

# Álgebra Lineal y Estructuras Matemáticas

J. C. Rosales y P. A. García Sánchez

DEPARTAMENTO DE ÁLGEBRA, UNIVERSIDAD DE GRANADA



## Índice general

Capítulo 1. Conjuntos, relaciones de equivalencia y aplicaciones	4
1. Conjuntos	4
2. Operaciones con conjuntos	4
3. Relaciones de equivalencia	7
4. Aplicaciones entre conjuntos	8
Capítulo 2. Aritmética entera y modular	11
1. Los números enteros	11
2. Ecuaciones diofánticas lineales	14
3. Ecuaciones en congruencias de grado uno	16
4. El anillo de los enteros módulo un entero positivo	17
Capítulo 3. El anillo de los polinomios sobre un cuerpo	19
1. Divisibilidad	19
2. Ecuaciones lineales y en congruencias	22
3. Cuerpos finitos	23
Capítulo 4. Matrices con coeficientes en un cuerpo	26
1. Matrices	26
2. Determinantes	27
Capítulo 5. Espacios vectoriales y aplicaciones lineales	31
1. Espacios y subespacios	31
2. Bases	33
3. Ecuaciones del cambio de base	35
4. Ecuaciones paramétricas de un subespacio vectorial	38
5. Aplicaciones lineales	39
6. Ecuaciones de una aplicación lineal	40
7. Espacio vectorial cociente	43
Capítulo 6. Sistemas de ecuaciones lineales	46
1. Rango de una matriz	46
2. Resolución de sistemas de ecuaciones lineales	47
3. Ecuaciones cartesianas o implícitas de un subespacio vectorial	50
Capítulo 7. Diagonalización de matrices	55
1. Matrices diagonalizables	55
2. Método para diagonalizar una matriz	56
Índice alfabético	59

## Conjuntos, relaciones de equivalencia y aplicaciones

### 1. Conjuntos

La idea de conjunto es una de las más significativas en Matemáticas. La mayor parte de los conceptos matemáticos están contruidos a partir de conjuntos. (Existe una aproximación funcional basada en el  $\lambda$ -cálculo y la Lógica Combinatoria, que hoy en día han tenido una papel fundamental en la programación funcional.)

Podríamos decir que un conjunto es simplemente una colección de objetos a los que llamaremos elementos del conjunto. Esta definición nos bastará para los contenidos de este curso, pero desde el punto de vista matemático es imprecisa y da lugar rápidamente a paradojas. Desde comienzos del siglo XX esta definición dejó de utilizarse por los problemas que acarrea. Por desgracia, dar una definición precisa está bastante lejos de los objetivos de este guión.

- Cuando  $x$  sea un elemento de un conjunto  $A$ , escribiremos  $x \in A$ , que se lee “ $x$  pertenece a  $A$ ”.
- Diremos que un conjunto  $A$  es subconjunto del conjunto  $B$ , y lo denotaremos por  $A \subseteq B$ , si todo elemento de  $A$  pertenece a  $B$ .
- Un conjunto  $A$  es igual que otro conjunto  $B$  si tienen los mismos elementos, a saber, si  $A \subseteq B$  y  $B \subseteq A$ . Cuando esto ocurre, escribiremos  $A = B$ .
- Admitiremos la existencia de un conjunto sin elementos, al que denotemos por  $\emptyset$  y llamaremos conjunto vacío.

### 2. Operaciones con conjuntos

Sean  $A$  y  $B$  conjuntos.

- 1) La intersección de  $A$  y  $B$  es el conjunto formado por los elementos comunes de  $A$  y de  $B$ , y lo denotamos así

$$A \cap B = \{x \text{ tales que } x \in A \text{ y } x \in B\}.$$

- 2) La unión de  $A$  y  $B$  es el conjunto formado al tomar todos los elementos de  $A$  y los de  $B$ .

$$A \cup B = \{x \text{ tales que } x \in A \text{ o } x \in B\}.$$

- 3) La diferencia de  $A$  y  $B$  es el conjunto que tiene por elementos los elementos de  $A$  que no están en  $B$ .

$$A \setminus B = \{x \in A \text{ tales que } x \notin B\}$$

(siempre que tachemos un símbolo, estamos indicando que no se cumple la condición sin tachar; así  $x \notin B$  significa que  $x$  no pertenece a  $B$ ,  $A \neq B$  significa que  $A$  es distinto de  $B$ , etcétera).

- 4)  $\mathcal{P}(A) = \{X \text{ tales que } X \subseteq A\}$  es el conjunto de partes de  $A$  o conjunto potencia de  $A$ .
- 5) El producto cartesiano de  $A$  y  $B$  es el conjunto de parejas cuya primera componente está en  $A$  y la segunda en  $B$ . Esto se escribe de la siguiente forma.

$$A \times B = \{(a, b) \text{ tales que } a \in A \text{ y } b \in B\}.$$

Al conjunto  $A \times \dots \times A$  lo denotaremos por  $A^n$ , para  $n$  un entero positivo.

El cardinal de un conjunto es el número de elementos que contiene. Usaremos  $\#A$  para denotar el cardinal del conjunto  $A$ .

- $\#\mathcal{P}(A) = 2^{\#A}$ .
- $\#(A \times B) = \#A \cdot \#B$ .

**Maxima 1:** Los conjuntos en maxima se pueden definir usando llaves o bien la función `set`.

```
(%i1) {a,a,b,c};
(%o1) {a,b,c}

Definamos un par de conjuntos y veamos cómo se pueden hacer las operaciones hasta ahora
descritas con ellos.

(%i2) A:{1,2,3,4};
(%o2) {1,2,3,4}

(%i3) B:set(3,4,5);
(%o3) {3,4,5}

(%i4) elementp(5,A);
(%o4) false

(%i5) elementp(1,A);
(%o5) true

(%i6) is (A=B);
(%o6) false

(%i7) is (A=A);
(%o7) true

(%i8) setequalp(A,B);
(%o8) false

(%i9) subsetp(A,B);
(%o9) false

(%i10) subsetp(A,union(A,B));
(%o10) true

(%i11) intersection(A,B);
(%o11) {3,4}

(%i12) union(A,B);
(%o12) {1,2,3,4,5}

(%i13) setdifference(A,B);
(%o13) {1,2}

(%i14) powerset(B);
```

```
( %o14)          {}, {3}, {3, 4}, {3, 4, 5}, {3, 5}, {4}, {4, 5}, {5}
```

Nótese que el conjunto vacío se denota por {}.

```
(%i15) is(cardinality(powerset(A))=2^(cardinality(A)));
```

```
( %o15)          true
```

```
(%i16) cartesian_product(A,B);
```

```
( %o16)          {[1, 3], [1, 4], [1, 5], [2, 3], [2, 4], [2, 5], [3, 3], [3, 4], [3, 5], [4, 3], [4, 4], [4, 5]}
```

Podemos además elegir los elementos de A que son impares.

```
(%i17) subset(A,oddp);
```

```
( %o17)          {1, 3}
```

O bien las sumas de los pares del producto cartesiano con A y B.

```
(%i18) makeset(a+b, [a,b], cartesian_product(A,B));
```

```
( %o18)          {4, 5, 6, 7, 8, 9}
```

**Maxima 2:** Pongamos un ejemplo de una función cuyos argumentos sean conjuntos. Podemos definir la diferencia simétrica de dos conjuntos A y B como  $(A \setminus B) \cup (B \setminus A)$ .

```
(%i1) A:{1,2,3,4};
```

```
( %o1)          {1, 2, 3, 4}
```

```
(%i2) B:set(3,4,5);
```

```
( %o2)          {3, 4, 5}
```

```
(%i3) dif_sim(X,Y):=union(setdifference(X,Y),setdifference(Y,X))$
```

Para definir funciones usamos := en vez de :. El “\$” al final de una línea inhibe la salida.

```
(%i4) dif_sim(A,B);
```

```
( %o4)          {1, 2, 5}
```

**Maxima 3:** Podemos definir conjuntos utilizando listas y viceversa, lo cual hace que podamos usar las funciones específicas para listas en conjuntos. Además se pueden definir subconjuntos utilizando funciones booleanas, tal y como vemos a continuación.

```
(%i1) l:makelist(i,i,1,100)$ A:setify(l)$
```

Crea un conjunto con los los enteros del uno al cien.

```
(%i3) B:subset(A,primep);
```

```
( %o3)          {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}
```

Escojo aquellos que son primos.

```
(%i4) C:subset(B,lambda([x],is(x>80)));
```

```
( %o4)          {83, 89, 97}
```

De entre ellos me quedo con los mayores de 80, que equivale a hacer lo siguiente (ahorrándome la definición de f, usando para ello lambda, que define de forma anónima una función).

(%i5) f(x):=is(x>80)\$

(%i6) D:subset(B,f);

(%o6) {83, 89, 97}

### 3. Relaciones de equivalencia

Sea  $A$  un conjunto. Una relación binaria en  $A$  es un subconjunto  $R$  de  $A \times A$ . Cuando  $(x, y) \in R$  escribimos  $x R y$  y decimos que  $x$  está relacionado (mediante  $R$ ) con  $y$ .

Una relación binaria  $R$  sobre un conjunto  $A$  es una relación de equivalencia si verifica las siguientes propiedades.

- 1) Para todo  $a \in A$ ,  $a R a$  ( $R$  es reflexiva).
- 2) Dados  $a, b \in A$ , si  $a R b$ , entonces  $b R a$  ( $R$  es simétrica).
- 3) Para cualesquiera  $a, b, c \in A$ , si  $a R b$  y  $b R c$ , entonces  $a R c$  ( $R$  es transitiva).

Si  $R$  es una relación de equivalencia sobre un conjunto  $A$ , y  $a$  es un elemento de  $A$ , entonces la clase de  $a$  es el conjunto de todos los elementos de  $A$  que están relacionados con  $a$ ,

$$[a] = \{x \in A \text{ tales que } x R a\}.$$

Se define el conjunto cociente de  $A$  por  $R$  como el conjunto de todas las clases de equivalencia de elementos de  $A$ , y se denota por  $A/R$ . Así

$$\frac{A}{R} = \{[a] \text{ tales que } a \in A\}.$$

**Ejercicio 1:** En el conjunto  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$  de los números enteros, definimos la siguiente relación de equivalencia.

$$x R y \text{ si } x - y \text{ es múltiplo de } 5.$$

- a) Demuestra que  $R$  es una relación de equivalencia.
- b) Calcula  $[2]$ .
- c) Describe el conjunto cociente  $\frac{\mathbb{Z}}{R}$ .
- d) ¿Qué cardinal tiene  $\frac{\mathbb{Z}}{R}$ ?

**Ejercicio 2:** En el conjunto  $\mathcal{P}(\{1, 2, 3\})$ , definimos la siguiente relación binaria.

$$A \sim B \text{ si } \#A = \#B.$$

- a) Demuestra que  $\sim$  es una relación de equivalencia.
- b) Calcula  $[\{1, 2\}]$ .
- c) Describe el conjunto cociente  $\frac{\mathcal{P}(\{1, 2, 3\})}{\sim}$ .
- d) ¿Cuántos elementos tiene dicho conjunto cociente?

Dado un conjunto  $X$ , una partición de  $X$  es una familia de subconjuntos de  $X$ ,  $\{A_i\}_{i \in I}$  ( $= \{A_i \text{ tales que } i \in I\}$ ), de forma que

- 1)  $A_i \neq \emptyset$  para todo  $i \in I$ ,
- 2)  $A_i \cap A_j = \emptyset$  para cualesquiera  $i, j \in I$  con  $i \neq j$ ,
- 3)  $X = \bigcup_{i \in I} A_i$  (la unión de todos los elementos de la familia  $\{A_i\}_{i \in I}$ ).

- Se puede comprobar fácilmente que el hecho de ser  $R$  una relación de equivalencia sobre  $A$  hace que  $A/R$  sea una partición de  $A$ .

**Maxima 4:** Veamos cómo se pueden calcular las clases de equivalencia del conjunto  $A = \{1, \dots, 10\}$  sobre la relación de equivalencia  $x \sim y$  si  $x - y$  es un múltiplo de 3.

Primero definimos el conjunto  $\{1, \dots, 10\}$ . Para ello hacemos una lista con los elementos del uno al diez, y luego la convertimos en conjunto.

```
(%i1) l:makelist(i,i,1,10);
(%o1) [1,2,3,4,5,6,7,8,9,10]
(%i2) s:setify(l);
(%o2) {1,2,3,4,5,6,7,8,9,10}
(%i3) equiv_classes(s,lambda([x,y],is(remainder(x-y,3)=0)));
(%o3) {{1,4,7,10},{2,5,8},{3,6,9}}
También podríamos haber definido R, y luego calculado A/R.
(%i4) R(x,y):=is(remainder(x-y,3)=0);
(%o4) R(x,y) := is(remainder(x-y,3)=0)
(%i5) equiv_classes(A,R);
(%o5) {{1,4,7,10},{2,5,8},{3,6,9}}
```

Se ve que es una partición de  $A$ , pues todos sus elementos son no vacíos, disjuntos dos a dos, y la unión de ellos da  $A$ .

#### 4. Aplicaciones entre conjuntos

Sean  $A$  y  $B$  dos conjuntos. Una aplicación  $f$  de  $A$  en  $B$ , que denotaremos como  $f : A \rightarrow B$ , es una correspondencia que a cada elemento de  $A$  le asocia un único elemento de  $B$  (de nuevo esta definición es algo imprecisa, pero suficiente para nuestro curso). Si  $a \in A$ , al elemento que le asocia  $f$  en  $B$  lo denotamos por  $f(a)$ , y se llama la imagen de  $a$  por  $f$ . Los conjuntos  $A$  y  $B$  son el dominio y codominio de  $f$ , respectivamente. Llamaremos conjunto imagen de  $f$  a

$$\text{Im}(f) = \{f(a) \text{ tales que } a \in A\}.$$

**Ejercicio 3:** Sea  $\mathbb{Q}$  el conjunto de los números racionales y  $\mathbb{R}$  el de los reales. ¿Tiene sentido decir que  $f : \mathbb{Q} \rightarrow \mathbb{R}, x \mapsto \frac{x+1}{x-1}$  es una aplicación?

Si  $f : A \rightarrow B$  es una aplicación, diremos que  $f$  es

- 1) inyectiva si  $f(a) = f(a')$  para  $a, a' \in A$ , implica  $a = a'$ ;
- 2) sobreyectiva si  $\text{Im}(f) = B$  (para todo  $b \in B$ , existe  $a \in A$  tal que  $f(a) = b$ );
- 3) biyectiva si es inyectiva y sobreyectiva.

**Ejercicio 4:** Demuestra que la aplicación  $f : \mathbb{Q} \rightarrow \mathbb{R}$  definida por  $f(x) = \frac{1}{2}(2x+1)$  es inyectiva pero no sobreyectiva.

Sean  $f : A \rightarrow B$  y  $g : B \rightarrow C$  dos aplicaciones. La aplicación composición de  $f$  y  $g$  (también conocida como  $f$  compuesta con  $g$ ) es la aplicación  $g \circ f : A \rightarrow C$ , definida como  $(g \circ f)(a) = g(f(a))$ . Para calcular la imagen de un elemento por la composición primero aplicamos  $f$  y luego  $g$ .

**Ejercicio 5:** Sean  $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto x^2$ , y  $g : \mathbb{Z} \rightarrow \mathbb{Q}, y \mapsto \frac{1}{2}(y+1)$ . Calcula  $g \circ f$ .

- La composición de aplicaciones es asociativa ( $f \circ (g \circ h) = (f \circ g) \circ h$ ) pero no es conmutativa ( $f \circ g$  no tiene por qué ser igual a  $g \circ f$ ).



**Maxima 5:** Veamos como las funciones cuadrado y sumar uno no conmutan al componerlas.

```
(%i1) f(x):=x^2$ g(x):=x+1$
```

```
(%i2) f(g(1)); g(f(1));
```

```
(%o2) 4
```

```
(%o3) 2
```

```
(%i4) f(g(x))=g(f(x));
```

```
(%o4) (x + 1)^2 = x^2 + 1
```

```
(%i5) expand(%);
```

```
(%o5) x^2 + 2x + 1 = x^2 + 1
```

Sea  $A$  un conjunto. La aplicación identidad en  $A$  es la aplicación  $1_A : A \rightarrow A$  definida como  $1_A(a) = a$  para todo  $a \in A$ .

Dada una aplicación  $f : A \rightarrow B$ , decimos que es

- 1) invertible por la izquierda si existe  $g : B \rightarrow A$  tal que  $g \circ f = 1_A$ ;
- 2) invertible por la derecha si existe  $g : B \rightarrow A$  de forma que  $f \circ g = 1_B$ ;
- 3) invertible si es invertible a izquierda y a derecha.

- Una aplicación es invertible por la izquierda si y sólo si es inyectiva.
- Una aplicación es invertible por la derecha si y sólo si es sobreyectiva.
- Por tanto, una aplicación es invertible si y sólo si es biyectiva.

**Ejercicio 6:** Sea  $\mathbb{N}$  el conjunto de enteros no negativos. Demuestra que la aplicación  $f : \mathbb{N} \rightarrow \mathbb{N}$ , definida por  $f(x) = x^2$  es invertible por la izquierda, pero no por la derecha.

Una aplicación biyectiva  $f$  tiene una única inversa que lo es por la derecha y por la izquierda. Dicha aplicación diremos que es la inversa de  $f$  y lo denotaremos por  $f^{-1}$ .

**Ejercicio 7:** Demuestra que la aplicación  $f : \mathbb{Q} \rightarrow \mathbb{Q}$ ,  $f(x) = \frac{1}{3}(2x + 1)$  es biyectiva. Calcula  $f^{-1}$ .

**Maxima 6:** Veamos que la inversa de la función  $f(x) = x+1$  (suponemos que el dominio y codominio son los números enteros) es  $g(x) = x - 1$ .

```
(%i1) f(x):=x+1$ g(x):=x-1$
```

```
(%i3) f(g(x)); g(f(x));
```

```
(%o3) x
```

```
(%o4) x
```

**Maxima 7:** Consideremos ahora la aplicación  $f : \{0, 1, \dots, 7\} \rightarrow \{0, 1, \dots, 7\}$ , que dado un elemento  $x$  de  $\{0, 1, \dots, 7\}$ , devuelve el resto de dividir por 8 la cantidad  $x^2 + 1$ .

```
(%i1) s:setify(makelist(i,i,0,7));
```

```
(%o1) {0, 1, 2, 3, 4, 5, 6, 7}
```

```
(%i2) f(x):=remainder(x^2+1,8)$
```

Calculemos el conjunto imagen de  $f$ .

```
(%i3) makelist(f(x),x,0,7);
(%o3) [1,2,5,2,1,2,5,2]
```

```
(%i4) setify(%);
(%o4) {1,2,5}
```

Por lo que esta aplicación no es sobreyectiva (por ejemplo, el 0 no está en la imagen).

Veamos ahora quién es la preimagen del 1. Para ello calculamos todos los elementos que se aplican en él por  $f$ .

```
(%i5) subset(s,lambda([x],is(f(x)=1)));
(%o5) {0,4}
```

Esto nos dice que  $f(0) = f(4) = 1$ , por lo que  $f$  tampoco es inyectiva.

