UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Construcció dels Nombres Reals: Estructura i Propietats del Continu

Autora: Mercè Reverté Jorge

Director: Dr. Joan Bagaria i Pigrau
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 12 de juny de 2023

Abstract

The linear continuum is a mathematical object of great importance. In this project we give a construction of the real numbers, a particular linear continuum, starting with the natural numbers and using basic notions of set theory. We briefly discuss the set of real numbers as a complete ordered field. Finally, we present some of its regularity properties under ZFC, where we also see the existence of pathological sets of real numbers that don't satisfy said properties.

Resum

El continu lineal és un objecte matemàtic de gran importància. En aquest treball realitzem la construcció d'un continu lineal particular, el dels nombres reals, partint dels nombres naturals i de nocions bàsiques de teoria de conjunts. Parlem breument del conjunt dels nombres reals com a cos ordenat complet. Acabem el nostre estudi tractant algunes de les seves propietats de regularitat sota la teoria axiomàtica ZFC, on veiem també l'existència de conjunts patològics de reals que no les compleixen.

2020 Mathematics Subject Classification. 03-01, 03E17, 03E99

Agraïments

Vull agrair al meu tutor, el Dr. Joan Bagaria, la seva ajuda, dedicació, i proposta de tema i estructura del treball.

Agraeixo també als meus amics i amigues (especialment a l'Ana, la Carla i les Emmes), així com a la meva família, el seu suport al llarg d'aquests mesos.

Índex

1 Introducció

El projecte

La teoria de conjunts és una formalització estàndard de la matemàtica a través de conjunts en lògica de primer ordre. L'objectiu principal d'aquest treball és exposar la construcció del continu lineal, és a dir, de la recta real a partir de la teoria de conjunts, així com comentar algunes propietats sobre el continu i observar com es comporta sota certes condicions.

L'estudi de la teoria de conjunts va començar a la dècada dels 1870 amb els matemàtics alemanys Richard Dedekind i Georg Cantor, considerat el fundador d'aquesta branca de les matemàtiques. La teoria de conjunts és fonamental per al desenvolupament general de les matemàtiques, la filosofia i la teoria de l'infinit. Al 1873 Cantor va descobrir que el continu lineal no és numerable. Així, tot i que tant el conjunt de nombres reals com el de naturals són tots dos infinits, hi ha més reals que no pas naturals. Aquest fet va obrir les portes a la investigació de les diferents mides de l'infinit. Cantor va introduir el concepte de cardinalitat per formalitzar aquestes idees i, al 1878, va formular la seva Hipòtesi del Continu, que afirma que tot conjunt infinit de reals és o bé numerable o bé de la mateixa cardinalitat que els reals. Aquest serà un dels punts que tocarem durant el treball.

El tema d'estudi particular d'aquest projecte és interessant perquè permet veure com es generen objectes matemàtics bàsics com són els nombres naturals a partir de la teoria de conjunts i es poden formalitzar amb tot detall l'aritmètica natural i la teoria dels reals. És també curiós observar com qüestions bàsiques sobre el continu poden no tenir solució en la teoria axiomàtica habitual.

Estructura de la Memòria

El treball està dividit en dues parts. La primera part està dedicada a la construcció detallada dels nombres reals. Partirem dels nombres naturals, definits a partir del concepte d'estructura de Dedekind, seguirem amb els enters i els racionals, i acabarem obtenint els reals fent servir talls de Dedekind.

Un cop construït el continu lineal, durant la darrera part del treball en veurem algunes propietats, tractant-lo inicialment com a cos ordenat complet i, finalment, com a estructura topològica; estudiarem tres propietats de regularitat diferents i trobarem conjunts patològics de reals per cada una d'elles.

Consideracions prèvies

La primera part del treball no requereix més coneixements previs que algunes propietats i definicions bàsiques de teoria de conjunts, ja que es detallen tots els procediments que es fan servir. Per a la segona, s'assumiran coneguts coneixements bàsics de topologia, anàlisi i alguns fets generals sobre ordinals i cardinals. En tot moment treballarem sota el sistema axiomàtic de Zermelo-Fraenkel amb l'axioma d'elecció (ZFC), que és una teoria que es pot formalitzar en lògica de primer ordre. De fet, l'axioma d'elecció (AC) només serà necessari al llarg de la segona part. Presentem ara els axiomes de ZFC.

1. **Axioma d'extensionalitat**
   Si els conjunts A i B tenen els mateixos elements, aleshores $A = B$. Formalment,

$$\forall x(x \in A \leftrightarrow x \in B) \rightarrow A = B.$$

2. **Axioma de separació**
   Sigui $\varphi(x_0, \ldots, x_n)$ una fórmula de teoria de conjunts. Si $A, a_1, \ldots, a_n$ són conjunts, aleshores $\{x : x \in A \wedge \varphi(x, a_1, \ldots, a_n)\}$ és un conjunt.

   En altres paraules, si A és un conjunt i P una *propietat*, $\{x : x \in A \wedge P(x)\}$ és un conjunt.

3. **Axioma del parell**
   Per tots x, y, existeix un conjunt $\{x, y\}$ els elements del qual són exactament x i y.

4. **Axioma de la unió**
   Per a tot conjunt A, existeix un conjunt $B = \bigcup A$ format pels elements dels elements de A. Formalment,

$$\forall A \exists B \forall x(x \in B \leftrightarrow \exists y \in A(y \in A \wedge x \in y)).$$

5. **Axioma del conjunt potència**
   Per a tot conjunt A, existeix un conjunt $B = \mathcal{P}(A)$ els elements del qual són els subconjunts de A. Formalment,

$$\forall A \exists B \forall x(x \in B \leftrightarrow x \subseteq A).$$

6. **Axioma de l'infinit**
   Existeix un conjunt infinit. Formalment, ens basarem en la definició de conjunt inductiu per expressar aquest axioma, és a dir, es postula l'existència d'un conjunt inductiu. Així,

$$\exists A(\emptyset \in A \wedge (\forall x \in A)(x \cup \{x\} \in A)).$$

7. **Axioma de regularitat**
   Per a tot conjunt no buit A, existeix $x \in A$ tal que $A \cap x = \emptyset$.

8. **Axioma de substitució**
   Sigui $\varphi(x, y, x_1, \ldots, x_n)$ una fórmula de teoria de conjunts. Per a tot conjunt A, si per tot $x \in A$ i per qualssevol conjunts $a_1, \ldots, a_n$ existeix un únic y tal que $\varphi(x, y, a_1, \ldots, a_n)$, llavors existeix el conjunt $\{y : \exists x \in A : \varphi(x, y, a_1, \ldots, a_n)\}$.

   Dit d'altra manera, si F és una *classe funcional* i A un conjunt, resulta que $F[A] = \{F(x) : x \in A\}$ és un conjunt.

9. **Axioma d'elecció**
   Per a tot conjunt A, si $\emptyset \notin A$, aleshores existeix una funció d'elecció per a A, és a dir, una funció $f : A \rightarrow \bigcup A$ tal que per tota $x \in A$, $f(x) \in x$.

Part I

Construcció dels nombres reals

2 Els nombres naturals

Iniciarem la nostra construcció presentant el concepte d'estructura de Dedekind (introduït pel matemàtic alemany Richard Dedekind al 1872) i el Teorema de Recursivitat. Tot seguit, veurem que aquest tipus d'estructura existeix i que és única a nivell d'isomorfisme. A partir d'això presentarem el conjunt dels nombres naturals i propietats importants sobre aquests, comprovant que satisfan els axiomes de l'aritmètica de Peano.

2.1 Estructures de Dedekind

Definició 2.1. Una *estructura de Dedekind* és una tripla ordenada $\mathcal{D} = \langle D, \sigma, e\rangle$, on $e \in D$, $\sigma : D \to D$, i

(D1) $e \notin \text{ran}(\sigma)$ (on ran és el rang de σ),

(D2) σ és injectiva, i

(D3) $(\forall X \subseteq D)((e \in X \wedge \sigma[X] \subseteq X) \to X = D)$.

A aquesta darrera clàusula se l'anomena *Principi d'Inducció* per a $\mathcal{D}$. Anomenarem *funció generatriu* a σ i *element base* a e.

Proposició 2.2. *Sigui $\mathcal{D} = \langle D, \sigma, e\rangle$ una estructura de Dedekind i φ una propietat qualsevol. Si l'element base té la propietat φ i aquesta és preservada per la funció generatriu, aleshores tot element de D també té la propietat. Formalment,*

$$\varphi(e) \wedge (\forall x \in D)(\varphi(x) \to \varphi(\sigma x)) \;\Rightarrow\; (\forall x \in D)\varphi(x).$$

Demostració. Sigui $X = \{x \in D : \varphi(x)\}$. Suposem que $e \in X$ i que $\sigma[X] \subseteq X$. Per la clàusula (D3), resulta que $X = D$, és a dir, que $(\forall x \in D)\varphi(x)$, com volíem veure. □

Proposició 2.3. *Si $\mathcal{D} = \langle D, \sigma, e\rangle$ és una estructura de Dedekind, aleshores:*

(a) $\forall x \in D(\sigma x \neq x)$ *(la funció generatriu no té punts fixos).*

(b) $\forall x \in D(x = e \vee \exists y(x = \sigma y))$ *(el rang de σ és $D \setminus e$).*

Demostració. Per veure (a), aplicarem la **Proposició 2.2** prenent $\sigma x \neq x$ com a propietat $\varphi(x)$ i procedirem per inducció. Per (D1), $e \neq \sigma e$. Suposem ara com a hipòtesi d'inducció que $\sigma x \neq x$. Volem veure $\sigma\sigma x \neq \sigma x$. Per la injectivitat de σ (D2), com que $x \neq \sigma x$, no pot ser que les imatges de x i σx coincideixin. Per tant, $\sigma x \neq \sigma\sigma x$.

Veiem ara (b) per inducció. Sigui $\psi(x)$ la fórmula $(x = e \vee \exists y(x = \sigma y))$. És evident que $e = e$ i que $\sigma x = \sigma x$ per tot $x \in D$. Per tant, tenim $\psi(e)$ i $\psi(\sigma x)$ per tot $x \in D$. Així, per inducció, obtenim que per tota $x \in D, \psi(x)$. □

2.2 Recursivitat per a estructures de Dedekind

En aquest apartat demostrarem un dels resultats més importants per la nostra construcció, el Teorema de Recursivitat. Abans, introduïm alguns conceptes previs.

Definició 2.4. Diem que un subconjunt $I \subseteq D$ és un *segment inicial* d'una estructura de Dedekind $\mathcal{D} = \langle D, \sigma, e\rangle$ si i només si $I \neq \emptyset$ i $\sigma^{-1}[I] \subseteq I$, és a dir que, si per algun $x \in D$ tenim $\sigma x \in I$, llavors $x \in I$.

Lema 2.5. *Sigui $\mathcal{D} = \langle D, \sigma, e\rangle$ una estructura de Dedekind.*

(a) *$\{e\}$ i D són segments inicials de $\mathcal{D}$.*

(b) *Si I és un segment inicial de $\mathcal{D}$ i $x \in I$, aleshores $I \cup \{\sigma x\}$ també és un segment inicial de $\mathcal{D}$.*

(c) *e pertany a tot segment inicial de $\mathcal{D}$.*

Demostració. La clàusula (a) és immediata per la definició de segment inicial. Pel que fa a (b), és evident que $I \cup \{\sigma x\} \neq \emptyset$. A més, si $\sigma y \in I \cup \{\sigma x\}$ per algun $y \in D$, o bé $\sigma y \in I$ i, en aquest cas, com que I és un segment inicial, $y \in I$, o bé $\sigma y = \sigma x$ i llavors $y = x \in I$.

Per veure (c), suposem que I és un segment inicial de $\mathcal{D}$ i considerem el conjunt $X = \{x \in D : x \in I \to e \in I\}$. Apliquem el principi d'inducció per demostrar que $X = D$. És clar que $e \in X$. Suposem ara $x \in X$ i $\sigma x \in I$. Per definició de segment inicial, això últim implica $x \in I$, de manera que $e \in I$. Per tant, $\sigma x \in X$. Així doncs, $X = D$ i concloem que $e \in I$ per tot segment inicial I de $\mathcal{D}$. □

Veiem ara el resultat principal d'aquesta secció.

Teorema 2.6. (Recursivitat per a estructures de Dedekind) *Sigui $\mathcal{D} = \langle D, \sigma, e\rangle$ una estructura de Dedekind. Sigui A un conjunt, $a \in A$ i $G : A \to A$ una funció. Aleshores existeix una única funció $h : D \to A$ de manera que:*

(a) *$h(e) = a$.*

(b) *$h(\sigma x) = G(h(x))$ per tot $x \in D$.*

Demostració. Demostrem el **Teorema 2.6** veient primer l'existència de la funció h i, tot seguit, la seva unicitat.

Existència. Una *aproximació* a la funció h és una funció $p : I \to A$, on I és un segment inicial de $\mathcal{D}$, de manera que $p(e) = a$ i, per tot $x \in D$, si $\sigma x \in I$ aleshores $p(\sigma x) = G(p(x))$.

Començarem demostrant per inducció que per a tot $x \in D$ existeix una aproximació p tal que x pertany al domini de p ($\mathrm{dom}(p)$). Partim de $\{\langle e, a\rangle\}$, que és una aproximació que té e com a element del seu domini. Sigui ara p una aproximació tal que $x \in \mathrm{dom}(p)$. Llavors $p \cup \{\langle \sigma x, G(p(x))\rangle\}$ és una aproximació el domini de la qual conté σx.

Veiem ara que dues aproximacions qualssevol són compatibles, és a dir, que si p i q són tals que $x \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$, llavors $p(x) = q(x)$. Apliquem inducció novament. En primer lloc, $p(e) = a = q(e)$. Sigui $x \in D$ i suposem inductivament que $r(x) = s(x)$ per totes les aproximacions r i s tals que x pertanyi al domini de totes dues. Siguin p i q aproximacions i suposem $\sigma x \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$. Per definició, el domini d'una

aproximació és un segment inicial. Per tant, de $\sigma x \in \mathrm{dom}(p)$ deduïm $x \in \mathrm{dom}(q)$ i, de $\sigma x \in \mathrm{dom}(q)$, $x \in \mathrm{dom}(q)$. Així, $x \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$ i, per hipòtesi d'inducció, $p(x) = q(x)$. Finalment, $p(\sigma x) = G(p(x)) = G(q(x)) = q(\sigma x)$.

A continuació definirem h i comprovarem que és la funció buscada. Sigui S el conjunt de totes les aproximacions. Posem $h = \bigcup S = \{x : (\exists y \in S)(x \in y)\}$. Com que tots els elements de S són funcions amb conjunt d'arribada A, h és una relació amb rang $\mathrm{ran}(h) \subseteq A$. D'altra banda, el fet que dues aproximacions qualssevol siguin compatibles implica que h és una funció. A més, com que cada $x \in D$ pertany al domini d'alguna aproximació, $\mathrm{dom}(h) = D$. Llavors $h : D \to A$ és una funció. Observem que per a tot $x \in D$ i per cada aproximació p, si $x \in \mathrm{dom}(p)$, $h(x) = p(x)$. Així doncs, per concloure amb la prova de l'existència de h només queda comprovar que es compleixen les dues condicions del teorema:

(a) $h(e) = a$, ja que $p(e) = a$ per a tota $p \in S$.

(b) Sigui $x \in D$, triem $p \in S$ tal que $\sigma x \in \mathrm{dom}(p)$. Aleshores $h(\sigma x) = p(\sigma x) = G(p(x)) = G(h(x))$, com volíem veure.

Unicitat. Suposem que f i g són dues funcions que satisfan les clàusules del teorema. En particular, f i g són aproximacions amb domini D. Per tant, f i g són compatibles i resulta que per a tota $x \in D = \mathrm{dom}(f) \cap \mathrm{dom}(g)$, $f(x) = g(x)$. □

El següent teorema és una variant del **Teorema 2.6**.

Teorema 2.7. *Sigui $\mathcal{D} = \langle D, \sigma, e\rangle$ una estructura de Dedekind. Sigui A un conjunt, $a \in A$ i $G : D \times A \to A$ una funció. Aleshores existeix una única funció $h : D \to A$ tal que:*

(a) $h(e) = a$.

(b) $h(\sigma x) = G(x, h(x))$ *per tot* $x \in D$.

Demostració. La demostració d'aquest teorema és anàloga a la del **Teorema 2.6**, considerant ara que una aproximació és una funció $p : I \to A$, on I és un segment inicial, de manera que $p(e) = a$ i, per tot $x \in D$, si $\sigma x \in I$, aleshores $p(\sigma x) = G(x, p(x))$. □

2.3 Unicitat d'estructures de Dedekind

Veurem ara que les estructures de Dedekind són úniques a nivell d'isomorfisme.

Definició 2.8. Un *isomorfisme* entre dues estructures de Dedekind $\mathcal{D} = \langle D, \sigma, e\rangle$ i $\mathcal{A} = \langle A, \rho, a\rangle$ és una bijecció h entre D i A tal que:

(a) $h(e) = a$.

(b) $h(\sigma x) = \rho(h(x))$.

Diem que $\mathcal{D}$ i $\mathcal{A}$ són *isomorfes* si i només si existeix un isomorfisme entre elles.

Teorema 2.9. *Totes les estructures de Dedekind són isomorfes entre sí. En particular, si $\mathcal{D} = \langle D, \sigma, e\rangle$ i $\mathcal{A} = \langle A, \rho, a\rangle$ són estructures de Dedekind, existeix un únic isomorfisme h entre elles.*

Demostració. Pel **Teorema 2.6** de recursivitat aplicat a $\mathcal{D}$, existeix una única funció $h : D \to A$ tal que $h(e) = a$ i $h(\sigma x) = \rho(h(x))$. Per tant, si veiem que aquesta h és una bijecció, haurem acabat.

Recordem que treballem amb les clàusules (D1), (D2) i (D3) de la definició d'estructura de Dedekind. Les reanomenarem de la següent manera per referir-nos a $\mathcal{A}$:

(A1) $a \notin \text{ran}(\rho)$,

(A2) ρ és injectiva, i

(A3) $(\forall X \subseteq A)((a \in X \wedge \rho[X] \subseteq X) \to X = A)$.

En primer lloc, veiem que h és exhaustiva, és a dir, que $h[D] = A$. Com que $a = h(e)$, $a \in h[D]$. També, per definició de h, $\rho[h[D]] \subseteq h[D]$. Així, per (A3), $h[D] = A$.

Queda veure que h és injectiva. Considerem el conjunt

$$Y = \{x \in D : \forall y(y \neq x \to h(y) \neq h(x))\}.$$

Volem veure que $Y = D$. N'hi ha prou amb demostrar que $e \in Y$ i que, per a tot $x \in D$, si $x \in Y$, aleshores $\sigma x \in Y$.

1. Sigui $y \neq e$. Existeix z tal que $\sigma z = y$, de manera que $h(y) = \rho(h(z))$. Però $h(e) = a \notin \text{ran}(\rho)$, per (A1). Obtenim, doncs, $h(e) \neq h(y)$ i, per tant, $e \in Y$.

2. Sigui $x \in D$. Assumim $x \in Y$. Sigui $y \neq \sigma x$. Si $y = e$, per (A1) tenim $h(y) = a \notin \text{ran}(\rho)$ i $h(\sigma x) = \rho(h(x))$, o sigui que $h(y) \neq h(\sigma x)$. D'altra banda, si $y \neq e$, sigui z tal que $y = \sigma z$. Com que $y \neq \sigma x$, $\sigma x \neq \sigma z$ i $x \neq z$. Per hipòtesi, $x \in Y$, de manera que $h(x) \neq h(z)$. Ara, per (A2), ρ és injectiva i obtenim $\rho(h(x)) \neq \rho(h(z))$. Així, $h(y) = h(\sigma z) = \rho(h(z)) \neq \rho(h(x)) = h(\sigma x)$. En qualsevol cas, $\sigma x \in Y$.

□

Proposició 2.10. *Sigui $\mathcal{D} = \langle D, \sigma, e\rangle$ una estructura de Dedekind. Sigui A un conjunt, $a \in A$ i $\rho : A \to A$ una funció. Si ρ és injectiva i $a \notin ran(\rho)$, existeix una única funció injectiva $h : D \to A$ tal que $h(e) = a$ i $h(\sigma x) = \rho(h(x))$.*

Demostració. Observem que les condicions per a $\langle A, \rho, a\rangle$ són les de la definició d'estructura de Dedekind excepte (A3). Aquesta prova és anàloga a la del **Teorema 2.9**, prenent només la part en què es demostra la injectivitat de h. Ho podem fer així perquè en aquesta no es fa servir de cap manera la clàusula (A3). □

Observació 2.11. Cap de les tres condicions de la definició d'estructura de Dedekind es pot deduir de les altres dues, és a dir, totes tres són necessàries.

2.4 Existència d'estructures de Dedekind

En aquest apartat, donarem una tripla concreta per demostrar l'existència d'estructures de Dedekind. Amb aquesta, busquem poder representar els nombres naturals. De fet, com que acabem de veure la unicitat d'estructures de Dedekind en el sentit d'isomorfisme, qualsevol estructura de Dedekind pot fer el paper de nombres naturals, matemàticament

parlant. Per tant, la demostració de l'existència d'una estructura de Dedekind que realitzarem a continuació és, de fet, una demostració de l'existència dels nombres naturals. Introduïm contextualització prèvia.

