

Matemàtiques 1
M1

Daniel Ramos Martínez

2 de maig de 2010

Índex

I	Fonaments d'Aritmètica i Combinatòria	5
1	Preliminars	7
1.1	Conjunts	7
1.1.1	Determinació d'un conjunt	7
1.1.2	Igualtat	8
1.1.3	Conjunt buit	8
1.1.4	Subconjunt	8
1.1.5	Cardinal	8
1.1.6	Conjunt de les parts	8
1.1.7	Tupla ordenada	9
1.1.8	Producte cartesià	9
1.1.9	Operacions entre conjunts	9
1.1.10	Propietats de les operacions entre conjunts	10
1.1.11	Representació amb cadenes binàries	10
1.2	Aplicacions	11
1.2.1	Composició	11
1.2.2	Aplicacions injectives	12
1.2.3	Aplicacions exhaustives	12
1.2.4	Aplicacions bijectives	12
1.2.5	Operacions bàsiques amb funcions	12
1.2.6	Funció part entera superior	12
1.2.7	Funció part entera inferior	12
1.3	Successions i sumatoris	13
1.3.1	Successions	13
1.3.2	Progressions aritmètiques	13
1.3.3	Progressions geomètriques	13
1.3.4	Sumatoris	13
1.3.5	Suma d'una progressió aritmètica	13
1.3.6	Suma d'una progressió geomètrica	13
1.3.7	Productori	13
1.4	Lògica i raonament matemàtic	14
1.4.1	Proposició	14
1.4.2	Connectors	14
1.4.3	Taula de la veritat	14
1.4.4	Propietats. Regles d'inferència	14
1.4.5	Quantificadors	14
1.5	Exemples de demostracions	15
1.5.1	Si x és múltiple de 8 també ho és de 2	15
1.5.2	$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$	15
1.5.3	$A \times B \neq B \times A$, A i B conjunts no buits, $A \neq B$	15
1.5.4	$A \subseteq B \implies \overline{B} \subseteq \overline{A}$	15

2	Aritmètica	17
2.1	Enters i divisibilitat	17
2.1.1	Propietats del grup dels enters \mathbb{Z}	17
2.1.2	Divisibilitat	17
2.1.3	Propietats de la divisibilitat	17
2.2	Nombres primers. Garbell d'Eratòstenes	18
2.2.1	Nombres primers	18
2.2.2	Teorema fonamental de l'aritmètica	18
2.2.3	Garbell d'Eratòstenes	18
2.3	MCD i MCM. Divisió Euclídea. Algorisme d'Euclides.	18
2.3.1	Màxim comú divisor	18
2.3.2	Mínim comú múltiple	19
2.3.3	Divisió entera o Euclídea	19
2.3.4	Algorisme d'Euclides	19
2.4	Identitat de Bézout	20
2.4.1	La identitat de Bézout	20
2.4.2	Propietats de la identitat de Bézout	20
2.4.3	Algorisme d'Euclides estès	20
2.5	Aritmètica modular	20
2.5.1	Mòdul	20
2.5.2	Congruències	21
2.5.3	Propietats de les congruències	21
2.5.4	Invers	21
2.5.5	Congruències lineals	21
2.5.6	Sistemes lineals. Teorema xinès del residu.	22
2.6	Petit teorema de Fermat	23
2.6.1	Càlcul de potències mòdul un nombre primer $a^n \bmod p$	23
2.7	Representació d'enters	24
2.8	Criptografia	24
2.8.1	Xifrat de Cèsar	24
2.8.2	Xifrat de Cesar afí	24
2.8.3	Criptografia de clau pública. RSA	24
2.9	Exemples de demostracions	25
2.9.1	Si $a b$ i $a c \implies a (b \pm c)$	25
2.9.2	Si $a b \implies a bk, \forall k \in \mathbb{Z}$	25
2.9.3	Sigui $a b$ i $b c \implies a c$	25
2.9.4	Hi ha infinits nombres primers	25
2.9.5	n enter compost, n té un divisor primer menor o igual que \sqrt{n}	25
2.9.6	$a, b \in \mathbb{Z}^+ \quad a \cdot b = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$	26
2.9.7	$a, b \in \mathbb{Z}, a, b \neq 0 \implies \text{mcd}(a, b) = \text{mcd}(a - bq, b) \quad \forall q \in \mathbb{Z}$	26
2.9.8	$r a$ i $r b \implies r \text{mcd}(a, b)$	26
2.9.9	$r ab, \text{mcd}(r, a) = 1 \implies r b$	26
2.9.10	Equivalència $a, b, m \in \mathbb{Z}, m > 1$	26
2.9.11	Propietats de les congruències	27
2.9.12	Invers	27
3	Raonament matemàtic	29
3.1	Mètodes de demostració	29
3.1.1	Demostració directe	29
3.1.2	Demostració indirecte o per el contrarecíproc	29
3.1.3	Demostració buida	30
3.1.4	Demostració evident o trivial	30
3.1.5	Demostració per contradicció o reducció a l'absurd	30
3.1.6	Demostració per casos	30

3.1.7	Demostracions d'equivalències	31
3.1.8	Demostració constructiva	31
3.1.9	Demostració no constructiva	31
3.1.10	Demostració per contraexemple	31
3.2	Inducció matemàtica	32
3.2.1	Principi d'inducció	32
3.2.2	Principi d'inducció forta o completa	32
4	Combinatoria	35
4.1	Principis bàsics	35
4.1.1	Principi de la suma	35
4.1.2	Principi del producte	35
4.2	Permutacions i combinacions	35
4.2.1	Permutacions	35
4.2.2	Combinacions	36
4.3	Nombres binomials	37
4.3.1	Identitat de Pascal	37
4.3.2	Triangle de Pascal o de Tartaglia	37
4.3.3	Teorema del binomi o binomi de Newton	37
4.3.4	Propietats dels nombres binomials	37
4.4	Permutacions i combinacions amb repetició	38
4.4.1	Permutacions amb repetició	38
4.4.2	Combinacions amb repetició	38
4.4.3	Permutacions d'objectes indistingibles	38
4.4.4	Teorema del multinomi	39
4.5	Principi d'inclusió-exclusió	39
4.5.1	Desarranjaments	39
4.6	Exemples de demostracions	40
4.6.1	Propietat d'addició dels nombres binomials	40
4.6.2	Propietat d'absorció	40
4.6.3	Corol·lari d'absorció	40
4.6.4	Identitat de Pascal	40
II	Àlgebra Lineal i Geometria	41
5	Espais vectorials. Càlcul Vectorial	43
5.1	Sistemes de coordenades	43
5.1.1	Sistema de coordenades a la recta unidimensional $S = (O, \{x\})$	43
5.1.2	Sistema de coordenades al pla bidimensional $S = (O, \{x, y\})$	43
5.1.3	Sistema de coordenades a l'espai tridimensional $S = (O, \{Ox, Oy, Oz\})$	44
5.2	Parametrització d'objectes geomètrics	44
5.2.1	Recta, semirecta i segment	44
5.2.2	La circumferència al pla bidimensional	44
5.2.3	El cilindre circular a l'espai tridimensional	45
5.3	Vectors	45
5.3.1	Visió geomètrica. Segments dirigits	45
5.3.2	Operacions amb vectors	45
5.3.3	Norma i distància	46
5.4	Espais vectorials	46
5.4.1	Definició i exemples	46
5.4.2	Combinacions lineals. Dependència i independència lineal	46
5.4.3	Sistemes de generadors. Bases.	48
5.4.4	Subespais vectorials	48

5.4.5	Espais de dimensió finita	49
5.5	Canvi de sistema de referència	49
5.5.1	Canvi d'origen	50
5.5.2	Canvi de base. Canvi d'eixos	50
5.5.3	Canvi complet de coordenades	51
5.6	Exemples de demostracions	51
5.6.1	L'expressió d'un vector com a combinació lineal de vectors L.I. és única	51
5.6.2	Teorema. $\langle S \rangle$ Subespai generat per S	52
5.6.3	F, H s.e.v. $\implies F \subset H$ s.e.v.	52
6	Aplicacions Lineals	53
6.1	Definició. Exemples. Propietats bàsiques	53
6.1.1	Propietats bàsiques	53
6.2	Nucli i imatge d'una aplicació lineal	54
6.3	Càlcul matricial	54
6.3.1	Matriu associada a una aplicació lineal	54
6.4	Canvi de base en la matriu d'una aplicació lineal	55
6.5	Algunes aplicacions lineals	56
6.5.1	Monomorfisme, epimorfisme i isomorfisme	56
6.5.2	Inversa d'una aplicació lineal	56

Part I

**Fonaments d'Aritmètica i
Combinatòria**

Capítol 1

Preliminars

1.1 Conjunts

Un **conjunt** és una col·lecció d'objectes ben determinada. Els *elements* són cada un dels objectes que formen el conjunt.

Exemples:

1. Conjunt que conté: a, b, c
 $A = \{a, b, c\}$
2. Conjunt de nombres naturals senars menors que 10.
 $A = \{1, 3, 5, 7, 9\}$
3. Nombres parells.
 $A = \{\dots, -4, -2, 0, 2, 4, \dots\}$
4. Nombres naturals.
 $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Si un element es troba dins d'un conjunt, direm que aquest element *pertany al conjunt*.

Notació

Notarem que un cert element a pertany a A : $a \in A$

Notarem que un cert element b no pertany a A : $b \notin A$

Exemples:

1. $A = \{a, b, c\} \implies b \in A$
2. $A = \{1, 3, 5, 7, 9\} \implies 11 \notin B$

1.1.1 Determinació d'un conjunt

Per determinar un conjunt necessitem conèixer:

- *Extensió*: Donant tots els elements del conjunt.
- *Comprensió*: Donades unes certes propietats que caracteritzen els elements.
- *Gràfica*: Diagrama de Venn.

1.1.2 Igualtat

Dos conjunts A i B són *iguals*, sí i només sí, tenen els mateixos elements.

Exemple: $A = \{1, 2, 3\}$ $B = \{1, 2, 3\}$

1.1.3 Conjunt buit

El *conjunt buit* és aquell que no conté cap element.

Exemple: $A = \emptyset$

1.1.4 Subconjunt

Direm que \mathbf{A} és un *subconjunt* de \mathbf{B} o que està contingut en \mathbf{B} , sí i només sí, tots els elements de \mathbf{A} són també elements de \mathbf{B} . Direm que el subconjunt és *propi* si \mathbf{A} és diferent de \mathbf{B} .

Notació

El conjunt A està contingut en el conjunt B : $A \subseteq B$

El conjunt A és subconjunt propi de B : $A \subset B$

Exemples:

$$1. A = \{1, 3, 5\} B = \{1, 2, 3, 4, 5\} \implies A \subseteq B \wedge A \subset B$$

$$2. A = \{1, 3, 5\} B = \{1, 3, 5\} \implies A \subseteq B \wedge A \not\subset B$$

Propietats $\forall A, B, C$ conjunts

1. $\emptyset \subseteq A$ i $A \subseteq A$ (reflexivitat)
2. $A \subseteq B$ i $A \neq B \implies A \subset B$ (subconjunt propi)
3. $A \subseteq B$ i $B \subseteq A \implies A = B$ (antisimetria)
4. $A \subseteq B$ i $B \subseteq C \implies A \subseteq C$ (transitivitat)

1.1.5 Cardinal

El *cardinal* d'un conjunt és el número d'elements d'aquest conjunt.

Notació

Anomenarem *n-conjunt* a tot conjunt d' n elements.

Notarem el cardinal de A : $n = |A| = \#A$

Exemples: $A = \{1, 3, 5, 7\} : |A| = 4$ $B = \{x \mid x \text{ vocal}\} : |B| = 5$

1.1.6 Conjunt de les parts

Donat un conjunt S , anomenarem *conjunt de les parts* de S al conjunt format per tots els subconjunts que es poden formar amb S .

Notació

Conjunt de les parts de A: $\mathfrak{S}(S) = \mathfrak{P}(S)$

Exemple: $S = \{a, b, c\}$

Conjunt de les parts que es poden fer segons cardinals:

$$\begin{aligned} |S| = 3 & \quad \{a, b, c\} \\ |S| = 2 & \quad \{a, b\} \quad \{a, c\} \quad \{b, c\} \\ |S| = 1 & \quad \{a\} \quad \{b\} \quad \{c\} \\ |S| = 0 & \quad \emptyset \end{aligned}$$

$$\mathfrak{S}(S) = \left\{ \{a, b, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}, \emptyset \right\}$$

Observació

El cardinal del conjunt de les parts d'un n -conjunt: $|\mathfrak{S}(S)| = 2^n$

1.1.7 Tupla ordenada

Una n -tupla ordenada és una col·lecció ordenada d'elements, on a_1 és el primer element, a_2 és el segon element... a_n és l' n -èssim element.

1.1.8 Producte cartesià

El *producte cartesià* de dos conjunts **A** i **B** és el conjunt dels parells ordenats (a, b) de manera que $a \in A$ i $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Exemples:

$$\begin{aligned} A &= \{1, 2\} \quad B = \{a, b, c\} \\ A \times B &= \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\} \end{aligned}$$

$$\begin{aligned} A &= \{1, 2\} \quad B = \{a, b, c\} \quad C = \{\alpha, \beta\} \\ A \times B \times C &= \{(1, a, \alpha), (1, a, \beta), (1, b, \alpha), (1, b, \beta), (1, c, \alpha), (1, c, \beta), (2, a, \alpha), (2, a, \beta), (2, b, \alpha), \dots\} \end{aligned}$$

1.1.9 Operacions entre conjunts

Unió: Conjunt que conté tots els elements de dos conjunts.

$$A \cup B = \{x \mid x \in A \vee x \in B\} \quad |A \cup B| = |A| + |B| - |A \cap B|$$

Intersecció: Conjunt que conté tots els elements comuns dels dos conjunts.

$$A \cap B = \{x \mid x \in A \wedge x \in B\} \quad |A \cap B| = |A| + |B| - |A \cup B|$$

Notació

A unió amb **B**: $A \cup B$

A intersecat amb **B**: $A \cap B$

Exemples: $A = \{1, 3, 5\}$ $B = \{2, 3, 4\}$

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5\} & |A \cup B| &= 5 \\ A \cap B &= \{3\} & |A \cap B| &= 1 \\ |A \cup B| &= |A| + |B| - |A \cap B| = 3 + 3 - 1 = 5 \end{aligned}$$

A i **B** són *disjunts* si no tenen cap element en comú, i per tant: $A \cap B = \emptyset$

Diferència: Elements que pertanyen a un grup però no a l'altre.

$$A - B = \{x \mid x \in A \text{ i } x \notin B\} \quad |A - B| = |A| - |A \cap B|$$

Exemples: $A = \{1, 2, 3\}$ $B = \{1, 3, 5, 7, 9\}$

$$\begin{aligned} A - B &= \{2\} & |A - B| &= 1 \\ B - A &= \{5, 7, 9\} & |B - A| &= 3 \end{aligned}$$

$$\begin{aligned} |A - B| &= |A| - |A \cap B| = 3 - 2 = 1 \\ |B - A| &= |B| - |A \cap B| = 5 - 2 = 3 \end{aligned}$$

Complementari: Tots els elements que no formen part d'un conjunt; sigui U el conjunt universal:

$$\bar{A} = U - A = \{x \in U : x \notin A\}$$

Notació

El complementari del conjunt A : $\bar{A} = A^c$

Exemple: Si $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $A = \{2, 4\}$

$$\bar{A} = U - A = \{1, 3, 5, 6, 7, 8, 9, 10\}$$

1.1.10 Propietats de les operacions entre conjunts

- $A \cup \emptyset = A$ $A \cap U = A$ *Identitat (universal)*
- $A \cap \emptyset = \emptyset$ $A \cup U = U$ *Dominació*
- $A \cap A = A \cup A = A$ *Impotència*
- $\overline{(\bar{A})} = A$ *Involució*
- $A \cup B = B \cup A$ $A \cap B = B \cap A$ *Commutativa*
- $A \cup (B \cup C) = (A \cup B) \cup C$ *Associativa*
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *Distributiva*
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cup B} = \bar{A} \cap \bar{B}$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$ *De Morgan*
- $A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$ *Complementari*
- $\overline{\emptyset} = U$ $\overline{U} = \emptyset$
- $A \cup (B \cap C) = A$ $A \cap (B \cup C) = A$ *Absorció*

Nota: Les lleis de Morgan es compleixen per varis conjunts units o intersecats.

$$\overline{\left(\bigcup_{i=1}^n A_i\right)} = \bigcap_{i=1}^n \bar{A}_i \quad \overline{\left(\bigcap_{i=1}^n A_i\right)} = \bigcup_{i=1}^n \bar{A}_i$$

1.1.11 Representació amb cadenes binàries

Per representar cada element numèric d'un conjunt podem indicar l'element amb un 1 en la seva posició corresponent, i amb un 0 a la resta de posicions que no contenen cap element.