Por último, para cualquier aplicación  $f : X \rightarrow Y$  podemos definir  $R_f$ , que es una relación de equivalencia en  $X$ , de la siguiente forma

$$x R_f y \text{ si } f(x) = f(y).$$

Veamos el conjunto de clases de equivalencia en nuestro ejemplo bajo esta relación.

```
(%i6) equiv_classes(s,lambda([x,y],is(f(x)=f(y))));
(%o6) {{0,4},{1,3,5,7},{2,6}}
```

## Aritmética entera y modular

### 1. Los números enteros

Dado un entero  $z$ ,  $-z$  es su opuesto, y denotamos por  $|z| = \max\{z, -z\}$  al valor absoluto de  $z$ .

**Propiedades de la suma.** La suma de enteros es

- asociativa,
- tiene elemento neutro (el cero sumado a cualquier elemento da de nuevo ese elemento),
- todo elemento tiene inverso (si sumamos un entero con su opuesto obtenemos el cero),
- conmutativa,
- cancelativa ( $a + b = a + c$  implica  $b = c$ ; esto es consecuencia inmediata de la existencia de elemento inverso).

El conjunto de los números enteros con la suma es por tanto un grupo abeliano.

**Propiedades del producto.** El producto de números enteros es

- conmutativo,
- asociativo,
- tiene elemento neutro (el uno),
- es cancelativo para elementos no nulos,
- distributivo ( $a(b + c) = ab + ac$ , que nos permite además sacar factor común).

Así el conjunto de los números enteros es un anillo conmutativo.

**Propiedad de la división.** Dados  $a, b \in \mathbb{Z}$ , con  $b \neq 0$ , existen  $q, r \in \mathbb{Z}$  únicos de forma que  $a = qb + r$  y  $0 \leq r < |b|$ .

A  $q$  y  $r$  los llamaremos cociente y resto de dividir  $a$  entre  $b$ , y los denotaremos por  $a \operatorname{div} b$  y  $a \operatorname{mód} b$ , respectivamente.

Dados  $a$  y  $b$  enteros, decimos que  $a$  divide a  $b$ , o que  $b$  es un múltiplo de  $a$ , si existe  $c \in \mathbb{Z}$  tal que  $b = ac$ . Usaremos  $a \mid b$  para denotar que  $a$  divide a  $b$ .

**Ejercicio 8:** Sean  $a, b, c \in \mathbb{Z}$ . Demuestra que si  $c \mid a$  y  $c \mid b$ , entonces para todo  $x, y \in \mathbb{Z}$ ,  $c \mid xa + yb$ .

Sea  $p \in \mathbb{Z} \setminus \{-1, 1\}$  ( $-1$  y  $1$  son los únicos enteros que tiene inverso para el producto). Decimos que  $p$  es irreducible si los únicos enteros que dividen a  $p$  son  $1, -1, p$  y  $-p$ . El entero  $p$  es primo si siempre que  $p \mid ab$ , para  $a$  y  $b$  enteros, se tiene que  $p \mid a$  o  $p \mid b$ .

- Un entero es primo si y sólo si es irreducible.

Decimos que dos enteros son primos relativos si los únicos enteros que dividen a ambos son  $1$  y  $-1$ . (Nótese que  $1$  y  $-1$  dividen a cualquier número entero.)

**Teorema de Bézout.** Sean  $a, b \in \mathbb{Z}$ . Entonces  $a$  y  $b$  son primos relativos si y sólo si existen  $u, v \in \mathbb{Z}$  tales que  $au + bv = 1$ .

**Teorema fundamental de la aritmética.** Todo número entero mayor que uno se puede expresar de forma única (salvo reordenaciones) como producto de números primos positivos.

**Ejercicio 9:** Calcula todos los divisores enteros positivos de 120.

Sean  $a, b \in \mathbb{Z}$ , con  $a \neq 0$  o  $b \neq 0$ . Un entero  $d$  es un máximo común divisor de  $a$  y  $b$  si

- 1)  $d \mid a$  y  $d \mid b$ ,
- 2) si  $c \mid a$  y  $c \mid b$ , con  $c$  un entero, entonces  $c \mid d$ .

Análogamente, un entero  $m$  es un mínimo común múltiplo de  $a$  y  $b$  si

- 1)  $a \mid m$  y  $b \mid m$ ,
- 2) si  $a \mid c$  y  $b \mid c$ , con  $c$  un entero, entonces  $m \mid c$ .

De forma similar se puede definir el máximo común divisor y el mínimo común múltiplo de un conjunto de enteros  $\{a_1, \dots, a_n\}$  con  $n$  un entero positivo.

- Si  $d$  es un máximo común divisor de  $a$  y  $b$ , también lo es  $-d$ , y éstos son los únicos máximos divisores comunes de  $a$  y  $b$ . Lo mismo ocurre con el mínimo común múltiplo. Esto se debe a que si  $a \mid b$ , entonces  $-a \mid b$ . Cuando escribamos  $\gcd\{a, b\}$  nos referiremos al máximo común divisor positivo de  $a$  y  $b$ . Para el mínimo común múltiplo utilizaremos  $\text{lcm}(a, b)$ .
- Sean  $a = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  y  $b = v p_1^{\beta_1} \cdots p_r^{\beta_r}$ , con  $u, v \in \{1, -1\}$ ,  $p_1, \dots, p_r$  primos distintos y  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$  enteros no negativos (algunos pueden ser cero, pues los primos que aparecen en  $a$  no tienen por qué aparecer en  $b$ ). Entonces

$$\gcd\{a, b\} = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}},$$

$$\text{lcm}\{a, b\} = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}.$$

- $\gcd\{a, b\} \text{lcm}\{a, b\} = |ab|$ .

**Algoritmo de Euclides.**

**Entrada:**  $a, b$  enteros positivos.

**Salida:**  $\gcd\{a, b\}$ .

$$(a_0, a_1) := (a, b).$$

Mientras  $a_1 \neq 0$

$$(a_0, a_1) := (a_1, a_0 \bmod a_1).$$

Devuelve  $a_0$ .

**Ejercicio 10:** Calcula el máximo común divisor de 237 y 99.

**Maxima 8:** Veamos algunos ejemplos de cálculo con maxima.

**(%i1)** `primep(38129);`

**(%o1)** `false`

**(%i2)** `next_prime(38129);`

**(%o2)** `38149`

**(%i3)** `prev_prime(38129);`

**(%o3)** `38119`

**(%i4)** `factor(38129);`

**(%o4)** `7 13 419`

```
(%i5) 7*13*419;
(%o5) 38129
(%i6) gcd(15,18);
(%o6) 3
(%i7) quotient(101,34);
(%o7) 2
(%i8) remainder(101,34);
(%o8) 33
(%i9) 2*34+33;
(%o9) 101
```

Hay que tener cuidado con estas funciones, pues el resto no se define como nosotros lo hemos hecho.

```
(%i10) quotient(-150,17);remainder(-150,17);
(%o10) -8
(%o11) -14
```

Si queremos un resto y cociente acordes a nuestra definición de división podemos hacer lo siguiente.

```
(%i12) cociente(a,b):=(a-mod(a,b))/b;
(%o12) cociente(a,b) :=  $\frac{a - \text{mod}(a,b)}{b}$ 
(%i13) cociente(-150,17);mod(-150,17);
(%o13) -9
(%o14) 3
(%i15) is(-8*17+-14=-9*17+3);
(%o15) true
```

**Maxima 9:** Una alternativa a `factor` es el comando `ifactor`, que devuelve una lista con pares de la forma (primo,exponente) para cada uno de los primos que aparecen en la factorización de un entero.

```
(%i1) ifactors(12);
(%o1) [[2, 2], [3, 1]]
```

Un entero es libre de cuadrados si no es divisible por un cuadrado (distinto de 1), o lo que es lo mismo, en su factorización los exponentes de todos los primos que aparecen son uno.

```
(%i2) libre_cuadradosp(x):=every(lambda([x],is(x[2]=1)),ifactors(x))$
(%i3) libre_cuadradosp(12);
(%o3) false
```

```
(%i4) libre_cuadradosp(2*3*5*7);
(%o4) true

(%i5) sublist(makelist(i,i,1,100),libre_cuadradosp);
(%o5) [1,2,3,5,6,7,10,11,13,14,15,17,19,21,22,23,26,29,30,31,33,34,35,37,38,39,41,
42,43,46,47,51,53,55,57,58,59,61,62,65,66,67,69,70,71,73,74,77,78,79,82,83,85,86,
87,89,91,93,94,95,97]
```

**Maxima 10:** Un entero positivo es perfecto si es suma de sus divisores propios.

```
(%i1) divisors(10);
(%o1) {1,2,5,10}

(%i2) perfectop(x):=is(2*x=apply("+",listify(divisors(x))))$
(%i3) perfectop(28);
(%o3) true

(%i4) sublist(makelist(i,i,1,500),perfectop);
(%o4) [6,28,496]
```

## 2. Ecuaciones diofánticas lineales

Una ecuación diofántica lineal es una expresión de la forma  $a_1x_1 + \dots + a_nx_n = b$ , con  $a_1, \dots, a_n, b \in \mathbb{Z}$ . Una solución a dicha ecuación es una  $n$ -upla  $(c_1, \dots, c_n)$  de elementos enteros de forma que  $a_1c_1 + \dots + a_nc_n = b$ .

**Teorema de Bézout generalizado.** Sea  $\{a_1, \dots, a_n\}$  un conjunto de enteros, y  $d$  su máximo común divisor. Entonces existen  $u_1, \dots, u_n \in \mathbb{Z}$  tales que  $a_1u_1 + \dots + a_nu_n = d$ .

Así la ecuación diofántica  $a_1x_1 + \dots + a_nx_n = b$  tiene solución si y sólo si  $d \mid b$ . Las soluciones de  $a_1x_1 + \dots + a_nx_n = b$  son las mismas que las de la ecuación  $\frac{a_1}{d}x_1 + \dots + \frac{a_n}{d}x_n = \frac{b}{d}$ .

Para  $n = 2$ , tenemos ecuaciones en dos variables. Usamos las incógnitas  $x$  y  $y$  por comodidad. Si  $x_0, y_0$  es una solución particular de  $ax + by = c$ , con  $\gcd\{a, b\} = 1$ , entonces todas las soluciones de esa ecuación son de la forma

$$\begin{cases} x = x_0 + bk, \\ y = y_0 - ak, \end{cases}$$

con  $k \in \mathbb{Z}$ .

### Algoritmo extendido de Euclides.

**Entrada:**  $a, b$  enteros positivos.

**Salida:**  $s, t, d \in \mathbb{Z}$  tales que  $d = \gcd\{a, b\}$  y  $as + bt = d$ .

$$(a_0, a_1) := (a, b).$$

$$(s_0, s_1) := (1, 0).$$

$$(t_0, t_1) := (0, 1).$$

Mientras  $a_1 \neq 0$

$$q := a_0 \operatorname{div} a_1.$$

$$(a_0, a_1) := (a_1, a_0 - a_1q).$$

$$(s_0, s_1) := (s_1, s_0 - s_1q).$$

$$(t_0, t_1) := (t_1, t_0 - t_1q).$$

$$d := a_0, s := s_0, t := t_0.$$

Devuelve  $s, t, d$ .

**Maxima 11:** Resolvamos la ecuación  $40x + 15y = 30$ . Usando `gcdex` obtenemos lo siguiente.

(%i1) `gcdex(40,15);`

(%o1)  $[-1, 3, 5]$

Lo que significa que  $40 \times (-1) + 15 \times 3 = 5$ . Como 5 divide a 30, la ecuación tiene solución. Multiplicamos por 6 ( $6 \times 5 = 30$ ) y obtenemos lo siguiente.

(%i2) `%*6;`

(%o2)  $[-6, 18, 30]$

Que equivale a multiplicar la igualdad  $40 \times (-1) + 15 \times 3 = 5$  por 6. Por tanto, una solución de nuestra ecuación  $30 \times (-6) + 15 \times 18 = 30$ .

Nótese que la ecuación  $40x + 15y = 30$  es equivalente a  $8x + 3y = 6$  (hemos dividido por el máximo común divisor de 40 y 15). Si  $x_0, y_0$  es una solución de dicha ecuación,  $x = x_0 + 3k$  e  $y = y_0 - 8k$  es una solución de  $8x + 3y = 6$  para todo  $k \in \mathbb{Z}$ .

(%i3) `gcdex(8,3);`

(%o3)  $[-1, 3, 1]$

(%i4) `%*6;`

(%o4)  $[-6, 18, 6]$

Así todas las soluciones de  $40x + 15y = 30$  son

$$\begin{cases} x = -6 + 3k, \\ y = 18 - 8k. \end{cases}$$

**Maxima 12:** Resolvamos ahora la ecuación  $121x - 77y = 88$ .

(%i1) `gcd(121,-77);`

(%o1)  $11$

Al dividir por 11, la ecuación queda reducida a  $11x - 7y = 8$ .

(%i2) `1:gcdex(11,-7);`

(%o2)  $[2, 3, 1]$

(%i3) `8*1;`

(%o3)  $[16, 24, 8]$

Por lo que tenemos que una solución particular es  $x_0 = 16$  e  $y_0 = 24$ . Siendo además todas las soluciones de la forma  $x = x_0 - 7k$ ,  $y = y_0 - 11k$  con  $k$  un entero cualquiera.

### 3. Ecuaciones en congruencias de grado uno

Sean  $a, b, m \in \mathbb{Z}$ . Escribimos  $a \equiv b \pmod{m}$ , que se lee “ $a$  es congruente con  $b$  módulo  $m$ ”, para indicar que  $m \mid a - b$ .

Una ecuación en congruencias de grado uno (o lineal) es una expresión de la forma  $ax \equiv b \pmod{m}$ . Una solución para dicha ecuación es un entero  $c$  de forma que  $ac \equiv b \pmod{m}$ . Nótese que las soluciones de  $ax \equiv b \pmod{m}$  son las posibles  $x$  de la ecuación diofántica  $ax + my = b$ .

- La ecuación  $ax \equiv b \pmod{m}$  tiene solución si y sólo si  $\gcd\{a, m\} \mid b$ .
- Si  $d = \gcd\{a, m\}$  y  $d \mid b$ , entonces las ecuaciones  $ax \equiv b \pmod{m}$  y  $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$  tienen las mismas soluciones.
- Si  $\gcd\{a, m\} = 1$ , y  $x_0$  es una solución de  $ax \equiv b \pmod{m}$ , entonces el conjunto de todas las soluciones de la ecuación es  $\{x_0 + km \text{ tales que } k \in \mathbb{Z}\}$ .
- La ecuación  $ax + c \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $ax \equiv b - c \pmod{m}$ .
- La ecuación  $ax \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $(a \pmod{m})x \equiv (b \pmod{m}) \pmod{m}$ .
- Si  $au + mv = 1$ , con  $u, v \in \mathbb{Z}$ , entonces  $bu$  es una solución de  $ax \equiv b \pmod{m}$ .

**Maxima 13:** Veamos si tiene solución la ecuación  $54x \equiv 6 \pmod{34}$ , y en caso de tener, vamos a describir su conjunto de soluciones.

```
(%i1) remainder(54,34);
```

```
(%o1) 20
```

Al ser  $54 \pmod{34}$  igual a  $20$ , la ecuación anterior es equivalente a  $20x \equiv 6 \pmod{34}$ .

```
(%i2) gcd(20,34);
```

```
(%o2) 2
```

Como  $2 \mid 6$ , la ecuación tiene solución, y es equivalente a  $10x \equiv 3 \pmod{17}$ . Usando `gcdex` obtenemos los coeficientes de Bézout para  $10$  y  $17$ .

```
(%i2) gcdex(10,17);
```

```
(%o2) [-5, 3, 1]
```

Lo que viene a decir que  $(-5) \times 10 + 3 \times 17 = 1$ . Así una solución de  $10x \equiv 3 \pmod{17}$  es  $(-5)3$ , que vale  $-15$ . Así todas las soluciones de nuestra ecuación son de la forma  $-15 + 17k$  con  $k \in \mathbb{Z}$ .

**Ejercicio 11:** Encuentra todas las soluciones enteras de

$$121x \equiv 2 \pmod{196}.$$

**Teorema chino de los restos.** Sean  $a_1, \dots, a_k$  enteros y  $m_1, \dots, m_k$  enteros positivos primos relativos dos a dos. Entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

tiene una única solución módulo  $m_1 m_2 \cdots m_k$ .



**Maxima 14:** Vamos a resolver el sistema

$$\begin{cases} x \equiv 5495 & (\text{mód } 7643) \\ x \equiv 7569 & (\text{mód } 8765) \end{cases}$$

Por la primera ecuación, sabemos que  $x$  es de la forma  $x = 5495 + 7643k$  con  $k$  un entero cualquiera. Substituímos en la segunda y  $k$  se convierte en la nueva incógnita:  $5495 + 7643k \equiv 7569 \pmod{8765}$ . Como

**(%i1)** `7569-5495;`

**(%o1)** `2074`

tenemos que resolver  $7643k \equiv 2074 \pmod{8765}$ . El inverso de  $7643$  módulo  $8765$  lo calculamos (de existir) con el algoritmo extendido de Euclides.

**(%i2)** `gcdex(7643,8765);`

**(%o2)** `[2617, -2282, 1]`

Despejamos

**(%i3)** `mod(2617*2074,8765);`

**(%o3)** `2123`

y obtenemos que  $k = 2123 + 8765t$  para cualquier entero  $t$ . Substituyendo  $k$  en la expresión de  $x$ , llegamos a  $x = 5495 + 7643(2123 + 8765t)$ .

**(%i4)** `expand(5495+7643*(2123+8765*t));`

**(%o4)** `66990895 t + 16231584`

Por lo que  $x = 66990895t + 16231584$  para todo  $t \in \mathbb{Z}$  es una solución del sistema de congruencias. Lo podemos comprobar como sigue.

**(%i6)** `mod(16231584, [7643,8765]);`

**(%o6)** `[5495, 7569]`

**Ejercicio 12:** Resuelve los siguientes sistemas de congruencias.

$$\begin{cases} 2x \equiv 3 \pmod{5} \\ 3x \equiv 1 \pmod{4} \end{cases} \quad \begin{cases} 2x \equiv 2 \pmod{4} \\ 6x \equiv 3 \pmod{9} \\ 2x \equiv 3 \pmod{5} \end{cases}$$

$$\begin{cases} 2x \equiv 2 \pmod{4} \\ 3x \equiv 6 \pmod{12} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2} \\ 3x \equiv 2 \pmod{6} \\ 5x \equiv 1 \pmod{7} \end{cases}$$

#### 4. El anillo de los enteros módulo un entero positivo

Dado un entero positivo  $m$ , denotamos por  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$  (que es el conjunto de restos posibles de la división por  $m$ ), y por eso este conjunto se conoce a veces como el conjunto de los enteros módulo  $m$ .

