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 emprarem 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 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

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

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

$$R \iff S = (R \implies S) \wedge (S \implies R).$$

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*

$$(R \vee R) \implies R$$

és vertadera.

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

$$R \implies (R \vee S)$$

és vertadera.

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

$$(R \vee S) \implies (S \vee R)$$

és vertadera.

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

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

és vertadera.

Axioma 1.1.11. *Siguin R i S dues relacions tals que R i $R \implies S$ 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 $R \implies S$ i $S \implies T$ siguin vertaderes. Aleshores la relació $R \implies T$ és vertadera.*

Demostració. Per l'axioma 1.1.10 la relació

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

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

$$(S \implies T) \implies ((R \implies S) \implies (R \implies T))$$

i com que, per hipòtesi, la relació $S \implies T$ és vertadera per l'axioma 1.1.11 tenim que la relació $(R \implies S) \implies (R \implies T)$ és vertadera, i com que, de nou per hipòtesi, tenim que la relació $R \implies S$ és vertadera tenim per l'axioma 1.1.11 que la relació $R \implies T$ 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 $R \implies R$. Per l'axioma 1.1.7 tenim que la relació $(R \vee R) \implies R$ és vertadera, i per l'axioma 1.1.8 tenim que la relació $R \implies (R \vee R)$ és vertadera. Per tant, per la tautologia 1.1.13, veiem que $R \implies R$. □

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 $R \implies (R \vee S)$ és vertadera, i per l'axioma 1.1.9 tenim que $(R \vee S) \implies (S \vee R)$ 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 $R \iff \neg(\neg R)$ 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*

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

és vertadera.

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

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

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

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

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*

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

és vertadera.

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

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

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

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

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

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

$$(R \implies S) \iff ((\neg S) \implies (\neg R))$$

és vertadera.

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

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

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

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

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 ($\implies$). 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 $R \implies S$ és vertadera. Ara bé, per la tautologia de la llei de les contrarecíproques (1.1.19) tenim que la relació $(\neg S) \implies (\neg R)$ és vertadera, i pels axiomes 1.1.10 i 1.1.7 tenim que la relació

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

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

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

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

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

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

$$R \implies (R \wedge S)$$

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 ($\Longleftarrow$). 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 $(R \wedge S) \implies S$ és vertadera si i només si la relació

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

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

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

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

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 $R \implies (\neg(\neg R))$ és vertadera, i per l'axioma 1.1.10 això és que la relació

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

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

$$(R \vee S) \iff ((\neg R) \implies S).$$

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

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. $\square$

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 suficient ($\Longleftarrow$). 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 necessària ($\Longrightarrow$). 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. $\square$

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 la 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 ($\Longrightarrow$). 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 ($\Longleftarrow$). 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.

Lema 3.1.2. $\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$.

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 3.1.3. Denotarem $S(1) = 2$, $S(2) = 3$, $S(3) = 4$, etc. Per tant

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

Això té sentit pel lema 3.1.2.

Notació 3.1.4. Denotarem l'acció d'aplicar l'aplicació S al nombre natural n un nombre natural k de vegades com $S^k(n)$.

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 lema 3.1.2 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 (1) tenim que $a \neq 1$, per tant, pel lema 3.1.2 tenim que $a = S(b)$ per a cert $b \in \mathbb{N}$. 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 (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 $n \in \mathbb{N}$. □

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 $A = \mathbb{N}$. $\square$

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 $A = \mathbb{N}$. $\square$

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

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

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

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

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

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. $\square$

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. $\square$

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 $-b \mid a$. $\square$

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 $c \mid ab$. $\square$

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

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

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 λ 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 la identitat de Bézout

Lema 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 lema 3.2.28.

Si $D < 0$ i $d > 0$ definim $D' = -D$. Aleshores $D' > 0$, i pel lema 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 α i β 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 $\operatorname{mcd}(a, b) = 1$. 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 α i β tals que*

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

Demostració. Veiem que la condició és suficient ($\Longrightarrow$). 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 ($\Longleftarrow$). Suposem doncs que existeixen dos enters α i β 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 $\operatorname{mcd}(a, b) = 1$. □

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 α i β 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

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

com el mínim comú múltiple de a i b.

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

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

Demostració. Sigui $d = \operatorname{mcd}(a, b)$. 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 α i β 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 $l = \mathrm{mcm}(a, b)$, i per tant

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

□

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. □

Lema 3.2.38. *Sigui a un enter amb $a > 1$. Aleshores existeixen $p_1, \ldots, p_n$ primers i $r_1, \ldots, r_n$ enters positius 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 α i β 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. □

Lema 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. $\square$

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 lema 3.2.38 i el lema 3.2.39. $\square$

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 lema 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. $\square$

3.3 Els nombres modulars

3.3.1 Construcció dels nombres modulars

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

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

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

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

Per veure el punt (2) fem

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

Per veure el punt (3) fem

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

Per veure el punt (4) fem

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

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

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

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

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

Per veure el punt (4) fem

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

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 de nombres modulars congruents (3.3.2) tenim que existeixen enters λ i μ tals que $a - a' = \lambda m$ i $b - b' = \mu m$. Per tant

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

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 λ 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 $\operatorname{mcd}(a, m) = 1$, 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

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

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

Lema 3.3.12. *Siguin $m_1, \dots, m_n$ naturals més grans que 1, $a_1, \dots, a_n$ 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* $M = \mathrm{mcm}(m_1, \dots, m_n)$ *i per a tot* λ *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 λ 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 $M = \mathrm{mcm}(m_1, \dots, m_n)$. Per la definició de mínim comú múltiple (3.2.34) i la definició de coprimers (3.2.31) tenim que

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

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

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

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 lema 3.3.12 tenim que

$$x = x_0 + \lambda M$$

amb $M = \mathrm{mcm}(m_1, \ldots, m_n)$ 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 σ 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 S_X és el grup simètric de X.

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

Proposició 3.4.4. *Siguin X un conjunt no buit i σ una permutació de S_X. Aleshores*

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

Demostració. Comencem veient l'implicació cap a la dreta ($\Longrightarrow$). 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 ($\Longleftarrow$). Prenem 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 σ i τ dues permutacions de 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 σ i τ dues permutacions de S_X tals que $\mathrm{M}(\sigma) \cap \mathrm{M}(\tau) = \emptyset$. Aleshores direm que σ i τ són disjuntes.

Proposició 3.4.7. *Siguin X un conjunt no buit i σ i τ dues permutacions disjuntes de 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, σ i τ 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) σ és una aplicació bijectiva, i per la definició d'aplicació bijectiva (2.2.9) trobem que σ 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

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

Lema 3.4.8. *Siguin X un conjunt no buit i τ una permutació de 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 σ és bijectiva, i per la definició de conjunt d'elements moguts per una permutació (3.4.3) trobem que $\sigma(x) = x$ 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 σ i τ dues permutacions disjuntes de 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 lema 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 lema 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 σ una permutació de 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 σ 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 σ un r-cicle de 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

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

Lema 3.4.12. *Siguin X un conjunt no buit i σ un r-cicle de 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 $a \in \mathrm{M}(\sigma)$,

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

i per la definició d'r-cicle (3.4.10) tenim que $\sigma^i(a) \neq a$ per a tot $i \in \{0, \ldots, r-1\}$, 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 σ un r-cicle de S_X. Aleshores*

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

Demostració. Pel lema 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 σ una permutació de S_X. Aleshores existeixen $\alpha_1, \dots, \alpha_s$ cicles disjunts dos a dos de 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 α_2 disjunt amb α_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 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 β_{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

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

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 τ un 2-cicle de S_X. Aleshores direm que τ és una transposició.

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

Proposició 3.4.17. *Siguin X un conjunt finit no buit i σ una permutació de S_X. Aleshores existeixen transposicions $\tau_1, \dots, \tau_s$ de S_X tals que*

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

Demostració. Observem que per a tot r-cicle α de S_X existeixen transposicions $\tau_1, \dots, \tau_r$ de 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 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, σ una permutació de S_X i $\tau_1, \dots, \tau_r$, $\tau'_1, \dots, \tau'_{r'}$ transposicions de 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. :(□

Definició 3.4.19 (Signe d'una permutació)**.** Siguin X un conjunt finit no buit, σ una permutació de S_X i $\tau_1, \dots, \tau_r$ transposicions de S_X tals que

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

Aleshores definim

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

com el signe de σ.

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. $\square$

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
$$(a, b) \sim (1, 1),$$
si i només si, per la definició de nombres enters (3.2.2), tenim
$$a \cdot 1 = b \cdot 1.$$
I per tant, per la proposició 3.2.6 trobem que ha de ser $a = b$. $\square$

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

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

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

Per veure el punt (2) fem

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

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

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

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

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

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] *Apunts d'un curs de Topologia elemental.* Vers. 1.2. 2017. URL: http://mat.uab.cat/~aguade/teaching.html.

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

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

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

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

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

[10] 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 part axiomàtica de la secció de teoria de conjunts està inspirada en [4], i la resta segueix [3].

La bibliografia del curs inclou els textos [2, 5, 6, 7, 8, 9, 10].

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. També escriurem $0_{n \times n} = 0_n$.

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 α 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

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

i trobem $A - A = 0$. □

Proposició 4.1.12. *Siguin A una matriu de mida $m \times n$ i α i β 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

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

□

Proposició 4.1.13. *Siguin A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$ i α i β 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

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

i hem acabat. □

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

$$[1A]_{i,j} = 1[A]_{i,j}$$

i per la definició de cos (4.1.1) trobem que

$$1[A]_{i,j} = [A]_{i,j},$$

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

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

com volíem veure. □

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*

$$(A + A')B = AB + A'B$$

i

$$A(B + B') = AB + AB'.$$

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

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

L'altre demostració és anàloga. □

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*

$$I_m A = A = A I_n.$$

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*

$$AA_1 = A_1 A = I_n \quad i \quad AA_2 = A_2 A = I_n.$$

Aleshores $A_1 = A_2$.

Demostració. Per la proposició 4.1.15 tenim que

$$A_1(AA_2) = (A_1 A) A_2$$

i per hipòtesi trobem que $A_1 I_n = I_n A_2$, 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.

Observació 4.1.21. *Sigui $A = (a_{i,j})$ una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$ tal que existeix un $i \in \{1, \dots, n\}$ satisfent*

$$a_{i,j} = 0 \text{ ó } a_{j,i} = 0 \quad \text{per a tot } j \in \{1, \dots, n\}.$$

Aleshores A no és invertible.

Proposició 4.1.22. *Siguin A i B dues matrius invertibles d'ordre n sobre un cos $\mathbb{K}$. Aleshores la matriu AB és invertible.*

Demostració. Per la proposició 4.1.15 i la definició de matriu invertible (4.1.20) tenim que

$$(AB)(B^{-1}A^{-1}) = \mathrm{Id} \quad \text{i} \quad (B^{-1}A^{-1})(AB) = \mathrm{Id},$$

i de nou per la definició tenim que AB és invertible. □

Proposició 4.1.23. *Siguin A i B dues matrius invertibles d'ordre n sobre un cos $\mathbb{K}$. Aleshores*

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

Aquest enunciat té sentit per la proposició 4.1.22.

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 4.1.24. *Sigui A una matriu invertible d'ordre n sobre un cos $\mathbb{K}$. Aleshores*

$$(A^{-1})^{-1} = A.$$

Demostració. Per la proposició 4.1.23 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 4.1.25 (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 4.1.26. *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 (4.1.25) 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 4.1.27. *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 (4.1.25) 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. □

Proposició 4.1.28. *Sigui A una matriu invertible d'ordre n sobre un cos $\mathbb{K}$. Aleshores la matriu A^t és invertible i $(A^t)^{-1} = \left(A^{-1}\right)^t$.*

Demostració. Per la proposició 4.1.27 tenim que

$$A^t \left(A^{-1}\right)^t = \left(A^{-1}A\right)^t \quad \text{i} \quad \left(A^{-1}\right)^t A^t = \left(AA^{-1}\right)^t,$$

i per la definició de matriu invertible (4.1.20) tenim que A^t és invertible i que $(A^t)^{-1} = \left(A^{-1}\right)^t$, com volíem veure. □

Definició 4.1.29 (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 4.1.30 (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 4.1.31. *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 4.1.32. 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 4.1.33. 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 4.1.34. *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 $k_i \in \{1, \ldots, p-1\}$, $k_j \in \{1, \ldots, r-1\}$, $i' \leq m_{k_i+1} - m_{k_i}$ 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 diferents amb $i, j \leq m$ i λ un element no nul de $\mathbb{K}$. 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 d'ordre m sobre $\mathbb{K}$ tal que $f(A) = PA$ i per a tota successió de transformacions elementals per columnes g existeix una matriu Q d'ordre 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). □

Definició 4.2.3 (Matriu elemental)**.** Sigui P una matriu d'ordre n sobre un cos $\mathbb{K}$ tal que existeixi una sèrie de transformacions elementals tals que per a tota matriu A de mida $m \times n$ sobre $\mathbb{K}$ tenim $f(A) = PA$. Aleshores direm que P és una matriu elemental.

Aquesta definició té sentit per la proposició 4.2.2.

Observació 4.2.4. *Siguin P i Q dues matrius elementals d'ordre n sobre un cos $\mathbb{K}$. Aleshores PQ és una matriu elemental.*

Notació 4.2.5. 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.

Proposició 4.2.6. *Sigui P una matriu elemental d'ordre n sobre un cos $\mathbb{K}$. Aleshores P és una matriu invertible.*

Demostració. En tenim prou amb veure que $P_{i,j}^{-1} = P_{i,j}$, $D_{i,\lambda}^{-1} = D_{i,\lambda^{-1}}$ i $E_{i,j,\lambda}^{-1} = E_{i,j,-\lambda}$. Per tant, per la definició de matriu elemental (4.2.3) i la definició de matriu invertible (4.1.20) tenim que P és una matriu invertible. □

4.2.2 Matrius esglaonades i mètode de Gauss

Definició 4.2.7 (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 $a_{i,j_i} = 1$; i per a tot $i > j_r$ i $j \in \{1, \ldots, n\}$ tenim $a_{i,j} = 0$.

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 4.2.8. *Sigui A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores A es pot esglaonar per files.*

Demostració. Denotem $A = (a_{i,j})$. Ho farem per inducció sobre n.

Suposem que $n = 1$. Si $a_{i,1} = 0$ per a tot $i \in \{1, \dots, m\}$ per la definició de matriu esglaonada (4.2.7) hem acabat. Suposem doncs que existeix un $i \in \{1, \dots, m\}$ tal que $a_{i,1} \neq 0$. Aleshores podem fer les transformacions elementals

$$A = \begin{bmatrix} a_{i,1} \\ \vdots \\ a_{m,1} \end{bmatrix} \xrightarrow{F_i \leftrightarrow F_1} \begin{bmatrix} a_{i,1} \\ \vdots \\ a_{i-1,1} \\ a_{1,1} \\ a_{i+1,1} \\ \vdots \\ a_{m,1} \end{bmatrix} \xrightarrow{F_1 \to a_{1,1}^{-1} F_1} \begin{bmatrix} 1 \\ a_{2,1} \\ \vdots \\ a_{m,1} \end{bmatrix} \xrightarrow[\text{per a tot } i \in \{2,\dots,m\}]{F_i \to F_i - a_{i,1} F_1} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

i per la definició de matriu esglaonada (4.2.7) hem acabat.

Suposem doncs que la hipòtesi és certa per a n. Veiem que també ho és per $n+1$. Sigui $A = (a_{i,j})$ una matriu de mida $m \times (n+1)$ sobre $\mathbb{K}$. Considerem la matriu

$$A' = \begin{bmatrix} a_{1,2} & \dots & a_{1,n+1} \\ \vdots & & \vdots \\ a_{m,2} & \dots & a_{m,n+1} \end{bmatrix}.$$

Per la definició de matriu (4.1.2) tenim que A' és una matriu de mida $m \times n$ sobre $\mathbb{K}$, i per l'hipòtesi d'inducció tenim que podem esglaonar-la. Sigui doncs B la matriu A' esglaonada. Considerem la matriu

$$\begin{bmatrix} a_{1,1} \\ \vdots \\ a_{1,m} \end{bmatrix},$$

que correspon a la primera columna de la matriu A. Hem vist que podem esglaonar-la, i per tant per la definició de matriu esglaonada (4.2.7) tenim que podem esglaonar la matriu A, ja que

$$A = \left[\begin{array}{c|c} a_{1,1} & \\ \vdots & A' \\ a_{1,m} & \end{array} \right],$$

i pel principi d'inducció (3.1.7) hem acabat. $\square$

Corol·lari 4.2.9. *Sigui A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores A es pot esglaonar per columnes.*

4.2.3 Teorema de la PAQ-reducció

Teorema 4.2.10 (Teorema de la PAQ-reducció)**.** *Sigui A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores existeixen un únic nombre natural r satisfent $r \leq \min(m, n)$, una matriu elemental P d'ordre m sobre $\mathbb{K}$ i una matriu elemental Q d'ordre n sobre $\mathbb{K}$ tals que*

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right].$$

Demostració. Denotem $A = (a_{i,j})$. Si $a_{i,j} = 0$ per a tot $i \in \{1, \dots, m\}$ i $j \in \{1, \dots, n\}$ aleshores tenim $r = 0$ i hem acabat. Suposem doncs que existeixen $i \in \{1, \dots, m\}$ i $j \in \{1, \dots, n\}$ tals que $a_{i,j} \neq 0$.

Per la proposició 4.2.8 tenim que existeix una matriu elemental P d'ordre m sobre $\mathbb{K}$ tal que PA està esglaonada per files. Per la definició de matriu esglaonada (4.2.7) tenim que existeixen j_i per a tot $i \in \{1, \dots, r\}$ amb $j_1 < \cdots < j_r$ tals que per a tot $j < j_i$ tenim $a_{i,j} = 0$ i $a_{i,j_i} = 1$. Fent les transformacions elementals

$$C_1 \leftrightarrow C_{j_1}, \quad C_2 \leftrightarrow C_{j_2}, \dots, C_r \leftrightarrow C_{j_r}$$

a la matriu PA obtenim la matriu

$$A_1 = \left[\begin{array}{cccc|ccc} 1 & b_{1,2} & \cdots & b_{1,r} & b_{1,r+1} & \cdots & b_{1,n} \\ 0 & 1 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & b_{r-1,r} & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & b_{r,r+1} & \cdots & b_{r,n} \\ \hline 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{array}\right],$$

i fent a la matriu A_1 les transformacions elementals

$$\begin{aligned} C_{k_1} &\to C_{k_1} - b_{1,k_1} C_1, \quad \text{per a } k_1 \in \{2, \dots, n\} \\ C_{k_2} &\to C_{k_2} - b_{2,k_2} C_2, \quad \text{per a } k_2 \in \{3, \dots, n\} \\ &\vdots \\ C_{k_r} &\to C_{k_r} - b_{r,k_r} C_r, \quad \text{per a } k_r \in \{r+1, \dots, n\}, \end{aligned}$$

i per la proposició 4.2.2 tenim que existeix una matriu P d'ordre n sobre $\mathbb{K}$ tal que

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right],$$

i per la definició de 4.2.2 tenim que les matrius P i Q són matrius elementals.

Veiem ara que r és únic. Suposem que existeixen un nombre natural $s \leq \min(m, n)$, una matriu elemental P_1 d'ordre m sobre $\mathbb{K}$ i una matriu elemental Q_1 d'ordre n sobre $\mathbb{K}$ tals que

$$P_1 A Q_1 = \left[\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right].$$

Hem de veure que $r = s$. Suposem que $r \leq s$.

Tenim que

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$$

i

$$P_1 A Q_1 = \left[\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right].$$

Com que, per la proposició 4.2.6, les matrius P, Q, P_1 i Q_1 són invertibles tenim que

$$A = P^{-1}\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]Q^{-1} = P_1^{-1}\left[\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right]Q_1^{-1},$$

i per tant

$$P_1 P^{-1}\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] = \left[\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right]Q_1^{-1}Q.$$

Denotem $P_2 = P_1P^{-1}$, $Q_2 = Q_1^{-1}Q$, $P_2 = (p_{i,j})$ i $Q_2 = (q_{i,j})$ i tenim

$$\left[\begin{array}{ccc|ccc} p_{1,1} & \cdots & p_{1,r} & p_{1,r+1} & \cdots & p_{1,m} \\ \vdots & & \vdots & \vdots & & \vdots \\ p_{s,1} & \cdots & p_{s,r} & p_{s,r+1} & \cdots & p_{s,m} \\ \hline p_{s+1,1} & \cdots & p_{s+1,r} & p_{s+1,r+1} & \cdots & p_{s+1,m} \\ \vdots & & \vdots & \vdots & & \vdots \\ p_{m,1} & \cdots & p_{m,r} & p_{m,r+1} & \cdots & p_{m,m} \end{array}\right]\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] =$$

$$= \left[\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right]\left[\begin{array}{ccc|ccc} q_{1,1} & \cdots & q_{1,r} & q_{1,r+1} & \cdots & q_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ q_{s,1} & \cdots & q_{s,r} & q_{s,r+1} & \cdots & q_{s,n} \\ \hline q_{s+1,1} & \cdots & q_{s+1,r} & q_{s+1,r+1} & \cdots & q_{s+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ q_{n,1} & \cdots & q_{n,r} & q_{n,r+1} & \cdots & q_{n,n} \end{array}\right],$$

i per la proposició 4.1.34 tenim que

$$\begin{bmatrix} p_{1,1} & \cdots & p_{1,r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ p_{s,1} & \cdots & p_{s,r} & 0 & \cdots & 0 \\ p_{s+1,1} & \cdots & p_{s+1,r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ p_{m,1} & \cdots & p_{m,r} & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} q_{1,1} & \cdots & q_{1,r} & q_{1,r+1} & \cdots & q_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ q_{s,1} & \cdots & q_{s,r} & q_{s,r+1} & \cdots & q_{s,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Per tant

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} q_{1,r+1} & \cdots & q_{1,n} \\ \vdots & & \vdots \\ q_{s,r+1} & \cdots & q_{s,n} \end{bmatrix}$$

i trobem que

$$Q_2 = \left[\begin{array}{ccc|ccc} q_{1,1} & \cdots & q_{1,r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ q_{s,1} & \cdots & q_{s,r} & 0 & \cdots & 0 \\ \hline q_{s+1,1} & \cdots & q_{s+1,r} & q_{s+1,r+1} & \cdots & q_{s+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ q_{n,1} & \cdots & q_{n,r} & q_{n,r+1} & \cdots & q_{n,n} \end{array}\right].$$

Denotem per tant

$$Q_2 = \left[\begin{array}{c|c} Q_2' & 0_{s\times(n-r)} \\ \hline Q_2'' & Q_2''' \end{array}\right].$$

Ara bé, pel que hem vist abans, existeixen un nombre natural $t \leq \min(r, s)$, una matriu invertible P_3 d'ordre s sobre $\mathbb{K}$ i una matriu invertible Q_3 d'ordre r sobre $\mathbb{K}$ tals que

$$P_3 Q_2'' Q_3 = \left[\begin{array}{c|c} I_t & 0 \\ \hline 0 & 0 \end{array}\right],$$

i com que, per hipòtesi, $r \leq s$ tenim $t \leq r \leq s$.

Per tant per la proposició 4.1.34 tenim que

$$\left[\begin{array}{c|c} P_3 & 0_{s\times(n-s)} \\ \hline 0_{(n-s)\times s} & I_{n-s} \end{array}\right] \left[\begin{array}{c|c} Q_2' & 0_{s\times(n-r)} \\ \hline Q_2'' & Q_2''' \end{array}\right] \left[\begin{array}{c|c} Q_3 & 0_{r\times(n-r)} \\ \hline 0_{(n-r)\times r} & I_{n-r} \end{array}\right] =$$

$$= \left[\begin{array}{c|c} \begin{array}{c|c} I_t & 0_{t\times(r-t)} \\ \hline 0_{(r-t)\times t} & 0_{(s-t)\times(r-t)} \end{array} & 0_{s\times(n-r)} \\ \hline Q_2''Q_3 & Q_2''' \end{array}\right] = B.$$

Per la proposició 4.1.22 trobem que la matriu B és invertible. Ara bé, per l'observació 4.1.21 trobem que ha de ser $r - t = s - t = 0$, i per tant $r = s$, com volíem veure. La demostració del cas $s \leq r$ és anàloga. $\square$

Definició 4.2.11 (Rang)**.** Siguin A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$, P una matriu invertible d'ordre n sobre $\mathbb{K}$ i Q una matriu invertible d'ordre m sobre $\mathbb{K}$ tals que

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right].$$

Aleshores direm que r és el rang de A i denotarem $\operatorname{rang}(A) = r$.

Observem que aquesta definició té sentit pel Teorema de la PAQ-reducció (4.2.10).

Proposició 4.2.12. *Sigui A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$. Aleshores* $\operatorname{rang}(A) = \operatorname{rang}(A^t)$.

Demostració. Per la definició de rang d'una matriu (4.2.11) tenim que existeixen una matriu P invertible d'ordre n sobre $\mathbb{K}$ i una matriu Q invertible d'ordre m sobre $\mathbb{K}$ tals que

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right].$$

Ara bé, per la proposició 4.1.27 tenim que

$$Q^t A^t P^t = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right].$$

Per la proposició 4.1.28 tenim que les matrius Q^t i P^t són invertibles, i per tant, per la definició de rang d'una matriu (4.2.11) tenim que rang $A^t = r$. □

Proposició 4.2.13. *Sigui A una matriu invertible d'ordre n sobre un cos $\mathbb{K}$. Aleshores A és una matriu elemental.*

Demostració. Pel Teorema de la PAQ-reducció (4.2.10) tenim que existeixen dues matrius invertibles P i Q d'ordre n sobre $\mathbb{K}$ tals que

$$PAQ = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right].$$

Ara bé, per la proposició 4.1.22 tenim que la matriu

$$\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$$

ha de ser invertible, i per l'observació 4.1.21 trobem que ha de ser $r = n$. Per tant tenim $PAQ = I_n$ i tenim que $A = P^{-1}Q^{-1}$, i per l'observació 4.2.4 tenim que A és una matriu elemental. □

Corol·lari 4.2.14. *Sigui A una matriu d'ordre n sobre un cos $\mathbb{K}$. Aleshores A és invertible si i només si* $\operatorname{rang}(A) = n$.

Observació 4.2.15. *Siguin A una matriu de mida $m \times n$ sobre un cos $\mathbb{K}$, P una matriu invertible d'ordre m sobre $\mathbb{K}$ i Q una matriu invertible d'ordre n sobre $\mathbb{K}$. Aleshores*

$$\operatorname{rang}(A) = \operatorname{rang}(PAQ).$$

4.3 Determinant d'una matriu

4.3.1 Propietats dels determinants

Definició 4.3.1 (Determinant)**.** Siguin $\mathbb{K}$ un cos i $\det\colon M_n(\mathbb{K}) \longrightarrow \mathbb{K}$ una aplicació que satisfà per a tot $i \in \{1,\dots,n\}$ i $j \in \{i+1,\dots,n\}$ i per a tot $C_i \in M_{n\times 1}(\mathbb{K})$

1. Per a tot $C'_j \in M_{n\times 1}(\mathbb{K})$ es satisfà

$$\begin{aligned}\det(C_1,\dots,C_{i-1},C_i + C'_i, C_{i+1},\dots,C_n) &= \\ = \det(C_1,\dots,C_n) &+ \det(C_1,\dots,C_{i-1},C'_i,C_{i+1},\dots,C_n).\end{aligned}$$

2. Per a tot $\alpha \in \mathbb{K}$ es satisfà

$$\det(C_1,\dots,C_{i-1},\alpha C_i,C_{i+1},\dots,C_n) = \alpha\det(C_1,\dots,C_n)$$

3. Si $C_i = C_j$ es satisfà

$$\det(C_1,\dots,C_n) = 0.$$

4. $\det(I_n) = 1$.

Aleshores direm que det és un determinant.

Proposició 4.3.2.

Part III

Coses per fer

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)**.**

Definició 5.1.3 (Producte escalar)**.** És lineal i més coses.

Definició 5.1.4 (Norma d'un vector)**.** $\|\vec{v}\| = \sqrt{\langle \vec{v}, \vec{v} \rangle}$.

Definició 5.1.5 (Dependència lineal)**.**

5.1.2 Proposicions

Proposició 5.1.6. *Vectors linealment independents* $\iff$ *determinant no nul.*

5.1.3 Teoremes

Teorema 5.1.7. *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 (Imatge)**.** Siguin X i Y dos conjunts, A un subconjunt de X i $f\colon X \longrightarrow Y$ una aplicació. Aleshores definim

$$\mathrm{Im}_A(f) = \{f(a) \in Y \mid a \in A\}$$

com la imatge de f per A.

Definició 5.2.2 (Antiimatge)**.** Siguin X i Y dos conjunts, B un subconjunt de Y i $f\colon X \longrightarrow Y$ una aplicació. Aleshores definim

$$\mathrm{Im}^{\text{-1}}{}_B(f) = \{x \in X \mid f(x) = b \text{ per a cert } b \in B\}$$

com la antiimatge de f per B.

Definició 5.2.3 (Límit)**.**

Definició 5.2.4 (Funció contínua)**.** Sigui f una funció. Direm que f és contínua en a si

$$\lim_{x\to a} f(x) = f(a).$$

Definició 5.2.5 (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 5.2.6 (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 5.2.7 (Derivada)**.**

Definició 5.2.8 (Notació de Landau)**.** $A(h) = \mathrm{o}(B(h))\ldots$

5.2.2 Proposicions

Proposició 5.2.9. *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 5.2.10. *Sigui $f\colon [a,b] \to \mathbb{R}$ una funció acotada i monòtona. Aleshores f és integrable Riemann.*

5.2.3 Teoremes

Teorema 5.2.11 (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 5.2.12 (Teorema del Valor Mig)**.** hmm trivial

Teorema 5.2.13 (Desigualtat de Cauchy-Schwarz)**.**

Teorema 5.2.14 (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 5.2.15 (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 5.2.16 (Teorema del sandvitx)**.**

Teorema 5.2.17 (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 $f'(c) = 0$.*

Teorema 5.2.18 (Teorema Fonamental del Càlcul)**.** *Siguin $[a, b]$ un interval de $\mathbb{R}$, $f\colon [a, b] \longrightarrow \mathbb{R}$ una funció contínua en $[a, b]$ i*

$$F(x) = \int_a^x f(t)dt$$

una funció. Aleshores $F(x)$ és derivable en $[a, b]$ i $F'(x) = f(x)$ per a tot x de $[a, b]$.

Teorema 5.2.19 (Teorema de Bolzano-Weierstrass)**.** *Successió acotada té parcial convergent*

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

$$1_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

5.3.1 Complexos

Definició 5.3.5 (Nombre complex)**.** Siguin a i b dos nombres reals, i una constant que satisfà $\mathrm{i}^2 = -1$ i

$$z = a + b\mathrm{i}.$$

Aleshores direm que z és un nombre complex i que i és la unitat imaginària.

Definició 5.3.6 (Norma d'un nombre complex)**.** Sigui $z = a + b\mathrm{i}$ un nombre complex. Aleshores definim la seva norma com

$$|z| = \sqrt{a^2 + b^2}.$$

Definició 5.3.7 (Conjugat d'un nombre complex)**.** Sigui $z = a + b\mathrm{i}$ un nombre complex. Aleshores definim

$$\overline{z} = a - b\mathrm{i}$$

com el conjugat de z.

Proposició 5.3.8. *Sigui z un nombre complex. Aleshores es satisfà*

$$|z| = \sqrt{z\overline{z}}.$$

Demostració. □

Definició 5.3.9 (Part real i part imaginària d'un nombre complex)**.** Sigui $z = a + b\mathrm{i}$ un nombre complex. Aleshores definim

$$\Re(z) = a$$

com la part real de z i

$$\Im(z) = b$$

com la part imaginària de z.

Definició 5.3.10 (Integral d'una funció complexa)**.** Sigui f una funció complexa i a i b dos reals. Aleshores definim

$$\int_a^b f(x)\mathrm{d}x = \int_a^b \Re(f(x))\mathrm{d}x + \mathrm{i}\int_a^b \Im(f(x))\mathrm{d}x$$

com la integral de f.

Definició 5.3.11 (Unió disjunta)**.** Siguin A i B dos conjunts. Aleshores definim

$$A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$$

com la unió disjunta entre A i B.

Definició 5.3.12 (Vectors perpendiculars)**.**

$$\langle \vec{u}, \vec{v} \rangle = 0.$$

5.4 Equacions diferencials ordinàries I

5.4.1 Teoria qualitativa

Observació 5.4.1. *Sigui*
$$\dot{u}(t) = X(u(t))$$
una equació diferencial autònoma sobre un obert $\mathcal{U} \subseteq \mathbb{R}^n$ *amb* $X \in \mathcal{C}^1$. *Aleshores la funció* X *és un camp vectorial.*

Definició 5.4.2 (Òrbites)**.** Sigui φ una solució d'una equació diferencial autònoma
$$\dot{u}(t) = X(u(t))$$
on $X \in \mathcal{C}^1$. Aleshores direm que φ és una òrbita de l'equació diferencial $\dot{u}(t) = X(u(t))$.

Proposició 5.4.3. *Siguin*
$$\dot{u}(t) = X(u(t))$$
una equació diferencial autònoma sobre un obert $\mathcal{U} \subseteq \mathbb{R}^n$ *amb* $X \in \mathcal{C}^1$ *i* $x \in \mathcal{U}$ *un punt. Aleshores existeix una solució maximal* φ_x *tal que* $\varphi_x(0) = x$.

Demostració. Considerem el problema de Cauchy
$$\begin{cases} \dot{u}(t) = X(u(t)) \\ u(0) = x. \end{cases}$$

Aleshores per la proposició 20.2.20 tenim que existeix una solució maximal φ_x d'aquest problema de Cauchy, i per la definició de problema de Cauchy (20.2.4) trobem que $\varphi_x(0) = x$ i hem acabat. □

Definició 5.4.4 (Flux)**.** Siguin
$$\dot{u}(t) = X(u(t))$$
una equació diferencial autònoma sobre un obert $\mathcal{U} \subseteq \mathbb{R}^n$ amb $X \in \mathcal{C}^1$, $x \in \mathcal{U}$ un punt i φ_x la solució maximal tal que $\varphi_x(0) = x$. Aleshores direm que φ_x és el flux de x.

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 Γ el conjunt definit per

$$\Gamma = \{f(t) \in \mathbb{R}^m \mid t \in (a,b)\},$$

aleshores direm que Γ 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 Γ és un arc continu si f és contínua en (a,b).
2. Direm que Γ 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 Γ és un arc tancat.
4. Direm que Γ és un arc regular si f és derivable en (a,b).
5. Direm que Γ 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 Γ un arc continu i f una manera de recórrer Γ 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 (5.2.5)

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\|.$$

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* Γ *un arc de classe* $\mathcal{C}^1$*. Aleshores* Γ *és rectificable.*

Demostració. Sigui f una funció que recorre Γ tal que

$$\begin{aligned} f\colon (a,b) \subseteq \mathbb{R} &\longrightarrow \mathbb{R}^m \\ t &\longmapsto (x_1(t), \ldots, x_m(t)). \end{aligned}$$

Donada una partició de (a,b), $a = t_0 < \cdots < t_n = b$ que defineix una poligonal $P_n = f(t_0), \ldots, f(t_n)$. Aleshores la longitud de la poligonal és, per la definició de partició (5.2.5),

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\| = \sum_{i=0}^{n-1} \sqrt{\sum_{j=1}^{m} (x_j(t_{i+1}) - x_j(t_i))^2}\,.$$

Per la proposició 5.2.9 f és contínua en (a,b), i per tant pel Teorema del Valor Mig (5.2.12) tenim

$$x_j(t_{i+1}) - x_j(t_i) = x_j'(\xi_{i,j})(t_{i+1} - t_i),$$

amb $t_i < \xi_{i,j} < t_{i+1}$, per a tot $i \in \{0, \ldots, n-1\}$, $j \in \{1, \ldots, m\}$. Per tant

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{m} \left(x_j'(\xi_{i,j})\right)^2}\,. \tag{6.1}$$

Ara volem veure que $\xi_{i,j} = t_i$ quan n tendeix a infinit. Observem que

$$\lim_{n\to\infty} t_i = \lim_{n\to\infty} t_{i+1}.$$

I com que $t_i < \xi_{i,j} < t_{i+1}$ tenim que $\xi_{i,j} = t_i$ per a tot $j \in \{1, \ldots, m\}$. Així veiem que si $n \to \infty$ podem reescriure (6.1) com

$$\mathrm{L}(P_n) = \lim_{n\to\infty} \sum_{i=0}^{n-1} (t_{i+1} - t_i) \|f'(t_i)\| = \int_a^b \|f'(t)\| \mathrm{d}t.$$

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 Γ 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

$$\begin{aligned}
\mathrm{d}_U(P,Q) &= \inf_{f \in F} \mathrm{L}(f) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{i,j})\right)^2} \right) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (-1)(t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{i,j})\right)^2} \right) \\
&= \inf_{f \in F} (-1) \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{i,j})\right)^2} \right) \\
&= \inf_{f \in F} (-1) \int_a^b \|f'(t)\| \mathrm{d}t \\
&= \inf_{f \in F} \int_b^a \|f'(t)\| \mathrm{d}t = \inf_{f \in F} \mathrm{L}(f) = \mathrm{d}_U(Q,P) \geq 0.
\end{aligned}$$

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

$$\begin{aligned} f\colon U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \dots, f_m(a)), \end{aligned}$$

i considerem, per a tot $i \in \{1, \dots, m\}$, 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

$$D_{\vec{u}} f(a) = (D_{\vec{u}} f_1(a), \dots, D_{\vec{u}} f_m(a)).$$

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 $i \in \{1, \dots, m\}$,

$$\begin{aligned} D_{\lambda\vec{u}} f_i(a) &= \lim_{t \to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{t} \\ &= \lim_{t \to 0} \lambda \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} \\ &= \lambda \lim_{t \to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} = \lambda D_{\vec{u}} f_i(a). \end{aligned}$$

□

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 $\mathbb{R}^d$

$$f(a + \vec{h}) = f(a) + df(a)(\vec{h}) + o(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Com que $df(a)$ és lineal, $df(a)(\vec{h}) \to (0, \dots, 0) \iff \|\vec{h}\| \to 0$. Així veiem que

$$\lim_{\|\vec{h}\| \to 0} f(a + \vec{h}) - f(a) - df(a)(\vec{h}) = o(\vec{h}).$$

I això compleix la definició de funció contínua (5.2.4), per tant f és contínua en el punt a. $\square$

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

$$f \text{ és diferenciable en } a \iff f_i \text{ és diferenciable en } a \text{ per a tot } i \in \{1, \dots, m\}.$$

Demostració. Per la definició de diferencial d'una funció (6.2.3) tenim que, per a qualsevol vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a + \vec{h}) = f(a) + df(a)(\vec{h}) + o(\vec{h}), \quad \|\vec{h}\| \to 0.$$

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. $\square$

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 λ, μ, $D_{\lambda\vec{u}+\mu\vec{v}}f(a) = \lambda D_{\vec{u}}f(a) + \mu D_{\vec{v}}(a)$.*

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 (5.2.12) per a funcions d'una variable i tenim que, per a tot $2 \leq k \leq d$ existeix un escalar ξ_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 ξ_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. $\square$

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

$$\begin{aligned}
\langle \nabla f(a), \vec{u} \rangle &= u_1 D_1 f(a) + \dots + u_d D_d f(a) && \text{(gradient d'una funció (6.2.18))}\\
&= D_{u_1 \vec{e}_1} f(a) + \dots + D_{u_d \vec{e}_1} f(a) && \text{(derivada direccional (6.2.1))}\\
&= D_{u_1 \vec{e}_1 + \dots + u_d \vec{e}_1} f(a) && \text{(Observació 6.2.8)}\\
&= D_{\vec{u}} f(a),
\end{aligned}$$

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 si i només si $\vec{u} = \lambda \nabla f(a)$, amb $\lambda \in \mathbb{R}$.*

Demostració. Pel Teorema de la Desigualtat de Cauchy-Schwarz (5.2.13) 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 d'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 Φ, Φ^{-1} siguin contínues. Aleshores direm que Φ és un homeomorfisme. Si pensem Φ com

$$\begin{aligned} \Phi\colon U &\longleftrightarrow V \\ a &\longmapsto (v_1(a), \dots, v_d(a)) \end{aligned}$$

aleshores donat un punt $a \in U$, interpretem $v_1(a), \dots, v_d(a)$ 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

$$\{x \in U \mid v_i(x) = v_j(a) \iff i \neq j, \text{ per a tot } i, j \in \{1, \dots, d\}\},$$

que són tots els punts amb totes les coordenades iguals, excepte la j-èsima.

Si Φ, Φ^{-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 Φ és diferenciable en un punt $a \in U$. Aleshores per la definició de difeomorfisme (6.2.27) tenim que Φ^{-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 Φ un difeomorfisme diferenciable en un punt $a \in U$. Aleshores*

$$\det(d\Phi(a)) \neq 0.$$

Definició 6.2.30 (Derivades parcials d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $a = (a_1, \dots, a_d)$ un punt de U i f una funció definida per

$$\begin{aligned} f\colon U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \dots, f_m(a)). \end{aligned}$$

Aleshores, donat un $t \in \mathbb{R}$, direm que la derivada parcial de f respecte la seva i-èsima coordenada és

$$\frac{\partial f}{\partial x_i}(a) = \lim_{t \to 0} \frac{f(a_1, \dots, a_i + t, \dots, a_d) - f(a)}{t}.$$

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 $a \in U$, $\Phi(a) = (\Phi_1(a), \dots, \Phi_d(a)) = (v_1, \dots, v_d)$. 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 $v_1, \dots, v_k\colon U \to \mathbb{R}$ k funcions, direm que f depèn funcionalment de $v_1, \dots, v_k$ si existeix una funció $h\colon \mathbb{R}^k \to \mathbb{R}^m$ tal que

$$f(x) = h(v_1(x), \dots, v_k(x)), \quad \text{per a tot } x \in U.$$

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 ($\Longrightarrow$) està vista a la proposició 6.3.2. Fem l'altre implicació ($\Longleftarrow$). Per l'observació 6.2.20, el subespai generat pels gradients $\nabla v_1(x), \ldots, \nabla v_k(x)$ 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, $f(x) = (k_1, \ldots, k_m)$ per a tot $x \in U$ tal que $f(x) \in M$. Aleshores existeix una funció $H\colon U \to M$ tal que

$$f(x) = H(v_1(x), \ldots, v_k(x)).$$

□

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 ($\Longrightarrow$). 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 ($\Longleftarrow$). 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

$$\left\|df(a)^{-1}(\vec{k})\right\| + \left\|df(a)^{-1}(\mathrm{o}(\vec{h}))\right\| \leq \|df(a)^{-1}\|\left\|\vec{k}\right\| + \|df(a)^{-1}\|\left\|\mathrm{o}(\vec{h})\right\|.$$

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 $\mathrm{o}(\vec{k})$. □

Lema 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 (5.2.11) 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* $\implies$ *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 (5.2.12) 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

$$\frac{m}{2}\|x-y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x-y\|.$$

□

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 lema 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

$$\sum_{i=1}^{d} D_j f_i(p)(p_i - f_i(q)) = 0, \quad \text{per a tot } j \in \{1, \ldots, d\}.$$

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. $\square$

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. $\square$

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 $v_1(a) = \dots = v_k(a) = 0$ i els seus gradients en a, $\nabla v_1(a), \dots, \nabla v_k(a)$ són linealment independents i M un conjunt definit per $M = \{x \in U \mid v_1(x) = \dots = v_k(x) = 0\}$. 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*

$$\begin{aligned} M &= \{x \in U \mid v_1(x) = \dots = v_k(x) = 0\} = \\ &= \{x = (x'; x'') \in W \mid x' = h(x''), x'' \in U''\}. \end{aligned}$$

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 Φ 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 Φ 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 Φ 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 Φ 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 φ_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 Φ 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 Φ 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 $u_1, \ldots, u_d$ 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 Φ defineix un sistema de coordenades, per la proposició 6.3.2 els gradients de $u_1, \ldots, u_d$ 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, $\vec{v}_1, \ldots, \vec{v}_n$ 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

$$d^n f(a)(\vec{v}_n \ldots \vec{v}_1) = \frac{\partial^n f}{\partial \vec{v}_n \cdots \partial \vec{v}_1} = D_{\vec{v}_n, \ldots, \vec{v}_1} f(a).$$

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 $f(x) = (f_1(x), \ldots, f_m(x))$, on $f_1, \ldots, f_m$ 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 (5.2.12) 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,

$$D_1 f(x,y) = D_1 f(0,0) + x D_{1,1} f(0,0) + y D_{2,1} f(0,0) + \mathrm{o}(\|x,y\|).$$

Ho apliquem a (6.6) i obtenim

$$\begin{aligned} hA'(c) = h\big(&D_1 f(0,0) + \xi D_{1,1} f(0,0) + \\ &+ h D_{2,1} f(0,0) - D_1 f(0,0) - \xi D_{1,1} f(0,0) + \mathrm{o}(h)\big) \end{aligned}$$

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

$$D_{2,1} f(0,0) = D_{1,2} f(0,0).$$ □

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, $f(x) = (f_1(x), \dots, f_m(x))$, 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, $t = (t_1, \dots, t_d)$. Introduïm la següent notació:

$$f^{(k)}[a,t] = \sum_{i_k=1}^{d} \cdots \sum_{i_1=1}^{d} D_{i_k,\dots,i_1} f(a) t_{i_1} \dots t_{i_k}.$$

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 (5.2.14) 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 $\implies$ a és un mínim relatiu.*
2. *$d^2 f(a)$ és definida estrictament negativa $\implies$ a és un màxim relatiu.*
3. *$d^2 f(a)$ és definida positiva $\impliedby$ a és un mínim relatiu.*
4. *$d^2 f(a)$ és definida negativa $\impliedby$ 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 (5.2.15) 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 $o(t) \to 0$ és si i només si $t \to 0$, existeix un $\varepsilon > 0$ tal que, amb $0 < \|t\| < \varepsilon$ tenim $o(t) < \frac{m}{2}$, i $0 \leq \|t\|^2 o(t) < \frac{m}{2}\|t\|^2$, 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 d'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

$$f(a+t) - f(a) \leq m\|t\|^2 + \|t\|^2 o(t).$$

Aleshores

$$\frac{f(a+t) - f(a)}{\|t\|^2} \leq m + o(t).$$

Per la definició d'extrem relatiu (6.2.23) tenim $f(a+t) - f(a) \geq 0$, i per tant, quan $t \to 0$, aleshores $o(t) \to 0$ 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 i 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

$$\begin{aligned}\sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| &= \sum_{i \in I \setminus I'} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| + \sum_{i' \in I'} \inf_{x \in \mathfrak{R}_{i'}} f(x) |\mathfrak{R}_{i'}| \leq \\ &\leq \sum_{j \in J} \inf_{x \in \mathfrak{R}_j} f(x) |\mathfrak{R}_j| + \sum_{i \in I \setminus J} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| = \sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|.\end{aligned}$$

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*

$$\int_{\mathfrak{R}^-} f \leq \int^{\mathfrak{R}^+} f.$$

Demostració. Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Com que, per la proposició 7.1.5, tenim $\mathrm{s}(f,P)\leq \mathrm{S}(f,Q)$ per a $P,Q\in\mathcal{P}$ arbitraris, ha de ser

$$\int_{\mathfrak{R}^-} f = \sup_{P\in\mathcal{P}} \mathrm{s}(f,P) \leq \inf_{P\in\mathcal{P}} \mathrm{S}(f,P) = \int^{\mathfrak{R}^+} f. \qquad \square$$

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 ($\Longrightarrow$). 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 $\mathrm{s}(f,P)\leq \mathrm{s}(f,P\cup Q)\leq \mathrm{S}(f,P\cup Q)\leq \mathrm{S}(f,Q)$, 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 ($\Longleftarrow$) veiem que, per hipòtesi,

$$0\leq \int^{\mathfrak{R}^+} f - \int_{\mathfrak{R}^-} f \leq \mathrm{S}(f,P)-\mathrm{s}(f,P)<\varepsilon,$$

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 δ.

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 (5.2.15) 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 ξ_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 (5.2.16) 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

$$\int_{\mathfrak{R}} f(x)\mathrm{d}x = \Sigma(f,P_n) = \sum_{i\in I} f(x)|\mathfrak{R}_i| = L.$$

on $\int$ es refereix al sumatori infinit, $f(\xi_i)$ es transforma en $f(x)$ i $|\mathfrak{R}_i|$ s'escriu $\mathrm{d}x$, 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 λ, μ 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 ξ_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 ξ_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 ($\Longleftrightarrow$). 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

$$\int_{\mathfrak{R}}|f| \leq \int_{\mathfrak{R}} M = M|\mathfrak{R}|.$$ □

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 δ 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. □

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 (5.2.4). $\square$

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, τ 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 τ d'una funció.

Observació 7.2.4. *D_τ 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 zero, és a dir, $c(D_\tau) = 0$ per a tot $\tau > 0$.*

Demostració. Comencem amb la implicació cap a l'esquerra ($\Longleftarrow$). 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 ($\Longrightarrow$). 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. $\square$

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

Anàlisi matemàtica

Capítol 9

Sèries

9.1 Sèries numèriques

9.1.1 Convergència d'una sèrie numèrica

Definició 9.1.1 (Sèrie numèrica)**.** Sigui $(a_n)_{n\in\mathbb{N}}$ una successió de nombres reals. Aleshores direm que

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + \cdots$$

és una sèrie numèrica o la sèrie de (a_n).

Definició 9.1.2 (Sèrie convergent)**.** Siguin $\sum_{n=1}^{\infty} a_n$ una sèrie numèrica i

$$S_N = \sum_{n=1}^{N} a_n$$

una successió tals que

$$\lim_{n\to\infty} S_n = L$$

on L és un nombre real. Aleshores direm que la sèrie $\sum_{n=1}^{\infty} a_n$ és una sèrie convergent amb valor L.

Si L no és un nombre real direm que la sèrie $\sum_{n=1}^{\infty} a_n$ és una sèrie divergent.

Exemple 9.1.3 (Sèries geomètriques)**.** *Sigui $r \neq 0$ un nombre real. Volem estudiar la convergència de la sèrie*

$$\sum_{n=0}^{\infty} r^n. \tag{9.1}$$

Solució. Observem que si $r = 1$, per la definició de límit (5.2.3), el límit

$$\lim_{N\to\infty} \sum_{n=0}^{N} 1^n = N$$

és divergent, i per la definició de sèrie convergent (9.1.2) tenim que la sèrie

$$\sum_{n=0}^{\infty} 1^n$$

és divergent.

Estudiem ara el cas $r \neq 1$. Tenim que $\sum_{n=0}^{N} r^n = r^0 + r^1 + r^2 + \cdots + r^N$, i per tant

$$\begin{aligned}(1-r)\sum_{n=0}^{N} r^n &= (1-r)(r^0 + r^1 + r^2 + \cdots + r^N)\\ &= r^0 + r^1 + r^2 + \cdots + r^N - (r^1 + r^2 + r^3 + \cdots + r^{N+1})\\ &= 1 - r^{N+1}\end{aligned}$$

i trobem

$$\sum_{n=0}^{N} r^n = \frac{1 - r^{N+1}}{1-r}.$$

Per tant tenim

$$\lim_{N\to\infty} \sum_{n=0}^{N} r^n = \begin{cases} \dfrac{1}{1-r} & \text{si } -1 < r < 1\\ +\infty & \text{si } r \geq 1\\ \text{no existeix} & \text{si } r \leq -1 \end{cases}$$

i per la definició de sèrie convergent (9.1.2) trobem que (9.1) és convergent si i només si r pertany a l'interval $(-1, 1)$, i si r pertany a l'interval $(-1, 1)$ aleshores es compleix

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}. \qquad \Diamond$$

Teorema 9.1.4 (Condició de Cauchy)**.** *Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie numèrica. Aleshores $\sum_{n=0}^{\infty} a_n$ és convergent si i només si per a tot $\varepsilon > 0$ existeix un n_0 natural tal que per a tot N i M naturals amb $N,M \geq n_0$ i $N \leq M$ tenim*

$$\left| \sum_{n=N}^{M} a_n \right| < \varepsilon.$$

Demostració. Suposem que $\sum_{n=0}^{\infty} a_n$ és convergent. Per la definició de sèrie convergent (9.1.2) això és que

$$\lim_{N\to\infty} \sum_{n=1}^{N} a_n = L$$

on L és un nombre real.

Per la definició de límit (5.2.3) tenim que per a tot $\delta_1 > 0$ real existeix un N tal que

$$\left| \sum_{n=1}^{N-1} a_n - L \right| < \delta_1$$

i de nou per la definició de límit (5.2.3) tenim que per a tot $\varepsilon > 0$ real existeix un $\delta_2 > 0$ real tal que $\delta_1 - \delta_2 < \varepsilon$ i que existeix un M natural satisfent

$$\left|\sum_{n=1}^{M} a_n - L\right| < \delta_2.$$

Per tant trobem

$$\left|\sum_{n=1}^{N-1} a_n - L\right| - \left|\sum_{n=1}^{M} a_n - L\right| < \delta_1 - \delta_2$$

i per la desigualtat triangular tenim que

$$\begin{aligned}
\left|\sum_{n=N}^{M} a_n\right| &= \left|\sum_{n=1}^{N-1} a_n - \sum_{n=1}^{M} a_n\right| \\
&= \left|\sum_{n=1}^{N-1} a_n - L - \sum_{n=1}^{M} a_n + L\right| \\
&\leq \left|\sum_{n=1}^{N-1} a_n - L\right| - \left|\sum_{n=1}^{M} a_n - L\right| \\
&< \delta_1 - \delta_2 < \varepsilon.
\end{aligned}$$

□

Corol·lari 9.1.5. *Sigui $\sum_{n=1}^{\infty} a_n$ una sèrie convergent. Aleshores*

$$\lim_{n\to\infty} a_n = 0.$$

Demostració. Per la condició de Cauchy (9.1.4) tenim que per a tot $\varepsilon > 0$ existeix un n_0 natural tal que per a tot N i M naturals amb $N,M \geq n_0$ tenim

$$\left|\sum_{n=N}^{M} a_n\right| < \varepsilon.$$

En particular, si triem $M = N + 1$, tenim $|a_n| < \varepsilon$ per a tot $n > n_0$, i per la definició de límit (5.2.3) veiem que $\lim_{n\to\infty} a_n = 0$, com volíem veure. □

Exemple 9.1.6 (Sèrie harmònica)**.** *Sigui α un nombre real. Volem estudiar la convergència de la sèrie*

$$\sum_{n=1}^{\infty} \frac{1}{n^{\alpha}}. \tag{9.2}$$

Solució. Observem que si $\alpha \leq 0$ tenim que

$$\lim_{n\to\infty} \frac{1}{n^{\alpha}} = \infty$$

i pel corol·lari 9.1.5 tenim que la sèrie és divergent.

Suposem que $0 < \alpha \leq 1$. Definim la successió

$$S_N = \sum_{n=1}^{N} \frac{1}{n^{\alpha}}$$

i tenim que

$$\begin{aligned} S_{2^N} &= 1 + \frac{1}{2^\alpha} + \frac{1}{3^\alpha} + \cdots + \frac{1}{2^{N\alpha}} \\ &\geq 1 + \frac{1}{2^\alpha} + \frac{2}{4^\alpha} + \cdots + \frac{2^{N-1}}{2^{N\alpha}} \\ &= 1 + \sum_{n=0}^{N-1} \frac{2^n}{2^{(n+1)\alpha}} = 1 + \frac{1}{2^\alpha} \sum_{n=0}^{N-1} 2^{n(1-\alpha)}. \end{aligned}$$

Ara bé, tenim que $1 - \alpha \geq 0$, i per tant trobem

$$\lim_{N\to\infty} 1 + \frac{1}{2^\alpha} \sum_{n=0}^{N-1} 2^{n(1-\alpha)} = \infty,$$

i tenim que $\lim_{N\to\infty} S_{2^N} = \infty$ i per la definició de sèrie divergent (9.1.2) trobem que $\sum_{n=1}^{\infty} \frac{1}{n^\alpha}$ és divergent.

Veiem ara el cas $\alpha > 1$. Definim de nou la successió

$$S_N = \sum_{n=1}^{N} \frac{1}{n^\alpha}.$$

Tenim que

$$\begin{aligned} S_{2^N} &= 1 + \frac{1}{2^\alpha} + \frac{1}{3^\alpha} + \cdots + \frac{1}{2^{N\alpha}} \\ &\leq 1 + \frac{1}{2^\alpha} + \frac{2}{4^\alpha} + \cdots + \frac{2^{N-1}}{2^{N\alpha}} \\ &= \frac{1}{2^{N\alpha}} + \sum_{n=0}^{N-1} \frac{2^n}{2^{n\alpha}} \\ &= \frac{1}{2^{N\alpha}} + \sum_{n=0}^{N-1} 2^{(1-\alpha)n} \\ &= \frac{1}{2^{N\alpha}} + \frac{1 - 2^{(1-\alpha)N}}{1 - 2^{1-\alpha}} \end{aligned} \tag{9.1.3}$$

i tenim que

$$\lim_{N\to\infty} \frac{1}{2^{N\alpha}} + \frac{1 - 2^{(1-\alpha)N}}{1 - 2^{1-\alpha}} = \frac{1}{1 - 2^{1-\alpha}}.$$

Per tant tenim que la successió (S_N) està fitada, i degut a que $S_{N+1} = S_N + \frac{1}{(N+1)^\alpha}$ tenim que és creixen i pel Teorema de Weierstrass (5.2.15) tenim que és convergent. Per tant per la definició de sèrie convergent (9.1.2) tenim que la sèrie (9.2) és convergent.

Per tant tenim que la sèrie

$$\sum_{n=1}^{\infty} \frac{1}{n^\alpha}$$

és convergent si i només si $\alpha > 1$. ♢

9.1.2 Sèries de termes positius

Definició 9.1.7 (Sèrie de termes positius)**.** Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie numèrica tal que $a_n > 0$ per a tot n natural. Aleshores direm que $\sum_{n=0}^{\infty} a_n$ és una sèrie de termes positius.

Notació 9.1.8. Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius. Aleshores escriurem $\sum_{n=0}^{\infty} a_n < \infty$ si $\sum_{n=0}^{\infty} a_n$ és convergent i $\sum_{n=0}^{\infty} a_n = \infty$ si $\sum_{n=0}^{\infty} a_n$ és divergent

Lema 9.1.9. *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius, $\sum_{n=0}^{\infty} b_n$ una sèrie de termes positius convergent, K un nombre real i n_0 un natural tal que per a tot $n > n_0$ es satisfà $a_n \leq K b_n$. Aleshores tenim que $\sum_{n=0}^{\infty} a_n$ és convergent.*

Demostració. Tenim que

$$\begin{aligned}\sum_{n=0}^{N} a_n &= \sum_{n=0}^{n_0-1} a_n + \sum_{n=n_0}^{N} a_n \\ &\leq \sum_{n=0}^{n_0-1} a_n + K \sum_{n=n_0}^{N} b_n\end{aligned}$$

i per la definició de sèrie convergent (9.1.2) tenim que la sèrie $K \sum_{n=n_0}^{N} b_n$ és convergent i, de nou per la definició de sèrie convergent (9.1.2), tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent, com volíem veure. □

Teorema 9.1.10 (Criteri de comparació)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ i $\sum_{n=0}^{\infty} b_n$ dues sèries de termes positius i*

$$\lim_{n\to\infty} \frac{a_n}{b_n} = L$$

tals que

1. *$L \neq 0$ i $L \neq \infty$. Aleshores $\sum_{n=0}^{\infty} a_n$ és convergent si i només si $\sum_{n=0}^{\infty} b_n$ és convergent.*
2. *$L = 0$ i $\sum_{n=0}^{\infty} b_n$ és convergent. Aleshores $\sum_{n=0}^{\infty} a_n$ és convergent.*
3. *$L = \infty$ i $\sum_{n=0}^{\infty} a_n$ és convergent. Aleshores $\sum_{n=0}^{\infty} b_n$ és convergent.*

Demostració. Comencem veient el punt (1). Suposem que $L \neq 0$ ó $L \neq \infty$. Observem que $L > 0$. Per tant prenem un $\varepsilon > 0$ tal que $L - \varepsilon > 0$. Per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà

$$\left| \frac{a_n}{b_n} - L \right| < \varepsilon.$$

Per tant tenim que per a tot $n > n_0$

$$l - \varepsilon < \frac{a_n}{b_n} < l + \varepsilon.$$

Suposem que $\sum_{n=0}^{\infty} b_n$ és convergent. Aleshores tenim

$$b_n(l - \varepsilon) < a_n < b_n(l + \varepsilon),$$

i pel lema 9.1.9 trobem que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.

Suposem ara que $\sum_{n=0}^{\infty} a_n$ és convergent. Aleshores tenim

$$\frac{a_n}{L-\varepsilon} < b_n < \frac{a_n}{L+\varepsilon},$$

i pe lema 9.1.9 trobem que la sèrie $\sum_{n=0}^{\infty} b_n$ és convergent.

Veiem ara el punt (2). Suposem doncs que $L = 0$ i que $\sum_{n=0}^{\infty} b_n$ és convergent. Per la definició de límit (5.2.3) tenim que per a tot $\varepsilon > 0$ existeix un natural n_0 tal que

$$\left|\frac{a_n}{b_n}\right| < \varepsilon,$$

i això és equivalent a

$$a_n < \varepsilon b_n$$

i pel lema 9.1.9 trobem que la sèries $\sum_{n=0}^{\infty} a_n$ és convergent.

