, -1)$ .

**Proposición 3.34:** Si  $X := (x_1, \dots, x_n)$  es base ordenada de  $M$ , entonces

1. Para todo  $i$  se cumple que  $\pi_i^X$  es un funcional.
2. Para todo  $i, j$  se cumple que  $\pi_i^X(x_j) = \delta_{ij}$ .
3.  $\pi^X$  es un isomorfismo con  $A^n$ .

Por ello en lugar de denotar un  $A$ -módulo de dimensión finita denotaremos  $A^n$ .

Supongamos entonces que si  $f : M \rightarrow N$  es un morfismo de módulos y  $M$  es libre, entonces  $f$  queda completamente determinado por una tupla de  $N$  correspondiente a la imagen de la base. Si además  $N$  es libre, entonces cada vector de  $N$  puede escribirse como una tupla de valores del anillo  $A$ . En síntesis, si el dominio y codominio son libres todo el homomorfismo se reduce a tuplas de tuplas de valores de  $A$ . Esto sucede más fácilmente si nos restringimos a espacios vectoriales, y en particular si éstos son de dimensión finita, en cuyo caso se cumple que toda la transformación lineal puede reducirse a  $n \cdot m$  escalares, donde  $n$  es la dimensión del dominio y  $m$  la del codominio.



**Definición 3.35 – Matrices:** Una matriz  $M$  sobre un anillo unitario  $A$  de orden  $n \times m$  es una función  $M : \{1, \dots, n\} \times \{1, \dots, m\} \rightarrow A$ , donde solemos denotar  $M(i, j)$  como  $M_{i,j}$ . A éstos últimos valores les decimos sus *coeficientes*. El conjunto de matrices sobre  $A$  de  $n \times m$  se denota  $\text{Mat}_{n \times m}(A)$ . El conjunto  $\text{Mat}_{n \times m}(A)$  es un  $A$ -módulo, en donde:

1.  $(B + C)_{i,j} := B_{i,j} + C_{i,j}$  para todo  $B, C \in \text{Mat}_{n \times m}(A)$ .
2.  $(\lambda B)_{i,j} := \lambda B_{i,j}$  para todo  $B \in \text{Mat}_{n \times m}(A)$  y  $\lambda \in A$ .

La diagonal de una matriz se le llama al conjunto de coeficientes de coordenadas  $(i, i)$ .

Si  $B \in \text{Mat}_{n \times m}(A)$  y  $C \in \text{Mat}_{m \times p}(A)$ , se define su producto interno como:

$$(B \cdot C)_{i,j} := \sum_{k=1}^m B_{i,k} C_{k,j}$$

Dado  $B \in \text{Mat}_{n \times m}(A)$  se define su *matriz traspuesta* como  $B^t \in \text{Mat}_{m \times n}(A)$  tal que  $(B^t)_{i,j} := B_{j,i}$ .

Se les llama matrices:

**Cuadradas** A las de orden  $n \times n$ .

**Simétricas** A las matrices cuadradas  $B$  tal que  $B = B^t$ .

**Antisimétricas** A las matrices cuadradas  $B$  tal que  $B = -B^t$ .

**Diagonales** A las que tienen coeficientes nulos en todas las coordenadas exceptuando tal vez la diagonal.

**Escalares** A las matrices diagonales que en la diagonal sólo contienen un valor escalar.

**Identidad** A la matriz escalar con valor 1. La matriz identidad de orden  $n \times n$  se denota  $I_n$ .

**Nula** A la matriz escalar con valor 0.

Por lo general, denotaremos los valores de la matriz en una tabla, por ejemplo

$$M := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \in \text{Mat}_{2 \times 3}(\mathbb{Q})$$

donde  $M_{2,1} = 4$ .

**Proposición 3.36:**  $\text{Mat}_{n \times m}(A)$  es un  $A$ -módulo libre de rango  $nm$ .

**Proposición 3.37:** Si  $B, C, D$  son matrices de orden apropiado en cada caso, se cumple:

1.  $B \cdot (C \cdot D) = (B \cdot C) \cdot D$  (asociatividad).
2.  $B \cdot (C + D) = B \cdot C + B \cdot D$  (distributividad izquierda).
3.  $(B + C) \cdot D = B \cdot D + C \cdot D$  (distributividad derecha).
4. Si  $B$  es de orden  $n \times m$ , entonces  $I_n \cdot B = B \cdot I_m = B$  (neutro).
5.  $\text{Mat}_n(A)$  es un anillo unitario de neutro aditivo la matriz nula y neutro multiplicativo la matriz identidad.

**Proposición 3.38:** Si  $B, C$  son matrices de orden apropiado en cada caso, se cumple:

1.  $(B^t)^t = B$ .
2.  $(B + C)^t = B^t + C^t$ .
3.  $(\lambda B)^t = \lambda B^t$  para todo  $\lambda \in A$ .
4. Si  $A$  es conmutativo, entonces  $(B \cdot C)^t = C^t \cdot B^t$ .
5. Si  $B$  es cuadrada e invertible, entonces  $(B^{-1})^t = (B^t)^{-1}$ .

**Definición 3.39:** Si  $f \in L(\mathbb{k}^n, \mathbb{k}^m)$ , y  $X := (x_1, \dots, x_n)$ ,  $Y := (y_1, \dots, y_m)$  son bases ordenadas de  $\mathbb{k}^n$  y  $\mathbb{k}^m$  resp., entonces denotamos  $M_X^Y(f)$  a la matriz de orden  $n \times m$  a aquella tal que sus columnas son las imagenes ordenadas de la base  $X$ , dicho de otro modo  $[M_X^Y(f)]_{i,*} = f(x_i)$  o que  $[M_X^Y(f)]_{i,j} := \pi_j(f(x_i))$ .

**Teorema 3.40:** Sean  $f \in L(\mathbb{k}^n, \mathbb{k}^m)$ ,  $X$  e  $Y$  bases ordenadas de  $\mathbb{k}^n$  y  $\mathbb{k}^m$  resp., entonces  $B = M_X^Y(f)$  syss para todo  $v \in \mathbb{k}^n$  se cumple:

$$\pi^Y(f(v)) = \pi^X(v) \cdot B.$$

DEMOSTRACIÓN:  $\implies$ . Sea  $X = (x_1, \dots, x_n)$ ,  $v = \sum_{i=1}^n v_i x_i$  y  $B := M_X^Y(f)$ , luego como  $f$  es lineal se cumple que

$$f(v) = \sum_{i=1}^n v_i f(x_i).$$

Las proyecciones son también lineales, luego

$$\pi_j^Y(f(v)) = \sum_{i=1}^n v_i \pi_j^Y[f(x_i)] = \sum_{i=1}^n v_i b_{ij} = (\pi^X(v) \cdot B)_{1j},$$

como se quería probar.