Definició 2.12. Diem que un conjunt A és inductiu si $\emptyset \in A$ i $x \cup \{x\} \in A$ per tot $x \in A$.

Axioma 2.13. (*Axioma de l'infinit*) Existeix un conjunt inductiu.

Teorema 2.14. *Existeix un conjunt inductiu mínim, és a dir, un conjunt inductiu que està contingut en tot conjunt inductiu. A més, és únic.*

Demostració. Observem abans que si $A \neq \emptyset$ és un conjunt de conjunts inductius, llavors $\bigcap A$ és un conjunt inductiu. D'una banda, com que $\emptyset$ pertany a tot element de A, $\emptyset \in \bigcap A$. Suposem ara $a \in \bigcap A$. Llavors $a \in x$ per tota $x \in A$ i, com que tot $x \in A$ és inductiu, $a \cup \{a\} \in x$ per tota $x \in A$. Per tant, $a \cup \{a\} \in \bigcap A$.

Segons l'axioma de l'infinit, existeix un conjunt inductiu, diem-li C. Sigui D el conjunt format per tots els subconjunts de C que són inductius. En particular, $C \in D$, de manera que $D \neq \emptyset$. Sigui $A = \bigcap D$. Aleshores A és un conjunt inductiu. Sigui B un conjunt inductiu arbitrari. Tenim $B \cap C \in D$, de manera que $A \subseteq B \cap C \subseteq B$. Per últim, si A i A' són dos conjunts inductius mínims, resulta que $A \subseteq A'$ i $A' \subseteq A$, és a dir, $A = A'$. □

Definició 2.15. Sigui ω el conjunt inductiu més petit.

Aquest serà el conjunt dels nombres naturals. Com farem que serveixi el nostre propòsit? Donem a continuació l'element base i la funció generatriu. Seguirem la definició proposada per John von Neumann.

Definició 2.16. Definim

1. $0 = \emptyset$,
2. La *funció successor* $S : \omega \to \omega$ com $Sx = x \cup \{x\}$ per a $x \in \omega$.

El nostre objectiu és ara demostrar que la tripla $\langle \omega, S, 0 \rangle$ és una estructura de Dedekind. Això provarà l'existència d'aquestes, així com dels nombres naturals, com ja hem establert.

Lema 2.17.

(a) $0 \notin ran(S)$.

(b) $(\forall X \subseteq \omega)((0 \in X \wedge S[X] \subseteq X) \to X = \omega)$.

Demostració. El punt (a) és evident, ja que $x \cup \{x\} = \emptyset$ no es compleix per a cap conjunt x. Pel que fa a (b), suposem que X és un subconjunt de ω de manera que $0 \in X$ i $S[X] \subseteq X$. En altres paraules, $\emptyset \in X$ i $(\forall x \in X)(x \cup \{x\} \in X)$. Però això vol dir que X és un subconjunt inductiu de ω i, com que ω és el conjunt inductiu mínim, $X = \omega$. □

Amb aquest lema hem obtingut que $\langle \omega, S, 0 \rangle$ satisfà les clàusules (D1) i (D3) de la definició d'estructura de Dedekind. Només ens queda per veure la injectivitat de S. Abans introduirem una definició i uns resultats que ens seran útils en aquesta tasca.

Definició 2.18. Un conjunt x és *transitiu* si i només si cada element de x és també un subconjunt de x. Formalment, $\forall y(y \in x \to y \subseteq x)$.

Lema 2.19. *Les següents afirmacions són equivalents per a qualsevol conjunt x:*

(a) *x és transitiu.*

(b) $\forall y \forall z(z \in y \wedge y \in x \to z \in x)$.

(c) $\bigcup x \subseteq x$.

(d) $x \subseteq \mathcal{P}(x)$.

Demostració. Ho veiem amb la cadena de dobles-implicacions (d) $\Leftrightarrow$ (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c).

$x \subseteq \mathcal{P}(x)$ (d) $\Leftrightarrow$ $\forall y(y \in x \to y \in \mathcal{P}(x))$ $\Leftrightarrow$ $\forall y(y \in x \to y \subseteq x)$ $\Leftrightarrow$ x és transitiu (a) $\Leftrightarrow$ $\forall y(y \in x \to (\forall z(z \in y \to z \in x)))$ $\Leftrightarrow$ $\forall y \forall z(z \in y \wedge y \in x \to z \in x)$ (b) $\Leftrightarrow$ $\forall z(z \in \{t : (\exists y \in x)(t \in y)\} \to z \in x)$ $\Leftrightarrow$ $\forall z(z \in \bigcup x \to z \in x)$ $\Leftrightarrow$ $\bigcup x \subseteq x$ (c). □

Lema 2.20.

(a) *$\emptyset$ és un conjunt transitiu.*

(b) *Si x és un conjunt transitiu, $x \cup \{x\}$ també ho és.*

(c) *Si x és un conjunt transitiu, $\bigcup(x \cup \{x\}) = x$.*

Demostració. (a) es compleix per definició. Per a (b), observem que si $y \in x \cup \{x\}$, o bé $y \in x$, o bé $y = x$. En el primer cas, com que x és transitiu, tenim $y \subseteq x \subseteq x \cup \{x\}$. De la mateixa manera, si $y = x$, $y \subseteq x \cup \{x\}$. Veiem ara (c), tenint en compte que

$$x = \bigcup\{x\} \subseteq \bigcup(x \cup \{x\}).$$

Ara, si x és transitiu, pel punt (c) del **Lema 2.19**, tenim $\bigcup x \subseteq x$. Així,

$$\bigcup(x \cup \{x\}) = \bigcup x \cup \bigcup\{x\} \subseteq x \cup x = x.$$

□

Teorema 2.21. *Tots els elements de ω són conjunts transitius.*

Demostració. Sigui $X = \{x \in \omega : x \text{ és transitiu}\}$. Pels punts (a) i (b) del **Lema 2.20**, X és un conjunt inductiu de ω. I com que ω és més petit, resulta que $X = \omega$. □

A continuació s'exposa el resultat que volíem demostrar.

Teorema 2.22. *Existeix una estructura de Dedekind. De fet, la tripla ordenada $\langle \omega, S, 0\rangle$ és una estructura de Dedekind.*

Demostració. Com s'ha esmentat prèviament, només queda comprovar la clàusula (D2) de la definició d'estructura de Dedekind, és a dir, la que afirma que S és injectiva. Siguin $x, y \in \omega$ i suposem $Sx = Sy$. Volem veure que $x = y$. Com que x i y són transitius (per ser elements de ω), fent servir (c) del **Lema 2.20**, obtenim

$$x = \bigcup(x \cup \{x\}) = \bigcup Sx = \bigcup Sy = \bigcup(y \cup \{y\}) = y.$$

□

Així, a partir d'ara ens referim a l'estructura $\langle \omega, S, 0\rangle$ com a l'*estructura dels nombres naturals*. Per a futures referències, podem reescriure ara el següent resultat, extret del **Teorema 2.6** i de la **Proposició 2.10**, en termes de $\langle \omega, S, 0\rangle$.

Teorema 2.23. *Si A és un conjunt, $a \in A$ i $G : A \to A$ és una funció, existeix una única funció $h : \omega \to A$ de manera que $h(0) = a$ i $h(Sx) = G(h(x))$ per tot $x \in \omega$. A més, si G és injectiva i $a \notin ran(G)$, resulta que h també és injectiva.*

Tenim un resultat addicional.

Teorema 2.24. *El conjunt ω és transitiu.*

Demostració. Considerem el conjunt $b = \{x \in \omega : x \subseteq \omega\}$. Provarem que b és inductiu, ja que si és així, com que ω és el conjunt inductiu més petit, tindrem $b = \omega$ i això voldrà dir que ω és transitiu. Com que $\emptyset \subseteq \omega$, $\emptyset \in b$. Sigui ara $x \in b$. Volem veure que $x \cup \{x\} \in b$, és a dir, que $x \cup \{x\} \subseteq \omega$. D'una banda, de $x \in \omega$, tenim $\{x\} \subseteq \omega$, i d'altra com que $x \in b$, $x \subseteq \omega$. Així doncs, $x \cup \{x\} \subseteq \omega$. □

2.5 L'ordre natural $\in_\omega$ en ω

Definició 2.25. Un *ordre total* (estricte) sobre un conjunt A és una relació binària sobre A irreflexiva, transitiva i total, és a dir que per tots $a, b \in A$ diferents, o bé aRb, o bé bRa.

Definició 2.26. Un conjunt dotat d'un ordre total és un *conjunt totalment ordenat* o un *ordre lineal*.

Com a matís, el terme "ordre lineal" seria, més correctament, "ordenació lineal", però farem servir "ordre lineal" per comoditat. Demostrarem en aquest apartat que la relació de pertinença en ω és un ordre total en ω. Aquesta és

$$\in_\omega = \{\langle n, m\rangle : n \in \omega \wedge m \in \omega \wedge n \in m\}.$$

Lema 2.27. *Per tot $n \in \omega$, $n \notin n$.*

Demostració. Veiem-ho per inducció. Evidentment $0 \notin 0 = \emptyset$. Suposem inductivament que $n \notin n$. Suposem també, amb l'objectiu d'arribar a una contradicció, que $Sn \in Sn = n \cup \{n\}$. Llavors o bé $Sn \in n$, o bé $Sn = n$. En el primer cas, com que n és transitiu, resulta que $Sn \subseteq n$ però amb això i $n \in Sn$ deduïm $n \in n$, cosa que contradiu la hipòtesi. El segon cas és anàleg. Sigui com sigui, arribem a una contradicció. □

Lema 2.28. *Per tots $k, n, m \in \omega$, si $k \in n$ i $n \in m$, aleshores $k \in m$.*

Demostració. Sabem que m és transitiu. Fent servir, doncs, l'equivalència entre els punts (a) i (b) del **Lema 2.19**, aquest resultat és immediat. □

Lema 2.29. *Per tots $m, n \in \omega$, $m \in n$ si i només si $Sm \in Sn$.*

Demostració. Siguin $m, n \in \omega$. Demostrem en primer lloc la implicació de dreta a esquerra. Suposem $Sm \in Sn = n \cup \{n\}$. Per tant, o bé $Sm = n$ o bé $Sm \in n$. Com que

$m \in Sm$, o bé $m \in n$, o bé $m \in Sm \in n$. En el darrer cas, per la transitivitat de n, també obtenim $m \in n$.

Demostrem ara la implicació contrària. Veurem per inducció que tots els nombres naturals pertanyen al conjunt

$$X = \{n \in \omega : (\forall m \in \omega)(m \in n \to Sm \in Sn)\}.$$

Vàcuament, $0 \in X$. Procedim inductivament suposant $n \in X$ i per concloure que $Sn \in X$, és a dir, que per tot $m \in Sn$, $Sm \in SSn$. Sigui $m \in Sn = n \cup \{n\}$. O bé $m \in n$, o bé $m = n$. En el darrer cas, $Sm = Sn \in SSn$. I si $m \in n$, per hipòtesi d'inducció, $Sm \in Sn$. Per tant, com que $Sn \in SSn$ i SSn és transitiu, arribem de nou a $Sm \in SSn$. □

Lema 2.30. *Per tot $n \in \omega \setminus \{0\}$, $0 \in n$.*

Demostració. Veiem per inducció que tot nombre natural pertany al conjunt

$$X = \{n \in \omega : n = 0 \vee 0 \in n\}.$$

És evident que $0 \in X$. Suposem que $n \neq 0$ pertany a X. Volem veure que Sn també hi és. Tenim $0 \in n \in Sn$ i com que Sn és transitiu, d'aquí deduïm $0 \in Sn$ i llavors $Sn \in X$.

□

Lema 2.31. *Per tots $n, m \in \omega$, o bé $n \in m$, o bé $n = m$, o bé $m \in n$.*

Demostració. Demostrarem per inducció que tots els nombres naturals pertanyen a

$$X = \{n \in \omega : \forall m \in \omega(n \in m \vee n = m \vee m \in n)\}.$$

Pel **Lema 2.30**, $0 \in X$. Suposem ara, inductivament, que $n \in X$. Sigui $m \in \omega$. Cal veure que $Sn \in X$, és a dir, que o bé $Sn \in m$, o bé $Sn = m$, o bé $m \in Sn$. De $n \in X$, tenim tres possibles casos: si $n \in m$, pel **Lema 2.29**, $Sn \in Sm$. Per tant, o $Sn \in m$ o bé $Sn = m$; si $n = m$, llavors $m = n \in Sn$; i si $m \in n$, tenim $m \in n \in Sn$ cosa que, per transitivitat, implica $m \in Sn$. En qualsevol cas, resulta que $Sn \in X$. □

Teorema 2.32. *$\langle \omega, \in_\omega \rangle$ és un conjunt totalment ordenat.*

Demostració. Cal veure que la relació $\in_\omega$ és irreflexiva, transitiva i que qualssevol dos elements diferents de ω són comparables amb $\in_\omega$. Veure que és irreflexiva és immediat per la propietat $n \notin n, \forall n \in \omega$. La transitivitat s'obté pel **Lema 2.28**. La darrera condició s'obté també de manera directa pel **Lema 2.31**. □

Queda vist, doncs, que $\in_\omega$ és una relació d'ordre total estricte sobre ω.

Definició 2.33. Direm que $\in_\omega$ és l'*ordre natural* en ω. Farem servir el símbol $<$, o simplement $\in$, per referir-nos a ell. Tenim, doncs, que per $n, m \in \omega$,

$$n < m \quad \Leftrightarrow \quad n \in m.$$

A més, considerarem l'ordre reflexiu $\leq$ associat a $<$ segons el qual, per $n, m \in \omega$,

$$n \leq m \quad \Leftrightarrow \quad n \subseteq m.$$

Lema 2.34. *Siguin $n, m \in \omega$. Aleshores $n \subseteq m$ si i només si $n \in m \vee n = m$.*

Demostració. Siguin $n, m \in \omega$. De dreta a esquerra, si $n \in m$, per la transitivitat de m, $n \subseteq m$, i si $n = m$ és clar que $n \subseteq n = m$. Per a la implicació contrària, suposem $n \subseteq m$. Com que $\in$ és un ordre total en ω, o bé $n \in m$, o bé $n = m$, o bé $m \in n$. Però la darrera opció no és possible, ja que si ho fos, per hipòtesi tindríem que $m \in n \subseteq m$ i ja sabem que $m \notin m$. Per tant, hem obtingut $n \in m \vee n = m$, com volíem. □

Definició 2.35. Sigui $\mathbb{A} = \langle A, < \rangle$ un ordre lineal. Sigui $B \subseteq A$. Tenim les següents definicions:

1. $a \in A$ és un *element minimal* de $B \quad \Leftrightarrow \quad a \in B$ i $\forall x \in B(a \leq x)$.
2. $b \in A$ és un *element maximal* de $B \quad \Leftrightarrow \quad b \in B$ i $\forall x \in B(x \leq b)$.
3. $b \in A$ és un *successor immediat* de $a \in A$ (equivalentment a és un *predecessor immediat* de b) si $a < b$ i no existeix cap $x \in A$ tal que $a < x < b$.

Proposició 2.36. *Sigui $\mathbb{A} = \langle A, < \rangle$ un conjunt totalment ordenat. Aleshores:*

(a) *Tot subconjunt de A té, com a molt, un element minimal* (el mínim) *i un element maximal* (el màxim).

(b) *Tot element de A té, com a molt, un successor immediat* (el successor immediat) *i un predecessor immediat* (el predecessor immediat).

Demostració. Si a i b són dos elements minimals de A, tenim $a \leq b$ i $b \leq a$, cosa que equival a $a \subseteq b$ i $b \subseteq a$, o sigui que $a = b$. De manera similar, si a i b són dos elements maximals de A, $b \leq a$ i $a \leq b$, si i només si $b \subseteq a$ i $a \subseteq b$, si i només si $a = b$.

Sigui $a \in A$ i suposem que b i c són successors immediats de a. Aleshores $a < b$, $a < c$, no existeix cap $x \in A$ tal que $a < x < b$ i no existeix cap $x \in A$ tal que $a < x < c$. Si $b < c$, llavors $a < b < c$, que és una contradicció. Anàlogament, si $c < b$, tenim $a < c < b$, que és una contradicció. Per tant, ha de ser $b = c$. De la mateixa manera, si $a \in A$ té dos predecessors immediats b i c, o bé $b < c < a$ (contradicció), o bé $c < b < a$ (contradicció), o bé $b = c$.

□

Lema 2.37. *$\langle \omega, < \rangle$ té el 0 com a mínim i cada $n \in \omega$ té successor immediat, que és Sn. A més, tot $n \in \omega$ diferent de 0 té predecessor immediat.*

Demostració. Pel **Lema 2.30**, 0 és el mínim natural segons l'ordre $<$. Sigui ara $n \in \omega$. Volem veure que no existeix cap $m \in \omega$ tal que $n < m < Sn$. Si existís tal m, tindríem $n \in m$ i $m \in Sn$, és a dir, $m = n$ o $m \in n$. En tots dos casos, per transitivitat, acabaríem concloent $n \in n$, cosa que no pot ser. Per tant, aquesta part queda demostrada.

Finalment, sabem que tot element de ω diferent de 0 té un predecessor immediat per la **Proposició 2.3**, ja que el rang de S és $\omega \setminus 0$. □

Parlarem ara de bons ordres i veurem com es relacionen amb el que hem tractat fins ara.

Definició 2.38. Un *bon ordre* en un conjunt A és un ordre total $<$ en A amb el qual qualsevol subconjunt no buit de A té mínim. Diem llavors que $\mathbb{A} = \langle A, < \rangle$ és un *conjunt ben ordenat* si i només si $<$ és un bon ordre en A.

Teorema 2.39. *El conjunt totalment ordenat $\langle \omega, < \rangle$ és un conjunt ben ordenat.*

Demostració. Sigui $B \subseteq \omega, B \neq \emptyset$. Suposem, amb l'objectiu d'arribar a una contradicció, que B no té element mínim. Considerem el conjunt

$$X = \{n \in \omega : \forall k(k \leq n \to k \notin B)\}.$$

Aleshores $B \cap X = \emptyset$. Com que B no té mínim, $0 \notin B$. Per definició, $0 \in X$. Addicionalment, si $n \in X$, també ha de ser $Sn \in X$, perquè si no Sn seria el mínim de B, que estem suposant que no existeix. Llavors, pel principi d'inducció, resulta que $X = \omega$. Amb això deduïm $B = \emptyset$, que és una contradicció amb la definició de B. □

Corol·lari 2.40. (Inducció completa per a ω) *Sigui $X \subseteq \omega$ tal que per a tot $n \in \omega$,*

$$\textit{si } (\forall k < n)k \in X, \textit{ aleshores } n \in X,$$

llavors $X = \omega$.

Demostració. Suposem que $X \subseteq \omega$ satisfà les hipòtesis del corol·lari però que $X \neq \omega$. Busquem arribar a una contradicció. La suposició que hem fet implica $\omega \setminus X \neq \emptyset$. Per tant, tenim un conjunt ben ordenat ω i un subconjunt no buit d'aquest $\omega \setminus X \neq \emptyset$, de manera que $\omega \setminus X \neq \emptyset$ tindrà un element mínim n. Aleshores $(\forall k < n)k \in X$, però $n \notin X$, cosa que contradiu la hipòtesi del corol·lari. □

Podem reformular el **Corol·lari 2.40** de la següent manera.

Corol·lari 2.41. *Si X és un subconjunt de ω de manera que per a tot $n \in \omega$ es compleix $(n \subseteq X \to n \in X)$, llavors $X = \omega$.*

2.6 Caracteritzacions de $\langle \omega, < \rangle$

A continuació, donarem dos teoremes que caracteritzen $\langle \omega, < \rangle$ a nivell d'isomorfisme, així com la definició de conjunt numerable. Introduirem per començar el concepte d'immersió i d'isomorfisme, que ens seran molt útils en futurs apartats.

Definició 2.42. Siguin $\mathbb{A} = \langle A, <^{\mathbb{A}} \rangle$ i $\mathbb{B} = \langle B, <^{\mathbb{B}} \rangle$ conjunts totalment ordenats.

