Claudi Lleyda Moltó

# Apunts de matemàtiques

*Les matemàtiques són un joc de definicions*


Notes de classe

Promoció 2016-17

# Índex

# Part I

# Fonaments de les matemàtiques

# Capítol 1

# Lògica matemàtica

## 1.1 Els fonaments

### 1.1.1 Processos fonamentals de les matemàtiques

Definirem de manera informal els conceptes d'*objecte matemàtic*, de *relació* entre objectes i de *demostració* d'una relació. Aquests són els tres processos fonamentals de les matemàtiques.

Els *objectes matemàtics* són abstraccions de conceptes. Anomenem a les possibles propietats d'aquests objectes *relacions*. Aquestes poden ser o bé vertaderes o bé falses.

Anomenem a algunes d'aquestes relacions *axiomes*, que són relacions que prenem com a vertaderes des d'un principi. Per determinar la veracitat d'altres relacions empararem les *demostracions*. Direm que una relació és vertadera quan es pot deduir a partir dels axiomes amb una demostració, que és una successió d'arguments rigorosos per convèncer-nos de que una relació és vertadera.

### 1.1.2 Operacions lògiques elementals

**Definició 1.1.1** (Disjunció)**.** Siguin $R$ i $S$ dues relacions. Aleshores definim una relació anomenada disjunció. L'escriurem $R \vee S$, i ho llegirem "$R$ o $S$".

**Definició 1.1.2** (Negació)**.** Sigui $R$ una relació. Aleshores definim una relació anomenada negació. L'escriurem $\neg R$ i ho llegirem "no $R$".

**Definició 1.1.3** (Conjunció)**.** Siguin $R$ i $S$ dues relacions. Aleshores definim una relació anomenada conjunció definida com

$$R \wedge S = \neg((\neg R) \vee (\neg S)).$$

Ho llegirem "$R$ i $S$".

**Definició 1.1.4** (Disjunció excloent)**.** Siguin $R$ i $S$ dues relacions. Aleshores definim una relació anomenada disjunció excloent definida com

$$R \veebar S = (R \wedge (\neg S)) \vee ((\neg R) \wedge S).$$

Ho llegirem "o bé $R$ o bé $S$".

**Definició 1.1.5** (Implicació)**.** Siguin $R$ i $S$ dues relacions. Aleshores definim una relació anomenada implicació definida com

$$R \Rightarrow S = S \vee (\neg R).$$

Ho llegirem "$R$ implica $S$" o "si $R$ aleshores $S$".

**Definició 1.1.6** (Doble implicació)**.** Siguin $R$ i $S$ dues relacions. Aleshores definim una relació anomenada doble implicació definida com

$$R \Leftrightarrow S = (R \Rightarrow S) \wedge (S \Rightarrow R).$$

Ho llegirem com "$R$ si i només si $S$" o "$R$ és equivalent a $S$".

### 1.1.3 Relacions vertaderes

**Axioma 1.1.7.** *Sigui $R$ una relació. Aleshores la relació*

$$(R \vee R) \Rightarrow R$$

*és vertadera.*

**Axioma 1.1.8.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació*

$$R \Rightarrow (R \vee S)$$

*és vertadera.*

**Axioma 1.1.9.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació*

$$(R \vee S) \Rightarrow (S \vee R)$$

*és vertadera.*

**Axioma 1.1.10.** *Siguin $R$, $S$ i $T$ tres relacions. Aleshores la relació*

$$(R \Rightarrow S) \Rightarrow ((R \vee T) \Rightarrow (S \vee T))$$

*és vertadera.*

**Axioma 1.1.11.** *Siguin $R$ i $S$ dues relacions tals que $R$ i $R \Rightarrow S$ siguin vertaderes. Aleshores $S$ és vertadera.*

**Definició 1.1.12** (Relació falsa)**.** Sigui $R$ una relació tal que $\neg R$ sigui vertadera. Aleshores direm que $R$ és falsa.

### 1.1.4 Tautologies

**Tautologia 1.1.13.** *Siguin $R$, $S$ i $T$ tres relacions tals que $R \Rightarrow S$ i $S \Rightarrow T$ siguin vertaderes. Aleshores la relació $R \Rightarrow T$ és vertadera.*

*Demostració.* Per l'axioma 1.1.10 la relació

$$(S \Rightarrow T) \Rightarrow (S \vee (\neg R) \Rightarrow (T \vee (\neg R)))$$

és vertadera. Ara bé, per la definició d'implicació (1.1.5) això ho podem escriure com

$$(S \Rightarrow T) \Rightarrow ((R \Rightarrow S) \Rightarrow (R \Rightarrow T))$$

i com que, per hipòtesi, la relació $S \Rightarrow T$ és vertadera per l'axioma 1.1.11 tenim que la relació $(R \Rightarrow S) \Rightarrow (R \Rightarrow T)$ és vertadera, i com que, de nou per hipòtesi, tenim que la relació $R \Rightarrow S$ és vertadera tenim per l'axioma 1.1.11 que la relació $R \Rightarrow T$ és vertadera, com volíem veure. □

**Tautologia 1.1.14** (Tercer exclòs)**.** *Sigui $R$ una relació. Aleshores la relació $R \vee (\neg R)$ és vertadera.*

*Demostració.* La relació $R \vee (\neg R)$ és equivalent, per la definició d'implicació (1.1.5), a $R \Rightarrow R$. Per l'axioma 1.1.7 tenim que la relació $(R \vee R) \Rightarrow R$ és vertadera, i per l'axioma 1.1.8 tenim que la relació $R \Rightarrow (R \vee R)$ és vertadera. Per tant, per la tautologia 1.1.13, veiem que $R \Rightarrow R$. □

**Tautologia 1.1.15.** *Siguin $R$ i $S$ dues relacions tals que $R$ sigui vertadera. Aleshores les relacions $R \vee S$ i $S \vee R$ són vertaderes.*

*Demostració.* Per l'axioma 1.1.8 tenim que $R \Rightarrow (R \vee S)$ és vertadera, i per l'axioma 1.1.9 tenim que $(R \vee S) \Rightarrow (S \vee R)$ és vertadera.

Ara bé, per hipòtesi tenim que $R$ és vertadera, i per l'axioma 1.1.11 veiem que les relacions $R \vee S$ i $S \vee R$ són vertaderes. □

**Tautologia 1.1.16.** *Sigui $R$ una relació. Aleshores la relació $R \Leftrightarrow \neg(\neg R)$ és vertadera.*

*Demostració.* Per la definició de doble implicació (1.1.6) hem de veure que la relació

$$(\neg(\neg R) \vee (\neg R)) \wedge (R \vee (\neg(\neg(\neg R))))$$

és vertadera. Ara bé, si $R$ és vertadera trobem per la definició de negació (1.1.2) que $\neg R$ és falsa, i aleshores per la tautologia del tercer exclòs (1.1.14) les relacions $\neg(\neg R) \vee (\neg R)$ i $R \vee (\neg(\neg(\neg R)))$ són vertaderes

Si $R$ és falsa trobem per la definició de negació (1.1.2) que $\neg R$ és vertadera, aleshores, de nou per la tautologia del tercer exclòs (1.1.14), les relacions $\neg(\neg R) \vee (\neg R)$ i $R \vee (\neg(\neg(\neg R)))$ són vertaderes, com volíem veure. □

**Tautologia 1.1.17** (Primera llei de De Morgan)**.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació*

$$\neg(R \vee S) \Leftrightarrow ((\neg R) \wedge (\neg S))$$

*és vertadera.*

*Demostració.* Per la definició de conjunció (1.1.3) volem veure que la relació

$$\neg(R \vee S) \Leftrightarrow \neg((\neg(\neg R)) \vee (\neg(\neg S)))$$

és vertadera. Aleshores, per la tautologia del tercer exclòs (1.1.14) això és equivalent a veure que la relació

$$\neg(R \vee S) \Leftrightarrow \neg(R \vee S)$$

és vertadera, i per l'axioma 1.1.9 hem acabat. □

**Tautologia 1.1.18** (Segona llei de De Morgan)**.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació*

$$\neg(R \wedge S) \Leftrightarrow ((\neg R) \vee (\neg S))$$

*és vertadera.*

*Demostració.* Per la definició de conjunció (1.1.3) hem de veure que la relació

$$((\neg R) \vee (\neg S)) \Leftrightarrow \neg((\neg(\neg R)) \wedge (\neg(\neg S))),$$

i per la tautologia 1.1.16 això és equivalent a veure que la relació

$$((\neg R) \vee (\neg S)) \Leftrightarrow \neg(R \wedge S),$$

que és conseqüència de la llei de De Morgan (1.1.17). □

**Tautologia 1.1.19** (Llei de les contrarecíproques)**.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació*

$$(R \Rightarrow S) \Leftrightarrow ((\neg S) \Rightarrow (\neg R))$$

*és vertadera.*

*Demostració.* Per la definició d'implicació (1.1.5) hem de veure que la relació

$$(S \vee (\neg R)) \Leftrightarrow ((\neg R) \vee (\neg(\neg S)))$$

és vertadera. Ara bé, per la tautologia 1.1.16 tenim que això és equivalent a veure que la relació

$$(S \vee (\neg R)) \Leftrightarrow ((\neg R) \vee S)$$

és vertadera, i pels axiomes 1.1.9 i 1.1.10 i la definició de doble implicació (1.1.6) tenim que aquesta relació és vertadera, com volíem veure. □

**Tautologia 1.1.20.** *Siguin $R$ i $S$ dues relacions. Aleshores la relació $R \wedge S$ és vertadera si i només si $R$ és vertadera i $S$ és vertadera.*

*Demostració.* Veiem primer l'implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $R$ i $S$ són vertaderes. Per l'axioma 1.1.8 la relació $S \vee (\neg R)$ és vertadera i, per la definició de implicació (1.1.5) tenim que $R \Rightarrow S$ és vertadera. Ara bé, per la tautologia de la llei de les contrarecíproques (1.1.19) tenim que la relació $(\neg S) \Rightarrow (\neg R)$ és vertadera, i pels axiomes 1.1.10 i 1.1.7 tenim que la relació

$$((\neg S) \vee (\neg R)) \Rightarrow (\neg R)$$

és vertadera, i de nou per la tautologia de la llei de les contrarecíproques (1.1.19) trobem que la relació

$$(\neg(\neg R)) \Rightarrow (\neg(\neg S) \vee (\neg R))$$

és vertadera, i per la tautologia 1.1.16 trobem que la relació

$$R \Rightarrow (\neg((\neg S) \vee (\neg R)))$$

és vertadera, i per la definició de conjunció (1.1.3) això és equivalent a que la relació

$$R \Rightarrow (R \wedge S)$$

és vertadera, i per tant per l'axioma 1.1.11 trobem que $R \wedge S$ és vertadera, com volíem veure.

Veiem ara l'implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que la relació $R \wedge S$ és vertadera. Per la tautologia de la llei de les contrarecíproques (1.1.19) tenim que la relació $(R \wedge S) \Rightarrow S$ és vertadera si i només si la relació

$$(\neg R) \Rightarrow (\neg(\neg((\neg R) \vee (\neg S))))$$

és vertadera. Ara bé, per la tautologia 1.1.16 tenim que això és equivalent a veure que la relació

$$(\neg R) \Rightarrow ((\neg R) \vee (\neg S))$$

és vertadera, que és conseqüència de l'axioma 1.1.8, i per tant la relació $(R \wedge S) \Rightarrow R$ és vertadera. La demostració del cas $(R \wedge S) \Rightarrow S$ és anàloga. □

**Tautologia 1.1.21.** *Siguin $R$ i $S$ dues relacions tals que $R$ sigui falsa i $R \vee S$ sigui vertadera. Aleshores la relació $S$ és vertadera.*

*Demostració.* Per la tautologia 1.1.16 tenim que la relació $R \Rightarrow (\neg(\neg R))$ és vertadera, i per l'axioma 1.1.10 això és que la relació

$$(R \vee S) \Leftrightarrow (\neg(\neg R) \vee S)$$

és vertadera. Ara bé, per la definició d'implicació (1.1.5) tenim que això és equivalent a la relació

$$(R \vee S) \Leftrightarrow ((\neg R) \Rightarrow S).$$

I com que, per hipòtesi, $R \vee S$ i $\neg R$ són vertaderes, tenim que $S$ és vertadera, com volíem veure. □

**Tautologia 1.1.22.** *Siguin $R$ i $S$ dues relacions tals que $S$ sigui falsa i $R \veebar S$ sigui vertadera. Aleshores $R$ és vertadera.*

*Demostració.* Tenim, per la definició de disjunció excloent (1.1.4), que la relació

$$(R \wedge (\neg S)) \vee ((\neg R) \wedge S)$$

és vertadera. Ara bé, com per hipòtesi $S$ és falsa per la tautologia 1.1.21 tenim que la relació $(\vee R) \wedge S$ és falsa. Per tant per la tautologia 1.1.20 tenim que la relació $R \wedge (\neg S)$ és vertadera, i per la tautologia 1.1.20 tenim que $R$ és vertadera. □

**Tautologia 1.1.23.** *Siguin $R$ i $S$ dues relacions tals que $R$ i $R \veebar S$ siguin vertaderes. Aleshores $S$ és falsa.*

*Demostració.* Tenim, per la definició de disjunció excloent (1.1.4), que la relació

$$(R \wedge (\neg S)) \vee ((\neg R) \wedge S)$$

és vertadera. Com per hipòtesi la relació $R$ és vertadera, per la definició de negació (1.1.2) tenim que $\neg R$ és falsa. I per la tautologia 1.1.20 tenim que la relació $(\neg R) \wedge S$ és falsa, i per la tautologia 1.1.21 tenim que la relació $R \wedge (\neg S)$ és vertadera.

Ara bé, de nou per la tautologia 1.1.20, tenim que la relació $\neg S$ ha de ser vertadera, i per la definició de negació (1.1.2) trobem que $S$ és falsa. □

# Capítol 2

# Teoria de conjunts

## 2.1 Conjunts

### 2.1.1 Elements i subconjunts

Igual que en la secció anterior, només farem una introducció informal a la teoria de conjunts.

Definirem *conjunt* com un objecte matemàtic, i entre conjunts la relació $\in$ de pertinència. Interpretem la relació $x \in A$ com que $x$ és un *element* de $A$ o que $x$ pertany a $A$. Si la relació $x \in A$ és falsa aleshores ho denotarem com $x \notin A$ i direm que $x$ no pertany a $A$.

**Axioma 2.1.1** (Axioma d'Extensionalitat)**.** *Siguin $A$ i $B$ dos conjunts tals que per a tot $x$ tenim $x \in A$ si i només si $x \in B$. Aleshores $A = B$.*

**Definició 2.1.2** (Subconjunt)**.** Siguin $A$ i $B$ dos conjunts tals que per a tot $x \in B$ tenim $x \in A$. Aleshores direm que $B$ és un subconjunt de $A$ i ho denotarem $B \subseteq A$.

**Teorema 2.1.3** (Doble inclusió)**.** *Siguin $A$ i $B$ dos conjunts. Aleshores $A = B$ si i només si $A \subseteq B$ i $B \subseteq A$.*

*Demostració.* Comencem veient que la condició és necessària ($\Rightarrow$). Suposem doncs que $A \subseteq B$ i $B \subseteq A$. Per la definició de subconjunt (2.1.2) tenim que si $x \in A$ aleshores $x \in B$, ja que per hipòtesi $A \subset B$. De mateixa manera tenim que si $x \in B$ aleshores $x \in A$, ja que per hipòtesi $B \subseteq A$. Per tant, per l'axioma d'extensionalitat (2.1.1) tenim que $A = B$.

Veiem ara que la condició és suficient ($\Leftarrow$). Suposem doncs que $A = B$. Tenim que si $x \in A$, aleshores $x \in B$, i per la definició de subconjunt (2.1.2) això és que $A \subseteq B$. De mateixa manera, si $x \in B$ tenim $x \in A$, i de nou per la definició de subconjunt (2.1.2) tenim que $B \subseteq A$, com volíem veure. □

**Axioma 2.1.4** (Axioma del Conjunt Potència)**.** *Sigui $A$ un conjunt. Aleshores existeix un conjunt $\mathcal{P}(A)$ tal que $B \subseteq A$ si i només si $B \in \mathcal{P}(A)$.*

**Notació 2.1.5.** Denotarem els conjunts com claus separant els seus elements amb comes. Per exemple, si tinguéssim un conjunt $X$ que conté únicament els elements $a$, $b$ i $c$ el podríem denotar com

$$X = \{a, b, c\}.$$

Si tots els elements de $X$ satisfan una relació $R$ denotarem

$$X = \{x \mid x \text{ satisfà } R\}.$$

**Axioma 2.1.6** (Axioma de Separació)**.** *Siguin $A$ un conjunt i $R$ una relació. Aleshores el conjunt $\{x \mid (x \in A) \wedge (x \text{ satisfà } R)\}$ existeix.*

**Proposició 2.1.7.** *Existeix un únic conjunt sense elements.*

*Demostració.* Considerem un conjunt $A$. Aleshores, per l'axioma de separació (2.1.6) tenim que existeix un conjunt

$$X = \{x \mid (x \in A) \wedge (x \notin A)\},$$

i per la tautologia 1.1.20 tenim que la relació $(x \in A) \wedge (x \notin A)$ és falsa. Per tant el conjunt $X$ no té elements.

La unicitat la tenim per l'axioma axioma d'extensionalitat (2.1.1). □

**Definició 2.1.8** (Conjunt buit)**.** Direm que el conjunt que no té elements és el conjunt buit, i el denotarem com $\emptyset$.

Aquesta definició té sentit per la proposició 2.1.7.

**Axioma 2.1.9** (Axioma de Regularitat)**.** *Sigui $A$ un conjunt. Aleshores tenim que $\emptyset \subseteq A$.*

### 2.1.2 Unió i intersecció de conjunts

**Axioma 2.1.10** (Axioma d'Infinitud)**.** *Existeix un conjunt infinit.*

**Axioma 2.1.11** (Axioma de la Unió)**.** *Sigui $\{A_i\}_{i \in I}$ és una família de conjunts. Aleshores el conjunt $\{x \mid x \in A_i \text{ per a cert } i \in I\}$ existeix.*

**Definició 2.1.12** (Unió de conjunts)**.** Siguin $A$ i $B$ dos conjunts. Aleshores direm que el conjunt

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$$

és la unió de $A$ i $B$.

Aquesta definició té sentit per l'axioma de la unió (2.1.11).

**Definició 2.1.13** (Intersecció de conjunts)**.** Siguin $A$ i $B$ dos conjunts. Aleshores direm que el conjunt

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$$

és la intersecció de $A$ i $B$.

Aquesta definició té sentit per l'axioma de separació (2.1.6).

**Notació 2.1.14.** Si $\{A_i\}_{i \in I}$ és una família de conjunts, denotarem la unió de tots aquests com

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ per a cert } i \in I\}.$$

Denotem la intersecció de tots aquests com

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ per a tot } i \in I\}.$$

## 2.2 Aplicacions entre conjunts

### 2.2.1 Aplicacions

**Axioma 2.2.1** (Axioma del Parell)**.** *Per a qualsevol parella d'elements $a, b$ existeix un conjunt $\{a, b\}$ que conté únicament $a$ i $b$.*

**Definició 2.2.2** (Parelles ordenades)**.** Siguin $a$ i $b$ dos elements. Aleshores direm que $(a, b) = \{a, \{a, b\}\}$ és una parella ordenada.

Aquesta definició té sentit per l'axioma del parell (2.2.1).

**Proposició 2.2.3.** *Siguin $(a, b)$ i $(c, d)$ dues parelles ordenades. Aleshores $(a, b) = (c, d)$ si i només si $a = c$ i $b = d$.*

*Demostració.* Suposem que $a = c$ i $b = d$. Aleshores tenim que $a \in \{c, \{c, d\}\}$, $\{a, b\} \in \{c, \{c, d\}\}$, $c \in \{a, \{a, b\}\}$ i $\{c, d\} \in \{a, \{a, b\}\}$, i per tant, per la definició de subconjunt (2.1.2) tenim que $\{c, \{c, d\}\} \subseteq \{a, \{a, b\}\}$ i $\{a, \{a, b\}\} \in \{c, \{c, d\}\}$, i pel Teorema de la doble inclusió (2.1.3) tenim que això és si i només si $\{a, \{a, b\}\} = \{c, \{c, d\}\}$, i per la definició de parelles ordenades (2.2.2) trobem que $(a, b) = (c, d)$. □

**Definició 2.2.4** (Producte cartesià de conjunts)**.** Siguin $A$ i $B$ dos conjunts. Aleshores definim el conjunt

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

com el producte cartesià de $A$ i $B$.

**Definició 2.2.5** (Aplicació)**.** Siguin $A$ i $B$ dos conjunts i $f$ un subconjunt de $A \times B$ tal que si $(a, b)$ i $(a, b')$ són elements de $f$, aleshores $b = b'$. Aleshores direm que $f$ és una aplicació de $A$ sobre $B$ i escriurem $b = f(a)$. També denotarem $f\colon A \longrightarrow B$ i

$$\begin{aligned} f\colon A &\longrightarrow B \\ a &\longmapsto b \end{aligned}$$

**Axioma 2.2.6** (Axioma de Reemplaçament)**.** *Siguin $A$ i $B$ dos conjunts i $f$ una aplicació de $A$ sobre $B$. Aleshores el conjunt $\{f(x) \in B \mid x \in A\}$ existeix.*

### 2.2.2 Tipus d'aplicacions

**Definició 2.2.7** (Aplicació injectiva)**.** Sigui $f\colon X \longrightarrow Y$ una aplicació tal que per a tot $a$, $a'$ elements de $X$ satisfent $f(a) = f(a')$ tenim $a = a'$. Aleshores direm que $f$ és injectiva.

**Definició 2.2.8** (Aplicació exhaustiva)**.** Sigui $f\colon X \longrightarrow Y$ una aplicació tal que per a tot $b \in Y$ existeix $a \in A$ satisfent $f(a) = b$. Aleshores direm que $f$ és exhaustiva.

**Definició 2.2.9** (Aplicació bijectiva)**.** Sigui $f\colon X \longrightarrow Y$ una aplicació injectiva i exhaustiva. Aleshores direm que $f$ és bijectiva.

### 2.2.3 Conjugació d'aplicacions

**Proposició 2.2.10.** *Siguin $f\colon A \to B$ i $g\colon B \to C$ dues aplicacions. Aleshores $h(a) = g(f(a))$ per a tot $a \in A$ és una aplicació de $A$ en $C$.*

*Demostració.* Per la definició d'aplicació (2.2.5) hem de veure que $h$ està ben definida. És a dir, que si prenem dos elements $a$ i $a'$ de $A$ tals que $a = a'$, aleshores $h(a) = h(a')$.

Siguin doncs $a$ i $a'$ dos elements de $A$ tals que $a = a'$. Com que, per hipòtesi, $f$ és una aplicació tenim per la definició d'aplicació (2.2.5) que $f(a) = f(a') = b$, per a cert $b \in B$, i per tant, com que per hipòtesi $g$ és una aplicació, trobem $g(f(a)) = g(b) = c$ i $g(f(a')) = g(b) = c$ per a cert $c \in C$, i per tant $h(a) = h(a')$, com volíem veure.

També tenim que $f \subseteq A \times C$, ja que si $c = h(a)$ tenim $c = g(f(a))$, i per la definició d'aplicació (2.2.5) tenim que $a \in A$ i $c \in C$. Per tant, per la definició de subconjunt (2.1.2) tenim que $h$ és una aplicació. □

**Definició 2.2.11** (Conjugació d'aplicacions)**.** Siguin $f\colon A \to B$ i $g\colon B \to C$ dues aplicacions. Aleshores direm que l'aplicació $g(f)$ és la composició de $g$ amb $f$ i ho denotarem com

$$\begin{aligned} g \circ f\colon A &\longrightarrow C \\ a &\longmapsto g(f(a)). \end{aligned}$$

Aquesta definició té sentit per la proposició 2.2.10.

**Proposició 2.2.12.** *Siguin $f\colon A \to B$, $g\colon B \to C$ i $h\colon C \to D$ aplicacions. Aleshores*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

*Demostració.* Hem de veure que per a tot $a \in A$ tenim $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$. Ara bé, tenim que

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

i

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))).$$

Per tant, per la definició d'aplicació (2.2.5) tenim que $(h \circ g) \circ f = h \circ (g \circ f)$. □

**Teorema 2.2.13.** *Siguin $f\colon A \to B$ i $g\colon B \to C$ dues aplicacions injectives. Aleshores l'aplicació $g \circ f$ és injectiva.*

*Demostració.* Prenem $a$ i $a'$ dos elements de $A$ tals que $(g \circ f)(a) = (g \circ f)(a')$. Aleshores tenim $g(f(a)) = g(f(a'))$, i per la definició d'aplicació injectiva (2.2.7) com que, per hipòtesi $g$ i és injectiva tenim que $f(a) = f(a')$, i com que, per hipòtesi, $f$ és injectiva, tenim que $a = a'$, i de nou per la definició d'aplicació injectiva (2.2.7) tenim que $g \circ f$ és injectiva. □

**Teorema 2.2.14.** *Siguin $f\colon A \to B$ i $g\colon B \to C$ dues aplicacions exhaustives. Aleshores l'aplicació $g \circ f$ és exhaustiva.*

*Demostració.* Prenem un element $c \in C$. Aleshores per la definició de aplicació exhaustiva (2.2.8) tenim que existeixen $a \in A$ i $b \in B$ tals que $b = f(a)$ i $c = g(b)$. Per tant per la definició de aplicació exhaustiva (2.2.8) tenim que $g \circ f$ és una aplicació exhaustiva, ja que per a tot $c \in C$ existeix $a \in A$ tal que $(g \circ f)(a) = c$. □

**Teorema 2.2.15.** *Siguin $f\colon A \to B$ i $g\colon B \to C$ dues aplicacions bijectiva. Aleshores l'aplicació $g \circ f$ és bijectiva.*

*Demostració.* Per la definició d'aplicació bijectiva (2.2.9) hem de veure que $g \circ f$ és injectiva i exhaustiva. Ara bé, per hipòtesi tenim que $f$ i $g$ són bijectives, i de nou per la definició d'aplicació bijectiva (2.2.9) tenim que $f$ i $g$ són ambdues injectives i exhaustives. Per tant, pel Teorema 2.2.13 tenim que $g \circ f$ és injectiva, i pel Teorema 2.2.14 tenim que $g \circ f$ és exhaustiva, com volíem veure. □

### 2.2.4 Aplicacions invertibles

**Definició 2.2.16** (Aplicació invertible)**.** Siguin $f\colon A \to B$ i $g\colon B \to A$ dues aplicacions tals que per a tot $a \in A$ i $b \in B$ es compleix

$$(f \circ g)(a) = a \quad \text{i} \quad (g \circ f)(b) = b.$$

Aleshores direm que $f$ és la inversa de $g$ i que $f$ és una aplicació invertible o que $f$ té inversa.

**Teorema 2.2.17.** *Siguin $f\colon A \to B$ una aplicació invertible i $g_1\colon B \to A$ i $g_2\colon B \to A$ dues inverses de $f$. Aleshores $g_1 = g_2$.*

*Demostració.* Per la definició de aplicació invertible (2.2.16) tenim que per a tot $a \in A$, $b \in B$

$$(g_1 \circ f)(a) = a \quad \text{i} \quad (f \circ g_2)(b) = b.$$

Ara bé, tenim

$$((g_1 \circ f) \circ g_2)(b) = g_2(b) \quad \text{i} \quad (g_1 \circ (f \circ g_2))(b) = g_1(b)$$

i per la proposició 2.2.12 trobem que $g_1 = g_2$, com volíem veure. □

**Notació 2.2.18.** Aprofitant el Teorema 2.2.17 denotarem l'inversa d'una aplicació $f : A \to B$ amb $f^{-1}$, i per tant definim l'aplicació

$$f^{-1} \circ f = \mathrm{Id}_A\,.$$

Aleshores tenim que $Id_A\colon A \to A$ és l'aplicació bijectiva i satisfà $Id_A(a) = a$ per a tot $a \in A$.

També denotarem la conjugació d'una aplicació $g\colon A \to A$ amb sí mateixa $k$ de vegades com

$$g^k = g \circ \overset{k)}{\cdots} \circ g.$$

**Teorema 2.2.19.** *Sigui $f\colon A \to B$ una funció. Aleshores $f$ és bijectiva si i només si $f$ és invertible.*

*Demostració.* Comencem veient que la condició és necessària ($\Rightarrow$). Suposem doncs que $f$ és una aplicació bijectiva. Per la definició d'aplicació bijectiva (2.2.9) tenim que $f$ és injectiva i exhaustiva. Per tant per la definició d'aplicació injectiva (2.2.7) i la definició d'aplicació exhaustiva (2.2.8) tenim que per a tot $b \in B$ existeix un únic $a \in A$ tal que $b = f(a)$.

Per tant definim l'aplicació $g\colon B \to A$ tal que $g(b) = a$. Ara bé, tenim que per a tot $a \in A$ i $b \in B$

$$(g \circ f)(a) = a \quad \text{i} \quad (f \circ g)(b) = b,$$

i per la definició de aplicació invertible (2.2.16) tenim que $f$ és invertible, com volíem veure.

Comprovem ara que la condició és suficient ($\Leftarrow$). Suposem doncs que $f$ té inversa. Prenem dos elements $a$ i $a'$ de $A$ tals que $f(a) = f(a')$. Ara bé, per la definició de aplicació invertible (2.2.16) tenim que $(f^{-1} \circ f)(a) = a$ i $(f^{-1} \circ f)(a') = a'$ amb $(f^{-1} \circ f)(a) = (f^{-1} \circ f)(a')$, i per tant $a = a'$ i per la definició d'aplicació injectiva (2.2.7) tenim que $f$ és injectiva.

Sigui $b$ un element de $B$ i prenem $a$ de $A$ tal que $f^{-1}(b) = a$. Aleshores trobem

$$b = Id_B(b) = f \circ f^{-1}(b) = f(a),$$

i per la definició d'aplicació exhaustiva (2.2.8) tenim que $f$ és un aplicació exhaustiva, i per la definició d'aplicació bijectiva (2.2.9) trobem que $f$ és bijectiva. □

**Corol·lari 2.2.20.** *Si $f$ és invertible aleshores $f^{-1}$ és invertible i $\left(f^{-1}\right)^{-1} = f$.*

## 2.3 Relacions d'equivalència

### 2.3.1 Relacions d'equivalència

**Definició 2.3.1** (Relació binària)**.** Siguin $X$ un conjunt no buit, $\sim$ un subconjunt de $X \times X$ i $(x, y)$ un element del subconjunt $\sim$. Aleshores direm que els elements $x$ i $y$ estan relacionats i escriurem $x \sim y$. També direm que $\sim$ és una relació binària.

Si $(x', y')$ no és un element de $\sim$ escriurem $x' \nsim y'$.

**Definició 2.3.2** (Relació d'equivalència)**.** Siguin $X$ un conjunt no buit i $\sim$ una relació que satisfà les propietats

1. Reflexiva: Si $x$ és un element de $X$, aleshores $x \sim x$.
2. Simètrica: Si $x, y$ són elements de $X$ tals que $x \sim y$, aleshores $y \sim x$.
3. Transitiva: Si $x, y, z$ són elements de $X$ tals que $x \sim y$ i $y \sim z$, aleshores $x \sim z$.

Aleshores direm que $\sim$ és una relació d'equivalència en $X$.

### 2.3.2 Classes d'equivalència i conjunt quocient

**Definició 2.3.3** (Classe d'equivalència)**.** Siguin $X$ un conjunt no buit, $\sim$ una classe d'equivalència en $X$ i

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

un subconjunt de $X$. Aleshores direm que $[x]$ és la classe d'equivalència de $x$.

També denotarem $[x] = \overline{x}$.

**Proposició 2.3.4.** *Siguin $X$ un conjunt no buit i $x, y$ elements de $X$. Aleshores o bé $[x] = [y]$ o bé $[x] \cap [y] = \emptyset$.*

*Demostració.* Denotarem la relació d'equivalència amb $\sim$.

Suposem que $x \sim y$. Tenim que $[x] \subseteq [y]$, ja que si prenem $z \in X$ tal que $z \in [x]$. Aleshores per la definició de classe d'equivalència (2.3.3) tenim que $x \sim z$. Per hipòtesi tenim que $x \sim y$, i per tant, per la definició de relació d'equivalència (2.3.2) tenim que $y \sim z$, i per la definició de classe d'equivalència (2.3.3) trobem $z \in [y]$. Per tant, per la definició de subconjunt (2.1.2) tenim que $[x] \subseteq [y]$.

Ara bé, també tenim que $[y] \subseteq [x]$, ja que si prenem $z \in X$ tal que $z \in [y]$. Aleshores per la definició de classe d'equivalència (2.3.3) tenim que $y \sim z$. Per hipòtesi tenim que $x \sim y$, i per tant, per la definició de relació d'equivalència (2.3.2) tenim que $z \sim z$, i per la definició de classe d'equivalència (2.3.3) trobem $z \in [x]$. Per tant, per la definició de subconjunt (2.1.2) tenim que $[y] \subseteq [z]$. Per tant, pel Teorema de la doble inclusió (2.1.3) tenim que $[x] = [y]$.

Suposem ara que $x \nsim y$ i prenem un element $z \in [x] \cap [y]$. Aleshores, per la definició de classe d'equivalència (2.3.3) tenim que $z \sim x$ i $y \sim z$, i per la definició de relació d'equivalència (2.3.2) tenim que $x \sim y$. Ara bé, havíem suposat que $x \nsim y$. Per tant $z$ no pot existir i trobem $[x] \cap [y] = \emptyset$. □

**Definició 2.3.5** (Conjunt quocient)**.** Siguin $X$ un conjunt no buit i $\sim$ una relació d'equivalència en $X$. Aleshores definim el conjunt

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

com el conjunt quocient de $X$ per $\sim$.

# Capítol 3

# Conjunts amb operacions i els nombres

## 3.1 Els nombres naturals

### 3.1.1 Axiomes de Peano

**Definició 3.1.1** (Nombres naturals)**.** Siguin $\mathbb{N}$ un conjunt i $S$ una aplicació que satisfan

1. $1 \in \mathbb{N}$.
2. Si $n \in \mathbb{N}$, aleshores $S(n) \in \mathbb{N}$.
3. Si $n \in \mathbb{N}$, aleshores $S(n) \neq 1$.
4. Si $n, m \in \mathbb{N}$ amb $S(n) = S(m)$, aleshores $n = m$.
5. Si $\mathbb{M}$ és un conjunt tal que $1 \in \mathbb{M}$ i tal que $S(m) \in \mathbb{M}$ per a tot $m \in \mathbb{M}$, aleshores $\mathbb{N} \subseteq \mathbb{M}$.

Aleshores direm que $\mathbb{N}$ és el conjunt dels nombres naturals, i anomenarem els elements de $\mathbb{N}$ nombres naturals.

**Notació 3.1.2.** Denotarem $S(1) = 2$, $S(2) = 3$, $S(3) = 4$, etc. Per tant

$$\mathbb{N} = \{1, 2, 3, 4 \dots\}$$

**Lemma 3.1.3.** $\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$.

*Demostració.* Ho farem pel principi de doble inclusió. Per la definició de nombres naturals (3.1.1) tenim que si $n \in \mathbb{N}$, aleshores $S(n) \in \mathbb{N}$. Per tant trobem que $\mathbb{N} \supseteq \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$.

Tenim també, per la definició de nombres naturals (3.1.1), que si $\mathbb{M}$ és un conjunt tal que $1 \in \mathbb{M}$ i tal que $S(m) \in \mathbb{M}$ per a tot $m \in \mathbb{M}$, aleshores $\mathbb{N} \subseteq \mathbb{M}$, i per tant $\mathbb{N} \subseteq \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$, i pel Teorema de la doble inclusió (2.1.3) tenim que $\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$, com volíem veure. □

**Notació 3.1.4.** Denotarem l'acció d'aplicar l'aplicació $S$ a l'element 1 un nombre natural $k$ de vegades com $S^k(1)$.

**Teorema 3.1.5** (Teorema del primer element)**.** *Sigui $A$ un subconjunt no buit de $\mathbb{N}$. Aleshores existeix $a \in A$ tal que no existeixi cap $b \in A$ satisfent $S(b) = a$.*

*Demostració.* Sigui $a$ un element de $A$. Aleshores pel lemma 3.1.3 tenim que $a = S^k(1)$ per a cert $k \in \mathbb{N}$. Si $1 \in A$ hem acabat per la definició de nombres naturals (3.1.1). Suposem doncs que $1 \notin A$. Si $S(1) \in A$ també hem vist el que volíem. Podem iterar aquest procés un màxim de $k$ vegades, ja que $S^k(1)$ és, per hipòtesi, un nombre natural, i per tant seria $a$ un element de $A$ tal que no existeix $b$ satisfent $S(b) = a$. □

**Definició 3.1.6** (Primer element)**.** Sigui $A$ un subconjunt no buit de $\mathbb{N}$ i $a$ un element de $A$ tal que no existeix cap $b \in A$ satisfent $S(b) = a$. Aleshores direm que $a$ és el primer element de $A$.

Aquesta definició té sentit per la definició de nombres naturals (3.1.1) i el Teorema Teorema del primer element (3.1.5).

**Teorema 3.1.7** (Principi d'inducció)**.** *Sigui $R(n)$ una relació depenent d'un paràmetre $n \in \mathbb{N}$ tal que*

1. *$R(1)$ és vertadera.*
2. *Si $R(n)$ és vertadera aleshores $R(S(n))$ és vertadera.*

*Aleshores $R(n)$ és vertadera per a tot $n \in \mathbb{N}$.*

*Demostració.* Definim el conjunt

$$A = \{n \in \mathbb{N} \mid R(n) \text{ és falsa}\}.$$

Per la definició de subconjunt (2.1.2) tenim que $A \subseteq \mathbb{N}$. Suposem que $A$ és un conjunt no buit. Aleshores pel Teorema del primer element (3.1.5) tenim que existeix un primer element $a$ de $A$. Ara bé, pel punt principi d'inducció (1) tenim que $a \neq 1$. Per tant, pel lemma 3.1.3 tenim que $a = S(b)$ per a cert $b \in \mathbb{N}$. Ara bé, com que $a$ és el primer element de $A$, per la definició de primer element (3.1.6) tenim que $b \notin A$, i per tant $P(b)$ és vertadera. Ara bé, pel punt principi d'inducció (2) tenim que $P(S(b)) = P(a)$ és vertadera, i per tant $a \notin A$, arribant a contradicció. Per tant trobem que $A$ és el conjunt buit, i trobem que $R(n)$ és vertadera per a tot $n \in \mathbb{N}$, com volíem veure. □

### 3.1.2 Operacions sobre els nombres naturals

**Definició 3.1.8** (Suma de nombres naturals)**.** Definim la suma de nombres naturals com una operació $+$ que satisfà per a tot $n, k \in \mathbb{N}$

$$n + 1 = S(n) \quad \text{i} \quad n + S(k) = S(n + k).$$

**Definició 3.1.9** (Producte de nombres naturals)**.** Definim el producte de nombres naturals com una operació $\cdot$ que satisfà per a tot $n, k \in \mathbb{N}$

$$n \cdot 1 = n \quad \text{i} \quad n \cdot S(k) = n \cdot k + n.$$

Denotarem $n \cdot k = nk$ per a tot $n, k \in \mathbb{N}$.

**Proposició 3.1.10.** *Siguin $x, y, z$ tres nombres naturals. Aleshores*

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

*Demostració.* Definim el conjunt

$$A = \{z \in \mathbb{N} \mid (x + y) + z = x + (y + z) \text{ per a tot } x, y \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que per a tot $x, y \in \mathbb{N}$ tenim

$$\begin{aligned} x + (y + 1) &= x + S(y) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(x + y) && \text{(suma de nombres naturals (3.1.8))} \\ &= (x + y) + 1. && \text{(suma de nombres naturals (3.1.8))} \end{aligned}$$

També tenim que si $z \in A$, aleshores $S(z) \in A$. Efectivament, tenim per a tot $x, y \in \mathbb{N}$

$$\begin{aligned} x + (y + S(z)) &= x + S(y + z) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(x + (y + z)) && \text{(suma de nombres naturals (3.1.8))} \\ &= S((x + y) + z) && \text{(Per hipòtesi)} \\ &= (x + y) + S(z). && \text{(suma de nombres naturals (3.1.8))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(z) \in A$ per a tot $z \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Proposició 3.1.11.** *Siguin $x, y$ dos nombres naturals. Aleshores*

$$x + S(y) = S(x) + y.$$

*Demostració.* Definim el conjunt

$$A = \{y \in \mathbb{N} \mid x + S(y) = S(x) + y \text{ per a tot } x \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que per a tot $x \in \mathbb{N}$

$$\begin{aligned} x + S(1) &= S(x + 1) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(S(x)) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(x) + 1. && \text{(suma de nombres naturals (3.1.8))} \end{aligned}$$

També tenim que si $y \in A$, aleshores $S(y) \in A$. Efectivament, tenim que per a tot $x \in \mathbb{N}$

$$\begin{aligned} x + S(S(y)) &= S(x + S(y)) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(S(x) + y) && \text{(Per hipòtesi)} \\ &= S(x) + S(y). && \text{(suma de nombres naturals (3.1.8))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(y) \in A$ per a tot $y \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Proposició 3.1.12.** *Siguin $x, y$ dos nombres naturals. Aleshores*

$$x + y = y + x.$$

*Demostració.* Definim el conjunt

$$B = \{y \in \mathbb{N} \mid 1 + y = y + 1\}.$$

Per la definició de subconjunt (2.1.2) trobem que $B \subseteq \mathbb{N}$.

Tenim que $1 \in B$, ja que $1+1 = 1+1$. També tenim que si $y \in B$, aleshores $S(y) \in B$. Efectivament,

$$\begin{aligned} S(y) + 1 &= y + S(1) && \text{(Proposició 3.1.11)} \\ &= S(y + 1) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(1 + y) && \text{(Per hipòtesi)} \\ &= 1 + S(y). && \text{(suma de nombres naturals (3.1.8))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $B$ és un conjunt tal que $1 \in B$ i tal que $S(y) \in B$ per a tot $y \in B$, aleshores $\mathbb{N} \subseteq B$, i pel Teorema de la doble inclusió (2.1.3) tenim que $\mathbb{N} = B$.

Definim ara el conjunt

$$A = \{y \in \mathbb{N} \mid x + y = y + x \text{ per a tot } x \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $B \subseteq A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que $1 \in B \subseteq A$. També tenim que si $y \in A$, aleshores $S(y) \in A$. Efectivament, tenim que per a tot $x \in \mathbb{N}$

$$\begin{aligned} x + S(y) &= S(x + y) && \text{(suma de nombres naturals (3.1.8))} \\ &= S(y + x) && \text{(Per hipòtesi)} \\ &= y + S(x). && \text{(suma de nombres naturals (3.1.8))} \\ &= S(y) + x. && \text{(Proposició 3.1.11)} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(y) \in A$ per a tot $y \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Proposició 3.1.13.** *Siguin $x, y, z$ tres nombres naturals. Aleshores*

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

*Demostració.* Definim el conjunt

$$A = \{z \in \mathbb{N} \mid x \cdot (y + z) = x \cdot y + x \cdot z \text{ per a tot } x, y \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que per a tot $x, y \in \mathbb{N}$ tenim

$$\begin{aligned} x \cdot (y + 1) &= x \cdot S(y) && \text{(suma de nombres naturals (3.1.8))} \\ &= x \cdot y + x && \text{(producte de nombres naturals (3.1.9))} \\ &= x \cdot y + x \cdot 1. && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

També tenim que si $z \in A$, aleshores $S(z) \in A$. Efectivament, tenim per a tot $x, y \in \mathbb{N}$

$$\begin{aligned} x \cdot (y + S(z)) &= x \cdot S(y + z) && \text{(suma de nombres naturals (3.1.8))} \\ &= x \cdot (y + z) + x && \text{(producte de nombres naturals (3.1.9))} \\ &= (x \cdot y + x \cdot z) + x && \text{(Per hipòtesi)} \\ &= x \cdot y + (x \cdot z + x) && \text{(Proposició 3.1.10)} \\ &= x \cdot y + x \cdot S(z). && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(z) \in A$ per a tot $z \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Proposició 3.1.14.** *Siguin $x, y, z$ tres nombres naturals. Aleshores*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

*Demostració.* Definim el conjunt

$$A = \{z \in \mathbb{N} \mid (x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ per a tot } x, y \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que per a tot $x, y \in \mathbb{N}$ tenim

$$\begin{aligned} x \cdot (y \cdot 1) &= x + y && \text{(producte de nombres naturals (3.1.9))} \\ &= (x \cdot 1) \cdot y. && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

També tenim que si $z \in A$, aleshores $S(z) \in A$. Efectivament, tenim per a tot $x, y \in \mathbb{N}$

$$\begin{aligned} x \cdot (y \cdot S(z)) &= x \cdot (y \cdot z + y) && \text{(producte de nombres naturals (3.1.9))} \\ &= x \cdot (y \cdot z) + x \cdot y && \text{(Proposició 3.1.13)} \\ &= (x \cdot y) \cdot z + x \cdot y && \text{(Per hipòtesi)} \\ &= (x \cdot y) \cdot S(z). && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(z) \in A$ per a tot $z \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Proposició 3.1.15.** *Siguin $x, y$ dos nombres naturals. Aleshores*

$$x \cdot y = y \cdot x.$$

*Demostració.* Definim el conjunt

$$B = \{y \in \mathbb{N} \mid 1 \cdot y = y \cdot 1\}.$$

Per la definició de subconjunt (2.1.2) trobem que $B \subseteq \mathbb{N}$.

Tenim que $1 \in B$, ja que $1 \cdot 1 = 1 \cdot 1$. També tenim que si $x \in B$, aleshores $S(x) \in B$. Efectivament,

$$\begin{aligned} S(x) \cdot 1 &= (x+1) \cdot 1 && \text{(suma de nombres naturals (3.1.8))} \\ &= x \cdot 1 + 1 \cdot 1 && \text{(producte de nombres naturals (3.1.9))} \\ &= x \cdot 1 + 1 && \text{(producte de nombres naturals (3.1.9))} \\ &= 1 \cdot x + 1 && \text{(Per hipòtesi)} \\ &= 1 \cdot S(x). && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $B$ és un conjunt tal que $1 \in B$ i tal que $S(y) \in B$ per a tot $y \in B$, aleshores $\mathbb{N} \subseteq B$, i pel Teorema de la doble inclusió (2.1.3) tenim que $\mathbb{N} = B$.

Definim ara el conjunt

$$A = \{y \in \mathbb{N} \mid x + y = y + x \text{ per a tot } x \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $B \subseteq A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que $1 \in B \subseteq A$. També tenim que si $y \in A$, aleshores $S(y) \in A$. Efectivament, tenim que per a tot $x \in \mathbb{N}$

$$\begin{aligned} x \cdot S(y) &= x \cdot y + x && \text{(producte de nombres naturals (3.1.9))} \\ &= y \cdot x + x && \text{(Per hipòtesi)} \\ &= y \cdot x + x \cdot 1 && \text{(producte de nombres naturals (3.1.9))} \\ &= y \cdot x + 1 \cdot x && (1 \in A) \\ &= (y+1) \cdot x && \text{(Proposició 3.1.13)} \\ &= S(y) \cdot x. && \text{(producte de nombres naturals (3.1.9))} \end{aligned}$$

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(y) \in A$ per a tot $y \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Teorema 3.1.16.** *Siguin $x$, $y$ i $z$ tres nombres naturals tals que $x + z = x + y$. Aleshores $x = y$.*

*Demostració.* Definim el conjunt

$$A = \{z \in \mathbb{N} \mid x + z = y + z \Rightarrow x = y \text{ per a tot } x, y \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que si $x+1 = y+1$ per la definició de suma de nombres naturals (3.1.8) trobem que $S(x) = S(y)$, i per la definició de nombres naturals (3.1.1) trobem que $x = y$. També tenim que si $z \in A$, aleshores $S(z) \in A$. Efectivament, per a tot $x, y \in \mathbb{N}$ tals que $x + S(z) = y + S(z)$ tenim per la definició de suma de nombres naturals (3.1.8) que

$$x + z + 1 = y + z + 1,$$

i per la proposició 3.1.12 tenim que

$$x + 1 + z = y + 1 + z.$$

Per tant, per la definició de suma de nombres naturals (3.1.8), trobem

$$S(x) + z = S(y) + z,$$

i per hipòtesi, $S(x) = S(y)$, i per la definició de nombres naturals (3.1.1) tenim que $x = z$.

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(z) \in A$ per a tot $z \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

**Teorema 3.1.17.** *Siguin $x$, $y$ i $z$ tres nombres naturals tals que $xz = yz$. Aleshores $x = y$.*

*Demostració.* Definim el conjunt

$$A = \{z \in \mathbb{N} \mid xz = yz \Rightarrow x = y \text{ per a tot } x, y \in \mathbb{N}\}.$$

Per la definició de subconjunt (2.1.2) trobem que $A \subseteq \mathbb{N}$.

Tenim que $1 \in A$, ja que si $x \cdot 1 = y \cdot 1$ per la definició de producte de nombres naturals (3.1.9) trobem que $x = y$. També tenim que si $z \in A$, aleshores $S(z) \in A$. Efectivament, per a tot $x, y \in \mathbb{N}$ tals que $x \cdot S(z) = y \cdot S(z)$ tenim per la definició de producte de nombres naturals (3.1.9) que

$$x \cdot z + x \cdot 1 = y \cdot z + y \cdot 1.$$

Ara bé, per hipòtesi tenim que $x \cdot z = y \cdot z$, i pel Teorema 3.1.16 trobem $x = y$.

Ara bé. Per la definició de nombres naturals (3.1.1), tenim que si $A$ és un conjunt tal que $1 \in A$ i tal que $S(z) \in A$ per a tot $z \in A$, aleshores $\mathbb{N} \subseteq A$, i pel Teorema de la doble inclusió (2.1.3) tenim que $A = \mathbb{N}$. □

## 3.2 Els nombres enters

### 3.2.1 Construcció dels nombres enters

**Proposició 3.2.1.** *Sigui $\sim$ una relació binària sobre $A = \mathbb{N} \cup \{0\}$, amb $n + 0 = 0 + n = n$ i $n \cdot 0 = 0 \cdot n = 0$, tal que per a tot $(a, b)$ i $(c, d)$ elements de $A \times A$*

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

*Aleshores $\sim$ és una relació d'equivalència.*

*Demostració.* Comprovem les propietats de la definició de relació d'equivalència:

1. Reflexiva: Sigui $(a, b)$ un element de $A \times A$. Aleshores per la proposició 3.1.12 tenim que $a + b = b + a$, i per tant $(a, b) \sim (a, b)$.

2. Simètrica: Siguin $(a, b)$ i $(c, d)$ elements de $A \times A$ tals que $(a, b) \sim (c, d)$. Aleshores significa que $a + d = b + c$, i per la la proposició 3.1.12 tenim que $c + b = d + a$ i per tant $(c, d) \sim (a, b)$.

3. Transitiva: Siguin $(a,b)$, $(c,d)$ i $(e,f)$ elements de $A \times A$ tals que $(a,b) \sim (c,d)$ i $(c,d) \sim (e,f)$. Això és que

$$a+d=b+c \quad \text{i} \quad c+f=d+e.$$

Ara bé, tenim

$$a+d+f=b+c+f$$

i per tant

$$a+d+f=b+d+e$$

d'on trobem $a+f=b+e$, i per tant $(a,b) \sim (e,f)$.

I per la definició de relació d'equivalència (2.3.2) hem acabat. □

**Definició 3.2.2** (Nombres enters)**.** Sigui $\sim$ una relació d'equivalència sobre $A = \mathbb{N} \cup \{0\}$, amb $n+0=0+n=n$ i $n \cdot 0 = 0 \cdot n = 0$, i $\sim$ una relació d'equivalència tal que per a tot $(a,b)$ i $(c,d)$ elements de $A \times A$

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

Aleshores direm que el conjunt quocient $\mathbb{Z} = A \times A/\sim$ és el conjunt dels nombres enters. També direm que els elements de $\mathbb{Z}$ són nombres enters.

**Definició 3.2.3** (Resta de nombres naturals)**.** Siguin $a$, $b$ i $c$ nombres naturals tals que $a \geq b$ i $a = b+c$. Aleshores escriurem $a-b=c$.

### 3.2.2 Operacions sobre els nombres enters

**Definició 3.2.4** (Suma de nombres enters)**.** Siguin $\overline{(a,b)}$ i $\overline{(c,d)}$ dos nombres enters. Definim la suma de nombres enters com una operació $+$ que satisfà

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$

**Definició 3.2.5** (Producte de nombres enters)**.** Siguin $\overline{(a,b)}$ i $\overline{(c,d)}$ dos nombres enters. Definim el producte de nombres enters com una operació $\cdot$ que satisfà

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}.$$

**Proposició 3.2.6.** *Sigui $\overline{(a,b)}$ un nombre enter. Aleshores*

1. $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$.
2. $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}$.
3. $\overline{(a,b)} + \overline{(b,a)} = \overline{(0,0)}$.

*Demostració.* Comencem veient el punt (1). Per la definició de producte de nombres enters (3.2.5) tenim que

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, 0+b)},$$

i per la proposició 3.1.12 i definició de nombres enters (3.2.2) trobem

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}.$$

Veiem ara el punt (2). Per la definició de producte de nombres enters (3.2.5) tenim que

$$\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)},$$

i per la definició de producte de nombres naturals (3.1.9) i la definició de nombres enters (3.2.2) trobem

$$\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}.$$

Veiem el punt (3). Per la definició de suma de nombres enters (3.2.4) tenim que

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)}.$$

Ara bé, per la proposició 3.1.12 i la definició de nombres enters (3.2.2) tenim que

$$a + b + 0 = b + a + 0$$

i, de nou per la definició de nombres enters (3.2.2), trobem $(a+b, b+a) \sim (0,0)$, i per la definició de classe d'equivalència (2.3.3) tenim que $\overline{(a+b, a+b)} = \overline{(0,0)}$. □

**Proposició 3.2.7.** *Sigui $\overline{(a,b)}$ un nombre enter. Aleshores*

1. *Si $a \geq b$, $\overline{(a,b)} = \overline{(a-b, 0)}$.*
2. *Si $a \leq b$, $\overline{(a,b)} = \overline{(0, b-a)}$.*

*Demostració.* Comencem veient el punt (1). Tenim que

$$a + 0 = a + b - b,$$

ja que $b + 0 = b$, i per tant, per la definició de resta de nombres naturals (3.2.3) tenim que $b - b = 0$. Per tant, per la definició de nombres enters (3.2.2) tenim $(a,b) \sim (a-b, 0)$, i per la definició de classe d'equivalència (2.3.3) trobem que $\overline{(a,b)} = \overline{(a-b,0)}$.

La demostració del punt (2) és anàloga. □

**Notació 3.2.8.** Denotarem $\overline{(a,0)} = a$ i $\overline{(0,a)} = -a$. Per tant

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

**Observació 3.2.9.** $a - b = 0 \iff a = b$.

**Teorema 3.2.10.** *Sigui $\overline{(a,b)}$ un nombre enter. Aleshores*

$$\overline{(a,b)} = \overline{(0,0)} \iff a = b.$$

*Demostració.* Suposem que $\overline{(a,b)} = \overline{(0,0)}$. Per la definició de classe d'equivalència (2.3.3) això és

$$(a,b) \sim (0,0),$$

i per la definició de nombres enters (3.2.2) tenim que això és

$$a + 0 = b + 0$$

i de nou per la definició de nombres enters (3.2.2) això és

$$a = b.$$

□

**Proposició 3.2.11.** *Siguin* $\overline{(a,b)}$ *i* $\overline{(c,d)}$ *nombres enters. Aleshores*

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}.$$

*Demostració.* Per la definició de suma de nombres enters (3.2.4) tenim que

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} &= \overline{(a+d, b+c)} \\
&= \overline{(d+a, c+b)} && (3.1.12) \\
&= \overline{(c,d)} + \overline{(a,b)}, && (\text{suma de nombres enters } (3.2.4))
\end{aligned}$$

com volíem veure. □

**Proposició 3.2.12.** *Siguin* $\overline{(a,b)}$ *i* $\overline{(c,d)}$ *nombres enters. Aleshores*

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(c,d)} \cdot \overline{(a,b)}.$$

*Demostració.* Per la definició de producte de nombres enters (3.2.5) tenim que

$$\begin{aligned}
\overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(ac+bd, ad+bc)} \\
&= \overline{(ca+db, da+cb)} && (3.1.15) \\
&= \overline{(ca+db, cb+da)} && (3.1.12) \\
&= \overline{(c,d)} \cdot \overline{(a,b)}, && (\text{producte de nombres enters } (3.2.5))
\end{aligned}$$

com volíem veure. □

**Proposició 3.2.13.** *Siguin* $\overline{(a,b)}$, $\overline{(c,d)}$ *i* $\overline{(e,f)}$ *nombres enters. Aleshores*

$$\overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right) = \left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)}.$$

*Demostració.* Per la definició de suma de nombres enters (3.2.4) tenim que

$$\begin{aligned}
\overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right) &= \overline{(a,b)} + \overline{(c+f, d+e)} \\
&= \overline{(a+(d+e), b+(c+f))} \\
&= \overline{((a+d)+e, (b+c)+f)} && (3.1.10) \\
&= \overline{(a+d, b+c)} + \overline{(e,f)} \\
&= \left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)},
\end{aligned}$$

com volíem veure. □

**Proposició 3.2.14.** *Siguin* $\overline{(a,b)}$, $\overline{(c,d)}$ *i* $\overline{(e,f)}$ *nombres enters. Aleshores*

$$\overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right) = \left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)}.$$

*Demostració.* Per la definició de producte de nombres enters (3.2.5) tenim que

$$\begin{aligned}
\overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right) &= \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\
&= \overline{(a(ce+df)+b(cf+de), a(cf+de)+b(cf+de))}
\end{aligned}$$

Per la proposició 3.1.13

$$= \overline{(ace + adf + bcf + bde, acf + ade + bcf + bde)}$$

i per la proposició 3.1.15

$$= \overline{(ace + bde + adf + bcf, acf + bdf + ade + bce)}$$

i de nou per la proposició 3.1.13

$$\begin{aligned} &= \overline{((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)} \\ &= \overline{(ac + bd, ad + bc)} \cdot \overline{(e, f)} \\ &= \left(\overline{(a, b)} \cdot \overline{(c, d)}\right) \cdot \overline{(e, f)}, \end{aligned}$$

com volíem veure. □

**Proposició 3.2.15.** *Siguin* $\overline{(a, b)}$, $\overline{(c, d)}$ *i* $\overline{(e, f)}$ *nombres enters. Aleshores*

$$\overline{(a, b)} \cdot \left(\overline{(c, d)} + \overline{(e, f)}\right) = \overline{(a, b)} \cdot \overline{(c, d)} + \overline{(a, b)} \cdot \overline{(e, f)}$$

*i*

$$\left(\overline{(a, b)} + \overline{(c, d)}\right) \cdot \overline{(e, f)} = \overline{(a, b)} \cdot \overline{(e, f)} + \overline{(c, d)} \cdot \overline{(e, f)}.$$

*Demostració.* Per la definició de suma de nombres enters (3.2.4) tenim que

$$\overline{(a, b)} \cdot \left(\overline{(c, d)} + \overline{(e, f)}\right) = \overline{(a, b)} \cdot \overline{(c + e, d + f)}$$

per la definició de producte de nombres enters (3.2.5)

$$= \overline{(a(c + e) + b(d + f), a(d + f) + b(c + e))}$$

per la proposició 3.1.13

$$= \overline{(ac + ae + bd + bf, ad + af + bc + be)}$$

per la proposició 3.1.12

$$= \overline{(ac + bd + ae + bd, ad + bc + af + be)}$$

per la definició de suma de nombres naturals (3.1.8)

$$= \overline{(ac + bd, ad + bc)} + \overline{(ae + bd, af + be)}$$

i per la definició de producte de nombres naturals (3.1.9)

$$= \overline{(a, b)} \cdot \overline{(c, d)} + \overline{(a, b)} \cdot \overline{(e, f)}$$ □

**Teorema 3.2.16.** *Siguin* $\overline{(a, b)}$ *i* $\overline{(c, d)}$ *dos nombres enters tals que* $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(0, 0)}$. *Aleshores* $\overline{(a, b)} = \overline{(0, 0)}$ *ó* $\overline{(c, d)} = \overline{(0, 0)}$.

