UNIVERSIDAD DE GRANADA

Álgebra Lineal y Estructuras Matemáticas

Temario de la asignatura

Ismael Sallami Moreno

Recursos Ingeniería Informática y Ade

Licencia

Álgebra Lineal y Estructuras Matemáticas

Ismael Sallami Moreno

https://elblogdeismael.github.io

Índice general

Capítulo 1

Aritmética entera y modular

Bloque 1 del programa. Divisibilidad, el algoritmo de Euclides, congruencias, la construcción de $\mathbb{Z}_n$, el teorema de Euler y los polinomios sobre cuerpos finitos.

1.1 Los números naturales y la división

El principio que sostiene todo el bloque:

Teorema 1.1 (Algoritmo de la división). Dados $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ con $b \neq 0$, existen enteros únicos q y r tales que

$$a = bq + r, \qquad 0 \leq r < |b|$$

La unicidad es lo que convierte el resto en una función bien definida, y de ahí sale la aritmética modular entera.

1.1.1 Sistemas de numeración

Todo entero positivo se escribe de forma única en base $b \geq 2$:

$$n = \sum_{i=0}^{k} d_i \, b^i, \qquad 0 \leq d_i < b$$

La conversión a base b es aplicar el algoritmo de la división repetidamente y leer los restos al revés. Con b potencia de 2 la conversión desde binario es agrupar dígitos, y de ahí que la informática use 8 y 16.

1.2 Divisibilidad

Concepto	Definición
$a \mid b$	existe c con $b = ac$
Máximo común divisor	el mayor d con $d \mid a$ y $d \mid b$
Mínimo común múltiplo	el menor positivo múltiplo de los dos
Primos entre sí	$\mathrm{mcd}(a, b) = 1$

Proposición 1.1 . $\mathrm{mcd}(a, b) \cdot \mathrm{mcm}(a, b) = |ab|$.

1.2.1 El algoritmo de Euclides

Se apoya en que $\mathrm{mcd}(a,b) = \mathrm{mcd}(b, a \bmod b)$, y termina porque los restos decrecen estrictamente.

Ejemplo 1.1 . $\mathrm{mcd}(1071, 462)$:

a	b	q	r
1071	462	2	147
462	147	3	21
147	21	7	0

El último resto no nulo es 21, así que $\mathrm{mcd}(1071, 462) = 21$.

Su coste es $O(\log \min(a,b))$ divisiones, que es lo que lo hace utilizable con números de cientos de cifras. Calcular el máximo común divisor factorizando sería inviable, y esa asimetría es la base de la criptografía de clave pública.

Teorema 1.2 (Identidad de Bézout). Para cualesquiera a, b enteros no ambos nulos existen $u, v \in \mathbb{Z}$ con

$$\mathrm{mcd}(a,b) = ua + vb$$

El **algoritmo extendido de Euclides** calcula u y v arrastrando los coeficientes hacia atrás. Su utilidad concreta: es como se calculan los inversos en $\mathbb{Z}_n$, que es el resultado central del bloque.

1.2.2 Números primos

Teorema 1.3 (Fundamental de la aritmética). Todo entero mayor que 1 se descompone en producto de primos de forma única salvo el orden.

Teorema 1.4 (Euclides). Hay infinitos primos.

Demostración 1.1 . Si solo hubiese finitos, $p_1, \ldots, p_k$, el número $N = p_1 p_2 \cdots p_k + 1$ no sería divisible por ninguno de ellos, ya que da resto 1 con todos. Entonces N o es primo o tiene un factor primo fuera de la lista; en los dos casos la lista no era completa.

Para decidir si n es primo basta probar divisores hasta $\sqrt{n}$: si $n = ab$ con $a \le b$, entonces $a \le \sqrt{n}$. Ese detalle rebaja el coste de $O(n)$ a $O(\sqrt{n})$, y la criba de Eratóstenes lo aprovecha para listar todos los primos hasta n.

1.3 El anillo $\mathbb{Z}$

$(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad, y además **dominio de integridad**: si $ab = 0$, entonces $a = 0$ o $b = 0$. No es un cuerpo, porque los únicos elementos con inverso son 1 y -1.

Esa carencia es justo la que $\mathbb{Z}_n$ va a resolver, para ciertos n.

1.4 Congruencias y $\mathbb{Z}_n$

Definición 1.1 (Congruencia). $a \equiv b \pmod{n}$ si $n \mid (a-b)$.

Es una relación de equivalencia, y sus clases forman $\mathbb{Z}_n$. Las operaciones se definen sobre representantes y **están bien definidas**: el resultado no depende del representante elegido, y eso es lo que hay que comprobar antes de usarlas.

Propiedad	Enunciado
Suma	$a \equiv b,\ c \equiv d \Rightarrow a+c \equiv b+d$
Producto	mismas hipótesis $\Rightarrow ac \equiv bd$
Potencia	$a \equiv b \Rightarrow a^k \equiv b^k$
Cancelación	$ac \equiv bc \pmod{n}$ y $\mathrm{mcd}(c,n)=1 \Rightarrow a \equiv b$

La cancelación **exige la hipótesis**: $2\cdot 3 \equiv 2\cdot 0 \pmod 6$ y sin embargo $3 \not\equiv 0$. Cancelar sin comprobar que el factor es primo con el módulo es el error más repetido del bloque.

1.4.1 Inversos

Teorema 1.5 . a tiene inverso en $\mathbb{Z}_n$ si y solo si $\mathrm{mcd}(a,n)=1$. En consecuencia, $\mathbb{Z}_n$ es un cuerpo si y solo si n es primo.

Demostración 1.2 . Si $\mathrm{mcd}(a,n)=1$, por Bézout hay u, v con $ua+vn=1$, y reduciendo módulo n queda $ua \equiv 1$, así que u es el inverso. Recíprocamente, si $ua \equiv 1 \pmod{n}$ entonces $ua-1=kn$, luego cualquier divisor común de a y n divide a 1.

El inverso se calcula con Euclides extendido, no probando candidatos.

Ejemplo 1.2 . Inverso de 7 módulo 26. Euclides: $26 = 3\cdot 7 + 5$, $7 = 1\cdot 5 + 2$, $5 = 2\cdot 2 + 1$. Hacia atrás:

$$1 = 5 - 2\cdot 2 = 5 - 2(7-5) = 3\cdot 5 - 2\cdot 7 = 3(26 - 3\cdot 7) - 2\cdot 7 = 3\cdot 26 - 11\cdot 7$$

Luego $-11\cdot 7 \equiv 1 \pmod{26}$, y el inverso es $-11 \equiv 15$. Comprobación: $7\cdot 15 = 105 = 4\cdot 26 + 1$.

1.4.2 La función de Euler y su teorema

Definición 1.2 . $\varphi(n)$ es la cantidad de enteros entre 1 y n primos con n.

Proposición 1.2 . φ es multiplicativa para argumentos primos entre sí, $\varphi(p) = p-1$ para p primo y $\varphi(p^k) = p^k - p^{k-1}$. De ahí

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Teorema 1.6 (Euler). Si $\mathrm{mcd}(a,n)=1$ entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corolario 1.1 (Pequeño teorema de Fermat). Si p es primo y $p \nmid a$, entonces $a^{p-1} \equiv 1$

(mód p).

El teorema de Euler es lo que permite **reducir exponentes enormes**: para calcular a^k mód n basta con k mód $\varphi(n)$. Sin él, la exponenciación modular de la criptografía no sería practicable.

Ejemplo 1.3 . 7^{1000} mód 26. Como $\varphi(26) = \varphi(2)\varphi(13) = 1 \cdot 12 = 12$ y $\mathrm{mcd}(7, 26) = 1$, se tiene $7^{12} \equiv 1$. Y $1000 = 83 \cdot 12 + 4$, así que $7^{1000} \equiv 7^4 = 2401 = 92 \cdot 26 + 9 \equiv 9 \pmod{26}$.

1.5 Ecuaciones y sistemas de congruencias

Teorema 1.7 (Ecuación lineal en congruencias). $ax \equiv b \pmod{n}$ tiene solución si y solo si $d = \mathrm{mcd}(a, n)$ divide a b, y en ese caso tiene exactamente d soluciones distintas módulo n.