1. Una funció $f : A \to B$ és *estrictament creixent* si i només si per tots $x, y \in A$,

$$x <^{\mathbb{A}} y \quad \Rightarrow \quad f(x) <^{\mathbb{B}} f(y).$$

2. Una *immersió* de $\mathbb{A}$ en $\mathbb{B}$ és una funció injectiva $f : A \to B$ tal que per tots $x, y \in A$,

$$x <^{\mathbb{A}} y \quad \Leftrightarrow \quad f(x) <^{\mathbb{B}} f(y).$$

Lema 2.43. *Tota funció estrictament creixent d'un ordre lineal $\mathbb{A}$ en un ordre lineal $\mathbb{B}$ és una immersió de $\mathbb{A}$ en $\mathbb{B}$.*

Demostració. Sigui $f : A \to B$ tal funció. La injectivitat és immediata per la definició de funció estrictament creixent. Queda veure que $\forall x, y \in A$, $f(x) <^{\mathbb{B}} f(y) \Rightarrow x <^{\mathbb{A}} y$. Observem que si $f(x) <^{\mathbb{B}} f(y)$, o bé $x <^{\mathbb{A}} y$, o bé $y <^{\mathbb{A}} x$. Però si fos cert el segon cas tindríem $f(y) <^{\mathbb{B}} f(x)$, que ens porta a una contradicció. □

Lema 2.44. *Sigui $\mathbb{A} = \langle A, <^{\mathbb{A}} \rangle$ un conjunt totalment ordenat i sigui $h : \omega \to A$ una funció de manera que per a tot $n \in \omega$, $h(n) <^{\mathbb{A}} h(Sn)$. Aleshores h és estrictament creixent.*

Demostració. Siguin $\mathbb{A}$ i h com en les hipòtesis del lema. Donat $m \in \omega$, definim

$$A_m = \{n \in \omega : m < n \to h(m) <^{\mathbb{A}} h(n)\}.$$

Demostrarem que $A_m = \omega$ per inducció. Vàcuament, $0 \in A_m$. Assumim $n \in A_m$ i sigui $m < Sn$. Cal veure que $h(m) <^{\mathbb{A}} h(Sn)$. Tenint $m < Sn$, pot ser que $m < n$, o bé que $m = n$. En el primer cas, fent servir la hipòtesi d'inducció i la propietat de h presentada a l'enunciat, tenim $h(m) <^{\mathbb{A}} h(n) <^{\mathbb{A}} h(Sn)$ i, per tant, $h(m) <^{\mathbb{A}} h(Sn)$. Per últim, si $m = n$, $h(m) = h(n) <^{\mathbb{A}} h(Sn)$. En qualsevol cas, $Sn \in A_m$. □

Definició 2.45. Un *isomorfisme* entre dos ordres lineals $\mathbb{A}, \mathbb{B}$ és una immersió exhaustiva de $\mathbb{A}$ en $\mathbb{B}$. Així, $\mathbb{A}$ i $\mathbb{B}$ són isomorfs si i només si existeix un isomorfisme h entre ells, que expressarem amb $h : \mathbb{A} \cong \mathbb{B}$.

Proposició 2.46. *Siguin $\mathbb{A}, \mathbb{B}, \mathbb{C}$ conjunts totalment ordenats. Es compleixen:*

(a) $\mathbb{A} \cong \mathbb{A}$.

(b) *Si $\mathbb{A} \cong \mathbb{B}$, llavors $\mathbb{B} \cong \mathbb{A}$.*

(c) *Si $\mathbb{A} \cong \mathbb{B}$ i $\mathbb{B} \cong \mathbb{C}$, llavors $\mathbb{A} \cong \mathbb{C}$.*

Demostració. Prenem la funció identitat, que és un isomorfisme entre $\mathbb{A}$ i $\mathbb{A}$, per veure (a). Per a (b), si tenim un isomorfisme f entre $\mathbb{A}$ i $\mathbb{B}$, resulta que f^{-1} és un isomorfisme entre $\mathbb{B}$ i $\mathbb{A}$. Per últim, si f és un isomorfisme entre $\mathbb{A}$ i $\mathbb{B}$ i g és un isomorfisme entre $\mathbb{B}$ i $\mathbb{C}$, aleshores $g \circ f$ és un isomorfisme entre $\mathbb{A}$ i $\mathbb{C}$. □

Veiem ara dos criteris per determinar si un ordre lineal és isomorf a $\langle \omega, < \rangle$.

Teorema 2.47. *Sigui $\mathbb{A}$ un conjunt no buit ben ordenat que no té màxim i tal que tots els seus elements excepte el mínim tenen un predecessor immediat. Aleshores $\mathbb{A} \cong \langle \omega, < \rangle$.*

Demostració. Sigui $\mathbb{A} = \langle A, <^{\mathbb{A}} \rangle$ un conjunt com el descrit. Com que $A \neq \emptyset$ està ben ordenat, A té mínim; li diem a_0. Comencem veient que tot element de A té successor immediat en $\mathbb{A}$. Sigui $a \in A$. El conjunt $\{x \in A : a <^{\mathbb{A}} x\}$ és no buit, ja que A no té màxim. Per tant, $\{x \in A : a <^{\mathbb{A}} x\}$ té un element mínim, el successor immediat de a.

Definim, doncs, $\rho : A \to A$ com la funció que envia $x \in A$ al seu successor en $\mathbb{A}$. Pel Teorema de Recursivitat, existeix una funció $h : \omega \to A$ tal que $h(0) = a_0$ i $h(Sn) = \rho(h(n))$ per tot $n \in \omega$. Demostrarem que h és un isomorfisme entre $\langle \omega, < \rangle$ i $\mathbb{A}$. Ara bé, tots dos conjunts són totalment ordenats, així que, pel **Lema 2.43**, n'hi ha prou amb veure que h és estrictament creixent (per tant, una immersió) i que h és exhaustiva.

Com que hem definit la funció ρ com la funció successor en $\mathbb{A}$, tenim que, per tot $n \in \omega$, $h(n) <^{\mathbb{A}} \rho(h(n)) = h(Sn)$. Aplicant el **Lema 2.44**, h és estrictament creixent.

Suposem ara que h no és exhaustiva per tal d'arribar a una contradicció. Sigui b_0 el mínim element del subconjunt no buit $A \setminus h[\omega]$. Com que $a_0 = h(0)$, sabem que $a_0 \neq b_0$. Per tant, per hipòtesi, b_0 té un predecessor immediat b en $\mathbb{A}$. Així, $b_0 = \rho(b)$. A més, com que b_0 és el mínim de $A \setminus h[\omega]$, $b \in h[\omega]$. Sigui, doncs, $n \in \omega$ tal que $h(n) = b$. Per definició de h, resulta que $b_0 = \rho(b) = \rho(h(n)) = h(Sn) \in h[\omega]$, que contradiu la tria de b_0. Per tant, h ha de ser exhaustiva. □

Abans de veure el segon teorema, caldrà tenir en compte algunes definicions.

Definició 2.48. Sigui $\mathbb{A} = \langle A, <^{\mathbb{A}} \rangle$ un conjunt totalment ordenat. Siguin $X \subseteq A$ i $a \in A$.

1. a és una *fita superior* de X en $\mathbb{A}$ si i només si per tot $x \in X, x \leq a$.
2. a és una *fita inferior* de X en $\mathbb{A}$ si i només si per tot $x \in X, a \leq x$.
3. X està *afitat superiorment* en $\mathbb{A}$ si i només si X té una fita superior en $\mathbb{A}$.
4. X està *afitat inferiorment* en $\mathbb{A}$ si i només si X té una fita inferior en $\mathbb{A}$.

Teorema 2.49. *Si $\mathbb{A} = \langle A, <^{\mathbb{A}} \rangle$ és un conjunt totalment ordenat tal que A té mínim, tot element de A té successor immediat, i tot subconjunt no buit afitat superiorment de A té màxim, aleshores $\mathbb{A} \cong \langle \omega, < \rangle$.*

Demostració. Sigui $\mathbb{A}$ com en l'enunciat del teorema. Llavors $\mathbb{A}$ no té màxim ni és buit. Si demostrem que $\mathbb{A}$ està ben ordenat i que tots els elements de $\mathbb{A}$ excepte el mínim tenen un predecessor immediat, pel **Teorema 2.47**, obtindrem $\mathbb{A} \cong \langle \omega, < \rangle$.

Si $a \in A$ no és el mínim, el conjunt $\{x \in A : x <^{\mathbb{A}} a\}$ no és buit i està afitat superiorment. Aleshores aquest conjunt tindrà màxim, que serà el predecessor immediat de a. Veiem ara que $\mathbb{A}$ és ben ordenat. Sigui X un subconjunt no buit de A. Cal veure que X té mínim. Sigui $Y = \{y \in A : (\forall x \in X)(y <^{\mathbb{A}} x)\}$. Si $Y = \emptyset$, el mínim de A és també el mínim element de X. Si $Y \neq \emptyset$, tenim que Y té màxim, que anomenem b. Sigui a el successor immediat de b en $\mathbb{A}$. Aleshores a és el mínim de X. □

Per últim, presentem el concepte de conjunt numerable.

Definició 2.50. Diem que un conjunt A és *numerable* si i només si A és finit, o bé infinit numerable, és a dir, que existeix una bijecció entre ω i A.

2.7 Les operacions aritmètiques

Definirem a continuació les operacions de suma i producte per als naturals i en veurem algunes propietats.

Definició 2.51. La *suma* de nombres naturals satisfà dues identitats que alhora la caracteritzen. Són:

$[1]_+$ $m + 0 = m$.

$[2]_+$ $m + Sn = S(m + n)$.

Definició 2.52. El *producte* de nombres naturals satisfà dues identitats que alhora el caracteritzen. Són:

[1]• $m \cdot 0 = 0$.

[2]• $m \cdot Sn = m + (m \cdot n)$.

Per tal de provar que aquestes funcions existeixen, demostrarem primer una generalització del teorema de recursivitat per a ω (**Teorema 2.23**), que ens permet definir i tractar amb funcions amb domini $\omega \times \omega$.

Teorema 2.53. *Donades dues funcions $g : \omega \to \omega$ i $h : \omega \times \omega \to \omega$, existeix una única funció $f : \omega \times \omega \to \omega$ tal que per tots $m, n \in \omega$:*

(a) $f(m, 0) = g(m)$.

(b) $f(m, Sn) = h(m, f(m, n))$.

Abans de demostrar aquest resultat, veiem que, efectivament, la funció f ens proporcionarà la suma i el producte tal i com els hem definit.

Observacions 2.54.

1. Per la suma, prenem $g(m) = m$ i $h(m, k) = Sk$. Aleshores $m + 0 = f(m, 0) = g(m) = m$ i $m + Sn = f(m, Sn) = h(m, f(m, n)) = S(f(m, n)) = S(m + n)$.
2. Pel que fa al producte, prenem $g(m) = 0$ i $h(m, k) = m+k$. Llavors $m \cdot 0 = f(m, 0) = g(m) = 0$ i $m \cdot Sn = f(m, Sn) = h(m, f(m, n)) = m + f(m, n) = m + (m \cdot n)$.

Demostrem ara el **Teorema 2.53**.

Demostració. Establirem en primer lloc la unicitat de f per inducció. Suposem que f i f' són dues funcions que satisfan les condicions del teorema. Volem veure que $f = f'$. Fixat $m \in \omega$, considerem el conjunt $X = \{n \in \omega : f(m, n) = f'(m, n)\}$. Tenim $0 \in X$, ja que $f(m, 0) = g(m) = f'(m, 0)$. Assumim inductivament $n \in X$. Per (b), $f(m, Sn) = h(m, f(m, n)) = h(m, f'(m, n)) = f'(m, Sn)$, de manera que $Sn \in X$.

Queda veure l'existència de f. Per cada $m \in \omega$, pel **Teorema 2.23**, prenent $A = \omega$, $a = g(m)$ i $G(k) = h(m, k)$, existeix una única funció $F_m : \omega \to \omega$ tal que $F_m(0) = g(m)$ i $\forall n \in \omega, F_m(Sn) = h(m, F_m(n))$. Definim llavors $f : \omega \times \omega \to \omega$ per $f(m, n) = F_m(n)$, és a dir, $f = \{\langle m, n, k\rangle : F_m(n) = k\}$. Comprovem que aquesta és la funció buscada:

(a) $f(m, 0) = F_m(0) = g(m)$.

(b) $f(m, Sn) = F_m(Sn) = h(m, F_m(n)) = h(m, f(m, n))$.

□

Proposició 2.55. *Per a tot $n \in \omega, Sn = n + 1$.*

Demostració. Com que $1 = S0, n + 1 = n + S0 = S(n + 0) = Sn$. □

Definició 2.56. Per a $n \neq 0$, escriurem $n - 1$ per referir-nos a l'únic m tal que $n = Sm$.

Teorema 2.57. *Per a qualssevol $m, n, k \in \omega$, es compleixen:*

(a) $m + n = n + m$ *(la suma és commutativa).*

(b) $m + (n + k) = (m + n) + k$ *(la suma és associativa).*

(c) $m \cdot (n + k) = m \cdot n + m \cdot k$ *(el producte és distributiu respecte de la suma).*

(d) $m \cdot n = n \cdot m$ *(el producte és commutatiu).*

(e) $m \cdot (n \cdot k) = (m \cdot n) \cdot k$ *(el producte és associatiu).*

Demostració. Veurem cada apartat per inducció.

(a) Abans, també per inducció, comprovem que $0 + m = m$ per tot $m \in \omega$. Si $m = 0, 0 + 0 = 0$. Suposem ara que m compleix $0 + m = m$. Aleshores $0 + Sm = S(0 + m) = S(m)$. Vist això, per $n = 0$, és clar que $m + 0 = 0 + m = m$.

Suposem ara que $n \in \omega$ compleix $m + n = n + m$. Cal veure que $m + Sn = Sn + m$. Farem novament una demostració prèvia, $Sm + n = S(m + n)$, per inducció. Si $n = 0$, $Sm + 0 = Sm = S(m + 0)$. Inductivament, si $Sm + n = S(m + n)$, llavors $Sm + Sn = S(Sm + n) = S(S(m + n)) = S(m + Sn)$. Ja podem acabar la demostració de (a). Tenim $m + Sn = S(m + n) = S(n + m) = Sn + m$.

(b) Per $k = 0$, $m + (n + 0) = m + n = (m + n) + 0$.

Suposem ara $m + (n + k) = (m + n) + k$. Aleshores $m + (n + Sk) = m + S(n + k) = S(m + (n + k)) = S((m + n) + k) = (m + n) + Sk$.

(c) Per $k = 0$, $m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$.

Suposem inductivament $m \cdot (n + k) = m \cdot n + m \cdot k$. Llavors $m \cdot (n + Sk) = m \cdot S(n + k) = m + (m \cdot (n + k)) = m + m \cdot n + m \cdot k = m \cdot n + m \cdot Sk$.

(d) Com amb la suma, comprovem abans per inducció que $0 \cdot m = 0$ per tot $m \in \omega$. Si $m = 0$, $0 \cdot 0 = 0$. I si assumim $0 \cdot m = 0$, aleshores $0 \cdot Sm = 0 + (0 \cdot m) = 0 + 0 = 0$, com calia veure. Per tant, per a $n = 0$, clarament $m \cdot 0 = 0 \cdot m = 0$.

Suposem ara que n compleix $m \cdot n = n \cdot m$. Cal veure que el mateix funciona també per a Sn. Demostrem prèviament que $Sn \cdot m = n \cdot m + m$ per inducció sobre m. Si $m = 0$, òbviament $Sn \cdot 0 = 0 = n \cdot 0 + 0$. I si la igualtat es compleix per a m, aleshores, fent servir els apartats anteriors junt amb la hipòtesi d'inducció, $Sn \cdot Sm = Sn + (Sn \cdot m) = Sn + n \cdot m + m = (m + Sn) + n \cdot m = S(m + n) + n \cdot m = S(n + m) + n \cdot m = n + Sm + n \cdot m = (n + n \cdot m) + Sm = n \cdot Sm + Sm$. Per tant, tornant a la demostració principal, $m \cdot Sn = m + (m \cdot n) = m + (n \cdot m) = n \cdot m + m = Sn \cdot m$.

(e) Per $k = 0$, $m \cdot (n \cdot 0) = m \cdot 0 = 0 = (m \cdot n) \cdot 0$.

Assumim $m \cdot (n \cdot k) = (m \cdot n) \cdot k$. Veiem-ho per a Sk. Tenim $m \cdot (n \cdot Sk) = m \cdot (n + (n \cdot k)) = m \cdot n + m \cdot (n \cdot k) = m \cdot n + (m \cdot n) \cdot k = (m \cdot n) \cdot Sk$.

□

Veiem ara que les operacions + i · preserven l'ordre natural.

Lema 2.58. *Siguin $n, m, k \in \omega$.*

(a) *Si $m < n \quad \Rightarrow \quad m + k < n + k$.*

(b) *Si $m < n$ i $k \neq 0 \quad \Rightarrow \quad m \cdot k < n \cdot k$.*

Demostració.

(a) Ho farem per inducció sobre k. Suposem $m < n$. Si $k = 0$, $m + 0 = m < n = n + 0$. Suposem ara que es compleix $m + k < n + k$. Cal veure que $m + Sk < n + Sk$. Fent servir la definició de la suma i la hipòtesi d'inducció, $m + Sk = S(m + k) < S(n + k) = n + Sk$.

(b) Farem de nou inducció sobre k. Suposem $m < n$. Si $k = 1$, clarament $m \cdot S0 = S(m + 0) = Sm < Sn = S(n + 0) = n + S0$. Suposem ara que $m \cdot k < n \cdot k$. Veiem-ho per a Sk. Fent servir l'apartat anterior i la definició del producte, obtenim $m \cdot Sk = m + (m \cdot k) < m + (n \cdot k) < n + (n \cdot k) = n \cdot Sk$.

□

Es compleix la següent *llei de cancel·lació* per als naturals.

Lema 2.59. *Siguin $n, m, k \in \omega$.*

(a) *Si $m + k = n + k \quad \Rightarrow \quad m = n$.*

(b) *Si $m \cdot k = n \cdot k$ i $k \neq 0 \quad \Rightarrow \quad m = n$.*

Demostració.

(a) Veiem-ho per inducció sobre k. Si $k = 0$, fàcilment $m = m + 0 = n + 0 = n$. Suposem ara que $m + k = n + k$ implica $m = n$ i suposem $m + Sk = n + Sk$. Cal veure que això també implica $m = n$. Però com que $S(m + k) = S(n + k)$, llavors $m + k = n + k$ i, per hipòtesi d'inducció, $m = n$.

(b) Fem-ho per inducció sobre m. Si $m = 0$, $0 \cdot k = 0 = n \cdot k$, que només pot ser si $n = 0$. Assumim ara que l'enunciat és vàlid per a m. Suposem $Sm \cdot k = n \cdot k$, amb $k \neq 0$. Volem veure que $Sm = n$. Tenim $m \cdot k + k = n \cdot k$. Per definició de k, ha de ser $n \neq 0$. Aleshores existeix p tal que $n = p + 1$. Així, $m \cdot k + k = p \cdot k + k$. Aplicant la llei de cancel·lació de la suma i la hipòtesi d'inducció, $m = p$, de manera que $Sm = Sp = n$.

□

2.8 Axiomes de l'aritmètica de Peano

Establim finalment que l'estructura $\langle \omega, S, +, \cdot, 0, 1 \rangle$ satisfà els axiomes de l'aritmètica de Peano. Es tracta d'una sèrie d'axiomes sobre els nombres naturals formulats pel matemàtic italià Giuseppe Peano al 1889. Són:

1. 0 és un nombre natural.

2. Tot nombre natural té un successor en els nombres naturals.

3. 0 no és el successor de cap nombre natural.

4. Si $S(n) = S(m)$, llavors $n = m$.

5. Es compleix el *principi d'inducció*.

6. La suma en ω satisfà els axiomes presentats en la seva definició.

7. El producte en ω satisfà els axiomes presentats en la seva definició.

Amb tota la presentació feta fins aquest punt veiem fàcilment que tots aquests axiomes són satisfets per l'estructura $\langle \omega, S, +\cdot, \cdot, 0, 1\rangle$, és a dir, que es tracta d'un model de l'aritmètica de Peano.

3 Els nombres enters

3.1 Definició de $\mathbb{Z}$

Volem estendre el conjunt ω dels nombres naturals a un conjunt $\mathbb{Z}$ d'enters, on considerarem nombres positius i negatius. De fet, ω no serà un subconjunt de $\mathbb{Z}$, si no que $\mathbb{Z}$ contindrà una còpia isomorfa a ω.

Inicialment podem pensar que un enter negatiu es pot determinar mitjançant l'ús de dos nombres naturals i un símbol de sostracció entre ells. Però si ho fem així, un mateix enter negatiu tindrà múltiples maneres diferents d'anomenar-se. Per solucionar aquest problema, definirem una relació d'equivalència entre diferències, és a dir, entre parells ordenats de nombres naturals.

Definició 3.1. Definim $\sim$ com la relació en $\omega \times \omega$ de manera que

$$\langle m, n\rangle \sim \langle p, q\rangle \quad \Leftrightarrow \quad m + q = p + n.$$

Teorema 3.2. *La relació $\sim$ és una relació d'equivalència en $\omega \times \omega$.*

Demostració. La reflexivitat i la simetria s'obtenen fàcilment per definició. Per veure que és transitiva, si tenim $\langle m, n\rangle \sim \langle p, q\rangle$ i $\langle p, q\rangle \sim \langle r, s\rangle$, aleshores $m+q = p+n$ i $p+s = r+q$. Llavors $m + q + p + s = p + n + r + q$ i, per la llei de cancel·lació, $m + s = r + n$. □

Definició 3.3. El conjunt $\mathbb{Z}$ dels *nombres enters* és el conjunt $(\omega \times \omega)/\sim$.

3.2 Operacions aritmètiques en $\mathbb{Z}$

Definirem ara la suma i el producte en $\mathbb{Z}$. Comencem per la suma, que representarem per $+_{\mathbb{Z}}$. Com que treballem amb classes d'equivalències, caldrà triar representants d'aquestes classes, operar amb ells i donar la classe d'equivalència del resultat obtingut. Prèviament, doncs, caldrà assegurar que l'elecció dels representats no afectarà al resultat.

Lema 3.4. *Si $\langle m, n\rangle \sim \langle m', n'\rangle$ i $\langle p, q\rangle \sim \langle p', q', \rangle$, aleshores*

$$\langle m + p, n + q\rangle \sim \langle m' + p', n' + q'\rangle.$$

Demostració. Per hipòtesi, $m+n' = m'+n$ i $p+q' = p'+q$. Sumant les dues equacions, $m+p+n'+q' = m'+p'+n+q$, és a dir, $\langle m+p, n+q\rangle \sim \langle m'+p', n'+q'\rangle$. □

Definició 3.5. Definim la *suma d'enters* per a dos enters a i b com

$$a +_{\mathbb{Z}} b = [\langle m+p, n+q\rangle],$$

on $\langle m, n\rangle$ és un representant de a i $\langle p, q\rangle$ és un representant de b.

