TEMA 1

Conjuntos, aplicaciones y relaciones

1.1 Conjuntos

Vamos a iniciar este primer tema con una aproximación muy intuitiva al concepto de conjunto. La primera idea que debemos destacar es que un conjunto está determinado por sus elementos.

Dado un objeto x y un conjunto X, la pregunta *¿es x elemento de X?* debe tener respuesta unívoca.

Observación. Que la pregunta anterior tenga respuesta no significa que la conozcamos. Por ejemplo, el número π no se supo hasta el siglo XIX si era racional o no.

Utilizamos los símbolos $\in$ y $\notin$ para indicar pertenencia y no pertenencia. Así $x \in X$ significa que x pertenece a (o es elemento de) X.

Definición 1. Hay un conjunto especial, el conjunto que no tiene elementos. Los llamamos *conjunto vacío*, y lo notamos $\varnothing = \{\}$. Observemos que la pregunta "¿es x elemento de $\varnothing$?" siempre tiene una respuesta inequívoca, y la respuesta es no.

Definición 2. El siguiente concepto que vamos a presentar es el concepto de subconjunto. Dados dos conjuntos X e Y, decimos que X es un *subconjunto* de (o está incluido en) Y si todo elemento de X es elemento de Y. Lo notamos $X \subseteq Y$. Se emplea además la notación $X \subsetneq Y$ o $X \subset Y$ para indicar que X es subconjunto de Y y que no son iguales. Es lo que se llama inclusión estricta.

Ejemplo 3.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

La presentación que acabamos de hacer de los conceptos de conjunto y subconjunto nos conduce a las propiedades que enumeramos a continuación

Proposición 4. *Si X, Y y Z son conjuntos cualesquiera, se tiene*

1. $\varnothing \subseteq X$;
2. $X \subseteq X$ *(esta propiedad recibe el nombre de reflexiva);*
3. *si* $X \subseteq Y$ *e* $Y \subseteq X$, *entonces* $X = Y$ *(esta propiedad recibe el nombre de antisimétrica);*
4. *si* $X \subseteq Y$ *e* $Y \subseteq Z$, *entonces* $X \subseteq Z$ *(y esta propiedad recibe el nombre de transitiva).*

Definición 5. Se define el conjunto potencia de X como el conjunto cuyos elementos son los subconjuntos de X, es decir

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}$$

Este conjunto también se llama partes de X.

Definición 6. Dados $A, B \subseteq X$ definimos los siguientes subconjuntos de X:

$$\begin{aligned} A \cap B &= \{x \in X \mid x \in A \text{ y } x \in B\} \\ A \cup B &= \{x \in X \mid x \in A \text{ o } x \in B\} \\ A \setminus B &= \{x \in X \mid x \in A \text{ y } x \notin B\} = \{x \in A \mid x \notin B\} \\ \overline{A} &= X \setminus A \end{aligned}$$

Proposición 7. *Sean $A, B, C \subseteq X$. Entonces*

- $A \subseteq A \cup B$, $A \cap B \subseteq A$,
- $A \cap B = B \cap A$, $A \cap (B \cap C) = (A \cap B) \cap C$,
- $A \cap \varnothing = \varnothing$, $A \cap X = A$,
- $A \cup B = B \cup A$, $A \cup (B \cup C) = (A \cup B) \cup C$,
- $A \cup \varnothing = A$, $A \cup X = X$,
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
- $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$, $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$,
- $\overline{\overline{A}} = A$, $A \setminus B = A \setminus (A \cap B)$.

Definición 8. Sean X, Y dos conjuntos. Se define el producto cartesiano de X e Y como el conjunto cuyos elementos son pares ordenados en los que el primer elemento pertenece a X y el segundo a Y, es decir,

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

Si $n \geq 2$ se define recursivamente $X^n = X^{n-1} \times X$.

1.2 Relaciones de equivalencia

Definición 9. Una relación binaria R en un conjunto X es un subconjunto de n$X \times X$, es decir, $R \subseteq X \times X$. Utilizamos la notación xRy para expresar que $(x, y) \in R$.

Definición 10. Algunas propiedades de las relaciones binarias tienes nombres específicos. Sea R una relación binaria en X.

- La relación se dice *reflexiva* si para cualquier $x \in X$ tenemos que xRx.
- La relación es *simétrica* si para cualesquiera $x, y \in X$, xRy implica yRx.
- La relación es *antisimétrica* si para cualesquiera $x, y \in X$, xRy e yRx implica $x = y$.
- La relación se dice *transitiva* si para cualesquiera $x, y, z \in X$, si xRy e yRz entonces xRz.

Definición 11. Una relación binaria reflexiva, simétrica y transitiva se llama *relación de equivalencia*. Si la relación binaria es reflexiva, antisimétrica y transitiva, recibe el nombre de *relación de orden.*

Definición 12. Sea X un conjunto y R una relación de equivalencia sobre X. Sea además $x \in X$. Se define la *clase de equivalencia* de x como

$$[x]_R = \{y \in X \mid xRy\}$$

Si no hay confusión con la relación se suele prescindir de la R en la notación, es decir, $[x] = [x]_R$.

Proposición 13. *Si R es una relación de equivalencia sobre un conjunto X y $x, y \in X$, tenemos*

$$xRy \iff [x] \cap [y] \neq \varnothing \iff [x] = [y]$$

Demostración. Supongamos que xRy; si $z \in [x]$ entonces xRz, por las propiedades simétrica y transitiva tenemos que yRz, por lo que $z \in [y]$. Hemos demostrado que $[x] \subseteq [y]$, análogamente se demuestra la otra inclusión y por tanto la igualdad.

Es evidente que $[x] = [y]$ implica que $[x] \cap [y] \neq \varnothing$, ya que las clases son no vacías por la propiedad reflexiva.

Finalmente si $z \in [x] \cap [y]$ tenemos que xRz y yRz. De nuevo por las propiedades simétrica y transitiva tenemos que xRy.

Hemos hecho una demostración circular. □

Observación 14. En primer lugar todo elemento está en al menos una clase de equivalencia. En segundo lugar dado $x \in X$, existe una y sólo una clase de equivalencia conteniendo a x.

Definición 15. Dada una relación de equivalencia R sobre X se define el conjunto cociente de X con respecto a R como

$$X/R = \{[x]_R \mid x \in X\}$$

¿Qué significa describir un conjunto cociente? Si X es finito podemos enumerar todas las clases de equivalencia y decir a su vez qué elementos de X están en cada una de ellas. Si X no es finito, es necesario encontrar otra forma de describirlo.

Definición 16. Sea R una relación de equivalencia sobre un conjunto X. Un *conjunto minimal de representantes* para R es un subconjunto $X_0 \subseteq X$ tal que:

1. todo elemento de X está relacionado con algún elemento de X_0, es decir, para cualquier $x \in X$ existe $y \in X_0$ tal que xRy;
2. dos elementos distintos de X_0 no están relacionados, es decir, si $x, y \in X_0$ y xRy entonces $x = y$.

En este caso podemos describir el conjunto cociente como

$$X/R = \{[x]_R \mid x \in X_0\}$$

Definición 17. Sea X un conjunto y $\mathcal{A} = \{A_i \mid i \in I\} \subseteq \mathcal{P}(X)$ con $\varnothing \notin \mathcal{A}$. Decimos que $\mathcal{A}$ es una partición de X si

1. $X = \bigcup_{i \in I} A_i$,
2. $A_i \neq A_j$ si y sólo si $A_i \cap A_j = \varnothing$.

Ejemplo 18. Si R es una relación de equivalencia sobre X entonces X/R es una partición sobre X.

Teorema 19. *Existe una correspondencia biunívoca entre las particiones sobre X y las relaciones de equivalencia en X.*

Demostración. Ya sabemos que X/R es una partición cuando R es una relación de equivalencia sobre X. Si $\mathcal{A}$ es una partición en X, definimos la relación $R_{\mathcal{A}}$ diciendo que dos elementos de X están relacionados si pertenecen al mismo elemento de la partición. Es sencillo comprobar que esta definición nos da una relación de equivalencia. También es sencillo verificar que el componer estos dos procesos deja invariantes a las relaciones o a las particiones. □

1.3 Relaciones de Orden

Observación 20. Recordemos que una relación $\leqslant$ en un conjunto X se dice *relación de orden* si satisface la propiedades reflexiva, antisimétrica y transitiva.

Observación 21. Si $\leqslant$ es una relación de orden es sencillo comprobar que la relación opuesta ($x \geqslant y \overset{\text{def}}{\iff} y \leqslant x$) también es una relación de orden. Normalmente utilizamos para expresar una relación de orden los siguientes símbolos $\leqslant, \preccurlyeq$, que leemos 'menor o igual que', y también $\geqslant, \succcurlyeq$ que leemos 'mayor o igual que'.

Definición 22 (Orden estricto)**.** Una relación $\prec$ en un conjunto X se dice *relación de orden estricto* si satisface la propiedades:

(a') (ANTIREFLEXIVA) para todo $x \in X$, $x \not\prec x$;

(b') (TRANSITIVA) para cualesquiera $x, y, z \in X$, si $x \prec y$ e $y \prec z$ entonces $x \prec z$.

Proposición 23. *Sea X un conjunto y sean $\leqslant, \prec$ relaciones de orden y orden estricto respectivamente. Entonces*

1. *La relación $x < y \overset{def}{\iff} (x \leqslant y \text{ y } x \neq y)$ es una relación de orden estricto.*
2. *La relación $x \preccurlyeq y \overset{def}{\iff} (x \prec y \text{ o } x = y)$ es una relación de orden.*

Demostración. Sencilla. □

Ejemplo 24. Los ejemplos más conocidos son la relación de orden usual en$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. La relación en $\mathbb{R}$ se define por $x \leq y \overset{\text{def}}{\iff} y - x \in \mathbb{R}_0^+$.

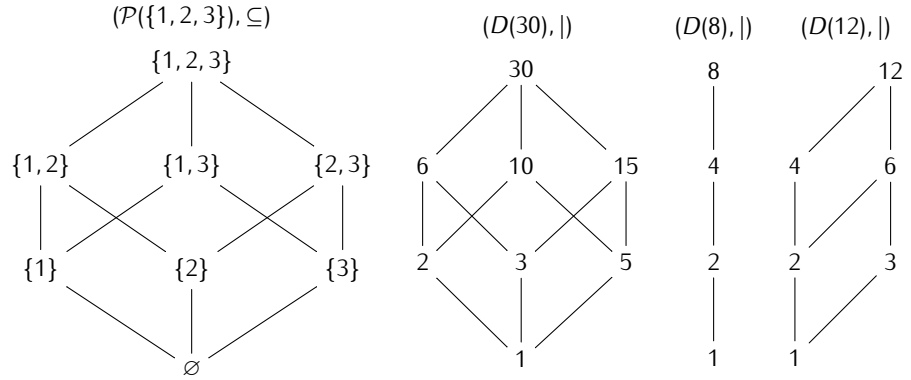
Ejemplo 25. Sea X un conjunto. La relación $\subseteq$ definida en $\mathcal{P}(X)$ es una relación de orden ya que para cualesquiera $A, B, C \subseteq X$ se tiene: $A \subseteq A$; si $A \subseteq B$ y $B \subseteq A$ entonces $A = B$; si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.

Ejemplo 26. La divisibilidad en $\mathbb{N}$ otra relación de orden. De hecho, ya que $a = a1$ tenemos que $a \mid a$ para todo $a \in \mathbb{N}$ (reflexiva); por otra parte, si $a = br$ y $b = as$ entonces $1 = rs$ y $r = s = 1$, de donde $a \mid b$ y $b \mid a$ implican que $a = b$ (antisimétrica); finalmente, si $b = ar$ y $c = bs$ entonces $c = a(rs)$, de donde $a \mid b$ y $b \mid c$ implican $a \mid c$ (transitiva).

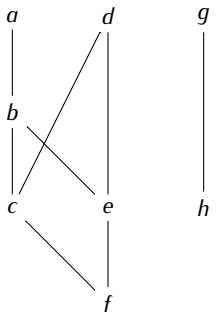
Destacamos $D(n) = \{a \in \mathbb{N} \,;\, a \mid n\} \subseteq \mathbb{N}$. Si no se indica lo contrario consideraremos $D(n)$ como un conjunto ordenado con respecto a la relación de divisibilidad, es decir, $(D(n), |)$ será uno de los ejemplos más importantes a tener en cuenta en este curso.

Definición 27. Sea $(X, \leqslant)$ un conjunto ordenado y sean $x, y \in X$. Decimos que y *cubre* a x si $x < y$ y no existe ningún otro elemento entre ellos, es decir, $x < y$ y no existe $u \in X$ tal que $x < u < y$.

Definición 28. El diagrama de Hasse de $(X, \leqslant)$ es un grafo dirigido cuyos vértices son los elementos de X y existe línea ascendente de x en y si y sólo si y cubre a x



El diagrama



(1)

produce las siguientes desigualdades además de las que vienen de la propiedad reflexiva: $\{b \leqslant a, c \leqslant b, c \leqslant a, c \leqslant d, e \leqslant b, e \leqslant a, e \leqslant d, f \leqslant a, f \leqslant b, f \leqslant c, f \leqslant d, f \leqslant e, h \leqslant g\}$.

Definición 29. Un elemento $x \in X$ se dice *maximal* si no existe $y \in X$ tal que $x < y$. Análogamente se definen los elementos minimales, $x \in X$ es *minimal* si no existe $y \in X$ tal que $y < x$.

En el ejemplo dado por el diagrama de Hasse (1) los elementos a, d, g son todos los maximales, mientras que los elementos f, h son los únicos minimales. Por otra parte, en $\mathbb{N}$ con el orden usual el único elemento minimal es el 0, mientras que no hay elementos maximales. $\mathbb{Z}$ no tiene maximales ni minimales.

Definición 30. Un elemento $x \in X$ se dice *máximo* si para todo $y \in X$ $y \leqslant x$. Análogamente se define el *mínimo* de un conjunto ordenado. Es inmediato comprobar que el máximo y el mínimo son únicos en caso de existir.

Definición 31. Sea $Y \subseteq X$. Decimos que x es una *cota superior* para Y si para cualquier $y \in Y$, $y \leqslant x$. Análogamente se definen las *cotas inferiores.*

Definición 32. Sea $Y \subseteq X$ y sea S el conjunto de las cotas superiores de Y. Si S tiene mínimo dicho elemento recibe el nombre de *supremo* de Y. Análogamente se define el *ínfimo*, como el máximo de las cotas inferiores.

Proposición 33. *$y \in Y$ es el máximo si y sólo si y es el supremo de Y e $y \in Y$. Análogamente, $y \in Y$ es el mínimo si y sólo si y es el ínfimo de Y e $y \in Y$.*

Definición 34. Una relación de orden $\leqslant$ sobre un conjunto X se dice que es un *orden total* si para cualesquiera $x, y \in X$ se tiene $x \leqslant y$ o $y \leqslant x$. En este case se dice que $(X, \leqslant)$ es un conjunto totalmente ordenado o una *cadena*. Los órdenes totales también se llaman *órdenes lineales.*

Proposición 35. *Todo subconjunto de un conjunto totalmente ordenado es totalmente ordenado.*

Observación 36. Es inmediato comprobar que en una cadena finita existe mínimo y máximo.