El número de soluciones sorprende y conviene retenerlo: **no es cero o una**, es cero o d. Con $6x \equiv 4$ (mód 8), $d = 2$ divide a 4 y hay dos soluciones, $x = 2$ y $x = 6$.

Teorema 1.8 (Chino de los restos). Si $n_1, \ldots, n_k$ son primos entre sí dos a dos, el sistema

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, \ldots, k$$

tiene solución única módulo $N = n_1 n_2 \cdots n_k$.

Es el resultado con más aplicaciones del bloque: permite trabajar con números grandes descomponiéndolos en restos módulo primos pequeños, hacer las operaciones en paralelo y recomponer al final.

1.6 Polinomios y cuerpos finitos

$K[x]$, con K un cuerpo, se comporta como $\mathbb{Z}$: hay división con resto, máximo común divisor por Euclides, identidad de Bézout y factorización única en irreducibles.

$\mathbb{Z}$	$K[x]$
valor absoluto	grado
número primo	polinomio irreducible
$\mathbb{Z}_n$	$K[x]/(p(x))$
$\mathbb{Z}_p$ es cuerpo si p primo	$K[x]/(p)$ es cuerpo si p es irreducible

La analogía es exacta, y verla ahorra memorizar la mitad de los resultados.

Concepto	Enunciado
Teorema del resto	el resto de dividir P entre $x - a$ es $P(a)$
Raíz	a es raíz $\iff (x - a) \mid P$
Multiplicidad	mayor k con $(x - a)^k \mid P$
Número de raíces	un polinomio de grado n tiene como mucho n raíces en un cuerpo

La última fila **falla si el anillo no es un cuerpo**: en $\mathbb{Z}_8$, el polinomio $x^2 - 1$ tiene cuatro raíces, que son 1, 3, 5 y 7.

1.6.1 Construcción de cuerpos finitos

Si $p(x)$ es irreducible de grado m sobre $\mathbb{Z}_q$, entonces $\mathbb{Z}_q[x]/(p(x))$ es un cuerpo con q^m elementos.

Ejemplo 1.4 . $x^2 + x + 1$ es irreducible sobre $\mathbb{Z}_2$, porque no tiene raíces: $p(0) = p(1) = 1$. El cociente $\mathbb{Z}_2[x]/(x^2 + x + 1)$ es un cuerpo de cuatro elementos $\{0, 1, \alpha, \alpha + 1\}$ con $\alpha^2 = \alpha + 1$.

Los cuerpos finitos tienen siempre p^m elementos con p primo. No existe ningún cuerpo de 6 elementos.

Los cuerpos finitos son la base de los códigos correctores de errores y del cifrado AES, y esa es su presencia en un grado de informática.

1.7 Ejercicios

Ejercicio 1.7.1. Resolver $14x \equiv 30 \pmod{100}$.

Solución 1.7.1. $d = \text{mcd}(14, 100) = 2$, que divide a 30, así que hay dos soluciones módulo 100. Se divide todo por 2: $7x \equiv 15 \pmod{50}$. El inverso de 7 módulo 50 es 43, porque $7 \cdot 43 = 301 = 6 \cdot 50 + 1$. Entonces $x \equiv 43 \cdot 15 = 645 \equiv 45 \pmod{50}$, y las dos soluciones módulo 100 son $x = 45$ y $x = 95$.

Ejercicio 1.7.2. Calcular $\varphi(360)$.

Solución 1.7.2. $360 = 2^3 \cdot 3^2 \cdot 5$, así que

$$\varphi(360) = 360\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right) = 360 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 96$$

Ejercicio 1.7.3. Encontrar el menor entero positivo que da resto 2 al dividirlo entre 3, resto 3 entre 5 y resto 2 entre 7.

Solución 1.7.3. Los módulos son primos entre sí, así que el teorema chino garantiza solución única módulo 105. De $x \equiv 2 \pmod 3$ y $x \equiv 2 \pmod 7$ sale $x \equiv 2 \pmod{21}$, es decir $x = 2 + 21k$. Imponiendo $x \equiv 3 \pmod 5$: $2 + 21k \equiv 3$, o sea $k \equiv 1 \pmod 5$. Con $k = 1$, $x = 23$. Comprobación: $23 = 7 \cdot 3 + 2 = 4 \cdot 5 + 3 = 3 \cdot 7 + 2$.

El desarrollo de la aritmética entera y modular está en Grimaldi, 1998 y Dorronsoro y Hernández, 1999, y su tratamiento con problemas en Merino y Santos, 2021.

Capítulo 2

Combinatoria

Bloque 2 del programa. Los principios de la suma y del producto, el principio de Dirichlet, y las variaciones, permutaciones y combinaciones.

2.1 Los dos principios básicos

Proposición 2.1 (Principio de la suma). Si una tarea se puede hacer de m formas o bien de n formas, y las dos maneras son excluyentes, hay $m + n$ formas de hacerla.

Proposición 2.2 (Principio del producto). Si una tarea consta de dos pasos sucesivos, el primero con m opciones y el segundo con n para cada elección del primero, hay mn formas de hacerla.

La regla para saber cuál aplicar: **«o» suma, «y» multiplica**. La condición de que las opciones sean excluyentes en la suma es esencial, y cuando no lo son hace falta el principio de inclusión-exclusión.

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

En general se alternan los signos: se suman las intersecciones de un número impar de conjuntos y se restan las de número par.

Ejemplo 2.1 . ¿Cuántos enteros de 1 a 1000 son múltiplos de 3 o de 5? Hay $\lfloor 1000/3 \rfloor = 333$ múltiplos de 3, $\lfloor 1000/5 \rfloor = 200$ de 5 y $\lfloor 1000/15 \rfloor = 66$ de los dos. Por inclusión-exclusión, $333 + 200 - 66 = 467$. Sumar sin restar daría 533 y contaría dos veces los múltiplos de 15.

2.2 El principio de Dirichlet

Teorema 2.1 (Principio del palomar). Si se reparten n objetos en m cajas con $n > m$, alguna caja recibe al menos dos objetos. En general, alguna recibe al menos $\lceil n/m \rceil$.

Es de enunciado trivial y de aplicación sorprendente. Lo difícil nunca es el principio: es **elegir qué son los objetos y qué son las cajas**.

Ejemplo 2.2 . En un grupo de 367 personas hay al menos dos que cumplen años el mismo día: los objetos son las personas y las cajas los 366 días posibles.

Más fino: entre 10 enteros cualesquiera del 1 al 100, hay dos subconjuntos disjuntos con la misma suma. Los objetos son los $2^{10} - 1 = 1023$ subconjuntos no vacíos y las cajas las sumas posibles, que van de 1 a $91 + \cdots + 100 = 955$. Como $1023 > 955$, dos subconjuntos comparten suma, y quitándoles su intersección quedan disjuntos.

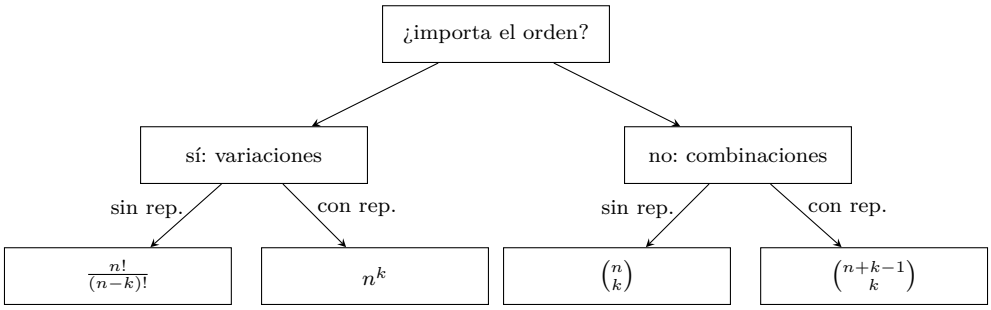
En informática, el palomar es lo que demuestra que **toda función hash tiene colisiones**, y que ningún compresor sin pérdida puede reducir el tamaño de todas las entradas.

2.3 Variaciones, permutaciones y combinaciones

Todo el bloque se resume en dos preguntas: **¿importa el orden?** y **¿se puede repetir?**

	Sin repetición	Con repetición
Ordenado	$V_{n,k} = \dfrac{n!}{(n-k)!}$	$VR_{n,k} = n^k$
No ordenado	$\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$	$\binom{n+k-1}{k}$

Y el caso $k = n$ en la primera fila da las **permutaciones**, $P_n = n!$.