Veiem ara el punt (3). Suposem doncs que $L = \infty$ i que $\sum_{n=0}^{\infty} a_n$ és convergent. Tenim que

$$\lim_{n\to\infty} \frac{b_n}{a_n} = 0,$$

i per tant pel punt (2) tenim que $\sum_{n=0}^{\infty} b_n$ és convergent. □

Exemple 9.1.11. *Considerem la sèrie*

$$\sum_{n=1}^{\infty} \left(1+\frac{1}{n}\right)^3 3^{-n}.$$

Volem estudiar si aquesta sèrie és convergent o divergent.

Solució. Definim

$$a_n = \left(1+\frac{1}{n}\right)^3 3^{-n} \quad \text{i} \quad b_n = \frac{1}{3^n}$$

Observem que per a tot n natural tenim $a_n > 0$ i $b_n > 0$, i per la definició de sèrie de termes positius (9.1.7) tenim que les sèries $\sum_{n=0}^{\infty} a_n$ i $\sum_{n=0}^{\infty}$ són sèries de termes positius.

Considerem el límit

$$\begin{aligned}\lim_{n\to\infty} \frac{a_n}{b_n} &= \lim_{n\to\infty} \frac{\left(1+\frac{1}{n}\right)^3 3^{-n}}{3^{-n}}\\ &= \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^3 = 1.\end{aligned}$$

Ara bé, per l'exercici 9.1.3 tenim que la sèrie $\sum_{n=0}^{\infty} \frac{1}{3^n}$ és convergent, ja que $-1 < \frac{1}{3} < 1$, i pel criteri de comparació de sèries de termes positius (9.1.10) trobem que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent. ◊

9.1.3 Criteris de convergència

Proposició 9.1.12 (Criteri de l'arrel)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius i*

$$\lim_{n\to\infty} \sqrt[n]{a_n} = L$$

tal que

1. *$L < 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.*
2. *$L > 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent.*

Demostració. Comencem veient el punt (1). Suposem doncs que $L < 1$. Prenem un $\varepsilon > 0$ tal que $L + \varepsilon < 1$. Per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà

$$|\sqrt[n]{a_n} - L| < \varepsilon,$$

i per tant per a tot $n > n_0$ tenim

$$\sqrt[n]{a_n} < L + \varepsilon,$$

i per tant

$$a_n < (L + \varepsilon)^n.$$

Ara bé, tenim que $L+\varepsilon < 1$, per tant per l'exercici 9.1.3 tenim que $\sum_{n=0}^{\infty}(L+\varepsilon)^n$ és convergent, i per tant pel lema 9.1.9 tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.

Veiem ara el punt (2). Suposem doncs que $L > 1$. Prenem $\varepsilon > 0$ tal que $L - \varepsilon > 1$. Per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà

$$|\sqrt[n]{a_n} - L| < \varepsilon,$$

i per tant

$$L - \varepsilon < \sqrt[n]{a_n}.$$

Ara bé, tenim que $L - \varepsilon > 1$, per tant per l'exercici 9.1.3 tenim que la sèrie $\sum_{n=0}^{\infty}(L-\varepsilon)^n$ és divergent, i per tant pel lema 9.1.9 tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent. $\square$

Exemple 9.1.13. *Siguin $\alpha \geq 0$ i $\beta \geq 0$ dos reals. Considerem la sèrie numèrica*

$$\sum_{n=1}^{\infty} n^\beta \alpha^n.$$

Volem estudiar la convergència d'aquesta sèrie en funció dels valors de α i β.

Solució. Definim

$$a_n = n^\beta \alpha^n.$$

Observem primer que $a_n > 0$ per a tot n natural. Per tant per la definició de sèrie de termes positius (9.1.7) tenim que $\sum_{n=1}^{\infty} a_n$ és una sèrie de termes positius. Veiem també que si $\alpha = 1$ tenim

$$\sum_{n=1}^{\infty} n^\beta,$$

i com que $\beta \geq 0$ la sèrie és divergent.

Considerem el límit

$$\begin{aligned}\lim_{n\to\infty} \sqrt[n]{a_n} &= \lim_{n\to\infty} \sqrt[n]{n^\beta \alpha^n}\\ &= \lim_{n\to\infty} \sqrt[n]{n^\beta}\,\sqrt[n]{\alpha^n}\\ &= \lim_{n\to\infty} \sqrt[n]{n}^{\beta}\alpha = \alpha.\end{aligned}$$

Per tant, pel criteri de l'arrel (9.1.12) tenim que la sèrie és convergent quan $\alpha > 1$ i divergent quan $\alpha \leq 1$. ♢

Proposició 9.1.14 (Criteri del quocient)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius i*

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = L$$

tal que

1. *$L < 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.*
2. *$L > 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent.*

Demostració. Comencem veient el punt (1). Suposem doncs que $L < 1$. Prenem un $\varepsilon > 0$ tal que $L + \varepsilon < 1$. Aleshores per la definició de límit (5.2.3) tenim que existeix un n_0 tal que per a tot $n > n_0$ es satisfà

$$\left|\frac{a_{n+1}}{a_n} - L\right| < \varepsilon,$$

i per tant per a tot $n > n_0$ tenim

$$\frac{a_{n+1}}{a_n} < L + \varepsilon,$$

i per tant

$$a_{n+1} < (L+\varepsilon)a_n$$

i trobem

$$\begin{aligned}a_{n+1} &< (L+\varepsilon)a_n\\ &< (L+\varepsilon)^2 a_{n-1}\\ &\ \ \vdots\\ &< (L+\varepsilon)^{n-n_0+1}a_{n_0}.\end{aligned}$$

Ara bé, com que $L + \varepsilon < 1$ tenim per l'exemple 9.1.3 que la sèrie $\sum_{n=0}^{\infty}(L+\varepsilon)^n$ és convergent, i pel lema 9.1.9 trobem que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.

Veiem ara el punt (2). Suposem doncs que $L > 1$. Prenem un $\varepsilon > 0$ tal que $L - \varepsilon > 1$. Aleshores per la definició de límit (5.2.3) tenim que existeix un n_0 natural tal que per a tot $n > n_0$ es satisfà

$$\left|\frac{a_{n+1}}{a_n} - L\right| < \varepsilon,$$

i per tant per a tot $n > n_0$ tenim

$$L - \varepsilon < \frac{a_{n+1}}{a_n}$$

i per tant

$$(L - \varepsilon)a_n < a_{n+1}$$

i trobem

$$\begin{aligned} a_{n+1} &> (L-\varepsilon)a_n \\ &> (L-\varepsilon)^2 a_{n-1} \\ &\ \ \vdots \\ &> (L-\varepsilon)^{n-n_0+1} a_{n_0}. \end{aligned}$$

Ara bé, com que $L - \varepsilon > 1$ tenim que

$$\lim_{n\to\infty} (L-\varepsilon)^n = \infty,$$

i per tant trobem

$$\lim_{n\to\infty} a_n = \infty$$

i tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent, com volíem veure. □

Lema 9.1.15. *Siguin x i α dos nombres reals no negatius. Aleshores*

$$1 - \frac{\alpha}{x} \leq \left(1 - \frac{1}{x+1}\right)^{\alpha}.$$

Demostració. :(□

Proposició 9.1.16 (Criteri de Raabe)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius i*

$$\lim_{n\to\infty} n\left(1 - \frac{a_{n+1}}{a_n}\right) = L$$

tal que

1. *$L > 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.*
2. *$L < 1$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent.*

Demostració. Comencem veient el cas (1). Suposem doncs que $L > 1$. Prenem un $\varepsilon > 0$ tal que $L - \varepsilon > 1$. Aleshores per la definició de límit (5.2.3) tenim que existeix un n_0 natural tal que per a tot $n > n_0$ es satisfà

$$\left| n\left(1 - \frac{a_{n+1}}{a_n}\right) - L \right| < \varepsilon,$$

i per tant per a tot $n > n_0$ tenim

$$L - \varepsilon < n\left(1 - \frac{a_{n+1}}{a_n}\right),$$

i per tant
$$a_{n+1} < a_n\left(1 - \frac{L-\varepsilon}{n}\right).$$

Aleshores, pel lema 9.1.15 trobem que
$$a_{n+1} < a_n\left(1 - \frac{1}{n+1}\right)^{L-\varepsilon}$$
i tenim
$$a_{n+1} < a_n\left(\frac{n}{n+1}\right)^{L-\varepsilon}. \tag{9.3}$$
Podem aplicar la desigualtat (9.3) recursivament per obtenir
$$\begin{aligned} a_{n+1} &< a_n\left(\frac{n}{n+1}\right)^{L-\varepsilon} \\ &< a_{n-1}\left(\frac{n-1}{n}\frac{n}{n+1}\right)^{L-\varepsilon} \\ &\vdots \\ &< a_{n_0}\left(\frac{n_0}{n_0+1}\frac{n_0+1}{n_0+2}\cdots\frac{n-1}{n}\frac{n}{n+1}\right)^{L-\varepsilon} \end{aligned}$$
i per tant trobem
$$a_{n+1} < a_{n_0}\left(\frac{n_0}{n+1}\right)^{L-\varepsilon},$$
i com que $L - \varepsilon > 1$ trobem per l'exemple 9.1.6 que la sèrie
$$\sum_{n=0}^{\infty}\left(\frac{1}{n+1}\right)^{L-\varepsilon}$$
és convergent, i pel lema 9.1.9 tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.

Veiem ara el punt (2). Suposem doncs que $L < 1$. □

Exemple 9.1.17. *Sigui $\alpha > 0$ un nombre real. Considerem la sèrie numèrica*
$$\sum_{n=1}^{\infty}\frac{\alpha^n n!}{n^n}. \tag{9.4}$$
Volem estudiar la convergència d'aquesta sèrie en funció del valor de α.

Solució. Considerem el límit
$$\begin{aligned} \lim_{n\to\infty}\frac{\frac{\alpha^{n+1}(n+1)!}{(n+1)^{n+1}}}{\frac{\alpha^n n!}{n^n}} &= \lim_{n\to\infty}\frac{\alpha^{n+1}(n+1)!n^n}{\alpha^n n!(n+1)^{n+1}} \\ &= \lim_{n\to\infty}\frac{\alpha(n+1)!n^n}{(n+1)!(n+1)^n} \\ &= \alpha\lim_{n\to\infty}\left(\frac{n}{n+1}\right)^n = \frac{\alpha}{\mathrm{e}} \end{aligned}$$

Per tant, si $\alpha > \mathrm{e}$ tenim que $\frac{\alpha}{\mathrm{e}} > 1$, i pel criteri del quocient (9.1.14) trobem que la sèrie és divergent. Si $\alpha < \mathrm{e}$ aleshores $\frac{\alpha}{\mathrm{e}} < 1$ i pel criteri del quocient (9.1.14) trobem que la sèrie és convergent.

Estudiem el cas $\alpha = \mathrm{e}$. Considerem el límit

$$\begin{aligned}\lim_{n\to\infty} n\left(1-\frac{\frac{\mathrm{e}^{n+1}(n+1)!}{(n+1)^{n+1}}}{\frac{\mathrm{e}^n n!}{n^n}}\right) &= \lim_{n\to\infty} n\left(1-\frac{\mathrm{e}^{n+1}(n+1)!n^n}{e^n n!(n+1)^{n+1}}\right)\\ &= \lim_{n\to\infty} n\left(1-\mathrm{e}\frac{(n+1)!n^n}{(n+1)!(n+1)^n}\right)\\ &= \lim_{n\to\infty} n\left(1-\mathrm{e}\left(\frac{n}{n+1}\right)^n\right)\\ &= \lim_{n\to\infty} n(1-e^2) = -\infty\end{aligned}$$

i pel criteri de Raabe (9.1.16) trobem que la sèrie (9.4) és divergent quan $\alpha = e$.

Per tant la sèrie

$$\sum_{n=1}^{\infty} \frac{\alpha^n n!}{n^n}$$

és convergent si i només si $\alpha < \mathrm{e}$. ♢

Proposició 9.1.18 (Criteri de condensació)**.** *Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius amb $(a_n)_{n\in\mathbb{N}}$ decreixent. Aleshores $\sum_{n=0}^{\infty} a_n$ és convergent si i només si la sèrie $\sum_{n=0}^{\infty} 2^n a_{2^n}$ és convergent.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent i definim

$$S_N = \sum_{n=0}^{N} a_n \quad \text{i} \quad T_N = \sum_{n=0}^{N} 2^n a_{2^n}.$$

Per la definició de sèrie convergent (9.1.2) tenim que existeix un real C tal que per a tot N natural

$$S_N \leq \frac{C}{2} \tag{9.5}$$

Aleshores tenim que la successió T_N és creixent, ja que $(2^n)_{n\in\mathbb{N}}$ és una successió de termes positius creixent i (a_n) és, per hipòtesi, una successió de termes positius.

Veiem ara que $T(N)$ està fitada. Tenim que

$$\begin{aligned}T_N &= 2a_2 + 4x_4 + 8x_6 + \cdots + 2^N a_{2^N}\\ &= 2(a_2 + 2a_4 + 4a_6 + \cdots + 2^{N-1} a_{2^N})\\ &\leq 2(a_2 + (a_3 + a_4) + (a_5 + a_6 + a_7 + a_8) + \cdots + (a_{2^{N-1}} + \cdots + a_{2^N}))\\ &= 2S_{2^N} \leq C & (9.5)\end{aligned}$$

i per tant la successió T_N és creixent i està fitada, i per tant és convergent, i per la definició de sèrie convergent (9.1.2) trobem que la sèrie

$$\sum_{n=0}^{\infty} 2^n a_{2^n}$$

és convergent.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que la sèrie

$$\sum_{n=0}^{\infty} 2^n a_{2^n}$$

és convergent. Definim

$$S_N = \sum_{n=0}^{N} a_n \quad \text{i} \quad T_N = \sum_{n=0}^{N} 2^n a_{2^n},$$

i com que, per hipòtesi, la sèrie $\sum_{n=0}^{\infty} 2^n a_{2^n}$ és convergent tenim que existeix un real C tal que per a tot N es satisfà

$$T(N) \leq C \tag{9.6}$$

Aleshores, com que per hipòtesi la successió a_n és decreixent, tenim que

$$\begin{aligned} S_N &= a_1 + (a_2 + a_3 +) + (a_4 + \cdots + a_7) + \cdots + a_N \\ &\leq a_1 + 2x_2 + 8a_8 + \cdots + 2^N a_N \\ &= a_1 + T(N) \leq a_1 + C. && (9.6) \end{aligned}$$

Per tant tenim que la successió (S_N) és acotada, i com que per hipòtesi la successió (a_n) és una successió de termes positius trobem que la sèrie S_N és creixent, i per tant convergent, i per la definició de sèrie convergent (9.1.2) trobem que la sèrie

$$\sum_{n=0}^{\infty} a_n$$

és convergent, com volíem veure. □

Proposició 9.1.19 (Criteri logarítmic)**.** *Siguin* $\sum_{n=0}^{\infty} a_n$ *una sèrie de termes positius i*

$$\lim_{n\to\infty} \frac{\log\left(\frac{1}{a_n}\right)}{\log(n)} = L$$

tal que

1. $L > 1$. *Aleshores la sèrie* $\sum_{n=0}^{\infty} a_n$ *és convergent.*
2. $L < 1$. *Aleshores la sèrie* $\sum_{n=0}^{\infty} a_n$ *és divergent.*

Demostració. Comencem veient el punt (2). Suposem doncs que $L > 1$. Prenem un $\varepsilon > 0$ tal que $L - \varepsilon > 1$. Aleshores per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà

$$\left| \frac{\log\left(\frac{1}{a_n}\right)}{\log(n)} - L \right| < \varepsilon,$$

i per tant per a tot $n > n_0$ tenim

$$L - \varepsilon < \frac{\log\left(\frac{1}{a_n}\right)}{\log(n)},$$

i per tant
$$(L-\varepsilon)\log(n) < \log\left(\frac{1}{a_n}\right)$$
o, equivalentment,
$$\log\left(n^{L-\varepsilon}\right) < \log\left(\frac{1}{a_n}\right)$$
i tenim que
$$n^{L-\varepsilon} < \frac{1}{a_n}.$$
Per tant,
$$a_n > \frac{1}{n^{L-\varepsilon}}$$
Ara bé, com que per hipòtesi $L-\varepsilon > 1$, per l'exercici 9.1.6 trobem que la sèrie
$$\sum_{n=0}^{\infty} \frac{1}{n^{L-\varepsilon}}$$
és convergent, i pel lemma 9.1.9 trobem que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.

Veiem ara el punt (1). Suposem doncs que $L < 1$. Prenem un $\varepsilon > 0$ tal que $L+\varepsilon < 1$. Per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà
$$\left|\frac{\log\left(\frac{1}{a_n}\right)}{\log(n)} - L\right| < \varepsilon,$$
i per tant trobem que
$$\frac{\log\left(\frac{1}{a_n}\right)}{\log(n)} < \varepsilon + L,$$
o equivalentment,
$$\log\left(\frac{1}{a_n}\right) < (\varepsilon+L)\log(n)$$
i tenim que
$$\log\left(\frac{1}{a_n}\right) < \log\left(n^{\varepsilon+L}\right)$$
i per tant
$$\frac{1}{a_n} < n^{\varepsilon+L}$$
i trobem
$$a_n > \frac{1}{n^{\varepsilon+L}}. \tag{9.7}$$
Ara bé, com que per hipòtesi $L+\varepsilon < 1$, per l'exemple 9.1.6 que la sèrie
$$\sum_{n=0}^{\infty} \frac{1}{n^{L+\varepsilon}}$$
és divergent, i pel lema 9.1.9 i (9.7) tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és divergent. $\square$

Exemple 9.1.20. *Sigui α un real. Volem estudiar per a quins valors de $\alpha > 0$ la sèrie*

$$\sum_{n=1}^{\infty} \frac{1}{\alpha^{\log(n)}} \tag{9.8}$$

és convergent.

Solució. Considerem el límit

$$\begin{aligned}\lim_{n\to\infty} \frac{\log\big(\alpha^{\log(n)}\big)}{\log(n)} &= \lim_{n\to\infty} \frac{\log(n)\log(\alpha)}{\log(n)} \\ &= \log(\alpha) \lim_{n\to\infty} \frac{\log(n)}{\log(n)} = \log(\alpha).\end{aligned}$$

Per tant, pel criteri logarítmic (9.1.19) trobem que si $\alpha > \mathrm{e}$ la sèrie (9.8) és convergent, i si $\alpha < \mathrm{e}$ la sèrie (9.8) és convergent. Estudiem el cas $\alpha = \mathrm{e}$. Això és la sèrie

$$\sum_{n=1}^{\infty} \frac{1}{\mathrm{e}^{\log(n)}} = \sum_{n=1}^{\infty} \frac{1}{n},$$

i per l'exercici 9.1.6 trobem que és divergent.

Per tant, la sèrie (9.8) és convergent quan $\alpha > \mathrm{e}$ i divergent quan $\alpha \leq \mathrm{e}$. $\diamondsuit$

Lema 9.1.21 (Criteri de la integral)**.** *Sigui $f\colon [1,\infty) \longrightarrow (0,\infty)$ una funció decreixent. Aleshores la sèrie $\sum_{n=1}^{\infty} f(n)$ és convergent si i només si existeix un real $C > 0$ tal que per a tot N natural es satisfà $\int_1^N f(x)\mathrm{d}x \leq C$.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que la sèrie $\sum_{n=1}^{\infty} f(n)$ és convergent. Com que, per hipòtesi, la sèrie és de termes positius, per la definició de sèrie convergent (9.1.2) tenim que existeix un real C tal que per a tot N natural es satisfà

$$\sum_{n=1}^{N} f(n) \leq C.$$

Considerem la integral

$$\int_1^N f(x)\mathrm{d}x.$$

Com que per hipòtesi la funció f és decreixent trobem que

$$\begin{aligned}\int_1^N f(x)\mathrm{d}x &\leq (2-1)f(1) + (3-2)f(2) + \cdots + (N-(N-1))f(N-1) \\ &= f(1) + 1f(2) + \cdots + 1f(N-1) \\ &= \sum_{n=1}^{N-1} f(n) \leq C,\end{aligned}$$

i hem acabat.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que existeix un real $C > 0$ tal que per a tot N natural es satisfà

$$\int_1^N f(x)\mathrm{d}x \leq C.$$

Tenim doncs que per a tot N natural

$$\begin{aligned} C &\geq \int_1^N f(x)\mathrm{d}x \\ &\geq (1-0)f(1) + (2-1)f(2) + \cdots + (N+1-N)f(N) \\ &= f(1) + 1f(2) + \cdots + 1f(N) \\ &= \sum_{n=1}^{N} f(n), \end{aligned}$$

i per la definició de sèrie convergent (9.1.2) trobem que la sèrie $\sum_{n=1}^{\infty} f(n)$ és convergent. $\square$

9.1.4 Sèries alternades

Definició 9.1.22 (Sèrie alternada)**.** Sigui $(a_n)_{n\in\mathbb{N}}$ una sèrie de termes positius. Aleshores direm que la sèrie

$$\sum_{n=0}^{\infty} (-1)^n a_n$$

és la sèrie alternada de $(a_n)_{n\in\mathbb{N}}$.

Teorema 9.1.23 (Criteri de Leibniz)**.** *Siguin $(a_n)_{n\in\mathbb{N}}$ una sèrie de termes positius decreixent amb*

$$\lim_{n\to\infty} a_n = 0.$$

Aleshores la sèrie alternada de $(a_n)_{n\in\mathbb{N}}$ és convergent.

Demostració. Definim

$$S_N = \sum_{n=0}^{N} (-1)^n a_n \tag{9.9}$$

i considerem les parcials

$$S_{2N+1} = \sum_{n=0}^{2N+1} (-1)^n a_n \quad \text{i} \quad S_{2N} = \sum_{n=0}^{2N} (-1)^n a_n.$$

Tenim que

$$S_{2(N+1)+1} = S_{2N+1} - a_{2N+2} + a_{2N+3},$$

i com que, per hipòtesi, la successió (a_n) és decreixent trobem que

$$S_{2(N+1)+1} \leq S_{2N+1},$$

i per tant la successió $(S_{2N+1})_{N\in\mathbb{N}}$ és decreixent. També tenim que

$$S_{2(N+1)} = S_{2N} + a_{2N+1} - a_{2N+2},$$

i de nou, com que la successió (a_n) és decreixent trobem que

$$S_{2(N+1)} \geq S_{2N},$$

i per tant la successió $(S_{2N})_{N\in\mathbb{N}}$ és creixent.

Ara bé, com que per hipòtesi la successió (a_n) és de termes positius tenim que

$$S_{2N+1} - S_{2N} = a_{2N+1} \geq 0,$$

i per tant $S_{2N+1} < S_{2N}$. Així trobem que

$$\begin{aligned} a_1 - a_2 &= S_2 \\ &\leq S_{2N} \\ &< S_{2N+1} \\ &\leq S_1 = a_1, \end{aligned} \tag{9.9}$$

i tenim que

$$\lim_{N\to\infty} (S_{2N+1} - S_{2N}) = \lim_{N\to\infty} a_{2N+1},$$

i com que per hipòtesi

$$\lim_{n\to\infty} a_n = 0$$

tenim que

$$\lim_{N\to\infty} S_{2N+1} = \lim_{N\to\infty} S_{2N}. \tag{9.10}$$

Per tant tenim que (S_{2N+1}) és una successió superiorment acotada i creixent, i per tant convergent, i (S_{2N}) és una successió inferiorment acotada i decreixent, i per tant convergent. També tenim per (9.10) que tenen el mateix límit, i per tant la successió (S_N) és convergent, i per la definició de sèrie convergent (9.1.2) trobem que la sèrie $\sum_{n=0}^{\infty}(-1)^n a_n$ és convergent, com volíem veure. □

Exemple 9.1.24 (Sèrie harmònica alternada)**.** *Sigui α un real. Volem estudiar per a quins valors de α la sèrie*

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^\alpha} \tag{9.11}$$

és convergent.

Solució. Si $\alpha \leq 0$ tenim que el límit

$$\lim_{n\to\infty} \frac{(-1)^n}{n^\alpha}$$

és divergent, i pel corol·lari 9.1.5 trobem que la sèrie és divergent.

Estudiem ara el cas $\alpha > 0$. Si denotem

$$a_n = \frac{1}{n^\alpha}$$

tenim que la successió $(a_n)_{n\in\mathbb{N}}$ és decreixent, i pel criteri de Leibniz per sèries alternades (9.1.23) trobem que la sèrie és convergent.

Per tant tenim que si $\alpha > 0$ la sèrie (9.11) és convergent, i si $\alpha \leq 0$ la sèrie és divergent. ♢

9.1.5 Convergència absoluta d'una sèrie

Definició 9.1.25 (Convergència absoluta)**.** Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie numèrica tal que la sèrie

$$\sum_{n=0}^{\infty} |a_n|$$

sigui convergent. Aleshores direm que la sèrie $\sum_{n=0}^{\infty} a_n$ és absolutament convergent.

Proposició 9.1.26. *Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie absolutament convergent. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent.*

Demostració. Com que, per hipòtesi, la sèrie $\sum_{n=0}^{\infty} |a_n|$ és convergent tenim per la condició de Cauchy (9.1.4) que per a tot $\varepsilon > 0$ real existeix un n_0 natural tal que per a tot N i M naturals amb $N, M \geq n_0$ i $N \leq M$ tenim

$$\left| \sum_{n=N}^{N} |a_n| \right| < \varepsilon. \tag{9.12}$$

Ara bé, com que $|a_n|$ és no negatiu per a tot n natural trobem que

$$\left| \sum_{n=N}^{N} |a_n| \right| = \sum_{n=N}^{N} |a_n|,$$

i per la desigualtat triangular tenim que

$$\left| \sum_{n=N}^{M} a_n \right| \leq \sum_{n=N}^{M} |a_n|$$

i per (9.12) trobem que per a tot N i M naturals amb $N, M \geq n_0$ i $N \leq M$ tenim

$$\left| \sum_{n=N}^{M} a_n \right| < \varepsilon,$$

i per la condició de Cauchy (9.1.4) tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent. □

Exemple 9.1.27. *Volem estudiar la convergència de la sèrie numèrica*

$$\sum_{n=1}^{\infty} \frac{\sin(n)}{n^3}. \tag{9.13}$$

Solució. Observem que no tots els termes de la sèrie (9.13) són positius. Per tant no podem aplicar els criteris de convergència de sèries de termes positius.

Estudiem la convergència absoluta de la sèrie. Per la definició de convergència absoluta d'una sèrie (9.1.25) això és estudiar la convergència de la sèrie

$$\sum_{n=1}^{\infty} \left| \frac{\sin(n)}{n^3} \right|, \tag{9.14}$$

que podem reescriure com

$$\sum_{n=1}^{\infty} \frac{|\sin(n)|}{n^3}.$$

Observem que $|\sin(n)| \leq 1$. Per tant trobem que

$$\sum_{n=1}^{\infty} \left| \frac{\sin(n)}{n^3} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^3}.$$

Ara bé, tenim per l'exemple 9.1.6 que la sèrie

$$\sum_{n=1}^{\infty} \frac{1}{n^3}$$

és convergent, i pel lema 9.1.9 trobem que la sèrie (9.14) és convergent.

Per tant, per la definició de convergència absoluta d'una sèrie (9.1.25) trobem que la sèrie (9.13) és absolutament convergent, i per la proposició 9.1.26 trobem que la sèrie (9.13) és convergent. ♢

Exemple 9.1.28. *Volem estudiar la convergència i la convergència absoluta de la sèrie*

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n}. \tag{9.15}$$

Solució. Tenim per l'exemple 9.1.24 que la sèrie (9.15) és convergent, i per l'exemple 9.1.6 trobem que la sèrie (9.15) no és absolutament convergent. ♢

9.1.6 Sèries del producte de successions

Lema 9.1.29 (Fórmula de sumació parcial d'Abel)**.** *Siguin $(a_n)_{n\in\mathbb{N}}$ i $(b_n)_{n\in\mathbb{N}}$ dues sèries numèriques i*

$$A_N = \sum_{n=0}^{N} a_n.$$

Aleshores per a tot naturals N i M amb $N \leq M$ tenim que

$$\sum_{n=N}^{M} a_n b_n = A_M b_M - A_{N-1} b_N + \sum_{n=N}^{M-1} A_n (b_n - b_{n+1}).$$

Demostració. Tenim que

$$\begin{aligned}
\sum_{n=N}^{M} a_n b_n &= \sum_{n=N}^{M} (A_n - A_{n-1}) b_n \\
&= \sum_{n=N}^{M} A_n b_n - \sum_{n=N}^{M} A_{n-1} b_n \\
&= \sum_{n=N}^{M} A_n b_n - \sum_{n=N-1}^{M-1} A_n b_{n+1} \\
&= A_M b_M - A_{N-1} b_N + \sum_{n=N}^{M-1} A_n b_n - \sum_{n=N-1}^{M-1} A_n b_{n+1} \\
&= A_M b_M - A_{N-1} b_N + \sum_{n=N}^{M-1} A_n (b_n - b_{n+1}).
\end{aligned}$$ □

Teorema 9.1.30 (Teorema de Dirichlet)**.** *Siguin* $(a_n)_{n\in\mathbb{N}}$ *una successió numèrica tal que existeix un real* C *tal que* $\left|\sum_{n=0}^{N} a_n\right| \leq C$ *per a tot* N *natural i* $(b_n)_{n\in\mathbb{N}}$ *una successió numèrica monòtona amb* $\lim_{n\to\infty} b_n = 0$*. Aleshores la sèrie*

$$\sum_{n=0}^{\infty} a_n b_n$$

és convergent.

Demostració. Definim

$$A_N = \sum_{n=0}^{N} a_n.$$

Per la fórmula de sumació parcial d'Abel (9.1.29) tenim que per a tot naturals N i M amb $N < M$

$$\sum_{n=N}^{M} a_n b_n = A_M b_M - A_{N-1} b_N + \sum_{n=N}^{M-1} A_n (b_n - b_{n+1}),$$

i per la desigualtat triangular tenim que

$$\left|\sum_{n=N}^{M} a_n b_n\right| \leq |A_M b_M| + |A_{N-1} b_N| + \left|\sum_{n=N}^{M-1} A_n (b_n - b_{n+1})\right|. \tag{9.16}$$

Ara bé, com que per hipòtesi tenim que

$$\lim_{n\to\infty} b_n = 0,$$

per la definició de límit (5.2.3) trobem que per a tot $\varepsilon > 0$ real existeix un natural n_0 tal que per a tot $n > n_0$ tenim

$$|b_n| < \frac{\varepsilon}{4C}.$$

Per tant, per a tot $N > n_0$ tenim que

$$\begin{aligned}|A_M b_M| &= |b_M||A_M| \\ &\leq |b_M|\left|\sum_{n=0}^{M} a_n\right| \\ &\leq \frac{\varepsilon}{4C}C = \frac{\varepsilon}{4},\end{aligned}$$

també tenim

$$\begin{aligned}|A_{M-1} b_M| &= |b_M||A_{M-1}| \\ &\leq |b_M|\left|\sum_{n=0}^{M-1} a_n\right| \\ &\leq \frac{\varepsilon}{4C}C = \frac{\varepsilon}{4},\end{aligned}$$

i

$$\begin{aligned}\left|\sum_{n=N}^{M-1} A_n(b_n - b_{n+1})\right| &\leq \sum_{n=N}^{M-1} |A_n||b_n - b_{n-1}| \\ &\leq \sum_{n=N}^{M-1} C|b_n - b_{n-1}| \\ &= C\sum_{n=N}^{M-1} |b_n - b_{n-1}| \\ &= C|b_N - b_M| \\ &\leq C(|b_N| + |b_M|) \\ &\leq C\Big(\frac{\varepsilon}{4C} + \frac{\varepsilon}{4C}\Big) = \frac{2\varepsilon}{4}.\end{aligned}$$

Per (9.16) trobem

$$\left|\sum_{n=N}^{M} a_n b_n\right| \leq \frac{\varepsilon}{4} + \frac{\varepsilon}{4} + \frac{2\varepsilon}{4},$$

i per tant tenim que per a tot $\varepsilon > 0$ real existeix un natural n_0 tal que per a tot natural N i M amb $N, M \geq n_0$ i $N \leq M$ tenim

$$\left|\sum_{n=N}^{M} a_n b_n\right| \leq \varepsilon,$$

i per la condició de Cauchy (9.1.4) tenim que la sèrie

$$\sum_{n=0}^{\infty} a_n b_n$$

és convergent, com volíem veure. □

Exemple 9.1.31. *Volem estudiar la convergència de la sèrie*

$$\sum_{n=1}^{\infty} \frac{\sin(n)}{n}.$$

Solució. Tenim que

$$\mathrm{e}^{n\mathrm{i}} = \cos(n) + \mathrm{i}\sin(n).$$

Per tant tenim que per a tot N natural

$$\sum_{n=0}^{N} \mathrm{e}^{n\mathrm{i}} = \sum_{n=0}^{N} \cos(n) + \mathrm{i}\sum_{n=0}^{N} \sin(n).$$

Aleshores

$$\begin{aligned}
\left|\sum_{n=0}^{N} \sin(n)\right| &\leq \left|\sum_{n=0}^{N} \mathrm{e}^{n\mathrm{i}}\right| \\
&= \left|\sum_{n=0}^{N} \left(\mathrm{e}^{\mathrm{i}}\right)^n\right| \\
&= \left|\frac{1-\left(\mathrm{e}^{\mathrm{i}}\right)^{N+1}}{1-\mathrm{e}^{\mathrm{i}}}\right| \\
&\leq \left|\frac{\mathrm{e}^{\mathrm{i}}-\mathrm{e}^{\mathrm{i}}\mathrm{e}^{N\mathrm{i}}}{\mathrm{e}^{\mathrm{i}}-1}\right| \\
&= \left|\mathrm{e}^{\mathrm{i}}\right|\left|\frac{1-\mathrm{e}^{N\mathrm{i}}}{\mathrm{e}^{\mathrm{i}}-1}\right| \\
&\leq \left|\frac{1+\mathrm{e}^{\mathrm{i}}}{\mathrm{e}^{\mathrm{i}}-1}\right| \\
&\leq \frac{1+\left|\mathrm{e}^{\mathrm{i}}\right|}{\left|\mathrm{e}^{\mathrm{i}}-1\right|} < C
\end{aligned} \tag{9.1.3}$$

per a cert C real. També tenim que la successió $(n^{-1})_{n\in\mathbb{N}}$ és monòtonament decreixent amb

$$\lim_{n\to\infty} \frac{1}{n} = 0,$$

i pel Teorema de Dirichlet per sèries numèriques (9.1.30) trobem que la sèrie

$$\sum_{n=1}^{\infty} \frac{\sin(n)}{n}$$

és convergent. ◊

Teorema 9.1.32 (Criteri d'Abel)**.** *Siguin* $\sum_{n=0}^{\infty} a_n$ *una sèrie convergent i* $(b_n)_{n\in\mathbb{N}}$ *una successió numèrica monòtona i convergent. Aleshores la sèrie*

$$\sum_{n=0}^{N} a_n b_n$$

és convergent.

Demostració. Definim
$$A_N = \sum_{n=0}^{N} a_n.$$
Aleshores tenim que
$$a_n = A_n - A_{n-1} \tag{9.17}$$
i per tant
$$\begin{aligned}
\sum_{n=0}^{N} a_n b_n &= A_0 b_0 + \sum_{n=1}^{N} (A_n - A_{n-1}) b_n && (9.17)\\
&= A_0 b_0 + (A_1 - A_0) b_1 + (A_2 - A_1) b_2 + \cdots + (A_N - A_{N-1}) b_N\\
&= A_0 (b_0 - b_1) + A_1 (b_1 - b_2) + \cdots + A_{N-1} (b_{N-1} - b_N) + A_N b_N\\
&= A_N b_N + \sum_{n=0}^{N-1} A_n (b_n - b_{n+1}).
\end{aligned}$$

Per hipòtesi tenim que $\sum_{n=0}^{\infty} a_n$ una sèrie convergent, i per la definició de sèrie convergent (9.1.2) tenim que existeix un real L tal que
$$\lim_{N\to\infty} A_N = L. \tag{9.18}$$
També tenim, per hipòtesi, que la successió (b_n) és convergent, i per tant existeix un real b tal que
$$\lim_{n\to\infty} b_n = b. \tag{9.19}$$
Estudiem la convergència absoluta de la sèrie $\sum_{n=0}^{\infty} A_n (b_n - b_{n+1})$. Com que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent tenim que existeix un real $C > 0$ tal que per a tot N natural es satisfà
$$|A_N| \le C. \tag{9.20}$$
Per tant, com que la successió (b_n) és monòtona, trobem que
$$\begin{aligned}
\sum_{n=0}^{N} |A_n (b_n - b_{n+1})| &\le \sum_{n=0}^{N} |C (b_n - b_{n+1})| && (9.20)\\
&\le C \sum_{n=0}^{N} |b_n - b_{n+1}|\\
&= C |b_0 - b_{N+1}|,
\end{aligned}$$
i per (9.19) tenim que
$$\lim_{N\to\infty} C|b_0 - b_{N+1}| = C|b_0 - b|,$$
i per tant la sèrie $\sum_{n=0}^{\infty} A_n (b_n - b_{n+1})$ és absolutament convergent, i per la proposició 9.1.26 tenim que la sèrie $\sum_{n=0}^{\infty} A_n (b_n - b_{n+1})$ és convergent.

Ara bé, per (9.18) i (9.19) trobem que
$$\lim_{N\to\infty} A_N b_N = Lb,$$

i per tant tenim que

$$\lim_{N\to\infty}\left(A_N b_N + \sum_{n=0} A_n(b_n - b_{n+1})\right) = Lb + C|b_0 - b|$$

i per tant

$$\lim_{N\to\infty}\sum_{n=0}^{N} a_n b_n = Lb + C|b_0 - b|$$

és convergent, i per la definició de sèrie convergent (9.1.2) trobem que la sèrie $\sum_{n=0}^{\infty} a_n b_n$ és convergent, com volíem veure. □

Exemple 9.1.33. *Volem estudiar la convergència de la sèrie*

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n}\left(1+\frac{1}{n}\right)^n. \tag{9.21}$$

Solució. Tenim que la successió

$$\left(\left(1+\frac{1}{n}\right)^n\right)_{n\in\mathbb{N}}$$

és monòtona i convergent, i per l'exercici 9.1.24 trobem que la sèrie

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n}$$

és convergent. Per tant pel criteri d'Abel per sèries numèriques (9.1.32) tenim que la sèrie (9.21) és convergent. ♢

9.1.7 Reordenació de sèries

Definició 9.1.34 (Reordenada d'una sèrie)**.** Siguin $\sum_{n=0}^{\infty} a_n$ i $\sum_{n=0}^{\infty} b_n$ dues sèries tals que existeix una permutació σ de $\mathbb{N}$ tal que

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} b_{\sigma(n)}.$$

Aleshores direm que la sèrie $\sum_{n=0}^{\infty} b_n$ és una reordenada de la sèrie $\sum_{n=0}^{\infty} a_n$

Lema 9.1.35. *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius convergent i σ una permutació de $\mathbb{N}$. Aleshores tenim que*

$$\sum_{n=0}^{\infty} a_{\sigma(n)} \leq \sum_{n=0}^{\infty} a_n.$$

Demostració. Fixem un natural N i considerem

$$M = \max\{\sigma(1),\ldots,\sigma(N)\}$$

i com que, per la definició de 9.1.7, tenim que $a_n \geq 0$ per a tot n natural trobem que

$$\sum_{n=0}^{N} a_{\sigma(n)} \leq \sum_{n=0}^{M} a_n,$$

i per la definició de sèrie convergent (9.1.2) trobem que

$$\sum_{n=0}^{\infty} a_{\sigma(n)} \leq \sum_{n=0}^{\infty} a_n. \qquad \square$$

Corol·lari 9.1.36. *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie de termes positius convergent i σ una permutació de $\mathbb{N}$. Aleshores tenim que*

$$\sum_{n=0}^{\infty} a_{\sigma(n)} = \sum_{n=0}^{\infty} a_n.$$

Proposició 9.1.37. *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie absolutament convergent i σ una permutació de $\mathbb{N}$. Aleshores la sèrie $\sum_{n=0}^{\infty} a_{\sigma(n)}$ és absolutament convergent.*

Demostració. Per la definició de convergència absoluta d'una sèrie (9.1.25) tenim que la sèrie

$$\sum_{n=0}^{\infty} |a_n|$$

és convergent, i pel corol·lari 9.1.36 trobem que

$$\sum_{n=0}^{\infty} \left|a_{\sigma(n)}\right| = \sum_{n=0}^{\infty} |a_n|,$$

i per tant tenim que $\sum_{n=0}^{\infty} a_{\sigma(n)}$ és absolutament convergent. $\square$

Notació 9.1.38. Definim

$$a_n^+ = \begin{cases} a_n & \text{si } a_n \geq 0 \\ 0 & \text{si } a_n < 0 \end{cases} \quad \text{i} \quad a_n^- = \begin{cases} 0 & \text{si } a_n \geq 0 \\ -a_n & \text{si } a_n < 0 \end{cases}$$

Observació 9.1.39. *Tenim que*

$$a_n = a_n^+ - a_n^- \quad i \quad |a_n| = a_n^+ + a_n^-$$

Lema 9.1.40. *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie absolutament convergent i σ una permutació de $\mathbb{N}$. Aleshores tenim que*

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} a_{\sigma(n)}.$$

Demostració. Aquest enunciat té sentit per la proposició 9.1.37.

Per la definició de 9.1.25 tenim que la sèrie $\sum_{n=0}^{\infty} a_n$ és absolutament convergent si i només si les sèries $\sum_{n=0}^{\infty} a_n^+$ i $\sum_{n=0}^{\infty} a_n^-$ són convergents. Per tant trobem que

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n &= \sum_{n=0}^{\infty} (a_n^+ - a_n^-) && (9.1.39)\\
&= \sum_{n=0}^{\infty} a_n^+ - \sum_{n=0}^{\infty} a_n^- \\
&= \sum_{n=0}^{\infty} a_{\sigma(n)}^+ - \sum_{n=0}^{\infty} a_{\sigma(n)}^- && (9.1.36)\\
&= \sum_{n=0}^{\infty} \left(a_{\sigma(n)}^+ - a_{\sigma(n)}^-\right) = \sum_{n=0}^{\infty} a_{\sigma(n)}, && (9.1.39)
\end{aligned}$$

com volíem veure. □

Lema 9.1.41. *Sigui $\sum_{n=0}^{\infty} a_n$ una sèrie convergent però no absolutament convergent. Aleshores les sèries $\sum_{n=0}^{\infty} a_n^+$ i $\sum_{n=0}^{\infty} a_n^-$ són divergents.*

Demostració. Per l'observació 9.1.39 tenim que

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} (a_n^+ - a_n^-), \tag{9.22}$$

i per tant

$$\sum_{n=0}^{\infty} a_n^- = \sum_{n=0}^{\infty} a_n^+ - \sum_{n=0}^{\infty} a_n. \tag{9.23}$$

Suposem que $\sum_{n=0}^{\infty} a_n^+$ és convergent. Aleshores per (9.23) tenim que la sèrie $\sum_{n=0}^{\infty} a_n^-$ és convergent.

Ara bé, per la definició de convergència absoluta d'una sèrie (9.1.25) tenim que les sèries $\sum_{n=0}^{\infty} a_n^+$ i $\sum_{n=0}^{\infty} a_n^-$ són absolutament convergents, i per (9.22) tenim que $\sum_{n=0}^{\infty} a_n$ és absolutament convergent, però això contradiu l'hipòtesi que $\sum_{n=0}^{\infty} a_n$ no és absolutament convergent. Per tant ha de ser que la sèrie $\sum_{n=0}^{\infty} a_n^+$ és divergent. El cas en que suposem que $\sum_{n=0}^{\infty} a_n^+$ és convergent és anàleg. □

Teorema 9.1.42 (Teorema de la reordenació de sèries de Riemann)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ una sèrie convergent però no absolutament convergent i L un nombre real. Aleshores existeix una permutació σ de $\mathbb{N}$ tal que*

$$\sum_{n=0}^{\infty} a_{\sigma(n)} = L.$$

Demostració. Prenem un α real. Tenim per hipòtesi que la sèrie $\sum_{n=0}^{\infty} a_n$ una sèrie convergent però no absolutament convergent, i pel lema 9.1.41 trobem que les sèries $\sum_{n=0}^{\infty} a_n^+$ i $\sum_{n=0}^{\infty} a_n^-$ són divergents.

Definim

$$S_N = \sum_{n=0}^{N} a_n^+ \quad \text{i} \quad T_N = \sum_{n=0}^{N} a_n^-.$$

Tenim que S_N no està fitada superiorment i T_N no està fitada inferiorment. Per tant tenim que existeix un mínim natural n_1 tal que

$$S_{n_1} \geq \alpha,$$

i tenim que

$$\begin{aligned}\alpha &\leq S_{n_1} \\ &= S_{n_1-1} + a^+_{n_1} \\ &< \alpha + a^+_{n_1},\end{aligned}$$

i per tant

$$\alpha < \alpha + a^+_{n_1}.$$

També tenim que existeix un mínim natural m_1 tal que

$$S_{n_1} + T_{m_1} \leq \alpha,$$

i tenim que

$$\begin{aligned}\alpha &\geq S_{n_1} - T_{m_1} \\ &= S_{n_1} - T_{m_1-1} - a^-_{m_1} \\ &> \alpha - a^-_{m_1},\end{aligned}$$

i per tant

$$\alpha > \alpha - a^-_{m_1}.$$

Definim doncs per a tot i natural

$$n_i = \min_{n > n_{i-1}} \{S_n - T_{m_i-1} \geq \alpha\} \quad \text{i} \quad m_i = \min_{m > m_{i-1}} \{S_{n_i} - T_m \leq \alpha\},$$

i trobem que

$$\begin{aligned}\alpha &\geq S_{n_i} - T_{n_i} \\ &= S_{n_i} - T_{m_i-1} - a^-_{m_i} \\ &\geq \alpha - a^-_{m_i}.\end{aligned}$$

Ara bé, tenim per hipòtesi que la sèrie $\sum_{n=0}^{\infty} a_n$ és convergent, i pel corol·lari 9.1.5 tenim que $\lim_{n\to\infty} a_n = 0$, i per tant $\lim_{n\to\infty} a^-_n = 0$, i pel Teorema del sandvitx (5.2.16) trobem que

$$\lim_{i\to\infty} S_{n_i} - T_{m_i} = \alpha.$$

□

Teorema 9.1.43 (Teorema de Cauchy)**.** *Siguin $\sum_{n=0}^{\infty} a_n$ i $\sum_{n=0}^{\infty} b_n$ dues sèries absolutament convergents i $(c_n)_{n\in\mathbb{N}}$ una successió tal que per a tot (i,j) de $\mathbb{N}\times\mathbb{N}$ existeix un únic n tal que $c_n = a_i b_j$ i tal que per a tot n de $\mathbb{N}$ existeix un únic (i,j) de $\mathbb{N}\times\mathbb{N}$ tal que $c_n = a_i b_j$. Aleshores tenim que*

$$\sum_{n=0}^{\infty} c_n = \left(\sum_{n=0}^{\infty} a_n\right)\left(\sum_{n=0}^{\infty} b_n\right).$$

Demostració. □

9.2 Successions de funcions

9.2.1 Convergència d'una successió de funcions

Definició 9.2.1 (Successió de funcions)**.** Siguin I un interval de $\mathbb{R}$ i $f_i\colon I \longrightarrow \mathbb{R}$ una funció real per a tot i natural. Aleshores direm que $(f_n)_{n\in\mathbb{N}}$ és una successió de funcions definides en I.

Definició 9.2.2 (Convergència puntual)**.** Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions definides en un interval I tal que existeix una funció f de I a $\mathbb{R}$ tal que

$$\lim_{n\to\infty} f_n(x) = f(x)$$

per a tot x de I. Aleshores direm que la successió (f_n) convergeix puntualment a la funció f.

Exemple 9.2.3. *Volem estudiar la convergència puntual de la successió de funcions* $(f_n)_{n\in\mathbb{N}}$ *definida per*

$$f_n(x) = \frac{nx^2+1}{nx+1}$$

en l'interval $[1,2]$.

Solució. Considerem el límit

$$\begin{aligned}\lim_{n\to\infty} f_n(x) &= \lim_{n\to\infty} \frac{nx^2+1}{nx+1}\\ &= \lim_{n\to\infty} \frac{nx^2+1}{nx+1}\frac{\frac{1}{n}}{\frac{1}{n}}\\ &= \lim_{n\to\infty} \frac{x^2+\frac{1}{n}}{x+\frac{1}{n}}\\ &= \frac{x^2}{x} = x,\end{aligned}$$

i per la definició de convergència puntual d'una sèrie de funcions (9.3.2) trobem que la successió (f_n) convergeix puntualment a la funció $f(x) = x$. ♢

9.2.2 Convergència uniforme

Definició 9.2.4 (Convergència uniforme)**.** Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions definides en un interval I que convergeix puntualment a una funció f tal que per a tot $\varepsilon > 0$ real existeix un n_0 natural tal que per a tot $n > n_0$ es satisfà

$$\sup_{x\in I}|f_n(x) - f(x)| < \varepsilon.$$

Aleshores direm que la successió $(f_n)_{n\in\mathbb{N}}$ convergeix uniformement a f i ho denotarem com $f_n \rightrightarrows f$.

Observació 9.2.5. *Una successió de funcions* $(f_n)_{n\in\mathbb{N}}$ *sobre un interval* I *convergeix uniformement a una funció* f *si i només si*

$$\lim_{n\to\infty} \sup_{x\in I}|f_n(x) - f(x)| = 0.$$

Demostració. Per la definició de límit (5.2.3). □

Exemple 9.2.6. *Volem estudiar la convergència uniforme de la successió de funcions* $(f_n)_{n\in\mathbb{N}}$ *definida per*

$$f_n(x) = \frac{nx^2+1}{nx+1}$$

en l'interval $[1,2]$.

Demostració. Per l'exercici 9.2.3 tenim que la successió de funcions (f_n) convergeix puntualment a la funció $f(x) = x$ en l'interval $[1,2]$. Considerem el límit

$$\begin{aligned}
\lim_{n\to\infty} \sup_{x\in[1,2]} |f_n(x) - f(x)| &= \lim_{n\to\infty} \sup_{x\in[1,2]} \left| \frac{nx^2+1}{nx+1} - x \right| \\
&= \lim_{n\to\infty} \sup_{x\in[1,2]} \left| \frac{nx^2+1-nx^2-x}{nx+1} \right| \\
&= \lim_{n\to\infty} \sup_{x\in[1,2]} \left| \frac{1-x}{nx+1} \right| \\
&\leq \lim_{n\to\infty} \sup_{x\in[1,2]} \frac{1+|x|}{nx+1} \\
&\leq \lim_{n\to\infty} \frac{3}{n+1} = 0,
\end{aligned}$$

i per l'observació 9.2.5 trobem que la successió de funcions (f_n) convergeix uniformement a $f(x)$ en l'interval $[1,2]$. □

Proposició 9.2.7. *Sigui* $(f_n)_{n\in\mathbb{N}}$ *una successió de funcions que convergeixen uniformement a una funció* f*. Aleshores la successió* $(f_n)_{n\in\mathbb{N}}$ *convergeix puntualment a* f*.*

Demostració. □

Teorema 9.2.8 (Condició de Cauchy)**.** *Sigui* $(f_n)_{n\in\mathbb{N}}$ *una successió de funcions sobre un interval* I*. Aleshores la successió* $(f_n)_{n\in\mathbb{N}}$ *convergeix uniformement a una funció* f *de* I *si i només si per a tot* $\varepsilon > 0$ *real existeix un* n_0 *natural tal que per a tots enters* n *i* m *amb* $n_0 < m < n$ *es satisfà*

$$\sup_{x\in I} |f_n(x) - f_m(x)| < \varepsilon.$$

Demostració. □

9.2.3 Continuïtat, integrabilitat i derivabilitat

Teorema 9.2.9. *Sigui* $(f_n)_{n\in\mathbb{N}}$ *una successió de funcions contínues sobre un interval* I *tal que* $f_n \rightrightarrows f$*. Aleshores* f *és contínua.*

Demostració. □

Teorema 9.2.10. *Sigui* $(f_n)_{n\in\mathbb{N}}$ *una successió de funcions integrables Riemann sobre un interval* I *tal que* $f_n \rightrightarrows f$*. Aleshores* f *és integrable Riemann.*

Demostració. □

Teorema 9.2.11. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions integrables Riemann sobre un interval I tal que $f_n \rightrightarrows f$. Aleshores*

$$\lim_{n\to\infty} \int_I f_n(x)\mathrm{d}x = \int_I \lim_{n\to\infty} f_n(x)\mathrm{d}x.$$

Demostració. □

Teorema 9.2.12. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions derivables sobre un interval I que convergeix uniformement a una funció f tal que la successió $(f'_n)_{n\in\mathbb{N}}$ convergeix uniformement a una funció g. Aleshores tenim que f és derivable i que $f'(x) = g(x)$.*

Demostració. □

9.3 Sèries de funcions

9.3.1 Convergència d'una sèrie de funcions

Definició 9.3.1 (Sèrie de funcions)**.** Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I. Aleshores definim, per a tot x de I,

$$F(x) = \sum_{n=0}^{\infty} f_n(x)$$

com la sèrie de funcions de la successió $(f_n)_{n\in\mathbb{N}}$.

Definició 9.3.2 (Convergència puntual)**.** Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I i

$$F_N(x) = \sum_{n=0}^{N} f_n(x)$$

tal que la successió de funcions $(F_n)_{n\in\mathbb{N}}$ sigui puntualment convergent en I. Aleshores direm que la sèrie de funcions de la successió $(f_n)_{n\in\mathbb{N}}$ és convergent puntualment en I.

Exemple 9.3.3. *Exemple de convergència puntual d'una sèrie de funcions.*

Solució. ◊

Definició 9.3.4 (Convergència uniforme)**.** Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I i

$$F_N(x) = \sum_{n=0}^{N} f_n(x)$$

tal que la successió de funcions $(F_n)_{n\in\mathbb{N}}$ sigui uniformement convergent en I. Aleshores direm que la sèrie de funcions de la successió $(f_n)_{n\in\mathbb{N}}$ és convergent uniformement en I.

Exemple 9.3.5. *Exemple de convergència uniforme d'una sèrie de funcions.*

Solució. $\Diamond$

Teorema 9.3.6 (Condició de Cauchy)**.** *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I. Aleshores la sèrie $\sum_{n=0}^{\infty} f_n(x)$ és convergent si i només si per a tot $\varepsilon > 0$ real existeixen enters N i M amb $N < M$ tals que*

$$\sup_{x\in I}\left|\sum_{n=N}^{M} f_n(x)\right| < \varepsilon.$$

Demostració. $\square$

9.3.2 Continuïtat, integrabilitat i derivabilitat

Teorema 9.3.7. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions contínues sobre un interval I tals que la sèrie $\sum_{n=0}^{\infty} f_n(x)$ convergeixi uniformement a una funció F en I. Aleshores F és contínua en I.*

Demostració. $\square$

Teorema 9.3.8. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions integrables Riemann sobre un interval I tals que la sèrie $\sum_{n=0}^{\infty} f_n(x)$ convergeixi uniformement a una funció F en I. Aleshores F és integrable Riemann en I.*

Demostració. $\square$

Teorema 9.3.9. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions integrables Riemann sobre un interval I tal que la sèrie de funcions de $(f_n)_{n\in\mathbb{N}}$ sigui uniformement convergent en I. Aleshores*

$$\sum_{n=0}^{\infty}\int_I f_n(x)\mathrm{d}x = \int_I \sum_{n=0}^{\infty} f_n(x)\mathrm{d}x.$$

Demostració. $\square$

Teorema 9.3.10. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions derivables sobre un interval I acotat tal que la sèrie de funcions $\sum_{n=0}^{\infty} f_n'(x)$ convergeix uniformement en I i existeix un $x_0 \in I$ tal que la sèrie de funcions $\sum_{n=0}^{\infty} f_n(x_0)$ sigui convergent. Aleshores tenim que la sèrie $\sum_{n=0}^{\infty} f_n(x)$ és derivable i*

$$\left(\sum_{n=0}^{\infty} f_n(x)\right)' = \sum_{n=0}^{\infty} f_n'(x).$$

Demostració. $\square$

9.3.3 Convergència d'una sèrie de funcions

Proposició 9.3.11. *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I tal que la sèrie de funcions $\sum_{n=0}^{\infty} f_n(x)$ convergeix uniformement en I. Aleshores la successió de funcions (f_n) convergeix uniformement a 0.*

Demostració. $\square$

Teorema 9.3.12 (Criteri M de Weierstrass)**.** *Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de funcions sobre un interval I i $(M_n)_{n\in\mathbb{N}}$ una successió de termes no negatius tals que per a tot n natural tenim*

$$\sup_{x\in I}|f_n(x)| \leq M_n$$

i la sèrie $\sum_{n=0}^{\infty} M_n$ és convergent. Aleshores la sèrie de funcions $\sum_{n=0}^{\infty} f_n(x)$ és uniformement convergent en I.

Demostració. □

Exemple 9.3.13. *Volem estudiar la convergència de la sèrie de funcions*

$$\sum_{n=1}^{\infty} \frac{\sin(nx)}{n^3}$$

en tot $\mathbb{R}$.

Solució. Observem que

$$\sup_{x\in\mathbb{R}}\left|\frac{\sin(nx)}{n^3}\right| \leq \frac{1}{n^3},$$

i per l'exemple 9.1.6 tenim que la sèrie

$$\sum_{n=1}^{\infty} \frac{1}{n^3}$$

és convergent. Per tant pel criteri M de Weierstrass (9.3.12) tenim que la sèrie de funcions

$$\sum_{n=1}^{\infty} \frac{\sin(nx)}{n^3}$$

és convergent en tot $\mathbb{R}$. ◊

Teorema 9.3.14 (Criteri de Dirichlet)**.** *Siguin $(f_n)_{n\in\mathbb{N}}$ i $(g_n)_{n\in\mathbb{N}}$ dues successions de funcions sobre un interval I tals que $g_n(x)$ és monòtona per a tot n natural, la successió de funcions (g_n) convergeix uniformement a 0 i existeix un real M tal que*

$$\sup_{x\in I}\left|\sum_{n=0}^{N} g_n(x)\right| \leq M \quad \textit{per a tot } N \textit{ natural.}$$

Aleshores la sèrie de funcions

$$\sum_{n=0}^{\infty} f_n(x)g_n(x)$$

és uniformement convergent en I.

Demostració. □

Exemple 9.3.15. *Exemple del criteri de Dirichlet.*

Solució. $\lozenge$

Teorema 9.3.16 (Criteri d'Abel)**.** *Siguin $(f_n)_{n\in\mathbb{N}}$ i $(g_n)_{n\in\mathbb{N}}$ dues sèries de funcions sobre un interval I tals que g_n és monòtona per a tot n natural, existeix un real L tal que per a tot n natural*

$$\sup_{x\in I}|g_n(x)| \leq L$$

i tal que la sèrie de funcions $\sum_{n=0}^{\infty} f_n(x)$ sigui uniformement convergent en I. Aleshores la sèrie de funcions

$$\sum_{n=0}^{\infty} f_n(x)g_n(x)$$

és absolutament convergent en I.

Demostració. $\square$

Exemple 9.3.17. *Exemple del criteri d'Abel.*

Solució. $\lozenge$

9.3.4 Sèries de potències

Definició 9.3.18 (Sèries de potències)**.** Sigui $(a_n)_{n\in\mathbb{N}}$ una successió de reals i x_0 un nombre real. Aleshores direm que la sèrie

$$\sum_{n=0}^{\infty} a_n(x-x_0)^n$$

és una sèrie de funcions amb terme general a_n al voltant de x_0.

Observació 9.3.19. *Les sèries de potències són sèries de funcions.*

Proposició 9.3.20. *Sigui $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ una sèrie de potències tal que existeix un real x_1 tal que la sèrie*

$$\sum_{n=0}^{\infty} a_n(x_1-x_0)^n$$

és convergent. Aleshores la sèrie $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és convergent per a tot x tal que

$$|x-x_0| < |x_1-x_0|.$$

Demostració. $\square$

Lema 9.3.21. *Sigui $(a_n)_{n\in\mathbb{N}}$ una successió creixent de nombres reals. Aleshores el límit de (a_n) existeix i*

$$\lim_{n\to\infty} a_n = \sup_{n\in\mathbb{N}} a_n.$$

Demostració. $\square$

Corol·lari 9.3.22. *Sigui $(a_n)_{n\in\mathbb{N}}$ una successió decreixent de nombres reals. Aleshores el límit de (a_n) existeix i*

$$\lim_{n\to\infty} a_n = \inf_{n\in\mathbb{N}} a_n.$$

Definició 9.3.23 (Límit superior i inferior)**.** Siguin $(a_n)_{n\in\mathbb{N}}$ una successió de nombres reals i $(b_n)_{n\in\mathbb{N}}$ i $(c_n)_{n\in\mathbb{N}}$ dues successions satisfent

$$b_n = \sup_{k\in\mathbb{N}}\{a_k \mid k \geq n\} \quad \text{i} \quad c_n = \sup_{k\in\mathbb{N}}\{a_k \mid k \leq n\}.$$

Aleshores definim

$$\limsup_{n\to\infty} a_n = \lim_{n\to\infty} b_n \quad \text{i} \quad \liminf_{n\to\infty} a_n = \lim_{n\to\infty} c_n$$

com el límit superior i límit inferior de (a_n).