Definición 37. Una relación de orden $\leqslant$ sobre un conjunto X se dice que es un *buen orden* si todo subconjunto $Y \subseteq X$ no vacío tiene mínimo. En este caso se dice que $(X, \leqslant)$ es un conjunto bien ordenado.

Proposición 38. *Todo buen orden es un orden total.*

Demostración. Basta observar que el conjunto $\{x, y\}$ tiene mínimo para cualesquiera $x, y \in X$. □

$(X_1, \leqslant_1)$ y $(X_2, \leqslant_2)$ son dos conjuntos ordenados.

Definición 39. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Se define el *orden producto* como

$$(x_1, x_2) \leqslant_1 \times \leqslant_2 (y_1, y_2) \text{ si y sólo si } x_1 \leqslant_1 y_1 \text{ y } x_2 \leqslant_2 y_2.$$

Proposición 40. *$(X_1 \times X_2, \leqslant_1 \times \leqslant_2)$ es un conjunto ordenado.*

Proposición 41. *(x_1, x_2) es un máximo (resp. mínimo) de $(X_1 \times X_2, \leqslant_1 \times \leqslant_2)$ si y sólo si x_1 es máximo (resp. mínimo) de X_1 y x_2 es máximo (resp. mínimo) de X_2.*

Proposición 42. *(x_1, x_2) es un elemento maximal (resp. minimal) de $(X_1 \times X_2, \leqslant_1 \times \leqslant_2)$ si y sólo si x_1 es elemento maximal (resp. minimal) de X_1 y x_2 es maximal (resp. minimal) en X_2.*

Definición 43. Sean $(X_1, \leqslant_1), \ldots, (X_n, \leqslant_n)$ conjuntos ordenados. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Se define el *orden lexicográfico* mediante la siguiente equivalencia

$$(x_1, x_2) \preccurlyeq_{\text{lex}} (y_1, y_2) \overset{\text{def}}{\iff} \begin{cases} x_1 <_1 y_1 & \text{o} \\ x_1 = y_1 \text{ y } x_2 \leqslant_2 y_2. \end{cases}$$

Por recurrencia podemos extender esta definición a tamaño n. Si $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in X_1 \times \cdots \times X_n$,

$$(x_1, \ldots, x_n) \preccurlyeq_{\text{lex}} (y_1, \ldots, y_n) \overset{\text{def}}{\iff}$$
$$\overset{\text{def}}{\iff} \begin{cases} x_1 <_1 y_1 & \text{o} \\ x_1 = y_1 \text{ y } (x_2, \ldots, x_n) \preccurlyeq_{\text{lex}} (y_2, \ldots, y_n). \end{cases}$$

Proposición 44. *$(X_1 \times \cdots \times X_n, \preccurlyeq_{lex})$ es un conjunto ordenado. Además, si $\leqslant_1, \cdots \leqslant_n$ son órdenes totales (resp. buenos) entonces $\preccurlyeq_{lex}$ es un orden total (resp. bueno).*

1.4 Aplicaciones

Definición 45. Una aplicación f es una terna $f = (X, Y, G)$ donde

1. X es un conjunto llamado dominio (origen, inicio),
2. Y es un conjunto llamado codominio (destino, fin),
3. $G \subseteq X \times Y$ satisfaciendo que para todo $x \in X$ existe un único $f(x) \in Y$ tal que $(x, f(x)) \in G$.

La aplicación anterior se denota

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned}$$

El conjunto de las aplicaciones de X en Y se denota Y^X

Ejemplo 46. Si X es un conjunto, la aplicación identidad en X se define como sigue,

$$\begin{aligned} \mathrm{id}_X : X &\longrightarrow X \\ x &\longmapsto \mathrm{id}_X(x) = x, \end{aligned}$$

es decir, $G = \{(x, x) \mid x \in X\} \subseteq X \times X$.

Definición 47. Si $f : X \to Y$ es una aplicación, se emplea la notación $\operatorname{im} f = \{f(x) \mid x \in X\} \subseteq Y$.

Ejemplo 48. Sea $f : X \to Y$ una aplicación. Definimos una relación R_f asociada a f de la siguiente forma: $xR_f y \iff f(x) = f(y)$. Es sencillo comprobar que R_f es una relación de equivalencia. El cociente se denota X/f. La clase de un elemento x suele denotarse $[x]_f$.

Definición 49. Sean $f : X \to Y$ y $g : Y' \to Z$ dos aplicaciones tales que $\operatorname{im} f \subseteq Y'$. Se define la composición de f con g como

$$\begin{aligned} g \circ f = gf : X &\longrightarrow Z \\ x &\longmapsto gf(x) = g(f(x)). \end{aligned}$$

Proposición 50. *Sean $f : X \to Y$, $g : Y' \to Z$ y $h : Z' \to W$ aplicaciones tales que $\operatorname{im} f \subseteq Y'$ e $\operatorname{im} g \subseteq Z'$. Se tienen las siguientes igualdades,*

1. $h(gf) = (hg)f$,
2. $f\,\mathrm{id}_X = f$,
3. $\mathrm{id}_Y\, f = f$.

Definición 51. Una aplicación $f : X \to Y$ se dice inyectiva si $f(x) = f(y)$ implica que $x = y$, es decir, elementos distintos de X tienen imágenes distintas. Se dice que f es sobreyectiva si $\operatorname{im} f = Y$.

Proposición 52. *Sea $f : X \to Y$ una aplicación.*

1. *f es inyectiva si y sólo si existe $g : Y \to X$ tal que $gf = \mathrm{id}_X$,*
2. *f es sobreyectiva si y sólo si existe $g : Y \to X$ tal que $fg = \mathrm{id}_Y$.*

Definición 53. Una aplicación f se dice biyectiva si es tanto inyectiva como sobreyectiva. Si $f : X \to Y$ es una aplicación biyectiva decimos que X e Y son biyectivos.

Ejemplo 54. Si X, Y, Z son tres conjuntos cualesquiera, es muy sencillo comprobar que $(X \times Y) \times Z$ y $X \times (Y \times Z)$ son biyectivos. Además son biyectivos con el conjunto $X \times Y \times Z$ de las ternas ordenadas. Por este motivo solemos identificar dichos conjuntos.

Proposición 55. *Una aplicación $f : X \to Y$ es biyectiva si y sólo si existe $g : Y \to X$ tal que $gf = \mathrm{id}_X$ y $fg = \mathrm{id}_Y$. En este caso la aplicación g es única y se denota f^{-1}.*

Demostración. En vista de la Proposición 52 existen $g_1, g_2 : Y \to X$ tales que $g_1 f = \mathrm{id}_X$ y $f g_2 = \mathrm{id}_Y$. Dado que

$$g_1 = g_1\,\mathrm{id}_Y = g_1(fg_2) = (g_1 f)g_2 = \mathrm{id}_X\, g_2 = g_2$$

obtenemos la tesis de la proposición. □

Definición 56. Sea $f : X \to Y$ una aplicación, y sea $A \subseteq X$. La aplicación con dominio A, codominio Y gráfica $x \mapsto f(x)$ se denota $f|_A$, es decir,

$$\begin{aligned} f|_A : A &\longrightarrow Y \\ x &\longmapsto f|_A(x) = f(x), \end{aligned}$$

aunque normalmente se abusa del lenguaje y se representa $f|_A = f$ si no hay riesgo de confusión.

Proposición 57. *f es inyectiva si y sólo si $f|_A$ es inyectiva para cualquier $A \subseteq X$.*

Demostración. Ejercicio. □

Vamos a denotar por $\mathbf{n} = \{0, \dots n-1\}$.

Lema 58. $\mathbf{n}$ *es biyectivo con* $\mathbf{m}$ *si y sólo si* $n = m$.

Demostración. Inducción en n. Para $n = 1$ el resultado es claro. Supongamos que el resultado es cierto para n y que $\mathbf{n+1}$ es biyectivo con $\mathbf{m}$ con f la biyección. Componiendo con la biyección de $\mathbf{m}$ en $\mathbf{m}$ adecuada no perdemos generalidad si suponemos que $f(n) = m-1$. De esta forma $f|_{\mathbf{n}}$ es una biyección de $\mathbf{n}$ en $\mathbf{m-1}$. Por hipótesis de inducción $n = m-1$, de donde $n+1 = m$. □

Definición 59. Un conjunto X se dice finito si es biyectivo con $\mathbf{n}$ para algún n. En este caso se dice que el cardinal de X es n, y se representa

$$|X| = n$$

Proposición 60. *Sean* X, Y *conjuntos y* $A, B \subseteq X$. *Entonces,*

1. $|A \cup B| + |A \cap B| = |A| + |B|$,
2. $|\mathcal{P}(X)| = 2^{|X|}$.
3. $|X \times Y| = |X|\,|Y|$

Teorema 61. *Un conjunto* X *no es finito si y sólo si existe* $Y \subset X$ *tal que* Y *es biyectivo con* X

TEMA 2

Elementos de combinatoria

2.1 Principios generales.

Existen dos principios generales que debemos estudiar para adentrarnos en las técnicas de conteo. Aunque la interpretación más intuitiva de los mismos se refiere a posibilidades de elección dentro de una gama de alternativas, la presentación más algebraica hace referencia a cardinales de conjuntos. La cuenta más simple que podemos analizar es la siguiente.

Proposición 1 (Principio de la suma). *Sean $A, B \subseteq X$ con $A \cap B = \varnothing$. Entonces $|A \cup B| = |A| + |B|$.*

En términos de opciones y elecciones debemos interpretar el principio de la suma de la siguiente forma. Para tomar una decisión tenemos dos alternativas. La primera nos lleva a seleccionar una opción entre n posibles, y la segunda una opción entre m posibles. Si no hay opciones comunes entre ambas alternativas entonces nuestra actuación consiste en decantarnos por una de las $n + m$ opciones totales.

Corolario 2. *Para cualesquiera $A, B \subseteq X$, $|A \cup B| + |A \cap B| = |A| + |B|$.*

Demostración. Basta con escribir $A \cup B = A \cup (B \setminus A)$ y $B = (B \setminus A) \cup (A \cap B)$ y aplicar la Proposición 1. □

El siguiente principio analiza aquellas situaciones en las que tenemos que realizar varias elecciones consecutivas entre alternativas no necesariamente iguales.

Proposición 3 (Principio del producto). *Si $X_1, \ldots, X_r$ son conjuntos de cardinal finito entonces $|X_1 \times \cdots \times X_r| = |X_1| \cdots |X_r|$.*

La interpretación de este principio es la siguiente: Si tenemos que realizar cadena de k selecciones independientes, la primera entre n_1 posibilidades, la segunda entre n_2 y así sucesivamente hasta la última selección que debemos realizar entre n_k alternativas, las alternativas totales entre las que debemos optar son $n_1 n_2 \cdots n_k$.

2.2 Orden importa. Factorial

El principio del producto nos permite calcular el número de palabras de longitud dada r que podemos formar con un alfabeto de n caracteres. Este número es n^r. La clave está en que podemos repetir las letras en cada elección. Vamos a analizar a continuación situaciones en las que no podemos realizar dicha repetición. Recordemos que el factorial de un natural $n \in \mathbb{N}$ se define recursivamente como

$$0! = 1, \qquad (n+1)! = (n+1)n!,$$

lo que podemos interpretar como

$$n! = n(n-1) \cdots 3 \cdot 2 \cdot 1$$

cuando $n \geq 1$.

Definición 4. Sean $r \leq n$ dos naturales. Una *r-permutación* en n es una aplicación inyectiva $\sigma : \{1, \ldots, r\} \to \{1, \ldots, n\}$. Al conjunto de las r-permutaciones en n lo denotamos $P(n, r)$.

Proposición 5.

$$|P(n, r)| = \frac{n!}{(n-r)!} = n(n-1) \cdots (n-r+1)$$

Demostración. Aplicación directa de la proposición 3, ya que comenzamos con n alternativas y tras cada elección tenemos una posibilidad menos para la siguiente. □

Corolario 6. *El número de permutaciones de un conjunto de n elementos (aplicaciones biyectivas del conjunto en si mismo) es n!.*

Definición 7. Una *partición ordenada* en un conjunto X es una partición en la que los subconjuntos están ordenados. Si bien los subconjuntos están ordenados, los elementos dentro de cada subconjunto no lo están.

El siguiente lema es intuitivo y fácil de demostrar a partir del principio de la suma. Además es muy útil para comprobar otros resultados.

Lema 8 (Lema de conteo)**.** *Sea $\phi : A \to B$ una aplicación sobreyectiva entre conjuntos finitos. Para cada $b \in B$ llamamos $\phi^{-1}(b) = \{a \in A \mid \phi(a) = b\}$. Si existe $k \in \mathbb{N}$ tal que $\left|\phi^{-1}(b)\right| = k$ para todo $b \in B$, entonces $|A| = k \cdot |B|$.*

Demostración. Basta observar que $A = \bigcup_{b\in B} \phi^{-1}(b)$, que la unión anterior es disjunta y aplicar la Proposición 1. □

Proposición 9. *Sea X un conjunto con $|X| = n$, y sean $n_1, \ldots, n_k$ números naturales tales que $n = n_1 + \cdots + n_k$. El número de particiones ordenadas $\langle A_1, \ldots, A_k\rangle$ con $\left|A_j\right| = n_j$ para cada $1 \leq j \leq k$ es*

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

Demostración. Consecuencia de la Proposición 5 y del Lema 8: Sea $\sigma : \{1, \ldots, n\} \to X$ una biyección y sea ϕ la aplicación que lleva σ en una partición ordenada $\langle A_1, \ldots, A_k\rangle$ llevando $\sigma(1), \ldots, \sigma(n_1)$ a A_1, $\sigma(n_1+1), \ldots, \sigma(n_1+n_2)$ a A_2, etcétera. Entonces $\phi^{-1}(\langle A_1, \ldots, A_k\rangle) = n_1! \cdots n_k!$. Como existen $n!$ permutaciones en X concluimos que el número de particiones ordenadas es $\frac{n!}{n_1!n_2!\cdots n_k!}$. □

El número de particiones ordenadas coincide con el número de permutaciones que podemos hacer en un conjunto con elementos repetidos.

Proposición 10. *Dado un conjunto de n elementos que tiene n_1 elementos repetidos de un primer tipo, n_2 de un segundo tipo y así sucesivamente hasta n_k de un tipo k-esimo. El número de permutaciones de dicho conjunto es*

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

Demostración. Si ordenamos los elementos y consideramos el conjunto X de las posiciones que ocupan, dar una permutación es equivalente a dar una partición ordenada $\langle A_1, \ldots, A_k\rangle$ donde A_i contiene las posiciones que ocupan los n_i elementos de tipo i-ésimo. □

2.3 Orden no importa. Coeficientes binomiales

Definición 11. Llamemos $\binom{n}{r}$ al número de subconjuntos de r elementos que tiene un conjunto de n elementos. Entonces

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Estos números reciben el nombre de coeficientes binomiales, debido sobre todo al teorema 13 que veremos con posterioridad.