Teorema 3.6.

(a) *L'operació* $+_{\mathbb{Z}}$ *és commutativa.*

(b) *L'operació* $+_{\mathbb{Z}}$ *és associativa.*

(c) $0_{\mathbb{Z}}$ *és l'*element neutre *per a* $+_{\mathbb{Z}}$*, és a dir,* $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a$ *per a tot* $a \in \mathbb{Z}$*.*

(d) *Existeix l'invers de la suma. En altres paraules, per a tot enter* a*, existeix un enter* b *de manera que* $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$*. A més, aquest és únic.*

Demostració.

(a) Siguin $\langle m, n\rangle$ i $\langle p, q\rangle$ representants dels enters a i b, respectivament. D'una banda $a +_{\mathbb{Z}} b = [\langle m+p, n+q\rangle]$. Per l'altra, $b +_{\mathbb{Z}} a = [\langle p+m, q+n\rangle]$. I aquestes dos classes són la mateixa, per ser commutativa la suma de naturals.

(b) Sigui $\langle m, n\rangle$ un representant de a, $\langle p, q\rangle$ un representant de b i $\langle r, s\rangle$ un representant de c. Cal veure que $a + (b + c) = (a + b) + c$. Fent servir l'associativitat de la suma de naturals, $a + (b + c) = a + [\langle p + r, q + s\rangle] = [\langle m + (p + r), n + (q + s)\rangle] = [\langle (m + p) + r, (n + q) + s\rangle] = [\langle m + p, n + q\rangle] + c = (a + b) + c$.

(c) Sigui $a \in \mathbb{Z}$ un enter i $\langle m, n\rangle$ un representant seu. Podem triar $\langle 0, 0\rangle$ com a representant de $0_{\mathbb{Z}}$. Aleshores $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = [\langle m + 0, n + 0\rangle] = [\langle m, n\rangle] = a$.

(d) Sigui $a = [\langle m, n\rangle]$ un enter. Prenem $b = [\langle n, m\rangle]$. Veiem que b és l'invers de a per la suma. Tenim $a +_{\mathbb{Z}} b = [\langle m + n, n + m\rangle] = [\langle 0, 0\rangle] = 0_{\mathbb{Z}}$. Per veure la unicitat, si existís b' que fos també invers de a, tindríem, fent servir les propietats prèviament demostrades, $b = b +_{\mathbb{Z}} 0_{\mathbb{Z}} = b +_{\mathbb{Z}} (a +_{\mathbb{Z}} b') = (b +_{\mathbb{Z}} a) +_{\mathbb{Z}} b' = 0_{\mathbb{Z}} +_{\mathbb{Z}} b' = b'$.

□

Denotem a partir d'ara l'invers d'un enter a per $-a$. Tenim $-[\langle m, n\rangle] = [\langle n, m\rangle]$.

Definició 3.7. Podem definir ara l'operació *resta* per

$$b - a = b +_{\mathbb{Z}} (-a).$$

Ara que hem vist la suma, treballarem amb el producte d'enters.

Definició 3.8. Definim el *producte d'enters* en $\mathbb{Z}$ com

$$[\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] = [\langle mp + nq, mq + np\rangle].$$

Veiem, com amb la suma, que l'elecció de diferències no afecta al resultat.

Lema 3.9. *Si* $\langle m, n\rangle \sim \langle m', n'\rangle$ *i* $\langle p, q\rangle \sim \langle p', q'\rangle$*, aleshores*

$$\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q', m'q' + n'p'\rangle.$$

Demostració. Per hipòtesi, $m+n' = m'+n$ i $p+q' = p'+q$. Per tant, $m(p+q')+n'(p+q') = m(p' + q) + n(p' + q)$, si i només si $m(p + q') + n'(p' + q) = m'(p' + q) + n(p + q')$. Ho desenvolupem per obtenir $mp + mq' + n'p' + n'q = m'p' + m'q + np + nq'$. Això equival a $(mp+n'p')+q'(m-n) = (m'p'+np)+q(m'-n')$, si i només si $(mp+n'p')+q'(m'-n') = (m'p' + np) + q(m - n)$. Per tant, $mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np$, és a dir que $\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q', m'q' + n'p'\rangle$. □

Teorema 3.10.

(a) *La multiplicació* $\cdot_{\mathbb{Z}}$ *és commutativa.*

(b) $\cdot_{\mathbb{Z}}$ *és associativa.*

(c) $\cdot_{\mathbb{Z}}$ *és distributiva respecte de* $+_{\mathbb{Z}}$*.*

(d) *L'enter* $1_{\mathbb{Z}}$ *és l'element neutre del producte, és a dir,* $a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$ *per tot* $a \in \mathbb{Z}$*.*

(e) $0_{\mathbb{Z}} \neq 1_{\mathbb{Z}}$*.*

(f) *Si* $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$*, o bé* $a = 0_{\mathbb{Z}}$*, o bé* $b = 0_{\mathbb{Z}}$*. En altres paraules, no hi ha divisors de zero en* $\mathbb{Z}$*.*

Demostració.

(a) $[\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] = [\langle mp + nq, mq + np\rangle] = [\langle pm + qn, pn + qm\rangle] = [\langle p, q\rangle] \cdot_{\mathbb{Z}} [\langle m, n\rangle]$.

(b) $([\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q, \rangle]) \cdot_{\mathbb{Z}} [\langle r, s\rangle] = [\langle mp + nq, mq + np\rangle] \cdot_{\mathbb{Z}} [\langle r, s\rangle] = [\langle mpr + nqr + mqs + nps, mps + nqs + mqr + npr\rangle] = [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle pr + qs, ps + qr\rangle] = [\langle m, n\rangle] \cdot_{\mathbb{Z}} ([\langle p, q\rangle] \cdot_{\mathbb{Z}} [\langle r, s\rangle])$.

(c) $[\langle m, n\rangle] \cdot_{\mathbb{Z}} ([\langle p, q\rangle] +_{\mathbb{Z}} [\langle r, s\rangle]) = [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p + r, q + s\rangle] = [\langle mp + mr + nq + ns, mq + ms + np + nr\rangle] = [\langle mp + nq, mq + np\rangle] +_{\mathbb{Z}} [\langle mr + ns, ms + nr\rangle] = [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] +_{\mathbb{Z}} [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle r, s\rangle]$.

(d) $[\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle 1, 0\rangle] = [\langle m + 0, 0 + n\rangle] = [\langle m, n\rangle]$.

(e) Sabem que $\langle 0, 0\rangle$ i $\langle 1, 0\rangle$ són representants de $0_{\mathbb{Z}}$ i $1_{\mathbb{Z}}$, respectivament. Observem fàcilment que $\langle 0, 0\rangle \not\sim \langle 1, 0\rangle$, ja que $1 + 0 = 1 \neq 0 = 0 + 0$.

(f) Suposem que $[\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] = 0_{\mathbb{Z}}$. Llavors $[\langle mp + nq, mq + np\rangle] = [\langle 0, 0\rangle]$. Per tant, $mp + nq = mq + np$. Suposem també $a \neq 0_{\mathbb{Z}}$, amb l'objectiu de demostrar que $b = 0_{\mathbb{Z}}$. Si $a \neq 0_{\mathbb{Z}}$, això vol dir que $m \neq n$. Sumant els inversos de nq i mq a cada banda de l'equació $mp + nq = mq + np$, obtenim $mp - mq = np - nq$, i d'aquí, per la propietat distributiva del producte, $m(p - q) = n(p - q)$. I com que $m \neq n$, l'única manera que això es compleixi és si $p - q = 0$, és a dir, si $p = q$, o sigui, si $b = 0_{\mathbb{Z}}$.

□

Proposició 3.11. *El conjunt dels nombres enters* $\mathbb{Z}$*, junt amb la suma* $+_{\mathbb{Z}}$*, el producte* $\cdot_{\mathbb{Z}}$*,* $0_{\mathbb{Z}}$ *i* $1_{\mathbb{Z}}$*, forma un anell commutatiu.*

Demostració. En primer lloc, cal veure que $\mathbb{Z}$ és un grup abelià amb la suma, és a dir, que $\mathbb{Z}$ és tancat sota $+_{\mathbb{Z}}$, que $+_{\mathbb{Z}}$ és associativa, commutativa, i que té element neutre i element oposat. Per definició de la suma d'enters, $\mathbb{Z}$ és tancat sota aquesta. La resta de condicions s'han vist al **Teorema 3.6**.

Queda veure ara que $\cdot_{\mathbb{Z}}$ és associativa, commutativa, que té element neutre, que és distributiva respecte de la suma i que $\mathbb{Z}$ és tancat sota $\cdot_{\mathbb{Z}}$. La darrera condició s'obté de la definició del producte d'enters. Les altres s'han demostrat al **Teorema 3.10**. □

Proposició 3.12. *$\mathbb{Z}$ és un conjunt numerable.*

Demostració. Considerem la funció $f : \omega \to \mathbb{Z}$ definida per

$$f(2k) = -k, \text{ per a } k \in \omega,$$
$$f(2k+1) = k+1, \text{ per a } k \in \omega.$$

Segons aquesta, $f(0) = 0, f(1) = 1, f(2) = -1, f(3) = 2, f(4) = -2, \ldots$ Per tant, hem obtingut una bijecció entre ω i $\mathbb{Z}$, de manera que $\mathbb{Z}$ és numerable. □

3.3 L'ordre $<_{\mathbb{Z}}$ en $\mathbb{Z}$

Definició 3.13. Definim l'ordre $<_{\mathbb{Z}}$ en $\mathbb{Z}$ com

$$[\langle m, n\rangle] <_{\mathbb{Z}} [\langle p, q\rangle] \quad \Leftrightarrow \quad m + q \in p + n.$$

La tria dels representants no afecta a aquesta definició.

Lema 3.14. *Si $\langle m, n\rangle \sim \langle m', n'\rangle$ i $\langle p, q\rangle \sim \langle p', q'\rangle$, aleshores*

$$m + q \in p + n \quad \Leftrightarrow \quad m' + q' \in p' + n'.$$

Demostració. Per les hipòtesis de l'enunciat, tenim $m + n' = m' + n$ i $p + q' = p' + q$. Així, $m + q \in p + n$, si i només si $m + q + n' + q' \in p + n + n' + q'$, si i només si $m' + n + q + q' \in p' + q + n + n'$, si i només si $m' + q' \in p' + n'$. □

Teorema 3.15. *La relació $<_{\mathbb{Z}}$ és un ordre total en $\mathbb{Z}$, és a dir, és irreflexiva, transitiva i, per tots $a, b \in \mathbb{Z}$, $a <_{\mathbb{Z}} b \vee a = b \vee b <_{\mathbb{Z}} a$.*

Demostració. La irreflexivitat és immediata per la irreflexivitat de l'ordre en ω. Veiem que la relació és transitiva. Suposem $[\langle m, n\rangle] <_{\mathbb{Z}} [\langle p, q\rangle]$ i $[\langle p, q\rangle] <_{\mathbb{Z}} [\langle r, s\rangle]$. Llavors $m + q \in p + n$ i $p + s \in r + q$. Aleshores $m + q + p + s \in p + n + r + q$ i, per cancel·lació, obtenim $m + s \in r + n$, és a dir, $[\langle m, n\rangle] <_{\mathbb{Z}} [\langle r, s\rangle]$.

Finalment, com que $\in$ és un ordre total, si $[\langle m, n\rangle]$ és un representant de a i $[\langle p, q\rangle]$ és un representant de b, o bé $m + q \in p + n$, o bé $m + q = p + n$, o bé $p + n \in m + q$. Respectivament, això equival a $a <_{\mathbb{Z}} b$, $a = b$ o $b <_{\mathbb{Z}} a$. □

Definició 3.16. Un enter a és *positiu* si i només si $0_{\mathbb{Z}} <_{\mathbb{Z}} a$.

Observació 3.17. Per tant, si $a \in \mathbb{Z}$, o bé a és positiu, o bé $a = 0$, o bé $-a$ és positiu.

Teorema 3.18. *Siguin $a, b, c \in \mathbb{Z}$. Es compleix:*

(a) $a <_{\mathbb{Z}} b$ *si i només si* $a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$.

(b) *Si* $0_{\mathbb{Z}} <_{\mathbb{Z}} c$, $a <_{\mathbb{Z}} b$ *si i només si* $a \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c$.

Demostració. Posem $a = [\langle m, n\rangle]$, $b = [\langle p, q\rangle]$ i $c = [\langle r, s\rangle]$. Per (a), tenim $m + q \in p + n$ que, per la preservació de l'ordre de la suma en ω, equival a $m+r+q+s \in p+r+n+s$, és a dir, a $a+_{\mathbb{Z}}c <_{\mathbb{Z}} b+_{\mathbb{Z}}c$, si tenim en compte que $a+_{\mathbb{Z}}c = [\langle m+r, n+s\rangle]$, $b+_{\mathbb{Z}}c = [\langle p+r, q+s]$ i $[\langle m + r, n + s\rangle] <_{\mathbb{Z}} [\langle p + r, q + s]$ $\iff$ $m + r + q + s \in p + r + n + s$.

Veiem ara (b). Suposem $0_{\mathbb{Z}} <_{\mathbb{Z}} c$. Això implica $s \in r$. Suposem també $a <_{\mathbb{Z}} b$, és a dir, $m + q \in p + n$. Volem veure que $a \cdot_{\mathbb{Z}} c = [\langle mr + ns, ms + nr\rangle] <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c = [\langle pr + qs, ps + qr\rangle]$, és a dir, que $mr + ns + ps + qr \in pr + qs + ms + nr$. És el mateix que veure $r(m+q)+s(p+n) \in r(p+n)+s(m+q)$. Existeix $k \in \omega\setminus\{0\}$ tal que $(m+q)+k = p+n$. I com que $s \in r$, $sk \in rk$. D'aquí, $sk + s(m + q) + r(m + q) \in rk + s(m + q) + r(m + q)$, d'on $r(m + q) + s(p + n) \in r(p + n) + s(m + q)$, com volíem veure.

Finalment, demostrem la implicació contrària de (b). Suposem $s \in r$ i $r(m + q) + s(p + n) \in r(p + n) + s(m + q)$. Volem veure $m + q \in p + n$. Anàlogament al procediment previ, existeix $l \in \omega \setminus \{0\}$ tal que $s + l = r$. Per tant, tenim $(s + l)(m + q) + s(p + n) \in (s + l)(p + n) + s(m + q)$, que implica $l(m + q) \in l(p + n)$ i llavors $m + q \in p + n$. □

Corol·lari 3.19. *La regla de cancel·lació és vàlida en els enters; per tots $a, b, c \in \mathbb{Z}$,*

(a) $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c \quad \Rightarrow \quad a = b.$

(b) $a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c$, $c \neq 0_{\mathbb{Z}} \quad \Rightarrow \quad a = b.$

Demostració. Posem $a = [\langle m, n\rangle]$, $b = [\langle p, q\rangle]$ i $c = [\langle r, s\rangle]$.

(a) $a+_{\mathbb{Z}}c = b+_{\mathbb{Z}}c \Rightarrow [\langle m+r, n+s\rangle] = [\langle p+r, q+s\rangle] \Rightarrow m+r+q+s = p+r+n+s \Rightarrow m + q = p + n \Rightarrow \langle m, n\rangle \sim \langle p, q\rangle \Rightarrow a = b.$

(b) Suposem $a\cdot_{\mathbb{Z}}c = b\cdot_{\mathbb{Z}}c$ i $c \neq 0_{\mathbb{Z}}$. Llavors $[\langle mr+ns, ms+nr\rangle] = [\langle pr+qs, ps+qr\rangle] \Rightarrow mr+ns+ps+qr = pr+qs+ms+nr \Rightarrow r(m+q)+s(p+n) = r(p+n)+s(m+q)$. Si c és positiu, $r-s \in \omega\setminus\{0\}$ i, sumant els inversos de $s(p+n)$ i $s(m+q)$ a banda i banda, tenim $(r-s)(m+q) = (r-s)(p+n) \Rightarrow m+q = p+n \Rightarrow \langle m, n\rangle \sim \langle p, q\rangle \Rightarrow a = b$. En canvi, si $-c$ és positiu, $s-r \in \omega\setminus\{0\}$. Sumant els inversos de $r(m+q)$ i $r(p+n)$ a les dues bandes, obtenim $(s-r)(p+n) = (s-r)(m+q)$, d'on $p+n = m+q \Rightarrow a = b$.

□

Definició 3.20. Per precisar el fet que $\mathbb{Z}$ té un subconjunt isomorf a ω, definim la funció $E : \omega \to \mathbb{Z}$ com $E(n) = [\langle n, 0\rangle]$.

Teorema 3.21. *E és una immersió isomorfa de $\langle \omega, +, \cdot, \in_\omega\rangle$ en $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}}\rangle$, és a dir, E és injectiva i satisfà, per tots $m, n \in \omega$,*

1. $E(m + n) = E(m) +_{\mathbb{Z}} E(n)$,
2. $E(mn) = E(m) \cdot_{\mathbb{Z}} E(n)$, *i*
3. $m \in n$ *si i només si* $E(m) <_{\mathbb{Z}} E(n)$.

Demostració. Per veure la injectivitat de E, siguin $n, m \in \omega$. Llavors $E(n) = E(m) \Leftrightarrow [\langle n, 0\rangle] = [\langle m, 0\rangle] \Leftrightarrow n + 0 = m + 0 \Leftrightarrow n = m$.

1. $E(m+n) = [\langle m+n, 0\rangle] = [\langle m, 0\rangle] + [\langle n, 0\rangle] = E(m) +_{\mathbb{Z}} E(n)$.
2. $E(mn) = [\langle mn, 0\rangle] = [\langle mn + 0\cdot 0, m\cdot 0 + 0\cdot n\rangle] = [\langle m, 0\rangle] \cdot_{\mathbb{Z}} [\langle n, 0\rangle] = E(m) \cdot_{\mathbb{Z}} E(n)$.
3. $E(m) <_{\mathbb{Z}} E(n) \Leftrightarrow [\langle m, 0\rangle] <_{\mathbb{Z}} [\langle n, 0\rangle] \Leftrightarrow m + 0 \in n + 0 \Leftrightarrow m \in n$.

□

Observació 3.22. $[\langle m, n\rangle] = E(m) - E(n)$, ja que $E(m) - E(n) = [\langle m, 0\rangle] - [\langle n, 0\rangle] = [\langle m, 0\rangle] +_{\mathbb{Z}} (-[\langle n, 0\rangle]) = [\langle m, 0\rangle] +_{\mathbb{Z}} [\langle 0, n\rangle] = [\langle m, n\rangle]$.

4 Els nombres racionals

4.1 Definició de $\mathbb{Q}$

Volem estendre ara el conjunt $\mathbb{Z}$ dels enters al conjunt $\mathbb{Q}$ dels racionals de manera similar a l'extensió de ω a $\mathbb{Z}$ que acabem de realitzar. L'ampliació cap a $\mathbb{Z}$ ens ha proporcionat inversos additius, és a dir, solucions de l'equació $a + x = 0$. Busquem ara trobar inversos multiplicatius, és a dir, solucions de l'equació $r \cdot_{\mathbb{Q}} x = 1_{\mathbb{Q}}$ per a $r \neq 0$.

Definició 4.1. Anomenarem *fracció* a un parell d'enters ordenats, el *numerador* i el *denominador*, respectivament, de manera que el denominador és diferent de zero.

A partir d'ara, per simplificar notació, posarem simplement + i $\cdot$ en lloc de $+_{\mathbb{Z}}$ i $\cdot_{\mathbb{Z}}$. El context ens indicarà si estem realitzant una suma o producte d'enters o de naturals.

Definició 4.2. Posem $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$. Definim la relació binària $\sim$ en $\mathbb{Z} \times \mathbb{Z}'$ com

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \Leftrightarrow \quad a \cdot d = c \cdot b.$$

Definició 4.3. El conjunt $\mathbb{Q}$ dels *nombres racionals* és el conjunt $(\mathbb{Z} \times \mathbb{Z}')/\sim$ de classes d'equivalència de fraccions.

Teorema 4.4. *La relació $\sim$ és una relació d'equivalència en $\mathbb{Z} \times \mathbb{Z}'$.*

Demostració. És immediat veure que és reflexiva i simètrica. Pel que fa a la transitivitat, si $\langle a, b\rangle \sim \langle c, d\rangle$ i $\langle c, d\rangle \sim \langle e, f\rangle$, tenim $a \cdot d = c \cdot b$ i $c \cdot f = e \cdot d$. Multipliquem la primera equació per f i la segona per b, cosa que podem fer sense conflictes perquè $b, f \neq 0$, i obtenim $adf = cbf$ i $cfb = edb$. Igualant, $adf = edb$. Podem aplicar cancel·lació amb $d \neq 0$ i, finalment, $a \cdot f = e \cdot b$, és a dir, $\langle a, b\rangle \sim \langle e, f\rangle$. □

4.2 Operacions aritmètiques en $\mathbb{Q}$

Intuïtivament, podem pensar en el càlcul de la suma de racionals com $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$. Amb aquesta idea, donem la següent definició fent servir classes d'equivalència per a la suma de racionals.