2.3.1 Permutaciones con elementos repetidos

Si hay n objetos de los que n_1 son de un tipo, n_2 de otro, y así:

$$PR_n^{n_1,\ldots,n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}$$

Ejemplo 2.3 . Anagramas de `MATEMATICA`: son 10 letras con A repetida 3 veces, M 2, T 2, y E, I, C una vez. El total es

$$\frac{10!}{3!\, 2!\, 2!} = \frac{3\,628\,800}{24} = 151\,200$$

2.3.2 Combinaciones con repetición

Elegir k elementos de n tipos, sin importar el orden y pudiendo repetir. La demostración estándar es la de **las barras y las estrellas**: se representan las elecciones como k estrellas separadas por $n - 1$ barras, y contar las disposiciones da

$$CR_{n,k} = \binom{n+k-1}{k}$$

$$\star\star \mid \star \mid\mid \star\star\star$$

2 del tipo 1, 1 del tipo 2, 0 del tipo 3, 3 del tipo 4

Es la fórmula que cuenta las soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_n = k$, y por eso aparece en tantos problemas que no parecen combinatorios.

2.4 Números combinatorios

Propiedad	Expresión
Simetría	$\binom{n}{k} = \binom{n}{n-k}$
Recurrencia de Pascal	$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
Suma de una fila	$\sum_{k=0}^{n} \binom{n}{k} = 2^n$
Suma alternada	$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ para $n \geq 1$
Binomio de Newton	$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

La recurrencia de Pascal tiene una lectura combinatoria directa, y es la mejor forma de recordarla: para elegir k de n, o se toma el último elemento —y quedan $k-1$ por elegir de $n-1$— o no se toma —y quedan k de $n-1$—.

La tercera fila cuenta los subconjuntos de un conjunto de n elementos, que son 2^n porque cada elemento entra o no entra.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

2.5 Ejercicios

Ejercicio 2.5.1. ¿De cuántas formas se pueden sentar 8 personas en una mesa redonda, si dos disposiciones que difieren en una rotación se consideran iguales?

Solución 2.5.1. Se fija una persona para eliminar la simetría de rotación, y las otras 7 se ordenan libremente: $7! = 5040$. En general, las permutaciones circulares de n elementos son $(n-1)!$. Si además se identificaran las disposiciones simétricas respecto de un eje, habría que dividir por 2.

Ejercicio 2.5.2. ¿Cuántas contraseñas de 8 caracteres se pueden formar con las 26 letras minúsculas y los 10 dígitos? ¿Y si se exige al menos un dígito?

Solución 2.5.2. Importa el orden y se puede repetir: $36^8 = 2{,}82 \times 10^{12}$. Para la segunda pregunta se cuenta el complementario: las que *no* tienen ningún dígito son $26^8 = 2{,}09 \times 10^{11}$, así que la respuesta es $36^8 - 26^8 = 2{,}61 \times 10^{12}$. Contar el complementario suele ser mucho más sencillo que contar los casos con «al menos uno».

Ejercicio 2.5.3. ¿Cuántas soluciones enteras no negativas tiene $x_1 + x_2 + x_3 + x_4 = 12$?

Solución 2.5.3. Es una combinación con repetición: repartir 12 unidades entre 4 variables sin importar el orden dentro de cada una. Son

$$\binom{4+12-1}{12} = \binom{15}{12} = \binom{15}{3} = 455$$

Con barras y estrellas: 12 estrellas y 3 barras, y hay que elegir dónde van las barras entre las 15 posiciones.

El desarrollo de la combinatoria está en Grimaldi, 1998, y sus problemas en Lipschutz, 1991.

Capítulo 3

Sistemas de ecuaciones lineales y matrices

Bloque 3 del programa. El método de Gauss-Jordan, la forma normal de Hermite, las operaciones con matrices, la matriz inversa y los determinantes.

3.1 Sistemas de ecuaciones lineales

Un sistema de m ecuaciones con n incógnitas sobre un cuerpo K:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \iff A\mathbf{x} = \mathbf{b}$$

Clasificación	Cuándo
Compatible determinado	solución única
Compatible indeterminado	infinitas soluciones
Incompatible	ninguna
Homogéneo	$\mathbf{b} = \mathbf{0}$; siempre compatible

Un sistema homogéneo nunca es incompatible, porque $\mathbf{x} = \mathbf{0}$ siempre lo resuelve. La pregunta interesante es si tiene **otras** soluciones, y la respuesta la da el rango.

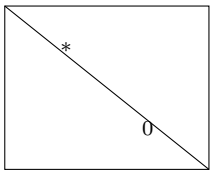
3.2 El método de Gauss-Jordan

Se aplican operaciones elementales por filas a la matriz ampliada hasta llegar a una forma en la que la solución se lee.

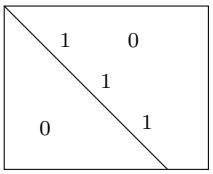
Operación elemental	Efecto
$F_i \leftrightarrow F_j$	intercambiar filas
$F_i \to \lambda F_i$, $\lambda \neq 0$	escalar una fila
$F_i \to F_i + \lambda F_j$	sumar un múltiplo de otra

Las tres son reversibles, y por eso **el sistema resultante tiene exactamente las mismas soluciones**. Esa es la justificación del método, y conviene tenerla presente: no se está simplificando por comodidad, se está sustituyendo por un sistema equivalente.

Forma	Qué exige
Escalonada (Gauss)	ceros bajo cada pivote; los pivotes avanzan a la derecha
Escalonada reducida (Gauss-Jordan)	además, pivotes iguales a 1 y ceros también encima



escalonada



escalonada reducida

3.2.1 El teorema de Rouché-Frobenius

Teorema 3.1 (Rouché-Frobenius). Sea $A\mathbf{x} = \mathbf{b}$ con n incógnitas y A^* la matriz ampliada.

- Si $\operatorname{rg} A \neq \operatorname{rg} A^*$, el sistema es incompatible.
- Si $\operatorname{rg} A = \operatorname{rg} A^* = n$, es compatible determinado.
- Si $\operatorname{rg} A = \operatorname{rg} A^* = r < n$, es compatible indeterminado con $n - r$ parámetros libres.

En la práctica no hace falta calcular rangos aparte: **la forma escalonada los muestra a la vez**. El número de pivotes es el rango de A; una fila del tipo $(0\ 0\ \ldots\ 0 \mid c)$ con $c \neq 0$ delata la incompatibilidad; y las columnas sin pivote son los parámetros libres.

Ejemplo 3.1 .

$$\left(\begin{array}{ccc|c} 1 & 2 & -1 & 3 \\ 2 & 4 & 1 & 9 \\ 1 & 2 & 2 & 6 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 2 & 0 & 4 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Hay dos pivotes, en las columnas 1 y 3, así que $\operatorname{rg} A = \operatorname{rg} A^* = 2 < 3$: compatible indeterminado con un parámetro. Tomando $x_2 = t$, la solución es $(4 - 2t,\ t,\ 1)$.

3.2.2 Forma normal de Hermite

Es la forma escalonada reducida por filas, y su interés es que **es única**: dos matrices tienen la misma forma de Hermite si y solo si sus filas generan el mismo subespacio. La forma escalonada sin reducir no lo es, porque depende de las operaciones concretas que se hayan hecho.

De ahí que sirva como forma canónica para decidir la equivalencia por filas de dos matrices, sin comparar los caminos que llevaron a ellas.

3.3 Matrices

Operación	Definición	Condición
Suma	elemento a elemento	mismo tamaño
Producto por escalar	elemento a elemento	—
Producto	$(AB)_{ij} = \sum_k a_{ik} b_{kj}$	columnas de A = filas de B

Operación	Definición	Condición
Traspuesta	$(A^T)_{ij} = a_{ji}$	—

El producto es asociativo y distributivo, y **no es conmutativo**. Dos consecuencias que se usan mal con frecuencia:

- $(A+B)^2 \neq A^2 + 2AB + B^2$ salvo que A y B conmuten.
- $(AB)^T = B^T A^T$, con el orden invertido. Lo mismo para la inversa.

Y hay **divisores de cero**: $AB = 0$ no obliga a que A o B sean nulas. El anillo de matrices no es un dominio de integridad, así que no se puede cancelar.

