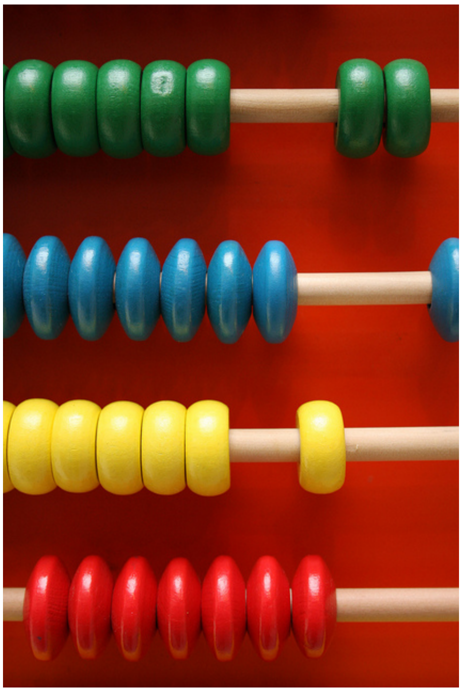
MATEMATIKARAKO SARRERA

OCW 2015



Mathieu Jarry iturria: Flickr CC-BY-NC-ND-2.0
https://www.flickr.com/photos/impactmatt/4581758027

Leire Legarreta Solaguren

EHU-ko Zientzia eta Teknologia Fakultatea

Matematika Saila

2 GAIA: MULTZO TEORIA ETA APLIKAZIOAK

Multzoekin operaketak. Aplikazioak. Multzo zenbakigarriak eta ez zenbakigarriak. Baliokidetasun eta ordenako erlazioak

1 Multzoak

Definizioa. Multzo *bat objektu batzuen bilduma da. Objektu horiek multzoaren elementuak dira. Normalean, multzoak maiuskulaz idatziko ditugu eta elementuak, berriz, minuskulaz. Gainera,* a *elementua* A *multzoan dagoela adierazteko* $a \in A$ *idatziko dugu, eta ez badago,* $a \notin A$ *adierazten da. (ohartu* $\in$ *ikurra "barne" irakurtzen dela)*

Multzorik sinpleenak zenbakien multzoak dira, eta horien artean honako hauek bereizten ditugu:

$\mathbb{N}$: Zenbaki arrunten multzoa, hau da, kontatzeko erabiltzen ditugun zenbakiak: $1, 2, 3, 4, \ldots$. Ohartu $0 \notin \mathbb{N}$ dela.

$\mathbb{Z}$: Zenbaki osoen multzoa, hau da, zenbaki arruntak, zero eta zenbaki arrunten negatiboak: $\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$

$\mathbb{Q}$: Zenbaki arrazionalen multzoa, hau da, zenbaki osoen a/b zatikiak. Gogoratu $b \neq 0$ izan behar duela, eta $a/b = c/d$ dela baldin eta soilik baldin $ad = bc$ bada.

Argi ikusten da edozein $a \in \mathbb{Z}$ zenbaki osoa, arrazionala ere dela, $a = \frac{a}{1} \in \mathbb{Q}$ delako, hau da, $\mathbb{Z} \subseteq \mathbb{Q}$. Ohartu zenbaki arrazional bat zatiki desberdinengatik adieraz daitekeela, horiek horien artean baliokideak direlarik. Aurrekoa, zatiki baten izendatzaile eta zenbakitzailea nulua ez den zenbaki oso berdinagatik biderkatzen badira, lortutako zatikia hasierako zatikiaren baliokidea delaren propietatetik ondorioztatzen da. Normalean, zenbaki arrazional bat adierazteko zatiki laburtezin bat erabiltzen da, hau da, izendatzailea eta zenbakitzailea elkarrekin lehenak dituen zatikiaren bidez.

$\mathbb{I}$: Zenbaki irrazionalen multzoa, ez arrazionalen multzoa da, hau da, alde dezimalean infinitu zifra ez errepikatuak dituzten zenbaki hamartarrek osatzen duten multzoa da. Beste modu batetan esanda, multzo honetako zenbakiak ezin daitezke bi zenbaki osoen zatiki moduan adierazi. Argi dago $\mathbb{Q} \cap \mathbb{I} = \emptyset$ dela. Adibidez, ondokoak dira zenbaki irrazionalak: $\sqrt{3} = 1,7320508...$, $\pi = 3,14159265....$ zirkunferentziaren luzera eta bere diametroaren arteko proportzioa edo $e = lim_{n \longrightarrow \infty}(1 + \frac{1}{n})^n$, hau da, $2,71828182845905......$ zenbakia.

$\mathbb{R}$: Zenbaki errealen multzoa. Ez da erraza frogatzea nola eraikitzen diren zenbaki horiek, zenbaki arrazionaletatik, baina zenbaki errealak oso ezagun digutu luzerak neurtzeko erabiltzen baitira. Hori dela eta, zenbaki errealak zuzen infinitu baten gainean irudikatzen dira. Gogoratu, bestalde, zenbaki errealak beren garapen hamartarraren bidez adieraz daitezkeela, eta zenbaki errealen multzo hori, zenbaki arrazionalen eta zenbaki irrazionalen multzoen bildura dela.

$\mathbb{C}$: Zenbaki konplexuen multzoa. Definizioz, zenbaki konplexu bat, $a + bi$ moduko adierazpen bat da, $a, b \in \mathbb{R}$ izanik. Zenbaki konplexuak zer diren ulertzea baino garrantzitsuagoa da, jakitea nola egiten diren eragiketak zenbaki konplexuekin. Batuketa honela egiten dugu:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

hau da, "osagaiz osagai" batzen da, eta bestalde, biderketaren erregela

$$(a + bi).(c + di) = (ac - bd) + (ad + bc)i$$

dugu. Azken formula hori buruz ikastea baino errazagoa da, $i^2 = -1$ dela gogoratzea eta biderkatzea ohituta gauden moduan.