Definició 4.5. Definim la *suma* de racionals com

$$[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ad + cb, bd\rangle].$$

Com amb les sumes donades per als naturals i els enters, cal comprovar que aquesta definició no depèn de la tria de representants per a cada racional.

Lema 4.6. *Si* $\langle a, b\rangle \sim \langle a', b'\rangle$ *i* $\langle c, d\rangle \sim \langle c', d'\rangle$*, llavors*

$$\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle.$$

Demostració. Tenim $a \cdot b' = a' \cdot b$ i $c \cdot d' = c' \cdot d$. Multipliquem la primera equació per $d \cdot d'$ i obtenim $ab'dd' = a'bdd'$. La segona la multipliquem per $b \cdot b'$. Llavors, $cd'bb' = c'dbb'$. Les sumem, $ab'dd' + cd'bb' = a'bdd' + c'dbb'$, i apliquem la propietat distributiva del producte d'enters respecte de la suma, $(ad + cb)b'd' = (a'd' + c'b')bd$, és a dir, $\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle$. □

Teorema 4.7.

(a) *La suma* $+_{\mathbb{Q}}$ *és commutativa.*

(b) *La suma* $+_{\mathbb{Q}}$ *és associativa.*

(c) $0_{\mathbb{Q}}$ *és l'element neutre per a* $+_{\mathbb{Q}}$*, és a dir,* $r +_{\mathbb{Q}} 0_{\mathbb{Q}} = r$ *per tot racional* r*.*

(d) *Existeixen els inversos additius per a* $+_{\mathbb{Q}}$*; per a tot* $r \in \mathbb{Q}$ *existeix* $s \in \mathbb{Q}$ *tal que* $r +_{\mathbb{Q}} s = 0_{\mathbb{Q}}$*.*

Demostració.

(a) $[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ad + cb, bd\rangle] = [\langle cb + ad, db\rangle] = [\langle c, d\rangle] +_{\mathbb{Q}} [\langle a, b\rangle]$.

(b) $([\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle]) +_{\mathbb{Q}} [\langle e, f\rangle] = [\langle ad + cb, bd\rangle] +_{\mathbb{Q}} [\langle e, f\rangle] = [\langle adf + cbf + ebd, bdf\rangle] = [\langle a, b\rangle] +_{\mathbb{Q}} [\langle cf + ed, df\rangle] = [\langle a, b\rangle] +_{\mathbb{Q}} ([\langle c, d\rangle] +_{\mathbb{Q}} [\langle e, f\rangle])$.

(c) Podem triar $\langle 0, 1\rangle$ com a representant de $0_{\mathbb{Q}}$. Llavors, per a $r = [\langle a, b\rangle]$, $r +_{\mathbb{Q}} 0_{\mathbb{Q}} = [\langle a, b\rangle] +_{\mathbb{Q}} [\langle 0, 1\rangle] = [\langle a + 0, b\rangle] = r$.

(d) Sigui $r = [\langle a, b\rangle]$. Si posem $s = [\langle -a, b\rangle]$, $r +_{\mathbb{Q}} s = [\langle ab + (-a)b, bb\rangle] = [\langle 0, bb\rangle] = 0_{\mathbb{Q}}$.

□

Observació 4.8. Denotarem l'invers additiu d'un racional $r = [\langle a, b\rangle]$ per $-r = [\langle -a, b\rangle]$.

Treballem ara amb el producte. Com abans, ens podem ajudar de la idea $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ per plantejar la següent definició.

Definició 4.9. Definim el *producte* de racionals com

$$[\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ac, bd\rangle].$$

Comprovem que aquesta definició no depèn de la tria de representants.

Lema 4.10. *Si* $\langle a,b\rangle \sim \langle a',b'\rangle$ *i* $\langle c,d\rangle \sim \langle c',d'\rangle$*, aleshores*

$$\langle ac,bd\rangle \sim \langle a'c',b'd'\rangle.$$

Demostració. Tenim $a\cdot b' = a'\cdot b$ i $c\cdot d' = c'\cdot d$. Multiplicant les dues equacions, $acb'd' = a'c'bd$, és a dir, $\langle ac,bd\rangle \sim \langle a'c',b'd'\rangle$. □

Observacions 4.11.

1. $r\cdot_{\mathbb{Q}} 1_{\mathbb{Q}} = r$ per tot $r\in\mathbb{Q}$, ja que $[\langle a,b\rangle]\cdot_{\mathbb{Q}} 1_{\mathbb{Q}} = [\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle 1,1\rangle] = [\langle a,b\rangle]$.
2. $r\cdot_{\mathbb{Q}} 0_{\mathbb{Q}} = 0_{\mathbb{Q}}$ per tot $r\in\mathbb{Q}$, ja que $[\langle a,b\rangle]\cdot_{\mathbb{Q}} 0_{\mathbb{Q}} = [\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle 0,1\rangle] = [\langle 0,b\rangle] = 0_{\mathbb{Q}}$.

Teorema 4.12.

(a) $\cdot_{\mathbb{Q}}$ *és commutativa.*

(b) $\cdot_{\mathbb{Q}}$ *és associativa.*

(c) $\cdot_{\mathbb{Q}}$ *és distributiva respecte de la suma* $+_{\mathbb{Q}}$*.*

(d) *Per tot* $r\in\mathbb{Q}$ *diferent de zero, existeix un no-zero* $q\in\mathbb{Q}$ *tal que* $r\cdot_{\mathbb{Q}} q = 1_{\mathbb{Q}}$*.*

Demostració.

(a) $[\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle c,d\rangle] = [\langle ac,bd\rangle] = [\langle c,d\rangle]\cdot_{\mathbb{Q}} [\langle a,b\rangle]$.

(b) $([\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle c,d\rangle])\cdot_{\mathbb{Q}} [\langle e,f\rangle] = [\langle ac,bd\rangle]\cdot_{\mathbb{Q}} [\langle e,f\rangle] = [\langle ace,bdf\rangle] = [\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle ce,df\rangle] = [\langle a,b\rangle]\cdot_{\mathbb{Q}} ([\langle c,d\rangle]\cdot_{\mathbb{Q}} [\langle e,f\rangle])$.

(c) $[\langle a,b\rangle]\cdot_{\mathbb{Q}} ([\langle c,d\rangle] +_{\mathbb{Q}} [\langle e,f\rangle]) = [\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle cf+ed,df\rangle] = [\langle acf+aed,bdf\rangle]$. D'altra banda, $[\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle c,d\rangle] +_{\mathbb{Q}} [\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle e,f\rangle] = [\langle ac,bd\rangle] +_{\mathbb{Q}} [\langle ae,bf\rangle] = [\langle acbf + aebd, bdbf\rangle] = [\langle acf+aed,bdf\rangle]$, de manera que es compleix la igualtat buscada.

(d) Sigui $r = [\langle a,b\rangle]$ diferent de zero. Posem $q = [\langle b,a\rangle]$, que està ben definit perquè $r\neq 0_{\mathbb{Q}}$, és a dir, $a\neq 0$. Com que $b\neq 0$, q tampoc és zero. Observem ara que $[\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle b,a\rangle] = [\langle ab,ba\rangle] = [\langle 1,1\rangle] = 1_{\mathbb{Q}}$.

□

Observacions 4.13.

1. Denotarem l'invers multiplicatiu de $r = [\langle a,b\rangle]$ per $r^{-1} = 1/r = [\langle b,a\rangle]$.
2. Igual que en els enters, si $r\cdot_{\mathbb{Q}} q = 0_{\mathbb{Q}}$, o bé $r = 0_{\mathbb{Q}}$, o bé $q = 0_{\mathbb{Q}}$. En altres paraules, no hi ha divisors de zero en $\mathbb{Q}$. Això és perquè si $[\langle a,b\rangle]\cdot_{\mathbb{Q}} [\langle c,d\rangle] = [\langle ac,bd\rangle] = [\langle 0,1\rangle]$, pel resultat anàleg en $\mathbb{Z}$, ha de ser o bé $a=0$, o bé $c=0$.

Amb aquesta darrera observació, obtenim el següent corol·lari.

Corol·lari 4.14. *Si* r *i* q *són racionals diferents de zero, llavors* $r\cdot_{\mathbb{Q}} q$ *és també diferent de zero. En altres paraules, el conjunt de racionals no-zero és tancat sota l'operació producte.*

Definició 4.15. Definim la *divisió* d'enters per a $s,r\in\mathbb{Q}$ amb $r\neq 0_{\mathbb{Q}}$ com

$$s\div r = s\cdot_{\mathbb{Q}} r^{-1}.$$

Amb la notació de classes,

$$[\langle c,d\rangle] \div [\langle a,b\rangle] = [\langle c,d\rangle] \cdot_{\mathbb{Q}} [\langle b,a\rangle] = [\langle cb,da\rangle].$$

Proposició 4.16. *El conjunt dels nombres racionals amb $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$, $0_{\mathbb{Q}}$ i $1_{\mathbb{Q}}$ forma un cos.*

Demostració. Cal veure que $\mathbb{Q}$ és tancat sota les operacions de suma i producte, que $+_{\mathbb{Q}}$ i $\cdot_{\mathbb{Q}}$ són associatives, commutatives i tenen element neutre, que existeixen inversos additius, que existeixen inversos multiplicatius per a elements diferents de zero i que $\cdot_{\mathbb{Q}}$ és distributiva respecte de $+_{\mathbb{Q}}$.

La primera condició ve donada per la definició de la suma i el producte de racionals. Podem veure la resta de condicions al **Teorema 4.7**, a les **Observacions 4.11** i al **Teorema 4.12**. □

Proposició 4.17. *$\mathbb{Q}$ és un conjunt numerable.*

Demostració. Observem inicialment que $\omega \times \omega$ és numerable. Per tant, si A és un conjunt numerable, $A \times A$ també ho és. Hem vist que $\mathbb{Z}$ és numerable, de manera que $\mathbb{Z} \times \mathbb{Z}$ també. Sigui $A = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\} \subseteq \mathbb{Z} \times \mathbb{Z}$. Aleshores A és numerable.

Definim la funció $f : A \to \mathbb{Q}$ per $f(a,b) = \frac{a}{b}$. Com que es tracta d'una funció exhaustiva i A és numerable, aleshores $\mathbb{Q}$ també ho és. □

4.3 L'ordre $<_{\mathbb{Q}}$ en $\mathbb{Q}$

Volem definir ara un ordre en el conjunt dels nombres racionals. Farem servir $<$ en lloc de $<_{\mathbb{Z}}$ a partir d'ara. Per $b, d \in \mathbb{Z}$ positius, sabem que $\frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < cd$. Farem servir aquesta idea i el fet que, com que $[\langle a,b\rangle] = [\langle -a,-b\rangle]$, tot nombre racional pot ser representat per una fracció amb denominador positiu.

Definició 4.18. Definim aleshores l'ordre $<_{\mathbb{Q}}$ com

$$[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] \quad \Leftrightarrow \quad ad < cb,$$

sempre que b i d siguin positius.

Comprovem que l'elecció de representants no resulta problemàtica.

Lema 4.19. *Si $\langle a,b\rangle \sim \langle a',b'\rangle$ i $\langle c,d\rangle \sim \langle c',d'\rangle$, i b, b', d, d' són positius, resulta que*

$$ad < cb \quad \Leftrightarrow \quad a'd' < c'b'.$$

Demostració. Tenim $a \cdot b' = a' \cdot b$ i $c \cdot d' = c' \cdot d$. Com que b, b', d i d' són positius, $ad < cb \Leftrightarrow adb'd' < cbb'd' \Leftrightarrow a'bdd' < c'dbb' \Leftrightarrow a'd' < c'b'$. □

Teorema 4.20. *La relació $<_{\mathbb{Q}}$ és un ordre total en $\mathbb{Q}$.*

Demostració. És clarament irreflexiva. Per veure la transitivitat, si $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle]$ i $[\langle c,d\rangle] <_{\mathbb{Q}} [\langle e,f\rangle]$, és a dir, si $ad < cb$ i $cf < ed$, llavors com que f i b són positius, $adf < cbf < edb$ i d'aquí, sent d positiu, $af < eb$, o sigui $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle e,f\rangle]$. Queda veure que l'ordre és total. Però per tots $a, b, c, d \in \mathbb{Z}$, o bé $ad < cb$, o bé $ad = cb$, o bé $cb < ad$. En altres paraules, o bé $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle]$, o bé $[\langle a,b\rangle] = [\langle c,d\rangle]$, o bé $[\langle c,d\rangle] < [\langle a,b\rangle]$. □

Definició 4.21. Direm que $q \in \mathbb{Q}$ és un *racional positiu* si i només si $0_{\mathbb{Q}} <_{\mathbb{Q}} q$.

Observacions 4.22.

1. $r <_{\mathbb{Q}} 0_{\mathbb{Q}}$ si i només si $0_{\mathbb{Q}} <_{\mathbb{Q}} -r$, ja que $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle 0,1\rangle] \Leftrightarrow a < 0 \Leftrightarrow 0 < -a \Leftrightarrow [\langle 0,1\rangle] <_{\mathbb{Q}} [\langle -a,b\rangle]$.
2. Per tot $r \in \mathbb{Q}$, o bé r és positiu, o bé $r = 0_{\mathbb{Q}}$, o bé $-r$ és positiu.

Teorema 4.23. *Siguin $r,s,t \in \mathbb{Q}$. Llavors:*

(a) *$r <_{\mathbb{Q}} s$ si i només si $r +_{\mathbb{Q}} t <_{\mathbb{Q}} s +_{\mathbb{Q}} t$.*

(b) *Si t és positiu, $r <_{\mathbb{Q}} s$ si i només si $r \cdot_{\mathbb{Q}} t <_{\mathbb{Q}} s \cdot_{\mathbb{Q}} t$.*

Demostració.

(a) $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] \Leftrightarrow ad < cb \Leftrightarrow afdf < cfbf \Leftrightarrow afdf + ebdf < cfbf + edbf \Leftrightarrow [\langle af+eb, bf\rangle] <_{\mathbb{Q}} [\langle cf+ed, df\rangle] \Leftrightarrow [\langle a,b\rangle] +_{\mathbb{Q}} [\langle e,f\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] +_{\mathbb{Q}} [\langle e,f\rangle]$.

(b) Suposem que $[\langle e,f\rangle]$ és positiu, és a dir, que $0 < e$. Llavors $[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] \Leftrightarrow ad < cb \Leftrightarrow aedf < cebf \Leftrightarrow [\langle ae, bf\rangle] <_{\mathbb{Q}} [\langle ce, df\rangle] \Leftrightarrow [\langle a,b\rangle] \cdot_{\mathbb{Q}} [\langle e,f\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] \cdot_{\mathbb{Q}} [\langle e,f\rangle]$.

□

Teorema 4.24. *Les següents lleis de cancel·lació són vàlides per tots $r,s,t \in \mathbb{Q}$:*

(a) *Si $r +_{\mathbb{Q}} t = s +_{\mathbb{Q}} t$, aleshores $r = s$.*

(b) *Si $r \cdot_{\mathbb{Q}} t = s \cdot_{\mathbb{Q}} t$ i $t \neq 0$, llavors $r = s$.*

Demostració.

(a) $[\langle a,b\rangle] +_{\mathbb{Q}} [\langle e,f\rangle] = [\langle c,d\rangle] +_{\mathbb{Q}} [\langle e,f\rangle] \Rightarrow [\langle af+eb, bf\rangle] = [\langle cf+ed, df\rangle] \Rightarrow afdf + ebdf = cfbf + edbf \Rightarrow a \cdot d = c \cdot b \Rightarrow [\langle a,b\rangle] = [\langle c,d\rangle]$.

(b) Suposem $[\langle e,f\rangle] \neq 0_{\mathbb{Q}}$, és a dir, $e \neq 0$. Llavors $[\langle a,b\rangle] \cdot_{\mathbb{Q}} [\langle e,f\rangle] = [\langle c,d\rangle] \cdot [\langle e,f\rangle] \Rightarrow [\langle ae, bf\rangle] = [\langle ce, df\rangle] \Rightarrow aedf = cebf \Rightarrow a \cdot d = c \cdot b \Rightarrow [\langle a,b\rangle] = [\langle c,d\rangle]$.

□

Veiem finalment que existeix un subconjunt de $\mathbb{Q}$ isomorf a $\mathbb{Z}$.

Definició 4.25. Definim la immersió $E : \mathbb{Z} \to \mathbb{Q}$ com $E(a) = [\langle a, 1\rangle]$.

Teorema 4.26. *E és una funció injectiva de $\mathbb{Z}$ en $\mathbb{Q}$ de manera que, per tots $a,b \in \mathbb{Z}$,*

1. $E(a+b) = E(a) +_{\mathbb{Q}} E(b)$,
2. $E(ab) = E(a) \cdot_{\mathbb{Q}} E(b)$,
3. $E(0) = 0_{\mathbb{Q}}$,
4. $E(1) = 1_{\mathbb{Q}}$, *i*
5. *$a < b$ si i només si $E(a) <_{\mathbb{Q}} E(b)$.*

Demostració. Demostrem inicialment la injectivitat de E. Siguin $a, b \in \mathbb{Z}$ i suposem $E(a) = E(b)$. Llavors $[\langle a, 1\rangle] = [\langle b, 1\rangle] \Rightarrow a = b$.

1. $E(a+b) = [\langle a+b, 1\rangle] = [\langle a, 1\rangle] +_{\mathbb{Q}} [\langle b, 1\rangle] = E(a) +_{\mathbb{Q}} E(b)$.
2. $E(ab) = [\langle ab, 1\rangle] = [\langle a, 1\rangle] \cdot_{\mathbb{Q}} [\langle b, 1\rangle] = E(a) \cdot_{\mathbb{Q}} E(b)$.
3. $E(0) = [\langle 0, 1\rangle] = 0_{\mathbb{Q}}$.
4. $E(1) = [\langle 1, 1\rangle] = 1_{\mathbb{Q}}$.
5. $E(a) <_{\mathbb{Q}} E(b) \Leftrightarrow [\langle a, 1\rangle] <_{\mathbb{Q}} [\langle b, 1\rangle] \Leftrightarrow a < b$.

□

Observació 4.27. $[\langle a, b\rangle] = E(a) \div E(b)$, ja que $E(a) \div E(b) = [\langle a, 1\rangle] \div [\langle b, 1\rangle] = [\langle a, 1\rangle] \cdot_{\mathbb{Q}} [\langle 1, b\rangle] = [\langle a, b\rangle]$.

5 Els nombres reals

El darrer pas en aquesta part és definir el conjunt dels nombres reals com a ordre continu lineal a partir dels racionals mitjançant talls de Dedekind. Un cop presentades les operacions aritmètiques bàsiques, a la segona part del treball podrem considerar els reals com a cos ordenat i complet, i també estudiar-lo des d'un punt de vista topològic.

5.1 Ordres lineals densos

Definició 5.1. Un conjunt totalment ordenat $\langle A, <\rangle$ és *dens* si i només si A té com a mínim dos elements i cap element de A no té ni successor ni predecessor immediat:

$$\forall x, y \in A(x < y \to (\exists z \in A)(x < z < y)).$$

Observacions 5.2. $\mathbb{Q}$ és un ordre lineal dens.

Definició 5.3. Sigui $\mathbb{A} = \langle A, <\rangle$ un ordre lineal i $X \subseteq A$. Tenim les següents definicions:

1. Si el conjunt de fites superiors de X en $\mathbb{A}$ té un element mínim, direm que és el *suprem* de X en $\mathbb{A}$. Escriurem $\sup^{\mathbb{A}} X$.
2. Si el conjunt de fites inferiors de X en $\mathbb{A}$ té màxim, aquest s'anomena l'*ínfim* de X en $\mathbb{A}$ i es representa per $\inf^{\mathbb{A}} X$.

Definició 5.4. Sigui $\mathbb{A} = \langle A, <\rangle$ un ordre lineal. Diem que un subconjunt B de A és *dens en* $\mathbb{A}$ si i només si $\forall x, y \in A(x < y \to (\exists b \in B)(x < b < y))$.

Introduïm el concepte d'isomorfisme parcial per demostrar un resultat important. Durant la resta d'aquesta subsecció considerarem $\langle P, <\rangle$ i $\langle Q, \prec\rangle$ dos ordres lineals densos numerables i sense extrems.

Definició 5.5. Direm que una funció h d'un subconjunt de P en Q és un *isomorfisme parcial* de P a Q si per tots $p, p' \in \mathrm{dom}(h)$ es compleix que $p < p'$ si i només si $h(p) \prec h(p')$.

Lema 5.6. *Si h és un isomorfisme parcial de P a Q amb dom(h) finit i $p \in P, q \in Q$, aleshores existeix un isomorfisme parcial $h_{p,q}$ tal que $h \subseteq h_{p,q}$, $p \in dom(h_{p,q})$ i $q \in ran(h_{p,q})$.*

Demostració. Com que P i Q són numerables, podem posar $P = \langle p_n : n \in \omega \rangle$ i $Q = \langle q_n : n \in \omega \rangle$. Sigui $h = \{(p_{i_1}, q_{i_1}), \ldots, (p_{i_k}, q_{i_k})\}$ amb $p_{i_1} < p_{i_2} < \cdots < p_{i_k}$. Per definició d'isomorfisme parcial, també tenim $q_{i_1} \prec q_{i_2} \prec \cdots \prec q_{i_k}$.