Tipo de matriz	Definición
Simétrica	$A^T = A$
Antisimétrica	$A^T = -A$
Diagonal	nula fuera de la diagonal
Triangular	nula por debajo o por encima
Ortogonal	$A^T A = I$
Idempotente	$A^2 = A$
Nilpotente	$A^k = 0$ para algún k

3.4 Rango

Definición 3.1 (Rango). Número de filas no nulas de una forma escalonada de A. Coincide con el número máximo de filas linealmente independientes y con el de columnas linealmente independientes.

Que el rango por filas y por columnas coincidan no es evidente y es uno de los resultados centrales del bloque: dice que la matriz tiene **una sola** dimensión esencial, mirada desde donde se mire.

Propiedad	Enunciado
Acotación	$\operatorname{rg} A \leq \min(m, n)$
Traspuesta	$\operatorname{rg} A = \operatorname{rg} A^T$
Producto	$\operatorname{rg}(AB) \leq \min(\operatorname{rg} A, \operatorname{rg} B)$
Invertibilidad	$A_{n\times n}$ es invertible $\iff \operatorname{rg} A = n$

3.5 Matriz inversa

Definición 3.2 . A cuadrada es invertible si existe A^{-1} con $AA^{-1} = A^{-1}A = I$. La inversa, cuando existe, es única.

Teorema 3.2 (Caracterizaciones de la invertibilidad). Para A de orden n, son equivalentes:

- A es invertible.
- $\operatorname{rg} A = n$.
- $\det A \neq 0$.
- $A\mathbf{x} = \mathbf{0}$ solo tiene la solución trivial.

- $A\mathbf{x} = \mathbf{b}$ tiene solución única para todo $\mathbf{b}$.
- Las filas de A son linealmente independientes.
- A es producto de matrices elementales.

Que las siete sean equivalentes es lo que hace del rango la herramienta que responde todas las preguntas del bloque.

3.5.1 Cálculo por Gauss-Jordan

Se escribe $(A \mid I)$ y se reduce hasta $(I \mid A^{-1})$. Si en el camino aparece una fila de ceros a la izquierda, la matriz no es invertible.

Es el método que se usa: la fórmula con la adjunta necesita n^2 determinantes de orden $n-1$ y **solo es practicable para orden 2 o 3**.

$$A^{-1} = \frac{1}{\det A}\,\operatorname{adj}(A)^T$$

3.6 Determinantes

Para orden 2 y 3, las reglas conocidas; en general, el desarrollo por una fila o columna:

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij}\, M_{ij}$$

con M_{ij} el menor complementario.

Propiedad	Enunciado
Filas	$\det A^T = \det A$
Intercambio	cambiar dos filas cambia el signo
Escalado	multiplicar una fila por λ multiplica el determinante por λ
Combinación	sumar a una fila un múltiplo de otra **no lo cambia**
Fila nula o repetida	el determinante es 0
Producto	$\det(AB) = \det A \cdot \det B$
Inversa	$\det\big(A^{-1}\big) = 1/\det A$
Escalar	$\det(\lambda A) = \lambda^n \det A$
Triangular	el producto de la diagonal

Las filas cuarta y última son las que dan el método de cálculo: se triangula por Gauss —que no cambia el determinante— y se multiplica la diagonal. Coste $O(n^3)$ frente a $O(n!)$ del desarrollo por menores.

Nota 3.1 . La tercera y la octava se confunden a menudo. Multiplicar *una* fila por λ multiplica el determinante por λ; multiplicar *toda* la matriz lo multiplica por λ^n, porque son n filas.

3.6.1 Regla de Cramer

Si $\det A \neq 0$, la solución del sistema es

$$x_i = \frac{\det A_i}{\det A}$$

con A_i la matriz A cambiando su columna i por $\mathbf{b}$.

Su valor es **teórico**: da la solución en forma cerrada y muestra que depende de los datos de manera continua. Para calcular es inviable, porque necesita $n+1$ determinantes.

3.7 Ejercicios

Ejercicio 3.7.1. Discutir según a el sistema

$$\begin{cases} x + y + z = 1 \\ x + ay + z = 1 \\ x + y + az = a \end{cases}$$

Solución 3.7.1. $\det A = (a-1)^2$. Si $a \neq 1$ el sistema es compatible determinado. Si $a = 1$, las tres ecuaciones se convierten en $x + y + z = 1$ las dos primeras y $x + y + z = 1$ la tercera: $\operatorname{rg} A = \operatorname{rg} A^* = 1 < 3$, compatible indeterminado con dos parámetros. No hay ningún valor que lo haga incompatible.

Ejercicio 3.7.2. Si A es de orden 4 y $\det A = 3$, calcular $\det(2A)$, $\det\left(A^{-1}\right)$ y $\det\left(A^T A\right)$.

Solución 3.7.2. $\det(2A) = 2^4 \cdot 3 = 48$, porque el factor afecta a las cuatro filas. $\det\left(A^{-1}\right) = 1/3$. Y $\det\left(A^T A\right) = \det A^T \cdot \det A = 3 \cdot 3 = 9$.

Ejercicio 3.7.3. Demostrar que si $A^2 = A$ y $A \neq I$, entonces A no es invertible.

Solución 3.7.3. Si lo fuera, multiplicando $A^2 = A$ por A^{-1} quedaría $A = I$, en contra de la hipótesis. Alternativamente, de $\det(A)^2 = \det A$ sale $\det A \in \{0, 1\}$, y el caso $\det A = 1$ lleva por el mismo argumento a $A = I$.

El desarrollo de sistemas, matrices y determinantes está en Merino y Santos, 2021 y Strang, 2007, y sus problemas en Rojo y Martín, 2005 y de Diego, 1995.

Capítulo 4

Espacios vectoriales

Bloque 4 del programa. La estructura de espacio vectorial, bases y coordenadas, y las operaciones con subespacios.

4.1 Definición

Definición 4.1 (Espacio vectorial). Un conjunto V con una suma interna y un producto por escalares de un cuerpo K, tal que $(V,+)$ es grupo abeliano y el producto cumple, para todos $\lambda,\mu \in K$ y $u,v \in V$:

$$\lambda(u+v)=\lambda u+\lambda v,\quad (\lambda+\mu)v=\lambda v+\mu v,\quad \lambda(\mu v)=(\lambda\mu)v,\quad 1\cdot v=v$$

Lo que hace potente la definición es lo que **no** dice: no menciona flechas, ni coordenadas, ni dimensión. Por eso los mismos teoremas valen para objetos muy distintos:

Espacio	Vectores	Dimensión
K^n	n-uplas	n
$\mathcal{M}_{m\times n}(K)$	matrices	mn
$K_n[x]$	polinomios de grado $\leq n$	$n+1$
$K[x]$	todos los polinomios	infinita
Soluciones de un sistema homogéneo	vectores de K^n	$n-\operatorname{rg} A$

La última fila es la que conecta con el bloque anterior: **el conjunto de soluciones de un sistema homogéneo es un espacio vectorial**, y el de uno no homogéneo no lo es, porque no contiene al cero.

4.2 Subespacios

Proposición 4.1 (Caracterización). $W \subseteq V$ no vacío es subespacio si y solo si

$$\lambda u+\mu v \in W \quad \text{para todos } u,v \in W,\ \lambda,\mu \in K$$

En la práctica se comprueban tres cosas: que $\mathbf{0} \in W$, que la suma no se sale y que el producto por escalar no se sale. **Empezar por el cero descarta la mayoría de los candidatos falsos en un segundo.**

4.2.1 Combinaciones lineales y sistemas generadores

Concepto	Definición
Combinación lineal	$\lambda_1 v_1 + \cdots + \lambda_k v_k$
Subespacio generado	$\langle S \rangle$, todas las combinaciones de S
Sistema generador	S con $\langle S \rangle = V$
Linealmente independiente	$\sum \lambda_i v_i = 0 \Rightarrow$ todos los $\lambda_i = 0$

Nota 4.1 . La independencia lineal se comprueba resolviendo un sistema homogéneo: los vectores son independientes si y solo si ese sistema solo tiene la solución trivial, es decir, si el rango de la matriz que forman es igual a su número. Toda pregunta de este bloque acaba siendo un cálculo de rango.

4.3 Bases y dimensión

Definición 4.2 (Base). Sistema generador linealmente independiente.