*Demostració.* Per la definició de producte de nombres enters (3.2.5) tenim que

$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac + bd, ad + bc)}.$$

Com que per hipòtesi $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(0, 0)}$, tenim que per la definició de nombres enters (3.2.2) tenim que

$$ac + bd + 0 = ad + bc + 0,$$

i de nou per la definició de nombres enters (3.2.2) això és

$$ac + bd = ad + bc.$$

Suposem que $\overline{(c,d)} \neq \overline{(0,0)}$. Pel Teorema 3.2.10 trobem que $c \neq d$.

Suposem també que $c > d$. Això és que existeix un natural $k$ satisfent $c + k = d$. Per tant

$$a(d+k) + db = ad + b(d+k)$$

i per la proposició 3.2.15 i la proposició 3.2.11 tenim que

$$ad + db + ak = ad + bd + bk.$$

Ara bé, pel Teorema 3.1.16 i el Teorema 3.1.17 tenim que

$$a = b$$

i per la proposició 3.2.10 trobem que $\overline{(a,b)} = \overline{(0,0)}$.

Les demostracions dels altres casos són anàlogues. □

**Corol·lari 3.2.17.** *Siguin $a$, $b$ i $c$ nombres enters amb $c \neq 0$ tals que*

$$ac = bc.$$

*Aleshores $a = b$.*

*Demostració.* Per la proposició 3.2.15 trobem

$$(a-b)c = 0,$$

aleshores pel Teorema 3.2.16 trobem que ha de ser $a - b = 0$, i per l'observació 3.2.9 tenim $a = b$, com volíem veure. □

### 3.2.3 Divisibilitat dels nombres enters

**Definició 3.2.18** (Divisors i múltiples)**.** Siguin $a$ i $b$ dos nombres enters tal que existeix un nombre enter $c$ satisfent $a = bc$. Aleshores direm que $b$ divideix a $a$ o que $a$ és múltiple de $b$.

**Notació 3.2.19.** Siguin $a$ i $b$ enters tals que $b$ divideix a $a$. Denotarem $b \mid a$.

**Proposició 3.2.20.** *Siguin $a$ i $b$ enters. Aleshores*

1. *$b \mid a$ si i només si $b \mid -a$.*
2. *$b \mid a$ si i només si $-b \mid a$.*

*Demostració.* Comencem veient el punt (1). Si $b \mid a$ per la definició de divisor (3.2.18) tenim que existeix un enter $c$ tal que $a = bc$, i per tant $-a = b(-c)$, i equivalentment $b \mid -a$.

Veiem ara el punt (2). Si $b \mid a$ per la definició de divisor (3.2.18) tenim que existeix un enter $c$ tal que $a = bc$, i per tant $a = (-c)(-b)$, i equivalentment $-b \mid a$. □

**Proposició 3.2.21.** *Siguin $c$, $b$ i $a$ enters tals que $c|a$. Aleshores $c \mid ab$.*

*Demostració.* Si $c \mid a$ per la definició de divisor (3.2.18) tenim que existeix un $k$ tal que $a = kc$. Ara bé, també tenim $ab = kbc$, i per tant $c \mid ab$. □

**Proposició 3.2.22.** *Siguin $a$, $b$ i $c$ enters tals que $c \mid a$ i $c \mid b$. Aleshores $c \mid a+b$ i $c \mid a-b$.*

*Demostració.* Per la definició de divisor (3.2.18) tenim que existeixen enters $k$ i $k'$ tals que $a = kc$ i $c = k'b$. Per tant per la proposició 3.2.15 trobem

$$a + b = (k + k')c \quad \text{i} \quad a - b = (k - k')c. \qquad \square$$

**Proposició 3.2.23.** *Siguin $a$, $b$ i $c$ enters tal que $a \mid b$ i $b \mid c$. Aleshores $a \mid c$.*

*Demostració.* Per la definició de divisor (3.2.18) tenim que existeixen enters $k$ i $k'$ tals que $a = kb$ i $b = k'c$. Per tant $a = kk'c$. $\square$

**Proposició 3.2.24.** *Siguin $a$ i $b$ enters tals que $a \mid b$ i $b \mid a$. Aleshores $a = b$ ó $a = -b$.*

*Demostració.* Per la definició de divisor (3.2.18) tenim que existeixen enters $k$ i $k'$ tals que $a = kb$ i $b = k'a$. Per tant trobem

$$b = kk'b$$

i tenim

$$0 = kk'b - b$$

i per la proposició 3.2.15 trobem

$$0 = (kk' - 1)b.$$

Ara bé, si $b = 0$ tenim que $a = k0$ i $a = 0$, i per tant $a = b$. Si $b \neq 0$ pel Teorema 3.2.16 trobem que ha de ser $kk' = 1$ i per tant ha de ser $k = 1$ i $k' = 1$ ó $k = -1$ i $k' = -1$ i trobem que $a = b$ ó $a = -b$. $\square$

### 3.2.4 Màxim comú divisor

**Definició 3.2.25** (Màxim comú divisor)**.** Siguin $a$ i $b$ enters. Aleshores definim

$$\operatorname{mcd}(a, b) = \max_{c \in \mathbb{Z}} \{c \mid a \text{ i } c \mid b\}$$

com el màxim comú divisor de $a$ i $b$.

**Proposició 3.2.26.** *Siguin $a$ i $b$ enters. Aleshores* $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, a)$.

*Demostració.* Per la definició de màxim comú divisor (3.2.25) tenim que

$$\operatorname{mcd}(a, b) = \max_{c \in \mathbb{Z}} \{c \mid a \text{ i } c \mid b\} \quad \text{i} \quad \operatorname{mcd}(b, a) = \max_{c \in \mathbb{N}} \{c \mid b \text{ i } c \mid a\},$$

i per tant, per la Tautologia 1.1.20 trobem que $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, a)$. $\square$

**Proposició 3.2.27.** *Siguin $a$ i $b$ enters. Aleshores per a tot $\lambda$ enter*

$$\operatorname{mcd}(a, b) = \operatorname{mcd}(a - \lambda b, b) = \operatorname{mcd}(a, b - \lambda a).$$

*Demostració.* Prenem un enter $c$ tal que $c \mid a$ i $c \mid b$. Aleshores per la proposició 3.2.21 tenim que $c$ divideix $-\lambda b$, i per la proposició 3.2.22 trobem que $c \mid a - \lambda b$, i per la definició de màxim comú divisor (3.2.25) tenim que, efectivament, $\operatorname{mcd}(a, b) = \operatorname{mcd}(a - \lambda b, b)$. $\square$

### 3.2.5 La divisió euclidiana i l'identitat de Bézout

**Lemma 3.2.28.** *Siguin $D$ i $d$ nombres enters amb $D, d > 0$. Aleshores existeixen dos únics $q$, $r$ enters tals que*

$$D = dq + r$$

*amb $0 \leq r < d$.*

*Demostració.* Definim el conjunt

$$S = \{x \in \mathbb{Z} \mid x \geq 0 \text{ i existeix } z \in \mathbb{Z} \text{ tal que } x = D - dz\}.$$

Observem que $D \in S$, i per tant $S \neq \emptyset$. Sigui doncs $r = \min\{x \in S\}$. Per tant existeix un enter $q$ tal que

$$r = D - dq.$$

Ara bé, tenim que $r < d$, ja que si $r \geq d$ tindríem

$$\begin{aligned} 0 &\geq r - d \\ &= D - dq - d \\ &= D - d(q+1) \end{aligned} \tag{3.2.15}$$

i per tant $r - d$ seria un element de $S$, amb $r - d < r$, però això entraria amb contradicció amb que $r = \min\{x \in S\}$. Per tant $\leq r < d$ i hem acabat. □

**Teorema 3.2.29** (Criteri de divisibilitat d'Euclides)**.** *Siguin $D$ i $d$ nombres enters amb $d \neq 0$. Aleshores existeixen dos únics $q$, $r$ enters tals que*

$$D = dq + r$$

*amb $0 \leq r < |d|$.*

*Demostració.* Veiem primer que si $q$ i $r$ existeixen aquests són únics. Suposem doncs que existeixen $q_1, q_2, r_1, r_2$ tals que

$$D = dq_1 + r_1 = dq_2 + r_2$$

amb $0 \leq r_1 < |d|$ i $0 \leq r_2 < |d|$. Aleshores tenim

$$D - D = d(q_1 - q_2) + (r_1 - r_2)$$

i per tant

$$r_2 - r_1 = d(q_1 - q_2).$$

Ara bé, tenim que $r_2 - r_1 < |d|$, ja que per hipòtesi $r_1, r_2 < |d|$, i per tant ha de ser $r_2 - r_1 = 0$, i per l'observació 3.2.9 tenim $r_1 = r_2$. Ara bé, aleshores tenim

$$0 = d(q_1 - q_2)$$

i com que, per hipòtesi, $d \neq 0$, pel Teorema 3.2.16 ha de ser $q_1 - q_2 = 0$, i de nou per l'observació 3.2.9 tenim $q_1 = q_2$. Per tant la unicitat queda demostrada.

Veiem ara que existeixen. Efectivament, si $D, d > 0$ l'enunciat és cert pel lemma 3.2.28.

Si $D < 0$ i $d > 0$ definim $D' = -D$. Aleshores $D' > 0$, i pel lemma 3.2.28 tenim que existeixen $q'$ i $r'$ enters tals que

$$D' = dq' + r'$$

amb $0 \leq r' < d$. I per tant

$$\begin{aligned} D &= -(dq' + r') \\ &= d(-q') - r' && (3.2.15) \\ &= d(-q') - d + d - r' \\ &= d(-q' - 1) + (d - r') && (3.2.15) \end{aligned}$$

i si prenem $q = -q' - 1$ i $r = d - r'$ tenim

$$D = dq + r$$

amb $0 \leq d - r' < d$.

Si $d < 0$ prenem $d' = -d$, i aleshores $d' > 0$ i pels casos anteriors hem acabat. □

**Teorema 3.2.30** (Identitat de Bézout)**.** *Siguin $a$ i $b$ dos enters. Aleshores existeixen enters $\alpha$ i $\beta$ tals que*

$$\alpha a + \beta b = \operatorname{mcd}(a, b).$$

*Demostració.* Considerem el conjunt

$$S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Observem que si $x = 1$ i $y = 0$, l'enter $a$ pertany a $S$. Per tant $S$ és un conjunt no buit i tenim que existeixen enters $s$ i $t$ tals que $as + bt = \min\{d \in S\}$. Posem $d = as + bt$. Pel criteri de divisibilitat d'Euclides (3.2.29) tenim que existeixen dos enters $q$ i $r$ amb $0 \leq r < d$ tals que

$$a = dq + r.$$

Tenim que $r$ és un element de $S \cup \{0\}$, ja que

$$\begin{aligned} r &= a - qd \\ &= a - q(as + bt) \\ &= a(1 - qs) - b(qt). \end{aligned}$$

Ara bé, tenim que $0 \leq r < d$ i $as + bt = \min\{d \in S\}$. Per tant ha de ser $r = 0$ i per la definició de divisor (3.2.18) trobem $d \mid a$. Amb un argument anàleg podem veure que $d \mid b$. Suposem ara que existeix $c$ tal que $c \mid a$ i $c \mid b$. Per la definició de divisor (3.2.18) tenim que existeixen $k$ i $k'$ satisfent

$$a = kc \quad \text{i} \quad b = k'c$$

i per tant

$$\begin{aligned} d &= as + bt \\ &= cks + ck't \\ &= c(ks + k't), \end{aligned}$$

i per tant $c < d$, i per la definició de màxim comú divisor (3.2.25) trobem que $\operatorname{mcd}(a, b) = as + bt$. □

**Definició 3.2.31** (Coprimers)**.** Siguin $a$ i $b$ dos enters tals que $\mathrm{mcd}(a,b)=1$. Aleshores direm que $a$ i $b$ són coprimers.

**Teorema 3.2.32.** *Siguin $a$ i $b$ dos enters. Aleshores $a$ i $b$ són coprimers si i només si existeixen dos enters $\alpha$ i $\beta$ tals que*

$$\alpha a+\beta b=1.$$

*Demostració.* Veiem que la condició és suficient ($\Rightarrow$). Suposem doncs que $a$ i $b$ són coprimers. Per la identitat de Bézout (3.2.30) hem acabat.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem doncs que existeixen dos enters $\alpha$ i $\beta$ tals que $\alpha a+\beta b=1$. Tenim que si existeix un enter $c$ tal que $c\mid a$ i $c\mid b$, aleshores $c\mid 1$, i per la definició de màxim comú divisor (3.2.25) trobem que $\mathrm{mcd}(a,b)=1$. □

**Proposició 3.2.33.** *Siguin $c$ un enter i $a$ i $b$ dos enters coprimers tals que $a\mid bc$. Aleshores $a\mid c$.*

*Demostració.* Pel Teorema 3.2.32 tenim que existeixen dos enters $\alpha$ i $\beta$ tals que

$$1=\alpha a+\beta b.$$

Per tant

$$c=c\alpha a+c\beta b,$$

i per la definició de divisor (3.2.18) tenim que existeix un enter $k$ tal que $ak=bc$. Per tant

$$c=c\alpha a+ak\beta$$

i per la proposició 3.2.15 tenim que $c=(c\alpha+k\beta)a$ i per la definició de divisor (3.2.18) tenim que $a\mid c$. □

### 3.2.6 Mínim comú múltiple

**Definició 3.2.34** (Mínim comú múltiple)**.** Siguin $a$ i $b$ dos enters. Aleshores definim

$$\mathrm{mcm}(a,b)=\min\{m\in\mathbb{Z}\mid m>0, a\mid m \text{ i } a\mid m\}$$

com el mínim comú múltiple de $a$ i $b$.

**Teorema 3.2.35.** *Siguin $a$ i $b$ dos enters. Aleshores*

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

*Demostració.* Sigui $d=\mathrm{mcd}(a,b)$. Per la definició de màxim comú divisor (3.2.25) existeixen $a'$ i $b'$ tals que $a=da'$ i $b=db'$. Per tant, per la proposició 3.2.21 trobem que $d\mid ab$, i per la definició de divisor (3.2.18) trobem que existeix un enter $l$ tal que $dl=|ab|$. Per tant $dl=da'b$ i $dl=adb'$, i pel corol·lari 3.2.17 tenim que $l=a'b$ i $l=ab'$, i per la definició de divisor (3.2.18) tenim que $a\mid l$ i $b\mid l$.

Sigui $m$ un enter tal que $a\mid m$ i $b\mid m$. Per la definició de divisor (3.2.18) tenim que existeixen dos enters $k_1$ i $k_2$ tals que $m=ak_1$ i $m=bk_2$. Ara bé,

per la identitat de Bézout (3.2.30) tenim que existeixen dos enters $\alpha$ i $\beta$ tals que $\alpha a + \beta b = d$. Per tant

$$\begin{aligned} md &= m\alpha a + ma\beta && (3.2.15)\\ &= bk_2\alpha a + ak_1\beta b \\ &= ab(bk_2 + ak_1) && (3.2.15)\\ &= dl(bk_2 + ak_1) \end{aligned}$$

i de nou pel corol·lari 3.2.17 trobem que $m = l(bk_2 + ak_1)$, i per tant $l \leq m$. Per tant, per la definició de mínim comú múltiple (3.2.34) tenim que $l = \operatorname{mcm}(a, b)$, i per tant

$$|ab| = \operatorname{mcd}(a, b) \operatorname{mcm}(a, b). \qquad \square$$

### 3.2.7 Teorema Fonamental de l'Aritmètica

**Definició 3.2.36** (Enter primer)**.** Siguin $p > 1$ un enter amb i $d$ un enter tal que si $d \mid p$ aleshores $d$ és igual a 1 ó $p$. Aleshores direm que $p$ és primer.

**Proposició 3.2.37.** *Siguin $a$ i $b$ dos enters i $p$ un primer tals que $p \mid ab$. Aleshores $p \mid a$ ó $p \mid b$.*

*Demostració.* Suposem que $p \nmid a$. Aleshores per la definició de coprimers (3.2.31) tenim que $p$ i $a$ són coprimers. Per tant per la proposició 3.2.33 tenim que $p \mid b$. El cas $p \nmid b$ és anàleg. $\square$

**Lemma 3.2.38.** *Sigui $a$ un enter amb $a > 1$. Aleshores existeixen $p_1, \ldots, p_n$ primers tals que*

$$a = p_1^{r_n} \cdots p_n^{r_n}.$$

*Demostració.* Observem primer que si $a$ és primer tenim $a = a$ i aquest cas particular de l'enunciat és cert.

Ho farem per inducció. Si $a = 2$ tenim que $a$ és primer i hem acabat.

Suposem ara que $a > 2$ i que l'enunciat és cert per a $a$ fix. Volem veure que també és cert per a $a + 1$. Si $a + 1$ és primer, per la definició d'enter primer (3.2.36) hem acabat. Suposem doncs que $a + 1$ no és primer. Aleshores existeixen enters $\alpha$ i $\beta$ tals que $a+1 = \alpha\beta$. Bé, tenim que es compleix $2 \leq \alpha \leq a$ i $2 \leq \beta \leq a$. Ara bé, per l'hipòtesi d'inducció tenim que existeixen $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ primers tals que

$$\alpha = p_1 \cdots p_r \quad \text{i} \quad \beta = q_1 \cdots q_s,$$

i per tant

$$a + 1 = p_1 \cdots p_r q_1 \cdots q_s,$$

i pel principi d'inducció (3.1.7) tenim que l'enunciat és cert. $\square$

**Lemma 3.2.39.** *Siguin $a > 1$ un enter i $p_1, \ldots, p_n$ i $q_1, \ldots, q_r$ primers satisfent $p_1 \leq \cdots \leq p_n$, $q_1 \leq \cdots \leq q_r$ tals que*

$$a = p_1 \cdots p_n \quad i \quad a = q_1 \cdots q_r.$$

*Aleshores $n = r$ i $p_i = q_i$ per a tot $i \in \{1, \ldots, n\}$.*

*Demostració.* Tenim que

$$p_1 \cdots p_n = q_1 \cdots q_r,$$

i per la definició de divisor (3.2.18) trobem que $p_1 \mid q_1 \cdots q_r$, i per la proposició 3.2.37 trobem que $p_1 \mid q_{j_1}$ per a cert $j_1 \in \{1, \ldots, r\}$ i per la definició d'enter primer (3.2.36) trobem que existeix un $\{j_1 \in \{1, \ldots, r\}$ tal que $p_1 = q_{j_1}$. Aleshores pel corol·lari 3.2.17 trobem que

$$p_2 \cdots p_n = q_1 \cdots q_{j_1 - 1} q_{j_1 + 1} \cdots q_r.$$

Podem iterar aquest procés $k = \min(n, r)$ vegades. Ara bé, si $n > r$ tenim

$$p_{k+1} \cdots p_n = 1,$$

que, per la definició d'enter primer (3.2.36), no és possible, i si $n < r$ trobem

$$1 = q_{j_{k+1}} \cdots q_{j_r}$$

on $j_{k+1}, \ldots, j_r \in \{1, \ldots, r\} \setminus \{j_1, \ldots, j_k\}$, i de nou per la definició d'enter primer (3.2.36), no és possible. Per tant ha de ser $n = r$ i hem acabat. □

**Teorema 3.2.40** (Teorema Fonamental de l'Aritmètica)**.** *Sigui $a > 1$ un enter. Aleshores existeixen $p_1, \ldots, p_n$ primers amb $p_1 \geq p_2 \geq \cdots \geq p_n$ únics tals que $a = p_1 \cdots p_n$.*

*Demostració.* És conseqüència del lemma 3.2.38 i el lemma 3.2.39. □

**Teorema 3.2.41** (Teorema d'Euclides)**.** *Sigui $m$ un natural. Aleshores existeix un nombre natural $n > m$ tal que $p_1, \ldots, p_n$ siguin nombres primers diferents dos a dos.*

*Demostració.* Siguin $p_1, \ldots, p_m$ primers diferents. Definim

$$p = \left( \prod_{i=1}^{m} p_i \right) + 1.$$

Per la definició de divisor (3.2.18) tenim que $p_j \mid \prod_{i=0}^{m} p_i$ per a tot $j \in \{1, \ldots, m\}$. Fixem aquest $j \in \{1, \ldots, m\}$, i de nou per la definició de divisor (3.2.18) tenim que existeix un enter $q$ tal que

$$q p_j = \prod_{i=0}^{m} p_i$$

i tenim que

$$p = q p_j + 1,$$

o equivalentment,

$$p - q p_j = 1.$$

Per tant pel Teorema 3.2.32 i la definició de coprimers (3.2.31) trobem que $p$ i $p_j$ són coprimers per a tot $j \in \{1, \ldots, m\}$.

Si $p$ és primer hem acabat, ja que $p$ és més gran que $p_1, \ldots, p_n$, i per tant diferent. Ara bé, si $p$ no és primer pel lemma 3.2.38 tenim que existeix un primer $p'$ tal que $p' \mid p$, però hem vist que $p_1 \, dots, p_m \nmid p$, per tant $p'$ és diferent de $p_1, \ldots, p_m$ i hem acabat. □

## 3.3 Els nombres modulars

### 3.3.1 Construcció dels nombres modulars

**Proposició 3.3.1.** *Siguin $m$ un nombre enter. Aleshores la relació*

$$x \sim y \iff x - y = mk \quad \text{per a cert } k \in \mathbb{Z} \text{ per a tot } x, y \in \mathbb{Z}$$

*és una relació d'equivalència.*

*Demostració.* Comprovem les propietats de la definició de relació d'equivalència:

1. Reflexiva: Sigui $x$ un nombre enter. Aleshores per l'observació 3.2.9 tenim que $x - x = 0$ i per la definició de nombres enters (3.2.2) trobem que $0 = m \cdot 0$, i per tant $x \sim x$.
2. Simètrica: Siguin $x$ i $y$ dos enters tals que $x \sim y$. Per hipòtesi tenim que $x - y = km$ per a cert $k$ enter, i per tant $y - x = -km$ i tenim $y \sim x$.
3. Transitiva: Siguin $x$, $y$ i $z$ nombres enters tals que $x \sim y$ i $y \sim z$. Per hipòtesi això és que $x - y = mk$ i $y - z = mk'$ per a cert $k, k'$ enters. Per tant trobem

$$\begin{aligned} x - z &= x - y + y - z \\ &= mk + mk' \\ &= m(k + k') \end{aligned}$$

   i per tant $x \sim z$.

I per la definició de relació d'equivalència (2.3.2) hem acabat. □

**Definició 3.3.2** (Nombres modulars)**.** Siguin $m$ un enter i

$$x \sim y \iff x - y = mk \quad \text{per a cert } k \in \mathbb{Z} \text{ per a tot } x, y \in \mathbb{Z}$$

una relació d'equivalència. Aleshores denotem el conjunt quocient $\mathbb{Z}/\sim$ com $\mathbb{Z}/(m)$, i si $x \sim y$ escriurem $x \equiv y \pmod{m}$. Direm que $\mathbb{Z}/(m)$ són nombres modulars i si $x \sim y$ direm que $x$ i $y$ són congruents mòdul $m$.

Aquesta definició té sentit per la proposició 3.3.1

### 3.3.2 Operacions sobre nombres modulars

**Definició 3.3.3** (Suma de nombres modulars)**.** Siguin $\overline{x}$ i $\overline{y}$ dos elements de $\mathbb{Z}/(m)$. Aleshores definim la seva suma com l'operació

$$\overline{x} + \overline{y} = \overline{x + y}.$$

**Definició 3.3.4** (Producte de nombres modulars)**.** Siguin $\overline{x}$ i $\overline{y}$ dos elements de $\mathbb{Z}/(m)$. Aleshores definim el seu producte com l'operació

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

**Proposició 3.3.5.** *Siguin $\overline{a}$, $\overline{b}$ i $\overline{c}$ elements de $\mathbb{Z}/(m)$. Aleshores*

1. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

2. $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.
3. $\overline{a} + \overline{0} = \overline{a}$.
4. $\overline{a} + \overline{-a} = \overline{0}$.

*Demostració.* Per veure el punt (1) fem

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} && \text{(suma de nombres modulars (3.3.3))} \\ &= \overline{b+a} && (3.2.11) \\ &= \overline{b} + \overline{a}. && \text{(suma de nombres modulars (3.3.3))} \end{aligned}$$

Per veure el punt (2) fem

$$\begin{aligned} \overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b+c} && \text{(suma de nombres modulars (3.3.3))} \\ &= \overline{a + (b+c)} && \text{(suma de nombres modulars (3.3.3))} \\ &= \overline{(a+b) + c} && (3.2.13) \\ &= \overline{a+b} + \overline{c} && \text{(suma de nombres modulars (3.3.3))} \\ &= (\overline{a} + \overline{b}) + \overline{c}. && \text{(suma de nombres modulars (3.3.3))} \end{aligned}$$

Per veure el punt (3) fem

$$\begin{aligned} \overline{a} + \overline{0} &= \overline{a+0} && \text{(suma de nombres modulars (3.3.3))} \\ &= \overline{a}. && (3.2.6) \end{aligned}$$

Per veure el punt (4) fem

$$\begin{aligned} \overline{a} + \overline{-a} &= \overline{a-a} && \text{(suma de nombres modulars (3.3.3))} \\ &= \overline{0}. && (3.2.9) \end{aligned}$$

I hem acabat. □

**Proposició 3.3.6.** *Siguin $\overline{a}$, $\overline{b}$ i $\overline{c}$ elements de $\mathbb{Z}/(m)$. Aleshores*

1. $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.
2. $\overline{a} \cdot \overline{1} = \overline{a}$.
3. $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.
4. $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

*Demostració.* Per veure el punt (1) fem

$$\begin{aligned} \overline{a} \cdot \overline{b} &= \overline{a \cdot b} && \text{(producte de nombres modulars (3.3.4))} \\ &= \overline{b \cdot a} && (3.2.12) \\ &= \overline{b} \cdot \overline{a}. && \text{(producte de nombres modulars (3.3.4))} \end{aligned}$$

Per veure el punt (2) fem, per la definició de producte de nombres modulars (3.3.4)

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1},$$

i per la proposició 3.2.6 trobem

$$\overline{a} \cdot \overline{1} = \overline{a}.$$

Per veure el punt (3) fem

$$\begin{aligned}
\overline{a} \cdot (\overline{b} \cdot \overline{c}) &= \overline{a} \cdot \overline{b \cdot c} && \text{(producte de nombres modulars (3.3.4))} \\
&= \overline{a \cdot (b \cdot c)} && \text{(producte de nombres modulars (3.3.4))} \\
&= \overline{(a \cdot b) \cdot c} && (3.2.14) \\
&= \overline{a \cdot b} \cdot \overline{c} && \text{(producte de nombres modulars (3.3.4))} \\
&= (\overline{a} \cdot \overline{b}) \cdot \overline{c}. && \text{(producte de nombres modulars (3.3.4))}
\end{aligned}$$

Per veure el punt (4) fem

$$\begin{aligned}
\overline{a} \cdot (\overline{b} + \overline{c}) &= \overline{a} \cdot \overline{b + c} && \text{(suma de nombres modulars (3.3.3))} \\
&= \overline{a \cdot (b + c)} && \text{(producte de nombres modulars (3.3.4))} \\
&= \overline{ab + ac} && (3.2.15) \\
&= \overline{ab} + \overline{ac} && \text{(suma de nombres modulars (3.3.3))} \\
&= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}. && \text{(producte de nombres modulars (3.3.4))}
\end{aligned}$$

I hem acabat. □

### 3.3.3 Congruències i aritmètica modular

**Proposició 3.3.7.** *Siguin $a$, $a'$, $b$, $b'$ i $m > 1$ enters tals que*

$$a \equiv a' \pmod{m} \quad i \quad b \equiv b' \pmod{m}.$$

*Aleshores*

$$a + b \equiv a' + b' \pmod{m} \quad i \quad ab \equiv a'b' \pmod{m}.$$

*Demostració.* Per la definició d'nombres modulars congruents (3.3.2) tenim que existeixen enters $\lambda$ i $\mu$ tals que $a - a' = \lambda m$ i $b - b' = \mu m$. Per tant

$$\begin{aligned}
(a + b) - (a' - b') &= (a - a') + (b - b') \\
&= \lambda m + \mu m \\
&= (\lambda + \mu)m, && (3.3.6)
\end{aligned}$$

i per la definició de nombres modulars congruents (3.3.2) trobem que $a + b \equiv a' + b' \pmod{m}$. També veiem que

$$\begin{aligned}
ab - a'b' &= (a' + \lambda m)(b' - \mu m) - a'b' \\
&= a'b' + (a'\mu + b'\lambda + \lambda\mu m)m - a'b' \\
&= (a'\mu + b'\lambda + \lambda\mu m)m,
\end{aligned}$$

i per tant $ab \equiv a'b' \pmod{m}$. □

**Definició 3.3.8** (Nombre modular invertible)**.** Sigui $\overline{a}$ un element de $\mathbb{Z}/(m)$ tal que existeix un element $\overline{a'}$ de $\mathbb{Z}/(m)$ satisfent $\overline{a}\overline{a'} = \overline{1}$. Aleshores direm que $\overline{a}$ és invertible pel producte i que $\overline{a'}$ és la inversa de $\overline{a}$.

Denotarem $\overline{a}^{-1}$ com la inversa de $\overline{a}$

**Proposició 3.3.9.** *Sigui $\overline{a}$ un element de $\mathbb{Z}/(m)$ Aleshores $\overline{a}$ és invertible si i només si $a$ i $m$ són coprimers.*

*Demostració.* Per la definició de nombre modular invertible (3.3.8) tenim que $\overline{a}$ és invertible si existeix un element $a'$ tal que $aa' \equiv 1 \pmod{m}$, i per la definició de nombres modulars congruents (3.3.2) tenim que això és si existeix un enter $\lambda$ tal que $aa' - 1 = \lambda m$.

Això és equivalent a que $aa' - \lambda m = 1$, i per la identitat de Bézout (3.2.30) tenim que això és si i només si $\mcd(a, m) = 1$, i per la definició de coprimers (3.2.31) tenim que $a$ i $m$ són coprimers. □

**Corol·lari 3.3.10.** *Sigui $p > 1$ un enter. Aleshores $p$ és primer si i només si $\overline{a}$ és invertible per a tot $\overline{a} \in \mathbb{Z}/(p) \setminus \{\overline{0}\}$.*

**Teorema 3.3.11** (El Petit Teorema de Fermat)**.** *Siguin $p$ un primer i $a$ un enter tal que $p \nmid a$. Aleshores*

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

*Demostració.* Observem que per la definició de divisor (3.2.18) i la definició de coprimers (3.2.31) tenim que $a$ i $p$ són coprimers. Per tant per la proposició 3.3.9 tenim que $a$ és invertible.

Considerem el conjunt

$$X = \{\overline{a}, \overline{2a}, \overline{3a}, \ldots, \overline{(p-1)a}\}.$$

Veiem que tots els elements de $X$ són diferents. Efectivament, si $na \equiv ma \pmod{p}$ per a certs enters $n$ i $m$ per la definició de nombre modular invertible (3.3.8) trobem que $n \equiv m \pmod{p}$.

També tenim que

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

i per tant

$$a^{n-1}(p-1)! \equiv (p-1)! \pmod{p},$$

i de nou per la definició de divisor (3.2.18) i la definició de coprimers (3.2.31) tenim que $(p-1)!$ i $p$ són coprimers, per tant per la proposició 3.3.9 tenim que $(p-1)!$ és invertible i trobem

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

### 3.3.4 El Teorema xinès de les restes

**Lemma 3.3.12.** *Siguin $m_1, \ldots, m_n$ naturals més grans que 1, $a_1, \ldots, a_n$ enters i $x_0$ un enter tal que*

$$\begin{cases} x_0 \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x_0 \equiv a_n \pmod{m_n} \end{cases}$$

*Aleshores, si* $x = x_0 + \lambda M$ *amb* $M = \text{mcm}(m_1, \dots, m_n$ *i per a tot* $\lambda$ *enter es satisfà*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

*Demostració.* Tenim que, per a tot $i \in \{1, \dots, n\}$, és satisfà $x \equiv a_i \pmod{m_i}$ si i només si es satisfà $x \equiv x_0 \pmod{m_i}$. Per tant hem de veure que es satisfà

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ \quad \vdots \\ x \equiv x_0 \pmod{m_n} \end{cases}$$

Ara bé, per la definició de nombres modulars congruents (3.3.2) i la definició de 3.2.25 tenim que ha de ser

$$x - x_0 = \lambda M$$

per a cert $\lambda$ enter. □

**Teorema 3.3.13** (Teorema xinès de les restes)**.** *Siguin* $m_1, \dots, m_n$ *enters més grans que* 1 *coprimers dos a dos i* $a_1, \dots, a_n$ *enters. Aleshores el sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

*té una única solució, que és* $|m_1 \cdots m_n|$.

*Demostració.* Prenem $M = \text{mcm}(m_1, \dots, m_n)$. Per la definició de mínim comú múltiple (3.2.34) i la definició de coprimers (3.2.31) tenim que

$$M = \text{mcm}(m_1, \dots, m_n) = \left| \prod_{i=1}^{n} m_i \right|.$$

Per a tot $i \in \{1, \dots, n\}$ definim

$$M_1 = m_1 \cdots m_{i-1} m_{i+1} \cdots m_n$$

i tenim, per la definició de coprimers (3.2.31), que $M_i$ i $m_i$ són coprimers.

Per tant la congruència

$$M_i x \equiv a_i \pmod{m_i}$$

té solució, ja que per la proposició 3.3.9 tenim que $M_i$ és invertible i per tant $x \equiv a_i M_i^{-1} \pmod{m_i}$. Denotem $b_i = a_i M_i^{-1}$ i considerem

$$x_0 = M_1 b_1 + \cdots + M_n b_n.$$

Aleshores tenim per la definició de nombres modulars (3.3.2) tenim que

$$x_0 \equiv M_i b_i \pmod{m_i}.$$

Per tant, pel lemma 3.3.12 tenim que

$$x = x_0 + \lambda M$$

amb $M = \text{mcm}(m_1, \ldots, m_n)$ són les solucions del sistema, i per la definició de nombres modulars (3.3.2) trobem que $x = x_0$ i per tant és única. □

## 3.4 Les permutacions

### 3.4.1 El grup simètric

**Definició 3.4.1** (Permutació)**.** Sigui $X$ un conjunt i $\sigma\colon X \to X$ una aplicació bijectiva. Aleshores direm que $\sigma$ és una permutació.

**Definició 3.4.2** (Grup simètric)**.** Siguin $X$ un conjunt no buit i

$$\mathrm{S}_X = \{\sigma\colon X \to X \mid \sigma \text{ és una permutació}\}$$

un conjunt. Aleshores direm que $\mathrm{S}_X$ és el grup simètric de $X$.

Si $X = \{1, \ldots, n\}$ aleshores denotarem el grup simètric de $X$ com $\mathrm{S}_n$.

**Definició 3.4.3** (Elements moguts per una permutació)**.** Siguin $X$ un conjunt no buit, $\sigma \in \mathrm{S}_X$ una permutació i

$$\mathrm{M}(\sigma) = \{x \in X \mid \sigma(x) \neq x\}$$

un conjunt. Aleshores direm que $\mathrm{M}(\sigma)$ és el conjunt d'elements de $X$ moguts per $\sigma$.

**Proposició 3.4.4.** *Siguin $X$ un conjunt no buit i $\sigma$ una permutació de $\mathrm{S}_X$. Aleshores*

$$\mathrm{M}(\sigma) = \emptyset \iff \sigma = \mathrm{Id}_X\,.$$

*Demostració.* Comencem veient l'implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $\mathrm{M}(\sigma) = \emptyset$. Aleshores per la definició de conjunt d'elements moguts per una permutació (3.4.3) trobem que $\{x \in X \mid \sigma(x) \neq x\} = \emptyset$, i per tant ha de ser $\sigma(x) = x$ per a tot $x \in X$, i per tant $\sigma = \mathrm{Id}_X$.

Veiem ara l'implicació cap a l'esquerra ($\Leftarrow$). Prenem $\mathrm{Id}_X$. Aleshores ha de ser $\mathrm{M}(\mathrm{Id}_X) = \emptyset$, ja que per la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que $\mathrm{M}(\mathrm{Id}_X) = \{x \in X \mid \mathrm{Id}_X(x) \neq x\}$. □

**Proposició 3.4.5.** *Siguin $X$ un conjunt no buit i $\sigma$ i $\tau$ dues permutacions de $\mathrm{S}_X$. Aleshores*

$$\mathrm{M}(\sigma \circ \tau) \subseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau).$$

*Demostració.* Prenem $a \in X$ tal que $a \in \mathrm{M}(\sigma \circ \tau)$. Això és, per la definició de conjunt d'elements moguts per una permutació (3.4.3), que $a \in \{x \in X \mid \sigma \circ \tau(x) \neq x\}$. Volem veure que $a \in \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$, i per la definició d'unió de conjunts (2.1.12) hem de veure que $a \in \mathrm{M}(\sigma)$ ó $a \in \mathrm{M}(\tau)$.

Si $a \notin \mathrm{M}(\tau)$ tenim que $\tau(a) = a$, i tenim $\sigma \circ \tau(a) = \sigma(a)$. Ara bé, ha de ser $\sigma(a) \neq a$, ja que si no tindríem $a \notin \mathrm{M}(\sigma \circ \tau)$. Per tant ha de ser $a \in \mathrm{M}(\sigma)$.

Si $a \notin \mathrm{M}(\sigma)$ tenim que $\sigma(a) = a$, i per tant tenim que $\tau(a) \neq a$, ja que si $\tau(a) = a$ tindríem $\sigma \circ \tau(a) = \sigma(a) = a$, i seria $a \notin \mathrm{M}(\sigma \circ \tau)$. Per tant ha de ser $a \in \mathrm{M}(\tau)$.

Per tant tenim que si $a \in \mathrm{M}(\sigma \circ \tau)$ aleshores $a \in \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$, i per la definició de subconjunt (2.1.2) trobem que $\mathrm{M}(\sigma \circ \tau) \subseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$, com volíem veure. □

### 3.4.2 Permutacions disjuntes

**Definició 3.4.6** (Permutacions disjuntes)**.** Siguin $X$ un conjunt no buit i $\sigma$ i $\tau$ dues permutacions de $\mathrm{S}_X$ tals que $\mathrm{M}(\sigma) \cap \mathrm{M}(\tau) = \emptyset$. Aleshores direm que $\sigma$ i $\tau$ són disjuntes.

**Proposició 3.4.7.** *Siguin $X$ un conjunt no buit i $\sigma$ i $\tau$ dues permutacions disjuntes de $\mathrm{S}_X$. Aleshores*

$$\mathrm{M}(\sigma \circ \tau) = \mathrm{M}(\sigma) \cup \mathrm{M}(\tau).$$

*Demostració.* Per la proposició 3.4.5 tenim que $\mathrm{M}(\sigma \circ \tau) \subseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$. Veiem doncs que $\mathrm{M}(\sigma \circ \tau) \supseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$.

Prenem un element $a \in \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$. Com que, per hipòtesi, $\sigma$ i $\tau$ són dues permutacions disjuntes, per la definició de permutacions disjuntes (3.4.6) tenim que $\mathrm{M}(\sigma) \cap \mathrm{M}(\tau) = \emptyset$ i per la definició d'intersecció de conjunts (2.1.13) tenim que o bé $a \in \mathrm{M}(\sigma)$ o bé $a \in \mathrm{M}(\tau)$.

Suposem que $a \in \mathrm{M}(\sigma)$. Per la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que $\sigma(a) \neq a$ i $\tau(a) = a$, ja que $a \notin \mathrm{M}(\tau)$. Per tant $\sigma \circ \tau(a) = \sigma(a) \neq a$, i per tant $a \in \mathrm{M}(\sigma \circ \tau)$.

Suposem ara que $a \in \mathrm{M}(\tau)$. Per la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que $\tau(a) \neq a$ i $\sigma(a) = a$, ja que $a \notin \mathrm{M}(\sigma)$. Per tant $\sigma \circ \tau(a) = \sigma(b)$ per a cert $b \neq a$, $b = \tau(a)$. Ara bé, com que per la definició de permutació (3.4.1) $\sigma$ és una aplicació bijectiva, i per la definició d'aplicació bijectiva (2.2.9) trobem que $\sigma$ és una aplicació injectiva, i per la definició d'aplicació injectiva (2.2.7) tenim que $\sigma(b) \neq a$, ja que $\sigma(a) = a$ i $b \neq a$. Per hem vist que

$$\mathrm{M}(\sigma \circ \tau) \subseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau) \quad \text{i} \quad \mathrm{M}(\sigma \circ \tau) \supseteq \mathrm{M}(\sigma) \cup \mathrm{M}(\tau),$$

i pel Teorema de la doble inclusió (2.1.3) tenim que

$$\mathrm{M}(\sigma \circ \tau) = \mathrm{M}(\sigma) \cup \mathrm{M}(\tau).$$ □

**Lemma 3.4.8.** *Siguin $X$ un conjunt no buit i $\tau$ una permutació de $\mathrm{S}_X$. Aleshores*

$$x \in \mathrm{M}(\sigma) \iff \sigma(x) \in \mathrm{M}(\sigma).$$

*Demostració.* Per la definició de permutació (3.4.1) tenim que $\sigma$ és bijectiva, i per tant $\sigma(x) = x$ si i només si $\sigma(\sigma(x)) = \sigma(x)$. Prenent la negació d'això trobem que $\sigma(x) \neq x$ si i només si $\sigma(\sigma(x)) \neq \sigma(x)$, que per la definició de conjunt d'elements moguts per una permutació (3.4.3) és equivalent a $x \in \mathrm{M}(\sigma) \iff \sigma(x) \in \mathrm{M}(\sigma)$. □

**Teorema 3.4.9.** *Siguin $X$ un conjunt no buit i $\sigma$ i $\tau$ dues permutacions disjuntes de $\mathrm{S}_X$. Aleshores*

$$\sigma \circ \tau = \tau \circ \sigma.$$

*Demostració.* Per la definició de permutacions disjuntes (3.4.6) i la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que, per hipòtesi, $\mathrm{M}(\sigma) \cap \mathrm{M}(\tau) = \emptyset$. Per tant, per a tot $x \in X$ tenim o bé $x \in \mathrm{M}(\sigma)$, o bé $x \in \mathrm{M}(\tau)$ o bé $x \notin \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$. Estudiem els cassos.

Suposem que $x \in \mathrm{M}(\sigma)$, i per tant $x \notin \mathrm{M}(\tau)$. Per la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que $\tau(x) = x$ i per tant $\sigma(\tau(x)) = \sigma(x)$. Ara bé, pel lemma 3.4.8 tenim que $\sigma(x) \in \mathrm{M}(\sigma)$, d'on trobem que $\sigma(x) \notin \mathrm{M}(\tau)$, ja que, per hipòtesi, $\mathrm{M}(\sigma) \cap \mathrm{M}(\tau) = \emptyset$, i per tant $\tau(\sigma(x)) = \sigma(x)$.

Suposem que $x \in \mathrm{M}(\tau)$, i per tant $x \notin \mathrm{M}(\sigma)$. Per la definició de conjunt d'elements moguts per una permutació (3.4.3) tenim que $\sigma(x) = x$ i per tant $\tau(\sigma(x)) = \tau(x)$. Ara bé, pel lemma 3.4.8 tenim que $\tau(x) \in \mathrm{M}(\tau)$, d'on trobem que $\tau(x) \notin \mathrm{M}(\sigma)$, ja que, per hipòtesi, $\mathrm{M}(\tau) \cap \mathrm{M}(\sigma) = \emptyset$, i per tant $\sigma(\tau(x)) = \tau(x)$.

Suposem per acabar que $x \notin \mathrm{M}(\sigma) \cup \mathrm{M}(\tau)$. Aleshores tenim que $\sigma(x) = x$ i $\tau(x) = x$, i per tant $\sigma \circ \tau = \tau \circ \sigma$, com volíem veure. □

### 3.4.3 Cicles

**Definició 3.4.10** ($r$-cicle)**.** Siguin $X$ un conjunt no buit i $\sigma$ una permutació de $\mathrm{S}_X$ tals que $\mathrm{M}(\sigma) = \{a_1, \ldots, a_r\}$ amb $\sigma(a_i) = a_{i+1}$ per a tot $i \in \{1, \ldots, r-1\}$ i $\sigma(a_r) = a_1$. Aleshores direm que $\sigma$ és un $r$-cicle, o un cicle, i denotarem

$$\sigma = (a_1, \ldots, a_r).$$

**Proposició 3.4.11.** *Siguin $X$ un conjunt no buit, $a$ un element de $\mathrm{M}(\sigma)$ i $\sigma$ un $r$-cicle de $\mathrm{S}_X$. Aleshores*

$$\sigma = (a, \sigma(a), \sigma^2(a), \ldots, \sigma^{r-1}(a)).$$

*Demostració.* Per la definició d'$r$-cicle (3.4.10) tenim que $\mathrm{M}(\sigma) = \{a_1, \ldots, a_r\}$, i com que $a \in \mathrm{M}(\sigma)$ tenim que $a = a_k$ per a cert $k \in \{1, \ldots, r\}$. Tenim doncs que

$$\sigma = (a, a_{k+1}, \ldots, a_{r-k}).$$

Ara bé, per la definició d'$r$-cicle (3.4.10) tenim que

$$a_{i+1} = \sigma(a_i) \quad \text{per a tot } i \in \{1, \ldots, r-1\}$$

i $a_1 = \sigma(a_r)$. Per tant trobem

$$\sigma^i(a) = a_{k+i} \quad \text{per a tot } i \in \{-k+1, \ldots, r-k-1\},$$

i per tant trobem

$$\sigma = (a, \sigma(a), \sigma^2(a), \ldots, \sigma^{r-1}(a)).$$ □

**Lemma 3.4.12.** *Siguin $X$ un conjunt no buit i $\sigma$ un $r$-cicle de $\mathrm{S}_X$. Aleshores $r = \min\{k \in \mathbb{N} \mid \sigma^k = \mathrm{Id}_X\}$.*

*Demostració.* Per la definició d'$r$-cicle (3.4.10) tenim que existeixen $a_1, \ldots, a_r$ tals que $\mathrm{M}(\sigma) = \{a_1, \ldots, a_r\}$ amb $\sigma(a_i) = a_{i+1}$ per a tot $i \in \{1, \ldots, r-1\}$ i

$\sigma(a_r) = a_1$, i per tant $\sigma^r = \mathrm{Id}_X$ ja que tenim $\sigma^r(x) = x$ per a tot $x \in X$. Ara bé, per la proposició 3.4.11 tenim que, amb $a \in \mathrm{M}(\sigma)$,

$$\sigma = (a, \sigma(a), \sigma^2(a), \dots, \sigma^{r-1}(a))$$

i per la definició d'$r$-cicle (3.4.10) tenim que $\sigma^i(a) \neq a$ per a tot $i \in \{0, \dots, r-1\}$, i per tant $r = \min\{k \in \mathbb{N} \mid \sigma^k = \mathrm{Id}_X\}$, com volíem veure. □

**Teorema 3.4.13.** *Siguin $X$ un conjunt no buit i $\sigma$ un $r$-cicle de $\mathrm{S}_X$. Aleshores*

$$\sigma^{-1} = \sigma^{r-1}.$$

*Demostració.* Pel lemma 3.4.12 tenim que $\sigma^r = \mathrm{Id}_X$. Aleshores tenim $\sigma \circ \sigma^{r-1} = \mathrm{Id}_X$ i $\sigma^{r-1} \circ \sigma = \mathrm{Id}_X$. Per tant per la definició d'inversa d'una aplicació (2.2.16) trobem que $\sigma^{-1} = \sigma^{r-1}$. □

**Teorema 3.4.14** (Descomposició de permutacions en cicles disjunts)**.** *Sigui $X$ un conjunt finit no buit i $\sigma$ una permutació de $\mathrm{S}_X$. Aleshores existeixen $\alpha_1, \dots, \alpha_s$ cicles disjunts dos a dos de $\mathrm{S}_X$ tals que*

$$\sigma = \alpha_1 \circ \cdots \circ \alpha_s,$$

*i aquests $\alpha_1, \dots, \alpha_s$ són únics llevat de l'ordre en que es conjuguen.*

*Demostració.* Prenem $a_1 \in \mathrm{M}(\sigma)$ i el conjunt $\{a_1, \sigma(a_1), \sigma^2(a_1), \dots\}$. Com que, per hipòtesi, $X$ és finit tenim que existeixen $i$ i $j$ tals que $\sigma^i(a_1) = \sigma^j(a_1)$, i per tant $\sigma^{i-j}(a_1) = a_1$.

Sigui doncs $k_1 = \min\{k \in \mathbb{N} \mid \sigma^k(a) = a\}$. Per la definició d'$r$-cicle (3.4.10) tenim que

$$\alpha_1 = (a_1, \sigma(a_1), \dots, \sigma^{k_1-1}(a_1)) \tag{3.1}$$

és un $k_1$-cicle.

Si existeix un $a_2 \in X$ que no pertanyi a $\{a_1, \sigma(a_1), \dots, \sigma^{k_1-1}(a_1)\}$. Amb el mateix procés podem generar un nou $k_2$-cicle $\alpha_2$ disjunt amb $\alpha_1$, i així obtenim $\alpha_1, \dots, \alpha_s$ cicles disjunts dos a dos. Aleshores trobem

$$\sigma = \alpha_1 \circ \cdots \circ \alpha_s,$$

ja que $\sigma(x) = \alpha_1 \circ \cdots \circ \alpha_s(x)$ per a tot $x \in X$.

Tenim doncs que

$$\alpha_i = \big(a_i, \sigma(\alpha_i), \dots, \sigma^{k_i-1}(\alpha_i)\big). \tag{3.2}$$

Suposem ara que existeixen $\beta_1, \dots, \beta_r$ cicles disjunts dos a dos de $\mathrm{S}_X$ tals que

$$\sigma = \alpha_1 \circ \cdots \circ \alpha_s = \beta_1 \circ \cdots \circ \beta_r. \tag{3.3}$$

Per la proposició 3.4.7 tenim que $a_i \in \mathrm{M}(\beta_{j_i})$ per a cert $j_i \in \{1, \dots, r\}$, i per la definició de permutacions disjuntes (3.4.6) i la definició d'intersecció de conjunts (2.1.13) tenim que aquest $j_i$ és únic.

Ara bé, com que per hipòtesi $\beta_{j_i}$ és un cicle, per la proposició 3.4.11 tenim que

$$\beta_{j_i} = \left(a_i, \beta_{j_i}(a_i), \dots, \beta_{j_i}^{k'_{j_i}-1}(a_i)\right)$$

per a cert $k'_{j_i}$. Ara bé, tenim per (3.3) que $\beta_{j_i}^k(a_i) = \sigma^k(a_i)$ per a tot $k$. Per tant

$$\beta_{j_i} = \Big(a_i, \sigma(a_i), \dots, \sigma^{k'_{j_i}-1}(a_i)\Big).$$

Ara bé, havíem definit $k_i = \min\{k \in \mathbb{N} \mid \sigma^k(a_i) = a_i\}$. Per tant $k'_{j_i} = k_i$ i, com que per hipòtesi $a_i \in \mathrm{M}(\alpha_{j_i})$ és un cicle, per la proposició 3.4.11, per (3.1) i per (3.2) tenim que $\alpha_i = \beta_{j_i}$. Per tant podem reescriure (3.1) com

$$\sigma = \alpha_1 \circ \cdots \circ \alpha_s = \alpha_1 \circ \cdots \circ \alpha_s \circ \beta_{j_{s+1}} \circ \cdots \circ \beta_{j_r},$$

i per tant ha de ser $\beta_{j_{s+1}} \circ \cdots \circ \beta_{j_r} = \mathrm{Id}_X$. □

### 3.4.4 Descomposició en transposicions i signe

**Definició 3.4.15** (Transposició)**.** Siguin $X$ un conjunt no buit i $\tau$ un 2-cicle de $\mathrm{S}_X$. Aleshores direm que $\tau$ és una transposició.

**Observació 3.4.16.** $\tau = \tau^{-1}$.

**Proposició 3.4.17.** *Siguin $X$ un conjunt finit no buit i $\sigma$ una permutació de $\mathrm{S}_X$. Aleshores existeixen transposicions $\tau_1, \dots, \tau_s$ de $\mathrm{S}_X$ tals que*

$$\sigma = \tau_1 \circ \cdots \circ \tau_s.$$

*Demostració.* Observem que per a tot $r$-cicle $\alpha$ de $\mathrm{S}_X$ existeixen transposicions $\tau_1, \dots, \tau_r$ de $\mathrm{S}_X$ tals que $\alpha = \tau_1 \circ \cdots \circ \tau_r$. Efectivament, per la definició d'$r$-cicle (3.4.10) tenim que si $\alpha = (a_1, \dots, a_r)$ aleshores

$$\alpha = (a_1, \dots, a_r) = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{n-1}, a_r),$$

i per la definició de transposició (3.4.15) tenim que $(a_i, a_{i+1})$ és una transposició de $\mathrm{S}_X$ per a tot $i \in \{1, \dots, r-1\}$.

Per tant, pel Teorema de descomposició de permutacions en cicles disjunts (3.4.14) hem acabat. □

**Teorema 3.4.18.** *Siguin $X$ un conjunt finit no buit, $\sigma$ una permutació de $\mathrm{S}_X$ i $\tau_1, \dots, \tau_r$, $\tau'_1, \dots, \tau'_{r'}$ transposicions de $\mathrm{S}_X$ tals que*

$$\sigma = \tau_1 \circ \cdots \circ \tau_r = \tau'_1 \circ \cdots \circ \tau'_{r'}.$$

*Aleshores $r - r'$ és parell.*

*Demostració.* No m'agraden les demostracions que veig ni em surt una millor. □

**Definició 3.4.19** (Signe d'una permutació)**.** Siguin $X$ un conjunt finit no buit, $\sigma$ una permutació de $\mathrm{S}_X$ i $\tau_1, \dots, \tau_r$ transposicions de $\mathrm{S}_X$ tals que

$$\sigma = \tau_1 \circ \cdots \circ \tau_r.$$

Aleshores definim

$$\mathrm{sig}(\sigma) = (-1)^r$$

com el signe de $\sigma$.

Aquesta definició té sentit pel Teorema 3.4.18.

## 3.5 Els nombres racionals

### 3.5.1 Construcció dels nombres racionals

**Proposició 3.5.1.** *Sigui $\sim$ una relació tal que per a tot $(a,b)$, $(c,d)$ elements de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ tenim*

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

*Aleshores $\sim$ és una relació d'equivalència.*

*Demostració.* Comprovem les propietats de la definició de relació d'equivalència:

1. Reflexiva: Per la proposició 3.2.12 tenim $ab=ba$, i per tant $(a,b)\sim(a,b)$.
2. Simètrica: Siguin $(a,b)$ i $(c,d)$ dos elements de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ tals que $(a,b)\sim(c,d)$. Per hipòtesi tenim que $ad=bc$, i per la proposició 3.2.12 tenim que $cb=da$ i trobem $(c,d)\sim(a,b)$.
3. Transitiva: Siguin $(a,b)$, $(c,d)$ i $(e,f)$ elements de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ tals que $(a,b)\sim(c,d)$ i $(c,d)\sim(e,f)$. Per hipòtesi això és $ad=bc$ i $cf=de$. Ara bé, tenim
$$bcf=bde$$
i per tant
$$adf=bde$$
i pel corol·lari 3.2.17 trobem que $af=be$ i tenim que $(a,b)\sim(e,f)$.

I per la definició de relació d'equivalència (2.3.2) hem acabat. □

**Definició 3.5.2** (Conjunt dels nombres racionals)**.** Sigui $\sim$ una relació d'equivalència tal que

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

per a tot $(a,b)$, $(c,d)$ elements de $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$. Aleshores direm que el conjunt quocient $\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}\setminus\{0\}/\sim$ és el conjunt dels nombres racionals. Direm que els elements de $\mathbb{Q}$ són nombres racionals.

Aquesta definició té sentit per la proposició 3.5.1.