Exemples:

$$\begin{array}{ll} U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} & \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \ \underline{1} \\ A = \{2, 4, 6, 8, 10\} & \underline{0} \ \underline{1} \ \underline{0} \ \underline{1} \ \underline{0} \ \underline{1} \ \underline{0} \ \underline{1} \ \underline{0} \ \underline{1} \\ A = \{1, 2, 4, 8\} & \underline{1} \ \underline{1} \ \underline{0} \ \underline{1} \ \underline{0} \ \underline{0} \ \underline{0} \ \underline{1} \ \underline{0} \ \underline{0} \end{array}$$

1.2 Aplicacions

Siguin X i Y dos conjunts. Una *aplicació* de X en Y és un dels subconjunts del producte cartesià entre X i Y , de manera que a cada element de X li correspon un únic element de Y .

$$f : X \longrightarrow Y \quad \forall x \in X : \exists y \in Y \mid (x, y) \in f$$

A y se li anomena *imatge* de x per f o *recorregut*. $y = f(x)$ imatge de x

A x se li anomena *antiimatge* de y per f o *domini*. $x = f^{-1}(y)$ antiimatge de y

Notació

Per notar una *aplicació* o *funció* de X en Y : $f : X \longrightarrow Y$

Exemple: $X = \{1, 2, 3, 4, 5\}$ $Y = \{a, b, c, d, e\}$

$$f : X \longrightarrow Y$$

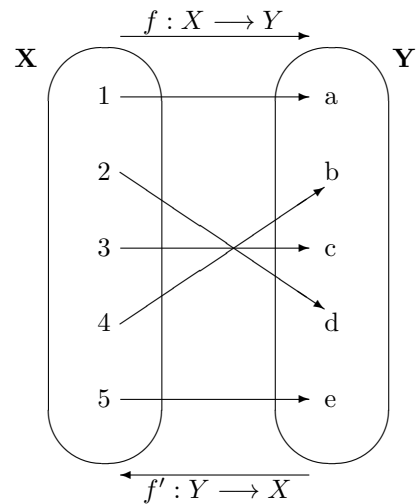
$$1 \mapsto a \quad f(1) = a$$

$$2 \mapsto d \quad f(2) = d$$

$$3 \mapsto c \quad f(3) = c$$

$$4 \mapsto b \quad f(4) = b$$

$$5 \mapsto e \quad f(5) = e$$



S'anomena *aplicació identitat* aquella que es dona entre dos conjunts iguals: $i_x : X \longrightarrow X$

1.2.1 Composició

Donats tres conjunts A , B , C , de manera que

$$f : A \longrightarrow B \quad g : B \longrightarrow C$$

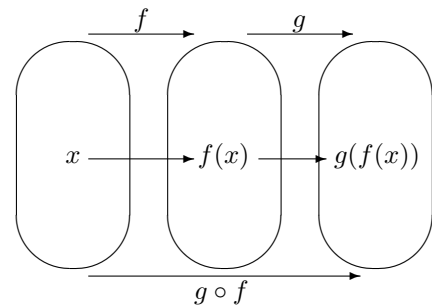
si tots els elements del conjunt A tenen imatge al conjunt C , podem definir una funció resultant de les dues:

$$g \circ f : A \longrightarrow C$$

Exemple: $f(x) = x^2$ $g(x) = x + 3$

$$(g \circ f)(x) = g(f(x)) = g(x^2) = (x + 3)^2$$

$$(g \circ f)(4) = (4 + 3)^2 = 49$$



1.2.2 Aplicacions injectives

Donats dos conjunts, \mathbf{A} i \mathbf{B} , i f una aplicació de \mathbf{A} en \mathbf{B} , aquesta aplicació serà *injectiva* si a cada element de \mathbf{A} li correspon un element diferent de \mathbf{B} , es a dir, un element de \mathbf{B} mai te més d'una antiimatge.

1.2.3 Aplicacions exhaustives

Donats dos conjunts, \mathbf{A} i \mathbf{B} , i una aplicació de \mathbf{A} en \mathbf{B} , aquesta aplicació serà *exhaustiva* o *suprajectiva* si tots els elements de \mathbf{B} tenen antiimatge a \mathbf{A} .

1.2.4 Aplicacions bijectives

Si una aplicació és injectiva i exhaustiva, l'aplicació també és *bijectiva* o *invertible*.

1.2.5 Operacions bàsiques amb funcions

Suma: $(f + g)(x) = f(x) + g(x)$

Multiplicació: $(f \cdot g)(x) = f(x) \cdot g(x)$

1.2.6 Funció part entera superior

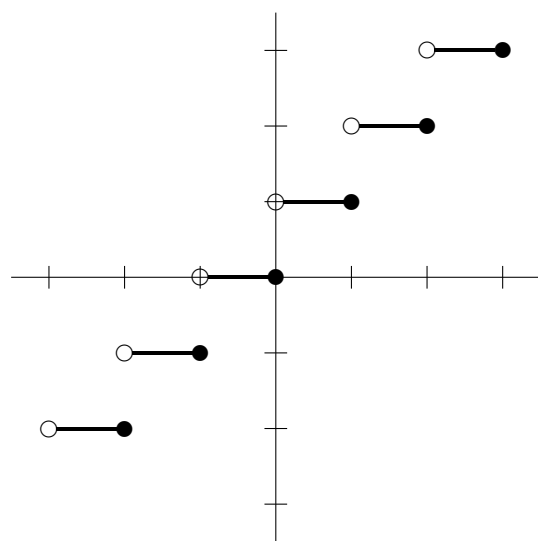
La funció *part entera superior* sobre x dona el enter més gran o igual que x .

Exemples: $\lceil 5.4 \rceil = 6$ $\lceil 5 \rceil = 5$ $\lceil 7.9 \rceil = 8$

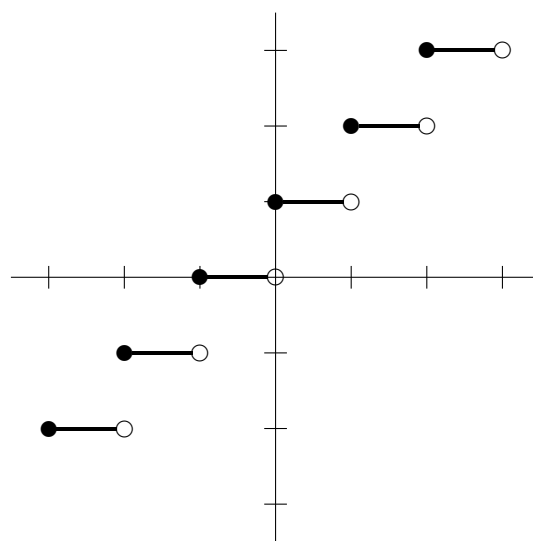
1.2.7 Funció part entera inferior

La funció *part entera inferior* sobre x dona el enter més petit o igual que x .

Exemples: $\lfloor 5.4 \rfloor = 5$ $\lfloor 5 \rfloor = 5$ $\lfloor 7.9 \rfloor = 7$



Funció part entera superior $\lceil x \rceil$



Funció part entera inferior $\lfloor x \rfloor$

1.3 Successions i sumatoris

1.3.1 Successions

Donat un conjunt S , una *successió* és una aplicació del conjunt dels enters en S . Les successions són estructures discretes que permeten representar llistes ordenades d'elements. Les *cadena de longitud n* són successions de longitud finita.

Exemple: $\mathbb{N} \rightarrow \mathbb{Q}$

$$a_n = \frac{1}{n} \quad 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$$

1.3.2 Progressions aritmètiques

Són *progressions aritmètiques* aquelles successions que creixen o decreixen linealment.

Exemple: $a_n = 6n - 1 \rightarrow 5, 11, 17, 23, 29$

1.3.3 Progressions geomètriques

Són *progressions geomètriques* aquelles successions que creixen exponencialment.

Exemple: $a_n = 2 \cdot 3^n \rightarrow 2, 6, 18, 54, 162$

1.3.4 Sumatoris

Un *sumatori* és una suma d'un seguit d'elements d'una successió.

$$\sum_{i=n}^m a_i = a_n + a_{n+1} + a_{n+2} + \dots + a_{m-2} + a_{m-1} + a_m$$

1.3.5 Suma d'una progressió aritmètica

$$\sum_{i=1}^n a_i = (a_1 + a_n) \frac{n}{2}$$

Exemple: $1 + 2 + 3 + 4 + 5 = (1 + 5) \frac{5}{2} = 15$

1.3.6 Suma d'una progressió geomètrica

$$\sum_{k=1}^n r^k = \frac{a_n \cdot r - a_1}{r - 1}$$

Exemple: $\sum_{n=1}^4 2^n = 2 + 4 + 8 + 16 = \frac{16 \cdot 2 - 2}{2 - 1} = 30$

1.3.7 Productori

Un *productori* és un producte d'un seguit d'elements d'una successió.

$$\prod_{i=n}^m i = n \cdot (n + 1) \cdot (n + 2) \cdot \dots \cdot (m - 1) \cdot m$$

Exemple: $5! = \prod_{i=1}^5 i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

1.4 Lògica i raonament matemàtic

1.4.1 Proposició

Les *proposicions* són afirmacions que poden ser certes o falses. Les proposicions es representen mitjançant lletres. Si una proposició és **certa** pren el valor **1** i si es falsa, **0**.

1.4.2 Connectors

Negació: \neg *no*

Conjunció: \wedge *i*

Disjunció: \vee *o*

Implicació: \implies *implica*

Doble Implicació: \iff *si i només si*

Exclusió: \oplus *o exclusiva*

1.4.3 Taula de la veritat

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$P \iff Q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

1.4.4 Propietats. Regles d'inferència

- $P \implies Q \equiv \neg P \vee Q$
- $P \iff Q \equiv (P \implies Q) \wedge (Q \implies P)$
- $P \equiv \neg \neg P$
- $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
 $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
- $P \wedge 1 \equiv P$ $P \vee 0 \equiv P$
- $P \vee 1 \equiv 1$ $P \wedge 0 \equiv 0$
- $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
 $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
- $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
 $(P \wedge (Q \vee R)) \equiv (P \wedge Q) \vee (P \wedge R)$
- $P \vee Q \equiv Q \vee P$ $P \wedge Q \equiv Q \wedge P$

Les proposicions que sempre prenen per valor 1 s'anomenen *tautologies* i les que sempre prenen valor 0 s'anomenen *contradiccions*. Si a una proposició **P** hi fixem un valor **x**, aleshores tenim un predicat **P(x)**.

1.4.5 Quantificadors

- **Quantificador Universal:** \forall *per a tot*
- **Quantificador Existencial:** \exists *existeix algun*
- **Oposat del Existencial:** \nexists *no existeix cap*
- **Unicitat:** $!$ *un únic*

Exemple:

$$\forall x, y \in \mathbb{Z} \quad \exists z \in \mathbb{Q} \mid z = \frac{x}{y}$$

1.5 Exemples de demostracions

1.5.1 Si x és múltiple de 8 també ho és de 2

$$A = \{x \in \mathbb{Z} \mid x = 8k \text{ per un cert } k \in \mathbb{Z}\} \quad B = \{x \in \mathbb{Z} \mid x = 2k' \text{ per un cert } k' \in \mathbb{Z}\}$$

Volem veure que: $(\forall x)(x \in A \implies x \in B)$

Si $x \in A$, com és múltiple de 8, podem escriure x en funció de k : $x = 8k$

$$x = 8k = 2(4k) = 2k' \quad k' \text{ és un nombre enter: } k' \in \mathbb{Z}$$

Per tant: $x \in B$ La hipòtesi és *certa*.

1.5.2 $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \wedge x \in (B \cup C) \iff x \in A \wedge (x \in B \vee x \in C) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \iff x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

Per tant: La hipòtesi és *certa*.

1.5.3 $A \times B \neq B \times A$, **A i B conjunts no buits**, $A \neq B$

Hipòtesi: $A \neq \emptyset$, $B \neq \emptyset$, $A \neq B$

Tesi: $A \times B \neq B \times A$

$$A \neq B \iff (\exists a \in A \mid a \notin B) \vee (\exists b \in B \mid b \notin A)$$

$$\text{Suposem: } \left. \begin{array}{l} \exists a \in A \mid a \in B \\ B \neq \emptyset \implies \exists b \in B \end{array} \right\} \implies (a, b) \in A \times B \quad \text{però} \quad (b, a) \notin B \times A \quad \text{Contradicció}$$

Per tant: La tesi és *certa*.