Teorema 4.1 (De la base). Todo espacio vectorial finitamente generado tiene base, y todas sus bases tienen el mismo número de elementos, llamado dimensión.

Teorema 4.2 (Unicidad de las coordenadas). Si $B = \{e_1, \ldots, e_n\}$ es base de V, todo $v \in V$ se escribe de forma única como $v = x_1 e_1 + \cdots + x_n e_n$.

La unicidad es lo que permite **identificar V con K^n**: fijada una base, un vector abstracto se convierte en una lista de números y todo lo del bloque 3 se puede aplicar.

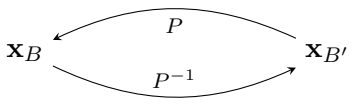
Resultado	Enunciado
Prolongación	todo conjunto independiente se amplía a una base
Extracción	de todo sistema generador se extrae una base
Con $\dim V = n$	n vectores independientes ya son base
Con $\dim V = n$	n generadores ya son base

Las dos últimas ahorran trabajo: **si el número coincide con la dimensión, basta comprobar una de las dos condiciones**.

4.3.1 Cambio de base

Si B y B' son bases y P es la matriz cuyas columnas son las coordenadas de los vectores de B' respecto de B:

$$\mathbf{x}_B = P\,\mathbf{x}_{B'}, \qquad \mathbf{x}_{B'} = P^{-1}\mathbf{x}_B$$



El sentido de la flecha se equivoca constantemente. La matriz cuyas columnas son los vectores nuevos en la base vieja transforma coordenadas *nuevas* en *viejas*, que es lo contrario de lo que sugiere la intuición.

4.4 Operaciones con subespacios

Operación	Definición	¿Es subespacio?
Intersección	$U \cap W$	sí, siempre
Unión	$U \cup W$	**no**, salvo que uno contenga al otro
Suma	$U + W = \{u + w\}$	sí; es el menor que contiene a los dos
Suma directa	$U \oplus W$ si $U \cap W = \{0\}$	sí

Que la unión no sea subespacio se ve en $\mathbb{R}^2$ con dos rectas distintas por el origen: sumando un vector de cada una se sale de las dos. **La suma es la reparación de ese fallo**: es el subespacio generado por la unión.

Teorema 4.3 (Fórmula de Grassmann).

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Es el principio de inclusión-exclusión del bloque 2, con dimensiones en lugar de cardinales. Y da un criterio inmediato: la suma es directa si y solo si $\dim(U + W) = \dim U + \dim W$.

Ejemplo 4.1 . En $\mathbb{R}^3$, dos planos distintos que pasan por el origen tienen dimensión 2 cada uno y su suma es todo $\mathbb{R}^3$, de dimensión 3. Grassmann da $\dim(U \cap W) = 2 + 2 - 3 = 1$: se cortan en una recta, nunca solo en el origen. Dos planos de $\mathbb{R}^3$ no pueden estar en suma directa.

4.4.1 Cómo se describe un subespacio

Hay dos formas, y saber pasar de una a otra es media asignatura:

Forma	Cómo se da	Cómo se obtiene la otra
Paramétrica	por un sistema generador	eliminar los parámetros
Implícita	por ecuaciones homogéneas	resolver el sistema

$$\dim W = n - (\text{número de ecuaciones independientes})$$

Cada forma sirve para una cosa distinta: con la implícita se comprueba de un vistazo si un vector pertenece, y con la paramétrica se generan vectores del subespacio. Y la **intersección** es inmediata en implícitas —se juntan las ecuaciones— mientras que la **suma** es inmediata en paramétricas —se juntan los generadores—.

4.5 Ejercicios

Ejercicio 4.5.1. ¿Es $W = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 1\}$ un subespacio de $\mathbb{R}^3$?

Solución 4.5.1. No: el vector nulo no cumple la ecuación, ya que $0 + 0 + 0 = 0 \neq 1$. Es un plano afín, trasladado del subespacio $x + y + z = 0$. La comprobación del cero descarta el candidato sin tener que mirar la suma ni el producto.

Ejercicio 4.5.2. Hallar la dimensión, una base y la ecuación implícita de $W = \langle (1,2,1),\ (2,1,-1),\ (4,5,1)\rangle$ en $\mathbb{R}^3$.

Solución 4.5.2. El determinante de los tres vectores es 0, así que el rango es menor que 3. De hecho $(4,5,1) = 2(1,2,1) + (2,1,-1)$, y los dos primeros son independientes, luego $\dim W = 2$ y una base es $\{(1,2,1),(2,1,-1)\}$. Para la ecuación implícita se impone que (x,y,z) sea combinación de la base, es decir que el determinante de los tres se anule, y sale $x - y + z = 0$. Comprobación: los dos vectores de la base la cumplen.

Ejercicio 4.5.3. En $\mathbb{R}^4$, $\dim U = 3$ y $\dim W = 2$. ¿Cuál es la dimensión mínima posible de $U \cap W$?

Solución 4.5.3. Por Grassmann, $\dim(U \cap W) = 3 + 2 - \dim(U + W)$, y como $U + W \subseteq \mathbb{R}^4$ se tiene $\dim(U + W) \leq 4$. Luego $\dim(U \cap W) \geq 1$: nunca se cortan solo en el origen. En $\mathbb{R}^4$ no caben un subespacio de dimensión 3 y otro de dimensión 2 en suma directa, porque sumarían 5.

El desarrollo de los espacios vectoriales está en Merino y Santos, 2021 y Strang, 2007, y sus problemas en Rojo y Martín, 2005 y de Burgos, 1989.

Capítulo 5

Aplicaciones lineales y diagonalización

Bloque 5 del programa. Aplicaciones lineales, núcleo e imagen, la matriz asociada, y la diagonalización por semejanza.

5.1 Aplicaciones lineales

Definición 5.1 (Aplicación lineal). $f : V \to W$ entre espacios sobre el mismo cuerpo es lineal si

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v)$$

para todos $u, v \in V$ y $\lambda, \mu \in K$.

De la definición sale de inmediato que $f(\mathbf{0}) = \mathbf{0}$, que es el primer descarte al comprobar si una aplicación es lineal.

Proposición 5.1 . Una aplicación lineal queda determinada por las imágenes de una base: si $B = \{e_1, \ldots, e_n\}$ es base de V y se fijan $f(e_1), \ldots, f(e_n)$ libremente en W, existe una única aplicación lineal con esas imágenes.

Ese resultado es lo que reduce el estudio de las aplicaciones lineales al de las matrices: **saber n imágenes basta para conocerlo todo**.

Tipo	Definición
Monomorfismo	inyectiva
Epimorfismo	sobreyectiva
Isomorfismo	biyectiva
Endomorfismo	de V en V
Automorfismo	endomorfismo biyectivo

5.2 Núcleo e imagen

Definición 5.2 .

$$\operatorname{Nuc} f = \{v \in V : f(v) = 0\}, \qquad \operatorname{Im} f = \{f(v) : v \in V\}$$

El primero es subespacio de V y el segundo de W.

Proposición 5.2 . f es inyectiva si y solo si $\operatorname{Nuc} f = \{0\}$.

Teorema 5.1 (De la dimensión). Si $\dim V = n$, entonces

$$\dim \operatorname{Nuc} f + \dim \operatorname{Im} f = n$$

El teorema de la dimensión es el resultado central del bloque, y es el mismo hecho que Rouché-Frobenius visto desde otro lado: $\dim \operatorname{Im} f$ es el rango de la matriz, y $\dim \operatorname{Nuc} f$ el número de parámetros libres del sistema homogéneo.

De él salen tres consecuencias inmediatas para un endomorfismo de V:

Si	Entonces
es inyectivo	es sobreyectivo, y por tanto biyectivo
es sobreyectivo	es inyectivo
$\dim V \neq \dim W$	no puede ser isomorfismo

La primera es falsa en dimensión infinita, y ese contraste conviene tenerlo presente: en $K[x]$, multiplicar por x es inyectivo y no sobreyectivo.