$\Leftarrow$ . Si se cumple para todo vector, en particular se cumple para los vectores de la base  $X$  y claramente

$$(M_X^Y(f))_{ij} = \pi_j^Y(f(x_i)) = \sum_{k=1}^n \delta_{ik} b_{kj} = b_{ij}$$

ergo  $B = M_X^Y(f)$ . □

**Ejemplo (matriz cambio de base).** Sea  $V$  un  $\mathbb{k}$ -espacio vectorial de dimensión  $n$ . Sean  $X, Y = (v_1, \dots, v_n)$  bases ordenadas de  $V$ , luego

$$\pi^X(v_i) = \pi^X(\text{Id}(v_i)) = \pi^Y(v_i) \cdot M_Y^X(\text{Id}) = e_i M_Y^X(\text{Id}) = [M_X^Y(\text{Id})]_{i,*}.$$

**Teorema 3.41:** Si  $f, g$  son funciones lineales y  $X, Y, Z$  son bases ordenadas adecuadas a las dimensiones en cada caso, se cumple:

1.  $M_X^X(\text{Id}) = I_n$ , donde  $n = |X|$ .
2. Para todo  $\lambda$  escalar se cumple  $M_X^Y(\lambda f) = \lambda M_X^Y(f)$ .
3.  $M_X^Y(f + g) = M_X^Y(f) + M_X^Y(g)$ .
4.  $M_X^Z(f \circ g) = M_X^Y(f) \cdot M_Y^Z(g)$ .
5. Son equivalentes:
  - a)  $f$  es invertible.
  - b) Para algún par de bases ordenadas  $X, Y$  se da que  $M_X^Y(f)$  es invertible.
  - c) Para todo par de bases ordenadas  $X, Y$  se da que  $M_X^Y(f)$  es invertible.

6.  $L(\mathbb{k}^n, \mathbb{k}^m) \cong \text{Mat}_{n \times m}(\mathbb{k}) \cong \mathbb{k}^{nm}$ . En particular,  $L(\mathbb{k}^n, \mathbb{k}) \cong \mathbb{k}^n$ .

Los últimos dos son los que justifican la definición de matrices.

**Ejemplo.** Si  $X, Y$  son bases ordenadas de  $\mathbb{k}^n$ , entonces

$$I_n = M_X^X(\text{Id}) = M_X^Y(\text{Id}) \cdot M_Y^X(\text{Id}).$$

Luego si  $B \in \text{Mat}_n(\mathbb{k})$  es invertible, entonces representa a una única matriz de cambio de base. De hecho, toda endo-aplicación lineal  $f \in L(\mathbb{k}^n)$  está representada por la familia

$$M_Y^Y(f) = M_Y^X(\text{Id}) \cdot M_X^X(f) \cdot M_X^Y(\text{Id}).$$

**Teorema 3.42:** Si  $B \in \text{Mat}_n(\mathbb{k})$ , entonces son equivalentes:

1.  $B$  es invertible.
2. Para todo  $v \in \mathbb{k}^n$  se cumple que  $v \cdot B = 0$  implica  $v = 0$ .

DEMOSTRACIÓN:  $\implies$ . Si  $B$  es invertible entonces sea  $B^{-1}$  su inversa, luego  $v = (v \cdot B)B^{-1} = 0 \cdot B^{-1} = 0$ .

$\impliedby$ . Si  $X$  es la base canónica, entonces  $f(v) := v \cdot B$  claramente es lineal y cumple que  $B = M_X^X(f)$  (¿por qué?). Si  $f^{-1}(0) = \{0\}$ , entonces  $\dim \ker f = 0$ , luego  $\dim \text{Im } f = n$  y  $f$  es una biyección, luego es invertible, y por el teorema anterior, cualquiera de sus representaciones matriciales (en particular,  $B$ ) lo son.  $\square$

### 3.4. Determinante

**Definición 3.43 – Forma multilineal:** Se dice que una función  $f : (A^n)^n \rightarrow A$  es una *forma multilineal* si es lineal coordenada a coordenada, es decir, si para todo  $v_1, \dots, v_n, v \in A^n$  y todo  $\lambda \in A$  se cumple que

$$f(v_1, \dots, v_i + \lambda v, \dots, v_n) = f(v_1, \dots, v_n) + \lambda f(v_1, \dots, v, \dots, v_n).$$

Además, una forma multilineal se dice *antisimétrica* si intercambiar dos vectores de coordenadas cambia el signo, es decir si

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j, \dots, v_i, \dots, v_n).$$

Y también se dice *alternada* si es nula si un vector aparece en más de una coordenada, es decir si

$$f(v_1, \dots, \underset{(i)}{v}, \dots, \underset{(j)}{v}, \dots, v_n) = 0.$$

**Proposición 3.44:** Si  $f$  es una forma multilineal entonces:

1. Toma valor nulo si alguna coordenada es nula.
2. Si es alternada, entonces es antisimétrica.
3. Si es antisimétrica y el campo escalar no tiene característica 2, entonces es alternada.
4. Es antisimétrica syss para todo  $\sigma \in S_n$  y todo  $(v_1, \dots, v_n) \in (A^n)^n$  se cumple:

$$f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = (\text{sgn } \sigma) \cdot f(v_1, \dots, v_n).$$

**Teorema 3.45:** Para todo  $a \in A$  existe una única forma multilineal  $f$  tal que  $f(e_1, \dots, e_n) = a$ . Y de hecho, si todo  $v_i := (v_{i1}, \dots, v_{in})$ , entonces dicha forma multilineal viene dada por

$$f(v_1, \dots, v_n) = a \sum_{\sigma \in S_n} \text{sgn } \sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)}.$$

DEMOSTRACIÓN: Utilizando la notación del enunciado  $v_i = \sum_{j=1}^n v_{ij}e_j$ , luego

$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{j=1}^n v_{1j} f(e_j, v_2, \dots, v_n) \\ &= \sum_{j_1=1}^n \sum_{j_2=1}^n v_{1j_1} v_{2j_2} f(e_{j_1}, e_{j_2}, v_3, \dots, v_n) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n v_{1j_1} \cdots v_{nj_n} f(e_{j_1}, \dots, e_{j_n}). \end{aligned}$$

Notemos que podemos reemplazar los  $j_k$  por funciones desde  $\{1, \dots, n\}$  a  $\{1, \dots, n\}$ , sin embargo, si las funciones no son inyectivas, entonces nos queda la forma multilineal de una tupla con coordenadas repetidas, lo que por

definición de alternada es nulo, luego podemos solo considerar los  $j_k$  como permutaciones de  $n$  elementos y nos queda:

$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{\sigma \in S_n} v_{1\sigma(1)} \cdots v_{n\sigma(n)} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \\ &= a \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)} \end{aligned}$$

□

Nótese que en lugar de considerar el dominio como un espacio  $(A^n)^n$ , se puede reemplazar por  $\operatorname{Mat}_n(A)$  que es isomorfo.