En  $\mathbb{Z}_m$  definimos una suma y un producto de la siguiente forma. Dados  $a, b \in \mathbb{Z}_m$ ,

- $a \oplus b = (a + b) \pmod{m}$ ,
- $a \otimes b = (ab) \pmod{m}$ .

**Propiedades de la suma.** Conmutativa, asociativa, elemento neutro y elemento inverso.

**Propiedades del productora.** Conmutativa, asociativa, elemento neutro y distributiva.

- Un elemento  $a \in \mathbb{Z}_m$  tiene inverso para el producto si y sólo si  $\gcd\{a, m\} = 1$ . Si  $au + mv = 1$ , entonces  $u \pmod m$  es el inverso de  $a$  en  $\mathbb{Z}_m$ .

**Ejercicio 13:** Calcula el inverso para el producto de 121 en  $\mathbb{Z}_{196}$ .

**Ejercicio 14:** Calcula el resto de dividir  $4225^{1000}$  entre 7.

**Ejercicio 15:** Prueba que dado un número entero  $m$  o bien se verifica que  $m^2 \equiv 0 \pmod 8$ , o  $m^2 \equiv 1 \pmod 8$ , o  $m^2 \equiv 4 \pmod 8$ .

**Maxima 15:** Escribamos una función para calcular  $\mathbb{Z}_m$ , para  $m$  un entero positivo.

```
(%i1) Z(m):=setify(makelist(i,i,0,m-1));
(%o1) Z(m) := setify (makelist (i, i, 0, m - 1))
(%i2) Z(10);
(%o2) {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
(%i3) tieneinverso(x,m):=is(gcd(x,m)=1);
(%o3) tieneinverso (x, m) := is (gcd (x, m) = 1)
```

El inverso lo podemos calcular con la función `inv_mod`.

```
(%i4) inv_mod(3,10);
(%o4) 7
(%i5) inv_mod(2,10);
(%o5) false
(%i6) subset(Z(12),lambda([x],tieneinverso(x,12)));
(%o6) 1, 5, 7, 11
```

Como 11 es primo, todo elemento no nulo de  $\mathbb{Z}_{11}$  tiene inverso:

```
(%i7) every(lambda([x],tieneinverso(x,11)),disjoin(0,Z(11)));
(%o7) true
```

Por último, resolvamos la ecuación  $137x \equiv 26 \pmod{155}$ , que es equivalente a resolver la ecuación  $137x = 26$  en  $\mathbb{Z}_{155}$ .

```
(%i9) inv_mod(137,155);
(%o9) 43
(%i10) mod(43*26,155);
(%o10) 33
```

## El anillo de los polinomios sobre un cuerpo

### 1. Divisibilidad

Un anillo es una terna  $(\mathbf{R}, +, \cdot)$ , donde  $\mathbf{R}$  es un conjunto, y  $+$  y  $\cdot$  son dos operaciones verificando:

- 1) la operación  $+$  es asociativa, conmutativa, tiene elemento neutro, y todo elemento tiene inverso (lo que hace de  $(\mathbf{R}, +)$  un grupo abeliano),
- 2) la operación  $\cdot$  es asociativa, tiene elemento neutro, y verifica la propiedad distributiva.

Diremos que el anillo  $\mathbf{R}$  es conmutativo si además  $\cdot$  cumple la propiedad conmutativa.

Un cuerpo es un anillo conmutativo en el que todo elemento distinto de cero (el elemento neutro de  $+$ ) tiene inverso para  $\cdot$ .

**Ejercicio 16:** Da algunos ejemplos de cuerpos.

Sea  $\mathbf{K}$  un cuerpo. El conjunto de polinomios con coeficientes en  $\mathbf{K}$  en la indeterminada  $x$  es

$$\mathbf{K}[x] = \{\mathbf{a}_0 + \mathbf{a}_1x + \cdots + \mathbf{a}_nx^n \text{ tales que } n \in \mathbb{N}, \mathbf{a}_0, \dots, \mathbf{a}_n \in \mathbf{K}\}.$$

- $\mathbf{K}[x]$  es un anillo conmutativo con las operaciones usuales de suma y producto de polinomios.

Dado  $\mathbf{a}(x) = \mathbf{a}_0 + \mathbf{a}_1x + \cdots + \mathbf{a}_nx^n \in \mathbf{K}[x]$ , con  $\mathbf{a}_n \neq 0$ , decimos que  $n$  es el grado de  $\mathbf{a}(x)$ , y lo notaremos por  $\text{gr}(\mathbf{a}(x))$  ( $\text{gr}(0) = -\infty$ ). A  $\mathbf{a}_n$  se le llama coeficiente líder de  $\mathbf{a}(x)$ , y a  $\mathbf{a}_nx^n$  término líder de  $\mathbf{a}(x)$ .

Un elemento  $\mathbf{a}$  de un anillo conmutativo  $\mathbf{R}$  es una unidad si existe  $\mathbf{b} \in \mathbf{R}$  de forma que  $\mathbf{a} \cdot \mathbf{b} = \mathbf{1}$  (donde  $\mathbf{1}$  es el elemento neutro de  $\cdot$ ).

- El conjunto de las unidades de  $\mathbf{K}[x]$  es  $\mathbf{K} \setminus \{0\}$ .

Sean  $\mathbf{a}(x), \mathbf{b}(x) \in \mathbf{K}[x]$ . Decimos que  $\mathbf{a}(x)$  divide a  $\mathbf{b}(x)$ , y lo denotamos por  $\mathbf{a}(x) \mid \mathbf{b}(x)$ , si existe  $\mathbf{c}(x) \in \mathbf{K}[x]$  tal que  $\mathbf{b}(x) = \mathbf{a}(x)\mathbf{c}(x)$ .

Un elemento  $\mathbf{a}(x) \in \mathbf{K}[x]$  es irreducible si

- 1)  $\mathbf{a}(x) \neq 0$ ,
- 2)  $\mathbf{a}(x)$  no es una unidad de  $\mathbf{K}[x]$  (no es un polinomio constante),
- 3) si  $\mathbf{a}(x) = \mathbf{b}(x)\mathbf{c}(x)$ , con  $\mathbf{b}(x), \mathbf{c}(x) \in \mathbf{K}[x]$ , entonces  $\mathbf{b}(x)$  o  $\mathbf{c}(x)$  es una unidad de  $\mathbf{K}[x]$ .

**Ejercicio 17:** Estudia la irreducibilidad de  $x^2 + x \in \mathbb{Z}_3[x]$  y de  $x^3 + x + 1 \in \mathbb{Z}_2[x]$ .

**Ejercicio 18:** Demuestra que en  $\mathbf{K}[x]$  todo polinomio de grado uno es irreducible.

Un polinomio  $\mathbf{a}(x) \in \mathbf{K}[x]$  es mónico si el coeficiente del término de mayor grado vale 1.

**Teorema de factorización única de polinomios.** Todo polinomio  $a(x) \in K[x] \setminus K$  se puede expresar de forma única (salvo reordenación de los factores) como  $a(x) = u p_1(x)^{\alpha_1} \cdots p_r(x)^{\alpha_r}$ , donde  $u \in K \setminus \{0\}$ ,  $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$  y  $p_1(x), \dots, p_r(x)$  son polinomios mónicos e irreducibles de  $K[x]$ .

A esa expresión la llamaremos la descomposición en irreducibles de  $a(x)$ .

Sean  $a(x), b(x) \in K[x]$ , con  $a(x) \neq 0$  o  $b(x) \neq 0$ . Un polinomio  $d(x)$  es un máximo común divisor de  $a(x)$  y  $b(x)$  si

- 1)  $d(x) \mid a(x)$  y  $d(x) \mid b(x)$ ,
- 2) si  $c(x) \mid a(x)$  y  $c(x) \mid b(x)$ , con  $c(x)$  otro polinomio, entonces  $c(x) \mid d(x)$ .

Análogamente, un polinomio  $m(x)$  es un mínimo común múltiplo de  $a(x)$  y  $b(x)$  si

- 1)  $a(x) \mid m(x)$  y  $b(x) \mid m(x)$ ,
- 2) si  $a(x) \mid c(x)$  y  $b(x) \mid c(x)$ , con  $c(x)$  otro polinomio, entonces  $m(x) \mid c(x)$ .

De forma similar se puede definir el máximo común divisor y el mínimo común múltiplo de un conjunto de polinomios  $\{a_1(x), \dots, a_n(x)\}$  con  $n$  un entero positivo.

- Si  $d(x)$  es un máximo común divisor de  $a(x)$  y  $b(x)$ , también lo es  $kd(x)$  para todo  $k \in K \setminus \{0\}$ , y éstos son los únicos máximos divisores comunes de  $a(x)$  y  $b(x)$ . Lo mismo ocurre con el mínimo común múltiplo. Esto se debe a que si  $a(x) \mid b(x)$ , entonces  $ka(x) \mid b(x)$  para cualquier  $k \in K \setminus \{0\}$ . Cuando escribamos  $\gcd\{a(x), b(x)\}$  nos referiremos al máximo común divisor de  $a(x)$  y  $b(x)$  que sea mónico. Para el mínimo común múltiplo utilizaremos  $\text{lcm}\{a(x), b(x)\}$ .
- Sean  $a(x) = u p_1(x)^{\alpha_1} \cdots p_r(x)^{\alpha_r}$  y  $b(x) = v p_1(x)^{\beta_1} \cdots p_r(x)^{\beta_r}$ , con  $u, v \in K \setminus \{0\}$ ,  $p_1(x), \dots, p_r(x)$  polinomios mónicos e irreducibles, y  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$  enteros no negativos (algunos pueden ser cero, pues los factores que aparecen en  $a(x)$  no tienen por qué aparecer en  $b(x)$ ). Entonces

$$\gcd\{a(x), b(x)\} = p_1(x)^{\min\{\alpha_1, \beta_1\}} \cdots p_r(x)^{\min\{\alpha_r, \beta_r\}},$$

$$\text{lcm}\{a(x), b(x)\} = p_1(x)^{\max\{\alpha_1, \beta_1\}} \cdots p_r(x)^{\max\{\alpha_r, \beta_r\}}.$$

- $\gcd\{a, b\} \text{lcm}\{a, b\} = uab$ , con  $u \in K[x] \setminus \{0\}$ .

**Ejercicio 19:** Calcula el máximo común divisor y el mínimo común múltiplo en  $\mathbb{Z}_5[x]$  de  $(x+1)(2x+3)$  y  $(x+2)(4x+1)$ .

**Propiedad de la división.** Dados  $a(x), b(x) \in K[x]$ , con  $b(x) \neq 0$ , existen  $q(x), r(x) \in K[x]$  únicos de forma que  $a(x) = q(x)b(x) + r(x)$  y  $\text{gr}(r(x)) < \text{gr}(b(x))$ .

A  $q(x)$  y  $r(x)$  los llamaremos respectivamente cociente y resto de dividir  $a(x)$  entre  $b(x)$ , y los denotaremos por  $a(x) \text{ div } b(x)$  y  $a(x) \text{ mód } b(x)$ .

**Ejercicio 20:** Calcula el cociente y el resto de dividir  $3x^3 + 4x^2 + 2x + 3$  entre  $2x^2 + x + 2$  en  $\mathbb{Z}_5[x]$ .

### Algoritmo de Euclides para polinomios.

**Entrada:**  $a(x), b(x) \in K[x] \setminus \{0\}$ .

**Salida:**  $\gcd\{a(x), b(x)\}$ .

$$(a_0(x), a_1(x)) := (a(x), b(x)).$$

Mientras  $a_1(x) \neq 0$

$$(a_0(x), a_1(x)) := (a_1(x), a_0(x) \text{ mód } a_1(x)).$$

Devuelve  $a_0(x)$  multiplicado por el inverso de su coeficiente líder.

**Ejercicio 21:** Calcula el máximo común divisor de los polinomios  $x^4 + x + 1$  y  $x^2 + 2x + 3$  en  $\mathbb{Z}_5[x]$ .

Sea  $a(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ . Un elemento  $\alpha \in K[x]$  es una raíz de  $a(x)$  si  $a(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ .

**Teorema del factor.** Sea  $a(x) \in K[x]$  y  $\alpha \in K$ . Entonces  $\alpha$  es una raíz de  $a(x)$  si y sólo si  $x - \alpha \mid a(x)$ .

- Un polinomio  $a(x)$  es un múltiplo de un polinomio de grado uno si y sólo si  $a(x)$  tiene una raíz en  $K$ .

**Ejercicio 22:** Calcula todos los polinomios irreducibles de grado 2 de  $\mathbb{Z}_3[x]$ .

**Ejercicio 23:** Determina la reducibilidad o irreducibilidad de los siguientes polinomios en  $\mathbb{Z}_3[x]$ :  $x^4 + x + 2$ ,  $x^3 + x + 1$ ,  $x^2 + 1$ ,  $x^4 + x^2 + 2$ .

**Teorema del resto.** Sea  $a(x) \in K[x]$  y  $\alpha \in K$ . Entonces  $a(x) \bmod (x - \alpha) = a(\alpha)$ .

**Ejercicio 24:** Calcula en  $\mathbb{Z}_5[x]$  el resto de dividir  $x^{1000} + 1$  entre  $x + 3$ .

Si  $\alpha$  es una raíz de  $a(x) \in K[x]$ , entonces aplicando reiteradamente el teorema del factor, tenemos que  $a(x) = (x - \alpha)^m b(x)$ , con  $m \in \mathbb{N} \setminus \{0\}$  y  $b(\alpha) \neq 0$ . El número natural  $m$  es la multiplicidad de la raíz  $\alpha$  en  $a(x)$ . Si  $m = 1$ , decimos que  $\alpha$  es una raíz simple. Si  $m \geq 2$ , entonces es una raíz múltiple.

**Ejercicio 25:** Calcula las raíces (y sus multiplicidades) del polinomio  $x^3 + 2x + 3 \in \mathbb{Z}_5[x]$ .

- Si  $a(x) \in K[x] \setminus \{0\}$ , entonces la suma de las multiplicidades de las raíces de  $a(x)$  es menor o igual que  $\text{gr}(a(x))$ .

**Caracterización de las raíces múltiples.** Si  $\alpha$  es una raíz de  $a(x) \in K[x]$ . Entonces  $\alpha$  es una raíz múltiple si y sólo si  $\alpha$  es también raíz de  $a'(x)$ , la derivada de  $a(x)$ .

**Ejercicio 26:** Demuestra que el polinomio  $x^{70} - 1 \in \mathbb{R}[x]$  no tiene raíces múltiples.

**Maxima 16:**

`maxima` no factoriza en polinomios mónicos. El comando `factor` muestra una descomposición en irreducibles.

`(%i1) factor(3*x^3-2*x+1);`

`(%o1) (x + 1) (3x^2 - 3x + 1)`

`(%i2) gcd(3*x^3+3,x^2-1);`

`(%o2) x + 1`

`(%i3) (x-1)^2*(x+1);`

`(%o3) (x - 1)^2 (x + 1)`

`(%i4) expand(%);`

`(%o4) x^3 - x^2 - x + 1`

`(%i5) gcd(%,diff(%,x));`

`(%o5) x - 1`

`(%i6) quotient(x^3+1,x-3);`

(%o6)  $x^2 + 3x + 9$

(%i7) remainder(x^3+1,x-3);

(%o7) 28

(%i8) expand((x^2+3\*x+9)\*(x-3)+28);

(%o8)  $x^3 + 1$

**Maxima 17:** Calculemos las raíces y sus multiplicidades del polinomio  $x^6 + 3x^5 + 6x^3 + 2x^2 + 6x + 3$  con coeficientes en  $\mathbb{Z}_7$ .

(%i1) modulus:7\$

(%i2) p:x^6+3\*x^5+6\*x^3+2\*x^2+6\*x+3\$

(%i3) gcd(p,diff(p,x));

(%o3)  $x^3 + 2x^2 + x + 3$

(%i4) factor(%);

(%o4)  $(x - 2)^2 (x - 1)$

(%i5) factor(p);

(%o5)  $(x - 3) (x - 2)^3 (x - 1)^2$

## 2. Ecuaciones lineales y en congruencias

**Teorema** ( $K[x]$  es un dominio de ideales principales). Dados  $a_1(x), \dots, a_n(x) \in K[x]$ , sea  $d(x) = \gcd\{a_1(x), \dots, a_n(x)\}$ . Existen  $u_1(x), \dots, u_n(x) \in K[x]$  tales que

$$a_1(x)u_1(x) + \dots + a_n(x)u_n(x) = d(x).$$

Así, la ecuación

$$a_1(x)X_1 + \dots + a_n(x)X_n = b(x)$$

tiene solución en  $K[x]$  si y sólo si  $d(x) \mid b(x)$ .

**Ejercicio 27:** ¿Tiene la ecuación  $(x^2 + 2)X_1 + (x^2 + 2x + 1)X_2 + (x^2 + x)X_3 = x + 2$  solución en  $\mathbb{Z}_3[x]$ ?

### Algoritmo extendido de Euclides.

**Entrada:**  $a(x), b(x) \in K[x] \setminus \{0\}$ .

**Salida:**  $s(x), t(x), d(x) \in K[x]$  tales que  $d(x) = \gcd\{a(x), b(x)\}$  y  $a(x)s(x) + b(x)t(x) = d(x)$ .

$$(a_0(x), a_1(x)) := (a(x), b(x)).$$

$$(s_0(x), s_1(x)) := (1, 0).$$

$$(t_0(x), t_1(x)) := (0, 1).$$

Mientras  $a_1(x) \neq 0$

$$q(x) := a_0(x) \operatorname{div} a_1(x).$$

$$(a_0(x), a_1(x)) := (a_1(x), a_0(x) - a_1(x)q(x)).$$

$$(s_0(x), s_1(x)) := (s_1(x), s_0(x) - s_1(x)q(x)).$$

$$(t_0(x), t_1(x)) := (t_1(x), t_0(x) - t_1(x)q(x)).$$

$$d(x) := a_0(x), s(x) := s_0(x), t(x) := t_0(x).$$

Devuelve  $s(x), t(x), d(x)$ .

**Maxima 18:** Veamos si tiene solución la ecuación

$$(6x^3 + 6)X + (4x^2 - 4)Y = x^2 + 2x + 1$$

en el anillo de polinomios con coeficientes racionales y con incógnita  $x$ .

(%i1) `gcdex(6*x^3+6,4*x^2-4);`

(%o1)  $[1, -\frac{3x}{2}, 6x + 6]$

Como no nos ha devuelto un máximo común divisor mónico, dividimos por su coeficiente líder.

(%i2) `%/6;`

(%o2)  $[\frac{1}{6}, -\frac{x}{4}, x + 1]$

(%i3) `%(x+1);`

(%o3)  $[\frac{x+1}{6}, -\frac{x^2+x}{4}, x^2 + 2x + 1]$

(%i4) `%[1]*(6*x^3+6)+%[2]*(4*x^2-4);`

(%o4)  $x^2 + 2x + 1$

Así  $X = \frac{x+1}{6}$ ,  $Y = -\frac{x^2+x}{4}$  es una solución a nuestra ecuación.

