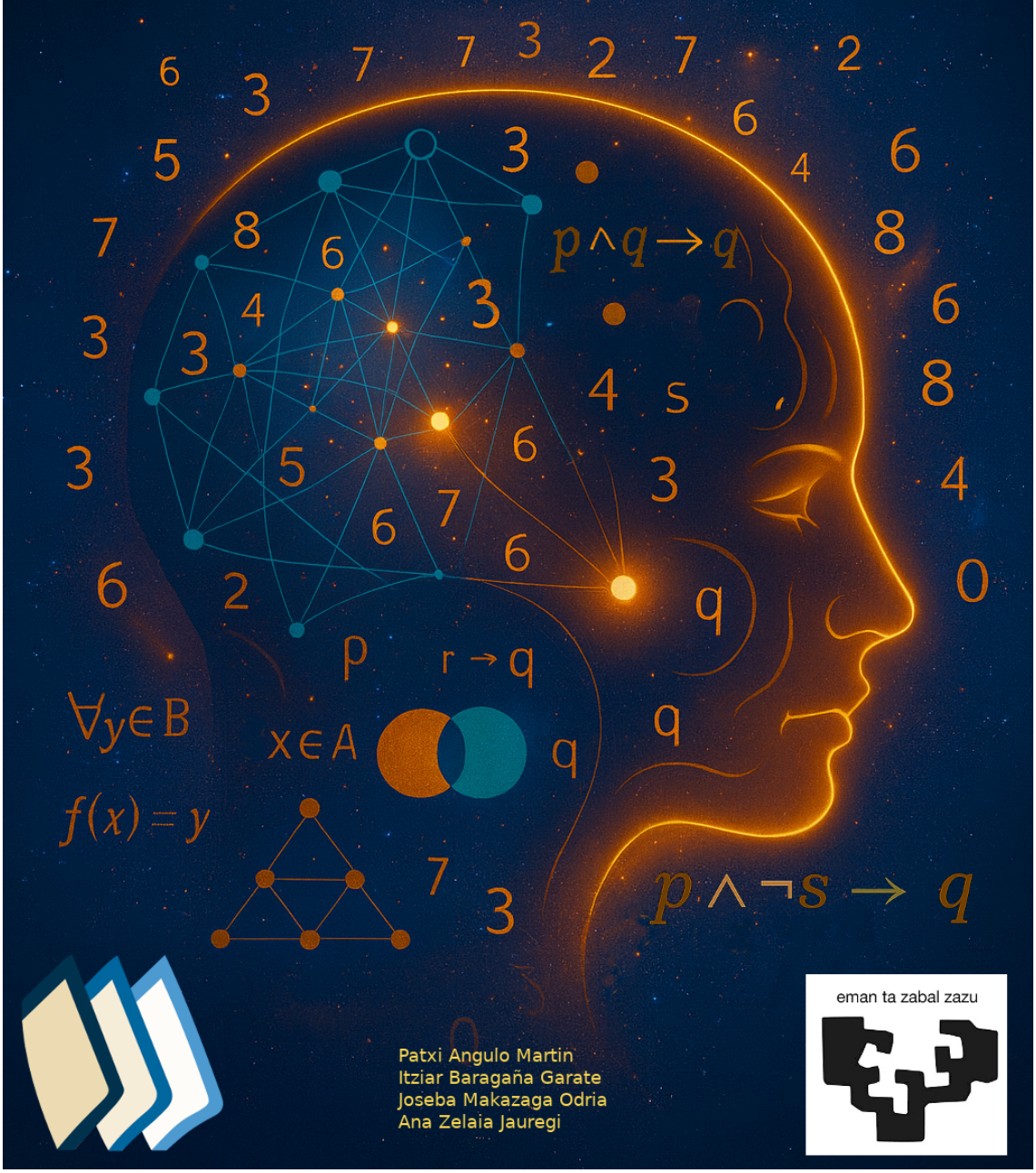
MATEMATIKA DISKRETUA



Patxi Angulo Martin
Itziar Baragaña Garate
Joseba Makazaga Odria
Ana Zelaia Jauregi

eman ta zabal zazu

Matematika Diskretua

Wikiliburua

(eu.wikibooks.org)

Patxi Angulo Martin

Itziar Baragaña Garate

Joseba Makazaga Odria

Ana Zelaia Jauregi

Konputazio Zientzia eta Adimen Artifiziala Saila
Informatika Fakultatea, EHU

eman ta zabal zazu

Donostia, 2025eko uztaila

Sarrera

Esku artean duzun liburuak Matematika Diskretuari buruzko gaiak jorratzen ditu. Garrantzia dute algoritmikan, programazio logikoan, software-sistemak eta hardware-sistemak garatzeko metodo formaletan, kriptografian, eta abarretan. Horregatik, Donostiako Informatika Fakultatean bai *Informatikaren Ingeniaritzako Graduan* eta bai *Adimen Artifizialeko Graduan* ere landu egiten den alorra da. Informatikaz haratago, beste hainbat arlotan beharrezkoa den oinarrizko ezagutza matematikoa jasotzeko ere garrantzitsua da.

EHUko irakasle garen aldetik, euskarazko irakaskuntzarako testu hau landu eta argitaratu dugu, ikasleari eskola-saioetan emandako azalpenetan sakontzeko lagungarri izango zaiolakoan. Bertan, ikasleak kontzeptu teorikoak eta horiek ulertzeko adibide ugari aurkituko ditu.

Gainera, Donostiako Informatika fakultateko EHU-Wikipedia proiektuan parte hartzen dugu eta bide horri jarraituz, ikasmaterial hau Wikimedia proiektuaren baitan Wikiliburuak plataforman (https://eu.wikibooks.org/) argitaratzeko erabakia hartu dugu. Formatu digitalean argitaratu nahi izan dugu, gure ikasleek eskura izan dezaten eta Matematika Diskretua ikasteko interesa duen edonork erraz aurkitzeko moduan egon dadin. Bi formatutan jarri dugu eskuragarri: wiki formatuan eta PDF formatuan. Horrela, dinamikoagoa izan daitekeen wiki formatuarekin batera, wikiliburuak 2025ean duen bertsio zainduaren argazki finko bat bertan geratuko da.

Wikiliburu moduan argitaratzeak hainbat onura ekar ditzakeela uste dugu:

1. Erraz aurkituko du Matematika Diskretuari buruzko interesa duenak, Web bilatzaileek eta Adimen Artifizialeko tresnek Wikipedia plataformak lehentasunez arakatzen dituztelako.

2. Erraz egunera daiteke, kapitulu berriren bat gehituz edo daudenak aberastuz. Horrela, wikiliburua izaki bizidun bihurtzen da eta euskal komunitatearen eskutik hobekuntzak jaso ditzake etengabe.

3. Edukia librea da, sormenezko lanak munduan zehar erraz partekatzeko CC-BY-SA nazioarteko lizentziapean argitaratua izan baita. Horrek esan nahi du, edonor aske dela materiala partekatzeko, beti ere, aitortza egokia eginez eta bertatik beste lanen bat eratortzen bada, jatorrizkoaren lizentzia berarekin banatuz.

Urtez urte, lan handia egiten da euskarazko liburugintzan bai EHUn, bai UEUn, bai Elhuyar-en, eta bai beste hainbat erakundetan ere; horien osagarri izan daiteke wikiliburuen aukera. Uste dugu bide horrek euskarazko ikasmaterialgintza dinamizatzeko aukera berriak irekitzen dituela eta bide berri hori bultzatu nahi izan dugu.

Donostia, 2025eko uztaila

Gaien Aurkibidea

1 Proposizio-logika **1**

1.1 Sarrera . . . 1
1.2 Proposizio-logika. Esaldien formalizazioa . . . 3
1.3 Sintaxia . . . 6
1.4 Semantika . . . 8
1.5 Baliozkotasuna. Inkontsistentzia. Baliokidetza logikoak . . . 11
1.6 Ondorio logikoak. Baliozko argumentuak . . . 15
1.7 Dedukzio formala . . . 20
1.7.1 Froga formala. Inferentzia-erregelak . . . 20
1.7.2 Ordezkapen-erregela . . . 23
1.7.3 Baldintzazko frogaren erregela . . . 25
1.7.4 Absurdora eramateko erregela . . . 27

2 Predikatu-logika **31**

2.1 Sarrera . . . 31
2.2 Sintaxia . . . 34
2.3 Semantika . . . 37
2.4 Baliozkotasuna. Inkontsistentzia. Ondorio logikoak . . . 43
2.5 Baliokidetza logikoak . . . 47
2.6 Dedukzio formala . . . 52

3 Multzoak. Erlazioak. Funtzioak **59**

3.1 Sarrera . . . 59
3.2 Multzoak . . . 59
3.2.1 Multzoak eta azpimultzoak . . . 59
3.2.2 Multzoen arteko eragiketak . . . 62
3.2.3 Multzo baten partiketa . . . 65
3.2.4 Bi multzoren arteko biderketa kartesiarra . . . 66
3.3 Erlazioak . . . 67
3.3.1 Definizioak . . . 67
3.3.2 Ordena-erlazioak . . . 69
3.3.3 Baliokidetasun-erlazioak . . . 70
3.3.4 n moduluko kongruentzia . . . 73
3.4 Funtzioak . . . 74
3.4.1 Definizioak . . . 74
3.4.2 Funtzio-motak . . . 78

3.4.3 Alderantzizko funtzioa . . . 79
3.4.4 Funtzioen konposizioa . . . 80

4 Zenbaki-teoria 85
4.1 Zenbaki osoak . . . 85
4.1.1 Eragiketak zenbaki osoen artean. Ordena onaren printzipioa . . . 85
4.1.2 Zatigarritasuna. Zenbaki lehenak . . . 86
4.1.3 Zatiketa euklidearra . . . 89
4.1.4 Zatitzaile komun handiena . . . 91
4.1.5 Euklidesen algoritmoa . . . 95
4.1.6 Multiplo komun txikiena . . . 99
4.1.7 Aritmetikaren oinarrizko teorema . . . 101
4.2 Aritmetika modularra . . . 104
4.2.1 Eragiketa modularrak . . . 104
4.2.2 Berreketa modularra . . . 107
4.3 RSA algoritmoa . . . 110
4.3.1 Oinarri teorikoa . . . 110
4.3.2 Algoritmoaren urratsak . . . 111
4.3.3 Mezu ziurtatuetarako erabilera . . . 114

5 Grafoak 115
5.1 Sarrera . . . 115
5.2 Definizioak . . . 116
5.3 Erpinen graduak . . . 118
5.4 Ibilaldiak grafo batean . . . 121
5.5 Grafo baten auzokidetasun-matrizea . . . 123
5.6 Azpigrafoak. Grafo osagarria . . . 125
5.7 Grafoen arteko isomorfismoak . . . 129
5.8 Kate eta zirkuitu eulertarrak . . . 130
5.9 Bide eta ziklo hamiltondarrak . . . 134
5.10 Zuhaitzak . . . 138
5.10.1 Sarrera . . . 138
5.10.2 Definizioak eta propietateak . . . 139
5.10.3 Zuhaitz errodunak. Zuhaitz bitarrak . . . 143

6 Konbinatoria 149
6.1 Sarrera . . . 149
6.2 Baturaren eta biderkaduraren arauak . . . 150
6.3 Aldakuntzak. Permutazioak . . . 151
6.4 Konbinazioak . . . 155
6.5 Errepikatuzko konbinazioak . . . 162

Bibliografia . . . 193

Aurkibide alfabetikoa . . . 195

1. Kapitulua

Proposizio-logika

1.1 Sarrera

Hizkuntzan adierazpen-perpausak, aginte-perpausak eta galde-perpausak erabiltzen ditugu. Ezagutza, funtsean, lehenek deskribatzen dute.

Ezagutza bi bidetik jaso dezakegu: gertakariak edo ideiak egiaztatuz, adierazpen-perpausen bidez, edo dedukzioaren bidez.

Logika formalaren helburua dedukzioa (arrazoibidea, inferentzia, argudiatzea) da. Dedukzioa ezagutzen diren datu batzuetatik ezagutza berria sortzean datza. Arrazoibide baten ezaugarri nagusia hau da: abiapuntutzat hartzen ditugun baieztapen (premisa) batzuetatik beste baieztapen (ondorio) bat ondorioztatzea. Gogoratzea edota imajinatzea, adibidez, pentsaerak dira, baina ez dira arrazoibideak.

Arrazoibide orok forma eta edukia ditu.

Arrazoibide hauek edukian bereizten dira:

(1) Lehoi guztiak ugaztunak dira.
Ugaztun guztiek birikak dituzte.
Beraz, lehoi guztiek birikak dituzte.

(2) Zenbaki arrunt guztiak bikoitiak dira.
Zenbaki bikoiti guztiak lehenak dira.
Beraz, zenbaki arrunt guztiak lehenak dira.

baina forma bera dute:

a guztiak b dira.
b guztiak c dira.
Beraz, a guztiak c dira.

Logika arrazoibideen forman bakarrik aritzen da. Horregatik da *logika formala* baliozko arrazoibideen eskemen edo formen zientzia.

Aurreko eskema baliozkoa da, premisak egiazkoak badira, ondorioa halabeharrez izango baita egiazkoa.

Ohar gaitezen arrazoibidea baliozkoa izan daitekeela premisak egiazkoak edo faltsuak diren kontuan izan gabe. Arrazoibide zuzena izan daiteke, nahiz eta premisak eta ondorioa faltsuak izan, (2) adibidean bezala.

Arrazoibide bat *baliozkoa* edo *zuzena* da, bere premisak egiazkoak izanik, ondorioa ezin denean faltsua izan. Premisak egiazkoak izan edo faltsuak izan beste kontu bat

da, logikatik at geratzen den kontua (zenbaki bikoitiak lehenak izan ala ez aritmetikaren kontua da, ez logikarena).

Ikus ditzagun beste adibide batzuk:

(3) Pilotan ari banaiz, kirolean ari naiz.
Kirolean ari naiz.
Beraz, pilotan ari naiz.

arrazoibidea eskema honi lotzen zaio:

a bada, orduan b.
b.
Beraz, a.

(4) Aberatsa banaiz, ona naiz.
Ez naiz aberatsa.
Beraz, ez naiz ona.

Dagokion eskema hau da:

a bada, orduan b.
Ez a.
Beraz, ez b.

Arrazoibide horiek ez dira zuzenak, gerta baitaiteke premisak egiazkoak izatea eta, hala ere, ondorioa faltsua izatea.

Logikak arrazoibideen forman oinarritu behar du, edukiak kontuan izan gabe. Horregatik gainditu behar du hizkuntza naturalaren joera, non forma eta edukia nahasirik ematen baitira. Bestalde, forma isolaturik agertzen duen lengoaia bat erabili behar dugu, hots, arrazoibideen egitura bakarrik erakusten duen lengoaia.

Horregatik sortuko dugu lengoaia artifiziala, *objektu lengoaia* deituko duguna. Eta horri buruz hitz egiteko erabiliko dugun hizkuntzari *metalengoaia* deituko diogu. Adibidez, euskaraz idatzitako ingelesari buruzko liburu batean, euskara metalengoaia da.

Zeinuak edo hizkuntzak, zeinu-sistema gisa, aztertzen dituen zientzia *semiotika* da. Semiotika sintaxiak, semantikak eta pragmatikak osatzen dute.

Sintaxiak zeinuen arteko erlazioak bakarrik aztertzen ditu. Ongi osatutako zeinuen segidak ezagutu eta eraiki egiten ditu. Esaterako, "da hau erloju Arantzarena" hitzen segida gaizki osaturik dagoela esaten dugunean, arazo sintaktiko bati heltzen diogu.

Semantikak, beste aldetik, zeinuen eta zeinuek adierazten dutenaren arteko erlazioak aztertzen ditu; hau da, zeinuen eta horiekin aipatzen ditugun zera horien arteko erlazioak (izen berezien eta izendatutakoen arteko erlazioak, enuntziatuen eta enuntziatuek deskribatzen dutenaren arteko erlazioak...): "Multzo-teorian, multzo hutsa elementurik ez duen multzoa da" esaten dugunean, semantikan ari gara.

Azkenik, *pragmatikan* hizkuntzaren elementuen eta hizkuntz komunitateko kideen arteko erlazioek ere hartzen dute parte. Esate baterako, "abertzale" hitzak esanahi desberdina du, erabiltzailearen arabera.

Hau da, pragmatika egiten dugunean, hizkuntzaz kezkatuko gara, subjektu baten edo talde baten jokabide gisa. Semantikan, aldiz, hiztunaz ahaztuko gara, eta bere hizkerak erabiltzen dituen zeinuen eta zeinu horiek irudikatzen dituzten gauzen arteko erlazioak aztertuko ditugu. Sintaxian, azkenik, zeinuak eta zeinuen arteko erlazioak bakarrik aztertuko ditugu, kontuan izan gabe zeinu horiek aipatzen dituzten gauzak edo egoerak.

Lengoaiaren formak sinbolizatzean, bi maila bereiz ditzakegu: Proposizio-logika eta Predikatu-logika.

Proposizio-logika: hizkuntza arruntaren adierazpen-perpausa bakunak (*proposizioak*) oinarrizko elementutzat hartuko ditugu, eta adierazi.

Predikatu-logika: proposizioen osagai batzuk oinarrizko elementutzat hartuko ditugu, eta adierazi: *terminoak* eta *predikatuak*.

Lengoaia adierazteko bi maila horietarako bi eratan adieraz daitezke dedukziozko egitura zuzenak:

Interpretazio-teoria edo *Eredu-teoria*: proposizioei eta dedukziozko egitura zuzenei egoki dakizkiekeen esanahiak (gehienetan egiazkoa eta faltsua) definitzean datza.

Frogabidearen eta dedukzio naturalaren teoria: dedukziozko egitura zuzen batzuk eta horietatik dedukziozko egitura berri batzuk lortzeko arauak axiomatikoki definitzean datza.

1.2 Proposizio-logika. Esaldien formalizazioa

Logika formalaren azterketa oinarritik hasiko dugu, proposizioen edo enuntziatuen logikatik hain zuzen.

Sinbolizazio-maila honetan lengoaia elementu hauek osatuko dute:

- Enuntziatu bakunak, proposizio atomikoak deituak;
- lokailuak.

Enuntziatu bakuna (*proposizio atomikoa*) informazioa duen hizkuntzaren gutxieneko unitatetzat har dezakegu, informazio horri buruz zerbait esan dezakegularik (egiazkoa edo faltsua dela):

Esate baterako, “euria ari du”, “Ane azkarra da”.

Hizkuntzaren “euria”, “Ane” elementuek ez dute berezko informaziorik, ez badira elkartzen beste elementu batzuekin; ez dira, beraz, proposizioak. Horregatik ez dira agertuko proposizio-logikan; predikatu-logikan, ordea, bere lekua izango dute.

Aurreko enuntziatuak ezin dira banatu informazioa duten hizkuntzaren elementu txikiagoetan. Izan ere, “ari du” zatiak ez du informaziorik ematen ez bazaio zerbaiti lotzen.

“Euria ari du eta bustitzen ari naiz” esaldia, ordea, bi zatitan bana dezakegu “eta” hitzaren bidez (“euria ari du”, “bustitzen ari naiz”), bakoitzak berezko informazioa ematen duelarik.

“Eta” hizkuntzaren elementua da eta bi proposiziotik esaldi berri bat eraikitzeko balio du; esaldi berriaren informazioa proposizioena bera da, baina aldiberekotasuna erantsiz. “Euria ari du eta bustitzen ari naiz” *proposizio konposatuaren* adibidea da.

Hizkuntzan badira beste hitz batzuk esaldiak alboratzeko: “baina”, “hala ere”, “ordea”, “nahiz eta”... Horiek guztiek, informazio-edukiaren ikuspuntutik, “eta” hitzaren paper bera jokatzen dute. Hala ere, hiztunari aukera ematen diote esaldi batzuk azpimarratzeko beste esaldi batzuen aurrean. Proposizio-logikan ez ditugu eite horiek kontuan izango, eta horregatik beren adierazpen matematikoa “eta” hitzarena izango da.

Aurreko adibidean “eta” lokailu bat da. *Lokailu* bat esaldi batzuetatik esaldi berri bat eraikitzeko aukera ematen duen hizkuntzaren elementu bat da, esaldi lotuen informazioei ñabardurak eransten dizkiona. Gorago esan bezala, lokailu bera, informazio-edukiaren ikuspuntutik, hizkuntza arruntaren zenbait elementuren bidez gauza daiteke.

Proposizio-logikaren lokailuak hauek dira: ukapena, konjuntzioa, disjuntzioa, baldintzazkoa eta baldintzabikoa.

Proposizio-logikaren sinbolizazio matematikoa proposizioetan eta lokailuetan oinarritzen da; honela:

- $p, q, r, s, \ldots$ hizkiek proposizio atomikoak adieraziko dituzte. Adibidez, "euria ari du" esaldia p adieraziko dugu, eta "bustitzen ari naiz" esaldia q.

- Lokailuak adierazteko sinbolo hauek erabiliko ditugu:

- Ukapena: $\neg$
- Konjuntzioa: $\wedge$
- Disjuntzioa: $\vee$
- Baldintzazkoa edo inplikazioa: $\rightarrow$
- Baldintzabikoa: $\leftrightarrow$

Horrela, "Euria ari du eta bustitzen ari naiz", "Aldi berean euria ari du eta bustitzen ari naiz" "Euria ari du, baina bustitzen ari naiz", "Euria ari du, hala ere bustitzen ari naiz", "Euria ari duen bitartean bustitzen ari naiz" esaldiak honela adieraziko ditugu:

$$p \wedge q$$

Azpimarratzekoa da $p \wedge q$ esaldiaren egitura adierazteko era bat dela, eta ez esaldia idazteko era bat. Logika egitura horien azterketaz arduratzen da, ez informazioaren edukiaz.

Jarraian lokailuak definituko ditugu:

Ukapena: $\neg p$

p motako proposizio batetik "ez p", "p faltsua da", "p ez da egiazkoa" motako proposizioa eraikitzeko aukera ematen duen lengoaiaren elementua da.

Konjuntzioa: $p \wedge q$

p, q bi proposizioak lotuz "p eta q", "p, baina q", "p, hala ere q", "p, nahiz eta q"... motako proposizioa eraikitzeko aukera ematen duen lengoaiaren elementua da.

Disjuntzioa: $p \vee q$

p, q bi proposizioak lotuz "edo p edo q edo biak", "gutxienez p edo q"... motako proposizioak eraikitzeko erabiliko dugun lengoaiaren elementua da.

Hizkuntza arruntaren "edo", "ala" hitzek bi esanahi dituzte: *Inklusiboa*: Larunbatean edo igandean hots egingo dizut. *Esklusiboa*: Zenbaki bakoitia edo bikoitia da.

Ez dakigu esaldi batzuetan zentzu inklusiboa edo esklusiboa dagoen. Baina logikaren ikuspuntutik interesgarriagoa da zentzu inklusiboa esklusiboa baino. Hortaz, $\vee$ beti izango da inklusiboa.

Baldintzazkoa edo *inplikazioa*: $p \rightarrow q$

Hizkuntza arruntaren kausa-ondorio erlazioa adierazteko erabiliko dugu: "p bada, q", "p soilik baldin q", "q p bada", "q beharrezkoa da p izateko", "p nahikoa da q izateko", "ez p ez bada q"... p *aurrekaria* (baldintza) eta q *atzekaria* (ondorioa) deituko ditugu.

Baldintzabikoa: $p \leftrightarrow q$

"p nahikoa eta beharrezkoa da q izateko", "p baldin eta soilik baldin q bada" bezalako esaldiak adierazteko erabiliko dugu.

Adibideak

1. "a bikoitia bada, $a-3$ bakoitia da eta a^2-3 bakoitia da".

   Proposizio atomikoak hauek dira:

   - p: "a bikoitia da"

   - q: "$a-3$ bakoitia da"

   - r: "a^2-3 bakoitia da"

   Formalki, esaldia inplikazio bat da, aurrekaria lehenengo proposizioa eta atzekaria azkeneko bien konjuntzioa izanik. Proposizio-logikan honela adieraziko dugu esaldi hori:

   $$p \to (q \wedge r)$$

   Adierazpen hori beste era honetan ere irakur dezakegu: "a ez da bikoitia $a-3$ eta a^2-3 ez badira bakoitiak".

2. "Mendira joango naiz edo hondartzara joango naiz soilik eguraldi ona egiten badu".

   - p: "mendira joango naiz"

   - q: "hondartzara joango naiz"

   - r: "eguraldi ona egiten du"

   Honela adieraziko dugu esaldia:

   $$(p \vee q) \to r$$

   Adierazpen hori bera erabiliko dugu honetarako: "Ni mendira edo hondartzara joateko, beharrezkoa da eguraldi ona egitea".

3. Programazioko "If p then q else r" egitura logikoak "p bada, orduan q, eta p ez bada, orduan r". Bere adierazpena proposizio-logikan hau da:

   $$(p \to q) \wedge (\neg p \to r)$$

Oharra. Hizkuntza arruntean, testuinguruak eta keinuek lagundu egiten dute esaldien arteko loturak ulertzen. Lengoaia formalean parentesiak erabili beharko ditugu lokailu bakoitzari dagokion proposizioa zehazteko. Horrez gain, hizkuntza arruntean ez dira gorago aipatutako bi lokailu jarraian agertzen.

Beraz, "forma" hauek idazteko arauak definitu beharko ditugu, hizkuntza arruntean esaldiak eraikitzeko erabiltzen ditugun arauetatik abiatuta.

Hau da, proposizioen "formak", formula deituko ditugunak, idazteko sintaxia definitu beharko dugu, aurretik aipatu ditugun baldintzak kontuan izanik (lokailuak jarraian ez, proposizioen eta lokailuen arteko erlazioak definitu...).

1.3 Sintaxia

Lengoaia baten sintaxia zeinuen arteko erlazioaz arduratzen da; hau da, zeinuen segida ongi eratuak ezagutu eta eraikitzen dituen teoria da.

1.1 Definizioa. *Proposizio-lengoaiaren* $\mathcal{A}$ alfabetoa *sinbolo hauek osatzen dute:*

1. *Enuntziatu bakunak adierazteko erabiliko ditugun sinboloak:* $\mathcal{P} = \{p, q, r, s, \cdots\}$. *Sinbolo hauei* atomo *deituko diegu.*

2. Lokailu logikoak *(edo* eragile logikoak*) adierazteko sinboloak:* $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.

3. *Sinbolo inpropioak: parentesiak,* $\{(,)\}$.

$$\mathcal{A} = \mathcal{P} \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\} \cup \{(,)\}.$$

1.2 Definizioa. Formula *bat* $\mathcal{A}$ *multzoaren elementuekin eratutako segida finitu bat da. Adibidez,* $p \vee \neg q \rightarrow$, $pr(\vee s$, $(q \vee t)$...

1.3 Definizioa. *Proposizio-logikan* ongi eratutako formulak *(oef) arau hauei jarraituz eraikiko ditugu:*

1. *Atomo bat ongi eratutako formula da.*

2. A *eta* B *ongi eratutako formulak badira,* $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ *eta* $(A \leftrightarrow B)$ *ere ongi eratutako formulak dira.*

3. *Aurreko bi arauak kopuru finitu aldiz erabiliz lortzen diren formulak soilik dira ongi eratutako formulak.*

Adibidez, hauek ongi eratutako formulak dira: p, q, r, $(\neg r)$, $(p \vee q)$ eta $((p \vee q) \rightarrow (\neg r))$. Beste hauek, ordea, ez dira: $(p \vee)$ eta $(q \rightarrow$.

Hemendik aurrera, formulez hitz egiten dugunean ongi eratutako formulei (oef) buruz arituko gara.

1.4 Definizioa. G *formula izanik,* G *formularen* azpiformula *ongi eratutako formula bat da,* G *formularen zatia bada eta ondoz ondo eraikia bada.*

Adibidez, $G = ((p \vee q) \rightarrow (\neg r))$ bada, $(p \vee q)$ eta $(\neg r)$ azpiformulak dira, baina $(q \rightarrow (\neg r))$ ez da azpiformula.

1.5 Definizioa. *Formula batean, lokailu baten* agerpen *baten* irismena *agerpen horrek eragiten dituen azpiformulak dira.*

Formula bat idazterakoan parentesi batzuk ezaba ditzakegu:

1. Nahasteko arriskurik ez dagoenean. Adibidez, $((p \vee q) \rightarrow (\neg r))$ formula honela idatz dezakegu: $(p \vee q) \rightarrow \neg r$.

2. Lokailuen artean hierarkia bat definituz:

   - 1. maila: $\neg$.
   - 2. maila: $\wedge$, $\vee$.
   - 3. maila: $\rightarrow$, $\leftrightarrow$.

   Formula batean maila desberdinetako lokailuak agertzen direnean, maila goreneko lokailuak ez du parentesien beharrik izango.

   Hierarkia hau aritmetikako eragiketetarako erabiltzen dugun hierarkiaren antzekoa da. Adibidez, $((\neg p) \wedge q) \rightarrow r$ formula honela idatz dezakegu: $\neg p \wedge q \rightarrow r$. Aritmetikan, $((-p) \cdot q) + r$ honela idazten dugun bezala: $-p \cdot q + r$.

1.6 Adibideak.

1. $(\neg p) \vee (\neg q)$ formula $\neg p \vee \neg q$ idatz dezakegu; izan ere, $\vee$ lokailua $\neg$ lokailua baino maila altuagokoa denez, $(\neg p)$ eta $(\neg q)$ formulen parentesiak ken ditzakegu.

   Lokailu baten agerpen bakoitzaren irismena adierazteko, agerpen hori eta bere irismena etiketatuko ditugu, honela:

$$\begin{array}{ccc} \underline{\neg p}_1 & \vee_1 & \underline{\neg q}_1 \\ \neg_2 \underline{p}_2 & & \neg_3 \underline{q}_3 \\ p & & q \end{array}$$

2. $(p \wedge q) \rightarrow (r \vee s)$ formula $p \wedge q \rightarrow r \vee s$ idatz dezakegu, $\rightarrow$ lokailua 3. mailakoa denez, $\wedge$ eta $\vee$ lokailuek lotzen dituzten $(p \wedge q)$ eta $(r \vee s)$ formulen parentesiak ken ditzakegu.

$$\begin{array}{ccc} \underline{p \wedge q}_1 & \rightarrow_1 & \underline{r \vee s}_1 \\ \underline{p}_2 \wedge_2 \underline{q}_2 & & \underline{r}_3 \vee_3 \underline{s}_3 \\ p \quad q & & r \quad s \end{array}$$

3. $((r \wedge s) \vee p) \rightarrow ((\neg p) \wedge q)$ formula $(r \wedge s) \vee p \rightarrow \neg p \wedge q$ idatz dezakegu.

   Ezin dugu parentesi gehiagorik kendu, $\wedge$ eta $\vee$ maila berekoak direlako.

$$\begin{array}{ccc} \underline{(r \wedge s) \vee p}_1 & \rightarrow_1 & \underline{\neg p \wedge q}_1 \\ \underline{(r \wedge s)}_2 \vee_2 \underline{p}_2 & & \underline{\neg p}_4 \wedge_4 \underline{q}_4 \\ \underline{r}_3 \wedge_3 \underline{s}_3 \quad p & & \neg_5 \underline{p}_5 \quad q \\ r \quad s & & p \end{array}$$

4. $(p \leftrightarrow q \wedge r) \rightarrow \neg s$ formulan lokailuen agerpenen irismenak hauek dira:

$$\begin{array}{ccc} \underline{(p \leftrightarrow q \wedge r)}_1 & \rightarrow_1 & \underline{\neg s}_1 \\ \underline{p}_2 \leftrightarrow_2 \underline{q \wedge r}_2 & & \neg_4 \underline{s}_4 \\ p \quad \underline{q}_3 \wedge_3 \underline{r}_3 & & s \\ q \quad r & & \end{array}$$

   Hortaz, parentesiak jarriz gero, formula hau izango dugu:

$$((p \leftrightarrow (q \wedge r)) \rightarrow (\neg s)).$$

1.4 Semantika

Atomoak adierazpen-perpausak idazteko erabiliko ditugu; eta horiek, beste perpausa motak ez bezala, egiazkoak edo faltsuak dira beti. Beraz, atomoak egiazko edo faltsu balioak har ditzaketen aldagaitzat hartuko ditugu. Proposizio atomiko baten egiazkotasunari edo faltsutasunari proposizioaren *egia-balio* deituko diogu.

Adibidez, p aldagaiak egiazko edo faltsu balioak har ditzake, eta honela azalduko dugu:

$$\begin{array}{c} p \\ \hline E \\ F \end{array} \quad \text{edo} \quad \begin{array}{c} p \\ \hline 1 \\ 0 \end{array},$$

non 1 balioak egiazkoa eta 0 balioak faltsua esan nahi duten.

p aldagai baten ordez, p eta q bi aldagai hartzen baditugu, eta dagozkien egia-balioak konbinatzen baditugu, honelako taula bat lortuko dugu:

p	q
E	E
E	F
F	E
F	F

$4 = 2^2$ aukera.

Hiru aldagai baditugu, p, q eta r taula hau izango dugu:

p	q	r
E	E	E
E	E	F
E	F	E
E	F	F
F	E	E
F	E	F
F	F	E
F	F	F

$8 = 2^3$ aukera.

Oro har, n atomo badauzkagu, $p_1, p_2, \ldots, p_n$, beren egia-balioen konbinazioen kopurua 2^n izango da.

1.7 Definizioa. *Izan bitez A ongi eratutako formula eta $p_1, p_2, \ldots, p_n$ ($p_i \neq p_j, i \neq j$) A formulan agertzen diren atomoak. A formularen* interpretazio *bat $p_1, p_2, \ldots, p_n$ atomoei egia-balioak esleitzean datza, honela: p_i atomoei balio bana, E edo F, esleitzen zaie.*

Formulak n atomo baditu, formulak 2^n interpretazio desberdin izango ditu.

1.8 Adibidea. Izan bedi $A = (p \to q) \wedge (q \to r)$. A formulan 3 atomo desberdin agertzen dira. Hortaz, 8 interpretazio desberdin izango ditu A formulak, aurreko taularen 8 lerroak hain zuzen.

$p_1, p_2, \ldots, p_n$ badira A ongi eratutako formulan agertzen diren atomo desberdinak, A formularen interpretazio bat multzo bat gisa adieraz dezakegu,

$$I = \{m_1, \ldots, m_n\},$$

non m_i bakoitza honela zehaztuko dugun:

$$m_i = \begin{cases} p_i, & p_i \text{ atomoari } E \text{ balioa esleitzen badiogu,} \\ \neg p_i, & p_i \text{ atomoari } F \text{ balioa esleitzen badiogu.} \end{cases}$$

1.9 Adibidea. Hona hemen $A = (p \to q) \wedge (q \to r)$ formularen interpretazio batzuk: $I_1 = \{p, q, r\}$, $I_2 = \{p, q, \neg r\}$, $I_3 = \{p, \neg q, r\}$, $I_5 = \{\neg p, q, r\}$, etab. I_3 interpretazioan, p eta r atomoei E balioa esleitu diegu, eta q atomoari F balioa.

G ongi eratutako formula eta I bere interpretazio bat izanik, G formularen I interpretaziorako *egia-balioa* kalkula dezakegu. Egia-balio hori $V(G, I)$ idatziko dugu eta ondoko bost erregelak, lokailu bakoitzeko bat, aplikatuz kalkulatuko dugu:

Erregelak

Izan bitez A eta B ongi eratutako bi formula, edozein:

1. $V((\neg A), I) = E$ izango da $V(A, I) = F$ denean eta $V((\neg A), I) = F$ izango da $V(A, I) = E$ denean. Taula eta definizioa:

A	$\neg A$
E	F
F	E

$$V((\neg A), I) = \begin{cases} E, & V(A, I) = F \text{ bada,} \\ F, & V(A, I) = E \text{ bada.} \end{cases}$$

2. $V((A \wedge B), I) = E$ izango da $V(A, I) = V(B, I) = E$ denean eta $V((A \wedge B), I) = F$ izango da bestelako kasuetan. Taula eta definizioa:

A	B	$A \wedge B$
E	E	E
E	F	F
F	E	F
F	F	F

$$V((A \wedge B), I) = \begin{cases} E, & V(A, I) = V(B, I) = E \text{ bada,} \\ F, & \text{bestela.} \end{cases}$$

3. $V((A \vee B), I) = F$ izango da $V(A, I) = V(B, I) = F$ denean eta $V((A \vee B), I) = E$ izango da bestelako kasuetan. Taula eta definizioa:

A	B	$A \vee B$
E	E	E
E	F	E
F	E	E
F	F	F

$$V((A \vee B), I) = \begin{cases} F, & V(A, I) = V(B, I) = F \text{ bada,} \\ E, & \text{bestela.} \end{cases}$$

Ohar gaitezen $\vee$ *disjuntzio inklusiboa* dela. *Disjuntzio esklusiboak* F bat izango luke lehenengo lerroan.

4. $V((A \to B), I) = F$ izango da $V(A, I) = E$ eta $V(B, I) = F$ direnean, eta bestelako kasuetan $V((A \to B), I) = E$ izango da. Taula eta definizioa:

A	B	$A \to B$
E	E	E
E	F	F
F	E	E
F	F	E

$$V((A \to B), I) = \begin{cases} F, & V(A, I) = E \text{ eta } V(B, I) = F \text{ bada,} \\ E, & \text{bestela.} \end{cases}$$

Ohar gaitezen, $V(A, I) = F$ bada, $V((A \to B), I) = E$ dela beti, nahiz eta A eta B formulen artean erlaziorik ez egon; berdin $V(B, I) = E$ denean.

5. $V((A \leftrightarrow B), I) = E$ izango da $V(A, I) = V(B, I)$ denean eta $V((A \leftrightarrow B), I) = F$ izango da bestelako kasuetan. Taula eta definizioa:

A	B	$A \leftrightarrow B$
E	E	E
E	F	F
F	E	F
F	F	E

$$V((A \leftrightarrow B), I) = \begin{cases} E, & V(A, I) = V(B, I) \text{ bada,} \\ F, & \text{bestela.} \end{cases}$$

1.10 Definizioa. *G ongi eratutako formula bada eta I bere interpretazio bat bada, esango dugu G formula I* interpretaziorako egiazkoa *dela, edo I interpretazioak G formula* egiazko egiten *duela, edo I interpretazioa G formularen* eredu *bat dela, $V(G, I) = E$ bada. Eta $I \models G$ idatziko dugu. $V(G, I) = F$ bada, ordea, G formula I* interpretaziorako faltsua *dela, edo I interpretazioak G formula* faltsu egiten *duela, esango dugu.*

Aurreko bost erregelekin ongi eratutako edozein formularen egia-balioa kalkula dezakegu interpretazio baterako.

1.11 Adibidea. Izan bedi $A = (p \to q) \wedge (q \to r)$ eta izan bedi $I_3 = \{p, \neg q, r\}$ interpretazioa. Ikus ditzagun, lehendabizi, lokailuen agerpenen irismenak:

$$\begin{array}{ccc} \underline{(p \to q)}_1 & \wedge_1 & \underline{(q \to r)}_1 \\ \underline{p}_2 \to_2 \underline{q}_2 & & \underline{q}_3 \to_3 \underline{r}_3 \end{array}$$

eta osa dezagun taula:

p	q	r	$p \to q$	$q \to r$	A
E	F	E	F	E	F

Beraz, I_3 interpretazioak A formula faltsu egiten du.

Saia gaitezen, orain, $I_7 = \{\neg p, \neg q, r\}$ interpretazioarekin. Taula hau da:

p	q	r	$p \to q$	$q \to r$	A
F	F	E	E	E	E

Beraz, I_7 interpretazioak A formula egiazko egiten du. Hau da, $I_7 \models A$.

Modu berean, A formularen egia-balioak kalkula ditzakegu 8 interpretazioetarako.

Adibidean ikus dezakegun bezala, formula bat ez da berez egiazkoa edo faltsua, baizik eta egiazkoa edo faltsua da interpretazio baterako.

Formula baten interpretazio guztietarako egia-balioak erakusten dituen taula bati formularen *egia-taula* deituko diogu.

1.12 Adibideak.

1. $A = (p \to q) \wedge (q \to r)$ formularen egia-taula:

p	q	r	$p \to q$	$q \to r$	A
E	E	E	E	E	E
E	E	F	E	F	F
E	F	E	F	E	F
E	F	F	F	E	F
F	E	E	E	E	E
F	E	F	E	F	F
F	F	E	E	E	E
F	F	F	E	E	E

2. $B = p \to (q \vee r \to (r \to \neg p))$ formularen egia-taula:

p	q	r	$\neg p$	$q \vee r$	$r \to \neg p$	$q \vee r \to (r \to \neg p)$	B
E	E	E	F	E	F	F	F
E	E	F	F	E	E	E	E
E	F	E	F	E	F	F	F
E	F	F	F	F	E	E	E
F	E	E	E	E	E	E	E
F	E	F	E	E	E	E	E
F	F	E	E	E	E	E	E
F	F	F	E	F	E	E	E

1.5 Baliozkotasuna. Inkontsistentzia. Baliokidetza logikoak

1.13 Definizioa. *A ongi eratutako formula bat izanik, esango dugu*

1. *A formula* kontsistentea *dela gutxienez A formularen interpretazio baterako egiazkoa bada.*

2. *A formula* tautologia *edo* baliozkoa *dela A formularen interpretazio guztietarako egiazkoa bada. Eta $\models A$ adieraziko dugu.*

3. *A formula* inkontsistentea *edo* kontraesana *dela ez bada kontsistentea, hau da, A formularen interpretazio guztietarako faltsua bada.*

4. *A formula* baliogabea *dela ez bada baliozkoa, hau da, gutxienez A formularen interpretazio baterako faltsua bada.*

1.14 Adibideak.

1. Izan bedi $A = (p \to q) \wedge p \to q$; bere egia-taula hau da:

p	q	$p \to q$	$(p \to q) \wedge p$	A
E	E	E	E	E
E	F	F	F	E
F	E	E	F	E
F	F	E	F	E

   Hortaz, A tautologia da, $\models A$, eta kontsistentea da.

2. Izan bedi $B = (p \to q) \wedge (p \wedge \neg q)$; bere egia-taula hau da:

p	q	$p \to q$	$\neg q$	$p \wedge \neg q$	B
E	E	E	F	F	F
E	F	F	E	E	F
F	E	E	F	F	F
F	F	E	E	F	F

   Beraz, B inkontsistentea eta baliogabea da.

3. Izan bedi $C = p \vee \neg q$; bere egia-taula hau da:

p	q	$\neg q$	$p \vee \neg q$
E	E	F	E
E	F	E	E
F	E	F	F
F	F	E	E

   Beraz, C kontsistentea eta baliogabea da.

Egia-taularen arabera aukera hauek guztiak izango ditugu formula baterako:

$$\text{Taula} \begin{cases} \text{Dena } E & \text{Tautologia; kontsistentea} \\ \text{Batzuk } E \text{ eta beste batzuk } F & \text{Kontsistentea; baliogabea} \\ \text{Dena } F & \text{Inkontsistentea; baliogabea} \end{cases}$$

Ondoko taulan, emandako lau definizioen arteko nahasketa guztiak ikusiko ditugu:

	Kontsistentea	Inkontsistentea (Kontraesana)
Baliozkoa (Tautologia)	Bai	Ez
Baliogabea	Bai	Bai

Bestalde, erraz ikus dezakegu, A formula bat izanik,

A tautologia da baldin eta soilik baldin $\neg A$ inkontsistentea bada.
A inkontsistentea da baldin eta soilik baldin $\neg A$ tautologia bada.
A tautologia bada, A kontsistentea da; baina elkarrekikoa ez da, orokorrean, egiazkoa.
A inkontsistentea bada, A baliogabea da, eta elkarrekikoa ez da, orokorrean, egiazkoa.

1.14 Adibidean, C kontsistentea da, baina ez da tautologia. Eta C baliogabea da, baina ez da kontraesana.

1.15 Definizioa. *A eta B ongi eratutako bi formulak* logikoki baliokideak *dira egia-balio berberak badituzte interpretazio guztietarako ($V(A, I) = V(B, I)$ da I interpretazio guztietarako), edo berdina dena, A eta B formulen egia-taulak berdinak direnean.*

A eta B formula logikoki baliokideak badira, $A \equiv B$ idatziko dugu.

1.16 Adibidea. Izan bitez $A = p \to q$ eta $B = \neg p \vee q$ formulak; beren egia-taulak hauek dira:

p	q	$p \to q$	$\neg p$	$\neg p \vee q$
E	E	E	F	E
E	F	F	F	F
F	E	E	E	E
F	F	E	E	E

Beraz, A eta B baliokideak dira, hots, $A \equiv B$.