**Definición 3.46 – Determinante:** Se define la función determinante  $\det : \operatorname{Mat}_n(A) \rightarrow A$  como la única forma multilineal tal que  $\det(I_n) = 1$ . También se denota por  $|B|$  a la determinante de la matriz cuadrada  $B$ .

Algo que destacar es que el cálculo de matrices se vuelve, en casos generales, exponencialmente más complejo de acuerdo a las dimensiones de las matrices, ésto es fácil de ver ya que  $|S_n| = 2^n$ , luego el determinante comprende una herramienta sólo en casos particulares, en matrices pequeñas o en contextos teóricos.

**Proposición 3.47 (Cálculo de determinantes):** Si  $B$  es una matriz, entonces:

1. Intercambiar columnas (o filas) cambia el signo de su determinante.
2. La matriz generada por ultiplicar una columna (o fila) por  $\lambda$  tiene determinante  $\lambda|B|$ .
3. Sumarle a una columna (resp. fila)  $\lambda$ -veces otra columna (resp. fila) distinta no varía el determinante.
4. Si para todo  $i < j$  (o que  $j < i$ ) se cumple que  $b_{ij} = 0$ , entonces  $\det B = b_{11}b_{22} \cdots b_{nn}$ .

**Proposición 3.48:** Para toda matriz  $B$  cuadrada se cumple  $\det(B^t) = \det(B)$ .

**Teorema 3.49:** Para todos  $B, C \in \operatorname{Mat}_n(\mathbb{k})$  se cumple que  $|BC| = |B||C|$ .

DEMOSTRACIÓN: Probaremos que  $f(B) := |BC|$  es una forma multilineal alternada. Para ello denotaremos  $B$  como una tupla de vectores que corresponden a sus columnas, es decir,  $B = (B_1, \dots, B_n)$  donde  $B_1 = (b_{11}, \dots, b_{1n})$ . Luego si  $B' := (B_1, \dots, B_u + \lambda v, \dots, B_n)$ ,  $D := BC$  y  $D' := B'C$ , entonces

$$(D')_{ij} = \sum_{k=1}^n B'_{ik} C_{kj}$$

luego si  $i \neq u$ , entonces  $(D')_{ij} = D_{ij}$ . Si  $i = u$ , entonces  $(D')_{u,*} = D_{u,*} + \lambda(vC)_*$ , y como el determinante es multilineal sobre columnas y filas (por traspuesta) se comprueba también la multilinealidad de  $f$ .

Para ver que es alternada notamos que si  $B$  repite columnas,  $D$  repite filas, luego como el determinante es alternado también por filas,  $f$  toma valor nulo.

Finalmente para calcular la constante  $a$  evaluamos en  $I_n$  lo que da  $|C|$  y comprueba el enunciado.  $\square$

**Definición 3.50 – Menor complemento:** Dada una matriz  $B \in \text{Mat}_n(A)$  con  $n > 1$ , se le llama *menor complemento*, denotado  $M_{ij}(B)$ , de la coordenada  $(i, j)$  al determinante de la matriz resultante de eliminar la  $i$ -ésima fila y  $j$ -ésima columna de  $B$ .

**Proposición 3.51:** Si  $B \in \text{Mat}_n(A)$  con  $n > 1$ , entonces para todo  $i, j \leq n$  se cumple que

$$\det B = \sum_{k=1}^n (-1)^{i+k} b_{ik} M_{ik}(B) = \sum_{k=1}^n (-1)^{k+j} b_{kj} M_{kj}(B). \quad (3.1)$$

**Definición 3.52 – Matriz adjunta:** Dada una matriz  $B \in \text{Mat}_n(A)$  con  $n > 1$ , se le llama *matriz adjunta*, denotado  $\text{adj } B$ , a la matriz

$$(\text{adj } B)_{ij} := (-1)^{i+j} M_{ji}(B).$$

**Teorema 3.53:** Para todo  $B \in \text{Mat}_n(D)$  con  $n > 1$  se cumple que

$$B \cdot \text{adj } B = \text{adj } B \cdot B = |B| \cdot I_n. \quad (3.2)$$

En consecuencia,  $B$  es invertible syss  $\det B$  es invertible, en cuyo caso,

$B^{-1} = \frac{1}{|B|} \operatorname{adj} B$ . Si  $D$  es un cuerpo, la condición se reduce a notar que las matrices invertibles son las de determinante no nula.

**Proposición 3.54:** Se cumple:

1.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

2.

$$\operatorname{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

3.

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - (afh + bdi + ceg).$$



---

## Extensiones de cuerpo

---

### 4.1. Extensiones algebraicas y transcendentales

**Definición 4.1 – Extensión de cuerpos:** Dado un cuerpo  $k$  se dice que  $K$  es una *extensión de cuerpos* de  $k$  si  $K$  tiene un subcuerpo isomorfo a  $k$ , lo que abreviamos diciendo que  $K/k$  es una extensión. Si  $K$  es una extensión de cuerpo, entonces con las operaciones usuales se puede ver como un  $k$ -espacio vectorial, de modo que llamamos su *grado* a  $[K : k] := \dim_k(K)$ .

Dada una extensión  $K$  del cuerpo  $k$ , un elemento  $\alpha \in K$  se dice  *$k$ -algebraico* si existe  $p \in k[x]$  tal que  $p(\alpha) = 0$ , de lo contrario se dice  *$k$ -trascendente*. Una extensión  $K$  se dice  *$k$ -algebraica* si todos sus elementos lo son, de lo contrario,  $K$  se dice  *$k$ -trascendente*. De no haber ambigüedad obviamos el “ $k$ ”.

**Teorema 4.2 (transitividad de grados):** Si  $k \subseteq K \subseteq L$  son cuerpos, entonces  $[L : k] = [L : K] \cdot [K : k]$ .