### 3. Cuerpos finitos

Sea  $m(x) \in K[x] \setminus \{0\}$ . Denotamos por

$$K[x]_{m(x)} = \{a(x) \in K[x] \text{ tales que } \text{gr}(a(x)) < \text{gr}(m(x))\},$$

que es el conjunto de los restos posibles de dividir por  $m(x)$ . Este conjunto es un anillo con las siguientes operaciones.

$$a(x) \oplus b(x) := (a(x) + b(x)) \text{ mód } m(x),$$

$$a(x) \otimes b(x) := (a(x)b(x)) \text{ mód } m(x).$$

- $a(x)$  es una unidad de  $K[x]_{m(x)}$  si y sólo si  $\text{gcd}\{a(x), m(x)\} = 1$ . Por tanto  $K[x]_{m(x)}$  es un cuerpo si y sólo si  $m(x)$  es irreducible.
- $\mathbb{Z}_p[x]_{m(x)}$ , con  $p$  un entero primo, tiene cardinal  $p^{\text{gr}(m(x))}$ .
- Si  $a(x)s(x) + m(x)t(x) = 1$ , entonces  $s(x)$  mód  $m(x)$  es el inverso para el producto de  $a(x)$  en  $K[x]_{m(x)}$ .

**Ejercicio 28:** Calcula el inverso para el producto de  $x + 1$  en  $\mathbb{Z}_5[x]_{x^2+x+1}$ .

**Ejercicio 29:** Encuentra un cuerpo con 8 elementos.

**Maxima 19:** En  $\mathbb{Z}_2[x]$ , el conjunto de posibles restos módulo un polinomio de grado dos viene dado por la siguiente lista.

(%i1) `f4: [0, 1, x, x+1];`

(%o1)  $[0, 1, x, x + 1]$

Hagamos la tabla de multiplicar de  $\mathbb{Z}_2[x]_{x^2+1}$ . Al ser  $x^2 + 1 = (x + 1)(x + 1)$  en  $\mathbb{Z}_2[x]$ , lo que obtenemos no es un cuerpo.

(%i2) `genmatrix(lambda([i,j],polymod(remainder(f4[i]*f4[j],x^2+1),2)),4,4);`

$$(\%o2) \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & x & x+1 \\ 0 & x & 1 & x+1 \\ 0 & x+1 & x+1 & 0 \end{pmatrix}$$

Si hacemos las cuentas módulo  $x^2 + x + 1$ , que es irreducible, obtenemos un cuerpo con cuatro elementos.

(%i3) `genmatrix(lambda([i,j],polymod(remainder(f4[i]*f4[j],x^2+x+1),2)),4,4);`

$$(\%o3) \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & x & x+1 \\ 0 & x & x+1 & 1 \\ 0 & x+1 & 1 & x \end{pmatrix}$$

Como se puede ver en la tabla, el inverso de  $x$  es  $x + 1$ .

**Maxima 20:** Resolvamos la congruencia

$$(x + 3)X \equiv x^2 \pmod{x^3 + 1}$$

en  $\mathbb{Z}_5[x]$ .

Primero fijamos el módulo a 5 (maxima representa  $\mathbb{Z}_5$  como  $\{-2, -1, 0, 1, 2\}$ ).

(%i1) `modulus:5;`

$$(\%o1) \quad 5$$

Luego comprobamos si el máximo común divisor de  $x + 3$  y  $x^3 + 1$  divide a  $x^2$ .

(%i2) `gcdex(x+3,x^3+1);`

$$(\%o2) \quad [x^2 + 2x - 1, -1, 1]$$

De esta forma sabemos además que el inverso de  $x + 3$  módulo  $x^3 + 1$  es  $x^2 + 2x - 1$ . Despejamos y tenemos que  $X = (x^2 + 2x - 1)x^2 \pmod{x^3 + 1}$ , que podemos calcular de la siguiente forma.

(%i3) `remainder(%[1]*x^2,x^3+1);`

$$(\%o3) \quad -x^2 - x - 2$$

Finalmente podemos comprobar el resultado obtenido.

(%i4) `remainder(%*(x+3),x^3+1);`

$$(\%o4) \quad x^2$$

Así las soluciones son de la forma  $X = -x^2 - x - 2 + (x^3 + 1)t(x)$ , para cualquier  $t(x) \in \mathbb{Z}_5[x]$ .

**Maxima 21:**

Encontremos ahora el conjunto de soluciones del sistema de ecuaciones

$$\begin{cases} (x + 3)X = x^2 & \pmod{x^3 + 1}, \\ (2x + 1)X = x & \pmod{x^2}. \end{cases}$$

Por el ejercicio anterior, sabemos que de la primera ecuación obtenemos que  $X = -x^2 - x - 2 + (x^3 + 1)t(x) = 4x^2 + 4x + 3 + t(x)(x^3 + 1)$ . Así que substituyendo este valor en la segunda y despejando  $t(x)$ , obtenemos lo siguiente.

(%i1) `modulus:5$`



```
(%i2) remainder(x-(2*x+1)*(4*x^2+4*x+3),x^2);
(%o2) x + 2
```

```
(%i3) remainder((2*x+1)*(x^3+1),x^2);
(%o3) 2x + 1
```

Por tanto  $(2x + 1)t(x) = x + 2$  (mód  $x^2$ ). Calculamos ahora el inverso de  $2x + 1$  módulo  $x^2$  en  $\mathbb{Z}_5[x]$  con el algoritmo extendido de Euclides.

```
(%i4) gcdex(2*x+1,x^2);
(%o4)/R/ [-2x + 1, -1, 1]
```

```
(%i4) gcdex(2*x+1,x^2);
(%o4)/R/ [-2x + 1, -1, 1]
```

De esta forma,  $t(x) = 2x+2+s(x)x^2$  y en consecuencia  $X = 4x^2+4x+3+(2x+2+s(x)x^2)(x^3+1)$ . Como

```
(%i6) expand(4*x^2+4*x+3+(2*x+2)*(x^3+1));
(%o6) 2x^4 + 2x^3 + 4x^2 + 6x + 5
```

```
(%i7) rat(%);
(%o7)/R/ 2x^4 + 2x^3 - x^2 + x
```

Llegamos a que  $X = 2x^4 + 2x^3 + 4x^2 + x + s(x)(x^5 + x^2)$ , para cualquier  $s(x) \in \mathbb{Z}_5[x]$ .

## Matrices con coeficientes en un cuerpo

### 1. Matrices

Sean  $I = \{1, 2, \dots, m\}$  y  $J = \{1, 2, \dots, n\}$ . Una matriz de orden  $m \times n$  sobre un cuerpo  $K$  es una aplicación

$$A : I \times J \rightarrow K, (i, j) \mapsto a_{ij}.$$

Normalmente a la matriz  $A$  la representaremos de la siguiente forma

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

y a veces simplemente escribiremos  $A = (a_{ij})$ , si queda claro dónde varían  $i$  y  $j$ . Diremos que  $A$  es una matriz con  $m$  filas y  $n$  columnas.

Denotaremos por  $\mathcal{M}_{m \times n}(K)$  al conjunto de las matrices de orden  $m \times n$  sobre  $K$ .

- $\mathcal{M}_{m \times n}(K)$  con la suma coordenada a coordenada tiene estructura de grupo abeliano, esto es, la suma es asociativa, tiene elemento neutro, toda matriz tiene inversa y es conmutativa.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

**Ejercicio 30:** Calcula suma de  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix}$  y  $\begin{pmatrix} 2 & 3 & 3 \\ 3 & 0 & 2 \end{pmatrix}$  en  $\mathcal{M}_{2 \times 3}(\mathbb{Z}_5)$ .

Sea  $A = (a_{ij}) \in \mathcal{M}_{m \times n}(K)$  y  $B = (b_{jk}) \in \mathcal{M}_{n \times p}(K)$ . Entonces podemos definir el producto de  $A$  y  $B$  como  $AB = C = (c_{ik}) \in \mathcal{M}_{m \times p}(K)$  con

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}.$$

**Ejercicio 31:** Sean  $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix} \in \mathcal{M}_{2 \times 3}$  y  $B = \begin{pmatrix} 1 & 2 & 1 & 2 \\ 2 & 0 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_{3 \times 4}$ . Calcula  $AB$ .

Una matriz de orden  $n \times n$  diremos que es una matriz cuadrada de orden  $n$ .

- $(\mathcal{M}_{n \times n}(K), +, \cdot)$  es un anillo.

**Ejercicio 32:** Sean  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$  and  $B = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$ . Comprueba que  $AB \neq BA$ .

## 2. Determinantes

Dada  $A = (a_{ij}) \in \mathcal{M}_{n \times n}(\mathbb{K})$ , definimos  $|A|$ , el determinante de  $A$ , recursivamente de la siguiente forma.

- 1) Para  $n = 1$ ,  $|(\mathbf{a}_{11})| = a_{11}$  (el determinante de una matriz de orden  $1 \times 1$  es su único coeficiente).
- 2) Supuesto que sabemos calcular el determinante de matrices de orden  $n - 1$ , dado  $i \in \{1, \dots, n\}$ ,

$$|A| = a_{i1}\alpha_{i1} + \dots + a_{in}\alpha_{in},$$

donde  $\alpha_{ij} = (-1)^{i+j}|A_{ij}|$  se conoce como el adjunto de la entrada  $a_{ij}$ , con  $A_{ij} \in \mathcal{M}_{(n-1) \times (n-1)}(\mathbb{K})$  la matriz que se obtiene al eliminar la fila  $i$ -ésima y la columna  $j$ -ésima de  $A$ . Esta fórmula se conoce como Desarrollo de Laplace por la fila  $i$  del determinante de  $A$ , y el resultado no depende de  $i$ . Es más, también se puede desarrollar por cualquier columna. Dado  $j$  el Desarrollo de Laplace por la columna  $j$  es

$$|A| = a_{1j}\alpha_{1j} + \dots + a_{nj}\alpha_{nj}.$$

Se puede comprobar fácilmente que

$$\begin{aligned} \blacksquare \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} &= a_{11}a_{22} - a_{12}a_{21}. \\ \blacksquare \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{12}a_{21}a_{33}. \end{aligned}$$

**Ejercicio 33:** Calcula el determinante de  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix} \in \mathcal{M}_{3 \times 3}(\mathbb{Z}_7)$ .

**Ejercicio 34:** Calcula el determinante de

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 2 & 0 & 1 & 3 \end{pmatrix} \in \mathcal{M}_{4 \times 4}(\mathbb{Z}_5).$$

Si  $A = (a_{ij}) \in \mathcal{M}_{m \times n}(\mathbb{K})$ , la matriz traspuesta de  $A$  es

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \dots & a_{nm} \end{pmatrix} \in \mathcal{M}_{n \times m}(\mathbb{K}),$$

esto es, la matriz que se obtiene a partir de  $A$  intercambiando filas por columnas.

**Propiedades de los determinantes.** Sea  $A \in \mathcal{M}_{n \times n}(\mathbb{K})$ .

- 1)  $|A| = |A^t|$ .
- 2) Si se intercambian dos filas (o dos columnas) de  $A$  se obtiene una nueva matriz cuyo determinante es  $-|A|$ .
- 3) Si multiplicamos todos los elementos de una fila (o de una columna) de  $A$  por  $\alpha \in \mathbb{K}$ , obtenemos una matriz con determinante  $\alpha|A|$ .
- 4) Si a una fila de  $A$  le sumamos otra fila de  $A$  multiplicada por un elemento de  $\mathbb{K}$ , entonces la nueva matriz tiene el mismo determinante que  $A$  (lo mismo ocurre si hacemos esta operación con columnas).

5) Si  $B \in \mathcal{M}_{n \times n}(\mathbb{K})$ , entonces  $|AB| = |A||B|$ .

**Ejercicio 35:** Calcula el determinante de la matriz

$$\begin{pmatrix} 2 & 3 & 4 & 0 \\ 3 & 1 & 2 & 2 \\ 4 & 3 & 3 & 1 \\ 2 & 3 & 3 & 2 \end{pmatrix} \in \mathcal{M}_{4 \times 4}(\mathbb{Z}_5).$$

El elemento neutro del producto en  $\mathcal{M}_{n \times n}(\mathbb{K})$  es la matriz identidad, que es la matriz que tiene todas sus entradas cero salvo en la diagonal que tiene unos (cero es el elemento neutro de  $\mathbb{K}$  para la suma, y uno el neutro para el producto). A dicha matriz la denotamos por  $I_n$ , o simplemente  $I$  cuando  $n$  queda claro en el contexto.

Una matriz  $A \in \mathcal{M}_{n \times n}(\mathbb{K})$  es regular si tiene inversa para el producto, esto es, si existe  $B$  tal que  $AB = BA = I_n$ . En dicho caso, a la matriz  $B$  se le denota por  $A^{-1}$ .

La matriz adjunta de  $A$  es la matriz formada por los adjuntos de las entradas de  $A$ , a saber,

$$\bar{A} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}.$$

**Teorema.** Sea  $A \in \mathcal{M}_{n \times n}(\mathbb{K})$ . Entonces  $A$  es regular si y sólo si  $|A| \neq 0$ . En ese caso

$$A^{-1} = |A|^{-1} \bar{A}^t.$$

**Ejercicio 36:** Calcula la inversa de

$$\begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix} \in \mathcal{M}_{3 \times 3}(\mathbb{Z}_3).$$

**Maxima 22:** Vamos a ilustrar algunos ejemplos de operaciones con matrices en `maxima`.

`(%i1) A:matrix([x,y],[z,t]);`

`(%o1)`  $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$

`(%i2) B:matrix([a,b],[c,d]);`

`(%o2)`  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Hay que tener cuidado con la operación de producto, pues en `maxima` dicha operación se hace como en con la suma, entrada a entrada. Para efectuar el producto usamos el punto.

`(%i3) A.B;`

`(%o3)`  $\begin{pmatrix} cy + ax & dy + bx \\ az + ct & bz + dt \end{pmatrix}$

`(%i4) A*B;`

$$(\%o4) \quad \begin{pmatrix} ax & by \\ cz & dt \end{pmatrix}$$

Lo mismo ocurre con la exponenciación.

(%i5)  $A^2$ ;

$$(\%o5) \quad \begin{pmatrix} x^2 & y^2 \\ z^2 & t^2 \end{pmatrix}$$

(%i6)  $A^{22}$ ;

$$(\%o6) \quad \begin{pmatrix} yz + x^2 & xy + ty \\ xz + tz & yz + t^2 \end{pmatrix}$$

(%i7) `determinant(A)`;

$$(\%o7) \quad tx - yz$$

(%i8) `determinant(A.B)=determinant(A)*determinant(B)`;

$$(\%o8) \quad (cy + ax)(bz + dt) - (dy + bx)(az + ct) = (ad - bc)(tx - yz)$$

(%i9) `expand(%)`;

$$(\%o9) \quad -adyz + bcyz + adtx - bctx = -adyz + bcyz + adtx - bctx$$

(%i10) `is(%)`;

$$(\%o10) \quad \text{true}$$

(%i11)  $A^{-1}$ ;

$$(\%o11) \quad \begin{pmatrix} -\frac{t}{yz-tx} & \frac{y}{yz-tx} \\ \frac{z}{yz-tx} & -\frac{x}{yz-tx} \end{pmatrix}$$

(%i12) `C:matrix([1,2,3],[4,5,6],[7,8,9])`;

$$(\%o12) \quad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

(%i13) `determinant(C)`;

$$(\%o13) \quad 0$$

Para calcular determinantes a veces es más eficiente usar las operaciones que hemos visto anteriormente. Así efectuando operaciones elementales por filas o columnas (intercambio o suma por un factor de otra) podemos llegar a una matriz triangular superior, esto es, una matriz cuyas entradas por debajo de la diagonal son todas cero. A este proceso se le conoce como eliminación de Gauss-Jordan.

(%i14) `triangularize(C)`;

$$(\%o14) \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

El determinante de una matriz de esta forma es trivial, pues sólo se multiplican los valores de la diagonal.

**Maxima 23:** Trabajemos ahora módulo 5.

```
(%i1) modulus:5$
(%i2) G:matrix([7,20],[16,47])$
(%i3) H:rat(G);
(%o3)/R/  $\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$ 
(%i4) determinant(H);
(%o4)/R/  $-1$ 
(%i5) I:invert(H);
(%o5)/R/  $\begin{pmatrix} -2 & 0 \\ 1 & -2 \end{pmatrix}$ 
(%i6) H.I;
(%o6)/R/  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 
```

## Espacios vectoriales y aplicaciones lineales

### 1. Espacios y subespacios

Sea  $K$  un cuerpo. Diremos que un conjunto  $V$  tiene estructura de espacio vectorial sobre  $K$  si

- 1) en  $V$  hay una operación  $+$  de forma que  $(V, +)$  es un grupo abeliano,
- 2) existe una aplicación  $K \times V \rightarrow V$ ,  $(a, \vec{v}) \mapsto a\vec{v}$  verificando
  - I)  $a(\vec{u} + \vec{v}) = a\vec{u} + a\vec{v}$ ,
  - II)  $(a + b)\vec{u} = a\vec{u} + b\vec{u}$ ,
  - III)  $a(b\vec{u}) = (ab)\vec{u}$ ,
  - IV)  $1\vec{u} = \vec{u}$ .

A los elementos de  $V$  los llamamos vectores y a los de  $K$  escalares. La aplicación descrita arriba se conoce como producto por escalares.

**Ejercicio 37:** Probar que si  $K$  es un cuerpo, entonces para cualesquiera enteros positivos  $n$  y  $m$ ,

- a)  $K^n$ ,
- b)  $\{a(x) \in K[x] \text{ tales que } \text{gr}(a(x)) \leq n\}$ ,
- c)  $\mathcal{M}_{m \times n}(K)$ ,

son espacios vectoriales sobre  $K$ .

**Ejercicio 38:** Encuentra un espacio vectorial de cardinal 81.

#### Propiedades que se deducen de la definición.

- 1)  $0\vec{u} = \vec{0}$  (el elemento neutro de  $+$  en  $V$ ).
- 2)  $a\vec{0} = \vec{0}$ .
- 3) Si  $a\vec{u} = \vec{0}$ , entonces  $a = 0$  o  $\vec{u} = \vec{0}$ .
- 4)  $-(a\vec{u}) = (-a)\vec{u} = a(-\vec{u})$ .
- 5)  $a(\vec{u} - \vec{v}) = a\vec{u} - a\vec{v}$ .
- 6)  $(a - b)\vec{u} = a\vec{u} - b\vec{u}$ .
- 7) Si  $a\vec{u} = a\vec{v}$  y  $a \neq 0$ , entonces  $\vec{u} = \vec{v}$ .
- 8) Si  $a\vec{u} = b\vec{u}$  y  $\vec{u} \neq \vec{0}$ , entonces  $a = b$ .

En adelante  $V$  denotará un espacio vectorial sobre un cuerpo  $K$ .

Un subconjunto  $U$  de  $V$  es un subespacio vectorial de  $V$  si

- 1)  $U \neq \emptyset$ ,
- 2) si  $\vec{u}, \vec{v} \in U$ , entonces  $\vec{u} - \vec{v} \in U$  ( $U$  es un subgrupo de  $(V, +)$ ),
- 3) si  $a \in K$  y  $\vec{u} \in U$ , entonces  $a\vec{u} \in U$ .