Baliokidetza logikoak

Baliokidetza logikoen artean hauek aipatuko ditugu: A, B eta C ongi eratutako formulak izanik,

1. Elkartze-legeak (ELKAR)

$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C) \qquad (A \vee B) \vee C \equiv A \vee (B \vee C)$$

2. Trukatze-legeak (TRUK)

$$A \wedge B \equiv B \wedge A \qquad A \vee B \equiv B \vee A$$

3. Banatze-legeak (BANA)

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

4. Tautologiak (TAUT)

$$A \wedge A \equiv A \qquad A \vee A \equiv A$$

5. Ukapen bikoitza (UB)

$$\neg\neg A \equiv A$$

6. De Morganen legeak (DeM)

$$\neg(A \wedge B) \equiv \neg A \vee \neg B \qquad \neg(A \vee B) \equiv \neg A \wedge \neg B$$

7. Transposizioa (TRANS)

$$A \to B \equiv \neg B \to \neg A$$

8. Inplikazio materiala (INP)

$$A \to B \equiv \neg A \vee B$$

9. Baliokidetza materialak (BALIO)

$$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$$

$$A \leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$$

10. Esportazioa (ESP)

$$A \to (B \to C) \equiv (A \wedge B) \to C$$

Baliokidetza horiek frogatzeko, egia-taulak kalkulatuko genituzke, eta berdinak direla egiaztatuko genuke.

1.17 Adibideak.

1. 9b) baliokidetza frogatzeko, bi formulen egia-taulak kalkulatuko ditugu:

A	B	$A \leftrightarrow B$	$A \wedge B$	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$(A \wedge B) \vee (\neg A \wedge \neg B)$
E	E	E	E	F	F	F	E
E	F	F	F	F	E	F	F
F	E	F	F	E	F	F	F
F	F	E	F	E	E	E	E
		$\uparrow$					$\uparrow$

2. Baliokidetza logikoetako A, B eta C formulak edozein formula direnez gero, $A = p \wedge q$ eta $B = r \vee s$ badira, $p \wedge q \to r \vee s \equiv \neg(p \wedge q) \vee (r \vee s)$ baliokidetza ere beteko da (inplikazio materiala).

Oharra. $\wedge$ eta $\vee$ lokailuen elkartze-legeak direla eta, $A \wedge B \wedge C$ eta $A \vee B \vee C$ parentesirik gabe idatz ditzakegu.

Hala ere, ezin izango dugu $A \wedge B \vee C$ idatzi, $(A \wedge B) \vee C \not\equiv A \wedge (B \vee C)$ delako.

A	B	C	$A \wedge B$	$(A \wedge B) \vee C$	$B \vee C$	$A \wedge (B \vee C)$
E	E	E	E	E	E	E
E	E	F	E	E	E	E
E	F	E	F	E	E	E
E	F	F	F	F	F	F
F	E	E	F	$\underline{E}$	E	$\underline{F}$
F	E	F	F	F	E	F
F	F	E	F	E	E	F
F	F	F	F	F	F	F

1.18 Teorema. *Izan bitez A eta B ongi eratutako bi formula,*

$$A \equiv B \text{ baldin eta soilik baldin } \models (A \leftrightarrow B).$$

Froga.

Soilik baldin. Demagun $A \equiv B$ dela. Horrek esan nahi du edozein I interpretaziotarako $V(A, I) = V(B, I)$ dela. $\models (A \leftrightarrow B)$ frogatu behar dugu, hau da, edozein I interpretaziotarako $V((A \leftrightarrow B), I) = E$ dela.

Izan bedi I edozein interpretazio. Bi aukera daude:

1. $V(A, I) = E$. Orduan, $A \equiv B$ denez, $V(B, I) = E$ izango dugu eta, hortaz, $V((A \leftrightarrow B), I) = E$.

2. $V(A, I) = F$. Orduan, $V(B, I) = F$ eta, berriro ere, $V((A \leftrightarrow B), I) = E$.

Bi kasuetan frogatuta geratu da $V((A \leftrightarrow B), I) = E$ dela.

Baldin. Demagun $\models (A \leftrightarrow B)$ dela.

Izan bedi I edozein interpretazio. Bi aukera daude:

1. $V(A, I) = E$. Orduan, $\models (A \leftrightarrow B)$ denez, $V((A \leftrightarrow B), I) = E$ izango dugu eta, hortaz, $V(B, I) = E$.

2. $V(A, I) = F$. Orduan, $V((A \leftrightarrow B), I) = E$ denez, $V(B, I) = F$ izango dugu.

Beraz, edozein I interpretaziotarako $V(A, I) = V(B, I)$ da eta, ondorioz, $A \equiv B$. □

1.6 Ondorio logikoak. Baliozko argumentuak

1.19 Definizioa. *$A_1, \ldots, A_n$ eta B formulak izanik, B formula $A_1, \ldots, A_n$ formulen* ondorio logikoa *dela edo formuletatik* logikoki deduzitzen *dela esango dugu $V(A_1, I) = E$, $\cdots$, $V(A_n, I) = E$ egiten duen edozein I interpretaziotarako $V(B, I) = E$ ere bada.*

B formula $A_1, \ldots, A_n$ formulen ondorio logikoa bada, honela adieraziko dugu:

$$A_1, \ldots, A_n \Rightarrow B \quad \text{edo} \quad A_1, \ldots, A_n \models B.$$

1.20 Adibideak.

1. q formula $p \to q$ eta p formulen ondorio logikoa da.

p	q	$p \to q$
E	E	E
E	F	F
F	E	E
F	F	E

   Bai p formula bai $p \to q$ formula E diren errenkadetan (lehenengo errenkada bakarrik) q formula ere E da.

2. Baina, p ez da $p \to q$ eta q formulen ondorio logikoa. Izan ere, lehenengo eta hirugarren errenkadetan $p \to q$ eta q formulak E dira, baina hirugarren errenkadan p formula F da.

1.21 Teorema. *$A_1, \ldots, A_n$ eta B $n+1$ formula izanik,*

B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin
$$\models (A_1 \wedge \ldots \wedge A_n \to B) \text{ bada.}$$

Froga.

Soilik baldin. Demagun B formula $A_1, \ldots, A_n$ formulen ondorio logikoa dela. Frogatu beharko dugu $\models (A_1 \wedge \ldots \wedge A_n \to B)$ dela, hau da, $V(A_1 \wedge \ldots \wedge A_n \to B, I) = E$ dela edozein I interpretaziotarako.

Izan bedi I edozein interpretazio. Bi aukera daude:

1. $V(A_1, I) = \cdots = V(A_n, I) = E$. Orduan, ondorio logikoaren definizioaren arabera, $V(B, I) = E$ izango dugu eta, hortaz, $V(A_1 \wedge \ldots \wedge A_n \to B, I) = E$ ere bai.

2. i-ren baterako, $V(A_i, I) = F$. Orduan, $V(A_1 \wedge \ldots \wedge A_n, I) = F$ izango da eta, hortaz, $V(A_1 \wedge \ldots \wedge A_n \to B, I) = E$ ere bai.

Baldin. Demagun, orain, $\models (A_1 \wedge \ldots \wedge A_n \to B)$ dela. B formula $A_1, \ldots, A_n$ formulen ondorio logikoa dela frogatu behar dugu, hau da, $V(A_1, I) = \cdots = V(A_n, I) = E$ bada, $V(B, I) = V$ ere izango dela, edozein I interpretaziotarako.

Izan bedi I edozein interpretazio, non $V(A_1, I) = \cdots = V(A_n, I) = E$ den. Orduan, $V(A_1 \wedge \ldots \wedge A_n, I) = E$ izango da. Horrez gain, $\models (A_1 \wedge \ldots \wedge A_n \to B)$ izateagatik, $V(A_1 \wedge \ldots \wedge A_n \to B, I) = E$ ere bada. Hortik $V(B, I) = E$ aterako dugu. □

1.22 Adibideak.

1. q formula $p \to q$ eta p formulen ondorio logikoa da. Hortaz, $\models ((p \to q) \wedge p \to q)$.

p	q	$p \to q$	$(p \to q) \wedge p$	$(p \to q) \wedge p \to q$
E	E	E	E	E
E	F	F	F	E
F	E	E	F	E
F	F	E	F	E

2. p formula ez da $p \to q$ eta q formulen ondorio logikoa. Hortaz, $(p \to q) \wedge q \to p$ formula baliogabea da.

p	q	$p \to q$	$(p \to q) \wedge q$	$(p \to q) \wedge q \to p$
E	E	E	E	E
E	F	F	F	E
F	E	E	E	$\underline{F}$
F	F	E	F	E

1.23 Teorema. *$A_1, \ldots, A_n$ eta B $n+1$ formula izanik,*

B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin $A_1 \wedge \ldots \wedge A_n \wedge \neg B$ formula inkontsistentea bada.

Teorema frogatu baino lehen, froga dezagun lema hau:

1.24 Lema. $\neg(A_1 \wedge \ldots \wedge A_n \to B) \equiv A_1 \wedge \ldots \wedge A_n \wedge \neg B$.

1.24 Lemaren froga.
$\neg(A_1 \wedge \ldots \wedge A_n \to B) \equiv \neg(\neg(A_1 \wedge \ldots \wedge A_n) \vee B)$ (inplikazio materiala) $\equiv$
$\equiv \neg\neg(A_1 \wedge \ldots \wedge A_n) \wedge \neg B$ (De Morganen legeak) $\equiv (A_1 \wedge \ldots \wedge A_n) \wedge \neg B$ (ukapen bikoitza) $\equiv A_1 \wedge \ldots \wedge A_n \wedge \neg B$ (elkartze-legea).
Hortaz, $\neg(A_1 \wedge \ldots \wedge A_n \to B) \equiv A_1 \wedge \ldots \wedge A_n \wedge \neg B$. □

1.23 Teoremaren froga.
1.21 Teorema frogatzeko teknika bera erabil genezake, baina beste frogabide-mota bat erabiliko dugu.
1.21 Teoremaren arabera, B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin $\models (A_1 \wedge \ldots \wedge A_n \to B)$ bada. Beste aldetik, badakigu $\models (A_1 \wedge \ldots \wedge A_n \to B)$ dela baldin eta soilik baldin $\neg(A_1 \wedge \ldots \wedge A_n \to B)$ formula inkontsistentea bada. Lema erabiliz, azkeneko formula inkontsistentea da baldin eta soilik baldin $A_1 \wedge \ldots \wedge A_n \wedge \neg B$ formula inkontsistentea bada, baliokideak direlako. Nahi genuena lortu dugu, B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin $A_1 \wedge \ldots \wedge A_n \wedge \neg B$ formula inkontsistentea bada. □

1.25 Adibideak.

1. q formula $p \to q$ eta p formulen ondorio logikoa da. Hortaz, $(p \to q) \wedge p \wedge \neg q$ formula inkontsistentea da.

   p formula ez da $p \to q$ eta q formulen ondorio logikoa. Hortaz, $(p \to q) \wedge q \wedge \neg p$ formula kontsistentea da.

p	q	$p \to q$	$\neg q$	$(p \to q) \wedge p \wedge \neg q$	$\neg p$	$(p \to q) \wedge q \wedge \neg p$
E	E	E	F	F	F	F
E	F	F	E	F	F	F
F	E	E	F	F	E	$\underline{E}$
F	F	E	E	F	E	F

2. $p \vee q$ formula p formularen ondorio logikoa da. Honela egiazta genezake: 1) definizioa erabiliz; 2) $\models (p \to p \vee q)$ egiaztatuz; 3) $p \wedge \neg(p \vee q)$ formula inkontsistentea dela egiaztatuz.

p	q	$p \vee q$	$p \to p \vee q$	$\neg(p \vee q)$	$p \wedge \neg(p \vee q)$
E	E	E	E	F	F
E	F	E	E	F	F
F	E	E	E	F	F
F	F	F	E	E	F
	1		2		3

1.26 Definizioa. Argumentu *bat edo* argumentu-eskema *bat* $P_1, \ldots, P_n, C$ *ongi eratutako formulen multzo bat da, non* $P_1, \ldots, P_n$ premisa *deitzen diren eta* C ondorio *deitzen den. Honela adieraziko dugu:*

$$\begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline C \end{array} \qquad \textit{edo} \qquad \begin{array}{l} P_1 \\ \vdots \\ P_n \ / \therefore C \end{array}$$

1.27 Definizioa. *Argumentu bat* baliozkoa *da edo* ongi eraikita *dago ondorioa premisen ondorio logikoa bada edo premisetatik logikoki deduzitzen bada, hau da, ezinezkoa bada premisak* E *izatea eta ondorioa* F *izatea.*

Argumentu bat baliogabea *da edo* gaizki eraikita *dago ez bada baliozko argumentua.*

1.28 Adibideak.

1. Baliozko argumentua (ikus 1.25 Adibidea).

$$\left.\begin{array}{l} \left.\begin{array}{l} p \to q \\ p \end{array}\right\} \text{premisak} \\ \hline q \qquad \text{ondorioa} \end{array}\right\}$$

2. Argumentu baliogabea (ikus 1.25 Adibidea).

$$\left.\begin{array}{l} p \to q \\ q \\ \hline p \end{array}\right\}$$

3. Baliozko argumentua.

$$\left.\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}\right\} \qquad \begin{array}{cccc} p & q & p \vee q & \neg p \\ \hline E & E & E & F \\ E & F & E & F \\ F & E & \underline{E} & \underline{E} \\ F & F & F & E \end{array}$$

4. Argumentu baliogabea.

$$\left.\begin{array}{l} p \vee q \\ p \\ \hline q \end{array}\right\} \qquad \begin{array}{ccc} p & q & p \vee q \\ \hline E & E & E \\ \underline{E} & F & \underline{E} \\ F & E & E \\ F & F & F \end{array}$$

Premisa egiazkoak izanik, ondorioa faltsua deneko kasua azpimarratu dugu, argumentua baliogabetzen duelako.

Baliozko argumentu-eskemak

Hona hemen ezagunak diren baliozko argumentu-eskema batzuk: A, B, C, D ongi eratutako edozein formula dira,

1. Modus Ponens (MP)

$$\begin{array}{l} A \to B \\ A \\ \hline B \end{array}$$

2. Modus Tollens (MT)

$$\begin{array}{l} A \to B \\ \neg B \\ \hline \neg A \end{array}$$

3. Silogismo Hipotetikoa (SH)

$$\begin{array}{l} A \to B \\ B \to C \\ \hline A \to C \end{array}$$

4. Silogismo Disjuntiboa (SD)

$$\begin{array}{l} A \vee B \\ \neg A \\ \hline B \end{array}$$

5. Dilema Eraikitzailea (DE)

$$\begin{array}{l} (A \to B) \wedge (C \to D) \\ A \vee C \\ \hline B \vee D \end{array}$$

6. Dilema Suntsitzailea (DS)

$$\begin{array}{l} (A \to B) \wedge (C \to D) \\ \neg B \vee \neg D \\ \hline \neg A \vee \neg C \end{array}$$

7. Konjuntzioaren Sinplifikazioa (KS)

$$\begin{array}{l} A \wedge B \\ \hline A \end{array}$$

8. Konjuntzioaren Konbinazioa (KK)

$$\begin{array}{l} A \\ B \\ \hline A \wedge B \end{array}$$

9. Disjuntzioaren Batuketa (DB)

$$\frac{A}{A \vee B}$$

Aurreko argumentuak baliozkoak direla egiazta dezakegu egia-taulen bidez. Esate baterako, silogismo disjuntiboa frogatzeko taula hau osatuko dugu:

A	B	$A \vee B$	$\neg A$
E	E	E	F
E	F	E	F
F	E	$\underline{E}$	$\underline{E}$
F	F	F	E

eta silogismo hipotetikoa frogatzeko beste hau:

A	B	C	$A \to B$	$B \to C$	$A \to C$
E	E	E	$\underline{E}$	$\underline{E}$	E
E	E	F	E	F	F
E	F	E	F	E	E
E	F	F	F	E	F
F	E	E	$\underline{E}$	$\underline{E}$	E
F	E	F	E	F	E
F	F	E	$\underline{E}$	$\underline{E}$	E
F	F	F	$\underline{E}$	$\underline{E}$	E

Oharra. A, B, C, D edozein oef direnez, argumentu hau ere baliozkoa da:

$$\frac{\begin{array}{l} p \wedge q \to (r \to s) \\ (r \to s) \to t \vee q \end{array}}{p \wedge q \to t \vee q}$$

Silogismo hipotetikoaren eskemari dagokio: $A = p \wedge q$, $B = r \to s$ eta $C = t \vee q$.

1.7 Dedukzio formala

1.7.1 Froga formala. Inferentzia-erregelak

Argumentuek bi edo hiru atomo baino gehiago dituztenean, baliozkotasuna frogatzeko egia-taulak erabiltzea luze eta astun egiten da.

Argumentuak baliozkoak direla frogatzeko, bide motzago bat argumentu elementalak erabiltzea da, baliozkoak direla badakigulako; *inferentzia-erregelak* deitzen dira.

Adibidez, hau inferentzia-erregela bat da:

$$\frac{\begin{array}{l} A \to B \\ A \end{array}}{B}$$

non A eta B edozein oef diren. Demagun argumentu hau baliozkoa dela frogatu nahi dugula:

$$\begin{array}{ll} 1. & p \wedge \neg s \to q \\ 2. & q \to r \\ 3. & p \wedge \neg s \ / \therefore r \end{array}$$

Erregela aplikatuz ($A = p \wedge \neg s$ eta $B = q$ direnean), 1 eta 3 premisetatik hau aterako dugu:

$$4. \quad q$$

Erregela berriro aplikatuz ($A = q$ eta $B = r$ direnean), 2 eta 4 formuletatik hau aterako dugu:

$$5. \quad r$$

ondorioa dena. Beraz, argumentua baliozkoa da.

Inferentzia-erregelak

Hasiera batean 9 inferentzia-erregela erabiliko ditugu, baliozko argumentu hauek, hain zuzen:

1. Modus Ponens (MP)
2. Modus Tollens (MT)
3. Silogismo Hipotetikoa (SH)
4. Silogismo Disjuntiboa (SD)
5. Dilema Eraikitzailea (DE)
6. Dilema Suntsitzailea (DS)
7. Konjuntzioaren Sinplifikazioa (KS)
8. Konjuntzioaren Konbinazioa (KK)
9. Disjuntzioaren Batuketa (DB)

1.29 Definizioa.
$P_1, \ldots, P_n$ premisak eta C ondorioa dituen

$$\begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline C \end{array}$$

argumentu baten baliozkotasunaren froga formal *bat $S_1, \ldots, S_m$ formulen segida finitu bat da, non:*

1. *$S_m = C$ den eta*

2. *$i = 1, \ldots, m$ balioetarako, S_i premisa bat den edo inferentzia-erregela baten bidez segidaren aurreko formuletatik deduzitzen den.*

Interpretazio baterako, premisa guztiak egiazkoak direla suposatzen badugu, horietatik inferentzia-erregelen bidez deduzituko ditugun formula guztiak egiazkoak izango dira, interpretazio horretarako. Hortaz, $S_m = C$ formula ere egiazkoa izango da, interpretazio horretarako.

1.30 Adibideak.

Hona hemen argumentu batzuen froga formalen adibideak:

1.

$$\frac{\begin{array}{l} A \to B \\ C \to D \\ (\neg B \vee \neg D) \wedge (\neg A \vee \neg B) \end{array}}{\neg A \vee \neg C}$$

1.	$A \to B$	premisa
2.	$C \to D$	premisa
3.	$(\neg B \vee \neg D) \wedge (\neg A \vee \neg B)$	premisa $/\therefore \neg A \vee \neg C$
4.	$(A \to B) \wedge (C \to D)$	KK(1,2)
5.	$\neg B \vee \neg D$	KS(3)
6.	$\neg A \vee \neg C$	DS(4,5)

2.

$$\frac{\begin{array}{l} A \vee (B \to D) \\ \neg C \to (D \to E) \\ A \to C \\ \neg C \end{array}}{B \to E}$$

1.	$A \vee (B \to D)$	premisa
2.	$\neg C \to (D \to E)$	premisa
3.	$A \to C$	premisa
4.	$\neg C$	premisa $/ \therefore B \to E$
5.	$\neg A$	MT(3,4)
6.	$B \to D$	SD(1,5)
7.	$D \to E$	MP(2,4)
8.	$B \to E$	SH(6,7)

3.

1.	$A \wedge B \to (A \to D \wedge E)$	premisa
2.	$(A \wedge B) \wedge C$	premisa $/ \therefore D \vee E$
3.	$A \wedge B$	KS(2)
4.	$A \to D \wedge E$	MP(1,3)
5.	A	KS(3)
6.	$D \wedge E$	MP(4,5)
7.	D	KS(6)
8.	$D \vee E$	DB(7)

4.

1.	$J \to K$	premisa
2.	$J \vee (K \vee \neg L)$	premisa
3.	$\neg K$	premisa $/ \therefore \neg L \wedge \neg K$
4.	$\neg J$	MT(1,3)
5.	$K \vee \neg L$	SD(2,4)
6.	$\neg L$	SD(5,3)
7.	$\neg L \wedge \neg K$	KK(6,3)

1.7.2 Ordezkapen-erregela

Baliozko argumentu askoren kasuan beren baliozkotasuna ezin da bederatzi inferentzia-erregela horien bidez frogatu. Adibidez,

$$\frac{A \wedge B}{B}$$

baliozko argumentuaren froga formalak inferentzia-erregela gehiago behar ditu.

Izan bitez A oef bat, A formularen B azpiformula bat eta B' beste oef bat, non $B \equiv B'$ den. A' idatziko dugu A formulan B azpiformularen ordez B' formula jartzean lortzen den formula adierazteko.

1.31 Adibideak.

1. Izan bedi $A = p \to q \vee \neg r$ formula. $B = q \vee \neg r$ A formularen azpiformula bat da. Bestalde, $B = q \vee \neg r \equiv \neg r \vee q = B'$ (trukatze-legea). Beraz, $A' = p \to \neg r \vee q$ izango da.

2. Izan bitez $A = p \wedge s \leftrightarrow (\neg q \to t)$ formula eta $B = \neg q \to t$ azpiformula. Baliokidetza logiko hau dugu: $B = \neg q \to t \equiv \neg\neg q \vee t = B'$ (inplikazio materiala). Orduan, $A' = p \wedge s \leftrightarrow (\neg\neg q \vee t)$ izango da.

Ohar gaitezen $A \equiv A'$ dela; izan ere, A eta A' formulen egia-taulak kalkulatzerakoan, diferentzia bakarra B eta B' azpiformulak dira; baina horiek egia-taula berdinak dituzte.

Ordezkapen-erregelak A formulatik A' formula deduzitzeko aukera ematen digu, eta honela adieraziko dugu:

$$\frac{A}{A'}$$

Ordezkapen-erregelari esker, aurreko bederatzi inferentzia-erregelei beste hamar erregela erants diezazkiekegu, baliokidetza logikoetan oinarrituz.

1.32 Adibideak.

Honela adieraziko dugu froga formal batean:

1.

$$\begin{array}{rll} & \vdots & \\ k. & p \to q \vee \neg r & \\ k+1. & p \to \neg r \vee q & \text{TRUK(k)} \\ & \vdots & \end{array}$$

2.

$$\begin{array}{rll} & \vdots & \\ k. & p \wedge s \leftrightarrow (\neg q \to t) & \\ k+1. & p \wedge s \leftrightarrow (\neg\neg q \vee t) & \text{INP(k)} \\ & \vdots & \end{array}$$

3. Baliozkotasunaren froga formala argumentu honetarako: $A \wedge B \ / \therefore B$.

1.	$A \wedge B$	premisa / $\therefore B$
2.	$B \wedge A$	TRUK(1)
3.	B	KS(2)

Diferentzia handi bat dago ordezkapen-erregelaren eta aurreko bederatzi inferentzia-erregelen artean. 1.7.1 atalean definitutako erregelak frogabide baten formula osoei aplikatu dizkiegu; ordezkapen-erregelaren barruan dauden hamar erregelak, ordea, formula osoei zein azpiformulei aplikatuko dizkiegu. Adibidez, konjuntzioaren sinplifikazioa formula osoei bakarrik aplika diezaiekegu: esaterako,

$\vdots$		
$k.$	$A \wedge B$	
$k+1.$	A	KS(k)
$\vdots$		

argumentuan ongi aplikaturik dago, baina

$\vdots$			
$k.$	$A \wedge B \to C$		
$k+1.$	$A \to C$	KS(k)	gaizki
$\vdots$			

argumentuan **gaizki** aplikaturik dago. Eta trukatze-legea, esate baterako, formula osoei aplika diezaiekegu,

$\vdots$		
$k.$	$A \wedge B$	
$k+1.$	$B \wedge A$	TRUK(k)
$\vdots$		

bai eta azpiformulei ere,

$\vdots$		
$k.$	$A \wedge B \to C$	
$k+1.$	$B \wedge A \to C$	TRUK(k)
$\vdots$		

Inferentzia-erregelen zerrendari beste erregela batzuk erants geniezazkioke, esate baterako, $A \wedge B \ / \therefore B$. Baina zerrenda luzeegia eta erabiltezina izango genuke.

Beste alde batetik, inferentzia-erregelen zerrendak erredundantziak ditu; esaterako Modus Tollens erregela ken genezake, beste erregelen bidez emaitza bera lor dezakegulako. Adibidez:

1.	$A \vee B$	premisa			
2.	$A \to C$	premisa			
3.	$\neg C$	premisa / $\therefore B$			
4.	$\neg A$	MT(2,3)	4.	$\neg C \to \neg A$	TRANS(2)
5.	B	SD(1,4)	5.	$\neg A$	MP(4,3)
			6.	B	SD(1,5)

Hala eta guztiz ere, Modus Tollens erregela sartu dugu, inferentzia-erregela ezaguna eta intuiziozkoa delako. Berdin gertatzen da beste erregela batzuekin.

1.33 Adibideak.

Hona hemen argumentu batzuen froga formalak inferentzia-erregelak eta ordezkapen-erregela erabiliz.

1.

1.	$A \vee B \to C \wedge D$	premisa
2.	$\neg C$	premisa / $\therefore \neg B$
3.	$\neg C \vee \neg D$	DB(2)
4.	$\neg(C \wedge D)$	DeM(3)
5.	$\neg(A \vee B)$	MT(1,4)
6.	$\neg A \wedge \neg B$	DeM(5)
7.	$\neg B \wedge \neg A$	TRUK(6)
8.	$\neg B$	KS(7)

2.

1.	$(E \wedge F) \wedge G$	premisa
2.	$(F \leftrightarrow G) \to H \vee I$	premisa / $\therefore I \vee H$
3.	$E \wedge (F \wedge G)$	ELKAR(1)
4.	$(F \wedge G) \wedge E$	TRUK(3)
5.	$F \wedge G$	KS(4)
6.	$(F \wedge G) \vee (\neg F \wedge \neg G)$	DB(5)
7.	$F \leftrightarrow G$	BALIO(6)
8.	$H \vee I$	MP(2,7)
9.	$I \vee H$	TRUK(8)

3.

1.	$S \to T$	premisa
2.	$S \vee T$	premisa / $\therefore T$
3.	$T \vee S$	TRUK(2)
4.	$\neg\neg T \vee S$	UB(3)
5.	$\neg T \to S$	INP(4)
6.	$\neg T \to T$	SH(5,1)
7.	$\neg\neg T \vee T$	INP(6)
8.	$T \vee T$	UB(7)
9.	T	TAUT(8)

1.7.3 Baldintzazko frogaren erregela

$P \to C$ motako baldintzazko formula bat deduzitu nahi dugunean erabil dezakegun inferentzia-erregela da. Adibidez, $A \to B$ / $\therefore A \to A \wedge B$.

1.34 Teorema. *Baldintzazko frogaren erregela*

$P_1, \ldots, P_n$ premisak eta $P \to C$ ondorioa dituen

$$(1) \quad \begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline P \to C \end{array}$$

argumentua baliozkoa da baldin eta soilik baldin

$$(2) \quad \begin{array}{c} P_1 \\ \vdots \\ P_n \\ P \\ \hline C \end{array}$$

argumentua baliozkoa bada.

Froga.

(1) argumentua baliozkoa da baldin eta soilik baldin $P \to C$ formula $P_1, \ldots, P_n$ formulen ondorio logiko bat bada, baliozko argumentuaren definizioaren arabera.

1.21 Teorema aplikatuz, $P \to C$ formula $P_1, \ldots, P_n$ formulen ondorio logiko bat da baldin eta soilik baldin $\models (P_1 \wedge \cdots \wedge P_n \to (P \to C))$ bada.

Eta hori horrela da baldin eta soilik baldin $\models (P_1 \wedge \cdots \wedge P_n \wedge P \to C)$ bada, $P_1 \wedge \cdots \wedge P_n \to (P \to C) \equiv P_1 \wedge \cdots \wedge P_n \wedge P \to C$ esportazioa delako.

Eta azken hori beteko da baldin eta soilik baldin C formula $P_1, \ldots, P_n, P$ formulen ondorio logiko bat bada, 1.21 Teorema erabiliz. Hau da, baldin eta soilik baldin (2) argumentua baliozkoa bada, baliozko argumentuaren definizioaren arabera. □

Erregela erabiltzeko bidea

$P_1, \ldots, P_n$ premisak dituen (1) argumentu bat izanik, $P \to C$ formula deduzitu nahi badugu, premisei P hipotesia erantsiko diegu, eta C deduzituko dugu. P hipotesia eranstean beste argumentu bat, (2), izango dugu, premisak $P_1, \ldots, P_n, P$ dituena. Behin C deduzitu eta gero, P hipotesia baztertuko dugu eta, baldintzazko frogaren erregela aplikatuz, $P \to C$ deduzituko dugu; hau da, $P \to C$ formula $P_1, \ldots, P_n$ formuletatik deduzituko dugu. Hori dena honela adieraziko dugu:

$$\begin{array}{cccl}
 & 1. & P_1 & \text{Premisa.} \\
 & \vdots & \vdots & \\
 & n. & P_n & \text{Premisa.} \\
 & \vdots & \vdots & \\
\to & m. & P & \text{BFEren hipotesia} \ / \ \therefore C \\
| & \vdots & \vdots & \\
| & k. & C & \\
\hline
 & k+1. & P \to C & \text{BFE(m-k)}
\end{array}$$

Idazkera horrekin adierazi nahi dugu $m+1$-etik k-ra bitartean formulak $P_1, \ldots, P_n, P$ premisak erabiliz deduzitu ditugula ((2) argumentua). $k+1$ formula, aldiz, $P_1, \ldots, P_n$ premisetatik deduzitu dugu ((1) argumentua), P hipotesia baztertu dugu. □

1.35 Adibideak.

Hona hemen argumentu batzuen froga formalak inferentzia-erregelak, ordezkapen-erregela eta baldintzazko frogaren erregela erabiliz.

1.

	1.	$A \to B$	premisa / $\therefore A \to A \wedge B$
$\to$	2.	A	BFEren hipotesia / $\therefore A \wedge B$
	3.	B	MP(1,2)
	4.	$A \wedge B$	KK(2,3)
	5.	$A \to A \wedge B$	BFE(2-4)

2.

	1.	$T \to E$	premisa
	2.	$A \to L$	premisa / $\therefore T \vee A \to L \vee E$
$\to$	3.	$T \vee A$	BFEren hipotesia / $\therefore L \vee E$
	4.	$(T \to E) \wedge (A \to L)$	KK(1,2)
	5.	$E \vee L$	DE(4,3)
	6.	$L \vee E$	TRUK(5)
	7.	$T \vee A \to L \vee E$	BFE(3-6)

3.

		1.	$Q \to R$	premisa / $\therefore (P \to Q) \to (P \to R)$
$\to$		2.	$P \to Q$	BFEren hipotesia / $\therefore P \to R$
	$\to$	3.	P	BFEren hipotesia / $\therefore R$
		4.	Q	MP(2,3)
		5.	R	MP(1,4)
		6.	$P \to R$	BFE(3-5)
		7.	$(P \to Q) \to (P \to R)$	BFE(2-6)

4.

		1.	$(A \to C) \to D$	premisa
		2.	$B \to E$	premisa
		3.	$A \wedge B \to C$	premisa / $\therefore B \to E \wedge D$
$\to$		4.	B	BFEren hipotesia / $\therefore E \wedge D$
		5.	E	MP(2,4)
	$\to$	6.	A	BFEren hipotesia / $\therefore C$
		7.	$A \wedge B$	KK(6,4)
		8.	C	MP(3,7)
		9.	$A \to C$	BFE(6-8)
		10.	D	MP(1,9)
		11.	$E \wedge D$	KK(5,10)
		12.	$B \to E \wedge D$	BFE(4-11)

1.7.4 Absurdora eramateko erregela

Absurdora eramateko metodoa frogatu nahi dugunaren aurkako hipotesia egin eta *kontraesan* bat (formula inkontsistente bat) deduzitzean datza.

Idazkera. Formula inkontsistente bat $\square$ adieraziko dugu (adibidez, $A \wedge \neg A$).

1.36 Teorema. *Absurdora eramateko erregela*
$P_1, \ldots, P_n$ premisak eta C ondorioa dituen

$$(1) \quad \begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline C \end{array}$$

argumentua baliozkoa da baldin eta soilik baldin

$$(2) \quad \begin{array}{c} P_1 \\ \vdots \\ P_n \\ \neg C \\ \hline \square \end{array}$$

argumentua baliozkoa bada.

Erregela frogatzeko lema hau erabiliko dugu:

1.37 Lema. *Izan bedi $\square$ oef inkontsistente bat eta izan bedi A edozein oef. Orduan,*

A inkontsistentea da baldin eta soilik baldin $\models (A \to \square)$ bada.

1.37 Lemaren froga.
Soilik baldin. Demagun A formula inkontsistentea dela; $\models (A \to \square)$ frogatu behar dugu, hau da, edozein I interpretaziotarako, $V((A \to \square), I) = E$ betetzen dela.

Izan bedi I edozein interpretazio. A formula inkontsistentea denez, $V(A, I) = F$ da eta, hortaz, $V((A \to \square), I) = E$ izango da.

Baldin. Demagun $\models (A \to \square)$ dela. A formula inkontsistentea dela frogatu behar dugu, hau da, edozein I interpretaziotarako, $V(A, I) = F$ dela.

Izan bedi I edozein interpretazio. $\models (A \to \square)$ denez, $V((A \to \square), I) = E$ izango da eta, $\square$ inkontsistentea denez, $V(\square, I) = F$ da. Hortaz, $V(A, I) = F$. $\square$

1.36 Teoremaren froga.
(1) argumentua baliozkoa da baldin eta soilik baldin C formula $P_1, \ldots, P_n$ formulen ondorio logikoa bada, baliozko argumentuaren definizioaren arabera. Hori horrela da baldin eta soilik baldin $P_1 \wedge \cdots \wedge P_n \wedge \neg C$ formula inkontsistentea bada (1.23 Teorema) eta, lemaren arabera, baldin eta soilik baldin $\models (P_1 \wedge \cdots \wedge P_n \wedge \neg C \to \square)$ bada. Hori dena beteko da baldin eta soilik baldin $\square$ formula $P_1, \ldots, P_n, \neg C$ formulen ondorio logikoa bada (1.21 Teorema). Hau da, baldin eta soilik baldin (2) argumentua baliozkoa bada, baliozko argumentuaren definizioaren arabera. $\square$

Erregela erabiltzeko bidea
$P_1, \ldots, P_n$ premisak dituen (1) argumentu bat izanik, C formula deduzitu nahi badugu, $\neg C$ hipotesia erantsiko dugu eta kontraesan bat deduzituko dugu ($A \wedge \neg A$ motako edozein formula). $\neg C$ hipotesia eranstean, $P_1, \ldots, P_n, \neg C$ premisak dituen beste argumentu bat, (2), lortuko dugu. Behin kontraesana deduzitu eta gero, $\neg C$ hipotesia baztertuko

dugu eta, absurdora eramateko erregela erabiliz, C formula deduzituko dugu (C formula $P_1, \ldots, P_n$ formuletatik deduzituko dugu).

$$
\begin{array}{rrcl}
 & 1. & P_1 & \text{Premisa} \\
 & \vdots & \vdots & \\
 & n. & P_n & \text{Premisa} \\
 & \vdots & \vdots & \\
\rightarrow & m. & \neg C & \text{AEEren hipotesia} \ / \ \therefore \ \Box \\
| & \vdots & \vdots & \\
| & k. & \Box & \\
\hline
 & k+1. & C & \text{AEE(m-k)}
\end{array}
$$

m+1etik $k$ra formulak $P_1, \ldots, P_n, \neg C$ premisak erabiliz deduzitu ditugu ((2) argumentua); $k+1$ formula, aldiz, $P_1, \ldots, P_n$ formuletatik deduzitu dugu ((1) argumentua).

1.38 Adibideak.

1. Ikus ditzagun argumentu beraren bi froga formal, bata AEE erabiliz eta bestea erabili gabe.

$$
\begin{array}{rrll}
 & 1. & p & \text{premisa} \ / \ \therefore \ q \vee (q \rightarrow r) \\
\rightarrow & 2. & \neg(q \vee (q \rightarrow r)) & \text{AEEren hipotesia} \ / \ \therefore \ \Box \\
| & 3. & \neg q \wedge \neg(q \rightarrow r) & \text{DeM(2)} \\
| & 4. & \neg q \wedge \neg(\neg q \vee r) & \text{INP(3)} \\
| & 5. & \neg q \wedge (\neg\neg q \wedge \neg r) & \text{DeM(4)} \\
| & 6. & (\neg q \wedge \neg\neg q) \wedge \neg r & \text{ELKAR(5)} \\
| & 7. & \neg q \wedge \neg\neg q & \text{KS(6)} \\
\hline
 & 8. & q \vee (q \rightarrow r) & \text{AEE(2-7)}
\end{array}
$$

Absurdora eramateko erregela erabili gabe:

$$
\begin{array}{rrll}
 & 1. & p & \text{premisa} \ / \ \therefore \ q \vee (q \rightarrow r) \\
\rightarrow & 2. & \neg(q \vee (q \rightarrow r)) & \text{BFEren hipotesia} \ / \ \therefore \ q \vee (q \rightarrow r) \\
| & 3. & \neg q \wedge \neg(q \rightarrow r) & \text{DeM(2)} \\
| & 4. & \neg q \wedge \neg(\neg q \vee r) & \text{INP(3)} \\
| & 5. & \neg q \wedge (\neg\neg q \wedge \neg r) & \text{DeM(4)} \\
| & 6. & (\neg\neg q \wedge \neg r) \wedge \neg q & \text{TRUK(5)} \\
| & 7. & \neg\neg q \wedge \neg r & \text{KS(6)} \\
| & 8. & \neg\neg q & \text{KS(7)} \\
| & 9. & q & \text{UB(8)} \\
| & 10. & q \vee (q \rightarrow r) & \text{DB(9)} \\
\hline
 & 11. & \neg(q \vee (q \rightarrow r)) \rightarrow q \vee (q \rightarrow r) & \text{BFE(2-10)} \\
 & 12. & \neg\neg(q \vee (q \rightarrow r)) \vee (q \vee (q \rightarrow r)) & \text{INP(11)} \\
 & 13. & (q \vee (q \rightarrow r)) \vee (q \vee (q \rightarrow r)) & \text{UB(12)} \\
 & 14. & q \vee (q \rightarrow r) & \text{TAUT(13)}
\end{array}
$$

2.

	1.	p	premisa / $\therefore q \vee (r \to \neg q)$
$\to$	2.	$\neg(q \vee (r \to \neg q))$	AEEren hipotesia / $\therefore \square$
	3.	$\neg q \wedge \neg(r \to \neg q)$	DeM(2)
	4.	$\neg q \wedge \neg(\neg r \vee \neg q)$	INP(3)
	5.	$\neg q \wedge (\neg\neg r \wedge \neg\neg q)$	DeM(4)
	6.	$\neg q \wedge (\neg\neg q \wedge \neg\neg r)$	TRUK(5)
	7.	$(\neg q \wedge \neg\neg q) \wedge \neg\neg r$	ELKAR(6)
	8.	$\neg q \wedge \neg\neg q$	KS(7)
	9.	$q \vee (r \to \neg q)$	AEE(2-8)

3. Ikus ditzagun, berriro ere, argumentu beraren bi froga formal, bata AEE erabiliz eta bestea erabili gabe.

	1.	$\neg q \wedge s$	premisa
	2.	$s \to \neg r$	premisa
	3.	$\neg r \to \neg p \vee q$	premisa / $\therefore \neg p$
$\to$	4.	$\neg\neg p$	AEEren hipotesia / $\therefore \square$
	5.	$\neg q$	KS(1)
	6.	$\neg\neg p \wedge \neg q$	KK(4,5)
	7.	$\neg(\neg p \vee q)$	DeM(6)
	8.	$\neg\neg r$	MT(3,7)
	9.	$\neg s$	MT(2,8)
	10.	$s \wedge \neg q$	TRUK(1)
	11.	s	KS(10)
	12.	$s \wedge \neg s$	KK(11,9)
	13.	$\neg p$	AEE(4-12)

4.	$s \wedge \neg q$	TRUK(1)
5.	s	KS(4)
6.	$\neg r$	MP(2,5)
7.	$\neg p \vee q$	MP(3,6)
8.	$q \vee \neg p$	TRUK(7)
9.	$\neg q$	KS(1)
10.	$\neg p$	SD(8,9)

2. Kapitulua

Predikatu-logika

2.1 Sarrera

Proposizio-logikan, argumentuen baliozkotasuna enuntziatu konposatuak sortzeko asmoz enuntziatu bakunak konbinatzeko eraren menpe dago, ez enuntziatuen barne-egituraren menpe.

Adibidez, intuizioz zuzena dirudien argumentu hau hartuko dugu:

Txakur guztiak ugaztunak dira.
Bizi txakurra da.
Beraz, Bizi ugaztuna da.

Proposizio-logikan, "Txakur guztiak ugaztunak dira" premisa proposizio bakuna da, eta p atomo batez adierazten dugu. Berdin gertatzen da bigarren premisarekin eta ondorioarekin, "Bizi txakurra da" proposizio bakuna q atomoaz adieraziko dugu eta "Bizi ugaztuna da" proposizio bakuna r atomoaz.

Beraz, proposizio-logikan, argumentua honela adieraziko dugu:

$$\begin{array}{c} p \\ q \\ \hline r \end{array}$$

Eta argumentu hori ez da baliozkoa; izan ere, $I = \{p, q, \neg r\}$ interpretaziorako premisak egiazkoak dira eta ondorioa faltsua da.

Hori hala da, argumentuaren baliozkotasuna enuntziatuen barne-egitura logikoaren menpe dagoelako. Horrelako kasuetan, barne-egitura horiek analizatzeko tresnak garatu beharko ditugu. Predikatu-logika proposizio-logikaren hedapena da, analisi horrek behar duen tresna.

Argumentuaren bigarren premisak dio "Bizi" izeneko banakoak txakur izatearen ezaugarria duela. "Bizi" *subjektua* da eta "txakurra" *predikatua* da (subjektuak duen ezaugarri bat adierazten du).

Enuntziatuen egiturak aztertzen ditugunean, funtsean, bi adierazpen-mota hauek interesatzen zaizkigu: alde batetik, banakoei (izaki zehatzak: pertsonak, zenbakiak...) dagozkien adierazpenak eta, beste aldetik, banakoen ezaugarriak edo banakoen arteko erlazioak azaltzen dituzten adierazpenak (predikatuak).

Esate baterako, “Bizi txakurra da”, “Ilargia zuria da”, “2 5 baino txikiagoa da”, “Anek tea nahiago du kafea baino” enuntziatuetan “Bizi”, “ilargia”, “2”, “5”, “Ane”, “tea”, “kafea” banakoak dira eta “txakurra da”, “zuria da”, “baino txikiagoa da”, “nahiago du” predikatuak dira, banakoen ezaugarriak edo banakoen arteko erlazioak azaltzen dituzten adierazpenak.

Formalizazioa

Banakoak adierazteko $a, b, c, \ldots$ letra xeheak erabiliko ditugu. Sinbolo horiek banakoak adierazten dituztenez, *konstante* deituko diegu.

Predikatuak adierazteko letra larriak erabiliko ditugu.

Adibidez,

1. Bizi txakurra da. b: “Bizi” T: “txakurra izan” $T(b)$

2. Ilargia zuria da. i: “ilargia” Z: “zuria izan” $Z(i)$

3. 2 5 baino txikiagoa da. b: “2” z: “5” T: “txikiagoa izan” $T(b, z)$

4. Anek tea nahiago du kafea baino. a: “Ane” t: “tea” k: “kafea” N: “nahiago izan” $N(a, t, k)$

Aurreko adibideetan ikus dezakegu predikatu batzuetan banakoen izen bakarra agertzen dela (banako predikatuak) eta beste batzuetan banakoen bi izen edo gehiago agertzen direla (predikatu anizkoitzak: bitarrak, hirutarrak...).

Azter dezagun, orain, predikatu-sinbolo bera duten proposizioak nola formulatzen diren:

Bizi txakurra da: $T(b)$

Lagun txakurra da: $T(l)$

7 txakurra da: $T(z)$

Proposizio horiek guztiak batera adierazteko $T(x)$ idatziko dugu. x letrari *aldagai* esango diogu. Ez da konstantea, eta edozein konstantez ordezka dezakegu.