DEMOSTRACIÓN: Se deriva de la transitividad de dimensiones.  $\square$

**Teorema 4.3:** Toda extensión de grado finito es algebraica.

DEMOSTRACIÓN: Sea  $K$  extensión de  $k$  de grado  $n$ . Si  $n = 1$ , entonces es trivial. De lo contrario sea  $\alpha \notin k$  y consideremos  $S := \{1, \alpha, \dots, \alpha^n\}$ .

Si alguna potencia de  $\alpha$  se repite, digamos  $\alpha^i = \alpha^j$ , entonces  $p(x) := x^j - x^i$  hace algebraico a  $\alpha$ . De lo contrario, como  $S$  tiene  $n + 1$  elementos no puede ser base, ergo existen  $c_i \in k$  tales que son no nulos y

$$\sum_{i=0}^n c_i \alpha^i = c_n \alpha^n + \cdots + c_1 \alpha + c_0 = 0,$$

pero luego  $p(x) := \sum_{i=0}^n c_i x^i$  es claramente un polinomio que hace que  $\alpha$  sea algebraico; por ende,  $K$  es algebraico.  $\square$

En principio parece muy específico el acto de clasificar elementos entre *algebraicos* y *transcendentes* de esa forma, sin embargo, hay una razón bastante natural para hacerlo.

**Teorema 4.4 – Teorema de extensión de Kronecker:** Sea  $k$  un cuerpo con  $p(x) \in k[x]$  no constante y sin raíces, entonces existe una extensión  $K/k$  que posee una raíz de  $p(x)$ .

DEMOSTRACIÓN: Si  $p(x)$  es no constante entonces y no posee raíces como  $k[x]$  es un DFU entonces se puede factorizar mediante irreducibles que tampoco tienen raíz, en particular sea  $q(x)$  uno de ellos. Como  $(q(x))$  es un ideal maximal, entonces  $K := k[x]/(q(x))$  resulta ser un cuerpo.

Nótese que para todo  $a \in k$  se tiene que  $[a] \in K$ , y es claro que la función  $y \mapsto [y]$  es un monomorfismo de cuerpos. Luego, denotamos nuestra raíz como  $\alpha := [x]$  (recordad que las clases de equivalencias son de polinomios de  $k[x]$ ), como el anillo cociente es respecto a  $q(x)$  que divide a  $p(x)$  tenemos que

$$0 = [p(x)] = \sum_{i \geq 0} [a_i][x]^i = \sum_{i \geq 0} a_i \alpha^i = p(\alpha),$$

osea que  $\alpha$  es una raíz de  $p$  en  $K$ .  $\square$

Cabe destacar que diremos que un elemento es una *raíz cuadrada* de  $a$  syss es la raíz de  $x^2 - a$ . Asimismo diremos que es *raíz cúbica* cuando es raíz de  $x^3 - a$  y, en general, que es una *n-ésima raíz* cuando es raíz de  $x^n - a$ . **Ojo** que ésto no tiene nada que ver con la función real  $\sqrt[n]{x}$ , pues se define de otra manera (ver def. 1.50 de [Top]).

**Definición 4.5:** Sea  $k$  un cuerpo con  $p(x) \in k[x]$  un polinomio no-constante sin raíz. Entonces denotando  $\alpha$  como una raíz de  $p$ , entonces

$k[\alpha]$  es la extensión de  $k$  construida en condiciones de la demostración anterior.

Nótese que para todo  $p(x) \in k[x]$ ,

$$[p(x)] = \sum_{i \geq 0} [a_i][x]^i = \sum_{i \geq 0} a_i \alpha^i = p(\alpha),$$

es decir, que la extensión que hemos construido resulta ser el cuerpo de polinomios de  $\alpha$  (de ahí la notación). De igual manera podríamos construir una extensión con un polinomio que si tuviese raíz, pero es inmediato notar que es el mismo  $k$ .

**Teorema 4.6:** Si  $K/k$  es una extensión de cuerpos y  $\alpha \in K$  es algebraico, entonces:

1. Existe un único polinomio mónico irreducible  $p(x) \in k[x]$  tal que  $p(\alpha) = 0$ . Al que llamaremos *polinomio minimal* de  $\alpha$  sobre  $k$ .
2. Si  $q(x) \in k[x]$  cumple que  $q(\alpha) = 0$ , entonces  $p(x) \mid q(x)$ .
3.  $k[\alpha] = k(\alpha) = \{r(\alpha) : r(x) \in k[x] \wedge \deg r < \deg p\}$
4.  $k[\alpha]/k$  es una extensión finita, de hecho  $[k(\alpha) : k] = \deg p =: n$  y  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es base para  $k(\alpha)$ .

DEMOSTRACIÓN: Consideremos  $\pi : k[x] \rightarrow k[\alpha]$  dada por  $\pi(q(x)) = q(\alpha)$ . Claramente  $\pi$  es un epimorfismo de anillos, luego  $\ker \pi$  es un ideal de  $k[x]$ , y como éste es un PID, entonces es generado por un polinomio  $p(x)$ . Como  $k[\alpha] \cong k[x]/(p(x))$  que es íntegro, entonces  $(p(x))$  es primo y  $p(x)$  es irreducible.

Supongamos que  $q(x)$  es tiene a  $\alpha$  de raíz, entonces  $q(x) \in \ker \pi = (p(x))$ , luego  $p(x) \mid q(x)$ . Si  $q(x)$  es irreducible, entonces  $q$  y  $p$  son asociados, pero cómo exigimos que el polinomio sea mónico se comprueba la unicidad.

El inciso 3. se deduce de la construcción de la extensión de Kronecker.

Veamos que la base explicitada en efecto lo es, dado que los elementos de  $k[\alpha]$  son de la forma  $q(\alpha)$  con  $\deg q < n$ , entonces se deduce que el conjunto propuesto es un sistema generador. Por otro lado, es libre pues si no lo fuese habría un polinomio no nulo  $r(x)$  tal que  $r(\alpha) = 0$  y  $\deg r \leq n - 1 < n$  lo que contradice la definición de  $p(x)$ .  $\square$

**Corolario 4.7:** Si  $K/k$  es una extensión de cuerpos, y  $S \subseteq K$  es finito y algebraico, entonces  $k(S)/k$  es una extensión finita.

**Teorema 4.8:** Si  $L/K/k$  son extensiones de cuerpos, entonces  $L/k$  es algebraica syss  $L/K$  y  $K/k$  lo son.

DEMOSTRACIÓN:  $\implies$ . Si  $L/k$  es algebraica, claramente  $K/k$  lo es y como  $k$  es subcuerpo de  $K$  se comprueba que  $L/K$  lo es.