1.5.4 $A \subseteq B \implies \overline{B} \subseteq \overline{A}$

Hipòtesi: $A \subseteq B \implies \forall x(x \in A \implies x \in B)$

Tesi: $\overline{B} \subseteq \overline{A} \implies \forall x(x \in \overline{B} \implies x \in \overline{A})$

$$x \in A \implies x \in B \implies \neg(x \in B) \implies \neg(x \in A) \implies x \notin B \implies x \notin A \quad \overline{B} \subseteq \overline{A} \implies A \subseteq B$$

$$x \in \overline{B} \implies x \in \overline{A} \implies \neg(x \in \overline{A}) \implies \neg(x \in \overline{B}) \implies x \in A \implies x \in B \quad A \subseteq B \implies \overline{B} \subseteq \overline{A}$$

Per tant: La tesi és *certa*.

Capítol 2

Aritmètica

La *aritmètica* és la part de les matemàtiques que s'encarrega d'estudiar els números i les operacions que es poden fer amb ells.

2.1 Enters i divisibilitat

2.1.1 Propietats del grup dels enters \mathbb{Z}

$(\mathbb{Z}, +)$

- *Commutativa*: $a + b = b + a$
- *Associativa*: $(a + b) + c = a + (b + c)$
- *Element neutre*: $a + 0 = 0 + a = a$
- *Element simètric*: $\forall a \in \mathbb{Z} \mid a + a' = 0$

(\mathbb{Z}, \cdot)

- *Commutativa*: $a \cdot b = b \cdot a$
- *Associativa*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *Element neutre*: $a \cdot 1 = 1 \cdot a = a$

- *Distributivitat*: $a(b + c) = ab + ac$

2.1.2 Divisibilitat

Donats $a, b \in \mathbb{Z}, a \neq 0$, es diu que **a divideix a** quan existeix un enter **c** tal que $b = ac$. En aquest cas direm que **a és un divisor de b** , que **a és un factor de b** o que **b és un múltiple de a** . Per tant, el residu de la divisió és sempre 0.

$$a, b \in \mathbb{Z} \quad a|b \implies \exists c \in \mathbb{Z} \mid b = a \cdot c$$

Notació

b divideix a , o a és múltiple de b : $b|a$

b no divideix a , o a no és múltiple de b : $b \nmid a$

Exemples: $6|12 \implies 12 = 6 \cdot 2$ $3|12 \implies 12 = 3 \cdot 4$ $5 \nmid 12 \implies 12 \neq 5 \cdot c \quad c \in \mathbb{Z}$

2.1.3 Propietats de la divisibilitat

Donats $a, b, c \in \mathbb{Z}, a \neq 0$

- $1, a, -1, -a$ divideixen sempre a
- $b|a \iff (-b)|a \iff b|(-a) \iff (-b)|(-a)$
- $a|b \wedge b|a \implies a = \pm b$
- $a|b \wedge b|c \implies a|c$
- $a|b \wedge a|c \implies a|(b + c)$
- $a|b \implies a|(bk), \quad \forall k \in \mathbb{Z}$

2.2 Nombres primers. Garbell d'Eratòstenes

2.2.1 Nombres primers

Un enter positiu $p > 1$ és un nombre *primer* si només és divisible per $1, -1, p$ i $-p$. Per tant, el residu de la divisió mai serà 0 per qualsevol altre nombre. Si un enter no és primer aleshores s'anomena enter *compost*. Per veure si un nombre n és primer només ens cal comprovar si és múltiple de tots els primers menors que \sqrt{n} .

2.2.2 Teorema fonamental de l'aritmètica

Tot enter $n > 1$ descomposa en producte de nombres primers de forma única, de manera que els seus factors primers estan en ordre creixent.

Exemples: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$ $143 = 11 \cdot 13$ $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

2.2.3 Garbell d'Eratòstenes

Per fer el garbell d'Eratòstenes es deixa el primer número no marcat i es marquen tots el seus múltiples; així, tots els números no marcats són números primers.

	2	3	4	5	6	7	8	9	10
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	<u>49</u>	<u>50</u>
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
<u>91</u>	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

2.3 MCD i MCM. Divisió Euclídea. Algorisme d'Euclides.

2.3.1 Màxim comú divisor

Donats $a, b \in \mathbb{Z}, b \neq 0$. L'enter més gran que divideix a **a** i a **b** se l'anomena *màxim comú divisor* de **a** i **b**.

$$a = \prod_{i=1}^n P_i^{\alpha_i} \quad a = \prod_{i=1}^n P_i^{\beta_i} \quad \text{mcd}(a, b) = \prod_{i=1}^n P_i^{\min(\alpha_i, \beta_i)}$$

Observacions

Notació: $\text{mcd}(a, b)$

- $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$
- $\text{mcd}(a, 0) = |a|$
- $\text{mcd}(a, b) = 1 \iff \mathbf{a}$ i \mathbf{b} són primers entre sí.

Exemple: $120 = 2^3 \cdot 3 \cdot 5^1$ $500 = 2^2 \cdot 3^0 \cdot 5^3$

$$\text{mcd}(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 2^2 \cdot 5 = 20$$

2.3.2 Mínim comú múltiple

Donats $a, b \in \mathbb{Z}^+$, el *mínim comú múltiple* de **a** i **b** és l'enter més petit que és múltiple de **a** i **b**.

$$a = \prod_{i=1}^n P_i^{\alpha_i} \quad a = \prod_{i=1}^n P_i^{\beta_i} \quad \text{mcm}(a, b) = \prod_{i=1}^n P_i^{\max(\alpha_i, \beta_i)}$$

Notació: $\text{mcm}(a, b)$

Exemple: $120 = 2^3 \cdot 3 \cdot 5^1 \quad 500 = 2^2 \cdot 3^0 \cdot 5^3$
 $\text{mcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 2^3 \cdot 3 \cdot 5^3 = 3000$

El mínim comú múltiple es relaciona amb el màxim comú divisor de la següent forma:

$$a \cdot b = \text{mcm}(a, b) \cdot \text{mcd}(a, b)$$

2.3.3 Divisió entera o Euclídea

Per tot $a, b \in \mathbb{Z}, b \neq 0$, si dividim existeixen uns únics **q** *quocient* i **r** *residu*.

$$\forall a, b \in \mathbb{Z}, b \neq 0 \quad \exists! q, r \mid a = bq + r, \quad 0 \leq r < |b|$$

Exemples:

<p>a=101, b=9</p> <p>$101 \div 9 = 11 \quad q = 11$ $101 - 11 \cdot 9 = 2 \quad r = 2$</p> <p>101 = 9 · 11 + 2</p>	<p>a=-14, b=3</p> <p>$14 \div 3 = 4 \quad q = -4$ $14 - 4 \cdot 3 = 2 \quad r = -2$</p> <p>-14=3(-4)+1</p>
---	---

En el cas que el dividend **a** sigui negatiu fem la divisió amb el seu valor absolut i tot seguit canviem el signe al quocient **q** i al residu **r** a la fórmula tal i com es mostra al exemple. Finalment, arreglem la fórmula per fer el residu positiu.

Lema $\text{mcd}(a, b) = \text{mcd}(r, b) = \text{mcd}(a - bq, b)$

2.3.4 Algorisme d'Euclides

L'*algorisme d'Euclides* consisteix en anar reduint el nombre, substituint-lo pel seu residu, utilitzant la fórmula del lema anterior.

Siguin $a, b \in \mathbb{Z}, a \geq b > 0$. Considerem les divisions enteres, amb $r_0 = a$ i $r_1 = b$:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ r_2 &= r_3 q_3 + r_4, & 0 \leq r_4 < r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= \mathbf{r}_n q_n \end{aligned}$$

Aleshores, $\text{mcd}(a, b) = \mathbf{r}_n$

$$\begin{array}{c|ccc} q & q_1 & q_2 & q_3 \\ r & a & b & r_2 & \mathbf{r}_3 \\ \hline & r_2 & r_3 & 0 & \end{array}$$

Aleshores, $\text{mcd}(a, b) = \mathbf{r}_3$

Exemples: $\text{mcd}(287, 91) = 7$

q		3	6	2
r	287	91	14	7
	14	7	0	

$\text{mcd}(68, 24) = 4$

q		2	1	5
r	68	24	20	4
	20	4	0	

2.4 Identitat de Bézout

2.4.1 La identitat de Bézout

$$d = \text{mcd}(a, b) \implies \exists x, y \in \mathbb{Z} \mid ax + by = d$$

Amb l'*algorisme d'Euclides estès* podem calcular la \mathbf{x} i la \mathbf{y} . Aquest teorema resulta útil per calcular moltes aplicacions sobre el màxim comú divisor.

2.4.2 Propietats de la identitat de Bézout

- $r|a \wedge r|b \implies r|\text{mcd}(a, b)$
- $r|ab \wedge \text{mcd}(r, a) = 1 \implies r|b$
- p primer $p|ab \implies p|a \vee p|b$
- p primer $p|a_1 a_2 \dots a_n \implies \exists i \in \{1, \dots, n\} \mid p|a_i$

2.4.3 Algorisme d'Euclides estès

Siguin $a, b \in \mathbb{Z}$, $a \geq b > 0$. Considerem les divisions enteres, amb $r_0 = a$ i $r_1 = b$:

$$\begin{array}{lll}
 r_0 = r_1 q_1 + r_2 & x_0 = 1 & y_0 = 0 \\
 r_1 = r_2 q_2 + r_3 & x_1 = 0 & y_1 = 1 \\
 r_2 = r_3 q_3 + r_4 & x_2 = x_0 - q_1 x_1 & y_2 = y_0 - q_1 y_1 \\
 \vdots & \vdots & \vdots \\
 r_{n-2} = r_{n-1} q_{n-1} + r_n & x_{n-2} = x_{n-4} - q_{n-3} x_{n-3} & y_{n-2} = y_{n-4} - q_{n-3} y_{n-3} \\
 r_{n-1} = \mathbf{r}_n q_n & x_{n-1} = x_{n-3} - q_{n-2} x_{n-2} & y_{n-1} = y_{n-3} - q_{n-2} y_{n-2} \\
 & \mathbf{x}_n = x_{n-2} - q_{n-1} x_{n-1} & \mathbf{y}_n = y_{n-2} - q_{n-1} y_{n-1}
 \end{array}$$

Si igualem $x = x_n$, $y = y_n$, $r = r_n$, aleshores tenim l'equació: $r = ax + by$

x	1	0	x_2	\mathbf{x}_3
y	0	1	y_2	\mathbf{y}_3
q		q_1	q_2	q_3
r	a	b	r_2	\mathbf{r}_3
	r_2	r_3	0	

Si igualem $x = x_3$, $y = y_3$, $r = r_3$, obtenim l'equació d'abans.

Exemple: $\text{mcd}(287, 91) = 7$

x	1	0	1	-6
y	0	1	-3	19
q		3	6	2
r	287	91	14	7
	14	7	10	

$$7 = 287 \cdot (-6) + 91 \cdot 19$$

2.5 Aritmètica modular

2.5.1 Mòdul

Siguin $a, r \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, definim \mathbf{a} mòdul \mathbf{m} com el residu de la diferència entre \mathbf{a} i \mathbf{m} .

Notació: $r = a \bmod m$

Exemple: $17 \bmod 5 = 2$

2.5.2 Congruències

Siguin $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, direm que a és congruent amb b mòdul m si $m|(a - b)$.

Notació: $a \equiv b \pmod{m}$

Exemple: $35 \equiv 11 \pmod{8} \iff 8|(35 - 11)$ $15 \equiv -9 \pmod{8} \iff 8|(35 - (-9))$

2.5.3 Propietats de les congruències

- Si $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
- Si $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$ aleshores: $a \equiv c \pmod{m}$
- Si $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$, $c, d \in \mathbb{Z}$ aleshores:
 - $a + c \equiv b + d \pmod{m}$
 - $a \cdot c \equiv b \cdot d \pmod{m}$
- Si $ac \equiv bc \pmod{m}$ i m, c primers entre si, aleshores $a \equiv b \pmod{m}$.

$$ac \equiv bc \pmod{m} \implies a \equiv b \left(\pmod{\frac{m}{\text{mcd}(c, m)}} \right)$$

- Si $a \equiv b \pmod{m}$, aleshores $\exists k \in \mathbb{Z} \mid a^k \equiv b^k \pmod{m}$

2.5.4 Invers

Donats $a \in \mathbb{Z}$ i $m \in \mathbb{Z}^+$, es diu que $\bar{a} \in \mathbb{Z}$ és un *invers de a mòdul m* quan $a\bar{a} \equiv 1 \pmod{m}$. Si a i m són primers entre sí, això implica que existeix un \bar{a} únic.

2.5.5 Congruències lineals

Una *congruència lineal* és una congruència amb una incògnita.

$$ax \equiv b \pmod{m} \quad a, b, m, x \in \mathbb{Z}, m > 1$$

Resoldre una congruència lineal és trobar tots els enters x que la satisfan. La congruència lineal només té solucions sí $\text{mcd}(a, m) | b$. La congruència sempre tindrà infinites sol·lucions o no en tindrà cap.

Per trobar una solució x_o , hem de seguir els passos següents:

1. Comprobar que a i m són primers entre si per verificar que hi ha sol·lució.
2. Trobar, mitjançant la identitat de Bézout, un *invers de a mòdul m* , que anomenarem \bar{a} .
3. Multiplicar la congruència per \bar{a} : $a\bar{a}x \equiv \bar{a}b \pmod{m}$
4. Solució general: $x = x_o + mt, \quad \forall t \in \mathbb{Z}$

Exemple: Resoldre la congruència $287x \equiv 9 \pmod{92}$.

$$a = 287 \quad b = 9 \quad m = 92$$

1). Trobar un invers de 285 mòdul 92 mitjançant la identitat de Bézout. A aquest invers l'anomenarem \bar{a} i serà la x resultant de l'algorisme d'Euclides estès. El residu r que és el $\text{mcd}(285, 92)$ ha de donar 1 perquè hi hagi sol·lució.

x	1	0	1	-8	17	-25
y	0	1	-3	25	-53	78
q		3	8	2	1	
r	287	92	11	4	3	1
	11	4	3	1		

2). Ara tenim l'invers de 287 mòdul 92 que és **-25**. Tot seguit multipliquem la congruència per l'invers:

$$287(-25) \equiv 9(-25) \pmod{92}$$

Com que qualsevol número multiplicat pel seu invers dona 1, podem substituir el $287(-25)$ per 1. Tot seguit simplifiquem la congruència:

$$1x \equiv 9(-25) \pmod{92} \implies x \equiv -225 \pmod{92} \implies x \equiv 51 \pmod{92}$$

Per tant la solució general és: $x = 51 + 92t, \quad \forall t \in \mathbb{Z}$

2.5.6 Sistemes lineals. Teorema xinès del residu.

Siguin $m_1, m_2, \dots, m_r \in \mathbb{Z}^+$ dos a dos primers entre si. Sigui $a_1, a_2, \dots, a_r \in \mathbb{Z}$. Aleshores el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

té una única solució de mòdul el producte de tots els mòduls de les congruències.

$$\exists! x \in \mathbb{Z} \quad 0 \leq x < m, \quad \text{mòdul: } m = \prod_{i=1}^r m_i$$

Per calcular la solució al sistema d'equacions hem de seguir els passos següents:

1. Trobem el mòdul \mathbf{m} amb la fórmula anterior.
2. Buscar els M_i per cada congruència: $M_i = \frac{m}{m_i}$
3. Buscar els y_i per cada congruència tals que: $M_i y_i \equiv 1 \pmod{m_i}$
4. Substituir els valors a la fórmula següent:

$$x \equiv \left(\sum_{i=1}^r a_i y_i M_i \right) \pmod{m}$$

Podem simplificar la congruència sense que canviï el resultat.