$T(b)$, $T(l)$, $T(z)$ proposizioak dira, hots, esan dezakegu egiazkoak edo faltsuak diren; baina $T(x)$ ez da egiazkoa, ezta faltsua ere, ez da proposizio.

$T(x)$ bezalako adierazpenei *proposizio-funtzio* deituko diegu. Banako aldagaiak onartzen dituzten adierazpenak dira, eta proposizio bihurtzen dira banako aldagaien ordez banako konstanteak jartzen ditugunean.

Proposizio-funtzio batetik proposizio bat lortzeko prozesuari, aldagai bat konstante batez ordezkatuz, *instantziazio* deituko diogu, eta ateratzen den proposizioari *ordezkapen-instantzia*.

Esaterako, $\neg T(b)$ (Bizi ez da txakurra) eta $\neg T(z)$ (7 ez da txakurra) $\neg T(x)$ proposizio-funtzioaren bi instantziazioren emaitzak dira. $\neg T(x)$ proposizio-funtzioaren bi ordezkapen-instantzia $\neg T(b)$ eta $\neg T(z)$ dira.

Badago beste prozedura bat proposizio-funtzio batetik proposizio bat lortzeko: aldagaiak kuantifikatzea.

Orain arte, banako enuntziatuen adibideak ikusi ditugu, eta horietan banako bati ezaugarri bat egokitu zaio edo bi banakoren edo gehiagoren arteko erlazio bat ezarri da. Baina enuntziatuak ez dira beti banakoak; adibidez, "Dena zuria da" eta "Zerbait zuria da" proposizio orokorrak dira, ez dute banako-izenik. Hala ere, proposizio-funtzio batetik lor ditzakegu, ez instantziazioen bidez, baizik eta *orokortzearen* edo *kuantifikatzearen* bidez.

Lehenengo adibidea, "Dena zuria da", beste era honetan ere adieraz dezakegu: "Edozein gauza izanik, gauza hori zuria da"; eta, x aldagaia erabiliz, "Edozein x izanik, x zuria da".

"Edozein x izanik" esaldia *zenbatzaile unibertsala* da, eta $\forall x$ idatziz adieraziko dugu. Sinbolo hori erabiliz, "Dena zuria da" esaldia honela idatziko dugu:

$$\forall x Z(x)$$

Antzeko eran, "Zerbait zuria da" esaldia honela idatz dezakegu:"Badago gutxienez gauza bat zuria dena"; eta, aldagai batekin, "Badago gutxienez x bat, non x zuria den".

"Badago gutxienez x bat" esaldia *zenbatzaile existentziala* da, eta $\exists x$ idatziz adieraziko dugu. Sinbolo hori erabiliz, "Zerbait zuria da" esaldia honela idatziko dugu:

$$\exists x Z(x)$$

Laburbilduz, "x zuria da" ($Z(x)$) bezalako proposizio-funtzio bat izanik (edo *enuntziatu irekia*), bi bide dauzkagu proposizio bat lortzeko (edo *enuntziatua ixteko*):

1. Instantziazioa, aldagaia konstante batez ordezkatzea: $Z(i)$, "Ilargia zuria da". Bide honen bidez banako enuntziatua lortuko dugu.

2. Orokortzea edo kuantifikazioa, zenbatzaile bat aurrean jartzea: $\forall x Z(x)$, "Dena zuria da"; $\exists x Z(x)$, "Zerbait zuria da".

   Bide honen bidez enuntziatu orokorra lortuko dugu.

Historiari begira, logika tradizionalak lau proposizio-mota nabarmendu zituen; ikus ditzagun adibide hauekin:

- A (*baiezko proposizio unibertsala*): "Txakur guztiak ugaztunak dira".
- E (*ezezko proposizio unibertsala*): "Txakur bat ere ez da ugaztun".
- I (*baiezko proposizio partikularra*): "Zenbait txakur ugaztunak dira".
- O (*ezezko proposizio partikularra*): "Zenbait txakur ez dira ugaztun".

$T(x)$="x txakurra da" eta $U(x)$="x ugaztuna da" proposizio-funtzioak erabiltzen baditugu, A, baiezko unibertsala, honela irakur genezake: "Edozein gauza izanik, gauza hori txakurra bada, gauza hori ugaztuna izango da" edo "Edozein x izanik, x txakurra bada, x ugaztuna izango da". Eta adierazpen sinbolikoan:

$$\forall x(T(x) \to U(x)).$$

Era berean gainerako hiru proposizioekin:
E: "Edozein x izanik, x txakurra bada, x ez da ugaztun". Adierazpen sinbolikoan:

$$\forall x(T(x) \to \neg U(x))$$

I: "Badago gutxienez x bat, non x txakurra den eta x ugaztuna den". Adierazpen sinbolikoan:

$$\exists x(T(x) \wedge U(x))$$

O: "Badago gutxienez x bat, non x txakurra den eta x ez den ugaztun". Adierazpen sinbolikoan:

$$\exists x(T(x) \wedge \neg U(x))$$

Adibideak

1. Arranoek altu egiten dute hegan: $\forall x(A(x) \to H(x))$.

   Arranoek bakarrik egiten dute hegan altu: $\forall x(H(x) \to A(x))$.

2. Beroki bat ere ez da iragazgaitza ez bada bereziki tratatua izan:

$$\forall x(B(x) \wedge I(x) \to T(x)).$$

3. Zenbaki arrazional bakoitza zenbaki erreala da, baina zenbait zenbaki erreal ez dira arrazional:

$$\forall x(Q(x) \to R(x)) \wedge \exists x(R(x) \wedge \neg Q(x)).$$

4. Edozein zenbaki arrunten hurrengoa zenbaki arrunta da:

$$\forall x \forall y(N(x) \wedge H(y,x) \to N(y)), \quad (H(y,x): \ y \ x\text{-ren hurrengoa da}).$$

5. Edozein zenbaki arrunten hurrengoa zeroren desberdina da:

$$\forall x \forall y(N(x) \wedge H(y,x) \to \neg B(y,a)), \quad (B(y,x): \ y \text{ eta } x \text{ berdinak dira; } a:0).$$

2.2 Sintaxia

2.1 Definizioa. *Predikatu-logikaren* $\mathcal{A}$ alfabetoa *sinbolo hauek osatzen dute:*

1. Aldagaiak*:* $\mathcal{V} = \{x, y, z, \ldots\}$*;*

2. Konstanteak*:* $\mathcal{C} = \{a, b, c, \ldots\}$*;*

3. Predikatuak*:* $\mathcal{P} = \{P, Q, R, \ldots\}$*; P predikatu bakoitzak zenbaki arrunt bat darama elkarturik, predikatuak onartzen duen aldagaien edo konstanteen kopurua adierazten duena, hain zuzen; zenbaki horri predikatuaren* aritate *deituko diogu eta* $ar(P)$ *idatziko dugu.*

4. Lokailu logikoak*:* $\{\neg, \wedge, \vee, \to, \leftrightarrow\}$.

5. Zenbatzaileak *:* $\{\forall, \exists\}$.

6. Sinbolo inpropioak*:* $\{(,),,\}$ *(parentesiak eta komak).*

$$\mathcal{A} = \mathcal{V} \cup \mathcal{C} \cup \mathcal{P} \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\} \cup \{(,),,\}.$$

2.2 Definizioa. *Aldagaiei eta konstanteei* lehen ordenako termino *deituko diegu.*

2.3 Definizioa. *P n aritateko predikatu-sinbolo bat bada eta $t_1, \ldots, t_n$ terminoak badira,* $P(t_1, \ldots, t_n)$ atomo *bat edo* formula atomiko *bat da.*

2.4 Adibidea. Har ditzagun $\mathcal{V} = \{x, y, z\}$ aldagaien multzoa, $\mathcal{C} = \{a, b\}$ konstanteen multzoa eta $\mathcal{P} = \{P, Q, R, S\}$ predikatuen multzoa, aritateak $ar(P) = 1$, $ar(Q) = 3$, $ar(R) = 2$, $ar(S) = 3$ izanik.

Hona hemen atomo batzuk: $P(x)$, $P(b)$, $Q(x, a, y)$, $Q(x, y, x)$, $R(x, y)$, $S(a, b, b)$.

Honako hauek, ordea, ez dira atomo: $P(x, y)$, $Q(a)$.

2.5 Definizioa. *Predikatu-logikan* ongi eratutako formulak *(oef) arau hauei jarraituz eraikiko ditugu:*

1. *Atomo bat ongi eratutako formula da.*

2. *A eta B ongi eratutako formulak badira,* $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ *eta* $(A \leftrightarrow B)$ *ere ongi eratutako formulak dira.*

3. *A ongi eratutako formula bat bada eta x aldagai bat bada,* $(\forall x A)$ *eta* $(\exists x A)$ *ongi eratutako formulak dira.*

4. *Aurreko hiru arauak kopuru finitu aldiz erabiliz lortzen diren formulak soilik dira ongi eratutako formulak.*

2.6 Adibidea. Har ditzagun $\mathcal{V} = \{x, y, z\}$ aldagaien multzoa, $\mathcal{C} = \{a, b\}$ konstanteen multzoa eta $\mathcal{P} = \{P, Q, R\}$ predikatuen multzoa, $ar(P) = 1$, $ar(Q) = 3$, $ar(R) = 2$ aritateak izanik.

Hona hemen ongi eratutako formula batzuk: $P(x)$, $P(b)$, $Q(x, a, y)$, $R(y, a)$, $(\exists y R(y, a))$, $(\exists x R(y, a))$, $(\forall x P(x))$, $((\neg P(x)) \rightarrow Q(x, a, y))$, $(\forall z(((\neg P(x)) \rightarrow Q(x, a, y)) \wedge (\exists x R(y, a))))$.

Hauek, aldiz, ez dira ongi eratutako formulak: $(\forall a P(x))$, $(\forall P(x, y))$, $(\forall x, y P(x, y))$.

Proposizio-logikan bezala, bi eratan ken ditzakegu parentesi batzuk, nahasteko arriskurik ez dagoenean eta zenbatzaileen eta lokailuen artean hierarkia bat definituz:

- 1. maila: $\neg$, $\forall$, $\exists$.
- 2. maila: $\wedge$, $\vee$.
- 3. maila: $\rightarrow$, $\leftrightarrow$.

2.7 Adibideak.

1. $(\forall z((P(x) \wedge R(x, z)) \rightarrow Q(x, a, y)))$ formula honela idatz dezakegu:
   $\forall z(P(x) \wedge R(x, z) \rightarrow Q(x, a, y))$.

2. $\forall x P(x) \rightarrow R(x, y)$ formula $((\forall x P(x)) \rightarrow R(x, y))$ formula da, baina ez hau:
   $(\forall x(P(x) \rightarrow R(x, y)))$.

3. $\forall x \forall y R(x,y) \vee P(y)$ formula $((\forall x(\forall y R(x,y))) \vee P(y))$ formula da.

2.8 Definizioa. *A formula izanik, A formularen* azpiformula *ongi eratutako formula bat da, A formularen zatia bada eta ondoz ondo eraikia bada.*

Adibidez, $A = \forall x P(x) \to R(x,y)$ formula izanik, $\forall x P(x)$ eta $R(x,y)$ azpiformulak dira, baina $P(x) \to R(x,y)$ ez da azpiformula.

2.9 Definizioa. *Formula batean, zenbatzaile baten* agerpen *baten* irismena *agerpen horrek eragiten duen azpiformula da.*

2.10 Adibideak.

1. $\forall x \exists y R(x,y)$ formulan, $\exists y$ zenbatzailearen irismena $R(x,y)$ azpiformula da, eta $\forall x$ zenbatzailearena $\exists y R(x,y)$.

2. $\forall y(\exists x R(x,y) \vee P(x))$ formulan, $\exists x$ zenbatzailearen irismena $R(x,y)$ azpiformula da, eta $\forall y$ zenbatzailearena $\exists x R(x,y) \vee P(x)$.

3. $\forall y(R(x,y) \to \forall x \exists y Q(x,a,y))$ formulan, $\exists y$ zenbatzailearen irismena $Q(x,a,y)$ azpiformula da, $\forall x$ zenbatzailearena $\exists y Q(x,a,y)$ azpiformula da, eta $\forall y$ zenbatzailearena $R(x,y) \to \forall x \exists y Q(x,a,y)$.

2.11 Definizioa. *Aldagai baten agerpen bat formula batean* lotua *da zenbatzaile batekin badago edo aldagaia erabiltzen duen zenbatzaile baten irismenaren barne badago. Agerpena* askea *da ez bada lotua.*

Aldagai bat askea *da formula batean gutxienez aldagaiaren agerpen bat askea bada formulan. Aldagai bat* lotua *da formula batean gutxienez aldagaiaren agerpen bat lotua bada formulan.*

Ohar gaitezen aldagai bat aldi berean askea eta lotua izan daitekeela.

2.12 Definizioa. *Formula bat* itxia *da ez badauka aldagai askeen agerpenik.*

2.13 Adibideak.

1. $\forall x R(x,y)$.

   Zenbatzaileen agerpenen irismenak azpimarratuko ditugu, eta irismenei eta zenbatzaileek lotzen dituzten aldagaien agerpenei azpiindize bera jarriko diegu:

   $\forall x_1 \underline{R(x_1,y)}_1$. x lotua da; y askea da.

2. $\forall x \exists y(R(x,y) \to \forall x P(x))$.

   Jakiteko zenbatzaileen agerpen bakoitzak aldagaien zer agerpen lotzen dituen, formularen barrutik kanpora joango gara, formula eraikitzeko bideari jarraituz.

   $\underline{\forall x_3 \exists y_2 \underline{(R(x_3,y_2) \to \forall x_1 \underline{P(x_1)}_1)}_2}_3$. x, y lotuak dira eta formula itxia da.

3. $\exists x \forall y R(x,y) \vee \exists z Q(x,a,z)$.

   $\exists x_2 \underline{\forall y_1 \underline{R(x_2,y_1)}_1}_2 \vee \exists z_3 \underline{Q(x,a,z_3)}_3$. x askea eta lotua da; y, z lotuak dira.

4. $\forall x \exists y R(x,y) \to \forall x P(x)$.

   $\underline{\forall x_2 \exists y_1 \underline{R(x_2,y_1)}_1}_2 \to \forall x_3 \underline{P(x_3)}_3$. x, y lotuak dira eta formula itxia da.

2.3 Semantika

Proposizio-logikan interpretazio bat atomoei egia-balioak esleitzea zen. Predikatu-logikan aldagaiak erabiltzen ditugunez, hori baino zerbait gehiago beharko dugu.

Lehendabizi, kontuan izan behar dugu zer objektu izan daitezkeen aldagaiaren balioak (hots, aldagaiaren definizio-eremua). Esaterako, demagun $Z(x, y)$ formulak "x y-ren zatitzailea dela" esan nahi duela. x eta y aldagaiak zenbaki osoz ordezkatzen baditugu, proposizio bat lortuko dugu, egiazkoa edo faltsua izango dena. Baina aldagaiak zuhaitz-izenez ordezkatzen baditugu, ez da horrela gertatzen. Ez du zentzurik "Pagoak haritza zatitzen du" esateak. Dena dela, horrelako eztabaida baztertuko dugu suposatuz D *eremu* ez-huts bat dagoela, non D eremuaren elementuak aldagaien balioak diren.

Suposatuko dugu D multzo ez-hutsa ez dugula ezagutzen; hau da, saiatuko gara predikatu-logika garatzen edozein D multzo ez-huts erabiliz.

Adibidez, D eremuak bi elementu baditu, elementuei 1 eta 2 deituko diegu; orduan, $D = \{1, 2\}$ idatz dezakegu. P 3 aritateko predikatu bat bada, $P(x, y, z)$ adierazpenean x, y, z aldagaiek 1 eta 2 balioak har ditzakete: $P(1, 1, 1)$, $P(1, 1, 2)$, ..., $P(2, 2, 2)$.

Guztira, $2^3 = 8$ aukera ditugu, 1 eta 2 zenbakiekin osa ditzakegun hirukote guztiak, hain zuzen. Hirukote horien multzoa honela adieraziko dugu:

$$D^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$$

Antzeko eran, $D^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ dugu.

$D = \{1, 2, 3\}$ eremua badugu, $3^2 = 9$ bikoteen multzoa hau izango da:

$$D^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\},$$

eta $3^3 = 27$ hirukoteen multzoa beste hau:

$$D^3 = \{(1, 1, 1), (1, 1, 2), (1, 1, 3), \ldots, (3, 3, 3)\}.$$

Oro har, D eremuak m elementu baditu, D^n multzoak m^n n-kote izango ditu.

Orain, $P(x, y, z)$ formulatik x, y, z aldagaiak D^3 multzoaren (d_1, d_2, d_3) hirukotearen balioez ordezkatzean lortzen den proposizioa egiazkoa edo faltsua izango da (baina ez biak). Hori D^3 multzoaren hirukote bakoitzarekin gertatuko da; beraz, 3 aritateko P predikatuari φ funtzio bat esleitu ahal izango diogu; funtzio horrek D^3 multzoaren hirukote bakoitzari E edo F balioa esleituko dio, hau da, $\varphi : D^3 \longrightarrow \{E, F\}$ funtzio bat izango dugu.

Adibidez, $D = \{1, 2\}$ bada, demagun $P(1, 1, 1)$, $P(1, 2, 1)$, $P(1, 2, 2)$ proposizioei E balioa esleitzen diegula, eta gainerakoei F balioa. Orduan, P predikatuari esleitzen diogun funtzioa hau da:

$$\begin{array}{llll} \varphi : & D^3 & \to & \{E, F\} \\ & 111 & \mapsto & E \\ & 112 & \mapsto & F \\ & 121 & \mapsto & E \\ & 122 & \mapsto & E \\ & 211 & \mapsto & F \\ & 212 & \mapsto & F \\ & 221 & \mapsto & F \\ & 222 & \mapsto & F \end{array}$$

D^3 zutabean $111, 112, ...$ idatzi dugu, $(1,1,1), (1,1,2), ...$ idatzi beharrean, idazkera sinplifikatzeko asmoz. Horrela egingo dugu nahasteko arriskurik ez dagoenean.

Funtzio horri 3 aritateko *funtzio logiko* deituko diogu, eta honela adieraziko dugu:

D^3	φ
111	E
112	F
121	E
122	E
211	F
212	F
221	F
222	F

$D = \{1, 2\}$ eremuaren kasuan 3 aritateko $2^8 = 256$ funtzio logiko daude P predikatuari esleitu ahal izateko:

D^3	φ_1	φ_2	φ_3	$\dots$	φ_{256}
111	E	E	E	$\dots$	F
112	E	E	E	$\dots$	F
121	E	E	E	$\dots$	F
122	E	E	E	$\dots$	F
211	E	E	E	$\dots$	F
212	E	E	E	$\dots$	F
221	E	E	F	$\dots$	F
222	E	F	E	$\dots$	F

Antzera, P n aritateko predikatu bakoitzari n aritateko funtzio logiko bat esleituko diogu, $\varphi : D^n \longrightarrow \{E, F\}$.

D eremuak m elementu baditu, D^n multzoak m^n elementu izango ditu; eta, beraz, n aritateko $2^{(m^n)}$ funtzio logiko daude.

2.14 Adibideak.

1. Izan bedi $D = \{1, 2\}$ eremua, $m = 2$.

   $n = 1$ aritateko 4 funtzio logikoak:

D	φ_1	φ_2	φ_3	φ_4
1	E	E	F	F
2	E	F	E	F

   $n = 2$ aritateko 16 funtzio logikoak:

D^2	φ_1	φ_2	φ_3	$\dots$	φ_{16}
11	E	E	E	$\dots$	F
12	E	E	E	$\dots$	F
21	E	E	F	$\dots$	F
22	E	F	E	$\dots$	F

2. Izan bedi $D = \{1, 2, 3\}$ eremua, $m = 3$.

   $n = 2$ aritateko 512 funtzio logikoak:

D^2	φ_1	φ_2	$\dots$	φ_{512}
11	E	E	$\dots$	F
12	E	E	$\dots$	F
13	E	E	$\dots$	F
21	E	E	$\dots$	F
22	E	E	$\dots$	F
23	E	E	$\dots$	F
31	E	E	$\dots$	F
32	E	E	$\dots$	F
33	E	F	$\dots$	F

2.15 Definizioa. *A ongi eratutako formula baten* interpretazio *bat emateko D eremu ez-huts bat hartuko dugu eta A formulan agertzen diren konstanteei, aldagai askeei eta predikatu-sinboloei balioak esleituko dizkiegu honela:*

1. *konstante bakoitzari D eremuaren elementu bat esleituko diogu;*

2. *aldagai aske bakoitzari D eremuaren elementu bat esleituko diogu;*

3. *n aritateko predikatu-sinbolo bakoitzari n aritateko funtzio logiko bat esleituko diogu.*

Batzuetan, D eremua azpimarratzeko, D eremuaren gaineko *interpretazioaz hitz egingo dugu.*

2.16 Adibidea. $A = P(x) \wedge \forall x Q(x, a)$.
Konstanteak: a.
Aldagai askeak: x.
Predikatu-sinboloak: P, Q; $ar(P) = 1$, $ar(Q) = 2$.
Dauden interpretazio guztien artean hona hemen bi:

1.

$D = \{1, 2\}$

x	a	P	Q
1	2	α	β

D	α
1	E
2	F

D^2	β
11	E
12	F
21	F
22	E

2.

$D = \{1, 2\}$

x	a	P	Q
2	2	α	β

D	α
1	E
2	E

D^2	β
11	E
12	F
21	F
22	E

2.17 Definizioa. *G ongi eratutako formula bat eta G formularen D eremuaren gaineko I interpretazio bat izanik, G formularen* egia-balioa *I interpretaziorako honela kalkulatuko dugu:*

1. *$G = (\neg A)$, $G = (A \wedge B)$, $G = (A \vee B)$, $G = (A \to B)$ edo $G = (A \leftrightarrow B)$ bada, egia-balioa proposizio-logikan bezala kalkulatuko dugu.*

2. *$G = (\forall x A)$ edo $G = (\exists x A)$ bada, A formularen egia-balioa kalkulatuko dugu x aldagaiak A formulan duen agerpen aske bakoitza D eremuaren elementu guztiez ordezkatuz; horrela, x aldagaiaren funtzio logiko bat lortuko dugu:*

x	A^*
1	E
2	F
$\vdots$	$\vdots$

$V(\forall x A, I) = E$ da funtzio logiko horrek E balioa hartzen badu D eremuaren elementu guztietarako, hau da, A^* zutabean dena E bada. Bestela, hau da, A^* zutabean gutxienez F bat badago, $V(\forall x A, I) = F$.

$V(\exists x A, I) = E$ da funtzio logiko horrek E balioa hartzen badu gutxienez D eremuaren elementu baterako, hau da, A^* zutabean gutxienez E bat badago. Bestela, hau da, A^* zutabean dena F bada, $V(\exists x A, I) = F$.

2.18 Adibideak.

1. $A = \forall x P(x)$

   A formularen I interpretazio bat emateko D eremu bat hartuko dugu eta P predikatu-sinboloari 1 aritateko α funtzio logiko bat esleituko diogu. Bi elementuko eremu baten gainean 1 aritateko lau funtzio logiko daude. Konstanterik eta aldagai askerik ez dagoenez, eta 1 aritateko predikatu bakarra dagoenez, guztira lau interpretazio izango ditugu (bi elementuko eremu baten gainean). Hona hemen horietako bat:

$$I: \quad D = \{1, 2\} \qquad \begin{array}{c} P \\ \hline \alpha \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & E \\ 2 & F \end{array}$$

   $V(A, I)$ kalkulatzeko honela jokatuko dugu:

   1 Funtzio logikoa formulan ordezkatu: $A^* = \forall x \alpha(x)$.

   2 Formula $\forall x$ (zenbatzaile) motakoa denez, zenbatzailearen ($\alpha(x)$) irismenaren egia-balioa kalkulatuko dugu x aldagaiak $\alpha(x)$ adierazpenean duen agerpen aske bakoitza D eremuaren elementu bakoitzaz ordezkatuz:

x	$\alpha(x)$
1	$\alpha(1) = E$
2	$\alpha(2) = F$

   Taulan F bat agertzen denez, $\forall x \alpha(x) = F$ da.

Hau da, $V(A, I) = F$ da.

2. $A = \exists x \neg P(x)$

   Bi elementuko eremu baten gainean lau interpretazio daude. Har dezagun A formularen interpretazio hau:

$$I: \quad D = \{1, 2\} \qquad \begin{array}{c} P \\ \hline \alpha \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & F \\ 2 & E \end{array}$$

   1 Funtzio logikoa formulan ordezkatu: $A^* = \exists x \neg \alpha(x)$.

   2 Formula $\exists x$ (zenbatzaile) motakoa denez, zenbatzailearen ($\neg\alpha(x)$) irismenaren egia-balioa kalkulatuko dugu x aldagaiak $\neg\alpha(x)$ adierazpenean duen agerpen aske bakoitza D eremuaren elementu bakoitzaz ordezkatuz. Bestalde, $\neg\alpha(x)$ adierazpena $\neg$ motakoa da, beraz, proposizio-logikan bezala kalkulatuko dugu:

x	$\alpha(x)$	$\neg\alpha(x)$
1	$\alpha(1) = F$	E
2	$\alpha(2) = E$	F

   Taulan E bat agertzen denez, $\exists x \neg \alpha(x) = E$ da.

   Beraz, $V(A, I) = E$ da.

3. $A = P(x) \vee \forall y(P(y) \to Q(a))$

   $2 \cdot 2 \cdot 4 \cdot 4 = 64$ interpretazio daude bi elementuko eremu baten gainean (aldagai aske bat, konstante bat eta bi predikatu-sinbolo). Interpretazio hau hartuko dugu:

$$I: \quad D = \{1, 2\} \qquad \begin{array}{cccc} x & a & P & Q \\ \hline 2 & 1 & \alpha & \beta \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & E \\ 2 & F \end{array} \qquad \begin{array}{cc} D & \beta \\ \hline 1 & F \\ 2 & F \end{array}$$

   1 $A^* = \alpha(2) \vee \forall y(\alpha(y) \to \beta(1)) = F \vee \forall y(\alpha(y) \to F)$.

   2 $\forall y(\alpha(y) \to F)$ kalkulatu behar dugu:

y	$\alpha(y)$	$\alpha(y) \to F$
1	$\alpha(1) = E$	F
2	$\alpha(2) = F$	E

   $\forall y$ motakoa denez, eta taulan F bat agertzen denez, $\forall y(\alpha(y) \to F) = F$ da. Eta, hortik, $A^* = F \vee F = F$ da.

   Beraz, $V(A, I) = F$ da.

4. $A = \forall x \exists y P(x, y)$

   $D = \{1, 2, 3\}$ eremuaren gainean $2^9 = 512$ interpretazio daude; hau hartuko dugu:

$$I: \quad D = \{1, 2, 3\} \qquad \frac{P}{\alpha}$$

D^2	α
11	E
12	E
13	F
21	F
22	E
23	E
31	F
32	F
33	E

1 $A^* = \forall x \exists y \alpha(x, y)$.

2 $\forall x \exists y \alpha(x, y)$ kalkulatu behar dugu; hona hemen dagokion taula:

x	$\exists y \alpha(x, y)$
1	$\exists y \alpha(1, y)$
2	$\exists y \alpha(2, y)$
3	$\exists y \alpha(3, y)$

$\exists y \alpha(1, y)$ adierazpena $\exists y$ motakoa denez, dagokion taula eraiki beharko dugu; eta berdin $\exists y \alpha(2, y)$ eta $\exists y \alpha(3, y)$ adierazpenekin. Beraz, taula baten barnean hiru taula izango ditugu; honela:

x	y	$\alpha(1, y)$	$\exists y \alpha(x, y)$
1	1	$\alpha(1, 1) = E$	$\exists y \alpha(1, y) = E$
	2	$\alpha(1, 2) = E$	
	3	$\alpha(1, 3) = F$	
	y	$\alpha(2, y)$	
2	1	$\alpha(2, 1) = F$	$\exists y \alpha(2, y) = E$
	2	$\alpha(2, 2) = E$	
	3	$\alpha(2, 3) = E$	
	y	$\alpha(3, y)$	
3	1	$\alpha(3, 1) = F$	$\exists y \alpha(3, y) = E$
	2	$\alpha(3, 2) = F$	
	3	$\alpha(3, 3) = E$	

$\forall x$ motakoa denez, eta (eskuineko) taulan dena E denez, $\forall x \exists y \alpha(x, y) = E$ da.

Hortaz, $V(A, I) = E$ da.

2.4 Baliozkotasuna. Inkontsistentzia. Ondorio logikoak

Baliozkotasunaren, kontsistentziaren eta ondorio logikoaren definizioek bere horretan diraute, proposizio-logikan bezala.

2.19 Definizioa. *A formula bat* tautologia *edo* baliozkoa *da A formularen interpretazio guztietarako egiazkoa bada. A formula* baliogabea *da ez bada baliozkoa.*

A formula bat kontsistentea *da gutxienez A formularen interpretazio baterako egiazkoa bada. A formula bat* inkontsistentea *edo* kontraesana *da ez bada kontsistentea.*

2.20 Definizioa. *$A_1, \ldots, A_n$ eta B formulak izanik, B formula $A_1, \ldots, A_n$ formulen* ondorio logikoa *dela edo formuletatik* logikoki deduzitzen *dela esango dugu $V(A_1, I) = E$, $\cdots$, $V(A_n, I) = E$ egiten duen edozein I interpretaziotarako $V(B, I) = E$ ere bada. Eta honela adieraziko dugu:*

$$A_1, \ldots, A_n \Rightarrow B \quad \textit{edo} \quad A_1, \ldots, A_n \models B.$$

2.21 Definizioa. *$P_1, \ldots, P_n / \therefore C$ argumentu bat* baliozkoa *da C ondorioa premisen ondorio logikoa bada. Hau da, $V(P_1, I) = E$, $\cdots$, $V(P_n, I) = E$ egiten duen edozein I interpretaziotarako $V(C, I) = E$ ere bada. Argumentua* baliogabea *da ez bada baliozko argumentua.*

Teorema hauek ere betetzen dira:

2.22 Teorema.

1. *B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin*
   $\models (A_1 \wedge \cdots \wedge A_n \rightarrow B)$ *bada.*

2. *B formula $A_1, \ldots, A_n$ formulen ondorio logikoa da baldin eta soilik baldin*
   $A_1 \wedge \cdots \wedge A_n \wedge \neg B$ *formula inkontsistentea bada.*

Hala eta guztiz ere, predikatu-logikaren egoera eta proposizio-logikaren egoera zeharo desberdinak dira. Azken horretan edozein formularen egia-taula eraikitzea posiblea den bitartean, predikatu-logikan ez da hori beti posible.

Predikatu-logikan, eremua finitua denean, egia-taula eraiki dezakegu, teorikoki bada ere. Baina formula bat baliozkoa izateko, edozein eremuren gaineko edozein interpretaziotarako egiazkoa izan behar du, eremu infinituak barne. Berdin formula inkontsistenteekin, baliogabeekin...

Dena dela, formula bat baliozkoa edo kontsistentea den ala ez arrazoi dezakegu egia-taula lerroz lerro eraiki gabe.

2.23 Adibideak.

1. Ikus dezagun $A = \exists x(P(x) \wedge \neg P(x))$ formula inkontsistentea dela.

   Izan bitez D edozein eremu ez-huts eta I edozein interpretazio eremu horren gainean.

$$I: \quad D \quad \frac{P}{\alpha} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \\ \vdots & \vdots \end{array}$$

1 $A^* = \exists x(\alpha(x) \wedge \neg\alpha(x))$.

2 $\exists x(\alpha(x) \wedge \neg\alpha(x))$ kalkulatu behar dugu.

x	$\alpha(x)$	$\neg\alpha(x)$	$\alpha(x) \wedge \neg\alpha(x)$
1	$\alpha(1) =?$	$\neg?$	$? \wedge \neg? = F$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

$\exists x$ motakoa denez eta taulan dena F denez, $\exists x(\alpha(x) \wedge \neg\alpha(x)) = F$ izango da.

Beraz, $V(A, I) = F$ da, non I edozein interpretazio eta D edozein eremu diren. Hortaz, A formula inkontsistentea da.

2. Ikus dezagun $A = P(y) \to \forall x P(x)$ formula baliogabea dela.

Horretarako nahikoa da $V(A, I) = F$ betetzen duen I interpretazio bat bilatzea.

Proba dezagun $D = \{1\}$ eremuarekin.

$$I: \qquad D = \{1\} \qquad \begin{array}{cc} y & P \\ \hline 1 & \alpha \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \end{array}$$

1 $A^* = \alpha(1) \to \forall x \alpha(x)$.

2 $A^* = F$ izateko, $\alpha(1) = E$ eta $\forall x \alpha(x) = F$ bete behar dira. Orduan, 1 aritateko funtzio logiko hau daukagu:

$$\begin{array}{cc} D & \alpha \\ \hline 1 & E \end{array}$$

Orduan, taula hau izango genuke:

$$\begin{array}{cc} x & \alpha(x) \\ \hline 1 & \alpha(1) = E \end{array}$$

Taulan dena E denez, $\forall x \alpha(x) = E$ izango da.

Beraz, $D = \{1\}$ eremurako ezin izan dugu aurkitu A formula faltsutzen duen interpretaziorik (A formula kontsistentea da).

Proba dezagun $D = \{1, 2\}$ eremuarekin.

$$I: \qquad D = \{1, 2\} \qquad \begin{array}{cc} y & P \\ \hline d & \alpha \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \\ 2 & ? \end{array}$$

(d D eremuaren elementu bat da)

1 $A^* = \alpha(d) \to \forall x \alpha(x)$.

2 $A^* = F$ izateko, $\alpha(d) = E$ eta $\forall x \alpha(x) = F$ bete behar dira. Biak bete daitezen:

$$\begin{array}{cc} x & \alpha(x) \\ \hline 1 & \alpha(1) \\ 2 & \alpha(2) \end{array} \quad F \text{ bat eta } E \text{ bat}$$

Har dezagun, adibidez, interpretazio hau:

$$I: \qquad D = \{1, 2\} \qquad \begin{array}{cc} y & P \\ \hline 1 & \alpha \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & E \\ 2 & F \end{array}$$

Egiaztapena:

1 $A^* = \alpha(d) \to \forall x \alpha(x)$.

2 Interpretazio honetarako $\alpha(1) = E$ eta $\forall x \alpha(x) = F$ dauzkagu, taula honetan F bat dagoelako:

x	$\alpha(x)$
1	$\alpha(1) = E$
2	$\alpha(2) = F$

Beraz, $A^* = E \to F = F$ da.

Ondorioz, $V(A, I) = F$ da eta A formula baliogabea da.

3. Ikus dezagun $B = Q(a)$ formula $A_1 = \forall x(P(x) \to Q(x))$ eta $A_2 = P(a)$ formulen ondorio logikoa dela.

Horretarako frogatu beharko dugu $V(A_1, I) = V(A_2, I) = E$ bada, $V(B, I) = E$ ere izango dela, edozein I interpretaziotarako.

Izan bitez D edozein eremu eta I edozein interpretazio D eremuaren gainean, non $V(A_1, I) = V(A_2, I) = E$ den.

$$I: \ D \qquad \begin{array}{ccc} a & P & Q \\ \hline d & \alpha & \beta \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \\ \vdots & \vdots \end{array} \qquad \begin{array}{cc} D & \beta \\ \hline 1 & ? \\ \vdots & \vdots \end{array}$$

$A_1^* = \forall x(\alpha(x) \to \beta(x))$.

$A_2^* = \alpha(d)$.

$A_2^* = E$ izateko $\alpha(d) = E$ bete behar da; beraz, α funtzioaren taulan, errenkada bat honelakoa izango da: $\boxed{d \qquad \alpha(d) = E}$.

$A_1^* = E$ denez, $\alpha(x) \to \beta(x)$ adierazpenaren taularen errenkada guztietan E agertuko da. Horien artean, d duen errenkada: $\boxed{d \qquad \alpha(d) \to \beta(d) = E}$.

$B^* = \beta(d)$.

$\alpha(d) \to \beta(d) = E$ eta $\alpha(d) = E$ direnez, $\beta(d) = E$ bete beharko da.

Hortaz, $V(B, I) = E$ eta B formula A_1 eta A_2 formulen ondorio logikoa da.

4. Ikus dezagun argumentu hau baliogabea dela:

$$\begin{array}{l} A_1 = \forall x(P(x) \to \neg Q(x)) \\ A_2 = \exists x(R(x) \wedge Q(x)) \\ \hline B = \forall x(P(x) \to R(x)) \end{array}$$

Argumentu bat baliogabea dela frogatzeko nahikoa da frogatzea ondorioa ez dela premisen ondorio logikoa. Hau da, nahikoa da premisak egiazko egiten dituen eta ondorioa faltsutzen duen interpretazio bat aurkitzea.

Proba dezagun $D = \{1\}$ eremuarekin.

$$I: \quad D \qquad \begin{array}{ccc} P & Q & R \\ \hline \alpha & \beta & \gamma \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \end{array} \qquad \begin{array}{cc} D & \beta \\ \hline 1 & ? \end{array} \qquad \begin{array}{cc} D & \gamma \\ \hline 1 & ? \end{array}$$

$A_1^* = \forall x(\alpha(x) \to \neg\beta(x))$.

$A_1^* = E$ izateko, $\begin{array}{cc} x & \alpha(x) \to \neg\beta(x) \\ \hline 1 & \alpha(1) \to \neg\beta(1) = E \end{array}$ bete behar da.

$A_2^* = \exists x(\gamma(x) \wedge \beta(x))$.

$A_2^* = E$ izateko, $\begin{array}{cc} x & \gamma(x) \wedge \beta(x) \\ \hline 1 & \gamma(1) \wedge \beta(1) = E \end{array}$ bete behar da.

Hortaz, azkenekotik, $\gamma(1) = E$ eta $\beta(1) = E$ dira. $\beta(1) = E$ denez, $\neg\beta(1) = F$ da eta, $\alpha(1) \to \neg\beta(1) = E$ bete behar denez, $\alpha(1) = F$ aterako dugu. Eta B^* adierazpenerako, taula hau daukagu:

$$\begin{array}{cc} x & \alpha(x) \to \gamma(x) \\ \hline 1 & \alpha(1) \to \gamma(1) = E \end{array}$$

eta, hortaz, $B^* = E$ da.

Ondorioz, $D = \{1\}$ eremuarekin ezin izan dugu aurkitu A_1 eta A_2 egiazko eta B faltsu egiten dituen interpretaziorik.

Proba dezagun $D = \{1, 2\}$ eremuarekin.

$$I: \quad D \qquad \begin{array}{ccc} P & Q & R \\ \hline \alpha & \beta & \gamma \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & ? \\ 2 & ? \end{array} \qquad \begin{array}{cc} D & \beta \\ \hline 1 & ? \\ 2 & ? \end{array} \qquad \begin{array}{cc} D & \gamma \\ \hline 1 & ? \\ 2 & ? \end{array}$$

$A_1^* = \forall x(\alpha(x) \to \neg\beta(x))$.

$A_1^* = E$ izateko,

$$\begin{array}{cc} x & \alpha(x) \to \neg\beta(x) \\ \hline 1 & \alpha(1) \to \neg\beta(1) = E \\ 2 & \alpha(2) \to \neg\beta(2) = E \end{array} \quad \text{bete behar da.} \tag{2.1}$$

$A_2^* = \exists x(\gamma(x) \wedge \beta(x))$.

$A_2^* = E$ izateko,

$$\begin{array}{cc} x & \gamma(x) \wedge \beta(x) \\ \hline 1 & \gamma(1) \wedge \beta(1) \\ 2 & \gamma(2) \wedge \beta(2) \end{array} \quad \text{batek } E \text{ izan behar du.} \tag{2.2}$$

$B^* = \forall x(\alpha(x) \to \gamma(x))$.

$B^* = F$ izateko,

x	$\alpha(x) \to \gamma(x)$
1	$\alpha(1) \to \gamma(1)$
2	$\alpha(2) \to \gamma(2)$

batek F izan behar du. (2.3)

(2.2) betetzeko, nahikoa da $\gamma(1) = \beta(1) = E$ betetzea ($\neg\beta(1) = F$). Orduan, (2.1) betetzeko, $\alpha(1) \to \neg\beta(1) = E$ izan behar denez, $\alpha(1) = F$ aterako dugu. Eta hortik $\alpha(1) \to \gamma(1) = E$ daukagu, hau da, (2.3) taulako lehenengo errenkadan E dugu.

Hortaz, (2.3) betetzeko, $\alpha(2) \to \gamma(2) = F$ bete behar da, hau da, $\alpha(2) = E$ eta $\gamma(2) = F$. Orain, (2.1) betetzeko, $\alpha(2) = E$ denez, $\alpha(2) \to \neg\beta(2) = E$ izateko, $\neg\beta(2) = E$ edo $\beta(2) = F$ izango dira.

Laburbilduz, hona hemen A_1 eta A_2 egiazko eta B faltsu egiten dituen interpretazio bat:

$I: \; D$

P	Q	R
α	β	γ

D	α
1	F
2	E

D	β
1	E
2	F

D	γ
1	E
2	F

Egiaztapena:

$A_1^* = \forall x(\alpha(x) \to \neg\beta(x))$

x	$\alpha(x)$	$\beta(x)$	$\neg\beta(x)$	$\alpha(x) \to \neg\beta(x))$
1	F	E	F	E
2	E	F	E	E

$A_2^* = \exists x(\gamma(x) \wedge \beta(x))$

x	$\gamma(x)$	$\beta(x)$	$\gamma(x) \wedge \beta(x)$
1	E	E	E
2	F	F	F

$B^* = \forall x(\alpha(x) \to \gamma(x))$

x	$\alpha(x)$	$\gamma(x)$	$\alpha(x) \to \gamma(x)$
1	F	E	E
2	E	F	F

Beraz, $V(A_1, I) = V(A_2, I) = E$ eta $V(B, I) = F$ betetzen dira. Eta argumentua baliogabea da.

2.5 Baliokidetza logikoak

2.24 Definizioa. *A eta B ongi eratutako bi formulak* logikoki baliokideak *dira ($A \equiv B$) egia-balio berberak badituzte interpretazio guztietarako, $V(A, I) = V(B, I)$.*

Ondorioak.

1. Proposizio-logikaren baliokidetza logikoek bere horretan diraute predikatu-logikan.
2. $A \equiv B$ da baldin eta soilik baldin $\models (A \leftrightarrow B)$ bada.

Horietaz gain, predikatu-logikan baliokidetza gehiago dauzkagu.

Idazkera.

- $A[x]$, $B[x]$: x aldagaia aske duten formulak dira. Adibideak:
  $A[x] = P(x)$, $A[x] = \forall y(P(x) \wedge Q(y) \to \exists x R(x,x))$, $A[x] = P(x) \to \forall y P(y)$, etab.
- J: x aldagaia aske ez duen formula da. Adibideak:
  $J = \forall y P(y)$, $J = \forall x P(x) \to Q(y)$, etab.
- $A^*[x]$, J^*: I interpretazio bat $A[x]$, J formuletan ordezkatzean lortzen diren adierazpenak dira.

Zenbatzaileen baliokidetzak

1. $\neg\forall x A[x] \equiv \exists x \neg A[x]$.
2. $\forall x \neg A[x] \equiv \neg\exists x A[x]$.
3. $\forall x A[x] \wedge \forall x B[x] \equiv \forall x(A[x] \wedge B[x])$, $\forall$ zenbatzailea banakorra da $\wedge$ lokailuarekiko.
4. $\exists x A[x] \vee \exists x B[x] \equiv \exists x(A[x] \vee B[x])$, $\exists$ zenbatzailea banakorra da $\vee$ lokailuarekiko.
5. 1. $\forall x A[x] \vee J \equiv \forall x(A[x] \vee J)$.
   2. $\exists x A[x] \vee J \equiv \exists x(A[x] \vee J)$.
6. 1. $\forall x A[x] \wedge J \equiv \forall x(A[x] \wedge J)$.
   2. $\exists x A[x] \wedge J \equiv \exists x(A[x] \wedge J)$.

Ez dira baliokideak

EB1: $\forall x A[x] \vee \forall x B[x] \not\equiv \forall x(A[x] \vee B[x])$, $\forall$ zenbatzailea ez da banakorra $\vee$ lokailuarekiko.

EB2: $\exists x A[x] \wedge \exists x B[x] \not\equiv \exists x(A[x] \wedge B[x])$, $\exists$ zenbatzailea ez da banakorra $\wedge$ lokailuarekiko.

Froga.

1. $G = \neg\forall x A[x] \equiv \exists x \neg A[x] = H$ dela frogatzeko ikusi behar dugu edozein I interpretaziotarako $V(G,I) = V(H,I)$ betetzen dela.

   Izan bitez D edozein eremu eta I edozein interpretazio D eremuaren gainean.