Aquesta definició té sentit pel lema 9.3.21 i el corol·lari 9.3.22.

Teorema 9.3.24. *Sigui $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ una sèrie de potències i R un real tal que*

$$R^{-1} = \limsup_{n\to\infty} \sqrt[n]{|a_n|}.$$

Aleshores

1. *la sèrie $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és absolutament convergent per a tot x satisfent $|x-x_0| < R$.*
2. *per a tot real $r < R$ la sèrie de funcions $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ convergeix uniformement per a tot x satisfent $|x-x_0| \leq r$.*
3. *La sèrie $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és divergent per a tot x satisfent $|x-x_0| > R$.*

Demostració. □

Proposició 9.3.25. *Sigui $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ una sèrie de potències i R un real tal que*

$$R^{-1} = \limsup_{n\to\infty} \frac{|a_{n+1}|}{|a_n|}.$$

Aleshores

$$R^{-1} = \limsup_{n\to\infty} \sqrt[n]{|a_n|}.$$

Demostració. □

Definició 9.3.26. Sigui $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ una sèrie de potències tal que existeix un real R satisfent

1. la sèrie $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és absolutament convergent per a tot x satisfent $|x-x_0| < R$.
2. per a tot real $r < R$ la sèrie de funcions $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ convergeix uniformement per a tot x satisfent $|x-x_0| \leq r$.
3. La sèrie $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és divergent per a tot x satisfent $|x-x_0| > R$.

Aleshores direm que R és el radi de convergència de la sèrie de potències.

Teorema 9.3.27 (Teorema d'Abel)**.** *Sigui $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ una sèrie de potències i L un real tal que la sèrie $\sum_{n=0}^{\infty} a_n L^n$ és convergent. Aleshores la sèrie de potències $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ és uniformement convergent per a tot x en l'interval $[x_0, x_0+L]$.*

Demostració. □

Exemple 9.3.28. *Volem estudiar per a quins valor de x la sèrie*

$$\sum_{n=0}^{\infty} \frac{x^{2n}}{2n}$$

és convergent.

Solució. ♢

Exemple 9.3.29. *Volem calcular la suma*

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{n+1}.$$

Solució. ♢

Exemple 9.3.30. *Volem calcular la suma*

$$\sum_{n=0}^{\infty} \frac{x^{2n}}{4^n(2n+1)}.$$

Solució. ♢

9.3.5 Teorema d'aproximació polinòmica de Weierstrass

Definició 9.3.31 (Suport d'una funció)**.** Sigui $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ una funció. Aleshores definim

$$\operatorname{Supp}(f) = \{x \in \mathbb{R} \mid f(x) \neq 0\}$$

com el suport de f.

Definició 9.3.32 (Suport compacte)**.** Sigui $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ una funció tal que $\operatorname{Supp}(f)$ sigui un compacte. Aleshores direm que f té suport compacte.

Definició 9.3.33 (Convolució)**.** Siguin $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ i $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ dues funcions amb suport compacte. Aleshores definim

$$(f * g)(x) = \int_{\mathbb{R}} f(t)g(x-t)\mathrm{d}t$$

com la convolució de f amb g.

Definició 9.3.34 (Aproximació de la unitat)**.** Sigui $(\phi_\varepsilon)_{\varepsilon\in\mathbb{R}}$ una successió de funcions amb suport compacte tal que

1. $\phi_\varepsilon \geq 0$.

2. $\int_{\mathbb{R}} \phi_\varepsilon(x)\mathrm{d}x = 1$.

3. per a tot $\delta > 0$ tenim que (ϕ_ε) convergeix uniformement a 0 quan ε tendeix a 0 en l'interval $(-\delta, \delta)$.

Aleshores direm que (ϕ_ε) és una aproximació de la unitat.

Lema 9.3.35. *Sigui $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ una funció contínua amb suport compacte i $(\phi_\varepsilon)_{\varepsilon\in\mathbb{R}}$ una aproximació de la unitat. Aleshores $f * \phi_\varepsilon$ convergeix uniformement a f quan ε tendeix a 0.*

Demostració. $\square$

Teorema 9.3.36 (Teorema d'aproximació polinòmica de Weierstrass)**.** *Sigui $f\colon [a,b] \longrightarrow \mathbb{R}$ una funció contínua. Aleshores existeix una successió de polinomis $(p_n)_{n\in\mathbb{N}}$ que convergeix uniformement a f en l'interval $[a,b]$.*

Demostració. $\square$

Corol·lari 9.3.37. *Sigui $f\colon [a,b] \longrightarrow \mathbb{R}$ una funció contínua tal que per a tot n natural es satisfà*

$$\int_a^b f(x)x^n\mathrm{d}x = 0.$$

Aleshores $f(x) = 0$.

Demostració. $\square$

Capítol 10

Integrals impròpies

10.1 Integral impròpia de Riemann

10.1.1 Funcions localment integrables

Definició 10.1.1 (Funció localment integrable)**.** Sigui $f\colon [a,b) \longrightarrow \mathbb{R}$ amb $b \in \mathbb{R} \cup \infty$ una funció tal que f és integrable Riemann per en $[a,x]$ per a tot $x < b$. Aleshores direm que f és localment integrable en un interval $[a,b)$.

Definició 10.1.2 (Integral impròpia)**.** Sigui f una funció localment integrable en un interval $[a,b)$ tal que existeix el límit

$$\lim_{x\to b} \int_a^x f(t)\mathrm{d}t.$$

Aleshores denotarem

$$\lim_{x\to b} \int_a^x f(t)\mathrm{d}t = \int_a^b f(t)\mathrm{d}t,$$

i direm que $\int_a^b f(t)\mathrm{d}t$ és la integral impròpia de f, i que la integral impròpia de f és divergent.

Si el límit

$$\lim_{x\to b} \int_a^x f(t)\mathrm{d}t.$$

no existeix direm que la integral impròpia de f és divergent.

Exemple 10.1.3. *Volem estudiar la convergència de la integral impròpia*

$$\int_1^\infty \frac{1}{x^\alpha}\mathrm{d}x$$

segons els valors de α real.

Solució. $\Diamond$

Exemple 10.1.4. *Volem estudiar la convergència de la integral impròpia*

$$\int_0^1 \frac{1}{x^\alpha}\mathrm{d}x$$

segons els valors de α real.

Solució. ◊

10.1.2 Integrals impròpies de funcions positives

Lema 10.1.5. *Siguin f i g dues funcions positives localment integrables en un interval $[a, b)$ tals que existeixen dos reals $C > 0$ i $x_0 < b$ satisfent, per a tot x en $[x_0, b)$, que*

$$f(x) \leq Cg(x)$$

i tals que la integral impròpia de g és convergent. Aleshores la integral impròpia de f és convergent.

Demostració. □

Teorema 10.1.6 (Criteri de comparació)**.** *Siguin f i g dues funcions positives localment integrables en un interval $[a, b)$ i*

$$L = \lim_{x \to b} \frac{f(x)}{g(x)}$$

tals que

1. *$L \neq 0$ i $L \neq \infty$. Aleshores $\int_a^b f(x)\mathrm{d}x$ és convergent si i només si $\int_a^b g(x)\mathrm{d}x$ és convergent.*
2. *$L = 0$ i $\int_a^b g(x)\mathrm{d}x$ és convergent. Aleshores $\int_a^b f(x)\mathrm{d}x$ és convergent.*
3. *$L = \infty$ i $\int_a^b f(x)\mathrm{d}x$ és convergent. Aleshores $\int_a^b g(x)\mathrm{d}x$ és convergent.*

Demostració. □

Exemple 10.1.7. *Exemple de criteri de comparació d'integrals impròpies.*

Solució. ◊

Teorema 10.1.8 (Criteri de la integral)**.** *Sigui $f\colon [1, \infty) \longrightarrow (0, \infty)$ una funció decreixent. Aleshores la integral impròpia $\int_1^\infty f(x)\mathrm{d}x$ és convergent si i només si la sèrie $\sum_{n=1}^\infty f(n)$ és convergent.*

Demostració. És conseqüència del lema criteri de la integral (9.1.21) i la definició d'integral impròpia convergent (10.1.2). □

Exemple 10.1.9. *Volem veure per a quins valors de $\alpha > 0$ real la integral*

$$\int_0^\infty \alpha^x \mathrm{d}x \tag{10.1}$$

és convergent.

Solució. ◊

10.1.3 Convergència d'una integral impròpia

Teorema 10.1.10 (Condició de Cauchy)**.** *Sigui $\int_a^b f(x)\mathrm{d}x$ una funció localment integrable en $[a,b)$. Aleshores la integral $\int_a^b f(x)\mathrm{d}x$ és convergent si i només si per a tot $\varepsilon > 0$ existeix un x_0 real tal que per a tot N i M reals amb $N, M \geq x_0$ i $N \leq M < b$ tenim*

$$\left|\int_N^M f(x)\mathrm{d}x\right| < \varepsilon.$$

Demostració. □

Definició 10.1.11 (Convergència absoluta)**.** Sigui $\int_a^b f(x)\mathrm{d}x$ una funció localment integrable en $[a,b)$ tal que la integral

$$\int_a^b |f(x)|\mathrm{d}x$$

és convergent. Aleshores direm que la integral $\int_a^b f(x)\mathrm{d}x$ és absolutament convergent.

Proposició 10.1.12. *Sigui $\int_a^b f(x)\mathrm{d}x$ una integral absolutament convergent. Aleshores la integral $\int_a^b f(x)\mathrm{d}x$ és convergent.*

Demostració. □

Exemple 10.1.13. *Siguin α i β dos reals no negatius i $p(x)$ un polinomi. Volem estudiar la convergència de la integral*

$$\int_0^\infty p(x)\mathrm{e}^{\alpha x^\beta}\mathrm{d}x.$$

Solució. ◊

Teorema 10.1.14 (Criteri de Dirichlet)**.** *Siguin f i g dues funcions localment integrables de classe $\mathcal{C}^1$ satisfent que existeix un real C tal que $\int_a^x |f(x)|\mathrm{d}x < C$ per a tot $x \in [a,b)$ i que g és una funció decreixent amb*

$$\lim_{x\to\infty} g(x) = 0.$$

Aleshores la integral

$$\int_a^b f(x)g(x)\mathrm{d}x$$

és convergent.

Demostració. □

Exemple 10.1.15. *Sigui $\alpha > 0$ un real. Volem estudiar la convergència de la integral*

$$\int_0^\infty \frac{\sin(x)}{x^\alpha}\mathrm{d}x.$$

Solució. ◊

Teorema 10.1.16 (Criteri d'Abel)**.** *Siguin f i g dues funcions localment integrables satisfent que f és monòtona i acotada i que la integral*

$$\int_a^b g(x)\mathrm{d}x$$

és convergent. Aleshores la integral

$$\int_a^b f(x)g(x)\mathrm{d}x$$

és convergent.

Demostració. □

Exemple 10.1.17. *Volem estudiar la convergència de la integral*

$$\int_0^\infty \frac{\sin(x)}{\mathrm{e}^x}\mathrm{d}x.$$

Solució. ♢

10.2 Aplicacions de les integrals impròpies

10.2.1 Integrals dependents d'un paràmetre

Teorema 10.2.1. *Sigui $f\colon [a,b]\times[c,d] \longrightarrow \mathbb{R}$ una funció contínua tal que f és derivable respecte la segona variable i $\frac{\partial f}{\partial y}(x,y)$ és contínua en $[a,b]\times[c,d]$. Aleshores la funció*

$$F(y) = \int_a^b f(x,y)\mathrm{d}x$$

és derivable en l'interval (c,d) i

$$F'(y) = \int_a^b \frac{\partial f}{\partial y}(x,y)\mathrm{d}x.$$

Demostració. □

Exemple 10.2.2 (Integral de Gauss)**.** *Volem calcular el valor de la integral*

$$\int_{-\infty}^\infty e^{-x^2}\mathrm{d}x.$$

Solució. $\sqrt{\pi}$. ♢

Teorema 10.2.3. *Siguin $f\colon [a,b)\times[c,d]$ una funció contínua tal que la seva derivada respecte la segona variable existeix i és contínua en $[a,b)\times[c,d]$ i y_0 un real en $[c,d]$ tal que existeixi un $\delta > 0$ satisfent que la integral*

$$\int_a^b \sup_{y\in(y_0-\delta,y_0+\delta)}\left|\frac{\partial f}{\partial y}(x,y)\right|\mathrm{d}x$$

és convergent. Aleshores la funció

$$F(y) = \int_a^b f(x,y)\mathrm{d}x$$

és derivable en y_0 i

$$F'(y_0) = \int_a^b \frac{\partial f}{\partial y}(x,y_0)\mathrm{d}x.$$

Demostració. □

Exemple 10.2.4. *Volem calcular*

$$\int_0^\infty \mathrm{e}^{-tx}\frac{\sin(x)}{x}\mathrm{d}x$$

per $t > 0$.

Solució. $\frac{\pi}{2} - \arctan(t)$. ◊

Exemple 10.2.5. *Volem calcular*

$$\int_0^1 \frac{x^2-1}{\log(x)}\mathrm{d}x.$$

Solució. $\log(3)$. ◊

10.2.2 La funció Gamma d'Euler

Definició 10.2.6 (Gamma d'Euler)**.** Sigui x un real positiu. Aleshores definim

$$\Gamma(x) = \int_0^\infty t^{x-1}\mathrm{e}^{-t}\mathrm{d}t$$

com la funció Gamma d'Euler.

Teorema 10.2.7. *La funció Gamma d'Euler és convergent.*

Demostració. □

Lema 10.2.8. *Sigui $x > 0$ un real. Aleshores*

$$\Gamma(x+1) = x\Gamma(x).$$

Demostració. □

Observació 10.2.9. *Es satisfà*

$$\Gamma(1) = 1.$$

Demostració. Per la definició de Gamma d'Euler (10.2.6) tenim que

$$\Gamma(1) = \int_0^\infty \mathrm{e}^{-t}\mathrm{d}t = \left.\frac{\mathrm{e}^{-t}}{-1}\right|_0^\infty = 1.$$ □

Lema 10.2.10. *Sigui n un natural. Aleshores*

$$\Gamma(n) = (n-1)!$$

Demostració. És conseqüència del lema 10.2.8 i l'observació 10.2.9. □

Teorema 10.2.11. *Es satisfà*

$$\lim_{x\to\infty} \frac{\Gamma(x+1)}{e^{-x}x^x\sqrt{2\pi x}} = 1.$$

Demostració. □

Corol·lari 10.2.12 (Fórmula d'Stirling)**.** *Es satisfà*

$$\lim_{n\to\infty} \frac{n!}{e^{-n}n^n\sqrt{2\pi n}} = 1.$$

Exemple 10.2.13. *Volem calcular*

$$\Gamma\left(\frac{1}{2}\right).$$

Solució. $\sqrt{\pi}$. ◊

Capítol 11

Sèries de Fourier

11.1 Funcions periòdiques

11.1.1 Funcions periòdiques complexes

Definició 11.1.1 (Funció T-periòdica)**.** Sigui $f\colon \mathbb{R} \longrightarrow \mathbb{C}$ una funció tal que existeix un $T > 0$ real satisfent

$$T = \min_{T\in\mathbb{R}^+} \{f(x+T) = f(x) \text{ per a tot } x \in \mathbb{R}\}.$$

Aleshores direm que f és una funció T-periòdica.

Exemple 11.1.2. *Volem veure que les funcions*

$$f(t) = \sin(2\pi\omega t), \quad g(t) = \cos(2\pi\omega t) \quad i \quad h(t) = \mathrm{e}^{2\pi\mathrm{i}\omega t}$$

són funcions $\frac{1}{\omega}$-periòdiques.

Solució. ◊

Lema 11.1.3. *Sigui f una funció T periòdica. Aleshores $f(x+T') = f(x)$ per a tot x real si i només si existeix un enter K tal que $T' = KT$.*

Demostració. □

Proposició 11.1.4. *Sigui f una funció T-periòdica i integrable. Aleshores per a tot a real es satisfà*

$$\int_0^T f(x)\mathrm{d}x = \int_a^{a+T} f(x)\mathrm{d}x.$$

Demostració. □

Lema 11.1.5. *Sigui f una funció T-periòdica i contínua. Aleshores $|f|$ està acotada.*

Demostració. □

Lema 11.1.6. *Sigui f una funció T-periòdica. Aleshores no existeix cap sèrie de potències $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ tal que $\sum_{n=0}^{\infty} a_n(x-x_0)^n$ convergeixi uniformement a f en $\mathbb{R}$.*

Demostració. □

11.1.2 Funcions contínues a trossos

Definició 11.1.7 (Funció contínua a trossos)**.** Sigui $f\colon [0,1] \longrightarrow \mathbb{C}$ una funció tal que el conjunt

$$\{x \in [0,1] \mid f \text{ té una discontinuïtat salt finit en } x\}$$

és finit. Aleshores direm que f és contínua a trossos.

Denotarem

$$\mathcal{C} = \{f\colon [0,1] \longrightarrow \mathbb{C} \mid f \text{ és contínua a trossos}\}.$$

Observació 11.1.8. *Si f pertany a $\mathcal{C}$ aleshores f és integrable Riemann.*

Demostració. □

Definició 11.1.9 (Conjunt d'extensions periòdiques)**.** Denotarem

$$\mathcal{P} = \{f\colon \mathbb{R} \longrightarrow \mathbb{C} \mid g \in \mathcal{C} \text{ i } f(x) = g(x-k) \text{ per } x \in [k, k+1), k \in \mathbb{Z}\}$$

com el conjunt d'extensions periòdiques. Direm que els elements de $\mathcal{P}$ són extensions periòdiques.

Lema 11.1.10. *Siguin f i g dues extensions periòdiques i λ un nombre complex. Aleshores el conjunt $\mathcal{P}$ amb les operacions*

$$(f+g)(x) = f(x) + g(x) \quad i \quad (\lambda f)(x) = \lambda f(x)$$

és un espai vectorial.

Demostració. □

Teorema 11.1.11. *Sigui E un $\mathcal{P}$-espai vectorial amb el producte escalar*

$$\langle f, g\rangle = \int_0^1 f(x)\overline{g(x)}\mathrm{d}x. \tag{11.1}$$

Aleshores E amb la norma (11.1) és un espai vectorial euclidià.

Demostració. □

Exemple 11.1.12. *Volem veure que el conjunt*

$$\{e_n(x) = e^{2\pi i n x} \mid n \in \mathbb{Z}\}$$

és un conjunt ortonormal de $\mathcal{P}$.

Solució. ◊

11.2 Sèries de Fourier

11.2.1 Coeficients de Fourier

Definició 11.2.1 (Coeficients de Fourier)**.** Sigui f una extensió periòdica. Definim

$$\widehat{f}(n) = \langle f(x), \mathrm{e}^{2\pi \mathrm{i} nx} \rangle = \int_0^1 f(x)\mathrm{e}^{-2\pi \mathrm{i} nx}\mathrm{d}x$$

com l'n-èsim coeficient de Fourier de f.

Proposició 11.2.2. *Siguin f i g dues extensions periòdiques i λ i μ dos nombres complexos. Aleshores*

$$\widehat{\lambda f + \mu g}(n) = \lambda \widehat{f}(n) + \mu \widehat{g}(n).$$

Demostració. □

Proposició 11.2.3. *Sigui f una extensió periòdica, τ un nombre de $(0,1)$ i f_τ una funció definida com $f_\tau(x) = f(x-\tau)$. Aleshores*

$$\widehat{f_\tau}(n) = \mathrm{e}^{-2\pi \mathrm{i} n\tau} \widehat{f}(n).$$

Demostració. □

Proposició 11.2.4. *Sigui f una extensió periòdica derivable. Aleshores*

$$\widehat{f'}(n) = 2\pi \mathrm{i} n \widehat{f}(n).$$

Demostració. □

Proposició 11.2.5. *Siguin f i g dues extensions periòdiques. Aleshores*

$$\widehat{f * g}(n) = \widehat{f}(n)\widehat{g}(n).$$

Demostració. □

Definició 11.2.6 (Sèrie de Fourier)**.** Sigui f una extensió periòdica. Aleshores definim

$$\mathrm{S}(f)(x) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)\mathrm{e}^{2\pi \mathrm{i} nx}$$

com la sèrie de Fourier de f.

Exemple 11.2.7. *Volem trobar la sèrie de Fourier de l'extensió periòdica de la funció*

$$f(x) = \begin{cases} \sin(\pi x) & \text{si } 0 \le x \le \frac{1}{2} \\ 0 & \text{si } \frac{1}{2} \le x \le 1 \end{cases}$$

Solució. $\mathrm{S}(f)(x) = \frac{1}{2}\sin(\pi x) - \frac{4}{\pi}\sum_{n=1}^{\infty}(-1)^n \frac{n}{4n^2-1}\sin(2\pi nx)$. ◊

Proposició 11.2.8. *Siguin f i g dues extensions periòdiques i λ i μ dos nombres complexos. Aleshores*

$$\mathrm{S}(\lambda f + \mu g)(n) = \lambda\, \mathrm{S}(f)(n) + \mu\, \mathrm{S}(g)(n).$$

Demostració. □

11.2.2 Paritat d'una funció

Definició 11.2.9 (Paritat d'una funció)**.** Sigui $f\colon \mathbb{R} \longrightarrow \mathbb{C}$ una funció tal que per a tot x real es satisfà

1. $f(x) = f(-x)$. Aleshores direm que f és una funció parell.
2. $f(x) = -f(-x)$. Aleshores direm que f és una funció senar.

Exemple 11.2.10. *Volem veure que la funció*

$$f(x) = \sin(x)$$

és senar i que la funció

$$g(x) = \cos(x)$$

és parell.

Solució. $\Diamond$

Proposició 11.2.11. *Siguin f una funció parell i g una funció senar. Aleshores les funcions f^2 i g^2 són parells i la funció fg és senar.*

Demostració. $\square$

Proposició 11.2.12. *Siguin f una funció parell i g una funció senar tals que f i g són integrables en l'interval $[-a, a]$. Aleshores*

$$\int_{-a}^{a} f(x)\mathrm{d}x = 2\int_{0}^{a} f(x)\mathrm{d}x \quad i \quad \int_{-a}^{a} g(x)\mathrm{d}x = 0.$$

Demostració. $\square$

Lema 11.2.13. *Sigui f una extensió periòdica tal que*

1. *f és parell. Aleshores $\widehat{f}$ és parell.*
2. *f és senar. Aleshores $\widehat{f}$ és senar.*

Demostració. $\square$

11.2.3 Sèries de Fourier en termes de sinus i cosinus

Proposició 11.2.14. *Sigui f una extensió periòdica parell. Aleshores*

$$\mathrm{S}(f)(x) = A_0 + 2\sum_{n=1}^{\infty} A_n \cos(2\pi n x),$$

on

$$A_n = \int_{0}^{1} f(x)\cos(2\pi n x)\mathrm{d}x.$$

Demostració. $\square$

Proposició 11.2.15. *Sigui f una extensió periòdica senar. Aleshores*

$$\mathrm{S}(f)(x) = 2\sum_{n=1}^{\infty} B_n \sin(2\pi n x),$$

on

$$B_n = \int_0^1 f(x)\sin(2\pi n x)\mathrm{d}x.$$

Demostració. □

Teorema 11.2.16. *Sigui f una extensió periòdica. Aleshores*

$$\mathrm{S}(f)(x) = A_0 + 2\sum_{n=1}^{\infty} A_n \cos(2\pi n x) + 2\sum_{n=1}^{\infty} B_n \sin(2\pi n x),$$

on

$$A_n = \int_0^1 f(x)\cos(2\pi n x)\mathrm{d}x \quad i \quad B_n = \int_0^1 f(x)\sin(2\pi n x)\mathrm{d}x.$$

Demostració. □

11.3 Transformació de Fourier

11.3.1 Convolució de funcions 1-periòdiques

Definició 11.3.1 (Convolució de dues extensions periòdiques)**.** Siguin f i g dues extensions periòdiques. Aleshores definim

$$(f * g)(x) = \int_0^1 f(t)g(x-t)\mathrm{d}t$$

com la convolució de f amb g.

Definició 11.3.2 (Aproximació de la unitat en extensions periòdiques)**.** Sigui $(\phi_\varepsilon)_{\varepsilon\in\mathbb{R}}$ una successió de funcions tals que ϕ_ε és una extensió periòdica satisfent

1. $\phi_\varepsilon \geq 0$.
2. $\int_0^1 \phi_\varepsilon(x)\mathrm{d}x = 1$.
3. per a tot $\delta > 0$ tenim que

$$\lim_{\varepsilon\to 0} \sup_{x\in[\delta,1-\delta]} |\phi_\varepsilon| = 0.$$

Aleshores direm que (ϕ_ε) és una aproximació de la unitat.

Teorema 11.3.3. *Sigui f una extensió periòdica contínua i $(\phi_\varepsilon)_{\varepsilon>0}$ una aproximació de la unitat en extensions periòdiques. Aleshores $f * \phi_\varepsilon$ convergeix uniformement a f en $\mathbb{R}$ quan ε tendeix a 0.*

Demostració. Per la definició d'aproximació de la unitat en extensions periòdiques (11.3.2) trobem que
$$\int_0^1 \phi_\varepsilon(x)\mathrm{d}x = 1,$$
i per 11.1.4 tenim que
$$\int_0^1 \phi_\varepsilon(x-t)\mathrm{d}t = 1,$$
i per tant
$$f(x) = \int_0^1 f(x)\phi_\varepsilon(x-t)\mathrm{d}t.$$

Considerem
$$\sup_{x\in[0,1]} |(f*\phi_\varepsilon)(x) - f(x)|.$$

Tenim qe
$$\begin{aligned}
\sup_{x\in[0,1]} |(f*\phi_\varepsilon)(x) - f(x)| &= \sup_{x\in[0,1]} \left|\int_0^1 f(t)\phi_\varepsilon(x-t)\mathrm{d}t - f(x)\right| && (11.3.1)\\
&= \sup_{x\in[0,1]} \left|\int_0^1 f(t)\phi_\varepsilon(x-t)\mathrm{d}t - \int_0^1 f(x)\phi_\varepsilon(x-t)\mathrm{d}t\right|\\
&= \sup_{x\in[0,1]} \left|\int_0^1 (f(t)-f(x))\phi_\varepsilon(x-t)\mathrm{d}t\right|\\
&\leq \sup_{x\in[0,1]} \int_0^1 |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t && (7.1.19)\\
&= \sup_{x\in[0,1]} \int_{x-\frac{1}{2}}^{x+\frac{1}{2}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t. && (11.1.4)
\end{aligned}$$

Tenim per hipòtesi que f és contínua, i per la definició de funció contínua (5.2.4) trobem que per a tot $\eta > 0$ existeix un $\delta > 0$ tal que per a tot t satisfent $|x-t| > \delta$ tenim
$$|f(x) - f(x)| \leq \frac{\eta}{2}.$$
Per tant, amb $I = [x-\frac{1}{2}, x+\frac{1}{2}]$ i $J = [0,1]$,
$$\begin{aligned}
&\sup_{x\in J} \int_{x-\frac{1}{2}}^{x+\frac{1}{2}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t =\\
&= \sup_{x\in J}\left(\int_{\substack{t\in I\\|x-t|<\delta}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t + \int_{\substack{t\in I\\|x-t|>\delta}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t\right)\\
&\leq \sup_{x\in J}\left(\frac{\eta}{2}\int_{\substack{t\in I\\|x-t|<\delta}} \phi_\varepsilon(x-t)\mathrm{d}t + \int_{\substack{t\in I\\|x-t|>\delta}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t\right)\\
&< \sup_{x\in J}\left(\frac{\eta}{2} + \int_{\substack{t\in I\\|x-t|>\delta}} |f(t)-f(x)|\phi_\varepsilon(x-t)\mathrm{d}t\right),
\end{aligned}$$

i, amb $y = x - t$ tenim que

$$\int_{\substack{t\in I\\|x-t|>\delta}} |f(t) - f(x)|\phi_\varepsilon(x-t)\mathrm{d}t = \int_{\substack{t\in[-\frac{1}{2},\frac{1}{2}]\\|y|>\delta}} |f(x-y) - f(x)|\phi_\varepsilon(y)\mathrm{d}y$$

□

11.3.2 Polinomis trigonomètrics

Definició 11.3.4.

Bibliografia

[1] Alejandro Molero Casanova. «Anàlisi Matemàtica». 2018.

[2] *Lectures 7 and 8: The Riemann series theorem*. 18 de des. de 2018. URL: https://math.uchicago.edu/~j.e.hickman/163%20Lecture%20notes/Lecture%207%20and%208.pdf.

[3] *Differentiating under the integral sign*. 18 de des. de 2018. URL: http://www.math.uconn.edu/~kconrad/blurbs/analysis/diffunderint.pdf.

[4] Félix Galindo Soto, Javier Sanz Gil i Luis A. Tristán Vega. *Guía práctica de cálculo infinitesimal en varias variables*. Castellà. Ediciones Paraninfo, 2005. ISBN: 978-8497323895.

[5] Joaquín M. Ortega Aramburu. *Introducció a l'anàlisi matemàtica*. Servei de Publicacions de la Universitat Autònoma de Barcelona, 2002. ISBN: 84-490-2271-1.

[6] Carles Perelló Valls. *Càlcul infinitesimal: amb mètodes numèrics i aplicacions*. Enciclopèdia Catalana, S.A., 1994. ISBN: 84-7739-518-7.

[7] Walter Rudin. *Principles of Mathematical Analysis*. Anglès. McGraw-Hill Education, 1976. ISBN: 978-0070542358.

[8] Georgi P. Tolstov. *Fourier Series*. Anglès. Dover Publications, 1976. ISBN: 9780486633176.

Els apunts estan escrits seguint la teoria donada a classe i complementats amb [1]. La secció de reordenació de sèries està fortament inspirada també en [2]. He copiat un exemple de [3].

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

Part VI

Estructures algebraiques

Capítol 12

Teoria de grups

12.1 Grups

12.1.1 Propietats bàsiques dels grups

Definició 12.1.1 (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 12.1.2. *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 12.1.3 (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 12.1.2.

Notació 12.1.4. 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 12.1.5. *Siguin G un grup amb l'operació $*$ i a, b, c tres elements de G. Aleshores*

1. $a * c = b * c \implies a = b$.
2. $c * a = c * b \implies a = b$.

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 (12.1.1) 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 12.1.6. *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 (12.1.1), 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 12.1.5 ha de ser $a' = a''$, com volíem demostrar. □

Definició 12.1.7 (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 12.1.6 i la notació introduïda en 12.1.4.

Proposició 12.1.8. *Sigui G un grup amb l'operació $*$ i element neutre e. Aleshores*

$$e^{-1} = e.$$

Demostració. Per la definició de grup (12.1.1) tenim que

$$e * e^{-1} = e^{-1} * e = e,$$

i per ha de ser $e^{-1} = e$. □

Proposició 12.1.9. *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 12.1.5 ha de ser

$$a = \left(a^{-1}\right)^{-1}.$$ □

Proposició 12.1.10. *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 12.1.6 tenim que $a * b$ és la inversa de $b^{-1} * a^{-1}$, és a dir

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$ □

Lema 12.1.11. *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 (12.1.1) 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 (12.1.1) 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 (12.1.3),

$$e * x = x = b^{-1} * a;$$

i la unicitat ve donada per la proposició 12.1.2. □

Teorema 12.1.12. *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) $\Longrightarrow$ (2). Suposem que G és un grup amb l'operació. Veiem que G no és buit per la definició de grup (12.1.1), i la segona part és el lema 12.1.11.

Demostrem ara (2) $\Longrightarrow$ (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) $\implies$ (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 (12.1.1) i tenim que G és un grup amb l'operació $*$.

Així tenim (1) $\implies$ (2) $\implies$ (3) $\implies$ (1), com volíem veure. □

12.1.2 Subgrups i subgrups normals

Definició 12.1.13 (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 12.1.14. $e \in H$.

Proposició 12.1.15. *Siguin G un grup amb l'operació $*$ 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. Sigui e l'element neutre de G. Demostrem primer que la condició és necessària ($\implies$). Això ho podem veure per la definició de grup (12.1.1), 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 ($\impliedby$). 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 12.1.9 tenim

$$x * y^{-1} = x * y$$

i per hipòtesi $x * y \in H$.

Per tant, per la definició de grup (12.1.1) tenim que H és un grup amb l'operació $*$, i com que per hipòtesi $H \subseteq G$ per la definició de subgrup (12.1.13) tenim que H és un subgrup de G. □

Proposició 12.1.16. *Siguin G un grup, $\{H_i\}_{i\in I}$ 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 12.1.15. Siguin $*$ l'operació de G i e l'element neutre de G. Tenim $H \subseteq G$ i $H \neq \emptyset$, ja que per l'observació 12.1.14 tenim 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 12.1.15, i per tant $x * y^{-1} \in H$, com volíem veure. □

Proposició 12.1.17. *Siguin G un grup, $S \neq \emptyset$ un subconjunt de G,*

$$\{H_i\}_{i\in I} = \{H \subseteq G \mid S \leq H\}$$

una família de subgrups de G i

$$H = \bigcap_{i\in I} H_i.$$

Aleshores H i és un subgrup de G.

Demostració. Sigui e l'element neutre de G. Comprovem que $H \neq \emptyset$. En tenim prou amb veure que $e \in H$. Per veure que H és un subgrup de G ho podem fer per la proposició 12.1.16. □

Definició 12.1.18 (Mínim subgrup generat per un conjunt)**.** Siguin G un grup, S un subconjunt de G,

$$\{H_i\}_{i\in I} = \{H \subseteq G \mid S \leq H\}$$

una família de subgrups de G 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 12.1.17.

Proposició 12.1.19. *Siguin G un grup i g un element de G. Aleshores*

$$\langle \{g\} \rangle = \{g^i\}_{i\in\mathbb{Z}}.$$

Demostració. Sigui $*$ l'operació de G. 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 (12.1.18) 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 (12.1.1), 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 $g^i, g^j \in H_g$ es satisfà $g^i * g^{-j} = g^{i-j} \in H_g$, 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 12.1.20 (Ordre d'un grup)**.** Sigui G un grup. 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 12.1.21. *Siguin G un grup amb 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. Sigui $*$ l'operació de G. Comencem amb la implicació cap a l'esquerra ($\Longleftarrow$). 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 ($\Longrightarrow$). 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 (12.1.1) 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 12.1.22 (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 12.1.23 (Subgrup normal)**.** Siguin G un grup 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 12.1.24. *Siguin G un grup 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. Sigui $*$ l'operació de G. Comencem demostrant (1) $\implies$ (2). Suposem que H és un subgrup normal de G, per la definició de subgrup normal (12.1.23) 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) $\implies$ (3). Suposem que $\{x\}H\{x^{-1}\} = H$. Tenim que $\{x\}H\{x^{-1}\} = H \subseteq H$.

Demostrem ara (3) $\implies$ (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 (12.1.1), $x * h = h' * x \in H$, 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) $\implies$ (2) $\implies$ (3) $\implies$ (1) i hem acabat. $\square$

12.1.3 Grups cíclics i grups abelians

Definició 12.1.25 (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 12.1.26. *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 ($\implies$) ho podem veure amb la definició de grup abelià (12.1.25) i la proposició 12.1.10.

Demostrem ara que la condició és suficient ($\impliedby$). Diem que l'element neutre de G és e. Per la definició de grup (12.1.1) tenim que

$$(a + b) - (a + b) = e, \tag{12.1}$$

que és equivalent a

$$(a+b)-(a+b)-(-(a+b)) = -(-(a+b)),$$

i aleshores

$$\begin{aligned} a+b &= -(-(a+b)) \\ &= -(-b-a) && \text{(Proposició 12.1.10)} \\ &= -(-(b+a)) && \text{(Hipótesi (12.1))} \\ &= b+a, && \text{(Proposició 12.1.9)} \end{aligned}$$

i per la definició de grup abelià (12.1.25), G és un grup abelià. □

Definició 12.1.27 (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 12.1.28. *Sigui G un grup cíclic. Aleshores G és un grup abelià.*

Demostració. Sigui $*$ l'operació de G. Com que G és un grup cíclic, per la definició de grup cíclic (12.1.27) 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 (12.1.25) hem acabat. □

Proposició 12.1.29. *Siguin G un grup cíclic i H un subgrup de G. Aleshores H és un grup cíclic.*

Demostració. Siguin $*$ l'operació de G i e l'element neutre de G. Per l'observació 12.1.14 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 (12.1.1) 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 12.1.19 $H = \langle\{g^m\}\rangle$ i hem acabat. □

Proposició 12.1.30. *Siguin G un grup cíclic d'ordre n finit i $d \in \mathbb{N}$ un divisor de n. Aleshores existeix un únic subgrup de G d'ordre d.*

Demostració. □

12.1.4 Grup quocient

Proposició 12.1.31. *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 12.1.14.

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 (12.1.1) tenim que $(x * y^{-1})^{-1} \in H$, ja que per hipòtesi H és un grup, i per les proposicions 12.1.10 i 12.1.9 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 12.1.32. *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 12.1.33 (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 12.1.32.

Lema 12.1.34. *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 12.1.35. $\{x\}G = G$.

Teorema 12.1.36 (Teorema de Lagrange)**.** *Siguin G un grup d'ordre finit i H un subgrup de G. Aleshores $|H|$ divideix $|G|$.*

Demostració. Sigui $*$ l'operació de G. Fixem $x \in G$ i considerem la funció

$$\begin{aligned} f_x \colon H &\longrightarrow \{x\}H \\ h &\longmapsto x * h \end{aligned}$$

Pel lema 12.1.34 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 $|G|$. □

Corol·lari 12.1.37. *Sigui G un grup d'ordre p primer. 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 (12.1.36) 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 (12.1.27) tenim que G és un grup cíclic. □

Definició 12.1.38 (L'índex d'un subgrup en un grup)**.** Siguin G un grup i H un subgrup de G. Aleshores definim

$$[G : H] = \frac{|G|}{|H|}$$

com l'índex de H a G.

[1] de fet, $f_x^{-1} = f_{x^{-1}}$

12.2 Tres Teoremes d'isomorfisme entre grups

12.2.1 Morfismes entre grups

Definició 12.2.1 (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 que 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 12.2.2. *Siguin G_1 un grup amb element neutre e, G_2 un grup amb element neutre e' i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. $f(e) = e'$.
2. $f\bigl(x^{-1}\bigr) = f(x)^{-1}$ *per a tot* $x \in G_1$.

Demostració. Siguin $*$ l'operació del grup G_1 i $\circ$ l'operació del grup G_2. Veiem primer el punt (1). Per la definició de morfisme tenim que per a tot $x \in G_1$

$$\begin{aligned} f(x) \circ f(e) &= f(x * e) && \text{(morfisme entre grups (12.2.1))}\\ &= f(x) && \text{(l'element neutre d'un grup (12.1.3))}\\ &= f(x) \circ e' \end{aligned}$$

i per la proposició 12.1.5 tenim $f(e) = e'$.

Per demostrar el punt (2) en tenim prou en veure que per a tot $x \in G$

$$\begin{aligned} f(x) \circ f(x^{-1}) &= f(x * x^{-1}) && \text{(morfisme entre grups (12.2.1))}\\ &= f(e) && \text{(l'invers d'un element d'un grup (12.1.7))}\\ &= f(x^{-1} * x) && \text{(morfisme entre grups (12.2.1))}\\ &= f(x^{-1}) \circ f(x) \end{aligned}$$

i pel punt (1) d'aquesta proposició $f(x) \circ f(x^{-1}) = f(x^{-1}) \circ f(x) = e'$, i per la proposició 12.1.6 tenim que $f(x^{-1}) = f(x)^{-1}$, com volíem. □

Proposició 12.2.3. *Siguin G, H i K tres grups 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. Siguin $*$, $\circ$ i $+$ les operacions de G, H i K, respectivament. Per la definició de morfisme entre grups (12.2.1) 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 (12.2.1) hem acabat. □

Proposició 12.2.4. *Siguin G_1 i G_2 dos grups tals 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. Siguin $*$ l'operació de G_1 i $\circ$ l'operació de G_2. Per la definició de isomorfisme entre grups (12.2.1) tenim que existeix un $f: G_1 \to G_2$ un isomorfisme entre grups.

Comencem demostrant el punt (1). Suposem doncs que G_1 és un grup abelià. Per la definició de grup abelià (12.1.25) 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 (12.2.1) tenim que

$$f(a) \circ f(b) = f(b) \circ f(a),$$

i per tant, com que per la definició de isomorfisme entre grups (12.2.1) f és un bijectiu, G_2 satisfà la definició de grup abelià (12.1.25).

Demostrem ara el punt (2). Suposem doncs que G_1 és un grup cíclic. Per la definició de grup cíclic (12.1.27) 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 (12.2.1) 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 (12.2.1) tenim que[2] $f(g^i) = f(g)^i$, i per la definició de grup cíclic (12.1.27) G_2 és un grup cíclic. □

Definició 12.2.5 (Nucli i imatge d'un morfisme entre grups)**.** Siguin G_1 un grup amb element neutre e, G_2 un grup amb element neutre e' i $f: G_1 \to G_2$ 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 12.2.6. $\ker(f) \subseteq G_1$, $\mathrm{Im}(f) \subseteq G_2$.

[2] el primer és amb l'operació $*$ i el segon amb l'operació $\circ$.

Proposició 12.2.7. *Siguin G_1 i G_2 dos grups 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 12.2.6.

Siguin $*$ l'operació de G_1 i $\circ$ l'operació de G_2 i e l'element neutre de G_1 i e' l'element neutre de G_2. Primer comprovem el punt (1). Comencem veient que $\ker(f)$ és un subgrup de G_1. Per la proposició 12.1.15 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 12.1.24 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 12.1.15 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 (12.2.1) i la proposició 12.2.2 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 (12.2.1) 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 12.2.8. *Siguin G_1 un grup amb element neutre e, G_2 un grup, 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. Siguin $*$ l'operació de G_1, $\circ$ l'operació de G_2 i e' l'element neutre de G_2. Comencem fent la demostració del punt (1) per la implicació cap a la dreta ($\Longrightarrow$). Suposem doncs que f és un monomorfisme, i per tant injectiva. Per la definició de nucli d'un morfisme entre grups (12.2.5) 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 12.2.2 ha de ser $\ker(f) = \{e\}$.

Demostrem ara la implicació cal a l'esquerra ($\Longleftarrow$). 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 12.2.7 $\ker(f)$ és un subgrup de G_1, tenim que $x*y^{-1} \in G_1$, i per tant

$$\begin{aligned} f(x * y^{-1}) &= f(x) \circ f(y^{-1}) && \text{(morfisme entre grups (12.2.1))} \\ &= f(x) \circ f(y)^{-1} && \text{(Proposició 12.2.2)} \\ &= f(y) \circ f(y)^{-1} = e', \end{aligned}$$

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 ($\Longrightarrow$). 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 (12.2.5) tenim que $\operatorname{Im}(f) = G_2$.

Acabem demostrant la implicació cap a l'esquerra ($\Longleftarrow$). Suposem doncs que $\operatorname{Im}(f) = G_2$ i prenem $y \in G_2$. Aleshores per la definició d'imatge d'un morfisme entre grups (12.2.5) tenim que existeix un $x \in G_1$ tal que $f(x) = y$, i per tant f és exhaustiva. $\square$

Proposició 12.2.9. *Siguin G_1 i G_2 dos grups i $f\colon G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *Si $H_1 \leq G_1 \implies \{f(h) \in G_2 \mid h \in H_1\} \leq G_2$.*
2. *Si $H_2 \leq G_2 \implies \{h \in G_1 \mid f(h) \in H_2\} \leq G_1$.*
3. *Si $H_2 \trianglelefteq G_2 \implies \{h \in G_1 \mid f(h) \in H_2\} \trianglelefteq G_1$.*

Demostració. Siguin $*$ l'operació de G_1 i $\circ$ l'operació de G_2. 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 12.1.15 només ens cal veure que $f(x) \circ f(y)^{-1} \in H$. Això és

$$\begin{aligned} f(x) \circ f(y)^{-1} &= f(x) \circ f(y^{-1}) && \text{(Proposició 12.2.2)} \\ &= f(x * y^{-1}). && \text{(morfisme entre grups (12.2.1))} \end{aligned}$$

Ara bé, com que $x, y \in H_1$ i H_1 és un subgrup de G_1, per la proposició 12.1.15 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 (12.2.1) i la proposició 12.2.2 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 12.1.15 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 (12.1.1) ha de ser $f(x) \circ f(y^{-1}) \in H_2$ Aleshores, per la definició de morfisme entre grups (12.2.1) 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

$$\begin{aligned} f(g) \circ f(h) \circ f(g)^{-1} &= f(g) \circ f(h) \circ f(g^{-1}) && \text{(Proposició 12.2.2)} \\ &= f(g * h * g^{-1}) && \text{(morfisme entre grups (12.2.1))} \end{aligned}$$

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 (12.1.23) per la proposició 12.1.24. $\square$

Teorema 12.2.10 (Teorema de representació de Cayley)**.** *Sigui G un grup amb l'operació $*$. Aleshores G és isomorf a un subgrup de S_G amb l'operació $\circ$, on S_G és el grup simètric dels elements de G.*

Demostració. Sigui e l'element neutre de G. Definim

$$\varphi\colon G \longrightarrow \mathrm{S}_G \tag{12.2}$$
$$g \longmapsto \sigma_g : G \longrightarrow G \tag{12.3}$$
$$x \longmapsto g * x$$

Tenim que σ_g és bijectiva ja que és una permutació. Comprovarem que φ és un monomorfisme entre grups. Veiem primer que és un morfisme entre grups. Prenem $g, g' \in G$. Per la definició (12.2) 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 (12.2.1) tenim que φ és un morfisme entre grups. Veiem ara que φ és un monomorfisme. Per la definició de nucli d'un morfisme entre grups (12.2.5) tenim que

$$\ker(\varphi) = \{x \in G \mid f(x) = \mathrm{Id}_G\}.$$

Ara bé, $\sigma_g = \mathrm{Id}$ és, per la definició (12.3), equivalent a dir que $g * x = x$ per a tota $x \in G$, i per la definició de l'element neutre d'un grup (12.1.3) això és si i només si $g = e$, i per tant

$$\ker(\varphi) = \{e\},$$

i per la proposició 12.2.8 tenim que φ és un monomorfisme, com volíem veure.

Per tant, per la proposició 12.2.9 tenim que

$$G \cong \mathrm{Im}(\varphi) \leq \mathrm{S}_G\,. \qquad \square$$

Corol·lari 12.2.11. *Si G té ordre $n!$ aleshores $G \cong \mathrm{S}_n$.*

12.2.2 Teoremes d'isomorfisme entre grups

Teorema 12.2.12. *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

$$\varphi\colon G_1/\ker(f) \longleftrightarrow \mathrm{Im}(f) \tag{12.4}$$
$$[x] \longmapsto f(x)$$

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

$$\begin{aligned}\varphi([x']) &= \varphi([x * h]) && \text{(Definició (12.1.33))}\\ &= f(x * h) && \text{(Definició (12.4))}\\ &= f(x) \circ f(h) && \text{(morfisme entre grups (12.2.1))}\\ &= f(x) \circ e' && \text{(nucli d'un morfisme entre grups (12.2.5))}\\ &= f(x) = \varphi([x]) && \text{(Definició (12.4))}\end{aligned}$$

i per tant φ està ben definida. Veiem ara que φ és un morfisme entre grups. Tenim que

$$\begin{aligned}
\varphi([x]*[y]) &= \varphi([x*y]) && \text{(Definició (12.1.33))}\\
&= f(x*y) && \text{(Definició (12.4))}\\
&= f(x)\circ f(y) && \text{(morfisme entre grups (12.2.1))}\\
&= \varphi([x])\circ\varphi([y]), && \text{(Definició (12.4))}
\end{aligned}$$

i per la definició de morfisme entre grups (12.2.1) φ és un morfisme entre grups. Continuem demostrant que φ és injectiva. Per la definició de nucli d'un morfisme entre grups (12.2.5) 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 12.2.8 φ és injectiva.

Per veure que φ és exhaustiva veiem que si $[x] \in G_1/\ker(f)$, per la definició de grup quocient (12.1.33) tenim que $x = x' * y$ per a uns certs $x' \in G_2$, $h \in \ker(f)$, i per tant

$$\begin{aligned}
\varphi([x]) &= \varphi([x'*h])\\
&= \varphi([x']*[h]) && \text{(grup quocient (12.1.33))}\\
&= f(x')\circ f(e) && \text{(morfisme entre grups (12.2.1))}\\
&= f(x') && \text{(grup (12.1.1))}\\
&= f(x*h^{-1})\\
&= f(x)\circ f(h^{-1}) && \text{(morfisme entre grups (12.2.1))}\\
&= f(x)\circ f(h)^{-1} && \text{(Proposició 12.2.2)}\\
&= f(x)\circ e^{-1} = f(x). && \text{(Proposició 12.1.8)}
\end{aligned}$$

Així veiem que $\operatorname{Im}(\varphi) = \operatorname{Im}(f)$. Per tant φ és un isomorfisme, i per la definició d'isomorfisme entre grups (12.2.1) tenim $G_1/\ker(f) \cong \operatorname{Im}(f)$, com volíem veure. $\square$

Teorema 12.2.13 (Primer Teorema de l'isomorfisme)**.** *Siguin G_1 i G_2 dos grups i $f\colon G_1 \to G_2$ un epimorfisme entre grups. Aleshores*

1. *$G_1/\ker(f) \cong G_2$.*
2. *L'aplicació*

$$\begin{aligned}
\varphi_1\colon \{H \mid \ker(f) \le H \le G\} &\longleftrightarrow \{K \mid K \le G_2\}\\
H &\longmapsto \{f(h) \in G_2 \mid h \in H\}
\end{aligned} \tag{12.5}$$

és bijectiva.

3. *L'aplicació*

$$\begin{aligned}
\varphi_2\colon \{H \mid \ker(f) \le H \trianglelefteq G\} &\longleftrightarrow \{K \mid K \trianglelefteq G_2\}\\
H &\longmapsto \{f(h) \in G_2 \mid h \in H\}
\end{aligned} \tag{12.6}$$

és bijectiva.

Demostració. Siguin $*$ l'operació de G_1, e l'element neutre de G_1 i e' l'element neutre de G_2.

El punt (1) és conseqüència del Teorema 12.2.12, 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 φ_1 està ben definida. Siguin $H_1 = H_2 \in \{H \mid \ker(f) \leq H \leq G\}$. Aleshores, per la hipòtesi (12.5) 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 φ_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 (12.5) 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 12.1.6 i la definició de l'invers d'un element d'un grup (12.1.7) i la proposició 12.1.8 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 (12.2.5) tenim $h_2^{-1} * h_1, h_1^{-1} * h_2 \in \ker(f)$, i per la hipòtesi (12.5) 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 φ_1 és exhaustiva tenim que per la proposició 12.2.9 i per la hipòtesi (12.5) 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 (12.2.5) tenim que es compleix $\ker(f) \leq H \leq G_1$, i per tant $\varphi_1(H) = K$, i per tant φ 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 12.2.14. *Siguin G un grup 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. Sigui $*$ l'operació de G. Comencem veient el punt (1). Per la proposició 12.1.15 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 $x * y^{-1}$:

$$\begin{aligned}
x * y^{-1} &= h_1 * k_1 * (h_2 * k_2)^{-1} \\
&= h_1 * k_1 * k_2^{-1} * h_2^{-1} && \text{(Proposició 12.1.10)} \\
&= h_1 * k_1 * h_2^{-1} * k_2^{-1}, && \text{(subgrup normal (12.1.23))} \\
&= h_1 * h_2^{-1} * k_1 * k_2^{-1}, && \text{(subgrup normal (12.1.23))}
\end{aligned}$$

i com que, per la definició de grup (12.1.1) 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). □

Lema 12.2.15. *Siguin G un grup, H un subgrup de G i K un subgrup normal de G. Aleshores $H \cap K \trianglelefteq H$.*

Demostració. Siguin $*$ l'operació de G. Prenem $x \in H$ i $y \in H \cap K$. Per la proposició 12.1.24 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 12.1.24, 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 (12.1.1) tenim que $x^{-1} * y * x \in H$, i per tant $x^{-1} * y * x \in H \cap K$. □

Teorema 12.2.16 (Segon Teorema de l'isomorfisme)**.** *Siguin G un grup, 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 lema 12.2.15.

Siguin $*$ l'operació de G i e l'element neutre de G. Definim

$$\begin{aligned} f\colon HK &\longrightarrow H/(H \cap K) \\ h * k &\longmapsto [h]. \end{aligned} \tag{12.7}$$

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 (12.1.7) 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 (12.1.1) 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 (12.1.33) 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

$$\begin{aligned} f(h_1 * k_1 * h_2 * k_2) &= [h_1 * h_2] && \text{(Definició (12.7))} \\ &= [h_1] * [h_2] && \text{(Definició (12.1.33))} \\ &= f(h_1 * k_1) * f(h_2 * k_2) && \text{(Definició (12.7))} \end{aligned}$$

i per tant f satisfà la definició de morfisme entre grups (12.2.1).

Continuem veient que f és exhaustiva. Prenem $[h] \in H/(H \cap K)$. Per la definició (12.7) 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 (12.2.13) tenim

$$HK/\ker(f) \cong H/(H \cap K).$$

Ara bé, per la definició de nucli d'un morfisme entre grups (12.2.5) 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 12.2.17 (Tercer Teorema de l'isomorfisme)**.** *Siguin G un grup 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 φ_1 i φ_2 són morfismes.

Per la proposició 12.2.3 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 (12.2.13) 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 (12.1.33) tenim que $G/K = \{gK \mid g \in G\}$ i $H/K = \{hK \mid h \in H\}$, i per tant

$$(G/K)/(H/K) = \{gKhK \mid g \in G, h \in H\}, \tag{12.8}$$

però com que, per hipòtesi, H i K són subgrups normals de G, per la definició de subgrup normal (12.1.23) podem reescriure (12.8) com

$$(G/K)/(H/K) = \{ghK \mid g \in G, h \in H\}. \tag{12.9}$$

Ara bé, com que per hipòtesi $K \subseteq H$ podem reescriure (12.9) com

$$(G/K)/(H/K) = \{gH \mid g \in G\},$$

i trobem, per la definició de nucli d'un morfisme entre grups (12.2.5), que $\ker(\varphi_2(\varphi_1)) = H$, i per tant

$$G/H \cong (G/K)/(H/K).$$ □

12.3 Tres Teoremes de Sylow

12.3.1 Accions sobre grups

Definició 12.3.1 (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 12.3.2. *Siguin X un G-conjunt amb l'acció $\cdot$ i $\sim$ una relació sobre el conjunt 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. Siguin $*$ l'operació de G i 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 d'acció d'un grup sobre un conjunt (12.3.1) 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 d'acció d'un grup sobre un conjunt (12.3.1) 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 d'acció d'un grup sobre un conjunt (12.3.1) 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. $\square$

Definició 12.3.3 (Òrbita d'un element d'un G-conjunt)**.** Siguin X un G-conjunt amb l'acció $\cdot$ 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 12.3.2.

Definició 12.3.4 (Estabilitzador d'un element per una acció)**.** Siguin X un G-conjunt amb l'acció $\cdot$ i x un element de 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 12.3.5. *Siguin X un G-conjunt amb l'acció $\cdot$ 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. Sigui $*$ l'operació de G. Per la definició de l'estabilitzador d'un element per una acció (12.3.4) 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 d'acció d'un grup sobre un conjunt (12.3.1) 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 (12.1.7) tenim que $g^{-1} \cdot x$ i per tant $g^{-1} \in \mathrm{St}(x)$. $\square$

Proposició 12.3.6. *Siguin X un G-conjunt amb l'acció $\cdot$ i $\mathrm{St}(x)$ l'estabilitzador de x per l'acció $\cdot$. Aleshores $\mathrm{St}(x)$ és un subgrup de G.*

Demostració. Sigui $*$ l'operació de G. Per la proposició 12.1.15 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 12.3.5 tenim que $g_2^{-1} \in \mathrm{St}(x)$, i per tant, per la definició de l'estabilitzador d'un element per una acció (12.3.4) tenim que $(g_1 * g_2^{-1}) \cdot x = x$, i per tant $g_1 * g_2^{-1} \in \mathrm{St}(x)$. $\square$

Proposició 12.3.7. *Siguin G un grup d'ordre finit, 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. Sigui $*$ l'operació de G. Considerem

$$\begin{aligned} f\colon G/\operatorname{St}(x) &\longrightarrow \mathcal{O}(x) \\ [g] &\longmapsto g\cdot x \end{aligned}$$

Volem veure que f és una aplicació bijectiva, per tant mirem si està ben definida:

Siguin $[g_1], [g_2] \in G/\operatorname{St}(x)$ tals que $[g_1] = [g_2]$. Per tant $g_1 = g_2 * g'$ per a cert $g' \in \operatorname{St}(x)$, i per la definició de l'estabilitzador d'un element per una acció (12.3.4) tenim $g_1 \cdot x = x$, $(g_2 * g')\cdot x = x$, i per la definició d'acció d'un grup sobre un conjunt (12.3.1) això és $g_2 \cdot (g'\cdot x) = x$, i per la proposició 12.3.5 $g_2 \cdot x = x$, 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 d'acció d'un grup sobre un conjunt (12.3.1), és equivalent a dir $x = (g^{-1} * g')\cdot x$, i per la definició de l'estabilitzador d'un element per una acció (12.3.4) tenim que $g^{-1} * g \in \operatorname{St}(x)$. Per tant, per la definició de grup quocient (12.1.33) 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 $|\operatorname{St}(x)| = |\mathcal{O}(x)|$, ja que per la definició d'aplicació bijectiva (2.2.9) tenim que f és una bijecció. □

12.3.2 Teoremes de Sylow

Definició 12.3.8 (p-subgrup de Sylow)**.** Siguin G un grup 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.

Lema 12.3.9. *Siguin p un primer i m un enter positiu tal que p no divideixi m. Aleshores per a tot n natural tenim que*

$$\binom{p^n m}{p^n} \tag{12.10}$$

no és divisible per p.

Demostració. Tenim que

$$\binom{p^n m}{p^n} = \frac{p^n m(p^n m - 1)\cdots(p^n m - p^n + 1)}{p^n(p^n - 1)\cdots(p^n - p^n + 1)} = \prod_{i=0}^{p^n-1} \frac{p^n m - i}{p^n - i}. \tag{12.11}$$

Com que, per hipòtesi, p és primer aquesta expressió només serà divisible per p si ho són els elements del numerador. Fixem doncs $i \in \{0, \dots, p^n+1\}$ i estudiem l'i-èsim terme del producte de (12.11). 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 (12.11) 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 (12.10) tampoc ho serà, com volíem veure. $\square$

Teorema 12.3.10 (Primer Teorema de Sylow)**.** *Siguin G un grup 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 lema 12.3.9 tenim que p no divideix k.

Siguin $*$ l'operació de G i e l'element neutre de G. Definim

$$\begin{aligned} \cdot \colon G \times \mathcal{P}_{p^n}(G) &\longrightarrow \mathcal{P}_{p^n}(G) \\ (g, X) &\longmapsto \{g\}X. \end{aligned} \tag{12.12}$$

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 (12.1.7) és $x^{-1} \cdot X$, i per tant $X \in \mathcal{P}_{p^n}(G)$.

Comprovem que $\cdot$ satisfà la definició d'acció d'un grup sobre un conjunt (12.3.1). 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 (12.1.22), $eX = X$.

De nou per la definició de conjugació entre conjunts sobre grups (12.1.22) 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 d'acció d'un grup sobre un conjunt (12.3.1).

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 (12.3.3) 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 12.3.7 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 (12.3.4) 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 12.3.6 tenim que $\mathrm{St}(X) \leq G$, i per tant, per la definició de p-subgrup de Sylow (12.3.8), $\mathrm{St}(X)$ és un p-subgrup de Sylow. □

Corol·lari 12.3.11 (Teorema de Cauchy per grups)**.** *Siguin G un grup d'ordre finit 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. Sigui e l'element neutre de G. Pel Primer Teorema de Sylow (12.3.10) tenim que existeix un p-subgrup de Sylow P de G, que per la definició de p-subgrup de Sylow (12.3.8) té ordre p^n per a cert $n \in \mathbb{N}$. Ara bé, pel Teorema de Lagrange (12.1.36) 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

$$\left(x^{p^{t-1}}\right)^p = x^{p^t} = e.$$ □

Lema 12.3.12. *Siguin G un grup d'ordre p^n on p és un primer, X un G-conjunt 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 (12.3.3) 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

$$|X| = \sum_{i=0}^{r} |\mathcal{O}(x_i)|. \tag{12.13}$$

Ara bé, per les proposicions 12.3.7 i 12.3.6 i el Teorema de Lagrange (12.1.36) 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 (12.13), que

$$|X_G| \equiv |X| \pmod{p}.$$ □

Teorema 12.3.13 (Segon Teorema de Sylow)**.** *Siguin G un grup d'ordre finit, 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. Observem que aquest enunciat té sentit pel Primer Teorema de Sylow (12.3.10).

Definim el conjunt $X = \{\{x\}P_1 \mid x \in G\}$ i

$$\begin{aligned} \cdot\colon P_2 \times X &\longrightarrow X \\ (y, \{x\}P_1) &\longmapsto \{y\}\{x\}P_1. \end{aligned} \tag{12.14}$$

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 $\{y\}\{x\}P_1 = \{y\}\{x'\}P_1$.

Siguin $*$ l'operació de G i e l'element neutre de G. Comprovem que $\cdot$ satisfà la definició d'acció d'un grup sobre un conjunt (12.3.1). 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 (12.14) 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 (12.1.1) tenim que $y * x \in G$, i per tant $y \cdot \{x\}P_1 \in X$.