Corolario 12. *El número de cadenas compuestas por $n - r$ ceros y r unos es $\binom{n}{r}$*

Demostración. Cada una de las cadenas referidas es la imagen de la aplicación característica de un subconjunto con cardinal r del conjunto $\{1, \ldots, n\}$, luego hay tantas cadenas como subconjuntos de r elementos. □

Entre otras, los coeficientes binomiales satisfacen las siguientes propiedades para $r \leq n$

$$\binom{n}{0} = 1, \qquad \binom{n}{r} = \binom{n}{n-r},$$
$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Teorema 13. *Sea A un anillo. Para cualesquiera $a, b \in A$ y $n \in \mathbb{N}$ se tiene*

$$\begin{aligned}(a+b)^n &= \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r} = \\ &= \binom{n}{0} b^n + \binom{n}{1} a b^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} b + \binom{n}{n} a^n\end{aligned}$$

Proposición 14. *Existen $\binom{n+k-1}{k-1}$ formas de descomponer $n \in \mathbb{N}$ como suma de k números naturales.*

Demostración. La aplicación

$$\langle n_1, \ldots, n_k \rangle \longmapsto \underbrace{0\cdots0}_{n_1}1\underbrace{0\cdots0}_{n_2}1\cdots1\underbrace{0\cdots0}_{n_k}$$

es una biyección entre el conjunto de las descomposiciones de n como suma de k naturales y cadenas con n ceros y $k-1$ unos, así el resultado es consecuencia directa del Corolario 12. □

Corolario 15. *Existen $\binom{n+k-1}{k-1}$ formas de distribuir n objetos indistinguibles en k cajas distinguibles.*

Corolario 16. *Existen $\binom{n+k-1}{k-1}$ formas de seleccionar n objetos entre k objetos distintos, permitiendo repeticiones.*

2.4 Otros principios de conteo

Teorema 17 (Principio de inclusión-exclusión). *Sean $A_1, \ldots, A_n \subseteq X$ subconjuntos finitos. Entonces*

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\}} |A_{i_1} \cap \cdots \cap A_{i_k}|,$$

es decir, sumamos los cardinales de los conjuntos obtenidos al realizar la intersección de un número impar de subconjuntos y restamos los cardinales de los conjuntos obtenidos al intersecar un número par de subconjuntos.

La fórmula se entiende más claramente si la describimos para tres y cuatro conjuntos:

$$\begin{aligned}|A \cup B \cup C| = {} & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \\ |A_1 \cup A_2 \cup A_3 \cup A_4| = {} & |A_1| + |A_2| + |A_3| + |A_4| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| \\ & \quad - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| \\ & + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\ & \quad + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\ & - |A_1 \cap A_2 \cap A_3 \cap A_4|\end{aligned}$$

Terminamos con otro principio aparentemente sencillo, pero de gran utilidad a la hora de resolver problemas. Se le conoce con el nombre de principio del palomar o de Dirichlet.

Proposición 18 (Principio de Dirichlet). *Sea $\{A_1, \ldots, A_k\}$ una partición de un conjunto X tal que $|X| = n$. Existe $i \in \{1, \ldots, k\}$ tal que $|A_i| \geq \frac{n}{k}$.*

Demostración. Como consecuencia de la Proposición 1 (principio de la suma) $|X| = |A_1| + \cdots + |A_k|$. Si para todo i $|A_i| < \frac{n}{k}$, necesariamente tendríamos que $|X| < k\frac{n}{k} = n$, lo que es imposible. □

Corolario 19. *Sea $\varphi : X \to Y$ una aplicación entre conjuntos finitos tales que $|X| > k\,|Y|$ para cierto $k \in \mathbb{N}$. Existe $y \in Y$ tal que $\left|\varphi^{-1}(y)\right| > k$.*

Demostración. Sencilla aplicación de la Proposición 18 a la partición $\{\varphi^{-1}(y) \mid y \in Y\} \setminus \{\varnothing\}$ de X. □

TEMA 3

Aritmética entera y polinomial

3.1 Números naturales: División y bases de numeración.

Definición 1. Denotamos al conjunto de los números naturales mediante el símbolo $\mathbb{N}$. En los naturales tenemos definidas dos operaciones conocidas por todos que son la suma y el producto, operaciones cuyas propiedades son sobradamente conocidas y que explicitaremos en el apartado de números enteros.

Definición 2 (Orden)**.** Decimos que $n \leq m$ si existe $c \in \mathbb{N}$ tal que $m = n + c$.

Proposición 3. *La relación $\leq$ satisface las propiedades siguientes:*

Reflexiva: *$n \leq n$ para cualquier natural n.*

Antisimétrica: *si $n \leq m$ y $m \leq n$ entonces $n = m$.*

Transitiva: *si $n \leq m$ y $m \leq p$ entonces $n \leq p$.*

Proposición 4. *Para cualesquiera $a, b, c \in \mathbb{N}$ con $a \leq b$ se tiene $a + c \leq b + c$ y $ac \leq bc$.*

Proposición 5. *1. La relación $\leq$ es un orden total, es decir, para cualesquiera $n, m \in \mathbb{N}$ se tiene $n \leq m$ o $m \leq n$.*

2. La relación $\leq$ es un buen orden, es decir, todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo.

Teorema 6 (Algoritmo de la división)**.** *Para cualesquiera $a, b \in \mathbb{N}$ con $b \neq 0$ existen únicos $c, r \in \mathbb{N}$ con $0 \leq r < b$ tales que $a = c \cdot b + r$.*

Teorema 7. *Dado un natural $b \geq 2$ y $k \geq 1$, todo $n < b^k$ se representa de manera única como*

$$n = d_{k-1} \cdot b^{k-1} + d_{k-2} \cdot b^{k-2} + \cdots + d_1 \cdot b + d_0$$

donde $0 \leq d_i < b$ para todo $i = 0, \ldots, k-1$.

Busquemos b símbolos que representen a cada uno de los números naturales comprendidos entre 0 y $b-1$. En virtud del Teorema 7 todo natural n se representa de manera única como $n = d_{k-1}d_{k-2}\ldots d_1 d_0)_b$ donde los d_i son los símbolos anteriores. La representación nos dice que

$$n = d_{k-1} \cdot b^{k-1} + \cdots + d_1 \cdot b + d_0.$$

Si $n = d_{k-1}d_{k-2}\ldots d_1 d_0)_b$ con $d_{k-1} \neq 0$ decimos que n es un número de exactamente k dígitos en base b. Observemos que n tiene exactamente k dígitos en base b si y sólo si $b^{k-1} \leq n < b^k$, lo que nos permite comprobar que el número de dígitos en base b de n es $\lfloor \log_b n \rfloor + 1$, donde $\lfloor \_ \rfloor$ representa la función *parte entera*.

Para pasar de base b a base 10 basta con utilizar la aritmética usual en la base 10. Para pasar de base 10 a base b el Teorema 7 nos da la clave, hay que realizar divisiones e ir tomando los restos. Por ejemplo, para convertir 25 a binario realizamos divisiones sucesivas entre 2, la base, y nos quedamos con los restos:

$$\begin{aligned} 25 &= 2 \times 12 + 1 \\ 12 &= 2 \times 6 + 0 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

Por tanto $25 = 11001)_2$

Existe una situación en la que es especialmente sencillo hacer cambios de base. Vamos a cambiar de base b a base b^s y viceversa. Todo natural comprendido entre 0 y $b^s - 1$ se escribe como $d_{s-1}b^{s-1} + \cdots + d_1 b + d_0$ donde los símbolos $d_0, \ldots d_{s-1}$ son dígitos en base b. Así, todo dígito en base b^s se escribe mediante s dígitos en base b. Así, si $n = (D_{k-1} \ldots D_1 D_0)_{b^s}$, y $D_i = (d_{s-1}^{(i)} \ldots d_1^{(i)} d_0^{(i)})_b$ tenemos que

$$\begin{aligned} n &= D_{k-1}(b^s)^{k-1} + \cdots + D_1 b^s + D_0 \\ &= (d_{s-1}^{(k-1)} b^{s-1} + \cdots + d_1^{(k-1)} b + d_0^{(k-1)})(b^s)^{k-1} + \\ &\quad \cdots + (d_{s-1}^{(1)} b^{s-1} + \cdots + d_1^{(1)} b + d_0^{(1)}) b^s + (d_{s-1}^{(0)} b^{s-1} + \cdots + d_1^{(0)} b + d_0^{(0)}) \\ &= d_{s-1}^{(k-1)} b^{(k-1)s+(s-1)} + \cdots + d_1^{(k-1)} b^{(k-1)s+1} + d_0^{(k-1)} b^{(k-1)s} + \\ &\quad \cdots + d_{s-1}^{(1)} b^{s+s-1} + \cdots + d_1^{(1)} b^{s+1} + d_0^{(1)} b^s + d_{s-1}^{(0)} b^{s-1} + \cdots + d_1^{(0)} b + d_0^{(0)}, \end{aligned}$$

es decir,

$$(D_{k-1} \ldots D_1 D_0)_{b^s} = (d_{s-1}^{(k-1)} \ldots d_1^{(k-1)} d_0^{(k-1)} \ldots d_{s-1}^{(1)} \ldots d_1^{(1)} d_0^{(1)} d_{s-1}^{(0)} \ldots d_1^{(0)} d_0^{(0)})_b.$$

Cada dígito en base b^s se sustituye por su representación mediante s dígitos en base b. El proceso inverso es completamente análogo.

Ejemplo 8. Convertimos

$$n = 10010010111010010011100 1010)_2$$

a base $16 = 2^4$. Para ello agrupamos n en bloques de cuatro bits,

$$n = \underline{100}\,\underline{1001}\,\underline{0111}\,\underline{0100}\,\underline{1001}\,\underline{1100}\,\underline{1010})_2$$

como $100)_2 = 4 = 4)_{16}$, $1001)_2 = 9 = 9)_{16}$, $0111)_2 = 7 = 7)_{16}$, $1100)_2 = 12 = C)_{16}$ y $1010)_2 = 10 = A)_{16}$,

$$n = 49749CA)_{16}.$$

Recíprocamente, convertimos $m = 74051)_8$ a base 2. Ya que $7)_8 = 111)_2$, $4)_8 = 100)_2$, $0)_8 = 000)_2$, $5)_8 = 101)_2$ y $1_8 = 001)_2$, tememos que $m = 111\,100\,000\,101\,001)_2$. Este es el motivo por el que las bases 8 y 16 se utilizan mucho en diversos campos de la informática.

3.2 Números enteros

En el conjunto $\mathbb{Z}$ de los números enteros conocemos dos operaciones, la suma y el producto, que satisfacen las propiedades que vamos a describir a continuación

Proposición 9. *La suma de números enteros es*

conmutativa, *es decir, para cualesquiera $x, y \in \mathbb{Z}$, $x + y = y + x$,*

asociativa, *es decir, para cualesquiera $x, y, z \in \mathbb{Z}$, $x + (y + z) = (x + y) + z$,*

tiene elemento neutro, *es decir, existe un elemento $0 \in \mathbb{Z}$ (necesariamente único) tal que para cualquier $x \in \mathbb{Z}$, $x + 0 = 0 + x = x$,*

tiene elemento simétrico, *es decir, para cualesquiera $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ (llamado opuesto) tal que $x + (-x) = (-x) + x = 0$.*

Proposición 10. *El producto de números enteros es*

conmutativo, *es decir, para cualesquiera $x, y \in \mathbb{Z}$, $xy = yx$,*

asociativo, *es decir, para cualesquiera $x, y, z \in \mathbb{Z}$, $x(yz) = (xy)z$,*

tiene elemento neutro, *es decir, existe un elemento $1 \in \mathbb{Z}$ (necesariamente único) tal que para cualquier $x \in \mathbb{Z}$, $x1 = 1x = x$*

distributivo respecto de la suma, *es decir, para cualesquiera* $x, y, z \in \mathbb{Z}$, $(x+y)z = xz+yz$ *y* $x(y+z) = xy+xz$.

Es decir, $\mathbb{Z}$ es un anillo conmutativo. Además es lo que se conoce como **dominio**, es decir, si $a, b \in \mathbb{Z} \setminus \{0\}$ entonces $ab \neq 0$

Definición 11 (Orden)**.** El orden en $\mathbb{Z}$ se define igual que en $\mathbb{N}$, es decir, decimos que $p \leq q$ si existe $n \in \mathbb{N}$ tal que $q = p + n$.

Muchas de las propiedades son análogas

Proposición 12. *La relación* $\leq$ *es reflexiva, antisimétrica y transitiva.*

Proposición 13. *Para cualesquiera* $a, b, c \in \mathbb{Z}$ *con* $a \leq b$ *se tiene* $a + c \leq b + c$*. Además, si* $c \geq 0$ *se tiene que* $ac \leq bc$*, y si* $c \leq 0$ $bc \leq ac$.

Definición 14 (Valor absoluto)**.** Para todo $p \in \mathbb{Z}$ se define el valor absoluto de p como

$$|p| = \begin{cases} p & \text{si } p \geq 0 \\ -p & \text{si } p < 0 \end{cases}$$

Teorema 15 (Algoritmo de la división)**.** *Para cualesquiera* $a, b \in \mathbb{Z}$ *con* $b \neq 0$*, existen únicos* $q, r \in \mathbb{Z}$ *tales que* $a = q \cdot b + r$ *y* $0 \leq r < |b|$.

En la división el resto se denota a mód b y el cociente suele representarse por a quo b.

3.3 Divisibilidad

Definición 16. Dados $a, b \in \mathbb{Z}$, decimos que a divide a b si existe $c \in \mathbb{Z}$ tal que $ac = b$. Se denota $a \mid b$. Es inmediato comprobar que

$$a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b,$$

por lo que para estudiar la divisibilidad podemos restringirnos siempre a los valores absolutos de los enteros implicados.

Proposición 17. *Para cualesquiera* $a, b \in \mathbb{Z}$*,*

1. $a \mid a$,
2. $1 \mid a$,
3. $a \mid 0$,
4. *si* $a, b \neq 0$ *y* $a \mid b$ *entonces* $|a| \leq |b|$.

Definición 18. Dados $a, b \in \mathbb{Z}$, decimos que d es el máximo común divisor de a y b ($d = \text{mcd}(a, b)$) si

1. $d \mid a$ y $d \mid b$,
2. si $e \mid a$ y $e \mid b$ entonces $e \leq d$.

Lema 19. *Si* $a = cb + r$ *entonces* $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración. Sean $d_1 = \text{mcd}(a, b)$ y $d_2 = \text{mcd}(b, r)$. Dado que d_2 divide a b y a r, también divide a a, por lo que $d_2 \leq d_1$. Análogamente, como $r = a - cb$ y d_1 divide a a y a b tenemos que d_1 divide a r, por lo que $d_1 \leq d_2$. Por tanto $d_1 = d_2$. □

Algoritmo de Euclides

procedure MCD(a, b)
  $a \leftarrow |a|$, $b \leftarrow |b|$
  repeat
    $r \leftarrow a$ mód b

$a \leftarrow b$
$b \leftarrow r$
until $r = 0$
return a
end procedure

El algoritmo termina porque los restos son todos mayores o iguales que 0 y cada vez menores.

Observación 20. Supongamos que $x = u_x a + v_x b$ e $y = u_y a + v_y b$, es decir, x, y son combinaciones lineales de a y b. Si $x = cy + r$ entonces, sustituyendo los valores de x e y, tenemos:

$$\begin{aligned} r &= x - cy \\ &= (u_x a + v_x b) - c(u_y a + v_y b) \\ &= (u_x - cu_y)a + (v_x - cv_y)b, \end{aligned}$$

por lo que r también puede escribirse como combinación lineal de a y b. En vista de esta propiedad en cada repetición del algoritmo de Euclides podemos expresar el resto como combinación lineal de a y b.