Oharra. (i) *$*$ ikurrarekin, dagokigun multzotik 0 elementua kentzen da. Adibidez, $\mathbb{Z}^* = \mathbb{Z} - \{0\}$.*

(ii) *$+$ ikurrarekin, 0 baino haundiagoak edo berdinak diren zenbakietara murrizten gara. Adibidez, $\mathbb{R}^+ = \{a \in \mathbb{R} \mid a \geq 0\}$.*

Multzoak definitzeko moduak. Honako aukera hauek ditugu:

(i) Multzoaren elementu guztiak giltzen artean zerrendatuz. Adibidez, $A = \{1, 2, 3, 4\}$.

(ii) Multzoaren elementuak bereizten dituzten propietateak emanez. Hala nola, aurreko multzoa $A = \{x \in \mathbb{Z} \mid 1 \leq x \leq 4\}$ moduan ere idatz daiteke.

(iii) Multzo parametrizatuak: multzoaren elementuak parametro batzuei balioak emanez lortzen dira. Adibidez, zenbaki oso bikoitien multzoa, $\{2n \mid n \in \mathbb{Z}\}$ moduan jar daiteke, eta $\{(\lambda, \mu, -\lambda - \mu) \mid \lambda, \mu \in \mathbb{R}\}$ multzoa, $x + y + z = 0$ planoa da $\mathbb{R}^3$-n.

Egia esan, hirugarren aukera bigarrenaren kasu berezi bat bezala ikus daiteke. Adibidez, $\{2n \mid n \in \mathbb{Z}\}$ multzoa, $\{x \in \mathbb{Z} \mid \exists \lambda \in \mathbb{Z} \text{ non } x = 2\lambda\}$ bezala jar genezake, eta orduan multzoko elementuak bereizten dituen propietate bat ematen ari gara.

Definizioa. *Elementu bat ere ez duen multzoari multzo hutsa esaten zaio eta $\varnothing$ ikurraz adierazten da.*

Definizioa. *Izan bitez A eta B multzoak.*

(i) *B, A-ren azpimultzoa dela (edo B, A-ren parte dela) diogu B-ren elementu guztiak A-n badaude. Partekotasun hau adierazteko, $B \subseteq A$ idazten dugu.*

(ii) *B, A-ren azpimultzoa bada baina ez bada A-ren berdina, orduan partekotasun hertsia dugula esaten da. Orduan $B \subsetneq A$ idazten dugu.*

(iii) *A eta B multzo berdinak dira baldin eta soilik baldin multzo biak elementu berdinak badituzte, hau da, $a \in A \Longleftrightarrow a \in B$. Beraz, $A = B \Longleftrightarrow A \subseteq B$ eta $B \subseteq A$, eta ondorioz $A \neq B$ baldin eta soilik baldin existitzen bada $a \in A$ non $a \notin B$ edo existitzen bada $b \in B$ non $b \notin A$.*

Teorema. *Izan bedi A multzoa. Orduan, $\varnothing \subseteq A$.*

Adibidea. *Izan bedi $A = \{1, 2, 3\}$. Nabaria da $\{1, 2\} \subseteq A$ eta $\{1, 4\} \nsubseteq A$ betetzen dela. Honako hauek dira A-ren azpimultzo guztiak:*

$$\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \text{ eta } \{1, 2, 3\}.$$

Beraz, A-k 8 azpimultzo ditu.

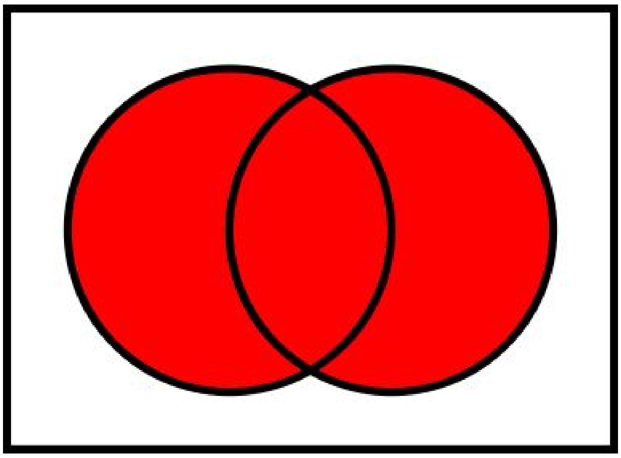
Definizioa. *Izan bedi A multzoa. A-ren elementuen kopuruari A-ren kardinala esaten zaio, eta $|A|$ ikurraren bidez adierazten da. Baldin eta multzoak ez badu elementuen kopuru finitua, multzoa infinitua dela esaten da.*

Adibidez, $|\mathbb{Z}| = \infty, |\varnothing| = 0,$ eta $|\{1, 2, 3, 4\}| = 4.$

Multzoen arteko eragiketak. Izan bitez A eta B multzoak. Orduan, honako multzo hauek definitzen ditugu:

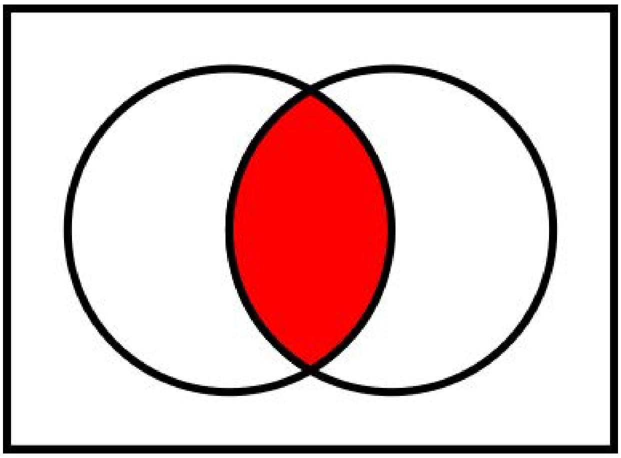
(i) A-ren eta B-ren *bildura*, $A \cup B$ idazten duguna ("A bildura B" irakurtzen dena):