**Notació 3.5.3.** Sigui $\overline{(a,b)}$ un element de $\mathbb{Q}$. Aleshores denotarem

$$\overline{(a,b)}=\frac{a}{b}.$$

**Proposició 3.5.4.** *Sigui $\frac{a}{b}$ un nombre racional. Aleshores*

$$\frac{a}{b}=\frac{1}{1}\iff a=b.$$

*Demostració.* Per la definició de classe d'equivalència (2.3.3) tenim que

$$(a,b)\sim(1,1),$$

i per la definició de nombres enters (3.2.2) això és

$$a\cdot 1=b\cdot 1.$$

I per tant, per la proposició 3.2.6 trobem que ha de ser $a=b$. □

**Proposició 3.5.5.** *Siguin* $\frac{0}{a}$ *i* $\frac{0}{b}$ *racionals. Aleshores*

$$\frac{0}{a} = \frac{0}{b}.$$

*Demostració.* Tenim que $0 \cdot b = 0 \cdot a$, i per tant per la definició de nombres racionals (3.5.2) trobem $\overline{(0,a)} \sim \overline{(0,b)}$ i per la definició de classe d'equivalència (2.3.3) trobem

$$\frac{0}{a} = \frac{0}{b}.$$ □

### 3.5.2 Operacions entre nombres racionals

**Definició 3.5.6** (Suma de nombres racionals)**.** Siguin $\frac{a}{b}$ i $\frac{c}{d}$ nombres racionals. Aleshores definim la suma de $\frac{a}{b}$ i $\frac{c}{d}$ com una operació $+$ que satisfà

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}.$$

**Definició 3.5.7** (Producte de nombres racionals)**.** Siguin $\frac{a}{b}$ i $\frac{c}{d}$ nombres racionals. Aleshores definim el producte de $\frac{a}{b}$ i $\frac{c}{d}$ com una operació $\cdot$ que satisfà

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Escriurem

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b}\frac{c}{d}.$$

**Proposició 3.5.8.** *Siguin* $\frac{a}{b}$, $\frac{c}{d}$ *i* $\frac{e}{f}$ *nombres racionals. Aleshores es satisfà*

1. $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$.
2. $\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}$.
3. $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$.
4. $\frac{a}{b} + \frac{-a}{b} = \frac{0}{1}$.

*Demostració.* Per veure el punt (1) fem

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= \frac{ad + cb}{bd} && \text{(suma de nombres racionals (3.5.6))} \\
&= \frac{cb + ad}{bd} && (3.2.11) \\
&= \frac{cb + ad}{db} && (3.2.12) \\
&= \frac{c}{d} + \frac{a}{b}. && \text{(suma de nombres racionals (3.5.6))}
\end{aligned}$$

Per veure el punt (2) fem

$$\begin{aligned}
\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}+\frac{cf+ed}{df} && \text{(suma de nombres racionals (3.5.6))}\\
&= \frac{adf+(cf+ed)b}{bdf} && \text{(suma de nombres racionals (3.5.6))}\\
&= \frac{adf+cfb+edb}{bdf} && (3.2.15)\\
&= \frac{adf+cbf+ebd}{bdf} && (3.2.12)\\
&= \frac{(ad+cb)f+ebd}{bdf} && (3.2.15)\\
&= \frac{ad+cb}{bd}+\frac{e}{f} && \text{(suma de nombres racionals (3.5.6))}\\
&= \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}. && \text{(suma de nombres racionals (3.5.6))}
\end{aligned}$$

Per veure el punt (3) fem

$$\begin{aligned}
\frac{a}{b}+\frac{0}{1} &= \frac{a\cdot 1}{b\cdot 1} && \text{(suma de nombres racionals (3.5.6))}\\
&= \frac{a}{b}. && (3.2.6)
\end{aligned}$$

Per veure el punt (4) fem

$$\begin{aligned}
\frac{a}{b}+\frac{-a}{b} &= \frac{ab-ab}{bb} && \text{(suma de nombres racionals (3.5.6))}\\
&= \frac{0}{bb} && (3.2.6)\\
&= \frac{0}{1}. && (3.5.5)
\end{aligned}$$

i hem acabat. □

**Proposició 3.5.9.** *Siguin $\frac{a}{b}$, $\frac{c}{d}$ i $\frac{e}{f}$ nombres racionals. Aleshores es satisfà*

1. $\frac{a}{b}\frac{c}{d}=\frac{c}{d}\frac{a}{b}$.
2. $\frac{a}{b}\frac{1}{1}=\frac{a}{b}$.
3. $\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)=\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f}$.
4. $\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}$.

*Demostració.* Per veure el punt (1) fem

$$\begin{aligned}
\frac{a}{b}\frac{c}{d} &= \frac{ac}{bd} && \text{(producte de nombres racionals (3.5.7))}\\
&= \frac{ca}{db} && (3.2.12)\\
&= \frac{c}{d}\frac{a}{b}. && \text{(producte de nombres racionals (3.5.7))}
\end{aligned}$$

Per veure el punt (2) fem

$$\begin{aligned}\frac{a}{b}\frac{1}{1} &= \frac{a\cdot 1}{b\cdot 1} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{a}{b}. && (3.2.6)\end{aligned}$$

Per veure el punt (3) fem

$$\begin{aligned}\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right) &= \frac{a}{b}\frac{ce}{df} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{a(ce)}{b(df)} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{(ac)e}{(bd)f} && (3.2.14)\\ &= \frac{ac}{bd}\frac{e}{f} && \text{(producte de nombres racionals (3.5.7))}\\ &= \left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f}. && \text{(producte de nombres racionals (3.5.7))}\end{aligned}$$

Per veure el punt (4) fem

$$\begin{aligned}\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}\frac{cf+de}{df} && \text{(suma de nombres racionals (3.5.6))}\\ &= \frac{a(cf+de)}{bdf} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{acf+ade}{bdf} && (3.2.15)\\ &= \frac{acf+ade}{bdf}\frac{1}{1} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{acf+ade}{bdf}\frac{b}{b} && (3.5.4)\\ &= \frac{(acf+aeb)b}{bdfb} && \text{(producte de nombres racionals (3.5.7))}\\ &= \frac{acfb+aedb}{bdfb} && \text{(producte de nombres enters (3.2.5))}\\ &= \frac{acbf+aebd}{bdbf} && (3.2.12)\\ &= \frac{ac}{bd}+\frac{ae}{bf} && \text{(suma de nombres racionals (3.5.6))}\\ &= \frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}. && \text{(producte de nombres racionals (3.5.7))}\end{aligned}$$

I hem acabat. □

**Teorema 3.5.10.** *Siguin* $\frac{a}{b}$ *i* $\frac{c}{d}$ *dos racionals tals que*

$$\frac{a}{b}\frac{c}{d}=\frac{0}{1}.$$

*Aleshores* $a=0$ *ó* $c=0$.

*Demostració.* Per la definició de producte de nombres racionals (3.5.7) trobem que

$$\frac{ac}{bd} = \frac{0}{1},$$

i per la definició de nombres racionals (3.5.2) tenim que es satisfà

$$ac \cdot 1 = bd \cdot 0.$$

Per tant

$$ac = 0,$$

i pel Teorema 3.2.16 tenim que ha de ser $a = 0$ ó $b = 0$. □

**Teorema 3.5.11.** *Sigui $\frac{a}{b}$ un racional amb $a \neq 0$. Aleshores*

$$\frac{a}{b}\frac{b}{a} = \frac{1}{1}.$$

*Demostració.* Per la definició de producte de nombres racionals (3.5.7) i la proposició 3.2.12 tenim que

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ab}$$

i per la proposició 3.5.4 tenim que

$$\frac{a}{b}\frac{b}{a} = \frac{1}{1}.$$ □

# Bibliografia


[1] *Construction of number systems*. 1 de jul. de 2018. URL: https://www.math.wustl.edu/~kumar/courses/310-2011/Peano.pdf.

[2] Ramon Antoine, Rosa Camps i Jaume Moncasi. *Introducció a l'àlgebra abstracta. Amb elements de matemàtica discreta*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 2007. ISBN: 978-84-490-2515-0.

[3] Agustí Reventós Tarrida. «Temes diversos de fonaments de les matemàtiques». 2014.

[4] Manuel Castellet i Irene Llerena. *Àlgebra lineal i geometria*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 2009. ISBN: 84-7488-943-X.

[5] Roger Godement. *Algebra*. Anglès. Kershaw Publishing Co Ltd, 1969. ISBN: 978-0901665003.

[6] Antonella Cupillari. *The Nuts and Bolts of Proofs. An Introduction to Mathematical Proofs*. Anglès. 4a ed. Academic Press, 2012. ISBN: 978-0123822178.

[7] Emilio Bujalance García et al. *Problemas de Matemática Discreta*. Castellà. Sanz y Torres, 1933. ISBN: 9788488667038.

[8] Peter Eccles. *An Introduction to Mathematical Reasoning*. Anglès. University of Manchester, 1997. ISBN: 9780521597180.

[9] Carol Schumacher. *Chapter Zero. Fundamental Notions of Abstract Mathematics*. Anglès. Addison Wesley, 2001. ISBN: 9780201826531.


La secció sobre els axiomes de Peano està fortament inspirada en [1]. La resta de la teoria és una combinació de [2] i [3], uns apunts de l'assignatura que sospito que només són accessibles des del campus virtual.

La bibliografia del curs inclou els textos [2, 4, 5, 6, 7, 8, 9].

# Part II

# Àlgebra Lineal

# Capítol 4

# Matrius

## 4.1 Matrius i operacions

### 4.1.1 Cossos

**Definició 4.1.1** (Cos)**.** Aclarir on va aquest apartat.

### 4.1.2 Les matrius

**Definició 4.1.2** (Matriu)**.** Siguin $m$ i $n$ dos enters i $\{a_{i,j}\}_{1\leq j\leq n}^{1\leq i\leq m}$ elements d'un cos $\mathbb{K}$. Aleshores direm que

$$[a_{i,j}] = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}$$

és una matriu de mida $m \times n$ sobre $\mathbb{K}$.

Direm que $a_{i,j}$ és el component $(i, j)$ de la matriu $[a_{i,j}]$. Si $A = [a_{i,j}]$ també denotarem $[A]_{i,j} = a_{i,j}$.

Si $n = m$ direm que $(a_{i,j})$ és una matriu quadrada d'ordre $n$.

**Notació 4.1.3** (Conjunt de matrius)**.** Siguin $m$ i $n$ dos enters, $\mathbb{K}$ un cos i

$$X = \{A \mid A \text{ és una matriu de mida } m \times n \text{ sobre } \mathbb{K}\}$$

un conjunt. Aleshores denotarem $X = M_{m\times n}(\mathbb{K})$.

Si $n = m$ denotarem $X = M_n(\mathbb{K})$.

**Definició 4.1.4** (Suma de matrius)**.** Siguin $A$ i $B$ dues matrius de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores definim la seva suma com una operació $+$ que satisfà

$$[A + B]_{i,j} = [A]_{i,j} + [B]_{i,j}.$$

**Definició 4.1.5** (Producte de matrius)**.** Siguin $A$ una matriu de mida $m \times l$ sobre un cos $\mathbb{K}$ i $B$ una matriu de mida $l \times n$ sobre un cos $\mathbb{K}$. Aleshores definim el seu producte com una operació $\cdot$ que satisfà

$$[A \cdot B]_{i,j} = \sum_{k=1}^{l} [A]_{i,k}[B]_{k,j}.$$

Escriurem $A \cdot B = AB$.

### 4.1.3 Propietats de les operacions amb matrius

**Proposició 4.1.6.** *Siguin $A$, $B$ i $C$ tres matrius de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$(A+B)+C = A+(B+C).$$

*Demostració.* Per la definició de suma de matrius (4.1.4) tenim que

$$\begin{aligned}
[(A+B)+C]_{i,j} &= [A+B]_{i,j} + [C]_{i,j} \\
&= [A]_{i,j} + [B]_{i,j} + [C]_{i,j} \\
&= [A]_{i,j} + ([B]_{i,j} + [C]_{i,j}) && \text{(cos (4.1.1))} \\
&= [A]_{i,j} + [B+C]_{i,j} \\
&= [A+(B+C)]_{i,j}. && \square
\end{aligned}$$

**Proposició 4.1.7.** *Siguin $A$ i $B$ dues matrius de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$A+B = B+A.$$

*Demostració.* Per la definició de suma de matrius (4.1.4) tenim que

$$\begin{aligned}
[A+B]_{i,j} &= [A]_{i,j} + [B]_{i,j} \\
&= [B]_{i,j} + [A]_{i,j} && \text{(cos (4.1.1))} \\
&= [B+A]_{i,j}. && \square
\end{aligned}$$

**Notació 4.1.8** (Matriu nul·la)**.** Denotarem la matriu de mida $m \times n$

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \in M_{m\times n}(\mathbb{K})$$

com $0_{m\times n}$, ó 0 si és clar pel context.

**Proposició 4.1.9.** *Sigui $A$ una matriu de mida $m\times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$A+0 = A.$$

*Demostració.* Per la definició de suma de matrius (4.1.4) tenim que

$$\begin{aligned}
[A+0]_{i,j} &= [A]_{i,j} + [0]_{i,j} \\
&= [A]_{i,j} + 0 \\
&= [A]_{i,j}, && \text{(cos (4.1.1))}
\end{aligned}$$

com volíem veure. $\square$

**Definició 4.1.10** (Producte d'una matriu per escalars)**.** Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$ i $\alpha$ un escalar de $\mathbb{K}$. Aleshores definim

$$[\alpha A]_{i,j} = \alpha [A]_{i,j}.$$

Denotarem $(-1)A$ com $-A$.

**Proposició 4.1.11.** *Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$A - A = 0.$$

*Demostració.* Per la definició de suma de matrius (4.1.4) tenim que

$$\begin{aligned} [A-A]_{i,j} &= [A]_{i,j} + [-A]_{i,j} \\ &= [A]_{i,j} - [A]_{i,j} \quad \text{(producte d'una matriu per escalars (4.1.10))} \\ &= 0 \quad \text{(cos (4.1.1))} \end{aligned}$$

i trobem $A - A = 0$. □

**Proposició 4.1.12.** *Siguin $A$ una matriu de mida $m \times n$ i $\alpha$ i $\beta$ dos escalars de $\mathbb{K}$. Aleshores*

$$(\alpha\beta)A = \alpha(\beta A).$$

*Demostració.* Per la definició de producte d'una matriu per escalars (4.1.10) tenim que

$$\begin{aligned} [(\alpha\beta)A]_{i,j} &= \alpha\beta[A]_{i,j} \\ &= \alpha(\beta[A_{i,j}]) \quad \text{(cos (4.1.1))} \\ &= \alpha[\beta A]_{i,j}. \end{aligned}$$ □

**Proposició 4.1.13.** *Siguin $A$ una matriu de mida $m \times n$ i $\alpha$ i $\beta$ dos escalars de $\mathbb{K}$. Aleshores*

$$(\alpha + \beta)A = \alpha A + \beta A.$$

*Demostració.* Per la definició de producte d'una matriu per escalars (4.1.10) tenim que

$$\begin{aligned} [(\alpha+\beta)A]_{i,j} &= (\alpha+\beta)[A]_{i,j} \\ &= \alpha[A]_{i,j} + \beta[A]_{i,j}, \quad \text{(cos (4.1.1))} \\ &= [\alpha A]_{i,j} + [\beta A]_{i,j}. \end{aligned}$$ □

**Proposició 4.1.14.** *Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$1A = A.$$

*Demostració.* Per la definició de producte d'una matriu per escalars (4.1.10) tenim que

$$\begin{aligned} [1A]_{i,j} &= 1[A]_{i,j} \\ &= [A]_{i,j}, \quad \text{(cos (4.1.1))} \end{aligned}$$

com volíem veure. □

**Proposició 4.1.15.** *Siguin $\mathbb{K}$ un cos i $A$ una matriu de mida $m \times l$ sobre $\mathbb{K}$, $B$ una matriu de mida $l \times s$ sobre $\mathbb{K}$ i $C$ una matriu de mida $s \times m$ sobre $\mathbb{K}$. Aleshores*

$$(AB)C = A(BC).$$

*Demostració.* Per la definició de producte de matrius (4.1.5) tenim que

$$\begin{aligned}
[(AB)C]_{i,j} &= \sum_{r=1}^{s} [AB]_{i,r}[C]_{r,j} \\
&= \sum_{r=1}^{s} \left( \sum_{k=1}^{l} [A]_{i,k}[B]_{k,r} \right) [C]_{r,j} \\
&= \sum_{r=1}^{s} \sum_{k=1}^{l} [A]_{i,k}[B]_{k,r}[C]_{r,j} && \text{(cos (4.1.1))} \\
&= \sum_{k=1}^{l} \sum_{r=1}^{s} [A]_{i,k}[B]_{k,r}[C]_{r,j} && \text{(cos (4.1.1))} \\
&= \sum_{k=1}^{l} [A]_{i,k} \sum_{r=1}^{s} ([B]_{k,r}[C]_{r,j}) && \text{(cos (4.1.1))} \\
&= \sum_{k=1}^{l} [A]_{i,k}[BC]_{k,j} \\
&= [A(BC)]_{i,j}. && \square
\end{aligned}$$

**Proposició 4.1.16.** *Siguin $A$ i $A'$ dues matrius de mida $m \times l$ sobre un cos $\mathbb{K}$ i $B$, $B'$ dues matrius de mida $l \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$(A + A')B = AB + A'B \quad i \quad A(B + B') = AB + AB'.$$

*Demostració.* Per la definició de producte de matrius (4.1.5) tenim que

$$\begin{aligned}
[(A + A')B]_{i,j} &= \sum_{k=1}^{l} [A + A']_{i,k}[B]_{k,j} \\
&= \sum_{k=1}^{l} ([A]_{i,k} + [A']_{i,k})[B]_{k,j} && \text{(suma de matrius (4.1.4))} \\
&= \sum_{k=1}^{l} ([A]_{i,k}[B]_{k,j} + [A']_{i,k}[B]_{k,j}) && \text{(cos (4.1.1))} \\
&= \sum_{k=1}^{l} [A]_{i,k}[B]_{k,j} + \sum_{k=1}^{l} [A']_{i,k}[B]_{k,j} && \text{(cos (4.1.1))} \\
&= [AB]_{i,j} + [A'B]_{i,j} \\
&= [AB + AB']_{i,j}, && \text{(suma de matrius (4.1.4))}
\end{aligned}$$

i

$$\begin{aligned}
[A(B+B')]_{i,j} &= \sum_{k=1}^{l}[A]_{i,k}[B+B']_{k,j} \\
&= \sum_{k=1}^{l}[A]_{i,k}([B]_{k,j}+[B']_{k,j}) && \text{(suma de matrius (4.1.4))} \\
&= \sum_{k=1}^{l}([A]_{i,k}[B]_{k,j}+[A]_{i,k}[B']_{k,j}) && \text{(cos (4.1.1))} \\
&= \sum_{k=1}^{l}[A]_{i,k}[B]_{k,j}+\sum_{k=1}^{l}[A]_{i,k}[B]_{k,j} && \text{(cos (4.1.1))} \\
&= [AB]_{i,j}+[AB']_{i,j} \\
&= [AB+AB']_{i,j}, && \text{(suma de matrius (4.1.4))}
\end{aligned}$$

com volíem veure. □

### 4.1.4 Matrius inverses i matrius transposades

**Notació 4.1.17** (Matriu identitat)**.** Denotarem la matriu d'ordre $n$

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \in M_n(\mathbb{K})$$

com $I_n$ i direm que $I_n$ és la matriu identitat d'ordre $n$.

**Proposició 4.1.18.** *Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$I_m A = A = AI_n.$$

*Demostració.* Per la definició de producte de matrius (4.1.5) tenim que

$$[I_m A]_{i,j} = \sum_{k=1}^{m}[I_m]_{i,k}[A]_{k,j}.$$

Ara bé, tenim que

$$[I_m]_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

i per la definició de cos (4.1.1) tenim que

$$\sum_{k=1}^{m}[I_m]_{i,k}[A]_{k,j} = [A]_{i,j}$$

i per tant $I_m A = A$.

La demostració de l'altre igualtat és anàloga. □

**Proposició 4.1.19.** *Sigui $A$ una matriu d'ordre $n$ sobre un cos $\mathbb{K}$ tal que existeixin dues matrius $A_1$ i $A_2$ d'ordre $n$ sobre $\mathbb{K}$ tal que*

$$AA_1 = A_1A = I_n \quad i \quad AA_2 = A_2A = I_m.$$

*Aleshores $A_1 = A_2$.*

*Demostració.* Per la proposició 4.1.15 tenim que

$$A_1(AA_2) = (A_1A)A_2$$

i per hipòtesi trobem que $A_1I_m = I_mA_2$, i per la proposició 4.1.18 trobem que $A_1 = A_2$, com volíem veure. □

**Definició 4.1.20** (Matriu invertible)**.** Sigui $A$ una matriu d'ordre $n$ sobre un cos $\mathbb{K}$ tal que existeixi una matriu $A'$ d'ordre $n$ sobre $\mathbb{K}$ tal que

$$AA' = A'A = I_n.$$

Aleshores direm que $A$ és una matriu invertible i que $A'$ és la inversa de $A$. També denotarem $A' = A^{-1}$.

Observem que aquesta definició té sentit per la proposició 4.1.19.

**Proposició 4.1.21.** *Siguin $A$ i $B$ dues matrius invertibles d'ordre $n$ sobre un cos $\mathbb{K}$. Aleshores*

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

*Demostració.* Per la definició de matriu invertible (4.1.20) tenim que

$$(AB)^{-1}AB = I_n,$$

i com que, per hipòtesi, les matrius $A$ i $B$ són invertibles trobem

$$\begin{aligned} B^{-1}A^{-1} &= (AB)^{-1}ABB^{-1}A^{-1} \\ &= (AB)^{-1}AA^{-1} \\ &= (AB)^{-1}. \end{aligned}$$

□

**Proposició 4.1.22.** *Sigui $A$ una matriu invertible d'ordre $n$ sobre un cos $\mathbb{K}$. Aleshores*

$$(A^{-1})^{-1} = A.$$

*Demostració.* Per la proposició 4.1.21 tenim que

$$A^{-1}(A^{-1})^{-1} = A^{-1}A$$

i com que, per hipòtesi, la matriu $A$ és invertible trobem

$$AA^{-1}(A^{-1})^{-1} = AA^{-1}A$$

i tenim

$$(A^{-1})^{-1} = A.$$

□

**Definició 4.1.23** (Matriu transposada)**.** Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Definim la transposada de $A$ com una matriu $A^t$ de mida $n \times m$ sobre $\mathbb{K}$ que satisfà

$$[A^t]_{i,j} = [A]_{j,i}.$$

**Proposició 4.1.24.** *Siguin $A$ i $B$ dues matrius de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores*

$$(A+B)^t = A^t + B^t.$$

*Demostració.* Per la definició de matriu transposada (4.1.23) tenim que

$$\begin{aligned}
[(A+B)^t]_{i,j} &= [A+B]_{j,i} \\
&= [A]_{j,i} + [B]_{j,i} && \text{(suma de matrius (4.1.4))} \\
&= [A^t]_{i,j} + [B^t]_{i,j} \\
&= [A^t + B^t]_{i,j}, && \text{(suma de matrius (4.1.4))}
\end{aligned}$$

com volíem veure. □

**Proposició 4.1.25.** *Siguin $A$ una matriu de mida $m \times l$ sobre un cos $\mathbb{K}$ i $B$ una matriu de mida $l \times n$ sobre $\mathbb{K}$. Aleshores*

$$(AB)^t = B^t A^t.$$

*Demostració.* Per la definició de matriu transposada (4.1.23) tenim que

$$\begin{aligned}
[(AB)^t]_{i,j} &= [AB]_{j,i} \\
&= \sum_{k=1}^{l} [A]_{j,k}[B]_{k,i} && \text{(producte de matrius (4.1.5))} \\
&= \sum_{k=1}^{l} [A^t]_{k,j}[B]_{i,k} \\
&= \sum_{k=1}^{l} [B^t]_{i,k}[A^t]_{k,j} && \text{(cos (4.1.1))} \\
&= [B^t A^t]_{i,j}, && \text{(cos (4.1.1))}
\end{aligned}$$

com volíem veure. □

**Definició 4.1.26** (Matriu simètrica)**.** Sigui $A$ una matriu d'ordre $n$ sobre un cos $\mathbb{K}$ tal que $A^t = A$. Aleshores direm que $A$ és una matriu simètrica.

### 4.1.5 Producte de matrius en blocs

**Definició 4.1.27** (Files i columnes)**.** Sigui $A = (a_{i,j})$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores definim

$$F_i = \begin{bmatrix} a_{i,1} & \cdots & a_{i,n} \end{bmatrix}$$

com la $i$-èsima fila de $A$ i

$$C_i = \begin{bmatrix} a_{1,i} \\ \vdots \\ a_{m,i} \end{bmatrix}$$

com la $i$-èsima columna de $A$.

**Observació 4.1.28.** *Si $A \in M_{m\times n}(\mathbb{K})$ tenim $F_i \in M_{1\times n}(\mathbb{K})$ i $C_i \in M_{m\times 1}(\mathbb{K})$.*

**Notació 4.1.29.** Si $A$ és una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$, $F_1, \dots, F_m$ les files de $A$ i $C_1, \dots, C_n$ les columnes de $A$. Aleshores denotem

$$A = \begin{bmatrix} F_1 \\ \vdots \\ F_m \end{bmatrix} = \begin{bmatrix} C_1 & \cdots & C_n \end{bmatrix}.$$

**Notació 4.1.30.** Siguin $A = (a_{i,j})$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$, $m_1, \dots, m_p$ i $n_1, \dots, n_q$ nombres naturals tals que $m_1 + \cdots + m_p = m$ i $n_1 + \cdots + n_q = n$, $m_0 = n_0 = 1$ i

$$A_{i,j} = \begin{bmatrix} a_{m_{i-1},n_{i-1}} & \cdots & a_{m_{i-1},n_i} \\ \vdots & & \vdots \\ a_{m_i,n_{i-1}} & \cdots & a_{m_i,n_i} \end{bmatrix}$$

matrius sobre un cos $\mathbb{K}$. Aleshores denotem

$$A = \begin{bmatrix} A_{1,1} & \cdots & A_{1,q} \\ \vdots & & \vdots \\ A_{p,1} & \cdots & A_{p,q} \end{bmatrix}.$$

**Proposició 4.1.31.** *Siguin $A$ una matriu de mida $m \times l$ sobre un cos $\mathbb{K}$, $B$ una matriu de mida $l \times n$ sobre $\mathbb{K}$, $m_1, \dots, m_p$, $l_1, \dots, l_q$ i $n_1, \dots, n_r$ nombres naturals satisfent $m_1 + \cdots + m_p = m$, $l_1 + \cdots + l_q = l$ i $n_1 + \cdots + n_r = n$, i per a tot $i \in \{1, \dots, p\}$, $k \in \{1, \dots, q\}$ i $j \in \{1, \dots, r\}$ tals que $A_{i,k}$ és una matriu de mida $m_i \times l_k$ sobre $\mathbb{K}$ i $B_{k,j}$ és una matriu de mida $l_k \times n_j$ sobre $\mathbb{K}$ tals que*

$$A = \begin{bmatrix} A_{1,1} & \cdots & A_{1,q} \\ \vdots & & \vdots \\ A_{p,1} & \cdots & A_{p,q} \end{bmatrix} \quad i \quad B = \begin{bmatrix} B_{1,1} & \cdots & B_{1,r} \\ \vdots & & \vdots \\ B_{q,1} & \cdots & B_{q,r} \end{bmatrix}.$$

*Aleshores*

$$AB = \begin{bmatrix} \sum_{k=1}^q A_{1,k}B_{k,1} & \sum_{k=1}^q A_{1,k}B_{k,2} & \cdots & \sum_{k=1}^q A_{1,k}B_{k,r} \\ \sum_{k=1}^q A_{2,k}B_{k,1} & \sum_{k=1}^q A_{2,k}B_{k,2} & \cdots & \sum_{k=1}^q A_{2,k}B_{k,r} \\ \vdots & \vdots & & \vdots \\ \sum_{k=1}^q A_{p,k}B_{k,2} & \sum_{k=1}^q A_{p,k}B_{k,2} & \cdots & \sum_{k=1}^q A_{p,k}B_{k,r} \end{bmatrix}.$$

*Demostració.* Per la definició de producte de matrius (4.1.5) tenim que

$$[AB]_{i,j} = \sum_{k=1}^{l} [A]_{i,k}[B]_{k,j}.$$

També tenim que $i = m_1 + \cdots + m_{k_i} + i'$ i $j = n_1 + \cdots + n_{k_j} + j'$ per a certs $k_i \in \{1, \dots, p-1\}$, $k_j \in \{1, \dots, r-1\}$, $i' \leq m_{k_i+1} - m_{k_i}$ i $j' \leq n_{k_j+1} - n_{k_j}$. Per tant hem de veure que

$$\sum_{k=1}^{l} [A]_{i,k}[B]_{k,j} = \left[ \sum_{k=1}^{q} A_{m_{k_i},k} B_{k,n_{k_j}} \right]_{i',j'}.$$

Per la definició de suma de matrius (4.1.4) tenim que

$$\left[\sum_{k=1}^{q} A_{m_{k_i},k}B_{k,n_{k_j}}\right]_{i',j'} = \sum_{k=1}^{q}[A_{m_{k_i},k}B_{k,n_{k_j}}]_{i',j'},$$

i per la definició de producte de matrius (4.1.5) trobem

$$\sum_{k=1}^{q}[A_{m_{k_i},k}B_{k,n_{k_j}}]_{i',j'} = \sum_{k=1}^{q}\left(\sum_{h=1}^{l_k}[A_{m_{k_i},k}]_{i',h}[B_{k,n_{k_j}}]_{h,j'}\right).$$

Ara bé, com que per hipòtesi tenim que

$$A = \begin{bmatrix} A_{1,1} & \cdots & A_{1,q} \\ \vdots & & \vdots \\ A_{p,1} & \cdots & A_{p,q} \end{bmatrix} \quad \text{i} \quad B = \begin{bmatrix} B_{1,1} & \cdots & B_{1,r} \\ \vdots & & \vdots \\ B_{q,1} & \cdots & B_{q,r} \end{bmatrix}.$$

i que $i = m_1 + \cdots + m_{k_i} + i'$ i $j = n_1 + \cdots + n_{k_j} + j'$, trobem

$$\sum_{k=1}^{q}\left(\sum_{h=1}^{l_k}[A_{m_{k_i},k}]_{i',h}[B_{k,n_{k_j}}]_{h,j'}\right) = \sum_{k=1}^{l}[A]_{i,k}[B]_{k,j}. \qquad \square$$

## 4.2 Rang d'una matriu

### 4.2.1 Transformacions elementals

**Definició 4.2.1** (Transformacions elementals)**.** Siguin $A = (a_{i,j})$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$ i $i$ i $j$ dos naturals amb $i, j \leq m$. Aleshores definim les funcions

$$P_{i,j}(A) = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ a_{j,1} & \cdots & a_{j,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{j-1,1} & \cdots & a_{j-1,n} \\ a_{i,1} & \cdots & a_{i,n} \\ a_{j+1,1} & \cdots & a_{j+1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}, \quad D_{i,\lambda}(A) = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ \lambda a_{i,1} & \cdots & \lambda a_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$$

$$\text{i} \quad E_{i,j,\lambda}(A) = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ a_{i,1} - \lambda a_{j,1} & \cdots & a_{i,n} - \lambda a_{j,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{m,1} & & a_{m,n} \end{bmatrix}$$

com les transformacions elementals per files de $M_n(\mathbb{K})$.

**Proposició 4.2.2.** *Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores per a tota successió de transformacions elementals per files $f$ existeix una matriu $P$ de mida $m \times m$ sobre $\mathbb{K}$ tal que $f(A) = PA$ i per a tota successió de transformacions elementals per columnes $g$ existeix una matriu $Q$ de mida $n \times n$ sobre $\mathbb{K}$ tal que $g(A) = AQ$.*

*Demostració.* En tenim prou amb veure que $P_{i,j}(A) = P_{i,j}(I_m)A$, $D_{i,\lambda}(A) = D_{i,\lambda}(I_m)A$ i $E_{i,j,\lambda}(A) = E_{i,j,\lambda}(I_m)A$ i que $P_{i,j}(A^t)^t = AP_{i,j}(I_n)$, $D_{i,\lambda}(A^t)^t = AD_{i,\lambda}(I_n)$ i $E_{i,j,\lambda}(A^t)^t = AE_{i,j,\lambda}(I_n)$, i això és conseqüència de la definició de producte de matrius (4.1.5). □

**Notació 4.2.3.** Denotarem les transformacions elementals per files $P_{i,j}$ com $F_i \leftrightarrow F_j$, $D_{i,\lambda}$ com $F_i \to \lambda F_i$ i $E_{i,j,\lambda}$ com $F_i \to F_i + \lambda F_j$.

Aprofitant la proposició 4.2.2 també denotarem una successió de transformacions elementals com una matriu quadrada.

Si apliquem una transformació elemental per files a una matriu transposada i transposem el resultat denotarem $P_{i,j}$ com $C_i \leftrightarrow C_j$, $D_{i,\lambda}$ com $C_i \to \lambda C_i$ i $E_{i,j,\lambda}$ com $C_i \to C_i + \lambda C_j$ i direm que són transformacions elementals per columnes.

### 4.2.2 Matrius esglaonades i mètode de Gauss

**Definició 4.2.4** (Matriu esglaonada)**.** Sigui $A = (a_{i,j})$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$ tal que existeixen $j_1 < \cdots < j_r$ nombres naturals tals que per a tot $i \in \{1, \ldots, r\}$ i per a tot $j < j_i$ tenim $a_{i,j} = 0$ i $a_{i,j_i} \neq 0$, i $a_{i,j} = 0$ per a tot $i > j_r$ i $j \in \{1, \ldots, n\}$.

Aleshores direm que $A$ està esglaonada per files i que $A^t$ està esglaonada per columnes.

Direm que una matriu $A$ es pot esglaonar per files si existeix una successió $P$ de transformacions elementals per files tals que $PA$ està esglaonada per files.

**Proposició 4.2.5.** *Sigui $A$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores $A$ es pot esglaonar per files.*

*Demostració.* □

# Part III

# Coses per fer a l'estiu

# Capítol 5

# Aviat

Podeu trobar la versió actualitzada d'aquest pdf seguint aquest link.

## 5.1 Àlgebra lineal

### 5.1.1 Definicions

**Definició 5.1.1** (Forma bilineal definida estrictament positiva o negativa)**.** Sigui $M$ una forma bilineal simètrica. Preguntar a en Cedò.

**Definició 5.1.2** (Norma d'una aplicació lineal)**.**

### 5.1.2 Proposicions

**Proposició 5.1.3.** *Vectors linealment independents $\Leftrightarrow$ determinant no nul.*

### 5.1.3 Teoremes

**Teorema 5.1.4.** *Sigui $A = (a_{i,j}) \in M_n(\mathbb{R})$ una matriu simètrica. Aleshores $A$ és definida positiva si i només si*

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,i} \\ \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,i} \end{vmatrix} > 0$$

*per a tot $i \in \{1, \ldots, n\}$.*

*Demostració.* Per inducció sobre $n$. □

## 5.2 Funcions de variable real

### 5.2.1 Definicions

**Definició 5.2.1** (Funció contínua)**.** Sigui $f$ una funció. Direm que $f$ és contínua en $a$ si

$$\lim_{x \to a} f(x) = f(a).$$

**Definició 5.2.2** (Partició, poligonal i longitud d'una poligonal)**.** Sigui $(a, b)$ un interval de $\mathbb{R}$. Direm que una partició de $(a, b)$ és un conjunt de escalars $t_0, \ldots, t_n \in [a, b]$ que compleixen $a = t_0 < \cdots < t_n = b$. Direm que $t_0, \ldots, t_n$ són els nodes de la partició.

Sigui $f\colon (a, b) \to \mathbb{R}^m$ una funció. Definirem la poligonal $P_n$ d'una partició en una funció $f$ com

$$P_n = f(t_0), \ldots, f(t_n).$$

Definim la longitud de la poligonal $P_n$ com

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\|.$$

**Definició 5.2.3** (Classe de diferenciabilitat d'una funció)**.** Sigui $f$ una funció $n$-vegades diferenciable amb $f^{(n)}$ contínua. Direm que $f$ és de classe $\mathcal{C}^n$ o que $f \in \mathcal{C}^n$.

**Definició 5.2.4** (Funció monòtona)**.** Sigui $f\colon [a, b] \to \mathbb{R}$ una funció. Direm que és $f$ és monòtona si, per a qualsevol $x, y \in [a, b]$, $x > y$ implica $f(x) \geq f(y)$.

**Definició 5.2.5** (Notació de Landau)**.** $A(h) = \mathrm{o}(B(h)) \ldots$

### 5.2.2 Proposicions

**Proposició 5.2.6.** *Siguin $I \subseteq \mathbb{R}$ un interval i $f\colon I \to \mathbb{R}$ una funció. Aleshores, si $f$ és derivable en un punt $a \in I$, $f$ és contínua en $a$.*

**Proposició 5.2.7.** *Sigui $f\colon [a, b] \to \mathbb{R}$ una funció acotada i monòtona. Aleshores $f$ és integrable Riemann.*

### 5.2.3 Teoremes

**Teorema 5.2.8** (Equivalència entre normes)**.** *Si $q(x)$ és una norma existeixen $m, M \in \mathbb{R}^+$ tals que $m\|x\| \leq q(x) \leq M\|x\|$ per a tot $x \in \mathbb{R}^m$.*

**Teorema 5.2.9** (Teorema del Valor Mig)**.** hmm trivial

**Teorema 5.2.10** (Desigualtat de Cauchy-Schwarz)**.**

**Teorema 5.2.11** (Teorema de Taylor)**.** *Siguin $(a, b)$ un interval obert de $\mathbb{R}$ i $f\colon (a, b) \to \mathbb{R}$ una funció de classe $\mathcal{C}^n$. Aleshores, per a dos punts $x, c \in (a, b)$, amb $x < c$, existeix un punt $x_1 \in (x, c)$ tal que*

$$f(x) = f(c) + \sum_{k=1}^{n-1} \frac{f^{(k)}(c)}{k!}(x - c)^k + \frac{f^{(n)}(x_1)}{n!}(x - c)^n.$$

**Teorema 5.2.12** (Teorema de Weierstrass)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció. Aleshores, donat un compacte $S \subset U$, si $f$ és contínua en $S$, $f$ té un màxim i un mínim absoluts en $S$.*

**Teorema 5.2.13** (Teorema del sandvitx)**.**

**Teorema 5.2.14** (Teorema de Rolle)**.** *Sigui $f\colon [a, b] \subset \mathbb{R} \longrightarrow \mathbb{R}$ una funció derivable en $(a, b)$ tal que $f(a) = f(b)$. Aleshores existeix un cert $c \in (a, b)$ tal que $f'(c) = 0$.*

## 5.3 Trobar lloc per tot això

**Definició 5.3.1** (Conjunt obert, tancat...)**.**

**Definició 5.3.2** (Continuïtat uniforme)**.** Siguin $U \subseteq \mathbb{R}^d, V \subseteq \mathbb{R}^m$ dos oberts i $f\colon U \to V$ una funció. Aleshores direm que $f$ és uniformement contínua en un conjunt $S \subseteq U$ si per a tot $\varepsilon > 0$ existeix un $\delta > 0$ tals que

$$d_U(x, y) < \varepsilon \text{ i } d_V(f(x) - f(y)) < \delta$$

per a tot punt $x, y \in U$.

**Teorema 5.3.3** (Teorema de Heine)**.** *Siguin $U \subseteq \mathbb{R}^d$ dos oberts, $S \subset U$ un compacte i $f\colon U \to \mathbb{R}^m$ una funció contínua. Aleshores $f$ és uniformement contínua en $S$.*

**Definició 5.3.4** (Funció indicatriu)**.** Siguin $X$ un conjunt i $A \subseteq X$ un subconjunt de $X$. Definim la funció indicatriu de $A$ com una funció

$$1_A\colon X \longrightarrow \{0, 1\}$$

tal que

$$1_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

# Part IV

# Càlcul en diverses variables i optimització

# Capítol 6

# Càlcul diferencial

## 6.1 Arcs i conjunts connexos

### 6.1.1 Arcs en múltiples variables

**Definició 6.1.1** (Arcs a l'espai)**.** Siguin $(a,b) \subseteq \mathbb{R}$ un interval, $f\colon (a,b) \to \mathbb{R}^m$ una funció i $\Gamma$ el conjunt definit per

$$\Gamma = \{x \in \mathbb{R}^m \mid x = f(t) \text{ per a tot } t \in (a,b)\},$$

aleshores direm que $\Gamma$ és un arc a $\mathbb{R}^m$. També direm que $f$ defineix o recorre aquest arc. Així mateix donem les següents definicions:

1. Direm que $\Gamma$ és un arc continu si $f$ és contínua en $(a,b)$.
2. Direm que $\Gamma$ és un arc simple si $f$ és injectiva en $(a,b)$.
3. Si $f$ està definida en $[a,b]$ direm que $f$ va de $f(a)$ a $f(b)$ o que $f(a)$ n'és el punt inicial i $f(b)$ el punt final. Si $f(a) = f(b)$ direm que $\Gamma$ és un arc tancat.
4. Direm que $\Gamma$ és un arc regular si $f$ és derivable en $(a,b)$.
5. Direm que $\Gamma$ és un arc de classe $\mathcal{C}^n$ si $f^{(n)}$ existeix i és contínua en $(a,b)$.

**Definició 6.1.2** (Longitud d'un arc continu)**.** Sigui $\Gamma$ un arc continu i $f$ una manera de recórrer $\Gamma$ donada per

$$f\colon (a,b) \subseteq \mathbb{R} \longrightarrow \mathbb{R}^m$$

Amb $m \in \mathbb{N}$, $m > 1$.

Considerem la partició $a = t_0 < \cdots < t_n = b$. Observem que els punts donats per $f(t_i)$ per a tot $i \in \{0,\ldots,n\}$ determinen una poligonal, $P_n$, la longitud de la qual és, per la definició de longitud d'una poligonal (5.2.2)

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\|.$$

Aleshores definim la longitud de $f$ com

$$\mathrm{L}(f) = \lim_{n\to\infty} \mathrm{L}(P_n).$$

Direm que els arcs amb recorreguts de longitud finita són arcs rectificables.

**Proposició 6.1.3.** *Sigui $\Gamma$ un arc de classe $\mathcal{C}^1$. Aleshores $\Gamma$ és rectificable.*

*Demostració.* Sigui $f$ una funció que recorre $\Gamma$ tal que

$$\begin{aligned} f\colon (a,b) \subseteq \mathbb{R} &\longrightarrow \mathbb{R}^m \\ t &\longmapsto (x_1(t), \dots, x_m(t)). \end{aligned}$$

Donada una partició de $(a,b)$, $a = t_0 < \cdots < t_n = b$ que defineix una poligonal $P_n = f(t_0), \dots, f(t_n)$. Aleshores la longitud de la poligonal és, per la definició de partició (5.2.2),

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\| = \sum_{i=0}^{n-1} \sqrt{\sum_{j=1}^{m} (x_j(t_{i+1}) - x_j(t_i)))^2}.$$

Per la proposició 5.2.6 $f$ és contínua en $(a,b)$, i per tant pel Teorema del Valor Mig (5.2.9) tenim

$$x_j(t_{i+1}) - x_j(t_i) = x_j'(\xi_{ij})(t_{i+1} - t_i),$$

amb $t_i < \xi_{ij} < t_{i+1}$, per a tot $i \in \{0, \dots, n-1\}$, $j \in \{1, \dots, m\}$. Per tant

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{m} \big(x_j'(\xi_{ij})\big)^2}. \tag{6.1}$$

Ara volem veure que $\xi_{ij} = \xi_i$ quan $n$ tendeix a infinit. Observem que

$$\lim_{n\to\infty} t_i = \lim_{n\to\infty} t_{i+1}.$$

I com que $t_i < \xi_{ij} < t_{i+1}$ tenim que $\xi_{ij} = \xi_i$ per a tot $j \in \{1, \dots, m\}$. Així veiem que si $n \to \infty$ podem reescriure (6.1) com

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) \|f'(\xi_i)\| = \int_a^b \|f'(t)\| \mathrm{d}t.$$

I ja hem acabat. Com que $f \in \mathcal{C}^1$ tenim $f'$ contínua, i $a, b \in \mathbb{R}$, aquesta integral és finita i $\Gamma$ és rectificable, com volíem veure. □

### 6.1.2 Oberts connexos

**Definició 6.1.4** (Conjunt arc-connex o connex)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert. Direm que $U$ és arc-connex si donats dos punts $P, Q \in U$ existeix una funció $f$ que defineix un arc continu tal que $f\colon [a,b] \longrightarrow U$ amb $P = f(a)$, $Q = f(b)$. Direm que $U$ és connex si el segment que els uneix està tot dins $U$.

**Proposició 6.1.5.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $U_1$, $U_2$ dos subconjunts de $U$ arc-connexos amb $U_1 \cup U_2 = U$ tals que $U_1 \cap U_2 \neq \emptyset$. Aleshores $U$ és arc-connex.*

*Demostració.* Siguin $P, Q$ dos punts en $U$ tals que $P \in U_2^{\complement}$ i $Q \in U_1^{\complement}$, i $R \in U_1 \cap U_2$ un altre punt. Com que $U_1$ i $U_2$ són arc-connexos, per la definició de conjunt arc-connex (6.1.4) existeixen dos arcs continus $f, g$ tals que

$$f\colon [a,b] \longrightarrow U_1, \quad g\colon [b,c] \longrightarrow U_2,$$

on $f(a) = P$, $f(b) = g(b) = R$ i $g(c) = Q$. Aleshores definim la funció

$$h(t) = \begin{cases} f(t) & \text{si } a \leq t \leq b \\ g(t) & \text{si } b < t \leq b. \end{cases}$$

Tenim que $h$ defineix un arc continu en $U$, i per la definició de longitud d'un arc continu (6.1.2), $U$ és arc-connex. □

**Definició 6.1.6** (Distància en un arc-connex)**.** Sigui $U \subseteq \mathbb{R}^d$ un arc-connex, siguin $P, Q \in U$ i $F$ el conjunt de totes les funcions $f$ que defineixen un arc continu en $U$ amb $f(a) = P$, $f(b) = Q$. Definim la distància entre $P$ i $Q$ en $U$ com

$$\mathrm{d}_U(P, Q) = \inf_{f \in F} \mathrm{L}(f).$$

**Observació 6.1.7.** *Notem que si $U$ és connex $\mathrm{d}_U(P, Q) = \|P - Q\|$.*

**Proposició 6.1.8.** *Siguin $U \subseteq \mathbb{R}^d$ un arc-connex i $P, Q, R \in U$ tres punts. Aleshores*

1. $\mathrm{d}_U(P, Q) = \mathrm{d}_U(Q, P) \geq 0$
2. $\mathrm{d}_U(P, Q) = 0 \iff P = Q$
3. $\mathrm{d}_U(P, Q) \leq \mathrm{d}_U(P, R) + \mathrm{d}_U(R, Q)$ *(desigualtat triangular)*

*Demostració.* Sigui $f\colon [a, b] \to U$ una funció contínua amb $f(a) = P$ i $f(b) = Q$, i amb $\mathrm{L}(f) = \inf_{f \in F} \mathrm{L}(f)$, on $F$ és el conjunt de funcions contínues de $[a, b]$ en $U$ que van de $P$ a $Q$.

Per veure el punt (1) fem

$$\begin{aligned}
\mathrm{d}_U(P, Q) &= \inf_{f \in F} \mathrm{L}(f) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left( \sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij})\right)^2} \right) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left( \sum_{i=0}^{n-1} (-1)(t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij})\right)^2} \right) \\
&= \inf_{f \in F} (-1) \lim_{n \to \infty} \left( \sum_{i=0}^{n-1} (t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij})\right)^2} \right) \\
&= \inf_{f \in F} (-1) \int_a^b \|f'(t)\| \mathrm{d}t \\
&= \inf_{f \in F} \int_b^a \|f'(t)\| \mathrm{d}t = \inf_{f \in F} \mathrm{L}(f) = \mathrm{d}_U(Q, P) \geq 0.
\end{aligned}$$

Continuem veient el punt (2). Suposem $P = Q$ i considerem, amb $\varepsilon > 0$, la bola oberta $\mathrm{B}(\varepsilon, P) \subset U$. Aquesta bola és connexa i, pel corol·lari 6.1.7, $\mathrm{d}_U(P, Q) = \|P - Q\| = 0 \iff P = Q$.

Acabem veient el punt (3). Sigui $F_1$ el conjunt de funcions contínues en $U$ que van de $P$ a $R$ i $F_2$ el conjunt de funcions contínues en $U$ que van de $R$ a $Q$. Aleshores

$$\mathrm{d}_U(P,Q) = \inf_{f\in F} \mathrm{L}(f) \leq \inf\left(\inf_{F_1} \mathrm{L}(g) + \inf_{F_2} \mathrm{L}(h)\right) = \mathrm{d}_U(P,R) + \mathrm{d}_U(R,Q).$$

Observem que aquestes són les mateixes propietats de una distància. □

## 6.2 Funcions diferenciables

### 6.2.1 Diferencial d'una funció en múltiples variables

**Definició 6.2.1** (Derivada direccional)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert, $t \in \mathbb{R}$ un escalar, $a \in U$ un punt, $\vec{u}$ un vector de $\mathbb{R}^d$ i $f$ una funció definida per

$$\begin{aligned} f\colon U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \ldots, f_m(a)), \end{aligned}$$

i considerem, per a tot $i \in \{1, \ldots, m\}$, els límits

$$D_{\vec{u}} f_i(a) = \lim_{t\to 0} \frac{f_i(a + t\vec{u}) - f_i(a)}{t}.$$

Si tots aquests límits existeixen, direm que la derivada de $f$ en direcció $\vec{u}$ és

$$D_{\vec{u}} f(a) = (D_{\vec{u}} f_1(a), \ldots, D_{\vec{u}} f_m(a)).$$

Si $\vec{u}$ és l'$i$-èsim vector de la base canònica utilitzarem la notació $D_i f(a)$.

**Proposició 6.2.2.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}^m$ una funció, $D_{\vec{u}} f(a)$ la seva derivada direccional respecte el vector $\vec{u}$ de $\mathbb{R}^d$ i $\lambda \in \mathbb{R}$ un escalar. Aleshores*

$$D_{\lambda\vec{u}} f(a) = \lambda D_{\vec{u}} f(a).$$

*Demostració.* Tenim que, per a tot $i \in \{1, \ldots, m\}$,

$$\begin{aligned} D_{\lambda\vec{u}} f_i(a) &= \lim_{t\to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{t} \\ &= \lim_{t\to 0} \lambda \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} \\ &= \lambda \lim_{t\to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} = \lambda D_{\vec{u}} f_i(a). \end{aligned}$$ □

**Definició 6.2.3** (Diferencial d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^m$ una funció i $a \in U$ un punt. Direm que el diferencial de $f$ en $a$ és una aplicació lineal $df(a)\colon U \to \mathbb{R}^m$ tal que, donat un vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a + \vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Direm que $f$ és diferenciable en $a$ si existeix aquest $df(a)$.

**Observació 6.2.4.** *Observem que en aquesta definició, si $d = 1$, $f$ és diferenciable en $a \iff f$ és derivable en $a$, i $df(a)(\vec{h}) = \vec{h} f'(a)$ (Si $d = 1$, multiplicar per un vector de $\mathbb{R}$ és com multiplicar per un escalar).*

**Proposició 6.2.5.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores $f$ és contínua en $a$.*

*Demostració.* Sigui $df(a)$ el diferencial de $f$ en $a$. Per la definició de diferencial d'una funció (6.2.3) tenim que, per a qualsevol vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a+\vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Com que $df(a)$ és lineal, $df(a)(\vec{h}) \to (0,\dots,0) \Leftrightarrow \|\vec{h}\| \to 0$. Així veiem que

$$\lim_{\|\vec{h}\|\to 0} f(a+\vec{h}) - f(a) - df(a)(\vec{h}) = \mathrm{o}(\vec{h}).$$

I això compleix la definició de funció contínua (5.2.1), per tant $f$ és contínua en el punt $a$. □

**Proposició 6.2.6.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt i $f$ una funció tal que*

$$\begin{aligned} f\colon U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a),\dots,f_m(a)). \end{aligned}$$

*Aleshores*

$$f \text{ és diferenciable en } a \Leftrightarrow f_i \text{ és diferenciable en } a \ \forall i \in \{1,\dots,m\}.$$

*Demostració.* Per la definició de diferencial d'una funció (6.2.3) tenim que, per a qualsevol vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a+\vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

El que és equivalent a

$$\lim_{\|\vec{h}\|\to 0} \frac{f(a+\vec{h}) - f(a) - df(a)(\vec{h})}{\|\vec{h}\|} = 0.$$

Sabent que $f(a) = (f_1(a),\dots,f_m(a))$ podem entendre aquest límit com el següent, amb un vector al numerador, que descomponem com

$$\lim_{\|\vec{h}\|\to 0} \frac{(f_1(a+\vec{h}) - f_1(a) - df_1(a)(\vec{h}),\dots,f_m(a+\vec{h}) - f_m(a) - df_m(a)(\vec{h}))}{\|\vec{h}\|} = 0$$

si i només si

$$\lim_{\|\vec{h}\|\to 0} \frac{f_i(a+\vec{h}) - f_i(a) - df_i(a)(\vec{h})}{\|\vec{h}\|} = 0$$

per a tot $i \in \{1,\dots,m\}$.

Tenint en compte la definició de diferencial d'una funció (6.2.3), és equivalent a dir que, per a tot $i \in \{1,\dots,m\}$, $f_i$ és diferenciable en el punt $a$. □

**Proposició 6.2.7.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores tenim que*

1. *Donat un vector $\vec{u}$ de $\mathbb{R}^d$, $D_{\vec{u}}f(a)$ existeix i $df(a)(\vec{u}) = D_{\vec{u}}f(a)$.*

*2. El diferencial de $f$ en $a$, $df(a)$, és únic.*

*Demostració.* Sigui $\vec{u}$ un vector de $\mathbb{R}^d$. Tenim que, si $\lambda \in \mathbb{R}$, $\lambda \neq 0$

$$f(a+\lambda\vec{u}) = f(a) + df(a)(\lambda\vec{u}) + \mathrm{o}(\lambda\vec{u})$$

$$f(a+\lambda\vec{u}) - f(a) = \lambda df(a)(\vec{u}) + \mathrm{o}(\lambda\vec{u})$$

$$\frac{f(a+\lambda\vec{u}) - f(a)}{\lambda} = df(a)(\vec{u}) + \frac{\mathrm{o}(\lambda\vec{u})}{\lambda}$$

Per tant, amb $\lambda \to 0$, per la definició de derivada direccional (6.2.1) tenim

$$D_{\vec{u}} f(a) = df(a)(\vec{u}).$$

Amb aquesta demostració també es veu la unicitat del diferencial d'una funció en un punt. □

**Observació 6.2.8.** *Com a conseqüència del primer apartat veiem que si $f$ és diferenciable en $a$ existeixen totes les seves derivades direccionals i que aquestes compleixen que, donats dos vectors $\vec{u}, \vec{v}$ i dos escalars $\lambda, \mu$, $D_{\lambda\vec{u}+\mu\vec{v}} f(a) = \lambda D_{\vec{u}} f(a) + \mu D_{\vec{v}}(a)$.*

**Teorema 6.2.9** (Condició suficient per a la diferenciabilitat)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}^m$ una funció, $a \in U$ un punt i $\mathrm{B}(a,\varepsilon)$, una bola centrada en $a$ de radi $\varepsilon > 0$. Si les derivades direccionals de $f$, $D_i f(x)$, existeixen per a tot punt $x \in \mathrm{B}(a,\varepsilon)$, per a tot $i \in \{1,\dots,d\}$ i són contínues en $a$, aleshores $f$ és diferenciable en $a$.*

*Demostració.* Donat un vector $\vec{h}$ de $\mathbb{R}^d$, considerem la diferencia

$$f(a+\vec{h}) - f(a),$$

amb $a = (a_1,\dots,a_d)$ i $\vec{h} = (h_1,\dots,h_d) = \sum_{i=1}^d h_i\vec{e}_i$, on $\vec{e}_i$ és l'$i$-èsim vector de la base canònica, i denotarem $\vec{h}_n = \sum_{i=1}^n h_i\vec{e}_i$ per a $1 \leq n \leq d$ i $\vec{h}_0 = (0,\dots,0)$. Escrivim la suma telescòpica

$$f(a+\vec{h}) - f(a) = \sum_{i=1}^{d} \Big( f(a+\vec{h}_i) - f(a+\vec{h}_{i-1}) \Big). \tag{6.2}$$

El primer terme d'aquesta suma telescòpica és $f(a+h_1\vec{e}_1) - f(a)$, i per la definició de derivada direccional (6.2.1) això és

$$f(a+h_1\vec{e}_1) - f(a) = h_1 D_1 f(a) + h_1\,\mathrm{o}(\vec{h}),$$

i la resta de termes de (6.2) són

$$f(a+\vec{h}_{k-1} + h_k\vec{e}_k) - f(a+\vec{h}_{k-1}).$$

Veiem que aquestes expressions varien només en $h_k\vec{e}_k$, que correspon a la $k$-èsima component, i com que les derivades parcials de $f$ existeixen, això vol dir que aquestes expressions són contínues, per tant podem aplicar el Teorema del

Valor Mig (5.2.9) per a funcions d'una variable i tenim que, per a tot $2 \leq k \leq d$ existeix un escalar $\xi_k$ tal que

$$f(a + \vec{h}_{k-1} + h_k\vec{e}_k) - f(a + \vec{h}_{k-1}) = h_k D_k f(\xi_k)$$

on $\xi_k$ està al segment que uneix $a + \vec{h}_{k-1} + h_k\vec{e}_k$ i $a + \vec{h}_{k-1}$.