Tenim que

$$\begin{aligned} e \cdot \{x\}P_1 &= \{e\}\{x\}P_1 \\ &= \{e * x\}P_1 = \{x\}P_1. && \text{(l'element neutre d'un grup (12.1.3))} \end{aligned}$$

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

$$\begin{aligned} (y * y') \cdot P_1 &= \{y * y'\}P_1 \\ &= \{y\}\{y'\}P_1 \\ &= \{y\}(\{y'\}P_1) = y \cdot (y' \cdot P_1). && \text{(Definició (12.14))} \end{aligned}$$

i per la definició d'acció d'un grup sobre un conjunt (12.3.1) tenim que X és un G-conjunt.

Definim el conjunt

$$X_{P_2} = \{\{x\}P_1 \in X \mid y \cdot \{x\}P_1 = \{x\}P_1 \text{ per a tot } y \in P_2\}. \tag{12.15}$$

Aleshores pel lema 12.3.12 tenim que

$$|X_{P_2}| \equiv |X| \pmod p.$$

Ara bé, per la definició de l'índex d'un subgrup en un grup (12.1.38) i (12.14) 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}, (12.15); 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 (12.3.8) trobem $|P_1| = |P_2| = \left|\{x^{-1}\}P_2\{x\}\right|$ i tenim que $\{x\}P_1\{x^{-1}\} = P_2$. $\square$

Corol·lari 12.3.14. *Un grup G finit té un únic p-subgrup de Sylow si i només si aquest és un subgrup normal.*

Teorema 12.3.15 (Tercer Teorema de Sylow)**.** *Siguin G un grup d'ordre $p^n m$ on p és un primer que no divideix m 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 (12.3.10) tenim que X és no buit[3] i fixem $P \in X$.
Definim

$$\begin{aligned} \cdot \colon P \times X &\longrightarrow X \\ (g, T) &\longmapsto \{g\}T\{g^{-1}\}. \end{aligned} \tag{12.16}$$

Siguin $*$ l'operació de G i e l'element neutre de G. 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 (12.3.8). Veiem ara que $\cdot$ satisfà les condicions de la definició d'acció d'un grup sobre un conjunt (12.3.1). Sigui e l'element neutre de G. Tenim que per a tot $T \in X$

$$\begin{aligned} e \cdot T &= \{e\}T\{e^{-1}\} && \text{(Definició (12.16))} \\ &= T \end{aligned}$$

i per a tot $g_1, g_2 \in P$ i $T \in X$

$$\begin{aligned} (g_1 * g_2) \cdot T &= \{g_1 * g_2\}T\{g_1 * g_2{}^{-1}\} && \text{(Definició (12.16))} \\ &= \{g_1 * g_2\}T\{g_2^{-1} * g_1^{-1}\} && \text{(Proposició 12.1.10)} \\ &= \{g_1\}\{g_2\}T\{g_2^{-1}\}\{g_1^{-1}\} \\ &= \{g_1\}(g_2 \cdot T)\{g_1^{-1}\} && \text{(Definició (12.16))} \\ &= g_1 \cdot (g_2 \cdot T) && \text{(Definició (12.16))} \end{aligned}$$

i per tant, per la definició d'acció d'un grup sobre un conjunt (12.3.1) X és un P-conjunt amb l'acció $\cdot$.
Definim el conjunt

$$X_P = \{T \in X \mid g \cdot T = T \text{ per a tot } g \in P\},$$

i per la definició (12.16) 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 lema 12.3.12 tenim que

$$|X| \equiv |X_P| \pmod{p},$$

o equivalentment

$$|X| \equiv 1 \pmod{p}.$$

[3]Tindrem que $|X| = n_p$.

Per veure que $|X|$ divideix l'ordre de G prenem $P \in X$ i tenim, pel Segon Teorema de Sylow (12.3.13) i la definició de l'òrbita d'un element d'un G-conjunt (12.3.3), 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 12.3.6 i 12.3.7 i el Teorema de Lagrange (12.1.36) tenim que $|X|$ divideix l'ordre de G. □

Corol·lari 12.3.16. *Si G té ordre $p^n q^m$ on p, q són primers amb $p < q$ aleshores $n_q = 1$, i pel corol·lari 12.3.14, el p-subgrup de Sylow de G és un subgrup normal de G.*

Capítol 13

Teoria d'anells

13.1 Anells

13.1.1 Propietats bàsiques dels anells i subanells

Definició 13.1.1 (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 13.1.2. *Sigui R un anell amb element neutre pel producte e. Aleshores l'element neutre pel producte de R és únic.*

Demostració. Sigui $\cdot$ el producte de R. Suposem que existeix un altre 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 $e = e'$ i tenim que aquest és únic. □

Definició 13.1.3 (Elements neutres d'un anell)**.** Sigui R un anell. 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 12.1.2 i la proposició 13.1.2.

Notació 13.1.4. Donat un anell R un anell amb el producte $\cdot$. Aleshores escriurem

$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot x_2 \cdot x_3.$$

Això té sentit per la definició d'anell (13.1.1). També, si el context ho permet (quan treballem amb un únic anell R), denotarem $1_R = 1$ i $0_R = 0$.

Proposició 13.1.5. *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 (13.1.3), per la definició d'anell (13.1.1) 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 (12.1.1)

$$0 \cdot a - (0 \cdot a) = 0 \cdot a + 0 \cdot a - (0 \cdot a)$$

d'on veiem

$$0 \cdot a = 0,$$

com volíem veure.

Veiem ara el punt (2). Per la definició d'anell (13.1.1) 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 (13.1.3), tenim que $a + (-1) \cdot a = (-1) \cdot a + a = 0$, però per la proposició 12.1.6 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 12.1.9 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 (13.1.1)

$$(-1) \cdot a \cdot b - (-1) \cdot (a \cdot b) = (-1 - (-1)) \cdot (a \cdot b),$$

i per la proposició 12.1.9 tenim que $-(-1) = 1$ i per tant, per la definició de grup (12.1.1) 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 12.1.6 tenim que

$$(-a) \cdot b = -(a \cdot b),$$

com volíem veure. □

Proposició 13.1.6. *Siguin R un anell amb 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 (13.1.3) trobem

$$b = b'.$$ □

Definició 13.1.7 (Element invertible)**.** Siguin R un anell amb 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 13.1.8 (L'invers d'un element)**.** Siguin R un anell amb 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 13.1.6.

Definició 13.1.9 (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 $S \leq R$.

13.1.2 Ideals i ideals principals

Definició 13.1.10 (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 13.1.11. $0 \in I$.

Notació 13.1.12. Si I és un ideal d'un anell R denotarem $I \triangleleft R$.

Proposició 13.1.13. *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 ($\Longrightarrow$). 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 (12.1.1) tenim que $x - y \in I$, ja que, per la definició d'ideal d'un anell (13.1.10) tenim que I és un grup amb la suma $+$. També trobem $r \cdot x \in I$ per la definició d'ideal d'un anell (13.1.10).

Veiem ara que la condició és necessària ($\Longleftarrow$). 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 12.1.15 tenim que I és un subgrup del grup R amb la suma $+$, i per la definició d'ideal d'un anell (13.1.10) tenim que I és un ideal de R. □

Notació 13.1.14. Si (a) és un ideal principal d'un anell R denotarem $(a) \trianglelefteq R$.

Proposició 13.1.15. *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. $IJ = \{x_1 \cdot y_1 + \dots x_n \cdot y_n \mid x_1, \dots, x_n \in I, y_1, \dots, y_n \in J, n \in \mathbb{N}\}$.

són ideals de R.

Demostració. Comencem demostrant el punt (1). Per la proposició 13.1.13 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

$$\begin{aligned} a_1 + a_2 - (b_1 + b_2) &= a_1 + a_2 - b_1 - b_2 && (13.1.5) \\ &= (a_1 - b_1) + (a_2 - b_2) && (\text{grup abelià } (12.1.25)) \end{aligned}$$

i com que, per hipòtesi, I, J són ideals de R per la proposició 13.1.13 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

$$\begin{aligned} r \cdot a &= r \cdot (a_1 + a_2) && (\text{anell } (13.1.1)) \\ &= r \cdot a_1 + r \cdot a_2 && (\text{anell } (13.1.1)) \end{aligned}$$

i per la proposició 13.1.13 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 13.1.13 tenim que $I + J$ és un ideal de l'anell R.

Veiem ara el punt (2). Per la proposició 13.1.13 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 13.1.13 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 (13.1.10) 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 13.1.13 $I \cap J$ és un ideal de R.

Acabem veient el punt (3). Per la proposició 13.1.13 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 13.1.5,

$$\begin{aligned} a - b = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - (x'_1 \cdot y'_1 + \cdots + x'_m \cdot y'_m) = \\ = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - x'_1 \cdot y'_1 - \cdots - x'_m \cdot y'_m \end{aligned}$$

i com que I és, per hipòtesi, un anell, per les proposicions 13.1.5 i 13.1.13 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

$$\begin{aligned} r \cdot a &= r \cdot (x_1 \cdot y_1 + \cdots + x_n \cdot y_n) \\ &= r \cdot x_1 \cdot y_1 + \cdots + r \cdot x_n \cdot y_n && (13.1.5) \end{aligned}$$

i com que I és, per hipòtesi, un anell, per les proposicions 13.1.5 i 13.1.13 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 13.1.13 tenim que IJ és un ideal de R. □

Definició 13.1.16 (Ideal principal)**.** Sigui I un ideal d'un anell R amb 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 $I = (a)$.

13.1.3 Cossos i l'anell quocient

Definició 13.1.17 (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 13.1.18. *Sigui* $\mathbb{K}$ *un anell commutatiu 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. Siguin $+$ la suma de R i $\cdot$ el producte de R. Comencem comprovant que la condició és suficient ($\Longrightarrow$). 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, $\mathbb{K} \setminus \{0\}$ és un grup amb l'operació $\cdot$ i $a \neq 0$ per la definició de l'invers d'un element d'un grup (12.1.7) existeix $a^{-1} \in \mathbb{K}$ tal que $a \cdot a^{-1} = 1$, i per la definició d'ideal d'un anell (13.1.10) trobem que $1 \in I$, i per tant per la proposició 13.1.13 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 ($\Longleftarrow$). 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 (13.1.16) tenim que existeix $a' \in (1)$ tal que $a \cdot a' = 1$, i per tant, per la definició de grup (12.1.1) tenim que $\mathbb{K} \setminus \{0\}$ és un grup amb el producte $\cdot$ i per la definició de cos (13.1.17) tenim que $\mathbb{K}$ és un cos amb la suma $+$ i el producte $\cdot$. ☐

Proposició 13.1.19. *Sigui* I *un ideal d'un anell* R *amb la suma* $+$. *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. Sigui $\cdot$ el producte de R. Comprovem que $\sim$ satisfà la definició de relació d'equivalència (2.3.2):

1. Reflexiva: Prenem $x \in R$. Per l'observació 13.1.11 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 (13.1.10) tenim que $(-1) \cdot (x_1 - x_2) \in I$, i per la proposició 13.1.5 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 (13.1.10) tenim que $x_3 - x_2 \in I$, i per la proposició 13.1.13 tenim que $x_1 - x_2 - (x_3 - x_2) \in I$. Ara bé, per la proposició 13.1.5 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 13.1.20. *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 13.1.19.

Per la proposició 12.1.31 tenim que R/I és un grup amb l'operació $+$, i com que

$$\begin{aligned} [x] + [y] &= [x + y] \\ &= [y + x] && \text{(grup abelià (12.1.25))} \\ &= [y] + [x] \end{aligned}$$

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 (13.1.1) tenim que R/I és un anell amb la suma $+$ i el producte $\cdot$, com volíem veure. □

Definició 13.1.21 (Anell quocient)**.** Siguin R un anell commutatiu 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 13.1.20.

13.2 Tres Teoremes d'isomorfisme entre anells

13.2.1 Morfismes entre anells

Definició 13.2.1 (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 13.2.2. *Si f és un morfisme entre anells aleshores f és un morfisme entre grups.*

Proposició 13.2.3. *Siguin R i S dos anells commutatius 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. Siguin $+_R$ la suma de R i $+_S$ la suma de S. Per l'observació 13.2.2 tenim que f és un morfisme entre els grups R amb la suma $+_R$ i S amb la suma $+_S$, i per la proposició 12.2.2 tenim que $f(0_R) = 0_S$ i $f(-x) = -f(x)$ per a tot $x \in R$. $\square$

Definició 13.2.4 (Nucli i imatge)**.** Siguin R i S dos anells commutatius 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

$$\operatorname{Im}(f) = \{y \in S \mid f(x) = y \text{ per a cert } x \in R\}$$

com la imatge de f.

Observació 13.2.5. $\ker(f) \subseteq R$, $\operatorname{Im}(f) \subseteq S$.

Proposició 13.2.6. *Siguin R i S dos anells commutatius amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f \colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

1. *$\ker(f) \lhd R$.*
2. *$\operatorname{Im}(f) \leq S$.*

Demostració. Aquest enunciat té sentit per l'observació 13.2.6

Siguin $+_R$ la suma de R, $*_R$ el producte de R, $+_S$ la suma de S i $*_S$ el producte de S. Comencem veient el punt (1). Com que, per la proposició 13.2.3, tenim que $f(0_R) = 0_S$ veiem, per la definició de nucli d'un morfisme entre anells (13.2.4), que $\ker(f) \neq \emptyset$. Prenem doncs $a \in \ker(f)$. Observem que, per la definició de morfisme entre anells (13.2.1), 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 (13.2.4) 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 d'ideal d'un anell (13.1.10) tenim que $\ker(f)$ és un ideal de R.

Veiem ara el punt (2). Veiem que per a tot $x, y \in \operatorname{Im}(f)$ tenim $x *_S y \in \operatorname{Im}(f)$. Per la definició d'imatge d'un morfisme entre anells (13.2.4) tenim que existeixen $a, b \in R$ tals que $f(a) = x$ i $f(b) = y$. Ara bé, per la definició d'anell (13.1.1) tenim que $a *_R b = c \in R$, i per tant per la definició d'imatge d'un morfisme entre anells (13.2.4) tenim que $f(c) = x *_S y \in \operatorname{Im}(f)$. Veiem ara que $\operatorname{Im}(f)$ és un anell amb la suma $+_S$ i el producte $*_S$. Com que, per l'observació 13.2.2 tenim que f és un morfisme entre grups per la proposició 12.2.7 tenim que $\operatorname{Im}(f)$ és un subgrup del grup S amb la suma $+_S$; i per la definició d'anell (13.1.1) 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 (13.1.9) tenim que $\operatorname{Im}(f)$ és un subanell de S. $\square$

Proposició 13.2.7. *Siguin R , S i 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. Siguin $+_R$ la suma de R, $*_R$ el producte de R, $+_S$ la suma de S, $*_S$ el producte de S, $+_D$ la suma de D i $*_D$ el producte de D. Per la definició de morfisme entre anells (13.2.1) 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 (13.2.1) tenim que $g \circ f$ és un morfisme entre anells, com volíem veure. $\square$

Corol·lari 13.2.8. *Si f, g són isomorfismes aleshores $g \circ f$ és isomorfisme.*

Lema 13.2.9. *Siguin R i S dos anells commutatius amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

$$\ker(f) \text{ és un ideal de } R \quad i \quad \operatorname{Im}(f) \text{ és un subanell de } S.$$

Demostració. Siguin $+_R$ la suma de R, $*_R$ el producte de R, $+_S$ la suma de S i $*_S$ el producte de S. Comencem veient que $\ker(f)$ és un ideal de R. Per l'observació 13.2.2 tenim que $\ker(f)$ és un morfisme entre grups, i per la proposició 12.2.7 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

$$\begin{aligned} f(r *_R x) &= f(r) *_S f(x) && \text{(morfisme entre anells (13.2.1))} \\ &= f(r) *_S 0_S && \text{(nucli d'un morfisme entre anells (13.2.4))} \\ &= 0_S && \text{(l'element neutre d'un anell pel producte (13.1.3))} \end{aligned}$$

i per la definició de nucli d'un morfisme entre anells (13.2.4) tenim que $r *_R x \in \ker(f)$, i per la proposició 13.1.13 tenim que $\ker(f)$ és un ideal de R.

Veiem ara que $\operatorname{Im}(f)$ és un subanell de S. Per l'observació 13.2.2 tenim que $\operatorname{Im}(f)$ és un morfisme entre grups, i per la proposició 12.2.7 tenim que $\operatorname{Im}(f)$ és un subgrup del grup S amb la suma $+_S$.

Prenem $x, y \in \operatorname{Im}(f)$. Volem veure que $x *_S y \in \operatorname{Im}(f)$. Per la definició d'imatge d'un morfisme entre anells (13.2.4) tenim que existeixen $x', y' \in R$ tals que $f(x') = x$ i $f(y') = y$. Ara bé, per la definició d'anell (13.1.1) tenim que $x' *_R y' \in R$, i per tant

$$\begin{aligned} f(x' *_R y') &+ f(x') *_S f(y') && \text{(morfisme entre anells (13.2.1))} \\ &= x *_S y \end{aligned}$$

i per la definició de imatge d'un morfisme entre grups (12.2.5) trobem que $x *_S y \in \operatorname{Im}(f)$.

També tenim, per la definició de morfisme entre anells (13.2.1), que $1_S \in \operatorname{Im}(f)$, ja que $f(1_R) = 1_S$, i per tant, per la definició de subanell (13.1.9), tenim que $\operatorname{Im}(f)$ és un subanell de S. □

13.2.2 Teoremes d'isomorfisme entre anells

Teorema 13.2.10 (Primer Teorema de l'isomorfisme)**.** *Siguin R i S dos anells i $\varphi\colon R \longrightarrow S$ un morfisme entre anells. Aleshores*

$$R/\ker(\varphi) \cong \operatorname{Im}(\varphi).$$

Demostració. Aquest enunciat té sentit per la proposició 13.2.6. □

Teorema 13.2.11 (Segon Teorema de l'isomorfisme)**.** *Siguin R un anell commutatiu amb $1 \neq 0$ i I i J dos ideals de R. Aleshores*

$$(I + J)/I \cong J/(I \cap J).$$

Demostració. □

Lema 13.2.12. *Siguin R un anell commutatiu amb $1 \neq 0$ i I i J dos ideals de R tals que $I \subseteq J$. Aleshores J/I és un ideal de R/I.*

Demostració. □

Teorema 13.2.13 (Tercer Teorema de l'isomorfisme)**.** *Siguin R un anell commutatiu amb $1 \neq 0$ i 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 lema 13.2.12. □

13.2.3 Característica d'un anell

Definició 13.2.14 (Característica)**.** Sigui R un anell amb la suma $+$. Direm que R té característica $n > 0$ si

$$n = \min_{m \in \mathbb{N}} \left\{ 1 + \overset{m)}{\cdots} + 1 = 0 \right\}.$$

Ho denotarem amb $\operatorname{ch}(R) = n$. Si aquest n no existeix diem que R té característica 0 i $\operatorname{ch}(R) = 0$.

Proposició 13.2.15. *Siguin R un anell amb la suma $+$ i*

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow R \\ n &\longmapsto 1 + \overset{n)}{\cdots} + 1 \end{aligned}$$

una aplicació. Aleshores f és un morfisme entre anells i $\ker(f) = (\operatorname{ch}(R))$.

Demostració. Aquest enunciat té sentit per la proposició 13.2.6.

Sigui $\cdot$ el producte de R. 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 (12.2.1) 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 (13.2.1) 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 (13.2.4) 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 (13.2.14) tenim que $n = \mathrm{ch}(R)$, i per tant $\ker(f) = \{k \cdot n \mid k \in \mathbb{N}\}$. Ara bé, per la definició d'ideal d'un anell (13.1.10) tenim que $\ker(f) = (n)$, com volíem veure. □

Corol·lari 13.2.16. *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* $S \cong \mathbb{Z}/(n)$.

13.3 Dominis

13.3.1 Dominis d'integritat, ideals primers i maximals

Definició 13.3.1 (Divisor de 0)**.** Siguin R amb el producte $\cdot$ un anell commutatiu 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 13.3.2 (Dominis d'integritat)**.** Sigui D un anell commutatiu 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 13.3.3. *Siguin* D *un domini d'integritat amb el producte* $\cdot$ *i* $a \neq 0$ *un element de* D. *Aleshores*

$$a \cdot x = a \cdot y \Longrightarrow x = y.$$

Demostració. Sigui $+$ la suma de D. Tenim

$$a \cdot x - a \cdot y = 0$$

i per la proposició 13.1.5 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 13.3.4 (Ideal primer)**.** Sigui I un ideal d'un anell R 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 13.3.5. *Sigui I un ideal d'un anell R amb $I \neq R$. Aleshores*

$$R/I \text{ és un domini d'integritat} \iff I \text{ és un ideal primer de } R.$$

Demostració. Siguin $+$ la suma de R i $\cdot$ el producte de R. Comencem demostrant que la condició és suficient ($\implies$). 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 (13.1.21) 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 (13.3.4) trobem que I és un ideal primer de R.

Veiem ara que la condició és necessària ($\impliedby$). Suposem doncs que I és un ideal primer de R. Per la proposició 13.1.20 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 (13.3.4) trobem que ha de ser $b \in I$, i per tant $[b] = [0]$ i per la definició de domini d'integritat (13.3.2) tenim que R/I és un domini d'integritat. □

Corol·lari 13.3.6. *Un anell R és un domini d'integritat si i només si* (0) *és un ideal primer.*

Definició 13.3.7 (Ideal maximal)**.** Sigui M un ideal d'un anell R 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 13.3.8. *Sigui M un ideal d'un anell R amb* $1 \neq 0$. *Aleshores*

$$R/M \text{ és un cos} \iff M \text{ és un ideal maximal de } R.$$

Demostració. Aquest enunciat té sentit per la proposició 13.1.20.

Comencem veient la implicació cap a la dreta ($\implies$). 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 13.1.18 tenim que els únics ideals de R/M són $([0])$ i R/M, i per tant ha de ser $I = M$ ó $I = R$, i per la definició d'ideal maximal (13.3.7) tenim que M és un ideal maximal de R.

Veiem ara la implicació cap a l'esquerra ($\impliedby$). Suposem doncs que M és un ideal maximal de l'anell R i considerem, per la proposició 13.1.20, l'anell R/M. Per la proposició 13.1.18 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 (13.3.7) tenim que ha de ser $I = M$ o $I = R$, i per tant I/M ha de ser $([0])$ ó R/M i per la proposició 13.1.20 tenim que R/M és un cos. □

Corol·lari 13.3.9. *M és maximal $\implies$ M és primer.*

Teorema 13.3.10. *Sigui R un anell commutatiu amb* $1 \neq 0$. *Aleshores R és un domini d'integritat si i només si $R \setminus \{0\}$ és un cos.*

Demostració. □

Proposició 13.3.11. *Sigui $I \neq (0)$ un ideal primer d'un domini d'integritat D. Aleshores I és maximal.*

Demostració. Sigui $\cdot$ el producte de D. 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 (13.1.16) tenim que $a = a' \cdot b$ per a cert $a' \in D$. Aleshores, per la definició d'ideal primer (13.3.4), tenim que $a' \in (a)$ ó $b \in (a)$.

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 13.3.3 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 d'ideal maximal (13.3.7) tenim que $I = (a)$ és un ideal maximal de D, com volíem veure. □

13.3.2 Lema de Zorn

Definició 13.3.12 (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 13.3.13 (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 13.3.14. *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 (13.3.12):

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 (13.3.12) i cadena (13.3.13) tenim que $\mathcal{X}$ amb $\subseteq$ és una cadena. □

Definició 13.3.15 (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 13.3.16 (Lema 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 13.3.17. *Sigui R un anell commutatiu amb $1 \neq 0$. Aleshores existeix $M \subseteq R$ tal que M sigui un ideal maximal de R.*

Demostració. Siguin $+$ la suma de R i $\cdot$ el producte de R. Definim el conjunt

$$A = \{I \triangleleft R \mid I \neq R\}.$$

i amb un subconjunt $\mathcal{C} \subseteq A$ considerem, per la proposició 13.3.14, la cadena $\mathcal{C}$ amb $\subseteq$. 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 (13.1.10) 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 Lema de Zorn (13.3.16) 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 (13.3.7) tenim que M és un ideal maximal de R. □

13.3.3 Divisibilitat

Definició 13.3.18 (Divisors i múltiples)**.** Siguin D un domini d'integritat amb 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 13.3.19. $b \mid a \iff (a) \subseteq (b)$.

Proposició 13.3.20. *Siguin D un domini d'integritat amb el producte $\cdot$ i a, b, c, c' quatre elements de D 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 13.3.3 tenim que $1 = c' \cdot c$, i per la definició d'element invertible (13.1.7) tenim que $c' = c^{-1}$. □

Proposició 13.3.21. *Sigui R un anell commutatiu amb el producte $\cdot$ 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 d'element invertible (13.1.7) 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 d'element invertible (13.1.7) 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 13.3.22 (Elements associats)**.** Siguin R un anell commutatiu 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 13.3.21.

Proposició 13.3.23. *Siguin D un domini d'integritat, a i 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 per a tot $d' \in D$ tenim que $d' \in X$ si i només si $d \sim d'$.*

Demostració. Sigui $\cdot$ el producte de D. Comencem amb la implicació cap a la dreta ($\implies$). 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 (13.3.18) trobem que $d \sim d'$.

Fem ara la implicació cap a l'esquerra ($\impliedby$). 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 13.3.20 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 (13.3.22) tenim que $d' \in X$. □

Definició 13.3.24 (Màxim comú divisor)**.** Siguin D un domini d'integritat 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 $d \sim \operatorname{mcd}(a, b)$. Entendrem que $\operatorname{mcd}(a, b)$ és un element de D.

Aquesta definició té sentit per la proposició 13.3.23.

Proposició 13.3.25. *Siguin D un domini d'integritat, a i 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. Sigui $\cdot$ el producte de D. Comencem amb la implicació cap a la dreta ($\implies$). 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 (13.3.18) trobem que $m \sim m'$.

Fem ara la implicació cap a l'esquerra ($\Longleftarrow$). 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 13.3.20 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 (13.3.22) tenim que $m' \in X$. □

Definició 13.3.26 (Mínim comú múltiple)**.** Siguin D un domini d'integritat 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 13.3.25.

Proposició 13.3.27. *Siguin $(a), (b)$ dos ideals principals d'un domini d'integritat D amb la suma $+$ i el producte $\cdot$. 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 13.1.15 tenim que $(a) + (b) = \{x + y \mid x \in (a), y \in (b)\}$, i per la definició d'ideal principal (13.1.16) 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 13.1.15 tenim que

$$(a) \cap (b) = \{x \mid x \in (a), x \in (b)\},$$

que, per la definició d'ideal principal (13.1.16), podem reescriure com

$$(a) \cap (b) = \{x \mid x \text{ divideix } a \text{ i } b\}$$

i per tant $(a) \cap (b) = (\mathrm{mcm}(a, b))$ és un ideal principal de R.

Acabem veient el punt (3). Per la proposició 13.1.15 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 (13.1.16) i la proposició 13.1.5, 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 (13.1.16) tenim que $(a)(b)$ és un ideal principal de R amb

$$(a)(b) = (a \cdot b).$$

□

Definició 13.3.28 (Primer)**.** Siguin D un domini d'integritat, $p \neq 0$ 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 13.3.29. *$a \neq 0$, (a) és un ideal primer si i només si a és primer.*

Definició 13.3.30 (Element irreductible)**.** Siguin D un domini d'integritat amb 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 13.3.31. *Siguin D un domini d'integritat i p un element primer de D. Aleshores p és irreductible.*

Demostració. Sigui $\cdot$ el producte de D. Suposem que a i b són dos elements de D tals que $p = a \cdot b$. Per la definició de primer (13.3.28) 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 13.3.3 tenim que $1 = \alpha \cdot b$, i per la definició d'element invertible (13.1.7) tenim que b és invertible i per la definició d'irreductible (13.3.30) tenim que p és irreductible.

El cas $p \mid b$ és anàleg. □

13.3.4 Dominis de factorització única

Definició 13.3.32 (Domini de factorització única)**.** Sigui D un domini d'integritat amb 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 13.3.33. *Sigui D un domini d'integritat amb 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 ($\Longrightarrow$). Suposem doncs que D és un domini de factorització única. El punt (1) és conseqüència de la definició de domini de factorització única (13.3.32). 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 (13.3.32) 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 (13.3.32) 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 (13.3.32), 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 (13.3.28) tenim que p és primer.

Veiem ara que la condició és necessària ($\Longleftarrow$). 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 (13.3.28) tenim que $p_1 \mid q_j$ per a cert $j \in \{1, \dots, s\}$, i per la definició de irreductible (13.3.30) i la definició d'elements associats (13.3.22) tenim que $p_1 \sim q_j$. Sigui doncs $\sigma \in S_s$ tal que $p_1 \mid q_{\sigma(1)}$. Aleshores tenim

$$p_1 \cdot p_2 \cdot \dots \cdot p_r = u_1 \cdot q_{\sigma(1)} \cdot \dots \cdot q_s$$

per a cert u_1 element invertible de D. Podem iterar aquest argument per a $p_2, \dots, p_t$, on $t = \min(r, s)$ per obtenir

$$p_1 \cdot \dots \cdot p_t \cdot p_{t+1} \cdot \dots \cdot p_r = (u_1 \cdot q_1) \cdot \dots \cdot (u_t \cdot q_t) \cdot p_{t+1} \cdot \dots \cdot p_s$$

per a certs $u_1, \dots, u_t$ elements invertibles de D. Ara bé, tenim que $r = s$, ja que si $r > s$ tindríem que $p_{s+1}, \dots, p_r$ són invertibles, i si $s > r$ tindríem que $q_{r+1}, \dots, q_s$ són invertibles, però per la definició d'irreductible (13.3.30) i la definició d'element invertible (13.1.7) tenim que això no pot ser, i per tant $r = s$ i per la definició de domini de factorització única (13.3.32) tenim que D és un domini de factorització única, com volíem veure. □

Proposició 13.3.34. *Siguin D un domini de factorització única amb i el producte $\cdot$ i a, b dos elements no invertibles i no nuls de D tals que existeixen $p_1, \dots, p_r$ tals que*

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} \quad i \quad b = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}$$

per a certs $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$ enters no negatius. 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

$$c = p_1^{\gamma_1} \cdot \dots \cdot p_r^{\gamma_r}$$

per a certs $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \dots, r\}$. Ara bé, com que $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \dots, r\}$, i per tant $d \mid c$, i per la definició de màxim comú divisor (13.3.24) tenim que $d \sim \operatorname{mcd}(a, b)$.

Prenem ara c un element de D tal que $a \mid c$ i $b \mid c$. Aleshores tenim que

$$c = q \cdot p_1^{\gamma_1} \cdot \dots \cdot p_r^{\gamma_r}$$

per a cert $q \in D$ i certs $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \dots, r\}$. Ara bé, com que $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \dots, r\}$, i per tant $m \mid c$, i per la definició de mínim comú múltiple (13.3.26) tenim que $m \sim \operatorname{mcm}(a, b)$. □

13.3.5 Anells Noetherians

Definició 13.3.35 (Anell Noetherià)**.** Sigui N un anell commutatiu amb $1 \neq 0$ tal que si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

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 13.3.36. *$\{I_1, I_2, I_3 \dots\}$ amb la relació d'ordre $\subseteq$ és una cadena.*

Lema 13.3.37. *Siguin N un domini d'integritat Noetherià amb el producte $\cdot$ i $a \neq 0$ un element no invertible de N. Aleshores existeixen $p_1, \dots, p_n$ elements irreductibles de N tals que*

$$a = p_1 \cdot \dots \cdot p_n.$$

Demostració. Ho farem per reducció a l'absurd. Definim el conjunt

$$X = \{a \in N \text{ invertible} \mid a \neq p_1 \cdot \dots \cdot p_n \text{ per a } p_1, \dots, p_n \in N \text{ irreductibles}\}.$$

Volem veure que $X = \emptyset$. Suposem doncs que $X \neq \emptyset$ i prenem $a_1 \in X$. Per la definició d'irreductible (13.3.30) 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 13.3.19, 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

$$(a_1) \subset (b_1) \subset (b_2) \subset (b_3) \subset \dots$$

però això entra en contradicció amb la definició de anell Noetherià (13.3.35), i per tant $X = \emptyset$, com volíem veure. $\square$

13.3.6 Dominis d'ideals principals

Definició 13.3.38 (Domini d'ideals principals)**.** Sigui D un domini d'integritat tal que tot ideal de D és un ideal principal. Aleshores direm que D és un domini d'ideals principals.

Proposició 13.3.39. *Sigui D un domini d'ideals principals. Aleshores un element $a \in D$ és irreductible si i només si (a) és un ideal maximal.*

Demostració. Sigui $\cdot$ el producte de D. Comencem veient que la condició és suficient ($\Longleftarrow$). 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 13.3.19 tenim que $b \mid a$, és a dir, existeix $r \in D$ tal que $a = b \cdot r$, i per la definició d'irreductible (13.3.30) 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 (13.1.7) tenim que $a \cdot r^{-1} = b$, per l'observació 13.3.19 tenim que $(a) = (b)$, i per la definició d'ideal maximal (13.3.7) tenim que (a) és un ideal maximal.

Tenim que la condició és necessària ($\Longrightarrow$) per la proposició 13.3.11. $\square$

Proposició 13.3.40. *Siguin D un domini d'ideals principals i a un element irreductible de D. Aleshores a és primer.*

Demostració. Per la proposició 13.3.39 tenim que (a) és maximal, pel corol·lari 13.3.9 veiem que (a) és primer, i per l'observació 13.3.29 trobem que a és primer, com volíem veure. $\square$

Teorema 13.3.41. *Sigui D un domini d'ideals principals. Aleshores D és Noetherià.*

Demostració. Siguin $I_1, \dots, I_i, \dots$ ideals de D tals que

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

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 (13.1.10) 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 (13.3.38) 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 pel Teorema de la doble inclusió (2.1.3) trobem que $I_n = I_{n+k}$ per a tot $k \in \mathbb{N}$, i per la definició de anell Noetherià (13.3.35) trobem que D és un anell Noetherià. □

Teorema 13.3.42. *Sigui D un domini d'ideals principals. Aleshores D és un domini de factorització única.*

Demostració. Sigui $\cdot$ el producte de D. Pel Teorema 13.3.41 tenim que D és un anell Noetherià, i pel lema 13.3.37 tenim que per a tot element no irreductible a de D existeixen $p_1, \dots, p_n$ elements irreductibles de N tals que

$$a = p_1 \cdot \dots \cdot p_n.$$

També tenim, per la proposició 13.3.40 que si a és un element irreductible de D aleshores a és primer.

Per acabar, pel Teorema 13.3.33 tenim que D és un domini de factorització única. □

13.3.7 Dominis Euclidians

Definició 13.3.43 (Domini Euclidià)**.** Siguin D un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $U\colon D \setminus \{0\} \longrightarrow \mathbb{N}$ 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 13.3.44. *Sigui D un domini Euclidià amb la norma U. Aleshores*

$$U(1) \leq U(x) \quad \textit{per a tot } x \in D \setminus \{0\}.$$

Demostració. Sigui $\cdot$ el producte de D. Per la definició de domini Euclidià (13.3.43) tenim que $U(x) \leq U(x \cdot y)$ per a tot $x, y \in D \setminus \{0\}$. Per tant

$$U(1) \leq U(1 \cdot x) = U(x) \quad \text{per a tot } x \in D \setminus \{0\}. \qquad \square$$

Proposició 13.3.45. *Sigui D un domini Euclidià amb la norma U. Aleshores*

$$U(u) = U(1) \iff u \text{ és un element invertible de } D.$$

Demostració. Siguin $+$ la suma de D i $\cdot$ el producte de D. Comencem veient l'implicació cap a la dreta ($\Longrightarrow$). Suposem doncs que u és un element invertible de D.

Per la proposició 13.3.44 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 (13.1.8) 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 ($\Longleftarrow$). Suposem que $U(u) = U(1)$.

Per la definició de domini Euclidià (13.3.43) tenim que existeixen Q i 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 13.3.44 trobem que ha de ser $r = 0$. Per tant tenim

$$1 = Q \cdot u$$

i per la definició d'element invertible (13.1.7) trobem que u és invertible. $\square$

Teorema 13.3.46. *Sigui D un domini Euclidià. Aleshores D és un domini d'ideals principals.*

Demostració. Siguin $+$ la suma de D, $\cdot$ el producte de D, 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 (13.3.43) 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 d'anell (13.1.1) tenim que D és un grup amb l'operació $+$ tenim

$$r = a - Q \cdot b,$$

i per la proposició 13.1.13 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 (13.3.38) tenim que D és un domini d'ideals principals. $\square$

Teorema 13.3.47. *Sigui $\mathbb{K}$ un cos. Aleshores $\mathbb{K}$ és un domini Euclidià.*

Demostració. $\square$

13.4 Anells de polinomis

13.4.1 Cos de fraccions d'un domini d'integritat

Proposició 13.4.1. *Siguin D un domini d'integritat amb 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. $\square$

Notació 13.4.2. Denotarem el conjunt quocient $D \times D \setminus \{0\} / \sim$ com $\mathrm{Q}(D)$ i la classe d'equivalència $\overline{(a, b)} \in \mathrm{Q}(D)$ com $\frac{a}{b}$.

Lema 13.4.3. *Siguin D un domini d'integritat amb la suma $+$ i el producte $\cdot$. Aleshores $\mathrm{Q}(D)$ 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. $\square$

Teorema 13.4.4. *Sigui D un domini d'integritat. Aleshores $\mathrm{Q}(D)$ és un cos.*

Demostració. $\square$

Teorema 13.4.5 (Unicitat de $\mathrm{Q}(D)$)**.** *Siguin D un domini d'integritat amb la suma $+$ i el producte $\cdot$ i $\mathrm{Q}_1(D)$ i $\mathrm{Q}_2(D)$ dos cossos amb la suma $+$ i el producte $\cdot$. Aleshores*

$$\mathrm{Q}_1(D) \cong \mathrm{Q}_2(D)$$

Demostració. $\square$

Definició 13.4.6 (Cos de fraccions)**.** Siguin D un domini d'integritat. Aleshores direm que $\mathrm{Q}(D)$ és el cos de fraccions de D.

13.4.2 El Teorema de Gauss

Proposició 13.4.7. *Siguin R un anell amb la suma $+$ i el producte $\cdot$ i*

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{N}, a_0, \ldots, a_n \in R\}$$

un conjunt. Aleshores $R[x]$ és un anell amb la suma $+$ i el producte $\cdot$.

Demostració. $\square$

Observació 13.4.8. $1_R = 1_{R[x]}$, $0_R = 0_{R[x]}$.

Observació 13.4.9. *Si R és un anell commutatiu aleshores $R[x]$ també és un anell commutatiu.*

Definició 13.4.10 (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 13.4.7.

Observació 13.4.11. $D \subseteq D[x]$.

Teorema 13.4.12 (Teorema de la base de Hilbert)**.** *Sigui R un anell Noetherià. Aleshores $R[x]$ és un anell Noetherià.*

Demostració. □

Definició 13.4.13 (Contingut d'un polinomi)**.** Siguin D un domini de factorització única i $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un element de $D[x]$. Aleshores definim

$$\mathrm{cont}(f) \sim \mathrm{mcd}(a_0, \ldots, a_n)$$

com el contingut de f.

Interpretarem $\mathrm{cont}(f(x))$ com un element de D.

Definició 13.4.14 (Polinomi primitiu)**.** Siguin D un domini de factorització única i $f(x)$ un element de $D[x]$ tal que

$$\mathrm{cont}(f(x)) \sim 1.$$

Aleshores direm que $f(x)$ és un polinomi primitiu.

Lema 13.4.15 (Lema de Gauss)**.** *Siguin D un domini de factorització única i $f(x), g(x)$ dos polinomis primitius de $D[x]$. Aleshores $f(x) \cdot g(x)$ és un polinomi primitiu.*

Demostració. □

Corol·lari 13.4.16. *Siguin D un domini de factorització única i $f(x)$ i $g(x)$ dos elements de $D[x]$. Aleshores*

$$\mathrm{cont}(f(x) \cdot g(x)) \sim \mathrm{cont}(f(x)) \cdot \mathrm{cont}(g(x)).$$

Demostració. □

Lema 13.4.17. *Siguin D un domini d'integritat i p un element irreductible de D. Aleshores tenim que p és un element irreductible de $D[x]$.*

Demostració. □

Teorema 13.4.18. *Sigui D un domini de factorització única i $f(x)$ un polinomi de $D[x]$. Aleshores* $\mathrm{grau}(f(x)) \geq 1$ *i $f(x)$ és un polinomi irreductible de $D[x]$ si i només si* $\mathrm{cont}(f(x)) \sim 1$ *i $f(x)$ és irreductible en* $\mathrm{Q}(D)[x]$.

Demostració. □

Teorema 13.4.19 (Teorema de Gauss)**.** *Sigui D un domini de factorització única. Aleshores $D[x]$ és un domini de factorització única.*

Demostració. ☐

Teorema 13.4.20. *Sigui D un domini d'integritat. 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. ☐

13.4.3 Criteris d'irreductibilitat

Definició 13.4.21 (Arrel)**.** Siguin R un anell commutatiu amb $1 \neq 0$, $f(x)$ un element de $R[x]$ i α un element de R tal que $f(\alpha) = 0$. Aleshores direm que α és una arrel de $f(x)$.

Proposició 13.4.22. *Siguin $\mathbb{K}$ un cos 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 13.4.23. *Siguin D un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomi de $D[x]$ i $\frac{a}{b} \in \mathrm{Q}(D)$ 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 13.4.24 (Criteri modular)**.** *Siguin D un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomi primitiu de $D[x]$ i p un element irreductible de D amb $p \nmid a_n$ tals que*

$$\overline{f(x)} = \overline{a_0} + \overline{a_1} \cdot x + \cdots + \overline{a_n} \cdot x^n$$

sigui un polinomi irreductible de $D/(p)[x]$. Aleshores $f(x)$ és un polinomi irreductible de $D[x]$.

Demostració. ☐

Teorema 13.4.25 (Criteri d'Eisenstein)**.** *Siguin D un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomi primitiu de $D[x]$ amb $n \geq 1$ i p un element irreductible de D satisfent $p \mid a_0, \ldots, p \mid a_{n-1}$ i $p \nmid a_n, p^2 \nmid a_0$. Aleshores $f(x)$ és un polinomi irreductible de $D[x]$.*

Demostració. ☐

Corol·lari 13.4.26. *Siguin D un domini de factorització única amb la suma $+$ i el producte $\cdot$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 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 $\mathrm{Q}(D)[x]$.*

Demostració. ☐

Capítol 14

Teoria de cossos finits

14.1 Cossos finits

14.1.1 Propietats bàsiques dels cossos finits

Proposició 14.1.1. *Siguin* $\mathbb{K}$ *i* $\mathbb{E}$ *dos cossos tals que* $\mathbb{K} \subseteq \mathbb{E}$. *Aleshores* $\mathbb{E}$ *és un* $\mathbb{K}$*-espai vectorial.*

Demostració. □

Definició 14.1.2 (Cos finit)**.** Sigui $\mathbb{K}$ un cos tal que $|\mathbb{K}| \in \mathbb{N}$. Aleshores direm que $\mathbb{K}$ és un cos finit.

Observació 14.1.3. *Sigui* $\mathbb{K}$ *un cos finit. Aleshores* $\mathrm{ch}(\mathbb{K})$ *és primer.*

Teorema 14.1.4. *Sigui* $\mathbb{K}$ *un cos finit. Aleshores*

$$\mathrm{ch}(\mathbb{K}) = p \iff |\mathbb{K}| = p^n \textit{ per a cert } n \in \mathbb{N}.$$

Demostració. □

Corol·lari 14.1.5. *Siguin* $\mathbb{K}$ *un cos finit i* $\mathbb{F}$ *un subcòs de* $\mathbb{K}$ *amb* $|\mathbb{K}| = p^n$. *Aleshores* $|\mathbb{F}| = p^d$ *amb* $d \mid n$.

Demostració. □

Teorema 14.1.6 (Teorema de l'element primitiu)**.** *Sigui* $\mathbb{K}$ *un cos finit. Aleshores* $\mathbb{K} \setminus \{0\}$ *és un grup cíclic amb el producte* $\cdot$.

Demostració. □

Definició 14.1.7 (Element primitiu)**.** Sigui $\mathbb{K}$ un cos finit i β un element de $\mathbb{K}$ tal que $\langle\{\beta\}\rangle = \mathbb{K} \setminus \{0\}$. Aleshores direm que β és un element primitiu de $\mathbb{K}$.

Aquesta definició té sentit pel Teorema de l'element primitiu (14.1.6).

Teorema 14.1.8. *Sigui* $\mathbb{K}$ *un cos finit 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. □

14.1.2 Arrels d'un polinomi

Definició 14.1.9 (Descomposició d'un polinomi)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ 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 14.1.10 (Teorema de Kronecker)**.** *Siguin $\mathbb{K}$ un cos 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 14.1.11 (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 (14.1.10).

Definició 14.1.12 (Derivada formal)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomi de $\mathbb{K}$. Aleshores definim la derivada formal de $f(x)$ com

$$f'(x) = a_1 + 2 \cdot a_2 x + 3 \cdot a_3 x^2 + \cdots + n \cdot a_n x^{n-1}.$$

Proposició 14.1.13. *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 14.1.14. *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $\mathrm{ch}(\mathbb{K}) = 0$ i $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomi de $\mathbb{K}$ amb $n \geq 1$. Aleshores $n \cdot a_n \neq 0$ i $f'(x) \neq 0$.*

Demostració. □

Proposició 14.1.15. *Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ amb $\mathrm{ch}(\mathbb{K}) = p$ no nul i $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ 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 14.1.16 (Arrels múltiples)**.** Siguin $\mathbb{K}$ un cos amb la suma $+$ i el producte $\cdot$ i $f(x)$ un polinomi de $\mathbb{K}[x]$, α 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 α és una arrel múltiple de $f(x)$.

Proposició 14.1.17. *Siguin* $\mathbb{K}$ *un cos i* $f(x)$ *un polinomi de* $\mathbb{K}[x]$*. Aleshores* α *és una arrel múltiple de* $f(x)$ *si i només si* α *és una arrel de* $f'(x)$*.*

Demostració. □

Corol·lari 14.1.18. *Siguin* $\mathbb{K}$ *un cos i* $f(x)$ *un polinomi de* $\mathbb{K}[x]$ *satisfent* $\operatorname{grau}(f(x)) \geq 1$*. Aleshores* $\operatorname{mcd}(f(x), f'(x)) = 1$ *si i només si* $f(x)$ *no té arrels múltiples.*

Demostració. □

14.2 Caracterització dels cossos finits i els seus subcossos

14.2.1 Teoremes d'existència i unicitat dels cossos finits

Teorema 14.2.1 (Teorema d'existència dels cossos finits)**.** *Siguin* p *un primer i* n *un natural. Aleshores existeix un cos* $\mathbb{K}$ *tal que* $|\mathbb{K}| = p^n$*.*

Demostració. □

Corol·lari 14.2.2. *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. □

Lema 14.2.3. *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 14.2.4 (Teorema d'unicitat dels cossos finits)**.** *Siguin* $\mathbb{K}$ *i* $\mathbb{F}$ *dos cossos finits amb* $|\mathbb{K}| = |\mathbb{F}| = p^n$*. Aleshores*

$$\mathbb{K} \cong \mathbb{F}.$$

Demostració. □

Teorema 14.2.5 (Teorema d'existència dels subcossos finits)**.** *Siguin* $\mathbb{K}$ *un cos 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 14.2.6 (Teorema d'unicitat dels subcossos finits)**.** *Siguin* $\mathbb{K}$ *un cos 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 14.2.7. Denotarem el cos de p^n elements com $\mathbb{F}_{p^n}$.

14.2.2 El morfisme de Frobenius

Teorema 14.2.8. *Siguin n un natural, p un primer i*

$$\mathcal{F} = \{f(x) \in \mathbb{Z}/(p)[x] \mid f(x) \text{ és un polinomi mònic irreductible de grau } d \mid n\}.$$

Aleshores

$$x^{p^n} - x = \prod_{f(x)\in\mathcal{F}} f(x).$$

Demostració. □

Proposició 14.2.9 (Morfisme de Frobenius)**.** *Sigui $\mathbb{F}_{p^n}$ un cos finit. Aleshores l'aplicació*

$$\begin{aligned}\Phi\colon \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n}\\ a &\longmapsto a^p\end{aligned}$$

és un automorfisme.

Demostració. □

Teorema 14.2.10. *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 α una arrel de $f(x)$ en $\mathbb{K}(p(x))$. Aleshores les arrels de $f(x)$ són $\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \dots, \alpha^{p^{n-1}}$ i $\alpha^{p^n} = \alpha$.*

Demostració. □

Teorema 14.2.11. *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 α una arrel de $f(x)$ en $\mathbb{K}(p(x))$. Aleshores les arrels de $f(x)$ són $\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \dots, \alpha^{p^{n-1}}$ i $\alpha^{p^i} \neq \alpha^{p^j}$ per a tot $i \neq j$, $i, j \in \{0, \dots, n-1\}$.*

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 [1, 2, 3, 4, 5, 6, 7].

Part VII

Mètodes numèrics

Capítol 15

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].

15.1 El problema d'interpolació

15.1.1 Problemes d'interpolació

Definició 15.1.1 (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 15.1.2. *Exemples de problemes d'interpolació lineal són problemes com la interpolació polinòmica:*

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1x + \cdots + a_nx^n;$$

o la interpolació trigonomètrica:

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1e^{xi} + \cdots + a_ne^{nxi}.$$

[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.

15.2 Polinomis interpoladors de Lagrange

15.2.1 Interpolació de Lagrange

Definició 15.2.1 (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 15.2.2 (Polinomis bàsics de Lagrange)**.** Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x; a_0, \ldots, a_n) \in \mathbb{R}_n[x]$ 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 15.2.3.

$$L_k(x_i) = \begin{cases} 1 & \text{si } i = k, \\ 0 & \text{si } i \neq k. \end{cases}$$

Proposició 15.2.4. *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 15.2.3 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 $i \in \{0, \ldots, n\}$. Això és equivalent a que

$$P(x_i) - Q(x_i) = 0$$

per a tot $i \in \{0, \ldots, n\}$. Ara bé, tenim que $x_0, \ldots, x_n$ són arrels diferents de $P(x) - Q(x)$ per la definició de problema d'interpolació de Lagrange (15.2.1). 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 $P(x) = Q(x)$. $\square$

Proposició 15.2.5. *Siguin $\{(x_i, y_i)\}_{i=0}^n$ un conjunt de punts de suport, $I = \{i_0, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ un conjunt i $\{(x_i, y_i)\}_{i \in I}$ un problema d'interpolació per $P_{i_0,\ldots,i_k} \in \mathbb{R}_k[x]$, on*

$$P_{i_0,\ldots,i_k}(x_{i_j}) = y_{i_j} \quad \text{per a tot } j \in \{0, \ldots, k\}.$$

Aleshores

$$P_i(x) = y_i$$

i

$$P_{i_0,\ldots,i_k}(x) = \frac{(x - x_{i_0})P_{i_1,\ldots,i_k}(x) - (x - x_{i_k})P_{i_0,\ldots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}.$$

Demostració. Fixem $k = 1$. Aleshores tenim

$$P_i(x) = y_i.$$

Veiem la segona part. Definim

$$G(x) = \frac{(x - x_{i_0})P_{i_1,\ldots,i_k}(x) - (x - x_{i_k})P_{i_0,\ldots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}$$

tenim $G = P_{i_0,\ldots,i_k}$ per la proposició 15.2.4, i per tant

$$G(x_{i_0}) = P_{i_0,\ldots,i_{k-1}}(x_{i_0}) = y_{i_0}$$

i

$$G(x_{i_k}) = P_{i_1,\ldots,i_k}(x_{i_k}) = y_{i_k},$$

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 $j \in \{1, \ldots, k-1\}$, com volíem veure. $\square$

Observació 15.2.6 (Algorisme de Neville)**.** *Aquest mètode recurrent es pot organitzar en una taula com*

$$\begin{array}{c|ccc}
 & k=0 & k=1 & k=2 \\
\hline
x_0 & y_0 = P_0(x) & & \\
 & & P_{0,1}(x) & \\
x_1 & y_1 = P_1(x) & & P_{0,1,2}(x) \\
 & & P_{1,2}(x) & \\
x_2 & y_2 = P_2(x) & & \\
\vdots & \vdots & &
\end{array}$$

que s'omple de columna a columna de dreta a esquerra. Es coneix com a algorisme de Neville.

Exemple 15.2.7. *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 (15.2.6) 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 $P_{0,1,2}(2) = \frac{10}{3}$. ◊

15.2.2 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 15.2.8 (Diferències dividides)**.** Sigui $P(x; a_0, \dots, a_n)$ el polinomi interpolador de Lagrange amb els punts de suport $\{(x_i, y_i)\}_{i=0}^n$. Aleshores direm que

$$[x_0, \dots, x_k] = a_k$$

és la diferència dividida d'ordre n del problema d'interpolació de Lagrange de $\{(x_i, y_i)\}_{i=0}^k$ per $P(x; a_0, \dots, a_k)$.

Aquesta definició té sentit per la proposició 15.2.4.

Proposició 15.2.9. *Sigui* $\{(x_i, y_i)\}_{i=0}^n$ *un problema d'interpolació de Lagrange per* $P(x)$. *Aleshores*

$$P(x) = [x_0] + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots$$
$$\cdots + [x_0, \dots, x_n](x - x_0)\cdots(x - x_{n-1}) = \sum_{i=0}^{n} \left([x_0, \dots, x_i] \prod_{j=0}^{i-1} (x - x_j) \right).$$

Demostració. Denotem per $P_{1,\dots,k} \in \mathbb{K}_{k+1}[x]$ el polinomi que satisfà

$$P_{0,\dots,k}(x_j) = y_j \quad \text{per a tot } j \in \{0, \dots, k\}.$$

Aleshores tenim que el polinomi

$$G_k(x) = P_{0,\dots,k}(x) - P_{0,\dots,k-1}(x)$$

té com arrels $x_0, \dots, x_{k-1}$, i per tant existeix una única costant 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 (15.2.8) tenim que

$$G_k(x) = [x_0, \ldots, x_k](x - x_0) \cdots (x - x_{k-1})$$

i per la proposició 15.2.4 tenim

$$P(x) = P_n$$

i per tant trobem recursivament

$$\begin{aligned}
P_n(x) =& P_{n-1}(x) + [x_0, \ldots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
=& P_{n-2}(x) + [x_0, \ldots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
& + [x_0, \ldots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
& \vdots \\
=& P_{n-r}(x) + \sum_{i=0}^{n-r+1} \left([x_0, \ldots, x_{n-l+1}] \prod_{j=0}^{n-r} (x - x_j) \right) \qquad \text{(r>0)} \\
& \vdots \\
=& P_1(x) + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots \\
& \cdots + [x_0, \ldots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
& + [x_0, \ldots, x_n](x - x_0) \cdots (x - x_{n-1})
\end{aligned}$$

i per la definició de diferències dividides (15.2.8) tenim que $P_1(x) = [x_0]$

$$\begin{aligned}
=& [x_0] + [x_0, x_1](x - x_0) + \cdots + [x_0, \ldots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
& + [x_0, \ldots, x_n](x - x_0) \cdots (x - x_{n-1}) = P(x).
\end{aligned}$$

□

Observació 15.2.10. *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange. Aleshores per a tot $\sigma \in S_4$ tenim*

$$[x_0, \ldots, x_n] = [x_{\sigma 0}, \ldots, x_{\sigma(n)}].$$

Demostració. Per la proposició 15.2.4. □

Proposició 15.2.11. *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$. Aleshores*

$$[x_i] = y_i \quad \textit{per a tot } i \in \{0, \ldots, n\} \tag{15.1}$$

i

$$[x_0, \ldots, x_n] = \frac{[x_1, \ldots, x_n] - [x_0, \ldots, x_{n-1}]}{x_n - x_0}. \tag{15.2}$$

Demostració. Per veure (15.1) 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 (15.2.8) trobem $[x] = y$.

Per veure (15.2) tenim, per la proposició 15.2.5

$$P_{0,\ldots,n}(x) = \frac{(x - x_0)P_{1,\ldots,n}(x) - (x - x_n)P_{0,\ldots,n-1}(x)}{x_n - x_0},$$

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 15.2.9 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. □

15.2.3 Error en la interpolació de Lagrange

Teorema 15.2.12. *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

$$S(x) = \frac{f(x) - P(x)}{\omega(x)}. \tag{15.3}$$

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 (5.2.17) 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 (15.3), tenim

$$\frac{f^{(n+1)}(\xi_{n+1}^{(n+1)})}{(n+1)!} = \frac{f(x) - P(x)}{\omega(x)}$$

d'on trobem

$$f(x) - P(x) = \frac{f^{(n+1)}(\xi_{n+1}^{(n+1)})}{(n+1)!}\omega(x),$$

com volíem veure. □

Observació 15.2.13.

$$f(x) - P(x) = [x_0, \ldots, x_n, x]\omega(x)$$

Corol·lari 15.2.14. *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 15.2.15. *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 (15.2.1) tenim que aquest problema d'interpolació és de Lagrange. Aleshores, pel Teorema 15.2.12 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 $\frac{1}{103} \le \frac{1}{\xi(102.5)} \le \frac{1}{100}$. Aleshores tenim

$$|\log(102.5) - P(x)| = \frac{3 \cdot 5}{2^4 \cdot \xi^4(102.5)} \le \frac{15}{64}\frac{1}{100^4} \approx 2.34 \cdot 10^{-9}.$$ ♢

15.2.4 Interpolació en nodes equiespaiats

Definició 15.2.16 (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 15.2.17. *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

$$\begin{aligned}
\Delta f(x_0) &= f(x_0 + h) - f(x_0) && \text{(nodes equiespaiats (15.2.16))} \\
&= f(x_1) - f(x_0) \\
&= h \frac{f(x_1) - f(x_0)}{x_1 - x_0} \\
&= h[x_0, x_n] && \text{(diferències dividides (15.2.8))}
\end{aligned}$$

i per tant

$$[x_0, x_n] = \frac{\Delta f(x_0)}{h}. \tag{15.4}$$

Suposem ara que l'enunciat és cert per a k fix i demostrem-ho pel cas $k + 1$. Tenim que

$$\begin{aligned}
\Delta^{k+1} f(x_0) &= \Delta(\Delta^k (f(x_0)) && \text{(nodes equiespaiats (15.2.16))} \\
&= \Delta^k f(x_1) - \Delta^k f(x_0) && \text{(nodes equiespaiats (15.2.16))} \\
&= k! h^k ([x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]) && (15.4) \\
&= k! h^k (k+1) h \frac{[x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]}{x_{k+1} - x_0} \\
&= (k+1)! h^{k+1} [x_0, \dots, x_{k+1}], && \text{(diferències dividides (15.2.8))}
\end{aligned}$$

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. □

15.3 Polinomis interpoladors per splines

15.3.1 Interpolació per splines

Definició 15.3.1. 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 Δ.

Denotarem

$$S_p(\Delta) = \{s \mid s \text{ és un spline de grau } p \text{ associat a } \Delta\}.$$

Nota 15.3.2. *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].

Part VIII

Topologia

Capítol 16

L'espai topològic

16.1 Espais mètrics

16.1.1 Boles i oberts

Definició 16.1.1 (Espai mètric)**.** Sigui X un conjunt i $\mathrm{d}\colon X \times X \longrightarrow \mathbb{R}$ una aplicació que per a tot x, y i z de X satisfà

1. $\mathrm{d}(x, y) = 0$ si i només si $x = y$.
2. $\mathrm{d}(x, y) = \mathrm{d}(y, x)$.
3. $\mathrm{d}(x, y) \leq \mathrm{d}(x, z) + \mathrm{d}(z, y)$.
4. $\mathrm{d}(x, y) \leq 0$.

Aleshores direm que X amb la distància d és un espai mètric. També direm que d és la distància o mètrica de l'espai mètric.

Definició 16.1.2 (Bola)**.** Siguin X amb la distància d un espai mètric, a un element de X i $r > 0$ un nombre real. Aleshores definim

$$\mathrm{B}(a, r) = \{x \in X \mid \mathrm{d}(x, a) < r\}$$

com la bola de radi r centrada en a.

Definició 16.1.3 (Obert)**.** Sigui X amb la distància d un espai mètric i $\mathcal{U}$ un subconjunt de X tals que per a tot element x de $\mathcal{U}$ existeix un $\varepsilon > 0$ real tal que $\mathrm{B}(x, \varepsilon) \subseteq \mathcal{U}$. Aleshores direm que $\mathcal{U}$ és un obert.