Si $p \notin \text{dom}(h)$, o bé $p < p_{i_1}$, o bé $p_{i_e} < p < p_{i_{e+1}}$ per algun $1 \leq e < k$, o bé $p_{i_k} < p$. Prenem el menor natural n tal que q_n estigui en la mateixa relació respecte de $q_{i_1}, \ldots, q_{i_k}$ que p amb $p_{i_1}, \ldots, p_{i_k}$. Això vol dir:

- Si $p < p_{i_1}$, llavors $q_n \prec q_{i_1}$;
- Si $p_{i_e} < p < p_{i_{e+1}}$, llavors $q_{i_e} \prec q_n \prec q_{i_k}$;
- Si $p_{i_k} < p$, llavors $q_{i_k} \prec q_n$.

Aquesta tria és possible perquè $\langle Q, \prec \rangle$ és dens i sense extrems. Clarament $h' = h \cup \{(p, q_n)\}$ és un isomorfisme parcial. Si $q \in \text{ran}(h)$, ja hem acabat. Si $q \notin \text{ran}(h)$, podem fer servir un argument anàleg al previ per veure que existeix $p_m \in P$ de manera que $h' \cup \{(p_m, q)\}$ és un isomorfisme parcial. Prenem el mínim m que ho compleixi i sigui $h_{p,q} = h' \cup \{(p_m, q)\}$. Hem demostrat el lema. □

Teorema 5.7. (Cantor) *$\langle P, < \rangle$ i $\langle Q, \prec \rangle$ són isomorfs.*

Demostració. Prenem la notació del lema i demostració previs. Construirem la següent successió d'isomorfismes parcials per recursivitat:

$$h_0 = \emptyset,$$
$$h_{n+1} = (h_n)_{p_n, q_n},$$

on $(h_n)_{p_n,q_n}$ és l'extensió de h_n (donada pel lema anterior) tal que $p_n \in \text{dom}((h_n)_{p_n,q_n})$ i $q_n \in \text{ran}((h_n)_{p_n,q_n})$. Sigui $h = \bigcup_{n \in \omega} h_n$. És trivial comprovar que $h : P \to Q$ és un isomorfisme entre $\langle P, < \rangle$ i $\langle Q, \prec \rangle$. □

5.2 Els nombres reals a partir de talls de Dedekind

Amb la construcció realitzada de $\mathbb{Q}$, podem pensar que falta "alguna cosa". Per exemple, podem observar que no existeix cap racional x que compleixi $x^2 = 2$, o bé que no existeix cap racional de la forma $0.a_1a_2a_3...$, on la successió decimal no és ni finita ni eventualment periòdica. En altres paraules, $\mathbb{Q}$ té forats. Formalitzem aquest concepte.

Definició 5.8. Sigui $\langle P, < \rangle$ un ordre lineal. Un *forat* és un parell de conjunts (A, B) de manera que

1. A i B són subconjunts disjunts no buits de P i $A \cup B = P$.
2. Si $a \in A$ i $b \in B$, llavors $a < b$.
3. A no té màxim i B no té mínim.

Exemple 5.9. El parell (A, B), amb $B = \{x \in \mathbb{Q} : 0 < x \text{ i } 2 < x^2\}$ i $A = \mathbb{Q} \setminus B$, és un forat en $\mathbb{Q}$.

Definició 5.10. Diem que un ordre lineal $\langle P, < \rangle$ és *complet* si tot subconjunt no buit $S \subseteq P$ afitat superiorment té suprem.

Observació 5.11. Un ordre lineal $\langle P, < \rangle$ és complet si i només si tot subconjunt no buit $S \subseteq P$ afitat inferiorment té ínfim.

Proposició 5.12. *$\langle P, < \rangle$ és complet si i només si no té forats.*

Demostració. Veurem les dues implicacions per contrarecíproc. En primer lloc, sigui (A, B) un forat en P. Observem que A està afitat superiorment per qualsevol $b \in B$. Demostrem, doncs, que A no té suprem. Si c fos el suprem de A, per la definició de forat i de suprem, o bé c seria el màxim de A, o el mínim de B, però cap d'aquests existeix.

Per veure la implicació contrària, sigui $S \subseteq P$ un conjunt no buit afitat superiorment que no té suprem. Veurem que P té un forat. Siguin $A = \{x \in P : \exists s \in S(x \leq s)\}$ i $B = \{x \in P : \forall s \in S(s < x)\}$. Veiem que (A, B) és un forat. Com que S no és buit, tant A com B són no buits. A més, són clarament disjunts i $A \cup B = P$. Per comprovar la segona condició, si $a \in A$ i $b \in A$, aleshores existeix $s \in S$ tal que $a \leq s$ i, per aquest s, es compleix també $s < b$. Per tant, $a < b$. Finalment, si existís el mínim de B o el màxim de A, aquest hauria de ser el suprem de S, que hem suposat que no existeix. □

Com hem vist, no tots els ordres lineals densos són complets. Com a contraexemple tenim el conjunt dels racionals. El nostre proper objectiu és veure que, tot i així, tot ordre lineal dens pot ser completat "omplint els forats" i que el resultat obtingut és únic.

Definició 5.13. Definim una *compleció* d'un ordre lineal dens sense màxim ni mínim $\langle P, < \rangle$ com l'ordre lineal complet $\langle C, \prec \rangle$ tal que:

1. $P \subseteq C$.
2. $\prec \cap (P \times P) = <$.
3. P és dens en C.
4. C no té màxim ni mínim.

Teorema 5.14. *Amb les condicions de la definició prèvia, existeix una compleció per a $\langle P, < \rangle$ que és, a més, única a nivell d'isomorfisme.*

Abans de demostrar aquest resultat, caldrà donar algunes definicions prèvies.

Definició 5.15. Un *tall* és un parell (A, B) de conjunts de manera que

1. A i B són conjunts disjunts no buits de P i $A \cup B = P$.
2. Si $a \in A$ i $b \in B$, llavors $a < b$.

Així doncs, un tall (A, B) és també un forat si, a més, A no té màxim i B no té mínim. A més, com que P és dens, no poden existir alhora el màxim de A i el mínim de B. Això ens dona tres tipus de talls diferents i excloents entre sí:

- Forats.
- Talls de manera que A té màxim i B no té mínim.
- Talls de manera que A no té màxim i B té mínim.

En qualsevol dels dos darrers casos, A té suprem. A partir d'ara, ens centrarem en un d'ells per simplificar la nostra feina.

Definició 5.16. Un tall (A, B) és un *tall de Dedekind* si A no té màxim element.

Observem aleshores que tenim dos tipus de talls de Dedekind: els forats, i aquells en què $B = \{x \in P : p \leq x\}$ per algun $p \in P$. En aquest darrer cas, escriurem $(A, B) = [p]$.

Tenim ara les eines necessàries per demostrar el **Teorema 5.14**.

Demostració. Unicitat. Siguin $\langle C, \prec\rangle$ i $\langle C^*, \prec^*\rangle$ dues complecions de $\langle P, <\rangle$. Volem veure que existeix un isomorfisme $h : C \to C^*$ de manera que $h(x) = x$ per tota $x \in P$.

Establim qüestions de notació. Per a $c \in C$, sigui $S_c = \{p \in P : p \preceq c\}$. Anàlogament, per a $c^* \in C^*$, sigui $S_{c^*} = \{p \in P : p \preceq c^*\}$. Si S és un subconjunt no buit de P afitat superiorment, posarem $\sup(S)$ per referir-nos al suprem de S en $\langle C, \prec\rangle$, i $\sup^*(S)$ per referir-nos al suprem de S en $\langle C^*, \prec^*\rangle$ (tots dos existeixen perquè aquests ordres són complets). Observem que $\sup(S_c) = c$ i $\sup^*(S_{c^*}) = c^*$.

Definim ara la funció h com segueix: $\forall c \in C, h(c) = \sup^*(S_c)$. Clarament h és una funció entre ordres lineals. Per tant, només cal verificar tres punts:

(a) h és exhaustiva.

(b) Si $c \prec d$, aleshores $h(c) \prec^* h(d)$.

(c) $h(x) = x, \forall x \in P$.

Per veure (a), sigui $c^* \in C^*$ un element arbitrari. Aleshores $c^* = \sup^*(S_{c^*})$. Si posem $c = \sup(S_{c^*})$, llavors $S_c = S_{c^*}$ i $c^* = h(c)$. Per (b), si $c \prec d$, com que P és dens en C, existeix $p \in P$ de manera que $c \prec p \prec d$. D'aquí, $\sup^*(S_c) \prec^* p \prec^* \sup^*(S_d)$, és a dir, $h(c) \prec^* h(d)$. Per últim, sigui $x \in P$. Llavors, $x = \sup(S_x) = \sup^*(S_x) = h(x)$.

Existència. Aquí és on farem servir la idea dels talls de Dedekind. Considerem el conjunt C de tots els talls de Dedekind (A, B) en $\langle P, <\rangle$ i definim l'ordre

$$(A, B) \prec (A', B') \quad \Leftrightarrow \quad A \subsetneq A'.$$

Clarament, $\prec$ és una relació irreflexiva i transitiva. Pel punt 2. de la definició de tall, l'ordre és total. Així, $\langle C, \prec\rangle$ és un conjunt totalment ordenat. Recordem que posem $[p] = (A, B)$, on (A, B) és el tall de Dedekind tal que $B = \{x \in P : p \leq x\}$. Aleshores, si $p, q \in P$ compleixen $p < q$, tenim $[p] \prec [q]$. Això ens defineix un isomorfisme entre els ordres lineals $\langle P, <\rangle$ i $\langle P', \prec\rangle$, on $P' = \{[p] : p \in P\}$. N'hi ha prou amb veure, doncs, que $\langle C, \prec\rangle$ és una compleció de $\langle P', \prec\rangle$. Veiem les condicions que encara no hem verificat:

1. És evident que $P' \subseteq C$.
2. L'ordre en P' i C és el mateix, de manera que aquesta condició també és immediata.

3. Veiem que P' és dens en C. Siguin $(A,B),(A',B') \in C$ tals que $(A,B) \prec (A',B')$, és a dir, $A \subsetneq A'$. Sigui $p \in P$ tal que $p \in A'$ però $p \notin A$. Podem assumir que p no és el mínim de B. Aleshores $(A,B) \prec [p] \prec (A',B')$. Així, P' és dens en C.

4. El següent pas és veure que C no té extrems. Si tenim $(A,B) \in C$, existeix $p \in B$ que no és el mínim de B, de manera que $(A,B) \prec [p]$. Llavors C no té màxim. Anàlogament, si prenem $q \in A$, llavors $[q] \prec (A,B)$ i C no té mínim.

5. Demostrem per acabar que $\langle C, \prec \rangle$ és complet. Sigui S un subconjunt no buit de C afitat superiorment. Volem veure que S té suprem en C. Existeix $(A_0,B_0) \in C$ tal que $(A,B) \preceq (A_0,B_0)$ per tot $(A,B) \in S$, és a dir, tal que $A \subseteq A_0$ per tot $(A,B) \in S$. Siguin

$$A_S = \bigcup\{A : (A,B) \in S\} \quad \text{i} \quad B_S = P \setminus A_S = \bigcap\{B : (A,B) \in S\}.$$

Tant A_S com B_S són no buits i $A_S \cup B_S = P$. A més, per tots $a \in A_S$ i $b \in B_S$ es compleix $a \prec b$. O sigui, (A_S,B_S) és un tall. En particular, com que cap A té màxim, A_S tampoc en té i (A_S,B_S) és un tall de Dedekind.

Per tot $(A,B) \in S$ es compleix $A \subseteq A_S$, de manera que (A_S,B_S) és una fita superior de S. Mostrem ara que és la mínima. Si (A',B') és una fita superior de S qualsevol, llavors $A \subseteq A'$ per tot $(A,B) \in S$ i, aleshores, $A_S = \bigcup\{A : (A,B) \in S\} \subseteq A'$. Per tant, $(A_S,B_S) \preceq (A',B')$ i (A_S,B_S) és el suprem de S. Queda vist, doncs, que C és complet.

□

Un cop hem vist aquest teorema de forma general, ens podem centrar en el cas que ens interessa. El conjunt dels racionals, junt amb el seu ordre, que denotarem simplement per $<$ a partir d'ara, com que és un ordre lineal dens sense extrems, té una compleció única (mòdul isomorfisme).

Definició 5.17. Denotarem per $\langle \mathbb{R}, < \rangle$ la compleció de $\langle \mathbb{Q}, < \rangle$. L'anomenarem *conjunt dels nombres reals*.

De fet, havent vist la unicitat de complecions, junt amb el **Teorema 5.7**, sabem que tots els ordres lineals densos sense extrems i separables (és a dir, que contenen un ordre lineal dens numerable) són isomorfs entre sí (Teorema de Cantor). En particular, són isomorfs als reals. A aquesta estructura l'anomenarem *continu lineal*.

5.3 Operacions aritmètiques en $\mathbb{R}$

Al llarg d'aquest apartat, com hem fet prèviament, simplificarem la notació de les operacions en $\mathbb{Q}$ fent servir simplement $+$ i $\cdot$. També farem servir aquesta notació per a la suma i el producte que definirem en $\mathbb{R}$, i sabrem si estem fent una operació en $\mathbb{Q}$ o en $\mathbb{R}$ pel context. Comencem definint la suma de reals.

Definició 5.18. Siguin $x, y \in \mathbb{R}$. Definim la *suma de reals* com

$$x + y = \inf\{r + s : r, s \in \mathbb{Q}, x \leq r, y \leq s\}.$$

Observació 5.19. Aquest ínfim existeix perquè el conjunt no buit al qual fa referència està afitat inferiorment (per qualssevol $p, q \in \mathbb{Q}$ de manera que $p < x$ i $q < y$). A més, si $x, y \in \mathbb{Q}$, aquesta definició dona exactament la suma en els racionals.

Donem un resultat auxiliar que farem servir en la demostració següent.

Lema 5.20. *Per a tot $x \in \mathbb{R}$ i tot $n \in \omega \setminus \{0\}$, existeixen $r, s \in \mathbb{Q}$ de manera que $r < x \leq s$ i $s - r \leq 1/n$.*

Demostració. Fixem $r_0, s_0 \in \mathbb{Q}$ de manera que $r_0 < x < s_0$ i $k \in \omega \setminus \{0\}$ tal que $k > n(s_0 - r_0)$. Considerem la successió creixent finita de racionals $\langle r_i \rangle_{i=0}^{k}$, on $r_i = r_0 + i/n$. Sigui j l'índex més gran de manera que $r_j < x$. Necessàriament $j < k$. Tenim llavors $r_j < x \leq r_{j+1}$ i $r_{j+1} - r_j = 1/n$. Prenem, doncs, $r = r_j$ i $s = r_{j+1}$. □

Lema 5.21. *Per $x, y, z \in \mathbb{R}$, es compleix*

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

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

(c) $x + 0 = x$.

(d) *Existeix un únic $w \in \mathbb{R}$ tal que $x + w = 0$, que és l'invers additiu de x, i que denotarem per $-x$.*

(e) *Si $x < y$, aleshores $x + z < y + z$.*

Demostració. Els apartats (a), (b) i (c) són evidents a partir dels resultats anàlegs per als racionals.

(d) Sigui $x = \inf\{s \in \mathbb{Q} : x \leq s\} = \sup\{r \in \mathbb{Q} : r < x\}$. Sigui $w = \inf\{-r : r \in \mathbb{Q},\ r < x\}$. Llavors $x + w = \inf\{s - r : r, s \in \mathbb{Q},\ x \leq s, r < x\}$. Com que $r < x \leq s$, tenim $0 \leq x + w$. Suposem $0 < x + w$. Com que $\mathbb{Q}$ és dens en $\mathbb{R}$, existeix $n \in \omega \setminus \{0\}$ de manera que $1/n < x + w$. Però el **Lema 5.20** garanteix l'existència de $r, s \in \mathbb{Q}$ tals que $r < x \leq s$ i $s - r \leq 1/n$. Per tant, $x + w \leq 1/n$, que és una contradicció. Hem vist, doncs, l'existència de w amb $x + w = 0$. Si $v \in \mathbb{R}$ és tal que $x + v = 0$, fent servir els apartats previs, tenim $w = w + 0 = 0 + w = (v + x) + w = v + (x + w) = v + 0 = v$.

(e) Si $x < y$, com que $\{r + s : r, s \in \mathbb{Q}, y \leq r, z \leq s\}$ està afitat inferiorment, $x + z \leq y + z$. I si fos $x + y = y + z$, llavors $x = x + 0 = x + (z + (-z)) = (x + z) + (-z) = (y + z) + (-z) = y + (z + (-z)) = y + 0 = y$, que és una contradicció.

□

Procedim amb el producte. El definirem primer per a nombres reals positius, que són aquells que pertanyen al conjunt $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$.

Definició 5.22. Siguin $x, y \in \mathbb{R}^+$. Definim el *producte de reals positius* per

$$x \cdot y = \inf\{r \cdot s : r, s \in \mathbb{Q}, x \leq r, y \leq s\}.$$

Lema 5.23. *Siguin $x, y, z \in \mathbb{R}^+$. Llavors:*

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

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

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

(d) $x \cdot 1 = x$.

(e) *Existeix un únic $w \in \mathbb{R}^+$ de manera que $x \cdot w = 1$. El denotarem $w = 1/x$ i l'anomenarem invers multiplicatiu de x.*

(f) *Si $x < y$, aleshores $x \cdot z < y \cdot z$.*

Demostració. La prova de (a), (b), (c) i (d) s'obté de les propietats anàlogues en $\mathbb{Q}$.

(e) Sigui $x = \inf\{s \in \mathbb{Q} : x \leq s\} = \sup\{r \in \mathbb{Q} : r < x\}$. Sigui $1/x = \inf\{1/r : r \in \mathbb{Q},\ 0 < r < x\}$. Llavors $x \cdot 1/x = \inf\{s/r : r, s \in \mathbb{Q},\ 0 < r < x \leq s\}$. Com que $0 < r < x \leq s$, $1 \leq x \cdot 1/x$. Suposem $1 < x \cdot 1/x$ per arribar a una contradicció. Observem que:

1. $1/x = \sup\{1/s : s \in \mathbb{Q},\ x \leq s\}$, i
2. per a tot $r \in \mathbb{Q}$, $x \cdot 1/x = \sup\{r \cdot 1/x : r \in \mathbb{Q},\ r < x\}$.

Pel punt 2., existeix $r \in \mathbb{Q}$ tal que $1 < r \cdot 1/x$. Però llavors, per 1., existeix $s \in \mathbb{Q}$ de manera que $x \leq s$ i $r \cdot 1/s > 1$. Per tant, $r > s$, cosa que contradiu $r < x \leq s$.

(f) Anàlogament a la demostració feta per a la suma, tenim $x \cdot z \leq y \cdot z$, i si es complís la igualtat, aleshores $x = x \cdot 1 = x \cdot (z \cdot 1/z) = (x \cdot z) \cdot 1/z = (y \cdot z) \cdot 1/z = y \cdot (z \cdot 1/z) = y \cdot 1 = y$, contradicció (recordem que x, y, z són positius, per això podem prendre inversos).

□

Busquem ara ampliar la multiplicació a tots els nombres reals.

Definició 5.24. Definim el *valor absolut* $|x|$ de $x \in \mathbb{R}$ per

$$|x| = \begin{cases} -x & \text{si } -x \text{ és positiu,} \\ x & \text{altrament.} \end{cases}$$

Observació 5.25. Si $x \neq 0$, llavors $|x| \in \mathbb{R}^+$.

Definició 5.26. Per $x, y \in \mathbb{R}$, definim el *producte de reals* com

$$x \cdot y = \begin{cases} |x| \cdot |y| & \text{si } 0 < x, y, \text{ o bé } x, y < 0, \\ -(|x| \cdot |y|) & \text{si } 0 < x \text{ i } y < 0, \text{ o bé si } x < 0 \text{ i } 0 < y, \\ 0 & \text{si } x = 0 \text{ o } y = 0. \end{cases}$$

Lema 5.27. *Siguin $x, y, z \in \mathbb{R}$. Els punts* (a)-(d) *del* **Lema 5.23** *es compleixen en aquest cas també. Pel que fa a les altres dues propietats, tenim:*

(e) *Si $x \neq 0$, existeix un únic $w \in \mathbb{R}$ tal que $x \cdot w = 1$.*

(f) *Si $x < y$ i $z > 0$, aleshores $x \cdot z < y \cdot z$.*

La demostració és anàloga a la del **Lema 5.23**.

Definició 5.28. Definim la *divisió* d'un real x entre un real $y \neq 0$ com

$$x \div y = x \cdot (1/y).$$

Proposició 5.29. (Cantor) *El conjunt dels reals no és numerable.*

Demostració. Veurem que l'interval $(0,1) = \{x \in \mathbb{R} : 0 < x < 1\}$ no és numerable per contradicció. Suposem que $(0,1)$ és numerable. Sigui $f : \omega \to (0,1)$ una bijecció. Aleshores, per a tot $n \in \omega$, existeix una successió de decimals $a_{n,0}, a_{n,1}, \ldots$ que determinen la imatge de n per f:

$$\begin{array}{l} 0 \mapsto 0.\ a_{0,0}\ a_{0,1}\ a_{0,2}\ a_{0,3}\ a_{0,4}\ldots \\ 1 \mapsto 0.\ a_{1,0}\ a_{1,1}\ a_{1,2}\ a_{1,3}\ a_{1,4}\ldots \\ 2 \mapsto 0.\ a_{2,0}\ a_{2,1}\ a_{2,2}\ a_{2,3}\ a_{2,4}\ldots \\ 3 \mapsto 0.\ a_{3,0}\ a_{3,1}\ a_{3,2}\ a_{3,3}\ a_{3,4}\ldots \\ 4 \mapsto 0.\ a_{4,0}\ a_{4,1}\ a_{4,2}\ a_{4,3}\ a_{4,4}\ldots \\ \ldots \end{array}$$

Volem veure que, de fet, f no és una bijecció. En particular, demostrarem que no és exhaustiva. Cal trobar un element $b \in (0,1)$ que no pertanyi a la imatge de f. Observem abans que un mateix decimal pot ser representat de maneres diferents, per exemple $0.4999\cdots = 0.50000\ldots$, així que, en aquests casos, triarem la representació que acaba en infinits 0's.