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



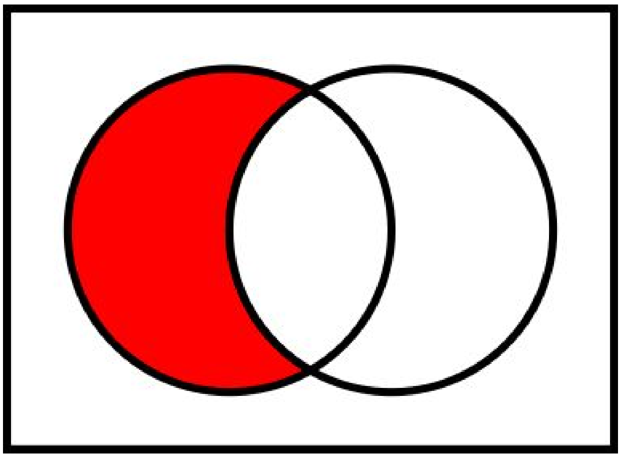
(ii) A-ren eta B-ren *ebakidura*, $A \cap B$ idazten duguna ("A ebaki B" irakurtzen dena):

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



(iii) A-ren eta B-ren *diferentzia*, $A - B$ idazten duguna ("A ken B" irakurtzen dena):

$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$



Eragiketa horiek grafikoki irudika daitezke. Honelako irudiei *Venn-en diagramak* deitzen zaie eta oso erabilgarriak dira multzoen arteko eragiketen propietateak ikusteko. Ohartu $A \cup B = B \cup A$ eta $A \cap B = B \cap A$ dela, baina $A - B \neq B - A$ izan daitekeela. Honez gain, $|A \cup B| = |A| + |B| - |A \cap B|$. Diagramen gainean propietateak ikus badaitezke ere, Matematikan ez ditugu marrazkiak onartzen besterik gabe emaitzak frogatzeko, frogapen formal bat eskatzen dugu beti. Ondorengo teoremaren propietateekin horrela arrazoitzea ondo legoke: lehenengo Vennen diagramak marraztea, ditugun emaitzen egiatasunaz konbentzitzeko, eta gero froga ikustea argudio logikoekin, eman diren definizioetan oinarrituta.

Teorema. *(Propietate banakorrak). Izan bitez A, B eta C multzoak. Orduan, propietate hauek betetzen dira:*

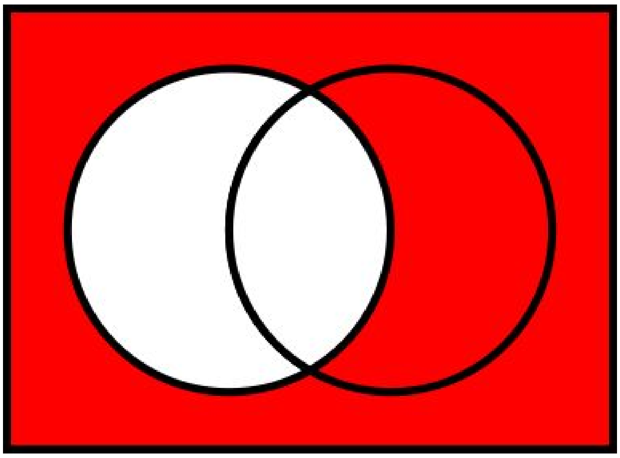
(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *(Bilduraren propietate banakorra ebakidurarekiko.)*

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *(Ebakiduraren propietate banakorra bildurarekiko.)*

Multzo unibertsala. Askotan, erabiltzen ditugun multzo guztiak erreferentzia multzo baten barruan daude, *multzo unibertsala* deitzen dena. Adibidez, bakarrik zenbaki errealak erabiltzen baditugu, multzo unibertsala $\mathbb{R}$ izango da.

Definizioa. *Demagun X multzo unibertsala duen testuinguruan lan egiten ari garela, eta izan bedi $A \subseteq X$. Orduan, A-ren* osagarria*, A^c idazten dena, honela definituriko multzoa da:*

$$A^c = X - A = \{x \in X \mid x \notin A\}.$$



Adibidez, multzo unibertsala $\mathbb{R}$ bada, orduan $(0,1)^c = (-\infty, 0] \cup [1, +\infty)$ dugu eta $(-\infty, 0]^c = (0, +\infty)$.

Garbi dago $A \cap A^c = \emptyset$ eta $A \cup A^c = X$ dela. Hurrengo teoreman multzo osagarrien propietate garrantzitsu bat ematen dugu. (Ez dugu ondoko teoremaren froga aurkezten, interesgarria delako irakurlea bere kabuz saia daiteen honen froga ematen.)

Teorema. *(De Morganen legeak). Izan bitez A eta B multzoak, multzo unibertsal berdinaren barruan. Orduan,*

(i) $(A \cup B)^c = A^c \cap B^c$.

(ii) $(A \cap B)^c = A^c \cup B^c$.

Atal hau bukatzeko, oso eraikuntza garrantzitsu bat emango dugu, biderkadura cartesiarra. Gogoratu *bikote ordenatu* bat (a, b) motako adierazpen bat dela, eta bi bikote (a, b) eta (c, d) berdinak direla baldin eta soilik baldin $a = c$ eta $b = d$ bada. Oro har, $(a_1, a_2, \ldots, a_n)$ itxurako adierazpen bat *tupla ordenatu* bat dela esaten dugu (edo, n-ren balioa azpimarratu nahi badugu n-*tupla* bat dela). Baldin eta $1 \leq i \leq n$ bada, a_i elementuari tuplaren i-*garren osagaia* deitzen diogu.

Definizioa. *Izan bitez A eta B multzoak. Orduan, A-ren eta B-ren* biderkadura cartesiarra, *$A \times B$ idazten duguna, lehenengo osagaia A-n eta bigarren osagaia B-n duten bikote guztien multzoa da. Hau da:*

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

Oro har, $A_1, A_2, \ldots, A_n$ multzoak badira, definitzen dugu

$$A_1 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, \forall i \in \{1, \ldots, n\}\}.$$

Multzo guztiak A multzo beraren berdinak badira, $A \times \overset{n}{\cdots} \times A$-ren ordez, A^n idazten dugu sinpleago.