Proposició 16.1.4. *Siguin X amb la distància* d *un espai mètric i $\mathrm{B}(a, r)$ una bola de X. Aleshores $\mathrm{B}(a, r)$ és un obert.*

Demostració. Prenem un element b de $\mathrm{B}(a, r)$ i definim

$$\varepsilon = \frac{r - \mathrm{d}(a, b)}{2}. \tag{16.1}$$

Aleshores considerem la bola $\mathrm{B}(b,\varepsilon)$ i tenim que $\mathrm{B}(b,\varepsilon) \subseteq \mathrm{B}(a,r)$, ja que si prenem un element x de $\mathrm{B}(b,\varepsilon)$, per la definició de distància (16.1.1) trobem que

$$\begin{aligned} \mathrm{d}(x,a) &\leq \mathrm{d}(x,b) + \mathrm{d}(b,a) \\ &< \varepsilon + \mathrm{d}(b,a) && \text{(bola (16.1.2))} \\ &= \frac{r - \mathrm{d}(a,b)}{2} + \mathrm{d}(b,a) && \text{(16.1)} \\ &= \frac{r - \mathrm{d}(a,b)}{2} + \mathrm{d}(a,b) && \text{(distància (16.1.1))} \\ &= \frac{r + \mathrm{d}(a,b)}{2} < r, \end{aligned}$$

ja que, per la definició de bola (16.1.2) tenim que $\mathrm{d}(a,b) < r$ i per tant trobem $r + \mathrm{d}(a,b) < 2r$. □

Proposició 16.1.5 (Propietat de Hausdorff)**.** *Siguin X amb la distància* d *un espai mètric i x i y dos elements diferents de X. Aleshores existeixen dos oberts $\mathcal{U}$ i $\mathcal{V}$ disjunts tals que x és un element de $\mathcal{U}$ i y és un element de $\mathcal{V}$.*

Demostració. Definim $r = \frac{\mathrm{d}(x,y)}{3}$ i considerem les boles $\mathrm{B}(x,r)$ i $\mathrm{B}(y,r)$. Per la definició de distància (16.1.1) i la definició de bola (16.1.2) tenim que x és un element de $\mathrm{B}(x,r)$ i y és un element de $\mathrm{B}(y,r)$.

També tenim que les boles $\mathrm{B}(x,r)$ i $\mathrm{B}(y,r)$ són disjuntes, ja que si prenem un element a de X tal que a pertanyi a $\mathrm{B}(x,r)$ i a $\mathrm{B}(y,r)$ aleshores tenim, per la definició de bola (16.1.2), que $\mathrm{d}(x,a) < r$ i $\mathrm{d}(a,y) < r$, i per la definició de distància (16.1.1) tenim que

$$\mathrm{d}(x,a) + \mathrm{d}(a,y) \geq \mathrm{d}(x,y).$$

Ara bé, tenim per hipòtesi que $r = \frac{\mathrm{d}(x,y)}{3}$. Per tant

$$\begin{aligned} \mathrm{d}(x,y) &\leq \mathrm{d}(x,a) + \mathrm{d}(a,y) \\ &\leq \frac{\mathrm{d}(x,y)}{3} + \frac{\mathrm{d}(x,y)}{3} \\ &\leq \frac{2\,\mathrm{d}(x,y)}{3} < \mathrm{d}(x,y), \end{aligned}$$

i per tant aquest a no existeix i trobem que $\mathrm{B}(x,r)$ i $\mathrm{B}(y,r)$ són disjunts.

Per acabar, per la proposició 16.1.4 tenim que les boles $\mathrm{B}(x,r)$ i $\mathrm{B}(y,r)$ són oberts, i hem acabat. □

16.2 L'espai topològic

16.2.1 Una topologia d'un conjunt i els oberts

Definició 16.2.1 (Topologia)**.** Sigui X un conjunt i τ una família de subconjunts de X tals que

1. $\emptyset$ i X són elements de τ.
2. La intersecció d'una família finita d'elements de τ és un element de τ.

3. La unió d'una família d'elements de τ és un element de τ.

Aleshores direm que τ és una topologia de X o que X amb la topologia τ és un espai topològic.

També direm que els elements de τ són oberts i que els elements de X són punts.

Exemple 16.2.2 (Topologia induïda per una mètrica)**.** *Siguin X amb la distància* d *un espai mètric i $\tau = \{\mathcal{U} \subseteq X \mid \mathcal{U}$ és un obert$\}$. Volem veure que X amb la topologia τ és un espai topològic.*

Solució. Per la definició d'obert (16.1.3) trobem que $\emptyset$ és un obert, ja que per l'axioma de regularitat (2.1.9) tenim que $\emptyset$ és un subconjunt de X, i per a tot x de X existeix un $\varepsilon > 0$ tal que $\mathrm{B}(x, \varepsilon)$ pertany a $\emptyset$. També tenim que X és un obert, ja que pel Teorema de la doble inclusió (2.1.3) tenim que $X \subseteq X$ i si prenem un element x de X tenim que per a tot $\varepsilon > 0$ la bola $\mathrm{B}(x, \varepsilon)$ és un subconjunt de X. Per tant $\emptyset$ i X són elements de τ.

Prenem $\{\mathcal{U}_i\}_{i=1}^n$ una família d'elements de τ i considerem

$$\mathcal{U} = \bigcap_{i=1}^n \mathcal{U}_i.$$

Sigui x un element de $\mathcal{U}$. Per la definició d'obert (16.2.1) tenim que per a tot $i \in \{1, \ldots, n\}$ existeix un $\varepsilon_i > 0$ real tal que

$$\mathrm{B}(x, \varepsilon_i) \subseteq \mathcal{U}_i.$$

Per tant, si definim $\varepsilon = \min_{i \in \{1,\ldots,n\}} \varepsilon_i$. Aleshores per la definició de bola (16.1.2) tenim que

$$\mathrm{B}(x, \varepsilon) \subseteq \mathrm{B}(x, \varepsilon_i) \quad \text{per a tot } i \in \{1, \ldots, n\}.$$

i per tant $\mathrm{B}(x, \varepsilon) \subset \mathcal{U}$ i per la definició d'obert (16.2.1) tenim que $\mathcal{U}$ és un obert.

Prenem $\{\mathcal{U}_i\}_{i \in I}$ una família d'oberts de τ i considerem

$$\mathcal{U} = \bigcup_{i \in I} \mathcal{U}_i.$$

Sigui x un element de $\mathcal{U}$. Per la definició d'unió de conjunts (2.1.12) tenim que existeix un $i \in I$ tal que $\mathcal{U}_i$ conté x. Ara bé, per hipòtesi tenim que $\mathcal{U}_i$ és un obert, i per la definició d'obert (16.1.3) trobem que existeix un $\varepsilon > 0$ tal que $\mathrm{B}(x, \varepsilon)$ és un subconjunt de $\mathcal{U}_i$, i com que $\mathcal{U}_i$ és un subconjunt de $\mathcal{U}$ tenim que $\mathrm{B}(x, \varepsilon)$ també és un subconjunt de $\mathcal{U}$, i per la definició d'obert (16.1.3) trobem que $\mathcal{U}$ és un obert, i per la definició d'espai topològic (16.2.1) hem acabat. $\diamondsuit$

Exemple 16.2.3 (Topologia grollera)**.** *Siguin X i $\tau = \{\emptyset, X\}$ dos conjunts. Aleshores τ és una topologia de X.*

Solució. Comprovem les condicions de la definició de topologia. Com que $\tau = \{\emptyset, X\}$ tenim que $\emptyset$ i X són elements de τ. Observem també que $\emptyset \cap X = \emptyset$, $X \cap X = X$ i $\emptyset \cup X = X \cup X = X$, i per la definició de topologia (16.2.1), tenim que τ és una topologia de X. $\diamondsuit$

Exemple 16.2.4 (Topologia discreta)**.** *Siguin X i $\tau = \mathcal{P}(X)$ dos conjunts. Aleshores τ és una topologia de X.*

Solució. Tenim per l'axioma del conjunt potència (2.1.4) que $\emptyset$ i X són subconjunts de τ, ja que per l'axioma de regularitat (2.1.9) trobem que $\emptyset \subseteq X$, i pel Teorema de la doble inclusió (2.1.3) trobem que $X \subseteq X$.

Per la definició d'unió de conjunts (2.1.12) trobem que si $\{\mathcal{U}_i\}_{i \in I}$ és una família de subconjunts de X aleshores

$$\bigcup_{i \in I} \mathcal{U}_i \subseteq X,$$

i per la definició d'intersecció de conjunts (2.1.13) trobem que si $\{\mathcal{U}_i\}_{i=1}^{n}$ és una família de subconjunts de X aleshores

$$\bigcap_{i=1}^{n} \mathcal{U}_i \subseteq X,$$

i per tant, com que $\tau = \mathcal{P}(X)$ trobem per la definició de topologia (16.2.1) que τ és una topologia de X. $\lozenge$

16.2.2 Tancats

Definició 16.2.5 (Tancat)**.** Siguin X amb la topologia τ un espai topològic i $\mathcal{C}$ un subconjunt de X tal que $X \setminus \mathcal{C}$ sigui obert. Aleshores direm que $\mathcal{C}$ és tancat.

Teorema 16.2.6. *Sigui X amb la topologia τ un espai topològic. Aleshores*

1. *$\emptyset$ i X són tancats.*
2. *La unió de qualsevol família finita de tancats és un tancat.*
3. *La intersecció de qualsevol família de tancats és un tancat.*

Demostració. Comencem veient el punt (1). Tenim que $X \setminus \emptyset = X$. Per la definició d'espai topològic (16.2.1) tenim que X és un obert, i per la definició de tancat (16.2.5) trobem que $\emptyset$ és un tancat.

També tenim que $X \setminus X = \emptyset$. Per la definició d'espai topològic (16.2.1) tenim que $\emptyset$ és un obert, i per la definició de tancat (16.2.5) trobem que X és un tancat.

Veiem ara el punt (2). Prenem una família $\{\mathcal{C}_i\}_{i=1}^{n}$ de tancats de X i considerem

$$X \setminus \bigcup_{i=1}^{n} \mathcal{C}_i = X \cap \left(\bigcup_{i=1}^{n} \mathcal{C}_i \right)^{\complement}.$$

Per la primera llei de De Morgan (1.1.17) trobem que

$$\begin{aligned} X \cap \left(\bigcup_{i=1}^{n} \mathcal{C}_i \right)^{\complement} &= X \cap \left(\bigcap_{i=1}^{n} \mathcal{C}_i^{\complement} \right) \\ &= \bigcap_{i=1}^{n} \left(X \cap \mathcal{C}_i^{\complement} \right) \\ &= \bigcap_{i=1}^{n} (X \setminus \mathcal{C}_i). \end{aligned}$$

Per hipòtesi tenim que per a tot $i \in \{1, \dots, n\}$ el conjunt $\mathcal{C}_i$ és un tancat, i per la definició de tancat (16.2.5) tenim que per a tot $i \in \{1, \dots, n\}$ el conjunt $X \setminus \mathcal{C}_i$ és un obert, i per la definició d'espai topològic (16.2.1) tenim que $\bigcap_{i=1}^{n}(X \setminus \mathcal{C}_i)$ és un obert. Ara bé, tenim que

$$X \setminus \bigcup_{i=1}^{n} \mathcal{C}_i = \bigcap_{i=1}^{n} (X \setminus \mathcal{C}_i),$$

i per tant, per la definició de tancat (16.2.5) trobem que $\bigcup_{i=1}^{n} \mathcal{C}_i$ és un tancat.

Veiem per acabat el punt (3). Prenem una família $\{\mathcal{C}_i\}_{i \in I}$ de tancats de X i considerem

$$X \setminus \bigcap_{i \in I} \mathcal{C}_i = X \cap \left(\bigcap_{i \in I} \mathcal{C}_i \right)^{\complement}.$$

Per la segona llei de De Morgan (1.1.18) trobem que

$$\begin{aligned} X \cap \left(\bigcap_{i \in I} \mathcal{C}_i \right)^{\complement} &= X \cap \left(\bigcup_{i \in I} \mathcal{C}_i^{\complement} \right) \\ &= \bigcup_{i \in I} \left(X \cap \mathcal{C}_i^{\complement} \right) \\ &= \bigcup_{i \in I} (X \setminus \mathcal{C}_i). \end{aligned}$$

Ara bé, per la definició de tancat (16.2.5) tenim que per a tot $i \in I$ el conjunt $X \setminus \mathcal{C}_i$ és un obert, i per la definició d'espai topològic (16.2.1) trobem que el conjunt $\bigcup_{i \in I}(X \setminus \mathcal{C}_i)$ és un obert. Tenim

$$X \setminus \bigcap_{i \in I} \mathcal{C}_i = \bigcup_{i \in I} (X \setminus \mathcal{C}_i),$$

i, de nou per la definició de tancat (16.2.5), tenim que $\bigcap_{i \in I} \mathcal{C}_i$ és un tancat, com volíem veure. □

16.2.3 Base d'una topologia

Definició 16.2.7 (Base d'una topologia)**.** Siguin X amb la topologia τ un espai topològic i $\mathcal{B}$ una família d'oberts tals que per a tot obert $\mathcal{U}$ de X i per a tot punt x de $\mathcal{U}$ existeix un $B \in \mathcal{B}$ tal que $x \in B \subseteq \mathcal{U}$. Aleshores direm que $\mathcal{B}$ és una base de la topologia τ.

Exemple 16.2.8. *Siguin X amb la distància* d *un espai mètric i*

$$\mathcal{B} = \{\mathrm{B}(x, \varepsilon) \mid x \in X \ i \ \varepsilon > 0\}$$

un conjunt. Aleshores $\mathcal{B}$ és una base de la topologia τ induïda per la mètrica.

Solució. Tenim que

$$\tau = \{\mathcal{U} \subseteq X \mid \mathcal{U} \text{ es un obert}\}.$$

Prenem doncs un obert $\mathcal{U}$ de τ i un punt x de $\mathcal{U}$. Per la definició d'obert (16.1.3) tenim que existeix un $\varepsilon > 0$ real tal que $\mathrm{B}(x, \varepsilon)$ és un subconjunt de $\mathcal{U}$, i per la definició de base d'una topologia (16.2.7) hem acabat. ♢

Definició 16.2.9 (Finor d'una topologia)**.** Siguin X un conjunt i τ, τ' dues topologies de X tals que $\tau \subset \tau'$. Aleshores direm que τ' és més fina que τ.

Proposició 16.2.10. *Siguin X un conjunt i $\mathcal{B}$ una família de subconjunts de X tals que*

$$\bigcup_{B \in \mathcal{B}} B = X$$

i tal que per a tot $\mathcal{U}$ i $\mathcal{V}$ de $\mathcal{B}$ i per a tot x de $\mathcal{U} \cap \mathcal{V}$ existeix un $\mathcal{W}$ de $\mathcal{B}$ tal que x pertanyi a $\mathcal{W}$ i $\mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}$. Aleshores existeix una única topologia τ de X tal que $\mathcal{B}$ és una base de τ i τ és la topologia menys fina que conté els elements de $\mathcal{B}$.

Demostració. Definim

$$\tau = \{\mathcal{U} \subseteq X \mid \mathcal{U} = \cup_{i \in I} B_i \text{ amb } B_i \in \mathcal{B}\} \tag{16.2}$$

Observem que X i $\emptyset$ pertanyen a τ.

Siguin $\mathcal{U}$ i $\mathcal{V}$ dos elements de $\mathcal{B}$ i prenem un element x de $\mathcal{U} \cap \mathcal{V}$. Per hipòtesi tenim que existeix un element $\mathcal{W}_x$ de $\mathcal{B}$ tal que $x \in \mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}$. Per tant

$$\mathcal{U} \cap \mathcal{V} = \bigcup_{x \in \mathcal{U} \cap \mathcal{V}} \mathcal{W}_x,$$

i per la definició del conjunt τ tenim que $\mathcal{U} \cap \mathcal{V}$ és un element de τ.

Prenem dos elements $\mathcal{U}$ i $\mathcal{V}$ del conjunt τ. Per la definició (16.2) trobem que existeixen dues famílies $\{\mathcal{U}_i\}_{i \in I}$ i $\{\mathcal{V}_j\}_{j \in J}$ d'elements de $\mathcal{B}$ tals que

$$\mathcal{U} = \bigcup_{i \in I} \mathcal{U}_i \quad \text{i} \quad \mathcal{V} = \bigcup_{j \in J} \mathcal{V}_j.$$

Per tant tenim que

$$\mathcal{U} \cap \mathcal{V} = \bigcup_{i \in I} \bigcup_{j \in J} (\mathcal{U}_i \cap \mathcal{V}_j),$$

i per la definició (16.2) trobem que $\mathcal{U} \cap \mathcal{V}$ pertany a τ. Per tant per la definició de topologia (16.2.1) trobem que τ és una topologia de X.

Veiem ara que $\mathcal{B}$ és base de la topologia τ. Prenem un obert $\mathcal{U}$ de τ i x un element de $\mathcal{U}$. Per la definició (16.2) tenim que existeix una família $\{B_i\}_{i \in I}$ d'elements de $\mathcal{B}$ tal que

$$\mathcal{U} = \bigcup_{i \in I} B_i.$$

Per tant existeix un element B de $\mathcal{B}$ tal que $x \in B$ i $B \subseteq \mathcal{U}$ i per la definició de base d'una topologia (16.2.7) trobem que $\mathcal{B}$ és una base de la topologia τ.

Continuem veient que τ és la topologia menys fina que conté els elements de $\mathcal{B}$. Suposem que existeix una topologia τ' de X tal que τ és més fina que τ' i tal que τ' conté els elements de $\mathcal{B}$. Per la definició de finor d'una topologia (16.2.9) això és que $\tau' \subset \tau$.

Prenem un obert $\mathcal{U}$ de τ. Per la definició (16.2) trobem que existeix una família $\{B_i\}_{i\in I}$ d'elements de $\mathcal{B}$ tals que

$$\mathcal{U} = \bigcup_{i\in I} B_i.$$

Ara bé, tenim per hipòtesi que $\mathcal{B}$ és un subconjunt de la topologia τ', i per la definició de topologia (16.2.1) trobem que $\mathcal{U}$ pertany a τ'. Per tant ha de ser $\tau \subseteq \tau'$, i trobem que τ és la topologia menys fina que conté els elements de $\mathcal{B}$.

Veiem ara que aquesta topologia τ és única. Suposem que existeix una altre topologia τ' tal que $\mathcal{B}$ és una base de τ' i τ' és la topologia menys fina que conté els elements de $\mathcal{B}$.

Prenem un obert $\mathcal{U}$ de τ. Per la definició (16.2) trobem que existeix una família $\{B_i\}_{i\in I}$ d'elements de $\mathcal{B}$ tals que

$$\mathcal{U} = \bigcup_{i\in I} B_i.$$

Per la definició de topologia (16.2.1) tenim que $\mathcal{U}$ és un element de τ', ja que per hipòtesi $\mathcal{B}$ és un subconjunt de τ'. Per tant tenim que $\tau \subseteq \tau'$. Ara bé, ja hem vist que τ és la topologia menys fina que conté els elements de $\mathcal{B}$, i per la definició de finor d'una topologia (16.2.9) això és que $\tau' \subseteq \tau$, i pel Teorema de la doble inclusió (2.1.3) ha de ser $\tau = \tau'$, com volíem veure. □

16.2.4 Entorns, interior i adherència

Definició 16.2.11 (Entorn)**.** Siguin X amb la topologia τ un espai topològic, x un punt i N un conjunt tal que existeix un obert $\mathcal{U}$ satisfent que x és un element de $\mathcal{U}$ i $\mathcal{U}$ és un subconjunt de N. Aleshores direm que N és un entorn de x.

També direm que x és un punt interior de N.

Observació 16.2.12. *Siguin X amb la topologia τ un espai topològic i x un punt. Aleshores existeix un subconjunt N de X tal que N és un entorn de x.*

Demostració. Si $N = X$ tenim $x \in X \subseteq N$. Per la definició de topologia (16.2.1) tenim que X és un obert i per la definició d'entorn (16.2.11) trobem que N és un entorn de x. □

Definició 16.2.13 (Interior)**.** Siguin X amb la topologia τ un espai topològic, x un punt de X, A subconjunt de X i

$$\operatorname{Int}(A) = \{x \in X \mid A \text{ és un entorn de } x\}.$$

Aleshores direm que $\operatorname{Int}(A)$ és l'interior del conjunt A.

Proposició 16.2.14. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores* $\mathrm{Int}(A)$ *és un obert.*

Demostració. Prenem un punt x de $\mathrm{Int}(A)$. Per la definició d'interior (16.2.13) tenim que existeix un obert $\mathcal{U}_x$ tal que $x \in \mathcal{U}_x$ i $\mathcal{U}_x \subseteq A$. Aleshores tenim

$$\begin{aligned}\mathrm{Int}(A) &= \bigcup_{x\in\mathrm{Int}(A)} \{x\} \\ &\subseteq \bigcup_{x\in\mathrm{Int}(A)} \mathcal{U}_x \\ &\subseteq \bigcup_{x\in\mathrm{Int}(A)} \mathrm{Int}(A) = \mathrm{Int}(A).\end{aligned}$$

Per tant tenim que

$$\mathrm{Int}(A) \subseteq \bigcup_{x\in\mathrm{Int}(A)} \mathcal{U}_x \quad \text{i} \quad \bigcup_{x\in\mathrm{Int}(A)} \mathcal{U}_x \subseteq \mathrm{Int}(A),$$

i pel Teorema de la doble inclusió (2.1.3) trobem

$$\mathrm{Int}(A) = \bigcup_{x\in\mathrm{Int}(A)} \mathcal{U}_x$$

i per la definició de topologia (16.2.1) trobem que $\mathrm{Int}(A)$ és un obert. □

Proposició 16.2.15. *Siguin X amb la topologia τ un espai topològic, A un subconjunt de X i*

$$Y = \{\mathcal{U} \in \tau \mid \mathcal{U} \subseteq A\}.$$

Aleshores

$$\mathrm{Int}(A) = \bigcup_{\mathcal{U}\in Y} \mathcal{U}.$$

Demostració. Sigui x un element de A tal que existeixi un obert $\mathcal{U}_x$ satisfent que x és un element de $\mathcal{U}_x$ i $\mathcal{U}_x$ és un subconjunt de A. Aleshores tenim

$$\begin{aligned}\mathrm{Int}(A) &= \bigcup_{x\in\mathrm{Int}(A)} \{x\} \\ &\subseteq \bigcup_{x\in\mathrm{Int}(A)} \mathcal{U}_x \\ &\subseteq \bigcup_{x\in\mathrm{Int}(A)} \mathrm{Int}(A) = \mathrm{Int}(A)\end{aligned}$$

i pel Teorema de la doble inclusió (2.1.3) trobem

$$\mathrm{Int}(A) = \bigcup_{\mathcal{U}\in Y} \mathcal{U}$$

com volíem veure. □

Corol·lari 16.2.16. *Siguin X amb la topologia τ un espai topològic, A un subconjunt de X i $\mathcal{U}$ un obert tal que $\mathcal{U}$ sigui un subconjunt de A. Aleshores $\mathcal{U}$ és un subconjunt de* $\mathrm{Int}(A)$.

Corol·lari 16.2.17. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores A és un obert si i només si $A = \mathrm{Int}(A)$.*

Definició 16.2.18 (Punt adherent)**.** Siguin X amb la topologia τ un espai topològic, A un subconjunt de X i x un punt tal que per a tot entorn N de x tenim

$$A \cap N \neq \emptyset.$$

Aleshores direm que x és un punt adherent a A.

Definició 16.2.19 (Clausura)**.** Siguin X amb la topologia τ un espai topològic i A un conjunt. Aleshores direm que

$$\mathrm{Cl}(A) = \{x \in X \mid x \text{ és un punt adherent a } A\}$$

és la clausura de A.

Observació 16.2.20. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores*

$$A \subseteq \mathrm{Cl}(A).$$

Proposició 16.2.21. *Siguin X amb τ un espai topològic i A un subconjunt de X. Aleshores $\mathrm{Cl}(A)$ és un tancat.*

Demostració. Prenem un element x de $X \setminus \mathrm{Cl}(A)$. Per la definició de clausura (16.2.19) tenim que existeix un entorn N de x tal que

$$A \cap N = \emptyset, \tag{16.3}$$

i per la definició d'entorn (16.2.11) tenim que existeix un obert $\mathcal{U}_x$ tal que x és un element de $\mathcal{U}_x$ i que $\mathcal{U}_x$ és un subconjunt de N. Per tant, per (16.3) tenim que $A \cap \mathcal{U}_x = \emptyset$.

Per tant trobem

$$\begin{aligned} X \setminus \mathrm{Cl}(A) &= \bigcup_{x \in X \setminus \mathrm{Cl}(A)} \{x\} \\ &\subseteq \bigcup_{x \in X \setminus \mathrm{Cl}(A)} \mathcal{U}_x \subseteq X \setminus \mathrm{Cl}(A), \end{aligned}$$

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

$$X \setminus \mathrm{Cl}(A) =\subseteq \bigcup_{x \in X \setminus \mathrm{Cl}(A)} \mathcal{U}_x,$$

i com que $\mathcal{U}_x$ és un obert, per la definició de topologia (16.2.1) tenim que $X \setminus \mathrm{Cl}(A)$ és un obert, i per la definició de tancat (16.2.5) trobem que $\mathrm{Cl}(A)$ és un tancat. ☐

Proposició 16.2.22. *Siguin X amb la topologia τ un espai topològic, A un subconjunt de X i*

$$Y = \{\mathcal{C} \subseteq X \mid A \subseteq \mathcal{C} \text{ i } \mathcal{C} \text{ és un tancat}\}.$$

Aleshores

$$\mathrm{Cl}(A) = \bigcap_{\mathcal{C} \in Y} \mathcal{C}.$$

Demostració. Sigui x un punt adherent a A amb $x \notin A$. Suposem que existeix un tancat $\mathcal{C}$ tal que A és un subconjunt de $\mathcal{C}$ i tal que x no pertany a $\mathcal{C}$. Aleshores x és un element de $X \setminus \mathcal{C}$, i per la definició de tancat (16.2.5) tenim que $\mathcal{U} = X \setminus \mathcal{C}$ és un obert. Ara bé, per la definició d'entorn (16.2.11) tenim que $\mathcal{U}$ és un entorn de x, però A és un subconjunt de $\mathcal{C}$, i per tant tenim que $X \setminus \mathcal{C}$ és un subconjunt de $X \setminus A$, i tenim que $\mathcal{U}$ és un subconjunt de $X \setminus A$, i per tant $A \cap \mathcal{U} = \emptyset$. Ara bé, per la definició de punt adherent (16.2.18) tenim que $A \cap \mathcal{U} \neq \emptyset$. Per tant ha de ser que x pertany a $\mathcal{C}$ i trobem que

$$\mathrm{Cl}(A) \subseteq \bigcap_{\mathcal{C} \in Y} \mathcal{C}. \tag{16.4}$$

Per la proposició 16.2.21 tenim que $\mathrm{Cl}(A)$ és un tancat, i per tant $\mathrm{Cl}(A)$ és un element de Y i tenim que

$$\bigcap_{\mathcal{C} \in Y} \mathcal{C} \subseteq \mathrm{Cl}(A). \tag{16.5}$$

Ara bé, tenim (16.4) i (16.5), i pel Teorema de la doble inclusió (2.1.3) trobem que

$$\mathrm{Cl}(A) = \bigcap_{\mathcal{C} \in Y} \mathcal{C}. \qquad \square$$

Corol·lari 16.2.23. *Siguin X amb la topologia τ un espai topològic, A un subconjunt de X i $\mathcal{C}$ un tancat tal que A és un subconjunt de $\mathcal{C}$. Aleshores* $\mathrm{Cl}(A) \subseteq \mathcal{C}$.

Corol·lari 16.2.24. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores A és tancat si i només si $A = \mathrm{Cl}(A)$.*

Proposició 16.2.25. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores*

$$\mathrm{Cl}(X \setminus A) = X \setminus \mathrm{Int}(A).$$

Demostració. Prenem un element x de $\mathrm{Cl}(X \setminus A)$. Per la definició de clausura (16.2.19) tenim que per a tot obert $\mathcal{U}$ que conté x tenim que

$$\mathcal{U} \cap (X \setminus A) \neq \emptyset.$$

Ara bé, per la definició d'interior (16.2.13) que $\mathrm{Int}(A)$ és un subconjunt de A, i per tant $X \setminus A$ és un subconjunt de $X \setminus \mathrm{Int}(A)$, i per tant $\mathcal{U} \cap (X \setminus \mathrm{Int}(A)) \neq \emptyset$. Per tant per la definició d'interior (16.2.13) trobem que

$$\mathrm{Cl}(X \setminus A) \subseteq X \setminus \mathrm{Int}(A) \tag{16.6}$$

Prenem ara un element x de $X \setminus \mathrm{Int}(A)$. Per la definició d'interior (16.2.13) tenim que no existeix cap obert $\mathcal{U}$ tal que x sigui un element de $\mathcal{U}$ i $\mathcal{U}$ sigui un subconjunt de A, o equivalentment, que $\mathcal{U} \cap (X \setminus A) \neq \emptyset$ per a tot obert $\mathcal{U}$ tal que x sigui un element de $\mathcal{U}$ i que $\mathcal{U}$ sigui un subconjunt de A. Ara bé, per la definició de clausura (16.2.19) tenim que $\mathcal{U}$ és un element de $\mathrm{Cl}(X \setminus A)$, i per tant trobem que

$$X \setminus \mathrm{Int}(A) \subseteq \mathrm{Cl}(X \setminus A). \tag{16.7}$$

Per tant, amb (16.6) i (16.7) i el Teorema de la doble inclusió (2.1.3) trobem que $\mathrm{Cl}(X \setminus A) = X \setminus \mathrm{Int}(A)$, com volíem veure. $\square$

16.3 Aplicacions contínues

16.3.1 Aplicacions obertes, tancades i contínues

Definició 16.3.1 (Aplicació oberta)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics i $f\colon X \longrightarrow Y$ una aplicació tal que per a tot obert $\mathcal{U}$ de X tenim que el conjunt $\{f(x) \in Y \mid x \in \mathcal{U}\}$ és un obert de Y. Aleshores direm que f és una aplicació oberta.

Observació 16.3.2. *La composició d'aplicacions obertes és oberta.*

Definició 16.3.3 (Aplicació tancada)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics i $f\colon X \longrightarrow Y$ una aplicació tal que per a tot tancat $\mathcal{C}$ de X tenim que el conjunt $\{f(x) \in Y \mid x \in \mathcal{C}\}$ és un tancat de Y. Aleshores direm que f és una aplicació tancada.

Observació 16.3.4. *La composició d'aplicacions tancades és tancada.*

Definició 16.3.5 (Aplicació contínua)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics i $f\colon X \longrightarrow Y$ una aplicació tal que per a tot obert $\mathcal{V}$ de Y el conjunt $\{x \in X \mid f(x) \in \mathcal{V}\}$ és un obert de X. Aleshores direm que f és una aplicació contínua.

Observació 16.3.6. *La composició d'aplicacions contínues és contínua.*

Exemple 16.3.7. *Considerem*

$$\mathrm{S}^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}.$$

Volem veure que S^n *és un tancat de* $\mathbb{R}^{n+1}$*.*

Solució. Definim l'aplicació

$$\begin{aligned} f : \mathbb{R}^{n+1} &\longrightarrow \mathbb{R} \\ x &\longmapsto \|x\|. \end{aligned}$$

Veiem que f és una aplicació contínua. Sigui $\mathcal{V}$ un obert de $\mathbb{R}$ i considerem el conjunt

$$\mathcal{U} = \{x \in \mathbb{R}^{n+1} \mid f(x) \in \mathcal{V}\}. \tag{16.8}$$

Prenem un element x de $\mathbb{R}^{n+1}$. Com que, per hipòtesi, tenim que $\mathcal{V}$ és un obert de $\mathbb{R}$, per la definició d'obert (16.1.3) tenim que existeix un real $\delta > 0$ tal que la bola $\mathrm{B}(f(x), \delta)$ és un subconjunt de $\mathbb{R}$, i per la definició (16.8) tenim que existeix un element y de $\mathbb{R}^{n+1}$ tal que $f(y)$ és un element de $\mathrm{B}(f(x), \delta)$, i per la definició de bola (16.1.2) trobem que $|f(x) - f(y)| < \delta$. $\diamondsuit$

16.3.2 Homeomorfismes entre topologies

Definició 16.3.8 (Homeomorfisme)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics i $f\colon X \longrightarrow Y$ una aplicació bijectiva, oberta i contínua. Aleshores direm que f és un homeomorfisme.

Definició 16.3.9 (Espais topològics homeomorfs)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics tals que existeix un homeomorfisme $f\colon X \longrightarrow Y$. Aleshores direm que X i Y són dos espais topològics homeomorfs. També denotarem

$$X \cong Y.$$

Exemple 16.3.10. *Volem veure que* $\mathbb{R}$ *és homeomorf a l'interval* $(0,1)$.

Solució. $\Diamond$

Proposició 16.3.11. *Siguin* X *amb la topologia* τ_X *i* Y *amb la topologia* τ_Y *dos espais topològics. Aleshores la relació*

$$X \cong Y \iff X \text{ és homeomorf a } Y$$

és una relació d'equivalència.

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

1. Reflexiva: Tenim que l'aplicació Id_X és bijectiva, oberta i contínua. Per la definició d'homeomorfisme entre topologies (16.3.8) tenim que Id_x és un homeomorfisme, i per la definició d'espais topològics homeomorfs (16.3.9) tenim que $X \cong X$.

2. Simètrica: Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics homeomorfs. Per la definició d'espais topològics homeomorfs (16.3.9) tenim que existeix un homeomorfisme $f\colon X \longrightarrow Y$.

   Pel Teorema 2.2.19 trobem que existeix l'aplicació inversa f^{-1} de Y a X, i pel corol·lari 2.2.20 tenim que l'aplicació f^{-1} és bijectiva.

   També trobem que f^{-1} és oberta, ja que per la definició d'homeomorfisme entre topologies (16.3.8) tenim que f és contínua, i per la definició d'aplicació oberta (16.3.1) i la definició d'aplicació contínua (16.3.5) trobem que f^1 és oberta. De mateixa manera trobem que f^{-1} és contínua, ja que per la definició d'homeomorfisme entre topologies (16.3.8) tenim que f és oberta, i per la definició d'aplicació contínua (16.3.5) i la definició d'aplicació oberta (16.3.1) trobem que f^{-1} és contínua.

   Per tant, per la definició d'homeomorfisme entre topologies (16.3.8) trobem que f^{-1} és un homeomorfisme entre topologies i per tant $Y \cong X$.

3. Transitiva: Siguin X_1 amb la topologia τ_1, X_2 amb la topologia τ_2 i X_3 amb la topologia τ_3 tres espais topològics tals que $X_1 \cong X_2$ i $X_2 \cong X_3$. Per la definició d'espais topològics homeomorfs (16.3.9) tenim que existeixen dos homeomorfismes $f\colon X_1 \longrightarrow X_2$ i $g\colon X_2 \longrightarrow X_3$.

   Considerem l'aplicació $h = g \circ f$. Pel Teorema 2.2.15 trobem que h és bijectiva, i per l'observació 16.3.2 i l'observació 16.3.6 trobem que h és oberta i contínua, i per la definició d'homeomorfisme entre topologies (16.3.8) trobem que h és un homeomorfisme entre X_1 i X_3, i per la definició d'espais topològics homeomorfs (16.3.9) trobem que $X_1 \cong X_3$.

I per la definició de relació d'equivalència (2.3.2) hem acabat. $\square$

Capítol 17

Altres topologies

17.1 Topologies induïdes

17.1.1 La topologia induïda per un subconjunt

Proposició 17.1.1. *Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores A amb la topologia*

$$\tau_A = \{\mathcal{U} \subseteq A \mid \textit{Existeix un obert } \mathcal{W} \textit{ de } X \textit{ tal que } \mathcal{U} = \mathcal{W} \cap A\} \tag{17.1}$$

és un espai topològic.

Demostració. Observem que A pertany a τ_A, ja que per la definició de topologia (16.2.1) tenim que X és un obert de X, i trobem $X \cap A = A$. També tenim que $\emptyset$ pertany a τ_A, ja que per la definició de topologia (16.2.1) tenim que $\emptyset$ és un obert de X, i trobem $\emptyset \cap A = \emptyset$.

Sigui $\{\mathcal{U}_i\}_{i\in I}$ una família d'elements de τ_A. Per la definició (17.1) tenim que existeix una família $\{\mathcal{W}_i\}_{i\in I}$ d'oberts de X tals que $\mathcal{U}_i = \mathcal{W}_i \cap A$, per a tot i de I. Considerem ara

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i.$$

Tenim que

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{W}_i \cap A,$$

i tenim

$$\mathcal{U} = A \cap \left(\bigcup_{i\in I} \mathcal{W}_i\right),$$

i per la definició de topologia (16.2.1) tenim que $\bigcup_{i\in I} \mathcal{W}_i$ és un obert de X, i per la definició (17.1) trobem que $\mathcal{U}$ pertany a τ_A.

Sigui $\{\mathcal{U}\}_{i=1}^n$ una família d'elements de τ_A. Per la definició (17.1) tenim que existeix una família $\{\mathcal{W}_i\}_{i=1}^n$ d'oberts de X tals que $\mathcal{U}_i = \mathcal{W}_i \cap A$, per a tot i de $\{1, \ldots, n\}$. Considerem ara

$$\mathcal{U} = \bigcap_{i=1}^{n} \mathcal{U}_i.$$

Tenim que
$$\mathcal{U} = \bigcap_{i=1}^{n} \mathcal{W}_i \cap A,$$
i tenim
$$\mathcal{U} = A \cap \left(\bigcap_{i=1}^{n} \mathcal{W}_i \right),$$
i per la definició de topologia (16.2.1) tenim que $\bigcap_{i=1}^{n} \mathcal{W}_i$ és un obert de X, i per la definició (17.1) trobem que $\mathcal{U}$ pertany a τ_A. Per tant per la definició d'espai topològic (16.2.1) trobem que A amb la topologia τ_A és un espai topològic. □

Definició 17.1.2 (Topologia induïda per un subconjunt)**.** Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores denotem
$$\tau_A = \{\mathcal{U} \subseteq A \mid \text{Existeix un obert } \mathcal{W} \text{ de } X \text{ tal que } \mathcal{U} = \mathcal{W} \cap A\}$$
i direm que τ_A és la topologia induïda per A.

Aquesta definició té sentit per la proposició 17.1.1.

Definició 17.1.3 (Subespai topològic)**.** Siguin X amb la topologia τ un espai topològic i A un subconjunt de X. Aleshores direm que A amb la topologia τ_A és un subespai topològic de X.

Proposició 17.1.4. *Siguin X amb la topologia τ un espai topològic i τ_A la topologia induïda per un subconjunt A de X. Aleshores $\mathcal{C}$ és un tancat de A si i només si existeix un tancat $\mathcal{K}$ de τ tal que $\mathcal{C} = A \cap \mathcal{K}$.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Sigui $\mathcal{C}$ un tancat de A. Per la definició de tancat (16.2.5) tenim que això és equivalent a que $A \setminus \mathcal{C}$ és un obert. Per la definició de topologia induïda per un subconjunt (17.1.2) tenim que això és si i només si existeix un obert $\mathcal{U}$ de X tal que $A \setminus \mathcal{C} = \mathcal{U} \cap A$. Ara bé, tenim que $\mathcal{U} = X \setminus (X \setminus \mathcal{U})$, i per la definició de tancat (16.2.5) tenim que $\mathcal{K} = X \setminus \mathcal{U}$ és un tancat, i tenim que
$$\begin{aligned}\mathcal{C} &= A \setminus A \setminus \mathcal{C} \\ &= A \setminus (\mathcal{U} \cap A) \\ &= A \setminus \mathcal{U} \\ &= A \cap (X \setminus \mathcal{U}) \\ &= A \cap \mathcal{K}\end{aligned}$$
i hem acabat.

Veiem ara que la condició és necessària ($\Longleftarrow$). Sigui $\mathcal{K}$ un tancat de X. Prenem $\mathcal{C} = A \cap \mathcal{K}$. Aleshores tenim
$$\begin{aligned}A \setminus \mathcal{C} &= A \setminus (A \cap \mathcal{K}) \\ &= A \cap (X \setminus \mathcal{K}).\end{aligned}$$
Ara bé, per hipòtesi, tenim que $\mathcal{K}$ és un tancat de X, i per tant $X \setminus \mathcal{K}$ és un obert, i per la definició de topologia induïda per un subconjunt (17.1.2) trobem que $A \cap (X \setminus \mathcal{K})$ és un obert de A, i per la definició de tancat (16.2.5) tenim que $A \setminus \mathcal{C}$ és un tancat de A, com volíem veure. □

Proposició 17.1.5. *Siguin X amb la topologia τ una espai topològic, $\mathcal{A}$ un obert de X, τ_A la topologia induïda per A i $\mathcal{U}$ un subconjunt de A. Aleshores $\mathcal{U}$ és un obert de A si i només si $\mathcal{U}$ és un obert de X.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $\mathcal{U}$ és un obert de A. Per la definició de topologia induïda per un subconjunt (17.1.2) tenim que existeix un obert $\mathcal{W}$ de X tal que $\mathcal{U} = A \cap \mathcal{W}$. Ara bé, com que, per hipòtesi, A i $\mathcal{W}$ són dos oberts de X per la definició de topologia (16.2.1) trobem que $\mathcal{U}$ és un obert de X.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que $\mathcal{U}$ és un obert de X. Com que, per la definició de topologia (16.2.1), $\mathcal{U}$ és un subconjunt de A, tenim que $\mathcal{U} = A \cap \mathcal{U}$, i per la definició de topologia induïda per un subconjunt (17.1.2) trobem que $\mathcal{U}$ és un obert de A. □

Proposició 17.1.6. *Siguin X amb la topologia τ una espai topològic, $\mathcal{A}$ un tancat de X, τ_A la topologia induïda per A i $\mathcal{C}$ un subconjunt de A. Aleshores $\mathcal{C}$ és un tancat de A si i només si $\mathcal{C}$ és un tancat de X.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $\mathcal{C}$ és un tancat de A. Per la proposició 17.1.4 tenim que existeix un tancat $tancatK$ de X tal que $\mathcal{C} = A \cap \mathcal{K}$. Ara bé, com que A i $\mathcal{K}$ són dos tancats de X, pel Teorema 16.2.6 trobem que $\mathcal{C}$ és un tancat de X.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que $\mathcal{C}$ és un tancat de X. Com que, per la definició de topologia (16.2.1), $\mathcal{C}$ és un subconjunt de A, tenim que $\mathcal{C} = A \cap \mathcal{C}$, i per la definició de topologia induïda per un subconjunt (17.1.2) trobem que $\mathcal{C}$ és un tancat de A. □

17.1.2 La topologia producte

Proposició 17.1.7. *Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics,*

$$\mathcal{B} = \{\mathcal{V}_X \times \mathcal{V}_Y \subseteq X \times Y \mid \mathcal{V}_X \in \tau_X \text{ } i \text{ } \mathcal{V}_Y \in \tau_Y\}$$

i

$$\tau = \{\mathcal{U} \subseteq X \times Y \mid \textit{Existeix una família } \{\mathcal{U}_i\}_{i\in I} \subseteq \mathcal{B} \textit{ tal que } \mathcal{U} = \cup_{i\in I}\mathcal{U}_i\}.$$

Aleshores τ és una topologia de $X \times Y$.

Demostració. Per l'axioma de regularitat (2.1.9) trobem que $\emptyset$ és un subconjunt de $\mathcal{B}$, i per la definició de τ trobem que $\emptyset$ és un element de τ.

Per la definició de topologia (16.2.1) trobem que X és un obert de X i Y és un obert de Y. Per tant $X \times Y$ és un element de $\mathcal{B}$ i per la definició de τ trobem que $X \times Y$ és un element de τ.

Prenem una família $\{\mathcal{U}_i\}_{i\in I}$ d'elements de τ i considerem

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i.$$

Per la definició de τ trobem que per a cada i de I existeix una família $\{\mathcal{V}_j\}_{j\in J_i}$ d'elements de $\mathcal{B}$ tals que

$$\mathcal{U}_i = \bigcup_{j\in J_i} V_j.$$

Ara bé, per la definició de $\mathcal{B}$ trobem que per a tot j de J_i existeixen oberts $\mathcal{V}_{j,X}$ de X i oberts $\mathcal{V}_{j,Y}$ de Y tals que

$$\mathcal{V}_j = \mathcal{V}_{j,X} \times \mathcal{V}_{j,Y},$$

i per tant trobem que

$$\mathcal{U} = \bigcup_{i\in I} \bigcup_{j\in J_i} (\mathcal{V}_{j,X} \times \mathcal{V}_{j,Y}),$$

i per la definició de τ trobem que $\mathcal{U}$ és un element de τ.

Siguin $\mathcal{U}$ i $\mathcal{V}$ dos elements de τ i considerem

$$\mathcal{W} = \mathcal{U} \cap \mathcal{V}.$$

Per la definició de τ tenim que existeixen dues famílies $\{\mathcal{U}_i\}_{i\in I}$ i $\{\mathcal{V}_j\}_{j\in J}$ de $\mathcal{B}$ tals que

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i \quad \text{i} \quad \mathcal{V} = \bigcup_{j\in J} \mathcal{V}_j,$$

i per la definició de $\mathcal{B}$ trobem que per a cada i de I existeixen un obert $\mathcal{U}_{i,X}$ de X i un obert $\mathcal{U}_{i,Y}$ de Y tals que

$$\mathcal{U}_i = \mathcal{U}_{i,X} \times \mathcal{U}_{i,Y}$$

i per a cada j de J existeixen un obert $\mathcal{V}_{j,X}$ de X i un obert $\mathcal{V}_{j,Y}$ de Y tals que

$$\mathcal{V}_j = \mathcal{V}_{j,X} \times \mathcal{V}_{j,Y}.$$

Per tant tenim que

$$\mathcal{U} = \left(\bigcup_{i\in I}(\mathcal{U}_{i,X} \times \mathcal{U}_{i,Y})\right) \cap \left(\bigcup_{j\in J}(\mathcal{V}_{j,X} \times \mathcal{V}_{j,Y})\right)$$

i trobem que

$$\mathcal{U} = \left(\bigcup_{i\in I}\mathcal{U}_{i,X} \times \bigcup_{i\in I}\mathcal{U}_{i,Y}\right) \cap \left(\bigcup_{j\in J}\mathcal{V}_{j,X} \times \bigcup_{j\in J}\mathcal{V}_{j,Y}\right)$$

i per tant

$$\mathcal{U} = \left(\bigcup_{i\in I}\mathcal{U}_{i,X} \cap \bigcup_{j\in J}\mathcal{V}_{j,X}\right) \times \left(\bigcup_{i\in I}\mathcal{U}_{i,Y} \cap \bigcup_{j\in J}\mathcal{V}_{j,Y}\right),$$

i per la definició de topologia (16.2.1) trobem que

$$\bigcup_{i\in I}\mathcal{U}_{i,X} \cap \bigcup_{j\in J}\mathcal{V}_{j,X} \quad \text{i} \quad \bigcup_{i\in I}\mathcal{U}_{i,Y} \cap \bigcup_{j\in J}\mathcal{V}_{j,Y}$$

són oberts, i per la definició de τ trobem que $\mathcal{U}$ és un element de τ, i per la definició de topologia (16.2.1) trobem que τ és una topologia de $X \times Y$, com volíem veure. □

Definició 17.1.8 (Topologia producte)**.** Siguin X amb la topologia τ_X i Y amb la topologia τ_Y dos espais topològics i

$$\mathcal{B} = \{\mathcal{V}_X \times \mathcal{V}_Y \subseteq X \times Y \mid \mathcal{V}_X \in \tau_X \text{ i } \mathcal{V}_Y \in \tau_Y\}.$$

Aleshores direm que $X \times Y$ amb la topologia

$$\tau = \{\mathcal{U} \subseteq X \times Y \mid \text{Existeix una família } \{\mathcal{U}_i\}_{i\in I} \subseteq \mathcal{B} \text{ tal que } \mathcal{U} = \cup_{i\in I}\mathcal{U}_i\}$$

és l'espai topològic producte de X i Y i que τ és la topologia producte de X i Y.

Aquesta definició té sentit per la proposició 17.1.7

Exemple 17.1.9 (Projeccions)**.** *Siguin $X \times Y$ amb la topologia τ la topologia producte de X i Y i*

$$\begin{aligned} \pi_X \colon X \times Y &\longrightarrow X \\ (x, y) &\longmapsto x \end{aligned}$$

un aplicació. Volem veure que π_X és contínua i oberta.

Solució. Comencem veient que π_X és contínua. Prenem un obert $\mathcal{U}$ de X i considerem

$$\{(x, y) \in X \times Y \mid \pi_X(x, y) \in \mathcal{U}\}.$$

Tenim doncs que

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

i com que, per hipòtesi, Y és un espai topològic, tenim que Y és un obert de Y, i de nou per hipòtesi tenim que $\mathcal{U}$ és un obert de X. Per tant trobem que $\mathcal{U} \times Y$ és un obert de $X \times Y$, i per la definició d'aplicació contínua (16.3.5) trobem que π_X és contínua.

Veiem ara que π_X és oberta. Prenem un obert A de $X \times Y$ i un punt x de $\{\pi_X(x, y) \in X \mid (x, y) \in A\}$. Aleshores tenim que existeix un punt a de A tal que $\pi_X(a) = x$. Per la definició de topologia producte (17.1.8) tenim que existeixen un obert $\mathcal{U}_x$ de X i un obert $\mathcal{V}_x$ de Y tals que

$$a \in \mathcal{U}_x \times \mathcal{V}_x \subseteq A.$$

Observem que

$$\mathcal{U} = \{\pi_X(x, y) \in X \mid (x, y) \in \mathcal{U}_x \times \mathcal{V}_x\}$$

és un obert de X, i per tant

$$x \in \mathcal{U}_x \subseteq \{\pi_X(x, y) \in X \mid (x, y) \in A\},$$

i, denotant $B = \{\pi_X(x, y) \in X \mid (x, y) \in A\}$, trobem que

$$\begin{aligned} B &\subseteq \bigcup_{x\in B} \{x\} \\ &\subseteq \bigcup_{x\in B} \mathcal{U}_x \subseteq B, \end{aligned}$$

i per tant trobem que $\{\pi_X(x, y) \in X \mid (x, y) \in A\}$ és un obert de X, i per la definició d'aplicació oberta (16.3.1) trobem que π_X és una aplicació oberta. $\Diamond$

Corol·lari 17.1.10. *Sigui X un espai topològic i y un element. Aleshores*

$$X \times \{y\} \cong X.$$

Teorema 17.1.11. *Siguin Z amb la topologia τ_Z un espai topològic, $X \times Y$ amb la topologia producte de X i Y, $f\colon Z \longrightarrow X \times Y$ una aplicació. Aleshores f és contínua si i només si les aplicacions $\pi_X \circ f$ i $\pi_Y \circ f$ són contínues.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que f és contínua. Aleshores per l'exemple 17.1.9 trobem que les aplicacions π_X i π_Y són contínues i per l'observació 16.3.6 hem acabat.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que les aplicacions $\pi_X \circ f$ i $\pi_Y \circ f$ són contínues.

Sigui $\mathcal{V} \times \mathcal{W}$ un obert de $X \times Y$. Per la definició de topologia producte (17.1.8) tenim que $\mathcal{V}$ és un obert de X i $\mathcal{W}$ és un obert de Y. Ara bé, com que per hipòtesi les aplicacions $\pi_X \circ f$ i $\pi_Y \circ f$ són contínues, tenim per la definició d'aplicació contínua (16.3.5) que els conjunts

$$\mathcal{U}_X = \{x \in Z \mid \pi_X \circ f(x) \in \mathcal{V}\} \quad \text{i} \quad \mathcal{U}_Y = \{x \in Z \mid \pi_Y \circ f(x) \in \mathcal{W}\}$$

són oberts de Z, i per la definició de topologia (16.2.1) trobem que el conjunt

$$\mathcal{U} = \mathcal{U}_X \cup \mathcal{U}_Y$$

és un obert de Z. Per tant tenim que

$$\mathcal{U} = \{x \in Z \mid f(x) \in \mathcal{V} \times \mathcal{W}\},$$

és un obert de Z, i com que per hipòtesi el conjunt $\mathcal{V} \times \mathcal{W}$ és un obert de $X \times Y$, per la definició d'aplicació oberta (16.3.1) trobem que f és una aplicació oberta. $\square$

Proposició 17.1.12. *Siguin X_1 amb la topologia τ_{X_1}, X_2 amb la topologia τ_{X_2}, Y_1 amb la topologia τ_{Y_1} i Y_2 amb la topologia τ_{Y_2} quatre espais topològics tals que*

$$X_1 \cong X_2 \quad i \quad Y_1 \cong Y_2.$$

Aleshores

$$X_1 \times Y_1 \cong X_2 \times Y_2.$$

Demostració. Per la definició d'espais topològics homeomorfs (16.3.9) trobem que existeixen dos homeomorfismes $f\colon X_1 \longrightarrow X_2$ i $g\colon Y_1 \longrightarrow Y_2$. Considerem doncs l'aplicació

$$\begin{aligned} h\colon X_1 \times Y_1 &\longrightarrow X_2 \times Y_2 \\ (x,y) &\longmapsto (f(x), g(y)). \end{aligned}$$

Com que, per hipòtesi, les aplicacions f i g són homeomorfismes, tenim per la definició d'homeomorfisme entre topologies (16.3.8) que f i g són bijectives. Ara bé, trobem que h també és bijectiva, ja que té per inversa la funció

$$\begin{aligned} h^{-1}\colon X_2 \times Y_2 &\longrightarrow X_1 \times Y_1 \\ (x,y) &\longmapsto (f^{-1}(x), g^{-1}(y)). \end{aligned}$$

Continuem veient que h és una aplicació oberta. Per la definició d'aplicació oberta (16.3.1) i la definició d'aplicació contínua (16.3.5) en tenim prou amb veure que h^{-1} és una aplicació contínua. Observem que per a tot (x,y) de $X_2 \times Y_2$ tenim

$$\pi_{X_1} \circ h^{-1}(x,y) = f^{-1}(x) \quad \text{i} \quad \pi_{Y_1} \circ h^{-1}(x,y) = g^{-1}(y),$$

i com que, per hipòtesi, les aplicacions f^{-1} i g^{-1} són contínues tenim pel Teorema 17.1.11 que l'aplicació h^{-1} és contínua, i per tant h és una aplicació oberta.

Per acabar veiem ara que h és una aplicació contínua. Observem que per a tot (x,y) de $X_1 \times Y_1$ tenim

$$\pi_{X_2} \circ h(x,y) = f(x) \quad \text{i} \quad \pi_{Y_2} \circ h(x,y) = g(y),$$

i com que, per hipòtesi, les aplicacions f i g són aplicacions contínues tenim pel Teorema 17.1.11 que l'aplicació h és contínua.

Per tant per la definició d'homeomorfisme entre topologies (16.3.8) trobem que h és un homeomorfisme, i per la definició d'espais topològics homeomorfs (16.3.9) trobem que $X_1 \times Y_1 \cong X_2 \times Y_2$, com volíem veure. □

17.2 La topologia quocient

17.2.1 Topologia quocient per una aplicació

Proposició 17.2.1. *Siguin X amb la topologia τ_X un espai topològic, Y un conjunt i $p\colon X \longrightarrow Y$ una aplicació exhaustiva. Aleshores*

$$\tau_Y = \{\mathcal{U} \subseteq Y \mid \mathrm{Im}^{-1}{}_{\mathcal{U}}(p) \in \tau_X\} \tag{17.2}$$

és una topologia de Y.

Demostració. Comprovem que τ_Y satisfà la definició de topologia (16.2.1). Tenim que $\emptyset$ pertany a τ_Y. Per la definició d'antiimatge d'una aplicació (5.2.2) trobem que $\mathrm{Im}_{\emptyset}(p) = \emptyset$, i com que per la definició de topologia (16.2.1) tenim que $\emptyset$ pertany a τ_X trobem que $\emptyset$ és un element de τ_Y.

Veiem ara que Y pertany a τ_Y. Per la definició d'antiimatge d'una aplicació (5.2.2) i com que, per hipòtesi, p és exhaustiva, per la definició d'aplicació exhaustiva (2.2.8) tenim que $\mathrm{Im}_Y^{-1}(p) = X$, i per la definició de topologia (16.2.1) tenim que X és un obert, i per tant Y pertany a τ_Y.

Sigui $\{\mathcal{U}_i\}_{i\in I}$ una família d'elements de τ_Y. Aleshores tenim que

$$\mathrm{Im}^{-1}{}_{\bigcup_{i\in I}\mathcal{U}_i}(p) = \bigcup_{i\in I} \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p),$$

i com que. per (17.2) trobem que $\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p)$ és un obert de X per a tot i de I, i per la definició de topologia trobem que

$$\bigcup_{i\in I} \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p)$$

és un obert de X, i per tant tenim que $\bigcup_{i\in I} \mathcal{U}_i$ és un element de τ_Y.

Prenem ara una família $\{\mathcal{U}_i\}_{i=1}^n$ d'elements de τ_Y. Tenim que

$$\mathrm{Im}^{-1}{}_{\bigcup_{i=1}^n \mathcal{U}_i}(p) = \bigcup_{i=1}^n \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p),$$

i com que. per (17.2) trobem que $\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p)$ és un obert de X per a tot i de $\{1, \ldots, n\}$, i per la definició de topologia trobem que

$$\bigcup_{i=1}^n \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(p)$$

és un obert de X, i per tant tenim que $\bigcup_{i=1}^n \mathcal{U}_i$ és un element de τ_Y. □

Definició 17.2.2 (Topologia quocient)**.** Siguin X amb la topologia τ_X un espai topològic, Y un conjunt i $p\colon X \longrightarrow Y$ una aplicació exhaustiva. Aleshores direm que Y amb la topologia

$$\tau_Y = \{\mathcal{U} \subseteq Y \mid \mathrm{Im}^{-1}{}_{\mathcal{U}}(p) \in \tau_X\}$$

és un espai topològic quocient, o que Y té la topologia quocient per p.

Aquesta definició té sentit per la proposició 17.2.1.

Observació 17.2.3. *Sigui Y un espai topològic amb la topologia quocient per una aplicació p. Aleshores p és contínua.*

Proposició 17.2.4. *Sigui Y un espai topològic amb la topologia quocient per una aplicació p. Aleshores un subconjunt $\mathcal{C}$ de Y és tancat si i només si $\mathrm{Im}^{-1}{}_{\mathcal{C}}(p)$ és un tancat.*

Demostració. Denotem per X l'espai topològic sobre el que p està definida. Sigui $\mathcal{C}$ un tancat de Y. Aleshores, per la definició de tancat (16.2.5), tenim que $Y \setminus \mathcal{C}$ és un obert de Y. Ara bé, tenim que $\mathrm{Im}^{-1}{}_{Y\setminus\mathcal{C}}(p)$ és un obert de X. Ara bé, tenim que

$$\mathrm{Im}^{-1}{}_{Y\setminus\mathcal{C}}(p) = X \setminus \mathrm{Im}^{-1}{}_{\mathcal{C}}(p),$$

i per la definició de tancat (16.2.5) trobem que $\mathrm{Im}^{-1}{}_{\mathcal{C}}(p)$ és un tancat de X, com volíem veure. □

Teorema 17.2.5. *Siguin Y un espai topològic amb la topologia quocient per una aplicació p, Z un espai topològic i $f\colon Y \longrightarrow Z$ una aplicació. Aleshores $f \circ p$ és contínua si i només si f és contínua.*

Demostració. Denotem per X l'espai topològic sobre el que p està definida.

Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $f \circ p$ és contínua. Sigui $\mathcal{U}$ un obert de Z. Per la definició d'aplicació contínua (16.3.5) en tenim prou en veure que $\mathrm{Im}^{-1}{}_{\mathcal{U}}(f)$ és un obert.

Tenim per la definició d'aplicació contínua (16.3.5) que $\mathrm{Im}^{-1}{}_{\mathcal{U}}(p \circ f)$ és un obert de X., i per tant, per la definició de topologia quocient (17.2.2) tenim que $\mathrm{Im}^{-1}{}_{\mathcal{U}}(f)$ és un obert de Y, com volíem.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que f és contínua. Aleshores per l'observació 16.3.6 hem acabat. □

Exemple 17.2.6. *Volem calcular la topologia de l'espai quocient $A = \{a, b, c\}$ induït per l'aplicació $p\colon \mathbb{R} \longrightarrow A$, definida per*

$$p(x) = \begin{cases} a & si\ x > 0 \\ b & si\ x < 0 \\ c & si\ x = 0. \end{cases} \tag{17.3}$$

Solució. Calculem els oberts de A. Tenim per la definició de topologia quocient (17.2.2) que aquests són les antiimatges dels oberts de $\mathbb{R}$ per p. Prenem un obert $\mathcal{U}$ de $\mathbb{R}$.

Observem primer que si $\mathcal{U} = \emptyset$ aleshores

$$\mathrm{Im}^{\text{-}1}{}_{\mathcal{U}}(p) = \emptyset,$$

i si 0 pertany a $\mathcal{U}$ aleshores, per la definició d'obert (16.1.3) tenim que existeixen un x de $\mathcal{U}$ positiu i un y de $\mathcal{U}$ negatiu, i per tant

$$\mathrm{Im}^{\text{-}1}{}_{\mathcal{U}}(p) = \{a, b, c\}.$$

Suposem doncs que 0 no pertany a $\mathcal{U}$.

Suposem que per a tot x de $\mathcal{U}$ tenim que $x > 0$. Aleshores, per la definició d'antiimatge d'una aplicació (5.2.2) i (17.3) tenim que

$$\mathrm{Im}^{\text{-}1}{}_{\mathcal{U}}(p) = \{a\}.$$

Suposem ara que per a tot x detext si 0 $\mathcal{U}$ tenim que $x > 0$. Aleshores, de nou per la definició d'antiimatge d'una aplicació (5.2.2) i (17.3) tenim que

$$\mathrm{Im}^{\text{-}1}{}_{\mathcal{U}}(p) = \{b\}.$$

Suposem ara que existeixen un x de $\mathcal{U}$ positiu i un y de $\mathcal{U}$ negatiu. Aleshores, com que tenim que 0 no pertany a $\mathcal{U}$, trobem que

$$\mathrm{Im}^{\text{-}1}{}_{\mathcal{U}}(p) = \{a, b\}.$$

Per tant trobem que els oberts de A són

$$\tau = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{a, b, c\}\}.$$ ♢

17.2.2 Topologia quocient per una relació d'equivalència

Exemple 17.2.7 (Projecció a un quocient)**.** *Siguin X un espai topològic i $\sim$ una relació d'equivalència. Volem veure que $X/\sim$ té la topologia quocient per l'aplicació*

$$\begin{aligned} \pi\colon X &\longrightarrow X/\sim \\ x &\longmapsto \overline{x}. \end{aligned}$$

Solució. Hem de veure que π és exhaustiva. Prenem un element $\overline{x}$ de $X/\sim$. Aleshores tenim que $\pi(x) = \overline{x}$ i per la definició de topologia quocient (17.2.2) hem acabat. ♢

Definició 17.2.8. Siguin X un espai topològic, $\sim$ una relació d'equivalència sobre X i π la projecció de X en $X/\sim$ donada per

$$\begin{aligned} \pi\colon X &\longrightarrow X/\sim \\ x &\longmapsto \overline{x}. \end{aligned}$$

Aleshores denotem la topologia Y induïda per π com $X/\sim$.