La Observación 20 tiene dos consecuencias. En primer lugar sirve para demostrar la Propiedad Lineal:

Proposición 21 (Propiedad lineal). *Si $d = \mathrm{mcd}(a, b)$ entonces existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.*

Demostración. Cada resto calculado puede escribirse como combinación lineal entera de a y b. □

Corolario 22. *Si $c \mid a$ y $c \mid b$ entonces $c \mid \mathrm{mcd}(a, b)$.*

Demostración. Por hipótesis tenemos que $a = sc$ y $b = tc$ para ciertos $s, t \in \mathbb{Z}$. Llamemos $d = \mathrm{mcd}(a, b)$, por la Proposición 21 existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$. Por tanto

$$d = ua + vb = usc + vtc = (us + vt)c,$$

luego $c \mid d$ como queríamos. □

En segundo lugar la Observación 20 también es la clave del conocido como Algoritmo de Euclides extendido:

Algoritmo 23 (Algoritmo de Euclides extendido). **procedure** MCDEX(a, b)
$s \leftarrow \frac{a}{|a|}$, $t \leftarrow \frac{b}{|b|}$
$a \leftarrow |a|$, $b \leftarrow |b|$
$u'' \leftarrow 1$, $v'' \leftarrow 0$
$u' \leftarrow 0$, $v' \leftarrow 1$
repeat
$r \leftarrow a$ mód b
$q \leftarrow a$ quo b
$a \leftarrow b$
$b \leftarrow r$
$u \leftarrow u'' - qu'$, $u'' \leftarrow u'$, $u' \leftarrow u$
$v \leftarrow v'' - qv'$, $v'' \leftarrow v'$, $v' \leftarrow v$
until $r = 0$
return a, su'', tv''
end procedure

Teorema 24 (Bezout). *Sean $a, b \neq 0$. $\mathrm{mcd}(a, b) = 1$ si y sólo si existen $u, v \in \mathbb{Z}$ tales que $1 = ua + vb$.*

Demostración. Una implicación es aplicación directa de la Proposición 21. Si $d \mid a$, $d \mid b$ y $1 = ua + vb$ entonces $d \mid 1$, de donde $d = \pm 1$, lo que nos dice que $\mathrm{mcd}(a, b) = 1$. □

Definición 25. Dados $a, b \in \mathbb{Z}$, decimos que $m \geq 0$ es el mínimo común múltiplo de a y b ($m = \mathrm{mcm}(a, b)$) si

1. $a \mid m$ y $b \mid m$,
2. si $a \mid n$ y $b \mid n$ entonces $m \leq |n|$.

Proposición 26. *Para cualesquiera $a, b \in \mathbb{Z}$*

$$|ab| = \mathrm{mcd}(a, b)\,\mathrm{mcm}(a, b)$$

3.4 Ecuaciones Diofánticas

Una ecuación diofántica es una ecuación del tipo

$$ax + by = c, \text{ donde } a, b, c \in \mathbb{Z}, \tag{2}$$

y de la que queremos encontrar sus soluciones enteras, es decir, encontrar valores $x_0, y_0 \in \mathbb{Z}$ que satisfagan la ecuación.

Proposición 27. *La ecuación* (2) *tiene solución si y sólo si* $\text{mcd}(a, b) \mid c$.

Proposición 28. *Si* (x_0, y_0) *es una solución de* (2) *y* $d = \text{mcd}(a, b)$*, entonces todas las soluciones se calculan mediante las fórmulas*

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n \tag{3}$$

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

3.5 Congruencias y aritmética modular

Definición 29. Sea $m \in \mathbb{Z}$ $m \neq 0, \pm 1$. Sean $a, b \in \mathbb{Z}$. Decimos que a es congruente con b módulo m si $m \mid a - b$. Este hecho se denota

$$a \equiv b \pmod{m}$$

Proposición 30. *La congruencia módulo* m *es una relación de equivalencia, es decir,*

1. (reflexiva) $a \equiv a \pmod{m}$,
2. (simétrica) *si* $a \equiv b \pmod{m}$ *entonces* $b \equiv a \pmod{m}$,
3. (transitiva) *si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$.

Proposición 31. *Si* $a \equiv a' \pmod{m}$ *y* $b \equiv b' \pmod{m}$*, entonces* $a + b \equiv a' + b' \pmod{m}$ *y* $ab \equiv a'b' \pmod{m}$

Observación 32. Hay otras propiedades sencillas referentes a congruencias

1. si $a \equiv b \pmod{m}$ y $d \mid m$ entonces $a \equiv b \pmod{d}$,
2. si $d \mid a, b, m$ y $a \equiv b \pmod{m}$ entonces $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,
3. si $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2}$ entonces $a \equiv b \pmod{\text{mcm}(m_1, m_2)}$.

Definición 33. Sea $m \in \mathbb{Z}$ con $m \neq 0, 1$. No perdemos generalidad con suponer que $m \geq 0$, ya que podemos sustituir m por $|m|$ para estudiar divisibilidad. Llamamos $\mathbb{Z}_m$ al conjunto cociente $\mathbb{Z}$ sobre la relación de equivalencia ser congruente módulo m. Tenemos entonces que $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$. Vamos a definir dos operaciones en $\mathbb{Z}_m$,

Suma $[a] + [b] = [a + b]$,

Producto $[a][b] = [ab]$.

Estas definiciones están bien hechas (es decir, no dependen del representante) en virtud de la Proposición 31. Vamos a identificar normalmente $\mathbb{Z}_m$ con $\{0, \ldots, m-1\}$. Vía esta identificación, las operaciones en $\mathbb{Z}_m$ quedan de la siguiente forma para $0 \leq a, b, c \leq m - 1$,

Suma $a + b = c$ si y sólo si $a + b \equiv c \pmod{m}$,

Producto $ab = c$ si y sólo si $ab \equiv c \pmod{m}$.

Lema 34. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y sólo si* $\text{mcd}(a, m) \mid b$*. Si* x_0 *es una solución de la ecuación anterior entonces todas las soluciones son de la forma* $x = x_0 + \frac{m}{\text{mcd}(a,m)}n$ *con* $n \in \mathbb{Z}$.

3.6 Sistemas de congruencias

Lema 35. *Sean $m, n, k \in \mathbb{Z}$ con* $\text{mcd}(m, n) = \text{mcd}(m, k) = 1$. *Entonces* $\text{mcd}(m, nk) = 1$.

Teorema 36 (Teorema chino del resto)**.** *Si $m_1, \ldots, m_k$ son enteros primos relativos dos a dos, entonces el sistema de ecuaciones*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{4}$$

tiene solución única módulo $M = m_1 m_2 \ldots m_k$.

Demostración. Para cada j sea $M_j = \frac{m_1 \ldots m_k}{m_j} = \frac{M}{m_j}$ y b_j un entero que satisface $M_j b_j \equiv 1 \pmod{m_j}$, el cual existe porque $\text{mcd}(m_j, M_j) = 1$ en virtud del Lema 35. La solución del sistema es $x = a_1 M_1 b_1 + \cdots + a_k M_k b_k$. La unicidad es consecuencia de que $\text{mcm}(m_i, m_j) = m_i m_j$ si $i \neq j$ y de la Observación 32. □

Analicemos el caso general. Vamos a dar un procedimiento iterativo para resolver sistemas de ecuaciones en congruencias del tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases} \tag{5}$$

sin restricciones en los posibles valores de $m_1, \ldots, m_k$. En primer lugar resolvemos la primera ecuación mediante el Lema 34, que en caso de tener solución será de la forma

$$x \equiv c_1 \pmod{m_1'}.$$

Consideremos las dos primeras ecuaciones,

$$\begin{cases} x \equiv c_1 \pmod{m_1'} \\ a_2 x \equiv b_2 \pmod{m_2} \end{cases}$$

La primera ecuación puede describirse como $x = c_1 + m_1' s$ donde $s \in \mathbb{Z}$. Sustituyendo dicho valor de x en la segunda ecuación tenemos

$$a_2(c_1 + m_1' s) \equiv b_2 \pmod{m_2},$$

o lo que es lo mismo

$$a_2 m_1' s \equiv b_2 - a_2 c_1 \pmod{m_2}.$$

Hallamos los valores de s para los que dicha ecuación es cierta, es decir, resolvemos la ecuación anterior de nuevo mediante el Lema 34. La solución será de la forma $s = s_0 + m_2' n$ para cualquier $n \in \mathbb{Z}$. Susituyendo s tenemos la solución $x = c_1 + m_1'(s_0 + m_2' n) = c_1 + m_1' s_0 + m_1' m_2' n$ para cualquier $n \in \mathbb{Z}$, o equivalentemente

$$x \equiv c_1 + m_1' s_0 \pmod{m_1' m_2'}.$$

Nuestro sistema (5) se ha convertido en el sistema

$$\begin{cases} x \equiv c_2 \pmod{m_1' m_2'} \\ a_3 x \equiv b_3 \pmod{m_3} \\ \quad \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases},$$

que es un sistema del mismo tipo que (5) pero con una ecuación menos. Podemos reiterar el proceso hasta alcanzar una única ecuación que nos dará la solución, si existe.

3.7 Números primos

Definición 37. Un número entero $p \in \mathbb{Z}$ $p \neq \pm 1$ se dice primo si satisface algunas de las siguientes afirmaciones equivalentes:

1. sus únicos divisores son ± 1 y $\pm p$,
2. para cualquier $1 \leq a < p$ se tiene que $\mathrm{mcd}(a, p) = 1$,
3. $\mathbb{Z}_p$ es un cuerpo, es decir, todo elemento no nulo de $\mathbb{Z}_p$ tiene inverso,
4. para cualesquiera $a, b \in \mathbb{Z}$, $p \mid ab$ implica $p \mid a$ o $p \mid b$.

Proposición 38. *Hay infinitos números primos.*

Teorema 39 (Fundamental de la aritmética). *Todo entero m se escribe de manera única como $m = \pm p_1^{\alpha_1} \dots p_k^{\alpha_k}$ donde $p_1 < \dots < p_k$ son primos positivos y $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.*

Teorema 40 (Pequeño de Fermat). *Sea p un entero primo. Si p no divide a a entonces $a^{p-1} \equiv 1$* (mód p).

Definición 41. La función φ de Euler es una aplicación $\varphi : \mathbb{N} \to \mathbb{N}$ definida por

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leq n, \mathrm{mcd}(n, m) = 1\}|,$$

es decir, $\varphi(n)$ nos dice cuantos naturales menores que n son primos relativos con n.

Proposición 42. *Si $n = p_1^{\alpha_1} \dots p_r^{\alpha^r}$ con $p_1 < \dots < p_r$, entonces*

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_r^{\alpha_r - 1}(p_r - 1).$$

Teorema 43 (Euler). *Si* $\mathrm{mcd}(a, n) = 1$, *entonces* $a^{\varphi(n)} \equiv 1$ (mód n).

3.8 Polinomios y aritmética

Definición 44. Sea A un anillo conmutativo y x una variable. Un polinomio sobre A es una expresión formal

$$a_0 + a_1 x + \dots + a_n x^n$$

donde $a_0, \dots a_n \in A$. Salvo que el polinomio sea cero la representación se suele presentar normalizada para que $a_n \neq 0$. En este caso decimos que el grado es n, y el coeficiente líder a_n. Si $p(x)$ es un polinomio cualquiera representamos el grado por $\deg(p)$ o $\deg(p(x))$. Al polinomio cero no se le asigna grado o se dice que tiene grado $-\infty$. El conjunto de los polinomios sobre A se denota $A[x]$.

Definición 45. Si $a(x) = a_0 + a_1 x + \dots a_n x^n$ y $b(x) = b_0 + b_1 x + \dots b_m x^m$, definimos la suma de $a(x)$ y $b(x)$ como

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_p + b_p)x^p$$

donde $p = \max\{n, m\}$, $a_i = 0$ si $i > n$ y $b_j = 0$ si $j > m$.

Definición 46. Igualmente, si $a(x) = a_0 + a_1 x + \dots a_n x^n$ y $b(x) = b_0 + b_1 x + \dots b_m x^m$, definimos el producto de $a(x)$ y $b(x)$ como

$$a(x)b(x) = c_0 + c_1 x + \dots + c_{n+m} x^{n+m}, \text{ con } c_k = \sum_{i+j=k} a_i b_j.$$

Observación 47. Si $p, q \in A[x]$, $\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$ y $\deg(pq) \leq \deg(p) + \deg(q)$.

Proposición 48. *$(A[x], +, \cdot)$ es un anillo conmutativo.*

Demostración. Mecánica, sólo hay que tener cuidado en manipular subíndices. □

3.9 Divisibilidad

Teorema 49. *Sea $\Bbbk$ un cuerpo. Para cualesquiera $p, q \in \Bbbk[x]$ con $q \neq 0$ existen únicos $c, r \in \Bbbk[x]$ tales que $p = cq + r$ y $\deg(r) < \deg(q)$.*

Definición 50. Sean $a, b \in \Bbbk[x]$. Decimos que d es un *máximo común divisor* de a y b si $d \mid a$, $d \mid b$ y para cualquier elemento c con $c \mid a$ y $c \mid b$ se tiene que $c \mid d$. Denotamos $\mathrm{MCD}(a, b)$ al conjunto de los elementos que son máximo común divisor de a y b.

Proposición 51. *Para cualesquiera $a, b \in \Bbbk[x]$, $d \in \mathrm{MCD}(a, b)$ si y sólo si*

$$\mathrm{MCD}(a, b) = \{ud \mid u \in \Bbbk \setminus \{0\}\}$$

Lema 52. *Sean $a, b \in \Bbbk[x]$. Si $a = cb + r$. Entonces $\mathrm{MCD}(b, r) = \mathrm{MCD}(a, b)$*

Demostración. Sea $d \in \mathrm{MCD}(a, b)$. Dado que $r = a - cb$, tenemos que cualquier divisor de a y b también divide a r, en particular $d \mid r$. Por otra parte, si $e \mid b$ y $e \mid r$, dado que $a = cb + r$ tenemos que $e \mid a$, de donde $e \mid d$ por la definición de máximo común divisor. Por tanto $d \in \mathrm{MCD}(b, r)$. La otra inclusión se obtiene análogamente. □

Teorema 53 (Algoritmo de Euclides)**.** *Si $a, b \in \Bbbk[x]$ entonces $\mathrm{MCD}(a, b) \neq \varnothing$.*

Demostración. El siguiente procedimiento permite justificar la existencia y calcular el máximo común divisor de a y b. Podemos suponer que tanto a como b son distintos de cero.

1. Realizamos la división, es decir, calculamos q, r tales que $a = qb + r$ con $r = 0$ o $\deg(r) < \deg(b)$.
2. Si $r = 0$ entonces $b \in \mathrm{MCD}(a, b)$, si no asignamos a el valor de b, a b el de r y repetimos el paso 1.