$\impliedby$ . Si  $\alpha \in L$  entonces  $\alpha$  es  $K$ -algebraico, luego sean  $\beta_1, \dots, \beta_n$  los coeficientes de su polinomio minimal, luego  $\alpha$  es algebraico sobre  $k(\beta_1, \dots, \beta_n)$ , por ende  $k(\beta_1, \dots, \beta_n)[\alpha]/k(\beta_1, \dots, \beta_n)$  es finita, y como los  $\beta_i$  son  $k$ -algebraicos, entonces  $k(\beta_1, \dots, \beta_n)/k$  es finito, finalmente  $k(\beta_1, \dots, \beta_n, \alpha)/k$  es finito y luego algebraico.  $\square$

**Corolario 4.9:** Si  $K/k$  es una extensión de cuerpos, entonces el conjunto de elementos algebraicos de  $K$  es un cuerpo.

DEMOSTRACIÓN: Basta notar que si  $\alpha, \beta$  son algebraicos sobre  $K$ , entonces  $k(\alpha, \beta)/k$  es finita, luego algebraica y por ende  $\alpha + \beta$ ,  $\alpha \cdot \beta$  y  $\alpha/\beta$  (si  $\beta \neq 0$ ) lo son.  $\square$

**Definición 4.10:** Dadas las extensiones de cuerpo  $K/k$  y  $L/l$ , entonces un monomorfismo de extensiones de cuerpo es un morfismo de cuerpos  $\sigma : K \rightarrow L$  tal que  $\sigma[k] = l$ . Además si las extensiones son  $K/k$  y  $L/k$ , entonces se les llaman  $k$ -morfismos. Llamamos grupo de Galois, denotado por  $\text{Gal}(K/k)$ , al grupo de  $k$ -automorfismos de  $K/k$ .

**Teorema 4.11:** Sean  $K/k$  y  $L/l$  extensiones de cuerpo con  $\sigma : k \rightarrow l$  un isomorfismo de cuerpo, que induce un morfismo de anillos  $\sigma : k[x] \rightarrow l[x]$ . Si  $\alpha \in K$  es algebraico, entonces sea  $p \in k[x]$  su polinomio minimal. Si  $L$  contiene una raíz  $\beta$  de  $\sigma p(x)$ , entonces  $\sigma$  se extiende un isomorfismo de extensiones  $\sigma^* : k(\alpha) \rightarrow l(\beta)$ .

DEMOSTRACIÓN: Sea  $\phi : k[x] \rightarrow k[\alpha]$  el morfismo de evaluación, i.e., tal que  $\phi(g) = g(\alpha)$ . Es claro que  $\ker \phi$  es el ideal  $(p(x))$ , luego por el primer teorema de isomorfismos  $k[x]/(p(x)) \cong k[\alpha]$ .

En primer lugar veamos que  $\sigma p(x)$  ha de ser el polinomio minimal de  $\beta$  en  $l$ . Luego, análogamente  $l[x]/(\sigma p(x)) \cong l[\beta]$ .

Finalmente  $\omega : k[x] \rightarrow l[x]$  que fija a la identidad induce un isomorfismo  $k[x]/(p(x)) \cong l[x]/(\sigma p(x))$ , de lo que se concluye que  $k[\alpha] \cong l[\beta]$ .  $\square$

**Definición 4.12 –  $k$ -conjugados:** Dados  $\alpha, \beta$  algebraicos sobre  $k$ , se dice que son  $k$ -conjugados si comparten el polinomio minimal.

**Teorema 4.13:** Dados  $\alpha, \beta$  algebraicos sobre  $k$ , entonces son  $k$ -conjugados syss existe un  $k$ -isomorfismo  $\sigma : k(\alpha) \rightarrow k(\beta)$  tal que  $\sigma(\alpha) = \beta$ .

**Ejemplo.** Si  $\lambda \in k$  no posee raíz cuadrada, y se denota  $\alpha$  a una raíz de  $\lambda$ , entonces  $\alpha$  y  $-\alpha$  son  $k$ -conjugados. Esto justifica la terminología sobre los números complejos.

**Ejemplo.** El polinomio ciclotómico  $p$ -ésimo, con  $p > 2$ , es irreducible luego carece de raíces, así que construyamos  $\mathbb{Q}(\omega)$  donde  $\omega$  es una raíz. Como  $\Phi_p(x) \cdot (x-1) = x^p - 1$ , entonces todas las raíces del polinomio son  $p$ -ésimas raíces de la unidad, ergo  $\omega^p = 1$ , luego  $(\omega^2)^p = 1^2 = 1$ , por lo que  $\omega^2$  también es raíz de  $\Phi_p(x)$ . De hecho, se concluye que todas las raíces de  $\Phi_p(x)$  son  $\omega^1, \omega^2, \dots, \omega^{p-1}$ ; luego ellos son  $k$ -conjugados.

**Teorema 4.14:** Si  $K/k$  es finito, entonces  $\text{Gal}(K/k)$  también.

DEMOSTRACIÓN: Sea  $S := \{\alpha_1, \dots, \alpha_n\}$  tal que  $K = k(S)$ . Sea  $\sigma \in \text{Gal}(K/k)$  y  $p \in k[S]$ , como  $\sigma$  es un  $k$ -automorfismo se cumple  $\sigma(p(\alpha_1, \dots, \alpha_n)) = p(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ . Notemos que todo elemento en  $K$  es de la forma  $p(\alpha_1, \dots, \alpha_n)$ , luego dos  $k$ -automorfismos coinciden syss lo hacen en  $S$ .

Sea  $p_i$  el polinomio minimal de  $\alpha_i$ , entonces  $p(\alpha_i) = 0 = \sigma(p(\alpha_i)) = p(\sigma(\alpha_i))$ . Y se sabe que un polinomio no nulo tiene finitas raíces, luego  $\sigma$  sólo puede tomar finitos valores en  $\alpha_i$ . Finalmente sólo hay finitas posibilidades para  $\sigma$ , luego  $\text{Gal}(K/k)$  es finito.  $\square$

**Definición 4.15:** Se dice que un polinomio  $p \in k[x]$  se escinde (en inglés, *split*) en una extensión de cuerpos  $K/k$ , si existen  $\alpha_0, \alpha_1, \dots, \alpha_n \in K$  tales que

$$p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n).$$

También llamamos *cuerpo de escisión* de  $p$  sobre  $k$  a la extensión  $K/k$  tal que  $p$  escinde en  $K$  y  $K = k(\alpha_1, \dots, \alpha_n)$ .