   I interpretazioa G eta H formuletan ordezkatuz, $G^* = \neg\forall x A^*[x]$ eta $H^* = \exists x \neg A^*[x]$ adierazpenak lortuko ditugu, hurrenez hurren.

   Bi aukerak ditugu: a) $V(G,I) = E$. b) $V(G,I) = F$.

   a) $V(G,I) = E$ bada, $G^* = \neg\forall x A^*[x] = E$ izango da; orduan, $\forall x A^*[x] = F$ izango da. Beraz, $A^*[x]$ adierazpenaren taulan honelako errenkada bat egongo da: $\boxed{d \quad A^*[d] = F}$.

$\neg A^*[x]$ adierazpenaren errenkada hori honelakoa izango da: $\boxed{d \quad \neg A^*[d] = E}$. Beraz, $H^* = \exists x \neg A^*[x] = E$ beteko da.

Hortaz, $V(H, I) = E = V(G, I)$ dugu.

b) $V(G, I) = F$ bada, $G^* = \neg \forall x A^*[x] = F$ izango da; orduan, $\forall x A^*[x] = E$ izango da. Beraz, $A^*[x]$ adierazpenaren taulan dena da E.

$A^*[x]$ adierazpenaren taulan dena E bada, $\neg A^*[x]$ adierazpenaren taulan dena F izango da. Beraz, $H^* = \exists x \neg A^*[x] = F$ da.

Hortaz, $V(H, I) = F = V(G, I)$ da.

Bi kasuetan, $V(G, I) = V(H, I)$ dugu, hau da, $G \equiv H$.

2. $G = \forall x \neg A[x] \equiv \neg \exists x A[x] = H$ dela frogatzeko baliokidetasun logikoaren definizioa erabil dezakegu, aurrekoan bezala, eta frogatu edozein I interpretaziotarako $V(G, I) = V(H, I)$ betetzen dela.

   Baina, jadanik frogatu ditugun baliokidetzak ere erabil ditzakegu, aurrekoa eta proposizio-logikarenak.

   $G = \forall x \neg A[x] \overset{UB}{\equiv} \neg(\neg \forall x \neg A[x]) \overset{1.}{\equiv} \neg \exists x \neg \neg A[x] \overset{UB}{\equiv} \neg \exists x A[x] = H.$

3. $G = \forall x A[x] \wedge \forall x B[x] \equiv \forall x (A[x] \wedge B[x]) = H$ dela frogatzeko baliokidetasun logikoaren definizioa erabiliko dugu.

   Izan bitez D edozein eremu eta I edozein interpretazio D eremuaren gainean.

   I interpretazioa G eta H formuletan ordezkatzean, $G^* = \forall x A^*[x] \wedge \forall x B^*[x]$ eta $H^* = \forall x (A^*[x] \wedge B^*[x])$ adierazpenak lortuko ditugu, hurrenez hurren.

   Bi aukerak ditugu: a) $G^* = E$. b) $G^* = F$.

   a) $G^* = E$ bada, $\forall x A^*[x] = E$ eta $\forall x B^*[x] = E$ izango dira. Beraz, $A^*[x]$ eta $B^*[x]$ adierazpenen tauletan errenkada guztiak dira E.

   Hortik, $A^*[x] \wedge B^*[x]$ adierazpenaren taularen errenkada guztietan E agertuko da. Ondorioz, $H^* = \forall x (A^*[x] \wedge B^*[x]) = E$ dugu.

   Hortaz, $V(H, I) = E = V(G, I)$ da.

   b) $G^* = F$ bada, beste bi aukera dauzkagu: b.1) $\forall x A^*[x] = E$. b.2) $\forall x A^*[x] = F$.

   b.1) $\forall x A^*[x] = E$ bada, $G^* = F$ denez, $\forall x B^*[x] = F$ izango da. Beraz, $B^*[x]$ adierazpenaren taulan honelako errenkada bat egongo da: $\boxed{d \quad B^*[d] = F}$.

   Errenkada hori bera baina orain $A^*[x] \wedge B^*[x]$ adierazpenaren taulan hau izango da: $\boxed{d \quad A^*[d] \wedge B^*[d] = F}$. Beraz, $H^* = \forall x (A^*[x] \wedge B^*[x]) = F$ beteko da.

   Ondorioz, $V(H, I) = F = V(G, I)$ dugu.

   b.2) $\forall x A^*[x] = F$ bada, $A^*[x]$ adierazpenaren taularen errenkadaren batean hau izango dugu: $\boxed{d \quad A^*[d] = F}$. $A^*[x] \wedge B^*[x]$ adierazpenaren taularen errenkada berean beste hau izango dugu: $\boxed{d \quad A^*[d] \wedge B^*[d] = F}$.

   Hortaz, $H^* = \forall x (A^*[x] \wedge B^*[x]) = F$ da.

Ondorioz, $V(H,I) = F = V(G,I)$ betetzen da

Hortaz, edozein I interpretaziotarako $V(H,I) = V(G,I)$ daukagu, hau da, $G \equiv H$.

4. $G = \exists x A[x] \vee \exists x B[x] \equiv \exists x(A[x] \vee B[x]) = H$ betetzen dela frogatzeko jadanik frogatu ditugun baliokidetzak erabiliko ditugu.

$G = \exists x A[x] \vee \exists x B[x] \overset{UB}{\equiv} \neg(\neg(\exists x A[x] \vee \exists x B[x])) \overset{DeM}{\equiv} \neg(\neg\exists x A[x] \wedge \neg\exists x B[x]) \overset{2.}{\equiv}$

$\equiv \neg(\forall x \neg A[x] \wedge \forall x \neg B[x]) \overset{3.}{\equiv} \neg\forall x(\neg A[x] \wedge \neg B[x]) \overset{1.}{\equiv} \exists x \neg(\neg A[x] \wedge \neg B[x]) \overset{DeM}{\equiv}$

$\equiv \exists x(\neg\neg A[x] \vee \neg\neg B[x]) \overset{UB}{\equiv} \exists x(A[x] \vee B[x]) = H$

5. 1. $G = \forall x A[x] \vee J \equiv \forall x(A[x] \vee J) = H$ betetzen dela frogatzeko baliokidetasun logikoaren definizioa erabiliko dugu.

Izan bitez D edozein eremu eta I edozein interpretazio D eremuaren gainean.

I interpretazioa G eta H bi formuletan ordezkatuz gero, $G^* = \forall x A^*[x] \vee J^*$ eta $H^* = \forall x(A^*[x] \vee J^*)$ adierazpenak lortuko ditugu, hurrenez hurren.

Aukerak: a) $G^* = \forall x A^*[x] \vee J^* = E$. b) $G^* = \forall x A^*[x] \vee J^* = F$.

a) $G^* = E$ bada, beste bi aukera ditugu: a.1) $J^* = E$. a.2) $J^* = F$.

a.1) $J^* = E$ bada, $A^*[x] \vee J^*$ adierazpenaren taularen errenkada guztietan E agertuko da. Beraz, $H^* = \forall x(A^*[x] \vee J^*) = E$ izango da.

Hortaz, $V(H,I) = E = V(G,I)$ beteko da.

a.2) $J^* = F$ bada, $G^* = E$ denez, $\forall x A^*[x] = E$ bete beharko da. Hau da, $A^*[x]$ adierazpenaren taularen errenkada guztietan E agertuko da. Hortik, $A^*[x] \vee J^*$ adierazpenaren taularen errenkada guztietan E agertuko da. Eta, horren ondorioz, $H^* = \forall x(A^*[x] \vee J^*) = E$ izango da.

Kasu honetan ere $V(H,I) = E = V(G,I)$ beteko da.

b) $G^* = \forall x A^*[x] \vee J^* = F$ bada, $\forall x A^*[x] = F$ eta $J^* = F$ bete beharko dira. Lehenengotik aterako dugu $A^*[x]$ adierazpenaren taularen errenkadaren batean F agertuko dela: $\boxed{d \quad A^*[d] = F}$. $A^*[x] \vee J^*$ adierazpenaren taularen errenkada berean ere F agertuko da: $\boxed{d \quad A^*[d] \vee J^* = F}$. Ondorioz, $H^* = \forall x(A^*[x] \vee J^*) = F$ izango da.

Kasu honetan $V(H,I) = F = V(G,I)$ dugu.

Hortaz, edozein I interpretaziotarako $V(H,I) = V(G,I)$ daukagu, hau da, $G \equiv H$.

2. $G = \exists x A[x] \vee J \equiv \exists x(A[x] \vee J) = H$ betetzen dela frogatzeko baliokidetasun logikoaren definizioa erabiliko dugu berriro.

Izan bitez D edozein eremu eta I edozein interpretazio D eremuaren gainean.

I interpretazioa G eta H bi formuletan ordezkatuz gero, $G^* = \exists x A^*[x] \vee J^*$ eta $H^* = \exists x(A^*[x] \vee J^*)$ adierazpenak lortuko ditugu, hurrenez hurren.

Aukerak: a) $G^* = E$. b) $G^* = F$.

a) $G^* = E$ bada, beste bi aukera ditugu: a.1) $J^* = E$. a.2) $J^* = F$.

a.1) $J^* = E$ bada, $A^*[x] \vee J^*$ adierazpenaren taulan dena E izango da. Beraz, $H^* = \exists x(A^*[x] \vee J^*) = E$ izango da.

Kasu honetan $V(H, I) = E = V(G, I)$ betetzen da.

a.2) $J^* = F$ bada, $G^* = E$ denez, $\exists x A^*[x] = E$ bete behar da. Beraz, $A^*[x]$ adierazpenaren taulan honelako errenkadaren bat egongo da: $\boxed{d \quad A^*[d] = E}$. Errenkada hori bera $A^*[x] \vee J^*$ adierazpenaren taulan hau izango da: $\boxed{d \quad A^*[d] \vee J^* = E}$. Beraz, $H^* = \exists x(A^*[x] \vee J^*) = E$ dugu.

Kasu honetan ere $V(H, I) = E = V(G, I)$ betetzen da.

b) $G^* = F$ bada, $\exists x A^*[x] = F$ eta $J^* = F$ izango dira. Lehenengotik aterako dugu $A^*[x]$ adierazpenaren taulan dena F dela. Beraz, $A^*[x] \vee J^*$ adierazpenaren taulan ere dena F da. Hortaz, $H^* = \exists x(A^*[x] \vee J^*) = F$ izango da.

Kasu honetan ere $V(H, I) = F = V(G, I)$ betetzen da.

Ondorioz, edozein I interpretaziotarako $V(H, I) = V(G, I)$ daukagunez, $G \equiv H$ betetzen da.

6. 6.1. eta 6.2. frogatzeko aurreko baliokidetza batzuk erabiliko ditugu.

1. $\forall x A[x] \wedge J \overset{UB}{\equiv} \neg\neg(\forall x A[x] \wedge J) \overset{DeM}{\equiv} \neg(\neg\forall x A[x] \vee \neg J) \overset{1.}{\equiv} \neg(\exists x \neg A[x] \vee \neg J) \overset{5.2.}{\equiv}$
$\equiv \neg\exists x(\neg A[x] \vee \neg J) \overset{DeM}{\equiv} \neg\exists x \neg(A[x] \wedge J) \overset{2.}{\equiv} \forall x \neg(\neg(A[x] \wedge J)) \overset{UB}{\equiv} \forall x(A[x] \wedge J)$.

2. $\exists x A[x] \wedge J \overset{UB}{\equiv} \neg\neg(\exists x A[x] \wedge J) \overset{DeM}{\equiv} \neg(\neg\exists x A[x] \vee \neg J) \overset{2.}{\equiv} \neg(\forall x \neg A[x] \vee \neg J) \overset{5.1.}{\equiv}$
$\equiv \neg(\forall x(\neg A[x] \vee \neg J)) \overset{DeM}{\equiv} \neg(\forall x \neg(A[x] \wedge J)) \overset{1.}{\equiv} \exists x \neg\neg(A[x] \wedge J) \overset{UB}{\equiv} \exists x(A[x] \wedge J)$.

Egiazta dezagun, orain, EB1 eta EB2 ez direla baliokidetzak.

EB1: $\forall x A[x] \vee \forall x B[x] \not\equiv \forall x(A[x] \vee B[x])$ dela frogatzeko ikus dezagun $A[x] = P(x)$ eta $B[x] = Q(x)$ direnean, $G = \forall x P(x) \vee \forall x Q(x) \not\equiv \forall x(P(x) \vee Q(x)) = H$ dela.

Horretarako nahikoa izango da $V(H, I) \neq V(G, I)$ betetzen duen I interpretazio bat aurkitzea.

Har dezagun interpretazio hau:

$$I: \quad D = \{1, 2\} \qquad \begin{array}{cc} P & Q \\ \hline \alpha & \beta \end{array} \qquad \begin{array}{cc} D & \alpha \\ \hline 1 & E \\ 2 & F \end{array} \qquad \begin{array}{cc} D & \beta \\ \hline 1 & F \\ 2 & E \end{array}$$

$G^* = \forall x \alpha(x) \vee \forall x \beta(x)$.

$$\left.\begin{array}{cc} x & \alpha(x) \\ \hline 1 & \alpha(1) = E \\ 2 & \alpha(2) = F \end{array}\right\} \forall x \alpha(x) = F \qquad \left.\begin{array}{cc} x & \beta(x) \\ \hline 1 & \beta(1) = F \\ 2 & \beta(2) = E \end{array}\right\} \forall x \beta(x) = F$$

Beraz, $G^* = F \vee F = F$ betetzen da.

$H^* = \forall x(\alpha(x) \vee \beta(x))$.

x	$\alpha(x)$	$\beta(x)$	$\alpha(x) \vee \beta(x)$	
1	$\alpha(1) = E$	$\beta(1) = F$	$\alpha(1) \vee \beta(1) = E$	$H^* = \forall x(\alpha(x) \vee \beta(x)) = E$
2	$\alpha(2) = F$	$\beta(2) = E$	$\alpha(2) \vee \beta(2) = E$	

Orduan, $V(H, I) \neq V(G, I)$. Eta, beraz, $G \not\equiv H$ daukagu.

EB2: $G = \exists x A[x] \wedge \exists x B[x] \not\equiv \exists x(A[x] \wedge B[x]) = H$ dela frogatzeko, ikus dezakegu, aurrekoan bezala, I interpretazio baterako $V(H, I) \neq V(G, I)$ dela. Baina jadanik frogaturik dauden baliokidetzak eta baliokidetza ez den aurrekoa ere erabil ditzakegu.

$$G = \exists x A[x] \wedge \exists x B[x] \overset{UB}{\equiv} \neg\neg(\exists x A[x] \wedge \exists x B[x]) \overset{DeM}{\equiv} \neg(\neg\exists x A[x] \vee \neg\exists x B[x]) \overset{2.}{\equiv}$$

$$\equiv \neg(\forall x \neg A[x] \vee \forall x \neg B[x]) \overset{EB1}{\not\equiv} \neg\forall x(\neg A[x] \vee \neg B[x]) \overset{1.}{\equiv} \exists x \neg(\neg A[x] \vee \neg B[x]) \overset{DeM}{\equiv}$$

$$\equiv \exists x(\neg\neg A[x] \wedge \neg\neg B[x]) \overset{UB}{\equiv} \exists x(A[x] \wedge B[x]) = H. \qquad \square$$

2.6 Dedukzio formala

Predikatu-logikan ere argumentuak baliozkoak diren ala ez ikusteko froga formalak egin ditzakegu.

Hona hemen erabiliko ditugun erregelak:

1. Proposizio-logikaren 9 inferentzia-erregelak (MP, MT, SH, SD, DE, DS, KS, KK, DB).

2. Ordezkapen-erregela, proposizio-logikaren 10 baliokidetza logikoak erabiliz, (ELKAR, TRUK, BANA, TAUT, UB, DeM, TRANS, INP, BALIO, ESP) eta aurreko atalean frogatutako zenbatzaileen 6 baliokidetzak.

3. Baldintzazko frogaren erregela (BFE) eta absurdora eramateko erregela (AEE).

4. Atal honetako erregela berriak : *Zenbatzaileen erregelak*. Erregela hauek froga baten errenkada osoei bakarrik aplika diezazkiekegu.

Idazkera. Erregela horiek erabiltzean idazkera hau erabiliko dugu:

$A(x)$ edozein formula da; $A(r)$ da x aldagaiak $A(x)$ formulan dituen agerpen aske guztiak r balioaz ordezkatzean lortzen den formula.

2.25 Adibideak.

1. $A(x) = \forall z(Q(x) \vee \forall x P(x, y, z))$ bada, $A(y) = \forall z(Q(y) \vee \forall x P(x, y, z))$ daukagu.

2. $A(y) = \exists x(P(x, y) \vee \forall z \exists y P(y, z))$ bada, $A(z) = \exists x(P(x, z) \vee \forall z \exists y P(y, z))$ daukagu.

3. $A(x) = \forall x P(x, y) \vee P(z, y)$ bada, $A(z) = \forall x P(x, y) \vee P(z, y)$ $(= A(x))$ daukagu.

4. $A(x) = \forall y P(y)$ bada, $A(y) = A(z) = A(x)$ daukagu.

2.26 Definizioa. *Esango dugu r aldagaia $A(x)$ formulan x aldagairako* askea *dela, ordezkapenaren ondoren, r aldagaiak $A(r)$ formulan dituen agerpen guztiak askeak badira (r posizio gehiagotan ager daiteke aske).*

2.27 Adibideak.

1. $A(x) = \forall z(Q(x) \vee \forall x P(x,y,z))$.
   $A(y) = \forall z(Q(y) \vee \forall x P(x,y,z))$. y askea da x aldagairako $A(x)$ formulan.
   $A(z) = \underline{\forall z}(Q(\underline{z}) \vee \forall x P(x,y,z))$. z ez da askea x aldagairako $A(x)$ formulan.
2. $A(y) = \exists x(P(x,y) \vee \forall z \exists y P(y,z))$.
   $A(z) = \exists x(P(x,z) \vee \forall z \exists y P(y,z))$. z askea da y aldagairako $A(y)$ formulan.
   $A(x) = \underline{\exists x}(P(x,\underline{x}) \vee \forall z \exists y P(y,z))$. x ez da askea y aldagairako $A(y)$ formulan.
3. $A(x) = \forall x P(x,y) \vee P(z,y)$.
   $A(z) = A(y) = \cdots = A(x)$. Edozein aldagai da askea x aldagairako $A(x)$ formulan.

Oharrak.

1. $A(x)$ formulak ez badu x aske, edozein r aldagaitarako $A(r) = A(x)$ izango da, eta r askea izango da x aldagairako $A(x)$ formulan.
2. Edozein $A(x)$ formulatarako, x askea da x aldagairako $A(x)$ formulan.

Zenbatzaileen erregelak

- $\boxed{\forall \text{ zenbatzailea ezabatu}}$

$$\frac{\forall x A(x)}{A(r)}$$

Murriztapenak: r askea da x aldagairako $A(x)$ formulan edo r konstante bat da.

2.28 Adibideak.

1. $$\frac{\forall x(P(x,x) \wedge Q(y))}{P(z,z) \wedge Q(y)}$$
   $A(x) = P(x,x) \wedge Q(y)$; $A(z) = P(z,z) \wedge Q(y)$, z askea da x-rako $A(x)$ formulan.
2. $$\frac{\forall x(P(x,x) \wedge Q(y))}{P(x,x) \wedge Q(y)} \qquad \frac{\forall x(P(x,x) \wedge Q(y))}{P(y,y) \wedge Q(y)}$$
   x eta y askeak dira x aldagairako $P(x,x) \wedge Q(y)$ formulan.
3. $$\frac{\forall y(P(y,y) \wedge Q(x) \wedge \forall x R(x))}{P(x,x) \wedge Q(x) \wedge \forall x R(x))}$$
   x askea da y aldagairako $P(y,y) \wedge Q(x) \wedge \forall x R(x)$ formulan.

4.
$$\frac{\forall x(P(x,x) \wedge Q(y) \wedge \exists x R(x))}{P(y,y) \wedge Q(y) \wedge \exists x R(x))}$$

y askea da x aldagairako $P(x,x) \wedge Q(y) \wedge \exists x R(x)$ formulan.

5.

Txakur guztiak ugaztunak dira.	$\forall x(T(x) \to U(x))$
Bizi txakurra da.	$T(b)$
Beraz, Bizi ugaztuna da.	$U(b)$

1.	$\forall x(T(x) \to U(x))$	premisa
2.	$T(b)$	premisa / $\therefore U(b)$
3.	$T(b) \to U(b)$	$\forall x$-ezab(1) (b konstantea da)
4.	$U(b)$	MP(3,2)

6.

1.	$\neg P(x)$	premisa
2.	$\forall y(P(y) \vee Q(y))$	premisa / $\therefore Q(x)$
3.	$P(x) \vee Q(x)$	$\forall y$-ezab(2) (x askea da y-rako $P(y) \vee Q(y)$ formulan)
4.	$Q(x)$	SD(3,1)

7. Hona hemen dedukzio **oker** bat:

1.	$\forall x \exists y P(x,y)$	premisa / $\therefore \exists y P(y,y)$
2.	$\exists y P(y,y)$	$\forall x$-ezab(1)

Erregela **gaizki** aplikatu dugu, y **ez** delako askea x aldagairako $\exists y P(x,y)$ formulan.

Horrez gain, argumentua baliogabea dela froga dezakegu. Har dezagun interpretazio hau:

$$I: \quad D = \{1,2\} \qquad \frac{P}{\alpha}$$

D^2	α
11	F
12	E
21	E
22	F

$V(\forall x \exists y P(x,y), I) = E$ da, eta $V(\exists y P(y,y), I) = F$.

8. Hona hemen erregelaren aplikazio **okerraren** beste adibide bat:

$$\frac{\forall x P(x,x)}{P(x,y)}$$

Ez dira ordezkatu x aldagaiak $P(x,x)$ formulan dituen agerpen aske guztiak y aldagaiarekin.

Horrez gain, argumentua baliogabea dela froga liteke.

- $\boxed{\exists \text{ zenbatzailea sartu}}$

$$\frac{A(r)}{\exists x A(x)}$$

Murriztapenak: r askea da x aldagairako $A(x)$ formulan edo r konstantea da.

2.29 Adibideak.

1.
$$\frac{P(x)}{\exists x P(x)} \qquad \frac{P(y)}{\exists x P(x)}$$

x eta y askeak dira x aldagairako $P(x)$ formulan.

2.
$$\frac{P(x,y) \wedge \forall z R(z)}{\exists z(P(x,z) \wedge \forall z R(z))}$$

y askea da z aldagairako $P(x,z) \wedge \forall z R(z)$ formulan.

3.
$$\frac{P(x) \to Q(x)}{\exists y(P(x) \to Q(y))}$$

x askea da y aldagairako $P(x) \to Q(y)$ formulan.

4.

	1.	$\forall x(P(x) \to Q(x))$	premisa / $\therefore P(y) \to \exists x(P(x) \wedge Q(x))$
$\to$	2.	$P(y)$	BFEren hipotesia / $\therefore \exists x(P(x) \wedge Q(x))$
|	3.	$P(y) \to Q(y)$	$\forall x$-ezab(1) (y askea x-rako, $P(x) \to Q(x)$)
|	4.	$Q(y)$	MP(3,2)
|	5.	$P(y) \wedge Q(y)$	KK(2,4)
|	6.	$\exists x(P(x) \wedge Q(x))$	$\exists x$-sar(5) (y askea x-rako, $P(x) \wedge Q(x)$)
	7.	$P(y) \to \exists x(P(x) \wedge Q(x))$	BFE(2-6)

5. Erregelaren aplikazio **oker** bat:

$$\frac{P(x) \leftrightarrow \neg P(y)}{\exists x(P(x) \leftrightarrow \neg P(x))}$$

Erregela **gaizki** aplikatu dugu ez ditugulako ordezkatu y aldagaiarekin x aldagaiak $P(x) \leftrightarrow \neg P(x)$ formulan dituen agerpen aske guztiak.

Eta argumentua baliogabea dela froga liteke.

6. Erregelaren beste aplikazio **oker** bat:

$$\frac{\forall x P(x,x)}{\exists y \forall x P(y,x)}$$

Erregela **gaizki** aplikatu dugu x **ez** delako askea y aldagairako $\forall x P(y,x)$ formulan.

Eta argumentua baliogabea dela froga liteke.

- $\boxed{\forall \text{ zenbatzailea sartu}}$

$$\begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline A \end{array} \text{ argumentua baliozkoa bada, } \begin{array}{c} P_1 \\ \vdots \\ P_n \\ \hline \forall x A \end{array} \text{ argumentua ere baliozkoa izango da.}$$

Murriztapenak: $P_1, \ldots, P_n$ premisek ez dute x aske.

Erabilbidea: Argumentu baten froga formal batean, premisek eta indarrean dauden hipotesiek ez badute x aske, eta frogaren formuletako bat A bada, $\forall$ zenbatzailea sartzeko erregelatik $\forall x A$ deduzi dezakegu.

1.	P_1	premisa
$\vdots$	$\vdots$	$\vdots$
$n.$	P_n	premisa / $\therefore C$
$\vdots$	$\vdots$	
$m.$	A	
$m+1.$	$\forall x A$	$\forall x$-sar(m)

($P_1, \ldots, P_n$ premisek eta indarrean dauden hipotesiek ez dute x aske)

2.30 Adibideak.

1.

1.	$\forall y P(y,y) \wedge \forall z R(z)$	premisa / $\therefore \forall y(P(y,y) \wedge R(y))$
2.	$\forall y P(y,y)$	KS(1)
3.	$P(y,y)$	$\forall y$-ezab(2) (y askea da y aldagairako $P(y,y)$ formulan)
4.	$\forall z R(z) \wedge \forall y P(y,y)$	TRUK(1)
5.	$\forall z R(z)$	KS(4)
6.	$R(y)$	$\forall z$-ezab(5) (y askea da z aldagairako $R(z)$ formulan)
7.	$P(y,y) \wedge R(y)$	KK(3,6)
8.	$\forall y(P(y,y) \wedge R(y))$	$\forall y$-sar(7) (1. premisak ez du y aske)

2.

	1.	$\forall x(P(x) \to Q(x))$	premisa
	2.	$\forall x(R(x) \to \neg Q(x))$	premisa / $\therefore \forall x(R(x) \to \neg P(x))$
$\to$	3.	$R(x)$	BFEren hipotesia / $\therefore \neg P(x)$
|	4.	$R(x) \to \neg Q(x)$	$\forall x$-ezab(2) (x askea x-rako, $R(x) \to \neg Q(x)$)
|	5.	$\neg Q(x)$	MP(4,3)
|	6.	$P(x) \to Q(x)$	$\forall x$-ezab(1) (x askea x-rako $P(x) \to Q(x)$ formulan)
|	7.	$\neg P(x)$	MT(6,5)
	8.	$R(x) \to \neg P(x)$	BFE(3-7)
	9.	$\forall x(R(x) \to \neg P(x))$	$\forall x$-sar(8)
			(1. eta 2. premisek ez dute x aske;
			3. hipotesia ez dago indarrean)

3. Aplikazio **okerraren** adibidea:

	1.	$\forall x(P(x) \to Q(x))$	premisa / $\therefore P(x) \to \forall x Q(x)$
$\to$	2.	$P(x)$	BFEren hipotesia / $\therefore \forall x Q(x)$
	3.	$P(x) \to Q(x)$	$\forall x$-ezab(1) (x askea x-rako $P(x) \to Q(x)$ formulan)
	4.	$Q(x)$	MP(3,2)
	5.	$\forall x Q(x)$	$\forall x$-sar(4)
			(**gaizki**: 2. hipotesiak x aske du)
	6.	$P(x) \to \forall x Q(x)$	BFE(2-5)

- $\boxed{\exists \text{ zenbatzailea ezabatu}}$

(1) $\dfrac{\begin{array}{c} P_1 \\ \vdots \\ P_n \\ A \end{array}}{C}$ argumentua baliozkoa bada, (2) $\dfrac{\begin{array}{c} P_1 \\ \vdots \\ P_n \\ \exists x A \end{array}}{C}$ argumentua ere baliozkoa da.

Murriztapenak: $P_1, \ldots, P_n$ premisek eta C ondorioak ez dute x aske.

Erabilbidea: (2) argumentuaren froga formalean, premisek eta indarrean dauden hipotesiek ez badute x aske, eta frogaren formuletako bat $\exists x A$ bada, A suposatuko dugu erregela aplikatzeko ((1) argumentua). Hipotesi horrekin C formula deduzituz gero, (1) argumentua frogatua dugu. Orduan, C formulak ere ez badu x aske, erregela aplikatuz, (2) argumentua ere baliozkoa dela esan ahal izango dugu.

	1.	P_1	premisa
	$\vdots$	$\vdots$	$\vdots$
	$n.$	P_n	premisa
	$\vdots$	$\vdots$	
	$p.$	$\exists x A$	
	$\vdots$	$\vdots$	
$\to$	$q.$	A	$\exists x$-ezabatzeko hipotesia(p)
	$\vdots$	$\vdots$	
	$m.$	C	
	$m+1.$	C	$\exists x$-ezab(p,q-m)

($P_1, \ldots, P_n$ premisek, hipotesiek eta C ondorioak ez dute x aske)

2.31 Adibideak.

1.

	1.	$\forall x(P(x) \to Q(x))$	premisa
	2.	$\exists y P(y)$	premisa / $\therefore \exists z Q(z)$
$\to$	3.	$P(y)$	$\exists y$-ezabatzeko hipotesia(2)
	4.	$P(y) \to Q(y)$	$\forall x$-ezab(1) (y askea x-rako $P(x) \to Q(x)$ formulan)
	5.	$Q(y)$	MP(4,3)
	6.	$\exists z Q(z)$	$\exists z$-sar(5) (y askea da z aldagairako $Q(z)$ formulan)
	7.	$\exists z Q(z)$	$\exists y$-ezab(2,3-6) (1. eta 2. premisek eta 6. ondorioak ez dute y aske)

2.

	1.	$\exists x(P(x) \wedge Q(x))$	premisa / $\therefore \exists x P(x) \wedge \exists x Q(x)$
$\rightarrow$	2.	$P(x) \wedge Q(x)$	$\exists x$-ezabatzeko hipotesia(1)
|	3.	$P(x)$	KS(2)
|	4.	$\exists x P(x)$	$\exists x$-sar(3) (x askea da x aldagairako $P(x)$ formulan)
|	5.	$Q(x) \wedge P(x)$	TRUK(2)
|	6.	$Q(x)$	KS(5)
|	7.	$\exists x Q(x)$	$\exists x$-sar(6) (x askea da x aldagairako $Q(x)$ formulan)
|	8.	$\exists x P(x) \wedge \exists x Q(x)$	KK(4,7)
	9.	$\exists x P(x) \wedge \exists x Q(x)$	$\exists x$-ezab(1,2-8) (1. premisak eta 8. ondorioak ez dute x aske)

3. Erregelaren aplikazio **okerraren** adibidea:

	1.	$\forall x \exists y P(x,y)$	premisa / $\therefore \forall y \exists x P(x,y)$
	2.	$\exists y P(x,y)$	$\forall x$-ezab(1) (x askea da x aldagairako $\exists y P(x,y)$ formulan)
$\rightarrow$	3.	$P(x,y)$	$\exists y$-ezabatzeko hipotesia(2)
|	4.	$\exists x P(x,y)$	$\exists x$-sar(3) (x askea da x aldagairako $P(x,y)$ formulan)
	5.	$\exists x P(x,y)$	$\exists y$-ezab(2,3-4) (**gaizki**: 4 ondorioak y aske du)
	6.	$\forall y \exists x P(x,y)$	$\forall y$-sar(5) (1. premisak eta 2. formulak ez dute y aske)

4. Argumentu beraren beste froga **oker** bat:

	1.	$\forall x \exists y P(x,y)$	premisa / $\therefore \forall y \exists x P(x,y)$
	2.	$\exists y P(x,y)$	$\forall x$-ezab(1) (x askea da x aldagairako $\exists y P(x,y)$ formulan)
$\rightarrow$	3.	$P(x,y)$	$\exists y$-ezabatzeko hipotesia(2)
|	4.	$\exists x P(x,y)$	$\exists x$-sar(3) (x askea da x aldagairako $P(x,y)$ formulan)
|	5.	$\forall y \exists x P(x,y)$	$\forall y$-sar(4) (**gaizki**: 3 hipotesiak y aske du)
	6.	$\forall y \exists x P(x,y)$	$\exists y$-ezab(2,3-5) (1. premisak eta 5. formulak ez dute y aske)

5. Erregelaren beste aplikazio **oker** bat:

		1.	$\exists x(P(x) \wedge R(x))$	premisa
		2.	$\exists x(Q(x) \wedge R(x))$	premisa / $\therefore \exists x(P(x) \wedge Q(x))$
$\rightarrow$		3.	$Q(x) \wedge R(x)$	$\exists x$-ezabatzeko hipotesia(2)
|		4.	$Q(x)$	KS(3)
|	$\rightarrow$	5.	$P(x) \wedge R(x)$	$\exists x$-ezabatzeko hipotesia(1)
|	|	6.	$P(x)$	KS(5)
|	|	7.	$P(x) \wedge Q(x)$	KK(6,4)
|	|	8.	$\exists x(P(x) \wedge Q(x))$	$\exists x$-sar(7) (x askea x-rako $P(x) \wedge Q(x)$ formulan)
|		9.	$\exists x(P(x) \wedge Q(x))$	$\exists x$-ezab(1,5-8) (**gaizki**: 3 hipotesiak x aske du)
		10.	$\exists x(P(x) \wedge Q(x))$	$\exists x$-ezab(2,3-9) (1. eta 2. premisek eta 9. formulak ez dute x aske)

3. Kapitulua

Multzoak. Erlazioak. Funtzioak

3.1 Sarrera

Lehendabizi, *multzo-teoria*ren oinarrizko kontzeptuak aztertzen hasiko gara; ondoren, multzo baten elementuen arteko *erlazioak* ikusiko ditugu; eta bukatzeko, bi multzoren arteko *funtzioak* landuko ditugu.

Logikaren kontzeptuek lotura handia dute multzo-teoriarekin. Atal honetan ikasiko ditugun froga asko kontzeptu horietan oinarriturik daude.

$\wedge$, $\vee$ eta $\neg$ zeinuez gain, idazkera hau ere erabiliko dugu:

$\Longrightarrow$: "halabeharrez", "orduan". $p \Longrightarrow q$ adierazpenak esanahi hau du: "q p-ren ondorio logikoa da", hau da, p egiazkoa bada, q-k ere egiazkoa izan behar du; eta honela irakurriko dugu: "baldin p halabeharrez q", "baldin p orduan q", "p baldintza nahikoa da q-rako", "q baldintza beharrezkoa da p-rako".

$\Longleftrightarrow$: "baldin eta soilik baldin". $p \Longleftrightarrow q$ adierazpenak "$(p \Longrightarrow q)$ eta $(q \Longrightarrow p)$" esan nahi du; eta honela irakurriko dugu: "p baldin eta soilik baldin q", "p baldintza nahikoa eta beharrezkoa da q-rako".

$\forall$: "bakoitzeko", "guztietarako", "edozein". Zenbatzaile unibertsala da. $\forall x$ honela irakurriko dugu: "x bakoitzeko", "x guztietarako", "edozein x".

$\exists$: "existitzen da", "badago". Zenbatzaile existentziala da. $\exists x$ honela irakurriko dugu: "badago (gutxienez) x (bat)", "(gutxienez) x bat existitzen da".

$\exists!$: "bakar bat existitzen da", "existitzen da eta bakarra da".

$\nexists$: "ez dago", "ez da existitzen".

3.2 Multzoak

3.2.1 Multzoak eta azpimultzoak

3.1 Definizioa. Multzo *bat ongi definitutako objektuen bilduma bat da. Objektu horiek* elementu *deitzen dira, multzoaren elementuak.*

Ongi definitutako bilduma esaten dugunean, esan nahi dugu, edozein objektu emanik, erabaki ahal izango dugula objektu hori multzoaren elementua den, edo ez.

Multzo bat bi eratan defini dezakegu:

- Hedapenaren arabera: bere elementu guztiak banan-banan aipatuz,

$$A = \{0, 1, 2, \ldots, 20\}.$$

- Ulermenaren arabera: Bere elementuen ezaugarriak erakusten dituzten propietateak aipatuz,

$$A = \{x \ / \ x \text{ zenbaki osoa da eta } 0 \leq x \leq 20\}.$$

Idazkera. Oro har, multzoak letra larriz izendatuko ditugu (A, B, C, X, ...), eta elementuak letra xehez ($a, b, c, x, \ldots$).

x objektua A multzoaren elementua dela esateko $x \in A$ idatziko dugu (x barne A, x A multzoan dago, x A multzoaren elementua da). x objektua A multzoaren elementua ez dela esateko, $x \notin A$ idatziko dugu.

3.2 Adibidea. $A = \{0, 1, 2, \ldots, 20\}$ bada, $11 \in A$, $21 \notin A$ idatz ditzakegu.

Maiz erabiltzen diren multzo batzuk sinbolo bereziez adierazten dira:

Zenbaki arrunten multzoa: $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Zenbaki osoen multzoa: $\mathbb{Z} = \{\ \ldots, -2, -1, 0, 1, 2, \ldots\}$.

Zenbaki arrazionalen multzoa: $\mathbb{Q} = \left\{x \ / \ x = \dfrac{a}{b}, \text{ non } a, b \in \mathbb{Z} \text{ eta } b \neq 0\right\}$.

Zenbaki errealen multzoa: $\mathbb{R}$.

Zenbaki konplexuen multzoa: $\mathbb{C}$.

0-ren desberdinak diren zenbaki arrunten multzoa (edo zenbaki oso positiboen multzoa): $\mathbb{N}^* = \mathbb{Z}^+ = \{x \ / \ x \in \mathbb{N} \text{ eta } x \neq 0\} = \{x \ / \ x \in \mathbb{Z} \text{ eta } x > 0\}$.

Antzeko eran, $\mathbb{Z}^*$, $\mathbb{Z}^-$, $\mathbb{Q}^*$, $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{R}^*$, $\mathbb{R}^+$, $\mathbb{R}^-$, $\mathbb{C}^*$.

3.3 Definizioa. *Elementu kopuru finitua duen A multzo bat izanik, A multzoaren elementu kopuruari A multzoaren* kardinal *deituko diogu eta honela adieraziko dugu:* $|A|$, $\mathrm{card}(A)$ *edo* $\#A$.

3.4 Adibidea. $A = \{0, 1, 2, \ldots, 20\}$ bada, $\mathrm{card}(A) = 21$ izango da.

3.5 Definizioa. *A multzoa B multzoaren* azpimultzoa *dela esango dugu, eta $A \subseteq B$ idatzi, A multzoaren elementu guztiak B multzoaren elementuak badira. Hau da,*

$$x \in A \implies x \in B$$

betetzen bada.

Adierazpen hauek ere erabiliko ditugu: A B multzoaren partea *da; A multzoa B* multzoan dago*; B multzoak A multzoa* barruan dauka.

A ez bada B multzoaren azpimultzoa, $A \not\subseteq B$ idatziko dugu. Kasu horretan gutxienez A multzoaren elementu bat ez dago B multzoan:

$$\exists x \in A, \text{ non } x \notin B \text{ den.}$$

Ohar gaitezen, A edozein multzo izanik, ondoko hau betetzen dela:

$$A \subseteq A.$$

3.6 Adibidea. $A = \{0, 1, 2\}$ eta $B = \{-2, -1, 0, 1, 2\}$ badira, $A \subseteq B$ eta $B \not\subseteq A$ betetzen dira.

3.7 Definizioa. *A eta B multzoak* berdinak *direla esango dugu, eta $A = B$ idatziko dugu, elementu berak badauzkate. Hau da,*

$$x \in A \iff x \in B$$

betetzen bada; edo gauza bera dena, $A \subseteq B$ eta $B \subseteq A$ betetzen badira.

3.8 Definizioa. *A multzoa B multzoaren* azpimultzo propioa *da, eta $A \subset B$ idatziko dugu, $A \subseteq B$ bada, baina $A \neq B$; hau da,*

$$x \in A \implies x \in B,$$

eta

$$\exists x \in B, \text{ non } x \notin A \text{ den}$$

betetzen badira.

Honela ere esan dezakegu: A multzoa B multzoaren parte propioa *da, edo A multzoa* zeharo *dago B multzoan, edo B multzoak A multzoa* zeharo *barruan dauka.*

3.9 Adibidea.

$$A = \{0, 1, 2\},\ B = \{-2, -1, 0, 1, 2\} \text{ eta } C = \{x \ / \ x \in \mathbb{Z} \text{ eta } 0 \leq x \leq 2\}$$

baditugu, $A = C \subset B$ betetzen da.

Multzoaren kontzeptua zabalduz, definizio hauek eman ditzakegu:

3.10 Definizioa. *Elementurik ez duen multzoari* multzo huts *deituko diogu. $\emptyset$ adierazten da.*

Ohar gaitezen $\emptyset \neq \{\emptyset\}$ dela; izan ere, $\emptyset$ elementurik ez duen multzoa den bitartean, $\{\emptyset\}$ elementu bakarra duen multzo bat da, elementu hori $\emptyset$ izanik. Bestalde, $\emptyset \neq 0$ dela ere esan behar dugu; $\emptyset$ elementurik ez duen multzoa delako eta 0 zenbaki bat delako. Azkenik, $\emptyset \neq \{0\}$, $\emptyset$ elementurik ez duen multzoa delako eta $\{0\}$ elementu bakarra, 0, duen multzo bat delako.

Horrez gain, A edozein multzo izanik,

$$\emptyset \subseteq A.$$

Izan ere,

$$x \in \emptyset \implies x \in A$$

betetzen da, $x \in \emptyset$ beti faltsua delako. (Ba al dago $\emptyset$ multzoan elementuren bat A multzoan ez dagoena?)

3.11 Definizioa. *Elementu guztiak dituen multzoari* multzo unibertsal *edo* erreferentzia multzo *deituko diogu. U izendatuko dugu.*

Esate baterako, zenbaki errealen propietateak aztertzen ari bagara, $\mathbb{R}$ hartuko dugu multzo unibertsaltzat.

A edozein multzo izanik,

$$A \subseteq U$$

betetzen da. Izan ere,

$$x \in A \implies x \in U$$

beti betetzen da, $x \in U$ beti delako egiazkoa.

3.12 Definizioa. *A multzo bat izanik, A multzoaren* parteen multzo *edo A multzoaren* potentzia multzo *deituko diogu elementutzat A multzoaren azpimultzo guztiak dituenari. $\mathcal{P}(A)$ adieraziko dugu.*

3.13 Adibidea. $A = \{0, 1, 2\}$ bada,

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, A\}$$

izango da.

A finitua bada eta $\operatorname{card}(A) = n$ bada,

$$\operatorname{card}(\mathcal{P}(A)) = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

beteko da.

3.2.2 Multzoen arteko eragiketak

Izan bitez A eta B bi multzo.

3.14 Definizioa.

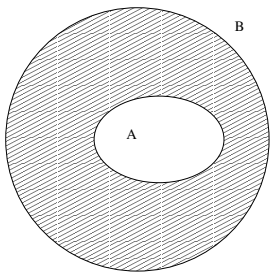
- *$A \subseteq B$ bada,*

  $$C_B(A) := \{x \ / \ x \in B \text{ eta } x \notin A\}$$

  multzoari A multzoaren multzo osagarri B multzoan *deituko diogu, eta $C_B(A)$ idatziko dugu.*

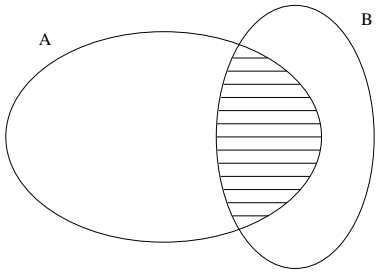
  $B = U$ (unibertsala) bada, $C_U(A)$ multzoari A multzoaren multzo osagarri *bakarrik deituko diogu eta A^c adieraziko dugu.*

$$A^c := \{x \ / \ x \notin A\}$$



- *Ondoko multzo honi A eta B multzoen arteko* ebakidura multzo *deituko diogu eta $A \cap B$ adieraziko dugu:*

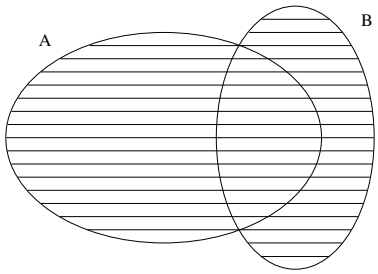
$$A \cap B := \{x \ / \ x \in A \ \textit{eta} \ x \in B\}$$



$A \cap B = \emptyset$ bada, A eta B multzo disjuntuak *direla esango dugu.*

- *Ondoko multzo honi A eta B multzoen arteko* bildura multzo *deituko diogu eta $A \cup B$ adieraziko dugu:*

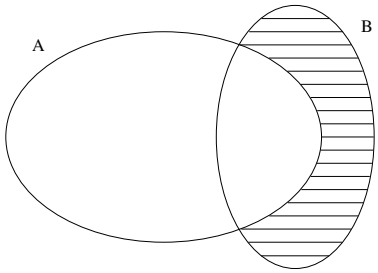
$$A \cup B := \{x \ / \ x \in A \ \textit{edo} \ x \in B\}$$



A eta B multzo disjuntuak badira, A eta B multzoen arteko bildura $\cup$ sinboloaren gainean puntu bat duela adierazi ohi da, honela: $A \dot{\cup} B$.