Ohartu $\mathbb{R}^2$ planoa eta $\mathbb{R}^3$ espazioa, biderkadura cartesiarrak direla. Egia esan, “cartesiar” izena Descartes matematikari frantsesarengandik dator, bera izan baitzen planoko puntuak (a, b) moduan eta espaziokoak (a, b, c) moduan idazten hasi zena. Horregatik, puntuen deskribapen horiek *koordenatu cartesiarrak* deitzen dira eta, analogiagatik, hortik dator biderkadura cartesiarraren izena.

Adibidea. $A = \{1, 2, 3\}$ *eta* $B = \{x, y\}$ *bada, orduan*

$$A \times B = \{(1, x), (2, x), (3, x), (1, y), (2, y), (3, y)\}.$$

Biderkadura cartesiarraren kardinala. A eta B multzo finituak badira, argi dago $|A \times B| = |A||B|$ dela eta, oro har, $|A_1 \times \cdots \times A_n| = |A_1| \ldots |A_n|$ dela.

2 Aplikazioak

Definizioa. *Baldin eta A eta B multzoak badira, f aplikazio bat erregela bat da, $a \in A$ elementu bakoitzari B-ko elementu bat eta bakar bat egokitzen diona. B-ko elementu horri a-ren irudia deitzen zaio eta $f(a)$ bidez idazten da. Gainera:*

(i) *A, f-ren eremua deitzen da, eta $A = E(f)$ idazten dugu.*

(ii) *B, f-ren koeremua deitzen da.*

Notazioa. f aplikazioa, A-tik B-ra doala adierazteko, $f : A \longrightarrow B$ edo $A \xrightarrow{f} B$ idazten da.

Adibideak. (i) *$f : \mathbb{R} \longrightarrow \mathbb{R}$ non $f(x) = x^2$ edo $f(x) = \sin x$, aplikazioak dira.*

(ii) *$f : \mathbb{R} \longrightarrow \mathbb{R}$ non $f(x) = 1/x$ ez da aplikazioa, 0 elementuak ez duelako irudirik. Eremu gisa $\mathbb{R}$-ren ordez, $\mathbb{R} - \{0\}$ hartzen badugu, orduan f aplikazioa da.*

(iii) *Izan bedi $f : \mathbb{R} \longrightarrow \mathbb{R}$ non*

$$f(x) = \begin{cases} x+1, & x > 0 \text{ bada,} \\ 1, & x \leq 0 \text{ bada.} \end{cases}$$

Orduan, f aplikazioa da eta f, zatika definiturik dagoela esaten da. Baldin eta $A, B \subseteq \mathbb{R}$ bada, gogoratu $f : A \longrightarrow B$ aplikazio bat planoan irudikatzen dugula, $(x, f(x))$ puntuak markatuz, $x \in A$ guztietarako.

(iv) *Izan bitez A eta B multzoak eta $b_0 \in B$ elementu finkoa. Orduan, $f(a) = b_0$ definitzen badugu $a \in A$ guztietarako, f aplikazio konstantea dela esaten dugu.*

(v) *A edozein multzoaren gainean identitate aplikazioa deitutako $1_A : A \longrightarrow A$, $1_A(x) = x$, edozein $x \in A$ elementuentzako, aplikazioa defini daitke.*

Batzuetan, $f : A \longrightarrow B$ aplikazioa emanda, interesatu ahal zaigu arreta A eremuko elementu batzuetara murriztea. Hori dela eta, hurrengo definizioa ematen dugu.

Definizioa. *Izan bitez $f : A \longrightarrow B$ aplikazioa eta $S \subseteq A$. Orduan, f-ren murrizketa S azpimultzora, $f_{|S}$ idazten dena, f-ren eremua S-ra murriztuz lortzen den aplikazioa da. Beraz, $f_{|S}$ honako bi baldintza hauen bidez definiturik dago:*

(i) *$f_{|S} : S \longrightarrow B$, (eremua S-ra murrizten da.)*

(ii) *$f_{|S}(s) = f(s), \forall s \in S$, ($S$-ko elementu baten irudia $f_{|S}$-ren bitartez, f-ren bitartez duen den berdina da.)*

Definizioa. Aplikazio mota nagusiak. *Izan bedi $f : A \longrightarrow B$ aplikazioa.*

(i) *f injektiboa dela esaten dugu, ez badago A-ren bi elementu desberdin irudi berdina dutenik.*

(ii) *f supraiektiboa dela esaten dugu, B-ko elementu guztiak irudiak badira.*

(iii) *f bijektiboa dela esaten dugu aldi berean injektiboa eta supraiektiboa bada.*

Adibideak. (i) *Izan bedi $f : A \longrightarrow B$ aplikazio konstante bat. Orduan, f injektiboa izateko, $|A| = 1$ izan behar du eta supraiektiboa izateko, $|B| = 1$. Beraz, f bijektiboa da baldin eta soilik baldin $|A| = |B| = 1$ bada.*

(ii) *Nabaria denez, 1_A identitate aplikazioa bijektiboa da.*

(iii) *Ezin daiteke eratu aplikazio bijektiborik $A = \{a, b, c\}$ multzotik, $B = \{x, y\}$-ra, ezta ere injektiborik. Aplikazio supraiektiborik, bai ordea.*

Proposizioa. *Izan bitez A eta B multzoak. Orduan:*

(i) *$f : A \longrightarrow B$ aplikazio injektibo bat eraiki daiteke baldin eta soilik baldin $|A| \leq |B|$ bada.*

(ii) *$f : A \longrightarrow B$ aplikazio supraiektibo bat eraiki daiteke baldin eta soilik baldin $|A| \geq |B|$ bada.*

(iii) *$f : A \longrightarrow B$ aplikazio bijektibo bat eraiki daiteke baldin eta soilik baldin $|A| = |B|$ bada.*

Hala ere, normalean aplikazioak ez dira hain sinpleak izango, Vennen diagramen bidez irudikatu ahal izateko. Nola froga dezakegu orduan $f : A \longrightarrow B$ aplikazio bat injektiboa, supraiektiboa edo bijektiboa den? Hau izango da jarraituko dugun metodoa:

(i) f injektiboa dela frogatzeko, bi elementuk irudi bera badute berdinak direla ikusiko dugu, hau da:

$$a, a' \in A \text{ eta } f(a) = f(a') \Longrightarrow a = a'$$

(ii) f supraiektiboa dela frogatzeko, zuzenean definizioa erabiltzen dugu. Notazio sinbolikora itzulita, hau ikusi behar dugu:

$$\forall b \in B, \exists a \in A \mid f(a) = b$$

edo, baliokideki:

$$b \in B \Longrightarrow \exists a \in A \mid f(a) = b$$

(iii) f bijektiboa den ikusteko, injektibotasuna eta supraiektibotasuna aztertzen ditugu, bakoitza bere aldetik.