Ara notem que quan $\vec{h} \to 0$ tindrem $a + \vec{h}_{k-1} + h_k\vec{e}_k \to a$ i com que, per hipòtesi, les derivades direccionals són contínues

$$h_k D_k f(\xi_k) = h_k D_k f(a) + h_k \, \mathrm{o}(\vec{h})$$

i obtenim

$$\begin{aligned} f(a + \vec{h}) - f(a) &= \sum_{i=1}^{d} h_i D_i f(a) + \sum_{i=1}^{d} h_i \, \mathrm{o}(\vec{h}) \\ &= \sum_{i=1}^{d} D_{h_i\vec{e}_i} f(a) + \sum_{i=1}^{d} h_i \, \mathrm{o}(\vec{h}) \end{aligned}$$

i mentre $a + \vec{h} \in \mathrm{B}(a, \varepsilon)$, el que tenim satisfà la definició de diferencial d'una funció (6.2.3) per la proposició 6.2.7, i per tant $f$ és diferenciable en $a$. □

**Nota 6.2.10.** *Notem que en aquesta demostració només hem hagut d'utilitzar la continuïtat de $d-1$ de les derivades parcials de $f$ en $a$. per tant en veritat tenim prou amb veure que totes les derivades parcials de $f$ existeixen en $a$ i que almenys totes menys una d'aquestes són contínues en $a$ per poder dir que $f$ és diferenciable en $a$, però a aquest curs només es dona l'enunciat reduït.*

**Proposició 6.2.11.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f, g \colon U \to \mathbb{R}^m$ dues funcions diferenciables en un punt $a \in U$ amb diferencials $df(a), dg(a)$, respectivament. Aleshores $f + g$ és diferenciable en $a$ i té per diferencial $df(a) + dg(a)$.*

*Demostració.* Siguin $\vec{u}$ un vector de $\mathbb{R}^d$ i $D_{\vec{u}}f(a)$, $D_{\vec{u}}g(a)$ les derivades parcials de $f$ i $g$, respectivament, en el punt $a$ amb direcció $\vec{u}$. La derivada parcial de $f + g$ en $a$ amb direcció $\vec{u}$ és $D_{\vec{u}}(f + g)(a)$. Com que les derivades direccionals es comporten, per definició, com les derivades d'una variable, tenim

$$D_{\vec{u}}f(a) + D_{\vec{u}}g(a) = D_{\vec{u}}(f + g)(a),$$

i per la proposició 6.2.7, com que l'argument no depèn de $\vec{u}$, ja hem acabat. □

### 6.2.2 La Matriu Jacobiana i la regla de la cadena

**Definició 6.2.12** (Matriu Jacobiana)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f \colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores definim la matriu Jacobiana de $f$ en $a$ com

$$\begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix}.$$

**Proposició 6.2.13.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$, $df(a)$ el diferencial de $f$ en el punt $a$ i $\vec{h} = (h_1, \dots, h_d)$ un vector de $\mathbb{R}^d$. Aleshores*

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f_1(a) & \cdots & D_d f_1(a) \\ \vdots & & \vdots \\ D_1 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_d \end{bmatrix},$$

*és a dir, la matriu Jacobiana de $f$ en $a$ és la matriu associada del diferencial de $f$ en el punt $a$.*

*Demostració.* Aquest enunciat té sentit per la definició de diferencial d'una funció (6.2.3) i la definició de matriu Jacobiana (6.2.12).

Donada la base canònica de $\mathbb{R}^d$, $(\vec{e_1}, \dots, \vec{e_d})$, tenim

$$df(a)(\vec{h}) = \sum_{i=1}^{d} h_i df(a)(\vec{e_i}) = \sum_{i=1}^{d} h_i D_i f(a),$$

i si $f(a) = (f_1(a), \dots, f_m(a))$,

$$D_i f(a) = \begin{bmatrix} D_i f_1(a) \\ \vdots \\ D_i f_m(a) \end{bmatrix}. \tag{6.3}$$

Per tant, podem reescriure aquestes dues igualtats com

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_d \end{bmatrix}.$$

On, recordant (6.3),

$$\begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} = \begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix}.$$

Així que

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_d \end{bmatrix}.$$

Així veiem que la matriu Jacobiana de $f$ en $a$ està ben definida com a matriu associada del diferencial de $f$ en $a$. □

**Observació 6.2.14.** *Suposem $m = 1$. Recordant la definició de diferencial d'una funció (6.2.3) i denotant $x = a + \vec{h}$, $a = (a_1, \dots, a_d)$, $x = (x_1, \dots, x_d)$*

$$f(x) - f(a) - \mathrm{o}(\|x - a\|) = df(a)(x - a)$$

*i per la definició de matriu Jacobiana (6.2.12) tenim*

$$f(x) - f(a) - \mathrm{o}(\|x-a\|) = \begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} \begin{bmatrix} x_1 - a_1 \\ \vdots \\ x_d - a_d \end{bmatrix}.$$

*El que, quan $\vec{h} \to 0$, ens diu que és una aproximació a*

$$(x_1 - a_1)D_1 f(a) + \cdots + (x_d - a_d)D_d f(a) = f(x) - f(a),$$

*el que és un espai afí de dimensió $d+1$ tangent a $f$ en el punt $a$.*

**Teorema 6.2.15** (Regla de la cadena)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$ i siguin $V \subseteq \mathbb{R}^m$ un obert i $g\colon V \to \mathbb{R}^p$ una funció diferenciable en un punt $f(a) = b \in V$. Aleshores $g(f(x))$ és diferenciable en $a$ amb diferencial $dg(b)(df(a)(\vec{h}))$, on $df(a)$ i $dg(b)$ són els diferencials de $f$ i $g$ en $a$ i $b$, respectivament, i $\vec{h}$ és un vector de $\mathbb{R}$.*

*Demostració.* Per la definició de diferencial d'una funció (6.2.3), tenim

$$f(a+\vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Reescrivim amb $x = a + \vec{h}$ i $y = b + \vec{h}$

$$f(x) = f(a) + df(a)(x-a) + \mathrm{o}(x-a),$$

$$g(y) = g(b) + dg(b)(y-b) + \mathrm{o}(y-b).$$

Si fem $y = f(x)$ i substituïm en la segona equació obtenim

$$g(f(x)) = g(b) + dg(b)(f(a) + df(a)(x-a) + \mathrm{o}(x-a) - b) + \mathrm{o}(f(x) - b)$$

Si simplifiquem i utilitzem la linealitat del diferencial obtenim

$$g(f(x)) = g(b) + dg(b)(df(x-a)) + dg(b)(\mathrm{o}(x-a)) + \mathrm{o}(f(x) - b)$$

Ara només hem de veure que $dg(b)(\mathrm{o}(x-a))$ i $\mathrm{o}(f(x)-b)$ són $\mathrm{o}(x-a)$. El primer el podem veure amb que

$$\|dg(b)(\mathrm{o}(x-a))\| \leq \|dg(b)\|\,\mathrm{o}(\|x-a\|).$$

I com que quan $x \to a$, $f(a) \to b$ (donat per $\vec{h} \to 0$), ja que $f$ és contínua. Aleshores podem escriure

$$f(x) - b = df(a)(x-a) + \mathrm{o}(x-a),$$

i observant el cas $x \to a$ trobem que $\|f(x) - b\| \leq C\|x-a\|$, on $C \in \mathbb{R}$ és la norma de l'aplicació lineal $dg(b)$. □

### 6.2.3 Gradient, punts crítics i extrems relatius

**Definició 6.2.16** (Funció escalar)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció. Direm que $f$ és una funció escalar de $d$ variables si $f$ és diferenciable per a tot $x \in U$.

**Definició 6.2.17** (Conjunts de nivell)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció. Aleshores direm que, per a tot $C \in \mathbb{R}$,

$$L_C = \{x \in U \mid f(x) = C\}$$

és el conjunt de nivell $C$ de la funció $f$.

**Definició 6.2.18** (Gradient d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció escalar. Definim el gradient de $f$ en un punt $a \in U$ com el vector

$$\nabla f(a) = (D_1 f(a), \dots, D_d f(a)).$$

**Proposició 6.2.19.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}$ una funció escalar i $\vec{u} = (u_1, \dots, u_d$ un vector de $\mathbb{R}^d$. Aleshores*

$$\langle \nabla f(a), \vec{u} \rangle = D_{\vec{u}} f(a).$$

*Demostració.* Ho veiem per la definició de gradient d'una funció (6.2.18), la definició de derivada direccional (6.2.1) i l'observació 6.2.8. Tenim

$$\begin{aligned}
\langle \nabla f(a), \vec{u} \rangle &= u_1 D_1 f(a) + \cdots + u_d D_d f(a) && \text{(gradient d'una funció (6.2.18))} \\
&= D_{u_1 \vec{e}_1} f(a) + \cdots + D_{u_d \vec{e}_1} f(a) && \text{(derivada direccional (6.2.1))} \\
&= D_{u_1 \vec{e}_1 + \cdots + u_d \vec{e}_1} f(a) && \text{(Observació 6.2.8)} \\
&= D_{\vec{u}} f(a),
\end{aligned}$$

com volíem demostrar. □

**Observació 6.2.20.** *El gradient d'una funció en un punt és perpendicular al conjunt de nivell que conté el punt.*

**Proposició 6.2.21.** *Sigui $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}$ una funció escalar i $D_{\vec{u}} f(a)$ la derivada direccional de $f$ en la direcció $\vec{u}$, on $\vec{u}$ és un vector de $\mathbb{R}^d$. Aleshores $D_{\vec{u}} f(a)$ és màxim $\iff$ $\vec{u} = \lambda \nabla f(a)$, amb $\lambda \in \mathbb{R}$.*

*Demostració.* Pel Teorema de la Desigualtat de Cauchy-Schwarz (5.2.10) tenim, amb $\|\vec{u}\| = 1$

$$-\|\nabla f(a)\| \leq \|\langle \nabla f(a), \vec{u} \rangle\| \leq \|\nabla f(a)\|$$

$$-\|\nabla f(a)\| \leq \|D_{\vec{u}}(a)\| \leq \|\nabla f(a)\|,$$

però si prenem $\vec{u} = \frac{\nabla f(a)}{\|\nabla f(a)\|}$ tenim $D_{\vec{u}} f(a) = \nabla f(a)$. Amb això es veu que el gradient d'una funció en un punt ens dona la direcció de màxim creixement de la funció en el punt. □

**Observació 6.2.22.** *Veiem que, donat que $\nabla f(a)$ ens diu la direcció de màxim creixement de $f$ en el punt $a$, $-\nabla f(a)$ ens dirà la direcció de màxim decreixement de $f$ en $a$.*

**Definició 6.2.23** (Extrems relatius i punts crítics)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt i $f\colon U \to \mathbb{R}$ una funció escalar. Direm que el punt $a$ és un extrem relatiu de $f$ si hi ha una bola de radi $r > 0$ centrada en el punt $a$, $\mathrm{B}(a, r)$, tal que, per a tot $x \in \mathrm{B}(a, r)$, $f(a) \geq f(x)$ (direm que $a$ és un màxim relatiu) o tal que $f(a) \leq f(x)$ (direm que $a$ és un mínim relatiu).

Si $f(a) \geq f(x)$ o $f(a) \leq f(x)$, per a tot $x \in U$, direm que $a$ és un màxim o un mínim absolut de $f$ en $U$, respectivament.

També direm que $a$ és un punt crític si $\nabla f(a) = \vec{0}$.

**Proposició 6.2.24.** *Sigui $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció escalar diferenciable en $a$. Aleshores*

$$a \text{ és un màxim o un mínim relatiu de } f \implies \nabla f(a) = \vec{0}.$$

*Demostració.* Si $\vec{u}$ és un vector qualsevol de $\mathbb{R}^d$, la funció $f(a + t\vec{u})$, amb $t \in \mathbb{R}$ té un extrem relatiu en $t = 0$, i per tant la seva derivada ha de ser 0; $D_{\vec{u}} f(a) = 0$, i com això no depèn de $\vec{u}$, per la definició de gradient d'una funció (6.2.18), $D_{\vec{u}} = \langle \nabla f(a), \vec{u} \rangle = 0$, el que és equivalent a $\nabla f(a) = \vec{0}$. □

**Observació 6.2.25.** *Amb la definició de extrem relatiu (6.2.23) i la proposició 6.2.24 tenim que el punt $a$ és un màxim o mínim relatiu de $f$ si $a$ és un punt crític de $f$.*

**Definició 6.2.26** (Punt de sella d'una funció)**.** Sigui $f$ una funció i $a$ un punt del seu domini. Si $a$ és un punt crític però no és ni màxim ni mínim local direm que $a$ és un punt de sella de $f$.

Aquesta definició té sentit per l'observació 6.2.25.

### 6.2.4 Canvis de coordenades diferenciables

**Definició 6.2.27** (Homeomorfisme i difeomorfisme)**.** Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $\Phi\colon U \longleftrightarrow V$ una aplicació bijectiva tal que $\Phi, \Phi^{-1}$ siguin contínues. Aleshores direm que $\Phi$ és un homeomorfisme. Si pensem $\Phi$ com

$$\begin{aligned} \Phi\colon U &\longleftrightarrow V \\ a &\longmapsto (v_1(a), \ldots, v_d(a)) \end{aligned}$$

aleshores donat un punt $a \in U$, interpretem $v_1(a), \ldots, v_d(a)$ com les noves coordenades del punt $a$. Amb aquest nou sistema els punts que fan d'eixos de coordenades, que són les famílies de punts definits per

$$\{x \in U \mid v_i(x) = v_j(a) \Leftrightarrow i \neq j, \forall i, j \in \{1, \ldots, d\}\},$$

que són tots els punts amb totes les coordenades iguals, excepte la $j$-èsima.

Si $\Phi, \Phi^{-1}$ són diferenciables direm que és un canvi de coordenades diferenciable o que és un difeomorfisme.

**Proposició 6.2.28.** *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $\Phi\colon U \longleftrightarrow V$ un difeomorfisme. Aleshores*

$$d(\Phi^{-1}) = (d\Phi)^{-1}.$$

*Demostració.* Suposem que $\Phi$ és diferenciable en un punt $a \in U$. Aleshores per la definició de difeomorfisme (6.2.27) tenim que $\Phi^{-1}$ existeix i és diferenciable en el punt $\Phi(a) \in V$. Volem veure que $d(\Phi^{-1}) = (d\Phi)^{-1}$.

Considerem la funció $\Phi^{-1}(\Phi)$ i un vector $\vec{h}$ de $\mathbb{R}^d$. Aleshores el diferencial de $\Phi^{-1}(\Phi)$ en $a$ aplicat a $\vec{h}$ és, per la regla de la cadena (6.2.15),

$$\mathrm{Id}_U(\vec{h}) = d(\Phi^{-1}(\Phi))(a)(\vec{h}) = d(\Phi^{-1})(\Phi(a))(d\Phi(a)(\vec{h})).$$

Anàlogament, el diferencial de $\Phi(\Phi^{-1})$ en $\Phi(a)$ aplicat a $\vec{h}$ és

$$\mathrm{Id}_V(\vec{h}) = d(\Phi(\Phi^{-1}))(\Phi(a))(\vec{h}) = d(\Phi)(a)(d\Phi^{-1}(\Phi(a))(\vec{h})),$$

i amb això tenim que $d(\Phi^{-1})$ és la inversa de $d\Phi$ pels dos costats, i per tant $d(\Phi^{-1}) = (d\Phi)^{-1}$, com volíem demostrar. □

**Corol·lari 6.2.29.** *Sigui $\Phi$ un difeomorfisme diferenciable en un punt $a$. Aleshores*

$$\det(df(a)) \neq 0.$$

**Definició 6.2.30** (Derivades parcials d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $a = (a_1, \ldots, a_d)$ un punt de $U$ i $f$ una funció definida per

$$\begin{aligned} f\colon U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \ldots, f_m(a)). \end{aligned}$$

Aleshores, donat un $t \in \mathbb{R}$, direm que la derivada parcial de $f$ respecte la seva $i$-èsima coordenada és

$$\frac{\partial f}{\partial x_i}(a) = \lim_{t \to 0} \frac{f(a_1, \ldots, a_i + t, \ldots, a_d) - f(a)}{t}.$$

Notem que això és equivalent a derivar respecte la $i$-èsima variable prenent les altres variables com a constants.

**Proposició 6.2.31.** *Siguin $U, V \subset \mathbb{R}^d$ dos oberts i $\Phi\colon U \to V$ un difeomorfisme tal que donat un punt $a \in U$, $\Phi(a) = (\Phi_1(a), \ldots, \Phi_d(a)) = (v_1, \ldots, v_d)$. Aleshores, donada una funció $f\colon U \to V$,*

$$\frac{\partial f}{\partial v_i} = \sum_{j=1}^{d} \frac{\partial f}{\partial x_j} \frac{\partial x_j}{\partial v_i}.$$

*Demostració.* □

## 6.3 Teoremes de la funció implícita i inversa

### 6.3.1 Dependència i independència funcional

**Definició 6.3.1** (Dependència funcional)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^m$ una funció. Donades $v_1, \ldots, v_k\colon U \to \mathbb{R}$ $k$ funcions, direm que $f$ depèn funcionalment de $v_1, \ldots, v_k$ si existeix una funció $h\colon \mathbb{R}^k \to \mathbb{R}^m$ tal que

$$f(x) = h(v_1(x), \ldots, v_k(x)), \quad \text{per a tot } x \in U.$$

**Proposició 6.3.2.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}^m$ una funció i $v_1, \dots, v_d$, $d$ funcions escalars sobre $U$ que defineixen un sistema de coordenades que anomenarem $\Phi(x) = (v_1(x), \dots, v_d(x))$. Aleshores, donat un $k < d$ els següents enunciats són equivalents:*

1. *$f$ depèn funcionalment de $v_1, \dots, v_k$ per a tot $x \in U$.*
2. *$\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \dots, \nabla v_k(x)$ per a tot $x \in U$.*
3. *La matriu que té per files $\nabla v_1(x), \dots, \nabla v_k(x)$ i $\nabla f(x)$ té rang $k$ per a tot $x \in U$.*
4. *$\frac{\partial f}{\partial v_{k+1}} = \cdots = \frac{\partial f}{\partial v_d} = 0$*

**Teorema 6.3.3.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ $k < d$ funcions escalars definides en $U$. Aleshores, donat un punt $a \in U$ i un real $\varepsilon > 0$, les funcions $v_1, \dots, v_k$ formen un sistema de coordenades en $\mathrm{B}(\varepsilon, a) \subset U$ si i només si els seus gradients en $a$, $\nabla v_1(a), \dots, \nabla v_k(a)$, són linealment independents.*

*Demostració.* Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ $k$ funcions escalars definides en $U$ que formen un sistema de coordenades en $\mathrm{B}(\varepsilon, a) \subset U$. Considerem les $d - k$ funcions escalars definides en $U$ $v_{k+1}, \dots, v_d$ tal que $v_1, \dots, v_d$ formin un sistema de coordenades de $U$. Per la proposició 6.3.2 tenim que aquestes $d$ funcions són funcionalment independents, el que ens diu que el determinant de la matriu composta per els seus gradients en un punt $x$, $\nabla v_1(x), \dots, \nabla v_d(x)$ té determinant no nul per a tot $x \in U$. Per tant, tenim que $\nabla v_1(x), \dots, \nabla v_d(x)$ són linealment independents per a tot $x \in U$ i, en particular, que $\nabla v_1(a), \dots, \nabla v_k(a)$ són linealment independents. □

### 6.3.2 Varietats

**Definició 6.3.4** (Varietat)**.** Siguin, amb $m < d$, $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts, $M \subseteq \mathbb{R}^d$ un conjunt i $r > 0$ un radi. Aleshores, si per a tot punt $p \in M$, existeix un homeomorfisme $H\colon U \to S \cap \mathrm{B}(p, r)$ direm que $M$ és una varietat de dimensió $m$ de $\mathbb{R}^d$.

**Definició 6.3.5** (Varietat regular)**.** Siguin, amb $m < d$, $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts amb $(0, \dots, 0) = 0 \in U$. Aleshores, donat un conjunt $M \subseteq \mathbb{R}^d$, direm que $M$ és una varietat regular de dimensió $m$ o una varietat diferenciable de classe $\mathcal{C}^1$ i de dimensió $m$ si per a tot punt $p \in M$ existeix un homeomorfisme $H\colon U \to \mathrm{B}(p, r) \cap S$ tal que $H(0) = p$ i el diferencial de $H$ en $t \in U$, $dH(t)$, tingui rang $m$ per a tot $t \in U$.

Si $m = 1$ tindrem un arc regular, i si $m = 2$ parlarem de superfície regular.

**Observació 6.3.6.** *Un cas particular d'aquesta definició és el dels gràfics. En aquest cas tenim que si*

$$\begin{aligned} H\colon U &\longleftrightarrow \mathrm{B}(p, r) \cap S \\ t &\longmapsto (h_1(t), \dots, h_d(t)) \end{aligned}$$

*aleshores $m$ de les components de $H$ fan de paràmetres; suposem que són els $m$ primers, així $H$ seria de la forma*

$$H(t_1, \dots, t_m) = (t_1, \dots, t_m, h_{m+1}(t_1, \dots, t_m), \dots, h_d(t_1, \dots, t_m)).$$

**Definició 6.3.7** (Espai tangent en un punt)**.** Siguin $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts i $M \subseteq \mathbb{R}^m$ una varietat regular de dimensió $m$. Això vol dir que per a tot punt $t \in M$ existeix un homeomorfisme $H\colon U \to S \cap \mathrm{B}(p,r)$ amb $H(0) = p$. Aleshores definim l'espai tangent a $M$ en $p$ com

$$T_p(M) = \{\vec{h} \text{ un vector de } \mathbb{R}^d\colon dH(0)(x) = \vec{h}, \text{ per a algun } x \in \mathbb{R}^d\},$$

això és l'imatge de $dH(0)$.

**Proposició 6.3.8.** *Siguin $U \subseteq \mathbb{R}^m$ un obert, $M$ una varietat regular de dimensió $m$ d'un obert $S \subseteq \mathbb{R}^d$, $p \in M$ un punt i*

$$\begin{aligned} H\colon U &\longleftrightarrow \mathrm{B}(p,r) \cap S \\ t &\longmapsto (h_1(t), \dots, h_d(t)) \end{aligned}$$

*un homeomorfisme tal que $H(0) = p$. Aleshores l'espai tangent a $M$ en un punt $p \in M$, $T_p(M)$, té dimensió $m$ i la seva base és*

$$\left(\left(\frac{\partial h_1}{\partial t_1}, \dots, \frac{\partial h_d}{\partial t_1}\right), \dots, \left(\frac{\partial h_1}{\partial t_d}, \dots, \frac{\partial h_d}{\partial t_d}\right)\right).$$

*Demostració.* Considerem la matriu Jacobiana (6.2.12) de $H$ en 0. Per hipòtesi, aquesta té rang $m$. Aleshores, per la definició d'espai tangent en $p$ tenim

$$T_p(M) = \{\vec{h} \text{ un vector de } \mathbb{R}^d \mid dH(0)(x) = \vec{h}, \text{ per a algun } x \in \mathbb{R}^d\},$$

per tant, els elements de $T_p(M)$ venen donades pel sistema lineal

$$\begin{bmatrix} D_1h_1(0) & D_2h_1(0) & \cdots & D_mh_1(0) \\ D_1h_2(0) & D_2h_2(0) & \cdots & D_mh_2(0) \\ \vdots & \vdots & & \vdots \\ D_1h_d(0) & D_2h_d(0) & \cdots & D_mh_d(0) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_d \end{bmatrix}.$$

Per tant, $T_p(M)$ està generat per les columnes de $dH(0)$, i la seva base és

$$(D_1H(0), \dots, D_dH(0)),$$

que és equivalent a

$$\left(\left(\frac{\partial h_1}{\partial t_1}, \dots, \frac{\partial h_d}{\partial t_1}\right), \dots, \left(\frac{\partial h_1}{\partial t_d}, \dots, \frac{\partial h_d}{\partial t_d}\right)\right).$$

Amb això també veiem que $T_p(M)$ té dimensió $m$. □

**Proposició 6.3.9.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $v_1, \dots, v_k \in \mathcal{C}^1$ $k < d$ funcions escalars definides en $U$ funcionalment independents en cada punt de $U$ de forma que els conjunts de nivell arc-connexos*

$$M = \{x \in U \mid v_1(x) = c_1, \dots, v_k(x) = c_k\}$$

*siguin varietats regulars de dimensió $m = d - k$. Aleshores, donada una funció $f\colon U \to \mathbb{R}^m$ diferenciable depèn funcionalment de $v_1, \dots, v_k$ si i només si $\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \dots, \nabla v_k(x)$ per a tot $x \in U$.*

*Demostració.* La implicació cap a la dreta ($\Rightarrow$) està vista a la proposició 6.3.2. Fem l'altre implicació ($\Leftarrow$). Per l'observació 6.2.20, el subespai generat pels gradients $\nabla v_1(x), \dots, \nabla v_k(x)$ és ortogonal a l'espai tangent $T_x(M)$. Per tant, per a tot vector $\vec{u}$ de $T_x(M)$ tindrem $D_{\vec{u}} f(x) = 0$, el que significa que $f(x)$ serà constant en $M$, és a dir, $f(x) = (k_1, \dots, k_m)$ per a tot $x \in U$ tal que $f(x) \in M$. Aleshores existeix una funció $H\colon U \to M$ tal que

$$f(x) = H(v_1(x), \dots, v_k(x)). \qquad \square$$

### 6.3.3 Teorema de la funció inversa

**Proposició 6.3.10.** *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $f\colon U \leftrightarrow V$ un homeomorfisme diferenciable en un punt $a \in U$, amb inversa $g = f^{-1}$. Aleshores, $g$ és diferenciable en $f(a)$ si i només si la Jacobiana de $f$ en $a$ té determinant diferent de zero.*

*Demostració.* Demostrem la implicació cap a la dreta ($\Rightarrow$). En un entorn de $a$, $f$ es comporta com un difeomorfisme per la definició de difeomorfisme (6.2.27). Per tant, amb el corol·lari 6.2.29 queda demostrat.

Demostrem ara l'altre implicació ($\Leftarrow$). Denotem $x = a + \vec{h}$, on $\vec{h}$ és un vector de $\mathbb{R}^d$. Per tant tenim, que amb un cert vector $\vec{k}$ de $\mathbb{R}^d$,

$$f(a + \vec{h}) = f(a) + \vec{k},$$

i com que per la definició de homeomorfisme (6.2.27) $f$ és un homeomorfisme tenim que $\vec{h} \to 0$ si i només si $\vec{k} \to 0$. Per tant

$$\vec{k} = f(a + \vec{h}) - f(a)$$

i per la definició de diferencial d'una funció (6.2.3) quan $\vec{k} \to 0$

$$\vec{k} = f(a + \vec{h}) - f(a) = df(a)(\vec{h}) + \mathrm{o}(\vec{h}).$$

Aplicant $df(a)^{-1}$ als costats de la igualtat tenim

$$df(a)^{-1}(\vec{k}) = df(a)^{-1}(df(a)(\vec{h}) + \mathrm{o}(\vec{h})),$$

i com que $df(a)^{-1}$ és lineal per la definició de diferencial d'una funció (6.2.3) tenim que

$$df(a)^{-1}(\vec{k}) = df(a)^{-1}(df(a)(\vec{h})) + df(a)^{-1}(\mathrm{o}(\vec{h})),$$

i aleshores

$$\vec{h} = df(a)^{-1}(\vec{k}) - df(a)^{-1}(\mathrm{o}(\vec{h})),$$

que és equivalent a, amb $b = f(a)$,

$$g(b + \vec{k}) - g(b) = df(a)^{-1}(\vec{k}) - df(a)^{-1}(\mathrm{o}(\vec{h})).$$

Ara en veure que $df(a)^{-1}(\mathrm{o}(\vec{h}))$ és com $\mathrm{o}(\vec{k})$ haurem acabat.

Això ho podem veure fent

$$\left\| df(a)^{-1}(\vec{k}) \right\| + \left\| df(a)^{-1}(\mathrm{o}(\vec{h})) \right\| \leq \left\| df(a)^{-1} \right\| \left\| \vec{k} \right\| + \left\| df(a)^{-1} \right\| \left\| \mathrm{o}(\vec{h}) \right\|.$$

I per tant, quan $\vec{h} \to 0$ tenim $\mathrm{o}(\vec{h}) \to 0$ i $\vec{k} \to 0$, i veiem que $df(a)^{-1}(\mathrm{o}(\vec{h}))$ ha de ser com $\mathrm{o}(\vec{k})$. $\square$

**Lemma 6.3.11.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$ amb diferencial de $f$ en un punt $a \in U$ de norma $m$, $df(a)$, invertible amb inversa $df(a)^{-1}$. Aleshores existeix una bola tancada centrada en $a$ de radi $r > 0$, $\overline{\mathrm{B}}(a,r)$, que, per a tot $x, y \in \overline{\mathrm{B}}(a,r)$ compleix*

1. $\det(df(x)) \neq 0$
2. $\|df(x) - df(a)\| \leq \frac{m}{2}$
3. $\frac{m}{2}\|x-y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x-y\|$

*Demostració.* Observem que el punt (1) és cert ja que si $r$ és prou petita, per la proposició 6.2.5, $f$ és contínua.

Per veure el punt (2) tenim que pel Teorema de l'equivalència entre normes (5.2.8) existeix $C \in \mathbb{R}$ tal que

$$\|df(x) - df(a)\| \leq C \sum_{i=1}^{n}\sum_{j=1}^{n}\left|\frac{\partial f_i}{\partial x_j}(x) - \frac{\partial f_i}{\partial x_j}(a)\right|,$$

i de nou, per a $r$ prou petita, com que $f$ és contínua, això és arbitràriament petit, i tenim $\|df(x) - df(a)\| \leq \frac{m}{2}$.

Per tant, de moment tenim que, amb $r$ prou petit, existeix una bola tancada $\overline{\mathrm{B}}(a,r)$ que compleix els punts (1) i (2); en veure que *2* $\Rightarrow$ *3* haurem acabat aquesta part.

Considerem l'aplicació $\widehat{f}(x) = f(x) - df(a)(x)$ amb diferencial $d\widehat{f} = d\widehat{f}(x) - d\widehat{f}(a)$. Per el punt (2) i el Teorema del Valor Mig (5.2.9) tenim, per a $x, y \in \overline{\mathrm{B}}(a,r)$,

$$\|f(x) - f(y) - df(a)(x-y)\| = \left\|\widehat{f}(x) - \widehat{f}(y)\right\| \leq \frac{m}{2}\|x-y\|.$$

Notem que, per a una funció $T$ amb inversa $T^{-1}$ per la definició de norma d'una aplicació lineal (5.1.2) tenim que existeix $K \in \mathbb{R}$ tal que

$$\|T(u)\| \leq K\|u\|,$$

per tant

$$\left\|T^{-1}(u)\right\| \leq K\|u\|.$$

Amb això veiem que existeix una $m$ tal que $\|df(a)(x-y)\| \leq m\|x-y\|$, i aleshores

$$\begin{aligned}\big|\|f(x) - f(y)\| - \|df(a)(x-y)\|\big| \leq \|f(x) - f(y) - df(a)(x-y)\| \leq \\ \leq \frac{m}{2}\|x-y\| \leq \frac{1}{2}\|df(a)(x-y)\|.\end{aligned}$$

amb el que obtenim

$$\frac{1}{2}\|df(a)(x-y)\| \leq \|f(x) - f(y)\| \leq \frac{3}{2}\|df(a)(x-y)\|,$$

i per tant

$$\frac{m}{2}\|x-y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x-y\|. \qquad \square$$

**Teorema 6.3.12** (Teorema de la funció inversa)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$ amb diferencial de $f$ en un punt $a \in U$, $df(a)$, invertible. Aleshores existeix un obert $W \subset U$ que conté $a$ tal que, la restricció de $f$ en $W$ sigui un difeomorfisme.*

*Demostració.* Sigui $df(a)^{-1}$ la inversa del diferencial de $f$ en $a$, $df(a)$, i $M = \frac{1}{m} = \left\|df(a)^{-1}\right\|$ la seva norma. Per la definició de norma d'una aplicació lineal (5.1.2) tenim que per a qualsevol vector $\vec{u}$ de $\mathbb{R}^d$,

$$\|df(a)(\vec{u})\| \leq m\|\vec{u}\|.$$

Pel lemma 6.3.11 tenim que existeix una bola tancada centrada en $a$ de radi $r > 0$, $\overline{\mathrm{B}}(a, r)$, que, per a tot $x, y \in \overline{\mathrm{B}}(a, r)$ compleix

1. $\det(df(x)) \neq 0$
2. $\|df(x) - df(a)\| \leq \frac{m}{2}$
3. $\frac{m}{2}\|x - y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x - y\|$

Considerem $S$, la frontera de $\overline{\mathrm{B}}(a, r)$, que és compacte. Per tant, el conjunt

$$S' = \{f(x) \mid \text{per a tot } x \in S\},$$

que és la imatge de $S$ respecte $f$ també és compacte i no conté $f(a)$, ja que $r > 0$. Aleshores considerem

$$d = \inf_{x \in S'} \|f(a) - x\| > 0$$

com la distància mínima de la imatge de $a$ respecte $f$ al conjunt $S'$, i definim la bola oberta centrada en $f(a)$ de radi $\frac{d}{2}$, $\mathrm{B}\big(f(a), \frac{d}{2}\big)$, i així $\|y - f(a)\| < \|y - f(x)\|$ per a tot $x \in S$. Ara considerem l'obert

$$W = \big\{x \in \overline{\mathrm{B}}(a, r) \mid f(x) \in \mathrm{B}\big(f(a), \tfrac{d}{2}\big)\big\}.$$

Pel punt (3) veiem que la restricció de $f$ en $\overline{\mathrm{B}}(a, r)$ és injectiva i, per tant, la restricció de $f$ en $W$ també és injectiva. Ara només ens queda veure que la restricció de $f$ en $W$ és exhaustiva i ja haurem acabat. Per a això hem de veure que per a tot $p \in \mathrm{B}\big(f(a), \frac{d}{2}\big)$ existeix un $q \in \overline{\mathrm{B}}(a, r)$ tal que $f(q) = p$.

Si entenem $f$ com $f(a) = (f_1(a), \ldots, f_d(a))$ i un punt $p \in \mathrm{B}\big(f(a), \frac{d}{2}\big)$ com $p = (p_1, \ldots, p_d)$, podem considerar la funció $h$ tal que

$$h(x) = \|p - f(x)\| = \sum_{i=1}^{d} (p_i - f_i(x))^2.$$

Aleshores $h$ té un mínim absolut en el compacte $\overline{\mathrm{B}}(a, r)$, que s'assoleix quan $x = q \in \overline{\mathrm{B}}(a, r)$. Per tant, per la proposició 6.2.24, $D_j h(q) = 0$, per a tot $j \in \{1, \ldots, d\}$, que és equivalent a dir

$$\sum_{i=1}^{d} D_j f_i(p)(p_i - f_i(q)) = 0, \quad \forall j \in \{1, \ldots, d\}.$$

Així hem vist que la restricció de $f$ en $W$ és exhaustiva, i per tant bijectiva, i ja teníem que era contínua. Podem veure de nou pel punt (3) del lema 6.3.11 que la seva inversa també és contínua. Amb tot això en tenim prou per dir que la restricció de $f$ en $W$ és un homeomorfisme diferenciable en un punt $a$ però, com que, per hipòtesi, tenim $\det(df(a)) \neq 0$, amb la proposició 6.3.10 queda demostrat el teorema. □

**Corol·lari 6.3.13.** *Una aplicació $f\colon U \to \mathbb{R}^d$ de classe $\mathcal{C}^1$ és un difeomorfisme si i només si $f$ és injectiva i $\det(df(a)) \neq 0$ per a tot $x \in U$.*

**Proposició 6.3.14.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ un sistema de $k$ funcions escalars definides en $U$. Aleshores, els seus gradients són linealment independents en un punt $a \in U$ si i només si aquest sistema de $k$ funcions escalars formen part d'un sistema de coordenades local en $a$.*

*Demostració.* La matriu formada pels gradients de $v_1, \dots, v_k$ en $a$ té un menor d'ordre $k$ no nul. Per tant, podem expandir aquest sistema de $k$ funcions amb $d-k$ funcions escalars definides en $U$ de classe $\mathcal{C}^1$, $v_{k+1} \dots, v_d$ amb gradients linealment independents en $a$, i aquestes $d$ funcions, $v_1, \dots, v_d$, formen un sistema de coordenades local en $a$. □

**Corol·lari 6.3.15.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ un sistema de $k$ funcions escalars definides en $U$. Aleshores una funció $f$ definida en un entorn d'un punt $a$ depèn funcionalment de $v_1, \dots, v_k$ en un entorn del punt $a$ si i només si $\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \dots, \nabla v_k(x)$ per a tot $x$ en un entorn del punt $a$.*

### 6.3.4 Teorema de la funció implícita

**Notació 6.3.16.** Podem interpretar $\mathbb{R}^d$ com $\mathbb{R}^d = \mathbb{R}^k \times \mathbb{R}^m$, on $d = k + m$. Per tant, denotarem un punt $a = (a_1, \dots, a_d)$ de $\mathbb{R}^d$ com $a = (a'; a'')$, on $a'$ correspon a $(a_1, \dots, a_k)$ i $a''$ a $(a_{k+1}, \dots, a_d)$.

També entenem que $a' \in \mathbb{R}^k$ i $a'' \in \mathbb{R}^m$.

**Teorema 6.3.17** (Teorema de la funció implícita)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $a = (a'; a'') \in U$ un punt, $v_1, \dots, v_k \in \mathcal{C}^1$ un sistema de $k = d - m$ funcions escalars definides en $U$ tals que $v_1(a) = \cdots = v_k(a) = 0$ i els seus gradients en $a$, $\nabla v_1(a), \dots, \nabla v_k(a)$ són linealment independents i $M$ un conjunt definit per $M = \{x \in U \mid v_1(x) = \cdots = v_k(x) = 0\}$. Aleshores hi ha un obert $W \subset \mathbb{R}^d$ que conté $a$, un obert $U'' \subset \mathbb{R}^m$ que conté $a''$ i una única funció $h\colon U'' \to \mathbb{R}^k$ tal que*

$$\begin{aligned} M &= \{x \in U \mid v_1(x) = \cdots = v_k(x) = 0\} = \\ &= \{x = (x'; x'') \in W \mid x' = h(x''), x'' \in U''\}. \end{aligned}$$

*Demostració.* Per començar definirem un obert $W \subseteq \mathbb{R}^d$, un obert $V \subseteq \mathbb{R}^d$ tal que $(0, \dots, 0) \in V$ i un difeomorfisme $\Phi$ tals que

$$\begin{aligned} \Phi\colon W &\longleftrightarrow V \\ x = (x_1, \dots, x_d) &\longmapsto (v_1(x), \dots, v_k(x), x_{k+1}, \dots, x_d), \end{aligned}$$

així $(v_1(x), \dots, v_k(x), x_{k+1}, \dots, x_d)$ forma un sistema de coordenades en $W$.

Observem que podem considerar $a = (0, \dots, 0)$ ja que si $(v_1(a), \dots, v_k(a)) = (c_1, \dots, c_k)$ podem treballar amb les funcions $v_1'(x) = v_1(x) - c_1, \dots, v_k'(x) = v_k(x) - c_k$ que compleixen $v_1'(a) = \cdots = v_k'(a) = 0$.

Com que $\Phi$ és un difeomorfisme, per la definició de difeomorfisme (6.2.27) és bijectiva, prenem la seva inversa

$$\begin{aligned} \Phi^{-1} \colon V &\longleftrightarrow W \\ y = (y_1, \dots, y_d) &\longmapsto (u_1(y), \dots, u_k(y), y_{k+1}, \dots, y_d), \end{aligned}$$

i, de nou, com que $\Phi$ és un difeomorfisme per la definició de difeomorfisme (6.2.27) tenim que $u_1, \dots, u_k \in \mathcal{C}^1$.

Aleshores, per a tot $x \in M$ tenim $\Phi(x) = (0'; x'')$. Definim un conjunt

$$U'' = \{y'' \in \mathbb{R}^m \mid (0; y'') \in V\},$$

i com que $\Phi$ és una bijecció, ja que és un difeomorfisme, tenim

$$U'' = \{x'' \in \mathbb{R}^m \mid \text{Existeix } x' \in \mathbb{R}^k \text{ tal que } (x'; x'') \in M \cap W\}.$$

Aleshores $U''$ és un obert de $\mathbb{R}^d$ i

$$M = \{(x'; x'') \in W \mid (u_1(0; x''), \dots, u_k(0; x''); y'') \text{ amb } y'' \in U''\},$$

i la funció que volíem demostrar que existeix és

$$h(x'') = (u_1(0; x''), \dots, u_k(0; x'')). \qquad \square$$

## 6.4 Extrems relatius

### 6.4.1 El mètode de multiplicadors de Lagrange

**Teorema 6.4.1** (Multiplicadors de Lagrange)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $S$ un conjunt definit per*

$$S = \{x \in U \mid g(x) = (g_1(x), \dots, g_k(x)) = 0\},$$

*on $g_1, \dots, g_k$ són $k < d$ funcions escalars definides en $U$ de classe $\mathcal{C}^1$.*

*Considerem la funció escalar $f \colon S \to \mathbb{R}$ tal que $a \in S$ sigui un màxim o un mínim relatiu de $f$ en $S$ i les funcions $g_1, \dots, g_k$ siguin funcionalment independents en $a$. Aleshores existeixen $\lambda_1, \dots, \lambda_k$ reals tals que*

$$D_i f(a) + \sum_{j=1}^{k} \lambda_j D_i g_j(a) = 0, \quad \forall i \in \{1, \dots, d\}.$$

*Demostració.* Siguin $\lambda_1, \dots, \lambda_k$, aleshores considerem el següent sistema d'equacions lineals

$$\sum_{j=1}^{k} \lambda_j D_i g_j(a) = -D_i f(a) \quad \forall i \in \{1, \dots, k\} \tag{6.4}$$

Com que $g_1, \dots, g_k$ són funcionalment independents en $a$, la matriu formada pels gradients de $g_1, \dots, g_k$ en $a$ té rang $k$ (proposició 6.3.2) el sistema d'equacions

lineals (6.4) té una única solució. Ara només ens cal veure que aquests mateixos reals $\lambda_1, \dots, \lambda_k$ també són solució de les $m = d - k$ equacions restants.

Per fer això ens caldrà el Teorema de la funció implícita (6.3.17). Com que $k < d$, amb la notació introduïda a 6.3.16, denotem el punt $a$ amb $a = (a'; a'')$, on $a' = (a_1, \dots, a_k)$ i $a'' = (a_{k+1}, \dots, a_d)$ i entenem $a' \in \mathbb{R}^k, a'' \in \mathbb{R}^m$. Aleshores definim una funció $g(x) = (g_1(x), \dots, g_k(x))$, que compleix $g(a', a'') = 0$ i $g \in \mathcal{C}^1$. Això, junt amb que per hipòtesi les funcions $v_1, \dots, v_k$ són funcionalment independents en $a$ i, per la proposició 6.3.2, la matriu

$$\begin{bmatrix} D_1 g_1(a) & \cdots & D_k g_1(a) \\ \vdots & & \vdots \\ D_1 g_k(a) & \cdots & D_k g_k(a) \end{bmatrix}$$

té determinant diferent de zero, complim les condicions del Teorema de la funció implícita (6.3.17) i l'apliquem. Per tant, existeix un obert $U'' \subset \mathbb{R}^m$ que conté $a''$ i una única funció $h\colon U'' \to \mathbb{R}^k$, $h \in \mathcal{C}^1$ amb $h(x) = (h_1(x), \dots, h_k(x))$, tal que $h(a'') = a'$ i que per a tot $y'' \in U''$ compleix $g(h(y''); y'') = 0$. Això significa que el sistema d'equacions

$$g_i(x_1, \dots, x_d) = 0, \quad \text{per a tot } i \in \{1, \dots, d\},$$

té una única solució de la forma $a' = h(a'')$, per tant definim les funcions, definides en $U''$,

$$F(y'') = f(h(y''); y'')$$

i, per a tot $i \in \{1, \dots, k\}$

$$G_i(y'') = g_i(h(y''); y'').$$

Degut a que $G_1 = \cdots = G_k = 0$, les seves derivades també són 0. □

### 6.4.2 Teorema del rang constant

No fer molt cas d'aquesta part. La faré bé quan sàpiga geometria diferencial. La part important d'aquí és l'últim corol·lari que ens diu que els difeomorfismes "conserven" els punts crítics.

**Definició 6.4.2** (Subvarietat regular)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert i $M \subseteq U$ un conjunt. Direm que $M$ és una subvarietat regular de dimensió $m$ si per a tot punt $p \in M$ existeix una bola centrada en $p$ de radi $r > 0$, $\mathrm{B}(p, r) \subseteq U$, i $k = d - m$ funcions escalars, $v_1, \dots, v_k \in \mathcal{C}^1$, definides en $U$ amb gradients linealment independents tals que

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) \mid v_1(x) = \cdots = v_k(x) = 0\}.$$

**Proposició 6.4.3.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $M \subseteq U$ una subvarietat regular de dimensió $m$ de $\mathbb{R}^d$. Aleshores, les afirmacions següents són equivalents:*

1. *Per a tot punt $p \in M$ existeix una bola centrada en $p$ de radi $r > 0$, $\mathrm{B}(p, r) \subseteq U$, i $k = d - m$ funcions escalars, $v_1, \dots, v_k \in \mathcal{C}^1$, definides en $U$ amb gradients linealment independents tals que*

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) \mid v_1(x) = \cdots = v_k(x) = 0\}.$$

2. *Per a tot punt $p \in M$ existeix un obert $V \subseteq U$ que conté $p$ i un sistema de coordenades $u_1, \dots, u_d$ definit en $V$ tal que*

$$M \cap V = \{x \in V \mid u_{k+1}(x) = \cdots = u_d(x) = 0\}.$$

3. *Per a tot punt $p \in M$ existeixen un obert $B \subseteq U$ que conté $p$, un obert $W \subseteq \mathbb{R}^m$ i un homeomorfisme $\Phi\colon W \to M \cap B$.*

*Demostració.* no □

**Teorema 6.4.4** (Teorema del rang constant)**.** *Sigui $U \subseteq \mathbb{R}^m$ un obert i $H\colon U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$, amb $\operatorname{rang}(dH(t)) = n$ per a tot $t \in U$. Aleshores el conjunt*

$$\{y \in \mathbb{R}^d \mid y = H(x) \text{ per algun } x \in U\}$$

*és una subvarietat de dimensió $n$.*

*Demostració.* Considerem $H(x) = (h_1(x), \dots, h_d(x))$ i fixem un punt $a \in U$ on es compleixin les condicions de la hipòtesi. Per la proposició 6.3.2, hi haurà $n$ components de $H$ tals que els seus gradients siguin linealment independents en $a$. Existeix una permutació $\sigma \in S_d$ tal que aquestes $n$ components de $H$ siguin $h_{\sigma(1)} \dots, h_{\sigma(n)}$.

Per continuïtat, els gradients $\nabla h_{\sigma(1)}(x), \dots, \nabla h_{\sigma(n)}(x)$ són linealment independents per a tot $x$ en un entorn obert de $a$, que denotarem per $V \subset U$. Per tant, podem expandir-les a un sistema de coordenades de $V$, $v_1, \dots, v_m$, on $v_i = h_{\sigma(i)}$, $\forall i \in \{1, \dots, n\}$. Com que $\operatorname{rang}(dH(t)) = n$ per a tot $t \in V$, per la proposició 6.3.2, els gradients $\nabla h_{\sigma(n+1)}, \dots, \nabla h_{\sigma(d)}$ depenen linealment dels gradients $\nabla v_1, \dots, \nabla v_n$ en $V$, per tant, pel corol·lari 6.3.15, per a cada $i \in \{n+1, \dots, d\}$, existeix una funció $\varphi_i$ que compleix $h_{\sigma(i)}(x) = \varphi_i(v_1(x), \dots, v_n(x))$ i per tant, si denotem $v(x) = (v_1(x), \dots, v_n(x))$,

$$\begin{aligned} H(x) &= G(v_1(x), \dots, v_n(x)) \\ &= (v_1(x), \dots, v_n(x), \varphi_{n+1}(v(x)), \dots, \varphi_d(v(x))) \end{aligned}$$

i es compleix la definició de subvarietat regular (6.4.2) per la proposició 6.4.3, ja que, per la definició de homeomorfisme (6.2.27), $G$ és un homeomorfisme definit en $V$. □

**Proposició 6.4.5.** *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts, $\Phi\colon U \longleftrightarrow V$ un difeomorfisme de classe $\mathcal{C}^1$ i $M \subseteq U$ una varietat regular de dimensió $m$ de $U$. Aleshores la imatge de $M$ per $\Phi$ és una subvarietat regular de dimensió $m$ de $V$.*

*Demostració. No fer-ne molt cas.* Per la definició de varietat regular (6.3.5), per a cada punt $p \in M$ existeixen $k = d - m$ equacions escalars, $v_1, \dots, v_k$ definides en $U$ amb gradients linealment independents i una bola de radi $r > 0$ centrada en $p$, $\mathrm{B}(p, r)$, tals que

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) \mid v_1(x) = \cdots = v_k(x) = 0\}.$$

Aleshores definim, per a tot $j \in \{1, \dots, k\}$, $u_j(x) = \Phi^{-1}(v_j(x))$. Aleshores tenim que si la imatge de $M$ per $\Phi$ és $N \subset V$, per a tot punt $q \in N$ hi ha una bola de radi $r > 0$, $\mathrm{B}(q, r)$, tal que

$$N \cap \mathrm{B}(q, r) = \{y \in \mathrm{B}(q, r) \mid u_1(x) = \cdots = u_k(x) = 0\},$$

i tenim que $u_1, \dots, u_d$ tenen gradients linealment independents, ja que, per la regla de la cadena (6.2.15), $\nabla v_j(x) = (d\Phi(x))^t(\nabla u_j(\Phi(x)))$, i com que $\Phi$ defineix un sistema de coordenades, per la proposició 6.3.2 els gradients de $u_1, \dots, u_d$ són linealment independents, i això compleix la definició de subvarietat regular (6.4.2). □

**Corol·lari 6.4.6.** *$d\Phi(a)(T_a(M)) = T_{\Phi(a)}(\Phi(M))$.*

### 6.4.3 Derivades d'ordre superior

Fixem-nos en que en derivar una funció $f$ obtenim una altre funció, i que aquesta, sota certes condicions, és derivable. En aquest capítol estudiarem algunes de les propietats d'aquest fet.

**Definició 6.4.7** ($n$-èsima derivada d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $\vec{v}_1, \dots, \vec{v}_n$ $n$ vectors de $\mathbb{R}^d$ (no necessàriament diferents) i $f\colon U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Si $\frac{\partial f}{\partial \vec{v}_1}$ és diferenciable en $a$ i prenem la seva derivada respecte $\vec{v}_2$ diem que

$$d^2 f(a)(\vec{v}_2, \vec{v}_1) = \frac{\partial}{\partial \vec{v}_2}\left(\frac{\partial f}{\partial \vec{v}_1}\right)(a) = \frac{\partial^2 f}{\partial \vec{v}_2 \partial \vec{v}_1}(a) = D_{\vec{v}_2,\vec{v}_1} f = D_{\vec{v}_2}(D_{\vec{v}_1} f)(a)$$

és la derivada de segon ordre de $f$ o la segona derivada de $f$.

Si la segona derivada de $f$ també és derivable podem parlar de la tercera derivada de $f$, que és la segona derivada de $\frac{\partial f}{\partial \vec{v}_1}$. Si iterem la suposició podem definir la $n$-èsima derivada de $f$ o una derivada d'ordre $n$ de $f$. També direm que $f$ és $n$-vegades diferenciable en $a$. Ho denotarem amb

$$d^n f(a)(\vec{v}_n \dots \vec{v}_1) = \frac{\partial^n f}{\partial \vec{v}_n \cdots \partial \vec{v}_1} = D_{\vec{v}_n,\dots,\vec{v}_1} f(a).$$

**Teorema 6.4.8.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}^d$ una funció 2-vegades diferenciable en $a \in U$, aleshores*

$$D_{\vec{v},\vec{u}} f(a) = D_{\vec{u},\vec{v}} f(a).$$

*Demostració.* Notem que podem dir $f(x) = (f_1(x), \dots, f_m(x))$, on $f_1, \dots, f_m$ són funcions escalars definides en $U$, i per la proposició 6.2.6 només cal que fem la demostració pel cas $m = 1$, ja que implicarà el general. També observem que podem donar un canvi de variables on els vectors $\vec{v}, \vec{u}$ siguin els nous eixos de coordenades, $\vec{e}_1, \vec{e}_2$ respectivament. En aquesta base tindríem que volem demostrar $D_{1,2} f(a) = D_{2,1} f(a)$, i com que això només afecta a una component del punt, podem considerar $d = 2$, i la demostració serà suficient per veure cas general. Per tant, ho demostrem per $m = 1, d = 2$. Aprofitant el canvi de coordenades també suposarem $a = (0, 0)$. Per tant, només hem de demostrar que $D_{2,1} f(0, 0) = D_{1,2} f(0, 0)$.

Considerem, amb un escalar $h > 0$, la següent diferencia:

$$Q(h) = f(h, h) - f(h, 0) - (f(0, h) - f(0, 0)) \tag{6.5}$$

Si fem $A(t) = f(t, h) - f(t, 0)$ tenim $Q(h) = A(h) - A(0)$, i pel Teorema del Valor Mig (5.2.9) existeix un escalar $0 < \xi < h$ tal que

$$A(h) - A(0) = hA'(\xi) = h(D_1 f(\xi, h) - D_1 f(\xi, 0)) \tag{6.6}$$

i com que, per hipòtesi, $D_1 f$ és diferenciable en $(0,0)$, per l'observació 6.2.14 podem escriure,

$$D_1 f(x,y) = D_1 f(0,0) + xD_{1,1} f(0,0) + yD_{2,1} f(0,0) + \mathrm{o}(\|x,y\|).$$

Ho apliquem a (6.6) i obtenim

$$\begin{aligned} hA'(c) = h\big(&D_1 f(0,0) + \xi D_{1,1} f(0,0) + \\ &+ hD_{2,1} f(0,0) - D_1 f(0,0) - \xi D_{1,1} f(0,0) + \mathrm{o}(h)\big) \end{aligned}$$

simplifiquem, i per la definició de $Q(h)$, (6.5),

$$hA'(c) = h^2 D_{2,1} f(0,0) + \mathrm{o}(h^2) = Q(h).$$

i tenim

$$\lim_{h\to 0} \frac{Q(h)}{h^2} = D_{2,1} f(0.0).$$

Repetint el mateix argument amb

$$Q(h) = f(h,h) - f(0,h) - (f(h,0) - f(0,0))$$

obtenim

$$\lim_{h\to 0} \frac{Q(h)}{h^2} = D_{1,2} f(0,0),$$

i per tant

$$D_{2,1} f(0,0) = D_{1,2} f(0,0). \qquad \square$$

**Nota 6.4.9.** *Sospito que una demostració "més general" seria similar a la del Teorema d'una condició suficient per a la diferenciabilitat (6.2.9), per si algun valent no ha quedat satisfet.*

**Corol·lari 6.4.10.** *$d^2 f(a)$ és una aplicació bilineal simètrica. De fet, si generalitzem la proposició iterant-la, tenim que $d^n f(a)$ és una aplicació $n$-lineal simètrica.*

### 6.4.4 Fórmula de Taylor en múltiples variables

Aquesta secció la farem considerant només funcions escalars (amb $m = 1$ en la notació que hem estat utilitzant). En el cas de voler fer el desenvolupament de Taylor d'una funció $f$ amb $m > 1$ només pensar $f$ com un vector de $m$ funcions escalars, $f(x) = (f_1(x), \ldots, f_m(x))$, i per tant el problema queda reduït a calcular $m$ desenvolupaments de Taylor (donat que es satisfacin certes condicions que estudiarem més endavant) i posar-los en forma de vector.

**Notació 6.4.11.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}$ una funció $n$-vegades diferenciable en un punt $a \in U$ i un altre punt de $U$, $t = (t_1, \ldots, t_d)$. Introduïm la següent notació:

$$f^{(k)}[a,t] = \sum_{i_k=1}^{d} \cdots \sum_{i_1=1}^{d} D_{i_k,\ldots,i_1} f(a) t_{i_1} \ldots t_{i_k}.$$

**Teorema 6.4.12** (Fórmula de Taylor en múltiples variables)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}$ una funció $n$-vegades diferenciable en un punt $a \in U$ i $b \in U$ un altre punt. Aleshores existeix un punt $z \in U$ tal que, per a algun $0 < \xi < 1$, $z = a + (b - \xi a)$ (això és que el punt $z$ es troba en el segment que uneix els punts $a$ i $b$) tal que*

$$f(b) - f(a) = \sum_{k=1}^{n-1} \frac{1}{k!} f^{(k)}[a, b-a] + \frac{1}{n} f^{(n)}[z, b-a].$$

*Demostració.* Com que, per hipòtesi, $U$ és obert, per la definició de conjunt obert (5.3.1) sabem que existeix un $\varepsilon > 0$ tal que, per a tot $-\varepsilon < t < 1 + \varepsilon$, tenim que $a + t(b-a) \in S$. Per tant, definim una funció $g$ com

$$\begin{aligned} g\colon (-\varepsilon, 1+\varepsilon) &\to \mathbb{R} \\ t &\mapsto f(a + t(b-a)) \end{aligned}$$

Aleshores $f(b) - f(a) = g(1) - g(0)$. Aleshores, amb $\xi \in (0,1)$, pel Teorema de Taylor (5.2.11) tenim

$$g(1) - g(0) = \sum_{k=1}^{n-1} \frac{1}{k!} g^{(k)}(0) + \frac{1}{m!} g^{(n)}(\xi). \tag{6.7}$$

Si pensem, amb $h(\xi) = a + \xi(b-a)$, que $g(\xi) = f(p(\xi))$, ha de ser $p(\xi) = (p_1(\xi), \ldots, p_d(\xi))$, i si denotem $a = (a_1, \ldots, a_d), b = (b_1, \ldots, b_d)$, tenim, amb $i \in \{1, \ldots, d\}$, que $\frac{\partial p}{\partial x_i}(\xi) = b_i - a_i$. Aplicant er la regla de la cadena (6.2.15) veiem que $g'$ està definida en $(-\varepsilon, 1+\varepsilon)$ i

$$g'(\xi) = \sum_{i=1}^{d} D_i f(p(\xi))(b_i - a_i) = f^{(1)}[p(\xi), b-a],$$

i aplicant la regla de la cadena una segona vegada,

$$g''(\xi) = \sum_{j=1}^{d} \sum_{i=1}^{d} D_{j,i} f(p(\xi))(b_i - a_i)(b_j - a_j) = f^{(2)}[p(\xi), b-a].$$

Si ho iterem $n$ vegades obtindrem que

$$g^{(n)}(t) = f^{(n)}[p(\xi), b-a],$$

i per tant, recordant (6.7), tenim

$$f(b) - f(a) = \sum_{k=1}^{n-1} \frac{1}{k!} f^{(k)}[a, b-a] + \frac{1}{n} f^{(n)}[z, b-a]$$

amb $z = p(\xi)$. □

### 6.4.5 Extrems lliures

En aquest apartat utilitzarem el que vam veure a l'observació 6.4.10 per classificar els extrems lliures d'una funció.

Això ens servirà per a classificar els punts crítics d'una funció escalar en un conjunt del seu domini, excloent-ne la frontera. Per exemple, en el cas d'utilitzar el Teorema dels multiplicadors de Lagrange (6.4.1) per obtenir un conjunt de punts crítics en el domini restringit de la funció. Més tard veurem com classificar els que es troben a la frontera.