El proceso debe terminar porque los restos tienen norma cada vez menor. Además, por el Lema 52 el resultado es el correcto. □

Proposición 54 (Propiedad lineal)**.** *Sean $a, b \in \Bbbk[x]$. Si $d \in \mathrm{MCD}(a, b)$ entonces existen $u, v \in \Bbbk[x]$ tales que $d = ua + vb$.*

Demostración. Esencialmente la misma que la de la Proposición 21. □

El Algoritmo Extendido de Euclides que se presenta en el Algoritmo 23 del Tema 3 funciona exactamente igual para $\Bbbk[x]$. De la misma manera tenemos el siguiente teorema:

Teorema 55 (Bezout)**.** *Sean $a, b \in \Bbbk[x] \setminus \{0\}$. $1 \in \mathrm{MCD}(a, b)$ si y sólo si existen polinomios u, v tales que $1 = ua + vb$.*

Observación 56. Algunas consecuencias directas del Teorema de Bezout son las siguientes:

1. Si $d \in \mathrm{MCD}(a, b)$ entonces $1 \in \mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$.
2. Si $1 \in \mathrm{MCD}(a, b)$ y $a \mid bc$, como $1 = ua + vb$ tenemos que $c = uac + vbc$, de donde $a \mid c$.
3. Es sencillo comprobar que $\mathrm{MCD}(a, b) = \Bbbk \setminus \{0\}$ si y sólo si $\mathrm{MCD}(a, b) \cap \Bbbk \setminus \{0\} \neq \varnothing$.

Terminamos la sección con un resultado que relaciona el máximo común divisor y el mínimo común múltiplo, que se define de forma natural.

Proposición 57. *Sean $a, b \in \Bbbk[x]$ y sea $d, m \in \Bbbk[x]$ tales que $dm = ab$. Entonces $d \in \mathrm{MCD}(a, b)$ si y sólo si $m \in \mathrm{MCM}(a, b)$.*

Demostración. Supongamos que $d \in \mathrm{MCD}(a, b)$ y escribamos $a = a'd$ y $b = b'd$. Necesariamente $m = a'b = ab'$, por lo que m es múltiplo de a y de b. Supongamos que c es múltiplo de a y b. Tenemos entonces que $c = a''a'd = b''b'd$. Así $b' \mid a''a'$, y en vista de la Observación 56 tenemos que $b' \mid a''$, es decir, $a'' = a'''b'$. Por tanto $c = a'''b'a'd = a'''m$ y $m \mid c$, lo que implica que $m \in \mathrm{MCM}(a, b)$.

Supongamos ahora que $m \in \mathrm{MCM}(a, b)$. Podemos escribir $m = a'a = b'b$, y dado que m es un mínimo común múltiplo podemos deducir que $1 \in \mathrm{MCD}(a', b')$. Dado que $dm = ab$ tenemos que $a'dm = a'ab = mb$, por lo que $b = a'd$ y $d \mid b$. Análogamente $a = b'd$ y $d \mid a$. Supongamos que $c \mid a$ y $c \mid b$. Como $1 = ua' + vb'$ tenemos que $d = ua'd + vb'd = ub + va$, de donde $c \mid d$ y $d \in \mathrm{MCD}(a, b)$. □

3.10 Congruencias

Todas las definiciones y propiedades de la Sección 3.5 del Tema 3 se pueden extender a $\Bbbk[x]$ de manera directa.

Definición 58. Sean $a, b, m \in \Bbbk[x]$. Decimos que a es congruente con b módulo m si $m \mid a - b$. Este hecho se denota

$$a \equiv b \pmod{m}$$

Proposición 59. *La congruencia módulo m es una relación de equivalencia, es decir,*

1. (reflexiva) $a \equiv a \pmod{m}$,
2. (simétrica) *si* $a \equiv b \pmod{m}$ *entonces* $b \equiv a \pmod{m}$,
3. (transitiva) *si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$.

Proposición 60. *Si* $a \equiv a' \pmod{m}$ *y* $b \equiv b' \pmod{m}$, *entonces* $a + b \equiv a' + b' \pmod{m}$ *y* $ab \equiv a'b' \pmod{m}$

Demostración. La misma que la Proposición 31 □

Observación 61. Las propiedades descritas en la Observación 32 también son ciertas para un anillo de polinomios:

1. si $a \equiv b \pmod{m}$ y $d \mid m$ entonces $a \equiv b \pmod{d}$,
2. si $d \mid a, b, m$, tenemos que $a \equiv b \pmod{m}$ si y sólo si $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,
3. $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2}$ si y sólo si $a \equiv b \pmod{m}$, donde $m \in \mathrm{MCM}(m_1, m_2)$.

Definición 62. Sea $m \in \Bbbk[x]$ con $\deg(m) > 0$. Llamamos $\Bbbk[x]_m$ al conjunto cociente $\Bbbk[x]$ sobre la relación de equivalencia ser congruente módulo m. De nuevo tenemos dos operaciones en $\Bbbk[x]_m$,

Suma $[a] + [b] = [a + b]$,

Producto $[a][b] = [ab]$.

Estas definiciones están bien hechas (es decir, no dependen del representante) en virtud de la Proposición 60. Como en el caso de $\mathbb{Z}$ podemos identificar $\Bbbk[x]_m$ con el conjunto de los restos de las divisiones por m. Vía esta identificación las operaciones en $\Bbbk[x]_m$ quedan de la siguiente forma para a, b, c restos módulo m,

Suma $a + b = c$ si y sólo si $a + b \equiv c \pmod{m}$,

Producto $ab = c$ si y sólo si $ab \equiv c \pmod{m}$.

Lema 63. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y sólo si* $\mathrm{MCD}(a, m) \mid b$.

Demostración. Se obtiene a partir de la Proposición 54 tal y como el Lema 34 se obtiene a partir de la Proposición 21 □

Teorema 64 (Teorema chino del resto). *Si* $m_1, \ldots, m_k \in A$ *tales que* $1 \in \mathrm{MCD}(m_i, m_j)$ *para toda pareja* i, j, *entonces el sistema de ecuaciones*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{6}$$

tiene solución única módulo $M = m_1 m_2 \ldots m_k$.

Demostración. Análoga al Teorema 36 del Tema 3, utilizando una versión para anillos de polinomios del Lema 35 del mismo Tema. □

3.11 Irreducibilidad y Teorema Fundamental de la Aritmética

Definición 65. Decimos que $a, b \in \Bbbk[x]$ son asociados (abreviadamente $a \sim b$) si $a = ub$ con $u \in \Bbbk \setminus \{0\}$. Un polinomio $p \in \Bbbk[x]$ se dice *irreducible* si no es una constante y sus únicos divisores no constantes son sus asociados, es decir, si $q \mid p$ y $q \notin \Bbbk$, entonces $q = up$ con $u \in \Bbbk \setminus \{0\}$.

Lema 66. *Un polinomio $p \in \Bbbk[x]$ es irreducible si y sólo si para cualesquiera $a, b \in \Bbbk[x]$, si $p \mid ab$ entonces $p \mid a$ o $p \mid b$.*

Demostración. Sea p irreducible. Si $p \mid ab$ entonces $ab = cp$. Sea $d \in \mathrm{MCD}(a, p)$, si $d \notin \mathcal{U}(A)$ entonces d tiene que ser asociado a p, de donde $p \mid a$. Así pues, si suponemos que $p \nmid a$ tenemos que $1 \in \mathrm{MCD}(a, p)$, de donde $1 = ua + vp$. Así $uab = ucp$, por lo que $b = ucp - vpb = (uc - vb)p$, es decir, $p \mid b$.

Recíprocamente, supongamos que $p \mid ab$ implica $p \mid a$ o $p \mid b$. Si $a \mid p$ tenemos que $p = ac$ para algún c. Así $p \mid ac$, de donde $p \mid a$ o $p \mid c$. En el primer caso $a \sim p$, y en el segundo $p \sim c$ de donde $a \in \Bbbk \setminus \{0\}$. □

Proposición 67. *$p \in \Bbbk[x]$ es irreducible si y sólo si $\Bbbk[x]_p$ es un cuerpo.*

Lema 68. *Si $a \mid b$ y $\deg(a) = \deg(b)$ entonces $a \sim b$.*

Lema 69. *Si $\varnothing \neq B \subseteq \Bbbk[x]$, existe $b \in B$ tal que para todo $a \in B$, $a \mid b$ implica $a \sim b$.*

Demostración. Supongamos que el resultado es falso. Podemos construir una sucesión $\{a_i \mid i \in \mathbb{N}\}$ tal que $a_{i+1} \mid a_i$ y $a_{i+1} \nsim a_i$. A partir de la sucesión anterior tenemos una nueva sucesión $\{\delta(a_i) \mid i \in \mathbb{N}\} \subseteq \mathbb{N}$ tal que $\delta(a_{i+1}) \leq \delta(a_i)$. Como $\{\delta(a_i) \mid i \in \mathbb{N}\} \subseteq \{0, \ldots, \delta(a_0)\}$ que es un conjunto finito, existe un natural n tal que $\delta(a_n) = \delta(a_{n+k})$ para todo k. En particular $\delta(a_n) = \delta(a_{n+1})$, y por el Lema 68 tenemos que $a_n \sim a_{n+1}$, lo que contradice nuestra hipótesis sobre las propiedades de la sucesión $\{a_i \mid i \in \mathbb{N}\}$. Por lo tanto el Lema es verdadero. □

Teorema 70 (Fundamental de la Aritmética)**.** *Todo polinomio $a \in \Bbbk[x]$ se descompone como $a = p_1 \cdots p_s$ con p_i irreducible. Además si $a = p_1 \cdots p_s = q_1 \cdots q_t$ son dos descomposiciones como producto de irreducibles entonces $s = t$ y salvo reordenación $p_i \sim q_i$.*

Demostración. Demostramos la existencia de descomposiciones. Sea B el subconjunto de A formado por todos los elementos que no se descomponen como producto de irreducibles. Supongamos que B es no vacío. Sea b el elemento dado por el Lema 69. Como $b \in B$ tenemos que b no es irreducible, así que $b = b_1 b_2$ y con $b_i \nsim b$. Como $b_i \mid b$ y $b_i \nsim b$ tenemos que $b_i \notin B$. Entonces tanto b_1 como b_2 tienes descomposiciones como producto de irreducibles, es decir, $b_1 = p_1 \cdots p_s$ y $b_2 = q_1 \cdots q_t$, de donde $b = b_1 b_2 = p_1 \cdots p_s q_1 \cdots q_t$ tiene una descomposición como producto de irreducibles, es decir, $b \notin B$, lo que contradice la elección de b. Así $B = \varnothing$ y todo elemento de A se escribe como producto de irreducibles.

Vayamos con la unicidad. Si $a = p_1 \cdots p_s = q_1 \cdots q_t$, entonces $p_1 \mid q_1 \cdots q_t$. Por el Lema 66 p_1 divide a algún q_i, que podemos suponer q_1 después de reordenar. Como q_1 es irreducible tenemos que $p_1 \sim q_1$. La reiteración del proceso nos da la unicidad. □

3.12 Criterios de Irreducibilidad de Polinomios

Proposición 71 (Criba de Eratóstenes)**.** *Sea $p \in \mathbb{Z}$. p es primo si y sólo si para todo natural n con $2 \leq n \leq \sqrt{|p|}$, $n \nmid p$.*

Demostración. Basta observar que si $p = ab$ el valor absoluto de alguno de los factores debe ser menor o igual que $\sqrt{|p|}$. □

Observación 72. La Criba de Eratóstenes proporciona un algoritmo para determinar si un natural p dado es irreducible o no, calcular las divisiones de p entre todos los naturales menores que $\sqrt{p}$. De esta forma tenemos un procedimiento para determinar sin ningún género de duda si un entero es primo o no. Por otra parte la Criba de Eratóstenes tiene complejidad exponencial, aunque existen algoritmos que determinan la primalidad de un entero en tiempo polinomial.

Observación 73. Lamentablemente la situación no es tan cómoda en $\Bbbk[x]$. Por ejemplo todos los polinomios de la forma $x - \alpha$ con $\alpha \in \Bbbk$ son irreducibles (lo que se argumenta fácilmente con el grado) y no asociados (el coeficiente de x es uno). Así pues, si $\Bbbk$ es infinito un algoritmo tipo Criba de Eratóstenes parece no funcionar a priori.

Vamos a estudiar cuándo un polinomio tiene como factor a un polinomio de grado uno.

Definición 74. Sea $p(x) = a_0 + \cdots + a_n x^n \in \Bbbk[x]$. Denotamos también por p a la aplicación

$$\begin{aligned} p : \Bbbk &\longrightarrow \Bbbk \\ \alpha &\longmapsto a_0 + a_1\alpha + \cdots + a_n\alpha^n \end{aligned}$$

Esta aplicación se llama *evaluación*.

Lema 75. *Sea p un polinomio y $a \in \Bbbk$. Existe un único $q \in \Bbbk[x]$ tal que*

$$p(x) = q(x)(x - a) + p(a).$$

Demostración. Por la división $p(x) = q(x)(x - a) + b$ con $b \in \Bbbk$ (el resto tiene grado cero porque el divisor tiene grado uno). Así

$$p(a) = q(a)(a - a) + b = q(a)0 + b = b.$$

□

Proposición 76. *$(x - a) \mid p(x)$ si y sólo si $p(a) = 0$.*

Si $p(a) = 0$ se dice que a es una raíz de p. Este resultado permite comprobar si un polinomio tiene raíces, o equivalentemente factores de grado uno.

Algoritmo de Horner–Ruffini

Sea el polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \Bbbk[x]$, y sea $a \in \Bbbk$. Sean

$$\begin{aligned} b_n &= a_n \\ b_{n-1} &= a_{n-1} + b_n a \\ &\vdots \\ b_j &= a_j + b_{j+1} a \qquad \text{y} \qquad q(x) = b_1 + b_2 x + \cdots + b_n x^{n-1} \\ &\vdots \\ b_0 &= a_0 + b_1 a \end{aligned}$$

Entonces

$$p(x) = q(x)(x - a) + b_0 \quad \text{y} \quad p(a) = b_0$$

Observación 77. Si $\Bbbk$ es un cuerpo finito, la evaluación en todos los elementos de $\Bbbk$ permite determinar si cierto polinomio tiene factores de grado uno. A partir de este algoritmo, y dado que hay un número finito de polinomios de un grado fijo, podemos construir TODOS los polinomios irreducibles del grado que queramos. Por ejemplo, serán irreducibles aquellos de grado dos que no tengan raíces. Lo mismo podemos decir de los de grado tres. Para los de grado cuatro basta estudiar sus raíces y si tienen algún factor irreducible de grado dos, que ya son conocidos. Podemos reiterar este procedimiento hasta el grado que queramos. Lamentablemente la complejidad es horrorosa, y mucho peor si $\Bbbk$ es grande.

Observación 78. Los casos $\Bbbk = \mathbb{R}, \mathbb{Q}$ no pueden estudiarse a priori de la misma manera ya que son infinitos. Vamos a estudiar en primer lugar $\mathbb{Q}[x]$. Todo polinomio con coeficientes racionales tiene como asociado otro en $\mathbb{Z}[x]$, es decir, otro cuyos coeficientes son enteros. Comprobamos primeramente que las posibles raíces son un conjunto finito.

Proposición 79. *Sea $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ donde $a_n \neq 0$. Sea $\frac{a}{b} \in \mathbb{Q}$ tal que $\operatorname{mcd}(a, b) = 1$. Si $p(\frac{a}{b}) = 0$ entonces $a \mid a_0$ y $b \mid a_n$.*

Demostración. Si $p(\frac{a}{b}) = 0$ entonces

$$a_0 + a_1\frac{a}{b} + \cdots + a_n\left(\frac{a}{b}\right)^n = 0$$

y multiplicando por b^n tenemos

$$a_0 b^n + a_1 a b^{n-1} + \cdots + a_n a^n = 0.$$

Por tanto $a \mid a_0 b^n$, y al ser a y b primos relativos necesariamente $a \mid a_0$. Análogamente $b \mid a_n$. □

Observación 80. Por tanto las posibles raíces de $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ hay que buscarlas en el conjunto $\{\frac{a}{b} \mid a \mid a_0, b \mid a_n\}$, que es un conjunto finito.