Adibidea. *$f : \mathbb{R} \longrightarrow \mathbb{R}$ aplikazioa non, $f(x) = 2x + 3$ den, $x \in \mathbb{R}$ guztietarako, bijektiboa da.*

Definizioa. *Demagun $f : A \longrightarrow B$ aplikazioa dela.*

(i) *Izan bedi $S \subseteq A$. Orduan, S-ren irudia (edo irudi zuzena) f-ren bitartez, $f(S)$ idazten duguna, S-ko elementu guztien irudiek osatutako multzoa da. Hau da,*

$$f(S) = \{f(s) \mid s \in S\}.$$

Bereziki, $f(A)$ irudi guztien multzoari f-ren irudia deitzen zaio eta $\operatorname{im} f$ idazten da.

(ii) *Izan bedi $T \subseteq B$. Orduan, T-ren alderantzizko irudia f-ren bitartez, $f^{-1}(T)$ idazten duguna, irudia T-ren barruan duten A-ko elementu guztien multzoa da. Hau da,*

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}.$$

Notazioa. B-ren barruan $T = \{b\}$ elementu bakar bateko multzoa hartzen badugu, $f^{-1}(\{b\})$ idatzi beharrean, $f^{-1}(b)$ idazten dugu sinpleago.

Adibidea. *Izan bedi $f(x) = x^2$ aplikazioa, $\mathbb{R}$-tik $\mathbb{R}$-ra. Orduan, honako irudi eta alderantzizko irudi hauek ditugu: $\operatorname{im} f = [0, +\infty)$, $f([0, 2]) = [0, 4]$, $f([2, +\infty)) = [4, +\infty)$, $f((-\infty, -1) \cup [2, +\infty)) = (1, +\infty)$, $f^{-1}(1) = \{-1, 1\}$, $f^{-1}(-1) = \emptyset$, $f^{-1}([-1, 0]) = \{0\}$ eta $f^{-1}((1, +\infty)) = (-\infty, -1) \cup (1, +\infty)$.*

Oharra. *Gogoratu tarteen notazioa: $a, b \in \mathbb{R}$ badira, orduan $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$, $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$, $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$ eta $[a, +\infty) = \{x \in \mathbb{R} \mid a \leq x\}$. Era berean definitzen dira beste konbinazio posible guztiak.*

Demagun orain $f : A \longrightarrow B$ aplikazioa, Vennen diagrama baten bidez irudikatu dugula eta gezi guztiak alderantziz idazten ditugula, hau da, A-tik B-ra idatzi beharrean B-tik A-ra idazten ditugula. Horrela lortzen den erregela, ba al da aplikazioa? Erantzuna baiezkoa zein ezezkoa izan daiteke.

Beraz, erregela berria aplikazioa izango da baldin eta soilik baldin B-ko elementu guztietara gezi bat eta bakar bat iristen bada. Dakigunez, honen esanahia da, f bijektiboa dela. Laburbilduz, $f : A \longrightarrow B$ aplikazioa emanda, **geziak alderantziz irudikatuz lortzen den erregela aplikazioa da baldin eta soilik baldin f bijektiboa bada**. Orduan, aplikazio horri f-ren *alderantzizko aplikazioa* deitzen zaio eta f^{-1} ikurraren bidez adierazten da. Beraz, $f^{-1} : B \longrightarrow A$ dugu.

Ohartu, $a \in A$ elementutik $b \in B$ elementura gezi bat joatearen esanahia oso sinplea dela: $f(a) = b$. Hori gertatzen denean, f^{-1}-ek gezi bat bidaltzen du b-tik a-ra, hau da, $f^{-1}(b) = a$ dugu. Honetaz jabetuta, alderantzizko aplikazioaren definizio formalago hau eman dezakegu.

Definizioa. *Izan bedi $f : A \longrightarrow B$ aplikazio bijektiboa. Orduan, f-ren alderantzizko aplikazioa honela definitzen da:*

(i) *f^{-1}, B-tik A-ra doa, hau da, $f^{-1} : B \longrightarrow A$ dugu.*

(ii) *$f^{-1}(b) = a$ dugu baldin eta soilik baldin $f(a) = b$ bada.*

Adibideak. *1) Har dezagun $f : \mathbb{R} \longrightarrow [0, +\infty)$ aplikazioa non $f(x) = x^2$ den $\forall x \in \mathbb{R}$. Garbi dago f ez dela bijektiboa (supraiektiboa da, baina ez injektiboa), beraz ez da f^{-1} alderantzizkoa existitzen.*

2) Izan bedi $g : [0, +\infty) \longrightarrow [0, \infty)$ berriro ere $g(x) = x^2$ formularen bidez emanda. Beraz, g, f-ren murrizketa da $[0, \infty)$ tartera eta g bijektiboa da. Beraz, existitzen da $g^{-1} : [0, +\infty) \longrightarrow [0, +\infty)$. Zein formularen bidez dago emanda? Gogoratu $g^{-1}(y) = x$ dela baldin eta soilik baldin $g(x) = y$ bada. Beraz, $y \in [0, +\infty)$ elementu baten irudia kalkulatzeko g^{-1}-en bitartez, $g(x) = y$ ekuazioa askatu behar da, x ezezagunarekiko. Hau supraiektibotasuna aztertzerakoan egiten da, eta $x = \sqrt{y}$ lortzen da. Beraz, $g^{-1}(y) = \sqrt{y}$ dugu edo, aldagaiaren izena aldatuz, $g^{-1}(x) = \sqrt{x}$, $\forall x \in [0, +\infty)$.