**Proposició 6.4.13.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f\colon U \to \mathbb{R}$ una funció 2-vegades diferenciable en un punt $a \in U$ amb segones derivades contínues, i $a$ és un punt crític de $f$. Aleshores*

1. *$d^2 f(a)$ és definida estrictament positiva $\Rightarrow$ $a$ és un mínim relatiu.*
2. *$d^2 f(a)$ és definida estrictament negativa $\Rightarrow$ $a$ és un màxim relatiu.*
3. *$d^2 f(a)$ és definida positiva $\Leftarrow$ $a$ és un mínim relatiu.*
4. *$d^2 f(a)$ és definida negativa $\Leftarrow$ $a$ és un màxim relatiu.*

*Demostració.* Comencem demostrant dels punts (1) i (2), que són demostracions anàlogues. Suposem que $d^2 f(a)$ és definida positiva, i considerem el punt $t \in U$, $t = (t_1, \dots, t_d)$ i la funció

$$Q(t) = \tfrac{1}{2} f^{(2)}[a,t] = \sum_{j=0}^{d} \sum_{i=0}^{d} D_{j,i} f(a) t_i t_j.$$

Per hipòtesi, $Q$ és contínua per a tot punt $t \in U$. També tenim, per la definició de $n$-èsima derivada d'una funció (6.4.7), que $Q(t)$ és definida positiva per a tot $t \neq (0, \dots, 0)$.

Definim ara la bola tancada de radi 1 centrada en $a$, $\overline{\mathrm{B}}(a,1) \subset U$ i la seva frontera, $S = \mathrm{Fr}(\overline{\mathrm{B}}(a,1))$. Com que $S$ és compacte, pel Teorema de Weierstrass (5.2.12) $Q$ té un mínim relatiu en $S$, suposem que en aquest punt $Q$ val $m$. Com que $Q$ és definida estrictament positiva per a tot punt de $S$, $m > 0$.

Sabent que $Q$ és una forma bilineal simètrica, tenim que, per a tot $c \in \mathbb{R}$, $Q(ct) = c^2 Q(t)$. Si considerem $c = \frac{1}{\|t\|}$, per a $t \neq (0, \dots, 0)$, tenim que $ct \in S$, i per tant $Q(ct) \geq m$, el que significa $Q(t) \geq m\|t\|^2$.

Pel Teorema de la fórmula de Taylor en múltiples variables (6.4.12) i la definició de gradient d'una funció (6.2.18) tenim

$$f(a+t) - f(a) = \langle \nabla f(a), t \rangle + \tfrac{1}{2} f^{(2)}[z,t],$$

per a algun $z = a + t + (a - \xi(a+t))$, amb $0 < \xi < 1$. Però com que $a$ és un punt crític de $f$ (observació 6.2.25), tenim $\nabla f(a) = 0$, i per tant

$$f(a+t) - f(a) = \tfrac{1}{2} f^{(2)}[z,t],$$

i si escrivim $\left\|t^2\right\| \mathrm{o}(t) = \frac{1}{2} f^{(2)}[z,t] - \frac{1}{2} f^{(2)}[a,t]$ tenim

$$f(a+t) - f(a) = \tfrac{1}{2} f^{(2)}[a,t] + \left\|t^2\right\| \mathrm{o}(t).$$

Per tant

$$f(a+t) - f(a) = Q(t) + \|t\|^2 \mathrm{o}(t) \geq m\|t\|^2 + \|t\|^2 \mathrm{o}(t). \tag{6.8}$$

Com que $\mathrm{o}(t) \to 0$ és si i només si $t \to 0$, existeix un $\varepsilon > 0$ tal que, amb $0 < \|t\| < \varepsilon$ tenim $\mathrm{o}(t) < \frac{m}{2}$, i $0 \leq \|t\|^2 \mathrm{o}(t) < \frac{m}{2}\|t\|^2$, i així

$$f(a+t) - f(a) > m\|t\|^2 - \frac{m}{2}\|t\|^2 = \frac{m}{2}\|t\|^2 > 0,$$

i, com que això no depèn de $t$, per la definició de extrem relatiu (6.2.23) tenim que $a$ és un mínim relatiu. Ara només ens queda demostrar (3) i (4), de nou, només ens caldrà demostrar-ne una, ja que l'altre demostració serà anàloga. Suposem doncs que $a$ és un mínim relatiu.

Seguint l'argument sobre la fórmula de Taylor per a múltiples variables que hem fet a la primera meitat d'aquesta demostració arribem a la desigualtat (6.8) i tenim

$$f(a+t) - f(a) \leq m\|t\|^2 + \|t\|^2 \mathrm{o}(t).$$

Aleshores

$$\frac{f(a+t) - f(a)}{\|t\|^2} \leq m + \mathrm{o}(t).$$

Per la definició de extrem relatiu (6.2.23) tenim $f(a+t) - f(a) \geq 0$, i per tant, quan $t \to 0$, aleshores $\mathrm{o}(t) \to 0$ i

$$0 \leq \frac{f(a+t) - f(a)}{\|t\|^2} \leq m,$$

i ja hem acabat. □

# Capítol 7

# Càlcul integral

## 7.1 La integral Riemann

### 7.1.1 Funcions integrables Riemann

**Definició 7.1.1** (Rectangle)**.** Siguin $[a_1, b_1], \ldots, [a_d, b_d] \subset \mathbb{R}$ $d$ intervals tancats. Direm que $\mathfrak{R} = [a_1, b_1] \times \cdots \times [a_d, b_d]$ és un rectangle de $\mathbb{R}^d$.

**Definició 7.1.2** (Partició d'un rectangle i finor d'una partició)**.** Siguin $\mathfrak{R} = [a_1, b_1] \times \cdots \times [a_d, b_d]$ un rectangle de $\mathbb{R}^d$ i $P_i$ una partició de $[a_i, b_i]$ per a tot $i \in \{1, \ldots, d\}$. Aleshores $P = P_1 \times \cdots \times P_d$ és una partició de $\mathfrak{R}$.

Si $P_i = \{t_{i,0}, \ldots, t_{i,n}\}$, amb $a_i = t_{i,0} < \cdots < t_{i,n} = b_i$, direm que els rectangles definits per $[t_{1,i_1}, t_{1,i_1+1}] \times \cdots \times [t_{d,i_d}, t_{d,i_d+1}] \subset \mathfrak{R}$, amb $0 \leq i_j \leq d-1$ per a tot $j \in \{1, \ldots, d\}$, són subrectangles de $\mathfrak{R}$.

Sigui $Q$ una altre partició de $\mathfrak{R}$. Direm que $Q$ és més fina que $P$ si $P \subset Q$.

**Definició 7.1.3** (Suma superior i inferior)**.** Sigui $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $P$ una partició i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Per a cada subrectangle de $\mathfrak{R}$, $\mathfrak{R}_i$, amb $i \in I$, on $I$ és el conjunt d'índexs que denoten els subrectangles de $\mathfrak{R}$ definits per $P$, definim la suma superior de $f$ per $P$ com

$$\mathrm{S}(f, P) = \sum_{i \in I} \sup_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|,$$

i la suma inferior de $f$ per $P$ com

$$\mathrm{s}(f, P) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|.$$

**Proposició 7.1.4.** *Siguin $P, Q$ dues particions d'un rectangle $\mathfrak{R} \subset \mathbb{R}^d$ i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores, si $Q$ és més fina que $P$*

$$\mathrm{s}(f, P) \leq \mathrm{s}(f, Q) \quad i \quad \mathrm{S}(f, Q) \leq \mathrm{S}(f, P).$$

*Demostració.* Demostrarem només la primera desigualtat, ja que la segona té una demostració anàloga. Comencem notant que podem fer la demostració suposant $P = P_1 \times \cdots \times P_d$, on $P_i = t_{i,0} < \cdots < t_{i,n}$ és una partició de $[a_i, b_i]$ i $Q = Q_1 \times \cdots \times Q_d$, on, per a tot $j \in \{1, \ldots, d\} \setminus k$, $P_j = Q_j$, i $Q_k = t_{k,0} < \cdots < t_{k,l} < q < t_{k,l+1} < \cdots < t_{k,n}$, per algun $l \in \{0, \ldots, n-1\}$.

Suposarem $l = 0, k = 1$ per simplificar la notació. Aleshores, per la definició de suma superior i inferior (7.1.3) tenim

$$\mathrm{s}(f, P) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i|,$$

on $I$ és el conjunt d'índexs dels subrectangles de $\mathfrak{R}$ definits per $P$.

Observem que tots els subrectangles de $\mathfrak{R}$ són els mateixos respecte les particions $P$ i $Q$, excepte els que s'obtenen fent $\{t_{1,0}, q, t_{1,1}\} \times Q_2 \times \cdots \times Q_d$. Per tant, els únics termes del sumatori que canvien són, amb un nou conjunt d'índexs $J$, per a tot $j \in J$,

$$\inf_{x \in \mathfrak{R}_j} f(x)|\mathfrak{R}_j|.$$

Ara considerem el conjunt d'índex dels rectangles definits per $\{t_{1,0}, t_{1,1}\} \times Q_2 \times \cdots \times Q_d$, $I' \subset I$, i tenim

$$\sum_{i' \in I'} \inf_{x \in \mathfrak{R}_{i'}} f(x)|\mathfrak{R}_{i'}| \leq \sum_{j \in J} \inf_{x \in \mathfrak{R}_j} f(x)|\mathfrak{R}_j|.$$

I per tant

$$\begin{aligned}\sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| &= \sum_{i \in I \setminus I'} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| + \sum_{i' \in I'} \inf_{x \in \mathfrak{R}_{i'}} f(x)|\mathfrak{R}_{i'}| \leq \\ &\leq \sum_{j \in J} \inf_{x \in \mathfrak{R}_j} f(x)|\mathfrak{R}_j| + \sum_{i \in I \setminus J} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| = \sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i|.\end{aligned}$$

Cut my life into pieces
This is my last resort
Suffocation ♫
No breathing
Don't give a fuck
if I cut my arm, bleeding

però, per la definició de suma superior i inferior (7.1.3),

$$\sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| = \mathrm{s}(f, P) \quad \text{i} \quad \sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| = \mathrm{s}(f, Q),$$

i per tant trobem

$$\mathrm{s}(f, P) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| \leq \sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x)|\mathfrak{R}_i| = \mathrm{s}(f, Q). \qquad \square$$

**Proposició 7.1.5.** *Siguin $P, Q$ dues particions arbitràries d'un rectangle $\mathfrak{R} \subset \mathbb{R}^d$ i $f \colon \mathfrak{R} \to \mathbb{R}^d$ una funció acotada. Aleshores*

$$\mathrm{s}(f, P) \leq \mathrm{S}(f, Q).$$

*Demostració.* Considerem la partició definida per $P \cup Q$. Com que $Q \subseteq P \cup Q$ i $Q \subseteq P \cup Q$, $P \cup Q$ és més fina que $P$ i $Q$. Per tant, per la proposició 7.1.4, tenim

$$\mathrm{s}(f, P) \leq \mathrm{s}(f, P \cup Q) \leq \mathrm{S}(f, P \cup Q) \leq \mathrm{S}(f, Q). \qquad \square$$

**Definició 7.1.6** (Integral superior i inferior)**.** Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores definim la integral superior de $f$ en $\mathfrak{R}$ com

$$\int^{\mathfrak{R}^+} f = \inf_{P \in \mathcal{P}} \mathrm{S}(f, P)$$

i la integral inferior de $f$ en $\mathfrak{R}$ com

$$\int_{\mathfrak{R}^-} f = \sup_{P\in\mathcal{P}} \mathrm{s}(f,P),$$

on $\mathcal{P}$ és el conjunt de particions de $\mathfrak{R}$.

**Proposició 7.1.7.** *Siguin $R$ un rectangle de $\mathbb{R}^d$ i $f\colon \mathfrak{R}\to\mathbb{R}$ una funció acotada. Aleshores*

$$\int_{\mathfrak{R}^-} f \le \int^{\mathfrak{R}^+} f.$$

*Demostració.* Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Com que, per la proposició 7.1.5, tenim $\mathrm{s}(f,P)\le \mathrm{S}(f,Q)$ per a $P,Q\in\mathcal{P}$ arbitraris, ha de ser

$$\int_{\mathfrak{R}^-} f = \sup_{P\in\mathcal{P}} \mathrm{s}(f,P) \le \inf_{P\in\mathcal{P}} \mathrm{S}(f,P) = \int^{\mathfrak{R}^+} f. \qquad \square$$

**Definició 7.1.8** (Funció integrable Riemann)**.** Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f\colon \mathfrak{R}\to\mathbb{R}$ una funció acotada. Direm que $f$ és integrable Riemann si $\int_{\mathfrak{R}^-} f = \int^{\mathfrak{R}^+} f$.

També direm que $\int_{\mathfrak{R}} f = \int_{\mathfrak{R}^-} f = \int^{\mathfrak{R}^+} f$ és la integral Riemann de $f$ en $\mathfrak{R}$.

**Teorema 7.1.9** (Criteri d'integrabilitat Riemann)**.** *Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$, $\{\mathfrak{R}_i\}_{i\in I}$ la família de subrectangles de $\mathfrak{R}$ definits per $P$ i $f\colon \mathfrak{R}\to\mathbb{R}$ una funció acotada. Aleshores $f$ és integrable Riemann si i només si per a tot $\varepsilon>0$ existeix una partició $P$ tal que*

$$\mathrm{S}(f,P)-\mathrm{s}(f,P) = \sum_{i\in I}\left(\sup_{x\in\mathfrak{R}_i} f(x) - \inf_{x\in\mathfrak{R}_i} f(x)\right)|\mathfrak{R}_j| < \varepsilon.$$

*Demostració.* Comencem demostrant que la condició és necessària ($\Rightarrow$). Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Per la definició de funció integrable Riemann (7.1.8) i la definició de integral superior i inferior (7.1.6) tenim

$$\sup_{P\in\mathcal{P}} \mathrm{s}(f,P) = \int_{\mathfrak{R}^-} f = \int_{\mathfrak{R}} f = \int^{\mathfrak{R}^+} f = \inf_{P\in\mathcal{P}} \mathrm{S}(f,P),$$

per tant, existeixen un $\varepsilon>0$ i unes particions $P,Q\in\mathcal{P}$ tals que

$$-\frac{\varepsilon}{2} + \int_{\mathfrak{R}} f < \mathrm{s}(f,P),$$

i

$$\mathrm{S}(f,Q) < \frac{\varepsilon}{2} + \int_{\mathfrak{R}} f.$$

Per la proposició 7.1.4 tenim $\mathrm{s}(f,P)\le \mathrm{s}(f,P\cup Q)\le \mathrm{S}(f,P\cup Q)\le \mathrm{S}(f,Q)$, per tant ha de ser $\mathrm{S}(f,P\cup Q)-\mathrm{s}(f,P\cup Q)<\varepsilon$, com calia veure.

Per demostrar que la condició és suficient ($\Leftarrow$) veiem que, per hipòtesi,

$$0 \le \int^{\mathfrak{R}^+} f - \int_{\mathfrak{R}^-} f \le \mathrm{S}(f,P)-\mathrm{s}(f,P) < \varepsilon,$$

i quan $\varepsilon \to 0$ ha de ser, per la definició de funció integrable Riemann (7.1.8),

$$\int^{\mathfrak{R}^+} f = \int_{\mathfrak{R}^-} f = \int_{\mathfrak{R}} f. \qquad \square$$

**Notació 7.1.10** (Límit d'una partició)**.** Sigui $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Quan vulguem parlar d'una partició de $\mathfrak{R}$ que es fa fina ho denotarem amb

$$\lim_{P \in \mathcal{P}},$$

que es refereix a definir una partició $P$ de $\mathfrak{R}$ tal que

$$\max_{i \in I} \max_{x,y \in \mathfrak{R}_i} \|x - y\| \to 0$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per $P$.

**Corol·lari 7.1.11.** *Si $\mathcal{P}$ és el conjunt de particions de $\mathfrak{R}$, aleshores $f$ és integrable Riemann si i només si*

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) - \mathrm{s}(f, P) = 0.$$

**Teorema 7.1.12.** *Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada i contínua. Aleshores $f$ és integrable Riemann en $\mathfrak{R}$.*

*Demostració.* Pel Teorema de Heine (5.3.3), $f$ és uniformement contínua en $\mathfrak{R}$, per tant, per la definició de continuïtat uniforme (5.3.2), donat un $\varepsilon > 0$ hi ha un $\delta > 0$ tal que

$$|f(x) - f(y)| < \frac{\varepsilon}{|\mathfrak{R}|} \text{ si } \|x - y\| < \delta.$$

Sigui $\{\mathfrak{R}_i\}_{i \in I}$ el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició $P$ de $\mathfrak{R}$ tal que

$$\max_{i \in I} \max_{x,y \in \mathfrak{R}_i} \|x - y\| < \delta,$$

això és que els diàmetres dels subrectangles definits per la partició $P$ estiguin fitats per $\delta$.

Considerem

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) = \sum_{i \in I} \left( \sup_{x \in \mathfrak{R}_i} f(x) - \inf_{x \in \mathfrak{R}_i} f(x) \right) |\mathfrak{R}_i|. \tag{7.1}$$

Com que, per hipòtesi, $f$ és contínua en cada $\mathfrak{R}_i$, pel Teorema de Weierstrass (5.2.12) tenim que els màxims i mínims de $f$ en cada $\mathfrak{R}_i$ són accessibles. Denotem doncs amb $M_i, m_i$ els punts de $\mathfrak{R}_i$ tals que $f(M_i) = \max_{x \in \mathfrak{R}_i} f(x)$ i $f(m_i) = \min_{x \in \mathfrak{R}_i} f(x)$. Per (7.1) tindrem $\|M_i - m_i\| < \delta$, i com que $f$ és contínuament uniforme en cada $\mathfrak{R}_i$, $f(M_i) - f(m_i) < \frac{\varepsilon}{|\mathfrak{R}|}$, i per tant tenim

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) = \sum_{i \in I} \left( \sup_{x \in \mathfrak{R}_i} f(x) - \inf_{x \in \mathfrak{R}_i} f(x) \right) |\mathfrak{R}_i| \leq \frac{\varepsilon}{|\mathfrak{R}|} \sum_{i \in \mathfrak{R}_i} |\mathfrak{R}_i| = \varepsilon,$$

i això completa la prova. $\square$

### 7.1.2 La integral com a límit de sumes

**Definició 7.1.13** (Suma de Riemann)**.** Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $f\colon \mathfrak{R} \to \mathbb{R}$ una funció acotada i $P$ una partició de $\mathfrak{R}$. Aleshores definim la suma de Riemann de $f$ associada a $P$ com

$$\Sigma(f, P) = \sum_{i \in I} f(\xi_i)|\mathfrak{R}_i|,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per $P$ i $\xi_i$ és un punt qualsevol de $\mathfrak{R}_i$, per a tot $i \in I$.

**Observació 7.1.14.**

$$\mathrm{s}(f, P) \leq \Sigma(f, P) \leq \mathrm{S}(f, P).$$

**Proposició 7.1.15.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$ i $f\colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores $f$ és integrable Riemann si i només si existeix un $L \in \mathbb{R}$ tal que*

$$\lim_{P \in \mathcal{P}} \Sigma(f, P) = L.$$

*Demostració.* Pel corol·lari 7.1.11 tenim

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) = \lim_{P \in \mathcal{P}} \mathrm{s}(f, P),$$

i per l'observació 7.1.14 i el Teorema del sandvitx (5.2.13) ha de ser

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) = \lim_{P \in \mathcal{P}} \Sigma(f, P) = \lim_{P \in \mathcal{P}} \mathrm{s}(f, P),$$

i amb això es veu que ha de existir un real $L$ tal que $\lim_{P \in \mathcal{P}} \Sigma(f, P) = L$. □

**Notació 7.1.16.** Seguint el resultat de la proposició 7.1.15 denotarem

$$\int_{\mathfrak{R}} f(x)dx = \Sigma(f, P_n) = \sum_{i \in I} f(x)|\mathfrak{R}_i| = L.$$

on $\int$ es refereix al sumatori infinit, $f(\xi_i)$ es transforma en $f(x)$ i $|\mathfrak{R}_i|$ s'escriu $dx$, tot quan fem la partició "infinitament més fina", amb el límit $\lim_{P \in \mathcal{P}} P$.

### 7.1.3 Propietats de la integral Riemann definida

**Proposició 7.1.17.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f, g\colon \mathfrak{R} \to \mathbb{R}$ dues funcions integrables Riemann. Aleshores són certs els següents enunciats:*

1. *Siguin $\lambda, \mu$ dos escalars. Aleshores*

$$\int_{\mathfrak{R}} (\lambda f + \mu g) = \lambda \int_{\mathfrak{R}} f + \mu \int_{\mathfrak{R}} g.$$

2. *La funció producte $fg$ també és integrable Riemann.*

*3. Sigui $C$ un escalar. Si $f(x) \leq Cg(x)$ per a tot $x \in \mathfrak{R}$, aleshores*

$$\int_{\mathfrak{R}} f \leq C \int_{\mathfrak{R}} g.$$

*Demostració.* Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$.

Comencem demostrant el punt (1), Per la proposició 7.1.15 i la definició de suma de Riemann (7.1.13) tenim

$$\sum_{i \in I} (\lambda f(\xi_i) + \mu g(\xi_i)) |\mathfrak{R}_i|,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició $P \in \mathcal{P}$ i $\xi_i$ és un punt qualsevol de $\mathfrak{R}_i$ per a tot $i \in I$. Això ho podem reescriure com

$$\lambda \sum_{i \in I} f(\xi_i)|\mathfrak{R}_i| + \mu \sum_{i \in I} g(\xi_i)|\mathfrak{R}_i|$$

i per tant

$$\int_{\mathfrak{R}} (\lambda f + \mu g) = \lambda \int_{\mathfrak{R}} f + \mu \int_{\mathfrak{R}} g,$$

com volíem demostrar.

Demostrem ara el punt (2) (En veritat la demostraré quan em doni la gana, i resulta que això no és ara).

Podem veure el punt (3) a partir del punt (1), ja que si $f(x) \leq Cg(x)$ per a tot $x \in \mathfrak{R}$, amb $\xi_i$ qualsevol punt de $\mathfrak{R}_i$ per tot $i \in I$, on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$, tenim

$$\sum_{i \in I} f(\xi_i)|\mathfrak{R}_i| \leq C \sum_{i \in I} g(\xi_i)|\mathfrak{R}_i|,$$

i ja hem acabat. □

**Teorema 7.1.18.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $\mathcal{S}$ un conjunt de rectangles disjunts de $\mathfrak{R}$ tals que $\bigcup_{S \in \mathcal{S}} S = \mathfrak{R}$ i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores $f$ és integrable Riemann en $\mathfrak{R}$ si i només si $f$ és integrable Riemann en cada $S \in \mathcal{S}$, i*

$$\int_{\mathfrak{R}} f = \sum_{S \in \mathcal{S}} \int_S f.$$

*Demostració.* Comencem demostrant la doble implicació ($\Leftrightarrow$). Suposem que $f$ és integrable Riemann en $\mathfrak{R}$. Com que $f$ és integrable Riemann en $\mathfrak{R}$, per la proposició 7.1.15 i la definició de suma de Riemann (7.1.13). Tenim que, sent $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$, existeix un real $L$ tal que

$$\sum_{i \in I} f(x)|\mathfrak{R}_i| = L,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició $P \in \mathcal{P}$. Considerem ara el conjunt de particions de $S$, per a tot $S \in \mathcal{S}$, que denotarem

com $\mathcal{P}_S$. Com que $S \subset \mathfrak{R}$ per a tot $S \in \mathcal{S}$, per la definició de partició d'un rectangle (7.1.2), tenim que

$$\lim_{P_S \in \mathcal{P}_S} P_S \subset \lim_{P \in \mathcal{P}} P,$$

per a tot $S \in \mathcal{S}$; i com que $\bigcup_{S \in \mathcal{S}} S = \mathfrak{R}$ tenim que

$$\bigcup_{S \in \mathcal{S}} \lim_{P_S \in \mathcal{P}_S} P_S = \lim_{P \in \mathcal{P}} P.$$

Per tant, si $I_S$ és el conjunt d'índexs dels subrectangles $\mathfrak{R}_{S,i}$ de $S$ definits per una partició $P_S$, per a tot $S \in \mathcal{S}$, com que, per hipòtesi, els rectangles $S \in \mathcal{S}$ són disjunts, tenim

$$\sum_{i \in I} f(x)|\mathfrak{R}_i| = \sum_{S \in \mathcal{S}} \sum_{i \in I_S} f(x)|\mathfrak{R}_{S,i}| = L,$$

i, de nou, per la proposició 7.1.15 tenim que $f$ és integrable en cada $S \in \mathcal{S}$, com volíem veure.

Aquesta demostració també ens serveix per veure que

$$\int_{\mathfrak{R}} f = \sum_{S \in \mathcal{S}} \int_S f,$$

per la definició de suma de Riemann (7.1.13). □

**Teorema 7.1.19.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f\colon \mathfrak{R} \to \mathbb{R}$ una funció integrable Riemann amb $|f(x)| \leq M$ per a tot $x \in \mathfrak{R}$. Aleshores la funció $|f|$ és integrable Riemann i*

$$\left| \int_{\mathfrak{R}} f \right| \leq \int_{\mathfrak{R}} |f| \leq M|\mathfrak{R}|.$$

*Demostració.* Sigui $\{\mathfrak{R}_i\}_{i \in I}$ el conjunt de subrectangles definits per una partició de $\mathfrak{R}$. Aleshores

$$\sup_{x \in \mathfrak{R}_i} f(x) - \inf_{x \in \mathfrak{R}_i} f(x) = \sup_{x,y \in \mathfrak{R}_i} |f(x) - f(y)|, \quad \text{per a tot } i \in I,$$

i

$$\sup_{x \in \mathfrak{R}_i} |f(x)| - \inf_{x \in \mathfrak{R}_i} |f(x)| = \sup_{x,y \in \mathfrak{R}'_i} ||f(x)| - |f(y)||, \quad \text{per a tot } i \in I.$$

Per tant, per la definició de suma superior i inferior (7.1.3), si $P$ és una partició de $\mathfrak{R}$ tenim

$$\mathrm{S}(|f|, P) - \mathrm{s}(|f|, P) \leq \mathrm{S}(f, P) - \mathrm{s}(f, P)$$

Com que, per hipòtesi, $f$ és integrable Riemann, pel Teorema del criteri d'integrabilitat Riemann (7.1.9) tenim que per a tot $\varepsilon > 0$ existeix una partició $P$ de $\mathfrak{R}$ tal que

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) < \varepsilon,$$

el que significa que

$$\mathrm{S}(|f|, P) - \mathrm{s}(|f|, P) \leq \mathrm{S}(f, P) - \mathrm{s}(f, P) < \varepsilon.$$

I pel mateix criteri d'integrabilitat Riemann $|f|$ també és integrable Riemann.

Per veure les desigualtats de l'enunciat, amb $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$ i $\{\mathfrak{R}_i\}_{i\in I}$ el conjunt de subrectangles definits per una partició $\lim_{P\in\mathcal{P}}$ de $\mathfrak{R}$, tenim

$$\left|\int_{\mathfrak{R}} f\right| = \lim_{P\in\mathcal{P}}\left|\sum_{i\in I} f(x)|\mathfrak{R}_i|\right| \leq \lim_{P\in\mathcal{P}}\sum_{i\in I}|f(x)||\mathfrak{R}_i| = \int_{\mathfrak{R}}|f|.$$

Com que, per hipòtesi, $|f(x)| \leq M$ per a tot $x \in \mathfrak{R}$, tenim

$$\int_{\mathfrak{R}}|f| \leq \int_{\mathfrak{R}} M = M|\mathfrak{R}|. \qquad \square$$

**Corol·lari 7.1.20.** *Si $f(x) \geq 0$ per a tot $x \in \mathfrak{R}$, $\int_{\mathfrak{R}} f \geq 0$.*

**Proposició 7.1.21.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f\colon \mathfrak{R} \to \mathbb{R}$ una funció contínua i acotada tal que $f(x) \geq 0$ per a tot $x \in \mathfrak{R}$ i $\int_{\mathfrak{R}} f = 0$. Aleshores $f(x) = 0$ per a tot $x \in \mathfrak{R}$.*

*Demostració.* Observem que la proposició té sentit pel Teorema 7.1.12.

Farem aquesta demostració per reducció a l'absurd. Suposem que existeix un punt $c \in \mathfrak{R}$ tal que $f(c) > 0$. Com que, per hipòtesi, $f$ és contínua en un rectangle $\mathfrak{R}$, acotat per la definició de rectangle (7.1.1), pel Teorema de Heine (5.3.3) $f$ és uniformement contínua en $\mathfrak{R}$, per tant, per la definició de continuïtat uniforme (5.3.2), per a tot $\varepsilon > 0$ existeix un $\delta > 0$ tals que

$$\text{si } |x-c| < \delta \text{ aleshores } |f(x) - f(c)|t < \varepsilon = \frac{f(c)}{2}.$$

Per tant, si definim un rectangle $S$ inscrit en la bola de radi $\delta$ centrada en el punt $c$, $\mathrm{B}(c,\delta)$, tenim

$$\int_{\mathfrak{R}} f \geq \int_S f \geq \frac{f(x)}{2}|S| > 0,$$

però això contradiu la hipòtesi de que $\int_{\mathfrak{R}} f = 0$, per tant la proposició queda demostrada per reducció a l'absurd. $\square$

## 7.2 Les funcions integrables Riemann

### 7.2.1 Caracterització de les funcions integrables Riemann

**Definició 7.2.1** (Oscil·lació d'una funció en un punt)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt, $\mathrm{B}(a,\delta) \subseteq U$ una bola oberta centrada en $a$ de radi $\delta > 0$ i $f\colon U \to \mathbb{R}^m$ una funció. Aleshores definim l'aplicació

$$\omega_f(a) = \lim_{\delta\to 0}\sup_{x,y\in B(a,\delta)}\|f(x) - f(y)\|$$

com l'oscil·lació de la funció $f$ en el punt $a$.

**Proposició 7.2.2.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f\colon U \to \mathbb{R}^m$ una funció definida en un punt $a \in U$. Aleshores $f$ és contínua en $a$ si i només si $\omega_f(a) = 0$, on $\omega_f(a)$ és la oscil·lació de $f$ en $a$.*

*Demostració.* Suposem que $\omega_f(a) = 0$. Observem que quan $\delta \to 0$, per a tot $x, y, \in \mathrm{B}(a, \delta)$ tenim $x \to a$ i $y \to a$, i com que $\omega_f(a) = 0$, podem escriure

$$\begin{aligned}\omega_f(a) &= \lim_{\delta \to 0} \sup_{x,y \in B(a,\delta)} \|f(x) - f(y)\| \\ &= \lim_{x,y \to a} \|f(a) - f(x)\| = 0\end{aligned}$$

i per tant tenim $\lim_{x \to a} f(x) = \lim_{y \to a} f(y)$, i equivalentment

$$\lim_{x \to a} f(x) = f(a),$$

que és la definició de funció contínua (5.2.1). □

**Definició 7.2.3** (Conjunt de discontinuïtats d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $f \colon U \to \mathbb{R}^m$ una funció, $\tau$ un escalar positiu i $\omega_f(x)$ l'oscil·lació de $f$ en un punt $x \in U$. Aleshores denotem el conjunt

$$D_\tau = \{x \in U \mid \omega_f(x) \geq \tau\}$$

com el conjunt de desigualtats majors que $\tau$ d'una funció.

**Observació 7.2.4.** *$D_\tau$ és compacte.*

**Definició 7.2.5** (Contingut exterior de Jordan)**.** Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $A \subseteq \mathfrak{R}$ un conjunt, $1_A$ la funció indicatriu de $A$ i $\{\mathfrak{R}_i\}_{i \in I}$ el conjunt de subrectangles definits per una partició de $\mathfrak{R}$ amb la condició de que $\mathfrak{R}_i \cap A \neq \emptyset$ per a tot $i \in I$. Aleshores definim

$$c(A) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} 1_A(x) |\mathfrak{R}_i|$$

com el contingut exterior de Jordan de $A$.

**Nota 7.2.6.** *La condició sobre $\mathfrak{R}_i$ pot dir-se com que els $\mathfrak{R}_i$ cobreixen $A$.*

**Observació 7.2.7.** *Siguin $\{A_i\}_{i \in I}$ un conjunt finit de conjunts amb $c(A_i) = 0$ per a tot $i \in I$ i $A = \bigcup_{i \in I} A_i$. Aleshores $c(A) = 0$.*

**Teorema 7.2.8.** *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f \colon \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores $f$ és integrable Riemann en $\mathfrak{R}$ si i només si el contingut exterior de Jordan del conjunt de desigualtats majors que $\tau > 0$ de $f$ en $\mathfrak{R}$ és cero, és a dir, $c(D_\tau) = 0$ per a tot $\tau > 0$.*

*Demostració.* Comencem amb la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $D_\tau = 0$ per a tot $\tau > 0$. Per la definició de contingut exterior de Jordan (7.2.5) això és

$$\sum_{i \in I} \inf_{x \in \mathfrak{R}_i} 1_{D_\tau}(x) |\mathfrak{R}_i| = 0$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició del conjunt $\mathcal{P}$ de particions de $\mathfrak{R}$. Considerem el conjunt de subrectangles $\{\mathfrak{R}_j\}_{j \in J}$ tals que $\mathfrak{R}_j \cap D_\tau \neq \emptyset$. Ara bé, per la proposició 7.2.2 tenim que $f$ és contínua, i pel Teorema 7.1.12 veiem que $f$ és integrable Riemann en $\mathfrak{R}$.

Comprovem ara la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $f$ és integrable Riemann en $\mathfrak{R}$ i fixem $\varepsilon > 0$. Pel Teorema del criteri d'integrabilitat Riemann (7.1.9) tenim que per a tot $\varepsilon > 0$ existeix una partició $P$ de $\mathfrak{R}$ tal que

$$\sum_{i\in I}\left(\sup_{x\in\mathfrak{R}_i} f(x) - \inf_{x\in\mathfrak{R}_i} f(x)\right)|\mathfrak{R}_j| < \varepsilon$$

on $\{\mathfrak{R}_i\}_{i\in I}$ és el conjunt de subrectangles definits per $P$. Sigui $J$ el conjunt de subrectangles $\{\mathfrak{R}_j\}_{j\in J}$ tals que $\mathfrak{R}_j \cap D_\tau \neq \emptyset$. Tindrem

$$\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x) \geq \tau$$

per a tot $j \in J$, i per tant, amb $\mathfrak{R}' = \bigcup_{j\in J}\mathfrak{R}_j$, per la definició de contingut exterior de Jordan (7.2.5)

$$\begin{aligned}\sum_{j\in J}\left(\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x)\right)|\mathfrak{R}_j| &\geq \sum_{j\in J}\tau|\mathfrak{R}_j| \\ &= \tau\sum_{j\in J}|\mathfrak{R}_j| \\ &\geq \tau\sum_{j\in I}\inf_{x\in\mathfrak{R}_j} 1_{\mathfrak{R}'}(x)|\mathfrak{R}_j| \\ &= \tau c(D_\tau)\end{aligned}$$

Ara bé, com que $f$ és integrable, pel Teorema del criteri d'integrabilitat Riemann (7.1.9) tenim que

$$\sum_{j\in J}\left(\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x)\right)|\mathfrak{R}_j| < \varepsilon$$

per a tota $\varepsilon > 0$, i per tant quan $\varepsilon \to 0$ ha de ser $D_\tau = 0$, com volíem veure. □

### 7.2.2 Integració sobre conjunts generals

**Nota 7.2.9.** *Tota la teoria de l'integració Riemann que hem vist ha estat sobre rectangles. Ara tractem de generalitzar-la desfent-nos d'aquesta limitació.*

# Capítol 8

# Càlcul vectorial

*sona divertit*

# Bibliografia


[1] Joaquim Bruna. «Aspectes mètrics, geomètrics i topològics de l'espai euclidià. Funcions de vàries variables, corbes i superfícies». 2017.

[2] Joaquim Bruna. «Càlcul Diferencial en varies variables». 2017.

[3] Joaquim Bruna. «Càlcul Integral en vàries variables». 2017.

[4] Joaquim Bruna. «Anàlisi Vectorial». 2017.

[5] T. Apostol. *Mathematical analysis*. Anglès. Addison-Wesley, 1974. ISBN: 0201002884.

[6] J.E. Marsden i A.J. Tromba. *Cálculo Vectorial*. Castellà. 5a ed. Addison-Wesley, 2004. ISBN: 9788478290697.

[7] Wendell Helms Fleming. *Functions of Several Variables*. Anglès. 1977. ISBN: 978-1-4684-9461-7.

[8] David M. Bressoud. *Second Year Calculus. From celestial mechanics to special relativity*. Anglès. Springer, 1991. ISBN: 978-1-4612-0959-1.


Els apunts que he seguit per escriure la majoria d'aquesta part són els escrits pel professor de l'assignatura; [1, 2, 3, 4]. De moment no han estat publicats però en té pensat fer-ne un llibre. Es poden trobar al campus virtual.

El llibre [5] és molt útil per tenir una visió més organitzada i pautada del curs. També tracta temes més avançats als de l'assignatura.

La bibliografia del curs inclou els textos [6, 7, 8].

# Part V

# Estructures algebraiques

# Capítol 9

# Teoria de grups

## 9.1 Grups

### 9.1.1 Propietats bàsiques dels grups

**Definició 9.1.1** (Grup)**.** Siguin $G \neq \emptyset$ un conjunt i $*\colon G \times G \to G$ una operació que satisfà

1. Per a tot $x, y, z \in G$
$$x * (y * z) = (x * y) * z.$$
2. Existeix un $e \in G$ tal que per a tot $x \in G$
$$x * e = e * x = x.$$
3. Per a cada $x \in G$ existeix $x'$ tal que
$$x * x' = x' * x = e.$$

Aleshores $G$ és un grup amb la l'operació $*$. També direm $*$ dota al conjunt $G$ d'estructura de grup.

**Proposició 9.1.2.** *Siguin $G$ un grup amb l'operació $*$ i $e \in G$ tal que $x * e = e * x = x$ per a tot $x \in G$. Aleshores $e$ és únic.*

*Demostració.* Suposem que existeix un altre element de $G$ amb aquesta propietat, diguem-ne $\hat{e} \in G$. Aleshores hauria de ser
$$e * \hat{e} = e,$$
però per hipòtesi
$$e * \hat{e} = \hat{e}.$$
Per tant, ha de ser $e = \hat{e}$. □

**Definició 9.1.3** (Element neutre d'un grup)**.** Siguin $G$ un grup amb l'operació $*$ i $e$ un element de $G$ tal que $x * e = e * x = x$ per a tot $x \in G$. Aleshores direm que $e$ és l'element neutre de $G$.

Aquesta definició té sentit per la proposició 9.1.2.

**Notació 9.1.4.** Donat un grup $G$ amb l'operació $*$ escriurem

$$(x_1 * x_2) * x_3 = x_1 * x_2 * x_3.$$

També denotarem

$$x^n = x * \overset{n)}{\cdots} * x.$$

Si denotem la conjugació del grup per $+$ usarem la notació additiva i escriurem

$$x_1 + \cdots + x_n$$

per referir-nos a la conjugació de $+$ amb si mateix $n$ vegades.

També denotarem

$$nx = x + \overset{n)}{\cdots} + x.$$

**Proposició 9.1.5.** *Siguin $G$ un grup amb l'operació $*$ i $a, b, c$ tres elements de $G$. Aleshores*

1. $a * c = b * c \Rightarrow a = b$.
2. $c * a = c * b \Rightarrow a = b$.

*Demostració.* Farem només la demostració del punt (1) ja que l'altre és anàloga.

Com que per hipòtesi $G$ és un grup, per la definició de grup (9.1.1) tenim que existeix $c'$ tal que $c * c' = e$, on $e$ és l'element neutre $G$, i tenim

$$a * c * c' = b * c * c',$$

el que significa que

$$a * e = b * e,$$

i ens queda $a = b$. □

**Proposició 9.1.6.** *Siguin $G$ un grup amb l'operació $*$ i element neutre $e$ i $a$ un element de $G$. Aleshores existeix un únic $a' \in G$ tal que*

$$a * a' = a' * a = e.$$

*Demostració.* Notem que existeix un $a' \in G$ que satisfà l'equació per la definició de grup (9.1.1), i per tant la proposició té sentit.

Suposem doncs que existeix $a'' \in G$ tal que

$$a * a'' = a'' * a = e.$$

Però aleshores tenim

$$a * a'' = e = a * a',$$

i per la proposició 9.1.5 ha de ser $a' = a''$, com volíem demostrar. □

**Definició 9.1.7** (Invers d'un element)**.** Siguin $G$ un grup amb l'operació $*$ i element neutre $e$ i $a$ un element de $G$. Per la definició de grup tenim que existeix un $a' \in G$ tal que

$$a * a' = a' * a = e.$$

Aleshores direm que $a'$ és l'invers de $a$ en $G$, i el denotarem per $a^{-1}$.

Aquesta definició té sentit per la proposició 9.1.6 i la notació introduïda en 9.1.4.

**Proposició 9.1.8.** *Sigui $G$ un grup amb l'operació $*$ i element neutre $e$. Aleshores*

$$e^{-1} = e.$$

*Demostració.* Per la definició de grup (9.1.1) tenim que

$$e * e^{-1} = e^{-1} * e = e,$$

i per ha de ser $e^{-1} = e$. □

**Proposició 9.1.9.** *Siguin $G$ un grup amb l'operació $*$ i $a$ un element de $G$. Aleshores*

$$\left(a^{-1}\right)^{-1} = a.$$

*Demostració.* Sigui $e$ l'element neutre de $G$. Com que $\left(a^{-1}\right)^{-1}$ és l'invers de $a^{-1}$ tenim

$$\left(a^{-1}\right)^{-1} * a^{-1} = e$$

però també tenim que

$$a * a^{-1} = e.$$

Per tant és

$$a * a^{-1} = (a^{-1})^{-1} * a^{-1},$$

i per la proposició 9.1.5 ha de ser

$$a = \left(a^{-1}\right)^{-1}.$$ □

**Proposició 9.1.10.** *Siguin $G$ un grup amb l'operació $*$ i $a, b$ dos elements de $G$. Aleshores*

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

*Demostració.* Sigui $e$ l'element neutre de $G$. Considerem

$$\begin{aligned}(b^{-1} * a^{-1}) * (a * b) &= b^{-1} * a^{-1} * a * b \\ &= b^{-1} * e * b \\ &= b^{-1} * b = e.\end{aligned}$$

i de manera anàloga trobem

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

Així doncs, per la proposició 9.1.6 tenim que $a * b$ és l'inversa de $b^{-1} * a^{-1}$, és a dir

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$ □

**Lemma 9.1.11.** *Siguin $G$ un grup amb l'operació $*$ i $a, b$ dos elements de $G$. Aleshores existeixen $x, y \in G$ únics tals que*

$$b * x = a \quad i \quad y * b = a.$$

*Demostració.* Fem només una de les demostracions, ja que l'altre és anàloga. Com que per hipòtesi $G$ és un grup, per la definició de grup (9.1.1) tenim que existeix $b^{-1} \in G$ tal que $b^{-1} * b = e$, on $e$ és l'element neutre de $G$. Per tant considerem

$$b^{-1} * (b * x) = b^{-1} * a$$

i per la definició de grup (9.1.1) tenim que això és equivalent a

$$(b^{-1} * b) * x = b^{-1} * a,$$

i de nou per la definició de grup, i per la definició de l'element neutre d'un grup (9.1.3),

$$e * x = x = b^{-1} * a;$$

i la unicitat ve donada per la proposició 9.1.2. □

**Teorema 9.1.12.** *Siguin $G$ un conjunt i $*\colon G \times G \to G$ una operació binària que satisfà $x * (y * z) = (x * y) * z$ per a tot $x, y, z \in G$. Aleshores els següents enunciats són equivalents:*

1. *$G$ és un grup amb l'operació $*$.*
2. *$G \neq \emptyset$ i per a tot $a, b \in G$ existeix uns únics $x, y \in G$ tals que*

$$b * x = a \quad i \quad y * b = a.$$

3. *Existeix $e \in G$ tal que per a tot $x \in G$ tenim $x * e = x$ i existeix un $x^{-1} \in G$ tal que $x * x^{-1} = e$.*

*Demostració.* Comencem demostrant (1)⇒(2). Suposem que $G$ és un grup amb l'operació. Veiem que $G$ no és buit per la definició de grup (9.1.1), i la segona part és el lemma 9.1.11.

Demostrem ara (2)⇒(3). La primera part es pot veure fixant $x \in G$. Pel punt (2) tenim que per a cada $a \in G$ existeix un únic $b \in G$ tal que

$$a * b = x,$$

i podem fer

$$a * b * e = x * e$$

i substituint ens queda

$$x * e = x.$$

Per veure la segona part notem que pel punt (2) tenim que per a tot $x \in G$ existeix un $a \in G$ tal que

$$x * a = e,$$

i aleshores $a = x^{-1}$.

Ara només ens queda veure (3)⇒(1). Tenim que per a tot $x \in G$ existeix un $x^{-1}$ tal que $x * x^{-1} = e$, i de la mateixa manera, existeix un $y \in G$ tal que $x^{-1} * y = e$. Per tant

$$\begin{aligned} e &= x^{-1} * y \\ &= x^{-1} * e * y \\ &= x^{-1} * x * x^{-1} * y \\ &= x^{-1} * x * e = x^{-1} * x. \end{aligned}$$

Així tenim que per a tot $x \in G$ es compleix $x * x^{-1} = x^{-1} * x = e$, d'on podem veure que $e * x = x * e$, i com que, per hipòtesi, l'operació $*$ satisfà $x * (y * z) = (x * y) * z$ per a tot $x, y, z \in G$ es compleix la definició de grup (9.1.1) i tenim que $G$ és un grup amb l'operació $*$.

Així tenim (1)⇒(2)⇒(3)⇒(1), com volíem veure. □

### 9.1.2 Subgrups i subgrups normals

**Definició 9.1.13** (Subgrup)**.** Siguin $G$ un grup amb l'operació $*$ i $H \subseteq G$ un subconjunt de $G$ tal que $H$ sigui un grup amb l'operació $*$. Aleshores diem que $H$ és un subgrup de $G$.

També ho denotarem com $H \leq G$.

**Observació 9.1.14.** *$e \in H$.*

**Proposició 9.1.15.** *Siguin $G$ un grup amb l'operació $*$ i element neutre $e$ i $H$ un subconjunt de $G$. Aleshores $H$ és un subgrup de $G$ si i només si per a tot $x, y \in H$ tenim que $x * y^{-1} \in H$.*

*Demostració.* Demostrem primer que la condició és necessària (⇒). Això ho podem veure per la definició de grup (9.1.1), ja que tenim que $y^{-1}$ existeix i pertany a $H$, i per tant $x * y^{-1}$ també pertany a $H$.

Demostrem ara que la condició és suficient (⇐). Tenim que per a tot $x \in H$ es compleix

$$x * x^{-1} = e,$$

i per tant $e \in H$. També tenim que per a tot $x \in H$ es compleix

$$e * x^{-1} = x^{-1},$$

i per tant $x^{-1} \in H$.

Ara només ens queda veure que $*$ és tancat en $H$; és a dir, que per a tot $x, y \in H$ tenim $x * y \in H$. Com que ja hem vist que $y^{-1}$ existeix i pertany a $H$, per la proposició 9.1.9 tenim

$$x * y^{-1} = x * y$$

i per hipòtesi $x * y \in H$.

Per tant, per la definició de grup (9.1.1) tenim que $H$ és un grup amb l'operació $*$, i com que per hipòtesi $H \subseteq G$ per la definició de subgrup (9.1.13) tenim que $H$ és un subgrup de $G$. □

**Proposició 9.1.16.** *Siguin $G$ un grup amb l'operació $*$ i element neutre $e$, $\{H_i\}_{i \in I}$ una família de subgrups de $G$ i $H = \bigcap_{i \in I} H_i$. Aleshores $H$ és un subgrup de $G$.*

*Demostració.* Ho demostrarem amb la proposició 9.1.15. Tenim $H \subseteq G$ i $H \neq \emptyset$, ja que $e \in H$. Comprovem ara que per a tot $x, y \in H$ tenim $x * y^{-1} \in H$. Tenim que si $x, y \in H$, per la definició de $H$, $x, y \in H_{i \in I}$; i com que $H_{i \in I}$ és un subgrup de $G$, $x * y^{-1} \in H_{i \in I}$ per la proposició 9.1.15, i per tant $x * y^{-1} \in H$, com volíem veure. □

**Proposició 9.1.17.** *Siguin $G$ un grup amb l'operació $*$ i element neutre $e$, $S \neq \emptyset$ un subconjunt de $G$, $\{H_i\}_{i\in I}$ una família de subgrups de $G$ tals que $S \subseteq H_i$ per a tot $i \in I$ i $H = \bigcap_{i\in I} H_i$. Aleshores $H$ i és un subgrup de $G$.*

*Demostració.* Comprovem que $H$ existeix, és a dir, que $H \neq \emptyset$ tenim prou amb veure que $e \in H$. Veiem que $H$ és un subgrup de $G$ ho podem veure per la proposició 9.1.16. □

**Definició 9.1.18** (Mínim subgrup generat per un conjunt)**.** Siguin $G$ un grup amb l'operació $*$, $S$ un subconjunt de $G$, $\{H_i\}_{i\in I}$ una família de subgrups de $G$ tals que $S \subseteq H_i$ per a tot $i \in I$ i $H = \bigcap_{i\in I} H_i$. Aleshores direm que el subgrup $H \leq G$ és el mínim subgrup generat per $S$ i ho denotarem amb $\langle S\rangle$.

Aquesta definició té sentit per la proposició 9.1.17.

**Proposició 9.1.19.** *Siguin $G$ un grup amb l'operació $*$ i $g$ un element de $G$. Aleshores $\langle\{g\}\rangle = \{g^i\}_{i\in\mathbb{Z}}$.*

*Demostració.* Ho demostrem per doble inclusió.

Comencem veient que $\{g^i\}_{i\in\mathbb{Z}} \subseteq \langle\{g\}\rangle$. Per la definició de mínim subgrup generat per un conjunt (9.1.18) tenim que existeix una família de subconjunts de $G$ que denotarem per $\{H_i\}_{i\in I}$, amb $\{g\} \subseteq H = \bigcap_{i\in I} H_i$. Com que $\{H_i\}_{i\in I}$ són subgrups de $G$ tenim que, donat que $g \in H_i$, $g^n \in H_i$ per a tot $i \in I$ i tot $n \in \mathbb{Z}$ per la definició de grup (9.1.1), i per tant $g^n \in H$, el que és equivalent a dir que $g^n \in \langle g\rangle$ per a tot $n \in \mathbb{Z}$

Ara veiem que $\langle\{g\}\rangle \subseteq \{g^i\}_{i\in\mathbb{Z}}$. Denotarem $H_g = \{g^i\}_{i\in\mathbb{Z}}$. Hem de veure que $H_g$ és un grup amb l'operació $*$. Observem que per a tot $g^i, g^j \in H_g$, $g^i * g^{-j} = g^{i-j} \in H_g$, i per tant $H_g \leq G$. Ara bé, com que $\{g\} \subseteq H_g$, tenim que $H_g \in \{H_i\}_{i\in I}$, és a dir, que $H_g$ pertany a la família de subconjunts de $G$ que contenen $\{g\}$; el que significa que $\langle\{g\}\rangle \leq H_g$, i per tant $\langle\{g\}\rangle \subseteq \{g^i\}_{i\in\mathbb{Z}}$. □

**Definició 9.1.20** (Ordre d'un grup)**.** Sigui $G$ un grup amb l'operació $*$. Direm que $|G|$ és l'ordre del grup. Si $|G|$ és finit direm que $G$ és un grup d'ordre finit, i si $|G|$ no és finit direm que $G$ és un grup d'ordre infinit.

**Proposició 9.1.21.** *Siguin $G$ un grup amb l'operació $*$ i element neutre $e$ i $g$ un element de $G$. Aleshores*

$$|\langle\{g\}\rangle| = n \iff n = \min\{k \in \mathbb{N} \mid g^k = e\}.$$

*Demostració.* Comencem amb la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $n = \min\{k \in \mathbb{N} \mid g^k = e\}$. Pel criteri de divisibilitat d'Euclides (3.2.29) tenim que per a tot $t \in \mathbb{Z}$ existeixen uns únics $Q \in \mathbb{Z}$, $r \in \mathbb{N}$, amb $r < n$ tals que $t = Qn + r$. Per tant

$$\begin{aligned} g^t &= g^{Qm+r} \\ &= g^{Qm} * g^r \\ &= (g^m)^Q * g^r \\ &= e^Q * g^r = g^r. \end{aligned}$$

Per tant, com que $0 \leq r < n$, $|\langle\{g\}\rangle| = n$.

Fem ara la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $|\langle\{g\}\rangle| = n$. Com que el grup és finit per a cada $i \in \mathbb{Z}$ existeix $j \in \mathbb{Z}$ tal que $g^i = g^j$ i, com

que $\langle\{g\}\rangle$ és un grup, per la definició de grup (9.1.1) existeix $g^{-j} \in \langle\{g\}\rangle$ tal que $g^{i-j} = e$.

Sigui doncs $t \in \mathbb{N}$ tal que $g^t = e$. Aleshores, pel criteri de divisibilitat d'Euclides (3.2.29) existeixen uns únics $Q, r \in \mathbb{N}$, amb $r < n$ tals que $t = Qn + r$. Per tant

$$\begin{aligned} g^t &= g^{Qn+r} \\ &= g^{Qn} * g^r \\ &= (g^n)^Q * g^r \\ &= e^Q * g^r \\ &= g^r = e. \end{aligned}$$

i per tant $r = 0$, i tenim $t = Qn$, i per tant $n = \min\{k \in \mathbb{N} \mid g^k = e\}$. □

**Definició 9.1.22** (Conjugació entre conjunts sobre grups)**.** Siguin $G$ un grup amb l'operació $*$ i $H$ un subconjunt de $G$. Aleshores definim

$$GH = \{g * h \mid g \in G, h \in H\} \quad \text{i} \quad HG = \{h * g \mid g \in G, h \in H\}.$$

**Definició 9.1.23** (Subgrup normal)**.** Siguin $G$ un grup amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores direm que $H$ és un subgrup normal de $G$ si per a tot $x \in G$ tenim

$$\{x\}H = H\{x\}.$$

Ho denotarem com $H \trianglelefteq G$.

**Proposició 9.1.24.** *Siguin $G$ un grup amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores són equivalents*

1. $\{x\}H = H\{x\}$ *per a tot* $x \in G$.
2. $\{x^{-1}\}H\{x\} = H$ *per a tot* $x \in G$.
3. $\{x^{-1}\}H\{x\} \subseteq H$ *per a tot* $x \in G$.

*Demostració.* Comencem demostrant (1)⇒(2). Suposem que $H$ és un subgrup normal de $G$, per la definició de subgrup normal (9.1.23) tenim $\{x\}H = H\{x\}$ per a tot $x \in G$. Aleshores tenim

$$\begin{aligned} \{x\}H\{x^{-1}\} &= H\{x\}\{x^{-1}\} \\ &= \{h * x * x^{-1} \mid h \in H\} \\ &= \{h \mid h \in H\} = H. \end{aligned}$$

Continuem demostrant (2)⇒(3). Suposem que $\{x\}H\{x^{-1}\} = H$. Tenim que $\{x\}H\{x^{-1}\} = H \subseteq H$.

Demostrem ara (3)⇒(1). Suposem doncs que $\{x^{-1}\}H\{x\} \subseteq H$ per a tot $x \in G$. Això significa que per a tot $h \in H$ existeix un $h' \in H$ tal que $x * h * x^{-1} = h'$, i aleshores, per la definició de grup (9.1.1), $x * h = h' * x \in H$, i per tant $x * h \in H\{x\}$ per a tot $x \in G$. Així hem vist que $\{x\}H \subseteq H\{x\}$. Per veure l'altre inclusió es pot donar un argument anàleg, i per tant $\{x\}H = H\{x\}$.

I així hem vist que (1)⇒(2)⇒(3)⇒(1) i hem acabat. □

### 9.1.3 Grups cíclics i grups abelians

**Definició 9.1.25** (Grup abelià)**.** Sigui $G$ un grup amb l'operació $+$ tal que per a tot $x, y \in G$ satisfà

$$x + y = y + x.$$

Aleshores direm que $G$ és un grup abelià.

**Proposició 9.1.26.** *Sigui $G$ un grup amb l'operació $+$. Aleshores $G$ és un grup abelià si i només si per a tot $a, b \in G$ es compleix*

$$-(a + b) = -a - b.$$

*Demostració.* Que la condició és necessària ($\Rightarrow$) ho podem veure amb la definició de grup abelià (9.1.25) i la proposició 9.1.10.

Demostrem ara que la condició és suficient ($\Leftarrow$). Diem que l'element neutre de $G$ és $e$. Per la definició de grup (9.1.1) tenim que

$$(a + b) - (a + b) = e, \tag{9.1}$$

que és equivalent a

$$(a + b) - (a + b) - (-(a + b)) = -(-(a + b)),$$

i aleshores

$$\begin{aligned} a + b &= -(-(a + b)) \\ &= -(-b - a) && \text{(Proposició 9.1.10)} \\ &= -(-(b + a)) && \text{(Hipótesi (9.1))} \\ &= b + a, && \text{(Proposició 9.1.9)} \end{aligned}$$

i per la definició de grup abelià (9.1.25), $G$ és un grup abelià. □

**Definició 9.1.27** (Grup cíclic)**.** Siguin $G$ un grup amb l'operació $*$ i $g$ un element de $G$. Aleshores diem que el grup $\langle\{g\}\rangle$ amb l'operació $*$ és un grup cíclic i que $g$ és un generador del grup.

**Proposició 9.1.28.** *Sigui $G$ un grup cíclic amb l'operació $*$. Aleshores $G$ és un grup abelià.*

*Demostració.* Com que $G$ és un grup cíclic, per la definició de grup cíclic (9.1.27) tenim que existeix un $g$ tal que $\langle\{g\}\rangle = G$. Siguin $a, b$ dos elements de $G$, i com que $G$ és un grup cíclic, ha de ser $a = g^m$ i $b = g^n$ per a certs $m, n \in \mathbb{N}$. Ara bé, tenim que $g^m * g^n = g^m * g^n$, ja que

$$\begin{aligned} g^n * g^m &= g^{n+m} \\ &= g^{m+n} = g^m * g^n \end{aligned}$$

i aleshores $a * b = b * a$, i per la definició de grup abelià (9.1.25) hem acabat. □

**Proposició 9.1.29.** *Sigui $G$ un grup cíclic amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores $H$ és un grup cíclic.*

*Demostració.* Sigui $e$ l'element neutre de $G$. Per l'observació 9.1.14 tenim que $e \in H$. Si $H = \{e\}$ no hi ha res a demostrar. Suposem que $H \neq \{e\}$, aleshores existeix un $g \in G$ tal que $g^n \in H$ per a cert $n \in \mathbb{N}$. Sigui doncs $m$ l'enter més petit tal que $g^m \in H$; volem demostrar que $H = \langle\{g^m\}\rangle$.