Dit això, procedim a construir l'element b. Per a $i = 0$, anem a definir el primer dígit decimal del nostre número, que denotarem b_0. El triarem de manera que $b_0 \neq a_{0,0}$. Per fer-ho, prendrem $b_0 = 1$ si $a_{0,0} \neq 1$ i $b_0 = 2$ si $a_{0,0} = 1$. Seguim d'aquesta manera; per definir b_i, observem $a_{i,i}$, és a dir, el dígit número i de la representació decimal de $f(i)$. Si $a_{i,i}$ és diferent de 1, triem $b_i = 1$. Si no, $b_i = 2$. Amb aquest procés de diagonalització, queda definit

$$b = 0.\ b_0\ b_1\ b_2\ b_3\ b_4 ...$$

Afirmem ara que aquest número no pertany a la imatge de f. Si hi fos, tindríem $b = f(i)$ per algun $i \in \omega$. Però hem construït b de manera que l'i-èssim dígit decimal de b és diferent de l'i-èssim dígit decimal de $f(i)$. Per tant, són nombres diferents. Així, b no és a la nostra llista, f no és una bijecció, i $(0,1) \subseteq \mathbb{R}$ no és numerable. Per tant, $\mathbb{R}$ tampoc ho és. □

Proposició 5.30. *El conjunt dels nombres reals, junt amb les operacions de suma i producte, el 0 i l'1, forma un cos ordenat complet.*

Demostració. La completesa ve donada per la construcció del continu lineal que hem donat.

Per veure que es tracta d'un cos, cal veure que que la suma i el producte són operacions associatives, commutatives, que tenen elements neutres respectius, que $\mathbb{R}$ és tancat

respecte d'aquestes operacions, que els reals tenen inversos additius, que els reals diferents de zero tenen inversos multiplicatius, i que el producte és distributiu respecte de la suma.

Per definició, $\mathbb{R}$ és tancat sota les dues operacions. Totes les altres propietats s'han verificat prèviament (**Lema 5.21**, **Lema 5.23** i **Lema 5.27**).

Queda veure que el cos és ordenat, és a dir, que les operacions respecten l'ordre total que hem presentat. Això ha quedat demostrat als apartats (e) i (f), respectivament, dels lemes de la suma i el producte que acabem de mencionar. □

Observació 5.31. Tots els cossos ordenats complets són isomorfs entre sí, de manera que $\mathbb{R}$ és únic mòdul isomorfisme.

5.4 Ampliació als nombres complexos

Un cop definits els nombres reals, podem estendre'ls als complexos.

Definició 5.32. Definim el nombre imaginari i com aquell que compleix $i^2 = -1$.

Definició 5.33. Definim el conjunt dels *nombres complexos* com el conjunt de parells ordenats de reals, $\mathbb{C} = \{\langle a, b\rangle : a, b \in \mathbb{R}\}$. Representarem $z = \langle a, b\rangle \in \mathbb{C}$ per $z = a + ib$. A més, definim la seva *part real* per $\mathrm{Re}(z) = a$, i la seva *part imaginaria* per $\mathrm{Im}(z) = b$.

Podem definir la suma i el producte de complexos com segueix.

Definició 5.34. Definim la *suma de complexos* per a $z = a + ib$ i $w = c + id$ com

$$z +_{\mathbb{C}} w = (a + c) + i(b + d).$$

Definició 5.35. Definim el *producte de complexos* $z = a + ib$ i $w = c + id$ per

$$z \cdot_{\mathbb{C}} w = (a \cdot c - b \cdot d) + i(b \cdot c + a \cdot d).$$

Els nombres complexos tenen les mateixes propietats d'addició i multiplicació que els reals (commutativitat, etc.), i totes elles s'obtenen a partir de les anàlogues en $\mathbb{R}$.

Observació 5.36. No podem establir un ordre total en $\mathbb{C}$ que respecti l'ordre de les operacions que hem definit.

Demostració. Suposem que $\prec$ és un ordre total en $\mathbb{C}$ que respecta la suma i el producte de complexos. Veiem primer que $0 \prec 1$. Si fos $1 \prec 0$, aleshores $1 - 1 \prec 0 - 1$, de manera que $0 \prec -1$, d'on $0 \cdot (-1) \prec (-1) \cdot (-1)$, i d'aquí $0 \prec 1$, que és una contradicció. Ha de ser $0 \prec 1$. A més, com que $0 - 1 \prec 1 - 1$, també tenim $-1 \prec 0$. D'altra banda, sabem que $0 \neq i$ perquè $0 \cdot 0 \neq -1$. Aleshores o bé $i \prec 0$, o bé $0 \prec i$.

Suposem $0 \prec i$. Llavors $0 \cdot i \prec i \cdot i$, de manera que $0 \prec -1$, que contradiu $-1 \prec 0$. Per contra, suposem $i \prec 0$. Aleshores $i - i \prec 0 - i$ i $0 \prec -i$. D'aquí, $0 \cdot (-i) \prec (-i) \cdot (-i)$, d'on $0 \prec -1$, que contradiu $-1 \prec 0$. En qualsevol cas, doncs, s'arriba a una contradicció.

□

Els complexos, junt amb la suma i el producte, formen un cos complet. A més, es tracta d'un cos *algebraicament tancat*, és a dir, de manera que tot polinomi no-constant en $\mathbb{C}$ té com a mínim una arrel en $\mathbb{C}$.

Part II

Propietats del continu

6 Algunes propietats inicials

6.1 Teoria de cossos ordenats complets

Com hem vist a la secció dels nombres reals, $\mathbb{R}$ junt amb la suma, el producte, 0 i 1, és un cos ordenat complet. Veiem a continuació un teorema que tracta la decidibilitat de la teoria d'aquest tipus de cossos. Recordem que un sistema formal és decidible si per cada sentència en el llenguatge del sistema podem determinar per mitjà d'un mètode efectiu si aquesta pertany o no al conjunt de veritats del sistema.

Teorema 6.1. (Teorema de Tarski) *La teoria de cossos ordenats complets és decidible.*

La prova completa d'aquest teorema es pot trobar a [8] o [9]. Aquí només en presentarem la idea.

Demostració. (*Idea*) Sigui T la teoria de cossos ordenats complets i $\mathcal{L}_T$ el llenguatge associat a aquesta. L'objectiu és demostrar que podem aplicar *eliminació de quantificadors* en T. En altres paraules, cal veure que per tota fórmula $\varphi \in \mathcal{L}_T$, existeix una fórmula φ^* que no té quantificadors i tal que $T \vdash \varphi \leftrightarrow \varphi^*$.

Un cop demostrat això, com que φ^* no té quantificadors, serà veritat en un model de T si i només si ho és en qualsevol altre, cosa que es demostra per inducció sobre la complexitat de la fórmula. Per tant, com que $\varphi \equiv \varphi^*$, prenent un model adequat podrem veure si φ és veritat en qualsevol cas. □

A [9] també podem trobar que la teoria de cossos algebraicament tancats (com els complexos) també accepta eliminació de quantificadors.

6.2 La propietat arquimediana

La següent proposició, també coneguda com a axioma d'Arquimedes, ens indica que el conjunt dels nombres naturals no està afitat en els reals.

Proposició 6.2. *Sigui $x \in \mathbb{R}$. Aleshores existeix $n \in \omega$ de manera que $x < n$.*

Aquesta propietat es pot demostrar en ZFC amb la construcció que hem fet fins ara.

Demostració. Sigui $x \in \mathbb{R}$ i $S = \{a \in \omega : a \leq x\}$. Suposem $S = \emptyset$. Aleshores ha de ser $x < 0$. Per tant, $0 \in \omega$ és un natural més gran que x.

En canvi, si $S \neq \emptyset$, tenim que S està afitat superiorment (per x, per exemple). Per tant, per completesa, S té suprem en $\mathbb{R}$. Sigui $y = \sup(S)$. Considerem ara $y - 1$. Com que y és el suprem de S, $y - 1$ no pot ser una fita superior de S. Per tant, existeix $m \in S$ tal que $y - 1 < m$. Així, $y < m + 1$. D'aquí, $m + 1 \notin S$, de manera que $x < m + 1$. □

Els conjunt dels nombres reals constitueix un cos arquimedià. Un cos ordenat que no tingui la propietat arquimediana serà un *cos no-arquimedià*. A l'apartat següent donarem un exemple de cos no-arquimedià.

6.3 Models no-estàndard

Fem servir el terme *model estàndard de l'aritmètica* per parlar dels nombres naturals estàndard $(0, 1, 2, \dots)$. Un model de l'aritmètica de Peano qualsevol està totalment ordenat, satisfà els axiomes de l'aritmètica Peano i té un segment inicial isomorf a ω.

Definició 6.3. Un *model no-estàndard* és aquell que té elements addicionals fora d'aquest segment inicial.

La construcció d'aquests models ve del matemàtic Thoralf Skolem (1934). Amb l'ajuda del següent teorema demostrarem l'existència d'aquests models construint-ne un. Donem abans una definició.

Definició 6.4. Una sentència φ de primer ordre és *satisfactible* si existeix un model M del llenguatge de φ que satisfà φ, és a dir, de manera que φ és verdadera en M.

Teorema 6.5. (Teorema de compacitat de la lògica de primer ordre) *Tot conjunt de fórmules de primer ordre que sigui finitament satisfactible, és a dir, tal que tot subconjunt finit d'aquest és satisfactible, és també satisfactible.*

Partint de l'aritmètica de Peano, afegim una constant c al llenguatge i considerem el conjunt d'axiomes següent:

$$\begin{gathered} 0 < c \\ 1 < c \\ 2 < c \\ \dots \end{gathered}$$

Observem que aquest conjunt és finitament satisfactible, atès que podem interpretar c com un nombre natural suficientment gran. Per tant, pel teorema de compacitat, ha de ser satisfactible. Hem obtingut, doncs, un model de l'aritmètica de Peano en el qual existeix un element c més gran que tots els nombres estàndard.

Fent servir aquesta idea, podem construir també un cos ordenat no-arquimedià, és a dir, que no compleixi la propietat arquimediana. Anàlogament al que acabem de veure, podem partir de la teoria dels reals i afegir la constant c al llenguatge, junt amb els axiomes

$$\begin{gathered} 0 < c \\ 1 < c \\ 2 < c \\ \dots \end{gathered}$$

Aplicant compacitat novament, obtenim un model de la teoria de cossos ordenats que no és arquimedià, ja que la interpretació de c és més gran que 0, més gran que 1, etcètera.

7 Estructura del continu

A continuació, seguirem el nostre estudi dels nombres reals veient-los com a ordre lineal complet, dens, separable i sense extrems. És natural fer-se preguntes sobre l'estructura del continu. Per exemple, quina és la seva cardinalitat? Algunes qüestions com aquesta no tenen resposta en la teoria axiomàtica de ZFC, amb la qual hem treballat fins ara, és a dir, que són independents de ZFC.

7.1 Espais polonesos

Definició 7.1. Un *espai polonès* és un espai topològic homeomorf a un espai mètric complet i separable.

En particular, $\mathbb{R}$ és un espai polonès amb la topologia natural generada per intervals oberts de $\mathbb{Q}$ i la distància en la recta real com a mètrica. Sovint convindrà treballar amb espais relacionats amb $\mathbb{R}$ per determinar-ne algunes propietats; per exemple, amb espais gairebé homeomorfs a $\mathbb{R}$, ja que les imatges homeomorfes d'alguns subconjunts de $\mathbb{R}$ tenen representacions fàcils de tractar en espais adequats. Veiem-ne un exemple.

Definició 7.2. L'*espai de Baire* $\mathcal{N}$ és el conjunt ω^ω de funcions de ω a ω, vist com a espai producte amb la topologia del producte, on ω té la topologia discreta. Es tracta del conjunt de totes les successions infinites de nombres naturals.

$\mathcal{N}$ és un espai separable, complet i homeomorf als irracionals (per tant, gairebé homeomorf als reals excepte pel subconjunt numerable dels racionals). Això es pot veure a [7] (capítol VII, secció 3). En aquest mateix llibre es donen més detalls generals sobre aquest tema, tant al capítol esmentat com a l'anterior. La mètrica que se sol fer servir per a $\mathcal{N}$ és:

$$d(a,b) = \begin{cases} 0 & \text{si } a = b, \\ \frac{1}{\min\{n : a(n) \neq b(n)\}+1} & \text{si } a \neq b. \end{cases}$$

Tant $\mathbb{R}$ com l'espai de Baire $\mathcal{N}$ són espais polonesos importants. Un altre espai polonès que més endavant farem servir és l'*espai de Cantor* 2^ω, vist com a espai producte amb la topologia del producte, on $2 = \{0, 1\}$ té la topologia discreta. És una abstracció topològica del *conjunt de Cantor* $\mathcal{C}$.

7.2 Jerarquies

Per poder seguir amb el nostre estudi, convindrà classificar els subconjunts de $\mathbb{R}$ per complexitat topològica. Ho farem inicialment a partir de la *jerarquia de Borel*.

Definició 7.3. Un *conjunt de Borel* d'un espai polonès X és un conjunt generat a partir dels oberts de X amb les operacions d'unió numerable i complementari en un nombre numerable de passos.

A cada conjunt de Borel se li pot assignar un únic ordinal numerable, que serà el seu *rang*. La jerarquia de Borel s'obté mitjançant una classificació dels conjunts de Borel d'un espai polonès. Com que $\mathbb{R}$ és un espai polonès, se li pot aplicar aquesta classificació. Expliquem a continuació com es construeix aquesta estratificació.

La *jerarquia de Borel* en un espai polonès X consisteix en classes Σ^0_α, Π^0_α i Δ^0_α per cada ordinal numerable α més gran que 0. Els elements d'aquestes classes són subconjunts de X i les classes venen definides inductivament per les següents regles. Sigui A un subconjunt de X. Aleshores:

- A és Σ^0_1 si i només si és obert.
- A és Π^0_α si i només si el seu complementari és Σ^0_α.
- A és Σ^0_α per a $\alpha > 1$ si i només si existeix una successió numerable de conjunts $A_1, A_2, ...$ de manera que cada A_i és $\Pi^0_{\alpha_i}$ per a $\alpha_i < \alpha$, i $A = \bigcup A_i$.
- A és Δ^0_α si i només si també és Σ^0_α i Π^0_α.

Definició 7.4. Un conjunt de Borel té *rang finit* si és Σ^0_α, per algun ordinal finit α. Si no, diem que té *rang infinit*.

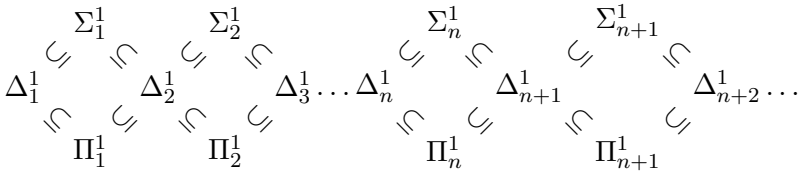
Exemples 7.5.

1. Σ^0_1 és la classe dels conjunts oberts.
2. Π^0_1 és la classe dels conjunts tancats.
3. Σ^0_2 és la classe de les unions numerables de conjunts tancats. També se li diu F_σ.
4. Π^0_2 és la classe de les interseccions numerables de conjunts oberts. També es coneix com a G_δ.

Podem estendre aquesta classificació més enllà dels conjunts de Borel, obtenint així els analítics, co-analítics, etc. Parlarem de la *jerarquia projectiva*. Els conjunts projectius en un espai polonès no numerable X són els conjunts que pertanyen a una de les següents classes:

- Δ^1_1, la classe dels conjunts de Borel.
- Σ^1_1, la classe dels *conjunts analítics*, és a dir, de les imatges contínues de conjunts de Borel d'un altre conjunt polonès Y.
- Π^1_1, la classe dels *conjunts co-analítics*, és a dir, dels complementaris dels conjunts analítics.
- Σ^1_{n+1}, la classe de les imatges contínues de conjunts Π^1_n en un conjunt polonès Y.
- Π^1_n, la classe dels complementaris dels conjunts en Σ^1_n.
- $\Delta^1_n = \Sigma^1_n \cap \Pi^1_n$.

Observació 7.6. Tenim algunes inclusions entre classes:



8 Propietats de regularitat

Estudiar l'estructura del continu vol dir, principalment, estudiar els seus subconjunts. Estudiarem, doncs, algunes propietats que poden tenir els conjunts de nombres reals. Veurem com es comporten certs conjunts de reals, o d'espais polonesos en general, segons el cas, pel que fa a diverses propietats de regularitat, com ara la propietat del conjunt perfecte, la mesura de Lebesgue o la propietat de Baire.

8.1 Cardinalitat del continu

Un dels problemes més bàsics que ens podem plantejar és el de la cardinalitat de $\mathbb{R}$. Comencem amb alguns conceptes previs. En primer lloc, recordem la definició de conjunt ben ordenat que hem donat en apartats anteriors.

Definició 8.1. Un *bon ordre* en un conjunt A és un ordre total $<$ en A amb el qual qualsevol subconjunt no buit de A té mínim. Diem llavors que $\mathbb{A} = \langle A, < \rangle$ és un *conjunt ben ordenat* si i només si $<$ és un bon ordre en A.

Axioma 8.2. (*Teorema del bon ordre*) Tot conjunt es pot ordenar bé.

Proposició 8.3. *L'axioma d'elecció i el teorema de bon ordre són equivalents.*

La prova es pot trobar al llibre [4] (capítol 8, secció 1).

A tot conjunt ben ordenat se li pot assignar un cardinal. Per l'axioma d'elecció, tot conjunt està ben ordenat. Per tant, tot subconjunt de $\mathbb{R}$ és bijectable amb un únic cardinal, que serà la seva *cardinalitat*. Denotarem la cardinalitat d'un conjunt A per $|A|$.

Proposició 8.4. $\mathbb{R}$ *té la mateixa cardinalitat que el conjunt potència dels naturals, és a dir,* $|\mathbb{R}| = |\mathcal{P}(\omega)|$. *A més, pel* Teorema de Cantor*, aquesta és* $|\mathcal{P}(\omega)| = 2^{\omega}$.

Podem trobar la demostració a [2] (capítol 6).

Axioma 8.5. (*Hipòtesi del continu*) No existeixen conjunts de cardinalitat intermèdia entre la dels naturals i la dels reals. En altres paraules, tot subconjunt infinit dels nombres reals és o bé numerable, o bé de la mateixa cardinalitat que $\mathbb{R}$.

Com sabem, la cardinalitat de conjunts finits es representa amb un nombre natural, la quantitat d'elements que té el conjunt. Per a conjunts infinits, fem servir el símbol $\aleph$ junt amb un subíndex ordinal. El cardinal infinit més petit, $\aleph_0$, representa la cardinalitat dels nombres naturals. Així, qualsevol conjunt infinit numerable té cardinalitat $\aleph_0$. El següent cardinal infinit és $\aleph_1$.

Aleshores, la hipòtesi del continu (CH) afirma que $2^{\aleph_0} = \aleph_1$ i que, per tant, no existeix cap $X \subseteq \mathbb{R}$ tal que $\aleph_0 < |X| < \aleph_1$. Kurt Gödel (1940) va demostrar que CH no es pot refutar en ZF ni en ZFC. D'altra banda, Paul Cohen (1963) va demostrar que CH no es pot demostrar a partir de ZFC. D'aquí s'obté que CH és independent de la teoria axiomàtica ZFC.

8.2 Mesurabilitat de Lebesgue

Definició 8.6. Un subconjunt de reals A és *de mesura zero* o *nul·la* si per tota $\epsilon > 0$ existeix una successió d'intervals $\{I_n\}_{n\in\omega}$ de manera que $A \subseteq \bigcup I_n$ i $\sum |I_n| < \epsilon$, on $|I_n|$ representa la llargada de l'interval I_n.

Definició 8.7. Un subconjunt de reals A és *Lebesgue-mesurable* si difereix d'un conjunt de Borel per un conjunt de mesura zero. En altres paraules, si existeix un conjunt de Borel B de manera que $A \triangle B = (A \setminus B) \cup (B \setminus A)$ té mesura zero.

La *mesura de Lebesgue* és una manera estàndard d'assignar una mesura a subconjunts d'espais euclidians n-dimensionals. Per a $n = 1, 2, 3$ es correspon amb la llargada, l'àrea i el volum, respectivament. Assumim possible el valor infinit com a mesura de Lebesgue. Dues propietats de la mesura de Lebesgue que farem servir a la següent demostració són la monotonia i la invariància per translació.