Aquesta definició té sentit per l'exemple 17.2.7.

Exemple 17.2.9. *Volem veure que l'espai quocient*

$$Y = [0,1]/\{0 \sim 1\}$$

amb la projecció π és homeomorf a

$$\mathrm{S}^1 = \{x \in \mathbb{R}^2 \mid \|x\| = 1\}.$$

Solució. ◊

17.2.3 Topologia quocient per un grup

Definició 17.2.10 (Acció d'un grup sobre un espai topològic)**.** Siguin G amb l'operació $*$ un grup amb element neutre e i X un espai topològic tals que per a tot g de G existeix una aplicació contínua $\theta_g\colon X \longrightarrow X$ tal que per a tot x de X es satisfà $\theta_e(x) = x$ i per a tot g i h de G es satisfà $\theta_g \circ \theta_h = \theta_{g*h}$. Aleshores direm que G actua sobre X.

Observació 17.2.11. *Sigui G un grup que actua sobre X i g un element de G. Aleshores θ_g és un homeomorfisme.*

Definició 17.2.12 (Domini fonamental)**.** Siguin G un grup que actua sobre un espai topològic X i D un subespai de X tal que per a tot x de X existeixen un g de G i d de D tals que

$$x = \theta_g(d).$$

Aleshores direm que D és un domini fonamental de X.

Exemple 17.2.13. *Considerem les aplicacions*

$$S(x,y) = (x, y+1) \quad i \quad T(x,y) = (x-1, -y)$$

sobre l'espai topològic $\mathbb{R}^2$ i el grup $G = \langle\{S,T\}\rangle$. Volem veure que $[0,1)\times[0,1)$ és un domini fonamental de X.

Solució. Observem que la inversa de T és $T^{-1} = (x+1, y)$, i T^{-1} per la definició de pertany a G.

Prenem un punt (x,y) de $\mathbb{R}^2$. Tenim que existeixen dos enters x_0 i y_0 tals que $x_0 \le x < x_0 + 1$ i $y_0 \le y < y_0 + 1$. Per tant

$$(x_0, y_0) = S^{x_0}(x - x_0, 0) + T^{-y_0}(0, y - y_0),$$

i per la definició de domini fonamental (17.2.12) hem acabat. ◊

Proposició 17.2.14. *Sigui G amb l'operació $*$ un grup que actua sobre un espai topològic X. Aleshores la relació $\sim$ definida per a tot x i y de X com*

$$x \sim y \iff \text{existeix un } g \in G \text{ tal que } \theta_g(x) = y$$

és una relació d'equivalència.

Demostració. □

Definició 17.2.15 (Quocient d'un espai per l'acció d'un grup)**.** Sigui G amb l'operació $*$ un grup que actua sobre un espai topològic X i $\sim$ la relació d'equivalència definida per a tot x i y de X com

$$x \sim y \iff \text{existeix un } g \in G \text{ tal que } \theta_g(x) = y.$$

Aleshores denotarem per

$$X/\sim = X/G$$

la topologia quocient de X per G.

Aquesta definició té sentit per la proposició 17.2.14.

Capítol 18

Espais topològics

18.1 Espais compactes

18.1.1 Recobriments

Definició 18.1.1 (Recobriment)**.** Siguin X un espai topològic i $\{\mathcal{U}_i\}_{i\in I}$ una família de subespais de X tals que

$$X = \bigcup_{i\in I} \mathcal{U}_i.$$

Aleshores direm que $\{\mathcal{U}_i\}_{i\in I}$ és un recobriment de X.

Si I és finit direm que $\{\mathcal{U}_i\}_{i\in I}$ és un recobriment finit de X, i si I és infinit direm que $\{\mathcal{U}_i\}_{i\in I}$ és un recobriment infinit de X.

Definició 18.1.2 (Recobriment obert)**.** Sigui $\{\mathcal{U}_i\}_{i\in I}$ un recobriment d'un espai topològic X tal que per a tot i de I tenim que $\mathcal{U}_i$ és un obert de X. Aleshores direm que $\{\mathcal{U}_i\}_{i\in I}$ és un recobriment obert de X.

Exemple 18.1.3. *Volem trobar un recobriment de* $\mathbb{R}$*.*

Solució. Prenem la família d'oberts $\{(-i,i)\}_{i\in\mathbb{N}}$. Aleshores tenim que

$$\mathbb{R} = \bigcup_{i\in\mathbb{N}} (-i,i),$$

ja que si x és un element de $\mathbb{R}$ trobem que existeix un natural m tal que $|x| < m$, i per tant x pertany a l'interval $(-m,m)$. $\Diamond$

Definició 18.1.4 (Subrecobriment)**.** Siguin $\{\mathcal{U}_i\}_{i\in I}$ un recobriment d'un espai topològic X i J un subconjunt de I tal que la família $\{\mathcal{U}_j\}_{j\in J}$ és un recobriment de X. Aleshores direm que $\{\mathcal{U}_j\}_{j\in J}$ és un subrecobriment de $\{\mathcal{U}_i\}_{i\in I}$.

Si J és finit direm que $\{\mathcal{U}_j\}_{j\in J}$ és un recobriment finit de $\{\mathcal{U}_i\}_{i\in I}$, i si J és infinit direm que $\{\mathcal{U}_j\}_{j\in J}$ és un recobriment infinit de $\{\mathcal{U}_i\}_{i\in I}$.

18.1.2 Compacitat

Definició 18.1.5 (Compacte)**.** Sigui X un espai topològic tal que tot recobriment obert de X admet un subrecobriment finit. Aleshores direm que X és compacte.

Exemple 18.1.6. *Volem veure que* $\mathbb{R}$ *no és compacte.*

Solució. Per l'exemple 18.1.3 tenim que $\{(-i,i)\}_{i\in\mathbb{N}}$ és un recobriment obert de $\mathbb{R}$.

Suposem que existeix un subrecobriment finit de $\{(-i,i)\}_{i\in\mathbb{N}}$. Això és que existeix un subconjunt I de $\mathbb{N}$ finit tal que $\{(-i,i)\}_{i\in I}$ és un recobriment de $\mathbb{R}$. Com que I és finit tenim que existeix un natural m tal que $m=\max\{i\in I\}$, i tenim que $m+1$ no pertany a cap interval de la família $\{(-i,i)\}_{i\in I}$. Per tant trobem que

$$m+1\notin\bigcup_{i\in I}(-i,i).$$

Ara bé, per la definició de recobriment d'un espai (18.1.1) trobem que ha de ser

$$m+1\in\mathbb{R}=\bigcup_{i\in I}(-i,i),$$

i arribem a contradicció, trobant que no existeix cap subrecobriment finit de $\{(-i,i)\}_{i\in\mathbb{N}}$. ♢

Proposició 18.1.7. *Siguin* X *i* Y *dos espais topològics homeomorfs. Aleshores* X *és compacte si i només si* Y *és compacte.*

Demostració. Per la definició de relació d'equivalència (2.3.2) tenim que si $X\cong Y$ aleshores $Y\cong X$, i per tant només ens cal veure que si X és compacte aleshores Y és compacte.

Suposem doncs que X és compacte. Per la definició d'espais topològics homeomorfs (16.3.9) tenim que existeix un homeomorfisme $f\colon X\longrightarrow Y$.

Sigui $\{\mathcal{U}_i\}_{i\in I}$ un recobriment obert de Y. Per la definició d'homeomorfisme entre topologies (16.3.8) i la definició de recobriment obert (18.1.2) tenim que la família $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)\}_{i\in I}$ és un recobriment obert de X.

Ara bé, per la definició d'espai topològic compacte (18.1.5) trobem que existeix un subrecobriment finit $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_j}(f)\}_{j\in J}$ de $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)\}_{i\in I}$, i de nou per la definició d'homeomorfisme entre topologies (16.3.8) i la definició de recobriment obert (18.1.2) tenim que la família $\{\mathcal{U}_j\}_{j\in J}$ és un subrecobriment obert de $\{\mathcal{U}_i\}_{i\in I}$, i per la definició d'espai topològic compacte (18.1.5) trobem que Y és compacte. □

Exemple 18.1.8. *Volem veure que l'interval* $(0,1)$ *no és compacte.*

Solució. Per l'exemple 16.3.10 tenim que l'interval $(0,1)$ és homeomorf a $\mathbb{R}$, per l'exemple 18.1.6 trobem que $\mathbb{R}$ no és compacte i per la proposició 18.1.7 tenim que $(0,1)$ no és compacte. ♢

Proposició 18.1.9. *Sigui* X *un espai topològic finit. Aleshores* X *és compacte.*

Demostració. Sigui $\{\mathcal{U}_i\}_{i\in I}$ un recobriment obert de X, i per la definició de recobriment obert (18.1.2) tenim que $\{\mathcal{U}_i\}_{i\in I} \subseteq \tau$.

Ara bé, tenim que $\tau \subseteq \mathcal{P}(X)$, i com que X és finit, $\mathcal{P}(X)$ també ho és, i per tant $\{\mathcal{U}_i\}_{i\in I}$ és finit i per la definició de recobriment finit d'un espai (18.1.1) trobem que $\{\mathcal{U}_i\}_{i\in I}$ és un recobriment finit de X, i per la definició d'espai topològic compacte (18.1.5) tenim que X és compacte. □

Proposició 18.1.10. *Sigui X un espai topològic amb la topologia discreta. Aleshores X és compacte si i només si X és finit.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Veurem que si X és infinit aleshores X no és compacte.

Per l'exemple 16.2.4 tenim que tot subconjunt de X és un obert, i com que

$$X = \bigcup_{x\in X} \{x\}$$

per la definició de recobriment obert (18.1.2) trobem que $\{\{x\}\}_{x\in X}$ és un recobriment obert de X.

Ara bé, com que X és infinit, si $\{\{x\}\}_{x\in I}$ és un subrecobriment finit de $\{\{x\}\}_{x\in X}$ tenim que existeix algun x_0 de X tal que $x_0 \notin I$, i per tant

$$x_0 \notin \bigcup_{x\in I} \{x\}$$

i trobem que el recobriment $\{\{x\}\}_{x\in X}$ no admet cap subrecobriment finit, i per la definició d'espai topològic compacte (18.1.5) trobem que X no és compacte.

Per veure que la condició és necessària ($\Longleftarrow$) en tenim prou amb la proposició 18.1.9. □

Definició 18.1.11 (Compacitat per tancats)**.** Sigui X un espai topològic tal que per a tota família de tancats $\{\mathcal{C}_i\}_{i\in I}$ de X amb

$$\bigcap_{i\in I} \mathcal{C}_i = \emptyset$$

existeix una subfamília finita $\{\mathcal{C}_i\}_{i\in J}$ tal que

$$\bigcap_{i\in J} \mathcal{C}_i = \emptyset.$$

Aleshores direm que X és compacte per tancats.

Proposició 18.1.12. *Sigui X un espai topològic. Aleshores X és compacte si i només si X és compacte per tancats.*

Demostració. Siguin X un espai topològic compacte i $\{\mathcal{C}_i\}_{i\in I}$ una família de tancats de X tals que

$$\bigcap_{i\in I} \mathcal{C}_i = \emptyset.$$

Per la definició de tancat (16.2.5) tenim que per a tot i de I el conjunt $\mathcal{U}_i = X \setminus \mathcal{C}_i$ és un obert de X, i tenim que

$$\begin{aligned} X &= X \setminus \emptyset \\ &= X \setminus \left(\bigcap_{i \in I} \mathcal{C}_i \right) \\ &= \bigcup_{i \in I} (X \setminus \mathcal{C}_i) = \bigcup_{i \in I} \mathcal{U}_i, \end{aligned}$$

i per la definició de recobriment obert (18.1.2) trobem que $\{\mathcal{U}_i\}_{i \in I}$ és un recobriment obert de X. Ara bé, per la definició d'espai topològic compacte (18.1.5) tenim que existeix un subrecobriment finit $\{\mathcal{U}_i\}_{i \in J}$ de $\{\mathcal{U}_i\}_{i \in I}$, i per la definició de subrecobriment (18.1.4) tenim que

$$\begin{aligned} X &= \bigcup_{i \in J} \mathcal{U}_i \\ &= \bigcup_{i \in J} (X \setminus \mathcal{C}_i) = X \setminus \bigcap_{i \in J} \mathcal{C}_i, \end{aligned}$$

i per tant trobem que

$$\bigcap_{i \in J} \mathcal{C}_i = \emptyset$$

i per la definició de compacte per tancats (18.1.11) trobem que X és compacte per tancats. □

Definició 18.1.13 (Compacitat de subconjunts)**.** Sigui A un subconjunt d'un espai topològic X tal que per a tota família d'oberts $\{\mathcal{U}_i\}_{i \in I}$ de X tal que

$$A \subseteq \bigcup_{i \in I} \mathcal{U}_i$$

existeix una subfamília finita $\{\mathcal{U}_i\}_{i \in J}$ de $\{\mathcal{U}_i\}_{i \in I}$ tal que

$$A \subseteq \bigcup_{i \in J} \mathcal{U}_i.$$

Aleshores direm que A és un subconjunt compacte de X. També direm que $\{\mathcal{U}_i\}_{i \in I}$ és un recobriment obert de A.

18.1.3 Propietats dels espais compactes

Teorema 18.1.14. *Siguin A un subconjunt compacte d'un espai topològic X, Y un espai topològic i $f \colon X \longrightarrow Y$ una aplicació contínua. Aleshores $\operatorname{Im}_A(f)$ és un subconjunt compacte de Y.*

Demostració. Sigui $\{\mathcal{U}_i\}_{i \in I}$ un recobriment obert de $\operatorname{Im}_A(f)$. Per la definició de recobriment obert d'un subconjunt (18.1.13) trobem que

$$\operatorname{Im}_A(f) \subseteq \bigcup_{i \in I} \mathcal{U}_i,$$

i per tant tenim que
$$A \subseteq \bigcup_{i \in I} \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f).$$
Com que, per la definició de recobriment obert d'un subconjunt (18.1.13), per a tot i de I el conjunt $\mathcal{U}_i$ és un obert de Y, per la definició de funció contínua (5.2.4) tenim que $\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)$ és un obert de X, i trobem per la definició de recobriment obert d'un subconjunt (18.1.13) que $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)\}_{i \in I}$ és un recobriment obert de A.

Ara bé, tenim per hipòtesi que A és un subconjunt compacte de X, i per la definició de subconjunt compacte (18.1.13) tenim que existeix una subfamília finita $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)\}_{i \in J}$ de $\{\mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f)\}_{i \in I}$ tal que
$$A \subseteq \bigcup_{i \in J} \mathrm{Im}^{-1}{}_{\mathcal{U}_i}(f).$$

Tenim doncs que
$$\mathrm{Im}_A(f) \subseteq \bigcup_{i \in J} \mathcal{U}_i,$$
i per la definició de compacitat d'un subconjunt (18.1.13) hem acabat. □

Corol·lari 18.1.15. *Siguin X un espai topològic compacte i p una aplicació exhaustiva. Aleshores X/p és compacte.*

Demostració. Per l'observació 17.2.3 tenim que $p\colon X \longrightarrow X/p$ és contínua. Per la definició d'imatge d'una aplicació (5.2.1) i la definició d'aplicació exhaustiva (2.2.8) tenim que $X/p = \mathrm{Im}(p)$, i pel Teorema 18.1.14 trobem que X/p és compacte. □

Teorema 18.1.16. *Sigui $\mathcal{C}$ un tancat d'un espai topològic compacte X. Aleshores $\mathcal{C}$ és compacte.*

Demostració. Sigui $\{\mathcal{U}_i\}_{i \in I}$ un recobriment obert de $\mathcal{C}$. Per la definició de recobriment obert d'un subconjunt (18.1.13) tenim que
$$\mathcal{C} \subseteq \bigcup_{i \in I} \mathcal{U}_i.$$
Per tant
$$X = \left(\bigcup_{i \in I} \mathcal{U}_i \right) \cup (X \setminus \mathcal{C}),$$
i per la definició de recobriment obert (18.1.2) tenim que $\{\mathcal{U}_i\}_{i \in I} \cup (X \setminus \mathcal{C})$ és un recobriment obert de X.

Ara bé, per hipòtesi tenim que X és un compacte, i per la definició d'espai topològic compacte (18.1.5) tenim que existeix un subrecobriment finit de $\{\mathcal{U}_i\}_{i \in I} \cup (X \setminus \mathcal{C})$, i per tant existeix un subconjunt finit J de I tal que
$$\mathcal{C} \subseteq \bigcup_{i \in J} \mathcal{U}_i,$$
i per la definició de compacitat d'un subconjunt (18.1.13) hem acabat. □

Teorema 18.1.17 (Teorema de Tychonoff)**.** *Siguin X i Y dos espais topològics no buits. Aleshores $X \times Y$ és compacte si i només si X i Y són compactes.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $X \times Y$ és un compacte. Per l'exemple 17.1.9 trobem que les projeccions

$$\begin{aligned} \pi_X : X \times Y &\longrightarrow X \\ (x, y) &\longmapsto x \end{aligned}$$

i

$$\begin{aligned} \pi_Y : X \times Y &\longrightarrow Y \\ (x, y) &\longmapsto y \end{aligned}$$

són aplicacions contínues, i per la proposició 18.1.7 trobem que X i Y són compactes.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que X i Y són compactes i sigui $\{\mathcal{W}_i\}_{i \in I}$ un recobriment obert de $X \times Y$.

Prenem un punt x_0 de X. Aleshores per la definició de recobriment d'un espai (18.1.1) tenim que per a tot y de Y existeix un $i_{x_0,y}$ de I tal que el punt (x_0, y) pertany a $\mathcal{W}_{i_{x_0,y}}$, i per la definició de topologia quocient (17.2.2) tenim que existeixen oberts $\mathcal{U}_{i_{x_0,y}}$ i $\mathcal{V}_{i_{x_0,y}}$ de X i Y, respectivament, tals que

$$(x_0, y) \in \mathcal{U}_{i_{x_0,y}} \times \mathcal{V}_{i_{x_0,y}} \subseteq \mathcal{W}_{i_{x_0,y}}.$$

Trobem doncs que

$$\begin{aligned} Y &= \bigcup_{y \in Y} \{y\} \\ &\subseteq \bigcup_{y \in Y} \mathcal{V}_{i_{x_0,y}} \subseteq Y, \end{aligned}$$

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

$$\bigcup_{y \in Y} \mathcal{V}_{i_{x_0,y}} = Y.$$

Aleshores per la definició de recobriment obert (18.1.2) trobem que $\{\mathcal{V}_{i_{x_0,y}}\}_{y \in Y}$ és un recobriment obert de Y, i com que, per hipòtesi, Y és compacte, tenim per la definició d'espai topològic compacte (18.1.5) que existeix un subrecobriment finit $\{\mathcal{V}_{i_{x_0,y}}\}_{y \in Y_{x_0}}$ de $\{\mathcal{V}_{i_{x_0,y}}\}_{y \in Y}$.

Definim ara

$$\mathcal{U}_{x_0} = \bigcap_{y \in Y_{x_0}} \mathcal{U}_{i_{x_0,y}}. \tag{18.1}$$

Com que Y_{x_0} és finit, trobem per la definició de topologia (16.2.1) que $\mathcal{U}_{x_0}$ és un obert de X. Tenim doncs que

$$\begin{aligned} X &= \bigcup_{x \in X} \{x\} \\ &\subseteq \bigcup_{x \in X} \mathcal{U}_x \subseteq X, \end{aligned}$$

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

$$\bigcup_{x\in X} \mathcal{U}_x = X,$$

i de nou per la definició de recobriment obert (18.1.2) trobem que $\{\mathcal{U}_x\}_{x\in X}$ és un recobriment obert de X, i per la definició d'espai topològic compacte (18.1.5) trobem que existeix un subrecobriment finit $\{\mathcal{U}_x\}_{x\in J'}$ de $\{\mathcal{U}_x\}_{x\in X}$.

Definim el conjunt

$$J = \{(x,y) \in X \times Y \mid x \in J' \text{ i } y \in Y_x\} \tag{18.2}$$

i considerem la subfamília

$$\{\mathcal{W}_{i_{x,y}}\}_{(x,y)\in J}$$

de $\{\mathcal{W}_i\}_{i\in I}$. Sigui (x,y) un punt de $X \times Y$. Aleshores, com que la família $\{\mathcal{U}_x\}_{x\in J'}$ és un recobriment de X trobem per la definició de recobriment d'un espai (18.1.1) que existeix un p de J' tal que x pertany a $\mathcal{U}_p$, i com que la família $\{\mathcal{V}_{i_{x_0,y}}\}_{y\in Y_p}$ és un recobriment de Y trobem que existeix un q de Y_p tal que y pertany a $\mathcal{V}_q$.

Ara bé, també tenim per (18.1) i la definició d'intersecció de conjunts (2.1.13) que x pertany a $\mathcal{U}_{i_{p,q}}$, i per tant

$$(x,y) \in \mathcal{U}_{i_{p,q}} \times \mathcal{V}_{i_{p,q}} \subseteq \mathcal{W}_{i_{p,q}},$$

i per tant tenim que $\{\mathcal{W}_{i_{x,y}}\}_{(x,y)\in J}$ és un subrecobriment de $\{\mathcal{W}_i\}_{i\in I}$, i com que els conjunts J' i Y_x són finits, trobem per (18.2) que J és finit, aleshores per la definició de subrecobriment finit (18.1.4) trobem que $\{\mathcal{W}_{i_{x,y}}\}_{(x,y)\in J}$ és un subrecobriment finit de $\{\mathcal{W}_i\}_{i\in I}$ i per la definició d'espai topològic compacte (18.1.5) tenim que $X \times Y$ és compacte, com volíem. □

18.2 Espais de Hausdorff

18.2.1 L'axioma de Hausdorff

Definició 18.2.1 (Espai Hausdorff)**.** Sigui X un espai topològic tal que per a tots dos punts diferents x i y de X existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ de X tals que x pertany a $\mathcal{U}$ i y pertany a $\mathcal{V}$. Aleshores direm que X és Hausdorff.

Proposició 18.2.2. *Sigui X un espai mètric. Aleshores X és Hausdorff.*

Demostració. Per l'exemple 16.2.2 trobem que X és un espai topològic i per la proposició 16.1.5 tenim que X és Hausdorff. □

Proposició 18.2.3. *Siguin X i Y dos espais topològics homeomorfs. Aleshores X és Hausdorff si i només si Y és Hausdorff.*

Demostració. Per la proposició 16.3.11 tenim que si $X \cong Y$ aleshores $Y \cong X$, i per tant només ens cal veure que si X és Hausdorff aleshores Y és Hausdorff.

Suposem doncs que X és Hausdorff. Prenem dos punts diferents x i y de Y. Per la definició d'espais topològics homeomorfs (16.3.9) tenim que existeix un homeomorfisme $f\colon X \longrightarrow Y$, i per la definició d'homeomorfisme entre topologies (16.3.8) trobem que f és bijectiva. Considerem doncs els punts $f^{-1}(x)$ i $f^{-1}(y)$.

Com que, per hipòtesi, X és Hausdorff, tenim per la definició d'espai Hausdorff (18.2.1) que existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ de X tals que $f^{-1}(x)$ pertany a $\mathcal{U}$ i $f^{-1}(y)$ pertany a $\mathcal{V}$.

Ara bé, per la definició d'homeomorfisme entre topologies (16.3.8) trobem que f és una aplicació oberta, i per tant trobem que els conjunts $\mathrm{Im}_{\mathcal{U}}(f)$ i $\mathrm{Im}_{\mathcal{V}}(f)$ són oberts de Y, i tenim que x pertany a $\mathrm{Im}_{\mathcal{U}}(f)$ i y pertany a $\mathrm{Im}_{\mathcal{V}}(f)$, i per la definició d'imatge d'una aplicació (5.2.1) tenim que aquests són disjunts. □

Proposició 18.2.4. *Sigui X un espai Hausdorff. Aleshores per a tot x el conjunt $\{x\}$ és un tancat.*

Demostració. Per la definició d'espai Hausdorff (18.2.1) trobem que per a tot punt y diferent de x existeixen dos oberts disjunts $\mathcal{U}_y$ i $\mathcal{V}_y$ tals que x pertany a $\mathcal{U}_y$ i y pertany a $\mathcal{V}_y$. Aleshores tenim que

$$\begin{aligned} X \setminus \{x\} &= \bigcup_{y \in X \setminus \{x\}} \{y\} \\ &\subseteq \bigcup_{y \in X \setminus \{x\}} \mathcal{U}_y \subseteq X \setminus \{x\} \end{aligned}$$

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

$$X \setminus \{x\} = \bigcup_{y \in X \setminus \{x\}} \mathcal{U}_y.$$

Ara bé, per la definició de topologia (16.2.1) trobem que $X \setminus \{x\}$ és un obert, i per la definició de tancat (16.2.5) trobem que $\{x\}$ és un tancat. □

Proposició 18.2.5. *Sigui X un espai Hausdorff i A un subespai de X. Aleshores A és Hausdorff.*

Demostració. Siguin x i y dos elements diferents de A. Aleshores per la definició d'espai Hausdorff tenim que existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ de X tals que x pertany a $\mathcal{U}$ i y pertany a $\mathcal{V}$. Aleshores per la definició de topologia induïda per un subconjunt (17.1.2) trobem que els conjunts $\mathcal{U} \cap A$ i $\mathcal{V} \cap A$ són oberts disjunts de A que contenen x i y, respectivament, i per la definició d'espai Hausdorff (18.2.1) hem acabat. □

18.2.2 Axiomes de separació de Tychonoff

Definició 18.2.6 (Espai de Kolmogorov)**.** Sigui X un espai topològic tal que per a tots dos punts diferents x i y existeix un obert $\mathcal{U}$ que o bé conté x i no y, o bé conté y i no x. Aleshores direm que X és un espai de Kolmogorov.

Definició 18.2.7 (Espai de Fréchet)**.** Sigui X un espai topològic tal que per a tots dos punts diferents x i y existeixen dos oberts $\mathcal{U}$ i $\mathcal{V}$ tals que x pertany a $\mathcal{U} \setminus \mathcal{V}$ i y pertany a $\mathcal{V} \setminus \mathcal{U}$. Aleshores direm que X és un espai de Fréchet.

Proposició 18.2.8. *Sigui X un espai de Fréchet. Aleshores X és un espai de Kolmogorov.*

Demostració. Siguin x i y dos punts diferents de X. Aleshores per la definició d'espai de Fréchet (18.2.7) trobem que existeixen dos oberts $\mathcal{U}$ i $\mathcal{V}$ tals que x pertany a $\mathcal{U} \setminus \mathcal{V}$ i y pertany a $\mathcal{V} \setminus \mathcal{U}$. En particular x pertany a $\mathcal{U}$ i y no pertany a $\mathcal{U}$, i per la definició d'espai de Kolmogorov (18.2.6) hem acabat. □

Proposició 18.2.9. *Sigui X un espai tal que per a tot x de X, el conjunt $\{x\}$ és un tancat. Aleshores X és un espai de Fréchet.*

Demostració. Siguin x i y dos punts diferents de X. Per hipòtesi tenim que els conjunts $\{x\}$ i $\{y\}$ són tancats i per la definició de tancat (16.2.5) trobem que els conjunts $X \setminus \{x\}$ i $X \setminus \{y\}$ són oberts. Ara bé, com que per hipòtesi els punts x i y són diferents trobem que x pertany a $X \setminus \{y\}$ i y pertany a $X \setminus \{x\}$, i per la definició d'espai de Fréchet (18.2.7) trobem que X és un espai de Fréchet, com volíem veure. □

Corol·lari 18.2.10. *Sigui X un espai Hausdorff. Aleshores X és un espai de Fréchet.*

Demostració. Per la proposició 18.2.4 trobem que si x és un punt de X aleshores el conjunt $\{x\}$ és un tancat, i per la proposició 18.2.9 trobem que X és un espai de Fréchet. □

Proposició 18.2.11. *Siguin X un espai de Fréchet i x un punt de X. Aleshores $\{x\}$ és un tancat.*

Demostració. Per la definició d'espai de Fréchet (18.2.7) trobem que per a tot punt y de X diferent de x existeixen dos oberts $\mathcal{U}_y$ i $\mathcal{V}_y$ tals que x pertany a $\mathcal{U}_y \setminus \mathcal{V}_y$ i y pertany a $\mathcal{V}_y \setminus \mathcal{U}_y$. Considerem

$$\mathcal{V} = \bigcup_{y \in X \setminus \{x\}} \mathcal{V}_y. \tag{18.3}$$

Tenim que x no pertany a $\mathcal{V}$, ja que x no pertany a cap dels $\mathcal{V}_y$, i tenim que

$$\begin{aligned} X \setminus \{x\} &\subseteq \bigcup_{y \in X \setminus \{x\}} \{y\} \\ &\subseteq \bigcup_{y \in X \setminus \{x\}} \mathcal{V}_y \\ &= \mathcal{V} \subseteq X \setminus \{x\}, \end{aligned}$$

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

$$\mathcal{V} = X \setminus \{x\}.$$

Per la definició de topologia (16.2.1) i (18.3) trobem que $\mathcal{V}$ és un obert, i per la definició de tancat (16.2.5) trobem que $\{x\}$ és un tancat. □

Definició 18.2.12 (Espai regular)**.** Sigui X un espai de Fréchet tal que donats un tancat $\mathcal{C}$ i un punt x que no pertany a $\mathcal{C}$ existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que x pertany a $\mathcal{U}$ i $\mathcal{C}$ és un subconjunt de $\mathcal{V}$. Aleshores direm que X és un espai regular.

Proposició 18.2.13. *Sigui X un espai regular. Aleshores X és un espai Hausdorff.*

Demostració. Prenem dos punts diferents x i y de X. Com que, per hipòtesi, X és un espai regular, i per la definició d'espai regular (18.2.12) trobem que X és un espai de Fréchet, per la proposició 18.2.11 trobem que $\{y\}$ és un tancat, i per la definició d'espai regular (18.2.12) trobem que existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que x pertany a $\mathcal{U}$ i $\{y\}$ és un subconjunt de $\mathcal{V}$, i en particular y pertany a $\mathcal{V}$. Aleshores per la definició d'espai Hausdorff (18.2.1) hem acabat. □

Definició 18.2.14 (Espai normal)**.** Sigui X un espai de Fréchet tal que donats dos tancats disjunts $\mathcal{C}$ i $\mathcal{K}$ existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que $\mathcal{C}$ és un subconjunt de $\mathcal{U}$ i $\mathcal{K}$ és un subconjunt de $\mathcal{V}$. Aleshores direm que X és un espai normal.

Proposició 18.2.15. *Sigui X un espai normal. Aleshores X és un espai regular.*

Demostració. Siguin $\mathcal{C}$ un tancat de X i x un punt de $X \setminus \mathcal{C}$. Com que per hipòtesi X és un espai normal, per la definició d'espai normal (18.2.14) trobem que X és un espai de Fréchet, i per la proposició 18.2.11 trobem que el conjunt $\{x\}$ és un tancat, i tenim que $\{x\}$ i $\mathcal{C}$ són disjunts.

Ara bé, per la definició d'espai normal (18.2.14) trobem que existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que $\{x\}$ és un subconjunt de $\mathcal{U}$ i $\mathcal{C}$ és un subconjunt de $\mathcal{V}$. Aleshores tenim que x pertany a $\mathcal{U}$, i per la definició d'espai regular (18.2.12) trobem que X és un espai regular. □

18.2.3 Propietats dels espais Hausdorff

Proposició 18.2.16. *Sigui X un espai Hausdorff i A un compacte de X. Aleshores A és un tancat de X.*

Demostració. Si $A = X$ ó $A = \emptyset$ aleshores pel Teorema 16.2.6 trobem que A és tancat i hem acabat.

Suposem doncs que A no és X ni $\emptyset$. Tenim que existeix un punt x de $X \setminus A$. Per la definició d'espai Hausdorff (18.2.1) trobem que per a tot a de A existeixen dos oberts disjunts $\mathcal{U}_{a,x}$ i $\mathcal{V}_{a,x}$ tals que x pertany a $\mathcal{U}_{a,x}$ i a pertany a $\mathcal{V}_{a,x}$. Aleshores trobem que

$$\begin{aligned} A &= \bigcup_{a \in A} \{a\} \\ &\subseteq \bigcup_{a \in A} \mathcal{V}_{a,x}, \end{aligned}$$

i per tant trobem que

$$\bigcup_{a \in A} \mathcal{V}_{a,x} \subseteq A.$$

Aleshores per la definició de recobriment obert (18.1.2) trobem que la família $\{\mathcal{V}_{a,x}\}_{a \in A}$ és un recobriment obert de A, i com que, per hipòtesi, A és compacte trobem per la definició de subconjunt compacte (18.1.13) que existeix un subrecobriment finit $\{\mathcal{V}_{a,x}\}_{a\in A'}$ de $\{\mathcal{V}_{a,x}\}_{a\in A}$, i per la definició de subrecobriment (18.1.4) trobem que

$$\bigcup_{a\in A'} \mathcal{V}_{a,x} \subseteq A. \tag{18.4}$$

Per la definició de topologia trobem que el conjunt

$$\mathcal{U}_x = \bigcap_{a\in A'} \mathcal{U}_{a,x}$$

és un obert de X i com que, per hipòtesi, per a tot a de A tenim que

$$\mathcal{U}_{a,x} \cap \mathcal{V}_{a,x} = \emptyset$$

trobem per (18.4) que per a tot x de $X \setminus A$ es satisfà

$$A \cap \mathcal{U}_x = \emptyset,$$

i per tant

$$\bigcup_{x\in X\setminus A} \mathcal{U}_x \subseteq X \setminus A.$$

Ara bé, tenim que

$$\begin{aligned} X \setminus A &= \bigcup_{x\in X\setminus A} \{x\} \\ &\subseteq \bigcup_{x\in X\setminus A} \mathcal{U}_x \\ &\subseteq X \setminus A, \end{aligned}$$

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

$$X \setminus A = \bigcup_{x\in X\setminus A} \mathcal{U}_x.$$

Aleshores per la definició de topologia (16.2.1) trobem que $X \setminus A$ és un obert i per la definició de tancat (16.2.5) trobem que A és un tancat. □

Teorema 18.2.17. *Siguin X i Y dos espais topològics no buits. Aleshores $X \times Y$ és Hausdorff si i només si X i Y són Hausdorff.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $X \times Y$ és Hausdorff. Prenem un element y de Y. Tenim pel corol·lari 17.1.10 que $X \times \{y\} \cong X$ i tenim que $X \times \{y\} \subseteq X \times Y$. Per hipòtesi tenim que $X \times Y$ és Hausdorff. Aleshores per la proposició 18.2.5 trobem que $X \times \{y\}$ és Hausdorff i per la proposició 18.2.3 trobem que X és Hausdorff.

La demostració per veure que Y és Hausdorff és anàloga.

Veiem ara que la condició és necessària. Suposem doncs que X i Y són Hausdorff. Prenem dos punts diferents (x_1, y_1) i (x_2, y_2) de $X \times Y$. Si $y_1 = y_2$ tenim per la proposició 2.2.3 que $x_1 \neq x_2$. Com que, per hipòtesi, X és Hausdorff tenim per la definició d'espai Hausdorff (18.2.1) que existeixen dos oberts disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que x_1 pertany a $\mathcal{U}$ i x_2 pertany a $\mathcal{V}$. Aleshores per la definició de topologia producte (17.1.8) i la definició de topologia (16.2.1) trobem que els conjunts $(\mathcal{U}, Y)$ i $(\mathcal{V}, Y)$ són oberts disjunts de $X \times Y$ i per la definició d'espai Hausdorff (18.2.1) tenim que $X \times Y$ és Hausdorff.

Si $x_1 = x_2$ tenim de nou per la proposició 2.2.3 que $y_1 \neq y_2$ i l'argument per veure que $X \times Y$ és Hausdorff és anàleg. $\square$

Teorema 18.2.18. *Siguin X un espai compacte, Y un espai Hausdorff i $f\colon X \longrightarrow Y$ una aplicació contínua i bijectiva. Aleshores $X \cong Y$.*

Demostració. per la definició d'espais topològics homeomorfs (16.3.9) en tenim prou amb veure que f és un homeomorfisme, i per la definició d'homeomorfisme entre topologies (16.3.8) en tenim prou amb veure que f és una aplicació tancada. Sigui $\mathcal{C}$ un tancat de X. Com que, per hipòtesi, X és un compacte, pel Teorema 18.1.16 trobem que $\mathcal{C}$ és un compacte. Per hipòtesi tenim també que f és contínua, i pel teorema 18.1.14 trobem doncs que $\mathrm{Im}_{\mathcal{C}}(f)$ és un compacte de Y. De nou per hipòtesi tenim que Y és Hausdorff i per la proposició 18.2.16 trobem que $\mathrm{Im}_{\mathcal{C}}(f)$ és un tancat de Y. Per tant per la definició d'aplicació tancada (16.3.3) trobem que f és tancada i hem acabat. $\square$

Teorema 18.2.19. *Sigui X un espai Hausdorff compacte. Aleshores X és un espai normal.*

Demostració. Siguin $\mathcal{C}$ i $\mathcal{K}$ dos tancats disjunts i fixem un punt x de $\mathcal{C}$. Com que, per hipòtesi, X és Hausdorff, per la definició d'espai Hausdorff (18.2.1) trobem que per a tot y de $\mathcal{K}$ existeixen dos oberts disjunts $\mathcal{U}_{x,y}$ i $\mathcal{V}_{x,y}$ tals que x pertany a $\mathcal{U}_{x,y}$ i y pertany a $\mathcal{V}_{x,y}$. Tenim doncs que

$$\begin{aligned} \mathcal{K} &= \bigcup_{y \in \mathcal{K}} \{y\} \\ &\subseteq \bigcup_{y \in \mathcal{K}} \mathcal{V}_{x,y}, \end{aligned}$$

i per la definició de recobriment obert (18.1.2) trobem que la família $\{\mathcal{V}_{x,y}\}_{y \in \mathcal{K}}$ és un recobriment obert de $\mathcal{K}$. Aleshores, com que per hipòtesi X és un espai compacte, pel Teorema 18.1.16 trobem que $\mathcal{K}$ és un compacte i per la definició de subconjunt compacte (18.1.13) tenim que existeix un subrecobriment finit $\{\mathcal{V}_{x,y}\}_{y \in I_x}$ de $\{\mathcal{V}_{x,y}\}_{y \in \mathcal{K}}$. Considerem els conjunts

$$\mathcal{U}_x = \bigcap_{y \in I_x} \mathcal{U}_{x,y} \quad \text{i} \quad \mathcal{V}_x = \bigcup_{y \in I_x} \mathcal{V}_{x,y}.$$

Com que I_x és finit, per la definició de topologia (16.2.1) trobem que $\mathcal{U}_x$ i $\mathcal{V}_x$ són oberts de X i tenim que

$$\mathcal{U}_x \cap \mathcal{V}_x = \emptyset$$

i x pertany a $\mathcal{U}_x$ i y pertany a $\mathcal{V}_x$.

Ara bé, tenim que

$$\begin{aligned} \mathcal{C} &= \bigcup_{x \in \mathcal{C}} \{x\} \\ &\subseteq \bigcup_{x \in \mathcal{C}} \mathcal{U}_x, \end{aligned}$$

i per la definició de recobriment obert (18.1.2) trobem que la família $\{\mathcal{U}_x\}_{y\in\mathcal{C}}$ és un recobriment obert de $\mathcal{C}$. Aleshores, com que per hipòtesi X és un espai compacte, pel Teorema 18.1.16 trobem que $\mathcal{C}$ és un compacte i per la definició de subconjunt compacte (18.1.13) tenim que existeix un subrecobriment finit $\{\mathcal{U}_x\}_{y\in I}$ de $\{\mathcal{U}_x\}_{y\in\mathcal{X}}$. Definim

$$\mathcal{U} = \bigcap_{x\in I} \mathcal{U}_x \quad \text{i} \quad \mathcal{V} = \bigcup_{x\in I} \mathcal{V}_x.$$

Com que I és finit, per la definició de topologia (16.2.1) trobem que $\mathcal{U}$ i $\mathcal{V}$ són oberts de X i tenim que

$$\mathcal{U} \cap \mathcal{V} = \emptyset$$

i $\mathcal{C}$ és un subconjunt de $\mathcal{U}$ i $\mathcal{K}$ és un subconjunt de $\mathcal{V}$, i per la definició d'espai normal (18.2.14) hem acabat. □

Lema 18.2.20. *Siguin G un grup finit que actua sobre un espai Hausdorff compacte X i x un punt de X. Aleshores $\overline{x}$ és un tancat de X.*

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

$$\overline{y} = \{x \in X \mid x \sim y\},$$

i per la definició de quocient d'un espai per l'acció d'un grup (17.2.15) trobem que

$$\overline{y} = \{x \in X \mid \text{ existeix un } g \in G \text{ tal que } y = \theta_g(x)\}.$$

Com que per hipòtesi G és finit, trobem que $\overline{y}$ és finit. Tenim també que

$$\overline{y} = \bigcup_{x\in\overline{y}} \{x\},$$

i com que $\overline{y}$ és finit aquesta és una unió finita. Ara bé, per la proposició 18.2.4 trobem que els conjunts $\{x\}$ són tancats i pel Teorema 16.2.6 hem acabat. □

Teorema 18.2.21. *Sigui G un grup finit que actua sobre un espai Hausdorff compacte X. Aleshores X/G és un espai Hausdorff compacte.*

Demostració. Siguin x i y dos punts de X tals que $\overline{x}$ és diferent de $\overline{y}$. Pel lema 18.2.20 trobem que $\overline{y}$ és un tancat, i per la proposició 18.2.4 trobem que el conjunt $\{x\}$ és un tancat.

Per hipòtesi tenim que X és un espai Hausdorff compacte, i pel Teorema 18.2.19 trobem que X és un espai normal. Aleshores per la definició d'espai normal (18.2.14) trobem que existeixen dos oberts disjunts $\mathcal{U}'$ i $\mathcal{V}'$ tals que $\{x\}$ és un subconjunt de $\mathcal{U}'$ i $\overline{y}$ és un subconjunt de $\mathcal{V}'$.

Sigui

$$\mathcal{V} = \bigcap_{g\in G} \mathrm{Im}_{\mathcal{V}'}(\theta_g).$$

Per la definició de topologia quocient (17.2.2) trobem que $\mathrm{Im}_{\mathcal{V}'}(\theta_g)$ és un obert de X/G, i com que per hipòtesi G és finit, pel Teorema 16.2.6 trobem que $\mathcal{V}$ és un obert de X/G. També tenim per la definició de quocient d'un espai per l'acció d'un grup (17.2.15) que $\overline{y}$ és un element de $\mathcal{V}$. Per l'observacióobs:els accions de grup en un espai topològic són homeomorfismes tenim que θ_g és un homeomorfisme, i per la definició d'homeomorfisme entre topologies (16.3.8) trobem que θ_g és bijectiva. Aleshores, com que tenim que $\mathcal{U}'$ i $\mathcal{V}'$ són disjunts tenim que $\mathcal{U}'$ i $\mathcal{V}$ són disjunts. Sigui ara

$$\mathcal{U} = \bigcup_{g \in G} \mathrm{Im}_{\mathcal{U}'}(\theta_g).$$

Per la definició de topologia quocient (17.2.2) trobem que $\mathrm{Im}_{\mathcal{U}'}(\theta_g)$ és un obert de X/G, i per la definició de topologia (16.2.1) trobem que $\mathcal{U}$ és un obert de X/G. Per l'observacióobs:els accions de grup en un espai topològic són homeomorfismes tenim que θ_g és un homeomorfisme, i per la definició d'homeomorfisme entre topologies (16.3.8) trobem que θ_g és bijectiva. Aleshores, com que tenim que $\mathcal{U}'$ i $\mathcal{V}$ són disjunts tenim que $\mathcal{U}$ i $\mathcal{V}$ són disjunts.

Sigui π la projecció

$$\begin{aligned} \pi \colon X &\longrightarrow X/G \\ x &\longmapsto \overline{x}. \end{aligned}$$

Per la definició de topologia quocient (17.2.2) trobem que els conjunts $\mathrm{Im}_{\mathcal{U}}(\pi)$ i $\mathrm{Im}_{\mathcal{V}}(\pi)$ són oberts de X/G, i tenim que aquests són disjunts ja que si $\pi(z)$ pertany a la seva intersecció, per la definició de quocient d'un espai per l'acció d'un grup (17.2.15) trobem que $\overline{z}$ ha de ser un element de $\mathcal{U} \cap \mathcal{V}$, i tenim que aquests són disjunts. Per tant per la definició d'espai Hausdorff (18.2.1) tenim que X/G és Hausdorff.

Per l'observació 17.2.3 tenim que π és contínua, i pel Teorema 18.1.14 trobem que X/G és compacte i hem acabat. □

Capítol 19

Espais connexos

19.1 Connexió

19.1.1 Els espais connexos

Proposició 19.1.1. *Siguin X amb la topologia τ_1 i Y amb la topologia τ_2 dos espais topològics. Aleshores el conjunt $X \sqcup Y$ amb la topologia*

$$\tau = \{\mathcal{U} \sqcup \mathcal{V} \mid \mathcal{U} \in \tau_1 \text{ i } \mathcal{V} \in \tau_2\} \tag{19.1}$$

és un espai topològic.

Demostració. Per la definició de topologia (16.2.1) tenim que X és un obert de X i Y és un obert de Y, i per (19.1) tenim que $X \sqcup Y$ pertany a τ. Tenim també per la definició de topologia (16.2.1) que $\emptyset$ és un obert de X i Y, i tenim que $\emptyset \times \{0\} = \emptyset$ i $\emptyset \times \{1\} = \emptyset$. Per tant de nou per (19.1) tenim que $\emptyset$ pertany a τ.

Prenem ara una família $\{\mathcal{U}_i \sqcup \mathcal{V}_i\}_{i\in I}$ d'elements de τ i considerem

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i \sqcup \mathcal{V}_i.$$

Tenim que

$$\begin{aligned}
\mathcal{U} &= \bigcup_{i\in I} \mathcal{U}_i \sqcup \mathcal{V}_i \\
&= \bigcup_{i\in I} \big((\mathcal{U}_i \times \{0\}) \cup (\mathcal{V}_i \times \{1\})\big) && (5.3.11) \\
&= \left(\bigcup_{i\in I} (\mathcal{U}_i \times \{0\})\right) \cup \left(\bigcup_{i\in I} (\mathcal{V}_i \times \{1\})\right) \\
&= \left(\bigcup_{i\in I} \mathcal{U}_i \times \{0\}\right) \cup \left(\bigcup_{i\in I} \mathcal{V}_i \times \{1\}\right).
\end{aligned}$$

Per la definició de topologia (16.2.1) trobem que els conjunts

$$\bigcup_{i\in I} \mathcal{U}_i \quad \text{i} \quad \bigcup_{i\in I} \mathcal{V}_i$$

són oberts de X i Y, respectivament; i per (19.1) trobem que $\mathcal{U}$ pertany a τ.

Prenem ara una família finita $\{\mathcal{U}_i \sqcup \mathcal{V}_i\}_{i=1}^n$ d'elements de τ i considerem

$$\mathcal{U} = \bigcap_{i=1}^n \mathcal{U}_i \sqcup \mathcal{V}_i.$$

Tenim que

$$\begin{aligned}
\mathcal{U} &= \bigcap_{i=1}^n \mathcal{U}_i \sqcup \mathcal{V}_i \\
&= \bigcap_{i=1}^n \big((\mathcal{U}_i \times \{0\}) \cup (\mathcal{V}_i \times \{1\})\big) && (5.3.11) \\
&= \left(\bigcap_{i=1}^n (\mathcal{U}_i \times \{0\})\right) \cup \left(\bigcap_{i=1}^n (\mathcal{V}_i \times \{1\})\right) \\
&= \left(\bigcap_{i=1}^n \mathcal{U}_i \times \{0\}\right) \cup \left(\bigcap_{i=1}^n \mathcal{V}_i \times \{1\}\right).
\end{aligned}$$

Per la definició de topologia (16.2.1) trobem que els conjunts

$$\bigcap_{i=1}^n \mathcal{U}_i \quad \text{i} \quad \bigcap_{i=1}^n \mathcal{V}_i$$

són oberts de X i Y, respectivament; i per (19.1) trobem que $\mathcal{U}$ pertany a τ.

Per tant per la definició de topologia (16.2.1) trobem que τ és una topologia de $X \sqcup Y$, com volíem veure. □

Definició 19.1.2 (Unió disconnexa)**.** Siguin X i Y dos espais topològics. Aleshores direm que l'espai topològic $X \sqcup Y$ amb la topologia

$$\tau = \{\mathcal{U} \sqcup \mathcal{V} \mid \mathcal{U} \text{ és un obert de } X \text{ i } \mathcal{V} \text{ és un obert de } Y\}$$

és la unió disconnexa de X i Y.

Aquesta definició té sentit per la proposició 19.1.1.

Definició 19.1.3 (Espai connex)**.** Sigui X un espai topològic tal que no existeixen dos espais no buits Y_1 i Y_2 tals que $X \cong Y_1 \sqcup Y_2$. Aleshores direm que X és connex.

Proposició 19.1.4. *Sigui X un espai topològic. Aleshores són equivalents*

1. *X és connex.*
2. *No existeixen dos oberts no buits disjunts $\mathcal{U}$ i $\mathcal{V}$ tals que $X = \mathcal{U} \cup \mathcal{V}$.*
3. *No existeixen dos tancats no buits disjunts $\mathcal{C}$ i $\mathcal{K}$ tals que $X = \mathcal{C} \cup \mathcal{K}$.*
4. *Si A és un subconjunt de X tal que A és obert i tancat aleshores $A = \emptyset$ ó $A = X$.*

Demostració. □

Exemple 19.1.5. *Volem veure que un espai topològic X amb la topologia grollera. Aleshores X és connex.*

Solució. Tenim per l'exemple 16.2.3 i la definició de tancat (16.2.5) que els tancats i els oberts de X són $\emptyset$ i X. Aleshores per la proposició 19.1.4 trobem que X és connex. $\Diamond$

19.1.2 Propietats dels espais connexos

Proposició 19.1.6. *Siguin X un espai topològic i $\{\mathcal{U}_i\}_{i\in I}$ una família de subespais topològics connexos de X tals que*

$$\bigcap_{i\in I} \mathcal{U}_i \neq \emptyset.$$

Aleshores tenim que

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i$$

és un espai topològic connex.

Demostració. $\square$

Corol·lari 19.1.7. *Siguin X un espai topològic i $\{\mathcal{U}_i\}_{i\in \mathbb{N}}$ una família de subespais topològics connexos de X tals que*

$$\mathcal{U}_i \cap \mathcal{U}_{i+1} \neq \emptyset \quad \text{per a tot } i \in \mathbb{N}.$$

Aleshores tenim que

$$\mathcal{U} = \bigcup_{i\in I} \mathcal{U}_i$$

és un espai topològic connex.

Demostració. $\square$

Exemple 19.1.8. *Volem veure que un subconjunt de $\mathbb{R}$ és connex si i només si és un interval.*

Solució. $\Diamond$

Proposició 19.1.9. *Siguin A un subespai connex d'un espai topològic X i $f\colon X \longrightarrow Y$ una aplicació contínua. Aleshores $\mathrm{Im}_A(f)$ és connex.*

Demostració. $\square$

Proposició 19.1.10. *Siguin X i Y dos espais topològics. Aleshores $X \times Y$ és un espai connex si i només si X i Y són espais connexos.*

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que $X \times Y$ és un espai connex. Tenim per l'exemple 17.1.9 que les projeccions π_X i π_Y són contínues, i per la proposició 19.1.9 tenim que X i Y són connexos.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que X i Y són espais connexos i fixem un y de Y. Aleshores tenim que

$$X \times Y = \bigcup_{x \in X} ((X \times \{y\}) \cup (\{x\} \times Y))$$

i per la proposició 19.1.6 hem acabat. □

Proposició 19.1.11. *Sigui A un subespai connex d'un espai topològic X i B un conjunt tal que*

$$A \subseteq B \subseteq \mathrm{Cl}(A).$$

Aleshores B és connex.

Demostració. □

19.1.3 Connexió per camins

Definició 19.1.12 (Camí)**.** Siguin X un espai topològic i $\omega\colon [0,1] \longrightarrow X$ una aplicació contínua. Aleshores direm que ω és un camí.

També direm que $\omega(0)$ és l'origen del camí i $\omega(1)$ el final del camí.

Definició 19.1.13 (Connex per camins)**.** Sigui X un espai topològic tal que per a tots dos punts x i y de X existeix un camí ω tal que x és l'origen de ω i y és el final de ω. Aleshores direm que X és connex per camins.

Proposició 19.1.14. *Sigui X un espai topològic connex per camins. Aleshores X és connex.*

Demostració. □

Exemple 19.1.15. *Volem veure que no tots els espais connexos són connexos per camins.*

Solució. ◊

19.1.4 Components connexos d'un espai

Proposició 19.1.16. *Sigui X un espai topològic i $\sim$ una relació sobre X tal que $x \sim y$ si i només si existeix un subespai C connex de X tal que x i y pertanyen a C. Aleshores $\sim$ és una relació d'equivalència.*

Demostració. □

Definició 19.1.17 (Components connexos)**.** Siguin X un espai topològic i $\sim$ una relació sobre X tal que $x \sim y$ si i només si existeix un subespai C connex de X tal que x i y pertanyen a C. Aleshores direm que les classes d'equivalència de $\sim$ són components connexos de X.

Denotarem $\overline{x}$ com $\mathrm{C}(x)$.

Aquesta definició té sentit per la proposició 19.1.16.

Proposició 19.1.18. *Sigui x un punt d'un espai topològic X. Aleshores*

$$\mathrm{C}(x) = \bigcup_{\substack{x \in C \\ C \text{ és connex}}} C.$$

Demostració. $\square$

Proposició 19.1.19. *Sigui x un punt d'un espai topològic X. Aleshores $\mathrm{C}(x)$ és connex.*

Demostració. $\square$

Proposició 19.1.20. *Siguin x un punt d'un espai topològic X i C un connex que conté x. Aleshores C és un subconjunt de $\mathrm{C}(x)$.*

Demostració. $\square$

Proposició 19.1.21. *Siguin x i y dos punts d'un espai topològic X tals que $\mathrm{C}(x) \neq \mathrm{C}(y)$. Aleshores $\mathrm{C}(x) \cap \mathrm{C}(y) = \emptyset$.*

Demostració. $\square$

Proposició 19.1.22. *Sigui x un punt d'un espai topològic X. Aleshores $\mathrm{C}(x)$ és un tancat.*

Demostració. $\square$

Bibliografia

[1] *Apunts d'un curs de Topologia elemental*. Vers. 1.2. 2017. URL: http://mat.uab.cat/~aguade/teaching.html.

[2] *Free actions of finite groups on Hausdorff spaces*. 2011. URL: http://math.ucr.edu/~res/math205C-2011/freeactions.pdf.

[3] Czes Kosniowski. *A first course in algebraic topology*. Anglès. Cambridge University Press, 1980. ISBN: 978-0521298643.

[4] William S. Massey. *A basic course in algebraic topology*. Anglès. Springer-Verlag, 1991. ISBN: 978-3540974307.

[5] Klaus Jänich. *Topology*. Anglès. Springer, 1995. ISBN: 978-0387908922.

La majoria del contingut està escrit seguint [1], que també s'utilitza per les classes de teoria de l'assignatura. He extret la demostració d'un Teorema de [2].

La bibliografia del curs inclou els textos [3, 4, 5, 1].

Part IX

Equacions diferencials ordinàries I

Capítol 20

Equacions diferencials de primer ordre en una variable

20.1 Espai de funcions contínues i acotades

20.1.1 L'espai de funcions contínues i acotades és complet

Notació 20.1.1 (Espai de funcions contínues i acotades)**.** Siguin X amb la topologia τ un espai topològic i T un compacte de $\mathbb{R}^n$. Aleshores denotem

$$\mathcal{C}_b(X,T) = \{f(x) \mid f(x) \text{ és una funció contínua i acotada de } X \text{ a } T\}.$$

Definició 20.1.2 (Norma d'una funció)**.** Siguin X un espai vectorial amb una topologia, T un compacte de $\mathbb{R}^n$ i $f(x)$ una funció de $\mathcal{C}_b(X,T)$. Aleshores definim

$$\|f\| = \sup_{x\in X} \|f(x)\|$$

com la norma de f.

Definició 20.1.3 (Successió de Cauchy)**.** Sigui $(a_n)_{n\in\mathbb{N}}$ una successió sobre un espai normat X tal que per a tots naturals n i m existeix un real $\varepsilon > 0$ tal que

$$\|a_n - a_m\| < \varepsilon.$$

Aleshores direm que $(a_n)_{n\in\mathbb{N}}$ és de Cauchy.

Definició 20.1.4 (Espai mètric complet)**.** Siguin X amb la distància d un espai mètric tal que per a tota successió $(a_n)_{n\in\mathbb{N}}$ de Cauchy tenim que

$$a = \lim_{n\to\infty} a_n$$

és un element de X. Aleshores direm que X és complet.

Proposició 20.1.5. *Siguin f i g dues funcions de $\mathcal{C}_b(X,T)$ i*

$$\mathrm{d}(f,g) = \|f-g\|.$$

Aleshores per a tot f, g i h de $\mathcal{C}_b(X,T)$ es satisfà

1. $\mathrm{d}(f,g) \geq 0$.

2. $\mathrm{d}(f,g) = 0$ *si i només si* $f = g$.

3. $\mathrm{d}(f,g) \leq \mathrm{d}(f,h) + \mathrm{d}(h,g)$.

4. $\mathrm{d}(f,g) = \mathrm{d}(g,f)$.

Demostració. Comencem veient el punt (1). Per la definició de norma d'una funció (20.1.2) tenim que

$$\mathrm{d}(f,g) = \sup_{x\in X} \|f(x) - g(x)\|,$$

i per tant ha de ser $\mathrm{d}(f,g) \geq 0$.

Veiem ara el punt (2). Si $f = g$ aleshores tenim que per a tot x de X es satisfà $f(x) = g(x)$, i per tant trobem

$$\sup_{x\in X} \|f(x) - g(x)\| = 0,$$

i això és que $\mathrm{d}(f,g) = 0$.

Suposem ara que $\mathrm{d}(f,g) = 0$. Per la definició de norma d'una funció (20.1.2) ha de ser

$$\sup_{x\in X} \|f(x) - g(x)\| = 0,$$

i per tant trobem que $f(x) = g(x)$ per a tot x de X i per tant tenim que ha de ser $f = g$.

Veiem ara el punt (3). Tenim que

$$\begin{aligned}
\mathrm{d}(f,g) &= \sup_{x\in X} \|f(x) - g(x)\| \\
&= \sup_{x\in X} \|f(x) - h(x) + h(x) - g(x)\| \\
&\leq \sup_{x\in X} \|f(x) - h(x)\| + \sup_{x\in X} \|h(x) - g(x)\| = \mathrm{d}(f,h) + \mathrm{d}(h,g).
\end{aligned}$$

Per acabar veiem el punt (4). Tenim que

$$\begin{aligned}
\mathrm{d}(f,g) &= \sup_{x\in X} \|f(x) - g(x)\| \\
&= \sup_{x\in X} \|g(x) - f(x)\| = \mathrm{d}(g,f).
\end{aligned}$$

□

Definició 20.1.6 (Distància entre funcions)**.** Siguin X amb la topologia τ un espai topològic, T un compacte de $\mathbb{R}^n$ i f i g dues funcions de $\mathcal{C}_b(X,T)$. Aleshores definim

$$\mathrm{d}(f,g) = \|f - g\|$$

com la distància entre f i g en $\mathcal{C}_b(X,T)$.

Aquesta definició té sentit per la proposició 20.1.5.

Lema 20.1.7. *Siguin X amb la topologia τ un espai topològic i T un compacte de $\mathbb{R}^n$. Aleshores $\mathcal{C}_b(X,T)$ amb la distància* d *és espai mètric.*

Demostració. □

Notació 20.1.8. Siguin X amb la topologia τ un espai topològic i T un compacte de $\mathbb{R}^n$. Aleshores denotarem per $\mathcal{C}_b(X,T)$ l'espai mètric de amb la distància entre funcions d.

Observem que això té sentit pel lema 20.1.7.