3.13 Cuerpos Finitos

Terminamos el tema con una de las principales aplicaciones de los polinomios irreducibles, la construcción de los cuerpos finitos. A lo largo de esta sección $\mathbb{F}$ representa un cuerpo con un número finito de elementos. Vamos a tratar de analizar cuántos elementos puede tener $\mathbb{F}$.

Proposición 81. *Si $\mathbb{F}$ es un cuerpo finito entonces $\mathbb{F}$ tiene p^f elementos con p un número primo.*

El siguiente teorema es una de las piezas clave en la clasificación de los cuerpos con un número finito de elementos.

Teorema 82. *Dados $p \in \mathbb{Z}$ primo y $f \geq 1$, existe un polinomio irreducible de grado f sobre $\mathbb{Z}_p[x]$.*

Dados un primo p y un natural f, el Teorema 82 permite construir un cuerpo finito con p^f elementos. Dicho cuerpo se denota por $\mathbb{F}$, y podemos verlo como $\mathbb{Z}_p[x]_\phi$, el conjunto de los restos obtenidos al dividir entre ϕ, donde ϕ es un polinomio irreducible de grado f en $\mathbb{Z}_p[x]$ (el problema de encontrar dicho polinomio no lo vamos a considerar por ahora). La suma y el producto se realizan conforme a la Definición 62, y el inverso se calcula con la versión extendida del algoritmo de Euclides que proporciona los coeficientes de Bezout, de manera totalmente análoga al algoritmo 23 del Tema 3.

TEMA 4

Matrices y sistemas de ecuaciones

4.1 Aritmética de Matrices

En este tema $\mathbb{k}$ representa un cuerpo, es decir, un conjunto $\mathbb{k}$ junto con dos operaciones suma y producto tales que

suma asociativa $x + (y + z) = (x + y) + z$ para cualesquiera $x, y, z \in \mathbb{k}$,

elemento neutro de la suma existe $0 \in \mathbb{k}$ tal que $x + 0 = 0 + x = x$ para cualquier $x \in \mathbb{k}$,

elemento opuesto para cualquier $x \in \mathbb{k}$ existe $-x \in \mathbb{k}$ tal que $x + (-x) = (-x) + x = 0$,

suma conmutativa $x + y = y + x$ para cualesquiera $x, y \in \mathbb{k}$,

producto asociativo $x(yz) = (xy)z$ para cualesquiera $x, y, z \in \mathbb{k}$,

elemento neutro para el producto existe $1 \in \mathbb{k} \setminus \{0\}$ tal que $x1 = 1x = x$ para cualquier $x \in \mathbb{k}$,

elemento inverso para cualquier $x \in \mathbb{k} \setminus \{0\}$ existe $x^{-1} \in \mathbb{k}$ tal que $xx^{-1} = x^{-1}x = 1$,

producto conmutativo $xy = yx$ para cualesquiera $x, y \in \mathbb{k}$,

distributiva del producto con respecto de la suma $x(y + z) = xy + xz$ y $(x + y)z = xz + yz$ para cualesquiera $x, y, z \in \mathbb{k}$.

Definición 1. Una matriz de m filas y n columnas sobre un cuerpo $\mathbb{k}$ es una aplicación

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \longrightarrow \mathbb{k}, \ \left[(i, j) \longmapsto a_{ij}\right].$$

Normalmente se representa a una matriz A de la forma siguiente:

$$A = \left(a_{ij}\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

El conjunto de las matrices de m filas y n columnas sobre $\mathbb{k}$ se denota $\mathcal{M}_{m\times n}(\mathbb{k})$

Definición 2. Sean $A, B \in \mathcal{M}_{m\times n}(\mathbb{k})$. Se define la suma de A y B como

$$A + B : \{1, \dots, m\} \times \{1, \dots, n\} \longrightarrow \mathbb{k}, \ \left[(i, j) \longmapsto a_{ij} + b_{ij}\right],$$

es decir,

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

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

Definición 3. Sean $A \in \mathcal{M}_{m\times n}(\Bbbk)$ y $B \in \mathcal{M}_{n\times p}(\Bbbk)$. Definimos el producto de A por B como

$$AB : \{1,\dots,m\} \times \{1,\dots,p\} \longrightarrow \Bbbk, \quad \left[(i,j) \longmapsto \sum_{k=1}^{n} a_{ik}b_{kj}\right],$$

o en otra notación

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mp} \end{pmatrix}$$

donde $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$.

Proposición 4. *La suma y el producto de matrices satisfacen las propiedades siguientes:*

suma asociativa $A + (B + C) = (A + B) + C$ *para cualesquiera* $A, B, C \in \mathcal{M}_{m\times n}(\Bbbk)$,

elemento neutro de la suma *existe* $0 \in \mathcal{M}_{m\times n}(\Bbbk)$ *tal que* $A + 0 = 0 + A = A$ *para cualquier* $A \in \mathcal{M}_{m\times n}(\Bbbk)$,

elemento opuesto *para cualquier* $A \in \mathcal{M}_{m\times n}(\Bbbk)$ *existe* $-A \in \mathcal{M}_{m\times n}(\Bbbk)$ *tal que* $A + (-A) = (-A) + A = 0$,

suma conmutativa $A + B = B + A$ *para cualesquiera* $A, B \in \mathcal{M}_{m\times n}(\Bbbk)$,

producto asociativo $A(BC) = (AB)C$ *para cualesquiera* $A, B, C \in \mathcal{M}_{*\times *}(\Bbbk)$,

elemento neutro para el producto *para cada* $n \in \mathbb{N}$ *existe* $I_n \in \mathcal{M}_{n\times n}(\Bbbk)$ *tal que* $AI_n = I_mA = A$ *para cualquier* $A \in \mathcal{M}_{m\times n}(\Bbbk)$,

distributiva del producto con respecto de la suma $A(B+C) = AB+AC$ *y* $(A+B)C = AC+BC$ *para cualesquiera* $A, B, C \in \mathcal{M}_{*\times *}(\Bbbk)$.

La matriz cero y la matriz identidad, elementos neutros para la suma y el producto, son

$$\left(0\right)_{\substack{1\le i\le m\\ 1\le j\le n}} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad I_n = \left(\delta_{ij}\right)_{1\le i,j\le n} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Las matrices con igual número de filas y de columnas se llaman matrices cuadradas. Para denotarlas empleamos un único tamaño: $\mathcal{M}_n(\Bbbk) = \mathcal{M}_{n\times n}(\Bbbk)$

Teorema 5. $(\mathcal{M}_n(\Bbbk), +, \cdot)$ *es un anillo.*

El producto de matrices es no conmutativo

1. Porque hay matrices que pueden multiplicarse en un orden y no en otro.
2. Porque hay matrices que aún multiplicándose en los dos órdenes los resultados tienen tamaño distinto.
3. Porque incluso hay matrices cuadradas cuyo producto en los dos sentidos dan resultados distintos.

Definición 6. Dada una matriz, se define su traspuesta como aquella que se obtiene intercambiando filas por columnas, es decir,

$$A = \left(a_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathcal{M}_{m\times n}(\Bbbk) \rightsquigarrow A^t = \left(a_{ji}\right)_{\substack{1\le j\le n\\ 1\le i\le m}} \in \mathcal{M}_{n\times m}(\Bbbk)$$

Definición 7. Una matriz cuadrada $A \in \mathcal{M}_n(\Bbbk)$ se dice simétrica si $A = A^t$.

Proposición 8. *Para cualesquiera matrices* A, B *de tamaños adecuados,*

$$(A + B)^t = A^t + B^t \text{ y } (AB)^t = B^tA^t$$

Definición 9. Una matriz por bloques es una matriz

$$A = \left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \cdots & A_{1r} \\ \hline A_{21} & A_{22} & \cdots & A_{2r} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_{s1} & A_{s2} & \cdots & A_{sr} \end{array}\right)$$

donde cada $A_{ij} \in \mathcal{M}_{*\times *}(\mathbb{k})$ de modo que matrices en la misma fila tienen el mismo número de filas y matrices en la misma columna el mismo número de columnas.

Proposición 10. *Sean* $A = \left(A_{ij}\right)_{s\times r}$ *y* $B = \left(B_{ij}\right)_{r\times t}$ *dos matrices por bloques de tamaños adecuados. Entonces*

$$AB = C = \left(C_{ij}\right)_{s\times t} \text{ donde } C_{ij} = \sum_{k=1}^{r} A_{ik}B_{kj}$$

4.2 Matrices escalonadas reducidas

Definición 11. Para una matriz cualquiera, el primer elemento no nulo de cada fila se llama pivote. Una matriz $A \in \mathcal{M}_{m\times n}(\mathbb{k})$ se dice que está en forma escalonada reducida si

1. las filas nulas (todos sus elementos son 0) ocupan las últimas posiciones de la matriz.
2. el pivote de cada fila es un 1,
3. si $i < j$, el pivote de la fila j está más a la derecha del pivote de la fila i,
4. el resto de los elementos de cada columna que contiene a un pivote es 0.

Definición 12. Sobre una matriz de cualquier tamaño definimos tres tipos de transformaciones elementales sobre las filas de la matriz:

Tipo 1 Intercambiar dos filas.

Tipo 2 Multiplicar una fila por una constante no nula.

Tipo 3 Sumar a una fila un múltiplo de otra.

Definición 13. Decimos que A y B son equivalentes por filas si existe una sucesión de transformaciones elementales sobre las filas $\sim_1, \sim_2, \ldots, \sim_t$ tales que

$$A \sim_1 A' \sim_2 \cdots \sim_t B.$$

Este hecho se denota $A \sim_f B$. Es sencillo comprobar que ser equivalentes por filas es una relación de equivalencia.

Teorema 14. *Dada una matriz A es equivalente por filas a una única matriz escalonada reducida H. H recibe el nombre de forma normal de Hermite de A.*

La demostración de la existencia de H consiste en describir el método de Gauss-Jordan para el cálculo de H. Para cada fila y en orden secuencial desde la primera hasta la última,

1. intercambiamos la fila actual por cualquiera que esté debajo de ella y que tenga su pivote lo más a la izquierda posible,
2. multiplicamos la fila por el inverso del pivote,
3. sumamos a cada una de las demás filas el correspondiente múltiplo de la fila actual hasta conseguir que todos los elementos por encima y por debajo del pivote sean 0.

Definición 15. Se define el rango de una matriz A como el número de filas no nulas de su forma normal de Hermite.

Proposición 16. *Si* $A \in \mathcal{M}_{m\times n}(\mathbb{k})$*, entonces* $\text{rango}(A) \leq \min\{m, n\}$.

4.3 Matrices regulares

Llamaremos matrices elementales de orden n a aquellas matrices cuadradas que se obtienen aplicando una transformación elemental a la matriz identidad. Tenemos por tanto tres tipos de matrices elementales.

$$E_{ij} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \dots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \; E_i(\alpha) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \text{ y}$$

$$E_{ij}(\alpha) = \begin{pmatrix} 1 & & & & \\ & \ddots & & \alpha & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \text{ o } E_{ij}(\alpha) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ \alpha & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

Proposición 17. *Sea $A \in \mathcal{M}_{m\times n}(\Bbbk)$ y sea $E \in \mathcal{M}_m(\Bbbk)$ una matriz elemental. Entonces EA es la matriz que se obtiene a partir de A aplicando a sus filas la misma transformación elemental elemental con la que se obtiene E a partir de I_m.*

Corolario 18. *Sean $A, H \in \mathcal{M}_{m\times n}(\Bbbk)$ tales que H es la forma normal de Hermite de A. Existen matrices elementales $E_1, \dots, E_t \in \mathcal{M}_m(\Bbbk)$ tales que*

$$H = E_t E_{t-1} \dots E_1 A$$

Definición 19. Una matriz cuadrada $A \in \mathcal{M}_n(\Bbbk)$ se dice regular si tiene inversa para el producto, es decir, si existe $B \in \mathcal{M}_n(\Bbbk)$ tal que $AB = BA = I_n$

Lo primero que hay que observar es que de existir la inversa es única: si B_1 y B_2 son inversas de A entonces

$$B_1 = B_1 I_n = B_1(AB_2) = (B_1A)B_2 = I_nB_2 = B_2.$$

La inversa de A, en caso de existir, se denota A^{-1} Dos propiedades muy fáciles de comprobar son:

1. $(AB)^{-1} = B^{-1}A^{-1}$,
2. $(A^t)^{-1} = (A^{-1})^t$.

Proposición 20. *Las matrices elementales son regulares, y sus inversas son matrices elementales.*

Teorema 21. *Para una matriz $A \in \mathcal{M}_n(\Bbbk)$ son equivalentes las siguientes afirmaciones:*

1. *A es regular,*
2. *$\text{rango}(A) = n$,*
3. *la forma de Hermite de A es I_n,*
4. *A se puede escribir como un producto de matrices elementales.*

Corolario 22. *$H \in \mathcal{M}_{m\times n}(\Bbbk)$ es la forma de Hermite de $A \in \mathcal{M}_{m\times n}(\Bbbk)$ si y sólo si existe una matriz regular $P \in \mathcal{M}_m(\Bbbk)$ tal que $H = PA$.*

Para calcular la inversa de una matriz procedemos de la siguiente forma.

1. Dada una matriz $A \in \mathcal{M}_n(\Bbbk)$, construimos la matriz $(A|I_n) \in \mathcal{M}_{n\times 2n}(\Bbbk)$.

2. Calculamos la forma normal de Hermite $H \sim_f (A|I_n)$.
3. Si $H = (I_n|B)$ entonces A es regular y su inversa es B, en caso contrario A no es regular.

La misma idea sirve para calcular la matriz de paso junto a la forma de Hermite:

1. Dada una matriz $A \in \mathcal{M}_{m\times n}(\Bbbk)$, construimos la matriz $(A|I_m) \in \mathcal{M}_{m\times(n+m)}(\Bbbk)$.
2. Calculamos la forma normal de Hermite $H \sim_f (A|I_m)$.
3. Si $H = (H_A|P)$ entonces H_A es la forma de Hermite de A y $H_A = PA$.

4.4 Sistemas de ecuaciones lineales

Definición 23. Un sistema de ecuaciones lineales (SEL) sobre un cuerpo $\Bbbk$ es una expresión de la forma

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned} \tag{7}$$

donde $a_{ij}, b_i \in \Bbbk$ para cualesquiera $1 \leq i \leq m$, $1 \leq j \leq n$.