Exemple: Resoldre el sistema següent:
$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{6} \\ x \equiv 2 \pmod{7} \end{cases}$$

1). Calcular m, M_1, M_2, M_3 :

$$m_1 = 5, \quad m_2 = 6, \quad m_3 = 7, \quad m = 210$$

$$M_1 = \frac{210}{5} = 42, \quad M_2 = \frac{210}{6} = 35, \quad M_3 = \frac{210}{7} = 30$$

2). Trobar els y_i per cada congruència tals que: $M_i y_i \equiv 1 \pmod{m_i}$

$$42y_1 \equiv 1 \pmod{5} \longrightarrow y_1 = 3$$

$$35y_2 \equiv 1 \pmod{6} \longrightarrow y_2 = 5$$

$$30y_3 \equiv 1 \pmod{7} \longrightarrow y_3 = 4$$

3). Aplicar la fórmula del punt 4.

$$x \equiv (1 \cdot 42 \cdot 3 + 3 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4) \pmod{210} \equiv 891 \pmod{210}$$

$$x \equiv 51 \pmod{210}$$

2.6 Petit teorema de Fermat

Sigui p un nombre primer i a un enter no divisible per p , aleshores

$$a^{p-1} \equiv 1 \pmod{p}$$

En general: per qualsevol enter a es té: $a^p \equiv a \pmod{p}$

Exemple: $a = 8$ i $p = 5$

$$8^{5-1} \pmod{5} = (8^2)^2 \pmod{5} = (64 \pmod{5})^2 \pmod{5} = 4^2 \pmod{5} = 1$$

$$8^5 \pmod{5} = (8^4 \cdot 8) \pmod{5} = (8^4 \pmod{5}) \cdot (8 \pmod{5}) = 1 \cdot 3 = 3$$

2.6.1 Càlcul de potències mòdul un nombre primer $a^n \pmod{p}$

$$s = a \pmod{p} \implies a^n \equiv s^n \pmod{p}$$

$$a^n \pmod{p} = s^n \pmod{p}$$

Aplicar el teorema de Fermat per anar simplificant fins trobar el resultat.

Exemple: Calcular $735^{378} \pmod{29}$

$$735 \pmod{29} = 10 \implies 735^{378} \equiv 10^{378} \pmod{29}$$

$$10^{378} = 10^{28 \cdot 13 + 14} = (10^{28})^{13} \cdot 10^{14}$$

Aplicant el teorema de Fermat: $10^{28} \equiv 1 \pmod{29} \implies 10^{378} \equiv 10^{14} \pmod{29}$

$$10^{14} \pmod{29} = (10^8 \cdot 10^4 \cdot 10^2) \pmod{29}$$

$$10^2 \pmod{29} = 13$$

$$10^4 \pmod{29} = (10^2 \pmod{29})^2 \pmod{29} = 13^2 \pmod{29} = 24$$

$$10^8 \pmod{29} = (10^4 \pmod{29})^2 \pmod{29} = 24^2 \pmod{29} = 25$$

$$(10^8 \cdot 10^4 \cdot 10^2) \pmod{29} = (13 \cdot 24 \cdot 25) \pmod{29} = 28 \implies 735^{378} \pmod{29} = 28$$

2.7 Representació d'enters

Donada una base $b > 1$, qualsevol enter n es pot representar de forma única:

$$n = a_0 + a_1b + a_2b^2 + \dots + a_{k-1}b^{k-1} + a_kb^k$$

Normalment utilitzem la base 10 (decimal), però els ordinadors solen utilitzar també la base 2 (binaria) y la base 16 (hexadecimal). Els algorismes de suma i multiplicació que coneixem també es poden aplicar en aquestes bases.

2.8 Criptografia

La *criptografia* és la ciència que s'encarrega de transformar missatges perquè no siguin llegibles per a personal no autoritzat.

- **Xifrar:** transformar un missatge clar en un missatge il·legible, el qual anomenarem missatge xifrat.
- **Desxifrar:** reconstruir el missatge original a partir del missatge xifrat.
- **Clau:** instrument que permet xifrar i desxifrar el missatge.
- **Criptosistema:** mètode que seguim per xifrar i desxifrar.

2.8.1 Xifrat de Cèsar

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Si diem m al número al que correspon la lletra, c al número al que correspon la lletra xifrada, i k a la clau, la fórmula seria la següent:

$$\begin{aligned} \text{Xifrat:} \quad & c = f(m) = (m + k) \bmod 26 && (\text{Xifrat de Cesar: } k = 3) \\ \text{Desxifrat:} \quad & f^{-1}(c) = (c - k) \bmod 26 \\ \text{Clau:} \quad & k \end{aligned}$$

2.8.2 Xifrat de Cesar afí

$$\begin{aligned} \text{Xifrat:} \quad & c = f(m) = (am + b) \bmod 26 && f \text{ bijectiva} \\ \text{Desxifrat:} \quad & f^{-1}(c) = \bar{a}(c - b) \bmod 26, \text{ on } \bar{a}a \equiv 1 \pmod{26} \\ \text{Clau:} \quad & (a, b) \end{aligned}$$

2.8.3 Criptografia de clau pública. RSA

- La clau de xifrar no serveix per desxifrar el missatge.
- La clau del criptosistema es divideix en dues:
 - clau pública: la clau per xifrar el missatge. Tothom la pot conèixer i amb ella xifrar els missatges per enviar.
 - clau privada: la clau per desxifrar el missatge. Només la pot conèixer aquell que ha de desxifrar-lo.

El missatge es converteix en una seqüència d'enters, que s'agafa per blocs. Amb $p, q, e \in \mathbb{Z}$, p, q primers, tal que $\text{mcd}(e, (p-1)(q-1)) = 1$, xifrem amb la fórmula $c = m^e \bmod n$ on m és un bloc. Per desxifrar, utilitzem la fórmula $m = c^d \pmod{n}$, on c és un bloc xifrat i $n = p \cdot q$

2.9 Exemples de demostracions

2.9.1 Si $a|b$ i $a|c \implies a|(b \pm c)$

Hipòtesi: $a|b$ i $a|c \implies \exists k_1, k_2 \in \mathbb{Z} \mid b = ak_1$ i $c = ak_2$

Tesi: $a|(b+c)$, és a dir, $\exists k \in \mathbb{Z} \mid b+c = ak$

$$b+c = ak_1 + ak_2 = a \underbrace{(k_1 + k_2)}_{k \in \mathbb{Z}} = ak \implies a|(b+c)$$

2.9.2 Si $a|b \implies a|bk, \forall k \in \mathbb{Z}$

Hipòtesi: $a|b$, és a dir, $\exists k_1 \in \mathbb{Z} \mid b = ak_1$

Tesi: $\forall x \in \mathbb{Z}, a|bx$, és a dir, $\forall x \in \mathbb{Z} \exists k_x \in \mathbb{Z} \mid bx = ak_x$

Sigui un $x \in \mathbb{Z}$ qualsevol, $bx = (ak_1)x = a(k_1x) \implies a|bx$

2.9.3 Sigui $a|b$ i $b|c \implies a|c$

Hipòtesi: $a|b$ i $b|c$, és a dir, $\exists k_1, k_2 \in \mathbb{Z} \mid b = ak_1, c = bk_2$

Tesi: $a|c$, és a dir, $\exists k \in \mathbb{Z} \mid c = ak$

$$c = bk_2 = (ak_1)k_2 = a \underbrace{(k_1k_2)}_{k \in \mathbb{Z}} \implies a|c$$

2.9.4 Hi ha infinits nombres primers

(Per reducció a l'absurd) Suposem que hi ha un nombre finit de primers: p_1, p_2, \dots, p_n

Sigui $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$, poden passar dues coses:

1). N **és primer**: llavors hi ha $n+1$ enters primers, i això per hipòtesi no pot ser.

2). N **és compost**: $N = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r}$, així: $\forall i \in \{1, \dots, r\}, q_i \in \{p_1, \dots, p_n\}$

Si $q_j = p_i$ llavors:

$$\left. \begin{array}{l} q_j | p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_n \\ q_j | N \end{array} \right\} \implies q_j | (N - p_1 \cdot \dots \cdot p_n) \implies q_j | 1$$

$q_j \nmid 1$, ja que és un nombre primer, $q_j > 1 \implies$ Hi ha infinits nombres primers

2.9.5 n enter compost, n té un divisor primer menor o igual que \sqrt{n}

$n \in \mathbb{Z}, n$ compost, llavors $\exists a \in \mathbb{Z} \mid a|n, 1 < a < n$

Es a dir, $n = a \cdot b, 1 < a < n, 1 < b < n$

Suposem que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$, altrament

$$a > \sqrt{n} \text{ i } b > \sqrt{n} \implies n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \implies n > n \quad \text{No pot ser!!}$$

Si $a \leq \sqrt{n}$, a descomposa en producte de n primers.

Sigui $p|a, p$ primer $\implies p|n$

$$p|a \implies p \leq a \leq \sqrt{n}$$

$$2.9.6 \quad a, b \in \mathbb{Z}^+ \quad a \cdot b = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$$

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n} \quad b = p_1^{\beta_1} \cdot \dots \cdot p_n^{\beta_n}, \quad p_i \text{ primers diferents} \quad \forall i = 1, \dots, n$$

$$a \cdot b = \prod_{i=1}^n p_i^{\alpha_i + \beta_i} \stackrel{?}{=} \prod_{i=1}^n p_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)} = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$$

$$\text{Cal probar: } p_i^{\alpha_i + \beta_i} = p_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)}, \quad \forall i = 1, \dots, n$$

$$\text{es a dir } \alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i), \quad \forall i = 1, \dots, n$$

$$\text{Per casos: } \left\{ \begin{array}{l} \alpha_i = \beta_i : \quad \underbrace{\min(\alpha_i + \beta_i)}_{\alpha_i} + \underbrace{\max(\alpha_i + \beta_i)}_{\alpha_i} = \alpha_i + \alpha_i = \alpha_i + \beta_i \\ \alpha_i < \beta_i : \quad \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i \\ \alpha_i > \beta_i : \quad \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i \end{array} \right.$$

$$\text{Per tant: } a \cdot b = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$$

$$2.9.7 \quad a, b \in \mathbb{Z}, \quad a, b \neq 0 \implies \text{mcd}(a, b) = \text{mcd}(a - bq, b) \quad \forall q \in \mathbb{Z}$$

Fixem $q \in \mathbb{Z}$ arbitrari. Siguin $D_1 = \text{mcd}(a, b)$ i $D_2 = \text{mcd}(a - bq, b)$

$$\text{Volem veure que: } D_1 = D_2$$

$$\left. \begin{array}{l} D_1 | a \\ D_1 | b \end{array} \right\} \implies D_1 | (a - bq) \implies D_1 \leq D_2$$

$$\left. \begin{array}{l} D_2 | b \\ D_2 | (a - bq) \end{array} \right\} \implies D_2 | ((a - bq) + bq) \implies D_2 | a \implies D_2 \leq D_1$$

$$\left. \begin{array}{l} D_1 \leq D_2 \\ D_2 \leq D_1 \end{array} \right\} \implies D_1 = D_2$$

$$2.9.8 \quad r | a \text{ i } r | b \implies r | \text{mcd}(a, b)$$

$$d = \text{mcd}(a, b) \iff d = rk \quad \text{per un cert } k \in \mathbb{Z}$$

$$\exists x, y \in \mathbb{Z} \mid ax + by = d$$

$$\left. \begin{array}{l} r | a \implies r | ax \\ r | b \implies r | by \end{array} \right\} \implies r | (ax + by) \implies r | d$$

$$2.9.9 \quad r | ab, \text{mcd}(r, a) = 1 \implies r | b$$

$$\exists x, y \in \mathbb{Z} \mid ax + by = 1 \implies bax + bry = b$$

$$\left. \begin{array}{l} r | abx \\ r | bry \end{array} \right\} \implies r | \underbrace{(abx + bry)}_b = r | b$$

2.9.10 Equivalència $a, b, m \in \mathbb{Z}, m > 1$

Siguin $a, b, m \in \mathbb{Z}, m > 1$, són equivalents si compleixen una de les tres condicions:

1. $a \equiv b \pmod{m}$
2. $\exists k \in \mathbb{Z} \mid a = b + mk$
3. $a \pmod{m} = b \pmod{m}$

Demostració1 \implies 2 *Hipòtesi:* $a \equiv b \pmod{m}$ *Tesi:* $\exists k \in \mathbb{Z} \mid a = b + mk$

$$a \equiv b \pmod{m} \implies m \mid (a - b) \implies \exists k \in \mathbb{Z} \mid (a - b) = mk \implies a = b + mk$$

2 \implies 3 *Hipòtesi:* $\exists k \in \mathbb{Z} \mid a = b + mk$ *Tesi:* $a \pmod{m} = b \pmod{m}$

$$mk \neq b = a = mq + r \quad 0 \leq r < m$$

$$b = m(q - k) + r \implies a \pmod{m} = b \pmod{m}$$

3 \implies 1 *Hipòtesi:* $a \pmod{m} = b \pmod{m}$ *Tesi:* $a \equiv b \pmod{m}$

$$\exists q_1, r \mid a = mq_1 + r \quad \exists q_2, r \mid b = mq_2 + r$$

$$a - b = (mq_1 + r) - (mq_2 + r) = m(q_1 - q_2) \implies m \mid (a - b) \implies a \equiv b \pmod{m}$$

2.9.11 Propietats de les congruènciesSiguin $a, b, c, d, m \in \mathbb{Z}, m > 1$ $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ a). $a + c \equiv b + d \pmod{m}$

$$\left. \begin{array}{l} a \equiv b \pmod{m} \iff m \mid (a - b) \\ c \equiv d \pmod{m} \iff m \mid (c - d) \end{array} \right\} \implies m \mid ((a + c) - (b + d))$$

b). $ac \equiv bd \pmod{m} \iff m \mid (ac - bd)$

$$ac - bd = ac - bc + bc - bd = c(c - b) + b(c - d) = m$$

c). $ac = bc \pmod{m}$ i $\text{mcd}(c, m) = 1 \iff a \equiv b \pmod{m}$

$$ac = bc \pmod{m} \implies \exists k \in \mathbb{Z} \mid ac - bc = mk$$

$$\left. \begin{array}{l} mk = c(a - b) \implies m \mid (a - b) \\ \text{mcd}(m, c) = 1 \end{array} \right\} \implies m \mid (a - b) \implies a \equiv b \pmod{m}$$

2.9.12 Invers

$$\text{mcd}(a, m) = 1 \implies \exists r, s \in \mathbb{Z} \mid ar + ms = 1 \iff ar = a + m(-s) \iff ar \equiv 1 \pmod{m}$$

Unicitat: Sigui $\bar{a}, \bar{c} \in \mathbb{Z} \mid \bar{a}a \equiv 1 \pmod{m}$ i $\bar{c}a \equiv 1 \pmod{m}$

$$\bar{a} \equiv \bar{a} \cdot 1 \pmod{m} \implies \bar{a} \equiv \bar{a}a\bar{c} \pmod{m} \implies \bar{a} \equiv 1 \cdot \bar{c} \pmod{m} \implies \bar{a} \pmod{m} = \bar{c} \pmod{m}$$

$$\text{Per tant } \exists r \in \{0, 1, \dots, m - 1\} \mid ar \equiv 1 \pmod{m}$$

Per tant: Tots els inversos de a mòdul m són: $\bar{a} = r + mt, \forall t \in \mathbb{Z}$

Capítol 3

Raonament matemàtic

Un *teorema* és una afirmació que es pot demostrar. Una *demostració* és una cadena on a cada pas es dedueixen noves afirmacions. Per deduir-les utilitzem:

1. Les *hipòtesis* del teorema.
2. Anteriors afirmacions de la demostració ja demostrades.
3. *Axiomes*. Proposicions evidents que no necessiten demostració.
4. *Teoremes*. Deduccions fetes a altres demostracions.