Las dos últimas propiedades se pueden substituir por

- 2') si  $\vec{u}, \vec{v} \in U$  y  $a, b \in K$ , entonces  $a\vec{u} + b\vec{v} \in U$  ( $U$  es cerrado para combinaciones lineales de sus elementos).

**Ejercicio 39:** Demuestra que  $\{(x, y, z) \in \mathbb{Q}^3 \text{ tales que } x + y + z = 0\}$  es un subespacio vectorial de  $\mathbb{Q}^3$ .

**Ejercicio 40:** Encuentra todos los elementos de  $\{(x, y) \in \mathbb{Z}_3^2 \text{ tales que } x + y = 0\}$ .

- Un subespacio vectorial de  $V$  es un espacio vectorial sobre  $K$ , con la misma suma y producto por escalares.
- La intersección de subespacios vectoriales de  $V$  es de nuevo un subespacio vectorial de  $V$ .

Sea  $S$  un subconjunto no vacío de  $V$ . El subespacio vectorial de  $V$  generado por  $S$  es la intersección de todos los subespacios vectoriales de  $V$  que contienen a  $S$ . A dicho subespacio lo denotaremos por  $\langle S \rangle$ .

- Si  $S = \{\vec{u}_1, \dots, \vec{u}_n\}$ , entonces

$$\langle S \rangle = \{a_1 \vec{u}_1 + \dots + a_n \vec{u}_n \text{ tales que } a_1, \dots, a_n \in K\}.$$

**Ejercicio 41:** Calcula todos los elementos del subespacio vectorial de  $\mathbb{Z}_3^3$  generado por  $\{(1, 2, 0), (0, 1, 2)\}$ .

Sean  $U_1, \dots, U_n$  subespacios vectoriales de  $V$ . El subespacio vectorial suma de  $U_1, \dots, U_n$  es

$$U_1 + \dots + U_n = \{\vec{u}_1 + \dots + \vec{u}_n \text{ tales que } \vec{u}_1 \in U_1, \dots, \vec{u}_n \in U_n\}.$$

- $U_1 + \dots + U_n = \langle U_1 \cup \dots \cup U_n \rangle$ .
- Si  $U_1 = \langle S_1 \rangle, \dots, U_n = \langle S_n \rangle$ , entonces  $U_1 + \dots + U_n = \langle S_1 \cup \dots \cup S_n \rangle$ .

Sean  $U$  y  $W$  subespacios vectoriales de  $V$ . Decimos que  $V$  es suma directa de  $U$  y  $W$ , y lo denotamos por  $V = U \oplus W$ , si todo vector  $\vec{v} \in V$  se puede expresar de forma única como  $\vec{v} = \vec{u} + \vec{w}$ , con  $\vec{u} \in U$  and  $\vec{w} \in W$ . En dicho caso, diremos que los subespacios vectoriales  $U$  y  $W$  son complementarios.

- $V = U \oplus W$  si, y sólo si,  $V = U + W$  y  $U \cap W = \{\vec{0}\}$ .

**Ejercicio 42:** Sean  $U = \{(x, y) \in \mathbb{R}^2 \text{ tales que } x + y = 0\}$  y  $W = \{(x, y) \in \mathbb{R}^2 \text{ tales que } x - y = 0\}$ . Demuestra que  $\mathbb{R}^2 = U \oplus W$ .

**Maxima 24:**

El conjunto  $K^n$  con  $K$  un cuerpo y  $n$  un entero positivo es un espacio vectorial. Para el caso  $n = 3$ , el producto por escalares está definido así.

```
(%i1) a*[x,y,z];
```

```
(%o1) [a x, a y, a z]
```

Y la suma de vectores se hace componente a componente.

```
(%i2) [x_1,y_2,z_3]+[x_2,y_2,z_2];
```

```
(%o2) [x_2 + x_1, 2y_2, z_3 + z_2]
```

Veamos que el conjunto de vectores de la forma  $(x, y, 0)$ , con  $x, y \in K$ , es un subespacio de  $K^3$ .

```
(%i3) a*[x_1,y_1,0]+b*[x_2,y_2,0];
```

```
(%o3) [b x_2 + a x_1, b y_2 + a y_1, 0]
```

Lo mismo ocurre con los de la forma  $(x, x, x)$ .



```
(%i4) a*[x,x,x]+b*[x,x,x];
```

```
(%o4) [bx + ax, bx + ax, bx + ax]
```

## 2. Bases

Un conjunto de vectores  $S \subseteq V$  es linealmente dependiente si existen  $n$  un entero positivo,  $\{\vec{v}_1, \dots, \vec{v}_n\} \subseteq S$  y  $(a_1, \dots, a_n) \in K^n \setminus \{(0, \dots, 0)\}$  tales que  $a_1 \vec{v}_1 + \dots + a_n \vec{v}_n = \vec{0}$ . En caso contrario, decimos que  $S$  es un conjunto de vectores linealmente independientes.

**Ejercicio 43:** Demuestra que los vectores  $(1, 1, 0), (0, 1, 1), (1, 0, 1) \in \mathbb{R}^3$  son linealmente independientes.

- $S$  es un conjunto de vectores linealmente dependientes si y sólo si existe  $\vec{v} \in S$  tal que  $\vec{v} \in \langle S \setminus \{\vec{v}\} \rangle$ .
- Si  $\vec{0} \in S$ , entonces  $S$  es un conjunto de vectores linealmente dependientes.
- Si  $S$  es un conjunto de vectores linealmente dependientes, entonces para todo  $\vec{v} \in V$ ,  $S \cup \{\vec{v}\}$  también es un conjunto de vectores linealmente dependientes.
- Si  $S$ ,  $\#S \geq 2$ , es un conjunto de vectores linealmente independientes, entonces para todo  $v \in S$   $S \setminus \{\vec{v}\}$  también es un conjunto de vectores linealmente independientes.

**Maxima 25:**

Veamos si  $\{(1, 2), (0, 1)\}$  es un conjunto de vectores linealmente independientes en  $\mathbb{Q}^2$ .

```
(%i1) solve(x*[1,2]+y*[0,1], [x,y]);
```

```
(%o1) [[x = 0, y = 0]]
```

Ahora probamos con  $\{(1, 2, 3), (2, 4, 6)\}$  en  $\mathbb{Q}^3$ , y vemos que son dependientes.

```
(%i2) solve(x*[1,2,3]+y*[2,4,6], [x,y]);
```

```
solve: dependent equations eliminated: (2 3)
```

```
(%o2) [[x = -2 %r6, y = %r1]]
```

Una base de  $V$  es un subconjunto  $S$  de vectores linealmente independientes de  $V$  tal que  $V = \langle S \rangle$ .

- Si  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  es una base de  $V$ , entonces para todo vector  $\vec{v} \in V$ , existen  $a_1, \dots, a_n \in K$  únicos tales que  $\vec{v} = a_1 \vec{v}_1 + \dots + a_n \vec{v}_n$ .

A la  $n$ -upla  $(a_1, \dots, a_n)$  se le llama coordenadas del vector  $\vec{v}$  respecto de la base  $B$ .

**Ejercicio 44:** Demuestra que  $B = \{(1, 2), (1, 3)\}$  es una base de  $\mathbb{Z}_5^2$ . Calcula las coordenadas del vector  $(2, 4)$  respecto de dicha base.

**Teorema de la base.** Todo espacio vectorial distinto de  $\{\vec{0}\}$  tiene al menos una base. Además todas sus bases tienen el mismo cardinal.

Al cardinal de una base de  $V$  lo denotamos por  $\dim(V)$ , y nos referiremos a él como la dimensión de  $V$ .

**Ejercicio 45:** Prueba que  $\dim(K^n) = n$ ,  $\dim(\mathcal{M}_{m \times n}(K)) = nm$  y  $\dim(\{\mathbf{a}(x) \in K[x] \text{ tales que } \text{gr}(\mathbf{a}(x)) \leq n\}) = n + 1$ .

**Teorema de ampliación a base.** Si  $\dim(V) = n$  y  $\{\vec{v}_1, \dots, \vec{v}_m\}$  es un conjunto de vectores linealmente independientes de  $V$ , entonces  $m \leq n$ . Además existen  $\vec{v}_{m+1}, \dots, \vec{v}_n \in V$ , de forma que  $\{\vec{v}_1, \dots, \vec{v}_m, \vec{v}_{m+1}, \dots, \vec{v}_n\}$  es una base de  $V$ .

**Ejercicio 46:** Amplia  $\{(1, 1, 1)\}$  una base de  $\mathbb{R}^3$ .

- Si  $\dim(V) = n$ , entonces cualquier conjunto de vectores de  $V$  linealmente independientes de cardinal  $n$  es una base de  $V$ .

**Ejercicio 47:** Prueba que  $\{(1, 2, 1), (1, 1, 1), (1, 0, 0)\}$  es una base de  $\mathbb{Z}_3^3$ .

**Ejercicio 48:** Calcula una base del subespacio vectorial de  $\mathbb{R}^3$  generado por  $\{(1, 2, 1), (2, 4, 2), (1, 3, 2), (2, 5, 3)\}$ .

**Maxima 26:** Calculemos una base del subespacio vectorial  $U$  de  $\mathbb{Q}^3$  generado por  $\{(1, 2, 3), (1, 1, 1), (3, 2, 1)\}$ .

```
[commandchars=
{}]
```

```
(%i1) C:matrix([1,2,3],[1,1,1],[3,2,1]);
```

```
(%o1) 
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

```

Como las operaciones elementales por filas en la matriz  $C$  no alteran los sistemas de generadores,

```
(%i2) triangularize(C);
```

```
(%o2) 
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

```

nos dice que  $\{(1, 2, 3), (0, -1, -2)\}$  es una base de  $U$ .

**Maxima 27:** Veamos que  $B = \{(1, 1, 1), (1, 2, 1), (0, 0, 2)\}$  es una base de  $\mathbb{Z}_5^3$ , calculemos las coordenadas de  $(2, 3, 4)$  respecto de esa base.

```
(%i1) modulus:5$
```

```
(%i2) solve(x*[1,1,1]+y*[1,2,1]+z*[0,0,2],[x,y,z]);
```

```
(%o2) [[x = 0, y = 0, z = 0]]
```

Al ser tres generadores linealmente independientes en  $\mathbb{Z}_5^3$ , el conjunto dado es una base.

```
(%i3) solve(x*[1,1,1]+y*[1,2,1]+z*[0,0,2]-[2,3,4],[x,y,z]);
```

```
(%o3) [[x = 1, y = 1, z = 1]]
```

**Maxima 28:** Sean  $U$  y  $W$  los subespacios vectoriales de  $\mathbb{Z}_5^3$  generados por  $\{(1, 1, 1), (1, 2, 1)\}$  y  $\{(1, 2, 3), (0, 0, 2)\}$ , respectivamente. ¿Es  $\mathbb{Z}_5^3 = U + W$ ?

```
(%i1) modulus:5$
```

```
(%i2) D:matrix([1,1,1],[1,2,1],[1,2,3],[0,0,2]);
```

```
(%o2) 
$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix}$$

```

```
(%i3) triangularize(D);
```

```
(%o3)
```

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Así, una base para  $U + W$  es  $\{(1, 1, 1), (0, 1, 0), (0, 0, 2)\}$ , por lo que  $U + W = \mathbb{Z}_5^3$ .

**Maxima 29:** Sea  $U$  el subespacio vectorial de  $\mathbb{Q}^3$  generado por  $\{(1, 1, 1), (2, 1, 3), (4, 3, 5)\}$ , calculemos un complementario de  $U$ .

Primero buscamos una base para  $U$ , aplicando operaciones elementales al sistema de generadores que nos dan.

```
(%i1) modulus:false$
(%i2) E:matrix([1,1,1],[2,1,3],[4,3,5])$
(%i3) triangularize(E);
```

```
(%o3)
```

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

Ahora probamos a añadir un vector que sea independiente con los dos anteriores.

```
(%i4) F:matrix([1,1,1],[0,-1,1],[1,0,0])$
(%i5) triangularize(F);
```

```
(%o6)
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -2 \end{pmatrix}$$

De esta forma la recta generada por  $(1, 0, 0)$  es un complemento de  $U$  en  $\mathbb{Q}^3$ .

**Maxima 30:** Veamos ahora la dimensión del subespacio de  $\mathbb{Z}_7^4$  generado por

$$\{(2, 4, 3, 4), (4, 1, 6, 1), (3, 3, 3, 3), (5, 0, 6, 0)\}.$$

```
(%i1) modulus:7$
(%i2) G:matrix([2,4,3,4],[4,1,6,1],[3,3,3,3],[5,0,6,0])$
(%i3) triangularize(G);
```