3) Izan bedi $h : (-\infty, 0] \longrightarrow [0, \infty)$ non $h(x) = x^2$ den, hau da, f-ren murrizketa $(-\infty, 0]$ tartera. Aurreko ataleko prozedura bera jarraituz h bijektiboa dela ikus daiteke eta $h^{-1}(x) = -\sqrt{x}$ dela $x \in [0, -\infty)$ guztietarako.

Oharra. *Demagun $f : A \longrightarrow B$ aplikazio bijektiboa dela. Orduan, $T \subseteq B$ bada, $f^{-1}(T)$ ikurrak bi esanahi posible ditu:*

(i) *T-ren alderantzizko irudia f-ren bitartez. Esanahi honekin, $a \in f^{-1}(T)$ baldin eta soilik baldin $f(a) \in T$. (Alderantzizko irudiaren definizioagatik.)*

(ii) *T-ren irudi zuzena f^{-1}-en bitartez. Bigarren esanahi honekin,*

$$\begin{aligned} a \in f^{-1}(T) &\Longleftrightarrow \exists b \in T \mid a = f^{-1}(b) \text{ (irudi zuzenaren definizioagatik)} \\ &\Longleftrightarrow \exists b \in T \mid f(a) = b, (f^{-1} - \text{en definizioagatik}) \\ &\Longleftrightarrow f(a) \in T. \end{aligned}$$

Beraz, bi kasuetan, $f^{-1}(T)$ multzoak elementu berdinak ditu eta ez dago inolako anbiguotasunik $f^{-1}(T)$ notazioari dagokionez.

Bestalde, $f : A \longrightarrow B$ bijektiboa ez denean, ohartu $f^{-1}(T)$-k zentzua duela (i)-eko esanahian, baina ez (ii)-koan: f ez bada bijektiboa ez da f^{-1} aplikazioa existitzen, eta ondorioz ezin da f^{-1}-en irudi zuzenari buruz hitz egin.

Proposizioa. *Demagun $f : A \longrightarrow B$ aplikazioa dela. Baldin eta f aplikazioaren alderantzizko aplikazioa existitzen bada, hau bakarra da, eta f^{-1} bidez denotatzen da.*

Proposizioa. *Demagun $f : A \longrightarrow B$ aplikazioa dela. Baldin eta A eta B multzo finituak badira, eta $|A| = |B|$ bada, ondokoa dugu,*

(i) *f injektiboa bada, orduan f bijektiboa da,*

(ii) *f supraiektiboa bada, orduan f bijektiboa da.*

Aurrekoa ez da egia multzoak ez badira finituak.

Orain aplikazioen arteko eragiketa garrantzitsu bat definitzen dugu.

Definizioa. *Izan bitez $f : A \longrightarrow B$ eta $g : B \longrightarrow C$ aplikazioak. Orduan, f-ren eta g-ren konposizioa, $g \circ f$ idazten dena, honako bi baldintza hauen bidez definituriko aplikazioa da:*

(i) *$g \circ f : A \longrightarrow C$.*

(ii) *$(g \circ f)(a) = g(f(a)), \forall a \in A$.*

Eman dugun definizioaren arabera, $g \circ f$ lortzeko, lehenengo f eta gero g aplikatu behar dira.

Ez da pentsatu behar bi aplikazio beti konposa daitezkeenik. Izan ere, konposizioaren definizioan f-ren koeremua eta g-ren eremua berdinak izan daitezen eskatzen da, bestalde jarrita, $\mathrm{im} f = \mathrm{dom} g$ bete behar da. Horrela posible izango da, g, f-ren ondoren aplikatzea. Egia esan, horretarako nahikoa litzateke $\mathrm{im} f \subseteq \mathrm{dom} g$ izatea. Hala ere, partekotasun hau betetzen bada, f-ren koeremua handiagoa egin dezakegu, g-ren eremuarekin bat etorri arte. Beraz, ez genuen ezer askorik irabaziko konposizioaren definizioan $\mathrm{im} f = \mathrm{dom} g$ berdintzaren ordez, soilik $\mathrm{im} f \subseteq \mathrm{dom} g$ eskatu izan bagenu.

Adibidea. *Izan bitez $f : \mathbb{R} \longrightarrow \mathbb{R}$ eta $g : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$ eta $g(x) = x + 2$ formulen bidez emanda. Orduan $f \circ f, f \circ g, g \circ f$ eta $g \circ g$ lau konposizioak egin daitezke, eta $\mathbb{R}$-tik $\mathbb{R}$-ra doazen aplikazioak dira. Konposizio hauen formulak honako hauek dira:*

$$(f \circ f)(x) = f(f(x)) = f(x^2) = (x^2)^2 = x^4,$$

$$(f \circ g)(x) = f(g(x)) = f(x + 2) = (x + 2)^2 = x^2 + 4x + 4,$$

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

$$(g \circ g)(x) = g(g(x)) = g(x + 2) = (x + 2) + 2 = x + 4.$$

Ikusten denez, $f \circ g \neq g \circ f$ dugu. Beraz, konposizioa egiterakoan garrantzitsua da zein ordenatan idazten diren aplikazioak.

Ondorengo teorema begibistakoa da.

Teorema. *Izan bedi $f : A \longrightarrow B$ aplikazioa. Orduan:*

(i) *$f \circ 1_A = f$ eta $1_B \circ f = f$ dugu. Beraz, identitate aplikazioak ez du eraginik konposizioak egiterakoan. (Ohartu batean, 1_A eta bestean, 1_B idazten dugula konposizioak egin ahal izateko.)*

(ii) *f bijektiboa bada, $f^{-1} \circ f = 1_A$ eta $f \circ f^{-1} = 1_B$. Hau da, aplikazio bijektibo bat bere alderantzizkoarekin konposatzean, dagokion identitate aplikazioa lortzen da.*

3 Multzo zenbakigarriak eta ez zenbakigarriak

Definizioa. *A multzoa B multzoari ekipotentea dela esaten da, ($A \sim B$) idazten dena, A multzotik B multzora definitutako aplikazio bijektibo bat existitzen bada. Bereziki ekipotentea izatea baliokidetasun erlazioa da (kontzeptu hori beranduago definituko da).*

Ohartu A multzoaren kardinala deitzen zaiola, A multzoak dituen elementu kopuruari, $|A|$ bidez denotatzen dena.