**Teorema 4.16:** Si  $p \in k[x]$  es no constante y posee dos cuerpos de escisión  $K, K'$ , entonces éstos son  $k$ -isomorfos.

DEMOSTRACIÓN: Lo haremos por inducción sobre el grado de  $p$ , donde el

caso  $n = 1$  es trivial.

Sea  $p$  de grado  $n + 1$  y sean  $\alpha_1, \dots, \alpha_{n+1}$  sus raíces en  $K$  y  $\beta_1, \dots, \beta_{n+1}$  sus raíces en  $K'$ . Llamemos  $L := k(\alpha_1, \dots, \alpha_{n+1}, \beta_1, \dots, \beta_{n+1})$  que es una extensión de  $k$  que contiene a  $K$  y a  $K'$ . Como  $L$  es cuerpo, entonces  $L[x]$  es DFU y por ende como

$$p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_{n+1}) = \beta_0(x - \beta_1) \cdots (x - \beta_{n+1}),$$

donde los factores son mónicos y  $\alpha_0$  es el coeficiente director, se cumple que  $\alpha_0 = \beta_0 \in k$  y que  $\alpha_i = \beta_{\sigma(i)}$  donde  $\sigma \in S_{n+1}$ . Reordenemos los  $\beta_i$ s de modo que  $\alpha_{n+1} = \beta_{n+1}$ , luego

$$\deg \left( q := \frac{p}{x - \alpha_{n+1}} \right) = n$$

donde  $q \in k(\alpha_{n+1})[x]$ . Claramente  $K, K'$  son cuerpos de escisión de  $q$ , que es no constante y de grado  $n$ , luego son  $k(\alpha_{n+1})$ -isomorfos, por ende, son  $k$ -isomorfos.  $\square$

**Proposición 4.17:** Si  $p \in k[x]$  es de grado  $n \geq 1$ , entonces su cuerpo de escisión tiene grado a lo más  $n!$

HINT: Usar inducción.

**Definición 4.18 – Extensión normal:** Se dice que una extensión de cuerpos  $K/k$  es *normal* si para todo  $p \in k[x]$  irreducible con alguna raíz en  $K$  se escinde en  $K$ .

### 5.1. Diagonalización

**Lema 5.1:** Si  $f \in \text{End}(\mathbb{k}^n)$  y  $X, Y$  son bases ordenadas cualesquiera de  $\mathbb{k}^n$ , entonces para todo  $x \in \mathbb{k}$

$$\det(xI_n - M_X^X(f)) = \det(xI_n - M_Y^Y(f))$$

DEMOSTRACIÓN: Como hemos visto

$$M_Y^Y(f) = M_Y^X(\text{Id}) M_X^X(f) M_X^Y(\text{Id}),$$

luego si llamamos  $B := M_X^Y(\text{Id})$  (que es invertible), cumple que

$$M_Y^Y(f) = B^{-1} M_X^X(f) B,$$

luego

$$\det(xI_n - M_Y^Y(f)) = \det(xI_n - B^{-1} M_X^X(f) B) = \det(B^{-1}(xI_n - M_X^X(f))B) = \det(xI_n - M_X^X(f)).$$

□

**Definición 5.2 – Polinomio característico:** Si  $f \in \text{End}(\mathbb{k}^n)$ , entonces dada una base  $X$  cualquiera se define

$$p_f(x) := \det(xI_n - M_X^X(f))$$

conocido como el *polinomio característico* de  $f$ . El polinomio característico de una matriz  $B$  es  $p_B(x) := \det(xI_n - B)$ .

**Definición 5.3:** Si  $M$  es un  $A$ -módulo y  $f \in \text{End}(M)$ , entonces si existen  $v \in M_{\neq 0}$  y  $\alpha \in A$  tales que

$$f(v) = \alpha v$$

entonces se dice que  $v$  es un *autovector* y  $\alpha$  un *autovalor* de  $f$ . Si  $M = A^n$  y  $B \in \text{Mat}_n(A)$ , entonces se definen los autovalores y autovectores de  $B$  a aquellos correspondientes a la función  $f(v) := Bv$ .

Si  $\alpha \in \mathbb{k}$ , entonces se le llama *autoespacio* generado por  $\alpha$  de  $f$  a:

$$V_\alpha^f := \{v \in V : f(v) = \alpha v\},$$

de no haber ambigüedad se obvia el “ $f$ ”.

Una transformación lineal  $f$  se dice *diagonalizable* si existe una base ordenada  $X$  tal que  $M_X^X(f)$  es una matriz diagonal.

**Teorema 5.4:** Un escalar  $\lambda$  es un autovalor del endomorfismo  $f$  syss  $p_f(\lambda) = 0$ .

**Proposición 5.5:** Los autoespacios de un endomorfismo son submódulos, o subespacios. En particular,  $\alpha$  es un autovalor de  $f$  syss  $V_\alpha \neq \{0\}$ .

**Teorema 5.6:** Si  $\alpha_1, \dots, \alpha_n$  son escalares distintos, entonces sus autoespacios son independientes.

DEMOSTRACIÓN: La demostración es por inducción. El caso base  $n = 1$  es trivial. Sean  $\lambda_i$  y  $v_i \in A_{\alpha_i} \setminus \{0\}$  tales que

$$\sum_{i=1}^{n+1} \lambda_i v_i = 0.$$

Si por contradicción fueran dependientes habría  $\lambda_k \neq 0$  para algún  $k$ . Reordenaremos los términos de modo que  $k = n + 1$ , luego

$$\lambda_{n+1} v_{n+1} = - \sum_{i=1}^n \lambda_i v_i.$$



Luego aplicando  $f$  a ambos lados tengo que

$$\lambda_{n+1}\alpha_{n+1}v_{n+1} = f(v_{n+1}) = -\sum_{i=1}^n \lambda_i f(v_i) = -\sum_{i=1}^n \lambda_i \alpha_i v_i.$$

Luego

$$0 = (\alpha_{n+1} - \alpha_{n+1})\lambda_{n+1}v_{n+1} = \sum_{i=1}^n \lambda_i(\alpha_{n+1} - \alpha_i)v_i.$$

Pero por hipótesis inductiva, los autoespacios de  $\alpha_1, \dots, \alpha_n$  son independientes, luego los coeficientes son nulos y en consecuencia los  $\lambda_i$  con  $i = 1, \dots, n$  lo son, por lo que  $\lambda_{n+1}$  también debe serlo.  $\square$

**Teorema 5.7:** Una transformación lineal es diagonalizable syss existe una base formada por sus autovectores.

**Teorema 5.8:** Son equivalentes:

1.  $\mathbb{k}$  es algebraicamente cerrado.
2. Toda matriz cuadrada con coeficientes en  $\mathbb{k}$  tiene un autovector.