Per fer les demostracions matemàtiques s'utilitzen les *regles d'inferència*, que es troben a l'apartat 1.4.4 de la pàgina 14.

Molts dels teoremes són implicacions. Donades dues proposicions, p i q , volem veure que $p \implies q$.

3.1 Mètodes de demostració

3.1.1 Demostració directe

Es suposa que p és cert i s'utilitzen les regles d'inferència i teoremes ja demostrats per veure que q també és cert.

Exemple: n és senar $\implies n^2$ és senar.

$$\exists k \in \mathbb{Z} : n = 2k + 1 \implies n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(\underbrace{2k^2 + 2k}_{\mathbb{Z}}) + 1 \implies n^2 \text{ és senar}$$

3.1.2 Demostració indirecte o per el contrarecíproc

$p \implies q$ equival a $\neg p \implies \neg q$. Per tant es tracta de demostrar que si q és fals, p per força també ho ha de ser.

Exemple: Si $3n + 2$ és senar, aleshores n és senar.

$$\neg(n \text{ és senar}) \implies \neg(3n + 2 \text{ és senar})$$

$$n \text{ parell} \implies \exists k \in \mathbb{Z} \mid n = 2k$$

$$3n + 2 = 3(2k) + 2 = 2(\underbrace{3k + 1}_{\mathbb{Z}}) \implies 3n + 2 \text{ és parell} \implies (n \text{ senar} \implies 3n + 2 \text{ senar})$$

3.1.3 Demostració buida

Es basa en veure que la hipòtesi és falsa, i per tant la implicació $p \implies q$ és sempre certa. Es sol utilitzar per comprobar casos especials dins de demostracions de teoremes.

Exemple: $\emptyset \subseteq A$, $\forall A$ conjunt

$$\forall x : (x \in \emptyset \implies x \in A), \forall A$$

Com que la hipòtesis $x \in \emptyset$ és falsa, la implicació és *certa*.

3.1.4 Demostració evident o trivial

Es basa en demostrar que la tesi és sempre certa; aleshores l'implicació també ho és.

Exemple: $a, b \in \mathbb{Z}$. Si $a = b$, aleshores $a^0 = b^0$.

Com que $a^0 = 1$ i $b^0 = 1$ siguin quins siguin els valors de a i b , la tesi és *certa* i per tant la implicació també ho és.

3.1.5 Demostració per contradicció o reducció a l'absurd

Per demostrar que que la implicació és certa s'oposem que $\neg p$ és cert i arribem a una contradicció. Aquesta contradicció indica que $\neg p$ és fals i per tant p és *cert*.

Exemple: $\sqrt{2}$ és irracional

Suposem que $\sqrt{2}$ és racional.

$$\text{Per tant: } \exists a, b \in \mathbb{Z} \mid \sqrt{2} = \frac{a}{b}, \text{ mcd}(a, b) = 1$$

$$\sqrt{2} = \frac{a}{b} \implies 2 = \frac{a^2}{b^2} \implies 2b^2 = a^2 \implies 2 \mid a^2 \implies a \text{ és parell}$$

$$\exists k \in \mathbb{Z} \mid a = 2k \implies 2b^2 = (2k)^2 \implies b^2 = 2k^2 \implies b \text{ és parell}$$

$$\left. \begin{array}{l} a \text{ és parell } 2 \mid a \\ b \text{ és parell } 2 \mid b \end{array} \right\} \implies 2 \mid \text{mcd}(a, b) \implies 2 \mid 1 \quad \text{Contradicció}$$

Per tant: $\neg(\sqrt{2} \text{ és racional}) \implies (\sqrt{2} \text{ és irracional})$

3.1.6 Demostració per casos

Una implicació $(p_1 \vee p_2 \vee \dots \vee p_n) \implies q$ equival a $(p_1 \implies q) \wedge (p_2 \implies q) \wedge \dots \wedge (p_n \implies q)$. Per tant, per demostrar una implicació d'aquest tipus és necessari demostrar les implicacions per cada cas $p_i \implies q$ individualment.

Exemple: Si un enter n no és divisible per 3, aleshores $n^2 \equiv 1 \pmod{3}$.

Si $n \nmid 3 \iff n \equiv 1 \pmod{3} \vee n \equiv 2 \pmod{3}$

Cas 1). $n \equiv 1 \pmod{3} \implies n^2 \equiv 1 \pmod{3}$

Cas 2). $n \equiv 2 \pmod{3} \implies n^2 \equiv 1 \pmod{3}$

Per tant: $n \nmid 3 \implies n^2 \equiv 1 \pmod{3}$

3.1.7 Demostracions d'equivalències

Quan varies proposicions són equivalents $p_1 \iff p_2 \iff \dots \iff p_n$, per demostrar-les només ens cal demostrar les implicacions següents $p_1 \implies p_2, p_2 \implies p_3, \dots, p_{n-1} \implies p_n, p_n \implies p_1$.

Exemple: Les afirmacions següents són equivalents

- 1). $n \bmod 3 = 1 \vee n \bmod 3 = 2$
- 2). n no és divisible per 3.
- 3). $n^2 \equiv 1 \pmod{3}$

Demostració

$$(1) \implies (2) \quad n \bmod 3 = 1 \vee n \bmod 3 = 2 \implies 3 \nmid n$$

$$(2) \implies (3) \quad 3 \nmid n \implies n^2 \equiv 1 \pmod{3} \quad (\text{Exemple anterior})$$

$$(3) \implies (1) \quad \text{Suposo que } \neg(n \bmod 3 = 1 \vee n \bmod 3 = 2) \implies \neg(n^2 \equiv 1 \pmod{3})$$

$$\exists k \mid n = 3k \implies n^2 = 9k^2 = 3(3k^2) \implies 3 \mid n^2 \implies n^2 \equiv 0 \pmod{3} \implies n^2 \not\equiv 1 \pmod{3}$$

Per tant: Les equivalències són *certes*.

3.1.8 Demostració constructiva

Els teoremes d'existència tenen una tesi del tipus $\exists x P(x)$. La *demostració constructiva* tracta de trobar un element a tal que $P(a)$ és cert.

Exemple: per tot enter positiu n existeixen n enters compostos consecutius.

$$\forall n \exists x | x + i \text{ és compost } \forall i = 0..n$$

Sigui $x = (n + 1)! + 1$.

Considerem els enters $x + 1, x + 2, \dots, x + n$

$$\forall i = 0..n \quad i + 1 \text{ divideix a } x + i = (n + 1)! + (i + 1)$$

Per tant $x + i$ és compost $\forall i = 0..n$

3.1.9 Demostració no constructiva

La *demostració no constructiva* tracta de demostrar $\exists x$ verificant $P(x)$.

Exemple: Consultar demostració *hi ha infinits nombres primers* de la pàgina 25.

3.1.10 Demostració per contraexemple

Donat que $\neg(\forall x P(x))$ equival a $\exists x \neg P(x)$, per demostrar que $\forall x P(x)$ és fals és suficient amb trobar un element a tal que $P(a)$ sigui fals.

Exemple: $n^2 - n + 41$ és primer $\forall n \in \mathbb{Z}^+$

$$n = 41 \implies 41^2 - 41 + 41 = 41^2 \quad 41^2 \text{ no és primer: FALS}$$

3.2 Inducció matemàtica

El *principi d'inducció* és útil per demostrar proposicions amb infinit nombre d'elements. També s'utilitza per demostrar resultats d'algorismes, verificar programes, grafs, arbres, etc.

Principi de bona ordenació Tot conjunt no buit d'enters no negatius te primer element $\forall A \in \mathbb{Z}^+ \exists \min A$.

3.2.1 Principi d'inducció

Per fer una demostració per inducció donada una propietat que compleixen tots els elements, hem de fer dos passos:

1. pas base: demostrar que $P(n_0)$ és cert, on n_0 és el primer element del conjunt.
2. pas inductiu: es demostra la implicació $P(n) \implies P(n+1)$. Per fer-ho, es suposa que $P(n)$ és cert per $n \geq n_0$ i es veu que $P(n+1)$ també ho és.

Exemple: Demostració de què la suma dels n primers enters positius imparells és n^2 .

$$\sum_{k=1}^n (2k-1) = n^2, \forall n \geq 1$$

pas base: $P(1) \longrightarrow 1 = 1^2 \implies \text{CERT}$.

pas inductiu: $P(n) \implies P(n+1)$

$$\sum_{k=1}^n (2k-1) = n^2 \implies \sum_{k=1}^{n+1} (2k-1) = (n+1)^2$$

$$\sum_{k=1}^{n+1} (2k-1) = \underbrace{\left(\sum_{k=1}^n (2k-1) \right)}_{P(n)} + (2n+1) = n^2 + 2n + 1 = (n+1)^2 \implies P(n+1) \text{ CERT}$$

Per tant: $P(n)$ és cert.

3.2.2 Principi d'inducció forta o completa

Si tenim per cada $n \geq n_0$ una proposició $P(n)$ que pot ser certa o falsa:

$$\forall n \geq n_0 : (P(n_0) \wedge P(n_0+1) \wedge \dots \wedge P(n-1) \wedge P(n)) \implies P(n+1)$$

per demostrar la implicació hem de fer dos passos:

1. pas base: demostrar que $P(n_0)$ és cert, on n_0 és el primer element del conjunt.
2. pas inductiu: es demostra que $P(n-1)$ és cert suposan que $P(n_0), P(n_0+1), \dots, P(n)$ són certs.

Exemple: Demostració de l'existència en el *Teorema Fonamental de l'Aritmètica*.

“Tot enter més gran que 1 és primer o producte de primers”.

pas base: $P(2) \rightarrow 2$ és un número primer.

pas inductiu: $\forall n \geq 2: (P(2), P(3), \dots, P(n)) \implies P(n+1)$

1. Si $n+1$ és primer, $P(n+1)$ és certa.

2. Si $n+1$ no és primer $\implies \exists d, q \in \mathbb{Z} \mid n+1 = dq, 1 < d, q < n+1$

Com que $d, q \geq 2$, d y q són primers o producte de primers. Com que $n+1 = dq$, $n+1$ és producte de primers.

Exemple: La factorització de tot enter $n \geq 2$ és única.

pas base: $P(1)$ és CERT.

pas inductiu: $(\forall n \geq 1)(P(n) \implies P(n+1))$

Suposem que $P(2), P(3), \dots, P(n)$ són certes. Veiem que que $P(n+1)$ també ho és.

- Si $n+1$ és primer aleshores $P(n+1)$ és CERT.

- Si $n+1$ no és primer $\implies \exists n_1, n_2 \in \mathbb{Z} \mid n = n_1 n_2, n_1, n_2 < n \implies P(n+1)$ CERT

Per hipòtesi d'inducció n_1 i n_2 descomposen en producte de primers, i, per tant, n també.

Capítol 4

Combinatoria

4.1 Principis bàsics

La *combinatòria* ens serveix per comptar sense haver de llistar explícitament tots els objectes o combinacions d'objectes.

Donats un conjunt finit A de cardinal n , i una aplicació bijectiva $f : A \rightarrow \{1, 2, 3, \dots, n\}$

4.1.1 Principi de la suma

Donats A, B conjunts finits, $A \cap B = \emptyset$ (conjunts disjunts), aleshores: $|A \cup B| = |A| + |B|$

En general:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$$

Exemple: Un estudiant ha d'escollir un projecte d'entre tres llistes. Les tres llistes tenen 23, 15 i 19 projectes respectivament. Quants projectes té per escollir?

$$\text{Projectes} = 23 + 15 + 19 = 57$$

4.1.2 Principi del producte

Donats A, B conjunts finits, aleshores: $|A \times B| = |A| \cdot |B|$

En general:

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

Exemple: Quantes cadenes de bits de longitud 5 es poden formar?

Cada bit té 2 possibles formes (0 i 1). En total, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$ formes

Exemple: Quantes cadenes de bits de longitud 5 es poden formar amb almenys un 1?

De 2^5 maneres que es podrien formar restem la combinació 00000 que no conté cap 1. Així:

$$2^5 - 1 = 31 \text{ formes}$$

4.2 Permutacions i combinacions

4.2.1 Permutacions

Una *permutació* d'un conjunt és una ordenació dels seus elements. Donat $r \in \mathbb{Z}^+$, i un conjunt de n elements, una **r -permutació** del conjunt és una selecció ordenada de r elements del conjunt.

Notació: $P(n, r)$ = nombre de r permutacions d'un n -conjunt.

TEOREMA

$$P(n, r) = n(n-1)(n-2) \dots (n-(r-1)); \quad P(n, r) = \frac{n!}{(n-r)!}$$

Exemple: Es venen 100 números de loteria a 100 persones, de manera que hi ha 4 premis diferents.

- De quantes maneres es poden repartir els premis?

$$P(100, 4) = \frac{100!}{(100-4)!} = 100 \cdot 99 \cdot 98 \cdot 97 = 94109400$$

- De quantes maneres es poden repartir els premis si la persona amb el número 47 té el primer premi?

$$P(99, 3) = \frac{99!}{(99-3)!} = 99 \cdot 98 \cdot 97 = 941094$$

- De quantes maneres es poden repartir els premis si la persona amb el número 47 té un dels premis?

$$4 \cdot P(99, 3) = 4 \frac{99!}{(99-3)!} = 4 \cdot 99 \cdot 98 \cdot 97 = 3764376$$

- De quantes maneres es poden repartir els premis si la persona amb el número 47 no guanya cap premi?

$$P(99, 4) = \frac{99!}{(99-4)!} = 99 \cdot 98 \cdot 97 \cdot 96 = 90345024$$

4.2.2 Combinacions

Donat $r \in \mathbb{Z}^x$, una **r -combinació** d'un conjunt és una selecció no ordenada de r elements del conjunt.