- *Ondoko multzo honi A eta B multzoen arteko* kendura multzo *deituko diogu eta $B \setminus A$ adieraziko dugu:*

$$B \setminus A := \{x \ / \ x \in B \ \textit{eta} \ x \notin A\}$$



$A \subseteq B$ bada, $B \setminus A = C_B(A)$ berdintza beteko da.

3.15 Adibideak.

Izan bitez $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $B = \{0, 2, 4, 6, 8, 10\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{0, 1, 2, 3, 4, 5\}$ eta $U = \mathbb{N}$ multzoak. Hau dena betetzen da:

$C_A(B) = A \setminus B = C$;	$A^c = \{x \ / \ x \in \mathbb{N}$ eta $x \geq 11\}$;
$B \cap D = \{0, 2, 4\}$;	B eta C disjuntuak dira;
$B \cup D = \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$;	$B \cup C = B \dot{\cup} C = A$;
$C \setminus D = \{7, 9\}$.	

3.16 Propietateak.

Trukatze-legea:

$A \cup B = B \cup A$	$A \cap B = B \cap A$

Elkartze-legea:

$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$

Banatze-legea:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan-en legeak:

$(A \cup B)^C = A^C \cap B^C$	$(A \cap B)^C = A^C \cup B^C$

Idenpotentzia:

$A \cup A = A$	$A \cap A = A$

Beste hainbat propietate:

$A \cup U = U$	$A \cap U = A$
$A \cup A^C = U$	$A \cap A^C = \emptyset$
$A \cup \emptyset = A$	$A \cap \emptyset = \emptyset$
$A \subseteq A \cup B$	$A \cap B \subseteq A$
$U^C = \emptyset$	$\emptyset^C = U$
$(A^C)^C = A$	

Froga.

Propietate horiek lokailu logikoen propietateak erabiliz frogatzen dira.
Adibide gisa, horietako bi frogatuko ditugu.

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

  Multzoen arteko berdintza frogatu behar dugu; hortaz, ondoko hau frogatu beharko dugu (3.7 Definizioa):

  1. $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$,
  2. $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

  1. $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ frogatzeko, beste hau frogatu behar dugu:

     $$x \in A \cup (B \cap C) \implies x \in (A \cup B) \cap (A \cup C).$$

     $x \in A \cup (B \cap C) \implies (x \in A) \vee (x \in B \cap C)$ ($\cup$ bilketaren definizioa) $\implies$
     $\implies (x \in A) \vee (x \in B \wedge x \in C)$ ($\cap$ ebaketaren definizioa) $\implies$
     $\implies (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ ($\vee$ disjuntzioaren banakortasuna $\wedge$ konjuntzioarekiko) $\implies (x \in A \cup B) \wedge (x \in A \cup C)$ ($\cup$ bilketaren definizioa); eta hortik, $x \in (A \cup B) \cap (A \cup C)$ ($\cap$ ebaketaren definizioa).
  2. $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ antzeko eran frogatzen da:
     $x \in (A \cup B) \cap (A \cup C) \implies (x \in A \cup B) \wedge (x \in A \cup C)$ ($\cap$ ebaketaren definizioa); beraz, $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ ($\cup$ bilketaren definizioa) $\implies$
     $\implies (x \in A) \vee (x \in B \wedge x \in C)$ ($\vee$ disjuntzioaren banakortasuna $\wedge$ konjuntzioarekiko) $\implies (x \in A) \vee (x \in B \cap C)$ ($\cap$ ebaketaren definizioa) $\implies$
     $\implies x \in A \cup (B \cap C)$ ($\cup$ bilketaren definizioa).

- $A \subseteq A \cup B$:

  $x \in A \implies (x \in A) \vee (x \in B)$ (erantsiz) $\implies x \in A \cup B$ ($\cup$ bilketaren definizioa). $\square$

Bilketaren eta ebaketaren elkarkortasunak aukera ematen digu $A \cup B \cup C$ eta $A \cap B \cap C$ idazteko, parentesirik erabili gabe. Horrek, trukakortasunarekin batera, aukera ematen digu zenbait multzoren arteko bilketaz eta ebaketaz hitz egiteko, multzoak ordenan eman beharrik gabe.

I indizeen multzo ez-huts bat bada eta $i \in I$ bakoitzeko A_i multzo bat bada,

$$\bigcup_{i \in I} A_i := \{x \ / \ \exists i \in I, \text{ non } x \in A_i\},$$

$$\bigcap_{i \in I} A_i := \{x \ / \ \forall i \in I \quad x \in A_i\}.$$

3.17 Adibideak.

1. Izan bedi $A_i = \{1, \ldots, i\} \quad i \in \mathbb{N}^*$ bakoitzeko. Orduan,

$$\bigcup_{i \in \mathbb{N}^*} A_i = \mathbb{N}^* \quad \text{eta} \quad \bigcap_{i \in \mathbb{N}^*} A_i = \{1\}.$$

2. $i \in \mathbb{Z}$ bakoitzeko, izan bedi $A_i = \{i, i+1\}$. Orduan,

$$\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{Z} \quad \text{eta} \quad \bigcap_{i \in \mathbb{Z}} A_i = \emptyset.$$

Froga genitzake *De Morganen lege orokortuak*:

$$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c,$$

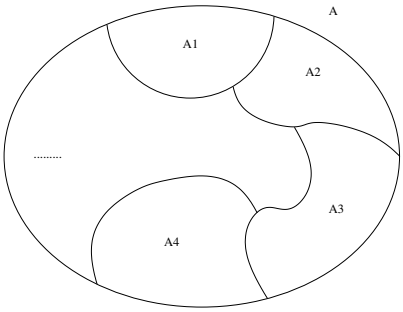
$$\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c.$$

3.2.3 Multzo baten partiketa

3.18 Definizioa. *A multzo bat izanik, A multzoaren* partiketa *bat A multzoaren azpimultzo ez-hutsen familia bat da, non multzoak binaka hartuta disjuntuak diren eta guztien bildura A den. Hau da,*

$\mathcal{P} = \{A_i \ / \ i \in I\}$ *familia A multzoaren partiketa bat da hiru baldintza hauek betetzen badira:*

- $(\forall i \in I) \quad \emptyset \neq A_i \subseteq A,$
- $(\forall i, j \in I) \quad A_i \neq A_j \implies A_i \cap A_j = \emptyset,$
- $\dot{\bigcup}_{i \in I} A_i = A.$



A_i *azpimultzoei partiketaren* klase *deituko diegu.*

3.19 Adibideak.

1. $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ izanik,

   $A_1 = \{1, 3, 5, 7, 9\}$ eta $A_2 = \{2, 4, 6, 8, 10\}$ multzoek A multzoaren bi klaseko partiketa bat osatzen dute: $\mathcal{P} = \{A_1, A_2\}$;

   $B_1 = \{1, 2, 3\}$, $B_2 = \{4, 6, 8, 10\}$ eta $B_3 = \{5, 7, 9\}$ multzoek A multzoaren hiru klaseko partiketa bat osatzen dute: $\mathcal{P}' = \{B_1, B_2, B_3\}$.

2. $\mathcal{P} = \{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$ familia $\mathbb{Z}$ multzoaren partiketa bat da.

Definizioaren ondorioa. A multzoaren partiketa bat $\mathcal{P} = \{A_i \ / \ i \in I\}$ bada, A multzoaren elementu bakoitza $\mathcal{P}$ partiketaren klase bakar baten elementua izango da:

$$\forall x \in A \quad \exists! A_i \in \mathcal{P}, \text{ non } x \in A_i.$$

3.2.4 Bi multzoren arteko biderketa kartesiarra

3.20 Definizioa. *Izan bedi a eta b bi objektuen bilduma bat, non a lehenengo osagaia den eta b bigarren osagaia den, (a, b) bildumari* bikote ordenatu *deituko diogu.*

Antzeko eran definitzen dira (a, b, c) hirukotea*, (a, b, c, d)* laukotea*... eta, orokorrean, $(a_1, \ldots, a_n)$ n-*kotea*.*

Beraz, $(a, b) \neq (b, a)$ eta $\{a, b\} = \{b, a\}$ betetzen dira.

Bestalde, (a, b) eta (c, d) bikoteak berdinak dira $a = c$ eta $b = d$ badira.

3.21 Definizioa. *A eta B bi multzo izanik, A eta B multzoen arteko* biderkadura kartesiar *deituko diogu, eta $A \times B$ adieraziko dugu, lehenengo osagaitzat A multzoaren elementua eta bigarren osagaitzat B multzoaren elementua dituzten bikote ordenatu guztien multzoari:*

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

Antzeko eran definitzen da $A_1, \ldots, A_n$ n multzoen arteko biderkadura kartesiarra*:*

$$A_1 \times \cdots \times A_n := \{(x_1, \ldots, x_n) \ / \ x_i \in A_i, \ i = 1, \ldots, n\}.$$

Idazkera. $A^n = A \times \overset{n}{\cdots} \times A$.

3.22 Adibideak.

Izan bitez $A = \{a, b\}, B = \{1, 2, 3\}, C = \{a\}$. Orduan,
$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$;
$B \times A = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$;
$A \times B \times C = \{(a, 1, a), (a, 2, a), (a, 3, a), (b, 1, a), (b, 2, a), (b, 3, a)\}$;
$B^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$;
$A^3 = \{(a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b)\}$;
$C^7 = \{(a, a, a, a, a, a, a)\}$.

3.3 Erlazioak

3.3.1 Definizioak

3.23 Definizioa. *A multzoa izanik, A multzoaren gaineko* erlazio bitar *bat $A \times A$ biderkadura kartesiarraren $\mathcal{R}$ azpimultzo bat da:*

$$\mathcal{R} \subseteq A \times A.$$

$(a, b) \in \mathcal{R}$ bada, *a b*-rekin ($\mathcal{R}$ erlazioaren bidez) *erlazionaturik* dagoela esango dugu, eta $a\mathcal{R}b$ idatziko dugu.

$(a, b) \notin \mathcal{R}$ bada, *a ez dagoela b*-rekin ($\mathcal{R}$ erlazioaren bidez) *erlazionaturik* esango dugu, eta $a \not\mathcal{R} b$ idatziko dugu.

3.24 Adibideak.

1. $A = \{1, 2, 3, 4\}$.

$$\mathcal{R}_1 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}.$$

2. $A = \mathbb{Z}$.

$$\mathcal{R}_2 = \{(x, y) \ / \ x, y \in \mathbb{Z} \text{ eta } x \leq y\}.$$

   Edo, $x, y \in \mathbb{Z}$ izanik, $x\mathcal{R}_2 y \iff x \leq y$.

3. $A = \mathbb{N}^*$.

$$\mathcal{R}_3 = \{(x, y) \ / \ x, y \in \mathbb{N}^* \text{ eta } x \ y\text{-ren zatitzailea da}\}.$$

   Edo, $x, y \in \mathbb{N}^*$ izanik, $x\mathcal{R}_3 y \iff x$ y-ren zatitzailea da. (Hori $x \mid y$ idatzi ohi da.)

4. $A = \mathbb{N}^*$.

$$\mathcal{R}_4 = \{(1,1), (2,2)\}.$$

5. $A = \mathbb{Z}$. $x, y \in \mathbb{Z}$ izanik,

$$x\mathcal{R}_5 y \iff |x| = |y|.$$

   Edo, baliokidea dena,

$$\mathcal{R}_5 = \{(x, y) \ / \ x, y \in \mathbb{Z} \text{ eta } |x| = |y|\}.$$

   ($x \in \mathbb{Z}$ bada, $|x|$ x-ren balio absolutua da).

3.25 Definizioa. *A multzoaren gaineko $\mathcal{R}$ erlazio bitarra izanik:*

- $\mathcal{R}$ bihurkorra *dela edo* bihurtze-propietatea *betetzen duela esango dugu*

$$(\forall x \in A) \quad (x, x) \in \mathcal{R} \textit{ bada,}$$

  edo, baliokidea dena,

$$(\forall x \in A) \quad x\mathcal{R}x \textit{ bada.}$$

- $\mathcal{R}$ simetrikoa *dela edo* simetria propietatea *betetzen duela esango dugu*

$$(\forall x, y \in A) \quad (x, y) \in \mathcal{R} \implies (y, x) \in \mathcal{R} \text{ bada,}$$

edo, baliokidea dena,

$$(\forall x, y \in A) \quad x\mathcal{R}y \implies y\mathcal{R}x \text{ bada.}$$

- $\mathcal{R}$ antisimetrikoa *dela edo* antisimetria propietatea *betetzen duela esango dugu*

$$(\forall x, y \in A) \quad (x, y) \in \mathcal{R} \text{ eta } (y, x) \in \mathcal{R} \implies x = y \text{ bada,}$$

edo, baliokidea dena,

$$(\forall x, y \in A) \quad x\mathcal{R}y \text{ eta } y\mathcal{R}x \implies x = y \text{ bada.}$$

- $\mathcal{R}$ iragankorra *dela edo* iragate-propietatea *betetzen duela esango dugu*

$$(\forall x, y, z \in A) \quad (x, y) \in \mathcal{R} \text{ eta } (y, z) \in \mathcal{R} \implies (x, z) \in \mathcal{R} \text{ bada,}$$

edo, baliokidea dena,

$$(\forall x, y, z \in A) \quad x\mathcal{R}y \text{ eta } y\mathcal{R}z \implies x\mathcal{R}z \text{ bada.}$$

3.26 Adibideak.

1. $A = \{1, 2, 3, 4\}$ multzoan,

$$\mathcal{R}_1 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$$

erlazioa bihurkorra, simetrikoa eta iragankorra da. Ez da antisimetrikoa.

2. $\mathcal{R}_2 = \{(x, y) \ / \ x, y \in \mathbb{Z} \text{ eta } x \leq y\}$, hau da, $\mathbb{Z}$ multzoan $x\mathcal{R}_2y$ baldin $x \leq y$.

   - Bihurkorra da: $x \in \mathbb{Z}$ bakoitzeko, $x \leq x$. Beraz, $x \in \mathbb{Z}$ bakoitzeko, $x\mathcal{R}_2x$.
   - Ez da simetrikoa: $0\mathcal{R}_27$, baina $7 \not\mathcal{R}_2 0$.
   - Antisimetrikoa da: $x, y \in \mathbb{Z}$ guztietarako,

$$x\mathcal{R}_2y \text{ eta } y\mathcal{R}_2x \implies x \leq y \text{ eta } y \leq x \implies x = y.$$

   - Iragankorra da: $x, y, z \in \mathbb{Z}$ guztietarako,

$$x\mathcal{R}_2y \text{ eta } y\mathcal{R}_2z \implies x \leq y \text{ eta } y \leq z \implies x \leq z \implies x\mathcal{R}_2z.$$

3. $\mathcal{R}_3 = \{(x, y) \ / \ x, y \in \mathbb{N}^* \text{ eta } x \mid y\}$, hau da, zatigarritasunaren definizioaren arabera, $\mathbb{N}^*$ multzoan $x\mathcal{R}_3y$ baldin $\exists k \in \mathbb{Z}$, non $y = kx$ den. (Ikus 4.1 Definizioa. Zatigarritasunaren definizioa.)

   - Bihurkorra da: $x \in \mathbb{N}^*$ guztietarako, $x\mathcal{R}_3x$, hau da, $x \mid x$. Bai, $k = 1 \in \mathbb{Z}$ existitzen delako, non $x = 1 \cdot x$ den.

- Ez da simetrikoa: $2\mathcal{R}_3 8$, baina $8 \not\mathcal{R}_3 2$ (2-k zatitzen du 8, baina 8-k ez du zatitzen 2). Bai, $\exists k = 4 \in \mathbb{Z}$, non $8 = 4 \cdot 2$ den, baina $\nexists k \in \mathbb{Z}$, non $2 = 8k$ den.
- Antisimetrikoa da: $x, y \in \mathbb{N}^*$ izanik, demagun $x\mathcal{R}_3 y$ eta $y\mathcal{R}_3 x$ betetzen direla; frogatu behar dugu $x = y$ dela.

$$\left.\begin{array}{l} x\mathcal{R}_3 y \\ y\mathcal{R}_3 x \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x \mid y \\ y \mid x \end{array}\right\} \Longrightarrow \begin{array}{l} y = kx,\ k \in \mathbb{Z} \\ x = ly,\ l \in \mathbb{Z} \end{array}$$

  eta bigarrenean y ordezkatuz,

$$x = lkx,\ lk \in \mathbb{Z} \Longrightarrow lk = 1.$$

  Bi aukera daude, $l, k \in \mathbb{Z}$ izanik, $l = k = 1$ edo $l = k = -1$. Hortik, $x = y$ edo $x = -y$. Baina $x, y \in \mathbb{N}^* \Longrightarrow x, y > 0 \Longrightarrow x = y$.
- Iragankorra da: $x, y, z \in \mathbb{N}^*$ guztietarako,

$$\left.\begin{array}{l} x\mathcal{R}_3 y \\ y\mathcal{R}_3 z \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x \mid y \\ y \mid z \end{array}\right\} \Longrightarrow \begin{array}{l} y = kx, k \in \mathbb{Z} \\ z = ly, l \in \mathbb{Z} \end{array}$$

  eta bigarrenean y ordezkatuz,

$$z = lkx,\ lk \in \mathbb{Z} \Longrightarrow x\mathcal{R}_3 z.$$

4. $A = \mathbb{N}^*$ multzoan, $\mathcal{R}_4 = \{(1,1),(2,2)\}$ erlazioa simetrikoa, antisimetrikoa eta iragankorra da; eta ez da bihurkorra.
5. $A = \mathbb{Z}$ multzoan, $x\mathcal{R}_5 y \iff |x| = |y|$ erlazioa bihurkorra, simetrikoa eta iragankorra da. Ez da antisimetrikoa.

3.3.2 Ordena-erlazioak

3.27 Definizioa. *A multzoaren gaineko $\mathcal{R}$ erlazio bitar bat* ordena-erlazioa *da bihurkorra, antisimetrikoa eta iragankorra bada.*

A multzo batek $\mathcal{R}$ ordena-erlazio bat badu definiturik, $\mathcal{R}$ erlazioak A multzoa ordenatzen *duela edo A* multzo ordenatua *dela esango dugu.*

3.28 Definizioa. *A multzoaren gaineko $\mathcal{R}$ ordena-erlazio bat* ordena osoko *erlazioa dela* (ordena totala) *esango dugu*

$$(\forall x, y \in A) \quad (x, y) \in \mathcal{R} \ \textit{edo}\ (y, x) \in \mathcal{R} \ \textit{bada,}$$

edo, baliokidea dena,

$$(\forall x, y \in A) \quad x\mathcal{R}y \ \textit{edo}\ y\mathcal{R}x \ \textit{bada.}$$

Kasu horretan, $\mathcal{R}$ erlazioak A multzoa osoki ordenatzen *duela edo A* multzo osoki ordenatua *dela esango dugu.*

Bestela, $\mathcal{R}$ erlazioa ordena partzialeko *erlazioa izango da, eta $\mathcal{R}$ erlazioak A multzoa* partzialki ordenatzen *duela edo A* multzo partzialki ordenatua *dela esango dugu.*

3.29 Adibideak.

1. $\mathcal{R}_2 = \{(x, y) \ / \ x, y \in \mathbb{Z}$ eta $x \leq y\}$ ordena-erlazioa da $\mathbb{Z}$ multzoan; hau da, $\mathcal{R}_2$ erlazioak $\mathbb{Z}$ multzoa ordenatzen du. Erlazioa ordena osoko erlazioa da: $x, y \in \mathbb{Z}$ guztietarako, $x \leq y$ edo $y \leq x$ delako.

2. $\mathcal{R}_3 = \{(x, y) \ / \ x, y \in \mathbb{N}^*$ eta $x \mid y\}$ ordena-erlazioa da $\mathbb{N}^*$ multzoan. $\mathcal{R}_3$ erlazioak $\mathbb{N}^*$ multzoa ordenatzen du. Erlazioa ordena partzialeko erlazioa da: $3 \not\mathcal{R}_3 7$ eta $7 \not\mathcal{R}_3 3$, hots, 3 eta 7 ez daude elkarrekin erlazionaturik.

3.3.3 Baliokidetasun-erlazioak

3.30 Definizioa. *A multzoaren gaineko $\mathcal{R}$ erlazio bitar bat* baliokidetasun-erlazioa *da bihurkorra, simetrikoa eta iragankorra bada.*

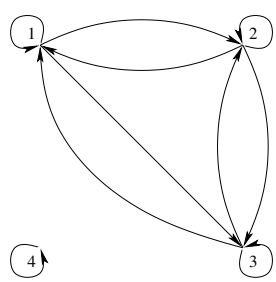
3.31 Adibideak.

1. $A = \{1, 2, 3, 4\}$ multzoaren gainean,

$$\mathcal{R}_1 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$$

   baliokidetasun-erlazioa da.

   Grafo moduan adieraz daiteke, non A erpinen multzoa den eta $\mathcal{R}_1$ ertzen multzoa den. Horrela, bere adierazpen grafikoan erraz ikus daiteke hiru baldintzak betetzen direla:



2. $\mathbb{Z}$ multzoan,

$$x \mathcal{R}_5 y \iff |x| = |y|$$

   baliokidetasun-erlazioa da.

3.32 Definizioa. *Izan bedi $\mathcal{R}$ baliokidetasun-erlazio bat A multzoaren gainean, eta $a \in A$ elementu bat; a-rekin erlazionaturik dauden A multzoaren elementu guztien multzoari a elementuaren* baliokidetasun-klase *deituko diogu, eta $[a]_{\mathcal{R}}$ idatziko dugu:*

$$\begin{aligned} [a]_{\mathcal{R}} &:= \{x \in A \ / \ (x, a) \in \mathcal{R}\} \\ &= \{x \in A \ / \ x \mathcal{R} a\}. \end{aligned}$$

Ez badu nahasmenik sortzen, $[a]$ idatziko dugu $[a]_{\mathcal{R}}$ idatzi beharrean.

3.33 Adibideak.

1. $A = \{1, 2, 3, 4\}$ multzoaren gaineko

$$\mathcal{R}_1 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$$

erlaziorako bi baliokidetasun-klase desberdin dauzkagu:

$$[1] = [2] = [3] = \{1, 2, 3\} \quad \text{eta} \quad [4] = \{4\}.$$

2. $\mathcal{R}_5$ erlazioa izanik $\mathbb{Z}$ multzoan,

$$x\mathcal{R}_5 y \iff |x| = |y|,$$

$x \in \mathbb{Z}$ guztietarako,

$$[x] = \{-x, x\} \text{ dugu.}$$

3.34 Teorema. *A multzoaren gaineko $\mathcal{R}$ baliokidetasun-erlazioa izanik,*

1. $(\forall x \in A) \quad x \in [x]$.

2. $(\forall x, y \in A) \quad x\mathcal{R}y \iff [x] = [y]$.

3. $(\forall x, y \in A) \quad [x] \neq [y] \implies [x] \cap [y] = \emptyset$.

4. $\bigcup_{x \in A} [x] = A$.

Froga.

1. $\mathcal{R}$ bihurkorra denez, $x \in A$ guztietarako $x\mathcal{R}x$ da, eta, beraz, $[x]$ klasearen definizioaren arabera, $x \in [x]$ betetzen da.

2. $x, y \in A$ guztietarako, $x\mathcal{R}y \iff [x] = [y]$ dela frogatu behar dugu:

$\implies$) Demagun $x\mathcal{R}y$ dela. $[x] = [y]$ dela frogatu behar dugu.

$\subseteq$) $z \in [x] \implies z\mathcal{R}x$ ($[x]$-aren definizioz) $\implies \left\{ \begin{array}{l} z\mathcal{R}x \\ x\mathcal{R}y \text{ (hipotesiz)} \end{array} \right\} \implies$

$\implies z\mathcal{R}y$ ($\mathcal{R}$ iragankorra delako) $\implies z \in [y]$ ($[y]$-aren definizioz).

$\supseteq$) $z \in [y] \implies z\mathcal{R}y$ ($[y]$-aren definizioz) $\implies \left\{ \begin{array}{l} z\mathcal{R}y \\ x\mathcal{R}y \text{ (hipotesiz)} \end{array} \right\} \implies$

$\implies \left\{ \begin{array}{l} z\mathcal{R}y \\ y\mathcal{R}x \text{ ($\mathcal{R}$ simetrikoa delako)} \end{array} \right\} \implies z\mathcal{R}x$ ($\mathcal{R}$ iragankorra delako);

hortaz, $z \in [x]$ ($[x]$-aren definizioz).

$\impliedby$) Demagun $[x] = [y]$ dela. $x\mathcal{R}y$ dela frogatu behar dugu.
1.aren arabera $x \in [x]$ denez eta hipotesiz $[x] = [y]$ denez, $x \in [y]$ betetzen da.
$[y]$-aren definiziotik $x\mathcal{R}y$ lortuko dugu.

3. Edozein $x, y \in A$ izanik, demagun $[x] \neq [y]$ dela. $[x] \cap [y] = \emptyset$ beteko dela frogatu behar dugu.

   Absurdora eramanez egingo dugu, $[x] \cap [y] \neq \emptyset$ dela pentsatuz eta kontraesan batera helduz.

   $$[x] \cap [y] \neq \emptyset \implies \exists z \in [x] \cap [y] \implies \left\{ \begin{array}{l} z \in [x] \implies z\mathcal{R}x \implies x\mathcal{R}z \\ z \in [y] \implies z\mathcal{R}y \end{array} \right\} \implies$$

   $$\implies x\mathcal{R}y \implies [x] = [y] \text{ (2.aren arabera).}$$

   Kontraesan batera heldu gara, hipotesiz $[x] \neq [y]$ delako. Beraz, $[x] \cap [y] \neq \emptyset$ ezin da izan; hortaz, $[x] \cap [y] = \emptyset$ beteko da.

4. $\subseteq$) Edozein $x \in A$ izanik, $[x] \subseteq A$; hortaz, $\bigcup_{x \in A} [x] \subseteq A$.

   $\supseteq$) $z \in A \implies z \in [z]$ (1.aren arabera) $\implies z \in \bigcup_{x \in A} [x]$, $\bigcup$-ren definizioz. □

3.35 Korolarioa. *Izan bedi $\mathcal{R}$ baliokidetasun-erlazioa A multzoaren gainean. Erlazio horren baliokidetasun-klase guztien familia,*

$$\mathcal{P} = \{[x] \,/\, x \in A\},$$

A-ren partiketa bat da.

Froga.

3.34 Teoremaren 1, 3 eta 4 propietateak $\mathcal{P}$ familiak partiketa izateko bete behar dituen baldintzak dira (ikus 3.18 Definizioa). □

Partiketaren definizioaren ondorioz, A-ren elementu bakoitza klase bakar baten elementua da:

$$\forall x \in A \quad \exists! [a] \in \mathcal{P} \quad / \quad x \in [a],$$

eta $[a]$ klasearen edozein elementuri klasearen *ordezkari* deituko diogu.

3.36 Definizioa. *Izan bedi $\mathcal{R}$ baliokidetasun-erlazioa A multzoaren gainean. Erlazio horren baliokidetasun-klase guztien multzoari A* gain $\mathcal{R}$ zatidura multzo *deituko diogu, eta $A/\mathcal{R}$ adieraziko dugu:*

$$A/\mathcal{R} := \{[x] \,/\, x \in A\}.$$

3.37 Adibideak.

1. $\mathcal{R}_1$ erlazioa izanik $A = \{1, 2, 3, 4\}$ multzoan,

   $$\mathcal{R}_1 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\},$$

   [1] klaseak hiru elementu dituenez, hiruetako edozein izan daiteke ordezkari: 1, 2 edo 3. [4] klaseak, ordea, ordezkari bakarra du: 4. Beraz,

   $$A/\mathcal{R}_1 = \{[1], [4]\} = \{[2], [4]\} = \{[3], [4]\}.$$

2. $\mathcal{R}_5$ erlazioa izanik $\mathbb{Z}$ multzoan,

   $$x\mathcal{R}_5 y \iff |x| = |y|,$$

   $x \in \mathbb{Z}^*$ guztietarako, $[x]$ klaseak bi ordezkari ditu: x eta $-x$. [0] klaseak, ordea, ordezkari bakarra du: 0. Beraz,

   $$\mathbb{Z}/\mathcal{R}_5 = \{[x] \,/\, x \in \mathbb{Z}\} = \{[0]\} \cup \{[x] \,/\, x \in \mathbb{Z}^+\} = \{[0]\} \cup \{[x] \,/\, x \in \mathbb{Z}^-\}.$$

3.3.4 n moduluko kongruentzia

3.38 Definizioa. *Izan bedi $n \in \mathbb{Z}$, $n > 1$. $a, b \in \mathbb{Z}$ izanik, a b-rekin* kongruentea da modulu *n, eta $a \equiv b \pmod{n}$ idatziko dugu, $n \mid a - b$ bada, hau da, $\exists k \in \mathbb{Z}$, non $a = b + kn$ den.* (Ikus 4.1 Definizioa. Zatigarritasunaren definizioa.)

3.39 Adibideak.

1. $17 \equiv 2 \pmod{5}$ da, $5 \mid 15$ betetzen delako, hau da, $\exists k \in \mathbb{Z}$, non $17 - 2 = 5k$ den.
2. $-23 \equiv -5 \pmod{6}$ da, $6 \mid -18$ betetzen delako, hau da, $\exists k \in \mathbb{Z}$, non $-23 + 5 = 6k$ den.
3. $-7 \equiv 2 \pmod{3}$ da, $3 \mid -9$ betetzen delako, hau da, $\exists k \in \mathbb{Z}$, non $-7 - 2 = 3k$ den.
4. $-7 \not\equiv 2 \pmod{4}$ da, $4 \nmid -9$ betetzen delako, hau da, $\nexists k \in \mathbb{Z}$, non $-7 - 2 = 4k$ den.

3.40 Teorema. *Izan bedi $n \in \mathbb{Z}$, $n > 1$. n moduluko kongruentzia baliokidetasun-erlazioa da $\mathbb{Z}$ multzoan.*

Froga.

n moduluko kongruentzia $\mathbb{Z}$ multzoan bihurkorra, simetrikoa eta iragankorra dela frogatu behar dugu.

1. Bihurkorra. Hau frogatu behar da:

$$(\forall x \in \mathbb{Z}) \quad x \equiv x \pmod{n}.$$

Izan bedi $x \in \mathbb{Z}$. $x - x = 0 = 0 \cdot n$ betetzen da; hortaz, $n \mid x - x$ betetzen da; eta hortik $x \equiv x \pmod{n}$.

2. Simetrikoa. Hau frogatu behar da:

$$(\forall x, y \in \mathbb{Z}) \quad x \equiv y \pmod{n} \implies y \equiv x \pmod{n}.$$

Izan bitez $x, y \in \mathbb{Z}$.

$$x \equiv y \pmod{n} \implies n \mid x - y \implies \exists k \in \mathbb{Z}, \text{ non } x - y = kn \implies$$
$$\implies \exists(-k) \in \mathbb{Z}, \text{ non } y - x = (-k)n \implies n \mid y - x \implies y \equiv x \pmod{n}.$$

3. Iragankorra. Hau frogatu behar da:

$$(\forall x, y, z \in \mathbb{Z}) \quad x \equiv y \pmod{n} \text{ eta } y \equiv z \pmod{n} \implies x \equiv z \pmod{n}.$$

Izan bitez $x, y, z \in \mathbb{Z}$.

$$\left.\begin{array}{l} x \equiv y \pmod{n} \\ y \equiv z \pmod{n} \end{array}\right\} \implies \left.\begin{array}{l} n \mid x - y \\ n \mid y - z \end{array}\right\} \implies \begin{array}{l} \exists k_1 \in \mathbb{Z}, \text{ non } x - y = k_1 n \\ \exists k_2 \in \mathbb{Z}, \text{ non } y - z = k_2 n \end{array}$$

eta $x - y$ balioari $y + z$ balioa gehituz,

$$(x - y) + (y - z) = k_1 n + k_2 n \implies x - z = (k_1 + k_2)n$$

ondorioz,

$$\exists(k_1 + k_2) \in \mathbb{Z}, \text{ non } x - z = (k_1 + k_2)n \implies n \mid x - z \implies x \equiv z \pmod{n}.$$

□

Baliokidetasun-erlazio honetarako zatidura-multzoa bi eratan adierazi ohi da, $\mathbb{Z}/\mathbb{Z}n$ edo $\mathbb{Z}_n$:

$$\mathbb{Z}/\mathbb{Z}n = \mathbb{Z}_n = \{[x] \ / \ x \in \mathbb{Z}\}.$$

n **moduluko kongruentzia erlazioaren baliokidetasun-klaseak lortzeko bidea**:

$x \in \mathbb{Z}$ izanik, n moduluko kongruentziak sortutako $[x]$ baliokidetasun-klasea kalkulatzeko, lehendabizi klasearen ordezkari bat aukeratuko dugu.

Horretarako, Euklidesen teorema erabiliz, x zati n egingo dugu. Izan bedi r zatidura euklidearraren hondarra; hau da, $x = qn + r$ da, $q, r \in \mathbb{Z}$ eta $0 \leq r < n$ izanik. Orduan, $x - r = qn$ dugu, eta, beraz, $n \mid x - r$ betetzen da, edo baliokidea dena, $x \equiv r \pmod{n}$, hau da, n moduluko kongruentziaren arabera $x\mathcal{R}r$. Hortaz, 3.34 Teoremaren 2. propietatearen arabera, $[x] = [r]$. Beraz, r hartuko dugu $[x]$ klasearen ordezkaritzat.

Ondoren, $[r]$ klasean dauden elementuak kalkulatuko ditugu.

$$\begin{aligned}
[r] &= \{y \in \mathbb{Z} \ / \ y\mathcal{R}r\} = \{y \in \mathbb{Z} \ / \ y \equiv r \pmod{n}\} = \\
&= \{y \in \mathbb{Z} \ / \ n \mid y - r\} = \{r + kn \ / \ k \in \mathbb{Z}\} = \\
&= \{\cdots, r - 2n, r - n, r, r + n, r + 2n, \cdots\} = \\
&= \{y \in \mathbb{Z} \ / \ r \text{ da } y \text{ zati } n \text{ zatidura euklidearraren hondarra}\}.
\end{aligned}$$

Horrela, n klase lortuko ditugu (hondar posibleak adina klase), eta klaseen multzoa honela adieraziko dugu (Ikus 3.36 Definizioa):

$$\mathbb{Z}/\mathbb{Z}n = \mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}.$$

3.41 Adibidea. Izan bedi 5 moduluko kongruentzia-erlazioa. Zatidura multzoan 5 klase daude:

$$\mathbb{Z}/\mathbb{Z}5 = \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}.$$

Baliokidetasun-klase horietan dauden elementu batzuk emango ditugu:

$22 \in [2]$ da. Erlazioa 5 moduluko kongruentzia izanik,

$22 = 2 + 5 \cdot 4 \implies 22 - 2 = 5 \cdot 4 \implies \exists k \in \mathbb{Z} \,/\, 22 - 2 = 5k \implies 5 \mid 22 - 2 \implies$
$\implies 22 \equiv 2 \pmod{5} \implies 22\mathcal{R}2 \implies 22 \in [2]$.

Hortaz, 22 zenbakia 5 moduluko kongruentziaren arabera zein klasetan dagoen jakiteko, zatiketa euklidearra egingo dugu, 22 zati 5 egin eta 2 hondarrarekin geratu.

Modu berean, $-22 \in [3]$ da, $-22 = (-5) \cdot 5 + 3$ delako, eta $-800 \in [0]$ da, $-800 = (-160) \cdot 5 + 0$ delako.

3.4 Funtzioak

3.4.1 Definizioak

3.42 Definizioa. *A eta B multzoak izanik, A multzotik B multzora doan* funtzio *bat A multzoaren elementu bakoitzari B multzoaren elementu bakar bat esleitzen dion f lege bat da.*

f A multzotik B multzora doan funtzio bat dela adierazteko honela idatziko dugu:

$$f : A \longrightarrow B \quad \textit{edo} \quad A \xrightarrow{f} B.$$

A f funtzioaren abiaburu multzoa *da eta B f funtzioaren* helburu multzoa *da.*

f funtzioak $a \in A$ elementuari $b \in B$ elementua esleitzen badio, esango dugu b dela a-ren (f-ren bidezko) irudia*, eta a dela b-ren (f-ren bidezko)* aurreirudi *bat. Eta honela adierazko dugu:*

$$f(a) = b \quad \textit{edo} \quad a \longmapsto b.$$

3.43 Adibideak.

1.
$$\begin{array}{rccc} h: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & x & \mapsto & x+1. \end{array}$$

   $7 \in \mathbb{N}$ elementuaren irudia 8 da, $h(7) = 8$. $1 \in \mathbb{N}$ elementuak aurreirudi bat du: 0, $h(0) = 1$. $0 \in \mathbb{N}$ elementuak ez du aurreirudirik, $\nexists x \in \mathbb{N} \,/\, h(x) = 0$ den.

2.
$$\begin{array}{rccl} l: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & \begin{cases} 0, & x \text{ bikoitia bada,} \\ 1, & x \text{ bakoitia bada.} \end{cases} \end{array}$$

3.
$$\begin{array}{rccc} p: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x_1, x_2) & \mapsto & x_1. \end{array}$$

   $(1,2) \in \mathbb{R}^2$ elementuaren irudia $p(1,2) = 1$ da.

4. Ondokoak **ez** dira funtzioak:

$$\begin{array}{rccc} f: & \{1,2,3\} & \longrightarrow & \{a,b,c,d\} \\ & 1 & \mapsto & a \\ & 1 & \mapsto & b \\ & 2 & \mapsto & c \\ & 3 & \mapsto & d. \end{array}$$

   Ez da funtzioa abiaburu multzoko 1 elementuari **bi** elementu esleitzen baitizkio helburu multzoan (1ak bi irudi ditu).

$$\begin{array}{rccc} g: & \{1,2,3\} & \longrightarrow & \{a,b\} \\ & 1 & \mapsto & a \\ & 2 & \mapsto & b. \end{array}$$

   Ez da funtzioa abiaburu multzoko 3 elementuari **ez** diolako elementurik esleitzen helburu multzoan (3ak ez du irudirik).

$$\begin{array}{rccc} h: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & x & \mapsto & x-1. \end{array}$$

0ak ez du irudirik.

$$\begin{array}{rccc} j: & \mathbb{N} & \longrightarrow & \mathbb{R} \\ & x & \mapsto & \sqrt{x}. \end{array}$$

Pentsa genezake 4ak bi irudi dituela, -2 eta 2. Baina ez da horrela. Erro karratua funtziotzat hartzeko, $+$ eta $-$ ikurren artean aukeratu behar dugu; $f(x) = +\sqrt{x}$ eta $f(x) = -\sqrt{x}$ bi funtzio dira. $+$ ikurra normalean ez da jartzen erroaren aurrean. Orduan, kasu honetan, $j(4) = +\sqrt{4} = 2$ da.

3.44 Definizioa. *$f : A \longrightarrow B$ funtzioa izanik, ondoko multzo honi f funtzioaren* grafo *deituko diogu:*

$$G_f := \{(x, f(x)) \ / \ x \in A\}.$$

Ohar gaitezen $G_f \subseteq A \times B$ dela, eta A-ren elementu bakoitza behin bakarrik agertzen dela G_f multzoaren elementuen lehenengo osagai gisa.

3.45 Adibideak.

1. h funtzio bat eta G_h bere grafoa:

$$\begin{array}{rccc} h: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & x & \mapsto & x+1. \end{array} \qquad G_h = \{(x, x+1) \ / \ x \in \mathbb{N}\}.$$

2. l funtzio bat eta G_l grafoa:

$$\begin{array}{rccc} l: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & \begin{cases} 0, \ x \text{ bikoitia bada,} \\ 1, \ x \text{ bakoitia bada.} \end{cases} \end{array}$$

$$G_l = \{(x, 0) \ / \ x \in \mathbb{Z} \text{ eta } x \text{ bikoitia da}\} \cup \{(x, 1) \ / \ x \in \mathbb{Z} \text{ eta } x \text{ bakoitia da}\}.$$

Beraz, funtzio bat izanik, grafo bat definitzen dugu. Alderantziz ere beteko da. Hau da, $G \subseteq A \times B$ multzo bat izanik, A-ren elementu bakoitza behin bakarrik agertzen delarik G-ren elementuen lehenengo osagai gisa, $f : A \longrightarrow B$ funtzio bat dago, zeinaren grafoa G den.

3.46 Definizioa. *f eta g funtzioak* berdinak *direla esango dugu, eta $f = g$ idatziko dugu, hau betetzen badute:*

1. *A abiaburu multzo bera badute;*

2. *B helburu multzo bera badute;*

3. *$(\forall x \in A) \quad f(x) = g(x)$ bada.*

3.47 Adibidea. Funtzio hauek izanik:

$$f: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \mapsto & x^2, \end{array} \qquad g: \begin{array}{ccc} \{-3,3\} & \longrightarrow & \mathbb{Z} \\ x & \mapsto & x^2, \end{array}$$

$$h: \begin{array}{ccc} \{-3,3\} & \longrightarrow & \mathbb{N} \\ x & \mapsto & x^2, \end{array} \qquad k: \begin{array}{ccc} \{-3,3\} & \longrightarrow & \mathbb{Z} \\ x & \mapsto & 9. \end{array}$$

$f \neq g$ da, f eta g funtzioek ez baitute abiaburu multzo bera; $g \neq h$ da, g eta h funtzioek ez baitute helburu multzo bera; eta $g = k$ da:

1. g eta k funtzioek abiaburu multzo bera dute: $\{-3,3\}$;
2. g eta k funtzioek helburu multzo bera dute: $\mathbb{Z}$; eta
3. $(\forall x \in \{-3,3\}) \quad g(x) = 9 = k(x)$ betetzen dutelako.

3.48 Definizioa. *$f : A \longrightarrow B$ funtzioa izanik eta abiaburu multzoaren $A_1 \subseteq A$ azpimultzo bat izanik, ondoko funtzioari f funtzioaren A_1 multzorako* murrizketa *deituko diogu, eta $f\,|_{A_1}$ adieraziko dugu:*

$$f\,|_{A_1}: \begin{array}{ccc} A_1 & \longrightarrow & B \\ x & \mapsto & f(x). \end{array}$$

3.49 Adibidea.

$$f: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \mapsto & x^2; \end{array} \qquad f\,|_{\{-3,3\}}: \begin{array}{ccc} \{-3,3\} & \longrightarrow & \mathbb{Z} \\ x & \mapsto & x^2. \end{array}$$

3.50 Definizioa. *A multzoa izanik, A multzoaren gaineko* identitate funtzioa *id_A edo 1_A adieraziko dugu eta honela definituko dugu:*

$$id_A: \begin{array}{ccc} A & \longrightarrow & A \\ x & \mapsto & x. \end{array}$$

3.51 Definizioa. *A multzoa izanik,* funtzio karakteristiko *deituko diogu eta f_A adieraziko dugu ondoko funtzio honi:*

$$f_A: \begin{array}{ccc} U & \longrightarrow & \{0,1\} \\ x & \mapsto & \begin{cases} 1, & x \in A \text{ bada,} \\ 0, & x \notin A \text{ bada,} \end{cases} \end{array}$$

non U multzo unibertsala baita.

3.52 Adibidea. Demagun multzo unibertsala $\mathbb{Z}$ dela.

$$f_{\mathbb{N}}: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \{0,1\} \\ x & \mapsto & \begin{cases} 1, & x \geq 0 \text{ bada,} \\ 0, & x < 0 \text{ bada.} \end{cases} \end{array}$$

3.53 Definizioa. *$f : A \longrightarrow B$ funtzioa eta $A_1 \subseteq A$ azpimultzoa izanik, A_1-en elementu guztien irudien multzoari A_1 azpimultzoaren (f-ren bidezko)* irudi *deituko diogu eta $f(A_1)$ adieraziko dugu; hau da,*

$$f(A_1) := \{f(x) \,/\, x \in A_1\}.$$

Ohar gaitezen $f(A_1) \subseteq B$ dela.

Hitzarmena. $f(\emptyset) := \emptyset$.