```
(%o3)
```

$$\begin{pmatrix} -2 & 0 & -1 & 0 \\ 0 & -2 & -1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Luego la dimensión es dos, al tener dos filas no nulas en su forma reducida.

### 3. Ecuaciones del cambio de base

Sean  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  y  $B' = \{\vec{v}'_1, \dots, \vec{v}'_n\}$  dos bases de  $V$ . Sea  $\vec{x} \in V$ . Entonces existen  $x_1, \dots, x_n, x'_1, \dots, x'_n \in K$  tales que  $\vec{x} = x_1 \vec{v}_1 + \dots + x_n \vec{v}_n$  y  $\vec{x} = x'_1 \vec{v}'_1 + \dots + x'_n \vec{v}'_n$ . Queremos

ver qué relación hay entre las coordenadas de  $\vec{x}$  respecto de B y de B'. Para ello utilizaremos las coordenadas de los vectores de B respecto de B'. Supongamos que

$$\begin{aligned}\vec{v}_1 &= a_{11} \vec{v}'_1 + \cdots + a_{1n} \vec{v}'_n, \\ &\vdots \\ \vec{v}_n &= a_{n1} \vec{v}'_1 + \cdots + a_{nn} \vec{v}'_n.\end{aligned}$$

Entonces

$$\begin{aligned}\vec{x} &= x_1 \vec{v}_1 + \cdots + x_n \vec{v}_n = x_1 (a_{11} \vec{v}'_1 + \cdots + a_{1n} \vec{v}'_n) + \cdots + x_n (a_{n1} \vec{v}'_1 + \cdots + a_{nn} \vec{v}'_n) \\ &= (x_1 a_{11} + \cdots + x_n a_{n1}) \vec{v}'_1 + \cdots + (x_1 a_{1n} + \cdots + x_n a_{nn}) \vec{v}'_n = x'_1 \vec{v}'_1 + \cdots + x'_n \vec{v}'_n.\end{aligned}$$

Por tanto

$$\left. \begin{aligned}x'_1 &= x_1 a_{11} + \cdots + x_n a_{n1} \\ &\vdots \\ x'_n &= x_1 a_{1n} + \cdots + x_n a_{nn}\end{aligned} \right\},$$

que se conocen como las ecuaciones de cambio de base de B a B'. Éstas se pueden también expresar en forma matricial

$$(x'_1 \dots x'_n) = (x_1 \dots x_n) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

A la matriz  $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$  se le llama matriz de cambio de base de B a B'. Esta matriz es

siempre regular y su inversa,  $A^{-1}$  es justamente la matriz de cambio de base de B' a B.

**Ejercicio 49:** Sean  $B = \{(1, 1, 0), (1, 2, 1), (1, 1, 2)\}$  y  $B' = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$  dos bases de  $\mathbb{Z}_5^3$ . Calcula las ecuaciones de cambio de base de B a B'.

**Maxima 31:** Supongamos que K es  $\mathbb{Z}_5$  y  $V = \mathbb{Z}_5^2$ .

**(%i1) modulus:5;**

**(%o1) 5**

Elegimos dos bases,  $B = \{\vec{v}_1, \vec{v}_2\}$  y  $B' = \{\vec{u}_1, \vec{u}_2\}$ .

**(%i2) v1:[1,2];v2:[0,3];**

**(%o2) [1,2]**

**(%o3) [0,3]**

**(%i4) u1:[1,1];u2:[2,0];**

**(%o4) [1,1]**

**(%o5) [2,0]**

Calculamos las coordenadas de  $\vec{u}_1$  y  $\vec{u}_2$  respecto de B.

**(%i6) solve(a11\*v1+a12\*v2-u1,[a11,a12]);**

**(%o6) [[a11 = 1, a12 = -2]]**

**(%i7) solve(a21\*v1+a22\*v2-u2,[a21,a22]);**

(%o7)  $[[a21 = 2, a22 = 2]]$

Así la matriz de cambio de base de  $B'$  a  $B$  es la siguiente.

(%i8) `A:matrix([1,-2],[2,2]);`

(%o8)  $\begin{pmatrix} 1 & -2 \\ 2 & 2 \end{pmatrix}$

El vector  $\vec{u}_1 + \vec{u}_2$  tiene coordenadas  $(1, 1)$  en  $B'$ . Veamos cuáles son sus coordenadas en  $B$ .

(%i9) `[1,1].A;`

(%o9)  $(3 \ 0)$

Comprobamos el resultado.

(%i10) `u1+u2=3*v1;`

(%o10)  $[3, 1] = [3, 6]$

(%i11) `mod(%,5);`

(%o11)  $[3, 1] = [3, 1]$

La matriz de cambio de base de  $B$  a  $B'$  es la inversa de  $A$ .

(%i12) `A^(-1);`

(%o12)  $\begin{pmatrix} 2 & 2 \\ -2 & 1 \end{pmatrix}$

**Maxima 32:** Dadas las bases de  $\mathbb{Q}^3$ ,  $B = \{(1, 2, 3), (0, 3, 1), (0, 0, 4)\}$  y  $B' = \{(1, 1, 1), (0, 2, 3), (0, 0, 7)\}$ , veamos cuál es la matriz de cambio de base de  $B$  a  $B'$  y la de  $B'$  a  $B$ .

(%i1) `modulus:false$`

(%i2) `solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[1,2,3],[x,y,z]);`

(%o2)  $[[x = 1, y = \frac{1}{2}, z = \frac{1}{14}]]$

(%i3) `solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[0,3,1],[x,y,z]);`

(%o3)  $[[x = 0, y = \frac{3}{2}, z = -\frac{1}{2}]]$

(%i4) `solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[0,0,4],[x,y,z]);`

(%o4)  $[[x = 0, y = 0, z = \frac{4}{7}]]$

(%i5) `[x,y,z],%o2;`

(%o5)  $[1, \frac{1}{2}, \frac{1}{14}]$

(%i6) `[x,y,z],%o3;`

(%o6)  $[0, \frac{3}{2}, -\frac{1}{2}]$

(%i7) `[x,y,z],%o4;`

(%o7)  $[0, 0, \frac{4}{7}]$

La matriz de cambio de base de  $B$  a  $B'$  es

(%i8) `H:matrix(%o5,%o6,%o7);`

(%o8) 
$$\begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{14} \\ 0 & \frac{2}{3} & -\frac{1}{2} \\ 0 & 0 & \frac{4}{7} \end{pmatrix}$$

y la de  $B'$  a  $B$  es

(%i9) `J:invert(%);`

(%o9) 
$$\begin{pmatrix} 1 & -\frac{1}{3} & -\frac{5}{12} \\ 0 & \frac{2}{3} & \frac{1}{2} \\ 0 & 0 & \frac{7}{4} \end{pmatrix}$$

Si las coordenadas de un vector respecto de la base  $B$  son  $(1, 1, 1)$ , sus coordenadas respecto de  $B'$  son

(%i10) `[1,1,1].H;`

(%o10) 
$$\left(1 \quad 2 \quad \frac{1}{7}\right)$$

#### 4. Ecuaciones paramétricas de un subespacio vectorial

Supongamos que  $\dim(V) = n$  y que  $U$  es un subespacio vectorial de  $V$  de dimensión  $r$ . Sea  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  una base de  $V$ , y  $B_U = \{\vec{u}_1, \dots, \vec{u}_r\}$  una base de  $U$ . Supongamos que

$$\vec{u}_1 = a_{11} \vec{v}_1 + \dots + a_{1n} \vec{v}_n,$$

$$\vdots$$

$$\vec{u}_r = a_{r1} \vec{v}_1 + \dots + a_{rn} \vec{v}_n.$$

Sea  $\vec{x} = x_1 \vec{v}_1 + \dots + x_n \vec{v}_n$  un vector de  $V$ . Veamos qué tienen que verificar las coordenadas  $(x_1, \dots, x_n)$  para que  $\vec{x} \in U$ .

El vector  $\vec{x} \in U$  si y sólo si existen  $\lambda_1, \dots, \lambda_r \in K$  tales que  $\vec{x} = \lambda_1 \vec{u}_1 + \dots + \lambda_r \vec{u}_r$ , y esto equivale a que

$$\begin{aligned} \vec{x} &= \lambda_1(a_{11} \vec{v}_1 + \dots + a_{1n} \vec{v}_n) + \dots + \lambda_r(a_{r1} \vec{v}_1 + \dots + a_{rn} \vec{v}_n) \\ &= (\lambda_1 a_{11} + \dots + \lambda_r a_{r1}) \vec{v}_1 + \dots + (\lambda_1 a_{1n} + \dots + \lambda_r a_{rn}) \vec{v}_n. \end{aligned}$$

Como las coordenadas son únicas,

$$\left. \begin{aligned} x_1 &= \lambda_1 a_{11} + \dots + \lambda_r a_{r1} \\ &\vdots \\ x_n &= \lambda_1 a_{1n} + \dots + \lambda_r a_{rn} \end{aligned} \right\}.$$

Estas ecuaciones son las ecuaciones paramétricas de  $U$  respecto de la base  $B$ .

**Ejercicio 50:** Dada la base  $B = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$  de  $\mathbb{Q}^3$ , y  $U$  el subespacio vectorial de  $\mathbb{Q}^3$  generado por  $\{(1, 2, 1), (1, 3, 2), (2, 5, 3)\}$ , calcula las ecuaciones paramétricas de  $U$  respecto de la base  $B$ .

**Maxima 33:** Sea  $U$  el subespacio de  $\mathbb{Z}_7^3$  generado por  $\{(2, 3, 4), (2, 4, 4), (4, 6, 1)\}$ , calculamos a continuación las ecuaciones paramétricas de  $U$  respecto de la base  $B = \{(1, 2, 3), (0, 3, 4), (0, 0, 6)\}$ .

Primero encontramos una base para  $U$ , y lo hacemos con el comando `triangularize`.

(%i1) `modulus:7$`

(%i2) `K:matrix([2,3,4],[2,4,4],[4,6,1])$`

(%i3) `triangularize(K);`

(%o3) 
$$\begin{pmatrix} 2 & 3 & -3 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto,  $\mathbf{U}$  tiene como base  $\{(2, 3, -3), (0, 2, 0)\}$ . Encontramos pues las coordenadas de sus elementos respecto de la base  $\mathbf{B}$ .

(%i4) `solve(x*[1,2,3]+y*[0,3,4]+z*[0,0,6]-[2,3,-3], [x,y,z]);`

(%o4)  $[[x = 2, y = 2, z = 3]]$

(%i5) `solve(x*[1,2,3]+y*[0,3,4]+z*[0,0,6]-[0,2,0], [x,y,z]);`

(%o5)  $[[x = 0, y = 3, z = -2]]$

Así un elemento de coordenadas  $(x, y, z)$  respecto de la base  $\mathbf{B}$  estará en  $\mathbf{U}$  si y sólo si  $(x, y, z) = \lambda(2, 2, 3) + \mu(0, 3, 5)$  para algún  $\lambda, \mu \in \mathbb{Z}_7$ . Las ecuaciones paramétricas son

$$\begin{cases} x = 2\lambda, \\ y = 2\lambda + 3\mu, \\ z = 3\lambda + 5\mu. \end{cases}$$

## 5. Aplicaciones lineales

En lo que queda de capítulo suponemos que  $V$  y  $V'$  son dos espacios vectoriales sobre el mismo cuerpo  $K$ .

Una aplicación  $f : V \rightarrow V'$  es lineal (o un homomorfismo) si

- 1) para todo  $\vec{u}, \vec{v} \in V$ ,  $f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$ ,
- 2) para todo  $\alpha \in K$  y  $\vec{v} \in V$ ,  $f(\alpha \vec{v}) = \alpha f(\vec{v})$ .

- $f(\vec{0}) = \vec{0}$  (el primer  $\vec{0}$  es de  $V$  y el segundo de  $V'$ ).
- $f(-\vec{v}) = -f(\vec{v})$ .
- El núcleo de  $f$ ,  $N(f) = \{\vec{v} \in V \text{ tales que } f(\vec{v}) = \vec{0}\}$ , es un subespacio vectorial de  $V$ .
- La imagen de  $f$ ,  $\text{Im}(f)$ , es un subespacio vectorial de  $V'$ .

Una aplicación lineal es un

- 1) monomorfismo si es inyectiva,
- 2) epimorfismo si es sobreyectiva,
- 3) isomorfismo si es biyectiva.

- Si  $f$  es un isomorfismo, también lo es  $f^{-1}$ .
- $f$  es un monomorfismo si y sólo si  $N(f) = \{\vec{0}\}$ .
- Si  $V = \langle \{\vec{v}_1, \dots, \vec{v}_n\} \rangle$ , entonces  $\text{Im}(f) = \langle \{f(\vec{v}_1), \dots, f(\vec{v}_n)\} \rangle$ .
- Si  $f$  es un monomorfismo y  $\{\vec{v}_1, \dots, \vec{v}_n\}$  son linealmente independientes, entonces  $\{f(\vec{v}_1), \dots, f(\vec{v}_n)\}$  también son linealmente independientes.

**Ejercicio 51:** Demuestra que  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ ,  $f(x, y, z) = (x+y, x+z)$  es una aplicación lineal. Calcula  $N(f)$  y  $\text{Im}(f)$ . ¿Es  $f$  un isomorfismo?

**Ejercicio 52:** Sea  $f : \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^3$ ,  $(x, y, z) \mapsto (x, y, z + y)$ . Calcula una base de  $\text{Im}(f)$ . ¿Es  $f$  un epimorfismo?

**Teorema:** Las aplicaciones lineales vienen determinadas por la imagen de una base.

Sea  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  una base de  $V$ , y  $\{\vec{v}'_1, \dots, \vec{v}'_m\} \subseteq V'$ . Entonces existe una única aplicación lineal  $f : V \rightarrow V'$  verificando que  $f(\vec{v}_1) = \vec{v}'_1, \dots, f(\vec{v}_n) = \vec{v}'_n$ . Además,  $\{\vec{v}'_1, \dots, \vec{v}'_n\}$  es una base de  $V'$  si y sólo si  $f$  es un isomorfismo.

Los espacios vectoriales  $V$  y  $V'$  diremos que son isomorfos si existe un isomorfismo  $f : V \rightarrow V'$ .

- $V$  y  $V'$  son isomorfos si y sólo si  $\dim(V) = \dim(V')$ .

**Ejercicio 53:** Sea  $U$  el subespacio vectorial de  $\mathbb{Z}_5^3$  generado por  $\{(1, 2, 3), (0, 1, 2), (1, 3, 0)\}$ . Calcula el cardinal de  $U$ .

**Maxima 34:** Sea  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$  definida por  $f(x, y, z) = (x + y, x + z, 2x + y + z, y - z)$ . Para calcular su núcleo usamos:

```
(%i1) solve([x+y=0,x+z=0,2*x+y+z=0,y-z=0],[x,y,z]);
```

```
solve : dependentequationseliminated : (34)
```

```
(%o1) [[x = -%r1, y = %r1, z = %r1]]
```

Así  $N(f) = \{(-a, a, a) \mid a \in \mathbb{R}\}$ , que tiene como base a  $\{(-1, 1, 1)\}$ . Para calcular una base de la imagen, sabiendo que  $\{f(1, 0, 0), f(0, 1, 0), f(0, 0, 1)\}$  es un sistema de generadores, hacemos lo siguiente.

```
(%i2) f(x,y,z):=[x+y,x+z,2*x+y+z,y-z]$
```

```
(%i3) A:matrix(f(1,0,0),f(0,1,0),f(0,0,1))$
```

```
(%i4) triangularize(A);
```

```
(%o4) (1 1 2 0)
      (0 -1 -1 1)
      (0 0 0 0)
```

Por tanto, una base de  $\text{Im}(f)$  es  $\{(1, 1, 2, 0), (0, -1, -1, 1)\}$ .

## 6. Ecuaciones de una aplicación lineal

Sea  $f : V \rightarrow V'$  una aplicación lineal, y  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  y  $B' = \{\vec{v}'_1, \dots, \vec{v}'_m\}$  bases de  $V$  y  $V'$ , respectivamente. Sean  $\vec{x} = x_1 \vec{v}_1 + \dots + x_n \vec{v}_n$  y  $f(\vec{x}) = x'_1 \vec{v}'_1 + \dots + x'_m \vec{v}'_m \in V'$ . Queremos estudiar la relación que existe entre las coordenadas de  $\vec{x}$  y  $f(\vec{x})$ .

Supongamos que

$$\begin{aligned} f(\vec{v}_1) &= a_{11} \vec{v}'_1 + \dots + a_{1m} \vec{v}'_m, \\ &\vdots \\ f(\vec{v}_n) &= a_{n1} \vec{v}'_1 + \dots + a_{nm} \vec{v}'_m. \end{aligned}$$

Entonces

$$\begin{aligned} f(\vec{x}) &= f(x_1 \vec{v}_1 + \dots + x_n \vec{v}_n) = x_1 f(\vec{v}_1) + \dots + x_n f(\vec{v}_n) \\ &= x_1 (a_{11} \vec{v}'_1 + \dots + a_{1m} \vec{v}'_m) + \dots + x_n (a_{n1} \vec{v}'_1 + \dots + a_{nm} \vec{v}'_m) \\ &= (x_1 a_{11} + \dots + x_n a_{n1}) \vec{v}'_1 + \dots + (x_1 a_{1m} + \dots + x_n a_{nm}) \vec{v}'_m. \end{aligned}$$

Así

$$\left. \begin{aligned} x'_1 &= a_{11} x_1 + \dots + a_{n1} x_n \\ &\vdots \\ x'_m &= a_{1m} x_1 + \dots + a_{nm} x_n \end{aligned} \right\}$$

que se conocen como ecuaciones de la aplicación lineal respecto de las bases  $B$  y  $B'$ .



Estas ecuaciones se pueden expresar de forma matricial como

$$(x'_1 \dots x'_m) = (x_1 \dots x_n) \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}.$$

La matriz  $A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$  es la matriz asociada a la aplicación lineal  $f$  respecto de las bases  $B$  y  $B'$ .

- $f$  es un isomorfismo si y sólo si  $A$  es regular.

**Ejercicio 54:** Sea  $f: \mathbb{Q}^2 \rightarrow \mathbb{Q}^3$ , la aplicación lineal definida por  $f(x, y, z) = (x, x+y, x-y)$ . Calcula las ecuaciones de  $f$  respecto de las bases  $\{(1, 1), (1, 2)\}$  de  $\mathbb{Q}^2$  y  $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$  de  $\mathbb{Q}^3$ .

**Ejercicio 55:** Sea  $f: \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^3$  una aplicación lineal tal que  $f(1, 2) = (2, 3, 1)$  y  $f(2, 5) = (3, 4, 2)$ . Calcula la expresión general  $f(x, y)$ .

**Ejercicio 56:** Encuentra la matriz asociada a la base  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$  de una aplicación lineal  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$  que verifica que  $(1, 0, 0) \in N(f)$  y  $\text{Im}(f) = \langle \{(2, 3, 1), (3, 3, 2)\} \rangle$ .

**Maxima 35:** Calculemos la expresión matricial de la aplicación lineal del ejemplo anterior respecto de las bases  $B = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$  y  $B' = \{(1, 1, 1, 1), (0, 1, 1, 1), (0, 0, 1, 1), (0, 0, 0, 1)\}$ . Podemos por ejemplo calcular las coordenadas de las imágenes por  $f$  de los elementos de  $B$  respecto de  $B'$ .

```
(%i1) f(x,y,z):=[x+y,x+z,2*x+y+z,y-z]$
(%i2) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
f(1,1,0),[x,y,z,t]);
(%o2) [[x = 2, y = -1, z = 2, t = -2]]
(%i3) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
f(1,0,1),[x,y,z,t]);
(%o3) [[x = 1, y = 1, z = 1, t = 3]]
(%i4) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
f(0,1,1),[x,y,z,t]);
(%o4) [[x = 1, y = 0, z = 1, t = -2]]
(%i5) C:matrix([2,-1,2,-2],[1,1,1,-4],[1,0,1,-2]);
(%o5) (2 -1 2 -2)
      (1 1 1 -4)
      (1 0 1 -2)
```

Por tanto la expresión matricial es  $(x', y', z', t') = (x, y, z)C$ .

**Maxima 36:** Tomamos una base  $B = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$  en  $\mathbb{Q}^3$ .

```
(%i1) v1:[1,2,1];v2:[1,1,0];v3:[0,0,3];
```

(%o1)  $[1, 2, 1]$

(%o2)  $[1, 1, 0]$

(%o3)  $[0, 0, 3]$

Y las imágenes de esos vectores respecto de la base usual  $\{(1, 0), (0, 1)\}$  en  $\mathbb{Q}^2$ .

(%i4) `fv1:[1,1];fv2:[2,1];fv3:[1,2];`

(%o4)  $[1, 1]$

(%o5)  $[2, 1]$

(%o6)  $[1, 2]$

La matriz de  $f$  asociada a dichas bases es:

(%i7) `A:matrix(fv1,fv2,fv3);`

(%o7) 
$$\begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}$$

Si queremos calcular la imagen de un elemento con coordenadas  $(x, y, z)$  respecto de  $B$ , sólo tenemos que multiplicar esas coordenadas por  $A$ .

(%i8) `[x,y,z].A;`

(%o8)  $(z + 2y + x \quad 2z + y + x)$

Así  $f(x, y, z) = (x + 2y + z, x + y + 2z)$ , donde  $(x, y, z)$  son coordenadas respecto de  $B$ .

Si lo que queremos es la expresión de  $f(x, y, z)$ , con  $(x, y, z)$  coordenadas respecto de la base usual  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ , lo que hacemos es calcular primero el cambio de base de  $B$  a la base usual, y luego lo multiplicamos por  $A$ , obteniendo así la expresión matricial respecto de las bases usuales.

(%i9) `B:matrix(v1,v2,v3);`

(%o9) 
$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

(%i10) `B^-1;`

(%o10) 
$$\begin{pmatrix} -1 & 2 & \frac{1}{3} \\ 1 & -1 & -\frac{1}{3} \\ 0 & 0 & \frac{1}{3} \end{pmatrix}$$

(%i11) `AA:%.A;`

(%o11) 
$$\begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ -\frac{4}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

Veamos que el resultado es el deseado ( $\vec{v}_i$  lo definimos en función de la base usual).

(%i12) `v1.AA;v2.AA;v2.AA`

$$(\%o12) \quad (1 \ 1)$$

$$(\%o13) \quad (2 \ 1)$$

$$(\%o14) \quad (1 \ 2)$$

Por tanto las coordenadas de  $f(x, y, z)$  respecto de la base usual de  $\mathbb{Q}^2$ , con  $(x, y, z)$  coordenadas en la base usual de  $\mathbb{Q}^3$ , la podemos calcular como sigue.

(%i17) `[x,y,z].AA;`

$$(\%o17) \quad \left( \frac{z}{3} - \frac{4y}{3} + \frac{10x}{3} \quad \frac{2z}{3} - \frac{2y}{3} + \frac{5x}{3} \right)$$

**Maxima 37:** Calculemos la expresión de una aplicación lineal  $g : \mathbb{Z}_5^3 \rightarrow \mathbb{Z}_5^2$  tal que  $g(1, 1, 1) = (2, 0)$ ,  $g(1, 2, 1) = (1, 1)$  y  $g(0, 0, 2) = (3, 3)$ .

(%i1) `modulus:5$`

(%i2) `D:matrix([1,1,1],[1,2,1],[0,0,2])$`

(%i3) `E:invert(D)$`

(%i4) `F:rat(E);`

$$(\%o4)/R/ \quad \begin{pmatrix} 2 & -1 & 2 \\ -1 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Tenemos así las coordenadas de los vectores  $(1, 0, 0)$ ,  $(0, 1, 0)$  y  $(0, 0, 1)$  respecto de la base  $\{(1, 1, 1), (1, 2, 1), (0, 0, 2)\}$ .

(%i5) `G:matrix([2,0],[1,1],[3,3])$`

Y sus imágenes por  $g$  se calculan multiplicando por  $G$ .

(%i6) `H:F.G;`

$$(\%o6)/R/ \quad \begin{pmatrix} -1 & 0 \\ -1 & 1 \\ -1 & -1 \end{pmatrix}$$

Por tanto  $g(x, y, z) = (4x + 4y + 4z, y + 4z)$ . Comprobemos si hemos hecho bien los cálculos.

(%i7) `g(x,y,z):=[4*x+4*y+4*z,y+4*z]$`

(%i8) `rat(g(1,1,1));`

$$(\%o8)/R/ \quad [2, 0]$$

(%i9) `rat(g(1,2,1));`

$$(\%o9)/R/ \quad [1, 1]$$

(%i10) `rat(g(0,0,2));`

$$(\%o10)/R/ \quad [-2, -2]$$

## 7. Espacio vectorial cociente

Sea  $U$  un subespacio vectorial de  $V$ . Definimos en  $V$  la siguiente relación de equivalencia:  $\vec{x} \sim \vec{y}$  si  $\vec{x} - \vec{y} \in U$ . Denotamos por  $\frac{V}{U}$  al conjunto cociente  $\frac{V}{U}$ .

- El conjunto  $\frac{V}{U}$  es un espacio vectorial con las operaciones  $[\vec{x}] + [\vec{y}] = [\vec{x} + \vec{y}]$  y  $k[\vec{x}] = [k\vec{x}]$ . A dicho espacio vectorial se le conoce como espacio vectorial cociente de  $V$  sobre  $U$ .

- Si  $\{\vec{u}_1, \dots, \vec{u}_m\}$  es una base de  $U$  y la ampliamos a una base de  $V$ ,  $\{\vec{u}_1, \dots, \vec{u}_m, \vec{u}_{m+1}, \dots, \vec{u}_n\}$ , entonces  $\{[\vec{u}_{m+1}], \dots, [\vec{u}_n]\}$  es una base de  $\frac{V}{U}$ . Así

$$\dim\left(\frac{V}{U}\right) = \dim(V) - \dim(U).$$

**Primer teorema de isomorfía.** Si  $f : V \rightarrow V'$  es una aplicación lineal, entonces los espacios vectoriales  $\frac{V}{N(f)}$  e  $\text{Im}(f)$  son isomorfos (el isomorfismo viene dado por  $[\vec{v}] \mapsto f(\vec{v})$ ).

- $\dim(V) = \dim(N(f)) + \dim(\text{Im}(f))$ .

**Ejercicio 57:** Sea  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$  definida por  $f(x, y, z) = (2x + y, 3x + z)$ . Encuentra una base de  $N(f)$ .

**Segundo teorema de isomorfía.** Si  $U_1$  y  $U_2$  son subespacios de  $V$ , entonces los espacios vectoriales  $\frac{U_2}{U_1 \cap U_2}$  y  $\frac{U_1 + U_2}{U_1}$  son isomorfos.

- $\dim(U_1) + \dim(U_2) = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$ .

**Ejercicio 58:** Dados los subespacios vectoriales de  $\mathbb{Z}_5^3$ ,  $U = \langle\langle(1, 1, 2), (1, 2, 3)\rangle\rangle$  y  $W = \langle\langle(1, 0, 0), (2, 1, 3)\rangle\rangle$ , calcula la dimensión de  $U \cap W$ .

**Ejercicio 59:** Sea  $U$  el subespacio vectorial de  $\mathbb{Q}^3$  generado por  $\{(1, 2, 1)\}$ . Calcula un complementario de  $U$ .

**Maxima 38:** Sea  $U$  el subespacio vectorial de  $\mathbb{Q}^4$  generado por  $\{(1, 1, 1, 1), (1, 2, 3, 4), (1, 0, -1, -2)\}$ , calculemos una base del espacio cociente  $\mathbb{Q}^4/U$ .