DEMOSTRACIÓN: Claramente  $1 \implies 2$ , veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

$\square$

**Definición 5.9:** Se dice que una endo-transformación lineal  $f \in L(\mathbb{k}^n)$  es *triangularizable* syss existe una base ordenada  $X$  tal que su representación matricial es triangular. En el caso de matrices cuadradas, si existe  $C \in \text{Mat}_n(\mathbb{k})$  tal que  $C^{-1}BC$  es triangular.

**Teorema 5.10:** Para una endo-transformación lineal sobre  $V$ , son equivalentes:

1.  $f$  es triangularizable.
2. Existe una cadena maximal de subespacios  $f$ -invariantes:

$$0 =: V_0 \subset V_1 \subseteq \cdots V_n := V$$

Es decir, tal que  $f[V_k] \subseteq V_k$ .

DEMOSTRACIÓN: 1)  $\implies$  2). Si  $f$  es triangularizable, entonces sea  $X := (x_1, \dots, x_n)$  la base para la que  $f$  es triangular.  $\square$

---

## Índice de notación

---

$\vee, \wedge$	Disyuntor, “o lógico” y conjuntor, “y lógico” respectivamente.
$\implies$	Implica, entonces.
$\iff$	Si y sólo si.
$\forall, \exists$	Para todo, existe respectivamente.
$\in$	Pertenencia.
$\subseteq, \subset$	Subconjunto, subconjunto propio resp.
$\cup, \cap$	Unión e intersección binaria respectivamente.
$A \setminus B$	Resta conjuntista, $A$ menos $B$ .
$A^c$	Complemento de $A$ (respecto a un universo relativo).
$A \times B$	Producto cartesiano de $A$ por $B$ .
$A_{\neq x}$	Abreviación de $A \setminus \{x\}$ .
$f : A \rightarrow B$	Función $f$ de dominio $A$ y codominio $B$ .
$f \circ g$	Composición de $f$ con $g$ . $(f \circ g)(x) = g(f(x))$ .
$\mathcal{P}(A)$	Conjunto potencia de $A$ .
resp.	Respectivamente.

---

$\text{syss}$	Si y sólo si.
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$	Conjuntos de números naturales, enteros y racionales resp.
$\aleph_0$	Cardinal numerable, cardinalidad de $\mathbb{N}$ .
AE	Axioma de elección.
DE, AEN	Axioma de elecciones dependientes, y de elecciones numerables resp.
ZF(C)	Teoría de Zermelo-Fraenkel. La C representa el axioma de elección.
$a \mid b$	$a$ es divisor de $b$ , p. 4.
$\text{mcd}(a, b), (a; b)$	Máximo común divisor entre $a$ y $b$ , p. 5.
$\nu_p(n)$	Orden $p$ -ádico de $n$ , p. 9.
$\tau(n)$	Número de divisores de $n$ , p. 9.
$a \equiv b \pmod{n}$	$a$ congruente a $b$ en módulo $n$ , i.e., $a - b \mid n$ , p. 10.
$\mathbb{Z}_n$	Conjunto cociente dado por las clases de equivalencia de las congruencias módulo $n$ , p. 10.
$\mathbb{Z}_p$	$\mathbb{Z}_p$ con $p$ primo, p. 10.
$a^{-1}$	Inversa de un elemento invertible en un grupo, p. 11.
$S \leq G$	$S$ es subgrupo (anillo o espacio) de $G$ , p. 12.
$\langle S \rangle$	Subgrupo, cuerpo o espacio generado por $S$ , p. 13.
$\text{ord } x$	Orden de un elemento $x$ , p. 14.
$G \cong H$	$G$ y $H$ son estructuras isomorfas, p. 15.
$\mathbb{Z}_n^\times$	Grupo multiplicativo o de las unidades de $n$ , aquél formado por los coprimos de $n$ , p. 16.
$\phi(n)$	Función indicatriz de Euler de $n$ , esto es, la cantidad de coprimos positivos menores a $n$ , p. 17.
$N \trianglelefteq G$	$N$ es subgrupo normal de $G$ , p. 18.

---

$Z(S), Z(G)$	Centralizador de $S$ , centro de $G$ resp., p. 18.
$N(S)$	Normalizador de $S$ , p. 18.
$C_G(S)$	Clase de conjugación de $S$ , p. 18.
$\text{Orb}_a$	Órbita de $a$ , osea, los $\tau_g(a)$ para todo $g \in G$ , p. 26.
$\text{Stab}_a$	Estabilizador de $a$ , osea, los $g \in G$ que dejan a $a$ fijo, p. 26.
$\text{Fix}_g(S)$	Puntos fijos de la acción $\tau_g$ sobre $S$ , p. 27.
$\text{Fix}_G(S)$	Puntos fijos de todas las acciones sobre $S$ , p. 27.
$\text{Syl}_p(G)$	El conjunto de $p$ -subgrupos de Sylow de $G$ , p. 28.
$S_n$	Grupo simétrico sobre $\{1, 2, \dots, n\}$ , p. 33.
$\text{sgn } \sigma$	Signo de la permutación $\sigma$ , p. 36.
$A_n$	Grupo alternante definido en $S_n$ , p. 37.
$D_{2n}$	Grupo diedral de cardinal $2n$ , p. 39.
$A^\times$	El conjunto de elementos invertibles de un anillo unitario $A$ , p. 42.
$\mathbb{k}$	Un cuerpo general, p. 43.
$A[S]$	Conjunto de polinomios con coeficientes en $A$ y con indeterminadas de $S$ , p. 54.
$\deg f$	Grado del polinomio $f$ , p. 54.
$c(f)$	Contenido del polinomio $f$ , p. 59.
$\mathbb{C}$	Conjunto de números complejos, p. 65.
$\text{Re } z, \text{Im } z$	Parte real e imaginaria de $z$ resp., p. 65.
$\text{Hom}_A(M, N)$	Espacio de morfismos de $A$ -módulos desde $M$ a $N$ , p. 72.
$\text{adj } B$	Matriz adjunta de $B$ , p. 89.
$[K : k]$	Grado de la extensión $K$ de $k$ . Su dimensión como $k$ -espacio vectorial, p. 91.
$\text{Gal}(K/k)$	Grupo de Galois de la extensión de cuerpo $K/k$ , p. 94.