5.3 Matriz asociada

Fijadas bases B de V y B' de W, la matriz $M(f)$ tiene por columnas las coordenadas de $f(e_i)$ respecto de B'. Entonces

$$\mathbf{y}_{B'} = M(f)\,\mathbf{x}_B$$

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & W \\ {\scriptstyle \text{coord. } B}\downarrow & & \downarrow{\scriptstyle \text{coord. } B'} \\ K^n & \xrightarrow[\quad M(f) \quad]{} & K^m \end{array}$$

Operación	Traducción matricial
Composición $g \circ f$	$M(g)\,M(f)$
Aplicación inversa	$M(f)^{-1}$
$\dim \operatorname{Im} f$	$\operatorname{rg} M(f)$
$\dim \operatorname{Nuc} f$	$n - \operatorname{rg} M(f)$

El producto de matrices se define como se define para que la primera fila sea cierta. No es una convención arbitraria: es la composición de aplicaciones escrita en coordenadas.

5.3.1 Cambio de base

Si P y Q son las matrices de cambio de base en V y en W:

$$M'(f) = Q^{-1}M(f)P$$

Y para un endomorfismo, con la misma base a los dos lados:

$$M'(f) = P^{-1}M(f)P$$

Definición 5.3 (Matrices semejantes). A y B son semejantes si existe P invertible con $B = P^{-1}AP$. Dos matrices son semejantes si y solo si representan al mismo endomorfismo en bases distintas.

La semejanza conserva rango, traza, determinante y polinomio característico. Esas cantidades son propiedades **del endomorfismo**, no de la base elegida, y por eso sirven como invariantes.

5.4 Diagonalización

El problema: dado un endomorfismo, encontrar una base en la que su matriz sea diagonal. Si se logra, casi todo se simplifica.

Definición 5.4 (Autovalor y autovector). $\lambda \in K$ es autovalor de f si existe $v \neq 0$ con $f(v) = \lambda v$. Ese v es un autovector asociado.

Geométricamente: **un autovector es una dirección que la aplicación no cambia**, solo escala.

5.4.1 Cálculo

Los autovalores son las raíces del polinomio característico:

$$p(\lambda) = \det(A - \lambda I)$$

y para cada uno, el subespacio propio es $V_\lambda = \mathrm{Nuc}(A - \lambda I)$.

Multiplicidad	Qué es
Algebraica, $m_a(\lambda)$	multiplicidad como raíz de $p(\lambda)$
Geométrica, $m_g(\lambda)$	$\dim V_\lambda$

Proposición 5.3 . $1 \leq m_g(\lambda) \leq m_a(\lambda)$ para todo autovalor.

Teorema 5.2 (Criterio de diagonalización). A de orden n es diagonalizable si y solo si su polinomio característico tiene todas sus raíces en K y, para cada autovalor, $m_g(\lambda) = m_a(\lambda)$.

Corolario 5.1 . Si A tiene n autovalores distintos, es diagonalizable.

El corolario es suficiente y no necesario: la identidad tiene un solo autovalor y es diagonal.

El procedimiento completo:

1. Calcular $p(\lambda) = \det(A - \lambda I)$ y sus raíces.

2. Comprobar que todas están en K.
3. Para cada λ, resolver $(A - \lambda I)\mathbf{x} = \mathbf{0}$ y hallar $m_g(\lambda)$.
4. Si $m_g = m_a$ para todos, juntar las bases de los subespacios propios: esa es la base P.
5. Entonces $D = P^{-1}AP$ es diagonal con los autovalores.

Ejemplo 5.1 . $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ tiene $p(\lambda) = (2-\lambda)^2$, así que $\lambda = 2$ con $m_a = 2$. Pero $A - 2I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ tiene rango 1, luego $m_g = 1 < 2$: **no es diagonalizable**. Su forma canónica es la de Jordan, con un 1 sobre la diagonal.

Nota 5.1 . El cuerpo importa. $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, la rotación de 90 grados, tiene $p(\lambda) = \lambda^2 + 1$: no es diagonalizable sobre $\mathbb{R}$ y sí sobre $\mathbb{C}$. Es coherente con la interpretación geométrica, porque una rotación no deja ninguna dirección real invariante.

5.4.2 Para qué sirve

Aplicación	Cómo
Potencias	$A^k = PD^kP^{-1}$, y D^k es elevar la diagonal
Sucesiones recurrentes	se escriben como $\mathbf{x}_{k+1} = A\mathbf{x}_k$
Sistemas de ecuaciones diferenciales	se desacoplan en la base de autovectores
Comportamiento a largo plazo	lo gobierna el autovalor de mayor módulo
Cadenas de Markov	el autovector del autovalor 1 es la distribución estacionaria

Ejemplo 5.2 . La sucesión de Fibonacci se escribe

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$$

Los autovalores son $\varphi = (1 + \sqrt{5})/2$ y $\psi = (1 - \sqrt{5})/2$, y diagonalizando sale la fórmula cerrada

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

Como $|\psi| < 1$, el segundo término se desvanece: el cociente F_{n+1}/F_n tiende a φ, y esa es la razón áurea.

Ese ejemplo resume el bloque: un problema que no parecía de álgebra lineal se resuelve escribiéndolo como una matriz y mirando sus autovalores.

5.5 Ejercicios

Ejercicio 5.5.1. Sea $f : \mathbb{R}^3 \to \mathbb{R}^2$ con $f(x, y, z) = (x + y,\ y - z)$. Hallar el núcleo, la imagen y comprobar el teorema de la dimensión.

Solución 5.5.1. La matriz es $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$, de rango 2, así que $\dim \operatorname{Im} f = 2$ y la imagen es todo $\mathbb{R}^2$: f es sobreyectiva. El núcleo resuelve $x + y = 0$, $y - z = 0$, de donde $(x, y, z) = t(-1, 1, 1)$: dimensión 1. En efecto, $1 + 2 = 3 = \dim \mathbb{R}^3$.

Ejercicio 5.5.2. Estudiar si $A = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$ es diagonalizable, y compararla con $B = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$.

Solución 5.5.2. Las dos tienen $p(\lambda) = (3 - \lambda)^2$ y el mismo autovalor con $m_a = 2$. En B, $B - 3I$ es la matriz nula, con rango 0, así que $m_g = 2$ y es diagonalizable —ya lo está—. En A, $A - 3I$ tiene rango 1 y $m_g = 1 < 2$: no lo es. Mismo polinomio característico y comportamiento opuesto, lo que muestra que el polinomio no basta para decidir.

Ejercicio 5.5.3. Si A es diagonalizable con autovalores 1 y -1, ¿qué se puede decir de A^2?

Solución 5.5.3. $A = PDP^{-1}$ con D diagonal de unos y menos unos, así que $A^2 = PD^2P^{-1} = PIP^{-1} = I$. La matriz es una involución, y geométricamente es una simetría respecto del subespacio propio del 1.

El desarrollo de las aplicaciones lineales y de la diagonalización está en Merino y Santos, 2021 y Strang, 2007, y sus problemas en Rojo y Martín, 2005 y de Burgos, 1989.

Capítulo 6

Seminario: conjuntos, aplicaciones y relaciones

El seminario que la guía sitúa en las primeras horas de los grupos reducidos. Es el lenguaje con el que está escrito todo lo demás.

6.1 Conjuntos

Operación	Definición
Unión	$A \cup B = \{x : x \in A \text{ o } x \in B\}$
Intersección	$A \cap B = \{x : x \in A \text{ y } x \in B\}$
Diferencia	$A \setminus B = \{x \in A : x \notin B\}$
Complementario	$A^c = U \setminus A$
Producto cartesiano	$A \times B = \{(a, b)\}$
Partes	$\mathcal{P}(A)$, todos los subconjuntos

Propiedad	Expresión
Conmutativa	$A \cup B = B \cup A$
Asociativa	$(A \cup B) \cup C = A \cup (B \cup C)$
Distributiva	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgan	$(A \cup B)^c = A^c \cap B^c$
Doble complementario	$(A^c)^c = A$

Las leyes son las mismas del álgebra de Boole, con $\cup$ por OR, $\cap$ por AND y el complementario por NOT. **No es una analogía**: el conjunto de partes con esas operaciones es un álgebra de Boole.

Cardinales que conviene recordar:

$$|\mathcal{P}(A)| = 2^{|A|}, \qquad |A \times B| = |A| \cdot |B|$$

El primero es el principio del producto: cada elemento entra o no entra.

6.2 Aplicaciones

Definición 6.1 (Aplicación). $f : A \to B$ asigna a cada elemento de A exactamente uno de B.