```
(%i1) A:matrix([1,1,1,1],[1,2,3,4],[1,0,-1,-2])$
```

```
(%i2) triangularize(A);
```

```
(%o2) 
$$\begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```

Una base de  $U$  es  $\{(1,0,-1,-2), (0,2,4,6)\}$ . Ahora la ampliamos a una base de  $\mathbb{Q}^4$ .

```
(%i3) B:matrix([1,0,-1,-2],[0,2,4,6],[0,0,1,0],[0,0,0,1])$
```

```
(%i4) determinant(B);
```

```
(%o4) 2
```

Una base del cociente es  $\{[(0, 0, 1, 0)], [(0, 0, 0, 1)]\}$ .

**Maxima 39:** Sea  $f : \mathbb{Q}^4 \rightarrow \mathbb{Q}^3$  definida por

```
(%i1) f(x,y,z,t):=[x+y+z,x+z+t,y-t]$
```

Como

```
(%i2) triangularize(matrix(f(1,0,0,0),f(0,1,0,0),f(0,0,1,0),f(0,0,0,1)));
```

```
(%o2) 
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

```

deducimos que la imagen de  $f$  tiene dimensión 2. Por el primer teorema de isomorfía, su núcleo debería también tener dimensión dos. Comprobémoslo:

```
(%i3) solve(f(x,y,z,t), [x,y,z,t]);
```

```
solve : dependentequationseliminated : (1)
```

```
(%o3) [[x = -%r3 - %r2, y = %r2, z = %r3, t = %r2]]
```

**Maxima 40:** Sean  $U$  y  $W$  los subespacios de  $\mathbb{Z}_7^4$  generados por  $\{(1, 0, 1, 0), (1, 2, 1, 2), (1, 5, 1, 5)\}$  y  $\{(2, 3, 4, 0), (1, 5, 2, 0), (2, 3, 2, 3)\}$ , respectivamente. Veamos cuál es la dimensión de  $U \cap W$ .

Un sistema de generadores para  $U+W$  es  $\{(1, 0, 1, 0), (1, 2, 1, 2), (1, 5, 1, 5), (2, 3, 4, 0), (1, 5, 2, 0), (2, 3, 2, 3)\}$ .

```
(%i1) modulus:7$
```

Las dimensiones de  $U$  y  $W$  son dos, ya que

```
(%i2) triangularize(matrix([1,0,1,0], [1,2,1,2], [1,5,1,5]));
```

```
(%o2) 
$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```

y

```
(%i3) triangularize(matrix([2,3,4,0], [1,5,2,0], [2,3,2,3]));
```

```
(%o3) 
$$\begin{pmatrix} 2 & 3 & -3 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```

Por último,

```
(%i4) triangularize(matrix([1,0,1,0], [1,2,1,2], [1,5,1,5], [2,3,4,0], [1,5,2,0], [2,3,2,3]));
```

```
(%o4) 
$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```

Esto nos dice que la dimensión de  $U+W$  es 3. Por el Segundo Teorema de Isomorfía, deducimos que la dimensión de  $U \cap W$  es 1.

## Sistemas de ecuaciones lineales

### 1. Rango de una matriz

Sea  $A = \begin{pmatrix} \mathbf{a}_{11} & \dots & \mathbf{a}_{1n} \\ \vdots & \ddots & \vdots \\ \mathbf{a}_{m1} & \dots & \mathbf{a}_{mn} \end{pmatrix} \in \mathcal{M}_{m \times n}(\mathbb{K})$ . El rango por filas de la matriz  $A$  es la dimensión del

subespacio vectorial de  $\mathbb{K}^n$  generado por sus filas, a saber,  $\{(\mathbf{a}_{11}, \dots, \mathbf{a}_{1n}), \dots, (\mathbf{a}_{m1}, \dots, \mathbf{a}_{mn})\}$ . El rango por columnas de  $A$  es la dimensión del subespacio vectorial de  $\mathbb{K}^m$  generado por las columnas de  $A$ .

**Ejercicio 60:** Calcula el rango por filas y por columnas de la matriz  $\begin{pmatrix} 1 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \in \mathcal{M}_{2 \times 3}(\mathbb{Z}_5)$ .

**Teorema.** El rango por filas de  $A$  coincide con el rango por columnas de  $A$ . A dicha cantidad la llamaremos simplemente rango de  $A$  y la denotaremos por  $\text{rango}(A)$ .

**Teorema (rango y determinantes).** El rango de una matriz es el máximo de los órdenes de sus submatrices cuadradas regulares.

**Ejercicio 61:** Calcula el rango de la matriz

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 1 & 3 & 1 \\ 4 & 5 & 5 & 1 \end{pmatrix} \in \mathcal{M}_{3 \times 4}(\mathcal{R}).$$

**Maxima 41:** El rango de una matriz también se puede calcular contando las filas no nulas de su forma triangular reducida asociada.

```
(%i1) A:matrix([0,1,2,3],[4,5,6,7],[8,9,10,11]);
```

```
(%o1)  $\begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{pmatrix}$ 
```

```
(%i2) rank(A);
```

```
(%o2) 2
```

```
(%i3) echelon(A);
```

```
(%o3)  $\begin{pmatrix} 1 & \frac{5}{4} & \frac{3}{2} & \frac{7}{4} \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ 
```

```
(%i4) triangularize(A);
```

$$(\%o4) \quad \begin{pmatrix} 4 & 5 & 6 & 7 \\ 0 & 4 & 8 & 12 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

## 2. Resolución de sistemas de ecuaciones lineales

Un sistema de ecuaciones lineales con  $n$  incógnitas sobre un cuerpo  $K$  es una expresión de la forma

$$\left. \begin{array}{l} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{array} \right\}.$$

Los elementos  $a_{ij} \in K$  son los coeficientes del sistema, los  $b_i \in K$  son los términos independientes, y las  $x_i$  son las incógnitas. Una solución es una  $n$ -upla  $(s_1, \dots, s_n) \in K^n$  tal que  $x_1 = s_1, \dots, x_n = s_n$  verifica las igualdades del sistema.

Las  $m$  igualdades del sistema anterior se pueden expresar como una única igualdad entre matrices,

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

a la que llamaremos expresión matricial del sistema. A dichas matrices se les llama matriz de coeficientes, matriz incógnita, y matriz de términos independientes.

La matriz ampliada del sistema es

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}.$$

Normalmente denotaremos a esta matriz por  $(A|B)$ .

Si un sistema tiene solución diremos que es compatible, y en caso contrario incompatible. Si tiene una única solución, es un sistema compatible determinado, y si tiene más de una solución decimos que es un sistema compatible indeterminado.

Dos sistemas de ecuaciones lineales sobre un cuerpo y con igual número de incógnitas son equivalentes si tienen las mismas soluciones.

### Proposición (operaciones elementales).

- 1) Si intercambiamos de posición dos ecuaciones de un sistema, obtenemos un sistema equivalente.
- 2) Si multiplicamos una ecuación por un escalar no nulo, obtenemos un sistema equivalente.
- 3) Si a una ecuación le sumamos otra multiplicada por un escalar, también obtenemos un sistema equivalente al original.

**Ejercicio 62:** Resuelve el siguiente sistema de ecuaciones con coeficientes en  $\mathbb{Z}_5$ .

$$\left. \begin{array}{l} x_1 + x_2 + x_3 + x_4 = 1 \\ 2x_1 + 3x_2 + x_3 + x_4 = 2 \\ 4x_1 + 3x_2 + x_3 + 2x_4 = 0 \\ x_1 + x_2 + 2x_3 + 3x_4 = 2 \end{array} \right\}.$$

**Teorema de Rouché-Frobenius.** Sea  $AX = B$  la expresión matricial de un sistema de ecuaciones lineales con  $n$  incógnitas.

- 1) El sistema es compatible si y sólo si  $\text{rango}(A) = \text{rango}(A|B)$ .
- 2) El sistema es compatible determinado si y sólo si  $\text{rango}(A) = \text{rango}(A|B) = n$ .

**Maxima 42:** Vamos a estudiar el siguiente sistema de ecuaciones con coeficientes en  $\mathbb{Z}_5$ .

$$\left. \begin{array}{l} x + y + z = 3 \\ 3x + y + 2z = 1 \\ x + 4y = 0 \end{array} \right\}.$$

```
(%i1) modulus:5$
(%i2) B:matrix([1,1,1],[3,1,2],[1,4,0])$
(%i3) rank(B);
(%o3) 2

(%i4) C:addcol(B,[3,1,0])$
(%i5) rank(C);
(%o5) 2
```

El sistema es compatible indeterminado.

**Maxima 43:** Estudiemos ahora el siguiente sistema con coeficientes en  $\mathbb{Z}_7$  en función del parametro  $a$ .

$$\left. \begin{array}{l} x + y + z = a \\ 2x + ay + z = 1 \\ 3x + 3y + az = 2 \end{array} \right\}.$$

```
(%i1) modulus:7$
(%i2) D:matrix([1,1,1],[2,a,1],[3,3,a])$
(%i3) determinant(D);
(%o3) a^2 - 5a + 6

(%i4) factor(a^2-5*a+6);
(%o4) (a - 3) (a - 2)
```

Así, si  $a \notin \{2, 3\}$ , la matriz de coeficientes tiene rango máximo y el sistema es compatible determinado.

Estudiemos por separado los casos  $a = 2$  y  $a = 3$ .

```
(%i5) E:subst(2,a,D);
(%o5) \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 1 \\ 3 & 3 & 2 \end{pmatrix}

(%i6) rank(E);
(%o6) 2

(%i7) F:addcol(E,[2,1,2])$
(%i8) rank(F);
(%o8) 3
```

Luego para  $a = 2$ , el sistema es incompatible.

```
(%i9) G:subst(3,a,D)$
```



```
(%i11) rank(G);
(%o11) 2
```

```
(%i12) H:addcol(G,[3,1,2])$
```

```
(%i13) rank(H);
(%o13) 2
```

Para  $\alpha = 3$  obtenemos un sistema compatible indeterminado.

**Ejercicio 63:** Estudia el siguiente sistema de ecuaciones con coeficientes en  $\mathbb{Z}_5$ .

$$\left. \begin{array}{l} 2x + 4y + 4z = 1 \\ 3x + y + 2z = 2 \\ 4y + z = 3 \end{array} \right\}.$$

**Ejercicio 64:** Estudia los siguientes sistemas con coeficientes en  $\mathbb{R}$  en función de los parámetros  $\alpha$  y  $b$ .

1)

$$\left. \begin{array}{l} \alpha x + y + z = 1 \\ x + y + z = 2 \end{array} \right\},$$

2)

$$\left. \begin{array}{l} \alpha x + y + z = 1 \\ x + y + z = b \\ \alpha x + by + z = 1 \end{array} \right\},$$

3)

$$\left. \begin{array}{l} \alpha x + y + z = 1 \\ x - y + z = 1 \end{array} \right\},$$

4)

$$\left. \begin{array}{l} \alpha x + y + z = 1 \\ x + 2y + \alpha z = 2 \end{array} \right\}.$$

**Maxima 44:** El comando `linsolve` en máxima puede ser utilizado para resolver sistemas lineales de ecuaciones.

```
(%i1) linsolve([2*x+y+z=2,x-y-2*z=0],[x,y,z]);
```

```
(%o1) [x = -(%r1 - 6)/3, y = -(%r1 + 6)/3, z = %r1]
```

Como vemos, las soluciones dependen de un parámetro, que aquí se denomina `%r1`. El rango de la matriz de coeficientes es 2 como vemos a continuación, y es el máximo posible (sólo hay dos filas), por lo que coincide con el de la matriz ampliada. El sistema es compatible indeterminado.

```
(%i2) rank(matrix([2,1,1],[1,-1,-2]));
```

```
(%o2) 2
```

**Fórmula de Cramer.** Un sistema es de Cramer si su matriz de coeficientes es cuadrada y regular. Si  $AX = B$  es la expresión matricial de un sistema de Cramer, entonces el sistema es compatible determinado y su única solución es

$$|A|^{-1}(|M_1|, \dots, |M_n|),$$

donde  $M_i$  es la matriz que se obtiene a partir de  $A$  cambiando la columna  $i$ -ésima por  $B$ .

**Ejercicio 65:** Prueba que el siguiente sistema de ecuaciones con coeficientes en  $\mathbb{R}$  es un sistema de Cramer, y encuentra sus soluciones usando la fórmula de Cramer.

$$\left. \begin{aligned} x + y + z &= 1 \\ x - y + z &= 0 \\ x + y - z &= 2 \end{aligned} \right\}.$$

### 3. Ecuaciones cartesianas o implícitas de un subespacio vectorial

Sea  $U$  un subespacio vectorial de  $V$ . Sea  $B = \{\vec{v}_1, \dots, \vec{v}_n\}$  una base de  $V$ , y  $B_U = \{\vec{u}_1, \dots, \vec{u}_r\}$  una base de  $U$ . Supongamos que

$$\begin{aligned} \vec{u}_1 &= a_{11}\vec{v}_1 + \dots + a_{1n}\vec{v}_n, \\ &\vdots \\ \vec{u}_r &= a_{r1}\vec{v}_1 + \dots + a_{rn}\vec{v}_n. \end{aligned}$$

Sea  $\vec{x} = x_1\vec{v}_1 + \dots + x_n\vec{v}_n$  un vector de  $V$ . Recordemos que el vector  $\vec{x} \in U$  si y sólo si existen  $\lambda_1, \dots, \lambda_r \in K$  tales que

$$\left. \begin{aligned} x_1 &= \lambda_1 a_{11} + \dots + \lambda_r a_{r1} \\ &\vdots \\ x_n &= \lambda_1 a_{1n} + \dots + \lambda_r a_{rn} \end{aligned} \right\}.$$

Luego  $\vec{x} \in U$  si y sólo si el sistema con incógnitas  $\lambda_1, \dots, \lambda_r$

$$\begin{pmatrix} a_{11} & \dots & a_{r1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{rn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

tiene solución. Y sabemos que equivale a  $\text{rango} \begin{pmatrix} a_{11} & \dots & a_{r1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{rn} \end{pmatrix} = \text{rango} \begin{pmatrix} a_{11} & \dots & a_{r1} & x_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{1n} & \dots & a_{rn} & x_n \end{pmatrix}$ .

Esto ocurre cuando unos cuantos determinantes valen cero, proporcionándonos así una sistema de ecuaciones de la forma

$$\left. \begin{aligned} b_{11}x_1 + \dots + b_{1n}x_n &= 0 \\ &\vdots \\ b_{k1}x_1 + \dots + b_{kn}x_n &= 0 \end{aligned} \right\},$$

a las que llamaremos ecuaciones cartesianas de  $U$  respecto de la base  $B$  de  $V$ .

- Si  $k$  es el número de ecuaciones cartesianas independientes que describen a  $U$ , entonces  $k + \dim(U) = \dim(V)$ .

**Ejercicio 66:** Dada la base  $B = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ , calcula las ecuaciones cartesianas respecto de la base  $B$  del subespacio vectorial de  $\mathbb{R}^3$  generado por  $\{(1, 2, 1)\}$ .

**Ejercicio 67:** Calcula las ecuaciones cartesianas del subespacio vectorial  $\langle\langle(1, 2, 3, 1), (1, 1, 1, 1), (3, 5, 7, 3)\rangle\rangle \subseteq \mathbb{Q}^4$ .

**Ejercicio 68:** Consideremos los subespacios vectoriales de  $\mathbb{R}^4$ ,  $E_1 = \langle\langle(1, 1, 1, 1), (1, -1, 1, -1)\rangle\rangle$  y  $E_2 = \langle\langle(1, 2, 0, 2), (1, 2, 1, 2), (3, 1, 3, 1)\rangle\rangle$ .

- Calcula una base de  $E_1 + E_2$ .
- Calcula las ecuaciones cartesianas de  $E_1 + E_2$ .
- Calcula las ecuaciones cartesianas de  $E_1 \cap E_2$ .
- Calcula una base de  $E_1 \cap E_2$ .

**Ejercicio 69:** Dada la aplicación lineal  $f : \mathbb{Z}_5^4 \rightarrow \mathbb{Z}_5^3$  definida por  $f(x, y, z, t) = (x+y, x+z, 2x+y+z)$ , calcula una base para su núcleo.

**Maxima 45:** Calculemos las ecuaciones cartesianas de  $U = \langle\langle(1, 1, 2), (1, -1, 0)\rangle\rangle \subseteq \mathbb{Q}^3$ . Sus ecuaciones paramétricas respecto de la base usual son

$$\left. \begin{aligned} x &= \lambda + \mu \\ y &= \lambda - \mu \\ z &= 2\lambda \end{aligned} \right\}.$$

La matriz ampliada de este sistema con incógnitas en los parámetros  $\lambda$  y  $\mu$  es

```
(%i1) A:matrix([1,1,x],[1,-1,y],[2,0,z]);
```

```
(%o1)
```

$$\begin{pmatrix} 1 & 1 & x \\ 1 & -1 & y \\ 2 & 0 & z \end{pmatrix}$$

Como su rango debe ser dos, su determinante es cero.