Sigui $a$ un element de $H$. Aleshores com que $a \in H \subseteq G$, $a = g^t$ per a cert $t \in \mathbb{N}$, i pel criteri de divisibilitat d'Euclides (3.2.29) existeixen $Q, r \in \mathbb{N}$, amb $r < m$ tals que $t = Qm + r$, i per tant $g^t = g^{Qm+r}$. Aleshores tenim

$$g^r = (g^m)^{-Q} * g^t,$$

i ha de ser $g^r \in H$, ja que $g^m \in H$, i per la definició de grup (9.1.1) tenim que $(g^m)^{-1} \in H$. Per tant $g^r \in H$. Però ara bé, $m$ era el mínim enter tal que $g^m \in H$, i $r < m$, per tant ha de ser $g^r = e$, és a dir, $r = 0$ i per tant $t = Qm$; el que significa que $H = \{(g^m)^Q \mid Q \in \mathbb{N}\}$ i per la proposició 9.1.19 $H = \langle\{g^m\}\rangle$ i hem acabat. □

**Proposició 9.1.30.** *Siguin $G$ un grup cíclic amb l'operació $*$ d'ordre $n$ finit i $d \in \mathbb{N}$ un divisor de $n$. Aleshores existeix un únic subgrup de $G$ d'ordre $d$.*

*Demostració.* □

### 9.1.4 Grup quocient

**Proposició 9.1.31.** *Siguin $G$ un grup amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores la relació*

$$x \sim y \iff x * y^{-1} \in H \text{ per a tot } x, y \in G$$

*és una relació d'equivalència.*

*Demostració.* Sigui $e$ l'element neutre del grup $G$. Comprovem les propietats de la definició de relació d'equivalència:

1. Reflexiva: Sigui $x \in G$. Aleshores $x * x^{-1} = e$, i tenim l'observació 9.1.14.

2. Simètrica: Siguin $x, y \in G$ i suposem que $x \sim y$, això significa que $x * y^{-1} \in H$, i per la definició de grup (9.1.1) tenim que $(x * y^{-1})^{-1} \in H$, ja que per hipòtesi $H$ és un grup, i per les proposicions 9.1.10 i 9.1.9 tenim que
$$(x * y^{-1})^{-1} = y * x^{-1},$$
i això és $y \sim x$.

3. Transitiva: Siguin $x, y, z \in G$ i suposem que $x \sim y$ i $y \sim z$. Per tant $x * y^{-1} \in H$, i $y * z^{-1} \in H$. Com que per hipòtesi $H$ és un grup, tenim que
$$(x * y^{-1}) * (y * z^{-1}) \in H,$$
que és equivalent a $x * z^{-1} \in H$, i per tant $x \sim z$.

I per la definició de relació d'equivalència (2.3.2) hem acabat. □

**Proposició 9.1.32.** *Siguin $G$ un grup amb l'operació $*$ i $H$ un subgrup de $G$ i $\sim$ una relació d'equivalència tal que*

$$x \sim y \iff x * y^{-1} \in H \text{ per a tot } x, y \in G.$$

*Aleshores el conjunt quocient $G/H$ amb l'operació*

$$\begin{aligned} *\colon G/H \times G/H &\longrightarrow G/H \\ [x] * [y] &\longmapsto [x * y] \end{aligned}$$

*és un grup si i només si $H$ és un subgrup normal de $G$.*

*Demostració.* □

**Definició 9.1.33** (Grup quocient)**.** Siguin $G$ un grup amb l'operació $*$ i $N$ un subgrup normal de $G$. Aleshores direm que el grup $G/N$ amb l'operació

$$\begin{aligned} *\colon G/N \times G/N &\longrightarrow G/N \\ [x] * [y] &\longmapsto [x * y] \end{aligned}$$

és el grup quocient $G$ mòdul $N$.

Aquesta definició té sentit per la proposició 9.1.32.

**Lemma 9.1.34.** *Siguin $G$ un grup amb l'operació $*$, $H$ un subgrup de $G$, $x$ un element de $G$ i*

$$\begin{aligned} f_x \colon H &\longrightarrow \{x\}H \\ h &\longmapsto x * h \end{aligned}$$

*una aplicació. Aleshores $f_x$ és bijectiva.*

*Demostració.* Veiem que aquesta funció és bijectiva trobant la seva inversa:

$$\begin{aligned} f_x^{-1} \colon \{x\}H &\longrightarrow H \\ y &\longmapsto x^{-1} * y \end{aligned}$$

i comprovant $f_x(f_x^{-1}(h)) = h$ i $f_x^{-1}(f_x(h)) = h$. Per tant $f$ és bijectiva[1]. □

**Observació 9.1.35.** $\{x\}G = G$.

**Teorema 9.1.36** (Teorema de Lagrange)**.** *Siguin $G$ un grup d'ordre finit amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores $|H|$ divideix $|G|$.*

*Demostració.* Fixem $x \in G$ i considerem la funció

$$\begin{aligned} f_x \colon H &\longrightarrow \{x\}H \\ h &\longmapsto x * h \end{aligned}$$

Pel lemma 9.1.34 trobem $|H| = |\{x\}H|$. Tenim que $|G|$ és el resultat de multiplicar el número de classes d'equivalència pel nombre d'elements d'una de les classes, és a dir

$$|G| = |G/H||H|$$

i per tant $|H|$ divideix $|G|$. □

[1] de fet, $f_x^{-1} = f_{x^{-1}}$

**Corol·lari 9.1.37.** *Sigui $G$ un grup d'ordre $p$ primer amb l'operació $*$. Aleshores $G$ és un grup cíclic.*

*Demostració.* Sigui $e$ l'element neutre de $G$.

Prenem un element $g \in G$ diferent de $e$ i considerem el subgrup de $G$ generat per $g$. Pel Teorema de Lagrange (9.1.36) tenim que l'ordre de $\langle\{g\}\rangle$ divideix l'ordre de $G$ i com que per hipòtesi l'orde de $G$ és primer i $g^1 \neq e$, ja que $g$ és per hipòtesi diferent de l'element neutre, tenim que $|\langle\{g\}\rangle| = p$, i per tant $\langle\{g\}\rangle = G$ i per la definició de grup cíclic (9.1.27) tenim que $G$ és un grup cíclic. □

**Definició 9.1.38** (l'índex d'un subgrup en un grup)**.** Siguin $G$ un grup amb l'operació $*$ i $H$ un subgrup de $G$. Aleshores definim

$$[G : H] = \frac{|G|}{|H|}$$

com l'índex de $H$ a $G$.

## 9.2 Tres Teoremes d'isomorfisme entre grups

### 9.2.1 Morfismes entre grups

**Definició 9.2.1** (Morfisme entre grups)**.** Siguin $G_1$ un grup amb l'operació $*$, $G_2$ un grup amb l'operació $\circ$ i $f\colon G_1 \to G_2$ una aplicació que, per a tot $x, y \in G_1$ satisfà

$$f(x * y) = f(x) \circ f(y).$$

Aleshores diem que $f$ és un morfisme entre grups. Definim també

1. Si $f$ és injectiva direm que $f$ és un monomorfisme entre grups.
2. Si $f$ és exhaustiva direm que $f$ és un epimorfisme entre grups.
3. Si $f$ és bijectiva direm que $f$ és un isomorfisme entre grups. També escriurem $G_1 \cong G_2$ i direm qe $G_1$ i $G_2$ són grups isomorfs.
4. Si $G_1 = G_2$ direm que $f$ és un endomorfisme entre grups.
5. Si $G_1 = G_2$ i $f$ és bijectiva direm que $f$ és un automorfisme entre grups.

**Proposició 9.2.2.** *Siguin $G_1$ un grup amb l'operació $*$ amb element neutre $e$, $G_2$ un grup amb l'operació $\circ$ amb element neutre $e'$ i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *$f(e) = e'$.*
2. *$f\left(x^{-1}\right) = f(x)^{-1}$ per a tot $x \in G_1$.*

*Demostració.* Demostrem primer el punt (1). Per la definició de morfisme tenim que per a tot $x \in G_1$

$$\begin{aligned} f(x) \circ f(e) &= f(x * e) && \text{(morfisme entre grups (9.2.1))} \\ &= f(x) && \text{(l'element neutre d'un grup (9.1.3))} \\ &= f(x) \circ e' \end{aligned}$$

i per la proposició 9.1.5 tenim $f(e) = e'$.

Per demostrar el punt (2) en tenim prou en veure que per a tot $x \in G$

$$\begin{aligned} f(x) \circ f(x^{-1}) &= f(x * x^{-1}) && \text{(morfisme entre grups (9.2.1))} \\ &= f(e) && \text{(l'invers d'un element d'un grup (9.1.7))} \\ &= f(x^{-1} * x) && \text{(morfisme entre grups (9.2.1))} \\ &= f(x^{-1}) \circ f(x) \end{aligned}$$

i pel punt (1) d'aquesta proposició $f(x) \circ f(x^{-1}) = f(x^{-1}) \circ f(x) = e'$, i per la proposició 9.1.6 tenim que $f(x^{-1}) = f(x)^{-1}$, com volíem. □

**Proposició 9.2.3.** *Siguin $G$, $H$ i $K$ tres grups amb les operacions $*$, $\circ$ i $+$, respectivament, i $f\colon G \longrightarrow H$ i $g\colon H \longrightarrow K$ dos morfismes entre grups. Aleshores $g(f)\colon G \longrightarrow K$ és un morfisme entre grups.*

*Demostració.* Per la definició de morfisme entre grups (9.2.1) tenim que per a tot $g_1, g_2 \in H$ i $h_1, h_2 \in H$ tenim $f(g_1 * g_2) = f(g_1) \circ f(g_2)$ i $g(h_1 \circ h_2) = g(h_1) + g(h_2)$. Per tant

$$g(f(g_1 * g_2)) = g(f(g_1) \circ f(g_2)) = g(f(g_1)) + g(f(g_2)),$$

i per la definició de morfisme entre grups (9.2.1) hem acabat. □

**Proposició 9.2.4.** *Siguin $G_1$ un grup amb l'operació $*$ i $G_2$ un grup amb l'operació $\circ$ tal que*

$$G_1 \cong G_2.$$

*Aleshores*

1. *$G_1$ és un grup abelià si i només si $G_2$ és un grup abelià.*
2. *$G_1$ és un grup cíclic si i només si $G_2$ és un grup cíclic.*

*Demostració.* Sigui $f\colon G_1 \to G_2$ un isomorfisme entre grups.

Comencem demostrant el punt (1). Suposem doncs que $G_1$ és un grup abelià. Per la definició de grup abelià (9.1.25) tenim que per a tot $a, b \in G_1$ es compleix $a * b = b * a$. Aleshores tenim

$$f(a * b) = f(b * a)$$

i per la definició de morfisme entre grups (9.2.1) tenim que

$$f(a) \circ f(b) = f(b) \circ f(a),$$

i per tant, com que per la definició de isomorfisme entre grups (9.2.1) $f$ és un bijectiu, $G_2$ satisfà la definició de grup abelià (9.1.25).

Demostrem ara el punt (2). Suposem doncs que $G_1$ és un grup cíclic. Per la definició de grup cíclic (9.1.27) tenim que $G_1 = \{g^i\}_{i \in \mathbb{Z}}$ per a un cert $g \in G_1$. Per tant, com que $f$ és bijectiva per la definició de isomorfisme entre grups (9.2.1) tenim que per a tot $x \in G_2$ es compleix $x = f(g^i)$ per a un cert $i \in \mathbb{Z}$, i per la definició de morfisme entre grups (9.2.1) tenim que[2] $f(g^i) = f(g)^i$, i per la definició de grup cíclic (9.1.27) $G_2$ és un grup cíclic. □

[2] el primer és amb l'operació $*$ i el segon amb l'operació $\circ$.

**Definició 9.2.5** (Nucli i imatge d'un morfisme entre grups)**.** Siguin $G_1$ un grup amb l'operació $*$ amb element neutre $e$, $G_2$ un grup amb l'operació $\circ$ amb element neutre $e'$ i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores definim el nucli de $f$ com

$$\ker(f) = \{x \in G_1 \mid f(x) = e'\},$$

i la imatge de $f$ com

$$\mathrm{Im}(f) = \{f(x) \in G_2 \mid x \in G_1\}.$$

**Observació 9.2.6.** $\ker(f) \subseteq G_1$, $\mathrm{Im}(f) \subseteq G_2$.

**Proposició 9.2.7.** *Siguin $G_1$ un grup amb l'operació $*$ amb element neutre $e$, $G_2$ un grup amb l'operació $\circ$ amb element neutre $e'$, i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. $\ker(f)$ *és un subgrup normal de* $G_1$.
2. $\mathrm{Im}(f)$ *és un subgrup de* $G_2$.

*Demostració.* Aquest enunciat té sentit per l'observació 9.2.6.

Primer comprovem el punt (1). Comencem veient que $\ker(f)$ és un subgrup de $G_1$. Per la proposició 9.1.15 tenim que ens cal amb veure que si $a, b \in \ker(f)$, aleshores $a*b^{-1} \in \ker(f)$. Això és cert ja que si $a, b \in \ker(f)$ aleshores $f(a) = e'$ i $f(b^{-1}) = e'$, i per tant $a*b^{-1} = e*e^{-1} = e$, el que significa que $f(a*b^{-1}) = e'$, i tenim $a * b^{-1} \in \ker(f)$.

Comprovem ara que el subgrup és normal. Per la proposició 9.1.24 en tenim prou en veure que per a tot $x \in \ker(f)$ i $g \in G$, $x*g*x^{-1} \in \ker(f)$. Això ho veiem notant que si $g \in \ker(f)$, $f(g) = e'$, i per tant $f(x*g*x^{-1}) = f(x) \circ e' \circ f(x^{-1})$i això és $f(x * x^{-1}) = e'$, i per tant $x * g * x^{-1} \in \ker(f)$.

Acabem veient el punt (2). De nou per la proposició 9.1.15 tenim que si per a tot $f(a), f(b) \in \mathrm{Im}(f)$ tenim $f(a) \circ f(b)^{-1} \in \mathrm{Im}(f)$ aleshores $\mathrm{Im}(f)$, és un subgrup de $G_2$. Això és cert, ja que per la definició de morfisme entre grups (9.2.1) i la proposició 9.2.2 tenim $f(a) \circ f(b)^{-1} = f(a * b^{-1})$; i per la definició de grup $a * b^{-1} \in G_1$, i per la definició de morfisme entre grups (9.2.1) tenim que $f(a) \circ f(b)^{-1} \in \mathrm{Im}(f)$, i per tant $\mathrm{Im}(f)$ és un subgrup de $G_2$, com volíem veure. □

**Proposició 9.2.8.** *Siguin $G_1$ un grup amb l'operació $*$ amb element neutre $e$, $G_2$ un grup amb l'operació $\circ$ amb element neutre $e'$, i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. $f$ *és un monomorfisme si i només si* $\ker(f) = \{e\}$.
2. $f$ *és un epimorfisme si i només si* $\mathrm{Im}(f) = G_2$.

*Demostració.* Comencem fent la demostració del punt (1) per la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $f$ és un monomorfisme, i per tant injectiva. Per la definició de nucli d'un morfisme entre grups (9.2.5) tenim que $\ker(f) = \{x \in G_1 \mid f(x) = e'\}$. Suposem $x \in G_1$, és a dir, $f(x) = e'$. Ara bé, com que $f$ és injectiva per la proposició 9.2.2 ha de ser $\ker(f) = \{e\}$.

Demostrem ara la implicació cal a l'esquerra ($\Leftarrow$). Suposem doncs que $\ker(f) = \{e\}$. Siguin $x, y \in G_1$ dos elements que satisfacin $f(x) = f(y)$. Com

que, per la proposició 9.2.7 $\ker(f)$ és un subgrup de $G_1$, tenim que $x * y^{-1} \in G_1$, i per tant

$$\begin{aligned} f(x * y^{-1}) &= f(x) \circ f(y^{-1}) && \text{(morfisme entre grups (9.2.1))} \\ &= f(x) \circ f(y)^{-1} && \text{(Proposició 9.2.2)} \\ &= f(y) \circ f(y)^{-1} = e', \end{aligned}$$

i per tant $x * y^{-1} \in \ker(f)$, però per hipòtesi teníem $\ker(f) = \{e\}$, i per tant ha de ser $x * y^{-1} = e$, el que és equivalent a $x = y$, i per tant $f$ és injectiva.

Demostrem ara el punt (2) començant per la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $f$ és un epimorfisme, i per tant exhaustiva, i per tant per a cada $y \in G_2$ existeix un $x \in G_1$ tal que $f(x) = y$, i per la definició d'imatge d'un morfisme entre grups (9.2.5) tenim que $\mathrm{Im}(f) = G_2$.

Acabem demostrant la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $\mathrm{Im}(f) = G_2$ i prenem $y \in G_2$. Aleshores per la definició d'imatge d'un morfisme entre grups (9.2.5) tenim que existeix un $x \in G_1$ tal que $f(x) = y$, i per tant $f$ és exhaustiva. □

**Proposició 9.2.9.** *Siguin $G_1$ un grup amb l'operació $*$, $G_2$ un grup amb l'operació $\circ$, i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *Si $H_1 \leq G_1 \Rightarrow \{f(h) \in G_2 \mid h \in H_1\} \leq G_2$.*
2. *Si $H_2 \leq G_2 \Rightarrow \{h \in G_1 \mid f(h) \in H_2\} \leq G_1$.*
3. *Si $H_2 \trianglelefteq G_2 \Rightarrow \{h \in G_1 \mid f(h) \in H_2\} \trianglelefteq G_1$.*

*Demostració.* Comprovem primer el punt (1). Suposem doncs que $H_1$ és un subgrup de $G_1$. Denotarem $H = \{f(h) \in G_2 \mid h \in H_1\}$. Siguin $x, y \in H_1$; per la proposició 9.1.15 només ens cal veure que $f(x) \circ f(y)^{-1} \in H$. Això és

$$\begin{aligned} f(x) \circ f(y)^{-1} &= f(x) \circ f(y^{-1}) && \text{(Proposició 9.2.2)} \\ &= f(x * y^{-1}). && \text{(morfisme entre grups (9.2.1))} \end{aligned}$$

Ara bé, com que $x, y \in H_1$ i $H_1$ és un subgrup de $G_1$, per la proposició 9.1.15 tenim que $x * y^{-1} \in H_1$, i per tant $f(x * y^{-1}) \in H$, i per la definició de morfisme entre grups (9.2.1) i la proposició 9.2.2 tenim que $f(x) \circ f(y)^{-1} \in H$, i per tant $H$ és un subgrup de $G_2$, com volíem veure.

Comprovem ara el punt (2). Suposem doncs que $H_2$ és un subgrup de $G_2$ i denotem $H = \{h \in G_1 \mid f(h) \in H_2\}$. Per la proposició 9.1.15 només ens cal veure que per a tot $x, y \in H$ es satisfà $x * y^{-1} \in H$. Si $x, y \in H$ aleshores tenim que $f(x), f(y) \in H_2$, i com que $H_2$ és un grup, aleshores per la definició de grup (9.1.1) ha de ser $f(x) \circ f(y^{-1}) \in H_2$ Aleshores, per la definició de morfisme entre grups (9.2.1) tenim $f(x) \circ f(y^{-1}) = f(x * y^{-1})$, i per tant $x * y^{-1} \in H$ i així tenim que $H$ és un subgrup de $G_1$.

Veiem el punt (3) per acabar. Suposem doncs que $H_2$ és un subgrup normal de $G_2$ i definim $H = \{h \in G_1 \mid f(h) \in H_2\}$. Per demostrar-ho prenem $g \in G_1$, $h \in H_1$ tal que $f(h) \in H$ i fem

$$\begin{aligned} f(g) \circ f(h) \circ f(g)^{-1} &= f(g) \circ f(h) \circ f(g^{-1}) && \text{(Proposició 9.2.2)} \\ &= f(g * h * g^{-1}) && \text{(morfisme entre grups (9.2.1))} \end{aligned}$$

Ara bé, com que $H_2$ és un subgrup normal de $G_2$, tenim que, per a tot $g \in G_1$, $f(g*h*g^{-1}) \in H_2$, i per tant $g*h*g^{-1} \in H$, que satisfà la definició de subgrup normal (9.1.23) per la proposició 9.1.24. □

**Teorema 9.2.10** (Teorema de representació de Cayley)**.** *Sigui $G$ un grup amb l'operació $*$. Aleshores $G$ és isomorf a un subgrup de $\mathrm{S}_G$ amb l'operació $\circ$, on $\mathrm{S}_G$ és el grup simètric dels elements de $G$.*

*Demostració.* Definim

$$\varphi\colon G \longrightarrow \mathrm{S}_G \tag{9.2}$$

$$\begin{aligned} g \longmapsto \sigma_g : G &\longrightarrow G \\ x &\longmapsto g*x \end{aligned} \tag{9.3}$$

Tenim que $\sigma_g$ és bijectiva ja que és una permutació. Comprovarem que $\varphi$ és un monomorfisme entre grups. Veiem primer que és un morfisme entre grups. Prenem $g, g' \in G$. Per la definició (9.2) tenim que $\varphi(g*g') = \sigma_{g*g'}$. Per veure que $\sigma_{g*g'} = \sigma_g \circ \sigma_{g'}$ observem que per a tot $x \in G$

$$\begin{aligned} \sigma_{g*g'}(x) &= g*g'*x \\ &= g*\sigma_{g'}(x) \\ &= \sigma_g \circ \sigma_{g'}(x), \end{aligned}$$

i per la definició de morfisme entre grups (9.2.1) tenim que $\varphi$ és un morfisme entre grups. Veiem ara que $\varphi$ és un monomorfisme. Per la definició de nucli d'un morfisme entre grups (9.2.5) tenim que

$$\ker(\varphi) = \{x \in G \mid f(x) = \mathrm{Id}_G\}.$$

Ara bé, $\sigma_g = \mathrm{Id}$ és, per la definició (9.3), equivalent a dir que $g*x = x$ per a tota $x \in G$, i per la definició de l'element neutre d'un grup (9.1.3) això és si i només si $g = e$, i per tant

$$\ker(\varphi) = \{e\},$$

i per la proposició 9.2.8 tenim que $\varphi$ és un monomorfisme, com volíem veure.

Per tant, per la proposició 9.2.9 tenim que

$$G \cong \mathrm{Im}(\varphi) \leq \mathrm{S}_G\,. \qquad \square$$

**Corol·lari 9.2.11.** *Si $G$ té ordre $n!$ aleshores $G \cong \mathrm{S}_n$.*

### 9.2.2 Teoremes d'isomorfisme entre grups

**Teorema 9.2.12.** *Siguin $G_1$ un grup amb l'operació $*$, $G_2$ un grup amb l'operació $\circ$ i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores $G_1/\ker(f) \cong \mathrm{Im}(f)$.*

*Demostració.* Siguin $e$ l'element neutre de $G_1$ i $e'$ l'element neutre de $G_2$. Definim l'aplicació

$$\begin{aligned} \varphi\colon G_1/\ker(f) &\longleftrightarrow \mathrm{Im}(f) \\ [x] &\longmapsto f(x) \end{aligned} \tag{9.4}$$

Comprovem primer que aquesta aplicació està ben definida:

Suposem que $[x] = [x']$. Això és que $x' \in \{x\}\ker(f)$, i equivalentment $x' = x * h$ per a cert $h \in \ker(f)$. Per tant

$$\begin{aligned}
\varphi([x']) &= \varphi([x * h]) && \text{(Definició (9.1.33))}\\
&= f(x * h) && \text{(Definició (9.4))}\\
&= f(x) \circ f(h) && \text{(morfisme entre grups (9.2.1))}\\
&= f(x) \circ e' && \text{(nucli d'un morfisme entre grups (9.2.5))}\\
&= f(x) = \varphi([x]) && \text{(Definició (9.4))}
\end{aligned}$$

i per tant $\varphi$ està ben definida. Veiem ara que $\varphi$ és un morfisme entre grups. Tenim que

$$\begin{aligned}
\varphi([x] * [y]) &= \varphi([x * y]) && \text{(Definició (9.1.33))}\\
&= f(x * y) && \text{(Definició (9.4))}\\
&= f(x) \circ f(y) && \text{(morfisme entre grups (9.2.1))}\\
&= \varphi([x]) \circ \varphi([y]), && \text{(Definició (9.4))}
\end{aligned}$$

i per la definició de morfisme entre grups (9.2.1) $\varphi$ és un morfisme entre grups. Continuem demostrant que $\varphi$ és injectiva. Per la definició de nucli d'un morfisme entre grups (9.2.5) tenim que $\ker(\varphi) = \{[x] \in G/\ker(f) \mid \varphi([x]) = e\}$, i per tant $\ker(\varphi) = \ker(f)$, ja que $f(x) = e$ si i només si $x \in \ker(f)$, i per tant $\ker(\varphi) = [e]$ i per la proposició 9.2.8 $\varphi$ és injectiva.

Per veure que $\varphi$ és exhaustiva veiem que si $[x] \in G_1/\ker(f)$, per la definició de grup quocient (9.1.33) tenim que $x = x' * y$ per a uns certs $x' \in G_2$, $h \in \ker(f)$, i per tant

$$\begin{aligned}
\varphi([x]) &= \varphi([x' * h])\\
&= \varphi([x'] * [h]) && \text{(grup quocient (9.1.33))}\\
&= f(x') \circ f(e) && \text{(morfisme entre grups (9.2.1))}\\
&= f(x') && \text{(grup (9.1.1))}\\
&= f(x * h^{-1})\\
&= f(x) \circ f(h^{-1}) && \text{(morfisme entre grups (9.2.1))}\\
&= f(x) \circ f(h)^{-1} && \text{(Proposició 9.2.2)}\\
&= f(x) \circ e^{-1} = f(x). && \text{(Proposició 9.1.8)}
\end{aligned}$$

Així veiem que $\mathrm{Im}(\varphi) = \mathrm{Im}(f)$. Per tant $\varphi$ és un isomorfisme, i per la definició d'isomorfisme entre grups (9.2.1) tenim $G_1/\ker(f) \cong \mathrm{Im}(f)$, com volíem veure. □

**Teorema 9.2.13** (Primer Teorema de l'isomorfisme)**.** *Siguin $G_1$ un grup amb l'operació $*$, $G_2$ un grup amb l'operació $\circ$ i $f\colon G_1 \to G_2$ un epimorfisme entre grups. Aleshores*

1. $G_1/\ker(f) \cong G_2$.
2. *L'aplicació*

$$\begin{aligned}
\varphi_1\colon \{H \mid \ker(f) \leq H \leq G\} &\longleftrightarrow \{K \mid K \leq G_2\}\\
H &\longmapsto \{f(h) \in G_2 \mid h \in H\}
\end{aligned} \tag{9.5}$$

Si ningú ve del futur per aturar-te, com de dolenta pot ser la decisió que estàs prenent?

*és bijectiva.*

3. *L'aplicació*

$$\begin{aligned}\varphi_2\colon \{H \mid \ker(f) \leq H \trianglelefteq G\} &\longleftrightarrow \{K \mid K \trianglelefteq G_2\} \\ H &\longmapsto \{f(h) \in G_2 \mid h \in H\}\end{aligned} \tag{9.6}$$

*és bijectiva.*

*Demostració.* Siguin $e$ l'element neutre de $G_1$ i $e'$ l'element neutre de $G_2$.

El punt (1) és conseqüència del Teorema 9.2.12, ja que si $f$ és exhaustiva, $\mathrm{Im}(f) = G_2$, i per tant $G_1/\ker(f) \cong G_2$.

Per veure el punt (2) comencem demostrant que $\varphi_1$ està ben definida. Siguin $H_1 = H_2 \in \{H \mid \ker(f) \leq H \leq G\}$. Aleshores, per la hipòtesi (9.5) tenim $\varphi_1(H_1) = \{f(h) \in G_2 \mid h \in H_1\}$ i $\varphi_1(H_2) = \{f(h) \in G_2 \mid h \in H_2\}$, i com que $f$ és una aplicació, i per tant ben definida, $\varphi_1(H_1) = \varphi_1(H_2)$.

Continuem comprovant que $\varphi_1$ és bijectiva. Per veure que és injectiva prenem $H_1, H_2 \in \{H \mid \ker(f) \leq H \leq G\}$ tals que $\varphi_1(H_1) = \varphi_1(H_2)$. Això, per la hipòtesi (9.5) és

$$\{f(h) \in G_2 \mid h \in H_1\} = \{f(h) \in G_2 \mid h \in H_2\}.$$

Per tant siguin $h_1 \in H_1$, $h_2 \in H_2$ tals que $f(h_1) = f(h_2)$. Equivalentment, per la proposició 9.1.6 i la definició de l'invers d'un element d'un grup (9.1.7) i la proposició 9.1.8 tenim les igualtats $f(h_2^{-1} * h_1) = f(h_1^{-1} * h_2) = e'$, i per la definició de nucli d'un morfisme entre grups (9.2.5) tenim $h_2^{-1} * h_1, h_1^{-1} * h_2 \in \ker(f)$, i per la hipòtesi (9.5) això és $h_2^{-1} * h_1 \in \ker(f) \subseteq H_2$ i $h_1^{-1} * h_2 \in \ker(f) \subseteq H_1$. Observem que això és que $h_1 \in \{h_2\}\ker(f)) \subseteq H_2$ i $h_2 \in \{h_1\}\ker(f)) \subseteq H_1$. Això vol dir que $H_1 \subseteq H_2$ i $H_2 \subseteq H_1$, i per doble inclusió això és $H_1 = H_2$, com volíem veure.

Per veure que $\varphi_1$ és exhaustiva tenim que per la proposició 9.2.9 i per la hipòtesi (9.5) tenim que donat un conjunt $K$ tal que $K \leq G_2$ aleshores el conjunt $H = \{k \in G_1 \mid f(h) \in K\}$ satisfà $H \leq G_1$, i per la definició de nucli d'un morfisme entre grups (9.2.5) tenim que es compleix $\ker(f) \leq H \leq G_1$, i per tant $\varphi_1(H) = K$, i per tant $\varphi$ és exhaustiva i per tant bijectiva.

Es pot demostrar el punt (3) amb el mateix argument que hem donat per demostrar el punt (2). □

**Proposició 9.2.14.** *Siguin $G$ un grup amb l'operació $*$ i $H$, $K$ subgrups de $G$. Aleshores*

1. *Si $K \trianglelefteq G$, aleshores $HK \leq G$.*
2. *Si $H, K \trianglelefteq G$, aleshores $HK \trianglelefteq G$.*

*Demostració.* Comencem veient el punt (1). Per la proposició 9.1.15 només ens cal comprovar que per a tot $x, y \in HK$ es satisfà $x * y^{-1} \in HK$. Siguin doncs $x, y \in HK$, que podem reescriure com $x = h_1 * k_1$ i $y = h_2 * k_2$. Calculem $x * y^{-1}$:

$$\begin{aligned} x * y^{-1} &= h_1 * k_1 * (h_2 * k_2)^{-1} \\ &= h_1 * k_1 * k_2^{-1} * h_2^{-1} && \text{(Proposició 9.1.10)} \\ &= h_1 * k_1 * h_2^{-1} * k_2^{-1}, && \text{(subgrup normal (9.1.23))} \\ &= h_1 * h_2^{-1} * k_1 * k_2^{-1}, && \text{(subgrup normal (9.1.23))} \end{aligned}$$

i com que, per la definició de grup (9.1.1) tenim $h_1 * h_2^{-1} \in H$ i $k_1 * k_2^{-1} \in K$, veiem que $x * y^{-1} \in HK$, com volíem demostrar.

La demostració del punt (2) és anàloga a la del punt (1). □

**Lemma 9.2.15.** *Siguin $G$ un grup amb l'operació $*$, $H$ un subgrup de $G$ i $K$ un subgrup normal de $G$. Aleshores $H \cap K \trianglelefteq H$.*

*Demostració.* Prenem $x \in H$ i $y \in H \cap K$. Per la proposició 9.1.24 només hem de veure que per a tot $x \in H$ i $y \in H \cap K$, es satisfà $x^{-1} * y * x \in H$. Ara bé, com que $K$ és un grup normal, per la mateixa proposició 9.1.24, com que per hipòtesi $y \in H \cap K$, i en particular $y \in K$, tenim que $x^{-1} * y * x \in K$. Per veure que $x^{-1} * y * x \in H$ tenim prou amb veure que $x, y \in H$, i com que $H$ és un subgrup de $G$, i per tant un grup, per la definició de grup (9.1.1) tenim que $x^{-1} * y * x \in H$, i per tant $x^{-1} * y * x \in H \cap K$, com volíem veure. □

**Teorema 9.2.16** (Segon Teorema de l'isomorfisme)**.** *Siguin $G$ un grup amb l'operació $*$, $H$ un subgrup de $G$ i $K$ un subgrup normal de $G$. Aleshores*

$$(HK)/K \cong H/(H \cap K).$$

*Demostració.* Aquest enunciat té sentit pel lemma 9.2.15.

Definim

$$\begin{aligned} f\colon HK &\longrightarrow H/(H \cap K) \\ h * k &\longmapsto [h]. \end{aligned} \tag{9.7}$$

Demostrarem que $f$ és un epimorfisme; però primer cal veure que $f$ està ben definida. Prenem doncs $h_1 * k_1, h_2 * k_2 \in HK$ amb $h_1, h_2 \in H$ i $k_1, k_2 \in K$ tals que $h_1 * k_1 = h_2 * k_2$, i per tant $h_2^{-1} * h_1 = k_2 * k_1^{-1}$. Ara bé, com que per hipòtesi i per la definició de l'invers d'un element d'un grup (9.1.7) tenim que $h_1, h_2^{-1} \in H$ i a la vegada $k_2, k_1^{-1} \in K$, per la definició de grup (9.1.1) tenim $h_2^{-1} * h_1 \in H$ i $k_2 * k_1^{-1} \in K$ i com que $h_2^{-1} * h_1 = k_2 * k_1^{-1}$ tenim que $[h_2^{-1} * h_1] = [k_2^{-1} * k_1] = [e]$, i per la definició de grup quocient (9.1.33) tenim que $[h_1] = [h_2]$ i per tant $f$ està ben definida.

Veiem ara que $f$ és un morfisme entre grups. Prenem $h_1, h_2 \in H$ i $k_1, k_2 \in K$, i per tant $h_1 * k_1, h_2 * k_2 \in HK$, i fem

$$\begin{aligned} f(h_1 * k_1 * h_2 * k_2) &= [h_1 * h_2] && \text{(Definició (9.7))} \\ &= [h_1] * [h_2] && \text{(Definició (9.1.33))} \\ &= f(h_1 * k_1) * f(h_2 * k_2) && \text{(Definició (9.7))} \end{aligned}$$

i per tant $f$ satisfà la definició de morfisme entre grups (9.2.1).

Continuem veient que $f$ és exhaustiva. Prenem $[h] \in H/(H \cap K)$. Per la definició (9.7) tenim que $f(h * k) = [h]$ per a qualsevol $k \in K$, i per tant $f$ és exhaustiva.

Per tant $f$ és un epimorfisme, i per tant, pel Primer Teorema de l'isomorfisme entre grups (9.2.13) tenim

$$HK/\ker(f) \cong H/(H \cap K).$$

Ara bé, per la definició de nucli d'un morfisme entre grups (9.2.5) tenim que $\ker(f) = \{h_1 * k_2 \in HK \mid f(h_1 * k_1) = [e]\}$, i per tant $\ker(f) = K$ i trobem

$$HK/K \cong H/(H \cap K).$$ □

**Teorema 9.2.17** (Tercer Teorema de l'isomorfisme)**.** *Siguin $G$ un grup amb l'operació $*$ i $H$, $K$ dos subgrups normals de $G$ amb $K \subseteq H$. Aleshores*

$$G/H \cong (G/K)/(H/K).$$

*Demostració.* Definim les aplicacions

$$\begin{aligned} \varphi_1 \colon G &\longrightarrow G/K \\ g &\longmapsto [g] \end{aligned} \qquad \text{i} \qquad \begin{aligned} \varphi_2 \colon G/K &\longrightarrow (G/K)/(H/K) \\ [g] &\longmapsto \overline{[g]}. \end{aligned}$$

Veiem que $\varphi_1$ i $\varphi_2$ són morfismes.

Per la proposició 9.2.3 tenim que $\varphi_2(\varphi_1) \colon G \longrightarrow (G/K)/(H/K)$ és un epimorfisme entre grups, i pel Primer Teorema de l'isomorfisme entre grups (9.2.13) trobem

$$G/\ker(\varphi_2(\varphi_1)) \cong (G/K)/(H/K).$$

Veiem ara que $\ker(\varphi_2(\varphi_1)) = H$. Per la definició de grup quocient (9.1.33) tenim que $G/K = \{gK \mid g \in G\}$ i $H/K = \{hK \mid h \in H\}$, i per tant

$$(G/K)/(H/K) = \{gKhK \mid g \in G, h \in H\}, \tag{9.8}$$

però com que, per hipòtesi, $H$ i $K$ són subgrups normals de $G$, per la definició de subgrup normal (9.1.23) podem reescriure (9.8) com

$$(G/K)/(H/K) = \{ghK \mid g \in G, h \in H\}. \tag{9.9}$$

Ara bé, com que per hipòtesi $K \subseteq H$ podem reescriure (9.9) com

$$(G/K)/(H/K) = \{gH \mid g \in G\},$$

i trobem, per la definició de nucli d'un morfisme entre grups (9.2.5), que $\ker(\varphi_2(\varphi_1)) = H$, i per tant

$$G/H \cong (G/K)/(H/K). \qquad \square$$

## 9.3 Tres Teoremes de Sylow

### 9.3.1 Accions sobre grups

**Definició 9.3.1** (Acció d'un grup sobre un conjunt)**.** Siguin $G$ un grup amb l'operació $*$ i element neutre $e$, $X$ un conjunt no buit i

$$\begin{aligned} \cdot \colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

una operació que satisfaci

1. $e \cdot x = x$ per a tot $x \in X$.
2. $(g_1 * g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ per a tot $x \in X$, $g_1, g_2 \in G$.

Aleshores direm que $\cdot$ és una acció de $G$ sobre $X$. També direm que $X$ és un $G$-conjunt amb l'acció $\cdot$.

**Proposició 9.3.2.** *Siguin $G$ un grup amb l'operació $*$, $X$ un conjunt, $\cdot$ una acció de $G$ sobre $X$ i $\sim$ una relació sobre $X$ tal que per a tot $x_1, x_2 \in X$ diem que $x_1 \sim x_2$ si i només si existeix un $g \in G$ tal que $x_1 = g \cdot x_2$. Aleshores la relació $\sim$ és una relació d'equivalència.*

*Demostració.* Sigui $e$ l'element neutre del grup $G$. Comprovem que $\sim$ satisfà la definició de relació d'equivalència (2.3.2):

1. Reflexiva: Sigui $x \in X$. Per la definició de acció d'un grup sobre un conjunt (9.3.1) tenim que $x = x \cdot e$, i per tant $x \sim x$.

2. Simètrica: Siguin $x_1, x_2 \in X$ tals que $x_1 \sim x_2$. Per tant existeix $g \in G$ tal que $x_1 = g \cdot x_2$. Per la definició de acció d'un grup sobre un conjunt (9.3.1) tenim que $g \cdot x_2 \in X$, i per tant podem prendre $g^{-2} \cdot (g * x_2)$, que és equivalent a $g^{-2} \cdot (g \cdot x_2) = g^{-2} \cdot x_1$, i així $x_2 = g^{-1} \cdot x_1$, i per tant $x_2 \sim x_1$.

3. Transitiva: Siguin $x_1, x_2, x_3 \in X$ tals que $x_1 \sim x_2$ i $x_2 \sim x_3$. Per tant existeixen $g_1, g_2 \in G$ tals que $x_1 = g_1 \cdot x_2$ i $x_2 = g_2 \cdot x_3$, i per tant $x_1 = g_1 \cdot (g_2 \cdot x_3)$, i per la definició de acció d'un grup sobre un conjunt (9.3.1) això és $x_1 = (g_1 * g_2) \cdot x_3$, i com que $G$ és un grup, $g_1 * g_2 \in G$, i tenim que $x_1 \sim x_3$.

per tant $\sim$ és una relació d'equivalència. □

**Definició 9.3.3** (Òrbita d'un element d'un $G$-conjunt)**.** Siguin $G$ un grup amb l'operació $*$, $\cdot$ una acció de $G$ sobre un conjunt $X$ i $\sim$ una relació d'equivalència sobre $X$ tal que per a tot $x_1, x_2 \in X$ diem que $x_1 \sim x_2$ si i només si existeix un $g \in G$ tal que $x_1 = g \cdot x_2$. Aleshores direm que $\mathcal{O}(x) = [x]$ és l'òrbita de $x$.

Aquesta definició té sentit per la proposició 9.3.2.

**Definició 9.3.4** (Estabilitzador d'un element per una acció)**.** Siguin $G$ un grup amb l'operació $*$, $X$ un conjunt i $\cdot$ una acció de $G$ sobre $X$. Aleshores direm que el conjunt

$$\mathrm{St}(x) = \{g \in G \mid g \cdot x = x\}$$

és l'estabilitzador de $x$ per l'acció $\cdot$.

**Proposició 9.3.5.** *Siguin $G$ un grup amb l'operació $*$, $\cdot$ una acció de $G$ sobre un conjunt $X$ i $\mathrm{St}(x)$ l'estabilitzador d'un element $x$ de $X$ per l'acció $\cdot$. Aleshores $g \in \mathrm{St}(x)$ si i només si $g^{-1} \in \mathrm{St}(x)$.*

*Demostració.* Per la definició de l'estabilitzador d'un element per una acció (9.3.4) tenim que $g \in \mathrm{St}(x)$ si i només si $g \cdot x = x$. Ara bé, si prenem $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, i per la definició de acció d'un grup sobre un conjunt (9.3.1) tenim que $g^{-1} \cdot (g \cdot x) = (g^{-1} * g) \cdot x$, i per la definició de l'invers d'un element d'un grup (9.1.7) tenim que $g^{-1} \cdot x$ i per tant $g^{-1} \in \mathrm{St}(x)$. □

**Proposició 9.3.6.** *Siguin $G$ un grup amb l'operació $*$, $\cdot$ una acció de $G$ sobre un conjunt $X$ i $\mathrm{St}(x)$ l'estabilitzador de $x$ per l'acció $\cdot$. Aleshores $\mathrm{St}(x)$ és un subgrup de $G$.*

*Demostració.* Per la proposició 9.1.15 només ens cal veure que per a tot $g_1, g_2 \in \mathrm{St}(x)$ es compleix $g_1 * g_2^{-1} \in \mathrm{St}(x)$.

Prenem doncs $g_1, g_2 \in \mathrm{St}(x)$. Per la proposició 9.3.5 tenim que $g_2^{-1} \in \mathrm{St}(x)$, i per tant, per la definició de l'estabilitzador d'un element per una acció (9.3.4) tenim que $(g_1 * g_2^{-1}) \cdot x = x$, i per tant $g_1 * g_2^{-1} \in \mathrm{St}(x)$. □

**Proposició 9.3.7.** *Siguin $G$ un grup d'ordre finit amb l'operació $*$, $X$ un $G$-conjunt finit amb una acció $\cdot$ i $\mathrm{St}(x)$ l'estabilitzador d'un element $x$ de $X$ per l'acció $\cdot$. Aleshores*

$$|G/\mathrm{St}(x)| = |\mathcal{O}(x)| = [G : \mathrm{St}(x)].$$

*Demostració.* Considerem

$$\begin{aligned} f\colon G/\mathrm{St}(x) &\longrightarrow \mathcal{O}(x) \\ [g] &\longmapsto g \cdot x \end{aligned}$$

Volem veure que $f$ és una aplicació bijectiva, per tant mirem si està ben definida:

Siguin $[g_1], [g_2] \in G/\mathrm{St}(x)$ tals que $[g_1] = [g_2]$. Per tant $g_1 = g_2 * g'$ per a cert $g' \in \mathrm{St}(x)$, i per la definició de l'estabilitzador d'un element per una acció (9.3.4) tenim $g_1 \cdot x = x$, $(g_2 * g') \cdot x = x$, i per la definició de acció d'un grup sobre un conjunt (9.3.1) això és $g_2 \cdot (g' \cdot x) = x$, i per la proposició 9.3.5 $g_2 \cdot x = x$, i per tant $f$ està ben definida.

Veiem ara que $f$ és injectiva. Prenem $g \cdot x, g' \cdot x \in \mathcal{O}(x)$ tals que $g \cdot x = g' \cdot x$. Això, per la definició de acció d'un grup sobre un conjunt (9.3.1), és equivalent a dir $x = (g^{-1} * g') \cdot x$, i per la definició de l'estabilitzador d'un element per una acció (9.3.4) tenim que $g^{-1} * g \in \mathrm{St}(x)$. Per tant, per la definició de grup quocient (9.1.33) tenim que $[g] = [g']$, i per tant $f$ és injectiva.

Per veure que $f$ és exhaustiva veiem que per a qualsevol $g \cdot x \in \mathcal{O}(x)$, $f([g]) = g \cdot x$, i per tant $f$ és exhaustiva i tenim que $|\mathrm{St}(x)| = |\mathcal{O}(x)|$, ja que $f$ és una bijecció. □

### 9.3.2 Teoremes de Sylow

**Definició 9.3.8** ($p$-subgrup de Sylow)**.** Siguin $G$ un grup amb l'operació $*$ tal que $|G| = p^n m$ amb $p$ primer que no divideix $m$ i $P$ un subgrup de $G$ amb $|P| = p^n$. Aleshores direm que $P$ és un $p$-subgrup de Sylow de $G$.

**Lemma 9.3.9.** *Siguin $p$ un primer i $m$ un enter positiu tal que $p$ no divideixi $m$. Aleshores per a tot $n$ natural tenim que*

$$\binom{p^n m}{p^n} \tag{9.10}$$

*no és divisible per $p$.*

*Demostració.* Tenim que

$$\binom{p^n m}{p^n} = \frac{p^n m(p^n m - 1) \cdots (p^n m - p^n + 1)}{p^n (p^n - 1) \cdots (p^n - p^n + 1)} = \prod_{i=0}^{p^n - 1} \frac{p^n m - i}{p^n - i}. \tag{9.11}$$

Com que, per hipòtesi, $p$ és primer aquesta expressió només serà divisible per $p$ si ho són els elements del numerador. Fixem doncs $i \in \{0, \ldots, p^n + 1\}$ i estudiem

l'$i$-èsim terme del producte de (9.11). Notem primer que si $i = 0$ aquest terme no és divisible per $p$. Imposem ara també que $i \neq 0$. Si el denominador, $p^n m - i$, és divisible per $p$ tindrem que $p^n m - i = p^k m'$, on $m'$ no és divisible per $p$, i per tant $k$ serà l'exponent més gran que satisfaci la igualtat. Si aïllem $i$ obtindrem $i = p^k(p^{n-k}m - m')$. Ara bé, tenim doncs que $p^n - i = p^n - p^k(p^{n-k}m - m')$, i això és $p^n - p^k(p^{n-k}m - m') = p^k(p^{n-k}(1-m) - m')$, i per tant tindrem que l'$i$-èsim terme del producte de (9.11) serà de la forma

$$\frac{p^n m - i}{p^n - i} = \frac{p^k m'}{p^k(p^{n-k}(1-m) - m')} = \frac{m'}{p^{n-k}(1-m) - m'},$$

i així veiem que aquest $i$-èsim terme del producte no serà divisible per $p$; i com que això és cert per a qualsevol $i \in \{0, \dots, p^n + 1\}$ tenim que (9.10) tampoc ho serà, com volíem veure. □

**Teorema 9.3.10** (Primer Teorema de Sylow)**.** *Siguin $G$ un grup amb l'operació $*$ tal que $|G| = p^n m$ amb $p$ primer que no divideix $m$. Aleshores existeix un subconjunt $P \subseteq G$ tal que $P$ sigui un $p$-subgrup de Sylow de $G$.*

*Demostració.* Sigui $\mathcal{P}_{p^n}(G) = \{H \subseteq G \mid |H| = p^n\} = \{H_1, \dots, H_k\}$ el conjunt de subconjunts d'ordre $p^n$ de $G$. Aleshores tenim que

$$k = |\mathcal{P}_{p^n}(G)| = \binom{p^n m}{p^n},$$

i pel lemma 9.3.9 tenim que $p$ no divideix $k$.

Sigui $e$ l'element neutre de $G$. Definim

$$\begin{aligned} \cdot \colon G \times \mathcal{P}_{p^n}(G) &\longrightarrow \mathcal{P}_{p^n}(G) \\ (g, X) &\longmapsto \{g\}X. \end{aligned} \tag{9.12}$$

Veurem que $\cdot$ és una acció de $G$ sobre $\mathcal{P}_{p^n}(G)$. Primer hem de veure que, efectivament, $\cdot$ està ben definida. Prenem $g_1, g_2 \in G$ i $X_1, X_2 \in \mathcal{P}_{p^n}(G)$ tals que $g_1 = g_2$ i $X_1 = X_2$. Per tant tenim $g_1 \cdot X_1 = g_2 \cdot X_2$ ja que $\{g_1\}X_1 = \{g_2\}X_2$. Per veure que $g_1 \cdot X_1 \in \mathcal{P}_{p^n}(G)$ en tenim prou amb veure que, per a tot $X \in \mathcal{P}_{p^n}(G)$, si fixem $g \in G$ l'aplicació $g \cdot X$ té inversa, que per la definició de l'invers d'un element d'un grup (9.1.7) és $x^{-1} \cdot X$, i per tant $X \in \mathcal{P}_{p^n}(G)$.

Comprovem que $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (9.3.1). Tenim que $e \cdot X = X$ per a tot $X \in \mathcal{P}_{p^n}(G)$ ja que, per la definició de conjugació entre conjunts sobre grups (9.1.22), $eX = X$.

De nou per la definició de conjugació entre conjunts sobre grups (9.1.22) veiem que per a tot $g_1, g_2 \in G$ i $X \in \mathcal{P}_{p^n}(G)$ tenim que

$$\begin{aligned} (g_1 * g_2) \cdot X &= \{g_1 * g_2\}X \\ &= \{g_1\}\{g_2\}X \\ &= \{g_1\}(\{g_2\}X) = g_1 \cdot (g_2 \cdot X). \end{aligned}$$

i per tant $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (9.3.1).

Veiem ara que existeix almenys un element $X \in \mathcal{P}_{p^n}(G)$ tal que la seva òrbita, $\mathcal{O}(X)$, tingui ordre no divisible per $p$. Per veure això observem que per la definició de l'òrbita d'un element d'un $G$-conjunt (9.3.3) veiem que $\mathcal{O}(X)$

és un classe d'equivalència, i per tant l'ordre del conjunt $\mathcal{P}_{p^n}$ és la suma dels ordres de les òrbites dels seus elements, $\mathcal{O}(X)$, i si $p$ dividís l'ordre de $\mathcal{O}(X)$ per a tot $X \in \mathcal{P}_{p^n}$ tindríem que $p$ també divideix $k$, però ja hem vist que això no pot ser. Per tant existeix almenys un element $X \in \mathcal{P}_{p^n}$ tal que $|\mathcal{O}(X)|$ no és divisible per $p$. Fixem aquest conjunt $X$.

Prenem l'estabilitzador de $X$, $\mathrm{St}(X)$. Per la proposició 9.3.7 tenim que $|\mathrm{St}(X)|$ divideix $p^n$. Prenem també $x_o \in X$ i $g \in \mathrm{St}(X)$. Per la definició de l'estabilitzador d'un element per una acció (9.3.4) tenim que $\{g\}X = X$, i per tant $g{*}x_0 \in X$, i equivalentment $g \in X\{x_0^{-1}\}$. Així veiem que $\mathrm{St}(X) \subseteq X\{x_0^{-1}\}$, i per tant tenim que $|\mathrm{St}(X)| \leq |X\{x_0\}|$. Observem que $X\{x_0\} \in \mathcal{P}_{p^n}(G)$ i per tant $|X\{x_0\}| = p^n$. Ara bé, l'ordre de $\mathrm{St}(X)$ divideix $p^n$, però acabem de veure que $|\mathrm{St}(X)| \leq p^n$. Per tant ha de ser $|\mathrm{St}(X)| = p^n$, i per tant, per la proposició 9.3.6 tenim que $\mathrm{St}(X) \leq G$, i per tant, per la definició de $p$-subgrup de Sylow (9.3.8), $\mathrm{St}(X)$ és un $p$-subgrup de Sylow. □

**Corol·lari 9.3.11** (Teorema de Cauchy per grups)**.** *Siguin $G$ un grup d'ordre finit amb l'operació $*$ i $p$ un primer que divideix l'ordre de $G$. Aleshores existeix un element $g \in G$ tal que l'ordre de $g$ sigui $p$.*

*Demostració.* Direm que $e$ és l'element neutre de $G$. Pel Primer Teorema de Sylow (9.3.10) tenim que existeix un $p$-subgrup de Sylow $P$ de $G$, que per la definició de $p$-subgrup de Sylow (9.3.8) té ordre $p^n$ per a cert $n \in \mathbb{N}$. Ara bé, pel Teorema de Lagrange (9.1.36) tenim que per a tot $x \in P$ diferent del neutre el grup cíclic generar per $x$ ha de tenir ordre $p^t$ amb $t \in \{2, \ldots, n\}$, i per tant l'element $x^{p^{t-1}}$ té ordre $p$, ja que

$$\left(x^{p^{t-1}}\right)^p = x^{p^t} = e. \qquad \square$$

**Lemma 9.3.12.** *Siguin $G$ un grup d'ordre $p^n$ on $p$ és un primer amb l'operació $*$, $X$ un $G$-conjunt d'ordre finit amb una acció $\cdot$ i $X_G = \{x \in X \mid g \cdot x = x \text{ per a tot } g \in G\}$ un conjunt. Aleshores*

$$|X_G| \equiv |X| \pmod{p}.$$

*Demostració.* Siguin $\mathcal{O}(x_1), \ldots, \mathcal{O}(x_r)$ les òrbites dels elements de $X$. Aleshores, com que per la definició de l'òrbita d'un element d'un $G$-conjunt (9.3.3) aquestes són classes d'equivalència, tenim que

$$X = \bigcup_{i=1}^{r} \mathcal{O}(x_i),$$

i com que aquestes òrbites són disjuntes per ser classes d'equivalència

$$|X| = \sum_{i=0}^{r} |\mathcal{O}(x_i)|. \tag{9.13}$$

Ara bé, per les proposicions 9.3.7 i 9.3.6 i el Teorema de Lagrange (9.1.36) tenim que l'ordre $\mathcal{O}(x_i)$ divideix l'ordre de $X$, i per tant els únics elements amb òrbites que tinguin un ordre que no sigui divisible per $p$ són els elements del

conjunt $X_G$; i com que les òrbites d'aquests elements tenen un únic element tenim que

$$|X_G| = \sum_{x \in X_G} |\mathcal{O}(x)|,$$

i per tant, recordant que totes les altres òrbites tenen ordre divisible per $p$, trobem, amb (9.13), que

$$|X_G| \equiv |X| \pmod{p}. \qquad \square$$

**Teorema 9.3.13** (Segon Teorema de Sylow)**.** *Siguin $G$ un grup d'ordre finit amb l'operació $*$, $p$ un primer que divideixi l'ordre de $G$ i $P_1$, $P_2$ dos $p$-subgrups de Sylow de $G$. Aleshores existeix $g \in G$ tal que*

$$\{g\}P_1\{g^{-1}\} = P_2.$$

*Demostració.* Primer observem que aquest enunciat té sentit pel Primer Teorema de Sylow (9.3.10).

Definim el conjunt $X = \{\{x\}P_1 \mid x \in G\}$ i

$$\begin{aligned} \cdot \colon P_2 \times X &\longrightarrow X \\ (y, \{x\}P_1) &\longmapsto \{y\}\{x\}P_1. \end{aligned} \tag{9.14}$$

Primer veurem que $\cdot$ és una acció. Per veure que $\cdot$ està ben definida prenem $\{x\}P_1, \{x'\}P_1 \in X$ tals que $\{x\}P_1 = \{x'\}P_1$. Aleshores per a tot $y \in P_2$ tindrem $y \cdot \{x\}P_1 = \{y\}\{x\}P_1$ i $y \cdot \{x'\}P_1 = \{y\}\{x'\}P_1$, i com que per hipòtesi $\{x\}P_1 = \{x'\}P_1$, ha de ser $\{y\}\{x\}P_1 = \{y\}\{x'\}P_1$.

Comprovem que $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (9.3.1). Veiem que per a tot $y \in P_2$, $\{x\}P_1 \in X$ es compleix que $y \cdot \{x\}P_1 \in X$. Per la definició (9.14) tenim $y \cdot \{x\}P_1 \in X = \{y\}\{x\}P_1 = \{y * x\}P_1$, i com que per hipòtesi $G$ és un grup i $x, y \in G$, per la definició de grup (9.1.1) tenim que $y * x \in G$, i per tant $y \cdot \{x\}P_1 \in X$.

Sigui $e$ l'element neutre de $G$. Tenim que

$$\begin{aligned} e \cdot \{x\}P_1 &= \{e\}\{x\}P_1 \\ &= \{e * x\}P_1 = \{x\}P_1. \qquad \text{(l'element neutre d'un grup (9.1.3))} \end{aligned}$$

i per últim veiem que per a tot $y, y' \in G$ tenim $(y * y') \cdot P_1 = y \cdot (y' \cdot P_1)$. Això és

$$\begin{aligned} (y * y') \cdot P_1 &= \{y * y'\}P_1 \\ &= \{y\}\{y'\}P_1 \\ &= \{y\}(\{y'\}P_1) = y \cdot (y' \cdot P_1). \qquad \text{(Definició (9.14))} \end{aligned}$$

i per la definició de acció d'un grup sobre un conjunt (9.3.1) tenim que $X$ és un $G$-conjunt.