Definizioa. *A multzoa finitua dela esaten da bere kardinala zenbaki arrunt bat bada, hau da, A multzoa, $\mathbb{N}_n = \{1, 2, \ldots, n\}$ motako multzo bati ekipotentea bada.*

Adibidez, ohartu $\mathbb{N}$ multzoak eta $2\mathbb{N}$, zenbaki bikoitien multzoak, kardinal berdina dutela.

Definizioa. *A multzoa infinitua dela esaten da, A multzoa bere azpimultzo propio bati ekipotentea bada. Hau da, baldin eta existitzen bada $B \subseteq A$ non $B \neq A$ eta $|B| = |A|$ baldintzak betetzen diren.*

Beraz, zenbaki arrunten multzoa, multzo infinitu bat da. $|\mathbb{N}|$ multzoaren kardinala $\aleph_0$ bidez adierazten da, eta kardinal zenbakigarria duela esaten da.

Definizioa. *Multzo bat zenbakigarria dela esaten da, baldin eta finitua edo infinitu zenbakigarria bada.*

Ariketa. *Zenbakigarriak diren bi multzoen bildura ere, multzo zenbakigarria da.*

Definizioa. *Izan bitez A eta B bi multzo. A multzoaren kardinala B multzoaren kardinala baino hertsiki txikiagoa dela esaten da, ($|A| < |B|$) idazten dena, ondoko bi baldintzak betetzen badira,*

(i) *A, B-ren azpimultzo propio bati ekipotentea*

(ii) *A-ren azpimultzo bat ere, ez da B-ri ekipotentea.*

Bestalde, $|A| \leq |B|$ dela esaten da, baldin eta $|A| < |B|$ edo $|A| = |B|$ badira.

$|A| \leq |B|$ dela frogatzeko, nahikoa da $f : A \longrightarrow B$ aplikazio injektibo bat existitzen dela frogatzea. Bereziki, $|\mathbb{N}| \leq |\mathbb{Q}|$ dugu.

Baldin eta A multzoa, B multzoaren azpimultzo propio bat bada, bereziki beti betetzen da $|A| \leq |B|$ erlazioa, identitate aplikazioa injektiboa delako.

Teorema. *Zenbaki arrazionalen multzoa, hau da, $\mathbb{Q}$, multzo infinitu zenbakigarria da.*

Teorema. *Zenbaki errealen $(0, 1) = \{x \in \mathbb{R}$ non $0 < x < 1\}$ azpimultzoa, multzo infinitu ez zenbakigarria da.*

Beraz, existitzen dira 0 eta 1 tartean zenbaki erreal kopuru gehiago, zenbaki arrazional guztiak batera baino. $(0, 1)$ tartearen kardinala eta $\mathbb{R}$ multzoaren kardinala berdina dira.

Orduan, $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$ dugu.

Gure hurrengo galdera, ea $\mathbb{R}$ baino kardinal haundiago duten multzoak existitzen diren, da.

Teorema. *Izan bedi A multzoa. Orduan, parteen multzoak, $\wp(A)$, hau da, A-ren azpimultzo guztietaz osatuta dagoen multzoak, A multzoaren kardinala baino kardinal haundiagoa du. Beste modu batetan esanda, $|A| < |\wp(A)|$.*

Beraz, edozein A multzoaren parteen multzoa osatuz, kardinal haundiagoa duen multzo bat eraikitzen da.

Orduan, kardinal infinitu duten infinitu multzo eraiki daitezke eta posible da horiek ordenatzea. $\mathbb{R}$-ren kardinala $\aleph_1$ bidez denotatuz, bere parteen multzoaren kardinala $\aleph_2$ bidez denotatuz, parte horien parteen multzoaren kardinala $\aleph_3$ bidez denotatuz, . . . , eta hurrenez hurren, $\aleph_0 < \aleph_1 < \aleph_2 < \ldots < \aleph_k < \ldots$, desberdintza erlazioa lortzen da.

Kardinal horiek *Kardinal transfinituak* deitzen dira.

4 Erlazio binarioak

Izan bitez A eta B bi multzo. Gogoratu A eta B multzoen biderkadura kartesiarra, $\{(a, b) \mid a \in A, b \in B\}$ multzo berria dela, $A \times B$ bidez denotatzen dena. Orduan, definizioz A multzoaren erlazio binarioa B multzoan, $A \times B$ multzoaren R azpimultzo bat da. Hau da, A multzotik B multzoan, $\Re$ erlazio binarioa ondoko eran definitzen da,

$$a \Re b \Longleftrightarrow (a, b) \in \text{ R } .$$

Orduan, $a \in A$ elementua, $b \in B$ elementu batekin $\Re$ erlazio binarioaren bidez erlazionatuta dagoela esaten da, baldin eta $(a,b) \in$ R bada, eta hori $a\Re b$ bidez denotatzen da.