3.54 Definizioa. $f : A \longrightarrow B$ *funtzioa izanik,* $f(A)$ *multzoari* f *funtzioaren* irudi multzo *deitzen zaio eta* $\operatorname{Im} f$ *adierazten da; hau da,*

$$\operatorname{Im} f := \{f(x) \ / \ x \in A\}.$$

3.4.2 Funtzio-motak

3.55 Definizioa. $f : A \longrightarrow B$ funtzio injektiboa *dela esango dugu* A*-ren elementu desberdinek irudi desberdinak badituzte* B *multzoan. Hau da,*

$$(\forall x_1, x_2 \in A) \quad x_1 \neq x_2 \quad \Longrightarrow f(x_1) \neq f(x_2) \text{ betetzen bada,}$$

edo, baliokidea dena,

$$(\forall x_1, x_2 \in A) \quad f(x_1) = f(x_2) \quad \Longrightarrow x_1 = x_2 \text{ betetzen bada.}$$

3.56 Definizioa. $f : A \longrightarrow B$ funtzio surjektiboa *dela esango dugu* B*-ren elementu guztiek gutxienez aurreirudi bat badute* A *multzoan. Hau da,* $\operatorname{Im} f = B$ *bada, edo, gauza bera dena:*

$$\forall y \in B \quad \exists x \in A, \text{ non } f(x) = y \text{ den.}$$

3.57 Definizioa. $f : A \longrightarrow B$ funtzio bijektiboa *dela esango dugu injektiboa eta surjektiboa bada.*

3.58 Adibideak.

1. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = 3x + 1$.
   - $f(x)$ funtzioa injektiboa da:
   $$x_1 \neq x_2 \implies 3x_1 \neq 3x_2 \implies 3x_1 + 1 \neq 3x_2 + 1 \implies f(x_1) \neq f(x_2).$$
   - $f(x)$ funtzioa surjektiboa da: $y \in \mathbb{R}$ izanik, $\exists x \in \mathbb{R} \,/ f(x) = y$?
   $y = f(x) \implies y = 3x + 1 \implies x = \dfrac{y-1}{3} \in \mathbb{R}$; beraz, bai.
   - Ondorioz, $f(x)$ funtzioa bijektiboa da.
2. $g : \mathbb{N} \longrightarrow \mathbb{N}$, $g(x) = x + 1$.
   - g injektiboa da: izan bitez $x_1, x_2 \in \mathbb{N}$ edozein,
   $$g(x_1) = g(x_2) \implies x_1 + 1 = x_2 + 1 \implies x_1 = x_2.$$
   - g **ez** da surjektiboa: $\nexists x \in \mathbb{N}$, non $g(x) = 0$ den, hau da, $x + 1 = 0$.
3. $|\cdot| : \mathbb{R} \longrightarrow \mathbb{R}$, balio absolutua:
   $$|x| = \begin{cases} -x, & x < 0, \\ x, & 0 \leq x. \end{cases}$$

- **Ez** da injektiboa: $|2| = |-2| = 2$, eta $2 \neq -2$.
- **Ez** da surjektiboa: $\forall x \in \mathbb{R}\ \ |x| \geq 0$ da; hau da, $\nexists x \in \mathbb{R} \,/\, |x| = -1$.

4. $p : \mathbb{R}^2 \longrightarrow \mathbb{R}$, $p(x_1, x_2) = x_1$.

   - p **ez** da injektiboa: $p(1, \pi) = p(1, 0)$, baina $(1, \pi) \neq (1, 0)$.
   - p surjektiboa da: $\forall y \in \mathbb{R}\ \exists (x_1, x_2) = (y, 0) \in \mathbb{R}^2$, non $p(x_1, x_2) = y$ den. Ohar gaitezen $y \in \mathbb{R}$ elementu bakoitzak aurreirudi bat baino gehiago duela; guk bat aukeratu dugu, baina infinitu daude; esaterako, $p(y, \pi) = y$.

3.59 Adibidea. A multzoa izanik, A multzoaren gaineko identitatea,

$$\begin{array}{rccc} id_A : & A & \longrightarrow & A \\ & x & \mapsto & x, \end{array}$$

injektiboa eta surjektiboa da. Hortaz, bijektiboa da.

3.4.3 Alderantzizko funtzioa

3.60 Teorema. *Funtzio bijektiboen karakterizazioa*
$f : A \longrightarrow B$ funtzio bat izanik,

$$f \ \textit{ bijektiboa da} \quad \Longleftrightarrow \quad \forall y \in B\ \exists! x \in A \,/\, f(x) = y \ \textit{ betetzen bada.}$$

Froga.

$\Longrightarrow$) f bijektiboa denez, surjektiboa da; beraz, hau beteko du:

$$\forall y \in B\ \exists x \in A \,/\, f(x) = y.$$

Ikus dezagun $x \in A$ hori bakarra dela. $\exists x_1, x_2 \in A$ baleude, non $f(x_1) = y$ eta $f(x_2) = y$ diren, orduan $f(x_1) = f(x_2)$ izango litzateke. Eta f injektiboa denez, $x_1 = x_2$ beteko litzateke.

$\Longleftarrow$) Demagun $\forall y \in B\ \exists! x \in A \,/\, f(x) = y$ betetzen dela.

$\forall y \in B\ \exists! x \in A \,/\, f(x) = y$ betetzen bada, f surjektiboa da, surjektiboa izateko nahikoa delako $x \in A$ existitzea.

Ikus dezagun f injektiboa dela.

Har ditzagun $x_1, x_2 \in A$, eta demagun $f(x_1) = f(x_2)$ dela. $f(x_1), f(x_2) \in B$; beraz, $\exists! x \in A \,/\, f(x) = f(x_1) = f(x_2)$; orduan, $x = x_1 = x_2$ izango da, $x \in A$ bakarra delako. $\square$

Orduan, $f : A \longrightarrow B$ funtzio bijektibo bat izanik, $\forall y \in B\ \exists! x \in A \,/\, f(x) = y$. Beraz, esan dezakegu $y \in B$ horri $x \in A$ bakar bat dagokiola; hau da, badago lege bat $y \in B$ bakoitzari $x \in A$ bakar bat esleitzen diona.

3.61 Definizioa. *$f : A \longrightarrow B$ funtzio bijektibo bat izanik, honako funtzio honi f funtzioaren alderantzizko funtzio deituko diogu, eta f^{-1} idatziko dugu:*

$$\begin{array}{rccl} f^{-1}: & B & \longrightarrow & A \\ & y & \mapsto & x, \ \textit{non } f(x) = y. \end{array}$$

3.62 Adibidea. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = 3x + 1$, funtzioa bijektiboa denez, alderantzizko funtzioa honela defini dezakegu:

$y \in \mathbb{R}$ izanik, $\exists! x \in \mathbb{R} \,/\, f^{-1}(y) = x$, non $f(x) = y$ den; beraz, $3x + 1 = y$ da, eta hortik, $x = \dfrac{y-1}{3}$ aterako dugu. Orduan,

$f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$, $f^{-1}(y) = \dfrac{y-1}{3}$ f funtzioaren alderantzizko funtzioa da.

3.63 Ondorioa. *$f : A \longrightarrow B$ funtzio bijektiboa izanik, f funtzioaren alderantzizko funtzioa $f^{-1} : B \longrightarrow A$ bada, propietate hauek beteko dituzte:*

1. $(\forall x \in A)\ (\forall y \in B) \quad f^{-1}(y) = x \iff f(x) = y.$
2. $(\forall x \in A) \quad f^{-1}(f(x)) = x.$
3. $(\forall y \in B) \quad f(f^{-1}(y)) = y.$

3.64 Teorema. *Funtzio bijektibo baten alderantzizko funtzioa ere bijektiboa da.*

3.65 Adibidea. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = 3x + 1$, funtzio bijektiboa denez, $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$, $f^{-1}(y) = \dfrac{y-1}{3}$, alderantzizko funtzioa ere bijektiboa da.

3.4.4 Funtzioen konposizioa

3.66 Definizioa. *$f : A \longrightarrow B$ eta $g : B \longrightarrow C$ funtzioak izanik, f eta g funtzioen arteko* funtzio konposatu *deituko diogu, eta $g \circ f$ idatziko dugu, honako funtzio honi:*

$$\begin{array}{rccc} g \circ f: & A & \longrightarrow & C \\ & x & \mapsto & g(f(x)). \end{array}$$

Ohar gaitezen $g \circ f$ definitu ahal izateko, f funtzioaren helburu multzoak bat etorri behar duela g funtzioaren abiaburu multzoarekin.

$$\begin{array}{rccccc} g \circ f: & A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & x & \longmapsto & f(x) & \longmapsto & g(f(x)). \end{array}$$

$g \circ f$ funtzioa ongi definiturik dago:

- abiaburu multzoko elementu bakoitzak irudi bat du helburu multzoan:

$$x \in A \implies f(x) \in B \implies g(f(x)) \in C.$$

- abiaburu multzoko elementu bakoitzaren irudia bakarra da: $x_1, x_2 \in A$ izanik,

$$x_1 = x_2 \implies f(x_1) = f(x_2) \implies g(f(x_1)) = g(f(x_2)).$$

3.67 Adibideak.

1. f eta g funtzio hauen $g \circ f$ funtzio konposatua horrela kalkulatuko dugu:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & x & \mapsto & x^2, \end{array} \qquad \begin{array}{rccc} g: & \mathbb{N} & \longrightarrow & \mathbb{R} \\ & x & \mapsto & x+3, \end{array} \qquad \begin{array}{rccc} g \circ f: & \mathbb{Z} & \longrightarrow & \mathbb{R} \\ & x & \mapsto & x^2+3. \end{array}$$

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

   Ohar gaitezen ezin dela $f \circ g$ definitu, g funtzioaren helburu multzoa ez datorrelako bat f funtzioaren abiaburu multzoarekin.

2. h eta j funtzio hauen $j \circ h$ eta $h \circ j$ funtzio konposatuak horrela kalkulatuko ditugu:

$$\begin{array}{rccc} h: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & x^2, \end{array} \qquad \begin{array}{rccc} j: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & x+3. \end{array}$$

$$\begin{array}{rccc} j \circ h: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & x^2+3, \end{array} \qquad \begin{array}{rccc} h \circ j: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & (x+3)^2. \end{array}$$

   $(j \circ h)(x) = j(h(x)) = j(x^2) = x^2 + 3. \quad (h \circ j)(x) = h(j(x)) = h(x+3) = (x+3)^2.$

   Beraz, nahiz eta $h \circ j$ eta $j \circ h$ funtzio konposatuak existitu, ez dira berdinak, hots, $h \circ j \neq j \circ h$.

Adibideetan ikusi dugu, oro har, funtzioen konposizioa ez dela trukakorra.

3.68 Propietateak.

1. Funtzioen konposizioa elkarkorra da.

   $f : A \longrightarrow B$, $g : B \longrightarrow C$ eta $h : C \longrightarrow D$ funtzioak izanik,

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

2. $f : A \longrightarrow B$ funtzioa izanik,

$$f \circ id_A = f, \quad id_B \circ f = f.$$

3. $f : A \longrightarrow B$ funtzio bijektiboa izanik,

$$f^{-1} \circ f = id_A, \quad f \circ f^{-1} = id_B.$$

4. Funtzio surjektiboen funtzio konposatua surjektiboa da.

   $f : A \longrightarrow B$ eta $g : B \longrightarrow C$ funtzioak izanik,

$$f, g \text{ surjektiboak} \quad \Longrightarrow \quad g \circ f \text{ surjektiboa.}$$

5. Funtzio injektiboen funtzio konposatua injektiboa da.

   $f : A \longrightarrow B$ eta $g : B \longrightarrow C$ funtzioak izanik,

$$f, g \text{ injektiboak} \quad \Longrightarrow \quad g \circ f \text{ injektiboa.}$$

6. Funtzio bijektiboen funtzio konposatua bijektiboa da.
   $f : A \longrightarrow B$ eta $g : B \longrightarrow C$ funtzioak izanik,
   $$f, g \text{ bijektiboak} \quad \Longrightarrow \quad g \circ f \text{ bijektiboa.}$$

7. $f : A \longrightarrow B$ eta $g : B \longrightarrow C$ funtzio bijektiboak izanik (beraz, $g \circ f$ bijektiboa da),
   $$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Oharra. Elkartze-propietateari esker, $h \circ g \circ f$ idatz dezakegu parentesiak jarri gabe.
Idazkera. $f^n = f \circ \overset{n}{\cdots} \circ f$.

Froga.

1. Ikusteko zeintzuk diren $h \circ (g \circ f)$ funtzioaren abiaburu multzoa eta helburu multzoa, lehenago, $g \circ f$ funtzioarenak ikusiko ditugu:
   $$g \circ f \ : \ A \xrightarrow{f} B \xrightarrow{g} C,$$
   eta gero, $h \circ (g \circ f)$ funtzioarenak:
   $$h \circ (g \circ f) \ : \ A \xrightarrow{g \circ f} C \xrightarrow{h} D.$$
   Ikusteko zeintzuk diren $(h \circ g) \circ f$ funtzioaren abiaburu multzoa eta helburu multzoa, lehenago, $h \circ g$ funtzioarenak ikusiko ditugu:
   $$h \circ g \ : \ B \xrightarrow{g} C \xrightarrow{h} D,$$
   eta gero, $(h \circ g) \circ f$ funtzioarenak:
   $$(h \circ g) \circ f \ : \ A \xrightarrow{f} B \xrightarrow{h \circ g} D.$$
   Ikus dezagun, orain, $h \circ (g \circ f) = (h \circ g) \circ f$ betetzen dela.
   - $h \circ (g \circ f)$ eta $(h \circ g) \circ f$ funtzioek abiaburu multzo bera dute: A.
   - $h \circ (g \circ f)$ eta $(h \circ g) \circ f$ funtzioek helburu multzo bera dute: D.
   - $(\forall x \in A) \quad (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$:
     $$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)));$$
     $$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

2. - $f \circ id_A \ : \ A \xrightarrow{id_A} A \xrightarrow{f} B, \quad f : A \longrightarrow B.$
     - $f \circ id_A$ eta f funtzioek abiaburu multzo bera dute: A.
     - $f \circ id_A$ eta f funtzioek helburu multzo bera dute: B.
     - $(\forall x \in A) \quad (f \circ id_A)(x) = f(x)$:
       $$(f \circ id_A)(x) = f(id_A(x)) = f(x).$$

- $id_B \circ f \,:\, A \xrightarrow{f} B \xrightarrow{id_B} B, \quad f : A \longrightarrow B.$
  - $id_B \circ f$ eta f funtzioek abiaburu multzo bera dute: A.
  - $id_B \circ f$ eta f funtzioek helburu multzo bera dute: B.
  - $(\forall x \in A) \quad (id_B \circ f)(x) = f(x)$:

$$(id_B \circ f)(x) = id_B(f(x)) = f(x).$$

3. - $f^{-1} \circ f \,:\, A \xrightarrow{f} B \xrightarrow{f^{-1}} A, \quad id_A : A \longrightarrow A.$
   - $f^{-1} \circ f$ eta id_A funtzioek abiaburu multzo bera dute: A.
   - $f^{-1} \circ f$ eta id_A funtzioek helburu multzo bera dute: A.
   - $(\forall x \in A) \quad (f^{-1} \circ f)(x) = id_A(x)$:

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = id_A(x).$$

   - $f \circ f^{-1} \,:\, B \xrightarrow{f^{-1}} A \xrightarrow{f} B, \quad id_B : B \longrightarrow B.$
     - $f \circ f^{-1}$ eta id_B funtzioek abiaburu multzo bera dute: B.
     - $f \circ f^{-1}$ eta id_B funtzioek helburu multzo bera dute: B.
     - $(\forall y \in B) \quad (f \circ f^{-1})(y) = id_B(y)$:

$$(f \circ f^{-1})(y) = f(f^{-1}(y)) = y = id_B(y).$$

4. $g \circ f \,:\, A \xrightarrow{f} B \xrightarrow{g} C$. Demagun f eta g surjektiboak direla.

   Frogatu behar dugu $g \circ f$ surjektiboa dela. Hau da,

$$\forall z \in C \quad \exists x \in A \,/\, (g \circ f)(x) = z \text{ betetzen dela.}$$

   Izan bedi $z \in C$ edozein. g surjektiboa denez, $\exists y \in B \,/\, g(y) = z$.

   $y \in B$ denez eta f surjektiboa denez, $\exists x \in A \,/\, f(x) = y$.

   Orduan, $z = g(y) = g(f(x)) = (g \circ f)(x)$. Hortaz, $\exists x \in A \,/\, (g \circ f)(x) = z$.

5. $g \circ f \,:\, A \xrightarrow{f} B \xrightarrow{g} C$. Demagun f eta g injektiboak direla.

   Frogatu behar dugu $g \circ f$ injektiboa dela. Hau da,

$$(\forall x_1, x_2 \in A) \quad (g \circ f)(x_1) = (g \circ f)(x_2) \implies x_1 = x_2 \text{ betetzen dela.}$$

   Izan bitez $x_1, x_2 \in A$ edozein,

$$\begin{aligned}&(g \circ f)(x_1) = (g \circ f)(x_2) \implies g(f(x_1)) = g(f(x_2)) \implies \\ &\implies f(x_1) = f(x_2), \ (g \text{ injektiboa delako}) \implies \\ &\implies x_1 = x_2, \ (f \text{ injektiboa delako}).\end{aligned}$$

6. Aurreko bi propietateen ondorio zuzena da.

7. $g \circ f \,:\, A \xrightarrow{f} B \xrightarrow{g} C, \quad (g \circ f)^{-1} : C \longrightarrow A, \quad f^{-1} \circ g^{-1} \,:\, C \xrightarrow{g^{-1}} B \xrightarrow{f^{-1}} A$

- $(g \circ f)^{-1}$ eta $f^{-1} \circ g^{-1}$ funtzioek abiaburu multzo bera dute: C.
- $(g \circ f)^{-1}$ eta $f^{-1} \circ g^{-1}$ funtzioek helburu multzo bera dute: A.
- $(\forall z \in C) \quad (g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z)$:
  Izan bedi $z \in C$ edozein. $(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z)$ betetzen dela frogatzeko, nahikoa da $(g \circ f)((f^{-1} \circ g^{-1})(z)) = z$ frogatzea:

$$(g \circ f)((f^{-1} \circ g^{-1})(z)) = (g \circ f \circ f^{-1} \circ g^{-1})(z) = (g \circ id_B \circ g^{-1})(z) =$$

$$= (g \circ g^{-1})(z) = id_C(z) = z.$$

$\square$

4. Kapitulua

Zenbaki-teoria

4.1 Zenbaki osoak

4.1.1 Eragiketak zenbaki osoen artean. Ordena onaren printzipioa

Atal honetan, 3.2.1 Atalean aipatu genuen zenbaki osoen $\mathbb{Z}$ multzoa aztertuko dugu, baita bertan defini daitezkeen eragiketak eta $\leq$ "txikiago edo berdin"ordena-erlazioa ere.

- Gogora dezagun $\mathbb{Z}$ multzoa azpimultzo disjuntutan deskonposa daitekeela, honela:

$$\mathbb{Z} = \mathbb{Z}^- \dot{\cup} \{0\} \dot{\cup} \mathbb{Z}^+.$$

- $\mathbb{Z}$ multzoa itxia da $(+)$ batuketarako, $(\cdot)$ biderketarako eta $(-)$ kenketarako:

$$x, y \in \mathbb{Z} \implies x + y,\, x \cdot y,\, x - y \in \mathbb{Z};$$

  baina ez da itxia $(/)$ zatiketarako; adibidez: $2, 3 \in \mathbb{Z}$, baina $\dfrac{2}{3} \notin \mathbb{Z}$.

  Hala ere, zatiketa murriztua, zatiketa euklidearra, definituko dugu $\mathbb{Z}$ multzoan, eta $\mathbb{Z}^+$ multzoaren elementu berezi batzuetan, *zenbaki lehenak*, jarriko dugu arreta.

- Bestalde, $\leq$ ordena-erlazioa da $\mathbb{Z}$ multzoan, Erlazioen 3.3.2 Atalean definitu ditugun propietateak betetzen dituelako:

  - Bihurtze-propietatea: $(\forall x \in \mathbb{Z}) \quad x \leq x.$
  - Antisimetria-propietatea: $(\forall x, y \in \mathbb{Z}) \quad x \leq y \ \wedge \ y \leq x \implies x = y.$
  - Iragate-propietatea: $(\forall x, y, z \in \mathbb{Z}) \quad x \leq y \ \wedge \ y \leq z \implies x \leq z.$

  Are gehiago, ordena osoko erlazioa da; hau da, $\leq$ ordena-erlazioak osoki ordenatzen du $\mathbb{Z}$ multzoa; horrek esan nahi du x eta y zeinahi zenbaki osoak izanik, beti ordenatu ahal izango ditugula:

$$(\forall x, y \in \mathbb{Z}) \quad x \leq y \ \vee \ y \leq x.$$

$\leq$ ordena-erlazioaren propietate horiek $\mathbb{Q}$ eta $\mathbb{R}$ multzoetan ere betetzen dira. $\mathbb{N}$ edo $\mathbb{Z}^+$ multzoa $\mathbb{Q}^+$ eta $\mathbb{R}^+$ multzoetatik bereizten duena da lehena **multzo ongi ordenatua** dela, bestela esanda, **ordena onaren printzipioa** betetzen dela: $\mathbb{N}$ edo $\mathbb{Z}^+$ multzoaren edozein azpimultzo ez-hutsek elementu minimo bat dauka.

Printzipio hori ez da $\mathbb{Q}^+$ multzoan betetzen, ezta $\mathbb{R}^+$ multzoan ere. Esate baterako,

$$(0,8) = \{x \in \mathbb{R} \ / \ 0 < x < 8\}$$

tarte irekia $\mathbb{R}^+$ multzoaren azpimultzo ez-hutsa da, baina ez du elementu minimorik. Hori frogatzeko, demagun tarteak m elementu minimoa duela. Orduan, $0 < m < 8$; hortik, $0 < \dfrac{m}{2} < 4 < 8$ dugu, $\dfrac{m}{2} \in (0,8)$ izanik. Baina $\dfrac{m}{2} < m$ betetzen da; beraz, kontraesan batera heldu gara, m baita $(0,8)$ tartearen minimoa.

4.1.2 Zatigarritasuna. Zenbaki lehenak

$\mathbb{Z}^*$ multzoa / zatiketarako itxia ez bada ere, badira kasu batzuk non zenbaki oso batek beste bat zehazki zatitzen duen. Esaterako, 4ak 12a zehazki zatitzen du ($12 = 3 \cdot 4$). Hau da, 12 zati 4 egitean, zatidura gisa 3 eta hondar gisa 0 zenbaki osoak lortuko ditugu.

4.1 Definizioa. *$a, b \in \mathbb{Z}$ zenbakiak badira, $a \neq 0$ izanik, a zenbakiak b zenbakia* zatitzen du*, eta $a \mid b$ adieraziko dugu, baldin*

$$\exists k \in \mathbb{Z}, \quad \textit{non} \ \ b = ka \ \textit{den.}$$

Hori gertatzen denean, a zenbakia b zenbakiaren zatitzaile *bat dela esango dugu, edo b zenbakia a zenbakiaren* multiplo *bat dela.*

Hitzarmena. $a \mid b$ idazten dugunean, $a \neq 0$ dela pentsatuko dugu.

4.2 Lema. *$a, b \in \mathbb{Z}^+$ bada, $a \mid b \implies a \leq b$.*

Ondoko teoreman zatigarritasunaren propietate batzuk frogatuko ditugu.

4.3 Teorema. *$a, b, c \in \mathbb{Z}$ izanik,*

1. $1 \mid a; \quad a \mid a; \quad a \mid 0.$ *$(a \neq 0)$*
2. $(a \mid b) \ \wedge \ (b \mid a) \implies a = b \ \vee \ a = -b.$ *$(a \neq 0, b \neq 0)$*
3. $(a \mid b) \ \wedge \ (b \mid c) \implies a \mid c.$ *$(a \neq 0, b \neq 0)$*
4. $a \mid b \implies (\forall x \in \mathbb{Z}) \ \ a \mid xb.$ *$(a \neq 0)$*
5. $(a \mid b) \wedge (a \mid c) \implies (\forall x, y \in \mathbb{Z}) \ \ a \mid xb + yc.$ *$(a \neq 0)$*

Froga.

1. $a = 1a$ da; beraz, $1 \mid a$ eta $a \mid a$.

   Bestalde, $0 = 0a$ da; beraz, $a \mid 0$.

2.
$$\left.\begin{array}{c} a \mid b \\ \wedge \\ b \mid a \end{array}\right\} \Longrightarrow \left.\begin{array}{c} b = k_1 a,\ k_1 \in \mathbb{Z} \text{ izanik} \\ \wedge \\ a = k_2 b,\ k_2 \in \mathbb{Z} \text{ izanik} \end{array}\right\} \Longrightarrow b = k_1(k_2 b) = (k_1 k_2)b,$$

$$k_1, k_2 \in \mathbb{Z} \text{ izanik} \Longrightarrow k_1 k_2 = 1,\ k_1, k_2 \in \mathbb{Z} \text{ izanik} \Longrightarrow \left.\begin{array}{c} k_1 = k_2 = 1 \\ \vee \\ k_1 = k_2 = -1 \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow a = b \vee a = -b.$$

3.
$$\left.\begin{array}{c} a \mid b \\ \wedge \\ b \mid c \end{array}\right\} \Longrightarrow \left.\begin{array}{c} b = k_1 a,\ k_1 \in \mathbb{Z} \text{ izanik} \\ \wedge \\ c = k_2 b,\ k_2 \in \mathbb{Z} \text{ izanik} \end{array}\right\} \Longrightarrow c = k_2(k_1 a) = (k_2 k_1)a,$$

$k_2 k_1 \in \mathbb{Z}$ izanik $\Longrightarrow a \mid c$.

4. Edozein $x \in \mathbb{Z}$ izanik,

   $a \mid b \Longrightarrow b = ka,\ k \in \mathbb{Z}$ izanik $\Longrightarrow xb = x(ka) = (xk)a,\ xk \in \mathbb{Z}$ izanik $\Longrightarrow$
   $\Longrightarrow a \mid xb$.

5. Edozein $x, y \in \mathbb{Z}$ izanik,

$$\left.\begin{array}{c} a \mid b \\ \wedge \\ a \mid c \end{array}\right\} \Longrightarrow \left.\begin{array}{c} b = k_1 a,\ k_1 \in \mathbb{Z} \text{ izanik} \\ \wedge \\ c = k_2 a,\ k_2 \in \mathbb{Z} \text{ izanik} \end{array}\right\} \Longrightarrow xb + yc = x(k_1 a) + y(k_2 a) =$$

$$= (xk_1 + yk_2)a,\ xk_1 + yk_2 \in \mathbb{Z} \text{ izanik} \Longrightarrow a \mid xb + yc. \qquad \square$$

Oharrak.

- $b, c \in \mathbb{Z}$ izanik,
$$xb + yc, \quad x, y \in \mathbb{Z} \text{ izanik},$$
  adierazpenari $b, c \in \mathbb{Z}$ zenbakien *konbinazio lineal* deituko diogu.

  a zenbakiak b eta c zenbakiak zatitzen baditu, 4.3-5 Teoremaren arabera, a zenbakiak b eta c zenbakien edozein konbinazio lineal zatituko du.

- Propietate hori honela zabal daiteke: $b_1, \ldots, b_n \in \mathbb{Z}$ izanik,
$$x_1 b_1 + \cdots + x_n b_n, \quad x_1, \ldots, x_n \in \mathbb{Z} \text{ izanik},$$
  adierazpenari $b_1, \ldots, b_n$ zenbakien *konbinazio lineal* deituko diogu.

  a zenbakiak $b_1, \ldots, b_n$ zenbakiak zatitzen baditu, a zenbakiak $b_1, \ldots, b_n$ zenbakien edozein konbinazio lineal zatituko du:
$$a \mid b_i,\ i = 1, \ldots, n \Longrightarrow (\forall x_1, \ldots, x_n \in \mathbb{Z}) \quad a \mid x_1 b_1 + \cdots + x_n b_n.$$

4.4 Adibidea. Ba al daude $5x + 10y + 20z = 1003$ ekuazioa betetzen duten zenbaki osoak?

Demagun x, y, z zenbaki oso horiek existitzen direla. $5 \mid 5$, $5 \mid 10$ eta $5 \mid 20$ betetzen direnez, $5 \mid 1003$ ere beteko litzateke; baina hori ez da gertatzen. Hortaz, ez daude ekuazioa betetzen duten x, y, z zenbaki osoak.

4.5 Definizioa. *Izan bedi $n \in \mathbb{Z}^+$, $n > 1$.*

n zenbaki lehena *dela esango dugu bere zatitzaile positibo bakarrak n eta 1 badira:*

$$m \mid n, \quad m \in \mathbb{Z}^+ \Longrightarrow m = 1 \vee m = n.$$

Eta n zenbaki konposatua *dela esango dugu ez bada lehena:*

$$\exists m_1, m_2 \in \mathbb{Z}^+, \quad non \;\; n = m_1 m_2 \;\; den, \qquad 1 < m_1 < n, \; 1 < m_2 < n.$$

4.6 Adibidea. 12 zenbaki konposatua da, $12 > 1$ delako eta 1, 2, 3, 4, 6 eta 12 zatitzaileak dituelako.

11 zenbaki lehena da, $11 > 1$ delako eta bere zatitzaile positibo bakarrak 1 eta 11 direlako.

Hurrengo teoreman zenbaki lehenen eta konposatuen arteko erlazio bat frogatuko dugu.

4.7 Teorema. *Zenbaki konposatu orok zatitzaile lehenen bat dauka. Hau da, $n \in \mathbb{Z}^+$, $n > 1$ izanik,*

$$n \;\; konposatua \;\; \Longrightarrow \exists p \in \mathbb{Z}^+, \, p \;\; lehena \;\; eta \;\; p \mid n.$$

Froga.

Izan bedi S zatitzaile lehenik ez duten zenbaki oso konposatu guztien multzoa:

$$S = \{x \in \mathbb{Z}^+ \;/\; x \;\; \text{konposatua da eta ez du zatitzaile lehenik}\}.$$

Absurdora eramanez, $S = \emptyset$ dela frogatuko dugu.

Demagun $S \neq \emptyset$ dela. S multzoa $\mathbb{Z}^+$ multzoaren azpimultzo ez-hutsa denez, ordena onaren printzipioaren arabera, S multzoak elementu minimoa izango du, m.

$m \in S$ denez, m konposatua da; beraz, $m_1, m_2 \in \mathbb{Z}^+$ badaude, non $m = m_1 m_2$ den, $1 < m_1 < m$, $1 < m_2 < m$ izanik.

m da S multzoaren minimoa eta $m_1 < m$ da; beraz, $m_1 \notin S$ beteko da. Hortaz, m_1 lehena da edo zatitzaile lehenen bat dauka.

m_1 lehena bada, m_1 lehena da eta $m_1 \mid m$ betetzen da.

m_1 zenbakiak p zatitzaile lehen bat badauka, p lehena da eta $p \mid m_1$ eta $m_1 \mid m$; hortaz, $p \mid m$.

Bi kasuetan kontraesan bat aurkitu dugu, m zenbakiak ez baitauka zatitzaile lehenik. Beraz, $S = \emptyset$ da; eta, ondorioz, zenbaki konposatu orok zatitzaile lehenen bat dauka. $\square$

4.8 Teorema. *(Euklides, Elementuak, IX, 20)*
Infinitu zenbaki lehen daude.

Froga.
Absurdora eramanez frogatuko dugu.
Jo dezagun zenbaki lehenen kopurua finitua dela: $p_1, \ldots, p_k$.
Izan bitez $a = p_1 \cdots p_k$, zenbaki lehenen biderkadura, eta $b = a + 1$.
Orduan, $p_i \mid a$, $i = 1, \ldots, k$ dugu eta, beraz, $a \geq p_i$, $i = 1, \ldots, k$; hortik $b \neq p_i$, $i = 1, \ldots, k$, aterako dugu. Beraz, b konposatua da. 4.7 Teoremaren arabera, badago $p_j \in \{p_1, \ldots, p_k\}$ zenbaki lehenen bat, non $p_j \mid b$ betetzen den.
Orduan, $p_j \mid b$ eta $p_j \mid a$ betetzen dira; beraz, $p_j \mid 1b + (-1)a$ ere beteko da. Baina $1b + (-1)a = b - a = 1$ dugu; beraz, $p_j \mid 1$ dugu; eta hori ezinezkoa da $p_j > 1$ delako.
Hortaz, ezin da egon zenbaki lehenen kopuru finitu bat bakarrik. Hau da, infinitu zenbaki lehen daude. □

4.1.3 Zatiketa euklidearra

Hurrengo emaitzak aukera emango digu 0 ez diren zenbaki osoen arteko zatiketarekin lan egiteko, zatiketa zehatza ez denean.

Adibidez, 38 zati 7 egiten badugu, zatidura 5 eta hondarra 3 aterako ditugu. Euklidesek (K.a. 300) frogatu zuen, a eta b bi zenbaki oso izanik, $b \neq 0$ izanik, zatidura bakar bat, q, eta hondar bakar bat, r, $0 \leq r < b$, lortzen ditugula beti.

Zatidura eta hondarra existitzen direla frogatzeko har dezagun kontuan nola egiten dugun 38 zati 7:

$$\begin{array}{r|l} 38 & 7 \\ \cline{2-2} 3 & 5 \end{array}$$

Zergatik ez da 6 zatidura? $6 \cdot 7 = 42 > 38$ delako. Hau da, x zenbaki bat bilatzen dugu, non $38 > x \cdot 7$ den; bestela esanda, $38 - x \cdot 7 > 0$ betetzen duena (beraz, $x < 6$ izango da). Zatidura x bada, hondarra $38 - x \cdot 7 > 0$ izango da.

Zergatik ez da 4 zatidura? $38 - 4 \cdot 7 = 10 > 38 - 5 \cdot 7$ delako. Izan ere, "hondar" positiboa sortzen duten zenbaki oso guztien artean, ahalik eta hondar txikiena uzten duena bilatzen dugu. Hau da, $38 - x \cdot 7$ ahalik eta txikiena, baina positiboa, egiten duen x zenbakia izango da zatidura. Bestela esanda, $\{x \in \mathbb{Z} \ / \ 38 - x \cdot 7 > 0\}$ multzoaren minimoa bilatzen dugu.

Ikus dezagun beste adibide bat:

$$\begin{array}{r|l} -38 & 7 \\ \cline{2-2} 4 & -6 \end{array}$$

$-38 - x \cdot 7 > 0$ izan dadin $x < -5$ bete behar da.

x	$-38 - x \cdot 7$
-4	-10
-5	-3
-6	4
-7	11
-8	18
$\vdots$	$\vdots$

"Hondar" positibo txikiena 4 da eta, beraz, zatidura -6 da.
Euklidesek ideia hori teorema honetan zehaztu zuen:

4.9 Teorema. *Zatiketa euklidearra*
$a, b \in \mathbb{Z}$ *izanik,* $b > 0$ *izanik,*

$$\exists! q \in \mathbb{Z} \ \exists! r \in \mathbb{Z}, \quad non \ \ a = qb + r \ \ den, \ 0 \leq r < b \ \ izanik.$$

q zatidura, r hondarra, a zatikizuna *eta* b zatitzailea *dira.*

Froga.
q eta r existitzen dira.
Bi kasu bereiziko ditugu: $b \mid a$ eta $b \nmid a$.

1. $b \mid a$.

   Orduan, $\exists k \in \mathbb{Z}$, non $a = kb$ den. Hortaz, nahikoa da $q = k$ eta $r = 0$ hartzea, eta $a = qb + r$ beteko da, $0 \leq r < b$ izanik.

2. $b \nmid a$.

   Izan bedi $S = \{a - xb \ / \ x \in \mathbb{Z} \text{ eta } a - xb > 0\}$ hondar positiboen multzoa. Lehendabizi, $S \neq \emptyset$ dela frogatuko dugu:

   1 $a > 0$ bada, $a = a - 0 \cdot b > 0$ beteko da, eta, hortaz, $a \in S$ da.

   2 $a \leq 0$ bada, izan bedi $t = a - 1$. Beraz, $t \in \mathbb{Z}$ eta

   $$a - tb = a - (a-1)b = a - ab + b = (1-b)a + b.$$

   beteko dira. Orduan,

   $$b > 0 \implies b \geq 1 \implies 1-b \leq 0 \implies (1-b)a \geq 0 \implies (1-b)a+b \geq b > 0 \implies$$
   $$\implies a - tb > 0 \implies a - tb \in S.$$

   Hortaz, $S \neq \emptyset$ da, eta ordena onaren printzipioaren arabera, S multzoak elementu minimoa du; izan bedi $r = \min S$.

   $$r \in S \implies r = a - qb > 0, \ q \in \mathbb{Z} \text{ izanik} \implies a = qb + r, \ q, r \in \mathbb{Z} \text{ eta } r > 0 \text{ izanik.}$$

   $r < b$ dela frogatzea baino ez da geratzen. Demagun $r \geq b$ dela; kontraesan batera helduko garela ikusiko dugu:

   1 $r = b$ bada, $a = qb + b = (q+1)b$ da eta, hortaz, $b \mid a$ beteko da, hartu dugun $b \nmid a$ baldintzaren kontrakoa dena.

   2 $r > b$ bada, $r = b + c$ beteko da, $c = r - b > 0$ izanik. Eta hortik

   $$a = qb + r = qb + b + c = (q+1)b + c \implies c = a - (q+1)b > 0 \implies c \in S.$$

   $r = \min S$ denez, $c \geq r$ da; $c = r - b$ denez, $r - b \geq r \implies b \leq 0$ lortuko dugu; eta hori ezinezkoa da $b > 0$ delako.

q eta r bakarrak dira.
Demagun ez direla bakarrak, hau da,

$$\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}, \quad \text{non} \quad a = q_1 b + r_1 \quad \text{eta} \quad a = q_2 b + r_2 \quad \text{den},$$

$0 \leq r_1 < b$ eta $0 \leq r_2 < b$ izanik. Orduan,

$$q_1 b + r_1 = q_2 b + r_2 \implies (q_1 - q_2)b = r_2 - r_1$$

beteko da.

Lehendabizi, $r_1 = r_2$ dela frogatuko dugu.

$r_1 \neq r_2$ dela pentsatuko dugu eta kontraesan bat aurkituko dugu.

1. $r_2 > r_1$ bada, $0 < (q_1 - q_2)b \leq r_2 < b$ izango dugu. $b > 0$ denez, $0 < q_1 - q_2 < 1$ aterako dugu; eta hori ezinezkoa da $q_1 - q_2 \in \mathbb{Z}$ delako.

2. $r_2 < r_1$ bada, arrazoibide bera da, kontuan izanik $(q_2 - q_1)b = r_1 - r_2$ dela.

Hortaz, $r_1 = r_2$ dugu; hortik $q_1 b = q_2 b$ aterako dugu. $b \neq 0$ denez, $q_1 = q_2$ lortuko dugu. □

4.10 Adibidea. Adibide hauetan ematen diren zatidurak eta hondarrak existitzen dira eta bakarrak dira.

$$\begin{array}{r|l} 27 & 6 \\ \hline 3 & 4 \end{array} \qquad \begin{array}{r|l} -27 & 6 \\ \hline 3 & -5 \end{array} \qquad \begin{array}{r|l} 6 & 27 \\ \hline 6 & 0 \end{array} \qquad \begin{array}{r|l} -6 & 27 \\ \hline 21 & -1 \end{array}$$

4.1.4 Zatitzaile komun handiena

4.11 Definizioa. *Izan bitez $a, b \in \mathbb{Z}$ eta izan bedi $c \in \mathbb{Z}^+$. c zenbakia a eta b zenbakien* zatitzaile komun *bat dela esango dugu $c \mid a$ eta $c \mid b$ betetzen badira.*

4.12 Adibidea. -24 zenbakiaren zatitzaile positiboak 1, 2, 3, 4, 6, 8, 12 eta 24 dira. 32 zenbakiaren zatitzaile positiboak 1, 2, 4, 8, 16 eta 32 dira. Bien zatitzaile positibo komunak 1, 2, 4 eta 8 dira.

4.13 Definizioa. *Izan bitez $a, b \in \mathbb{Z}$, $a \neq 0$ edo $b \neq 0$, eta izan bedi $d \in \mathbb{Z}^+$. d zenbakia a eta b zenbakien* zatitzaile komun handienetako *bat dela esango dugu baldin*

1. *d bada a eta b zenbakien zatitzaile komun bat:*

$$d \mid a \quad \text{eta} \quad d \mid b;$$

2. *a eta b zenbakien edozein zatitzaile komunek d zatitzen badu (d "handienetakoa" da zatigarritasunaren arabera):*

$$(\forall c \in \mathbb{Z}^+) \quad c \mid a, \quad c \mid b \implies c \mid d.$$

4.14 Adibidea. 4.12 Adibidean ikus dezakegu -24 eta 32 zenbakien zatitzaile komun handiena 8 dela.

Galdera batzuk egin ditzakegu: beti aurkitu ahal izango dugu bi zenbaki osoren zatitzaile komun handienetako bat? Bi zenbaki osok zenbait zatitzaile komun handien izan ditzakete?

Azkenekoari erantzuteko hona hemen teorema hau.

4.15 Teorema. *Zatitzaile komun handienaren bakartasuna*

$a, b \in \mathbb{Z}$ izanik, a eta b zenbakien zatitzaile komun handiena, existitzen bada, bakarra da.

Froga.

Demagun a eta b zenbakien bi zatitzaile komun handien daudela, d_1 eta d_2. $d_1 = d_2$ dela frogatuko dugu.

d_1 a eta b zenbakien zatitzaile komuna da; beraz, $d_1 \mid a$ eta $d_1 \mid b$; hortaz, $d_1 \mid d_2$, d_2 delako a eta b zenbakien zatitzaile komun handienetako bat.

Antzeko eran frogatuko genuke $d_2 \mid d_1$ ere betetzen dela. Orduan,

$$\left.\begin{array}{l} d_1 \mid d_2 \\ d_2 \mid d_1 \end{array}\right\} \Longrightarrow d_1 = d_2 \text{ edo } d_1 = -d_2.$$

$d_1, d_2 \in \mathbb{Z}^+$ denez, aukera bakarra $d_1 = d_2$ izatea da. □

Idazkera. $a, b \in \mathbb{Z}$ izanik, a eta b zenbakien zatitzaile komun handiena badago, $\text{zkh}(a, b)$ adieraziko dugu.

Hitzarmena. $\text{zkh}(0, 0)$ ez dago definiturik.

4.16 Propietateak.

1. $\text{zkh}(a, b)$ badago, $\text{zkh}(b, a) = \text{zkh}(a, b)$ beteko da.
2. $a \in \mathbb{Z}^*$ bada, $\text{zkh}(a, 0)$ badagoela eta $\text{zkh}(a, 0) = |a|$ betetzen dela froga daiteke.

   Froga.

   - $|a|$ zenbakia a eta 0 zenbakien zatitzaile komuna da:

   $$a = |a| \text{ edo } a = (-1)|a| \Longrightarrow |a| \,\Big|\, a;$$

   $$|a| \,\Big|\, 0 \text{ (edozein zenbaki oso da 0 zenbakiaren zatitzailea).}$$

   - $|a|$ zenbakia a eta 0 zenbakien zatitzaile komun handiena da: $c \in \mathbb{Z}^+$ izanik,

   $$\left.\begin{array}{l} c \mid a \\ c \mid 0 \end{array}\right\} \Longrightarrow c \mid a \Longrightarrow c \,\Big|\, |a| \quad (|a| = a \text{ edo } |a| = -a \text{ delako}).$$

□

Laburbilduz, a edo b zenbakietako bat bakarrik 0 bada, badago $\text{zkh}(a, b)$. Beraz, $\text{zkh}(a, b)$ existitzen dela frogatzeko, a eta b positiboak direla pentsatuko dugu.

4.17 Teorema. *Zatitzaile komun handienaren existentzia*
$a, b \in \mathbb{Z}^+$ zenbaki oso positibo guztietarako existitzen da zatitzaile komun handiena.

Froga.
Har dezagun a eta b zenbakien konbinazio lineal positibo guztien multzoa:

$$S = \{xa + yb \ / \ x, y \in \mathbb{Z} \quad \text{eta} \quad xa + yb > 0\}.$$

$S \subseteq \mathbb{Z}^+$ da. $0 < a = 1 \cdot a + 0 \cdot b$ betetzen denez, $a \in S$ dugu eta, beraz, $S \neq \emptyset$ da. Ordena onaren printzipioaren arabera, S multzoak elementu minimoa du; izan bedi $d = \min S$.