Definición 24. Una solución de (7) es una lista $(s_1, s_2, \ldots, s_n) \in \Bbbk^n$ tal que

$$\begin{aligned} a_{11}s_1 + a_{12}s_2 + \cdots + a_{1n}s_n &= b_1 \\ a_{21}s_1 + a_{22}s_2 + \cdots + a_{2n}s_n &= b_2 \\ &\vdots \\ a_{m1}s_1 + a_{m2}s_2 + \cdots + a_{mn}s_n &= b_m \end{aligned}$$

Asociado al sistema de ecuaciones (7), podemos definir dos matrices la matriz de los coeficientes y la matriz de los términos independientes:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Estas matrices permiten describir el sistema (7) de forma matricial como

$$AX = B \tag{8}$$

donde

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Un sistema de ecuaciones lineales

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

está por tanto determinado por la llamada matriz ampliada:

$$(A|B) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

Cada matriz sistema con m ecuaciones y n incógnitas está determinado por una matriz de tamaño $m \times (n+1)$, y recíprocamente cada matriz de tamaño $m \times (n+1)$ determina un sistema con m ecuaciones y n incógnitas.

Definición 25. Dos sistemas se dicen equivalentes si tienen las mismas soluciones.

Proposición 26. *Los sistemas asociados a dos matrices que se diferencian en transformaciones elementales sobre filas son equivalentes, es decir, si* $(A|B) \sim_f (A'|B')$*, entonces los sistemas de ecuaciones*

$$AX = B \text{ y } A'X = B'$$

tienen las mismas soluciones.

Esta proposición es sencilla de demostrar una vez que sabemos que las transformaciones elementales se corresponden con los productos por matrices elementales.

Definición 27. Un sistema se llama *compatible* si tiene solución, en caso contrario se llama *incompatible*.
Un sistema compatible se llama *determinado* si la solución es única. En caso contrario se llama *indeterminado*.

Teorema 28 (Rouché–Frobenius)**.** *Un sistema* $AX = B$ *es compatible si y solo si* $\operatorname{rango}(A) = \operatorname{rango}(A|B)$*; en otro caso es incompatible. Un sistema compatible es determinado si y solo si* $\operatorname{rango}(A) = n$*, el número de incógnitas; en otro caso es indeterminado.*

4.5 Determinantes

Dada una matriz $M \in \mathcal{M}_{m\times n}(\Bbbk)$, denotamos M_{ij} a la submatriz de M que se obtiene eliminando la fila i y la columna j de A.

Definición 29. Definimos el determinante de una matriz cuadrada $A \in \mathcal{M}_n(\Bbbk)$ de forma recursiva:

- Si $A = (a) \in \mathcal{M}_1(\Bbbk)$ entonces $\det(A) = a$.
- Si $A \in \mathcal{M}_n(\Bbbk)$ llamamos $\alpha_{ij} = (-1)^{i+j}\det(A_{ij})$ (que ya está definido por tener un tamaño menor), y definimos

$$\det(A) = a_{11}\alpha_{11} + a_{12}\alpha_{12} + \cdots + a_{1n}\alpha_{1n}.$$

Se denota

$$\det(A) = |A| = \det\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Propiedad 1

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 + y_1 & x_2 + y_2 & \dots & x_n + y_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Propiedad 2

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

En particular el determinante es cero si hay dos filas iguales.

Propiedad 3

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda x_1 & \lambda x_2 & \dots & \lambda x_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \lambda \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Propiedad 4

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 + \lambda y_1 & x_2 + \lambda y_2 & \dots & x_n + \lambda y_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Propiedad 5

$$\det(AB) = \det(A)\det(B).$$

Propiedad 6

$$\det(A^t) = \det(A).$$

Propiedad 7

$$A \text{ es regular} \iff \det(A) \neq 0$$

Propiedad 8

$$\det(A) = a_{i1}\alpha_{i1} + a_{i2}\alpha_{i2} + \cdots + a_{in}\alpha_{in}$$

para cualquier $1 \leq i \leq n$, donde $\alpha_{ij} = (-1)^{i+j}\det(A_{ij})$.

Los elementos $\alpha_{ij} = (-1)^{i+j}\det(A_{ij})$ reciben el nombre de adjuntos. La matriz

$$A^* = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}$$

se llama matriz adjunta. De las propiedades anteriores se deduce que para cualquier matriz $A \in \mathcal{M}_n(\Bbbk)$

$$A \cdot (A^*)^t = \det(A) I_n$$

y por lo tanto,

Teorema 30. *Si A es regular entonces $A^{-1} = \det(A)^{-1}(A^*)^t$.*

Proposición 31. *El rango de una matriz $A \in \mathcal{M}_{m\times n}(\Bbbk)$ coincide con el tamaño de la mayor submatriz cuadrada con determinante distinto de cero.*

TEMA 5

Espacios Vectoriales y Aplicaciones Lineales

5.1 Espacios Vectoriales. Bases

Como siempre $\mathbb{k}$ es un cuerpo. Un conjunto no vacío V es un $\mathbb{k}$–espacio vectorial si satisface las siguientes propiedades:

1. Existe una operación $+$ en V tal que $(V,+)$ es un grupo abeliano, es decir, la operación
   - es asociativa: $(u+v)+w = u+(v+w)$ para cualesquiera $u,v,w \in V$,
   - es conmutativa: $u+v = v+u$ para cualesquiera $u,v \in V$,
   - tiene elemento neutro: existe $0 \in V$ tal que $0+v = v+0 = v$ para cualquier $v \in V$,
   - tiene elemento opuesto: para cualquier $v \in V$, existe $-v \in V$ tal que $v+(-v) = (-v)+v = 0$.
2. Existe una acción de $\mathbb{k}$ sobre V denotada por yuxtaposición tal que
   - $a(u+v) = au+av$ para cualquier $a \in \mathbb{k}$ y cualesquiera $u,v \in V$,
   - $(a+b)u = au+bu$ para cualesquiera $a,b \in \mathbb{k}$ y cualquier $u \in V$,
   - $a(bu) = (ab)u$ para cualesquiera $a,b \in \mathbb{k}$ y cualquier $u \in V$,
   - $1u = u$ para cualquier $u \in V$.

Ya conocemos muchos ejemplos:

- $\mathcal{M}_{m\times n}(\mathbb{k})$,
- $\mathbb{k}^n$,
- $\mathbb{k}[x]$,
- $\mathbb{k}[x]_m = \{p(x) \in \mathbb{k}[x] \mid \deg(p) \leq m\}$,
- el conjunto de las funciones reales definidas en un intervalo fijo sobre $\mathbb{R}$,
- soluciones de un sistema de ecuaciones lineales homogéneo.

Proposición 1. *Sea V un $\mathbb{k}$–espacio vectorial. Para cualesquiera $a,b \in \mathbb{k}$ y $u,v \in V$ se tiene que:*

- $0u = 0$,
- $a0 = 0$,
- *si* $au = 0$ *entonces* $a = 0$ *o* $u = 0$,
- $-(au) = (-a)u = a(-u)$,
- $a(u-v) = au-av$,
- $(a-b)u = au-bu$.

Definición 2. Sean $\{v_1, \ldots, v_n\} \subseteq V$. Una *combinación lineal* de $\{v_1, \ldots, v_n\}$ es un vector de la forma

$$a_1 v_1 + \cdots + a_n v_n = \sum_{i=1}^{n} a_i v_i$$

donde $a_1, \ldots, a_n \in \mathbb{k}$.

Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se dice *linealmente dependiente* si el vector 0 se puede escribir como una combinación lineal de $\{v_1, \ldots, v_n\}$ en la que no todos los escalares son cero, es decir,

$$\exists a_1, \ldots, a_n \in \mathbb{k}\ \exists i_0 \in \{1, \ldots, n\} \mid a_{i_0} \neq 0 \text{ y } a_1 v_1 + \cdots + a_n v_n = 0.$$

Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se dice *linealmente independiente* si no es linealmente dependiente, es decir,

$$a_1 v_1 + \cdots + a_n v_n = 0 \Longrightarrow a_1 = \cdots = a_n = 0.$$

Proposición 3.

- *Si* $0 \in \{v_1, \ldots, v_n\}$ *entonces* $\{v_1, \ldots, v_n\}$ *es linealmente dependiente.*
- $\{v\}$ *es linealmente independiente si y solo si* $v \neq 0$.
- *Si* $\{v_1, \ldots, v_n\}$ *es linealmente dependiente entonces* $\{v_1, \ldots, v_n, v_{n+1}, \ldots, v_r\}$ *es linealmente dependiente.*
- *Si* $\{v_1, \ldots, v_n, v_{n+1}, \ldots, v_r\}$ *es linealmente independiente entoces* $\{v_1, \ldots, v_n\}$ *es linealmente independiente.*

Proposición 4. *Un conjunto* $\{v_1, \ldots, v_n\}$ *es linealmente dependiente si y solo si uno de los vectores se puede escribir como combinación lineal de los demás.*

Definición 5. Se dice que $S \subseteq V$ es un *sistema de generadores* de V si todo vector de V se puede expresar como combinación lineal de un subconjunto finito de S.

Proposición 6. *Si* $\{v_1, \ldots, v_n\}$ *es un sistema de generadores de* V *y* v_i *es combinación lineal de los demás, entonces* $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ *es un conjunto de generadores de* V.

Lema 7. *Si* $\{v_1, \ldots, v_m\}$ *es linealmente independiente y* $\{u_1, \ldots, u_s\}$ *es un sistema de generadores entonces* $m \leq s$.

Definición 8. Una base de un espacio vectorial V es un subconjunto $B \subseteq V$ tal que

- B es linealmente independiente,
- B es sistema de generadores.

Teorema 9 (Teorema de la base). *Si un espacio vectorial* V *tiene una base formada por un número finito de vectores entonces todas las bases de* V *son finitas y tienen el mismo número de vectores.*

Definición 10. Si V tiene una base finita definimos la dimensión de V como

$$\dim(V) = \dim_{\mathbb{k}}(V) = |B|$$

donde B es una base cualquiera de V.

Teorema 11. *En un espacio vectorial, de cada sistema de generadores finito puede extraerse una base.*

Teorema 12. *Sea* V *un espacio vectorial de dimensión* n *y sea* $\{v_1, \ldots, v_m\}$ *un conjunto linealmente independiente. Existen vectores* $\{v_{m+1}, \ldots, v_n\}$ *tales que* $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ *es una base de* V.

Corolario 13. *Sea* V *un espacio vectorial de dimensión* n *y sea* $\{v_1, \ldots, v_n\} \subseteq V$. *Son equivalentes:*

(1) $\{v_1, \ldots, v_n\}$ *es linealmente independiente,*

(2) $\{v_1, \ldots, v_n\}$ *es sistema de generadores de* V,

(3) $\{v_1, \ldots, v_n\}$ *es una base de* V.

Proposición 14. *Sea* $B = \{e_1, \ldots, e_n\}$ *una base de un* $\mathbb{k}$*–espacio vectorial* V. *Entonces todo vector se escribe de forma única como combinación lineal de los vectores de* B.

Si $B = \{e_1, \dots, e_n\}$ es una base y $v \in V$ entonces existe un único $(x_1, \dots, x_n) \in \mathbb{k}^n$ tal que $x = x_1 e_1 + \cdots + x_n e_n$. Se suele denotar

$$x_B = (x_1, \dots, x_n),$$

y $(x_1, \dots, x_n)$ se llaman las coordenadas de x en la base B. La aritmética del espacio vectorial se recupera a partir de las coordenadas:

- $(x + y)_B = x_B + y_B$,
- $(\lambda x)_B = \lambda x_B$.

Proposición 15. *Sea V un $\mathbb{k}$–espacio vectorial y sea B una base. Un conjunto de vectores $\{v_1, \dots, v_r\} \subseteq V$ es linealmente independiente si y solo si la matriz que tiene por columnas (o por filas) las coordenadas de los vectores $\{v_1, \dots, v_r\}$ respecto de B tiene rango r.*

Teorema 16 (Cambio de base). *Sean $B = \{e_1, \dots, e_n\}$ y $B' = \{e'_1, \dots, e'_n\}$ dos bases de V. Sea $M_{B'B}$ la matriz que tiene como columnas las coordenadas de los vectores de B' en la base B, es decir*

$$M_{B'B} = ((e'_1)_B | \dots | (e'_n)_B).$$

Entonces para todo vector $v \in V$ se tiene

$$v_B = M_{B'B} v_{B'}.$$

$$M_{B''B} = M_{B'B} M_{B''B'}, \qquad M_{B'B}^{-1} = M_{BB'}.$$

5.2 Subespacios vestoriales

Definición 17. Un subconjunto no vacío U de un $\mathbb{k}$–espacio vectorial V es un subespacio vectorial si

- U es cerrado para sumas: $\forall u, v \in U$, $u + v \in U$,
- U es cerrado para producto de escalares: $\forall u \in U$ y $\forall \lambda \in \mathbb{k}$, $\lambda u \in U$.

Proposición 18. *Sea V un $\mathbb{k}$–espacio vectorial. Para $\varnothing \neq U \subseteq V$ son equivalentes:*

1. *U es un subespacio vectorial,*
2. *$\forall u, v \in U$ y $\forall \lambda, \mu \in \mathbb{k}$, $\lambda u + \mu v \in U$,*
3. *U es cerrado para combinaciones lineales.*

Dado $S \subseteq V$ denotamos $\langle S \rangle$ al conjunto de todas las combinaciones lineales de vectores de S, es decir,

$$\langle S \rangle = \{a_1 s_1 + \cdots + a_n s_n \mid a_i \in \mathbb{k}, s_i \in S, i = 1, \dots, n\}$$

Proposición 19. *$\langle S \rangle$ es el menor subespacio vectorial que contiene a S. Se llama el subespacio vectorial generado por S.*

Proposición 20. *Sea V un $\mathbb{k}$–espacio vectorial de dimensión n y sea B una base de V. Sea $U = \langle u_1, \dots, u_r \rangle$ y sea A la matriz $r \times n$ sobre $\mathbb{k}$ que tiene por filas las coordenadas de los vectores $u_1, \dots, u_r$ en la base B. Entonces*

- $\operatorname{rango}(A) = \dim U$,
- *las filas no nulas de la forma de Hermite de A son las coordenadas en B de una base de $\langle u_1, \dots, u_r \rangle$.*

Sea V un subespacio vectorial de dimensión n y sea B una base de V. Sea $U = \langle u_1, \dots, u_r \rangle$ un subespacio vectorial de V. Las coordenadas de los vectores $\{u_1, \dots, u_r\}$ en B las denotamos por

$$(u_i)_B = (c_{1i}, c_{2i}, \dots, c_{ni}) \quad 1 \leq i \leq r.$$

Por tanto, si $x \in U$ tenemos que $x = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_r u_r$ y si sus coordenadas en B son $x_B = (x_1, x_2, \dots, x_n)$ éstas deben verificar

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{n1} \end{pmatrix} \lambda_1 + \begin{pmatrix} c_{12} \\ c_{22} \\ \vdots \\ c_{n2} \end{pmatrix} \lambda_2 + \cdots + \begin{pmatrix} c_{1r} \\ c_{2r} \\ \vdots \\ c_{nr} \end{pmatrix} \lambda_r,$$

o equivalentemente

$$\begin{cases} x_1 = c_{11}\lambda_1 + c_{12}\lambda_2 + \cdots + c_{1r}\lambda_r \\ x_2 = c_{21}\lambda_1 + c_{22}\lambda_2 + \cdots + c_{2r}\lambda_r \\ \qquad \vdots \\ x_n = c_{n1}\lambda_1 + c_{n2}\lambda_2 + \cdots + c_{nr}\lambda_r. \end{cases} \tag{9}$$

Las ecuaciones (9) reciben el nombre de *ecuaciones implícitas o paramétricas* de U. Estas ecuaciones permiten producir todos vectores de U a partir de todos los posibles valores asignables a los parámetros. Es inmediato calcular unas ecuaciones paramétricas a partir de un sistema de generadores de U y viceversa.