Notació: $C(n, r)$ = nombre de r combinacions d'un n -conjunt.

TEOREMA

$$C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}; \quad P(n, r) = C(n, r) \cdot r!$$

Observem: $\binom{n}{0} = 1$ $\binom{n}{n} = 1$ $\binom{n}{1} = n$

Corol·lari: $\binom{n}{r} = \binom{n}{n-r}$ $0 \leq r \leq n$

Exemple: De quantes maneres es poden escollir dos números enters menors de 100?

$$C(100, 2) = \binom{100}{2} = \frac{100!}{2!(100-2)!} = 4950 \text{ maneres}$$

Exemple: Donats 6 estudiants de geografia i 11 estudiants d'història, de quantes maneres puc triar 5 estudiants de forma que hi hagi 2 de geografia i 3 d'història.

$$C(11, 3) \cdot C(5, 2) = \binom{11}{3} \cdot \binom{5}{2} = \frac{11!}{3!(11-3)!} \cdot \frac{5!}{2!(5-2)!} = 165 \cdot 10 = 1650 \text{ maneres}$$

4.4 Permutacions i combinacions amb repetició

4.4.1 Permutacions amb repetició

Una **r -permutació amb repetició** d'un conjunt X és una seqüència de r elements de X no necessàriament diferents, es a dir, és una selecció ordenada de r elements que poden ser iguals.

$$\text{PR}(n, r) = n^r$$

Exemple: Quantes cadenes binàries de 5 bits podem fer?

$$\text{PR}(2, 5) = 2^5 = 32 \text{ cadenes}$$

4.4.2 Combinacions amb repetició

Una **r -combinació amb repetició** d'un n -conjunt X és una seqüència no ordenada de r elements de X , no necessàriament diferent.

$$\text{CR}(n, r) = \binom{n-1+r}{r} = \binom{n-1+r}{n-1}$$

Exemple: De quantes maneres es poden barrejar taronges, pomes i peres de forma que al plat hi hagi 3 peces de fruita.

$$\text{CR}(3, 3) = \binom{3-1+3}{3} = \binom{5}{3} = \frac{5!}{3!(5-3)!} = 10 \text{ maneres}$$

Exemple: Trobar el nombre de solucions de l'equació $x_1 + x_2 + x_3 = 11$, $x_i \leq 0$.

Tenim que seleccionar 11 elements: x_1 del tipus u, x_2 del tipus dos, x_3 del tipus 3. Per tant, el nombre de solucions és:

$$\text{CR}(3, 11) = \binom{3-1+11}{11} = \binom{13}{11} = \frac{13!}{11!(13-11)!} = 78 \text{ solucions}$$

Exemple: Trobar el nombre de solucions de l'equació:

$$x_1 + x_2 + x_3 = 11, \quad x_1 \geq 1, \quad x_2 \geq 2, \quad x_3 \geq 3$$

Tenim que seleccionar 11 elements dels quals restem 1, 2 i 3, solucions que no ens interessin, i per tant ens queda una combinació amb 5 elements a seleccionar:

$$\text{CR}(3, 11 - 1 - 2 - 3) = \text{CR}(3, 5) = \binom{3-1+5}{5} = \binom{7}{5} = \frac{7!}{5!(7-5)!} = 21 \text{ solucions}$$

4.4.3 Permutacions d'objectes indistingibles

Donats k tipus d'objectes diferents, el nombre de permutacions de n objectes, de manera que hi ha n_i objectes del tipus i és:

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

Exemple: Quantes paraules diferents es poden formar reordenant la paraula RETRASAR?

Com que la R es repeteix 3 vegades i la A 2 vegades, la fórmula quedaria:

$$\frac{8!}{3!2!1!1!} = 3360 \text{ paraules}$$

4.4.4 Teorema del multinomi

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{n_1+n_2+\dots+n_m=n} \binom{n}{n_1, n_2, \dots, n_m} x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$$

4.5 Principi d'inclusió-exclusió

Siguin A_1, A_2, \dots, A_n conjunts finits, aleshores:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} \left| \bigcap_{1 \leq i \leq n} A_i \right|$$

Exemple: Quants enters hi ha entre 1 i 100 són divisibles entre 3, 5 o 7?

Si anomenem A al conjunt d'enters divisibles per 3, B als divisibles per 5 i C als divisibles per 7:

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ |A| &= 100 \div 3 = 33 & |A \cap B| &= 100 \div (3 \cdot 5) = 6 \\ |B| &= 100 \div 5 = 20 & |A \cap C| &= 100 \div (3 \cdot 7) = 4 \\ |C| &= 100 \div 7 = 14 & |B \cap C| &= 100 \div (5 \cdot 7) = 2 \\ |A \cap B \cap C| &= 100 \div (3 \cdot 5 \cdot 7) = 0 \\ |A \cup B \cup C| &= 33 + 20 + 14 - 6 - 4 - 2 + 0 = 55 \text{ enters} \end{aligned}$$

Exemple: Calcular el nombre de solucions no negatives de l'equació:

$$x_1 + x_2 + x_3 + x_4 = 11 \mid x_1 \leq 3, x_2 \leq 4, x_3 \leq 5$$

Sigui N el nombre de solucions de l'equació sense la condició $x_1 \leq 3, x_2 \leq 4, x_3 \leq 5$, i siguin P_1, P_2 i P_3 els conjunts de les solucions amb $x_1 \leq 3, x_2 \leq 4$ i $x_3 \leq 5$ respectivament, i S el conjunt de les solucions que necessitem:

$$S = N - |P_1 \cup P_2 \cup P_3| = N - |P_1| - |P_2| - |P_3| + |P_1 \cap P_2| + |P_1 \cap P_3| + |P_2 \cap P_3| - |P_1 \cap P_2 \cap P_3|$$

$$\begin{aligned} S &= \text{CR}(3, 11) - \text{CR}(3, 7) - \text{CR}(3, 6) - \text{CR}(3, 4) + \text{CR}(3, 2) + \text{CR}(3, 0) - 0 \\ &= \binom{13}{11} - \binom{9}{7} - \binom{8}{6} - \binom{6}{4} + \binom{4}{2} + \binom{3}{0} = 78 - 36 - 28 - 15 + 6 + 1 = 6 \text{ solucions} \end{aligned}$$

4.5.1 Desarranjaments

Un *desarranjament* d'un n -conjunt $X = \{1, 2, \dots, n\}$ és una permutació σ tal que $\sigma(n) \neq n$, es a dir, una permutació de forma que cap objecte vagi al seu lloc inicial. El nombre de desarranjaments D_n es calcula amb la següent fórmula:

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!} = n! \left(\frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right)$$

Exemple: Quantes desordenacions hi ha dels números 1234? [4 números]

$$D_4 = 4! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \right) = 9$$

4.6 Exemples de demostracions

4.6.1 Propietat d'addició dels nombres binomials

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

$$\begin{aligned} \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k-1)!} \left(\frac{1}{k} + \frac{1}{n-k} \right) \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \left(\frac{n}{k(n-k)} \right) = \frac{n!}{k!(n-k)!} = \binom{n}{k} \end{aligned}$$

4.6.2 Propietat d'absorció

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$$

$$\frac{n}{k} \binom{n-1}{k-1} = \frac{n}{k} \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

4.6.3 Corol·lari d'absorció

$$(n-k) \binom{n}{k} = n \binom{n-1}{k}$$

$$n \binom{n-1}{k} = n \frac{(n-1)!}{k!(n-k-1)!} = \frac{n!}{k!(n-k-1)!} = (n-k) \frac{n!}{k!(n-k)!} = (n-k) \binom{n}{k}$$

4.6.4 Identitat de Pascal

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$$

$$\begin{aligned} \binom{m}{n} + \binom{m}{n-1} &= \frac{m!}{n!(m-n)!} + \frac{m!}{(n+1)!(m-n-1)!} = \frac{m!(n+1)}{(n+1)!(m-n)!} + \frac{m!(m-n)}{(n+1)!(m-n)!} \\ &= \frac{m!(n+1) + m!(m-n)}{(n+1)!(m-n)!} = \frac{m!(m+1)}{(n+1)!(m-n)!} = \frac{(m+1)!}{(n+1)!(m-n)!} = \binom{m+1}{n+1} \end{aligned}$$

Part II

Àlgebra Lineal i Geometria

Capítol 5

Espais vectorials. Càlcul Vectorial

5.1 Sistemes de coordenades

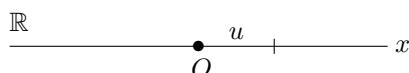
Un *sistema de coordenades* és la manera de poder assignar a un punt unes coordenades. Està format per un origen i uns eixos (sistema de referència).

1. Origen de coordenades: Punt fix i arbitrari O .
2. Eixos de coordenades: Conjunt ordenat de rectes diferents que passen per O . Cada recta té un sentit de recorregut i una unitat de mesura, $\{x_1, x_2, \dots, x_n\}$

Notació: $S = (O, \{x_1, x_2, \dots, x_n\})$

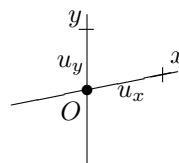
5.1.1 Sistema de coordenades a la recta unidimensional $S = (O, \{x\})$

1. Punt d'origen fixe O .
2. Recta x que passa per l'origen O .
3. Unitat de mesura u_x .



5.1.2 Sistema de coordenades al pla bidimensional $S = (O, \{x, y\})$

1. Punt d'origen fixe O .
2. Rectes x i y ordenades diferents que passen per O .
3. Unitats de mesura u_x i u_y .



Coordenades cartesianes rectangulars

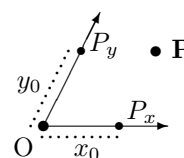
Un *sistema de coordenades cartesianes rectangular* és tal que els seus eixos formen un angle de $\frac{\pi}{2}$ (són ortogonals) i les seves unitats de mesura són iguals a tots dos eixos.

Coordenades d'un punt P

P_x projecció paral·lela de P sobre Ox en la direcció Oy .

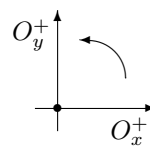
P_y projecció paral·lela de P sobre Oy en la direcció Ox .

Les components de P són: $P = (x_0, y_0)$.

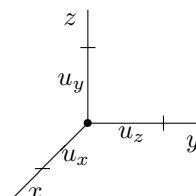


Orientació dels eixos

L'orientació ve definida per l'ordre dels eixos y la orientació de cada eix.
La orientació més utilitzada és antihorària positiva.

**5.1.3 Sistema de coordenades a l'espai tridimensional $S = (O, \{Ox, Oy, Oz\})$**

1. Punt d'origen fixe O.
2. Rectes x , y i z ordenades diferents que passen per O.
3. Unitats de mesura u_x , u_y i u_z .
4. Oz no es troba al pla determinat per Ox i Oy .

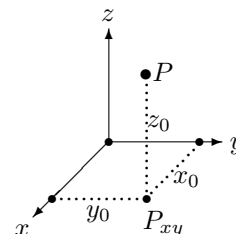
**Coordenades d'un punt**

P_{xy} Projectió paral·lela de P sobre $OxOy$ en la direcció Oz .

(x_0, y_0) coordenades de P_{xy} en el pla $OxOy$.

$|z_0|$ distància de P a P_{xy} , i per tant component de P .

Les components de P són: $P = (x_0, y_0, z_0)$.

**5.2 Parametrització d'objectes geomètrics****5.2.1 Recta, semirecta i segment**

Siguin A i B dos punts, l'equació paramètrica de la recta que passa per A i B és:

$$P(t) = A + t\overrightarrow{AB} \implies \begin{cases} x_1(t) = a_1 + t(b_1 - a_1) \\ x_2(t) = a_2 + t(b_2 - a_2) \\ \vdots \\ x_n(t) = a_n + t(b_n - a_n) \end{cases} \quad t \in \mathbb{R}$$

Si acotem t amb valor mínim $n \leq t \leq \infty$, o un valor màxim $\infty \leq t \leq m$, aleshores estem definint una **semirecta**.

Si acotem t amb dos valors $n \leq t \leq m$, aleshores estem definint un **segment**.

5.2.2 La circumferència al pla bidimensional

L'equació de la circumferència de centre $c = (a, b)$ i radi R és:

$$(x - a)^2 + (y - b)^2 = R^2$$

Si fixem $c = (0, 0)$ i $R = 1$, aleshores parlem de la *circumferència unitat*: $x^2 + y^2 = 1$

Parametrització de la circumferència

$$P(t) = (a + R \cos t, b + R \sin t) \implies \begin{cases} x(t) = a + R \cos t \\ y(t) = b + R \sin t \end{cases} \quad 0 \leq t \leq 2\pi$$

Si acotem t , aleshores estem definint un **arc**.

5.2.3 El cilindre circular a l'espai tridimensional

Sigui R el radi del cilindre, $c = (a, b, 0)$ el centre i h l'altura, l'equació del cilindre és:

$$P(t) = (a + R \cos t, b + R \sin t, s) \implies \begin{cases} x(t) = a + R \cos t \\ y(t) = b + R \sin t \\ z(t) = s \end{cases} \quad 0 \leq t \leq 2\pi, \quad 0 \leq s \leq h$$

Si fixem a s un valor determinat, aleshores tenim una circumferència a l'espai.

5.3 Vectors

5.3.1 Visió geomètrica. Segments dirigits

Vector fix Siguin A i B dos punts, és el segment orientat de A cap a B , que notem \overrightarrow{AB} . Aquest vector té les següents característiques

- Direcció. Recta única que conté A i B .
- Sentit. Orientació del vector.
- Norma. Longitud o distància entre A i B .

Vector posició Un vector posició en un sistema de coordenades S és aquell que va des de l'origen O a un punt P . Les components del vector són les del punt.

5.3.2 Operacions amb vectors

Suma Operació interna, on el vector resultant és la suma de les components dels dos vectors que se sumen.

$$\vec{u} + \vec{v} = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$$

Propietats de la suma

- Associativa: $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$
- Element neutre: $\exists \vec{0} \mid \vec{0} + \vec{u} = \vec{u}$
- Element oposat: $\forall \vec{u} \exists (-\vec{u}) \mid \vec{u} + (-\vec{u}) = \vec{0}$
- Commutativa: $\vec{u} + \vec{v} = \vec{v} + \vec{u}$

Aquestes propietats fan del conjunt \mathbb{R}^n i la operació suma un *grup abelià* $(\mathbb{R}^n, +)$.