$d \in S$ denez, d izango da a eta b zenbakien konbinazio lineal positibo bat; hau da, $d \in \mathbb{Z}^+$ eta

$$d = xa + yb, \quad x, y \in \mathbb{Z} \text{ izanik.}$$

Ikus dezagun $d = \text{zkh}(a, b)$ dela:

- d zenbakia a eta b zenbakien zatitzaile <u>komun bat</u> da:
  - Demagun $d \not| a$ dela, eta kontraesan bat aurkituko dugu:
    $d \not| a$ bada, a zati d zatiketa euklidearra egitean, 0 ez den hondar bat lortuko dugu:
    $$\begin{array}{l|l} a & d \\ \cline{2-2} r & q \end{array}, \qquad r > 0.$$
    Hau da, $a = qd + r$ da, $0 < r < d$ izanik. Hortaz,
    $0 < r = a - qd = a - q(xa + yb) = (1 - qx)a + (-qy)b$ ere izango dugu. Beraz, r hondarra a eta b zenbakien konbinazio lineal positibo bat da. Orduan, $r \in S$ dugu eta, ondorioz, $r \geq d = \min S$ beteko da; eta hori ezinezkoa da, $r < d$ delako.
  - $d \mid b$ betetzen dela frogatzeko, antzeko arrazoibidea erabiliko genuke.
- d zenbakia a eta b zenbakien zatitzaile komun <u>handiena</u> da: $c \in \mathbb{Z}^+$ beste zatitzaile komun bat izanik,
  $$\left.\begin{array}{l} c \mid a \\ c \mid b \end{array}\right\} \Longrightarrow c \mid xa + yb = d \Longrightarrow c \leq d,$$
  zenbaki oso batek bi zenbaki zatitzen baditu, horien edozein konbinazio lineal zatituko duelako. □

Oharra. Aurreko teoreman, $a, b \in \mathbb{Z}^+$ zenbakietarako $\text{zkh}(a, b)$ existitzen dela frogatu dugu. Orain, $a, b \in \mathbb{Z}$ izanik, $\text{zkh}(a, b)$ beti existitzen dela froga dezakegu ($a = b = 0$ denean izan ezik).

$\text{zkh}(|a|, |b|)$ existitzen dela jadanik frogatu dugu. Orain, $\text{zkh}(a, b) = \text{zkh}(|a|, |b|)$ betetzen dela frogatzea baino ez zaigu geratzen.

Horretarako, izan bedi $d = \text{zkh}(|a|, |b|)$ (badakigu existitzen dela); ikus dezagun $d = \text{zkh}(a, b)$ dela:

- d zenbakia a eta b zenbakien zatitzaile komun bat da:

$$d = \text{zkh}(|a|, |b|) \implies \begin{cases} d \mid |a| \implies d \mid a \\ d \mid |b| \implies d \mid b \end{cases}$$

- d zenbakia a eta b zenbakien zatitzaile komun handiena da: $c \in \mathbb{Z}^+$ beste zatitzaile komun bat izanik,

$$\left.\begin{array}{l} c \mid a \\ c \mid b \end{array}\right\} \implies \left\{\begin{array}{l} c \mid |a| \\ c \mid |b| \end{array}\right\} \implies c \mid d \implies c \leq d,$$

  d zenbakia $|a|$ eta $|b|$ zenbakien zatitzaile komun handiena delako.

4.18 Lema. *Bézout-en lema*

$a, b \in \mathbb{Z}$ badira, $a \neq 0$ edo $b \neq 0$ izanik, $\exists x, y \in \mathbb{Z}$, non $\text{zkh}(a, b) = xa+yb$ baita. Horrez gain, $\text{zkh}(a, b)$ da a eta b zenbakien konbinazio lineal moduan adieraz daitekeen zenbaki oso positiborik txikiena.

$$\text{zkh}(a, b) = \min\{xa + yb \,/\, x, y \in \mathbb{Z} \ \textit{eta} \ xa + yb > 0\}.$$

Froga.

$a, b \in \mathbb{Z}^+$ direnean, emaitza hori 4.17 Teoremaren frogatik atera dezakegu.

$a \in \mathbb{Z}^-$ edo $b \in \mathbb{Z}^-$ direnean frogatzeko, nahikoa da $\text{zkh}(a, b) = \text{zkh}(|a|, |b|)$ dela kontuan hartzea eta konbinazio lineal positiboen S eta S' multzoak berdinak direla frogatzea, hots, berdintza hau betetzen dela:

$$S = \{xa+yb \,/\, x, y \in \mathbb{Z} \ \text{eta} \ xa+yb > 0\} = \{x|a|+y|b| \,/\, x, y \in \mathbb{Z} \ \text{eta} \ x|a|+y|b| > 0\} = S'.$$

$\supseteq$: Demagun, esaterako, $a < 0$ eta $b > 0$ direla. Orduan,

$$z \in \{x|a| + y|b| \,/\, x, y \in \mathbb{Z} \ \text{eta} \ x|a| + y|b| > 0\} \implies$$

$$\implies z = x_1|a| + y_1|b|, \ \ x_1, y_1 \in \mathbb{Z} \ \text{eta} \ x_1|a| + y_1|b| > 0 \ \text{izanik} \implies$$

$$\implies z = x_1(-a)+y_1b = (-x_1)a+y_1b, \ \ (-x_1), y_1 \in \mathbb{Z} \ \text{eta} \ (-x_1)a+y_1b > 0 \ \text{izanik} \implies$$

$$\implies z \in \{xa + yb \,/\, x, y \in \mathbb{Z} \ \text{eta} \ xa + yb > 0\}.$$

Eta hortik partekotasun hau aterako dugu:

$$S' = \{x|a|+y|b| \,/\, x, y \in \mathbb{Z} \ \text{eta} \ x|a|+y|b| > 0\} \subseteq \{xa+yb \,/\, x, y \in \mathbb{Z} \ \text{eta} \ xa+yb > 0\} = S.$$

$\subseteq$: $S \subseteq S'$ beste partekotasuna antzeko eran frogatuko genuke.

Bézouten leman agertzen diren x eta y koefizienteak ez dira bakarrak; esate baterako, $\text{zkh}(a, b) = xa + yb$ bada, $p \in \mathbb{Z}$ guztietarako hau beteko da:

$$\text{zkh}(a, b) = (x + pb)a + (y - pa)b.$$

4.19 Adibidea. 4.12 Adibidean ikusi dugu $\text{zkh}(-24, 32) = 8$ dela eta 4.17 Teoremaren oharrean $\text{zkh}(-24, 32) = \text{zkh}(24, 32)$ dela frogatu dugu; hortaz,

$$\text{zkh}(24, 32) = \text{zkh}(-24, 32) = 8.$$

Bestalde, Bezouten lemari esker badakigu $\exists x, y \in \mathbb{Z}$, non $\text{zkh}(24, 32) = x24 + y32$ baita; adibidez, $x = -1$ eta $y = 1$ badira, $8 = (-1) \cdot 24 + 1 \cdot 32$.

Aurreko formula erabiliz, beste konbinazio lineal batzuk aurki ditzakegu:

$p = 1$ denean, $8 = ((-1) + 1 \cdot 32) \cdot 24 + (1 - 1 \cdot 24) \cdot 32 = 31 \cdot 24 + (-23) \cdot 32$;

$p = 2$ denean, $8 = ((-1) + 2 \cdot 32) \cdot 24 + (1 - 2 \cdot 24) \cdot 32 = 63 \cdot 24 + (-47) \cdot 32$.

Badakigu $a, b \in \mathbb{Z}$ eta $d \in \mathbb{Z}^+$ izanik, $d = \text{zkh}(a, b)$ bada, d zenbakia a eta b zenbakien konbinazio lineala dela, hau da,

$$d = \text{zkh}(a, b) \implies d = xa + yb, \quad x, y \in \mathbb{Z} \text{ izanik.}$$

Baina elkarrekikoa ez da orokorrean betetzen

$$d = xa + yb, \quad x, y \in \mathbb{Z} \text{ izanik} \not\Longrightarrow d = \text{zkh}(a, b).$$

Izan ere, orokorrean $d \geq \text{zkh}(a, b)$ betetzen da. Berdintza ziurtatzen duen kasu bakarra $d = 1$ kasua da, hots,

$$1 = xa + yb, \quad x, y \in \mathbb{Z} \text{ izanik} \iff \text{zkh}(a, b) = 1.$$

Kasu horrek hurrengo definiziora garamatza:

4.20 Definizioa. *$a, b \in \mathbb{Z}$ badira, a, b zenbakiak zenbaki* lehen erlatiboak *direla esango dugu* $\text{zkh}(a, b) = 1$ *denean.*

4.21 Ondorioa. *$a, b \in \mathbb{Z}$ badira,*

$$a, b \textit{ lehen erlatiboak dira} \iff \exists x, y \in \mathbb{Z}, \textit{ non } xa + yb = 1 \textit{ den.}$$

4.22 Adibideak.

1. $x = -2$ eta $y = 2$ hartuz, $16 = (-2) \cdot 24 + 2 \cdot 32$ dugu. Hortaz, $\text{zkh}(24, 32) \leq 16$ da.

2. Orain, $a = 3$ eta $b = 4$ zenbakiak hartuz, $1 = (-1) \cdot 3 + 1 \cdot 4$ dugu. Hortaz, $\text{zkh}(3, 4) = 1$ da eta 3 eta 4 zenbaki lehen erlatiboak dira.

4.1.5 Euklidesen algoritmoa

$a, b \in \mathbb{Z}^+$ izanik, $b \mid a$ bada, $\text{zkh}(a, b) = b$ izango da. Bestela, $\text{zkh}(a, b)$ kalkulatzeko, algoritmo hau erabiliko dugu:

Euklidesen algoritmoa. Ondoko zatiketak egingo ditugu:

$$
\begin{array}{r|l}
a & b \\ \cline{2-2}
r_1 & q_1
\end{array}
\qquad a = q_1 b + r_1, \qquad 0 < r_1 < b;
$$

$$
\begin{array}{r|l}
b & r_1 \\ \cline{2-2}
r_2 & q_2
\end{array}
\qquad b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1;
$$

$$
\begin{array}{r|l}
r_1 & r_2 \\ \cline{2-2}
r_3 & q_3
\end{array}
\qquad r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2;
$$

$$
\begin{array}{r|l}
 & \\
 & \vdots
\end{array}
\qquad \vdots \qquad \vdots
$$

$$
\begin{array}{r|l}
r_i & r_{i+1} \\ \cline{2-2}
r_{i+2} & q_{i+2}
\end{array}
\qquad r_i = q_{i+2} r_{i+1} + r_{i+2}, \qquad 0 < r_{i+2} < r_{i+1};
$$

$$
\begin{array}{r|l}
 & \\
 & \vdots
\end{array}
\qquad \vdots \qquad \vdots
$$

Gero eta hondar txikiagoak lortzen ditugunez, noizbait 0 hondarra lortuko dugu:

$$
\begin{array}{r|l}
r_{k-1} & r_k \\ \cline{2-2}
0 & q_{k+1}
\end{array}
\qquad r_{k-1} = q_{k+1} r_k + 0.
$$

$$
b > r_1 > r_2 > \cdots > r_{k-1} > r_k > 0 \ (= r_{k+1}).
$$

4.23 Teorema. *$a, b \in \mathbb{Z}^+$ izanik, Euklidesen algoritmoan lortzen den azken hondar eznulua r_k bada,* $\operatorname{zkh}(a, b) = r_k$ *beteko da.*

Froga.

Berdintza hauek dauzkagu:

$$
\left.
\begin{array}{l}
a = q_1 b + r_1, \\
b = q_2 r_1 + r_2, \\
r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad i = 1, \ldots, k-2.
\end{array}
\right\} \tag{4.1}
$$

$r_0 = b$ eta $r_{-1} = a$ izendatzen baditugu, (4.1) honela idatz ditzakegu:

$$
r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad i = -1, \ldots, k-2. \tag{4.2}
$$

Eta horrez gain, beste hau ere betetzen da:

$$
r_{k-1} = q_{k+1} r_k. \tag{4.3}
$$

$\operatorname{zkh}(a, b) = r_k$ dela frogatzeko, ondokoa frogatu beharko dugu:

1. r_k hondarra a eta b zenbakien zatitzaile komun bat da; hau da, $r_k \mid a$ eta $r_k \mid b$ betetzen dira.

   Horretarako, ondoz ondo frogatuko dugu r_k hondarrak r_k, r_{k-1}, r_{k-2}, r_{k-3}, etab. zatitzen dituela, $r_0 = b$ eta $r_{-1} = a$ ere zatitzen dituela frogatu arte.

   (4.2) berdintzan ikus dezakegu $i = -1, \ldots, k-2$ balioetarako r_i hondarra r_{i+2} eta r_{i+1} hondarren konbinazio lineala dela, eta hori erabiliko dugu.

   - Badakigu $r_k \mid r_k$ betetzen dela, $r_k \neq 0$ izanik.
   - Bestalde, (4.3) berdintzatik $r_k \mid r_{k-1}$ ateratzen da.
   - $r_k \mid r_{k-2}$ frogatzeko, (4.2) berdintzetako $i = k-2$ kasuan, $r_{k-2} = q_k r_{k-1} + r_k$ berdintza dugu; hau da, r_{k-2} hondarra r_k eta r_{k-1} hondarren konbinazio lineala da. $r_k \mid r_k$ eta $r_k \mid r_{k-1}$ frogatu ditugunez, $r_k \mid r_{k-2}$ daukagu.
   - $r_k \mid r_{k-3}$ frogatzeko, antzeko arrazoibidea erabiliko dugu: (4.2) berdintzetako $i = k-3$ kasuan, $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ berdintza dugu; hau da, r_{k-3} hondarra r_{k-1} eta r_{k-2} hondarren konbinazio lineala da. $r_k \mid r_{k-1}$ eta $r_k \mid r_{k-2}$ frogatuta daudenez, $r_k \mid r_{k-3}$ ere beteko da.
   - Antzeko eran frogatuko ditugu $r_k \mid r_{k-4}$, $r_k \mid r_{k-5}$, etab. $r_k \mid r_0 = b$ eta $r_k \mid r_{-1} = a$ kasuetara heldu arte.

2. r_k hondarra a eta b zenbakien zatitzaile komun handiena da; hau da, a eta b zenbakien edozein zatitzaile komun r_k hondarraren zatitzailea da.

   Izan bedi $c \in \mathbb{Z}^+$ a eta b zenbakien zatitzaile komun bat, hots, $c \mid a$ eta $c \mid b$ betetzen dira. $c \mid r_k$ ere betetzen dela frogatu behar dugu. Horretarako, ondoz ondo frogatuko dugu c zenbakiak r_{-1}, r_0, r_1, r_2, etab. zatitzen dituela, r_k hondarrera heldu arte.

   (4.2) berdintzatik r_{i+2} bakanduz gero, berdintza hauek lortuko ditugu:

   $$r_{i+2} = r_i - q_{i+2} r_{i+1}, \quad i = -1, \ldots, k-2. \tag{4.4}$$

   Ohar gaitezen, orduan, $i = -1, \ldots, k-2$ balioetarako r_{i+2} hondarra r_i eta r_{i+1} hondarren konbinazio lineala dela; propietate hori erabiliko dugu.

   - $c \mid a = r_{-1}$.
   - $c \mid b = r_0$.
   - $c \mid r_1$ frogatzeko, (4.4) ekuazioetako $i = -1$ kasuan, $r_1 = r_{-1} - q_1 r_0$ dugu; hau da, r_1 hondarra r_{-1} eta r_0 hondarren konbinazio lineala da. $c \mid r_{-1}$ eta $c \mid r_0$ betetzen direnez, $c \mid r_1$ ere beteko da.
   - $c \mid r_2$ frogatzeko, arrazoibidea antzekoa da: (4.4) ekuazioetako $i = 0$ kasuan, $r_2 = r_0 - q_2 r_1$ dugu; hau da, r_2 hondarra r_0 eta r_1 hondarren konbinazio lineala da. $c \mid r_0$ eta $c \mid r_1$ betetzen direla frogatu dugunez, $c \mid r_2$ ere beteko da.
   - Antzeko eran frogatuko dugu $c \mid r_3$, $c \mid r_4$, etab. betetzen direla $c \mid r_k$ betetzen dela frogatu arte. □

4.24 Adibidea. zkh$(250, 12)$ kalkulatzeko:

$$\begin{array}{r|l} 250 & 12 \\ \cline{2-2} 10 & 20 \end{array} \qquad \begin{array}{r|l} 12 & 10 \\ \cline{2-2} 2 & 1 \end{array} \qquad \begin{array}{r|l} 10 & 2 \\ \cline{2-2} 0 & 5 \end{array}.$$

Hortaz,

$$\text{zkh}(250, 12) = \text{zkh}(-250, 12) = \text{zkh}(250, -12) = \text{zkh}(-250, -12) = 2.$$

Oharrak.

1. Euklidesen algoritmoa bai $a > b$ denean bai $a < b$ denean erabil daiteke; azken kasu horretan zatiketa bat gehiago egin beharko da.

2. Euklidesen algoritmoak zkh(a, b) a, b zenbakien konbinazio lineal bezala adierazteko metodoa erakutsi digu.

4.25 Adibideak.

1. 4.24 Adibidean, zkh$(250, 12) = 2$ kalkulatu dugu. 2 emaitza 250 eta 12 zenbakien konbinazio lineal bezala adierazteko, 2 azkeneko hondar ez-nulua 10 eta 12 zenbakien konbinazio lineal bezala adierazten hasiko gara:

$$\begin{array}{r|l} 12 & 10 \\ \cline{2-2} 2 & 1 \end{array} \qquad 12 = 1 \cdot 10 + 2, \qquad 2 = 12 - 1 \cdot 10.$$

   Orain, kontuan izanik 10 dela aurreko hondarra, 10 hori 250 eta 12 zenbakien konbinazio lineal bezala adieraz dezakegu:

$$\begin{array}{r|l} 250 & 12 \\ \cline{2-2} 10 & 20 \end{array} \qquad 250 = 20 \cdot 12 + 10, \qquad 10 = 250 - 20 \cdot 12.$$

   Orduan, hau lortuko dugu:

$$2 = 12 - 1 \cdot \mathbf{10} = 12 - 1 \cdot (250 - 20 \cdot 12) = (-1) \cdot 250 + 21 \cdot 12.$$

2. zkh$(-250, 12) = 2 = 1 \cdot (-250) + 21 \cdot 12$.
   zkh$(250, -12) = 2 = (-1) \cdot 250 + (-21) \cdot (-12)$.
   zkh$(-250, -12) = 2 = 1 \cdot (-250) + (-21) \cdot (-12)$.

3. Euklidesen algoritmoa erabiliko dugu zkh$(250, 111)$ kalkulatzeko eta 250 eta 111 zenbakien konbinazio lineal bezala adierazteko:

$$\begin{array}{r|l} 250 & 111 \\ \cline{2-2} 28 & 2 \end{array} \qquad 250 = 2 \cdot 111 + 28, \qquad 28 = 250 - 2 \cdot 111;$$

$$\begin{array}{r|l} 111 & 28 \\ \cline{2-2} 27 & 3 \end{array} \qquad 111 = 3 \cdot 28 + 27, \qquad 27 = 111 - 3 \cdot 28;$$

$$\begin{array}{r|l} 28 & 27 \\ \cline{2-2} 1 & 1 \end{array} \qquad 28 = 1 \cdot 27 + 1, \qquad 1 = 28 - 1 \cdot 27;$$

$$\begin{array}{r|l} 27 & 1 \\ \cline{2-2} 0 & 27 \end{array} \qquad 27 = 27 \cdot 1.$$

$\text{zkh}(250, 111) = 1$; beraz, 250 eta 111 zenbaki lehen erlatiboak dira.

$$\begin{aligned} 1 = &\ 28 - 1 \cdot 27 = 28 - 1 \cdot (111 - 3 \cdot 28) = \\ = &\ (-1) \cdot 111 + 4 \cdot 28 = (-1) \cdot 111 + 4 \cdot (250 - 2 \cdot 111) = \\ = &\ 4 \cdot 250 + (-9) \cdot 111. \end{aligned}$$

4.1.6 Multiplo komun txikiena

4.26 Definizioa. *Izan bitez $a, b, c \in \mathbb{Z}^+$, c zenbakia a eta b zenbakien* multiplo komun *bat dela esango dugu baldin $a \mid c$ eta $b \mid c$ bada.*

4.27 Adibideak.

1. 40 zenbakia 2 eta 10 zenbakien multiplo komun bat da; izan ere, $2 \mid 40$ eta $10 \mid 40$ betetzen dira.

2. 180 zenbakia 12 eta 18 zenbakien multiplo komun bat da; izan ere, $12 \mid 180$ eta $18 \mid 180$ betetzen dira.

4.28 Definizioa. *Izan bitez $a, b, m \in \mathbb{Z}^+$, m zenbakia a eta b zenbakien* multiplo komun txikiena *dela esango dugu ($m = \text{mkt}(a, b)$) a eta b zenbakien multiplo komunen artean zenbaki oso txikiena bada; hau da,*

1. *m zenbakia a eta b zenbakien multiplo komun bat da:*

$$a \mid m \ \text{ eta } \ b \mid m.$$

2. *a eta b zenbakien edozein multiplo komun m baino handiago edo berdina da:*

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \implies m \leq c.$$

4.29 Adibideak.

1. 40 zenbakia 2 eta 10 zenbakien multiplo komuna da, baina ez da $\text{mkt}(2, 10)$; izan ere, 20 ere 2 eta 10 zenbakien multiplo komuna da eta $20 \leq 40$. Gainera, $\text{mkt}(2, 10) = 10$ dela groga dezakegu:

   - $2 \mid 10$ eta $10 \mid 10$.
   - $(\forall c \in \mathbb{Z}^+) \quad 2 \mid c, \quad 10 \mid c \implies 10 \mid c \implies 10 \leq c.$

2. 180 zenbakia 12 eta 18 zenbakien multiplo komuna da, baina ez da $\text{mkt}(12, 18)$; izan ere, 72 ere 12 eta 18 zenbakien multiplo komuna da eta $72 \leq 180$. Froga genezake $\text{mkt}(12, 18) = 36$ dela.

Hurrengo teoreman a eta b zenbakien multiplo komun guztiak $\text{mkt}(a, b)$ zenbakiaren multiploak direla frogatuko dugu.

4.30 Teorema. *$a, b, m \in \mathbb{Z}^+$ izanik, $m = \text{mkt}(a, b)$ bada, a eta b zenbakien edozein multiplo komun m zenbakiaren multiploa da:*

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \implies m \mid c.$$

Froga.

Demagun $m = \text{mkt}(a, b)$ dela; hau da, m zenbakiak 4.28 Definizioaren 1 eta 2 baldintzak betetzen ditu.

Izan bedi $c \in \mathbb{Z}^+$ zenbakia a eta b zenbakien multiplo komun bat; beteko al da $m \mid c$?

Demagun $m \not\mid c$ betetzen dela; kontraesan bat bilatuko dugu.

$m \not\mid c$ bada, $c = qm + r$ izango da, $0 < r < m$ izanik; beraz, $r = c - qm$ da; hau da, r zenbakia c eta m zenbakien konbinazio lineala da.

Batetik $a \mid c$, bestetik $m = \text{mkt}(a, b) \implies a \mid m$ ditugu; hortaz, $a \mid r$ ere beteko da.

Horrez gain, $b \mid c$ ere betetzen da, eta $m = \text{mkt}(a, b) \implies b \mid m$; hortaz, $b \mid r$ ere beteko da.

Horrela, r zenbakia a eta b zenbakien multiplo komun bat da; eta, beraz, $m \leq r$ bete beharko litzateke; baina hori $r < m$ izatearen kontra doa.

Ondorioz, $m \mid c$ dugu. □

4.31 Adibidea. $\text{mkt}(12, 18) = 36$ denez, 12 eta 18 zenbakien edozein multiplo komun 36 zenbakiaren multiploa da. Esaterako, $36 \mid 72$.

Ondoko teoreman, zatitzaile komun handiena eta multiplo komun txikiena erlazionatuko ditugu.

4.32 Teorema. $a, b \in \mathbb{Z}^+$ *izanik,* $ab = \text{mkt}(a, b)\,\text{zkh}(a, b)$ *betetzen da.*

Froga.

Izan bitez $d = \text{zkh}(a, b)$ eta $m = \text{mkt}(a, b)$. $ab = md$ dela frogatu beharko dugu.

$d = \text{zkh}(a, b)$ denez, $a = k_1 d$ eta $b = k_2 d$ ditugu, $k_1, k_2 \in \mathbb{Z}$ izanik. Gainera, $d = xa + yb$ da, $x, y \in \mathbb{Z}$ izanik.

Bestalde, $m = \text{mkt}(a, b)$ denez, $m = k_1' a$ eta $m = k_2' b$ ditugu, $k_1', k_2' \in \mathbb{Z}$ izanik.

- $md \mid ab$:

$$ab = ak_2 d = bk_1 d \implies \frac{ab}{d} = ak_2 = bk_1 \implies \left\{ \begin{array}{c} a \mid \dfrac{ab}{d} \\ \\ b \mid \dfrac{ab}{d} \end{array} \right\} \implies m \mid \frac{ab}{d}$$

(4.30 Teoremaren arabera) $\implies md \mid ab$.

- $ab \mid md$:

$$md = mxa + myb = k_2' bxa + k_1' ayb = (xk_2' + yk_1')ab \implies ab \mid md.$$

$$\left.\begin{array}{l} md \mid ab \\ ab \mid md \end{array}\right\} \implies ab = md \text{ edo } ab = -md \implies ab = md \quad (ab, md \in \mathbb{Z}^+ \text{ direlako}).$$ □

Oharra. $a, b \in \mathbb{Z}^+$ bi zenbaki izanik, $\text{zkh}(a, b)$ Euklidesen algoritmoa erabiliz kalkula dezakegu, eta $\text{mkt}(a, b)$ kalkulatzeko, aurreko teorema erabili.

4.33 Adibideak.

1. $\text{zkh}(250, 12) = 2$; hortaz, $\text{mkt}(250, 12) = \dfrac{250 \cdot 12}{2} = 1500$ da.

2. $\text{zkh}(250, 111) = 1$; hortaz, $\text{mkt}(250, 111) = 250 \cdot 111$ da.

3. $\text{zkh}(12, 18) = 6$; hortaz, $\text{mkt}(12, 18) = \dfrac{12 \cdot 18}{6} = 36$ da.

4.1.7 Aritmetikaren oinarrizko teorema

4.7 Teoreman ikusi genuen edozein zenbaki konposatuk gutxienez zatitzaile lehen bat duela. Emaitza hura zabalduko dugu atal honetan eta beste hau frogatuko dugu: edozein $n \in \mathbb{Z}^+$, $n > 1$, izanik, n lehena da edo n zenbaki lehenen biderketa bezala idatz daiteke era bakarrean, faktoreen ordena kontuan izan gabe.

Emaitza hori frogatu baino lehen bi lema hauek frogatuko ditugu.

4.34 Lema. *$a, b, p \in \mathbb{Z}^+$ izanik, p lehena izanik,*

$$p \mid ab \implies (p \mid a) \ \textit{edo} \ (p \mid b).$$

Froga.

Demagun $p \mid ab$ betetzen dela; hau da,

$$ab = kp, \quad k \in \mathbb{Z} \text{ izanik.}$$

Bietako bat, $p \mid a$ edo $p \mid b$ betetzen dela frogatu behar dugu.

Horretarako, $p \not\mid a$ betetzen dela pentsatuko dugu eta, orduan, $p \mid b$ betetzen dela ikusiko dugu.

Izan bedi $d = \text{zkh}(a, p)$.

$d \mid p$ denez eta p lehena denez, $d = 1$ edo $d = p$ ditugu. $d \mid a$ eta $p \not\mid a$ direnez, aukera bakarra $d = 1$ izatea da.

Orduan, hau lortuko dugu:

$\text{zkh}(a, p) = 1 \implies 1 = xa + yp, \quad x, y \in \mathbb{Z}$ izanik $\implies$

$\implies b = xab + ypb = xkp + ypb = (xk + yb)p, \quad xk + yb \in \mathbb{Z}$ izanik $\implies p \mid b.$ □

4.35 Lema. *$a_1, \ldots, a_n, p \in \mathbb{Z}^+$ izanik, p lehena izanik,*

$$p \mid a_1 \cdots a_n \implies p \mid a_j, \ j \in \{1, \cdots, n\} \ \textit{baterako.}$$

Froga.

Demagun $p \mid a_1 \cdots a_n$ betetzen dela.

n-ren gaineko indukzioa erabiliz frogatuko dugu $j \in \{1, \cdots, n\}$ baterako $p \mid a_j$ beteko dela.

$n = 1$ denean, ez dago zer frogatu, $p \mid a_1$ betetzen da.

Demagun propietate hori betetzen dela $n = k$ denean, eta izan bedi $n = k + 1$.

Orduan,

$$p \mid a_1 \cdots a_n = a_1 \cdots a_k a_{k+1} = (a_1 \cdots a_k) a_{k+1}.$$

4.34 Lema aplikatuz, $p \mid a_1 \cdots a_k$ edo $p \mid a_{k+1}$ lortuko dugu.

$p \mid a_1 \cdots a_k$ betetzen bada, indukzio-hipotesiaren arabera,

$$p \mid a_j \text{ beteko da, } j \in \{1, \cdots, k\} \subset \{1, \cdots, k+1\} = \{1, \cdots, n\} \text{ baterako.}$$

$p \mid a_{k+1}$ betetzen bada, $p \mid a_j$ betetzen da, $j = k + 1 \in \{1, \cdots, k+1\} = \{1, \cdots, n\}$ kasurako. □

4.36 Adibidea. Ikus dezagun $\sqrt{2}$ zenbaki irrazionala dela.

Irrazionala ez dela pentsatuko dugu. Orduan, ondoko hau idatzi ahal izango dugu: $\sqrt{2} = \dfrac{a}{b}$, non $a, b \in \mathbb{Z}$ eta $\text{zkh}(a, b) = 1$ diren.

Hortik,

$$\sqrt{2} = \frac{a}{b} \implies 2 = \frac{a^2}{b^2} \implies 2b^2 = a^2 \implies 2 \mid a^2 = a \cdot a$$

atera dezakegu. 4.34 Lema aplikatuz, $2 \mid a$ ateratzen dugu. Eta hortik,

$$2 \mid a \implies a = 2k, \quad k \in \mathbb{Z} \text{ izanik} \implies 4k^2 = a^2 = 2b^2, \quad k \in \mathbb{Z} \text{ izanik} \implies$$

$$\implies b^2 = 2k^2, \quad k^2 \in \mathbb{Z} \text{ izanik} \implies 2 \mid b^2 = b \cdot b.$$

4.34 Lema aplikatuz, $2 \mid b$ ateratzen dugu.

$2 \mid a$ eta $2 \mid b$ betetzen direnez, $2 \mid \text{zkh}(a, b) = 1$ ere beteko da; baina hori ezinezkoa da.

4.37 Teorema. *Aritmetikaren oinarrizko teorema*

Edozein $n \in \mathbb{Z}^+$, $n > 1$, izanik, n lehena da edo n zenbaki lehenen biderketa bezala idatz daiteke era bakarrean, faktoreen ordena kontuan izan gabe. (n lehena bada, bera da faktore lehen bakarra)

Froga.

Izan bedi S multzo hau:

$$S = \{n \ / \ n \in \mathbb{Z}^+, n > 1, n \text{ ezin da adierazi zenbaki lehenen biderketa bezala}\}.$$

Absurdora eramanez, $S = \emptyset$ dela frogatuko dugu. Horretarako, $S \neq \emptyset$ dela pentsatuko dugu.

Ordena onaren printzipioaren arabera, S multzoak elementu minimoa izango du; izan bedi $m = \min S$. $m \in S$ denez, m ez da lehena eta, hortaz, $m = m_1 m_2$ izango da, $1 < m_1 < m$ eta $1 < m_2 < m$ izanik.

$m_1 < m = \min S$ eta $m_2 < m = \min S$ direnez, $m_1, m_2 \notin S$ beteko da; beraz, badago m_1 eta m_2 zenbaki lehenen biderketa bezala adieraztea; eta hori $m \in S$ hipotesiaren kontra doa.

Ondorioz, $S = \emptyset$ da. Hortaz, edozein $n \in \mathbb{Z}^+$, $n > 1$, izanik, n zenbakiaren faktorizazioa lor dezakegu zenbaki lehenekin.

Faktorizazioa bakarra dela frogatzea baino ez da geratzen. n-ren gaineko indukzioz frogatuko dugu.

- $n = 2$ denean (lehenengo kasua), nabaria da faktorizazioa bakarra dela: $n = 2$ da.
- Demagun faktorizazioa bakarra dela $n = 3, \ldots, k$ kasuetarako (indukzio-hipotesia) eta froga dezagun $n = k + 1$ kasuan ere bakarra dela.

  Horretarako $k + 1$ zenbakiak bi faktorizazio onartzen dituela pentsatuko dugu:

  $k + 1 = p_1^{s_1} \cdots p_r^{s_r}$, $\quad p_1 < \cdots < p_r$ zenbaki lehenak eta $\quad s_i > 0$, $\quad i = 1, \ldots, r$, izanik;

  $k + 1 = q_1^{t_1} \cdots q_u^{t_u}$, $\quad q_1 < \cdots < q_u$ zenbaki lehenak eta $\quad t_i > 0$, $\quad i = 1, \ldots, u$, izanik.

Frogatu beharko dugu $r = u$ eta $p_i = q_i$, $s_i = t_i$ direla, $i = 1, \ldots, r$ kasuetan.

$p_1 \mid k+1 = q_1^{t_1} \cdots q_u^{t_u}$ betetzen denez eta p_1 zenbaki lehena denez, 4.35 Lemaren arabera, $p_1 \mid q_j$ beteko da $j \in \{1, \ldots, u\}$ baterako. p_1, q_j zenbaki lehenak direnez eta $p_1 \mid q_j$ betetzen denez, $p_1 = q_j$ bete beharko da.

Ikus dezagun, absurdora eramanez, $j = 1$ dela. Demagun $j \neq 1$ dela, kontraesan batera helduko gara. $j > 1$ denez, $q_1 < q_j$ izango da. $q_1 \mid k+1 = p_1^{s_1} \cdots p_r^{s_r}$ denez eta q_1 zenbaki lehena denez, 4.35 Lemaren arabera, $q_1 \mid p_i$ beteko da $i \in \{1, \ldots, r\}$ baterako. q_1, p_i zenbaki lehenak direnez eta $q_1 \mid p_i$ denez, $q_1 = p_i$ bete beharko da. Orduan, $p_1 \leq p_i = q_1 < q_j = p_1$ izango dugu, eta hor dago kontraesana.

Hortaz, $j = 1$ eta $p_1 = q_1$ beteko dira.

Izan bedi $n_1 = \dfrac{k+1}{p_1} = \dfrac{k+1}{q_1}$. n_1 zenbakiaren bi faktorizazio dauzkagu:

$$n_1 = p_1^{s_1 - 1} \cdots p_r^{s_r},$$

$$n_1 = q_1^{t_1 - 1} \cdots q_u^{t_u}.$$

Baina, $n_1 < k+1$ denez, indukzio-hipotesiaren arabera, n_1 zenbakiak faktorizazio bakarra dauka; beraz, hau dena beteko da: $r = u$, $p_i = q_i$, $i = 1, \ldots, r$ guztietarako, eta $s_1 - 1 = t_1 - 1$ (hots, $s_1 = t_1$) eta $s_i = t_i$, $i = 2, \ldots, r$ guztietarako. $\square$

4.38 Adibidea. Kalkula dezagun 6552 zenbakiaren faktorizazioa zenbaki lehenekin:

- $2 \mid 6552$: $6552 = 2 \cdot 3276$.
- $2 \mid 3276$: $3276 = 2 \cdot 1638 \implies 6552 = 2^2 \cdot 1638$.
- $2 \mid 1638$: $1638 = 2 \cdot 819 \implies 6552 = 2^3 \cdot 819$.
- $2 \nmid 819$; $3 \mid 819$: $819 = 3 \cdot 273 \implies 6552 = 2^3 \cdot 3 \cdot 273$.
- $3 \mid 273$: $273 = 3 \cdot 91 \implies 6552 = 2^3 \cdot 3^2 \cdot 91$.
- $3 \nmid 91$; $5 \nmid 91$; $7 \mid 91$: $91 = 7 \cdot 13 \implies 6552 = 2^3 \cdot 3^2 \cdot 7 \cdot 13$.
- 13 lehena da; beraz, bukatu dugu.

$$\begin{array}{r|l} 6552 & 2 \\ 3276 & 2 \\ 1638 & 2 \\ 819 & 3 \\ 273 & 3 \\ 91 & 7 \\ 13 & \end{array}$$

$$6552 = 2^3 \cdot 3^2 \cdot 7 \cdot 13.$$

4.2 Aritmetika modularra

Atal honetan, zenbaki osoak n zenbakiaz zatiketa euklidearra (4.1.3 Atala) egitean lortuko den hondarrarekin erlazionatuko ditugu, eta hondar bereko elementuen multzoak hartuko ditugu kontuan. Horrez gain, multzo horietako elementuen arteko eragiketa aritmetikoak aztertuko ditugu.

3.3.4 Atalean, n moduluko kongruentziaren definizioa eman genuen:

$$a \equiv b \pmod{n} \iff n \mid a-b \iff \exists k \in \mathbb{Z} \,/\, a = b + kn.$$

Kasu horretan, $a-b$ zenbakia n-ren multiploa da.

Bestalde, 4.1.3 Atalean, zatiketa euklidearraren 4.9 Teorema eman genuen:

$$a, n \in \mathbb{Z} \text{ izanik, } n > 0, \exists! q \in \mathbb{Z} \ \exists! r \in \mathbb{Z}, \text{ non } a = qn + r \text{ den, } 0 \leq r < n \text{ izanik.}$$

$$\begin{array}{c|c} a & n \\ \cline{2-2} r & q \end{array} \qquad a = qn + r, \quad 0 \leq r < n.$$

Horren arabera, hondar posible guztiak 0, 1, ..., $n-1$ dira.

Oharrak.

- Zatiketa euklidearra eta kongruentziaren definizioa kontutan izanik, $a \equiv b \pmod{n}$ bada, hau da, $a - b = kn$ bada, a eta b zenbakiek hondar bera emango dute n zenbakiaz zatitzean; izan ere, b zenbakiak r hondarra ematen badu, $b = qn + r$ izango da; bestalde $a - b = kn$ denez, eta $a = b + (a - b)$ denez, $a = qn + r + kn$ izango da; ondorioz, $a = (q + k)n + r$ dela esan dezakegu; beraz, a zenbakiak, n zenbakiaz zatitzean, r hondarra emango du, alegia, b zenbakiak ematen duen hondar bera:

  $$\begin{array}{c|c} b & n \\ \cline{2-2} r & q \end{array} \quad b = qn + r,\ 0 \leq r < n. \qquad \begin{array}{c|c} a & n \\ \cline{2-2} r & q+k \end{array} \quad a = (q+k)n + r,\ 0 \leq r < n.$$

- n moduluko kongruentzian, zatitzailea n denez, hondar posible guztiak 0, 1, ..., $n-1$ dira. Horiek dira n moduluko kongruentziari dagokion $\mathbb{Z}_n$ zatidura-multzoaren klaseak idazteko erabiliko ditugun ordezkariak: $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$.

  Multzo horretan n elementu besterik ez dago, eta $\mathbb{Z}$ multzoko elementu oro $\mathbb{Z}_n$ multzoko elementu bakarrarekin erlazionatuta dago (3.40 Teorema: n moduluko kongruentzia baliokidetasun-erlazioa da).

  Aritmetika modularrean, klaseak adierazteko erabiltzen diren kortxeteak ez ditugu idatziko idazkera errazteko; beraz, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ idatziko dugu.

  Bestalde, formaltasuna erabili behar dugunean, $\mathbb{Z}_n$ multzoko $[a]$ klasea adierazteko, $a \pmod{n}$ idatziko dugu.

4.2.1 Eragiketa modularrak

4.39 Definizioa. $\mathbb{Z}_n$ *multzoan,* batuketa *eta* biderketa modularra *honela definitzen dira:*

$$(a \pmod{n}) + (b \pmod{n}) = (a + b) \pmod{n}.$$

$$(a \pmod{n}) \cdot (b \pmod{n}) = (a \cdot b) \pmod{n}.$$

Definizioak esaten digu $\mathbb{Z}_n$ multzoko $a \pmod{n}$ eta $b \pmod{n}$ bi klaseren arteko eragiketak egiteko, nahikoa dela klaseen a eta b ordezkarien arteko eragiketak egitea eta, ondoren, emaitzaren klasea ematea.

Gogoratu behar da $\mathbb{Z}$ multzoan elementu guztiek aurkakoa dutela, baina guztiek ez dutela alderantzizkorik. Berdin gertatzen da $\mathbb{Z}_n$ multzoan.

4.40 Definizioa.

1. *$\mathbb{Z}_n$ multzoan, a elementua izanik, $b \in \mathbb{Z}_n$ existitzen bada, non $a + b \equiv 0 \pmod{n}$ den, b elementuari a elementuaren* aurkako modularra *deituko diogu eta $-a$ idatziko dugu.*

2. *$\mathbb{Z}_n$ multzoan, a elementua* alderantzikagarria *da $\exists b \in \mathbb{Z}_n$, non $a \cdot b \equiv 1 \pmod{n}$ den. b elementuari a elementuaren* alderantzizko modularra *deituko diogu eta a^{-1} idatziko dugu.*

$\mathbb{Z}_n$ multzoan, **kenketa** honela kalkulatuko dugu:

$$(a \pmod{n}) - (b \pmod{n}) = (a + (-b)) \pmod{n},$$

non $-b$ elementua b-ren aurkakoa den $\mathbb{Z}_n$ multzoan.

$\mathbb{Z}_n$ multzoan, **zatiketa** ez dago elementu guztietarako definituta, eta existitzen denean honela kalkulatuko dugu:

$$(a \pmod{n}) \div (b \pmod{n}) = (a \cdot (b^{-1})) \pmod{n},$$

non b^{-1} elementua b-ren alderantzizkoa den $\mathbb{Z}_n$ multzoan.

4.41 Adibidea. Egin ditzagun ondoko eragiketak $\mathbb{Z}_{12}$ multzoan:

$$5 + 7, \quad 3 \cdot 8, \quad 4 - 9, \quad 5/7 \quad \text{eta} \quad 10/3.$$

Formalki honela egingo genuke:

- $(5 \pmod{12}) + (7 \pmod{12}) = (5 + 7) \pmod{12} = 12 \pmod{12} \equiv 0 \pmod{12}$.
- $(3 \pmod{12}) \cdot (8 \pmod{12}) = (3 \cdot 8) \pmod{12} = 24 \pmod{12} \equiv 0 \pmod{12}$.
- $(4 \pmod{12}) - (9 \pmod{12}) = (4 + (-9)) \pmod{12} \equiv (4 + 3) \pmod{12} =$
  $= 7 \pmod{12}$, $-9 \equiv 3 \pmod{12}$ delako.
- $(5 \pmod{12}) \div (7 \pmod{12}) = (5 \cdot (7^{-1})) \pmod{12} \equiv (5 \cdot 7) \pmod{12} =$
  $= 35 \pmod{12} \equiv 11 \pmod{12}$, $7^{-1} \equiv 7 \pmod{12}$ delako.
- $(10 \pmod{12}) \div (3 \pmod{12}) = (10 \cdot (3^{-1})) \pmod{12}$, ezin da egin ez delako existitzen $3^{-1} \pmod{12}$, hots, $\nexists p \in \mathbb{Z}_{12} \,/\, 3 \cdot p \equiv 1 \pmod{12}$.

Idazkera sinplifikatuz, honela egingo dugu: $5 + 7 = 12 \equiv 0 \pmod{12}$.
Eta horrela egingo dugu kasu praktikoetan.

4.42 Teorema. *Alderantzizko modularraren existentzia*
$a^{-1} \pmod n$ *existitzen da baldin eta soilik baldin* $\text{zkh}(a,n)=1$ *bada.*

Froga.

$$\Longrightarrow : \exists x = a^{-1} \pmod n \Longrightarrow xa \equiv 1 \pmod n \Longrightarrow n \mid xa-1 \Longrightarrow$$
$$\Longrightarrow \exists y \in \mathbb{Z} \,/\, xa-1 = yn \Longrightarrow xa - yn = 1 \Longrightarrow \text{zkh}(a,n)=1.$$

$\Longleftarrow$: $\text{zkh}(a,n)=1 \Longrightarrow \exists x,y \in \mathbb{Z}$, non $xa+yn=1$ den. Hortik,
$xa-1=-yn \Longrightarrow n \mid xa-1 \Longrightarrow xa \equiv 1 \pmod n \Longrightarrow \exists x = a^{-1} \pmod n$. □

$\mathbb{Z}_n$ multzoan alderantzikagarri diren elementuen multzoari *hondarren multzo murriztu* deituko diogu eta $\mathbb{Z}_n^*$ idatziko dugu: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \,/\, \text{zkh}(a,n)=1\}$.

Alderantzizko modularra existitzen denean, $a^{-1} \pmod n$ kalkulatzeko, Euklidesen algoritmoa erabiliko dugu.

Alderantzizko modularra kalkulatzeko bidea:
Izan bitez $a,n \in \mathbb{Z}$ zenbaki lehen erlatiboak; hots, $\text{zkh}(a,n)=1$ da.
4.18 Bézouten lematik dakigunez, $\exists x,y \in \mathbb{Z}$, non $xa+yn=\text{zkh}(a,n)=1$ den.
Hortik ondoriozta daiteke a-ren alderantzizko modularra x dela:
$xa+yn=1 \Longrightarrow xa = 1+(-y)n \Longrightarrow xa \equiv 1 \pmod n \Longrightarrow a^{-1} = x \pmod n$.
Euklidesen algoritmoa erabiliz x kalkulatuko dugu, hau da, a^{-1}.