Tipo	Condición	Consecuencia sobre cardinales
Inyectiva	$f(a) = f(a') \Rightarrow a = a'$	$\lvert A\rvert \leq \lvert B\rvert$
Sobreyectiva	$\operatorname{Im} f = B$	$\lvert A\rvert \geq \lvert B\rvert$
Biyectiva	las dos	$\lvert A\rvert = \lvert B\rvert$

La columna de la derecha, para conjuntos finitos, es exactamente el principio del palomar: **no hay aplicación inyectiva de un conjunto en otro más pequeño**.

Y para conjuntos finitos del mismo tamaño, inyectiva, sobreyectiva y biyectiva son equivalentes. Es el mismo fenómeno que en los endomorfismos de un espacio de dimensión finita, y **falla igualmente en el caso infinito**: $n \mapsto n+1$ es inyectiva de $\mathbb{N}$ en $\mathbb{N}$ y no sobreyectiva.

Concepto	Definición
Composición	$(g \circ f)(a) = g(f(a))$
Imagen directa	$f(S) = \{f(s) : s \in S\}$
Imagen inversa	$f^{-1}(T) = \{a : f(a) \in T\}$
Inversa	existe si y solo si f es biyectiva

Nota 6.1 . $f^{-1}(T)$ se escribe igual que la aplicación inversa y **no la presupone**: la imagen inversa de un conjunto está definida para cualquier aplicación, sea o no biyectiva. Confundir las dos notaciones es el tropiezo habitual del seminario.

6.3 Relaciones binarias

Una relación en A es un subconjunto $R \subseteq A \times A$.

Propiedad	Definición
Reflexiva	aRa para todo a
Simétrica	$aRb \Rightarrow bRa$
Antisimétrica	aRb y $bRa \Rightarrow a = b$
Transitiva	aRb y $bRc \Rightarrow aRc$

Tipo de relación	Propiedades
De equivalencia	reflexiva, simétrica y transitiva
De orden	reflexiva, antisimétrica y transitiva

6.3.1 Relaciones de equivalencia

Definición 6.2 (Clase de equivalencia). $[a] = \{x \in A : xRa\}$. El conjunto de todas las clases es el conjunto cociente A/R.

Teorema 6.1 . Las clases de equivalencia de una relación forman una partición de A: son no vacías, disjuntas dos a dos y su unión es A. Recíprocamente, toda partición define una relación de equivalencia.

La correspondencia entre relaciones de equivalencia y particiones es biunívoca, y es el resultado que hace útil el concepto: clasificar es lo mismo que relacionar.

Ejemplo 6.1 . La congruencia módulo n es de equivalencia, y su conjunto cociente es $\mathbb{Z}_n$, con n clases. Toda la aritmética modular del bloque 1 es esta construcción.

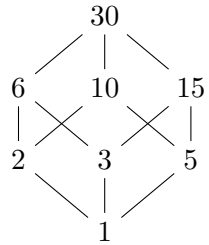
Al definir operaciones sobre el cociente hay que comprobar que **están bien definidas**: que el resultado no depende del representante elegido. Es el paso que parece burocrático y que falla en cuanto uno se descuida.

6.3.2 Relaciones de orden

Concepto	Definición
Orden total	dos elementos cualesquiera son comparables
Orden parcial	hay elementos incomparables
Elemento maximal	ninguno es mayor que él
Máximo	mayor que todos; si existe, es único
Cota superior de S	mayor o igual que todo elemento de S
Supremo	menor de las cotas superiores

Maximal y máximo no son lo mismo, y la diferencia solo se ve en órdenes parciales. En la divisibilidad sobre $\{2, 3, 4, 9\}$ hay dos maximales, 4 y 9, y ningún máximo.

Un orden parcial se representa con el **diagrama de Hasse**: se dibujan los elementos por niveles y se unen solo los pares consecutivos, sin los enlaces que la reflexividad y la transitividad ya implican.



divisores de 30, ordenados por divisibilidad

En ese diagrama, 30 es el máximo y 1 el mínimo; 2, 3 y 5 son incomparables entre sí. Es un orden parcial, y la estructura completa es un retículo, porque todo par tiene supremo —el mínimo común múltiplo— e ínfimo —el máximo común divisor—.

6.4 Ejercicios

Ejercicio 6.4.1. Demostrar que $(A \cup B)^c = A^c \cap B^c$.

Solución 6.4.1. Doble inclusión. Si $x \in (A \cup B)^c$, entonces $x \notin A \cup B$, luego $x \notin A$ y $x \notin B$, es decir $x \in A^c \cap B^c$. Todos los pasos son reversibles, así que la otra inclusión sale leyendo el argumento al revés y los dos conjuntos coinciden.

Ejercicio 6.4.2. En $\mathbb{Z}$, ¿es de equivalencia la relación $aRb \iff a - b$ es par? ¿Cuántas clases tiene?

Solución 6.4.2. Sí. Reflexiva porque $a - a = 0$ es par; simétrica porque si $a - b$ es par también lo es $b - a$; transitiva porque la suma de dos pares es par. Tiene dos clases, la de los pares y la de los impares, y el conjunto cociente es $\mathbb{Z}_2$.

Ejercicio 6.4.3. En el conjunto $\{1, 2, 3, 4, 6, 12\}$ con la divisibilidad, indicar máximo, mínimo y elementos maximales.

Solución 6.4.3. El 12 es máximo, porque todos lo dividen, y en consecuencia es el único maximal. El 1 es mínimo. Si se quita el 12 del conjunto, quedan dos maximales —4 y 6— y ningún máximo, que es la situación que distingue los dos conceptos.

El material del seminario está en Grimaldi, 1998 y Lipschutz, 1991.

Capítulo 7

Relación de problemas

El temario práctico de la guía es la resolución de problemas en los grupos reducidos. Esta relación recorre los cinco bloques, con la solución completa.

7.1 Aritmética entera y modular

Ejercicio 7.1.1. Calcular $\mathrm{mcd}(2024, 748)$ y expresarlo como combinación entera de los dos números.

Solución 7.1.1. Euclides: $2024 = 2\cdot 748 + 528$; $748 = 1\cdot 528 + 220$; $528 = 2\cdot 220 + 88$; $220 = 2\cdot 88 + 44$; $88 = 2\cdot 44 + 0$. El máximo común divisor es 44.

Hacia atrás: $44 = 220 - 2\cdot 88 = 220 - 2(528 - 2\cdot 220) = 5\cdot 220 - 2\cdot 528 = 5(748 - 528) - 2\cdot 528 = 5\cdot 748 - 7\cdot 528 = 5\cdot 748 - 7(2024 - 2\cdot 748) = 19\cdot 748 - 7\cdot 2024$.

Comprobación: $19\cdot 748 = 14\,212$ y $7\cdot 2024 = 14\,168$, cuya diferencia es 44.

Ejercicio 7.1.2. Hallar el resto de dividir 3^{2024} entre 11.

Solución 7.1.2. 11 es primo y no divide a 3, así que por Fermat $3^{10} \equiv 1 \pmod{11}$. Como $2024 = 202\cdot 10 + 4$, se tiene $3^{2024} \equiv 3^4 = 81 = 7\cdot 11 + 4 \equiv 4$. El resto es 4.

Ejercicio 7.1.3. Resolver el sistema $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 9$, $x \equiv 3 \pmod{25}$.

Solución 7.1.3. Los módulos son primos entre sí, así que hay solución única módulo $4\cdot 9\cdot 25 = 900$. De la primera, $x = 1 + 4k$. Sustituyendo en la segunda: $1 + 4k \equiv 2 \pmod 9$, o sea $4k \equiv 1$; el inverso de 4 módulo 9 es 7, luego $k \equiv 7 \pmod 9$ y $x = 29 + 36m$. En la tercera: $29 + 36m \equiv 3 \pmod{25}$, es decir $11m \equiv -1 \equiv 24$; el inverso de 11 módulo 25 es 16, así que $m \equiv 16\cdot 24 = 384 \equiv 9 \pmod{25}$. Por tanto $x = 29 + 36\cdot 9 = 353$, y la solución general es $353 + 900t$.

Ejercicio 7.1.4. Comprobar que $x^3 + x + 1$ es irreducible sobre $\mathbb{Z}_2$ y decir cuántos elementos tiene el cuerpo que genera.