Producte per escalars Operació externa, on el vector resultant és la multiplicació dels components del vector per l'escalar que el multiplica.

$$\lambda \vec{u} = (\lambda u_1 + \lambda u_2, \dots, \lambda u_n), \quad \lambda \in \mathbb{R}$$

Propietats del producte per escalar

- Associativa: $\lambda(\mu \vec{u}) = (\lambda\mu) \vec{u}$
- Distributiva respecte la suma: $\lambda(\vec{u} + \vec{v}) = \lambda \vec{u} + \lambda \vec{v}, \quad (\lambda + \mu) \vec{u} = \lambda \vec{u} + \mu \vec{u}$
- Element neutre: $1 \in \mathbb{R}, \quad 1 \vec{u} = \vec{u}$

5.3.3 Norma i distància

Sigui S un sistema de referència cartesià rectangular. Definim la norma d'un vector $\|\vec{u}\|$ com la distància entre els seus extrems, o la longitud de \vec{u} .

$$\|\vec{u}\| = \sqrt{(u_1)^2 + (u_2)^2 + \dots + (u_n)^2}$$

Per tant, la distància entre dos punts A i B és la norma del vector que els uneix.

$$\|\overrightarrow{AB}\| = \sqrt{(b_1 - a_1)^2 + (b_2 - a_2)^2 + \dots + (b_n - a_n)^2}$$

Propietats bàsiques

- $\|\vec{u}\| = 0 \iff \vec{u} = \vec{0}$
- $d(A, B) = 0 \iff \overrightarrow{AB} = \vec{0} \iff A = B$
- $\|\lambda\vec{u}\| = |\lambda|\|\vec{u}\|$

5.4 Espais vectorials

5.4.1 Definició i exemples

Sigui k un cos i E un conjunt, amb $|E| \neq 0$. E és un k -espai vectorial si té

- Operació interna suma, que compleix les propietats: associativa, element neutre, element oposat i commutativa.

$$\begin{aligned} E \times E &\longrightarrow E \\ (\vec{u}, \vec{v}) &\longmapsto \vec{u} + \vec{v} \end{aligned}$$

- Operació externa producte per escalar, que compleix les propietats: associativa, distributiva respecte la suma i element neutre.

$$\begin{aligned} k \times E &\longrightarrow E \\ (\lambda, \vec{u}) &\longmapsto \lambda\vec{u} \end{aligned}$$

Exemples

1. $\mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^n$
2. $M_{n \times m}(k) = \{\text{matrius } n \times m \text{ amb suma i producte per escalar}\}$
3. $\mathbb{R}_n = \{\text{polinomis amb coeficients reals de grau } \leq n, \text{ amb suma i producte per escalar}\}$

Nota Per demostrar que un conjunt amb dues operacions és un espai vectorial, hem de demostrar cada una de les propietats de l'operació suma i multiplicació.

5.4.2 Combinacions lineals. Dependència i independència lineal

Sigui E un k -espai vectorial, i $S = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_r\} \subset E$ un subconjunt de vectors de E .

Combinació lineal

Una *combinació lineal* dels vectors de S és qualsevol vector \vec{v} que compleix

$$\vec{v} = \lambda_1\vec{u}_1 + \lambda_2\vec{u}_2 + \dots + \lambda_r\vec{u}_r, \quad \forall i, \lambda_i \in k$$

Exemples

1. $(5, 4)$ és combinació lineal de $(1, 2), (3, 0) \longrightarrow (5, 4) = 2(1, 2) + (3, 0)$
2. Les combinacions lineals de $(2, 3, 4)$ i $(1, -1, 3)$ són

$$\vec{v} = \lambda(2, 3, 4) + \mu(1, -1, 3) = (2\lambda + \mu, 3\lambda - \mu, 4\lambda + 3\mu) \quad \lambda, \mu \in \mathbb{R}$$

Teorema

Qualsevol vector de \mathbb{R}^n és combinació lineal dels vectors $\{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$, on

$$\begin{cases} \vec{e}_1 = (1, 0, 0, \dots, 0) \\ \vec{e}_2 = (0, 1, 0, \dots, 0) \\ \vdots \\ \vec{e}_n = (0, 0, \dots, 0, 1) \end{cases}$$

Dependencia lineal

Un conjunt de vectors $S = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_r\}$ és *linealment dependent* (LD) si almenys un dels vectors és combinació lineal de la resta. Per tant

$$\exists \lambda_1, \lambda_2, \dots, \lambda_n \in k, \lambda_i \neq 0 \quad | \quad \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_r = \vec{0}$$

Altrament, el conjunt S és *linealment independent* (LI), i per tant

$$\nexists \lambda_1, \lambda_2, \dots, \lambda_n \in k, \lambda_i \neq 0 \quad | \quad \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_r = \vec{0}$$

Exemple $S = \{(1, 2), (3, 0)\}$ és linealment independent

$$\lambda(1, 2) + \mu(3, 0) = (0, 0) = \vec{0} \implies \lambda = \mu = 0$$

Teorema

L'expressió d'un vector com a combinació lineal de vectors linealment independents és única. Sigui $S = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ linealment independents.

$$\forall i, \exists! \lambda_i \quad | \quad \vec{v} = \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_n$$

Teorema

$$n \text{ vectors } \begin{cases} \vec{u}_1 = (u_{11}, u_{12}, \dots, u_{1r}) \\ \vec{u}_2 = (u_{21}, u_{22}, \dots, u_{2r}) \\ \vdots \\ \vec{u}_n = (u_{n1}, u_{n2}, \dots, u_{nr}) \end{cases} \text{ són linealment independents si}$$

$$\lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_n = (0, 0, \dots, 0) = \vec{0} \implies \lambda_1 = \lambda_2 = \dots = \lambda_n = 0$$

$$\begin{cases} \lambda_1 u_{11} + \lambda_2 u_{21} + \dots + \lambda_n u_{n1} = 0 \\ \lambda_1 u_{12} + \lambda_2 u_{22} + \dots + \lambda_n u_{n2} = 0 \\ \vdots \\ \lambda_1 u_{1r} + \lambda_2 u_{2r} + \dots + \lambda_n u_{nr} = 0 \end{cases} \iff \left(\begin{array}{cccc|c} u_{11} & u_{21} & \dots & u_{n1} & 0 \\ u_{12} & u_{22} & \dots & u_{n2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_{1r} & u_{2r} & \dots & u_{nr} & 0 \end{array} \right)$$

La matriu és el resultat de posar els n vectors en columna. Com que és un sistema homogeni, un resultat és $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$. Si el resultat és únic, llavors es tracta de vectors linealment independents. Perquè el resultat sigui únic, cal que el sistema sigui compatible determinat, es a dir, que el rang de la matriu sigui n , i per tant que el determinant de la matriu sigui diferent a 0. Altrament, serà un sistema compatible determinat i els vectors seran linealment dependents.

$$\begin{vmatrix} u_{11} & u_{21} & \dots & u_{n1} \\ u_{12} & u_{22} & \dots & u_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{1r} & u_{2r} & \dots & u_{nr} \end{vmatrix} \neq 0 \iff \vec{u}_1, \vec{u}_2, \dots, \vec{u}_n \text{ LI}$$

Exemple $S = \{(1, 0, 5, 3), (7, 1, -1, 0), (17, 2, 13, 9)\}$

$$\left(\begin{array}{ccc|c} 1 & 7 & 17 & 0 \\ 0 & 1 & 2 & 0 \\ 5 & -1 & 13 & 0 \\ 3 & 0 & 9 & 0 \end{array} \right) \longrightarrow \left| \begin{array}{ccc} 1 & 7 & 17 \\ 0 & 1 & 2 \\ 5 & -1 & 13 \end{array} \right| = 0, \quad \left| \begin{array}{ccc} 0 & 1 & 2 \\ 5 & -1 & 13 \\ 3 & 0 & 9 \end{array} \right| = 0 \iff \text{vectors LD}$$

5.4.3 Sistemes de generadors. Bases.

$S = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_r\} \subset E$ és un sistema de generadors de E si tot vector de E es pot expressar com a combinació lineal de S .

$$\forall \vec{v} \in E, \exists \lambda_1, \lambda_2, \dots, \lambda_r \in k \mid \vec{v} = \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_r \vec{u}_r$$

Exemple $S = \{(-1, 2), (1, 1)\}$ Sigui $\vec{v} = (x, y)$. Perquè S sigui generador, tot vector \vec{v} ha de ser combinació lineal dels vectors de S .

$$(x, y) = \lambda(-1, 2) + \mu(1, 1) \quad \forall v_1, v_2$$

$$\left. \begin{array}{l} x = -\lambda + \mu \\ y = 2\lambda + \mu \end{array} \right\} \longrightarrow \lambda = \frac{y-x}{3}, \mu = \frac{2x+y}{3} \implies \text{Són generadors}$$

Base

Una *base* de E és un conjunt de vectors $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$ linealment independents que són generadors. La *dimensió* de E és el nombre de vectors de la base.

Notem que totes les bases d'un espai vectorial tenen el mateix nombre de vectors.

Teorema

Sigui E un subespai vectorial, i $B = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ una base de E , les components d'un vector existeixen (perquè els vectors de B són generadors) i són úniques (perquè els vectors de B són linealment independents).

$$\vec{v} \in E \implies \exists! \lambda_1, \lambda_2, \dots, \lambda_n \in k \mid \vec{v} = \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_n$$

5.4.4 Subespais vectorials

Sigui E un k -espai vectorial. Un subconjunt $F \subset E$ és un *subespai vectorial* si compleix

- $\vec{u}, \vec{v} \in F \implies \vec{u} + \vec{v} \in F$
- $\forall \lambda \in k, \vec{u} \in F \implies \lambda \vec{u} \in F$

Aquestes dues propietats es poden resumir en una de sola

- $\forall \lambda, \mu \in k, \vec{u}, \vec{v} \in F \implies \lambda \vec{u} + \mu \vec{v} \in F$

Exemple $F = \{(x, 0, z)\} \in \mathbb{R}^3$

$$\lambda \vec{u} + \mu \vec{v} = \lambda(x, 0, z) + \mu(x', 0, z') = (\lambda x + \mu x', 0, \lambda z + \mu z') \in F$$

Teorema

Sigui E un k -espai vectorial, i $S = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\} \in E$ un conjunt de vectors. El conjunt $F = \{\lambda_1 \vec{u}_1, \lambda_2 \vec{u}_2, \dots, \lambda_n \vec{u}_n\}$ de totes les combinacions lineals és un subespai vectorial. Es denota $F = \langle S \rangle = \langle \vec{u}_1, \vec{u}_2, \dots, \vec{u}_n \rangle$.

Interpretació geomètrica. Plans

Donats un punt A i dos vectors \vec{u}, \vec{v} , tot punt del pla ve determinat per A en la direcció $\langle \vec{u}, \vec{v} \rangle$ de la forma

$$\overrightarrow{OP} = \overrightarrow{OA} + \lambda\vec{u} + \mu\vec{v}$$

$$P(\lambda, \mu) = A + \lambda\vec{u} + \mu\vec{v}$$

Teorema

Sigui E un espai vectorial, i F, H dos subespais vectorials de E .

- $F \cap H$ és un subespai vectorial.
- $F + H$ és un subespai vectorial.

5.4.5 Espais de dimensió finita**Teorema**

Sigui $\{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ base d'un espai vectorial E de dimensió n , i sigui \vec{w} una combinació lineal dels vectors de la base, aleshores $\{\vec{w}, \vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\} - \{\vec{u}_i\}$ és també base de E .

Teorema d'Steinitz

Sigui E un k -espai vectorial de dimensió finita n . Tot conjunt de vectors linealment independent es pot ampliar fins a obtenir una base de E .

Teorema

Totes les bases d'un espai vectorial de dimensió finita tenen el mateix nombre de vectors.

Base d'un subespai vectorial

Sigui $F \subset E$ un subespai vectorial de E . Una base de F és un conjunt de vectors linealment independents i que generen F .

Propietats bàsiques

- Si $\dim F = \dim E \implies F = E$
- Sigui $G \subset E$ s.e.v. Si $\dim F = \dim G \implies F = G$
- Un conjunt amb més vectors que la base de F és linealment dependent.

5.5 Canvi de sistema de referència

Sigui S un sistema de coordenades. Un **canvi de referència** consisteix en canviar l'origen i/o la base del sistema de coordenades.

5.5.1 Canvi d'origen

Teorema

Siguin S i S' dos sistemes de referència a \mathbb{R}^n

$$S = (O, \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}) \quad S' = (O', \{\vec{u}'_1, \vec{u}'_2, \dots, \vec{u}'_n\}) \quad O' = (\alpha_1, \alpha_2, \dots, \alpha_n)_S$$

Sigui $P \in \mathbb{R}^n$ un punt qualsevol: $P = (x_1, x_2, \dots, x_n)_S \quad P' = (x'_1, x'_2, \dots, x'_n)_{S'}$

$$\begin{cases} x_1 = \alpha_1 + x'_1 \\ x_2 = \alpha_2 + x'_2 \\ \vdots \\ x_n = \alpha_n + x'_n \end{cases} \iff \begin{cases} x'_1 = x_1 - \alpha_1 \\ x'_2 = x_2 - \alpha_2 \\ \vdots \\ x'_n = x_n - \alpha_n \end{cases}$$

A nivell matricial:

$$\overrightarrow{OP} = \overrightarrow{OO'} + \overrightarrow{O'P} \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} + \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

Exemple $S = (O, \{\vec{u}_1, \vec{u}_2, \vec{u}_3\}) \quad S' = (O', \{\vec{u}'_1, \vec{u}'_2, \vec{u}'_3\}) \quad O' = (1, 2, 3)_S$

$$P = (x, y, z)_S = (x - 1, y - 2, z - 3)_{S'}$$

5.5.2 Canvi de base. Canvi d'eixos

Siguin dos sistemes de coordenades $S = (O, B)$, $S' = (O, B')$, amb

$$B = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\} \quad B' = \{\vec{u}'_1, \vec{u}'_2, \dots, \vec{u}'_n\}$$

on les components dels vectors \vec{u}'_i són

$$\begin{aligned} \vec{u}'_1 &= a_{11}\vec{u}_1 + a_{21}\vec{u}_2 + \dots + a_{n1}\vec{u}_n \\ \vec{u}'_2 &= a_{12}\vec{u}_1 + a_{22}\vec{u}_2 + \dots + a_{n2}\vec{u}_n \\ &\vdots \\ \vec{u}'_n &= a_{1n}\vec{u}_1 + a_{2n}\vec{u}_2 + \dots + a_{nn}\vec{u}_n \end{aligned}$$

La matriu del canvi de base de B' a B està formada per les components a_{ij} dels vectors de la base B' , expressats respecte als vectors u_i de la base B .

$$M_{B' \rightarrow B} = A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Mentres que la matriu del canvi de base de B a B' és la inversa de la matriu $M_{B' \rightarrow B}$.