Proposició 8.8. *Sota l'axioma d'elecció, existeixen conjunts de reals que no són Lebesgue-mesurables.*

Demostració. Veurem un conegut exemple, el del conjunt de Vitali (1905). Considerem l'interval tancat $[0, 1]$. Definim la relació $\sim$ per a $x, y \in [0, 1]$ com

$$x \sim y \quad \Leftrightarrow \quad x - y \in \mathbb{Q}.$$

És trivial veure que és una relació d'equivalència. Per tant, podem partir $[0, 1]$ en classes d'equivalència disjuntes de $\sim$. Una formulació equivalent de l'axioma d'elecció ens diu que, donat qualsevol conjunt X de conjunts disjunts no buits, existeix un conjunt C que conté exactament un element en comú amb cada un dels conjunts de X. Per tant, per AC, un cop feta la partició de $[0, 1]$, podem triar un representant de cada classe d'equivalència. Sigui A un conjunt de representants d'aquestes classes.

Considerem ara $\mathbb{Q} \cap [-1, 1]$. Com que es tracta d'un conjunt numerable, podem triar $\{r_i : i < \omega\}$ una enumeració d'aquest. Considerem ara la col·lecció de conjunts

$$\{A + r_i : i < \omega\},$$

on $A + r_i = \{y + r_i : y \in A\}$. Els conjunts d'aquesta col·lecció són disjunts entre sí. Per veure-ho, siguin $i, j \in \omega$ amb $i \neq j$ i suposem que $x \in (A + r_i) \cap (A + r_j)$. Aleshores existeixen $a, b \in A$ tals que $x = a + r_i$ i $x = b + r_j$. Per tant, $a - b = r_j - r_i \neq 0$. Com que $r_j - r_i \in \mathbb{Q}$, a i b són de la mateixa classe d'equivalència. Però això és una contradicció amb la definició de A.

Suposem ara que A és Lebesgue-mesurable per tal d'arribar a una contradicció. Aleshores també els $A + r_i$ són Lebesgue-mesurables. A més, si $m(X)$ representa la mesura de Lebesgue d'un conjunt X, resulta que

$$m\left(\bigcup_{i=1}^{\omega}(A + r_i)\right) = \sum_{i=1}^{\omega} m(A + r_i) = \sum_{i=1}^{\omega} m(A) = \infty \cdot m(A).$$

Com que $A \subseteq [0, 1]$ i $-1 \leq r_i \leq 1$ per tota $i \in \omega$, tenim $A + r_i \subseteq [-1, 2]$. A més, si $x \in [0, 1]$, x pertany a una classe d'equivalència $[y]$ per algun $y \in N$. Així, existeix r_k tal que $x - r_k = y$. Així, $x = y + r_k$, de manera que $x \in A + r_k$. Per tant,

$$[0, 1] \subseteq \bigcup_{i=1}^{\omega}(A + r_i) \subseteq [-1, 2].$$

Per monotonia de la mesura de Lebesgue, doncs, obtenim

$$1 = m([0, 1]) \leq \infty \cdot m(A) \leq m([-1, 2]) = 3.$$

Però havíem suposat $0 \leq m(A)$, de manera que la desigualtat que acabem de deduir no és possible. Com que hem arribat a una contradicció, deduïm que A no és Lebesgue-mesurable. □

8.3 Propietat de Baire

La següent propietat de regularitat que veurem és la de Baire. Cal introduir abans el concepte de conjunt de primera categoria.

Definició 8.9. Diem que un subconjunt A d'un espai topològic X és un *conjunt magre* o un *conjunt de primera categoria* si és una unió numerable de subconjunts disseminats de X, és a dir, de subconjunts de X l'adherència dels quals és d'interior buit (també s'anomenen conjunts *no-densos enlloc*).

Definició 8.10. Un subconjunt A d'un espai topològic X té la *propietat de Baire* o és *gairebé obert* si difereix d'un conjunt obert per un conjunt magre. Això vol dir que existeix un conjunt obert $U \subseteq X$ tal que $A \triangle U = (A \setminus U) \cup (U \setminus A)$ és magre.

Teorema 8.11. *Amb AC, existeixen conjunts de* $\mathbb{R}$ *que no tenen la propietat de Baire.*

Demostració. Veurem de nou l'exemple del conjunt de Vitali que hem definit a l'apartat de conjunts Lebesgue-mesurables, modificant lleugerament la seva construcció.

Recordem que partim de la relació d'equivalència definida per a $x, y \in \mathbb{R}$ (no ens limitarem a l'interval $[0, 1]$ aquest cop) com

$$x \sim y \quad \Leftrightarrow \quad x - y \in \mathbb{Q}.$$

Sigui llavors A un conjunt que tingui exactament un representant de cada classe d'equivalència generada per $\sim$.

Per $x \in \mathbb{R}$, considerem $A + x = \{a + x : a \in A\}$. Com hem vist en la prova de l'existència de conjunts que no són Lebesgue-mesurables, per a $q \in \mathbb{Q}$, tots els $A + q$ són disjunts entre sí. En particular, tot $A + q$ és disjunt amb A. Obtenim que $\{A + q : q \in \mathbb{Q}\}$ és una partició numerable de $\mathbb{R}$.

Ara bé, $\mathbb{R}$ no és un conjunt magre en sí mateix, és a dir, que no es pot expressar com a unió numerable de conjunts disseminats. Per tant, com a mínim un dels $A + q$ no és disseminat. Però, de fet, cada conjunt d'aquests és una translació d'algun altre, de manera que cap d'ells és disseminat. En particular, A no és disseminat ni tampoc magre.

Suposem que ara A té la propietat de Baire. Sigui U un conjunt obert i M un conjunt magre de manera que $A = U \triangle M$. Evidentment, $U \neq \emptyset$, o sigui que existeixen $a, b \in \mathbb{R}$ tals que $a < b$ i $(a, b) \subseteq U$. Sigui $I = (a, b)$ i posem $r = b - a$. Prenem ara $x \in \mathbb{R}$ tal que $|x| < r$. Aleshores $(I + x) \cap I$ és un interval obert. D'altra banda, $M \cup (M + x)$ és de primera categoria. Per tant, per definició de subespai magre,

$$((I + x) \cap I) \setminus (M \cup (M + x)) \neq \emptyset.$$

Clarament, $((I + x) \cap I) \setminus (M \cup (M + x)) \subseteq (A + x) \cap A$. Per tant, per tot $x \in \mathbb{R}$ amb $x < r$, tenim $(A + x) \cap A \neq \emptyset$. Fixem ara un $x = q$ racional positiu menor que r. Arribem a una contradicció perquè hem vist que tot $A + q$ és disjunt de A. Per tant, el conjunt A no té la propietat de Baire. □

8.4 Conjunts perfectes

Per acabar, estudiarem els conjunts perfectes i la propietat del conjunt perfecte.

Definició 8.12. Diem que un subconjunt X d'un espai topològic és *perfecte* si és tancat, no buit i no té punts aïllats.

Definició 8.13. Un conjunt de nombres reals té la *propietat del conjunt perfecte* si és numerable o bé si conté un subconjunt perfecte.

El nostre proper objectiu serà demostrar dos resultats de Cantor sobre conjunts perfectes. En primer lloc, veurem que tot conjunt perfecte de reals té la mateixa cardinalitat que el continu. Després, que tot conjunt tancat no numerable de reals és la unió d'un conjunt perfecte i un conjunt numerable. D'aquí, doncs, obtenim que els conjunts tancats satisfan CH.

Teorema 8.14. (Cantor) *Els subconjunts de $\mathbb{R}$ perfectes tenen la mateixa cardinalitat que $\mathbb{R}$.*

Demostració. Sabem que $\mathbb{R} \sim (0,1) \sim \mathcal{P}(\omega) \sim 2^\omega$. Per tant, donat un conjunt perfecte $P \subseteq \mathbb{R}$, volem trobar una funció injectiva de 2^ω en P. Sigui S el conjunt de successions finites de zeros i uns. Per inducció en la llargada de $s \in S$, podem trobar intervals tancats I_s de manera que per cada $n \in \omega$ i cada $s \in S$ de longitud n,

(a) $I_s \cap P$ és perfecte.

(b) El diàmetre de I_s és més petit o igual que $1/n$.

(c) $I_{s^\frown 0} \subseteq I_s$, $I_{s^\frown 1} \subseteq I_s$ i $I_{s^\frown 0} \cap I_{s^\frown 1} = \emptyset$.

Per tota $f \in 2^\omega$, el conjunt $P \cap \bigcap_{n=0}^{\infty} I_{f\restriction n}$ té exactament un element. Sigui $F(f)$ aquest element de P. Tenim llavors la funció buscada.

□

Passem ara a veure el següent resultat. L'enunciarem i demostrarem de manera general per a espais polonesos.

Teorema 8.15. (Cantor) *Els conjunts tancats no numerables d'un espai polonès X tenen la propietat del conjunt perfecte i, en particular, tot conjunt tancat no numerable de X es pot escriure de manera única com a unió disjunta d'un conjunt perfecte i un conjunt numerable.*

Demostració. Sigui Y un subconjunt tancat de l'espai polonès X. Diem que un punt x és un *punt de condensació* si tot entorn de x en Y és no numerable. Sigui Z el conjunt de punts de condensació de Y. Volem veure que $Y = Z \cup C$, amb Z perfecte i C numerable.

Definim $C = Y \setminus Z$. Com que X és separable i metritzable (per ser un espai polonès), podem prendre una base numerable de X i intersecar-la amb Y per obtenir una base numerable U_n de Y. Per definició de Z, C és la unió de tots els U_n que són numerables.

Ara tindrem en compte l'axioma d'elecció numerable, que és una versió dèbil de l'axioma d'elecció, independent de ZF. Amb aquest obtenim que la unió numerable de conjunts numerables és numerable. Per tant, C és numerable.

Queda veure que Z és perfecte. Veurem que no té cap punt aïllat i que és tancat. Sigui $x \in Z$. Volem veure que és un punt d'acumulació. Sigui V un entorn de x en Y. Com que x és un punt de condensació (per ser de Z), V és no numerable. I com que $C = Y \setminus Z$ és numerable, V ha de contenir una quantitat no numerable de punts de Z. Per últim, els U_n són oberts, de manera que C també ho és, i llavors Z és tancat.

Hem obtingut, doncs, $Y = Z \cup C$, amb Z perfecte i C numerable. Queda veure que aquesta composició és única. Suposem que $Y = W \cup D$ és una unió disjunta amb W perfecte i D numerable. Sigui W^* el conjunt de punts de condensació de W. Com que W és perfecte, si $x \in W$ té un entorn obert U en Y, llavors $U \cap W$ és un conjunt perfecte, de manera que no és numerable, i llavors $W^* = W$. Per tant, $W \subseteq Z$. Per últim, si $x \in D$, com que D és un conjunt obert numerable, $x \in C$ i $D \subseteq C$. Ha de ser $Z = W$ i $C = D$.

□

Observació 8.16. En particular, tot espai polonès no numerable té la propietat del conjunt perfecte i es pot escriure com a la unió disjunta d'un conjunt perfecte i un conjunt obert numerable.

Ara que hem detallat els resultats de Cantor, veurem tal i com hem fet amb les propietats de regularitat prèvies, que, sota AC, hi ha conjunts de reals que no tenen la propietat del conjunt perfecte. Ho farem presentant els conjunts de Bernstein, que, per definició, no tenen la propietat del conjunt perfecte (de fet, els conjunts de Bernstein tampoc són Lebesgue-mesurables ni tenen la propietat de Baire).

Definició 8.17. Diem que $A \subseteq \mathbb{R}$ és un *conjunt de Bernstein* si per tot conjunt perfecte $P \subseteq \mathbb{R}$ tenim

$$(P \cap A \neq \emptyset) \wedge (P \cap (\mathbb{R} \setminus A) \neq \emptyset).$$

Teorema 8.18. *Sota AC, existeix un conjunt de Bernstein en els reals.*

Demostració. Veiem primer quants subconjunts perfectes de reals hi ha. Recordem que $\aleph_0$ representa la cardinalitat de ω. Llavors hi ha com a mínim $2^{\aleph_0}$ subconjunts perfectes de $\mathbb{R}$ (els $[0, a]$ per a $a \in \mathbb{R}^+$).

Com que hi ha $2^{|\mathbb{R}|}$ conjunts de reals, i com que $2^{\aleph_0} = |\mathbb{R}| < 2^{\mathbb{R}}$, només cal veure que no hi ha més de $2^{\aleph_0}$ subconjunts perfectes de reals. Com que els conjunts perfectes són tancats (complementaris d'oberts), de fet, n'hi ha prou amb veure que, com a molt, $\mathbb{R}$ conté $2^{\aleph_0}$ conjunts oberts.

Un conjunt obert és una unió numerable d'intervals oberts amb extrems racionals. D'aquests n'hi ha una quantitat numerable. Per tant, com a molt tindrem ${\aleph_0}^{\aleph_0} = 2^{\aleph_0}$ subconjunts oberts en $\mathbb{R}$. Així, hi ha exactament $2^{\aleph_0}$ subconjunts perfectes de $\mathbb{R}$.

Considerem una llista dels conjunts perfectes de $\mathbb{R}$, $\{P_\xi : \xi < 2^{\aleph_0}\}$. Cada un d'ells té cardinalitat $2^{\aleph_0}$ (demostració de Cantor que ja hem vist).

Sigui $\eta < 2^{\aleph_0}$. Aplicarem recursivitat de manera inductiva. Suposem que per tot $\xi < \eta$ hem triat punts $x_\xi, y_\xi \in P_\xi$ de manera que tots aquests punts són diferents. Siguin $X_\eta = \{x_\xi : \xi < \eta\}$ i $Y_\eta = \{y_\xi : \xi < \eta\}$. Aleshores la cardinalitat de $X_\eta \cup Y_\eta$ és estrictament menor que $2^{\aleph_0}$, de manera que $P_\eta \setminus (X_\eta \cup Y_\eta)$ és infinit, i podem triar punts diferents $x_\eta, y_\eta \in P_\eta \setminus (X_\eta \cup Y_\eta)$ per seguir la construcció.

Definim ara $X = \bigcup_{\xi<2^{\aleph_0}} X_\xi$ i $Y = \bigcup_{\xi<2^{\aleph_0}} Y_\xi$. Per construcció, X i Y són subconjunts disjunts de $\mathbb{R}$. Sigui P un subconjunt perfecte de $\mathbb{R}$. Llavors existeix $\xi < 2^{\aleph_0}$ de manera que $P = P_\xi$ i $x_\xi \in P \cap X$. Anàlogament, $P \cap Y$ tampoc és buit. A més, com que X i Y són disjunts, també tenim $X \setminus P \neq \emptyset$ i $Y \setminus P \neq \emptyset$. Per tant, $P \cap (\mathbb{R} \setminus X) \neq \emptyset$ i $P \cap (\mathbb{R} \setminus Y) \neq \emptyset$. Així, X i Y són dos exemples de subconjunts de reals de manera que tant ells com els seus complementaris intersequen amb tots els conjunts perfectes de $\mathbb{R}$, és a dir, que són conjunts de Bernstein. □

Per tancar aquest apartat, veurem un teorema sobre conjunts perfectes relacionat amb els conjunts analítics, és a dir, els de la classe Σ^1_1.

Teorema 8.19. *Tot conjunt analític té la propietat del conjunt perfecte. Això és, tot conjunt analític no numerable conté un conjunt perfecte.*

Demostració. Farem servir el conjunt 2^ω de les successions infinites de zeros i uns, així com l'espai de Baire $\mathcal{N} = \omega^\omega$ de les successions infinites de naturals. Considerarem $\omega^{<\omega}$ el conjunt de les successions finites de naturals.

Sigui X un conjunt polonès i $A \subseteq X$ un conjunt analític no numerable. Això implica que existeix una funció contínua $F : \mathcal{N} \to X$ amb $A = F[\mathcal{N}]$. Volem veure que A conté un subconjunt perfecte. De fet, el conjunt de cantor $\mathcal{C} \subseteq [0,1]$ és un conjunt perfecte. A més, $2^\omega \simeq \mathcal{C}$, de manera que A conté un subconjunt perfecte si i només si A conté un conjunt de Cantor o, equivalentment, si existeix una funció contínua injectiva de 2^ω a A.

Per $s \in \omega^{<\omega}$, escrivim $[s] = \{x : x \in \mathcal{N}, s \subseteq x\}$ (branques que estenen el node s). Escrivim també $F[s] = \{f(x) : x \in \mathcal{N}, s \subseteq x\}$.

Demostrarem l'enunciat assumint que $F[s]$ té més d'un element per tot s. Si no fos així, ho podem arreglar: eliminem de manera iterada aquells s per als quals no es compleix, de manera que amb cada s eliminem de $\mathcal{N}$ tots els elements que estenen s, però tots ells tenen la mateixa imatge. Com que només s'elimina una quantitat numerable de s, només s'ha eliminat una quantitat numerable d'elements de A, de manera que no es genera cap conflicte.

Considerem la següent construcció:

- Sigui $t = \langle\rangle$ una successió buida.
- Trobem dos conjunts oberts no buits i disjunts entre sí U_0 i U_1 en $F[t]$.
- Trobem $t_0, t_1 \in \omega^{<\omega}$ que estenen t de manera que $F[t_0] \subseteq U_0$ i $F[t_1] \subseteq U_1$ (cosa que podem fer fent servir la continuïtat de F).
- Anàlogament, podem separar t_0 en t_{00} i t_{01}, i t_1 en t_{10} i t_{11} fent servir conjunts disjunts oberts U_{00}, U_{01}, U_{10} i U_{11}.

Repetim aquest procés inductivament. Què obtenim? Per a cada successió finita s de zeros i uns, hem trobat una successió finita $t_s \in \omega^{<\omega}$ tal que

- Si s' estén s, aleshores t'_s estén t_s.
- Si s i s' són incompatibles, aleshores t_s i t'_s també ho són. És més, $F[t_s]$ i $F[t'_s]$ són disjunts.

Recordem que buscàvem una funció contínua injectiva de 2^ω a $F[\mathcal{N}]$. Per a tot $x \in 2^\omega$, si $x = (a, b, c \dots)$, definim t_x com el límit de la successió $t, t_a, t_{ab}, t_{abc}, \dots$ Aleshores la funció $x \mapsto F[t_x]$ és injectiva i contínua. □

8.5 Conjunts patològics

Com hem vist al llarg d'aquesta secció, l'axioma d'elecció ens permet trobar conjunts patològics de reals, com ara els conjunts de Vitali o els de Bernstein, que no compleixen les propietats de regularitat presentades. El que hem vist, però, són només alguns exemples; hi ha moltes altres propietats de regularitat de les quals, amb l'ajuda de l'axioma d'elecció, també es poden trobar conjunts patològics. Per contra, l'ús d'altres axiomes, com els de grans cardinals, permet demostrar que tots els conjunts projectius de nombres reals són Lebesgue-mesurables, tenen la propietat de Baire, la propietat del conjunt perfecte, etc.

9 Conclusions

Al llarg de la primera part de la memòria hem realitzat la construcció dels nombres naturals amb estructures de Dedekind, la dels enters a partir dels naturals, la dels racionals a partir dels enters i, finalment, la dels reals a partir dels racionals fent servir talls de Dedekind, i la dels complexos a partir dels reals. Hem donat les operacions aritmètiques corresponents en cada cas.

Després de veure algunes propietats inicials del conjunt dels nombres reals com a cos ordenat complet, hem introduït la jerarquia projectiva per a conjunts polonesos i ens hem centrat en tres propietats de regularitat: la propietat de Baire, la mesura de Lebesgue i la propietat del conjunt perfecte. Les hem estudiat i hem trobat conjunts patològics de reals per totes elles.

Aquesta segona part del treball s'ha tractat a un nivell més alt que la primera, que té més detall i precisió. Una possibilitat per continuar aquest projecte seria una ampliació d'aquesta part. En particular, el Teorema de Tarski d'eliminació de quantificadors, la demostració del qual només s'ha referenciat. També s'haurien pogut estudiar altres propietats de regularitat.

Els coneixements inicials que he fet servir venen principalment de l'assignatura de Teoria de Conjunts, que he realitzat a la carrera. He ampliat aquesta base al llarg de la primera part del treball, proporcionant més rigor als conceptes tractats. La segona part ha requerit un estudi i comprensió més profunds de material més avançat de teoria de conjunts, en particular, de teoria descriptiva de conjunts.

Referències

[1] Bagaria, J., Jané, I.: *Basic Set Theory* (apunts de l'assignatura *Basic Set Theory* del Màster en Lògica Pura i Aplicada).

[2] Enderton, H. B.: *Elements of Set Theory*, Academic Press, 1977.

[3] Goldstern, M.: *Descriptive Set Theory*, Institute of Discrete Mathematics and Geometry, Vienna University of Technology, `https://www.math.uni-hamburg.de/home/loewe/INFTY@ESSLLI2011/goldstern123.pdf`, 2011.

[4] Hrbáček, K., Jech, T.: *Introduction to Set Theory, Third Edition, Revised and Expanded*, Marcel Dekker Inc., 1999.

[5] Jech, T.: *Set Theory: The Third Millennium Edition, Revised and Expanded*, Springer Monographs in Mathematics, 2002.

[6] Kechris, A. S.: *Classical Descriptive Set Theory*, Graduate Texts in Mathematics, Volume 156, Springer Publishing, 1995.

[7] Levy, A.: *Basic Set Theory*, Perspectives in Mathematical Logic, Springer Publishing, 1979.

[8] Marker, D.: *Model Theory: An Introduction* (chapter 3, *Algebraic examples*), Graduate Texts in Mathematics, Volume 217, Springer Publishing, 2002.

[9] Swan, R. G.: *Tarski's Principle and the Elimination of Quantifiers*, 2005.