Solución 7.1.4. Un polinomio de grado 3 es reducible sobre un cuerpo si y solo si tiene alguna raíz. Aquí $p(0) = 1$ y $p(1) = 1 + 1 + 1 = 1$ en $\mathbb{Z}_2$, así que no tiene raíces y es irreducible. El cociente $\mathbb{Z}_2[x]/(p)$ es un cuerpo con $2^3 = 8$ elementos.

7.2 Combinatoria

Ejercicio 7.2.1. ¿Cuántos números de cinco cifras tienen todas sus cifras distintas y son pares?

Solución 7.2.1. Conviene empezar por las restricciones. Si la última cifra es 0, las cuatro primeras se eligen entre las nueve restantes ordenadamente: $9 \cdot 8 \cdot 7 \cdot 6 = 3024$. Si la última es 2, 4, 6 u 8 —cuatro opciones—, la primera no puede ser 0 ni repetir, así que hay 8 opciones, y las tres del medio $8 \cdot 7 \cdot 6$: $4 \cdot 8 \cdot 8 \cdot 7 \cdot 6 = 10\,752$. En total 13 776.

Ejercicio 7.2.2. De un grupo de 12 personas se elige un comité de 5. ¿De cuántas formas, si dos personas concretas se niegan a coincidir?

Solución 7.2.2. Por el complementario: el total es $\binom{12}{5} = 792$, y los comités que contienen a las dos son $\binom{10}{3} = 120$, porque las otras tres se eligen libremente. La respuesta es $792 - 120 = 672$.

Ejercicio 7.2.3. Demostrar que en cualquier conjunto de 6 personas hay 3 que se conocen mutuamente o 3 que son mutuamente desconocidas.

Solución 7.2.3. Se fija una persona A. Tiene 5 relaciones, de dos tipos, así que por el palomar al menos 3 son del mismo tipo; sea el de «conoce», con B, C y D. Si dos de esos tres se conocen entre sí, junto con A forman el trío que se conoce. Si ninguno de los tres pares se conoce, entonces B, C y D son mutuamente desconocidos. En los dos casos existe el trío buscado.

7.3 Matrices y sistemas

Ejercicio 7.3.1. Discutir y resolver según a:

$$\begin{cases} ax + y + z = 1 \\ x + ay + z = a \\ x + y + az = a^2 \end{cases}$$

Solución 7.3.1. $\det A = (a-1)^2(a+2)$.

Si $a \neq 1$ y $a \neq -2$: compatible determinado.

Si $a = 1$: las tres ecuaciones son $x + y + z = 1$, así que $\operatorname{rg} A = \operatorname{rg} A^* = 1$, compatible indeterminado con dos parámetros.

Si $a = -2$: $\operatorname{rg} A = 2$, y al escalonar la ampliada aparece una fila $(0\ 0\ 0 \mid 3)$, así que $\operatorname{rg} A^* = 3$ y el sistema es incompatible.

Ejercicio 7.3.2. Calcular la inversa de $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{pmatrix}$ por Gauss-Jordan.

Solución 7.3.2. Se reduce $(A \mid I)$. El resultado es

$$A^{-1} = \begin{pmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{pmatrix}$$

La comprobación obligatoria es $AA^{-1} = I$: la primera fila de A por la primera columna de A^{-1} da $-24 + 40 - 15 = 1$, y por la segunda, $18 - 30 + 12 = 0$.

Ejercicio 7.3.3. Demostrar que si A es antisimétrica de orden impar, entonces $\det A = 0$.

Solución 7.3.3. $A^T = -A$, así que $\det A = \det A^T = \det(-A) = (-1)^n \det A$. Con n impar queda $\det A = -\det A$, es decir $2\det A = 0$, y por tanto $\det A = 0$ en cualquier cuerpo de característica distinta de 2.

7.4 Espacios vectoriales

Ejercicio 7.4.1. En $\mathbb{R}^4$, sean $U = \langle (1,0,1,0), (0,1,0,1)\rangle$ y $W = \{(x,y,z,t) : x+y=0,\ z=t\}$. Hallar $\dim(U \cap W)$ y $\dim(U+W)$.

Solución 7.4.1. W está dado por dos ecuaciones independientes, así que $\dim W = 4-2 = 2$. Un vector de U es $a(1,0,1,0) + b(0,1,0,1) = (a,b,a,b)$; imponerle las ecuaciones de W da $a+b=0$ y $a=b$, de donde $a=b=0$. Luego $U \cap W = \{0\}$ y su dimensión es 0. Por Grassmann, $\dim(U+W) = 2+2-0 = 4$: la suma es directa y llena $\mathbb{R}^4$.

Ejercicio 7.4.2. Hallar las ecuaciones implícitas de $U = \langle (1,1,0), (0,1,1)\rangle$ en $\mathbb{R}^3$.

Solución 7.4.2. Un vector (x,y,z) está en U si es combinación de los dos generadores, es decir si el determinante de la matriz 3×3 que forman los tres se anula:

$$\begin{vmatrix} x & y & z \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix} = x - y + z = 0$$

Una sola ecuación, coherente con $\dim U = 2 = 3-1$.

7.5 Aplicaciones lineales y diagonalización

Ejercicio 7.5.1. Diagonalizar $A = \begin{pmatrix} 4 & -2 \\ 1 & 1 \end{pmatrix}$.

Solución 7.5.1. $p(\lambda) = (4-\lambda)(1-\lambda)+2 = \lambda^2 - 5\lambda + 6$, con raíces 2 y 3, distintas: es diagonalizable.

Para $\lambda = 2$: $(A-2I)\mathbf{x} = 0$ da $2x - 2y = 0$, es decir $v_1 = (1,1)$. Para $\lambda = 3$: $x - 2y = 0$, es decir $v_2 = (2,1)$.

Con $P = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ se tiene $P^{-1}AP = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

Ejercicio 7.5.2. Sea $f : \mathbb{R}^3 \to \mathbb{R}^3$ con matriz $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{pmatrix}$. Hallar núcleo e imagen, y decir si es diagonalizable.

Solución 7.5.2. Las tres filas son proporcionales, así que $\operatorname{rg} A = 1$: la imagen tiene dimensión 1 y está generada por $(1,2,3)$, y el núcleo tiene dimensión 2, dado por $x + 2y + 3z = 0$.

El polinomio característico es $-\lambda^2(\lambda - 14)$, con $\lambda = 0$ de multiplicidad algebraica 2 y $\lambda = 14$ simple.

La multiplicidad geométrica del 0 es $\dim \operatorname{Nuc} A = 2$, que coincide, y la del 14 es 1. Por tanto **sí es diagonalizable**, semejante a $\operatorname{diag}(0, 0, 14)$.

Ejercicio 7.5.3. Si A es diagonalizable y todos sus autovalores tienen módulo menor que 1, ¿qué le ocurre a A^k cuando k crece?

Solución 7.5.3. $A^k = PD^kP^{-1}$, y D^k es la diagonal con los λ_i^k. Como $|\lambda_i| < 1$, cada uno tiende a 0, luego $D^k \to 0$ y por tanto $A^k \to 0$. Es la condición que garantiza la convergencia de los métodos iterativos del tema de sistemas: el radio espectral de la matriz de iteración debe ser menor que 1.

Los problemas siguen el estilo de Rojo y Martín, 2005, de Diego, 1995 y Lipschutz, 1991, con la teoría de Merino y Santos, 2021 y Grimaldi, 1998.

Bibliografía

de Burgos, J. (1989). *Curso de Álgebra y Geometría*. Alhambra Universidad.

de Diego, B. (1995). *Problemas de Álgebra lineal*. Deimos.

Dorronsoro, J., & Hernández, E. (1999). *Números, grupos y anillos*. Addison-Wesley.

Grimaldi, R. P. (1998). *Matemáticas discreta y combinatoria. Una introducción con aplicaciones* (3.ª ed.). Addison Wesley Iberoamericana.

Lipschutz, S. (1991). *Teoría de conjuntos y temas afines*. McGraw-Hill.

Merino, L., & Santos, E. (2021). *Álgebra lineal con métodos elementales* (3.ª ed.). Paraninfo.

Rojo, J., & Martín, I. (2005). *Ejercicios y problemas de Álgebra lineal*. McGraw-Hill.

Strang, G. (2007). *Álgebra lineal y sus aplicaciones* (3.ª ed.). Addison-Wesley Iberoamericana.