Teorema 20.1.9. *Siguin X amb la topologia τ un espai topològic i T un compacte de $\mathbb{R}^n$. Aleshores $\mathcal{C}_b(X,T)$ és espai mètric complet.*

Demostració. Sigui $(f_n)_{n\in\mathbb{N}}$ una successió de Cauchy de $\mathcal{C}_b(X,T)$. Per la definició de successió de Cauchy (20.1.3) tenim que per a tots naturals n i m existeix un real $\varepsilon > 0$ tal que

$$\|f_n - f_m\| < \varepsilon.$$

Per la definició de distància entre funcions (20.1.6) trobem que

$$\sup_{x\in X}\|f_n(x) - f_m(x)\| < \varepsilon$$

i trobem que per a tot x de X es satisfà

$$\|f_n(x) - f_m(x)\| < \varepsilon$$

i per la definició de successió de Cauchy (20.1.3) trobem que la successió $(f_n(x))_{n\in\mathbb{N}}$ és de Cauchy, i per la definició de límit (5.2.3) trobem que la successió $(f_n(x))_{n\in\mathbb{N}}$ és convergent. Denotem, per a tot x de X,

$$\lim_{n\to\infty} f_n(x) = f(x). \tag{20.1}$$

Sigui n_0 un natural. Per la definició de límit (5.2.3) tenim que existeix un real $\varepsilon > 0$ tal que per a tot n i m enters amb $n, m \geq n_0$

$$\|f_n(x) - f_m(x)\| < \frac{\varepsilon}{2}.$$

Ara bé, per (20.1) tenim, per a tot x de X, que

$$\lim_{m\to\infty}\|f_n(x) - f_m(x)\| = \|f_n(x) - f(x)\|.$$

Per tant tenim que per a tot x de X es satisfà

$$\|f_n(x) - f(x)\| \leq \frac{\varepsilon}{2} < \varepsilon$$

i per la definició de convergència uniforme (9.2.4) tenim que $(f_n)_{n\in\mathbb{N}}$ convergeix uniformement a $f(x)$, i per la definició de espai mètric complet (20.1.4) tenim que $\mathcal{C}_b(X,T)$ és complet. □

20.1.2 Aplicacions contractives i punts fixes

Definició 20.1.10 (Aplicació contractiva)**.** Siguin X amb la distància d un espai mètric i $T\colon X \longrightarrow X$ una aplicació tal que existeixi un real $0 < k < 1$ satisfent, per a tots x i y de X,

$$\mathrm{d}(T(x), T(y)) \leq k\,\mathrm{d}(x,y).$$

Aleshores direm que T és una aplicació contractiva sobre X.

Observació 20.1.11. *Siguin X amb la distància* d *un espai mètric i T una aplicació contractiva sobre X. Aleshores T és uniformement contínua.*

Definició 20.1.12 (Punt fix)**.** Siguin X amb la distància d un espai mètric, T una aplicació contractiva sobre X i a un punt tal que $\mathrm{d}(a, T(a)) = 0$. Aleshores direm que a és un punt fix de T.

Teorema 20.1.13. *Siguin X amb la distància* d *un espai mètric complet i T una aplicació contractiva sobre X. Aleshores T té un únic punt fix.*

Demostració. Per la definició d'aplicació contractiva (20.1.10) tenim que existeix un real $0 < k < 1$ tal que per a tots x i y de X es satisfà

$$\mathrm{d}(T(x), T(y)) \leq k\,\mathrm{d}(x, y). \tag{20.2}$$

Veiem que si existeix un punt fix aquest és únic. Suposem que existeixen dos punts a i b de X tals que a i b són punts fixos de T. Aleshores tenim que

$$\mathrm{d}(a, b) = \mathrm{d}(T(a), T(b)),$$

i per (20.2) tenim que

$$\mathrm{d}(a, b) \leq k\,\mathrm{d}(a, b).$$

Ara bé, com que $0 < k < 1$, ha de ser $\mathrm{d}(a, b) = 0$, i per tant trobem que $a = b$.

Veiem ara que existeix un punt fix. Prenem un element x de X i considerem la successió $(T^n(x))_{n\in\mathbb{N}}$. Sigui r un natural. Aleshores tenim que per a tot n natural

$$\begin{aligned}
\mathrm{d}(T^{n+r}(x), T^n(x)) &\leq k\,\mathrm{d}(T^{n+r-1}(x), T^{n-1}(x)) && (20.2)\\
&\leq k^2\,\mathrm{d}(T^{n+r-2}(x), T^{n-2}(x)) && (20.2)\\
&\vdots\\
&\leq k^n\,\mathrm{d}(T^r(x), x) && (20.2)\\
&\leq k^n(\mathrm{d}(T^r(x), T^{r-1}(x)) + \mathrm{d}(T^{r-1}(x), T^{r-2}(x)) + \dots\\
&\quad \dots + \mathrm{d}(T(x), x))\\
&\leq k^n\big(k^{r-1}\,\mathrm{d}(T(x), x) + k^{r-2}\,\mathrm{d}(T(x), x) + \dots + \mathrm{d}(T(x), x)\big)\\
&= k^n(1 + k + k^2 + \dots + k^{r+1})\,\mathrm{d}(T(x), x)\\
&< \frac{k^n}{1-k}\,\mathrm{d}(T(x), x). && (9.1.3)
\end{aligned}$$

Ara bé, com que $0 < k < 1$ tenim que existeix un real $\varepsilon > 0$ tal que

$$\mathrm{d}(T^{n+r}(x), T^n(x)) < \varepsilon,$$

i per la definició de successió de Cauchy (20.1.3) tenim que la successió $(T^n(x))$ és una successió de Cauchy, i com que, per hipòtesi, X és complet, tenim que existeix un element p de X tal que

$$p = \lim_{n\to\infty} T^n(x). \tag{20.3}$$

Considerem el límit

$$\lim_{n\to\infty} T(T^n(x)).$$

Com que, per l'observació 20.1.11, T és contínua, tenim que

$$\lim_{n\to\infty} T(T^n(x)) = T\Big(\lim_{n\to\infty} T^n(x)\Big)$$

i per (20.3) trobem que

$$\lim_{n\to\infty} T(T^n(x)) = T(p).$$

Ara bé, tenim que

$$\lim_{n\to\infty} T(T^n(x)) = \lim_{n\to\infty} T^{n+1}(x)$$

i per tant trobem que

$$T(p) = p,$$

i per la definició de punt fix d'una aplicació contractiva (20.1.12) hem acabat. □

Corol·lari 20.1.14. *Siguin X amb la distància d un espai mètric complet i T una aplicació de X en X tal que existeix un natural k satisfent que T^k sigui una aplicació contractiva sobre X. Aleshores T té un únic punt fix.*

Demostració. Suposem que existeixen dos punts x i y de X tals que x i y són punts fixos de T. Aleshores per la definició de punt fix d'una aplicació contractiva (20.1.12) tenim que

$$T^k(x) = x$$

i

$$T^k(y) = y.$$

Ara bé, pel Teorema 20.1.13 tenim que ha de ser $x = y$, i per tant aquest punt és únic.

Veiem ara que existeix un punt x tal que $T(x) = x$. Tenim, per hipòtesi, que existeix un k natural tal que T^k és contractiva, i pel Teorema 20.1.13 tenim que existeix un punt x de X tal que $T^k(x) = x$. Tenim també que

$$T^{k+1}(x) = T(T^k(x)), \tag{20.4}$$

i per tant

$$T^{k+1}(x) = x \tag{20.5}$$

i amb (20.4) i (20.5), com que $T^k(x) = x$, trobem que

$$T(x) = x.$$

□

20.2 Teoremes d'existència i unicitat

20.2.1 Problema de Cauchy

Definició 20.2.1 (Equació diferencial ordinària)**.** Siguin $\Omega \subseteq \mathbb{R}\times\mathbb{R}^n$ un conjunt i $f\colon \Omega \longrightarrow \mathbb{R}^n$ una funció. Aleshores direm que l'expressió

$$\frac{\mathrm{d}u(t)}{\mathrm{d}t} = f(t, u(t))$$

és una equació diferencial ordinària sobre Ω.

Denotarem

$$\dot{u}(t) = f(t, u(t)).$$

Definició 20.2.2 (Solució d'una equació diferencial ordinària)**.** Siguin

$$\dot{u}(t) = f(t, u(t))$$

una equació diferencial ordinària sobre Ω, $I \subseteq \mathbb{R}$ un interval i $u\colon I \longrightarrow \mathbb{R}^n$ una funció tal que per a tot $t \in I$ es satisfà que $(t, u(t)) \in \Omega$ i que u és derivable en I amb $u'(t) = f(t, u(t))$. Aleshores direm que u és una solució de l'equació diferencial ordinària

$$\dot{u}(t) = f(t, u(t)).$$

Exemple 20.2.3. *Volem trobar una solució a l'equació diferencial ordinària*

$$\dot{u}(t) = u(t).$$

Solució. $\mathrm{e}^t K$. $\diamondsuit$

Definició 20.2.4 (Problema de Cauchy)**.** Sigui

$$\dot{u}(t) = f(t, u(t))$$

una equació diferencial ordinària sobre Ω i $(t_0, x_0) \in \Omega$ un punt. Aleshores direm que el sistema

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ u(t_0) = x_0 \end{cases}$$

és un problema de Cauchy sobre Ω. Direm que una solució d'aquest problema de Cauchy és una funció u tal que u és solució de l'equació diferencial

$$\dot{u}(t) = f(t, u(t))$$

i es satisfà $u(t_0) = x_0$.

Això té sentit per la definició de solució d'un equació diferencial ordinària (20.2.2).

Observació 20.2.5. *Sigui*

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ u(t_0) = x_0 \end{cases}$$

un problema de Cauchy sobre Ω*. Aleshores una funció* u *és una solució d'aquest sistema si i només si*

$$u(t) = x_0 + \int_{t_0}^{t} f(s, u(s))\mathrm{d}s.$$

20.2.2 El Teorema de Picard

Definició 20.2.6 (Funció Lipschitz respecte la segona variable)**.** Siguin $\Omega = \mathbb{R} \times \mathbb{R}^n$ un conjunt, $K \geq 0$ un real i $f\colon \Omega \longrightarrow \mathbb{R}^n$ una funció tal que

$$\|f(t, x) - f(t, y)\| \leq K\|x - y\|$$

per a tot (t, x) i (t, y) de Ω. Aleshores direm que f és Lipschitz respecte la segona variable.

Exemple 20.2.7. *Volem veure que els polinomis són funcions Lipschitz respecte la segona variable.*

Solució. $\diamondsuit$

Teorema 20.2.8 (Teorema de Picard)**.** *Siguin a i b dos reals positius,*

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ u(t_0) = x_0 \end{cases}$$

un problema de Cauchy sobre $\Omega = [t_0 - a, t_0 + a] \times \overline{\mathrm{B}}(x_0, b)$ i

$$M = \max_{(t,x)\in\Omega} \|f(t,x)\|.$$

Aleshores aquest problema de Cauchy té una única solució sobre l'interval

$$\left[t_0 - \min\left\{a, \frac{b}{M}\right\}, t_0 + \min\left\{a, \frac{b}{M}\right\}\right].$$

Demostració. Denotem $X = \mathcal{C}_b((t_0 - a, t_0 + a), \overline{\mathrm{B}}(x_0, b))$ i definim una aplicació

$$\begin{aligned} T\colon X &\longrightarrow X \\ u(t) &\longmapsto x_0 + \int_{t_0}^{t} f(s, u(s))\mathrm{d}s. \end{aligned}$$

Per l'observació 20.2.5 trobem que una funció $u(t)$ és solució del problema de Cauchy de l'enunciat si i només si

$$T(u(t)) = u(t).$$

Tenim que si u és un element de X, aleshores $T(u)$ també pertany a X, ja que si prenem un t de $(t_0 - a, t_0 + a)$ trobem que

$$\begin{aligned} \|T(u(t)) - x_0\| &= \left\| x_0 - x_0 + \int_{t_0}^{t} f(s, u(s))\mathrm{d}s \right\| \\ &= \left\| \int_{t_0}^{t} f(s, u(s))\mathrm{d}s \right\| \\ &\leq \left| \int_{t_0}^{t} \|f(s, u(s))\|\mathrm{d}s \right| && (7.1.19) \\ &\leq M|t - t_0| \leq b. \end{aligned}$$

i per tant tenim que

$$\|T(u(t)) - x_0\| \leq b.$$

Per la definició de bola (16.1.2) trobem que $T(u(t))$ és un element de $\overline{\mathrm{B}}(x_0, b)$, i per tant $T(u)$ és un element de X per a tot u de X.

Per hipòtesi tenim que f és Lipschitz respecte la segona variable, i per la definició de funció Lipschitz respecte la segona variable (20.2.6) trobem que existeix un real $K \geq 0$ tal que

$$\|f(t,x) - f(t,y)\| \leq K\|x - y\|. \tag{20.6}$$

Volem veure que per a tot m natural, u i v funcions de X i t de $(t_0 - a, t_0 + a)$ tenim
$$\|T^m(u(t)) - T^m(v(t))\| \leq \frac{K^m}{m!}|t - t_0|^m \,\mathrm{d}(u, v).$$
Ho fem per inducció. Veiem el cas $m = 1$. Tenim
$$\begin{aligned}
\|T(u(t)) - T(v(t))\| &= \left\|\int_{t_0}^{t} f(s, u(s))\mathrm{d}s - \int_{t_0}^{t} f(s, v(s))\mathrm{d}s\right\| \\
&= \left\|\int_{t_0}^{t} (f(s, u(s)) - f(s, v(s)))\mathrm{d}s\right\| && (7.1.17) \\
&\leq \left|\int_{t_0}^{t} \|f(s, u(s)) - f(s, v(s))\|\mathrm{d}s\right| && (7.1.19) \\
&\leq \left|\int_{t_0}^{t} K\|u(s) - v(s)\|\mathrm{d}s\right| && (20.6) \\
&= K\left|\int_{t_0}^{t} \|u(s) - v(s)\|\mathrm{d}s\right| && (7.1.17) \\
&\leq K|t - t_0| \,\mathrm{d}(u, v).
\end{aligned}$$

Suposem ara que l'hipòtesi és certa per a $m - 1$ fix. És a dir, suposem que
$$\left\|T^{m-1}(u(t))(t) - T^{m-1}(v)(t)\right\| \leq \frac{K^{m-1}}{(m-1)!}|t - t_0|^{m-1} \,\mathrm{d}(u, v) \tag{20.7}$$
i veiem que també és cert per m. Tenim pel Teorema 7.1.19 que
$$\begin{aligned}
\|T^m(u(t)) - T^m(v(t))\| &= \left\|\int_{t_0}^{t} \big(f(s, T^{m-1}(u(s))) - f(s, T^{m-1}(v(s)))\big)\mathrm{d}s\right\| \\
&\leq \left|\int_{t_0}^{t} \big\|f(s, T^{m-1}(u(s))) - f(s, T^{m-1}(v(s)))\big\|\mathrm{d}s\right| \\
&\leq \left|\int_{t_0}^{t} K\big\|T^{m-1}(u(s)) - T^{m-1}(v(s))\big\|\mathrm{d}s\right| && (20.6) \\
&\leq \left|\int_{t_0}^{t} \frac{K^m}{(m-1)!}|s - t_0|^{m-1} \,\mathrm{d}(u, v)\mathrm{d}s\right| && (20.7) \\
&= \frac{K^m}{(m-1)!} \,\mathrm{d}(u, v) \int_{t_0}^{t} |s - t_0|^{m-1}\mathrm{d}s && (7.1.17) \\
&= \frac{K^m}{m!}|t - t_0|^m \,\mathrm{d}(u, v).
\end{aligned}$$

Per tant, pel principi d'inducció (3.1.7) tenim que per a tot m natural, u i v funcions de X i t de $(t_0 - a, t_0 + a)$ es satisfà
$$\|T^m(u(t)) - T^m(v(t))\| \leq \frac{K^m}{m!}|t - t_0|^m \,\mathrm{d}(u, v),$$
com volíem veure.

Ara bé, tenim que
$$\lim_{m\to\infty} \frac{K^m}{m!}|t - t_0|^m = 0,$$

i per la definició de límit (5.2.3) tenim que existeix un natural n_0 tal que per a tot $n > n_0$ es satisfà
$$0 < \frac{K^m}{m!}|t - t_0|^m < 1.$$

Per tant, per la definició d'aplicació contractiva (20.1.10) tenim que per a tot $n > n_0$ l'aplicació T^n és una aplicació contractiva, i pel corol·lari 20.1.14 tenim que existeix una única funció u de X tal que

$$T(u(t)) = u(t).$$ □

Corol·lari 20.2.9. *Siguin $I \subseteq \mathbb{R}$ un interval tancat i*

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ u(t_0) = x_0. \end{cases}$$

un problema de Cauchy sobre $\Omega = I \times \mathbb{R}^n$ tal que f és una funció contínua i Lipschitz respecte la segona variable. Aleshores aquest problema de Cauchy té una única solució definida en l'interval I.

Demostració. Quan b tendeix a infinit tenim que $\overline{\mathrm{B}}(x_0, b) = \mathbb{R}^n$. □

20.2.3 El Teorema de Peano

Definició 20.2.10 (Família de funcions puntualment acotada)**.** Sigui H una família de funcions de $\mathcal{C}_b(X, T)$ tal que per a tot x de X existeix un real M_x tal que
$$\|f(x)\| < M_x$$
per a tot f de H. Aleshores direm que H és puntualment acotada.

Definició 20.2.11 (Família de funcions equicontínua)**.** Siguin H un una família de funcions de $\mathcal{C}_b(X, T)$ i x un punt de X tal que per a tot $\varepsilon > 0$ existeix un entorn N_x de x tal que per a tot y de N_x i f de H es satisfà

$$\|f(y) - f(x)\| < \varepsilon.$$

Aleshores direm que H és equicontínua en x. Si H és equicontínua en x per a tot x de X direm que H és equicontínua en X.

També, si $\mathcal{C}_b(X, T)$ té la distància d i, per a tot $\varepsilon > 0$ existeix un $\delta > 0$ tal que per a tot $y \in X$ tal que $\mathrm{d}(x, y) < \delta$, i per a tot $f \in H$ es satisfà

$$\|f(x) - f(y)\| < \varepsilon.$$

Aleshores direm que H és uniformement equicontínua en X.

Observació 20.2.12. *Sigui H una família de funcions uniformement equicontínua. Aleshores H és una família de funcions equicontínua.*

Lema 20.2.13 (Teorema d'Arzelà-Ascoli)**.** *Siguin X un compacte i $(f_n)_{n\in\mathbb{N}}$ una successió de funcions de $\mathcal{C}_b(X, T)$ equicontínua i puntualment acotada. Aleshores la successió $(f_n)_{n\in\mathbb{N}}$ té una parcial uniformement convergent.*

Demostració. Prenem un real $\varepsilon > 0$. Per la definició de família de funcions equicontínua (20.2.11) tenim que per a tot punt x de X existeix un entorn N_x de x tal que per a tot y de N_x tenim, per a tot n natural, que

$$\|f_n(y) - f_n(x)\| < \frac{\varepsilon}{3}.$$

Ara bé, per la definició d'entorn (16.2.11) tenim que existeix un obert $\mathcal{V}_x$ de X tal que x és un element de $\mathcal{V}_x$ i $\mathcal{V}_x$ és un subconjunt de N_x. Per tant tenim que per a tot y de $\mathcal{V}_x$, per a tot n natural, es satisfà

$$\|f_n(y) - f_n(x)\| < \frac{\varepsilon}{3}. \tag{20.8}$$

També tenim, per hipòtesi, que X és compacte, i per tant existeix una família $\{x_i\}_{i=1}^k$ de punts de X tals que

$$X = \bigcup_{i=1}^{k} \mathcal{V}_{x_i}. \tag{20.9}$$

Com que, per hipòtesi, la $(f_n)_{n\in\mathbb{N}}$ és una successió de funcions puntualment acotada, per la definició de família de funcions puntualment acotada (20.2.10) tenim que existeix un real M tal que per a tot n natural tenim

$$\|f_n(x_i)\| < M,$$

i tenim pel Teorema de Bolzano-Weierstrass (5.2.19) que existeix una parcial $(f_n^1(x_1))_{n\in\mathbb{N}}$ de $(f_n(x_i))_{n\in\mathbb{N}}$ convergent. Podem repetir l'argument per trobar una successió de la forma

$$(f_n^k(x_i))_{n\in\mathbb{N}} \quad \text{per a tot } i \text{ de } \{1,\dots,k\}.$$

Tenim que la successió $(f_n^k(x_i))_{n\in\mathbb{N}}$ és convergent. Per tant, per la definició de límit (5.2.3) trobem que existeix un element de X, $f^k(x_i)$ tal que existeix un natural n'_ε satisfent que per a tot $n > n'_\varepsilon$ es compleix

$$\left\|f_n^k(x_i) - f^k(x_i)\right\| < \frac{\varepsilon}{6}, \tag{20.10}$$

per tant trobem, si $m > n$ i $n > n'_\varepsilon$, que

$$\begin{aligned}\left\|f_n^k(x_i) - f_m^k(x_i)\right\| &\le \left\|f_n^k(x_i) - f^k(x_i)\right\| + \left\|f^k(x_i) - f_m^k(x_i)\right\| \\ &\le \frac{\varepsilon}{6} + \frac{\varepsilon}{6} && (20.10)\end{aligned}$$

i per tant

$$\left\|f_n^k(x_i) - f_m^k(x_i)\right\| \le \frac{\varepsilon}{3}. \tag{20.11}$$

Prenem ara un element x de X. Per (20.9) tenim que existeix un j de $\{1,\dots,k\}$ tal que x és un element de V_{x_j}, i tenim que

$$\begin{aligned}\left\|f_n^k(x) - f_m^k(x)\right\| \le& \left\|f_n^k(x) - f_n^k(x_j)\right\| + \left\|f_n^k(x_j) - f_m^k(x)\right\| \\ \le& \left\|f_n^k(x) - f_n^k(x_j)\right\| + \left\|f_n^k(x_j) - f_m^k(x_j)\right\| + \\ &+ \left\|f_m^k(x_j) - f_m^k(x)\right\| \\ \le& \frac{\varepsilon}{3} + \left\|f_n^k(x_j) - f_m^k(x_j)\right\| + \frac{\varepsilon}{3} && (20.8) \\ \le& \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon && (20.11)\end{aligned}$$

Tenim doncs que per a tot $\varepsilon > 0$ real existeix una parcial $(g^{(\varepsilon)}_{n'_\varepsilon+n})_{n\in\mathbb{N}}$ de $(f_n)_{n\in\mathbb{N}}$ que satisfà

$$\left\| g^{(\varepsilon)}_{n'_\varepsilon+n} - g^{(\varepsilon)}_{n'_\varepsilon+m} \right\| \leq \varepsilon$$

per a tot n i m enters.

Definim, per simplificar la notació, la successió

$$\left(g^{(\varepsilon)}_{n'_\varepsilon+n} \right)_{n\in\mathbb{N}} = \left(f^{(\varepsilon^{-1})}_{n'_{\varepsilon^{-1}}+n} \right)_{n\in\mathbb{N}}.$$

Per tant tenim que per a $\varepsilon = 1$ es satisfà

$$\left\| f^{(1)}_{n'_1+n}(x) - f^{(1)}_{n'_1+m}(x) \right\| \leq 1.$$

Si prenem $\varepsilon = \frac{1}{2}$ trobem una parcial $(f^2_{n_2+n})_{n\in\mathbb{N}}$ de $(f^1_{n_1+n})_{n\in\mathbb{N}}$ que satisfà

$$\left\| f^{(2)}_{n_2+n}(x) - f^{(2)}_{n_2+m}(x) \right\| \leq \frac{1}{2}.$$

Tenim doncs que per a tot i natural la successió $(f^{i+1}_{n_{i+1}+n})_{n\in\mathbb{N}}$ és una parcial de la successió $(f^{i+1}_{n_{i+1}+n})_{n\in\mathbb{N}}$ i per a tot n i m naturals tenim

$$\left\| f^{i+1}_{n_{i+1}+n}(x) - f^{i+1}_{n_{i+1}+m}(x) \right\| < \frac{1}{i},$$

i per tant, per la definició de successió de Cauchy (20.1.3) trobem que la successió $(f^{i+1}_{n_{i+1}+n})_{n\in\mathbb{N}}$ és de Cauchy per a tot i natural, i com que pel Teorema 20.1.9 tenim que $\mathcal{C}_b(X,T)$ és un espai complet, i per la condició de Cauchy per successions de funcions (9.2.8) trobem que la parcial $(f^{i+1}_{n_{i+1}+n})_{n\in\mathbb{N}}$ és uniformement convergent. □

Teorema 20.2.14 (Teorema Peano). *Siguin a i b dos reals positius i*

$$\begin{cases} \dot{u}(t) = f(t,u(t)) \\ u(t_0) = x_0 \end{cases} \tag{20.12}$$

un problema de Cauchy sobre $\Omega = [t_0 - a, t_0 + a] \times \overline{\mathrm{B}}(x_0, b)$, tal que f és una funció contínua i M un real tal que $\|f(t,x)\| < M$ per a tot (t,x) de Ω. Aleshores aquest problema de Cauchy té una solució sobre l'interval

$$\left[t_0 - \min\left\{a, \frac{b}{M}\right\}, t_0 + \min\left\{a, \frac{b}{M}\right\} \right].$$

Demostració. Per a tot $(t,x) \in \Omega$ denotem

$$f(t,x) = (f_1(t,x), \ldots, f_n(t,x)).$$

Aleshores pel Teorema d'aproximació polinòmica de Weierstrass (9.3.36) trobem que existeixen n successions de polinomis $\{(p^i_m)_{m\in\mathbb{N}}\}_{i=1}^n$ tals que (p^i_m) convergeix uniformement a f_i per a tot $i \in \{1, \ldots, n\}$. Per la proposició 9.2.7 trobem que (p^i_m) convergeix puntualment a f_i per a tot $i \in \{1, \ldots, n\}$, i per la definició de convergència puntual (9.2.2) trobem que per a tot $(t,x) \in \Omega$ tenim

$$\lim_{m\to\infty} p^i_m(t,x) = f_i(t,x),$$

i denotant $p_m(t,x) = (p_m^1(t,x), \dots, p_m^n(t,x))$ trobem que

$$\lim_{m\to\infty} p_m(t,x) = f(t,x). \tag{20.13}$$

Per la definició de límit (5.2.3) trobem que per a tot $\varepsilon > 0$ existeix un n_0 tal que per a tot $m > n_0$ es satisfà

$$\|f(t,x) - p_m(t,x)\| < \varepsilon,$$

per a tot (t,x) de Ω. Com que, per hipòtesi, tenim que $\|f(t,x)\| < M$, trobem que ha de ser $\|p_m(t,x)\| < M$ per a tot $(t,x) \in \Omega$ i per a tot $m > n_0$.

Considerem el problema de Cauchy

$$\begin{cases} \dot{u}(t) = p_m(t,u(t)) \\ u(t_0) = x_0 \end{cases}$$

sobre Ω. Com que p_m és un polinomi, per l'exemple 20.2.7 trobem que p_m és Lipschitz respecte la segona variable, i pel Teorema de Picard (20.2.8) trobem que, per a tot $m > n_0$ aquest problema de Cauchy té una única solució, φ_m, definida sobre l'interval

$$I = \left[t_0 - \min\left\{a, \frac{b}{M}\right\}, t_0 + \min\left\{a, \frac{b}{M}\right\}\right].$$

Observem que, per a tot $m > n_0$ i per a tot $t \in I$, tenim que $\varphi_m(t) \in \overline{\mathrm{B}}(x_0, b)$, i per la definició de 16.1.2 trobem que

$$\|\varphi_m(t)\| \leq \|x_0\| + b.$$

Aleshores per la definició de família de funcions puntualment acotada (20.2.10) trobem que la successió de funcions $(\varphi_{m+n_0})_{m\in\mathbb{N}}$ és una família de funcions puntualment acotada.

Fixem un $\varepsilon > 0$ i prenem dos t i t' de I amb $t' < t$ tals que $|t,t'| < \frac{\varepsilon}{M}$. Aleshores, per l'observació 20.2.5, tenim que per a tot $m > n_0$

$$\begin{aligned} \|\varphi_m(t) - \varphi_m(t')\| &= \left\| x_0 + \int_{t_0}^{t} p_m(s,\varphi_m(s))\mathrm{d}s - \left(x_0 + \int_{t_0}^{t'} p_m(s,\varphi_m(s))\mathrm{d}s\right)\right\| \\ &= \left\|\int_{t_0}^{t} p_m(s,\varphi_m(s))\mathrm{d}s - \int_{t_0}^{t'} p_m(s,\varphi_m(s))\mathrm{d}s\right\| \\ &= \left\|\int_{t'}^{t} p_m(s,\varphi_m(s))\mathrm{d}s\right\| && (7.1.18) \\ &\leq M|t'-t| < \varepsilon, && (7.1.19) \end{aligned}$$

i per la definició de família de funcions uniformement equicontínua (20.2.11) trobem que la família de funcions $\{\varphi_{m+n_0}\}_{m\in\mathbb{N}}$ és uniformement equicontínua, i per l'observació 20.2.12 trobem que $\{\varphi_{m+n_0}\}_{m\in\mathbb{N}}$ és equicontínua.

Aleshores pel Teorema d'Arzelà-Ascoli (20.2.13) trobem que existeix una parcial uniformement convergent, $(\varphi_k)_{k\in\mathbb{N}}$, de $(\varphi_{n_0+m})_{m\in\mathbb{N}}$, i per la definició de convergència uniforme (9.2.4) existeix una funció φ tal que $\varphi_k \rightrightarrows \varphi$, i per la proposició 9.2.7 trobem que la successió $(\varphi_k)_{k\in\mathbb{N}}$ convergeix puntualment a

φ, i per la definició de convergència puntual (9.2.2) trobem que per a tot $t \in I$ tenim

$$\varphi(t) = \lim_{k\to\infty} \varphi_k(t). \tag{20.14}$$

Ara bé, tenim que per a tot $t \in I$

$$\begin{aligned}
\varphi(t) &= \lim_{k\to\infty} \varphi_k(t) && (20.14)\\
&= \lim_{k\to\infty} \left(x_0 + \int_{t_0}^{t} p_k(s, \varphi_k(s))\mathrm{d}s \right) && (20.2.5)\\
&= x_0 + \lim_{k\to\infty} \int_{t_0}^{t} p_k(s, \varphi_k(s))\mathrm{d}s && (20.2.5)\\
&= x_0 + \int_{t_0}^{t} \lim_{k\to\infty} p_k(s, \varphi_k(s))\mathrm{d}s && (9.2.11)\\
&= x_0 + \int_{t_0}^{t} f(s, \varphi(s))\mathrm{d}s, && (20.13)
\end{aligned}$$

i per l'observació 20.2.5 tenim que φ és una solució del problema de Cauchy (20.12), i hem acabat. □

Corol·lari 20.2.15. *Siguin*

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ x(t_0) = x_0 \end{cases}$$

un problema de Cauchy sobre Ω *tal que* f *sigui contínua i* Ω *sigui obert, i* $K \subseteq \Omega$ *un compacte. Aleshores existeix un real* $\alpha > 0$ *tal que per a tot punt* (t_0, x_0) *de* K *aquest problema de Cauchy té una solució sobre l'interval*

$$[t_0 - \alpha, t_0 + \alpha].$$

Demostració. □

20.2.4 Solucions improrrogables

Definició 20.2.16 (Conjunt de solucions d'un problema de Cauchy)**.** Sigui

$$\begin{cases} \dot{u}(t) = f(t, u(x)) \\ u(t_0) = x_0 \end{cases} \tag{20.15}$$

un problema de Cauchy sobre Ω amb f contínua. Aleshores definirem

$$A(t_0, x_0) = \{(I, u) \mid u \text{ és solució del problema de Cauchy en l'interval } I\}$$

con el conjunt de solucions del problema de Cauchy (20.15).

Observació 20.2.17. $A(t_0, x_0) \neq \emptyset$.

Demostració. Per la definició de conjunt de solucions d'un problema de Cauchy (20.2.16) tenim que f és contínua i pel Teorema de Peano (20.2.14) hem acabat. □

Proposició 20.2.18. *Siguin $A(t_0, x_0)$ el conjunt de solucions d'un problema de Cauchy i $\leq$ una relació tal que per a dos elements (I, u) i (J, v) de $A(t_0, x_0)$ tenim*

$$(I, u) \geq (J, v)$$

si i només si

$$J \subseteq I \quad i \quad u(x) = v(x) \text{ per a tot } x \in J.$$

Aleshores la relació $\leq$ és una relació d'ordre.

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

1. Reflexiva: Pel Teorema de la doble inclusió (2.1.3) tenim que $I \subseteq I$ i per la definició d'aplicació (2.2.5) tenim que $u(x) = u(x)$ per a tot x de I. Per tant trobem $(I, u) \geq (I, u)$.

2. Antisimètrica: Suposem que $(I, u) \geq (J, v)$ i $(J, v) \geq (I, u)$. Aleshores tenim que $J \subseteq I$ i $I \subseteq J$, i pel Teorema de la doble inclusió (2.1.3) trobem que $I = J$. També tenim que $u(x) = v(x)$ per a tot x de I, i per la definició d'aplicació (2.2.5) trobem que $u = v$, i per tant $(I, u) = (J, v)$.

3. Transitiva: Siguin (I_1, u_1), (I_2, u_2) i (I_3, u_3) tres elements de $A(t_0, x_0)$ tals que $(I_1, u_1) \geq (I_2, u_2)$ i $(I_2, u_2) \geq (I_3, u_3)$. Aleshores tenim que $I_3 \subseteq I_2$ i $I_2 \subseteq I_1$, i per la definició de subconjunt (2.1.2) trobem que $I_3 \subseteq I_1$.

   També tenim que $u_1(x) = u_2(x)$ per a tot x de I_2, i $u_2(x) = u_3(x)$ per a tot x de I_3. Ara bé, com que I_3 és un subconjunt de I_1 tenim que $u_1(x) = u_2(x)$ per a tot x de I_3, i per tant $u_1(x) = u_3(x)$ per a tot x de I_3, i trobem que $(I_1, u_1) \geq (I_3, u_3)$.

I per la definició de relació d'ordre (13.3.12) hem acabat. □

Definició 20.2.19 (Prolongació)**.** Siguin $A(t_0, x_0)$ el conjunt de solucions d'un problema de Cauchy i (I, u) i (J, v) dos elements de $A(t_0, x_0)$ tals que

$$J \subseteq I \quad \text{i} \quad u(x) = v(x) \text{ per a tot } x \in J.$$

Aleshores direm que (I, u) és una prolongació de (J, v).

Si (I, u) és un element maximal direm que (I, u) és una solució improrrogable i que u és una solució maximal.

Proposició 20.2.20. *Sigui $A(t_0, x_0)$ el conjunt de solucions d'un problema de Cauchy. Aleshores existeix un element (I, u) de $A(t_0, x_0)$ tal que (I, u) és una solució improrrogable.*

Demostració. Sigui $\{I_i, u_i\}_{i \in J}$ una família de solucions del problema de Cauchy amb $(I_i, u_i) \leq (I_j, u_j)$ si $i \leq j$. Aleshores, per la definició de cadena (13.3.13), trobem que la família $\{I_i, u_i\}_{i \in J}$ és una cadena.

Considerem $I = \bigcup_{i \in J} I_i$ i definim la funció $u \colon I \longrightarrow \mathbb{R}^n$ com $u(t) = u_n(t)$ si t pertany a I_n. Veiem que u està ben definida. Prenem t_0 de I. Suposem que t_0 pertany a I_n i I_m fixats. Aleshores, com que per hipòtesi, $(I_n, u_n) \leq (I_m, u_m)$ ó $(I_m, u_m) \leq (I_n, u_n)$. Suposem que $(I_n, u_n) \leq (I_m, u_m)$. Aleshores per la definició de prolongació (20.2.19) tenim que per a tot t de I_n tenim que $u_n(t) = u_m(t)$, i per tant u està ben definida. El cas $(I_m, u_m) \leq (I_n, u_n)$ és anàleg.

Ara bé, tenim que $(I_i, u_i) \leq (I, u)$ per a tot i de J, i per la definició de cota superior d'una cadena (13.3.15) tenim que $(I_i, u_i) \leq (I, u)$ és un element maximal de la cadena $(I_i, u_i)_{i \in J}$, i pel Lema de Zorn (13.3.16) tenim que existeix un element maximal de la cadena, i per la definició de solució improrrogable (20.2.19) hem acabat. □

Proposició 20.2.21. *Sigui $A(t_0, x_0)$ el conjunt de solucions d'un problema de Cauchy i (I, u) una solució improrrogable. Aleshores I és un interval obert.*

Demostració. □

Proposició 20.2.22. *Sigui*

$$\begin{cases} \dot{u}(t) = f(t, u(t)) \\ u(t_0) = x_0 \end{cases}$$

un problema de Cauchy sobre Ω amb f contínua tal aquest tingui una única solució per a tot $(t_0, x_0) \in \Omega$. Aleshores per a cada $(t_0, x_0) \in \Omega$ aquest problema de Cauchy té una única solució improrrogable.

Demostració. Prenem un element (t_0, x_0) de Ω i siguin (I, u) i (J, v) dues solucions de $A(t_0, x_0)$ □

Teorema 20.2.23 (Lema de Wintner)**.** *Siguin $\Omega \subseteq \mathbb{R} \times \mathbb{R}^n$ un obert i $f \colon \Omega \longrightarrow \mathbb{R}^n$ una funció contínua, (φ, I) una solució de l'equació diferencial*

$$\dot{u}(t) = f(t, u(t))$$

i (b, y) un punt d'acumulació de la gràfica de φ en Ω. Aleshores

$$\lim_{t \to b} \varphi(t) = y$$

i existeix una solució (J, v) de l'equació diferencial tal que $I \subseteq J$ i $b \in J$.

Demostració. □

20.3 Dependència de les solucions d'un problema de Cauchy

Lema 20.3.1. *Sigui $(\varphi_n)_{n \in \mathbb{N}}$ una successió uniformement equicontínua i uniformement acota de funcions contínues reals sobre un espai mètric compacte F tal que tota parcial uniformement convergent de la successió té per límit una funció φ. Aleshores la successió (φ_n) convergeix uniformement a φ.*

Demostració. Suposem que la successió $(\varphi_n)_{n \in \mathbb{N}}$ no convergeix uniformement a φ. Per la definició de límit (5.2.3) tenim que existeix un $\varepsilon > 0$ tal que per a tot N natural existeix un $n_N > N$ tal que

$$\|\varphi_{n_N} - \varphi\| \geq \varepsilon.$$

Per tant podem construir una successió $(\varphi_{n_N})_{N \in \mathbb{N}}$ tal que

$$\|\varphi_{n_N} - \varphi\| \geq \varepsilon \tag{20.16}$$

per a tot N natural. Ara bé, pel Teorema d'Arzelà-Ascoli (20.2.13) la successió $(\varphi_{n_N})_{N\in\mathbb{N}}$ té una parcial uniformement convergent, que contradiu (20.16). Per tant tenim que la successió (φ_n) convergeix uniformement a φ. □

Definició 20.3.2 (Convergència uniforme sobre compactes)**.** Sigui X un espai mètric i $(f_m)_{m\in\mathbb{N}}$ una successió de funcions contínues sobre $\mathbb{R}$ tal que per a tot compacte K la successió de funcions $(f_m^K)_{m\in\mathbb{R}}$ definides com

Teorema 20.3.3 (Continuïtat respecte les condicions inicials)**.** *Siguin Ω un obert de $\mathbb{R}\times\mathbb{R}^n$, $f\colon\Omega\longrightarrow\mathbb{R}^n$ una funció contínua tal que per a cada punt (t_0,x_0) de Ω el problema de Cauchy*

$$\begin{cases}\dot{u}(t)=f(t,u(t))\\ u(t_0)=x_0\end{cases}$$

té una única solució maximal φ_{t_0,x_0} definida en un interval I_{t_0,x_0} i

$$D=\{(t,t_0,x_0)\in\mathbb{R}\times\mathbb{R}\times\mathbb{R}^n\mid(t_0,x_0)\in\Omega, t\in I_{t_0,x_0}\}.$$

Aleshores D és un obert i l'aplicació

$$\begin{aligned}\varphi\colon D&\longrightarrow\mathbb{R}\\ (t,t_0,x_0)&\longmapsto\varphi_{t_0,x_0}(t)\end{aligned}$$

és contínua.

Demostració. □

Part X

Geometria diferencial

Capítol 21

Corbes

21.1 Parametritzacions i longitud

21.1.1 Reparametrització d'una corba

Definició 21.1.1 (Corba)**.** Siguin $I \subseteq \mathbb{R}$ un interval i $\alpha\colon I \longrightarrow \mathbb{R}^n$ una funció contínua. Aleshores direm que α és una corba sobre I.

Exemple 21.1.2. *Volem veure que donats dos punts a i b de $\mathbb{R}^n$ existeix una corba contínua que els uneix.*

Solució. Observem que la funció contínua

$$\begin{aligned} \alpha\colon [0,1] &\longrightarrow \mathbb{R}^n \\ t &\longmapsto a + t(b-a) \end{aligned}$$

satisfà que $\alpha(0) = a$ i $\alpha(1) = b$, i per la definició de corba (21.1.1) trobem que és una corba contínua sobre $[0,1]$. ♢

Definició 21.1.3 (Corba regular)**.** Sigui α una corba diferenciable sobre I tal que per a tot $t \in I$ es satisfà $\alpha'(t) \neq \vec{0}$. Aleshores direm que α és regular.

Definició 21.1.4 (Reparametrització)**.** Siguin α una corba sobre I i $h\colon J \longrightarrow I$ un difeomorfisme. Aleshores direm que la funció

$$\beta(t) = (\alpha \circ h)(t)$$

és una reparametrització en J de α i que h és el canvi de paràmetre.

Proposició 21.1.5. *Sigui β una reparametrització en J d'una corba regular α sobre I. Aleshores β és una corba regular.*

Demostració. Per la definició de reparametrització d'una corba (21.1.4) trobem que existeix un canvi de paràmetre $h : J \longrightarrow I$ tal que $\beta = (\alpha \circ h)(t)$. Aleshores tenim que

$$\begin{aligned} \beta\colon J &\longrightarrow \mathbb{R}^n \\ t &\longmapsto \alpha(h(t)), \end{aligned}$$

i per la definició de corba (21.1.1) trobem que β és una corba.

Per la definició de canvi de paràmetre (21.1.4) trobem que h és un difeomorfisme, i per la definició de difeomorfisme (6.2.27) trobem que h és derivable, i per la la regla de la cadena (6.2.15) trobem que

$$\beta'(t) = h'(t)\alpha'(h(t)).$$

Com que per hipòtesi α és regular, per la definició de corba regular (21.1.3) trobem que $\alpha'(h(t)) \neq \vec{0}$ per a tot $t \in J$. Ara bé, pel corol·lari 6.3.13 trobem que $h'(t) \neq \vec{0}$ per a tot $t \in J$, i per tant tenim que $\beta'(t) \neq \vec{0}$ per a tot $t \in J$, i per la definició de corba regular (21.1.3) trobem que β és una corba regular. □

21.1.2 La longitud d'una corba i el paràmetre arc

Definició 21.1.6 (Longitud d'una corba)**.** Siguin α una corba sobre I i a, b dos punts de I. Aleshores definim

$$\mathrm{L}_a^b(\alpha) = \int_a^b \|\alpha'(t)\|\mathrm{d}t$$

com la longitud de α entre a i b.

Exemple 21.1.7. *Volem calcular la longitud de la corba*

$$\alpha(t) = (\cos(t), \sin(t), t)$$

entre 0 *i* x *per a tot* x *positiu.*

Solució. Per la definició de longitud d'una corba (21.1.6) trobem que això és

$$\begin{aligned}
\mathrm{L}_0^x(\alpha) &= \int_0^x \|\alpha'(t)\|\mathrm{d}t \\
&= \int_0^x \|(-\sin(t), \cos(t), 1)\|\mathrm{d}t \\
&= \int_0^x \sqrt{\sin^2(t) + \cos^2(t) + 1}\,\mathrm{d}t \\
&= \int_0^x \sqrt{2}\,\mathrm{d}t \\
&= [\sqrt{2}\,t]_0^x = \sqrt{2}\,x.
\end{aligned}$$

◊

Proposició 21.1.8. *Sigui β una reparametrització d'una corba α en I amb canvi de paràmetre h. Aleshores per a tot a i b de I, amb $c = h^{-1}(a)$ i $d = h^{-1}(d)$ tenim*

$$\mathrm{L}_a^b(\alpha) = \mathrm{L}_c^d(\beta).$$

Demostració. Això té sentit per la definició de canvi de paràmetre (21.1.4) i la definició de difeomorfisme (6.2.27).

Per la definició de longitud d'una corba (21.1.6) trobem que

$$\begin{aligned}
\mathrm{L}_c^d(\beta) &= \int_c^d \|\beta'(s)\|\mathrm{d}s \\
&= \int_c^d \|(\alpha \circ h)'(s)\|\mathrm{d}s, && (21.1.4)
\end{aligned}$$

i com que, per la definició de canvi de paràmetre (21.1.4) tenim que h és un difeomorfisme, per la definició de difeomorfisme (6.2.27) trobem que h és diferenciable i per la la regla de la cadena (6.2.15) trobem que

$$\int_c^d \|(\alpha \circ h)'(s)\| \mathrm{d}s = \int_c^d \|h'(s)\alpha'(h(s))\| \mathrm{d}s,$$

i per la definició de norma tenim que

$$\int_c^d \|h'(s)\alpha'(h(s))\| \mathrm{d}s = \int_c^d |h'(s)| \|\alpha'(h(s))\| \mathrm{d}s.$$

Ara bé, com que h és un difeomorfisme tenim per la definició de difeomorfisme (6.2.27) que h' és contínua, i pel corol·lari 6.3.13 trobem que $h'(t) \neq 0$ per a tot $t \in [c,d]$. Aleshores tenim que ha de ser o bé $h'(t) > 0$ per a tot $t \in [c,d]$ o bé $h'(t) < 0$ per a tot $t \in [c,d]$.

Comencem suposant que $h'(t) > 0$ per a tot $t \in [c,d]$. Aleshores tenim que

$$\int_c^d |h'(s)| \|\alpha'(h(s))\| \mathrm{d}s = \int_c^d h'(s) \|\alpha'(h(s))\| \mathrm{d}s,$$

i pel Teorema del canvi de variable tenim que

$$\begin{aligned}\int_c^d h'(s)\|\alpha'(h(s))\| \mathrm{d}s &= \int_{h(c)}^{h(d)} \|\alpha(t)\| \mathrm{d}t \\ &= \int_a^b \|\alpha(t)\| \mathrm{d}t = \mathrm{L}_a^b(\alpha),\end{aligned}$$

i per tant

$$\mathrm{L}_c^d(\beta) = \mathrm{L}_a^b(\alpha).$$

Suposem ara que $h'(t) < 0$ per a tot $t \in [c,d]$. Aleshores tenim que

$$\begin{aligned}\int_c^d |h'(s)| \|\alpha'(h(s))\| \mathrm{d}s &= \int_c^d -h'(s)\|\alpha'(h(s))\| \mathrm{d}s \\ &= \int_d^c h'(s)\|\alpha'(h(s))\| \mathrm{d}s\end{aligned}$$

i pel Teorema del canvi de variable tenim que

$$\begin{aligned}\int_d^c h'(s)\|\alpha'(h(s))\| \mathrm{d}s &= \int_{h(c)}^{h(d)} \|\alpha(t)\| \mathrm{d}t \\ &= \int_a^b \|\alpha(t)\| \mathrm{d}t = \mathrm{L}_a^b(\alpha),\end{aligned}$$

i per tant

$$\mathrm{L}_c^d(\beta) = \mathrm{L}_a^b(\alpha). \qquad \square$$

Definició 21.1.9 (Funció longitud d'arc)**.** Siguin α una corba sobre I i $a \in I$ un punt. Aleshores direm que la funció

$$\begin{aligned}\mathrm{S}_\alpha(a)(t) \colon I &\longrightarrow \mathbb{R} \\ t &\longmapsto \int_a^t \|\alpha'(s)\| \mathrm{d}s\end{aligned}$$

és la funció longitud d'arc de α amb origen en a.

Observació 21.1.10. *Sigui α una corba sobre I i $a \in I$ un punt. Aleshores per a tot $t \in I$*

$$\frac{\mathrm{d}\,\mathrm{S}_\alpha(a)}{\mathrm{d}t}(t) \geq 0.$$

Demostració. Per la definició de funció longitud d'arc (21.1.9) trobem que

$$\mathrm{S}_\alpha(a)(t) = \int_a^t \|\alpha'(s)\| \mathrm{d}s,$$

i pel Teorema Fonamental del Càlcul (5.2.18) tenim que

$$\frac{\mathrm{d}\,\mathrm{S}_\alpha(a)}{\mathrm{d}t}(t) = \|\alpha'(t)\| \geq 0. \qquad \square$$

Proposició 21.1.11. *Siguin α una corba regular sobre I i $a \in I$ un punt. Aleshores la funció $\mathrm{S}_\alpha(a)$ és un difeomorfisme.*

Demostració. Per la definició de corba regular (21.1.3) trobem que $\alpha'(t) \neq 0$ per a tot $t \in I$, i pel Teorema Fonamental del Càlcul (5.2.18) tenim que

$$\frac{\mathrm{d}\,\mathrm{S}_\alpha(a)}{\mathrm{d}t}(t) = \|\alpha'(t)\|.$$

Per tant trobem que

$$\frac{\mathrm{d}\,\mathrm{S}_\alpha(a)}{\mathrm{d}t}(t) \neq 0,$$

i per l'observació 6.2.4 i el corol·lari 6.3.13 tenim que $\mathrm{S}_\alpha(a)$ és un difeomorfisme, com volíem veure. $\square$

Proposició 21.1.12. *Sigui α una corba regular sobre I. Aleshores existeix una reparametrització β de α tal que per a tot $t \in I$*

$$\|\beta'(t)\| = 1.$$

Demostració. Per la proposició 21.1.11 tenim que per a tot $a \in I$ la funció $\mathrm{S}_\alpha(a)$ és un difeomorfisme, i per la definició de difeomorfisme (6.2.27) trobem que la funció $\mathrm{S}_\alpha(a)$ és bijectiva, i pel Teorema 2.2.19 trobem que $\mathrm{S}_\alpha(a)$ és invertible i per la definició de aplicació invertible (2.2.16) tenim que existeix una funció t_a tal que t_a sigui la inversa de $\mathrm{S}_\alpha(a)$. Considerem

$$\beta(s) = \alpha(t(s)).$$

Aleshores tenim que

$$\begin{aligned}
\|\beta'(s)\| &= \left\| \frac{\mathrm{d}t}{\mathrm{d}s} \alpha'(s) \right\| \\
&= \left| \frac{\mathrm{d}t}{\mathrm{d}s} \right| \|\alpha'(s)\| \\
&= \frac{\mathrm{d}t}{\mathrm{d}s}(s(t)) \frac{\mathrm{d}s}{\mathrm{d}t}(t(s)) \\
&= \frac{1}{\frac{\mathrm{d}s}{\mathrm{d}t}(t(s))} \frac{\mathrm{d}s}{\mathrm{d}t}(t(s)) = 1.
\end{aligned} \qquad \square$$

Definició 21.1.13 (Corba parametritzada per l'arc)**.** Sigui α una corba regular sobre I tal que per a tot $t \in I$ es satisfà

$$\|\alpha'(t)\| = 1.$$

Aleshores direm que α està parametritzada per l'arc.

Exemple 21.1.14. *Volem donar una reparametrització de la corba*

$$\alpha(t) = (R\cos(t), R\sin(t))$$

tal que estigui parametritzada per l'arc.

Solució. Tenim que

$$\alpha'(t) = (-R\sin(t), R\cos(t)),$$

i per tant

$$\begin{aligned}\|\alpha'(t)\| &= \|(-R\sin(t), R\cos(t))\| \\ &= \sqrt{(-R\sin(t))^2 + (R\cos(t))^2} \\ &= \sqrt{R^2(\sin^2(t) + \cos^2(t))} = R.\end{aligned}$$

Per la definició de funció longitud d'arc (21.1.9) trobem que

$$\begin{aligned}s(t) &= \int_0^t \|\alpha'(x)\|\mathrm{d}x \\ &= \int_0^t R\mathrm{d}x = Rt.\end{aligned}$$

Prenem ara el canvi de paràmetre

$$h(s) = \frac{s}{R}.$$

Tenim que

$$\beta(s) = (\alpha \circ h)(s) = \left(-R\sin\left(\frac{s}{R}\right), R\cos\left(\frac{s}{R}\right)\right).$$

Tenim que β és una reparametrització de α. Veiem ara que β està parametritzada per l'arc. Tenim que

$$\begin{aligned}\|\beta'(s)\| &= \|\alpha(h(s))'\| \\ &= \|h'(s)\alpha'(h(s))\| && (6.2.15) \\ &= \left\|\frac{1}{R}\left(-R\sin\left(\frac{s}{R}\right), R\cos\left(\frac{s}{R}\right)\right)\right\| \\ &= \left\|\left(-\sin\left(\frac{s}{R}\right), \cos\left(\frac{s}{R}\right)\right)\right\| \\ &= \sqrt{\sin^2\left(\frac{s}{R}\right) + \cos^2\left(\frac{s}{R}\right)} = 1,\end{aligned}$$

i per la definició de corba parametritzada per l'arc (21.1.13) hem acabat. ◊

Observació 21.1.15. *Sigui α una corba en I parametritzada per l'arc i $a \in I$ un punt. Aleshores per a tot $t \in I$ tenim*

$$\mathrm{S}_\alpha(a)(t) = t - a.$$

Demostració. Per la definició de funció longitud d'arc (21.1.9) trobem que

$$\mathrm{S}_\alpha(a)(t) = \int_a^t \|\alpha'(s)\| \mathrm{d}s,$$

i per la definició de corba parametritzada per l'arc (21.1.13) tenim que per a tot $t \in I$ es satisfà $\|\alpha'(t)\| = 1$, i per tant

$$\begin{aligned} \mathrm{S}_\alpha(a)(t) &= \int_a^t \|\alpha'(s)\| \mathrm{d}s \\ &= \int_a^t \mathrm{d}s = t - a. \end{aligned}$$

□

Definició 21.1.16 (Contacte)**.** Siguin α i β dues corbes en I parametritzades per l'arc i $t_0 \in I$ un punt tals que existeix un r satisfent

$$\lim_{t \to t_0} \frac{\alpha(t) - \beta(t)}{(t - t_0)^p} = 0 \quad \text{i} \quad \lim_{t \to t_0} \frac{\alpha(t) - \beta(t)}{(t - t_0)^{r+1}} \neq 0$$

per a tot $p \leq r$. Aleshores direm que α i β tenen contacte d'ordre r en t_0.

Proposició 21.1.17. *Siguin α i β dues corbes en I parametritzades per l'arc i $t_0 \in I$ un punt. Aleshores α i β tenen contacte d'ordre r en t_0 si i només si*

$$\alpha^{(p)}(t_0) = \beta^{(p)}(t_0) \quad i \quad \alpha^{(r+1)}(t_0) \neq \beta^{(r+1)}(t_0)$$

per a tot $p \leq r$.

Demostració. Suposem que

$$\alpha^{(p)}(t_0) = \beta^{(p)}(t_0) \quad \text{i} \quad \alpha^{(r+1)}(t_0) \neq \beta^{(r+1)}(t_0)$$

per a tot $p \leq r$. Tenim que, per a tot $p \leq r$ es satisfà

$$\alpha^{(p)}(t_0) = \beta^{(p)}(t_0),$$

o equivalentment

$$\alpha^{(p)}(t_0) - \beta^{(p)}(t_0) = 0. \tag{21.1}$$

Prenem $n \leq r$, i per la definició de derivada (5.2.7) trobem que

$$\begin{aligned} \alpha^{(n)}(t_0) - \beta^{(n)}(t_0) &= \lim_{t \to t_0} \left(\frac{\alpha^{(n-1)}(t_0) - \alpha^{(n-1)}(t)}{t - t_0} - \frac{\beta^{(n-1)}(t_0) - \beta^{(n-1)}(t)}{t - t_0} \right) \\ &= \lim_{t \to t_0} \left(\frac{\alpha^{(n-1)}(t_0) - \alpha^{(n-1)}(t) - \beta^{(n-1)}(t_0) + \beta^{(n-1)}(t)}{t - t_0} \right) \\ &= \lim_{t \to t_0} \left(\frac{\alpha^{(n-1)}(t_0) - \beta^{(n-1)}(t_0)}{t - t_0} - \frac{\alpha^{(n-1)}(t) - \beta^{(n-1)}(t)}{t - t_0} \right) \end{aligned}$$

Ara bé, tenim que $\alpha^{(n-1)}(t_0) - \beta^{(n-1)}(t_0) = 0$, i per tant

$$= \lim_{t \to t_0} \frac{\beta^{(n-1)}(t) - \alpha^{(n-1)}(t)}{t - t_0} = 0,$$

i tenim que

$$\lim_{t \to t_0} \frac{\alpha(t) - \beta(t)}{(t - t_0)^p} = 0.$$

Considerem ara

$$\alpha^{(r+1)}(t_0) \neq \beta^{(r+1)}(t_0).$$

Tenim que

$$\alpha^{(r+1)}(t_0) - \beta^{(r+1)}(t_0) \neq 0.$$

Ara bé, per la definició de derivada (5.2.7) trobem que

$$\begin{aligned}
\alpha^{(r+1)}(t_0) - \beta^{(r+1)}(t_0) &= \lim_{t \to t_0} \left(\frac{\alpha^{(r)}(t_0) - \alpha^{(r)}(t)}{t - t_0} - \frac{\beta^{(r)}(t_0) - \beta^{(r)}(t)}{t - t_0} \right) \\
&= \lim_{t \to t_0} \frac{\alpha^{(r)}(t_0) - \alpha^{(r)}(t) - \beta^{(r)}(t_0) + \beta^{(r)}(t)}{t - t_0} \\
&= \lim_{t \to t_0} \frac{\beta^{(r)}(t) - \alpha^{(r)}(t)}{t - t_0} \neq 0 \qquad (21.1)
\end{aligned}$$

i per tant

$$\lim_{t \to t_0} \frac{\alpha(t) - \beta(t)}{(t - t_0)^{r+1}} \neq 0$$

i per la definició de contacte (21.1.16) tenim que α i β tenen contacte r. □

21.2 Curvatura i torsió

21.2.1 Producte escalar i producte vectorial

Proposició 21.2.1. *Siguin α i β dues corbes diferenciables sobre I. Aleshores*

$$\frac{\mathrm{d}\langle \alpha(t), \beta(t) \rangle}{\mathrm{d}t} = \langle \alpha'(t), \beta(t) \rangle + \langle \alpha(t), \beta'(t) \rangle$$

Demostració. Tenim per la definició de derivada (5.2.7) que

$$\frac{\mathrm{d}\langle \alpha(t), \beta(t) \rangle}{\mathrm{d}t} = \lim_{h \to 0} \frac{\langle \alpha(t+h), \beta(t+h) \rangle - \langle \alpha(t), \beta(t) \rangle}{h},$$

i que

$$\alpha'(t) = \lim_{h \to 0} \frac{\alpha(t+h) - \alpha(t)}{h} \quad \text{i} \quad \beta'(t) = \lim_{h \to 0} \frac{\beta(t+h) - \beta(t)}{h}.$$

Per tant trobem que quan $h \to 0$ tenim que

$$\alpha(t+h) = \alpha(t) + h\alpha'(t) \quad \text{i} \quad \beta(t+h) = \beta(t) + h\beta'(t).$$

Per tant tenim que

$$\frac{\mathrm{d}\langle \alpha(t), \beta(t) \rangle}{\mathrm{d}t} = \lim_{h \to 0} \frac{\langle \alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t) \rangle - \langle \alpha(t), \beta(t) \rangle}{h},$$

i per la definició de producte escalar (5.1.3) trobem que

$$\begin{aligned}\langle \alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t)\rangle - \langle \alpha(t), \beta(t)\rangle &= \\ &= \langle \alpha(t), \beta(t) + h\beta'(t)\rangle + \langle h\alpha'(t), \beta(t) + h\beta'(t)\rangle - \langle \alpha(t), \beta(t)\rangle\end{aligned}$$

i

$$\begin{aligned}\langle \alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t)\rangle &= \\ &= \langle \alpha(t), \beta(t)\rangle + \langle \alpha(t), h\beta'(t)\rangle + \langle h\alpha'(t), \beta(t) + h\beta'(t)\rangle = \\ &= \langle \alpha(t), \beta(t)\rangle + \langle \alpha(t), h\beta'(t)\rangle + \langle h\alpha'(t), \beta(t)\rangle + \langle h\alpha'(t), h\beta'(t)\rangle\end{aligned}$$

i per tant

$$\begin{aligned}\langle \alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t)\rangle - \langle \alpha(t), \beta(t)\rangle &= \\ &= \langle \alpha(t), h\beta'(t)\rangle + \langle h\alpha'(t), \beta(t)\rangle + \langle h\alpha'(t), h\beta'(t)\rangle = \\ &= h\langle \alpha(t), \beta'(t)\rangle + h\langle \alpha'(t), \beta(t)\rangle + h^2\langle \alpha'(t), \beta'(t)\rangle.\end{aligned}$$

Per tant ens queda que

$$\begin{aligned}\lim_{h\to 0} \frac{\langle \alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t)\rangle - \langle \alpha(t), \beta(t)\rangle}{h} &= \\ &= \lim_{h\to 0} \frac{h\langle \alpha(t), \beta'(t)\rangle + h\langle \alpha'(t), \beta(t)\rangle + h^2\langle \alpha'(t), \beta'(t)\rangle}{h} = \\ &= \langle \alpha(t), \beta'(t)\rangle + \langle \alpha'(t), \beta(t)\rangle + \lim_{h\to 0} h\langle \alpha'(t), \beta'(t)\rangle = \\ &= \langle \alpha(t), \beta'(t)\rangle + \langle \alpha'(t), \beta(t)\rangle,\end{aligned}$$

i trobem

$$\frac{\mathrm{d}\langle \alpha(t), \beta(t)\rangle}{\mathrm{d}t} = \langle \alpha'(t), \beta(t)\rangle + \langle \alpha(t), \beta'(t)\rangle.$$ □

Proposició 21.2.2. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors de $\mathbb{R}^3$. Aleshores existeix un únic vector $\vec{w}$ de $\mathbb{R}^3$ tal que per a tot vector $\vec{x}$ de $\mathbb{R}^3$*

$$\langle \vec{w}, \vec{x}\rangle = \det(\vec{u}, \vec{v}, \vec{x}).$$

Demostració. □

Definició 21.2.3 (Producte vectorial)**.** Siguin $\vec{u}$ i $\vec{v}$ dos vectors de $\mathbb{R}^3$ i $\vec{w}$ el vector de $\mathbb{R}^3$ tal que

$$\langle \vec{w}, \vec{x}\rangle = \det(\vec{u}, \vec{v}, \vec{x}).$$

Aleshores definim el producte vectorial de $\vec{u}$ i $\vec{v}$ com

$$\vec{u} \wedge \vec{v} = \vec{w}.$$

Aquesta definició té sentit per la proposició 21.2.2.