Oharra. *Erlazio binario bat P propietate bategatik ere defini daiteke:*

$$a\Re b \Longleftrightarrow P(a,b) \textit{ egia}$$

Ondorioz, R ondoko eran adieraz daiteke,

$$R = \{(a,b) \in A \times B \mid P(a,b) \textit{ egia } \}.$$

Ondoren, $\Re$ erlazio binario baten eremua eta heina definituko ditugu,

(i) Eremua$(\Re) = \{a \in A \mid a\Re b, b \in B$ batentzat $\}$

(ii) Heina$(\Re) = \{b \in B \mid a\Re b, a \in A$ batentzat $\}$

Definizioa. *$\Re$ erlazio baten alderantzizkoa, $\Re^{-1}$ bidez denotatzen dena, $\{(b,a) \in B \times A \mid (a,b) \in R\}$ multzoari deitzen zaio.*

Definizioa. *Izan bitez $\Re$, A eta B multzoen arteko erlazio bat eta S, B eta C multzoen arteko beste erlazio bat. Definizioz, $\Re$ eta S erlazioen konposaketa deitzen zaio, $A \times C$ multzoko (a,c), zeinentzat existitzen den $b \in B$ elementu bat non $a\Re b$ eta bSc osatzen duten bikoteen azpimultzoari. Ondorioz, $S \circ \Re$, A eta C multzoen arteko erlazio bat da.*

Hemendik aurrera A multzo berdinaren gainean definitutako erlazio binarioekin lan egingo dugu, hau da, R $\subseteq A \times A$.

Definizioa. *Izan bedi A multzoa. A-tik A-ra definitutako $\Re$ erlazio bat, A-n erlazio binarioa dela esaten da. A-ren $\Re$ erlazio binarioa, ondoko eratatakoa izan daiteke,*

(i) *Erreflexiboa:* $\forall a \in A, a\Re a$

(ii) *Simetrikoa:* $\forall a,b \in A, a\Re b$ *baldintzatik,* $b\Re a$ *ondorioztatzen bada*

(iii) *Iragankorra:* $\forall a,b,c \in A, a\Re b$ *eta* $b\Re c$ *baldintzetatik,* $a\Re c$ *ondorioztatzen bada*

(iv) *Antisimetrikoa:* $\forall a,b \in A$, $a\Re b$ *eta* $b\Re a$ *baldintzetatik,* $a = b$ *ondorioztatzen bada*

(v) *Osoa: baldin eta* $a\Re b$ *edo* $b\Re a$ *bada, edozein* $a,b \in A$*-rako,* $a \neq b$ *izanik.*

Definizioa. *Izan bedi A-ren $\Re$ erlazio binarioa.*

(i) *A-n ordenazko erlazioa dela esaten da, baldin eta $\Re$ erreflexiboa, antisimetrikoa eta iragankorra bada. Kasu honetan, $(A, \Re)$ multzo ordenatua dela esaten da.*

(ii) *A-n baliokidetasun erlazioa dela esaten da, baldin eta $\Re$ erreflexiboa, simetrikoa eta iragankorra bada.*

Adibidea. *Ondokoak multzo ordenatuak dira,*

$$(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq),$$

$\leq$ ikurrak, aurreko multzo bakoitzean, ohiko txikiago edo berdina den desberdintza adierazten duelarik.

Adibideak. *Ondokoak baliokidetasun erlazio binarioak dira,*

(i) *$\mathbb{Z} \times \mathbb{Z}^*$ multzoan definitzen da,*

$$(a, b)\Re(c, d) \Longleftrightarrow ad = cb.$$

(ii) *$\mathbb{Z}$-n 2 moduluarekiko kongruentzia erlazioa. Izan bitez $a, b \in \mathbb{Z}$,*

$$a\Re b \Longleftrightarrow b - a, 2 \text{ zenbaki osoaren multiploa bada.}$$

(iii) *$\mathbb{Z}$-n n moduluarekiko kongruentzia erlazioa, $n \in \mathbb{N}$ izanik. Izan bitez $a, b \in \mathbb{Z}$,*

$$a\Re b \Longleftrightarrow b - a, n \text{ zenbaki osoaren multiploa bada.}$$

Aurreko $\Re$ erlazioan, baldin eta $a\Re b$ bada, $a \equiv b \pmod{n}$ bidez denotatuko da, eta a, b-rekin n moduluarekiko kongruentea dela esaten da.

Oharra. *Ondokoa dugu,*

$$a \equiv b \pmod{n} \Longleftrightarrow \exists k \in \mathbb{Z} \text{ non } b = a + nk.$$

Definizioa. *Izan bedi $\Re$, A multzoan definitutako baliokidetasun erlazioa. Orduan, $a \in A$ elementu bakoitzarentzat, a-ren baliokidetasun klasea, $\overline{a}$ bidez denotatzen dena, A-ko a-rekin erlazionatuta dauden elementu guztiek osatzen duten multzoari deitzen zaio.*

$$\overline{a} = \{x \in A \mid x\Re a\}.$$

Edozein $x \in \overline{a}$, $\overline{a}$ klasearen adierazlea edo errepresentantea da.

Proposizioa. *Izan bedi A multzoan definitutako $\Re$ baliokidetasun erlazioa. Edozein $a, b \in A$ elementuetako, ondokoa betetzen da,*

(i) $a \in \overline{a}$ *(eta ondorioz, $\overline{a} \neq \emptyset$ da). Bereziki, A-ko elementu guztiak baliokidetasun klaseren batetan daude.*

(ii) $\overline{a} = \overline{b} \Longleftrightarrow a\Re b$.

(iii) $\overline{a} \cap \overline{b} = \emptyset \Longleftrightarrow a$ *ez badago b-rekin erlazionatuta.*

Definizioa. *Izan bedi A multzoan definitutako $\Re$ baliokidetasun erlazioa. Definitzen da, A-ren zatikien multzoa $\Re$ erlazioren bidez, $A/\Re$ bidez denotatzen dena, A-ren elementu guztien baliokidetasun klaseetaz osatutako multzo gisa,*

$$A/\Re = \{\overline{a} \mid a \in A\}.$$

Adibidea. *Izan bedi $\mathbb{Z} \times \mathbb{Z}^*$ multzoan ondoren definitutako baliokidetasun erlazioa,*

$$(a, b)\Re(c, d) \Longleftrightarrow ad = cb.$$

Orduan, $\overline{(a, b)} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid \frac{a}{b} = \frac{c}{d}\}$, eta zatikien multzoa $(\mathbb{Z} \times \mathbb{Z}^*)/\Re = \mathbb{Q}$ da.

Ariketa. *Definitu zein den $\mathbb{Z}$-n, ($n \in \mathbb{N}$ izanik), n-moduluarekiko kongruentzia erlazioaren zatikien multzoa.*