```
(%i2) determinant(A);
```

```
(%o2)
```

$$-2z + 2y + 2x$$

Así la ecuación cartesiana de  $U$  es  $x + y - z = 0$ .

Esta ecuación también la podemos encontrar haciendo operaciones elementales por filas en  $A$ . Primero extraemos la matriz de coeficientes. Para ello eliminamos la última columna de  $A$ .

```
(%i3) C:submatrix(A,3);
```

```
(%o3)
```

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 2 & 0 \end{pmatrix}$$

Para guardar traza de la operaciones elementales que hacemos en  $C$  para obtener su forma triangular reducida, le añadimos al final la matriz identidad.

```
(%i4) M:addcol(C,ident(3));
```

```
(%o4)
```

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ahora triangularizamos y nos quedamos con las últimas columnas, que forman una matriz regular con las operaciones elementales para que  $C$  alcance su forma reducida for filas.

```
(%i5) triangularize(M);
```

```
(%o5)
```

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & -2 & 0 & 2 & -1 \\ 0 & 0 & -2 & -2 & 2 \end{pmatrix}$$

```
(%i6) P:submatrix(% ,1,2);
```

```
(%o6)
```

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & -1 \\ -2 & -2 & 2 \end{pmatrix}$$

Aplicamos estas operaciones por filas a la matriz inicial y obtenemos en las últimas filas las ecuaciones (en esta caso sólo en la última, pues hay una).

```
(%i7) P.A;
```

```
(%o7)
```

$$\begin{pmatrix} 2 & 0 & z \\ 0 & -2 & 2y - z \\ 0 & 0 & 2z - 2y - 2x \end{pmatrix}$$

Si vemos  $\mathbf{U}$  dentro de  $\mathbb{Z}_2^3$ , al ser  $(1, 1, 2) = (1, -1, 0) = (1, 1, 0)$ , tenemos que las ecuaciones paramétricas ahora son

$$\left. \begin{array}{l} x = \lambda \\ y = \lambda \\ z = 0 \end{array} \right\}.$$

Así la matriz ampliada de este sistema es

$$\begin{pmatrix} 1 & x \\ 1 & y \\ 0 & z \end{pmatrix},$$

por lo que una de las ecuaciones,  $z = 0$ , ya la tenemos. Al ser la dimensión de  $\mathbf{U}$  uno, necesitamos una ecuación más, que viene de imponer que el determinante de  $\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}$  es cero (el rango de la matriz ampliada es uno), obteniendo  $x - y = 0$ .

Podemos también utilizar operaciones elementales por filas para llegar a la mismas ecuaciones. En este caso no vamos a utilizar `triangularize`, pues se ve claramente qué operación tenemos que hacer.

```
(%i5) A:matrix([1,x],[1,y],[0,z]);
```

```
(%o5)
```

$$\begin{pmatrix} 1 & x \\ 1 & y \\ 0 & z \end{pmatrix}$$

```
(%i5) rowop(A,2,1,1);
```

```
(%o5)
```

$$\begin{pmatrix} 1 & x \\ 0 & y - x \\ 0 & z \end{pmatrix}$$

Obtenemos también que las ecuaciones de  $\mathbf{U}$  son

$$\left. \begin{array}{l} x + y = 0 \\ z = 0 \end{array} \right\}.$$

**Maxima 46:**

Sea  $\mathbf{U}$  el subespacio de  $\mathbb{R}^4$  generado por  $\{(1, 1, 1, 1), (1, 2, 3, 1), (1, 0, -1, 1)\}$ . Calculemos sus ecuaciones cartesianas respecto de la base  $\mathbf{B} = \{(1, 1, 1, 1), (0, 1, 1, 1), (0, 0, 1, 1), (0, 0, 0, 1)\}$ .

```
(%i1) modulus:false$
```

```
(%i2) A:matrix([1,1,1,1],[1,2,3,1],[1,0,-1,1])$
(%i3) triangularize(A);
```

```
(%o3) 
$$\begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```

$\{(1,0,-1,1), (0,2,4,0)\}$  es una base de  $U$ . Calculamos ahora las coordenadas de estos vectores respecto de la base  $B$ .

```
(%i4) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]
+t*[0,0,0,1]-[1,0,-1,1],[x,y,z,t]);
```

```
(%o4) [[x = 1, y = -1, z = -1, t = 2]]
```

```
(%i5) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]
+t*[0,0,0,1]-[0,2,4,0],[x,y,z,t]);
```

```
(%o5) [[x = 0, y = 2, z = 2, t = -4]]
```

```
(%i6) J:matrix([1,-1,-1,2],[0,2,2,-4],[x,y,z,t]);
```

```
(%o6) 
$$\begin{pmatrix} 1 & -1 & -1 & 2 \\ 0 & 2 & 2 & -4 \\ x & y & z & t \end{pmatrix}$$

```

Al exigir que la matriz  $J$  tenga rango 2 obtenemos que los siguientes determinantes deben de valer cero.

```
(%i7) determinant(matrix([1,-1,-1],[0,2,2],[x,y,z]));
```

```
(%o7) 2z - 2y
(estilo lo podíamos haber obtenido con determinant(submatrix(J,4));)
```

```
(%i8) determinant(matrix([1,-1,2],[0,2,-4],[x,y,t]));
```

```
(%o8) 4y + 2t
```

Las ecuaciones cartesianas de  $U$  respecto de  $B$  son

$$\left. \begin{array}{l} z - y = 0 \\ y + t = 0 \end{array} \right\}.$$

**Maxima 47:**

Sean  $U = \{(x, y, z, t) \in \mathbb{Z}_5^4 \mid x + y + z + t = 0, x + 2t = 0\}$  y  $W = \{(x, y, z, t) \in \mathbb{Z}_5^4 \mid 4y + 4z + t = 0, x + 4y = 0\}$ . Calculemos una base de la intersección.

```
(%i1) modulus:5$
```

```
(%i2) M:matrix([1,1,1,1],[1,0,0,2],[0,4,4,1],[1,4,0,0])$
```

```
(%i3) nullspace(M);
```

```
(%o3) span 
$$\left( \begin{pmatrix} -2 \\ -2 \\ -2 \\ 1 \end{pmatrix} \right)$$

```

Una base es de la intersección es  $\{(3, 3, 3, 1)\}$ .

**Maxima 48:**

Sea  $f: \mathbb{Q}^4 \rightarrow \mathbb{Q}^3$ ,  $f(x, y, z, t) = (x + y, z + t, x + y + z + t)$ . Calculemos una base de  $N(f)$ .

```
(%i1) modulus:false4  
(%i2) N:matrix([1,1,0,0],[0,0,1,1],[1,1,1,1])$  
(%i3) nullspace(N);
```

```
(%o3) span  $\left( \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \right)$ 
```

Por tanto una base de  $N(f)$  es  $\{(-1, 1, 0, 0), (0, 0, 1, -1)\}$ .

## Diagonalización de matrices

### 1. Matrices diagonalizables

Una matriz diagonal es una matriz cuadrada que tiene todas sus entradas nulas, salvo eventualmente las de la diagonal. Una matriz cuadrada  $A$  es diagonalizable si existen una matriz diagonal  $D$  y una matriz regular  $P$  tales que  $A = PDP^{-1}$ .

La diagonalización de matrices es útil para el cálculo de potencias grandes de una matriz, ya que

$$A^r = (PDP^{-1})^r = PDP^{-1}PDP^{-1} \dots PDP^{-1} = PD^rP^{-1}.$$

En adelante,  $A$  representará una matriz cuadrada de orden  $n \times n$  sobre un cuerpo  $K$ .

Un elemento  $\lambda \in K$  es un valor propio de  $A$  si existe  $x \in K^n \setminus \{(0, \dots, 0)\}$  tal que  $Ax = \lambda x$ . En tal caso diremos que  $x$  es un vector propio asociado al valor propio  $\lambda$ .

**Teorema de caracterización de los valores propios.** Un elemento  $\lambda \in K$  es un valor propio de  $A$  si y sólo si  $|A - \lambda I_n| = 0$ .

Así los valores propios de  $A$  son las raíces del polinomio  $|A - \lambda I_n| \in K[\lambda]$ , que se conoce como polinomio característico de  $A$ , y lo denotaremos por  $p_A(\lambda)$ . Nótese que  $\text{gr}(p_A(\lambda)) = n$ .

**Ejercicio 70:** Calcula el polinomio característico y los valores propios de  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$ .

#### Propiedades.

- 1) Si  $A$  es una matriz triangular, entonces sus valores propios son los valores de la diagonal.
- 2) Los valores propios de  $A$  y  $A^t$  coinciden.
- 3)  $|A| = 0$  si y sólo si  $0$  es un valor propio de  $A$ .
- 4) Si  $A$  es regular y  $\lambda$  es un valor propio de  $A$ , entonces  $\lambda^{-1}$  lo es de  $A^{-1}$ .
  - Si  $\lambda$  es un valor propio de  $A$ , entonces

$$V(\lambda) = \{x \in K^n \text{ tales que } (A - \lambda I_n)x = 0\},$$

(en este caso  $0 = (0, \dots, 0) \in K^n$ ) es un subespacio vectorial de  $K^n$ . Dicho subespacio lo llamamos subespacio vectorial propio asociado al valor propio  $\lambda$ .

**Ejercicio 71:** Encuentra los subespacios propios asociados a los valores propios de  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$ .

Sean  $\lambda_1, \dots, \lambda_k$  los valores propios de la matriz  $A$ . A la multiplicidad de la raíz  $\lambda_i$  de  $p_A(\lambda)$  la llamaremos multiplicidad algebraica de  $\lambda_i$ , mientras que la dimensión de  $V(\lambda_i)$  es la multiplicidad geométrica de  $\lambda_i$ .

**Ejercicio 72:** Calcula las multiplicidades algebraicas y geométricas de los valores propios de  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$ .

- La multiplicidad geométrica de un valor propio es menor o igual que su multiplicidad algebraica.

**Criterio de diagonalización.**  $A$  es diagonalizable si, y sólo si, la suma de las multiplicidades algebraicas de los valores propios de  $A$  es  $n$  y además para todo valor propio las multiplicidades algebraica y geométrica coinciden.

- Toda matriz cuadrada y simétrica con coeficientes en  $\mathbb{R}$  es diagonalizable.

## 2. Método para diagonalizar una matriz

- 1) Calculamos  $p_A(\lambda)$ , sus raíces  $\lambda_1, \dots, \lambda_k$  y sus multiplicidades algebraicas,  $m_1, \dots, m_k$ .
- 2) Si  $m_1 + \dots + m_k \neq n$ ,  $A$  no es diagonalizable.
- 3) En caso contrario, para cada  $\lambda_i$ , calculamos el subespacio propio  $V(\lambda_i)$  y su dimensión. Si dicha dimensión no coincide con  $m_i$  para algún  $i$ , entonces  $A$  no es diagonalizable.
- 4) Llegado este paso, la matriz  $A$  es diagonalizable y  $D$  es la matriz que tiene en la diagonal  $m_1$  entradas  $\lambda_1$ ,  $m_2$  entradas  $\lambda_2$ , y así hasta  $m_k$  entradas  $\lambda_k$ . La matriz de paso  $P$  se construye colocando en las primeras  $m_1$  columnas una base de  $V(\lambda_1)$ , a continuación en las siguientes  $m_2$  columnas una base de  $V(\lambda_2)$ , y así hasta que colocamos en las últimas  $m_k$  columnas una base de  $V(\lambda_k)$ .

**Ejercicio 73:** Diagonaliza la matriz  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$ .

**Ejercicio 74:** Diagonaliza la matriz

$$\begin{pmatrix} 2 & 0 & 0 \\ -15 & -4 & 3 \\ -35 & -14 & 9 \end{pmatrix} \in \mathcal{M}_{3 \times 3}(\mathbb{R}).$$

**Ejercicio 75:** Demuestra que  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  con coeficientes reales no es diagonalizable.

**Maxima 49:** Sea

```
(%i1) A:matrix([-1,3,3],[0,2,0],[3,-3,-1]);
```

```
(%o1)  $\begin{pmatrix} -1 & 3 & 3 \\ 0 & 2 & 0 \\ 3 & -3 & -1 \end{pmatrix}$ 
```

El comando `eigenvectors` nos proporciona toda la información para saber si es diagonalizable.

```
(%i2) eigenvectors(A);
```

```
(%o2) [[[-4,2],[1,2]], [[[1,0,-1],[1,0,1],[0,1,-1]]]]
```

La salida nos dice que los valores propios son  $-4$  y  $2$ , con multiplicidades  $1$  y  $2$ , respectivamente. Además nos da bases para  $V(-4)$ ,  $\{(1, 0, -1)\}$  y  $V(2)$ ,  $\{(1, 0, 1), (0, 1, -1)\}$ . Como las multiplicidades algebraicas y geométricas coinciden, y suman  $3$ ,  $A$  es diagonalizable.

La matriz de paso se calcula poniendo dichas bases una a continuación de la otra en columnas.

```
(%i3) P:matrix([1,1,0],[0,0,1],[-1,1,-1]);
```



$$(\%o3) \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}$$

Comprobamos que efectivamente están bien hechos los cálculos:

(%i4) `P^(-1).A.P;`

$$(\%o4) \quad \begin{pmatrix} -4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Podríamos también haber hecho los cálculos paso a paso, calculando primero el polinomio característico de  $A$ .

(%i5) `charpoly(A,x);`

$$(\%o5) \quad (-x-1)^2(2-x) - 9(2-x)$$

Para ver los valores propios, lo factorizamos.

(%i6) `factor(%);`

$$(\%o6) \quad -(x-2)^2(x+4)$$

Y para calcular una base de por ejemplo  $V(2)$  utilizamos `nullspace`.

(%i7) `nullspace(A-2*ident(3));`

$$(\%o7) \quad \text{span} \left( \begin{pmatrix} -3 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix} \right)$$

Maxima 50:

Veamos para qué valores de  $a$  la siguiente matriz es diagonalizable.

(%i1) `A:matrix([0,1,1],[1,0,-1],[0,0,a]);`

$$(\%o1) \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & a \end{pmatrix}$$

Calculamos su polinomio característico:

(%i2) `charpoly(A,x);`

$$(\%o2) \quad (a-x)x^2 + x - a$$

(%i3) `factor(%);`

$$(\%o3) \quad -(x-1)(x+1)(x-a)$$

Por lo que si  $a \notin \{-1, 1\}$ , la matriz es diagonalizable.

(%i4) `eigenvectors(A);`

$$(\%o4) \quad [[[a, 1, -1], [1, 1, 1]], [[1, -1, a+1], [1, 1, 0]], [[1, -1, 0]]]$$

Veamos qué ocurre para  $a = 1$ .

(%i5) `B:subst(1,a,A);`

$$(\%o5) \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

(%i6) `eigenvectors(B);`

(%o6) `[[[-1, 1], [1, 2]], [[[1, -1, 0]], [[1, 0, 1], [0, 1, -1]]]]`

Podemos observar que en este caso la matriz también es diagonalizable.

Por último, para  $a = -1$ , tenemos:

(%i7) `C:subst(-1,a,A);`

(%o7) 
$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

(%i8) `eigenvectors(C);`

(%o8) `[[[1, -1], [1, 2]], [[[1, 1, 0]], [[1, -1, 0]]]]`

lo que nos dice que en este caso la matriz no es diagonalizable, pues la multiplicidad algebraica del valor propio 2 es mayor que la geométrica.

## Índice alfabético

- adjunto, 23
- algoritmo de Euclides, 11, 17
- algoritmo extendido de Euclides, 13, 19
- anillo, 16
  - conmutativo, 16
- aplicación, 7
  - biyectiva, 7
  - composición, 8
  - identidad, 8
  - inversa, 8
  - invertible, 8
  - invertible a derecha, 8
  - invertible a izquierda, 8
  - inyectiva, 7
  - lineal, 31
  - sobreyectiva, 7
- base, 28
- cardinal, 5
- clase de equivalencia, 6
- cociente, 10, 17
- codominio, 7
- coeficiente líder, 16
- coeficientes de un sistema de ecuaciones, 36
- combinación lineal, 26
- composición de aplicaciones, 8
- congruente, 14
- conjunto, 4
  - cociente, 6
  - de partes, conjunto
    - potencia, 4
  - diferencia, 4
  - imagen de una aplicación, 7
  - intersección, 4
  - unión, 4
  - vacío, 4
- coordenadas, 28
- cuerpo, 16
- dimensión, 28
- divisor, 10
- dominio, 7
- ecuación en congruencias, 14
- ecuaciones cartesianas, 38
- ecuaciones de cambio de base, 29
- ecuaciones de una aplicación lineal, 32
- ecuaciones implícitas, 38
- ecuaciones paramétricas, 31
- elemento inverso, 10
- elemento neutro, 10
- epimorfismo, 31
- escalar, 26
- espacio vectorial, 26
- espacio vectorial cociente, 34
- espacios vectoriales isomorfos, 32
- expresión matricial de un sistema, 36
- Fórmula de Cramer, 38
- grado de un polinomio, 16
- homomorfismo, 31
- igualdad
  - de conjuntos, 4
- imagen, 7
- irreducible, 10
- isomorfismo, 31
- mínimo común múltiplo, 11, 17
- máximo común divisor, 11, 17
- múltiplo, 10
- matriz, 22
  - adjunta, 24
  - ampliada de un sistema, 36
  - cuadrada, 22
  - de coeficientes de un sistema, 36
  - de términos independientes de un sistema, 36
  - diagonal, 41
  - diagonalizable, 41
  - identidad, 24
  - incógnita de un sistema, 36
  - regular, 24
  - traspuesta, 23
- matriz asociada a una aplicación lineal, 32
- matriz de cambio de base, 29
- monomorfismo, 31
- multiplicidad, 18
  - algebraica, 41
  - geométrica, 41

opuesto, 10

partición, 7

pertenece, 4

polinomio, 16

- característico, 41
- irreducible, 16
- monico, 16

Primer teorema de isomorfía, 34

primo, 10

primos relativos, 10

producto de matrices, 22

producto por escalares, 26

propiedad cancelativa, 10

raíz de un polinomio, 18

- múltiple, 18
- simple, 18

rango de una matriz, 35

relación

- binaria, 6
- equivalencia, 6
- reflexiva, 6
- simétrica, 6
- transitiva, 6

resto, 10, 17

Segundo teorema de isomorfía, 34

sistema compatible, 36

- determinado, 36
- indeterminado, 36

sistema de ecuaciones lineales, 36

sistema incompatible, 36

sistemas equivalentes, 36

solución de un sistema de ecuaciones, 36

subconjunto, 4

subespacio propio, 41

subespacio vectorial, 26

- generado por un conjunto, 27

subespacios complementarios, 27

suma de matrices, 22

suma directa, 27

término independiente, 36

término líder, 16

Teorema de Bézout, 10

Teorema de Rouché-Frobenius, 37

Teorema fundamental de la aritmética, 11

unidad, 16

valor absoluto, 10

valor propio, 41

vector, 26

vector propio, 41

vectores

- linealmente dependientes, 28
- linealmente independientes, 28