Observació 21.2.4. $\langle \vec{u} \wedge \vec{v}, \vec{x}\rangle = \det(\vec{u}, \vec{v}, \vec{x})$.

Proposició 21.2.5. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors de $\mathbb{R}^3$. Aleshores*

$$\vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u}.$$

Demostració. Sigui $\vec{x}$ un vector de $\mathbb{R}^3$. Considerem

$$\det(\vec{u}, \vec{v}, \vec{x}).$$

Per la definició de determinant d'una matriu (4.3.1) trobem que

$$\det(\vec{u}, \vec{v}, \vec{x}) = -\det(\vec{v}, \vec{u}, \vec{x}), \tag{21.2}$$

i per l'observació 21.2.4 tenim que

$$\begin{aligned} \langle \vec{u} \wedge \vec{v}, \vec{x} \rangle &= \det(\vec{u}, \vec{v}, \vec{x}) \\ &= -\det(\vec{v}, \vec{u}, \vec{x}) && (21.2) \\ &= -\langle \vec{v} \wedge \vec{u}, \vec{x} \rangle, \end{aligned}$$

i per tant $\vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u}$, com volíem veure. □

Proposició 21.2.6. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors. Aleshores $\vec{u} \wedge \vec{v} \neq \vec{0}$ si i només si $\vec{u}$ i $\vec{v}$ són linealment independents.*

Demostració. Suposem que $\vec{u} \wedge \vec{v} = \vec{0}$. Aleshores tenim, per a tot vector $\vec{x}$ de $\mathbb{R}^3$, que

$$\langle \vec{u} \wedge \vec{v}, \vec{x} \rangle = \langle \vec{0}, \vec{x} \rangle,$$

i per la definició de producte escalar (5.1.3) trobem que

$$\langle \vec{u} \wedge \vec{v}, \vec{x} \rangle = 0.$$

Ara bé, per l'observació 21.2.4 trobem que per a tot vector $\vec{x}$ de $\mathbb{R}^3$ tenim

$$\det(\vec{u}, \vec{v}, \vec{x}) = 0,$$

i per tant tenim que $\vec{u}$ i $\vec{v}$ no són linealment independents. □

Proposició 21.2.7. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors linealment independents de $\mathbb{R}^3$. Aleshores $\vec{u} \wedge \vec{v}$ és perpendicular a $\vec{u}$ i $\vec{v}$.*

Demostració. □

Proposició 21.2.8. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors linealment independents de $\mathbb{R}^3$. Aleshores* $\det(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v}) \neq 0$.

Demostració. Per l'observació 21.2.4 tenim que

$$\langle \vec{u} \wedge \vec{v}, \vec{u} \wedge \vec{v} \rangle = \det(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v}).$$

Ara bé, com que per hipòtesi els vectors $\vec{v}$ i $\vec{u}$ són linealment independents, per la proposició 21.2.6 trobem que

$$\vec{u} \wedge \vec{v} \neq \vec{0},$$

i per la definició de producte escalar (5.1.3) trobem que

$$\langle \vec{u} \wedge \vec{v}, \vec{u} \wedge \vec{v} \rangle \neq 0.$$

Per tant tenim que

$$\det(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v}) \neq 0.$$ □

Definició 21.2.9 (Orientació d'una base)**.** Sigui $(\vec{u}, \vec{v}, \vec{w})$ una base tal que $\det(\vec{u}, \vec{v}, \vec{w}) > 0$. Aleshores direm que $(\vec{u}, \vec{v}, \vec{w})$ és una base positiva.

Proposició 21.2.10. *Siguin $\vec{u}$ i $\vec{v}$ dos vectors linealment independents. Aleshores la base $(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v})$ és una base positiva.*

Demostració. Aquest enunciat té sentit per la proposició 21.2.8.

Per l'observació 21.2.4 trobem que

$$\langle \vec{u} \wedge \vec{v}, \vec{u} \wedge \vec{v} \rangle = \det(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v}),$$

i per la definició de producte escalar (5.1.3) trobem que

$$\langle \vec{u} \wedge \vec{v}, \vec{u} \wedge \vec{v} \rangle > 0.$$

Per tant tenim que

$$\det(\vec{u}, \vec{v}, \vec{u} \wedge \vec{v}) > 0,$$

i per la definició de base positiva (21.2.9) hem acabat. □

Proposició 21.2.11 (Fórmula de Lagrange)**.** *Siguin $\vec{u}$ i $\vec{v}$ dos vectors de $\mathbb{R}^3$. Aleshores per a tots $\vec{x}$ i $\vec{y}$ de $\mathbb{R}^3$ es satisfà*

$$\langle \vec{u} \wedge \vec{v}, \vec{x} \wedge \vec{y} \rangle = \det \begin{bmatrix} \langle \vec{u}, \vec{x} \rangle & \langle \vec{v}, \vec{x} \rangle \\ \langle \vec{u}, \vec{y} \rangle & \langle \vec{v}, \vec{y} \rangle \end{bmatrix}.$$

Demostració. □

Proposició 21.2.12 (Fórmula de Leibniz)**.** *Siguin α i β dues corbes sobre I en $\mathbb{R}^3$ diferenciables en I. Aleshores*

$$\frac{\mathrm{d}(\alpha(t) \wedge \beta(t))}{\mathrm{d}t} = \frac{\mathrm{d}\alpha(t)}{\mathrm{d}t} \wedge \beta(t) + \alpha(t) \wedge \frac{\mathrm{d}\beta(t)}{\mathrm{d}t}.$$

Demostració. Per la definició de derivada (5.2.7) tenim que

$$\frac{\mathrm{d}(\alpha(t) \wedge \beta(t))}{\mathrm{d}t} = \lim_{h \to 0} \frac{\alpha(t+h) \wedge \beta(t+h) - \alpha(t) \wedge \beta(t)}{h}. \tag{21.3}$$

Per la definició de producte vectorial (21.2.3) tenim que per a tot vector $\vec{x}$ de $\mathbb{R}^3$ es satisfà

$$\langle \alpha(t+h) \wedge \beta(t+h), \vec{x} \rangle = \det(\alpha(t+h), \beta(t+h), \vec{x}).$$

De nou per la definició de derivada (5.2.7) trobem que quan $h \to 0$ es satisfà

$$\alpha(t+h) = \alpha(t) + h\alpha'(t) \quad \text{i} \quad \beta(t+h) = \beta(t) + h\beta'(t), \tag{21.4}$$

i per tant tenim que per a tot vector $\vec{x}$ de $\mathbb{R}^3$ es satisfà

$$\begin{aligned} \langle \alpha(t+h) \wedge \beta(t+h), \vec{x} \rangle &= \det(\alpha(t+h), \beta(t+h), \vec{x}) \\ &= \det(\alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t), \vec{x}) && (21.4) \end{aligned}$$

i per la definició de determinant d'una matriu (4.3.1) tenim que

$$\begin{aligned} &\det(\alpha(t) + h\alpha'(t), \beta(t) + h\beta'(t), \vec{x}) = \\ &\qquad = \det(h\alpha'(t), \beta(t) + h\beta'(t), \vec{x}) + \det(\alpha(t), \beta(t) + h\beta'(t), \vec{x}) \end{aligned}$$

i de nou per la definició de determinant d'una matriu (4.3.1) trobem que

$$\begin{aligned}\det(\alpha(t), \beta(t) + h\beta'(t), \vec{x}) + \det(h\alpha'(t), \beta(t) + h\beta'(t), \vec{x}) =\\ = \det(\alpha(t), \beta(t), \vec{x}) + \det(\alpha(t), h\beta'(t), \vec{x}) +\\ + \det(h\alpha'(t), \beta(t), \vec{x}) + \det(h\alpha'(t), h\beta'(t), \vec{x}),\end{aligned}$$

i per la definició de producte vectorial (21.2.3) això és

$$\begin{aligned}&\langle \alpha(t+h) \wedge \beta(t+h), \vec{x}\rangle =\\ &= \langle \alpha(t) \wedge \beta(t), \vec{x}\rangle + \langle \alpha(t) \wedge h\beta'(t), \vec{x}\rangle + \langle h\alpha'(t) \wedge \beta(t), \vec{x}\rangle + \langle h\alpha'(t) \wedge h\beta'(t), \vec{x}\rangle,\end{aligned}$$

i de nou per la definició de producte vectorial (21.2.3) trobem que

$$\begin{aligned}&\langle \alpha(t+h) \wedge \beta(t+h), \vec{x}\rangle =\\ &\qquad = \langle \alpha(t) \wedge \beta(t) + h\alpha(t) \wedge \beta'(t) + h\alpha'(t) \wedge \beta(t) + h^2\alpha'(t) \wedge \beta'(t), \vec{x}\rangle.\end{aligned}$$

Ara bé, ens queda que per a tot vector $\vec{x}$ de $\mathbb{R}^3$ es satisfà

$$\langle \alpha(t+h) \wedge \beta(t+h), \vec{x}\rangle = \det(\alpha(t+h), \beta(t+h), \vec{x})$$

i

$$\begin{aligned}\langle \alpha(t) \wedge \beta(t) + h\alpha(t) \wedge \beta'(t) + h\alpha'(t) \wedge \beta(t) + h^2\alpha'(t) \wedge \beta'(t), \vec{x}\rangle =\\ = \det(\alpha(t+h), \beta(t+h), \vec{x}),\end{aligned}$$

i per la proposició 21.2.2 trobem que

$$\alpha(t+h) \wedge \beta(t+h) = \alpha(t) \wedge \beta(t) + h\alpha(t) \wedge \beta'(t) + h\alpha'(t) \wedge \beta(t) + h^2\alpha'(t) \wedge \beta'(t).$$

Per tant per (21.3) tenim que

$$\begin{aligned}\frac{\mathrm{d}(\alpha(t) \wedge \beta(t))}{\mathrm{d}t} &= \lim_{h\to 0} \frac{\alpha(t+h) \wedge \beta(t+h) - \alpha(t) \wedge \beta(t)}{h}\\ &= \lim_{h\to 0} \frac{h\alpha(t) \wedge \beta'(t) + h\alpha'(t) \wedge \beta(t) + h^2\alpha'(t) \wedge \beta'(t)}{h}\\ &= \alpha(t) \wedge \beta'(t) + \alpha'(t) \wedge \beta(t) + \lim_{h\to 0} \frac{h^2\alpha'(t) \wedge \beta'(t)}{h}\\ &= \alpha(t) \wedge \beta'(t) + \alpha'(t) \wedge \beta(t),\end{aligned}$$

i trobem

$$\frac{\mathrm{d}(\alpha(t) \wedge \beta(t))}{\mathrm{d}t} = \frac{\mathrm{d}\alpha(t)}{\mathrm{d}t} \wedge \beta(t) + \alpha(t) \wedge \frac{\mathrm{d}\beta(t)}{\mathrm{d}t}.$$ □

21.2.2 Fórmules de Frenet

Proposició 21.2.13. *Sigui α una corba parametritzada per l'arc sobre I tal que α és dues vegades diferenciable en un punt t_0. Aleshores tenim que $\alpha'(t_0)$ i $\alpha''(t_0)$ són perpendiculars.*

Demostració. Per la definició de corba parametritzada per l'arc (21.1.13) trobem que
$$\|\alpha'(t)\| = 1.$$

Aleshores tenim que
$$\begin{aligned}
0 &= \frac{\mathrm{d}}{\mathrm{d}t}1 \\
&= \frac{\mathrm{d}}{\mathrm{d}t}\|\alpha'(t)\| \\
&= \frac{\mathrm{d}}{\mathrm{d}t}\|\alpha'(t)\|^2 \\
&= \frac{\mathrm{d}}{\mathrm{d}t}\langle\alpha'(t), \alpha'(t)\rangle && (5.1.4) \\
&= \langle\alpha''(t), \alpha'(t)\rangle + \langle\alpha'(t), \alpha''(t)\rangle && (21.2.1) \\
&= 2\langle\alpha'(t), \alpha''(t)\rangle.
\end{aligned}$$

Per tant trobem que
$$\langle\alpha'(t), \alpha''(t)\rangle = 0,$$

i per la definició de vectors perpendiculars (5.3.12) tenim que α' i α'' són perpendiculars, com volíem veure. □

Definició 21.2.14 (Curvatura)**.** Sigui α una corba parametritzada per l'arc sobre I i dues vegades diferenciable. Aleshores direm que l'aplicació
$$\begin{aligned}
\kappa_\alpha \colon I &\longrightarrow \mathbb{R} \\
t &\longmapsto \|\alpha''(t)\|
\end{aligned}$$

és la curvatura de α.

Si $\kappa_\alpha(t) \neq 0$ direm que α té curvatura no nul·la en t.

Exemple 21.2.15. *Volem calcular la curvatura d'una circumferència.*

Solució. Per l'exercici 21.1.14 tenim que podem parametritzar una circumferència de radi R per l'arc com
$$\alpha(t) = \left(-R\sin\left(\frac{t}{R}\right), R\cos\left(\frac{t}{R}\right)\right).$$

Aleshores tenim que
$$\alpha''(t) = \frac{\mathrm{d}}{\mathrm{d}t}\left(-\cos\left(\frac{t}{R}\right), -\sin\left(\frac{t}{R}\right)\right) = \left(\frac{1}{R}\sin\left(\frac{t}{R}\right), \frac{-1}{R}\cos\left(\frac{t}{R}\right)\right),$$

i trobem que
$$\|\alpha''(t)\| = \sqrt{\frac{1}{R^2}\sin^2\left(\frac{t}{R}\right) + \frac{1}{R^2}\cos^2\left(\frac{t}{R}\right)} = \frac{1}{R},$$

i per la definició de curvatura (21.2.14) trobem que $\kappa_\alpha(s) = \frac{1}{R}$. ♢

Proposició 21.2.16. *Sigui α una corba sobre I parametritzada per l'arc i dues vegades diferenciable. Aleshores α és una recta si i només si $\kappa(t) = 0$ per a tot $s \in I$.*

Demostració. Comencem veient que la condició és necessària ($\Longrightarrow$). Suposem doncs que α és una recta sobre $\mathbb{R}^n$. Tenim que existeixen K_1 i K_2 de $\mathbb{R}^n$ tals que

$$\alpha(t) = K_1 s + K_2.$$

Aleshores tenim que $\alpha''(t) = \vec{0}$, i per la definició de curvatura (21.2.14) trobem que $\kappa(t) = 0$.

Veiem ara que la condició és suficient ($\Longleftarrow$). Suposem doncs que $\kappa(t) = 0$ per a tot $s \in I$. Tenim doncs que $\alpha''(t) = \vec{0}$, i per tant existeixen K_1 i K_2 de $\mathbb{R}^n$ tals que $\alpha'(t) = K_1$ i $\alpha''(t) = K_1 s + K_2$ i trobem que α és una recta. $\square$

Definició 21.2.17 (Normal)**.** Sigui α una corba sobre I parametritzada per l'arc i dues vegades diferenciable i tal que $\kappa_\alpha(t) \neq 0$ per a tot $s \in I$. Aleshores direm que l'aplicació

$$\begin{aligned} \mathrm{N}_\alpha \colon I &\longrightarrow \mathbb{R} \\ t &\longmapsto \frac{\alpha''(t)}{\|\alpha''(t)\|} \end{aligned}$$

és la normal de α.

Observació 21.2.18. *Tenim que $\|\mathrm{N}_\alpha(t)\| = 1$.*

Definició 21.2.19 (Tangent)**.** Sigui α una corba sobre I parametritzada per l'arc. Aleshores direm que l'aplicació

$$\begin{aligned} \mathrm{T}_\alpha \colon I &\longrightarrow \mathbb{R} \\ t &\longmapsto \alpha'(t) \end{aligned}$$

és la tangent de α.

Observació 21.2.20. *Tenim que $\mathrm{T}'_\alpha(t) = \kappa_\alpha(t)\,\mathrm{N}_\alpha(t)$.*

Proposició 21.2.21. *Sigui α una corba sobre I amb curvatura no nul·la i $t \in I$ un real. Aleshores els vectors $\mathrm{T}_\alpha(t)$ i $\mathrm{N}_\alpha(t)$ són perpendiculars.*

Demostració. Considerem

$$\langle \mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t) \rangle.$$

Per la definició de tangent (21.2.19) i normal (21.2.17) trobem que

$$\begin{aligned} \langle \mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t) \rangle &= \left\langle \alpha'(t), \frac{\alpha''(t)}{\|\alpha''(t)\|} \right\rangle \\ &= \frac{1}{\|\alpha''(t)\|} \langle \alpha'(t), \alpha''(t) \rangle && (5.1.3) \\ &= 0. && (21.2.13) \end{aligned}$$

Aleshores per la definició de vectors perpendiculars (5.3.12) trobem que $\mathrm{T}_\alpha(t)$ i $\mathrm{N}_\alpha(t)$ són perpendiculars. $\square$

Proposició 21.2.22. *Siguin α una corba parametritzada per l'arc sobre I i $t_0 \in I$ un punt tal que $\alpha''(t_0) \neq \vec{0}$. Aleshores existeix una única circumferència β de $\mathbb{R}^3$ tal que α i β tenen contacte d'ordre 2 en $\alpha(t_0)$, que té radi $\rho_\alpha(s_0) = \frac{1}{\kappa_\alpha(t_0)}$ i és de la forma*

$$\beta(t) = Q + \rho_\alpha(t_0)\left(-N(t_0)\cos\left(\frac{t}{\rho_\alpha(t_0)}\right) + T(t_0)\sin\left(\frac{t}{\rho_\alpha(t_0)}\right)\right).$$

Demostració. □

Definició 21.2.23 (Circumferència osculadora)**.** Sigui α una corba parametritzada per l'arc sobre I i $t_0 \in I$ un punt tal que $\alpha''(t_0) \neq \vec{0}$ i $\rho_\alpha(t_0) = \frac{1}{\kappa_\alpha(t_0)}$. Aleshores direm que la circumferència

$$\beta(t) = Q + \rho_\alpha(t_0)\left(-N(t_0)\cos\left(\frac{t}{\rho_\alpha(t_0)}\right) + T(t_0)\sin\left(\frac{t}{\rho_\alpha(t_0)}\right)\right).$$

és la circumferència osculadora de α en t_0. Denotarem per $\rho_\alpha(t_0) = \frac{1}{\kappa_\alpha(t_0)}$ el radi de la circumferència osculadora.

Aquesta definició té sentit per la proposició 21.2.22.

Definició 21.2.24 (Binormal)**.** Sigui α una corba amb curvatura no nul·la. Aleshores definim

$$\mathrm{B}_\alpha(t) = \mathrm{T}_\alpha(t) \wedge \mathrm{N}_\alpha(t)$$

com la binormal de α.

Proposició 21.2.25. *Sigui α una corba sobre I amb curvatura no nul·la. Aleshores $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \mathrm{B}_\alpha(t))$ és una base ortonormal i positiva de $\mathbb{R}^3$.*

Demostració. Per la proposició 21.2.21 trobem que $\mathrm{T}_\alpha(t)$ i $\mathrm{N}_\alpha(t)$ són perpendiculars. Aleshores per la definició de binormal (21.2.24) trobem que $\mathrm{B}_\alpha(t) = \mathrm{T}_\alpha(t) \wedge \mathrm{N}_\alpha(t)$ i per la proposició 21.2.10 tenim que la base $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \mathrm{B}_\alpha(t))$ és positiva.

Per la definició de producte vectorial (21.2.3) tenim que per a tot $\vec{x}$ de $\mathbb{R}^3$ es satisfà

$$\langle \mathrm{B}_\alpha(t), \vec{x}\rangle = \det(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \vec{x}).$$

Si prenem $\vec{x}$ tal que $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \vec{x})$ sigui una base ortonormal de $\mathbb{R}^3$ trobem que

$$\det(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \vec{x}) = 1,$$

i per tant

$$\langle \mathrm{B}_\alpha(t), \vec{x}\rangle = 1,$$

i tenim que $\|\mathrm{B}_\alpha(t)\| = 1$. Aleshores per l'observació 21.2.18 i la definició de corba parametritzada per l'arc (21.1.13) tenim que $\|\mathrm{T}_\alpha(t)\| = 1$ i que $\|\mathrm{N}_\alpha(t)\| = 1$, i per tant $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \mathrm{B}_\alpha(t))$ és una base ortonormal i positiva de $\mathbb{R}^3$. □

Definició 21.2.26 (Triedre de Frenet)**.** Siguiα una corba amb curvatura no nul·la. Aleshores direm que la base $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \mathrm{B}_\alpha(t))$ és el triedre de Frenet.

Aquesta definició té sentit per la proposició 21.2.25.

Proposició 21.2.27. *Sigui α una corba parametritzada per l'arc amb curvatura no nul·la. Aleshores existeix un $\tau_\alpha(t) \in \mathbb{R}$ tal que*

$$\mathrm{B}'_\alpha(t) = \tau_\alpha(t)\,\mathrm{N}(t).$$

Demostració. Tenim per la proposició 21.2.25 que $(\mathrm{T}_\alpha(t), \mathrm{N}_\alpha(t), \mathrm{B}_\alpha(t))$ és una base ortonormal de $\mathbb{R}^3$, i per tant tenim que

$$\mathrm{B}'_\alpha(t) = \langle \mathrm{B}'_\alpha(t), \mathrm{T}_\alpha(t)\rangle\,\mathrm{T}_\alpha(t) + \langle \mathrm{B}'_\alpha(t), \mathrm{N}_\alpha(t)\rangle\,\mathrm{N}_\alpha(t) + \langle \mathrm{B}'_\alpha(t), \mathrm{B}_\alpha(t)\rangle\,\mathrm{B}_\alpha(t).$$

Tenim que $\langle \mathrm{B}_\alpha(t), \mathrm{B}_\alpha(t)\rangle = 1$, per tant trobem que

$$\frac{\mathrm{d}\langle \mathrm{B}_\alpha(t), \mathrm{B}_\alpha(t)\rangle}{\mathrm{d}t} = 0,$$

i per la proposició 21.2.12 trobem que

$$\langle \mathrm{B}'_\alpha, \mathrm{B}_\alpha\rangle + \langle \mathrm{B}_\alpha, \mathrm{B}'_\alpha\rangle = 0,$$

i per la definició de producte escalar (5.1.3) tenim que

$$2\langle \mathrm{B}'_\alpha(t), \mathrm{B}_\alpha(t)\rangle = 0,$$

i per tant

$$\langle \mathrm{B}'_\alpha(t), \mathrm{B}_\alpha(t)\rangle = 0.$$

Per la proposició 21.2.25 trobem que

$$\langle \mathrm{B}_\alpha(t), \mathrm{T}_\alpha(t)\rangle = 0,$$

i per tant

$$\frac{\mathrm{d}\langle \mathrm{B}_\alpha(t), \mathrm{T}_\alpha(t)\rangle}{\mathrm{d}t} = 0,$$

i de nou per la proposició 21.2.12 tenim que

$$\frac{\mathrm{d}\langle \mathrm{B}_\alpha(t), \mathrm{T}_\alpha(t)\rangle}{\mathrm{d}t} = \langle \mathrm{B}'_\alpha(t), \mathrm{T}_\alpha(t)\rangle + \langle \mathrm{B}_\alpha(t), \mathrm{T}'_\alpha(t)\rangle.$$

Ara bé, tenim que

$$\begin{aligned} \langle \mathrm{B}_\alpha(t), \mathrm{T}'_\alpha(t)\rangle &= \langle \mathrm{B}_\alpha(t), \kappa_\alpha(t)\,\mathrm{N}_\alpha(t)\rangle && (21.2.20) \\ &= 0, && (21.2.25) \end{aligned}$$

i per tant

$$\langle \mathrm{B}'_\alpha(t), \mathrm{T}_\alpha(t)\rangle = 0,$$

i per tant, denotant $\tau_\alpha(t) = \langle \mathrm{B}'_\alpha(t), \mathrm{N}_\alpha(t)\rangle$ trobem que

$$\mathrm{B}'_\alpha(t) = \tau_\alpha(t)\,\mathrm{N}_\alpha(t). \qquad \square$$

Definició 21.2.28 (Torsió)**.** Sigui α una corba parametritzada per l'arc amb curvatura no nul·la i $\tau_\alpha(t)$ un real tal que

$$\mathrm{B}'_\alpha(t) = \tau_\alpha(t)\,\mathrm{N}(t).$$

Aleshores direm que $\tau_\alpha(t)$ és la torsió de α.

Aquesta definició té sentit per la proposició 21.2.27.

Proposició 21.2.29 (Fórmules de Frenet)**.** *Sigui α una corba parametritzada per l'arc amb curvatura no nul·la. Aleshores*

$$\begin{bmatrix} \mathrm{T}'_\alpha(t) \\ \mathrm{N}'_\alpha(t) \\ \mathrm{B}'_\alpha(t) \end{bmatrix} = \begin{bmatrix} 0 & \kappa_\alpha(t) & 0 \\ -\kappa_\alpha(t) & 0 & -\tau_\alpha(t) \\ 0 & \tau_\alpha(t) & 0 \end{bmatrix} \begin{bmatrix} \mathrm{T}_\alpha(t) \\ \mathrm{N}_\alpha(t) \\ \mathrm{B}_\alpha(t) \end{bmatrix}.$$

Demostració. Per l'observació 21.2.20 trobem que

$$\mathrm{T}'_\alpha(t) = \kappa_\alpha(t)\,\mathrm{N}_\alpha(t), \tag{21.5}$$

i per la definició de torsió (21.2.28) trobem que

$$\mathrm{B}'_\alpha(t) = \tau_\alpha(t)\,\mathrm{N}(t). \tag{21.6}$$

Per la definició de binormal (21.2.24) trobem que

$$\mathrm{B}_\alpha(t) = \mathrm{T}_\alpha(t) \wedge \mathrm{N}_\alpha(t),$$

i per tant

$$\mathrm{N}_\alpha(t) = \mathrm{B}_\alpha(t) \wedge \mathrm{T}_\alpha(t).$$

Aleshores per la proposició 21.2.12 tenim que

$$\mathrm{N}'_\alpha(t) = \mathrm{B}'_\alpha(t) \wedge \mathrm{T}_\alpha(t) + \mathrm{B}_\alpha(t) \wedge \mathrm{T}'_\alpha(t).$$

Ara bé, per (21.5) i (21.6) trobem que

$$\begin{aligned} \mathrm{N}'_\alpha(t) &= \tau_\alpha(t)\,\mathrm{N}_\alpha(t) \wedge \mathrm{T}_\alpha(t) + \mathrm{B}_\alpha(t) \wedge \kappa_\alpha(t)\,\mathrm{N}_\alpha(t) \\ &= \tau_\alpha(t)\big(\mathrm{N}_\alpha(t) \wedge \mathrm{T}_\alpha(t)\big) + \kappa_\alpha(t)\big(\mathrm{B}_\alpha(t) \wedge \mathrm{N}_\alpha(t)\big) \\ &= \tau_\alpha(t)\,\mathrm{B}_\alpha(t) + \kappa_\alpha(t)\big(\mathrm{B}_\alpha(t) \wedge \mathrm{N}_\alpha(t)\big) && (21.2.24) \\ &= -\tau_\alpha(t)\,\mathrm{B}_\alpha(t) - \kappa_\alpha(t)\,\mathrm{T}_\alpha(t). && (21.2.24) \end{aligned}$$

Per tant ens queda

$$\begin{aligned} \mathrm{T}'_\alpha(t) &= \kappa_\alpha(t)\,\mathrm{N}_\alpha(t) \\ \mathrm{N}'_\alpha(t) &= -\tau_\alpha(t)\,\mathrm{B}_\alpha(t) - \kappa_\alpha(t)\,\mathrm{T}_\alpha(t) \\ \mathrm{B}'_\alpha(t) &= \tau_\alpha(t)\,\mathrm{N}(t) \end{aligned}$$

i per la definició de producte de matrius (4.1.5) hem acabat. □

Proposició 21.2.30. *Sigui α una corba amb curvatura no nul·la i h un canvi de paràmetre de α tal que $\tilde{\alpha} = \alpha \circ h$ estigui parametritzada per l'arc. Aleshores $\tilde{\alpha}$ té curvatura no nul·la si i només si $\alpha' \wedge \alpha'' \neq \vec{0}$.*

Demostració. Tenim que $\tilde{\alpha} = \alpha \circ h$, i per la proposició 21.2.12 i la la regla de la cadena (6.2.15) tenim que

$$\alpha' = h'(\tilde{\alpha}' \circ h)$$

i

$$\alpha'' = h''(\tilde{\alpha}' \circ h) + (h')^2(\tilde{\alpha}'' \circ h).$$

Per tant tenim que

$$\begin{aligned}\alpha' \wedge \alpha'' &= (h'(\tilde{\alpha}' \circ h)) \wedge (h''(\tilde{\alpha}' \circ h) + (h')^2(\tilde{\alpha}'' \circ h)) \\ &= (h'(\tilde{\alpha}' \circ h)) \wedge (h''(\tilde{\alpha}' \circ h)) + (h'(\tilde{\alpha}' \circ h)) \wedge ((h')^2(\tilde{\alpha}'' \circ h)) \\ &= h'h''(\tilde{\alpha}' \circ h) \wedge (\tilde{\alpha}' \circ h) + (h')^2(h'(\tilde{\alpha}' \circ h)) \wedge (\tilde{\alpha}'' \circ h) \\ &= (h')^2(\tilde{\alpha}' \circ h) \wedge (\tilde{\alpha}'' \circ h).\end{aligned}$$

Ara bé, per la definició de canvi de paràmetre (21.1.4) tenim que h és un difeomorfisme, i per la definició de difeomorfisme (6.2.27) trobem que $h \neq 0$. Tenim també que $h'' \neq 0$, i per tant trobem que

$$\alpha' \wedge \alpha'' = \vec{0} \iff (\tilde{\alpha}' \circ h) \wedge (\tilde{\alpha}'' \circ h) = \vec{0},$$

i com que, per hipòtesi, $\tilde{\alpha}$ està parametritzada per l'arc, per la definició de corba parametritzada per l'arc (21.1.13) tenim que $\tilde{\alpha}' \circ h \neq \vec{0}$, i per la proposició 21.2.13 trobem que $(\tilde{\alpha}' \circ h) \wedge (\tilde{\alpha}'' \circ h) = \vec{0}$ si i només si $\tilde{\alpha}'' = \vec{0}$, i per tant

$$\alpha' \wedge \alpha'' = \vec{0} \iff \|\tilde{\alpha}''\| = \vec{0}.$$

□

Definició 21.2.31 (Curvatura per una reparametrització)**.** Sigui α una corba amb curvatura no nul·la i $\alpha' \wedge \alpha'' = \vec{0}$ i h un canvi de paràmetre de α tal que $\tilde{\alpha} = \alpha \circ h$ estigui parametritzada per l'arc. Aleshores direm que

$$\kappa_\alpha = \kappa_{\tilde{\alpha}} \circ h^{-1}$$

és la curvatura de α.

Això té sentit per la definició de curvatura (21.2.14) i la proposició 21.2.30.

Definició 21.2.32 (Torsió per una reparametrització)**.** Sigui α una corba amb curvatura no nul·la i h un canvi de paràmetre de α tal que $\tilde{\alpha} = \alpha \circ h$ estigui parametritzada per l'arc. Aleshores direm que

$$\tau_\alpha = \tau_{\tilde{\alpha}} \circ h^{-1}$$

és la curvatura de α.

Aquesta definició té sentit per la definició de torsió (21.2.28).

Definició 21.2.33 (Rapidesa)**.** Sigui α una corba regular. Aleshores direm que

$$v_\alpha(t) = \|\alpha'(t)\|$$

és la rapidesa de α.

Proposició 21.2.34 (Fórmules de Frenet)**.** *Sigui α una corba amb curvatura no nul·la i tal que $\alpha' \wedge \alpha'' = \vec{0}$. Aleshores*

$$\begin{bmatrix} \mathrm{T}'_\alpha(t) \\ \mathrm{N}'_\alpha(t) \\ \mathrm{B}'_\alpha(t) \end{bmatrix} = v_\alpha(t) \begin{bmatrix} 0 & \kappa_\alpha(t) & 0 \\ -\kappa_\alpha(t) & 0 & -\tau_\alpha(t) \\ 0 & \tau_\alpha(t) & 0 \end{bmatrix} \begin{bmatrix} \mathrm{T}_\alpha(t) \\ \mathrm{N}_\alpha(t) \\ \mathrm{B}_\alpha(t) \end{bmatrix}.$$

Demostració. Sigui h una reparametrització de α tal que $\tilde{\alpha} = \alpha \circ h$ estigui parametritzada per l'arc.

Ai haig de tornar a definir les coses aquestes per corbes no parametritzades per l'arc. Quina mandra. Imagineu una demostració patrocinada per la regla de la cadena (6.2.15) i les fórmules de Frenet (21.2.29). Us prometo que tot quadra, com volíem veure. □

21.2.3 Teorema Fonamental de la teoria local de corbes

Exemple 21.2.35 (Grup ortogonal)**.** *Volem veure que el conjunt*

$$\mathrm{O}(n) = \{A \in M_n(\mathbb{R}) \mid \textit{per a tot } \vec{u}, \vec{v} \in M_{n\times 1}(\mathbb{R}) \textit{ tenim } \langle A\vec{u}, A\vec{v}\rangle = \langle \vec{u}, \vec{v}\rangle\}$$

amb el producte de matrius és un grup.

Solució. ♢

Exemple 21.2.36 (Grup especial ortogonal)**.** *Volem veure que*

$$\mathrm{SO}(n) = \{A \in \mathrm{O} \mid \det(A) = 1\}$$

és un subgrup de $\mathrm{O}(n)$*.*

Solució. ♢

Proposició 21.2.37. *Sigui $A \in \mathrm{O}(n)$ una matriu. Aleshores els valors propis reals de A són -1 ó 1.*

Demostració. □

Proposició 21.2.38. *Es satisfà*

$$\mathrm{SO}(2) = \left\{ \begin{bmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{bmatrix} \mid t \in \mathbb{R} \right\}$$

i

$$\mathrm{O}(2) \setminus \mathrm{SO}(2) = \left\{ \begin{bmatrix} \cos(t) & \sin(t) \\ \sin(t) & -\cos(t) \end{bmatrix} \mid t \in \mathbb{R} \right\}.$$

Demostració. □

Proposició 21.2.39. *Sigui $A \in \mathrm{SO}(3)$ una matriu. Aleshores existeixen una base ortonormal $\mathcal{B}$ de $\mathbb{R}^3$ i un $t \in \mathbb{R}$ tals que*

$$M(\mathcal{B}, \mathcal{C})AM(\mathcal{C}, \mathcal{B}) = \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & \cos(t) & \sin(t) \\ 0 & \sin(t) & -\cos(t) \end{bmatrix}.$$

Demostració. □

Proposició 21.2.40. *Sigui $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ una aplicació conserva distàncies. Aleshores existeixen una matriu $A \in \mathrm{O}(n)$ i un $\vec{C} \in \mathbb{R}^n$ tals que*

$$f(\vec{v}) = A\vec{v} + \vec{C}.$$

Demostració. □

Proposició 21.2.41. *Siguin α una corba regular i $A \in M_n$ una matriu. Aleshores*

$$\frac{\mathrm{d}(A\alpha(t))}{\mathrm{d}t} = A\alpha'(t).$$

Demostració. □

Proposició 21.2.42. *Siguin $A \in \mathrm{SO}(n)$ una matriu i $\vec{u}$, $\vec{v}$ dos vectors de $\mathbb{R}^n$. Aleshores*
$$A(\vec{u} \wedge \vec{v}) = (A\vec{u}) \wedge (A\vec{v}).$$

Demostració. □

Corol·lari 21.2.43. *Siguin α una corba parametritzada per l'arc, $A \in \mathrm{SO}(3)$ una matriu, $\vec{C}$ un vector de $\mathbb{R}^3$ i β una corba tal que*

$$\beta(t) = A\alpha(t) + \vec{C}.$$

Aleshores $\beta(t)$ està parametritzada per l'arc i es satisfà

$$\mathrm{T}_\beta = A\,\mathrm{T}_\alpha, \quad \mathrm{N}_\beta = A\,\mathrm{N}_\alpha, \quad \mathrm{B}_\beta = A\,\mathrm{B}_\alpha, \quad \kappa_\beta = A\,\kappa_\alpha \quad i \quad \tau_\beta = A\,\tau_\alpha\,.$$

Demostració. □

Lema 21.2.44. *Siguin α i β dues corbes. Aleshores la relació*

$$\alpha \sim \beta \iff \textit{Existeixen } A \in \mathrm{SO}(3) \textit{ i } \vec{C} \in \mathbb{R}^3 \textit{ tals que } \alpha = A\beta + \vec{C}$$

és una relació d'equivalència.

Demostració. □

Teorema 21.2.45 (Teorema Fonamental de la teoria local de corbes)**.** *Siguin $\kappa(t)$ i $\tau(t)$ dues funcions diferenciables sobre I, amb $\kappa(t) > 0$ per a tot $t \in I$. Aleshores existeix una única corba α sobre I parametritzada per l'arc satisfent $\kappa_\alpha(t) = \kappa(t)$ i $\tau_\alpha(t) = \tau(t)$, llevat d'equivalència.*

Demostració. □

Capítol 22

Superfícies

22.1 Superfícies regulars

22.1.1 Immersions i submersions

Definició 22.1.1 (Immersió)**.** Siguin $n \leq m$ dos naturals, $\mathcal{U} \subseteq \mathbb{R}^n$ un obert, $x_0 \in \mathcal{U}$ un punt i $f\colon \mathcal{U} \longrightarrow \mathbb{R}^m$ una funció diferenciable tal que $df(a)$ sigui injectiva. Aleshores direm que f és una immersió en x_0.

Observació 22.1.2. *f és una immersió en x_0 si i només si* $\operatorname{rang}(df(a)) = n$.

Exemple 22.1.3. *Volem veure que la inclusió canònica és una immersió.*

Solució. La inclusió canònica ve definida com

$$\begin{aligned} i\colon \mathbb{R}^p &\longrightarrow \mathbb{R}^{p+q} \\ x &\longmapsto (x;0), \end{aligned} \tag{6.3.16}$$

i per la definició de matriu Jacobiana (6.2.12) tenim que la seva diferencial és

$$\left[\begin{array}{c} I_p \\ \hline 0_{q\times(p-q)} \end{array}\right].$$

Aleshores per la definició de rang d'una matriu (4.2.11) trobem que aquesta té rang p, i per l'observació 22.1.2 tenim que i és una immersió. $\lozenge$

Definició 22.1.4 (Submersió)**.** Siguin $n \geq m$ dos naturals, $\mathcal{U} \subseteq \mathbb{R}^n$ un obert, $x_0 \in \mathcal{U}$ un punt i $f\colon \mathcal{U} \longrightarrow \mathbb{R}^m$ una funció diferenciable tal que $df(a)$ sigui exhaustiva. Aleshores direm que f és una submersió en x_0.

Observació 22.1.5. *f és una submersió en x_0 si i només si* $\operatorname{rang}(df(a)) = m$.

Exemple 22.1.6. *Volem veure que la projecció canònica és una submersió.*

Solució. La projecció canònica ve definida com

$$\begin{aligned} \pi\colon \mathbb{R}^{p+q} &\longrightarrow \mathbb{R}^p \\ (x;y) &\longmapsto x, \end{aligned} \tag{6.3.16}$$

i per la definició de matriu Jacobiana (6.2.12) trobem que la seva diferencial és

$$\left[\begin{array}{c|c} I_p & 0_{p\times(p+q)} \end{array}\right].$$

Aleshores per la definició de rang d'una matriu (4.2.11) trobem que aquesta té rang p i per l'observació 22.1.5 tenim que π és una submersió. $\Diamond$

Proposició 22.1.7. *Siguin $\mathcal{U} \subseteq \mathbb{R}^n$ i $\mathcal{V} \subseteq \mathbb{R}^m$ dos oberts, $g\colon \mathcal{U} \longrightarrow \mathcal{V}$ i $f\colon \mathcal{V} \longrightarrow \mathbb{R}^d$ dues submersions. Aleshores la funció $f \circ g$ és una submersió.*

Demostració. Per la la regla de la cadena (6.2.15) tenim que

$$d(f \circ g) = dgdf(g),$$

i per tant trobem que $\operatorname{rang}(d(f \circ g)) \leq \min\{\operatorname{rang}(dg), \operatorname{rang}(df(g))\}$, i per l'observació 22.1.5 hem acabat. $\square$

Teorema 22.1.8 (Teorema d'estructura local de les immersions)**.** *Siguin $\mathcal{U} \subseteq \mathbb{R}^n$ un obert i $f\colon \mathcal{U} \longrightarrow \mathbb{R}^m$ una immersió en un punt $x_0 \in \mathcal{U}$. Aleshores existeixen dos oberts $\mathcal{U}' \subseteq \mathbb{R}^n$ i $\mathcal{V} \subseteq \mathbb{R}^m$ satisfent $x_0 \subseteq \mathcal{U}' \subseteq \mathcal{U}$ i existeix un difeomorfisme $g\colon \mathcal{V} \longleftrightarrow \operatorname{Im}_{\mathcal{U}'}(g) \subseteq \mathbb{R}^n$ i satisfent $i(x_0) \in \mathcal{V}$ tals que el diagrama*

$$\begin{tikzcd} \mathcal{U}' \arrow[r, "i"] \arrow[dr, "f"'] & \mathcal{V} \arrow[d, "g"] \\ & \mathbb{R}^m \end{tikzcd}$$

és un diagrama commutatiu.

Demostració. Denotem

$$f(x) = (f_1(x), \ldots, f_m(x)).$$

Per la definició de immersió (22.1.1) trobem que $n \leq m$ i per l'observació 22.1.2 trobem que

$$\operatorname{rang}\left(\frac{\partial f_i}{\partial x_j}(x_0)\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} = n.$$

Aleshores tenim que existeix una permutació $\sigma \in \mathrm{S}_n$ tal que

$$\operatorname{rang}\left(\frac{\partial f_i}{\partial x_{\sigma(j)}}(x_0)\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} = n,$$

i per la proposició 5.1.6 trobem que

$$\det\left(\frac{\partial f_i}{\partial x_{\sigma(j)}}(x_0)\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \neq 0.$$

Denotem doncs

$$F(x) = (f_{\sigma(1)}(x), \ldots, f_{\sigma(m)}(x))$$

i tenim que

$$\det(dF(x_0)) \neq 0. \tag{22.1}$$

Considerem la funció

$$\begin{aligned} g\colon \mathbb{R}^n \times \mathbb{R}^{m-n} &\longrightarrow \mathbb{R}^m \\ (x,y) &\longmapsto F(x) + (0,y). \end{aligned}$$

Tenim que $g(x,0) = F(x)$, i per l'exemple 22.1.3 trobem que

$$(g \circ i)(x) = g(x,0) = F(x).$$

Per la definició de matriu Jacobiana (6.2.12) i la proposició 6.2.13 tenim que

$$dg(x_0) = \left[\begin{array}{ccc|c} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} & \\ \vdots & & \vdots & 0_{n\times(m-n)} \\ \frac{\partial F_n}{\partial x_1} & \cdots & \frac{\partial F_n}{\partial x_n} & \\ \hline \frac{\partial F_{n+1}}{\partial x_1} & \cdots & \frac{\partial F_{n+1}}{\partial x_n} & \\ \vdots & & \vdots & I_{(m-n)\times(m-n)} \\ \frac{\partial F_m}{\partial x_1} & \cdots & \frac{\partial F_m}{\partial x_n} & \end{array}\right].$$

Aleshores tenim que

$$\det(dg(x_0)) = \det(dF(x_0)),$$

i per (22.1) trobem que

$$\det(dg(x_0)) \neq 0,$$

i pel Teorema de la funció inversa (6.3.12) hem acabat. $\square$

Teorema 22.1.9 (Teorema d'estructura local de les submersions)**.** *Siguin $\mathcal{U} \subseteq \mathbb{R}^n$ un obert i $f\colon \mathcal{U} \longrightarrow \mathbb{R}^m$ una submersions en un punt $x_0 \in \mathcal{U}$. Aleshores existeix un obert $\mathcal{U}'$ satisfent $x_0 \subseteq \mathcal{U}' \subseteq \mathcal{U}$ i existeix un difeomorfisme $g\colon \mathcal{U}' \longleftrightarrow \operatorname{Im}_{\mathcal{U}'}(g) \subseteq \mathbb{R}^n$ tals que el diagrama*

$$\begin{tikzcd} \mathcal{U}' \arrow[r, "g"] \arrow[dr, "f"'] & \operatorname{Im}_{\mathcal{U}'}(g) \arrow[d, "\pi"] \\ & \mathbb{R}^m \end{tikzcd}$$

és un diagrama commutatiu.

Demostració. Denotem

$$f(x) = (f_1(x), \dots, f_m(x)).$$

Per la definició de submersió (22.1.4) trobem que $n \geq m$ i per l'observació 22.1.5 trobem que

$$\operatorname{rang}\left(\frac{\partial f_i}{\partial x_j}(x_0)\right)_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} = m.$$

Aleshores tenim que existeix una permutació $\sigma \in \mathrm{S}_m$ tal que

$$\operatorname{rang}\left(\frac{\partial f_i}{\partial x_{\sigma(j)}}(x_0)\right)_{\substack{1\leq i\leq m \\ 1\leq j\leq m}} = m,$$

i per la proposició 5.1.6 trobem que

$$\det\left(\frac{\partial f_i}{\partial x_{\sigma(j)}}(x_0)\right)_{\substack{1\leq i\leq m\\ 1\leq j\leq m}} \neq 0.$$

Denotem doncs

$$F(x) = (f_{\sigma(1)}(x), \dots, f_{\sigma(m)}(x))$$

i tenim que

$$\det(dF(x_0)) \neq 0. \tag{22.2}$$

Considerem la funció

$$\begin{aligned} g\colon \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ x &\longmapsto (F(x), 0) + (0, \pi_2(x)). \end{aligned}$$

Per l'exemple 22.1.6 trobem que

$$(\pi_1 \circ g)(x) = \pi_1(F(x), \pi_2(x)) = F(x).$$

Per la definició de matriu Jacobiana (6.2.12) i la proposició 6.2.13 tenim que

$$dg(x_0) = \left[\begin{array}{ccc|ccc} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} & \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial F_m}{\partial x_{n+1}} & \cdots & \frac{\partial F_m}{\partial x_n} & \frac{\partial F_m}{\partial x_{n+1}} & \cdots & \frac{\partial F_m}{\partial x_m} \\ \hline & 0_{(n-m)\times n} & & & I_{(n-m)\times(n-m)} & \end{array}\right].$$

Aleshores tenim que

$$\det(dg(x_0)) = \det(dF(x_0)),$$

i per (22.2) trobem que

$$\det(dg(x_0) \neq 0,$$

i pel Teorema de la funció inversa (6.3.12) hem acabat. □

Definició 22.1.10 (Superfície)**.** Sigui $S \subseteq \mathbb{R}^3$ un subconjunt tal que per a tot $p \in S$ existeix un entorn obert $\mathcal{U}$ de p i un difeomorfisme $g\colon \mathcal{U} \longrightarrow g(\mathcal{U})$ tal que

$$g(\mathcal{U} \cap S) = g(\mathcal{U}) \cap (\mathbb{R}^2 \times \{0\}).$$

Aleshores direm que S és una superfície regular.

Teorema 22.1.11. *Sigui $S \subseteq \mathbb{R}^3$ un subconjunt. Aleshores S és una superfície si i només si per a tot punt $p \in S$ existeixen un entorn obert $\mathcal{U}$ de p i una submersió $F\colon \mathcal{U} \longrightarrow \mathbb{R}$ tals que*

$$S \cap \mathcal{U} = F^{-1}(\{0\}).$$

Demostració. Comencem veient que la condició és suficient ($\Longrightarrow$). Suposem doncs que S és una superfície. Per la definició de superfície (22.1.10) trobem que que per a tot $p \in S$ existeix un entorn obert $\mathcal{U}$ de p i un difeomorfisme $g\colon \mathcal{U} \longrightarrow g(\mathcal{U})$ tal que

$$g(\mathcal{U} \cap S) = g(\mathcal{U}) \cap (\mathbb{R}^2 \times \{0\}).$$

Considerem la funció

$$\begin{aligned} F\colon \mathcal{U} &\longrightarrow \mathbb{R} \\ x &\longmapsto (\pi_3 \circ g)(x). \end{aligned}$$

Aleshores tenim que

$$\begin{aligned} F^{-1}(\{0\}) &= (\pi_3 \circ g)^{-1}(\{0\}) \\ &= g^{-1}(\mathbb{R}^2 \times \{0\}) = \mathcal{U} \cap S, \end{aligned}$$

i hem acabat.

Veiem ara que la condició és necessària ($\Longleftarrow$). Suposem doncs que per a tot punt $p \in S$ existeixen un entorn obert $\mathcal{U}$ de p i una submersió $F\colon \mathcal{U} \longrightarrow \mathbb{R}$ tals que $S \cap \mathcal{U} = F^{-1}(\{0\})$. Pel Teorema d'estructura local de les submersions (22.1.9) tenim que per a tot $p \in S$ existeix un obert $\mathcal{U}'$ satisfent $x_0 \subseteq \mathcal{U}' \subseteq \mathcal{U}$ i existeix un difeomorfisme $g\colon \mathcal{U}' \longleftrightarrow g(\mathcal{U}') \subseteq \mathbb{R}^n$ tals que

$$F(x) = (\pi_3 \circ g)(x).$$

Aleshores tenim que

$$\begin{aligned} S \cap \mathcal{U}' &\subseteq S \cap \mathcal{U} \\ &= F^{-1}(\{0\}) \\ &= (\pi_3 \circ g)^{-1}(\{0\}) \\ &= g^{-1}(\mathbb{R}^2 \times \{0\}), \end{aligned}$$

i per tant tenim

$$g(S \cap \mathcal{U}') \subseteq g(g^{-1}(\mathbb{R}^2 \times \{0\})) = \mathbb{R}^2 \times \{0\}$$

continuar □

Exemple 22.1.12. *Exemple d'alguna superfície amb el teorema aquest.*

Solució. ◊

Definició 22.1.13 (Carta local)**.** Sigui $S \subseteq \mathbb{R}^3$ un conjunt i $p \in S$ un punt tals que existeix un entorn obert $\mathcal{U}$ de p, un conjunt $\Omega \subseteq \mathbb{R}^2$ i una aplicació $\Psi\colon \Omega \longrightarrow S \cap \mathcal{U}$ que és una immersió i un homeomorfisme. Aleshores direm que Ω amb Ψ és una carta local de p en S.

Teorema 22.1.14. *Sigui $S \subseteq \mathbb{R}^3$ un subconjunt. Aleshores S és una superfície si i només si per a tot $p \in S$ existeix una carta local de p en S.*

Demostració. □

Exemple 22.1.15. *Volem veure que si tenim $S \subseteq \mathbb{R}^3$ una superfície i $\Psi\colon \Omega \longrightarrow \Psi(\Omega) \subseteq S$ una immersió injectiva, aleshores Ω amb Ψ és una carta local si i només si $\Psi\colon \Omega \longrightarrow \Psi(\Omega)$ és un homeomorfisme.*

Solució. ◊

22.1.2 Funcions diferenciables i l'espai tangent

Definició 22.1.16 (Funció diferenciable)**.** Siguin $S \subseteq \mathbb{R}^3$ una superfície i $f\colon S \longrightarrow \mathbb{R}^k$ una funció tal que per a tot $p \in S$ existeix una carta local Ω amb Ψ satisfent $p \in \Psi(\Omega)$ tals que

$$f \circ \Psi\colon \Omega \longrightarrow \mathbb{R}^k$$

és un difeomorfisme. Aleshores direm que f és diferenciable.

Teorema 22.1.17. *Siguin $S \subseteq \mathbb{R}^3$ una superfície i Ω_1 amb Ψ_1 i Ω_2 amb Ψ_2 dues parametritzacions locals de S amb*

$$\Psi_1(\Omega_1) \cap \Psi_2(\Omega_2) \neq \emptyset.$$

Aleshores la funció

$$\Psi_2^{-1} \circ \Psi_1\colon \Omega_1 \cap \Omega_2 \longrightarrow \Omega_1 \cap \Omega_2$$

és diferenciable.

Demostració. □

Proposició 22.1.18. *Siguin $S \subseteq \mathbb{R}^3$ una superfície, $f\colon S \longrightarrow \mathbb{R}^k$ una funció diferenciable i $p \in S$ un punt. Aleshores existeix un entorn obert $\mathcal{U} \subseteq \mathbb{R}^3$ de p i una funció diferenciable $\tilde{f}\colon \mathcal{U} \longrightarrow \mathbb{R}^k$ tals que per a tot $x \in S \cap \mathcal{U}$ tenim*

$$f(x) = \tilde{f}(x).$$

Demostració. □

Definició 22.1.19 (Funció diferenciable entre superfícies)**.** Siguin $S_1 \subseteq \mathbb{R}^3$ i $S_2 \subseteq \mathbb{R}^3$ dues superfícies i $f\colon S_1 \longrightarrow \mathbb{R}^3$ una funció diferenciable. Aleshores diem que la funció $f\colon S_1 \longleftarrow S_2$ és diferenciable.

Proposició 22.1.20. *Siguin $S_1 \subseteq \mathbb{R}^3$ i $S_2 \subseteq \mathbb{R}^3$ dues superfícies i $f\colon S_1 \longrightarrow S_2$ una funció. Aleshores f és diferenciable si i només si existeixen dues cartes locals Ω_1 amb Ψ_1 i Ω_2 amb Ψ_2 de S_1 i S_2, respectivament, satisfent que existeix un $p \in \Psi_1(\Omega_1)$ i $f(p) \in \Psi_2(\Omega_2)$ i tals que l'aplicació*

$$\Psi_2^{-1} \circ f \circ \Psi_1\colon \Omega_1 \cap \Omega_2 \longrightarrow \Omega_1 \cap \Omega_2$$

és un difeomorfisme.

Demostració. □

22.2 Primera forma fonamental

22.2.1 Espai tangent a una superfície

Definició 22.2.1 (Vectors tangents)**.** Siguin $S \subseteq \mathbb{R}^3$ una superfície i $p \in S$ un punt. Aleshores direm que el conjunt

$$\mathrm{T}_p(S) = \{\alpha'(0) \in \mathbb{R}^3 \mid \alpha \text{ és una corba regular en } S \text{ amb } \alpha(0) = p\}$$

és l'espai tangent a S en p, i els elements de $\mathrm{T}_p(S)$ són els vectors tangents a S en p.

Definició 22.2.2 (Primera forma fonamental)**.** Siguin $S \subseteq \mathbb{R}^3$ una superfície i $p \in S$ un punt. Aleshores direm que l'aplicació

$$\begin{aligned} \mathrm{I}_p\colon\ \mathrm{T}_p(S) \times \mathrm{T}_p(S)\colon &\longrightarrow \mathbb{R} \\ (\vec{u}, \vec{w}) &\longmapsto \langle \vec{v}, \vec{w} \rangle \end{aligned}$$

és la primera forma fonamental de S en p.

Nota 22.2.3. *Després justificaré això però tenim*

$$\mathrm{I}_p(\vec{v}, \vec{w}) = \vec{v}^{\top} \begin{bmatrix} E & F \\ F & G \end{bmatrix} \vec{w}$$

i si $\Psi = \Psi(u, v)$*, denotant*

$$\Psi_u = \frac{\partial \Psi}{\partial u} \quad i \quad \Psi_v = \frac{\partial \Psi}{\partial v}$$

tenim

$$\begin{bmatrix} E & F \\ F & G \end{bmatrix} = \begin{bmatrix} \langle \Psi_u, \Psi_u \rangle & \langle \Psi_u, \Psi_v \rangle \\ \langle \Psi_u, \Psi_v \rangle & \langle \Psi_v, \Psi_v \rangle \end{bmatrix}.$$

22.2.2 Longitud d'una corba

Proposició 22.2.4. *Siguin* $S \subseteq \mathbb{R}^3$ *una superfície,* Ψ *amb* Ω *una carta local de* S *i* α *una corba en* $\Psi(\Omega)$*. Aleshores*

$$\mathrm{S}_\alpha(t_0)(t) = \int_{t_0}^{t} \sqrt{E u'(\tau)^2 + 2F u'(\tau) v'(\tau) + G v'(\tau)^2}\, \mathrm{d}\tau.$$

Part XI

Equacions diferencials ordinàries II

Capítol 23

Sistemes autònoms al pla

23.1 Sistemes no integrables

23.1.1 Comportament límit de les òrbites

Definició 23.1.1 (Conjunts ω-límit i α-límit)**.** Sigui $\varphi_x \colon \mathbb{R} \longrightarrow \mathbb{R}^n$ l'òrbita d'un punt $x \in \mathbb{R}^n$. Aleshores definim

$$\omega(x) = \{y \in \mathbb{R}^n \mid \text{existeix } (t_n)_{n\in\mathbb{N}} \text{ amb } t_n \overset{n\to\infty}{\longrightarrow} +\infty \text{ tal que } \varphi_x(t_n) \overset{n\to\infty}{\longrightarrow} y\}$$

com el conjunt ω-límit de x i

$$\alpha(x) = \{y \in \mathbb{R}^n \mid \text{existeix } (t_n)_{n\in\mathbb{N}} \text{ amb } t_n \overset{n\to\infty}{\longrightarrow} -\infty \text{ tal que } \varphi_x(t_n) \overset{n\to\infty}{\longrightarrow} y\}$$

com el conjunt α-límit de x.

Observació 23.1.2. *Siguin $x \in \mathbb{R}^n$ un punt i*

$$\dot{x} = f(x) \quad i \quad \dot{x} = -f(x)$$

dues equacions diferencials. Aleshores el conjunt ω-límit de x en la primera equació diferencial és el conjunt α-límit de x en la segona equació diferencial i, anàlogament, el conjunt α-límit de x en la primera equació diferencial és el conjunt ω-límit de x en la segona equació diferencial.

Definició 23.1.3 (Conjunts invariants)**.** Sigui φ_x l'òrbita d'un punt $x \in \mathbb{R}^n$. Aleshores definim

$$\gamma^+(x) = \{\varphi_x(t) \mid t \geq 0\}, \quad \gamma^-(x) = \{\varphi_x(t) \mid t \leq 0\} \quad \text{i} \quad \gamma(x) = \gamma^+(x) \cup \gamma^-(x),$$

i direm que un conjunt $C \subseteq \mathbb{R}^n$ és positivament invariant si per a tot $y \in C$ tenim que $\gamma^+(y) \subseteq C$, que és negativament invariant si per a tot $y \in C$ tenim que $\gamma^-(y) \subseteq C$ i que és invariant si per a tot $y \in C$ tenim que $\gamma(y) \subseteq C$.

Teorema 23.1.4. *Siguin*

$$\dot{x} = f(x)$$

una equació diferencial sobre $\mathbb{R}^n$, $\mathcal{K}$ un compacte de $\mathbb{R}^n$ i $p \in \mathbb{R}^n$ un punt tals que $\gamma^+(x) \subset \mathcal{K}$. Aleshores

1. $\omega(x) \neq \emptyset$.

2. $\omega(x)$ *és un tancat.*

3. $\omega(x) = \omega(\varphi_x(t))$ *per a tot* $t \in \mathbb{R}$.

4. $\omega(x)$ *és connex.*

Demostració. Comencem veient el punt (1). Per hipòtesi tenim que $\gamma^+(x) \subset \mathcal{K}$. Ara bé, tenim que $\varphi_x(0) = x \in \gamma^+(x)$, i per tant $x \in \mathcal{K}$ i tenim que $\mathcal{K} \neq \emptyset$. □

23.1.2 Teorema de Poincaré-Bendixson

Definició 23.1.5 (Gràfic)**.**

Teorema 23.1.6 (Teorema de Poincaré-Bendixson)**.** *Siguin* $\dot{x} = f(x)$ *una equació diferencial en* $\Omega \subseteq \mathbb{R}^2$ *amb un nombre finit de punts crítics i* $\mathcal{K} \subseteq \Omega$ *un compacte tal que* $\gamma^+(x) \subseteq \mathcal{K}$*. Aleshores*

1. si $\omega(x)$ *només conté punts crítics tenim que* $\omega(x) = \{p\}$.

2. si $\omega(x)$ *conté punts crítics i punts regulars tenim que* $\omega(x)$ *és un gràfic.*

3. si $\omega(x)$ *no conté punts crítics tenim que* $\omega(x)$ *és una òrbita periòdica.*

Demostració. Aquest enunciat té sentit pel Teorema 23.1.4. □