Definim el conjunt

$$X_{P_2} = \{\{x\}P_1 \in X \mid y \cdot \{x\}P_1 = \{x\}P_1 \text{ per a tot } y \in P_2\}. \tag{9.15}$$

Aleshores pel lemma 9.3.12 tenim que

$$|X_{P_2}| \equiv |X| \pmod{p}.$$

Ara bé, per la definició de l'índex d'un subgrup en un grup (9.1.38) i (9.14) tenim que $|X| = [G : P_1]$, i per hipòtesi tenim que $|X| = \frac{p^n m}{p^n} = m$, en particular $|X_{P_2}| \neq 0$. Així veiem que existeix almenys un element que satisfà la definició de $X_{P_2}$, (9.15); és a dir, existeix almenys un $\{x\}P_1$ tal que $y \cdot \{x\}P_1 = \{x\}P_1$ per a tot $y \in P_2$, i per tant tenim que $\{y\}\{x\}P_1 = \{x\}P_1$, i per tant $\{x^{-1}\}\{y\}\{x\}P_1 \in \{x^{-1}\}\{x\}P_1$, i equivalentment $x^{-1} * y * x \in P_1$ per a tot $y \in P_2$, i per tant $\{x^{-1}\}P_2\{x\} \subseteq P_1$, però, per hipòtesi, al ser els dos $p$-subgrups de Sylow, per la definició de $p$-subgrup de Sylow (9.3.8) trobem $|P_1| = |P_2| = \left|\{x^{-1}\}P_2\{x\}\right|$ i tenim que $\{x\}P_1\{x^{-1}\} = P_2$. □

**Corol·lari 9.3.14.** *$G$ té un únic $p$-subgrup de Sylow si i només si aquest és un subgrup normal.*

**Teorema 9.3.15** (Tercer Teorema de Sylow)**.** *Siguin $G$ un grup d'ordre $p^n m$ on $p$ és un primer que no divideix $m$ amb l'operació $*$ i $n_p$ el número de $p$-subgrups de Sylow de $G$. Aleshores $n_p \equiv 1 \pmod p$ i $n_p$ divideix l'ordre de $G$.*

*Demostració.* Definim el conjunt

$$X = \{T \subseteq G \mid T \text{ és un } p\text{-subgrup de Sylow de } G\}.$$

Pel Primer Teorema de Sylow (9.3.10) tenim que $X$ és no buit[3] i fixem $P \in X$.

Definim

$$\begin{aligned} \cdot \colon P \times X &\longrightarrow X \\ (g, T) &\longmapsto \{g\}T\{g^{-1}\}. \end{aligned} \tag{9.16}$$

Anem a veure que $\cdot$ és una acció. Veiem que $\cdot$ està ben definida, ja que si $T \in X$, aleshores per a tot $x \in G$, i en particular per a tot $x \in P$ ja que $P \leq G$, tenim $\left|\{x\}T\{x^{-1}\}\right| = |T|$, i per tant $\left|\{x\}T\{x^{-1}\}\right| \in X$ per la definició de $p$-subgrup de Sylow (9.3.8). Veiem ara que $\cdot$ satisfà les condicions de la definició de acció d'un grup sobre un conjunt (9.3.1). Sigui $e$ l'element neutre de $G$. Tenim que per a tot $T \in X$

$$\begin{aligned} e \cdot T &= \{e\}T\{e^{-1}\} && \text{(Definició (9.16))} \\ &= T \end{aligned}$$

i per a tot $g_1, g_2 \in P$ i $T \in X$

$$\begin{aligned} (g_1 * g_2) \cdot T &= \{g_1 * g_2\}T\{{g_1 * g_2}^{-1}\} && \text{(Definició (9.16))} \\ &= \{g_1 * g_2\}T\{g_2^{-1} * g_1^{-1}\} && \text{(Proposició 9.1.10)} \\ &= \{g_1\}\{g_2\}T\{g_2^{-1}\}\{g_1^{-1}\} \\ &= \{g_1\}(g_2 \cdot T)\{g_1^{-1}\} && \text{(Definició (9.16))} \\ &= g_1 \cdot (g_2 \cdot T) && \text{(Definició (9.16))} \end{aligned}$$

i per tant, per la definició de acció d'un grup sobre un conjunt (9.3.1) $X$ és un $P$-conjunt amb l'acció $\cdot$.

Definim el conjunt

$$X_P = \{T \in X \mid g \cdot T = T \text{ per a tot } g \in P\},$$

[3] Tindrem que $|X| = n_p$.

i per la definició (9.16) tenim que si $T \in X_P$ aleshores per a tot $g \in G$ es compleix $\{g\}T\{g^{-1}\} = T$. Ara bé, això és que $T = P$ per a tot $T \in X_P$, i per tant $|X_P| = 1$. Aleshores pel lemma 9.3.12 tenim que

$$|X| \equiv |X_P| \pmod{p},$$

o equivalentment

$$|X| \equiv 1 \pmod{p}.$$

Per veure que $|X|$ divideix l'ordre de $G$ prenem $P \in X$ i tenim, pel Segon Teorema de Sylow (9.3.13) i la definició de l'òrbita d'un element d'un $G$-conjunt (9.3.3), que

$$\mathcal{O}(P) = X,$$

on $\mathcal{O}(P)$ és l'òrbita de $P$, i per tant

$$|\mathcal{O}(P)| = |X|,$$

i per les proposicions 9.3.6 i 9.3.7 i el Teorema de Lagrange (9.1.36) tenim que $|X|$ divideix l'ordre de $G$. □

**Corol·lari 9.3.16.** *Si $G$ té ordre $p^n q^m$ on $p, q$ són primers amb $p < q$ aleshores $n_q = 1$, i pel corol·lari 9.3.14, aquest és normal en $G$.*

# Capítol 10

# Teoria d'anells

## 10.1 Anells

### 10.1.1 Propietats bàsiques dels anells i subanells

**Definició 10.1.1** (Anell)**.** Sigui $R$ un conjunt no buit i

$$+\colon R \times R \longrightarrow R \qquad\qquad \cdot\colon R \times R \longrightarrow R$$

dues operacions que satisfan

1. $R$ amb l'operació $+$ és un grup abelià.
2. Existeix un element $e$ de $R$ tal que $x \cdot e = e \cdot x = x$ per a tot $x \in R$.
3. Per a tot $x, y, z \in R$ tenim
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$
4. Per a tot $x, y, z \in R$ tenim
$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{i} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Aleshores direm que $R$ és un anell amb la suma $+$ i el producte $\cdot$. També direm que $R$ és un anell amb element neutre pel producte $e$.

Si per a tot $x, y \in R$ tenim $x \cdot y = y \cdot x$ direm que $R$ és un anell commutatiu.

**Proposició 10.1.2.** *Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$ i element neutre pel producte $e$. Aleshores l'element neutre pel producte de $R$ és únic.*

*Demostració.* Suposem que existeix un altre $e' \neq e$ tal que $x \cdot e' = e' \cdot x = x$ per a tot $x \in R$. Aleshores tindríem

$$e \cdot e' = e' \cdot e = e$$

a la vegada que

$$e \cdot e' = e' \cdot e = e'$$

i per tant ha de ser $e = e'$, que contradiu la hipòtesi que existeix un altre element neutre pel producte a $R$, i en conseqüència aquest és únic. □

**Definició 10.1.3** (Elements neutres d'un anell)**.** Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$. Aleshores direm que $0_R$ és l'element neutre de $R$ per la suma i $1_R$ és l'element neutre de $R$ pel producte i els denotarem per $0_R$ i $1_R$, respectivament.

Aquesta definició té sentit per la proposició 9.1.2 i la proposició 10.1.2.

**Notació 10.1.4.** Donat un anell $R$ un anell amb la suma $+$ i el producte $\cdot$, aprofitant que el producte $\cdot$ és associatiu escriurem

$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot x_2 \cdot x_3.$$

També, si el context ho permet (quan treballem amb un únic anell $R$), denotarem $1_R = 1$ i $0_R = 0$.

**Proposició 10.1.5.** *Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$. Aleshores per a tot $a, b, c \in R$ tenim*

1. $0 \cdot a = a \cdot 0 = 0$.
2. $(-1) \cdot a = a \cdot (-1) = -a$.
3. $(-a) \cdot (-b) = a \cdot b$.
4. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

*Demostració.* Comprovem el punt (1). Només veurem que $0 \cdot a = 0$ ja que l'altre demostració és anàloga. Com que $0 = 0 + 0$ per la definició de l'element neutre d'un anell per la suma (10.1.3), per la definició d'anell (10.1.1) tenim que

$$\begin{aligned} 0 \cdot a &= (0 + 0) \cdot a \\ &= 0 \cdot a + 0 \cdot a \end{aligned}$$

i per tant, per la definició de grup (9.1.1)

$$0 \cdot a - (0 \cdot a) = 0 \cdot a + 0 \cdot a - (0 \cdot a)$$

d'on veiem

$$0 \cdot a = 0,$$

com volíem veure.

Veiem ara el punt (2). Per la definició d'anell (10.1.1) tenim

$$1 \cdot a + (-1) \cdot a = (1 - 1) \cdot a \quad \text{i} \quad (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a$$

i per tant, com que $1 - 1 = -1 + 1 = 0$ per la definició de l'element neutre d'un anell per la suma (10.1.3), tenim que $a + (-1) \cdot a = (-1) \cdot a + a = 0$, però per la proposició 9.1.6 tenim que $(-1) \cdot a = -a$. L'altre igualtat és anàloga.

Continuem veient el punt (3). Pel punt (2) tenim que

$$(-a) \cdot (-b) = a \cdot (-1) \cdot (-1) \cdot b.$$

Ara bé, pel punt (2) de nou tenim que $(-1) \cdot (-1) = -(-1)$, i per la proposició 9.1.9 tenim que $-(-1) = 1$ i per tant

$$(-a) \cdot (-b) = a \cdot b.$$

Per veure el punt (4) només veurem que $(-a)\cdot b = -(a\cdot b)$ ja que l'altre demostració és anàloga. Pel punt (2) tenim que

$$-(a\cdot b) = (-1)\cdot(a\cdot b) \quad \text{i} \quad (-a)\cdot b = (-1)\cdot a\cdot b.$$

Ara bé, per la definició d'anell (10.1.1)

$$(-1)\cdot a\cdot b - (-1)\cdot(a\cdot b) = (-1-(-1))\cdot(a\cdot b),$$

i per la proposició 9.1.9 tenim que $-(-1) = 1$ i per tant, per la definició de grup (9.1.1) tenim $-1+1=0$ i trobem

$$(-1)\cdot a\cdot b - (-1)\cdot(a\cdot b) = 0\cdot(a\cdot b) = 0,$$

i podem veure també que

$$(-1)\cdot(a\cdot b) - (-1)\cdot a\cdot b = 0$$

de manera anàloga. Aleshores, per la proposició 9.1.6 tenim que

$$(-a)\cdot b = -(a\cdot b),$$

com volíem veure. □

**Proposició 10.1.6.** *Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i $a$ un element de $R$ tal que existeixi $b\in R$ que satisfaci*

$$a\cdot b = b\cdot a = 1.$$

*Aleshores $b$ és únic.*

*Demostració.* Suposem que existeix un altre element $b'\in R$ tal que

$$a\cdot b' = b'\cdot a = 1.$$

Aleshores tenim

$$a\cdot b = a\cdot b'$$

i per tant

$$b\cdot a\cdot b = b\cdot a\cdot b'$$

i com que per hipòtesi $b\cdot a = 1$ per la definició de l'element neutre d'un anell pel producte (10.1.3) trobem

$$b = b'.$$ □

**Definició 10.1.7** (Element invertible)**.** Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i $x$ un element de $R$ tal que existeixi $x'\in R$ tals que

$$x\cdot x' = x'\cdot x = 1.$$

Aleshores direm que $x$ és invertible o que $x$ és un element invertible de $R$.

**Definició 10.1.8** (L'invers d'un element)**.** Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i $x$ un element invertible de $R$. Aleshores denotarem per $x^{-1}$ l'element de $R$ tal que

$$x\cdot x^{-1} = x^{-1}\cdot x = 1.$$

Direm que $x^{-1}$ és l'invers de $x$.

Aquesta definició té sentit per la proposició 10.1.6.

**Definició 10.1.9** (Subanell)**.** Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i $S \subseteq R$ un subconjunt amb $1 \in S$ tal que per a tot $a, b \in S$ tenim $a \cdot b, a+b \in S$ i $S$ un anell amb la suma $+$ i el producte $\cdot$. Aleshores direm que $S$ és un subanell de $R$

Ho denotarem amb $S \leq R$.

### 10.1.2 Ideals i ideals principals

**Definició 10.1.10** (Ideal)**.** Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I$ un subconjunt no buit de $R$ tal que $I$ sigui un subgrup del grup $R$ amb la suma $+$ i tal que per a tot $x \in I$, $r \in R$ tenim $r \cdot x \in I$. Aleshores direm que $I$ és un ideal de $R$.

**Observació 10.1.11.** $0 \in I$.

**Notació 10.1.12.** Si $I$ és un ideal d'un anell $R$ denotarem $I \triangleleft R$.

**Proposició 10.1.13.** *Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I$ un subconjunt no buit de $R$. Aleshores tenim que $I$ és un ideal de $R$ si i només si*

1. *Per a tot $x, y \in I$ tenim $x - y \in I$.*
2. *Per a tot $r \in R$, $x \in I$ tenim $r \cdot x \in I$.*

*Demostració.* Veiem que la condició és suficient ($\Rightarrow$). Suposem que $I$ és un ideal de $R$. Hem de veure que per a tot $x, y \in I$, $r \in R$ tenim $x - y \in I$ i $r \cdot x \in I$. Per la definició de grup (9.1.1) tenim que $x - y \in I$, ja que, per la definició d'ideal d'un anell (10.1.10) tenim que $I$ és un grup amb la suma $+$. També trobem $r \cdot x \in I$ per la definició d'ideal d'un anell (10.1.10).

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem que per a tot $x, y \in I$, $r \in R$ tenim $x - y \in I$ i $r \cdot x \in I$. Per la proposició 9.1.15 tenim que $I$ és un subgrup del grup $R$ amb la suma $+$, i per la definició d'ideal d'un anell (10.1.10) tenim que $I$ és un ideal de $R$. □

**Notació 10.1.14.** Si $(a)$ és un ideal principal d'un anell $R$ denotarem $(a) \trianglelefteq R$.

**Proposició 10.1.15.** *Siguin $I, J$ dos ideals d'un anell $R$ amb la suma $+$ i el producte $\cdot$. Aleshores els conjunts*

1. $I + J = \{x + y \mid x \in I, y \in J\}$.
2. $I \cap J$.
3. $IJ = \{x_1 \cdot y_1 + \ldots x_n \cdot y_n \mid x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J, n \in \mathbb{N}\}$.

*són ideals de $R$.*

*Demostració.* Comencem demostrant el punt (1). Per la proposició 10.1.13 només ens cal veure que per a tot $a, b \in I + J$, $r \in R$ tenim $a - b \in I + J$ i $r \cdot a \in I + J$. Prenem doncs $a, b \in I + J$. Aleshores tenim $a = a_1 + a_2$ i

$b = b_1 + b_2$ per a certs $a_1, b_1 \in I$ i $a_2, b_2 \in J$. Volem veure que $a - b \in I + J$. Això és

$$\begin{aligned} a_1 + a_2 - (b_1 + b_2) &= a_1 + a_2 - b_1 - b_2 && (10.1.5) \\ &= (a_1 - b_1) + (a_2 - b_2) && (\text{grup abelià } (9.1.25)) \end{aligned}$$

i com que, per hipòtesi, $I, J$ són ideals de $R$ per la proposició 10.1.13 tenim que $a_1 - b_1 \in I$ i $a_2 - b_2 \in J$, i per tant $a - b = (a_1 - b_1) + (a_2 - b_2) \in I + J$.

Veiem ara que per a tot $r \in R$ es satisfà $r \cdot a \in I + J$. Tenim

$$\begin{aligned} r \cdot a &= r \cdot (a_1 + a_2) && (\text{anell } (10.1.1)) \\ &= r \cdot a_1 + r \cdot a_2 && (\text{anell } (10.1.1)) \end{aligned}$$

i per la proposició 10.1.13 tenim que $r \cdot a_1 \in I$ i $r \cdot a_2 \in J$, i per tant $r \cdot a = r \cdot a_1 + r \cdot a_2 \in I + J$. Aleshores per la proposició 10.1.13 tenim que $I + J$ és un ideal de $(R, +, \cdot)$.

Veiem ara el punt (2). Per la proposició 10.1.13 només ens cal veure que per a tot $a, b \in I \cap J$, $r \in R$ tenim $a - b \in I \cap J$ i $r \cdot a \in I \cap J$. Prenem doncs $a, b \in I \cap J$, i per tant $a, b \in I$ i $a, b \in J$, i per la proposició 10.1.13 tenim que $a - b \in I$ i $a - b \in J$, i tenim que $a - b \in I \cap J$.

Per veure que $r \cdot a \in I \cap J$ per a tot $r \in R$ tenim per la definició d'ideal d'un anell (10.1.10) que $r \cdot a \in I$ i $r \cdot a \in J$, i per tant $r \cdot a \in I \cap J$ i per la proposició 10.1.13 $I \cap J$ és un ideal de $R$.

Acabem veient el punt (3). Per la proposició 10.1.13 només ens cal veure que per a tot $a, b \in IJ$, $r \in R$ tenim $a - b \in IJ$ i $r \cdot a \in IJ$. Prenem doncs $a, b \in IJ$, i tenim que $a = x_1 \cdot y_1 + \cdots + x_n \cdot y_n$, $b = x'_1 \cdot y'_1 + \cdots + x'_m \cdot y'_m$ per a certs $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in I$, $y_1, \ldots, y_n, y'_1, \ldots, y'_m \in J$. Per veure que $a - b \in IJ$ fem, per la proposició 10.1.5,

$$\begin{aligned} a - b = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - (x'_1 \cdot y'_1 + \cdots + x'_m \cdot y'_m) = \\ = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - x'_1 \cdot y'_1 - \cdots - x'_m \cdot y'_m \end{aligned}$$

i com que $I$ és, per hipòtesi, un anell, per les proposicions 10.1.5 i 10.1.13 tenim que $-x'_1, \ldots, -x'_m \in I$ i $a - b = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - x'_1 \cdot y'_1 - \cdots - x'_m \cdot y'_m \in IJ$.

Veiem ara que per a tot $r \in R$ es satisfà $r \cdot a \in I$. Això és

$$\begin{aligned} r \cdot a &= r \cdot (x_1 \cdot y_1 + \cdots + x_n \cdot y_n) \\ &= r \cdot x_1 \cdot y_1 + \cdots + r \cdot x_n \cdot y_n && (10.1.5) \end{aligned}$$

i com que $I$ és, per hipòtesi, un anell, per les proposicions 10.1.5 i 10.1.13 tenim que $r \cdot x_1, \ldots, r \cdot x_n \in I$, i per tant $r \cdot a = r \cdot x_1 \cdot y_1 + \cdots + r \cdot x_n \cdot y_n \in IJ$ i per la proposició 10.1.13 tenim que $IJ$ és un ideal de $R$. □

**Definició 10.1.16** (Ideal principal)**.** Sigui $I$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$ tal que $I = \{a\}R = R\{a\} = \{r \cdot a \mid r \in R\}$ per a cert $a \in I$. Aleshores direm que $I$ és un anell principal de $R$. Ho denotarem amb $I = (a)$.

### 10.1.3 Cossos i l'anell quocient

**Definició 10.1.17** (Cos)**.** Sigui $\mathbb{K}$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ tal que $\mathbb{K} \setminus \{0\}$ sigui un grup abelià amb el producte $\cdot$. Aleshores direm que $\mathbb{K}$ és un cos amb la suma $+$ i el producte $\cdot$.

**Proposició 10.1.18.** *Sigui $\mathbb{K}$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$. Aleshores tenim que $\mathbb{K}$ és un cos si i només si els únics ideals de $\mathbb{K}$ són $(0)$ i $\mathbb{K}$.*

*Demostració.* Comencem comprovant que la condició és suficient ($\Rightarrow$). Suposem doncs que $\mathbb{K}$ és un cos amb la suma $+$ i el producte $\cdot$ i que $I$ és un ideal de $\mathbb{K}$ amb $I \neq (0)$, i per tant existeix $a \in \mathbb{K}$, $a \neq 0$ tal que $a \in I$. Com que, per hipòtesi, $(\mathbb{K} \setminus \{0\}, \cdot)$ és un grup i $a \neq 0$ per la definició de l'invers d'un element d'un grup (9.1.7) existeix $a^{-1} \in \mathbb{K}$ tal que $a \cdot a^{-1} = 1$, i per la definició d'ideal d'un anell (10.1.10) trobem que $1 \in I$, i per tant per la proposició 10.1.13 tenim que per a tot $x \in \mathbb{K}$ tenim $x \cdot 1 = x \in I$, i per tant $I = \mathbb{K}$.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem que els únics ideals de $\mathbb{K}$ són $(0)$ i $\mathbb{K}$. Prenem un element $a \in \mathbb{K}$, $a \neq 0$ i considerem l'ideal principal $(a)$, que per hipòtesi ha de ser $(a) = (1) = \mathbb{K}$, i per la definició d'ideal principal (10.1.16) tenim que existeix $a' \in (1)$ tal que $a \cdot a' = 1$, i per tant, per la definició de grup (9.1.1) tenim que $\mathbb{K} \setminus \{0\}$ és un grup amb el producte $\cdot$ i per la definició de cos (10.1.17) tenim que $\mathbb{K}$ és un cos amb la suma $+$ i el producte $\cdot$. □

**Proposició 10.1.19.** *Sigui $I$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$. Aleshores la relació*

$$x \sim y \iff x - y \in I \quad \textit{per a tot } x, y \in R$$

*és una relació d'equivalència.*

*Demostració.* Comprovem que $\sim$ satisfà la definició de relació d'equivalència (2.3.2):

1. Reflexiva: Prenem $x \in R$. Per l'observació 10.1.11 tenim que $0 \in I$, i per tant $x - x = 0 \in I$ i veiem que $x \sim x$.

2. Simètrica: Siguin $x_1, x_2 \in I$ tals que $x_1 \sim x_2$. Això és que $x_1 - x_2 \in I$. Per la definició d'ideal d'un anell (10.1.10) tenim que $(-1) \cdot (x_1 - x_2) \in I$, i per la proposició 10.1.5 tenim que $x_2 - x_1 \in I$, és a dir, $x_2 \sim x_1$.

3. Transitiva: Siguin $x_1, x_2, x_3 \in R$ tals que $x_1 \sim x_2$ i $x_2 \sim x_3$. Per la definició d'ideal d'un anell (10.1.10) tenim que $x_3 - x_2 \in I$, i per la proposició 10.1.13 tenim que $x_1 - x_2 - (x_3 - x_2) \in I$. Ara bé, per la proposició 10.1.5 tenim que això és $x_1 - x_3 \in I$, i per tant $x_1 \sim x_3$.

Per tant $\sim$ és una relació d'equivalència. □

**Proposició 10.1.20.** *Sigui $I$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$. Aleshores $R/I$ amb la suma $[x] + [y] = [x + y]$ i el producte $[x] \cdot [y] = [x \cdot y]$ és un anell.*

*Demostració.* Aquest enunciat té sentit per la proposició 10.1.19.

Per la proposició 9.1.31 tenim que $(R/I, +)$ és un grup, i com que

$$\begin{aligned} [x] + [y] &= [x + y] \\ &= [y + x] && \text{(grup abelià (9.1.25))} \\ &= [y] + [x] \end{aligned}$$

tenim que $R/I$ és un grup abelià amb la suma $+$. Veiem ara que per a tot $x, y, z \in R/I$ tenim $[x]\cdot([y]\cdot[z]) = ([x]\cdot[y])\cdot[z]$ i $[x]\cdot([y]+[z]) = [x]\cdot[y]+[x]\cdot[z]$. Tenim

$$\begin{aligned}[x]\cdot([y]\cdot[z]) &= [x]\cdot[y\cdot z]\\ &= [x\cdot(y\cdot z)]\\ &= [(x\cdot y)\cdot z]\\ &= [x\cdot y]\cdot[z] = ([x]\cdot[y])\cdot[z]\end{aligned}$$

i

$$\begin{aligned}[x]\cdot([y]+[z]) &= [x]\cdot[y+z]\\ &= [x\cdot(y+z)]\\ &= [x\cdot y + x\cdot z] = [x]\cdot[y]+[x]\cdot[z]\end{aligned}$$

i per la definició d'anell (10.1.1) tenim que $R/I$ és un anell amb la suma $+$ i el producte $\cdot$. □

**Definició 10.1.21** (Anell quocient)**.** Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I$ un ideal de $R$. Aleshores direm que $R/I$ és un anell quocient.

Aquesta definició té sentit per la proposició 10.1.20.

## 10.2 Tres Teoremes d'isomorfisme entre anells

### 10.2.1 Morfismes entre anells

**Definició 10.2.1** (Morfisme entre anells)**.** Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$ amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ una aplicació tal que

1. $f(x +_R y) = f(x) +_S f(y)$ per a tot $x, y \in R$.
2. $f(x *_R y) = f(x) *_S f(y)$ per a tot $x, y \in R$.
3. $f(1_R) = 1_S$.

Aleshores diem que $f$ és un morfisme entre anells. Definim també

1. Si $f$ és injectiva direm que $f$ és un monomorfisme entre anells.
2. Si $f$ és exhaustiva direm que $f$ és un epimorfisme entre anells.
3. Si $f$ és bijectiva direm que $f$ és un isomorfisme entre anells. També escriurem $R \cong S$.
4. Si $R = S$ direm que $f$ és un endomorfisme entre anells.
5. Si $R = S$ i $f$ és bijectiva direm que $f$ és un automorfisme entre anells.

**Observació 10.2.2.** *Si $f$ és un morfisme entre anells aleshores $f$ és un morfisme entre grups.*

**Proposició 10.2.3.** *Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$ amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

1. $f(0_R) = 0_S$.
2. $f(-x) = -f(x)$ *per a tot* $x \in R$.

*Demostració.* Per l'observació 10.2.2 tenim que $f$ és un morfisme entre els grups $R$ amb la suma $+_R$ i $S$ amb la suma $+_S$, i per la proposició 9.2.2 tenim que $f(0_R) = 0_S$ i $f(-x) = -f(x)$ per a tot $x \in R$. □

**Definició 10.2.4** (Nucli i imatge)**.** Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$ amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ un morfisme entre anells. Aleshores definim

$$\ker(f) = \{x \in R \mid f(x) = 0_S\}$$

com el nucli de $f$, i

$$\mathrm{Im}(f) = \{y \in S \mid f(x) = y \text{ per a cert } x \in R\}$$

com la imatge de $f$.

**Observació 10.2.5.** $\ker(f) \subseteq R$, $\mathrm{Im}(f) \subseteq S$.

**Proposició 10.2.6.** *Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$ amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

1. $\ker(f) \triangleleft R$.
2. $\mathrm{Im}(f) \leq S$.

*Demostració.* Aquest enunciat té sentit per l'observació 10.2.6

Comencem veient el punt (1). Com que, per la proposició 10.2.3, tenim que $f(0_R) = 0_S$ veiem, per la definició de nucli d'un morfisme entre anells (10.2.4), que $\ker(f) \neq \emptyset$. Prenem doncs $a \in \ker(f)$. Observem que, per la definició de morfisme entre anells (10.2.1), tenim que $f(r *_R a) = f(r) *_S f(a)$ per a tot $r \in R$, i per tant, com que per la definició de nucli d'un morfisme entre anells (10.2.4) es compleix $f(a) = 0_S$ tenim que

$$f(r *_R a) = f(r) *_S f(a) = f(r) *_S 0_S = 0_S$$

i per tant $r *_R a \in \ker(f)$ per a tot $r \in R$, $a \in \ker(f)$. Ara bé per la definició de ideal d'un anell (10.1.10) tenim que $\ker(f)$ és un ideal de $R$.

Veiem ara el punt (2). Veiem que per a tot $x, y \in \mathrm{Im}(f)$ tenim $x *_S y \in \mathrm{Im}(f)$. Per la definició d'imatge d'un morfisme entre anells (10.2.4) tenim que existeixen $a, b \in R$ tals que $f(a) = x$ i $f(b) = y$. Ara bé, per la definició d'anell (10.1.1) tenim que $a *_R b = c \in R$, i per tant per la definició d'imatge d'un morfisme entre anells (10.2.4) tenim que $f(c) = x *_S y \in \mathrm{Im}(f)$. Veiem ara que $\mathrm{Im}(f)$ és un anell amb la suma $+_S$ i el producte $*_S$. Com que, per l'observació 10.2.2 tenim que $f$ és un morfisme entre grups per la proposició 9.2.7 tenim que $\mathrm{Im}(f)$

és un subgrup del grup $S$ amb la suma $+_S$; i per la definició d'anell (10.1.1) tenim que per a tot $x, y, z \in R$ es satisfà

$$x *_R (y *_R z) = (x *_R y) *_R z \quad \text{i} \quad x *_R (y +_R z) = x *_R y +_R x *_R z,$$

i per la definició de subanell (10.1.9) tenim que $\mathrm{Im}(f)$ és un subanell de $S$, com volíem veure. □

**Proposició 10.2.7.** *Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$, $D$ un anell commutatiu amb la suma $+_D$ i el producte $*_D$ tres anells commutatius amb $1_R \neq 0_R$, $1_S \neq 0_S$ i $1_D \neq 0_D$ i $f\colon R \longrightarrow S$, $g\colon S \longrightarrow D$ dos morfismes entre anells. Aleshores $g \circ f\colon R \longrightarrow D$ és un morfisme entre anells.*

*Demostració.* Per la definició de morfisme entre anells (10.2.1) trobem que

$$\begin{aligned} g(f(x +_R y)) &= g(f(x) +_S g(y)) \\ &= g(f(x)) +_D g(f(x)), \end{aligned}$$

i

$$\begin{aligned} g(f(x *_R y)) &= g(f(x) *_S g(y)) \\ &= g(f(x)) *_D g(f(x)). \end{aligned}$$

També tenim

$$g(f(1_R)) = g(1_S) = 1_D$$

i per la definició de morfisme entre anells (10.2.1) tenim que $g \circ f$ és un morfisme entre anells. □

**Corol·lari 10.2.8.** *Si $f, g$ són isomorfismes aleshores $g \circ f$ és isomorfisme.*

**Lemma 10.2.9.** *Siguin $R$ un anell commutatiu amb la suma $+_R$ i el producte $*_R$, $S$ un anell commutatiu amb la suma $+_S$ i el producte $*_S$ amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

$$\ker(f) \text{ és un ideal de } R \quad i \quad \mathrm{Im}(f) \text{ és un subanell de } S.$$

*Demostració.* Comencem veient que $\ker(f)$ és un ideal de $R$. Per l'observació 10.2.2 tenim que $\ker(f)$ és un morfisme entre grups, i per la proposició 9.2.7 tenim que $\ker(f)$ és un subgrup del grup $R$ amb la suma $+_R$.

Prenem $x \in \ker(f)$ i $r \in R$. Volem veure que $r *_R r \in \ker(f)$. Tenim

$$\begin{aligned} f(r *_R x) &= f(r) *_S f(x) && \text{(morfisme entre anells (10.2.1))} \\ &= f(r) *_S 0_S && \text{(nucli d'un morfisme entre anells (10.2.4))} \\ &= 0_S && \text{(l'element neutre d'un anell pel producte (10.1.3))} \end{aligned}$$

i per la definició de nucli d'un morfisme entre anells (10.2.4) tenim que $r *_R x \in \ker(f)$, i per la proposició 10.1.13 tenim que $\ker(f)$ és un ideal de $R$.

Veiem ara que $\mathrm{Im}(f)$ és un subanell de $S$. Per l'observació 10.2.2 tenim que $\mathrm{Im}(f)$ és un morfisme entre grups, i per la proposició 9.2.7 tenim que $\mathrm{Im}(f)$ és un subgrup del grup $S$ amb la suma $+_S$.

Prenem $x, y \in \mathrm{Im}(f)$. Volem veure que $x *_S y \in \mathrm{Im}(f)$. Per la definició d'imatge d'un morfisme entre anells (10.2.4) tenim que existeixen $x', y' \in R$ tals que $f(x') = x$ i $f(y') = y$. Ara bé, per la definició d'anell (10.1.1) tenim que $x' *_R y' \in R$, i per tant

$$\begin{aligned} f(x' *_R y') + f(x') *_S f(y') & \qquad \text{(morfisme entre anells (10.2.1))} \\ = x *_S y & \end{aligned}$$

i per la definició de imatge d'un morfisme entre grups (9.2.5) trobem que $x *_S y \in \mathrm{Im}(f)$.

També tenim, per la definició de morfisme entre anells (10.2.1), que $1_S \in \mathrm{Im}(f)$, ja que $f(1_R) = 1_S$, i per tant, per la definició de subanell (10.1.9), tenim que $\mathrm{Im}(f)$ és un subanell de $S$. □

### 10.2.2 Teoremes d'isomorfisme entre anells

**Teorema 10.2.10** (Primer Teorema de l'isomorfisme)**.** *Siguin $R$ un anell amb la suma $+_R$ i el producte $*_R$, $S$ un anell amb la suma $+_S$ i el producte $*_S$ i $\varphi\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

$$R/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

*Demostració.* Aquest enunciat té sentit per la proposició 10.2.6. □

**Teorema 10.2.11** (Segon Teorema de l'isomorfisme)**.** *Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I, J$ dos ideals de $R$. Aleshores*

$$(I + J)/I \cong J/(I \cap J).$$

*Demostració.* □

**Lemma 10.2.12.** *Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I$, $J$ dos ideals de $R$ tals que $I \subseteq J$. Aleshores $J/I$ és un ideal de $R/I$.*

*Demostració.* □

**Teorema 10.2.13** (Tercer Teorema de l'isomorfisme)**.** *Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $I$, $J$ dos ideals de $R$ tals que $I \subseteq J$. Aleshores*

$$(R/I)/(J/I) \cong R/J.$$

*Demostració.* Aquest enunciat té sentit pel lemma 10.2.12. □

### 10.2.3 Característica d'un anell

**Definició 10.2.14** (Característica)**.** Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$. Direm que $R$ té característica $n > 0$ si $n = \min_{n \in \mathbb{N}}\{n \cdot 1 = 0\}$. Ho denotarem amb $\mathrm{ch}(R) = n$. Si aquest $n$ no existeix diem que $R$ té característica 0 i $\mathrm{ch}(R) = 0$.

**Proposició 10.2.15.** *Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i*

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n\cdot 1 = 1 + \overset{n)}{\cdots} + 1 \end{aligned}$$

*una aplicació. Aleshores $f$ és un morfisme entre anells i* $\ker(f) = (\mathrm{ch}(R))$.

*Demostració.* Aquest enunciat té sentit per la proposició 10.2.6.

Comencem veient que $f$ és un morfisme entre anells. Veiem que $f$ és un morfisme entre els grup. Tenim que per a tot $n, m \in \mathbb{Z}$

$$\begin{aligned} f(n+m) &= 1 + \overset{n+m)}{\cdots} + 1 \\ &= (1 + \overset{n)}{\cdots} + 1) + (1 + \overset{m)}{\cdots} + 1) \\ &= f(n) + f(m) \end{aligned}$$

i per la definició de morfisme entre grups (9.2.1) tenim que $f$ és un morfisme entre grups. Veiem ara que $f(1) = 1$. Tenim que $f(1) = 1 \cdot 1 = 1$ i per tant per la definició de morfisme entre anells (10.2.1) tenim que $f$ és un morfisme entre anells.

Veiem ara que $\ker(f) = (\mathrm{ch}(n))$. Per la definició de nucli d'un morfisme entre anells (10.2.4) tenim que $\ker(f) = \{x \in \mathbb{N} \mid f(n) = 0\}$. Per tant

$$\ker(f) = \{n \in \mathbb{N} \mid n \cdot 1 = 0\}$$

i per la definició de característica d'un anell (10.2.14) tenim que $n = \mathrm{ch}(R)$, i per tant $\ker(f) = \{k \cdot n \mid k \in \mathbb{N}\}$. Ara bé, per la definició de ideal d'un anell (10.1.10) tenim que $\ker(f) = (n)$, com volíem veure. □

**Corol·lari 10.2.16.** *Si* $\mathrm{ch}(R) = 0$ *aleshores existeix un subanell $S$ de $R$ tal que $S \cong \mathbb{Z}$.*

*Si* $\mathrm{ch}(R) = n$ *aleshores existeix un subanell $S$ de $R$ tal que $S \cong \mathbb{Z}/(n)$.*

## 10.3 Dominis

### 10.3.1 Dominis d'integritat, ideals primers i maximals

**Definició 10.3.1** (Divisor de 0)**.** Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $a, b \neq 0$ dos elements de $R$ tals que $a \cdot b = 0$. Aleshores diem que $a$ és un divisor de 0 en $R$.

**Definició 10.3.2** (Dominis d'integritat)**.** Sigui $D$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ tal que no existeix cap $a \in D$ tal que $a$ sigui un divisor de 0 en $D$. Aleshores direm que $D$ és un domini d'integritat.

**Proposició 10.3.3.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $a \neq 0$ un element de $D$. Aleshores*

$$a \cdot x = a \cdot y \Longrightarrow x = y.$$

*Demostració.* Tenim

$$a \cdot x - a \cdot y = 0$$

i per la proposició 10.1.5 tenim que

$$(x - y) \cdot a = 0.$$

Ara bé, com que, per hipòtesi, $D$ és un domini d'integritat i $a \neq 0$ tenim que ha de ser $x - y = 0$, i per tant trobem $x = y$. □

**Definició 10.3.4** (Ideal primer)**.** Sigui $I$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$ amb $I \neq R$ tal que si $a \cdot b \in I$ tenim $a \in I$ o $b \in I$. Aleshores direm que $I$ és un ideal primer de $R$.

**Proposició 10.3.5.** *Sigui $I$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$ amb $I \neq R$. Aleshores*

$$R/I \text{ és un domini d'integritat} \iff I \text{ és un ideal primer de } R.$$

*Demostració.* Comencem demostrant que la condició és suficient ($\Rightarrow$). Suposem doncs que $R/I$ és un domini d'integritat i prenem $[a], [b] \in R/I$ tals que $[a] \cdot [b] = [0]$. Aleshores per la definició de anell quocient (10.1.21) tenim que $a \cdot b \in I$. Ara bé, com que per hipòtesi $R/I$ és un domini d'integritat tenim que ha de ser $[a] = [0]$ ó $[b] = [0]$, i per tant trobem que ha de ser $a \in I$ o $b \in I$, i per la definició d'ideal primer (10.3.4) trobem que $I$ és un ideal primer de $R$.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem doncs que $I$ és un ideal primer de $R$. Per la proposició 10.1.20 tenim que $R/I$ és un anell commutatiu amb $1 \neq 0$. Prenem doncs $a \in R$, $a \notin I$ i suposem que existeix $b \in R$ tal que $[a] \cdot [b] = [0]$. Això és que $a \cdot b \in I$, i com que per hipòtesi $I$ és un ideal primer, per la definició d'ideal primer (10.3.4) trobem que ha de ser $b \in I$, i per tant $[b] = [0]$ i per la definició de domini d'integritat (10.3.2) tenim que $R/I$ és un domini d'integritat. □

**Corol·lari 10.3.6.** *$R$ és un domini d'integritat si i només si $(0)$ és un ideal primer.*

**Definició 10.3.7** (Ideal maximal)**.** Sigui $M$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$ amb $M \neq R$ tal que per a tot ideal $I$ de $R$ amb $M \subseteq I \subseteq R$ ha de ser $I = M$ o $I = R$. Aleshores direm que $M$ és un ideal maximal de $R$.

**Proposició 10.3.8.** *Sigui $M$ un ideal d'un anell $R$ amb la suma $+$ i el producte $\cdot$ amb $I \neq R$. Aleshores*

$$R/M \text{ és un cos} \iff M \text{ és un ideal maximal de } R.$$

*Demostració.* Aquest enunciat té sentit per la proposició 10.1.20.

Comencem veient la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $R/M$ és un cos i prenem un ideal $I/M$ de $R/M$. Aleshores ha de ser $M \subseteq I \subseteq R$. Per la proposició 10.1.18 tenim que els únics ideals de $R/M$ són $([0])$ i $R/M$, i per tant ha de ser $I = M$ o $I = R$, i per la definició d'ideal maximal (10.3.7) tenim que $M$ és un ideal maximal de $R$.

Veiem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $M$ és un ideal maximal de l'anell $R$ i considerem, per la proposició 10.1.20, l'anell

$R/M$. Per la proposició 10.1.18 tenim que només hem de veure que els únics ideals de $R/M$ són (0) i $R$. Prenem un ideal $I/M$ de $R/M$. Aquest ha de ser tal que $M \subseteq I \subseteq R$, i per la definició d'ideal maximal (10.3.7) tenim que ha de ser $I = M$ o $I = R$, i per tant $I/M$ ha de ser ([0]) o $R/M$ i per la proposició 10.1.20 tenim que $R/M$ és un cos. □

**Corol·lari 10.3.9.** *$M$ és maximal $\implies$ $M$ és primer.*

**Teorema 10.3.10.** *Sigui $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$. Aleshores $R$ és un domini d'integritat si i només si $R \setminus \{0\}$ és un cos amb la suma $+$ i el producte $\cdot$.*

*Demostració.* □

**Proposició 10.3.11.** *Sigui $I \neq (0)$ un ideal primer d'un domini d'integritat $D$ amb la suma $+$ i el producte $\cdot$. Aleshores $I$ és maximal.*

*Demostració.* Posem $I = (a)$. Per hipòtesi tenim que $a \neq 0$ i que $I$ és un ideal primer. Sigui $b \in D$ tal que $(a) \subseteq (b)$. Aleshores tenim que $a \in (b)$, i per la definició d'ideal principal (10.1.16) tenim que $a = a' \cdot b$ per a cert $a' \in D$. Aleshores, per la definició d'ideal primer (10.3.4), tenim que $a' \in (a)$ o $b \in (a)$.

Suposem que $a' \in (a)$. Aleshores tenim que $a' = a \cdot \beta$ per a cert $\beta \in D$, i per tant $a = a \cdot \beta \cdot b$, i per la proposició 10.3.3 tenim que $1 = \beta \cdot b$, i per tant $1 \in (b)$, d'on trobem $(b) = R$. Suposem ara que $b \in I$. Aleshores $(a) = (b)$, i per la definició de ideal maximal (10.3.7) tenim que $I = (a)$ és un ideal maximal de $D$. □

### 10.3.2 Lemma de Zorn

**Definició 10.3.12** (Relació d'ordre)**.** Sigui $A$ un conjunt no buit i $\leq$ una relació binària en $A$ que satisfaci

1. Reflexiva: $a \leq a$ per a tot $a \in A$.
2. Antisimètrica: $a \leq b$ i $b \leq a$ impliquen $a = b$ per a tot $a, b \in A$.
3. Transitiva: Si $a \leq b$ i $b \leq c$, aleshores $a \leq c$ per a tot $a, b, c \in A$.

Aleshores direm que $\leq$ és una relació d'ordre.

**Definició 10.3.13** (Cadena)**.** Siguin $\mathcal{C}$ un conjunt i $\leq$ una relació d'ordre en $A$ tal que per a tot $a, b \in A$ es satisfà $a \leq b$ ó $b \leq a$. Aleshores direm que $\mathcal{C}$ amb $\leq$ és una cadena.

**Proposició 10.3.14.** *Siguin $Y$ i $\mathcal{X} \subseteq \mathcal{P}(Y)$ dos conjunts tals que per a tot $A, B \in X$ tenim $A \subseteq B$ o $B \subseteq A$. Aleshores $\mathcal{X}$ amb $\subseteq$ és una cadena.*

*Demostració.* Comprovem que $\subseteq$ satisfà les condicions de la definició de relació d'ordre (10.3.12):

1. Reflexiva: Si $A \in \mathcal{X}$ tenim $A = A$, i en particular $A \subseteq A$.
2. Antisimètrica: Si $A, B \in \mathcal{X}$ tals que $A \subseteq B$ i $B \subseteq A$ tenim, per doble inclusió, que $A = B$.

3. Transitiva: Si $A, B, C \in \mathcal{X}$ tals que $A \subseteq B$ i $B \subseteq C$ aleshores $A \subseteq C$.

per tant, per les definicions de relació d'ordre (10.3.12) i cadena (10.3.13) tenim que $\mathcal{X}$ amb $\subseteq$ és una cadena. □

**Definició 10.3.15** (Cota superior d'una cadena)**.** Siguin $\mathcal{C}$ amb $\leq$ una cadena, $a$ un element de $\mathcal{C}$ i $B$ un subconjunt de $\mathcal{C}$ tal que per a tot $b \in B$ es compleix $b \leq A$. Aleshores direm que $a$ és una cota superior de $B$.

Si $a \leq b$ implica $b = a$ per a tot $b \in B$ direm que $a$ és maximal per $B$.

**Axioma 10.3.16** (Lemma de Zorn)**.** *Sigui $\mathcal{A}$ amb $\leq$ una cadena tal que per a tot subconjunt $\mathcal{C} \subseteq \mathcal{A}$ la cadena $\mathcal{C}$ té alguna cota superior. Aleshores $\mathcal{A}$ té algun element maximal.*

**Teorema 10.3.17.** *Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$ commutatiu amb $1 \neq 0$. Aleshores existeix $M \subseteq R$ tal que $M$ sigui un ideal maximal de $R$.*

*Demostració.* Definim el conjunt

$$A = \{I \lhd R \mid I \neq R\}.$$

i amb un subconjunt $\mathcal{C} \subseteq A$ considerem, per la proposició 10.3.14, la cadena $(\mathcal{C}, \subseteq)$. Considerem ara el conjunt

$$J = \bigcup_{I \in \mathcal{C}} I$$

i veiem que $J$ és un ideal de $R$, ja que si $x, y \in J$ tenim $x \in J_1$ i $y \in J_2$ per a certs $J_1, J_2 \in \mathcal{C}$. Ara bé, si $J_2 \subseteq J_1$ tenim que $x - y \in J_1$, i per tant $x - y \in J$, i si $J_1 \subseteq J_2$ tenim que $x - y \in J_2$, i per tant $x - y \in J$. Si prenem $x \in J$ i $r \in R$ aleshores $r \cdot x \in J$, ja que tenim $x \in J_1$ per a cert $J_1 \in \mathcal{C}$, i per tant $r \cdot x \in J_1$, i en particular $r \cdot x \in J$. Per tant per la definició d'ideal d'un anell (10.1.10) tenim que $J$ és un ideal de $R$. Per veure que $J \in A$ hem de comprovar que $J \neq R$. Ho fem per contradicció. Suposem que $J = R$. Aleshores $1 \in J$, i per tant $1 \in I$ per a cert $I \in A$, però això no pot ser ja que si $I \in A$ s'ha de complir $I \neq A$, i per tant $1 \notin I$. Per tant $J \neq R$ i tenim que $J \in A$.

Ara bé, pel Lemma de Zorn (10.3.16) tenim que existeix $M \in \mathcal{C}$ tal que per a tot $I \in \mathcal{C}$ tenim $I \subseteq M$ i per la definició d'ideal maximal (10.3.7) tenim que $M$ és un ideal maximal de $(R, +, \cdot)$. □

### 10.3.3 Divisibilitat

**Definició 10.3.18** (Divisors i múltiples)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $a, b \in D$ tals que existeix $c \in D$ tal que $b = a \cdot c$. Aleshores direm que $a$ divideix $b$ o que $b$ és múltiple de $a$. Ho denotarem amb $a \mid b$.

**Observació 10.3.19.** $b \mid a \iff (a) \subseteq (b)$.

**Proposició 10.3.20.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $a, b, c, c'$ quatre elements, amb $a \neq 0$, $b \neq 0$, tals que $a \mid b$ i $b \mid a$, i $a = c \cdot b$ i $b = c' \cdot a$. Aleshores $c' = c^{-1}$.*

*Demostració.* Tenim que $b = c' \cdot c \cdot b$, i per la proposició 10.3.3 tenim que $1 = c' \cdot c$, i per la definició d'element invertible (10.1.7) tenim que $c' = c^{-1}$. □

**Proposició 10.3.21.** *Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$ commutatiu amb $1 \neq 0$ i $\sim$ una relació binària tal que per a tot $x, y \in R$ tenim*

$$x \sim y \Longrightarrow x = u \cdot y \text{ per a algun } u \in R \text{ invertible.}$$

*Aleshores $\sim$ és una relació d'equivalència.*

*Demostració.* Comprovem les condicions de la definició de relació d'equivalència (2.3.2):

1. Simètrica: Per a tot $x \in R$ tenim $x = 1 \cdot x$.

2. Reflexiva: Siguin $x, y \in R$ tals que $x \sim y$. Aleshores tenim que existeix $u \in R$ invertible tal que $x = u \cdot y$. Ara bé, com que $u$ és invertible tenim per la definició de element invertible (10.1.7) que $y = u^{-1} \cdot x$, i per tant $y \sim x$.

3. Transitiva: Siguin $x, y, z \in R$ tals que $x \sim y$ i $y \sim z$. Aleshores tenim que $x = u \cdot y$ i $y = u' \cdot z$ per a certs $u, u' \in R$ invertibles, i per tant $x = u \cdot u' \cdot z$, i com que $1 = u \cdot u' \cdot u'^{-1} \cdot u^{-1}$ per la definició de element invertible (10.1.7) tenim que $x \sim z$.

i per la definició de relació d'equivalència (2.3.2) tenim que $\sim$ és una relació d'equivalència. □

**Definició 10.3.22** (Elements associats)**.** Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ i $a, b \in R$ dos elements tals que existeix un element invertible $u \in R$ tal que $a = u \cdot b$. Aleshores direm que $a$ i $b$ són associats i escriurem $a \sim b$.

Aquesta definició té sentit per la proposició 10.3.21.

**Proposició 10.3.23.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$, $a, b$ dos elements de $D$ i $X \subseteq D$ un conjunt tal que per a tot $d \in X$ tenim $d \mid a$, $d \mid b$ i per a tot $c \in D$ tal que $c \mid a$, $c \mid b$ es compleix $c \mid d$. Aleshores tenim que per a tot $d' \in X$ si i només si $d \sim d'$.*

*Demostració.* Comencem amb la implicació cap a la dreta ($\Rightarrow$). Suposem que $d' \in X$. Hem de veure que $d \sim d'$. Tenim $d \mid d'$ i $d' \mid d$ i per la definició de divisor (10.3.18) trobem que $d \sim d'$.

Fem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem que $d' \sim d$. Hem de veure que $d' \in X$. Per hipòtesi tenim que $d \mid a$ i $d \mid b$. Per tant existeixen $\alpha, \beta \in D$ tals que $a = \alpha d$ i $b = \beta d$, i per la proposició 10.3.20 tenim que si $d' = d \cdot u$ amb $u \in D$ invertible aleshores $d = d' \cdot u^{-1}$. Per tant

$$a = \alpha \cdot d' \cdot u^{-1} \quad \text{i} \quad b = \beta \cdot d' \cdot u^{-1}$$

i per tant $d' \mid a$ i $d' \mid b$. Ara bé, com que per hipòtesi $d \sim d'$, per la definició d'elements associats (10.3.22) tenim que $d' \in X$. □

**Definició 10.3.24** (Màxim comú divisor)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $a, b, d \in D$ tres elements tals que $d \mid a$ i $d \mid b$ i tals que per a tot $c \in D$ que satisfaci $c \mid a$ i $c \mid b$ tenim $c \mid d$. Aleshores direm que $d$ és el màxim comú divisor de $a$ i $b$. Direm que $d$ és un màxim comú divisor de $a$ i $b$ o que $d \sim \mathrm{mcd}(a, b)$. Entendrem que $\mathrm{mcd}(a, b)$ és un element de $D$.

Aquesta definició té sentit per la proposició 10.3.23.

**Proposició 10.3.25.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$, $a, b$ dos elements de $D$ i $X \subseteq D$ un conjunt tal que per a tot $m \in X$ tenim $a \mid m$, $b \mid m$ i per a tot $c \in D$ tal que $a \mid c$, $b \mid c$ es compleix $m \mid c$. Aleshores tenim que per a tot $m' \in X$ si i només si $m \sim m'$.*

*Demostració.* Comencem amb la implicació cap a la dreta ($\Rightarrow$). Suposem que $m' \in X$. Hem de veure que $m \sim m'$. Tenim $m' \mid m$ i $m \mid m'$ i per la definició de múltiple (10.3.18) trobem que $m \sim m'$.

Fem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem que $m' \sim m$. Hem de veure que $m' \in X$. Per hipòtesi tenim que $a \mid m$ i $b \mid m$. Per tant existeixen $\alpha, \beta \in D$ tals que $m = \alpha \cdot a$ i $m = \beta \cdot b$, i per la proposició 10.3.20 tenim que si $m' = u \cdot m$ amb $u \in D$ invertible aleshores $m = m' \cdot u^{-1}$. Per tant

$$m' = \alpha \cdot a \cdot u^{-1} \quad \text{i} \quad m' = \beta \cdot b \cdot {u'}^{-1}$$

i per tant $m' \mid a$ i $m' \mid b$. Ara bé, com que per hipòtesi $m \sim m'$, per la definició d'elements associats (10.3.22) tenim que $m' \in X$. □

**Definició 10.3.26** (Mínim comú múltiple)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $a, b, m \in D$ tres elements tals que $a \mid m$ i $b \mid m$ i tals que per a tot $c \in D$ que satisfaci $a \mid c$ i $b \mid c$ tenim $m \mid c$. Aleshores direm que $m$ és el mínim comú múltiple de $a$ i $b$. Direm que $m$ és un mínim comú múltiple de $a$ i $b$ o que $m \sim \mathrm{mcm}(a, b)$. Entendrem que $\mathrm{mcm}(a, b)$ és un element de $D$.

Aquesta definició té sentit per la proposició 10.3.25.

**Proposició 10.3.27.** *Siguin $(a), (b)$ dos ideals principals d'un domini d'integritat $(D, +, \cdot)$. Aleshores tenim les igualtats*

1. $(a) + (b) = (\mathrm{mcd}(a, b))$.
2. $(a) \cap (b) = (\mathrm{mcm}(a, b))$.
3. $(a)(b) = (a \cdot b)$.

*Demostració.* Comencem veient el punt (1). Per la proposició 10.1.15 tenim que $(a) + (b) = \{x + y \mid x \in (a), y \in (b)\}$, i per la definició d'ideal principal (10.1.16) això és

$$(a) + (b) = \{r_1 \cdot a + r_2 \cdot b \mid r_1, r_2 \in R\},$$

que podem reescriure com

$$(a) + (b) = \{x \mid \text{existeixen } m, n \in R \text{ tals que } x = n \cdot m + b \cdot n\}$$

i per tant $(a) + (b) = (\mathrm{mcd}(a, b))$ és un ideal principal de $R$.

Continuem veient el punt (2). Per la proposició 10.1.15 tenim que

$$(a) \cap (b) = \{x \mid x \in (a), x \in (b)\},$$

que, per la definició d'ideal principal (10.1.16), podem reescriure com

$$(a) \cap (b) = \{x \mid x \text{ divideix } a \text{ i } b\}$$

i per tant $(a) \cap (b) = (\text{mcm}(a, b))$ és un ideal principal de $R$.

Acabem veient el punt (3). Per la proposició 10.1.15 tenim que

$$(a)(b) = \{x_1 \cdot y_1 + \cdots + x_n \cdot y_n \mid x_1, \ldots, x_n \in (a), y_1, \ldots, y_n \in (b)\},$$

que, per la definició d'ideal principal (10.1.16) i la proposició 10.1.5, podem reescriure com

$$\begin{aligned}(a)(b) &= \{(r_1 \cdot a)(r_1' \cdot b) + \cdots + (r_n \cdot a)(r_n' \cdot b) \mid r_1, \ldots, r_n, r_1', \ldots, r_n' \in R\} \\ &= \{(r_1 \cdot r_1' + \cdots + r_n \cdot r_n') \cdot (a \cdot b) \mid r_1, \ldots, r_n, r_1', \ldots, r_n' \in R\},\end{aligned}$$

i si fixem $r_2 = \ldots r_n = 0$ i $r_1' = 1$ tenim, amb $r_1 = r$ que

$$(a)(b) = \{r \cdot (a \cdot b) \mid r \in R\},$$

i per la definició d'ideal principal (10.1.16) tenim que $(a)(b)$ és un ideal principal de $R$ amb

$$(a)(b) = (a \cdot b). \qquad \square$$

**Definició 10.3.28** (Primer)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$, $p \neq 0$ un element de $D$ tal que per a tot $a, b$ dos elements de $D$ que satisfacin $p \mid a \cdot b$ tenim $p \mid a$ ó $p \mid b$. Aleshores direm que $p$ és primer.

**Observació 10.3.29.** *$a \neq 0$, $(a)$ és un ideal primer si i només si $a$ és primer.*

**Definició 10.3.30** (Element irreductible)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$, $a \neq 0$ un element no invertible de $D$ i $b, c$ dos elements de $D$ tals que $a = b \cdot c$. Aleshores direm que $a$ és irreductible si $b$ ó $c$ són invertibles.

**Proposició 10.3.31.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $p$ un element primer de $D$. Aleshores $p$ és irreductible.*

*Demostració.* Suposem que $a, b$ són dos elements de $D$ tals que $p = a \cdot b$. Per la definició de primer (10.3.28) tenim que ha de ser $p \mid a$ ó $p \mid b$. Si $p \mid a$ tenim que $a = \alpha \cdot p$ per a cert $\alpha \in D$. Ara bé, per hipòtesi, tenim que $p = a \cdot b$. Per tant $a = \alpha \cdot a \cdot b$, i per la proposició 10.3.3 tenim que $1 = \alpha \cdot b$, i per la definició d'element invertible (10.1.7) tenim que $b$ és invertible i per la definició d'irreductible (10.3.30) tenim que $p$ és irreductible.

El cas $p \mid b$ és anàleg. $\square$

### 10.3.4 Dominis de factorització única

**Definició 10.3.32** (Domini de factorització única)**.** Sigui $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ tal que per a tot element no invertible $a \neq 0$ de $D$

1. Existeixen $p_1, \ldots, p_n$ elements irreductibles de $D$ tals que
$$a = p_1 \cdot \ldots \cdot p_n.$$
2. Si existeixen $p_1, \ldots, p_r$ i $q_1, \ldots, q_s$ elements irreductibles de $D$ tals que
$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$
aleshores $r = s$ i existeix $\sigma \in S_r$ tal que
$$p_1 \cdot \ldots \cdot p_r = q_{\sigma(1)} \cdot \ldots \cdot q_{\sigma(r)},$$
amb $p_i \sim q_{\sigma(i)}$ per a tot $i \in \{1, \ldots, r\}$.

Aleshores direm que $D$ és un domini de factorització única.