$p_f(x), p_B(x)$  Polinomio característico de un endomorfismo o una matriz,  
p. 98.

---

## *Índice alfabético*

---

- acción, 25
  - fiel, 26
  - transitiva, 26
- algebraico (elemento, extensión), 91
- algoritmo
  - de Euclides, 6
  - de Horner-Ruffini, 57
  - división entera, 3
  - división polinómica, 56
- anillo, 41
  - de división, 42
  - noetheriano, 47
  - ordenado, 43
- asociatividad, 11
- automorfismo, 15
- base, 75
- cancelación, 12
- centralizador, 18
- centro, 18
- ciclo, 34
- cociente, 4
- coeficiente
  - director, 54
  - polinomio, 53
- conjunto
  - libre, 75
  - ligado, 75
- conmutador, 21
- conmutatividad, 11
- contenido
  - de un polinomio, 59
- criterio
  - de irreductibilidad
    - de Eisenstein, 61
    - de Gauss, 61
  - de subgrupos, 12
- cuerpo, 42
  - de cocientes, 52
  - de escisión, 95
- descomposición
  - prima, 8
- determinante, 88
- divisor, 4
  - propio, impropio, 48
- dominio

- de factorización única (DFU), 49
- de ideales principales (DIP), 44
- euclídeo, 46
- íntegro, 42
- ecuación
  - de clases, 24
- elemento
  - neutro, 11
  - primo, 48
  - reductible, irreductible, 48
- endomorfismo, 15
- epimorfismo, 15
- escalar, 71
- espacio
  - vectorial, 71
- extensión
  - de cuerpos, 91
  - normal, 96
- forma
  - multilineal, 86
- fórmula
  - de Grossman, 81
- funcional, 72
- función
  - indicatriz de Euler, 16
  - lineal, 72
- grado
  - de un polinomio, 54
- grupo, 11
  - cíclico, 14
  - de Galois, 94
  - diedral, 39
  - multiplicativo de  $n$ , 16
  - resoluble, 33
  - simple, 30
- ideal, 43
  - impropio, 44
  - maximal, 47, 50
  - primo, 50
  - principal, 44
- identidad
  - de Bézout, 6
- índice (subgrupo), 16
- invertible (elemento), 11, 42
- isomorfas (estructuras), 15
- isomorfismo, 15
- $k$ -conjugados (elementos), 95
- lema
  - de Euclides, 7
  - de Gauss, 60
- matriz
  - adjunta, 89
- máximo
  - común divisor, 5, 52
- menor
  - complemento, 89
- mínimo
  - común múltiplo, 52
- módulo
  - libre, 75
- monoide, 11
- monomio, 53
- monomorfismo, 15
- morfismo, 15
  - mónico, 15
- norma
  - euclídea, 46
- normalizador, 18
- número
  - complejo, 64
- número
  - compuesto, 7



- 
- coprimo, 7
  - primo, 7
  - órbita, 34
  - orden
    - $p$ -ádico, 9
  - $p$ -grupo, 25
  - $p$ -subgrupo, 25
    - de Sylow, 28
  - polinomio
    - característico, 97
    - ciclotómico, 62
    - de interpolación de Lagrange, 58
    - minimal, 93
    - mónico, 54
    - primitivo, 59
  - propiedad
    - de factorización, 49
  - punto
    - fijo, 34
  - raíz
    - $n$ -ésima, 92
    - cuadrada, 92
    - cúbica, 92
    - de un polinomio, 54
  - regla
    - de Ruffini, 57
  - resto, 4
  - semigrupo, 11
  - sistema
    - generador, 73
  - subanillo, 43
  - subgrupo, 12
    - normal, 18
    - propio, 12
  - submódulo, 73
    - impropio, 73
  - sucesión
    - exacta, 21
  - teorema
    - chino del resto, 17
    - de bases de Hilbert, 59
    - de Cauchy, 28
    - de Cayley, 34
    - de De Moivre, 66
    - de extensión de Kronecker, 92
    - de isomorfismos
      - (primero), 22
      - (segundo), 23
      - (tercero), 23
    - de Jordan-Hölder, 31
    - de Lagrange, 16
    - de Sylow
      - (cuarto), 31
      - (primero), 28
      - (segundo), 29
      - (tercero), 30
    - fundamental
      - de la aritmética, 8
      - de los grupos abelianos finitos, 21
      - del álgebra, 68
  - trasposición, 34
  - vector, 71



---

## Bibliografía

---

### Álgebra abstracta

1. ALUFFI, P. *Algebra. Chapter 0* (American Mathematical Society, 1960).
2. CASTILLO, C. I. *Álgebra* <https://www.uv.es/ivorra/Libros/Al.pdf> (2020).
0. FINE, B. y ROSENBERGER, G. *The Fundamental Theorem of Algebra. subtitle* (Springer-Verlag New York, 1997).
3. GARRETT, P. *Abstract Algebra* <http://www-users.math.umn.edu/~garrett/m/algebra/> (2007).
4. JACOBSON, N. *Lectures in Abstract Algebra* (Springer-Verlag, 1951).
5. LEE, G. T. *Abstract Algebra. An Introductory Course* (Springer International, Switzerland, 2018).
6. MILNE, J. S. *Group Theory* <https://www.jmilne.org/math/CourseNotes/gt.html> (2020).
7. PASTÉN, H. *MAT 2218: Álgebra Abstracta II* <http://www.mat.uc.cl/~hector.pasten/mat2218files/mat2218apunte.pdf> ().

### Álgebra lineal

8. IBORT, A. y RODRÍGUEZ, M. A. *Notas de Álgebra Lineal* [http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra\\_lineal.pdf](http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra_lineal.pdf) (2014).

9. KATZNELSON, Y. y KATZNELSON, Y. R. *A (Terse) Introduction to Linear Algebra* (American Mathematical Society, 2008).

## Artículos

10. BANASCHEWSKI, B. A New Proof that “Krull implies Zorn”. *Mathematical Logic Quarterly* (1994).
11. BLASS, A. Existence of Basis implies the Axiom of Choice. *Contemporary Mathematics* **31**. <http://www.math.lsa.umich.edu/~ablass/bases-AC.pdf> (1984).
12. CONRAD, K. The Sylow Theorems. <https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf> (2018).
13. CONRAD, K. Zorn’s Lemma and some applications. <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf> (2018).