Por otra parte las ecuaciones (9) pueden verse como las soluciones de un sistema de ecuaciones homogéneo. Decimos que un sistema de ecuaciones homogéneo forma unas *ecuaciones explícitas o cartesianas* de U si su conjunto de soluciones constituyen unas ecuaciones paramétricas de U.

Sean

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{10}$$

unas ecuaciones cartesianas de U.

¿Cómo podemos calcular unas ecuaciones paramétricas (9) de U a partir de unas ecuaciones cartesianas (10) de U? Este paso es sencillo, resolviendo el sistema dado por (10). De esta forma podemos construir un sistema de generadores y una base de U.

¿Cómo podemos calcular unas ecuaciones cartesianas (10) de U a partir de unas ecuaciones paramétricas (9) de U? Consideremos las variables de (9) como parámetros y viceversa, es decir, consideremos el sistema de ecuaciones lineales

$$\begin{cases} c_{11}\lambda_1 + c_{12}\lambda_2 + \cdots + c_{1r}\lambda_r = x_1 \\ c_{21}\lambda_1 + c_{22}\lambda_2 + \cdots + c_{2r}\lambda_r = x_2 \\ \qquad\qquad\qquad\qquad \vdots \\ c_{n1}\lambda_1 + c_{n2}\lambda_2 + \cdots + c_{nr}\lambda_r = x_n \end{cases} \tag{11}$$

o en forma matricial

$$C\Lambda = X.$$

Los elementos de U son aquellos para los cuales el sistema de ecuaciones (11) tiene solución, es decir, aquellos para los cuales $\text{rango}(C) = \text{rango}(C|X)$. Por tanto, si calculamos transformaciones sobre las filas para calcular el rango tenemos:

$$\left(\begin{array}{cccc|c} c_{11} & c_{12} & \cdots & c_{1r} & x_1 \\ c_{21} & c_{22} & \cdots & c_{2r} & x_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nr} & x_n \end{array}\right) \sim_f \left(\begin{array}{c|c} H & * \\ \hline 0 & \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{array} \end{array}\right)$$

donde H es la forma de Hermite de C (o cualquier matriz escalonada equivalente a C). Unas ecuaciones cartesianas de U vienen dadas al hacer cero las últimas filas por debajo de H, es decir,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

Proposición 21. *Sea V un $\Bbbk$–espacio vectorial de dimensión n y sea U un subespacio vectorial de V. Sean $AX = 0$ y $X = C\Lambda$ ecuaciones cartesianas y paramétricas respectivamente de U. Entonces:*

- $\dim U + \text{rango}(A) = n$,
- $\dim U = \text{rango}(C)$.

Proposición 22. *Sean U y W dos subespacios vectoriales de un $\Bbbk$–espacio vectorial V.*

- *$U \cap W$ es un subespacio vectorial de V, el mayor subespacio vectorial contenido en U y W.*
- *El conjunto $U + W = \{u + w \mid u \in U, w \in W\}$ es un subespacio vectorial de V, el menor subespacio vectorial que contiene tanto a U como a W. Se llama la suma de U y W.*

Proposición 23. *Si $U = \langle S \rangle$ y $W = \langle T \rangle$ entonces $U + W = \langle S \cup T \rangle$.*

Proposición 24. *Sea V un $\Bbbk$–espacio vectorial de dimensión n y sean U y W subespacios vectoriales. Sean*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases} \quad y \quad \begin{cases} b_{11}x_1 + \cdots + b_{1n}x_n = 0 \\ \vdots \\ b_{p1}x_1 + \cdots + b_{pn}x_n = 0 \end{cases}$$

ecuaciones cartesianas de U y W respectivamente. Entonces unas ecuaciones cartesianas de $U \cap W$ son

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \\ b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n = 0 \\ \vdots \\ b_{p1}x_1 + b_{p2}x_2 + \cdots + b_{pn}x_n = 0 \end{cases}$$

Definición 25. Sea V un $\Bbbk$–espacio vectorial y sean U y W subespacios vectoriales. Decimos que la suma de U y W es directa si $U \cap W = \{0\}$. En este caso la suma se denota $U + W = U \oplus W$.

Proposición 26. *Sea V un $\Bbbk$–espacio vectorial de dimensión n y sean U y W subespacios vectoriales tales que $U \cap W = \{0\}$. Si B es una base de U y C una base de W entonces $B \cup C$ es una base de $U \oplus W$.*

Proposición 27 (Fórmula de las dimensiones)**.** *Sea V un $\Bbbk$–espacio vectorial de dimensión n y sean U y W subespacios vectoriales. Entonces*

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

5.3 Aplicaciones lineales

Definición 28. Una aplicación $f : V \to V'$ entre $\Bbbk$–espacios vectoriales V y V' se dice *lineal* si

(1) $f(u + v) = f(u) + f(v)$, $\forall u, v \in V$,

(2) $f(\lambda u) = \lambda f(u)$, $\forall \lambda \in \Bbbk$, $\forall u \in V$.

O equivalentemente si

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v),\ \forall \lambda, \mu \in \Bbbk,\ \forall u, v \in V.$$

Proposición 29. *Cualquier aplicación lineal $f : V \to V'$ verifica*

1. $f(0) = 0$,
2. $f(-u) = -f(u)$,
3. $f(\sum_{i=1}^{n} \lambda_i u_i) = \sum_{i=1}^{n} \lambda_i f(u_i)$ *para cualesquiera* $\lambda_1, \ldots, \lambda_n \in \Bbbk$ $u_1, \ldots, u_n \in V$.

Lema 30. *Sea $f : V \to V'$ una aplicación lineal y sea U un subespacio vectorial de V. Entonces $f(U)$ es un subespacio vectorial de V'. En particular* $\operatorname{im} f$ *es un subespacio vectorial de V'.*

Lema 31. *Sea $f : V \to V'$ una aplicación lineal y sea $S \subseteq V$. Entonces $f(\langle S \rangle) = \langle f(S) \rangle$. En particular, si S es un sistema de generadores de V entonces* $\operatorname{im} f$ *está generado por $f(S)$.*

Como consecuencia de los resultados anteriores podemos determinar si una aplicación lineal es sobreyectiva calculando la dimensión de $\operatorname{im} f$ y comparándola con la dimensión de V'. Además

Lema 32. *Una aplicación lineal $f : V \to V'$ es sobreyectiva si y solo si para cada sistema de generadores $S \subseteq V$, $f(S)$ es un sistema de generadores de V'.*

Definición 33. Sea $f : V \to V'$ una aplicación lineal. Se define el núcleo de f como $\ker f = \{v \in V \mid f(v) = 0\}$.

Lema 34. *Una aplicación lineal $f : V \to V'$ es inyectiva si y sólo si* $\ker f = \{0\}$.

Lema 35. *Una aplicación lineal $f : V \to V'$ es inyectiva si y sólo si para cualquier conjunto $\{u_1, \ldots, u_r\}$ linealmente independiente el conjunto $\{f(u_1), \ldots, f(u_r)\}$ es también linealmente independiente.*

Sean $f, g : V \to V'$ aplicaciones lineales, y sea $\lambda \in \Bbbk$. Las siguientes aplicaciones son también lineales:

- Suma:

$$\begin{aligned} f + g : V &\longrightarrow V' \\ v &\longmapsto (f+g)(v) = f(v) + g(v) \end{aligned}$$

- Producto por escalar:

$$\begin{aligned} \lambda f : V &\longrightarrow V' \\ v &\longmapsto (\lambda f)(v) = \lambda f(v) \end{aligned}$$

Proposición 36. *Dados dos espacios vectoriales V y V', el conjunto* $\operatorname{Hom}_{\Bbbk}(V, V')$ *de todas las aplicaciones lineales de V en V' es un espacio vectorial.*

Proposición 37. *La composición de aplicaciones lineales es una aplicación lineal, es decir, si $f : V \to V'$ y $g : V' \to V''$ son aplicaciones lineales entonces $g \circ f = gf : V \to V''$ es lineal.*

Proposición 38. *Si una aplicación lineal $f : V \to V'$ es biyectiva entonces $f^{-1} : V' \to V$ es también una aplicación lineal.*

Dos espacios vestoriales V y V' se dicen *isomorfos* si existe una aplicación lineal biyectiva entre ellos. Las aplicaciones lineales biyectivas se llaman *isomorfismos*. Similarmente las aplicaciones lineales inyectivas se llaman *monomorfismos* y las aplicaciones lineales sobreyectivas se llaman *epimorfismos*.

5.4 Matrices y aplicaciones lineales

Sea $f : V \to V'$ una aplicación lineal y sean $B = \{e_1, \dots, e_n\}$ y $B' = \{e'_1, \dots, e'_m\}$ bases de V y V' respectivamente. Para cada $1 \leq j \leq n$ la imagen del correspondiente vector de B se escribe como combinación lineal de los vectores de B', es decir,

$$f(e_j) = a_{1j}e'_1 + a_{2j}e'_2 + \cdots + a_{mj}e'_m = \sum_{i=1}^{m} a_{ij}e'_j.$$

Sea $M_{BB'}(f)$ la matriz que tiene por columnas las coordenadas de las imágenes por f de los vectores de B respecto de B', es decir,

$$M_{BB'}(f) = \left(\begin{array}{c|c|c|c} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{array}\right)$$

Lema 39. *En la situación anterior, para cualquier vector $v \in V$ si las coordenadas*[1] *de v con respecto a B son $v_B = (x_1, \dots, x_n)$, entonces las coordenadas de $f(v)$ con respecto a B' son*

$$f(v)_{B'} = M_{BB'}(f)v_B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Corolario 40. *Para conocer una aplicación lineal basta con conocer las imágenes de los vectores de una base del dominio.*

Proposición 41. *Sean $f, f_1, f_2 : V \to V'$ y $g : V' \to V''$ aplicaciones lineales, $\lambda \in \Bbbk$ y sean B, B' y B'' bases de V, V' y V'' respectivamente. Entonces:*

$$M_{BB'}(f_1 + f_2) = M_{BB'}(f_1) + M_{BB'}(f_2),$$
$$M_{BB'}(\lambda f) = \lambda M_{BB'}(f),$$
$$M_{BB''}(g \circ f) = M_{B'B''}(g)M_{BB'}(f).$$

Lema 42. *Sean B_1 y B_2 bases de un espacio vectorial V. Entonces $M_{B_1B_2} = M_{B_1B_2}(\mathrm{id}_V)$.*

Corolario 43. *Sea $f : V \to V'$ una aplicación lineal y sean B_1, B_2 y B'_1, B'_2 bases de V y V' respectivamente. Entonces*

$$M_{B_2B'_2}(f) = M_{B'_1B'_2}M_{B_1B'_1}(f)M_{B_2B_1}$$

Sea $f : V \to V'$ una aplicación lineal y sean $B = \{e_1, \dots, e_n\}$ y $B' = \{e'_1, \dots, e'_m\}$ bases de V y V' respectivamente. Sea

$$M_{BB'}(f) = \left(\begin{array}{c|c|c|c} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{array}\right)$$

Proposición 44. *Las columnas de $M_{BB'}(f)$ son las coordenadas en B' de un sistema de generadores de* $\operatorname{im} f$. *En particular* $\dim \operatorname{im} f = \operatorname{rango}(M_{BB'}(f))$.

Proposición 45. *La matriz $M_{BB'}(f)$ es la matriz de coeficientes de unas ecuaciones cartesianas de* $\ker f$. *En particular* $\dim \ker f = n - \operatorname{rango}(M_{BB'}(f))$.

Corolario 46. *Sea $f : V \to V'$ una aplicación lineal. Entonces* $\dim V = \dim \ker f + \dim \operatorname{im} f$.

[1] Las coordenadas las escribiremos indistintamente como filas o como columnas según nos interese.

5.5 Diagonalización

Definición 47. Dos matrices $M, N \in \mathcal{M}_n(\Bbbk)$ se dicen *semejantes* si existe una matriz regular $P \in \mathcal{M}_n(\Bbbk)$ tal que $M = PNP^{-1}$.

Proposición 48. *Dos matrices M, N son semejantes si y solo si existen bases B_1 y B_2 en un espacio vectorial V y una aplicación lineal $f : V \to V$ tales que $M = M_{B_1B_1}(f)$ y $N = M_{B_2B_2}(f)$, en cuyo caso $P = M_{B_2B_1}$.*

Definición 49. Una matriz cuadrada se dice diagonalizable si es semejante a una matriz diagonal.

Diagonalizar una matriz $A \in \mathcal{M}_n(\Bbbk)$ consiste en comprobar que es diagonalizable y en caso afirmativo encontrar matrices $D, P \in \mathcal{M}_n(\Bbbk)$ tales que D es diagonal, P es regular y $A = PDP^{-1}$.

Vamos a responder a esas preguntas.

Sea $f : V \to V$ una aplicación lineal.

Definición 50. Decimos que $\lambda \in \Bbbk$ es un *valor propio* de f si existe un vector $v \neq 0$ tal que $f(v) = \lambda v$.

Sea

$$V_\lambda = \ker(f - \lambda \,\mathrm{id}) = \{v \in V \mid f(v) = \lambda v\}$$

Definición 51. Dado un valor propio $\lambda \in \Bbbk$ llamamos a V_λ el *subespacio propio* asociado al valor propio λ. Los elementos no nulos de V_λ se llaman *vectores propios* de valor propio λ.

Sea V un espacio vectorial tal que $\dim V = n$. Sea B una base de V. Sea $f : V \to V$ una aplicación lineal y sea $A = M_{BB}(f)$. En vista de lo anterior, λ es un valor propio para f si y solo si $\mathrm{rango}(A - \lambda I_n) < n$, o equivalentemente

Lema 52. *λ es un valor propio para f si y solo si* $\det(A - \lambda I_n) = 0$.

Proposición 53. *Los valores propios de f son las raíces del polinomio $p(x) = \det(A - xI_n)$. Dicho polinomio recibe el nombre de* polinomio característico.

Lema 54. *Sean $\lambda_1, \lambda_2 \in \Bbbk$ valores propios de una aplicación lineal $f : V \to V$. Entonces $V_{\lambda_1} \cap V_{\lambda_2} = \{0\}$.*

Teorema 55. *Sea $A \in \mathcal{M}_n(\Bbbk)$ y sea $f : \Bbbk^n \to \Bbbk^n$ la aplicación lineal asociada a A. Sean $\lambda_1, \ldots, \lambda_s \in \Bbbk$ los valores propios de f. A es diagonalizable si y solo si $n = \dim V_{\lambda_1} + \cdots + \dim V_{\lambda_s}$. En este caso, si $B_{\lambda_1}, \ldots, B_{\lambda_s}$ son bases de $V_{\lambda_1}, \ldots, V_{\lambda_s}$ respectivamente, entonces $B = B_{\lambda_1} \cup \cdots \cup B_{\lambda_s}$ es una base de V formada por vectores propios y*

$$A = P \left(\begin{array}{c|c|c|c} \lambda_1 I_{n_1} & 0 & \cdots & 0 \\ \hline 0 & \lambda_2 I_{n_2} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & \lambda_s I_{n_s} \end{array}\right) P^{-1}$$

donde $n_i = \dim V_{\lambda_i}$ para todo $1 \leq i \leq s$ y $P = M_{BB_c}$.