**Teorema 10.3.33.** *Sigui $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores $D$ és un domini de factorització única si i només si tenim*

1. *Per a tot $a \neq 0$ element no invertible de $D$ existeixen $p_1, \ldots, p_r$ elements irreductibles de $D$ tals que*
$$a = p_1 \cdot \ldots \cdot p_r$$
2. *Si $a$ és in element irreductible de $D$ aleshores $a$ és primer.*

*Demostració.* Comencem demostrant que la condició és suficient ($\Rightarrow$). Suposem doncs que $D$ és un domini de factorització única. El punt (1) és conseqüència de la definició de domini de factorització única (10.3.32). Per tant només ens queda veure que tot element irreductible és primer. Siguin $p$ un element irreductible de $D$ i $a, b$ dos elements no invertibles no nuls de $D$ tals que $p \mid a \cdot b$. Per la definició de domini de factorització única (10.3.32) tenim que existeixen $p_1, \ldots, p_r, q_1, \ldots, q_s$ elements irreductibles de $D$ tals que

$$a = p_1 \cdot \ldots \cdot p_r \quad \text{i} \quad b = q_1 \cdot \ldots \cdot q_s$$

i per tant

$$a \cdot b = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$$

i com que, per hipòtesi, $p \mid a \cdot b$ i la definició de domini de factorització única (10.3.32) tenim que

$$a \cdot b = p \cdot \alpha_1 \cdot \ldots \cdot \alpha_t$$

per a certs $\alpha_1, \cdots, \alpha_t$ elements irreductibles de $D$. Per tant tenim

$$a \cdot b = p \cdot \alpha_1 \cdot \ldots \cdot \alpha_t = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$$

i, de nou, per la definició de domini de factorització única (10.3.32) tenim que $p \sim p_i$ ó $p \sim q_j$ per a certs $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$, i per tant $p \mid a$ ó $p \mid b$, i per la definició de primer (10.3.28) tenim que $p$ és primer.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem doncs que

1. Per a tot $a$ element no invertible de $D$ existeixen $p_1, \ldots, p_r$ elements irreductibles de $D$ tals que
$$a = p_1 \cdot \ldots \cdot p_r$$
2. Si $a$ és in element irreductible de $D$ aleshores $a$ és primer.

Sigui $a$ un element no invertible de $D$. Pel punt (1) tenim que existeixen $p_1, \ldots, p_r$ elements irreductibles de $D$ tals que
$$a = p_1 \cdot \ldots \cdot p_r.$$
Suposem que existeixen també $q_1, \ldots, q_s$ elements irreductibles de $D$ tals que
$$a = q_1, \ldots, q_s.$$
Aleshores volem veure que $r = s$ i que existeix $\sigma \in S_r$ tal que
$$p_1 \cdot \ldots \cdot p_r = q_{\sigma(1)} \cdot \ldots \cdot q_{\sigma(r)},$$
amb $p_i \sim q_{\sigma(i)}$ per a tot $i \in \{1, \ldots, r\}$.

Tenim que $p_1 \mid a$, i com que pel punt (2) tenim que $p_1$ és primer, per la definició de primer (10.3.28) tenim que $p_1 \mid q_j$ per a cert $j \in \{1, \ldots, s\}$, i per la definició de irreductible (10.3.30) i la definició d'elements associats (10.3.22) tenim que $p_1 \sim q_j$. Sigui doncs $\sigma \in S_s$ tal que $p_1 \mid q_{\sigma(1)}$. Aleshores tenim
$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = u_1 \cdot q_{\sigma(1)} \cdot \ldots \cdot q_s$$
per a cert $u_1$ element invertible de $D$. Podem iterar aquest argument per a $p_2, \ldots, p_t$, on $t = \min(r, s)$ per obtenir
$$p_1 \cdot \ldots \cdot p_t \cdot p_{t+1} \cdot \ldots \cdot p_r = (u_1 \cdot q_1) \cdot \ldots \cdot (u_t \cdot q_t) \cdot p_{t+1} \cdot \ldots \cdot p_s$$
per a certs $u_1, \ldots, u_t$ elements invertibles de $D$. Ara bé, tenim que $r = s$, ja que si $r > s$ tindríem que $p_{s+1}, \ldots, p_r$ són invertibles, i si $s > r$ tindríem que $q_{r+1}, \ldots, q_s$ són invertibles, però per la definició d'irreductible (10.3.30) i la definició de element invertible (10.1.7) tenim que això no pot ser, i per tant $r = s$ i per la definició de domini de factorització única (10.3.32) tenim que $D$ és un domini de factorització única, com volíem veure. □

**Proposició 10.3.34.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $a, b$ dos elements no invertibles i no nuls de $D$ tals que existeixen $p_1, \ldots, p_r$ tals que*
$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \quad i \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$$
*per a certs $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \in \mathbb{N}$. Aleshores*
$$\prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \sim \operatorname{mcd}(a, b) \quad i \quad \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)} \sim \operatorname{mcm}(a, b).$$

*Demostració.* Denotem $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$ i $m = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$.

Prenem $c$ un element de $D$ tal que $c \mid a$ i $c \mid b$. Aleshores tenim que

$$c = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$$

per a certs $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$. Ara bé, com que $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$, i per tant $d \mid c$, i per la definició de màxim comú divisor (10.3.24) tenim que $d \sim \mathrm{mcd}(a, b)$.

Prenem ara $c$ un element de $D$ tal que $a \mid c$ i $b \mid c$. Aleshores tenim que

$$c = q \cdot p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$$

per a cert $q$ element de $D$ i certs $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$. Ara bé, com que $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$, i per tant $m \mid c$, i per la definició de mínim comú múltiple (10.3.26) tenim que $m \sim \mathrm{mcm}(a, b)$. □

### 10.3.5 Anells Noetherians

**Definició 10.3.35** (Anell Noetherià)**.** Sigui $N$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$ tal que si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

són ideals de $N$ existeix $n_0$ tal que per a tot $i \geq n_0$ tenim $I_i = I_{i+1}$. Aleshores diem que $N$ és Noetherià.

**Observació 10.3.36.** *$(\{I_1, I_2, I_3 \ldots\}, \subseteq)$ és una cadena.*

**Lemma 10.3.37.** *Siguin $N$ un domini d'integritat Noetherià amb la suma $+$ i el producte $\cdot$ i $a \neq 0$ un element no invertible de $N$. Aleshores existeixen $p_1, \ldots, p_n$ elements irreductibles de $N$ tals que*

$$a = p_1 \cdot \ldots \cdot p_n.$$

*Demostració.* Ho farem per reducció a l'absurd. Definim el conjunt

$$X = \{a \in N \text{ invertible} \mid a \neq p_1 \cdot \ldots \cdot p_n \text{ per a } p_1, \ldots, p_n \in N \text{ irreductibles}\}.$$

Volem veure que $X = \emptyset$. Suposem doncs que $X \neq \emptyset$ i prenem $a_1 \in X$. Per la definició d'irreductible (10.3.30) tenim que $a_1$ no és irreductible, i per tant existeixen $b_1, c_1 \in N$ no invertibles tals que

$$a_1 = b_1 \cdot c_1$$

i ha de ser $b_1 \in X$ o $c_1 \in X$.

Suposem que $b_1 \in X$, la demostració de l'altre opció és anàloga. Aleshores tenim, per l'observació 10.3.19, que $(a) \subset (b)$. Ara bé, també tindríem que $b_1 = b_2 \cdot c_2$ per a certs $b_2, c_2$ elements no invertibles de $N$ amb $b_2 \in X$ o $c_2 \in X$, i podem iterar aquest argument per construir

$$(a_1) \subset (b_1) \subset (b_2) \subset (b_3) \subset \ldots$$

però això entra en contradicció amb la definició de anell Noetherià (10.3.35), i per tant $X = \emptyset$, com volíem veure. □

### 10.3.6 Dominis d'ideals principals

**Definició 10.3.38** (Domini d'ideals principals)**.** Sigui $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ tal que tot ideal de $D$ és un ideal principal. Aleshores direm que $D$ és un domini d'ideals principals.

**Proposició 10.3.39.** *Sigui $D$ un domini d'ideals principals amb la suma $+$ i el producte $\cdot$. Aleshores un element $a \in D$ és irreductible si i només si $(a)$ és un ideal maximal.*

*Demostració.* Comencem veient que la condició és suficient ($\Leftarrow$). Suposem doncs que $a$ és un element irreductible de $D$ i prenem $b \in D$ tal que $(a) \subseteq (b) \neq D$. Aleshores, per l'observació 10.3.19 tenim que $b \mid a$, és a dir, existeix $r \in D$ tal que $a = b \cdot r$, i per la definició d'irreductible (10.3.30) tenim que $r$ ó $b$ són invertibles. Ara bé, com que, per hipòtesi, $(b) \neq D$ tenim que $b$ no és invertible, per tant ha de ser $r$ invertible per la definició d'element invertible (10.1.7) tenim que $a \cdot r^{-1} = b$, per l'observació 10.3.19 tenim que $(a) = (b)$, i per la definició d'ideal maximal (10.3.7) tenim que $(a)$ és un ideal maximal.

Tenim que la condició és necessària ($\Rightarrow$) per la proposició 10.3.11. □

**Proposició 10.3.40.** *Siguin $D$ un domini d'ideals principals amb la suma $+$ i el producte $\cdot$ i $a$ un element irreductible de $D$. Aleshores $a$ és primer.*

*Demostració.* Per la proposició 10.3.39 tenim que $(a)$ és maximal, pel corol·lari 10.3.9 veiem que $(a)$ és primer, i per l'observació 10.3.29 trobem que $a$ és primer, com volíem veure. □

**Teorema 10.3.41.** *Sigui $D$ un domini d'ideals principals amb la suma $+$ i el producte $\cdot$. Aleshores $D$ és Noetherià.*

*Demostració.* Siguin $I_1, \ldots, I_i, \ldots$ ideals de $D$ tals que

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

i

$$\mathcal{I} = \bigcup_{i=1}^{\infty} I_i.$$

Aleshores tenim que $\mathcal{I}$ és un ideal. També veiem que si $x \in \mathcal{I}$ existeix $n$ tal que $x \in I_n$, i per la definició d'ideal d'un anell (10.1.10) tenim que si $y \in D$ aleshores $x \cdot y \in I_n$.

Ara bé, com que per hipòtesi $D$ és un domini d'ideals principals tenim, per la definició de domini d'ideals principals (10.3.38) que existeix $a \in D$ tal que $\mathcal{I} = (a)$, i per tant existeix $n$ tal que $a \in I_n$, i trobem que

$$\mathcal{I} = (a) \subseteq I_n \subseteq I_{n+k} \subseteq \mathcal{I}$$

per a tot $k \in \mathbb{N}$, i per tant $I_n = I_{n+k}$ per a tot $k \in \mathbb{N}$, i per la definició de anell Noetherià (10.3.35) trobem que $D$ és un anell Noetherià. □

**Teorema 10.3.42.** *Sigui $D$ un domini d'ideals principals amb la suma $+$ i el producte $\cdot$. Aleshores $D$ és un domini de factorització única.*

*Demostració.* Pel Teorema 10.3.41 tenim que $D$ és un anell Noetherià, i pel lemma 10.3.37 tenim que per a tot element no irreductible $a$ de $D$ existeixen $p_1, \ldots, p_n$ elements irreductibles de $N$ tals que

$$a = p_1 \cdot \ldots \cdot p_n.$$

També tenim, per la proposició 10.3.40 que si $a$ és un element irreductible de $D$ aleshores $a$ és primer.

Per acabar, pel Teorema 10.3.33 tenim que $D$ és un domini de factorització única. □

### 10.3.7 Dominis Euclidians

**Definició 10.3.43** (Domini Euclidià)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $U \mid D \setminus \{0\} \longrightarrow \mathbb{N}$ una aplicació tal que

1. $U(x) \leq U(x \cdot y)$ per a tot $x, y \in D \setminus \{0\}$.
2. Per a tot $x, y \in D$, $y \neq 0$ existeixen $Q, r \in D$ tals que $x = Q \cdot y + r$, amb $r = 0$ ó $U(r) < U(y)$.

Aleshores direm que $D$ és un domini Euclidià amb la norma $U$.

**Proposició 10.3.44.** *Sigui $D$ un domini Euclidià amb la suma $+$ i el producte $\cdot$ amb la norma $U$. Aleshores*

$$U(1) \leq U(x) \quad \textit{per a tot } x \in D \setminus \{0\}.$$

*Demostració.* Per la definició de domini Euclidià (10.3.43) tenim que $U(x) \leq U(x \cdot y)$ per a tot $x, y \in D \setminus \{0\}$. Per tant

$$U(1) \leq U(1 \cdot x) = U(x) \quad \text{per a tot } x \in D \setminus \{0\}.$$ □

**Proposició 10.3.45.** *Sigui $D$ un domini Euclidià amb la suma $+$ i el producte $\cdot$ amb la norma $U$. Aleshores*

$$U(u) = U(1) \Longleftrightarrow u \textit{ és un element invertible de } D.$$

*Demostració.* Comencem veient l'implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $u$ és un element invertible de $D$.

Per la proposició 10.3.44 tenim que $U(1) \leq U(u)$ i que $U(u) \leq U(u \cdot u^{-1})$. Ara bé, per la definició de l'invers d'un element invertible (10.1.8) tenim que $u \cdot u^{-1} = 1$, i per tant

$$U(1) \leq U(u) \leq U(u \cdot u^{-1}) = U(1),$$

i trobem $U(u) = U(1)$.

Veiem ara l'implicació cap a l'esquerra ($\Leftarrow$). Suposem que $U(u) = U(1)$.

Per la definició de domini Euclidià (10.3.43) tenim que existeixen $Q, r$ elements de $D$ tals que

$$1 = Q \cdot u + r$$

amb $r = 0$ ó $U(r) < U(u)$. Ara bé, per hipòtesi $U(u) = U(1)$, i per la proposició 10.3.44 trobem que ha de ser $r = 0$. Per tant tenim

$$1 = Q \cdot u$$

i per la definició d'element invertible (10.1.7) trobem que $u$ és invertible. □

**Teorema 10.3.46.** *Sigui $D$ un domini Euclidià amb la suma $+$ i el producte $\cdot$. Aleshores $(D, +, \cdot)$ és un domini d'ideals principals.*

*Demostració.* Siguin $U$ una norma de $D$ i $I$ un ideal de $D$. Si $I = \{0\}$ aleshores $I = (0)$. Suposem doncs que $I \neq (0)$ i prenem $b \in I$ tal que $U(b) \leq U(x)$ per a tot $x \in I$, $x \neq 0$.

Prenem ara $a \in I$. Per la definició de domini Euclidià (10.3.43) tenim que existeixen $Q, r \in D$ tals que

$$a = Q \cdot b + r$$

amb $r = 0$ ó $U(r) < U(b)$. I com que, per la definició de anell (10.1.1) tenim que $(D, +)$ és un grup tenim

$$r = a - Q \cdot b,$$

i per la proposició 10.1.13 tenim que

$$r = a - Q \cdot b \in I$$

i per tant, $r \in I$ amb $r = 0$ ó $U(r) < U(b)$. Ara bé, per hipòtesi tenim que $U(r) \geq U(b)$, per tant ha de ser $r = 0$ i tenim que

$$a = Q \cdot b,$$

d'on trobem que $I$ és un ideal principal, i per la definició de domini d'ideals principals (10.3.38) tenim que $D$ és un domini d'ideals principals. □

**Teorema 10.3.47.** *Sigui $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$. Aleshores $\mathbb{K}$ és un domini Euclidià.*

*Demostració.* □

## 10.4 Anells de polinomis

### 10.4.1 Cos de fraccions d'un domini d'integritat

**Proposició 10.4.1.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $\sim$ definida a $D \times D \setminus \{0\}$ una relació binària tal que per a tot $a, c \in D$, $b, d \in D \setminus \{0\}$*

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

*Aleshores $\sim$ és una relació d'equivalència.*

*Demostració.* □

**Notació 10.4.2.** Denotarem el conjunt quocient $D \times D \setminus \{0\}/\sim$ com $\mathbb{Q}(D)$ i la classe d'equivalència $\overline{(a, b)} \in \mathbb{Q}(D)$ com $\frac{a}{b}$.

**Lemma 10.4.3.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores $\mathbb{Q}(D)$ és un anell commutatiu amb $1 \neq 0$ amb les operacions*

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d} \quad i \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}. \quad \text{per a tot } a, c \in D,\ b, d \in D \setminus \{0\}.$$

*Demostració.* □

**Teorema 10.4.4.** *Sigui $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores $\mathbb{Q}(D)$ és un cos amb la suma $+$ i el producte $\cdot$.*

*Demostració.* □

**Teorema 10.4.5** (Unicitat de $\mathbb{Q}(D)$)**.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $\mathbb{Q}_1(D)$ i $\mathbb{Q}_2(D)$ dos cossos amb la suma $+$ i el producte $\cdot$. Aleshores*

$$\mathbb{Q}_1(D) \cong \mathbb{Q}_2(D)$$

*Demostració.* □

**Definició 10.4.6** (Cos de fraccions)**.** Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores direm que $\mathbb{Q}(D)$ és el cos de fraccions de $D$.

### 10.4.2 El Teorema de Gauss

**Proposició 10.4.7.** *Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i*

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R\}$$

*un conjunt. Aleshores $R[x]$ és un anell amb la suma $+$ i el producte $\cdot$.*

*Demostració.* □

**Observació 10.4.8.** $1_R = 1_{R[x]}$, $0_R = 0_{R[x]}$.

**Observació 10.4.9.** *Si $R$ és un anell commutatiu aleshores $R[x]$ també és un anell commutatiu.*

**Definició 10.4.10** (Anell de polinomis)**.** Siguin $R$ un anell amb la suma $+$ i el producte $\cdot$ i

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R\}.$$

Aleshores direm que l'anell $R[x]$ és l'anell de polinomis de $R$.

Aquesta definició té sentit per la proposició 10.4.7.

**Observació 10.4.11.** $D \subseteq D[x]$.

**Teorema 10.4.12** (Teorema de la base de Hilbert)**.** *Sigui $R$ un anell amb la suma $+$ i el producte $\cdot$ Noetherià. Aleshores l'anell de fraccions de $R$, $R[x]$ és un anell Noetherià.*

*Demostració.* □

**Definició 10.4.13** (Contingut d'un polinomi)**.** Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $f(x) = \sum_{i=0}^{n} a_ix^i$ un element de $D[x]$. Aleshores definim

$$\text{cont}(f) \sim \text{mcd}(a_0, \ldots, a_n)$$

com el contingut de $f$.

Interpretarem $\text{cont}(f(x))$ com un element de $D$.

**Definició 10.4.14** (Polinomi primitiu)**.** Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $f(x)$ un element de $D[x]$ tal que

$$\text{cont}(f(x)) \sim 1.$$

Aleshores direm que $f(x)$ és un polinomi primitiu.

**Lemma 10.4.15** (Lemma de Gauss)**.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $f(x), g(x)$ dos polinomis primitius de $D[x]$. Aleshores $f(x) \cdot g(x)$ és un polinomi primitiu.*

*Demostració.* □

**Corol·lari 10.4.16.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $f(x)$, $g(x)$ dos elements de $D[x]$. Aleshores*

$$\text{cont}(f(x) \cdot g(x)) \sim \text{cont}(f(x)) \cdot \text{cont}(g(x)).$$

*Demostració.* □

**Lemma 10.4.17.** *Siguin $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $p$ un element irreductible de $D$. Aleshores tenim que $p$ és un element irreductible de $D[x]$.*

*Demostració.* □

**Teorema 10.4.18.** *Sigui $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $D[x]$. Aleshores* $\text{grau}(f(x)) \geq 1$ *i $f(x)$ és un polinomi irreductible de $D[x]$ si i només si* $\text{cont}(f(x)) \sim 1$ *i $f(x)$ és irreductible en $\mathbb{Q}(D)[x]$.*

*Demostració.* □

**Teorema 10.4.19** (Teorema de Gauss)**.** *Sigui $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$. Aleshores $D[x]$ és un domini de factorització única.*

*Demostració.* □

**Teorema 10.4.20.** *Sigui $D$ un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores són equivalents*

1. *$D$ és un domini de factorització única.*
2. *$D[x]$ és un domini de factorització única.*
3. *$D[x_1, \ldots, x_n]$ és un domini de factorització única.*

*Demostració.* □

### 10.4.3 Criteris d'irreductibilitat

**Definició 10.4.21** (Arrel)**.** Siguin $R$ un anell commutatiu amb la suma $+$ i el producte $\cdot$ amb $1 \neq 0$, $f(x)$ un element de $R[x]$ i $\alpha$ un element de $R$ tal que $f(\alpha) = 0$. Aleshores direm que $\alpha$ és una arrel de $f(x)$.

**Proposició 10.4.22.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un element de $\mathbb{K}[x]$. Aleshores*

1. *Si $\text{grau}(f(x)) = 1$ aleshores $f(x)$ és irreductible.*
2. *Si $\text{grau}(f(x)) = 2$ ó $3$ aleshores $f(x)$ és irreductible si i només si $f(x)$ no té cap arrel.*

*Demostració.* □

**Proposició 10.4.23.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi de $D[x]$ i $\frac{a}{b} \in \mathbb{Q}(D)$ una arrel de $f(x)$ amb $\text{mcd}(a, b) \sim 1$. Aleshores tenim que $a \mid a_0$ ó $b \mid a_n$.*

*Demostració.* □

**Teorema 10.4.24** (Criteri modular)**.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi primitiu de $D[x]$ i $p$ un element irreductible de $D$ amb $p \nmid a_n$ tals que*

$$\overline{f(x)} = \overline{a_0} + \overline{a_1} \cdot \overline{x} + \cdots + \overline{a_n} \cdot \overline{x}^n$$

*sigui un polinomi irreductible de $D/(p)[x]$. Aleshores $f(x)$ és un polinomi irreductible de $D[x]$.*

*Demostració.* □

**Teorema 10.4.25** (Criteri d'Eisenstein)**.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi primitiu de $D[x]$ amb $n \geq 1$ i $p$ un element irreductible de $D$ tal que $p \mid a_0, \ldots, p \mid a_{n-1}$ i $p \nmid a_n, p^2 \nmid a_0$. Aleshores $f(x)$ és un polinomi irreductible de $D[x]$.*

*Demostració.* □

**Corol·lari 10.4.26.** *Siguin $D$ un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi de $D[x]$ amb $n \geq 1$ i $p$ un element irreductible de $D$ tal que $p \mid a_0, \ldots, p \mid a_{n-1}$ i $p \nmid a_n, p^2 \nmid a_0$. Aleshores $f(x)$ és un polinomi irreductible de $\mathbb{Q}(D)[x]$.*

*Demostració.* □

# Capítol 11

# Teoria de cossos finits

## 11.1 Cossos finits

### 11.1.1 Propietats bàsiques dels cossos finits

**Proposició 11.1.1.** *Siguin $\mathbb{K}$ i $\mathbb{E}$ dos cossos amb la suma $+$ i el producte $\cdot$ tals que $\mathbb{K} \subseteq \mathbb{E}$. Aleshores $\mathbb{E}$ és un $\mathbb{K}$-espai vectorial.*

*Demostració.* □

**Definició 11.1.2** (Cos finit)**.** Sigui $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ tal que $|\mathbb{K}| \in \mathbb{N}$. Aleshores direm que $\mathbb{K}$ és un cos finit.

**Observació 11.1.3.** *Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$. Aleshores $\mathrm{ch}(\mathbb{K})$ és primer.*

**Teorema 11.1.4.** *Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$. Aleshores*

$$\mathrm{ch}(\mathbb{K}) = p \iff |\mathbb{K}| = p^n \text{ per a cert } n \in \mathbb{N}.$$

*Demostració.* □

**Corol·lari 11.1.5.** *Siguin $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$ i $\mathbb{F}$ un subcòs de $\mathbb{K}$ amb $|\mathbb{K}| = p^n$. Aleshores $|\mathbb{F}| = p^d$ amb $d \mid n$.*

*Demostració.* □

**Teorema 11.1.6** (Teorema de l'element primitiu)**.** *Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$. Aleshores $\mathbb{K} \setminus \{0\}$ és un grup cíclic amb el producte $\cdot$.*

*Demostració.* □

**Definició 11.1.7** (Element primitiu)**.** Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$ i $\beta$ un element de $\mathbb{K}$ tal que $\langle\{\beta\}\rangle = \mathbb{K} \setminus \{0\}$. Aleshores direm que $\beta$ és un element primitiu de $\mathbb{K}$.

Aquesta definició té sentit pel Teorema de l'element primitiu (11.1.6).

**Teorema 11.1.8.** *Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$ amb $|\mathbb{K}| = p$. Aleshores existeix un polinomi irreductible $f(x)$ en $\mathbb{Z}/(p)[x]$ tal que*

$$\mathbb{K} \cong \mathbb{Z}/(p)[x]/(f(x)).$$

*Demostració.* □

### 11.1.2 Arrels d'un polinomi

**Definició 11.1.9** (Descomposició d'un polinomi)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$, $\mathbb{L}$ un subcòs de $\mathbb{K}$ i $f(x)$ un polinomi de $\mathbb{K}$ tal que existeixen $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ satisfent $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$. Aleshores direm que $f(x)$ descompon en $\mathbb{K}$.

**Teorema 11.1.10** (Teorema de Kronecker)**.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $\mathbb{K}[x]$. Aleshores existeix un cos $\mathbb{L}$, amb $\mathbb{K} \subseteq \mathbb{L}$, tal que $f(x)$ descompon en $\mathbb{L}$.*

*Demostració.* □

**Definició 11.1.11** (Cos de descomposició)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$, $f(x)$ un polinomi de $\mathbb{K}$ i $\mathbb{L}$ el mínim cos on $f(x)$ descompon amb $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, amb $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$. Aleshores direm que $\mathbb{L}$ és el cos descomposició de $f(x)$. Denotarem $\mathbb{L} = \mathbb{K}(f(x))$.

Aquesta definició té sentit pel Teorema de Kronecker (11.1.10).

**Definició 11.1.12** (Derivada formal)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi de $\mathbb{K}$. Aleshores definim la derivada formal de $f(x)$ com

$$f'(x) = a_1 + 2 \cdot a_2 x + 3 \cdot a_3 \cdot x^2 + \cdots + n \cdot a_n \cdot x^{n-1}.$$

**Proposició 11.1.13.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$, $g(x)$ dos polinomis de $\mathbb{K}$. Aleshores es compleix*

1. $(a \cdot f(x))' = a \cdot f'(x)$ *per a tot* $a \in \mathbb{K}$.
2. $(f(x) + g(x))' = f'(x) + g'(x)$.
3. $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.
4. $(f(x)^n)' = n \cdot f(x)^{n-1}$.

*Demostració.* □

**Proposició 11.1.14.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $\mathrm{ch}(\mathbb{K}) = 0$ i $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi de $\mathbb{K}$ amb $n \geq 1$. Aleshores $n \cdot a_n \neq 0$ i $f'(x) \neq 0$.*

*Demostració.* □

**Proposició 11.1.15.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $\mathrm{ch}(\mathbb{K}) = p$ no nul i $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$ un polinomi de $\mathbb{K}$ amb $n \geq 1$. Aleshores*

$$f'(x) \neq 0 \iff p \mid i \text{ per a tot } i \geq 1 \text{ tal que } a_i \neq 0.$$

*Demostració.* □

**Definició 11.1.16** (Arrels múltiples)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $\mathbb{K}[x]$, $\alpha$ una arrel de $f(x)$ i $g(x)$ un polinomi de $\mathbb{K}(f(x))$ tal que

$$f(x) = (x - \alpha)^m \cdot g(x)$$

amb $m \geq 2$. Aleshores direm que $\alpha$ és una arrel múltiple de $f(x)$.

**Proposició 11.1.17.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $\mathbb{K}[x]$. Aleshores $\alpha$ és una arrel múltiple de $f(x)$ si i només si $\alpha$ és una arrel de $f'(x)$.*

*Demostració.* □

**Corol·lari 11.1.18.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $\mathbb{K}[x]$ amb* $\operatorname{grau}(f(x)) \geq 1$*. Aleshores* $\operatorname{mcd}(f(x), f'(x)) = 1$ *si i només si $f(x)$ no té arrels múltiples.*

*Demostració.* □

## 11.2 Caracterització dels cossos finits i els seus subcossos

### 11.2.1 Teoremes d'existència i unicitat dels cossos finits

**Teorema 11.2.1** (Teorema d'existència dels cossos finits)**.** *Siguin $p$ un primer i $n$ un natural. Aleshores existeix un cos $\mathbb{K}$ amb la suma $+$ i el producte $\cdot$ tal que $|\mathbb{K}| = p^n$.*

*Demostració.* □

**Corol·lari 11.2.2.** *Siguin $p$ un primer i $n$ un natural. Aleshores existeix un polinomi $f(x)$ de $\mathbb{Z}/(p)[x]$ amb* $\operatorname{grau}(f(x)) = n$*.*

*Demostració.* □

**Lemma 11.2.3.** *Siguin $n$, $d$ dos naturals tal que $d \mid n$, $p$ un primer i $f(x)$ un polinomi irreductible de $\mathbb{Z}/(p)[x]$. Aleshores $f(x) \mid (x^{p^n} - x)$.*

*Demostració.* □

**Teorema 11.2.4** (Teorema d'unicitat dels cossos finits)**.** *Siguin $\mathbb{K}$ un cos finit amb la suma $+_{\mathbb{K}}$ i el producte $*_{\mathbb{K}}$ i $\mathbb{F}$ un cos finit amb la suma $+_{\mathbb{F}}$ i el producte $*_{\mathbb{F}}$ amb $|\mathbb{K}| = |\mathbb{F}| = p^n$. Aleshores*

$$(\mathbb{K}, +_{\mathbb{K}}, *_{\mathbb{K}}) \cong (\mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}}).$$

*Demostració.* □

**Teorema 11.2.5** (Teorema d'existència dels subcossos finits)**.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $|\mathbb{K}| = p^n$ i $d$ un natural tal que $d \mid n$. Aleshores existeix un $\mathbb{L} \subseteq \mathbb{K}$ amb $|\mathbb{L}| = p^d$ tal que $\mathbb{L}$ és un subcòs de $\mathbb{K}$.*

*Demostració.* □

**Teorema 11.2.6** (Teorema d'unicitat dels subcossos finits)**.** *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $|\mathbb{K}| = p^n$, $d$ un natural tal que $d \mid n$ i $\mathbb{L}_1$, $\mathbb{L}_2$ dos subcossos de $\mathbb{K}$ amb $|\mathbb{L}_1| = |\mathbb{L}_2| = p^d$. Aleshores $\mathbb{L}_1 = \mathbb{L}_2$.*

*Demostració.* □

**Notació 11.2.7.** Denotarem el cos de $p^n$ elements com $\mathbb{F}_{p^n}$.

### 11.2.2 El morfisme de Frobenius

**Teorema 11.2.8.** *Siguin $n$ un natural, $p$ un primer i*

$$\mathcal{F} = \{f(x) \in \mathbb{Z}/(p)[x] \mid f(x) \text{ és un polinomi mónic irreductible de grau } d \mid n\}.$$

*Aleshores*

$$x^{p^n} - x = \prod_{f(x)\in\mathcal{F}} f(x).$$

*Demostració.* □

**Proposició 11.2.9** (Morfisme de Frobenius)**.** *Sigui $\mathbb{K}$ un cos finit amb la suma $+$ i el producte $\cdot$ amb $\mathrm{ch}(\mathbb{K}) = p$. Aleshores l'aplicació*

$$\begin{aligned} \Phi\colon \mathbb{K} &\longrightarrow \mathbb{K} \\ a &\longmapsto a^p \end{aligned}$$

*és un automorfisme.*

*Demostració.* □

**Teorema 11.2.10.** *Siguin $p$ un primer, $f(x)$ un polinomi irreductible de l'anell de polinomis $\mathbb{Z}/(p)[x]$ amb $\mathrm{grau}(f(x)) = n$ i $\alpha$ una arrel de $f(x)$ en $\mathbb{K}(p(x))$. Aleshores les arrels de $f(x)$ són $\alpha, \alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{pn-1}$ i $\alpha^{p^n} = \alpha$.*

*Demostració.* □

**Teorema 11.2.11.** *Siguin $p$ un primer, $f(x)$ un polinomi irreductible de l'anell de polinomis $\mathbb{Z}/(p)[x]$ amb $\mathrm{grau}(f(x)) = n$ i $\alpha$ una arrel de $f(x)$ en $\mathbb{K}(p(x))$. Aleshores les arrels de $f(x)$ són $\alpha, \alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{n-1}}$ i $\alpha^{p^i} \neq \alpha^{p^j}$ per a tot $i \neq j$, $i, j \in \{0, \ldots, n-1\}$.*

*Demostració.* □

# Bibliografia


[1] José Dorronsoro i Eugenio Hernández. *Números, grupos y anillos*. Castellà. Addison-Wesley, 1996. ISBN: 9788478290093.

[2] Ramon Antoine, Rosa Camps i Jaume Moncasi. *Introducció a l'àlgebra abstracta. Amb elements de matemàtica discreta*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 2007. ISBN: 978-84-490-2515-0.

[3] Ferran Cedó Giné i Vladimir Gisin. *Àlgebra bàsica*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 2007. ISBN: 978-84-490-2495-5.

[4] Paul Moritz Cohn. *Basic Algebra. Groups, Rings and Fields*. Anglès. Springer, 2003. ISBN: 978-0-85729-428-9.

[5] Félix Delgado De La Mata, Concepción Fuertes Fraile i Sebastian Xambó Descamps. *Introducción Al Álgebra. Anillos, Factorización Y Teoría De Cuerpos*. Castellà. Ediciones Universidad de Valladolid, 1998. ISBN: 978-8477628668.

[6] John B. Fraleigh. *A First Course in Abstract Algebra*. Anglès. Addison-wesley, 1982. ISBN: 978-0201020847.

[7] Thomas W. Hungerford. *Algebra*. Anglès. Addison-wesley, 1974. ISBN: 978-0201020847.


El capítol de teoria de grups està molt ben explicat en [1], i la teoria de cossos finits està complementada amb [2] sobre la teoria de classe.

La bibliografia del curs inclou els textos [2, 3, 4, 1, 5, 6, 7].

# Part VI

# Mètodes numèrics

# Capítol 12

# Interpolació numèrica

Sovint podem mesurar un procés físic com un número de punts (per exemple, la temperatura d'una habitació en diferents instants de temps), però no tenim una expressió analítica per aquest procés que ens permeti calcular el seu valor en un punt arbitrari. L'interpolació ens proporciona un mètode simple per estimar aquesta expressió analítica en el rang dels punts mesurats[1].

## 12.1 El problema d'interpolació

### 12.1.1 Problemes d'interpolació

**Definició 12.1.1** (Problema d'interpolació)**.** Siguin

$$\Phi(x; a_1, \ldots, a_n) \colon \mathbb{R} \longrightarrow \mathbb{R}$$

una família de funcions que depenen dels paràmetres reals $a_0, \ldots, a_n$, una família $\{(x_i, y_i)\}_{i=0}^n$ de $n$ punts. Direm que el problema d'interpolació de $\{(x_i, y_i)\}_{i=0}^n$ per $\Phi(x; a_0, \ldots, a_n)$ consisteix a determinar $a_0, \ldots, a_n$ tals que

$$\Phi(x_i; a_0, \ldots, a_n) = y_i \quad \text{per a tot } i \in \{1, \ldots, n\}.$$

També direm que $\{(x_i, y_i)\}_{i=0}^n$ són els punts de suport, $\{x_i\}_{i=0}^n$ són les abscisses de suport i $\{y_i\}_{i=0}^n$ les ordenades de suport.

Direm que un problema d'interpolació de $\{(x_i, y_i)\}_{i=0}^n$ per $\Phi(x; a_0, \ldots, a_n)$ és un problema d'interpolació lineal si existeixen $\Phi_0, \ldots, \Phi_n \colon \mathbb{R} \longrightarrow \mathbb{R}$ tals que

$$\Phi(x; a_0, \ldots, a_n) = a_0\Phi_0(x) + \cdots + a_n\Phi_n(x).$$

**Exemple 12.1.2.** *Exemples de problemes d'interpolació lineal són problemes com la interpolació polinòmica:*

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1 x + \cdots + a_n x^n;$$

*o la interpolació trigonomètrica:*

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1 e^{xi} + \cdots + a_n e^{nxi}.$$

[1] Si el punt que avaluem es troba fora del rang aquest problema s'anomena extrapolació i sol ser menys precís que la interpolació.

*Mentre que exemples de problemes d'interpolació no lineals són problemes com la interpolació racional:*

$$\Phi(x; a_0, \ldots, a_n, b_0, \ldots, b_m) = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m};$$

*o la interpolació exponencial:*

$$\Phi(x; a_0, \ldots, a_n, \lambda_0, \ldots, \lambda_n) = a_0 e^{\lambda_0 x} + \cdots + a_n e^{\lambda_n x}.$$

*La interpolació trigonomètrica es fa servir en l'anàlisi numèric de les sèries de Fourier, la interpolació exponencial és útil en l'anàlisi de desintegració radioactiva.*

## 12.2 Polinomis interpoladors de Lagrange

### 12.2.1 Interpolació de Lagrange

**Definició 12.2.1** (Problema d'interpolació de Lagrange)**.** Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació per $P(x; a_0, \ldots, a_n) \in \mathbb{R}_n[x]$ tal que $x_i \neq x_j$ per a tot $i, j \in \{0, \ldots, n-1\}$, amb $i \neq j$. Aleshores direm que el problema d'interpolació és un problema d'interpolació de Lagrange.

**Definició 12.2.2** (Polinomis bàsics de Lagrange)**.** Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x; a_0, \ldots, a_n)$ on, per a cert $k \in \{0, \ldots, n\}$ fix tenim que $y_k = 1$ i per a tot $i \in I = \{0, \ldots, k-1, k+1, \ldots, n\}$ tenim $y_i = 0$. Aleshores direm que els polinomis

$$L_k(x) = \prod_{i \in I} \frac{x - x_i}{x_k - x_i} = \frac{(x - x_0) \cdots (x - x_{k-1})(x - x_{k+1}) \cdots (x - x_n)}{(x_k - x_0) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_n)}$$

són polinomis bàsics de Lagrange.

**Observació 12.2.3.**

$$L_k(x_i) = \begin{cases} 1 & \text{si } i = k, \\ 0 & \text{si } i \neq k. \end{cases}$$

**Proposició 12.2.4.** *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$. Aleshores la funció $P(x)$ que satisfà*

$$P(x_i) = y_i$$

*per a tot $i \in \{0, \ldots, n\}$ és única.*

*Demostració.* Per l'observació 12.2.3 veiem que una solució a aquest problema d'interpolació és

$$P(x) = y_0 L_0(x) + y_1 L_1(x) + \cdots + y_n L_n(x).$$

Per veure'n la unicitat suposem que existeix un altre $Q(x) \in \mathbb{R}_{n+1}[x]$ tal que

$$P(x_i) = Q(x_i) = y_i$$

per a tot $i \in \{0, \dots, n\}$. Això és equivalent a que

$$P(x_i) - Q(x_i) = 0$$

per a tot $i \in \{0, \dots, n\}$. Ara bé, tenim que $x_0, \dots, x_n$ són arrels diferents de $P(x) - Q(x)$ per la definició de problema d'interpolació de Lagrange (12.2.1). Com que $P(x) - Q(x) \in \mathbb{R}_{n+1}[x]$, aquests són els seus únics zeros, i pel Teorema Fonamental de l'Àlgebra tenim que ha de ser $P(x) = Q(x)$. □

**Proposició 12.2.5.** *Siguin $\{(x_i, y_i)\}_{i=0}^n$ un conjunt de punts de suport, $I = \{i_0, \dots, i_k\} \subseteq \{1, \dots, n\}$ un conjunt i $\{(x_i, y_i)\}_{i \in I}$ un problema d'interpolació per $P_{i_0,\dots,i_k} \in \mathbb{R}_k[x]$, on*

$$P_{i_0,\dots,i_k}(x_{i_j}) = y_{i_j} \quad \textit{per a tot } j \in \{0, \dots, k\}.$$

*Aleshores*

$$P_i(x) = y_i$$

*i*

$$P_{i_0,\dots,i_k}(x) = \frac{(x - x_{i_0})P_{i_1,\dots,i_k}(x) - (x - x_{i_k})P_{i_0,\dots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}.$$

*Demostració.* Fixem $k = 1$. Aleshores tenim

$$P_i(x) = y_i.$$

Veiem la segona part. Definim

$$G(x) = \frac{(x - x_{i_0})P_{i_1,\dots,i_k}(x) - (x - x_{i_k})P_{i_0,\dots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}$$

tenim $G = P_{i_0,\dots,i_k}$ per la proposició 12.2.4, i per tant

$$G(x_{i_0}) = P_{i_0,\dots,i_{k-1}}(x_{i_0}) = y_{i_0}$$

i

$$G(x_{i_k}) = P_{i_1,\dots,i_k}(x_{i_k}) = y_{i_k},$$

i per tant

$$G(x_{i_j}) = \frac{(x_{i_j} - x_{i_0})y_{i_j} - (x_{i_j} - x_{i_k})y_{i_j}}{x_{i_k} - x_{i_0}} = y_{i_j}$$

per a tot $j \in \{1, \dots, k-1\}$, com volíem veure. □

**Observació 12.2.6** (Algorisme de Neville)**.** *Aquest mètode recurrent es pot organitzar en una taula com*

| | $k=0$ | $k=1$ | $k=2$ |
|---|---|---|---|
| $x_0$ | $y_0 = P_0(x)$ | | |
| | | $P_{0,1}(x)$ | |
| $x_1$ | $y_1 = P_1(x)$ | | $P_{0,1,2}(x)$ |
| | | $P_{1,2}(x)$ | |
| $x_2$ | $y_2 = P_2(x)$ | | |
| $\vdots$ | $\vdots$ | | |

*que s'omple de columna a columna de dreta a esquerra. Es coneix com a algorisme de Neville.*

**Exemple 12.2.7.** *Sigui* $\{(0,1),(1,3),(3,2)\}$ *un problema d'interpolació per* $P_{0,1,2}(x) \in \mathbb{R}_2[x]$. *Volem avaluar el polinomi interpolador de Lagrange en* $x = 2$, *és a dir, volem trobar* $P_{0,1,2}(2)$.

*Solució.* La taula de l'algoritme de Neville plantejada en l'observació algorisme de Neville (12.2.6) per aquest problema és

| | $k=0$ | $k=1$ | $k=2$ |
|---|---|---|---|
| $x_0 = 0$ | $y_0 = P_0(2) = 1$ | | |
| | | $P_{0,1}(2) = 5$ | |
| $x_1 = 1$ | $y_1 = P_1(2) = 3$ | | $P_{0,1,2}(2) = \frac{10}{3}$ |
| | | $P_{1,2}(2) = \frac{5}{2}$ | |
| $x_2 = 3$ | $y_2 = P_2(2) = 2$ | | |

i per tant trobem $P_{0,1,2}(2) = \frac{10}{3}$. ◊

### 12.2.2 Mètode de les diferències dividides de Newton

El mètode de Neville és útil per avaluar un polinomi interpolador en un punt una vegada, però si es vol obtenir l'expressió general del polinomi interpolador per poder avaluar-lo múltiples vegades en diferents punts s'hauran d'emparar altres solucions.

**Definició 12.2.8** (Diferències dividides)**.** Sigui $P(x; a_0, \ldots, a_n)$ el polinomi interpolador de Lagrange amb els punts de suport $\{(x_i, y_i)\}_{i=0}^n$. Aleshores direm que

$$[x_0, \ldots, x_k] = a_k$$

és la diferència dividida d'ordre $n$ del problema d'interpolació de Lagrange de $\{(x_i, y_i)\}_{i=0}^k$ per $P(x; a_0, \ldots, a_k)$.

Aquesta definició té sentit per la proposició 12.2.4.

**Proposició 12.2.9.** *Sigui* $\{(x_i, y_i)\}_{i=0}^n$ *un problema d'interpolació de Lagrange per* $P(x)$. *Aleshores*

$$P(x) = [x_0] + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots$$
$$\cdots + [x_0, \ldots, x_n](x - x_0)\cdots(x - x_{n-1}) = \sum_{i=0}^{n} \left( [x_0, \ldots, x_i] \prod_{j=0}^{i-1} (x - x_j) \right).$$

*Demostració.* Denotem per $P_{1,\ldots,k} \in \mathbb{K}_{k+1}[x]$ el polinomi que satisfà

$$P_{0,\ldots,k}(x_j) = y_j \quad \text{per a tot } j \in \{0, \ldots, k\}.$$

Aleshores tenim que el polinomi

$$G_k(x) = P_{0,\ldots,k}(x) - P_{0,\ldots,k-1}(x)$$

té com arrels $x_0, \ldots, x_{k-1}$, i per tant existeix una única constant $C_k$ tal que

$$G_k(x) = C_k(x - x_0)\cdots(x - x_{k-1})$$

i per tant, si fem

$$G_k(x) = a_0 + a_1 x + \cdots + a_k x^k$$

tenim que $C_k = a_k$. Aleshores per la definició de diferències dividides (12.2.8) tenim que

$$G_k(x) = [x_0, \dots, x_k](x - x_0) \cdots (x - x_{k-1})$$

i per la proposició 12.2.4 tenim

$$P(x) = P_n$$

i per tant trobem recursivament

$$\begin{aligned}
P_n(x) =& P_{n-1}(x) + [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
=& P_{n-2}(x) + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
&\vdots \\
=& P_{n-r}(x) + \sum_{i=0}^{n-r+1} \left( [x_0, \dots, x_{n-l+1}] \prod_{j=0}^{n-r} (x - x_j) \right) \qquad \text{(r>0)} \\
&\vdots \\
=& P_1(x) + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots \\
&\cdots + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1})
\end{aligned}$$

i per la definició de diferències dividides (12.2.8) tenim que $P_1(x) = [x_0]$

$$\begin{aligned}
=& [x_0] + [x_0, x_1](x - x_0) + \cdots + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) = P(x).
\end{aligned}$$

□

**Observació 12.2.10.** *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange. Aleshores per a tot $\sigma \in S_4$ tenim*

$$[x_0, \dots, x_n] = [x_{\sigma 0}, \dots, x_{\sigma(n)}].$$

*Demostració.* Per la proposició 12.2.4. □

**Proposició 12.2.11.** *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$. Aleshores*

$$[x_i] = y_i \quad \textit{per a tot } i \in \{0, \dots, n\} \tag{12.1}$$

*i*

$$[x_0, \dots, x_n] = \frac{[x_1, \dots, x_n] - [x_0, \dots, x_{n-1}]}{x_n - x_0}. \tag{12.2}$$

*Demostració.* Per veure (12.1) tenim prou en veure que per a un problema d'interpolació de $\{(x, y)\}$ per $P(x)$ tenim que $P(x) \in \mathbb{R}_0[x]$, i per tant és una constant i per la definició de diferències dividides (12.2.8) trobem $[x] = y$.

Per veure (12.2) tenim, per la proposició 12.2.5

$$P_{0,\dots,n}(x) = \frac{(x - x_0)P_{1,\dots,n}(x) - (x - x_n)P_{0,\dots,n-1}(x)}{x_n - x_0},$$

on $P_{i_1,\dots,i_k}(x)$ és el polinomi interpolador de Lagrange del problema interpolador del problema $\{(x_i, y_i)\}_{i\in\{i_1,\dots,i_k\}}$. Per tant per la proposició 12.2.9 trobem

$$[x_0,\dots,x_n] = \frac{[x_1,\dots,x_n]-[x_0,\dots,x_{n-1}]}{x_n-x_0},$$

com volíem veure. □

### 12.2.3 Error en la interpolació de Lagrange

**Teorema 12.2.12.** *Siguin $f\colon [a,b]\longrightarrow\mathbb{R}$ una funció de classe de diferenciabilitat $\mathcal{C}^{n+1}$ i $\{(x_i,f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$ amb abscisses de suport que satisfan $\{x_i\}_{i=0}^n\subset[a,b]$. Aleshores per a tot $x\in[a,b]$ tenim*

$$f(x)-P(x)=\frac{f^{(n+1)}(\xi(x))}{(n+1)!}\omega(x),$$

*on $\omega(x)=(x-x_0)\cdots(x-x_n)$, per a una certa funció $\xi(x)\colon[a,b]\longrightarrow[c,d]$ amb $c=\min\{\min_{i\in[0,n]}\{x_i\},x\}$ i $d=\max\{\max_{i\in[0,n]}\{x_i\},x\}$.*

*Demostració.* Fixem $x\in[a,b]$. Tenim $f(x_i)-P(x_i)=0$ per a tot $i\in\{0,\dots,n\}$. Si imposem $x\notin\{x_0,\dots,x_n\}$ i definim la funció

$$F(z)=f(z)-P(z)-\omega(z)S(x)$$

on

$$S(x)=\frac{f(x)-P(x)}{\omega(x)}. \tag{12.3}$$

Observem que $S(x)$ està ben definida pel Teorema Fonamental de l'Àlgebra.

Observem també que

$$F(x_i)=f(x_i)-P(x_i)-\omega(x_i)S(x)=0$$

i

$$F(x)=f(x)-P(x)-\omega(x)\frac{f(x)-P(x)}{\omega(x)}=0$$

és a dir, $F(z)$ existeixen $\xi_0^{(0)},\dots,\xi_{n+1}^{(0)}\in[a,b]$ tals que $F(\xi_i^{(0)})=0$ per a tot $i\in\{0,\dots,n+1\}$ amb $\xi_{i+1}^{(0)}>\xi_i^{(0)}$ per a tot $i\in\{0,\dots,n\}$.

Aplicant el Teorema de Rolle (5.2.14) trobem que per a tot $i\in\{1,\dots,n+1\}$ existeixen $\{\xi_i^{(1)}\}_{i=1}^{n+1}$ tals que $F'(\xi_i^{(1)})=0$ amb $\xi_i^{(1)}\in(\xi_{i-1}^{(0)},\xi_i^{(0)})$. Iterant aquest argument trobem que per a $k\in\{0,\dots,n+1\}$ tenim que per a tot $i\in\{k,\dots,n+1\}$ existeixen $\{\xi_i^{(k)}\}_{i=k}^{n+1}$ tals que $F^k(\xi_i^{(k)})=0$ amb $\xi_i^{(k)}\in(\xi_{i-1}^{(k-1)},\xi_i^{(k-1)})$; i per tant quan $k=n+1$ tenim que existeix $\xi_{n+1}^{(n+1)}\in(\xi_n^{(n)},\xi_{n+1}^{(n)})$ tal que $F^{(n+1)}(\xi_{n+1}^{(n+1)})=0$ i trobem

$$F^{(n+1)}(\xi_{n+1}^{(n+1)})=f^{(n+1)}(\xi_{n+1}^{(n+1)})-(n+1)!S(x)$$

i per tant, recordant (12.3), tenim

$$\frac{f^{(n+1)}(\xi_{n+1}^{(n+1)})}{(n+1)!}=\frac{f(x)-P(x)}{\omega(x)}$$

Dime si es verdad
Que alguien ha logrado escapar de esta tela de araña.
Dime cuanto cuesta ♫
Saber la puta verdad
Y quien le pone precio.

d'on trobem

$$f(x) - P(x) = \frac{f^{(n+1)}(\xi_{n+1}^{(n+1)})}{(n+1)!}\omega(x),$$

com volíem veure. □

**Observació 12.2.13.**

$$f(x) - P(x) = [x_0, \ldots, x_n, x]\omega(x)$$

**Corol·lari 12.2.14.** *Sigui $\{(x_i, f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange. Aleshores existeix un cert $\xi \in [x_0, x_n]$ tal que*

$$[x_0, \ldots, x_n] = \frac{f^{(n)}(\xi)}{n!}.$$

**Exemple 12.2.15.** *Considerem el següent problema d'interpolació*

| $i$ | 0 | 1 | 2 | 4 |
|---|---|---|---|---|
| $x_i$ | 100 | 101 | 102 | 103 |
| $\log(x_i)$ | $\log(100)$ | $\log(101)$ | $\log(102)$ | $\log(103)$ |

*per $P(x)$. Volem estimar l'error comés en calcular el valor de $P(102.5)$.*

*Solució.* Per la definició de problema d'interpolació de Lagrange (12.2.1) tenim que aquest problema d'interpolació és de Lagrange. Aleshores, pel Teorema 12.2.12 tenim que

$$f(x) - P(x) = \frac{f^{(4)}(\xi(x))}{4!}\omega(x)$$

i per tant, amb $f(x) = \log(x)$,

$$\log(x) - P(x) = \frac{-1}{\xi^4(x)4}(x-100)(x-101)(x-102)(x-103)$$

i si prenem $x = 102.5$ tenim

$$\log(102.5) - P(102.5) = \frac{-1}{\xi^4(102.5)4}\frac{5}{2}\frac{3}{2}\frac{1}{2}\frac{-1}{2}$$

amb $\xi(102.5) \in [100, 103]$, i per tant $\frac{1}{103} \leq \frac{1}{\xi(102.5)} \leq \frac{1}{100}$. Aleshores tenim

$$|\log(102.5) - P(x)| = \frac{3 \cdot 5}{2^4 \cdot \xi^4(102.5)} \leq \frac{15}{64}\frac{1}{100^4} \approx 2.34 \cdot 10^{-9}. \qquad \Diamond$$

### 12.2.4 Interpolació en nodes equiespaiats

**Definició 12.2.16** (Nodes equiespaiats)**.** Sigui $\{x_i\}_{i=0}^n$ abscisses de suport que satisfacin

$$x_i = x_0 + ih$$

amb $h = \frac{x_n - x_0}{n}$ per a tot $i \in \{0, \ldots, n\}$. Aleshores direm que les abscisses de suport $\{x_i\}_{i=0}^n$ són equiespaiades o que un problema d'interpolació $\{(x_i, y_i)\}_{i=0}^n$ és un problema d'interpolació amb nodes equiespaiats.

També denotarem

$$\Delta f(x) = f(x+h) - f(x) \quad \text{i} \quad \Delta^{n+1} f(x) = \Delta(\Delta^n f(x)).$$

**Teorema 12.2.17.** *Sigui $\{(x_i, f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange amb nodes equiespaiats. Aleshores, si $h = \frac{x_n - x_0}{n}$ tenim*

$$[x_0, \dots, x_n] = \frac{\Delta^n f(x_0)}{n! h^n}.$$

*Demostració.* Ho farem per inducció sobre $n$. El cas $n = 1$ és cert, ja que

$$\begin{aligned}
\Delta f(x_0) &= f(x_0 + h) - f(x_0) && \text{(nodes equiespaiats (12.2.16))} \\
&= f(x_1) - f(x_0) \\
&= h \frac{f(x_1) - f(x_0)}{x_1 - x_0} \\
&= h[x_0, x_n] && \text{(diferències dividides (12.2.8))}
\end{aligned}$$

i per tant

$$[x_0, x_n] = \frac{\Delta f(x_0)}{h}. \tag{12.4}$$

Suposem ara que l'enunciat és cert per a $k$ fix i demostrem-ho pel cas $k+1$. Tenim que

$$\begin{aligned}
\Delta^{k+1} f(x_0) &= \Delta(\Delta^k(f(x_0)) && \text{(nodes equiespaiats (12.2.16))} \\
&= \Delta^k f(x_1) - \Delta^k f(x_0) && \text{(nodes equiespaiats (12.2.16))} \\
&= k! h^k([x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]) && (12.4) \\
&= k! h^k (k+1) h \frac{[x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]}{x_{k+1} - x_0} \\
&= (k+1)! h^{k+1} [x_0, \dots, x_{k+1}], && \text{(diferències dividides (12.2.8))}
\end{aligned}$$

i per tant tenim

$$[x_0, \dots, x_{k+1}] = \frac{\Delta^{k+1} f(x_0)}{(k+1)! h^{k+1}},$$

com volíem veure. □

## 12.3 Polinomis interpoladors per splines

### 12.3.1 Interpolació per splines

**Definició 12.3.1.** Siguin $\Delta = \{x_i\}_{i=0}^n$ una partició d'un interval $[a, b] \subset \mathbb{R}$ i $s \colon [a, b] \longrightarrow \mathbb{R}$ una funció a trossos de classe $\mathcal{C}^{p-1}$ de la forma

$$s(x) = \begin{cases} s_1(x) & \text{si } x \in [x_0, x_1] \\ \vdots & \\ s_{k+1}(x) & \text{si } x \in [x_k, x_{k+1}] \\ \vdots & \\ s_n(x) & \text{si } x \in [x_{n-1}, x_n] \end{cases}$$

amb $s_i \in \mathbb{R}_p[x]$ per a tot $i \in \{1, \dots, n\}$. Aleshores direm que $s$ és un spline de grau $p$ associat a $\Delta$.

Denotarem

$$S_p(\Delta) = \{s \mid s \text{ és un spline de grau } p \text{ associat a } \Delta\}.$$

**Nota 12.3.2.** *Només treballarem amb splines cúbics, és a dir, amb $p = 3$, que són els més emparats.*

ai haig de córrer

# Bibliografia


[1] Josep Maria Mondelo. «Apunts de Mètodes Numèrics». 2008.

[2] Antoni Aubanell, Antoni Benseny i Amadeu Delshams. *Eines bàsiques de càlcul numèric. Amb 87 problemes resolts*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 1994. ISBN: 84-7929-231-8.

[3] Richard L. Burden i D. Douglas Faires. *Numerical Analysis*. Castellà. 7a ed. Brooks/Cole, 2000. ISBN: 978-0534382162.

[4] Miguel Grau Sánchez i Miquel Noguera Batlle. *Càlcul numèric*. Edicions UPC, 2000. ISBN: 9788483013816.

[5] David R. Kincaid i Cheney E. Ward. *Numerical Analysis. Mathematics of Scientific Computing*. Anglès. 2a ed. Brooks Cole, 1996. ISBN: 978-0534338923.

[6] Peter Henrici. *Elements of Numerical Analysis*. John Wiley & Sons, 1964. ISBN: 978-0471372417.

[7] Germund Dahlquist i Ake Bjorck. *Numerical Methods*. Anglès. Prentice Hall PTR, 1964. ISBN: 978-0136273158.

[8] Eugene Isaacson i Herbert Bishop Keller. *Analysis of Numerical Methods*. Anglès. Dover Publications, 1966. ISBN: 978-0486680293.

[9] Josef Stoer i Roland Bulirsch. *Introduction to Numerical Analysis*. Anglès. Springer, 2002. ISBN: 978-0-387-21738-3.

[10] Brian Kernighan i Dennis Ritchie. *The C Programming Language*. Anglès. 2a ed. Prentice Hall, 1998. ISBN: 978-0131103627.

[11] Brian Kernighan i Rob Pike. *The Practice of Programming*. Addison-Wesley, 1999. ISBN: 978-0201615869.


La bibliografia del curs inclou els textos [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11].