Teorema

Sigui $\vec{v} = (x_1, x_2, \dots, x_n)_B = (x'_1, x'_2, \dots, x'_n)_{B'}$

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} \quad A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

Exemple

$$B = \{\vec{u}_1, \vec{u}_2, \vec{u}_3\} \quad B' = \{\vec{u}'_1 = \vec{u}_1 + \vec{u}_2 + \vec{u}_3, \vec{u}'_2 = \vec{u}_1 - 2\vec{u}_2, \vec{u}'_3 = -\vec{u}_2 + \vec{u}_3\}$$

$$\begin{aligned} \vec{u}'_1 &= (1, 1, 1)_B \\ \vec{u}'_2 &= (1, -2, 0)_B \\ \vec{u}'_3 &= (0, -1, 1)_B \end{aligned} \quad \longrightarrow \quad M_{B' \rightarrow B} = A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & -1 \\ 1 & 0 & -1 \end{pmatrix}$$

$$\text{Si } \vec{v} = (x, y, z)_B = (x', y', z')_{B'}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & -1 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \quad \longrightarrow \quad \begin{cases} x = x' + y' \\ y = x' - 2y' - z' \\ z = x' + z' \end{cases}$$

5.5.3 Canvi complet de coordenades

Siguin

- $S = (O, \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\})$ $S' = (O', \{\vec{u}'_1, \vec{u}'_2, \dots, \vec{u}'_n\})$ dos sistemes de coordenades
- A la matriu del canvi de base de $\{u'_i\}$ a $\{u_i\}$
- $O' = (\alpha_1, \alpha_2, \dots, \alpha_n)_S$ l'origen de S' amb coordenades a S

Teorema

Sigui el punt $P = (x_1, x_2, \dots, x_n)_S = (x'_1, x'_2, \dots, x'_n)_{S'}$

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \quad A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + A^{-1} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

Exemple

$$\text{Sigui } \begin{aligned} S &= (O, \{\vec{u}_1, \vec{u}_2, \vec{u}_3\}) \\ S' &= (O', \{\vec{u}'_1, \vec{u}'_2, \vec{u}'_3\}) \\ O' &= (1, 2, 3)_S \end{aligned} \quad \text{amb } \quad A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & -1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & -1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad \longrightarrow \quad \begin{cases} x = x' + y' + 1 \\ y = x' - 2y' - z' + 2 \\ z = x' + z' + 3 \end{cases}$$

5.6 Exemples de demostracions**5.6.1 L'expressió d'un vector com a combinació lineal de vectors L.I. és única**

Suposem que l'expressió no és única.

$$\vec{u} = \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 + \dots + \lambda_n \vec{u}_n = \mu_1 \vec{u}_1 + \mu_2 \vec{u}_2 + \dots + \mu_n \vec{u}_n$$

Com que els vectors u_i són L.I., aleshores

$$(\lambda_1 - \mu_1) + (\lambda_2 - \mu_2) + \dots + (\lambda_n - \mu_n) = 0 \iff \begin{cases} (\lambda_1 - \mu_1) = 0 \\ (\lambda_2 - \mu_2) = 0 \\ \vdots \\ (\lambda_n - \mu_n) = 0 \end{cases} \iff \begin{cases} \lambda_1 = \mu_1 \\ \lambda_2 = \mu_2 \\ \vdots \\ \lambda_n = \mu_n \end{cases}$$

5.6.2 Teorema. $\langle S \rangle$ Subespai generat per S

$$\langle S \rangle = \{\lambda_1 \vec{v}_1, \lambda_2 \vec{v}_2, \dots, \lambda_n \vec{v}_n\}$$

$$\left. \begin{array}{l} \vec{u}, \vec{w} \in \langle S \rangle \\ \beta, \gamma \in k \end{array} \right\} \beta \vec{u} + \lambda \vec{w} = \beta(\theta_1 \vec{v}_1 + \theta_2 \vec{v}_2 + \dots + \theta_n \vec{v}_n) + \gamma(\mu_1 \vec{v}_1 + \mu_2 \vec{v}_2 + \dots + \mu_n \vec{v}_n)$$

$$\beta \vec{u} + \lambda \vec{w} = (\beta\theta_1 + \gamma\mu_1)\vec{v}_1 + (\beta\theta_2 + \gamma\mu_2)\vec{v}_2 + \dots + (\beta\theta_n + \gamma\mu_n)\vec{v}_n \in \langle S \rangle$$

5.6.3 F, H s.e.v. $\implies F \subset H$ s.e.v.

$$\left. \begin{array}{l} \vec{u} \in F \cap E \implies \vec{u} \in F \wedge \vec{u} \in H \\ \vec{v} \in F \cap E \implies \vec{v} \in F \wedge \vec{v} \in H \end{array} \right\} \implies \vec{u} + \vec{v} \in F \wedge \vec{u} + \vec{v} \in H \implies \vec{u} + \vec{v} \in F \cap H$$

Capítol 6

Aplicacions Lineals

6.1 Definició. Exemples. Propietats bàsiques

Siguin E, F dos k -espais vectorials, una aplicació lineal $f : E \rightarrow F$ és una aplicació tal que

1. $f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v}) \quad \forall \vec{u}, \vec{v} \in E$
2. $f(\lambda \vec{u}) = \lambda f(\vec{u}) \quad \forall \lambda \in k$

és a dir, conserva les propietats d'espai vectorial.

Exemples

1. $f : \mathbb{R}^2 \rightarrow \mathbb{R}$
 $(x, y) \mapsto 2x - 5y$

2. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ Demostració
 $(x, y) \mapsto (y, x, x + y)$

(a) $\vec{u} = (x, y) \in \mathbb{R}^2$
 $\vec{v} = (x', y') \in \mathbb{R}^2 \quad f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$

$$f(\vec{u} + \vec{v}) = f(x + x', y + y') = (y + y', x + x', x + x' + y + y')$$
$$f(\vec{u}) + f(\vec{v}) = f(x, y) + f(x', y') = (y, x, x + y) + (y', x', x' + y') = (y + y', x + x', x + x' + y + y')$$

(b) $\lambda \in \mathbb{R} \quad f(\lambda \vec{u}) = \lambda f(\vec{u})$

$$f(\lambda \vec{u}) = f(\lambda x, \lambda y) = (\lambda y, \lambda x, \lambda x + \lambda y)$$
$$\lambda f(\vec{u}) = \lambda f(x, y) = \lambda(y, x, x + y) = (\lambda y, \lambda x, \lambda x + \lambda y)$$

6.1.1 Propietats bàsiques

Siguin E, F dos k -espais vectorials, i $f : E \rightarrow F$ una aplicació lineal

1. $f(0_E) = f(0_F)$
2. $f(-\vec{u}) = -f(\vec{u})$
3. $f(\vec{u} - \vec{v}) = f(\vec{u}) - f(\vec{v})$

Teorema

Una aplicació lineal $f : E \rightarrow F$ queda determinada de manera única per la imatge dels vectors de la base.

6.2 Nucli i imatge d'una aplicació lineal

Siguin E, F dos k -espais vectorials i $f : E \rightarrow F$ una aplicació lineal.

- El **nucli** de f és el conjunt de vectors de E que tenen imatge 0_F .

$$\ker(f) = \{\vec{u} \in E \mid f(\vec{u}) = 0_F\} = f^{-1}(0_F) \subset E$$

- La **imatge** de f és el conjunt de vectors de F que tenen antiimatge a E .

$$\text{Im}(f) = \{f\vec{u} \mid \vec{u} \in E\} \subset F$$

Exemples

$$1. \quad \begin{array}{ccc} f : \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & 2x - 5y \end{array}$$

$$\begin{aligned} \ker(f) &= \{(x, y) \mid f(x, y) = 0\} = \{(x, \frac{2}{5}x)\} = \langle (1, \frac{2}{5}) \rangle \\ \text{Im}(f) &= \{2x - 5y \mid (x, y) \in \mathbb{R}^2\} = \mathbb{R} \end{aligned}$$

$$2. \quad \begin{array}{ccc} f : \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x, y) & \longmapsto & (x - y, 2x - 2y) \end{array}$$

$$\begin{aligned} \ker(f) &= \{(x, y) \mid f(x, y) = (0, 0)\} = \{(x, x)\} = \langle (1, 1) \rangle \\ \text{Im}(f) &= \{(x - y, 2x - 2y)\} = \{x(1, 2) - y(1, 2)\} = \{(x - y)(1, 2)\} = \langle (1, 2) \rangle \end{aligned}$$

Teorema

- $\ker(f)$ és un subespai vectorial de E .
- $\text{Im}(f)$ és un subespai vectorial de F .
- $\dim \ker(f) + \dim \text{Im}(f) = \dim E$

6.3 Càlcul matricial

6.3.1 Matriu associada a una aplicació lineal

Siguin E, F dos k -espais vectorials, i $f : E \rightarrow F$ una aplicació lineal. Fixem a E una base $\{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ i una base a F $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_m\}$. Com que la aplicació lineal queda determinada per les imatges dels vectors de la base E , podem escriure una matriu amb aquestes imatges, que se l'anomena **matriu associada**.

$$\begin{array}{l} f(\vec{u}_1) = a_{11}\vec{v}_1 + a_{21}\vec{v}_2 + \dots + a_{m1}\vec{v}_m \\ f(\vec{u}_2) = a_{12}\vec{v}_1 + a_{22}\vec{v}_2 + \dots + a_{m2}\vec{v}_m \\ \vdots \\ f(\vec{u}_n) = a_{1n}\vec{v}_1 + a_{2n}\vec{v}_2 + \dots + a_{mn}\vec{v}_m \end{array} \quad \longrightarrow \quad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Exemples

$$1. \quad \begin{array}{ccc} f : \mathbb{R}^3 & \longrightarrow & \mathbb{R}^4 \\ (x, y, z) & \longmapsto & (x + y, x + z, 2x + y + z, y - z) \end{array} \quad \text{matriu en les bases canòniques.}$$

$$\begin{aligned} f(1, 0, 0) &= (1, 1, 2, 0) = 1(1, 0, 0, 0) + 1(0, 1, 0, 0) + 2(0, 0, 1, 0) + 0(0, 0, 0, 1) \\ f(0, 1, 0) &= (1, 0, 1, 1) = 1(1, 0, 0, 0) + 0(0, 1, 0, 0) + 1(0, 0, 1, 0) + 1(0, 0, 0, 1) \\ f(0, 0, 1) &= (0, 1, 1, -1) = 0(1, 0, 0, 0) + 1(0, 1, 0, 0) + 1(0, 0, 1, 0) - 1(0, 0, 0, 1) \end{aligned} \quad \longrightarrow \quad \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$2. \quad f: \mathbb{R}^2 \longrightarrow \mathbb{R}^3 \quad \text{amb bases} \quad \begin{array}{l} B_1 = \{(2, 1), (-1, 0)\} \in \mathbb{R}^2 \\ B_2 = \{(1, 0, 1), (0, 0, 1), (0, -1, 1)\} \in \mathbb{R}^3 \end{array}$$

$$(x, y) \longmapsto (2x + y, x - y, x + y)$$

$$\begin{aligned} f(2, 1) &= (5, 1, 3) = 5(1, 0, 1) - 1(0, 0, 1) - 1(0, -1, 1) \\ f(-1, 0) &= (-2, -1, -1) = -2(1, 0, 1) + 0(0, 0, 1) + 1(0, -1, 1) \end{aligned} \longrightarrow \begin{pmatrix} 5 & -2 \\ -1 & 0 \\ -1 & 1 \end{pmatrix}$$

Teorema

Sigui $f: E \longrightarrow F$ una aplicació lineal i A la seva matriu associada en unes certes bases B_E de E i B_F de F . La imatge d'un vector $\vec{v} = (x_1, x_2, \dots, x_n)_{B_E}$ és $f(\vec{v}) = (z_1, z_2, \dots, z_m)_{B_F}$, on $F(\vec{v})$ és el vector resultant de multiplicar el vector \vec{v} per la matriu A

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{pmatrix}$$

Exemple

$$f: \mathbb{R}^2 \longrightarrow \mathbb{R}^3 \quad \text{amb matriu associada } A = \begin{pmatrix} 2 & 1 \\ 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$f(x, y) = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + y \\ x - y \\ x + y \end{pmatrix} = (2x + y, x - y, x + y)$$

6.4 Canvi de base en la matriu d'una aplicació lineal**Teorema**

Siguin E i F dos k -espais vectorials amb les seves bases $B = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ i $V = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_m\}$ respectivament, si sigui $f: E \longrightarrow F$ una aplicació lineal amb matriu associada A .

Considerem unes noves bases B' i V' , amb P la matriu del canvi de base de B' a B i M la matriu del canvi de base de V' a V . La matriu de f en les noves bases B' i V' és

$$A' = MAP$$

En particular, si $E = F$ i $B = V, B' = V'$, aleshores $A' = P^{-1}AP$

Exemple 1 $f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ amb matriu $A = \begin{pmatrix} 6 & -2 \\ 6 & 1 \end{pmatrix}$ en les bases canòniques.

Problema: Canviar la matriu de f a la base $\{(1, 2), (1, 3)\}$ (tenin en compte que tots dos espais vectorials tenen la mateixa base).

$$A' = P^{-1}AP = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 6 & -2 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ 0 & 3 \end{pmatrix}$$

Exemple 2 $f: \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ amb matriu $A = \begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix}$ i bases $\begin{array}{l} \{\vec{u}_1, \vec{u}_2, \vec{u}_3\} \in \mathbb{R}^3 \\ \{\vec{v}_1, \vec{v}_2\} \in \mathbb{R}^2 \end{array}$

Problema: Trobar la matriu f en les bases $\{\vec{u}_1, \vec{u}_1 + \vec{u}_2, 2\vec{u}_1 + \vec{u}_3\} \in \mathbb{R}^3$
 $\{3\vec{v}_1 + \vec{v}_2, 2\vec{v}_1\} \in \mathbb{R}^2$

$$A' = MAP = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 4 & 6 & 10 \\ -5 & -5 & -13 \end{pmatrix}$$

6.5 Algunes aplicacions lineals

6.5.1 Monomorfisme, epimorfisme i isomorfisme

Siguin E, F k -espais vectorials, i $f : E \rightarrow F$ una aplicació lineal.

1. f és *injectiva* (**monomorfisme**) si $\ker(f) = \{0_E\}$. Transforma vectors LI en vectors LI.
2. f és *exhaustiva* (**epimorfisme**) si $\dim(\text{Im } f) = \dim(F) \iff \text{Im } f = F$
3. f és *bijectiva* (**isomorfisme**) si $\dim(\text{Im } f) = \dim(F) = \dim(E) \iff f$ té inversa

Com a conseqüència, si $\dim(E) = \dim(F)$: f bijectiva $\iff f$ injectiva $\iff f$ exhaustiva

6.5.2 Inversa d'una aplicació lineal

Una aplicació lineal f té inversa si i només si és bijectiva. Aquesta inversa també és lineal.