4.43 Adibidea. Kalkula ditzagun elementu hauen alderantzizkoak $\mathbb{Z}_{12}$ multzoan:

$$5, \quad 3, \quad 9, \quad 7 \quad \text{eta} \quad 10.$$

Aurreko teoremak esaten digu a elementu baten alderantzizkoa existitzeko $\mathbb{Z}_{12}$ multzoan, $\text{zkh}(a,12)=1$ bete behar dela.

$\text{zkh}(3,12)=3$, $\text{zkh}(9,12)=3$ eta $\text{zkh}(10,12)=2$ direnez, 3, 9 eta 10 elementuen alderantzizkoak ez dira existitzen.

$\text{zkh}(5,12)=1$ eta $\text{zkh}(7,12)=1$ direnez, 5 eta 7 elementuen alderantzizkoak existitzen dira, eta kalkula ditzakegu.

Kalkula dezagun, orain, $5^{-1} \pmod{12}$). Badakigu, Bézouten lemagatik, $x,y \in \mathbb{Z}$ existitzen direla, non $5x+12y=\text{zkh}(5,12)=1$ den.

Euklidesen algoritmoa erabiliko dugu $x=5^{-1}$ kalkulatzeko.

$$\begin{array}{r|l} 12 & 5 \\ \cline{2-2} 2 & 2 \end{array} \qquad 12 = 2\cdot 5 + 2, \qquad 2 = 12 - 2\cdot 5;$$

$$\begin{array}{r|l} 5 & 2 \\ \cline{2-2} 1 & 2 \end{array} \qquad 5 = 2\cdot 2 + 1, \qquad 1 = 5 - 2\cdot 2;$$

$$\begin{array}{r|l} 2 & 1 \\ \cline{2-2} 0 & 2 \end{array} \qquad 2 = 2\cdot 1.$$

Hortik, $1 = 5 - 2\cdot 2 = 5 - 2\cdot(12 - 2\cdot 5) = (5)\cdot 5 + (-2)\cdot 12$.

Eta, ondorioz, 5aren alderantzizko modularra 5 bera da, hots, $5^{-1} \equiv 5 \pmod{12}$ da.

Egiazta daiteke hori: $5 \cdot 5^{-1} = 5 \cdot 5 = 25 \equiv 1 \pmod{12}$.

Kalkula dezagun, orain, $7^{-1} \pmod{12}$). $\exists x, y \in \mathbb{Z}, \quad / \quad 7x + 12y = \text{zkh}(7, 12) = 1$.

Euklidesen algoritmoa erabiliko dugu $x = 7^{-1}$ kalkulatzeko.

$$\begin{array}{r|l} 12 & 7 \\ \cline{2-2} 5 & 1 \end{array} \qquad 12 = 1 \cdot 7 + 5, \qquad 5 = 12 - 1 \cdot 7;$$

$$\begin{array}{r|l} 7 & 5 \\ \cline{2-2} 2 & 1 \end{array} \qquad 7 = 1 \cdot 5 + 2, \qquad 2 = 7 - 1 \cdot 5;$$

$$\begin{array}{r|l} 5 & 2 \\ \cline{2-2} 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1. \qquad 1 = 5 - 2 \cdot 2;$$

$$\begin{array}{r|l} 2 & 1 \\ \cline{2-2} 0 & 2 \end{array} \qquad 2 = 2 \cdot 1.$$

Hortik, $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 1 \cdot 5) = (3) \cdot 5 + (-2) \cdot 7 = (3) \cdot (12 - 1 \cdot 7) + (-2) \cdot 7 = = (3) \cdot 12 + (-5) \cdot 7$.

Ondorioz, 7aren alderantzizko modularra -5 da $\mathbb{Z}_{12}$ multzoan, hots, $7^{-1} \equiv -5 \pmod{12}$ da. Baina, 5aren aurkakoa 7 da $\mathbb{Z}_{12}$ multzoan, $5 + 7 = 12 \equiv 0 \pmod{12}$ delako. Hortaz, $7^{-1} \equiv 7 \pmod{12}$ da.

4.2.2 Berreketa modularra

$\mathbb{Z}$ multzoan, a^x berreketa, $a, x \in \mathbb{Z}$ eta $x \geq 0$ izanik, biderketen bidez kalkulatu ohi da, baina x berretzailea handia denean, bi arazo sortzen dira:

- a^x zenbaki handiegia izan daiteke, konputagailuak kalkulatu ahal izateko.
- a zenbakia bere buruarekin $x - 1$ aldiz biderkatu behar da eta, beraz, biderketa kopuru handia egin behar da, kostu konputazionala handituz.

$\mathbb{Z}_n$ multzoan, ordea, $a^x \pmod{n}$ kalkulatzean,

- Zenbaki handiegien arazoa ekiditen da, kalkuluetan n moduluko kongruentzia erabiltzen delako, eta sortzen diren zenbaki berriak n baino txikiagoak direlako, biderketa modularraren definizioari esker:

$$(a \pmod{n}) \cdot (b \pmod{n}) = (a \cdot b) \pmod{n}.$$

- Bestalde, kostu konputazionala txikitu daiteke berreketa bitarraren metodoa erabiliz.

Berreketa bitarraren metodoa

- Berreketaren honako hiru propietateetan oinarritzen da:

$$a^1 = a, \qquad a^{x+y} = a^x a^y, \qquad a^{xy} = (a^x)^y.$$

- a^x berreketa kalkulatzeko, adierazpena behin eta berriz deskonposatzen da, berretzaile guztiak 1 edo 2 izan arte:

$$a^x = \begin{cases} a, & x = 1 \text{ bada,} \\ \left(a^{\frac{x}{2}}\right)^2, & x \text{ bikoitia bada,} \\ a \cdot a^{x-1}, & x \text{ bakoitia bada.} \end{cases}$$

4.44 Adibidea. Kalkula ditzagun ondoko berreturak $\mathbb{Z}_{12}$ multzoan: 3^8 eta 7^9.
Aurreko irizpidea erabiliz, honela deskonposatuko ditugu berreturak:
$3^8 = (3^4)^2 = ((3^2)^2)^2$ eta $7^9 = 7 \cdot 7^8 = 7 \cdot (7^4)^2 = 7 \cdot ((7^2)^2)^2$.

Orain, 3^2 eta 7^2 berreturak kalkulatuko ditugu, eta aurreko adierazpenetan ordezkatu: $81 \equiv 9 \pmod{12}$ eta $7^2 = 49 \equiv 1 \pmod{12}$ dira. Hortaz,

- $3^8 = ((3^2)^2)^2 = ((9)^2)^2 = (81)^2 \equiv (9)^2 = 81 \equiv 9 \pmod{12}$.
- $7^9 = 7 \cdot ((7^2)^2)^2 \equiv 7 \cdot ((1)^2)^2 = 7 \cdot (1)^2 = 7 \cdot 1 = 7 = 7 \pmod{12}$.

Berreketa modularraren kalkuluan hurrengo teoremek lagunduko digute.

4.45 Teorema. *Fermat-en teorema txikia*
Izan bedi $n \in \mathbb{Z}^+$ zenbaki lehena. $a \in \mathbb{Z}^+$ izanik, $a^{n-1} \equiv 1 \pmod{n}$ betetzen da.

4.46 Adibidea. Kalkula dezagun 6^{52} berretura $\mathbb{Z}_{17}$ multzoan.
Aurreko teoremaren arabera, 17 zenbaki lehena denez, $6^{17-1} = 6^{16} \equiv 1 \pmod{17}$ beteko da.
Beraz, 6^{52} berretura 6^{16} berreturaren bidez adieraztea komeniko zaigu. $52 = 3 \cdot 16 + 4$ denez,

$6^{52} = 6^{(3\cdot 16+4)} = 6^{3\cdot 16} \cdot 6^4 = (6^{16})^3 \cdot 6^4 \equiv (1)^3 \cdot 6^4 = 1 \cdot 6^4 = 6^4 = (6^2)^2 = (36)^2 \equiv 2^2 =$
$= 4 \pmod{17}$, $36 \equiv 2 \pmod{17}$ izanik.

Hortaz, $6^{52} \equiv 4 \pmod{17}$ da.

Kasu hori, ordea, oso sinplea da n zenbaki lehena delako. Fermaten emaitza Eulerrek orokortu zuen teorema hauekin.

4.47 Definizioa. Euler-en $\phi(n)$ funtzioa *n moduluko hondarren multzo murriztuak duen elementu kopurua da, hau da, $\mathbb{Z}_n^*$ multzoaren kardinala da: $\phi(n) = \operatorname{card}(\mathbb{Z}_n^*)$.*

4.48 Teorema. *Izan bitez $p, q, n \in \mathbb{Z}$.*

1. *n zenbaki lehena bada, $\phi(n) = n - 1$ da.*
2. *$n = pq$ bada, p eta q bi zenbaki lehen desberdinak izanik, $\phi(n) = (p-1)(q-1)$ da.*
3. *$n = p_1^{e_1} \cdots p_r^{e_r}$ moduan deskonposa badaiteke, $p_1, \ldots, p_r$ zenbaki lehen desberdinak izanik, $\phi(n) = \dfrac{n}{p_1 \cdots p_r}(p_1 - 1) \cdots (p_r - 1)$ da.*

4.49 Teorema. *Eulerren teorema*

Izan bitez $a, n \in \mathbb{Z}^+$ *zenbaki lehen erlatiboak, hots,* $\text{zkh}(a, n) = 1$. *Kasu horretan* $a^{\phi(n)} \equiv 1 \pmod{n}$ *betetzen da.*

4.50 Adibidea. Kalkula dezagun 22^{83} berretura $\mathbb{Z}_{75}$ multzoan.

Aurreko teoremak aplikatzeko, 75 zenbakia deskonposatuko dugu: $75 = 3^1 \cdot 5^2$ da.

Beraz, $\phi(75) = \dfrac{75}{3 \cdot 5}(3-1)(5-1) = \dfrac{75}{15}(2)(4) = 40$ da.

Eulerren teoremak dio $a^{40} \equiv 1 \pmod{75}$ betetzen dela, $\text{zkh}(a, 75) = 1$ bada; gure kasuan, $\text{zkh}(22, 75) = 1$ denez, $22^{40} \equiv 1 \pmod{75}$ da.

Beraz, berreturaren 83 berretzailea honela deskonposatuko dugu: $83 = 2 \cdot 40 + 3$.

Hortaz,

$22^{83} = 22^{(2\cdot 40+3)} = 22^{2\cdot 40} \cdot 22^3 = (22^{40})^2 \cdot 22^3 \equiv (1)^2 \cdot 22^3 = 1 \cdot 22^3 = 22^3 = 22 \cdot (22^2) =$
$= 22 \cdot 484 \equiv 22 \cdot 34 = 748 \equiv 73 \pmod{75}$, $484 \equiv 34 \pmod{75}$ izanik.

Ondorioz, $22^{83} \equiv 73 \pmod{75}$ da.

4.51 Korolarioa. $a, n \in \mathbb{Z}^+$ *badira,* $\text{zkh}(a, n) = 1$ *izanik,* $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$ *betetzen da.*

Froga.

Izan ere, $a^{\phi(n)} = a \cdot a^{\phi(n)-1}$ da eta $a^{\phi(n)} \equiv 1 \pmod{n}$ betetzen da; beraz, $a \cdot a^{\phi(n)-1} \equiv 1 \pmod{n}$ denez, a-ren alderantzizko modularra $a^{\phi(n)-1}$ da. □

4.52 Adibidea. Kalkula ditzagun elementu hauen alderantzizkoak $\mathbb{Z}_{12}$ multzoan:

$$5 \quad \text{eta} \quad 7.$$

Aurreko teoremak aplikatzeko, $\text{zkh}(5, 12) = 1$ eta $\text{zkh}(7, 12) = 1$ betetzen direla egiaztatzen dugu.

Beraz, $5^{-1} \equiv 5^{\phi(12)-1} \pmod{12}$ eta $7^{-1} \equiv 7^{\phi(12)-1} \pmod{12}$ izango dira.

Orain, $\phi(12)$ kalkulatuko dugu: $12 = 2^2 \cdot 3$ denez, $\phi(12) = \dfrac{12}{2 \cdot 3}(2-1)(3-1) =$
$= \dfrac{12}{6}(1)(2) = 4$ da. Hortaz,

- $5^{-1} \equiv 5^{4-1} \pmod{12} = 5^3 = 125 \equiv 5 \pmod{12}$.
- $7^{-1} \equiv 7^{4-1} \pmod{12} = 7^3 = 7 \cdot (7^2) = 7 \cdot 49 \equiv 7 \cdot 1 = 7 \equiv 7 \pmod{12}$.

Emaitza horiek berak 4.43 Adibidean lortu genituen.

Oharrak.

1. Berreketa modularra Euler-en eta Fermat-en teoremak erabiliz kalkulatzea posible bada ere, gehienetan ez da praktikoa.
   - $\phi(n)$ kalkulatzea ez da beti erraza gertatzen, n oso handia denean, zenbaki lehenetan faktorizatzea ez da erraza.
   - Teoremei esker zenbait kasutan berreketa modularraren kalkulua asko laburtzea lortzen da, baina ez beti.
2. Kriptografian, gako publikoko zifratze-algoritmoetan, oso garrantzitsuak gertatzen dira Euler-en eta Fermat-en teoremak

4.3 RSA algoritmoa

RSA algoritmoa mezuak zifratzeko (enkriptatzeko) erabiltzen den sistema kriptografiko bat da. Zenbaki teoriaren eta aritmetika modularraren aplikaziotzat har daiteke.

Algoritmoaren izena bere asmatzaileen izenetatik dator. 1977. urtean, Ronald **R**ivest-ek, Adi **S**hamir-ek eta Leonard **A**dleman-ek sortu zuten.

RSA bidez zifratzeko, gako publikoa eta pribatua sortu behar dira. Horretarako, ezkutuan geratzen diren bi zenbaki lehen erabiltzen dira. Mezuak edonork zifra ditzake gako publikoarekin, baina gako pribatua ezagutzen duenak bakarrik deszifra ditzake

RSA algoritmoaren segurtasuna zenbaki osoen faktorizazioa egiteak praktikan duen zailtasunean oinarritzen da, zenbakiak handiak direnean, ez baita ezagutzen faktorizazioa modu eraginkorrean egiteko gai den algoritmorik.

4.3.1 Oinarri teorikoa

4.53 Teorema. *Izan bedi $n = pq$, p eta q zenbaki lehenak izanik, eta izan bitez e eta d zenbaki osoak $d \equiv e^{-1} \pmod{\phi(n)}$ betetzen dutenak, non $\phi(n) = (p-1)(q-1)$ Eulerren funtzioa den. Orduan, $a^{ed} \equiv a \pmod{n}$ da, $a < \min\{p, q\}$ guztietarako.*

Froga.

$n = pq$ denez, eta p eta q lehenak direnez, $\phi(n) = (p-1)(q-1)$ da (ikus 4.48 Teorema). Bestalde, $d \equiv e^{-1} \pmod{\phi(n)}$ denez, $ed \equiv 1 \pmod{\phi(n)}$ da (ikus 4.40 Definizioa). Ondorioz, $\exists k \in \mathbb{Z}$, non $ed = 1 + k\phi(n)$ den; hau da, $a^{ed} = a^{1+k\phi(n)}$ da $k \in \mathbb{Z}$ baterako.

n moduluko kongruentzian zera daukagu:

$$a^{ed} \equiv a^{1+k\phi(n)} \equiv a(a^{\phi(n)})^k \pmod{n}.$$

Bestalde, $a < \min\{p, q\}$ denez eta $n = pq$ denez, a eta n zenbaki lehen erlatiboak dira, n-ren zatitzaile bakarrak p eta q direlako, biak lehenak izanik. Eulerren teorema aplikatuz, hau da, $a^{\phi(n)} \equiv 1 \pmod{n}$ (ikus 4.49 Teorema) denez,

$$a^{ed} \equiv a(a^{\phi(n)})^k \equiv a(1)^k \equiv a \pmod{n}.$$

□

4.54 Adibidea. Izan bitez $p = 7$ eta $q = 13$ zenbaki lehenak eta izan bitez $d = 29$ eta $e = 5$ non $5 \equiv 29^{-1} \pmod{\phi(7 \cdot 13)}$ den.

$n = pq = 7 \cdot 13 = 91$ da, eta $\phi(n) = \phi(91) = (7-1)(13-1) = 72$ da. Egiazta dezagun $29 \equiv 5^{-1} \pmod{\phi(91)}$ edo $5 \equiv 29^{-1} \pmod{\phi(91)}$ dela. Alegia, 5 eta 29 elkarren alderantzizkoak direla $\phi(91) = 72$ moduluko kongruentzian.

Hona hemen kalkuluak $d = 29$ zenbakirako alderantzizko modularra kalkulatzeko bidea jarraituz (ikus 4.2.1):

$$\begin{array}{r|l} 72 & 29 \\ \cline{2-2} 14 & 2 \end{array} \qquad 72 = 2 \cdot 29 + 14, \qquad 14 = 72 - 2 \cdot 29;$$

$$\begin{array}{r|l} 29 & 14 \\ \cline{2-2} 1 & 2 \end{array} \qquad 29 = 2 \cdot 14 + 1, \qquad 1 = 29 - 2 \cdot 14.$$

Beraz, zkh(29, 72)=1 da eta alderantzizko modularraren existentziaren teoremagatik dakigu $\exists 29^{-1} \pmod{\phi(91)}$ (ikus 4.42 Teorema).

Atzera ordezkatzeak eginez, Bezouten identitatea lortuko dugu:

$$1 = 29 - 2 \cdot 14 = 29 - 2 \cdot (72 - 2 \cdot 29) = 29 \cdot (1 + 4) + (-2) \cdot 72.$$

Hortik,

$$1 = 5 \cdot 29 + (-2) \cdot 72 \quad \rightarrow \quad 5 \cdot 29 = 1 + 2 \cdot 72.$$

Frogatuta geratzen da $d = 29$ eta $e = 5$ bata bestearen alderantzizkoak direla 72 moduluko kongruentzian. Hau da, $de = 1 + k\phi(n)$ da, $k = 2$ izanik.

Egiazta dezagun $a^{ed} \equiv a \pmod{n}$ dela. Eulerrren teorematik $a^{72} \equiv 1 \pmod{91}$ denez (ikus 4.49 Teorema),

$$a^{5 \cdot 29} = a^{1+2 \cdot 72} = a \cdot a^{2 \cdot 72} = a \cdot (a^{72})^2 \equiv a \cdot 1^2 \equiv a \pmod{91}.$$

Ikus dezagun, adibidez, $a = 6$ baliorako $(6^5)^{29} \equiv 6 \pmod{91}$ dela. Berreketaren kalkulurako berreketa bitarrerako metodoa erabiliko dugu (ikus 4.2.2 Atala). Bi urratsetan egingo dugu:

- Lehenik, $a^e \pmod{n} = 6^5 \pmod{91}$ kalkulatuko dugu:
  $6^5 = 6 \cdot (6^2)^2 = 6 \cdot (36)^2 = 6 \cdot 1296 \equiv 6 \cdot 22 = 132 \equiv 41 \pmod{91}$.
- Orain $(a^e)^d \pmod{n}$ kalkulatuko dugu, hau da, $41^{29} \pmod{91}$:
  $41^{29} = 41 \cdot (41^{14})^2 = 41 \cdot ((41^7)^2)^2 = 41 \cdot ((41 \cdot (41^3)^2)^2)^2 = 41 \cdot ((41 \cdot (41 \cdot (41)^2)^2)^2)^2 =$
  $= 41 \cdot ((41 \cdot (41 \cdot 1.681)^2)^2)^2 \equiv 41 \cdot ((41 \cdot (41 \cdot 43)^2)^2)^2 = 41 \cdot ((41 \cdot (1.763)^2)^2)^2 \equiv$
  $\equiv 41 \cdot ((41 \cdot (34)^2)^2)^2 = 41 \cdot ((41 \cdot 1.156)^2)^2 \equiv 41 \cdot ((41 \cdot 64)^2)^2 = 41 \cdot ((2.624)^2)^2 \equiv$
  $\equiv 41 \cdot ((76)^2)^2 = 41 \cdot (5.776)^2 \equiv 41 \cdot (43)^2 = 41 \cdot 1.849 \equiv 41 \cdot 29 = 1.189 \equiv 6 \pmod{91}$.

Espero zitekeen bezala, $(6^5)^{29} \equiv 6 \pmod{91}$ da.

4.3.2 Algoritmoaren urratsak

RSA algoritmoak lau urrats ditu: gakoak sortzea, gako publikoa zabaltzea, mezua zifratzea eta mezua deszifratzea.

Gakoak sortzea

RSA gakoak sortzeko, 4.53 Teoremaren baldintzak betetzen dituzten zenbakiak aukeratu behar dira. Jarraitu beharreko urratsak honakoak dira:

1. Bi zenbaki lehen p eta q aukeratu, $p \neq q$ eta handiak (100 digitutik gorakoak).
2. Kalkulatu $n = pq$ (p eta q handiak diren heinean n-ren faktorizazioa zaila izango da).

3. Gako publikoa kalkulatu (n eta e zenbakiak). $\phi(n) = (p-1)(q-1)$ izanik, $\phi(n)$ zenbakiarekin lehen erlatiboa den e zenbaki bat aurkitu behar da, hau da, zkh($\phi(n)$,e)=1 beteko duena. e handia aukeratzea gomendatzen da.

4. Gako pribatua kalkulatu (d zenbakia). $\phi(n)$ moduluko kongruentzian e gako publikoaren alderantzizkoa den d balioa kalkulatu behar da, hau da, $d = e^{-1} \pmod{\phi(n)}$.

Gako publikoa zabaltzea

Argitara eman zifratzeko behar den gako publikoa, alegia, n eta e zenbakiak. Eta ezkutuan gorde deszifratzeko beharrezkoa den gako pribatua, alegia, d zenbakia.

Mezua zifratzea

a mezua RSA algoritmoaren bidez zifratzea, (n, e) gako publikoa erabiliz honako berreketa modularra kalkulatzea da:

$$z \equiv a^e \pmod{n}.$$

Horrela z mezu zifratua lortzen da.

Mezua deszifratzea

z mezu zifratua RSA algoritmoaren bidez deszifratzea honako berreketa modularra kalkulatzea da, d gako pribatua eta publikoa den n erabiliz:

$$a \equiv z^d \pmod{n}.$$

Aukeratu ditugun gakoek 4.53 Teoremaren baldintzak betetzen dituztenez,

$$a \equiv z^d \equiv (a^e)^d \pmod{n}$$

betetzen da, eta ondorioz z zifratutako mezua deszifratu eta a mezu originala berreskuratzea lortzen da.

4.55 Adibidea. Begoñak Asierri "kaixo"mezua bidali nahi dio zifratuta, RSA zifratze-algoritmoa erabiliz. Algoritmoaren segurtasuna bermatzeko zenbaki oso handiak erabili behar diren arren, kalkuluak errazteko zenbaki txikiak erabiliko ditugu:

Gakoak sortzea

Asierrek gakoak sortuko ditu mezu zifratua jaso ahal izateko.

1. $p = 17$ eta $q = 23$ zenbaki lehenak aukeratu ditu.

2. $n = p \cdot q = 17 \cdot 23 = 391 \quad \rightarrow \quad \boxed{n = 391}$.

3. Gako publikoa (n, e). $n = 391$ zenbakirako e egoki bat aukeratu behar du.

   - $\phi(n) = (p-1)(q-1) = 16 \cdot 22 = 352 \quad \rightarrow \quad \phi(n) = 352.$

- $\text{zkh}(\phi(n), e) = 1 \quad \rightarrow \quad \text{zkh}(352, e) = 1.$
  e baliorako aukera bat baino gehiago existitzen da. $\phi(n)$ zenbakiarekin lehen erlatiboa den zenbaki handi bat aukeratzea gomendatzen bada ere, berak txikiena aukeratu du: $\boxed{\text{e=3}}$.

4. Gako pribatua (d). Alderantzizko modularra kalkulatzeko bidea jarraituz egiazta daiteke $\boxed{\text{d=235}}$ dela, hau da, $3 \cdot 235 \equiv 1 \pmod{352}$.

Oharra. Gako publikoko n zenbakia txikia da, eta faktorizatuz p eta q erraz kalkula daitezke. n faktorizatzea lortzen denean, sistema kriptografikoak porrot egin duela esaten da. Izan ere, e publikoa denez, goiko kalkulu guztiak egin daitezke eta d gako pribatua kalkulatu.

Gako publikoa zabaltzea

Asierrek $n = 391$ eta $e = 3$ balioak publiko egingo ditu eta $d = 235$ gako pribatua ezkutuan gordeko du. Bere gako publikoak eta RSA zifratze-algoritmoa erabiliz zifratutako mezuak jasotzeko prest dago.

Mezua zifratzea ($a_i \rightarrow z_i$)

Begoñak Asierren gako publikoa erabiliz "kaixo"mezua zifratu behar du. baina, zifratzeak eskatzen duen berreketa modularra kalkulatu ahal izateko, nahitaezkoa da mezua zifratu aurretik kodetzea, hau da, karakterez osatuta dagoen mezu originala zenbakietara bihurtzea.

Kodeketa erabiliena ASCII kodeketa da. "kaixo"mezuaren karaktereei dagozkien kodeak honakoak dira: 107, 97, 105, 120, 111. Kalkuluak hauek dira:

- $a_1 = 107 \quad \Longrightarrow \quad z_1 = a_1^e \pmod{n} = 107^3 \pmod{391} = 40.$
- $a_2 = 97 \quad \Longrightarrow \quad z_2 = a_2^e \pmod{n} = 97^3 \pmod{391} = 79.$
- $a_3 = 105 \quad \Longrightarrow \quad z_3 = a_3^e \pmod{n} = 105^3 \pmod{391} = 265.$
- $a_4 = 120 \quad \Longrightarrow \quad z_4 = a_4^e \pmod{n} = 120^3 \pmod{391} = 171.$
- $a_5 = 111 \quad \Longrightarrow \quad z_5 = a_5^e \pmod{n} = 111^3 \pmod{391} = 304.$

Begoñak Asierri $(40, 79, 265, 171, 304)$ mezu zifratua bidaliko dio.

Mezua deszifratzea ($z_i \rightarrow a_i$)

Asierrek mezu zifratua deszifratuko du bere $d = 235$ gako pribatua erabiliz.

- $z_1 = 40 \quad \Longrightarrow \quad a_1 = z_1^d \pmod{n} = 40^{235} \pmod{391} = 107.$
- $z_2 = 79 \quad \Longrightarrow \quad a_2 = z_2^d \pmod{n} = 79^{235} \pmod{391} = 97.$
- $z_3 = 265 \quad \Longrightarrow \quad a_3 = z_3^d \pmod{n} = 265^{235} \pmod{391} = 105.$
- $z_4 = 171 \quad \Longrightarrow \quad a_4 = z_4^d \pmod{n} = 171^{235} \pmod{391} = 120.$

- $z_5 = 304 \quad \Longrightarrow \quad a_5 = z_5^d \pmod{n} = 304^{235} \pmod{391} = 111.$

Deszifratu ondoren, mezua ASCII kodeetan lortu du $(107, 97, 105, 120, 111)$, eta ASCII kodeak karaktere bihurtuz, "kaixo"mezu originala lortu du.

Oharra. Adibide honetan ez da betetzen 4.53 Teoremako $a < \min\{p, q\}$ baldintza, Asierrek $p = 17$ eta $q = 23$ zenbaki lehenak txikiegiak aukeratu dituelako. Dena den, Eulerren teoremaren baldintza betetzen da, $\text{zkh}(a_i, n) = 1$ betetzen delako adibideko a_i guztietarako.

4.3.3 Mezu ziurtatuetarako erabilera

RSA gakoek beste erabilera bat ere badute: mezu ziurtatua bidaltzeko aukera ematen dute. Alegia, mezua sortu duena nor izan den ziurtatzeko aukera ematen dute. Mezua sinatzearen pareko prozesua da.

Mezua sinatzeko gako pribatuarekin zifratu behar da. Hori gakoen jabeak baino ezin du egin, berak bakarrik ezagutzen baitu d gakoa. Gakoen jabeak (sinatzaileak) a mezua sinatzeko

$$z \equiv a^d \pmod{n}$$

mezu sinatua sortuko du. z mezu ziurtatu hori edonork deszifra dezake sinatzailearen beraren gako publikoak erabiliz:

$$a = z^e \pmod{n}.$$

Horrela, mezu hori gakoen jabe den sinatzaileak sortua dela ziurtatzen da.

5. Kapitulua

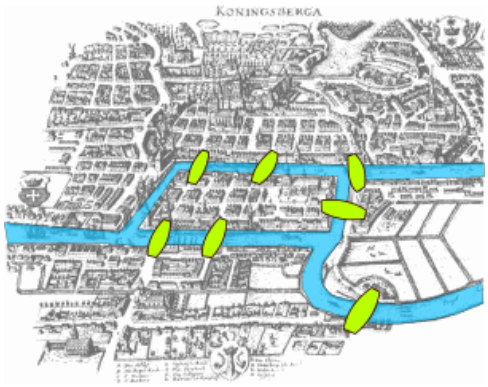
Grafoak

5.1 Sarrera

XVIII. mendean Königsberg (gaur Kaliningrado, Errusia) hiritik Pregel ibaia pasatzen zen, eta bi irla osatzen zituen. Ibaiaren ertzak eta irlak zazpi zubiz zeuden loturik. Biztanleek ibilbideak egiten zituzten etxetik atera, zubietatik behin bakarrik pasatu eta etxera bueltatzen saiatzen; baina ez zuten lortzen.

Istorio hura Leonhard Euler-en eskuetara heldu zen, eta 1736an eman zion soluzioa artikulu batean: ezinezkoa zen.

Euler konturatu zen problemaren soluzioa ez zegoela distantziaren mende. Orduan, problema aztertzeko, lur-eremu bakoitzari puntu bat eta zubi bakoitzari lerro bat egokitu zien. Hortik aurrera Eulerrek Grafo-Teoriaren oinarrizko kontzeptuak landu zituen. Horrela jaio zen Grafo-Teoria.



Grafo-Teoria elementu-kopuru finitua duten problemak islatzeko erabili da. Lehendabizi, problema grafo baten bidez adierazten da; gero, grafoaren propietateak aztertzen dira; azkenik, problemaren soluzioa ondorioztatzen da.

Grafo-Teoriaren aplikazio asko aurki ditzakegu Informatikan: datuen adierazpena, sareen diseinua, zirkuitu integratuen diseinua...

5.2 Definizioak

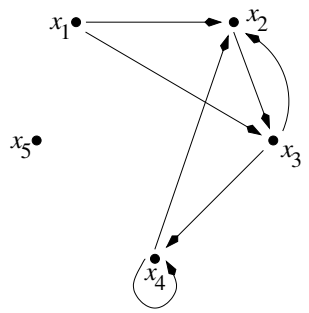
5.1 Definizioa. *(V-ren gaineko)* grafo zuzendua (V, E) *bikote bat da, non V multzo finitu ez-hutsa den, eta $E \subseteq V \times V$.*

V multzoaren elementuei erpin *edo* adabegi *deituko diegu, eta E multzoaren elementuei* ertz.

5.2 Adibidea. Diagrama honekin adieraziko dugu 5 erpin eta 7 ertz dituen grafo zuzendu bat:

$$V = \{x_1, x_2, x_3, x_4, x_5\},$$

$$E = \{(x_1, x_2), (x_1, x_3), (x_2, x_3), (x_3, x_2), (x_3, x_4), (x_4, x_2), (x_4, x_4)\}.$$



5.3 Definizioa. (a, b) *ertza izanik, kontzeptu hauek erabiliko ditugu:*

- *ertza* intzidentea *da a eta b erpinekin.*
- *a eta b erpinak elkarren* auzokideak *dira.*
- *a erpina ertzaren* jatorria *da.*
- *b erpina ertzaren* amaiera *da.*

$a = b$ bada, (a, a) ertzari begizta *deituko diogu.*

a erpin isolatua *da ez badu ertz intzidenterik.*

5.4 Definizioa. *Ertzen noranzkoak ez badu garrantzirik, hau da,*

$$(a, b) \in E \implies (b, a) \in E,$$

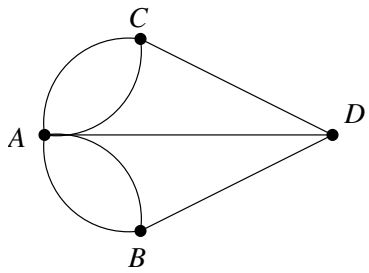
$G = (V, E)$ grafoa ez-zuzendua *dela esango dugu.*

Grafo ez-zuzendu batean ertzak ez-zuzenduak *dira: $\{a, b\} = \{(a, b), (b, a)\}$.*

Eta $a = b$ bada, begizta *bat izango dugu: $\{a, a\} = (a, a)$.*

Oharra. Ez bada ezer esaten, grafoa ez-zuzendua izango da.

5.5 Adibidea. Hona hemen Königsbergeko zubien problemari dagokion grafoa: lau lureremuak erpinak dira, eta zubiak ertzak:

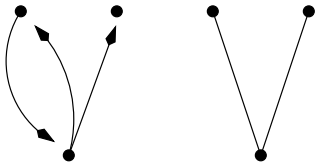


Grafoak 7 ertz ez-zuzendu ditu: $\{A, B\}$, $\{A, B\}$, $\{A, C\}$, $\{A, C\}$, $\{A, D\}$, $\{B, D\}$ eta $\{C, D\}$.

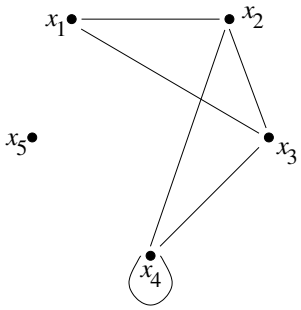
5.6 Definizioa. $G = (V, E)$ *grafo zuzendu bat izanik,* grafo ez-zuzendu elkartua G *grafotik lortzen da ertzen noranzkoa kontuan izan gabe. Bi erpinekin intzidenteak diren ertz bat baino gehiago lortzen badira, horietako bat bakarrik hartuko dugu kontuan.*

5.7 Adibideak.

1. Hona hemen grafo zuzendu bat eta bere grafo ez-zuzendu elkartua.



2. Hau da 5.2 Adibideko grafoaren grafo ez-zuzendu elkartua:



5.8 Definizioa. $G = (V, E)$ *grafoa* multigrafoa *da* $a, b \in V$ *erpinak badaude bi edo ertz intzidente gehiagorekin:*

- (a, b) *grafo zuzenduetan.*
- $\{a, b\}$ *grafo ez-zuzenduetan.*

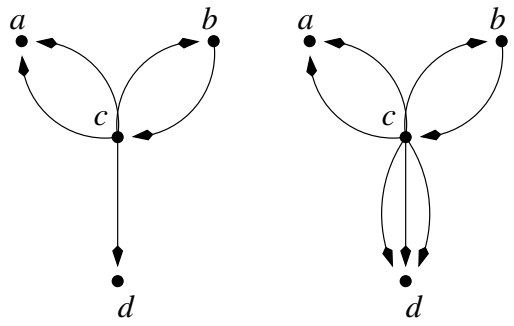
(a, b) ($\{a, b\}$) *moduko ertzen kopurua* (a, b) ($\{a, b\}$) *ertzaren* anizkoiztasuna *da.*

Grafo bat k-grafoa *da bere ertz batek ere ez badu* k *baino anizkoiztasun handiagoa.*

Grafo bat bakuna *da ez bada multigrafoa, hots, bere ertz guztiek* 1 *anizkoiztasuna badute.*

5.9 Adibideak.

1. Hona hemen bi multigrafo: lehena 2-grafo zuzendua da, eta bigarrena 3-grafo zuzendua.



2. Königsbergeko zubien problemaren grafoa (5.5 Adibidea) 2-grafo ez-zuzendua da.

3. 5.7 Adibideko grafoak bakunak dira.

5.3 Erpinen graduak

5.10 Definizioa. *Izan bedi $G = (V, E)$ grafo zuzendua, eta $a \in V$.*

- *a erpinaren* irteera-gradua *a-tik ateratzen diren ertzen kopurua da, $d^+(a)$ adierazten da:*
$$d^+(a) = \text{card}\{b \,/\, (a, b) \in E\}.$$

- *a erpinaren* sarrera-gradua *a-ra iristen diren ertzen kopurua da, $d^-(a)$ adierazten da:*
$$d^-(a) = \text{card}\{b \,/\, (b, a) \in E\}.$$

$d^+(a)$ eta $d^-(a)$ a erpinaren graduerdi *deitzen dira, eta a erpinaren graduerdien baturari a-ren* gradu *deituko diogu, $d(a)$ adierazten da:*

$$d(a) = d^+(a) + d^-(a).$$

5.11 Adibidea. 5.2 Adibideko grafoan,

$d^+(x_1) = 2$, $d^+(x_2) = 1$, $d^+(x_3) = 2$, $d^+(x_4) = 2$, $d^+(x_5) = 0$.
$d^-(x_1) = 0$, $d^-(x_2) = 3$, $d^-(x_3) = 2$, $d^-(x_4) = 2$, $d^-(x_5) = 0$.
$d(x_1) = 2$, $d(x_2) = 4$, $d(x_3) = 4$, $d(x_4) = 4$, $d(x_5) = 0$.

5.12 Definizioa. *$G = (V, E)$ grafo ez-zuzendua eta $a \in V$ izanik, a erpinaren* gradua *a-rekin intzidenteak diren ertzen kopurua da, eta $d(a)$ adieraziko dugu.*

Kasu honetan, $\{a, a\}$ begizta a-rekin intzidenteak diren bi ertz bezala kontatzen da.

a erpina zintzilikatua *da $d(a) = 1$ denean.*

5.13 Adibideak.

1. Königsbergeko zubien problemaren grafoan (5.5 Adibidea),

$$d(A) = 5, \quad d(B) = d(C) = d(D) = 3.$$

2. 5.7-2 Adibideko grafoan,

$$d(x_1) = 2, \quad d(x_2) = d(x_3) = 3, \quad d(x_4) = 4, \quad d(x_5) = 0.$$

5.14 Teorema. *Izan bedi $G = (V, E)$ m ertz dituen grafo ez-zuzendua. Orduan,*

$$\sum_{x \in V} d(x) = 2m.$$

Froga.
(Ideia: $\{a, b\}$ ertz bakoitzak unitate bat eransten dio $d(a)$ graduari, eta beste bat $d(b)$ graduari, eta, hortaz, bi unitate $\sum_{x \in V} d(x)$ baturari, hau da, erpinen graduen batura kalkulatzean, bi aldiz kontatzen ditugu grafoaren ertzak.)

Froga m ertz kopuruaren gaineko indukzioaz egingo dugu.
$m = 1$ bada, G grafoak $e = \{a, b\}$ ertz bakarra du.
$a \neq b$ bada,

$$\begin{cases} d(a) = 1, \\ d(b) = 1, \\ d(y) = 0, \quad a \neq y \neq b \text{ bada.} \end{cases}$$

$a = b$ bada,

$$\begin{cases} d(a) = 2, \\ d(y) = 0, \quad y \neq a \text{ bada.} \end{cases}$$

Bi kasuetan,

$$\sum_{x \in V} d(x) = 2 = 2m.$$

Demagun, orain, teorema betetzen dela $m = p$ denean, eta har dezagun $m = p + 1$.
Izan bedi $e = \{a, b\} \in E$ G grafoaren ertz bat eta izan bedi G' grafoa G grafotik e ertza kentzean geratzen den grafoa. G' grafoaren ertzen kopurua m' bada, eta $d'(x)$ bada x erpinaren gradua G' grafoan, $m' = p$ izango da. Eta, indukzio-hipotesiaren arabera,

$$\sum_{x \in V} d'(x) = 2m' = 2p.$$

Horrez gain, $a \neq b$ bada,

$$\begin{cases} d(a) = d'(a) + 1, \\ d(b) = d'(b) + 1, \\ d(y) = d'(y), \qquad a \neq y \neq b \text{ bada.} \end{cases}$$

Eta $a = b$ bada,

$$\begin{cases} d(a) = d'(a) + 2, \\ d(y) = d'(y), \qquad y \neq a \text{ bada.} \end{cases}$$

Bi kasuetan,

$$\sum_{x\in V} d(x) = \sum_{x\in V} d'(x) + 2 = 2p + 2 = 2(p+1) = 2m.$$

□

5.15 Adibideak.

1. Königsbergeko zubien problemaren grafoan (5.5 Adibidea), $n = 4$, $m = 7$,

$$d(A) + d(B) + d(C) + d(D) = 5 + 3 + 3 + 3 = 14 = 2 \cdot 7.$$

2. 5.7-2 Adibideko grafoan, $n = 5$, $m = 6$,

$$d(x_1) + d(x_2) + d(x_3) + d(x_4) + d(x_5) = 2 + 3 + 3 + 4 + 0 = 12 = 2 \cdot 6.$$

5.16 Korolarioa. *Izan bedi $G = (V, E)$ grafo ez-zuzendua. Gradu bakoitiko erpinen kopurua bikoitia da.*

Froga.
Izan bedi $V = \{x_1, \ldots, x_n\}$ eta demagun badaudela gradu bikoitiko p erpin eta gradu bakoitiko q erpin ($p + q = n$).

$$\begin{aligned} d(x_i) &= 2k_i, & i &= 1, \ldots, p; \\ d(x_i) &= 2k_i + 1, & i &= p+1, \ldots, p+q. \end{aligned}$$

Orduan,

$$2m = \sum_{x\in V} d(x) = \sum_{i=1}^{p} d(x_i) + \sum_{i=p+1}^{p+q} d(x_i) = \sum_{i=1}^{p} (2k_i) + \sum_{i=p+1}^{p+q} (2k_i + 1) = 2\sum_{i=1}^{p+q} k_i + q.$$

Hortaz,

$$q = 2\left(m - \sum_{i=1}^{p+q} k_i\right).$$

□

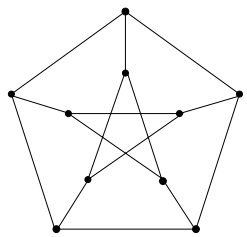
5.17 Adibideak.

1. Königsbergeko zubien problemaren grafoan (5.5 Adibidea) gradu bakoitiko 4 erpin daude (A, B, C eta D).

2. 5.7-2 Adibideko grafoan gradu bakoitiko 2 erpin daude (x_2 eta x_3).

5.18 Definizioa. *Grafo ez-zuzendu bat* erregular *deitzen da erpin guztiek gradu bera badute; eta k-*erregular *deitzen da erpin guztiek k gradua badute.*

5.19 Adibidea. Grafo hau 3-erregularra da:



5.4 Ibilaldiak grafo batean

5.20 Definizioa. *Izan bedi $G = (V, E)$ grafo ez-zuzendua. $x, y \in V$ bi erpin badira, $x - y$* ibilaldia *x erpinean hasi eta y erpinean bukatzen den erpinen eta ertzen segida txandakatu finitu bat da:*

$$x = x_0, e_1, x_1, e_2, x_2, e_3, \ldots, e_{p-1}, x_{p-1}, e_p, x_p = y,$$

$e_i = \{x_{i-1}, x_i\}$ ertza izanik, $i = 1, \ldots, p$.

Ibilaldiaren luzera *ertzen kopurua da, p. Eta $p = 0$ bada, $x = y$ izango da eta* ibilaldi nabaria *izango dugu.*

$x = y$ eta $p \geq 1$ badira, ibilaldi itxia *da; bestela,* ibilaldi irekia *da.*

Oharra. Grafoa bakuna denean, ibilaldi bat adieraztean ertzak ez ditugu idatziko.

5.21 Adibidea. 5.7-2 Adibideko grafoan, x_1, x_3, x_2 ibilaldi irekia da, 2 luzerako $x_1 - x_2$ ibilaldia hain zuzen: $x_1, \{x_1, x_3\}, x_3, \{x_3, x_2\}, x_2$.

Beste hau, ordea, 6 luzerako ibilaldi itxia da: $x_1, x_3, x_2, x_4, x_3, x_2, x_1$.

5.22 Definizioa. *Izan bedi $x - y$ ibilaldi bat $G = (V, E)$ grafo ez-zuzenduan,*

- *Ertzik ez bada errepikatzen, $x - y$ ibilaldiari* kate *deituko diogu. Katea itxia denean, $x - x$ ibilaldi itxiari* zirkuitu *deituko diogu.*
- *Erpinik ez bada errepikatzen, $x - y$ ibilaldiari* bide *deituko diogu. Bidea itxia denean, $x - x$ ibilaldi itxiari* ziklo *deituko diogu.*

Hitzarmena. Zirkuituetan, gutxienez ertz bat existitzen dela pentsatuko dugu; eta bat bakarrik dagoenean, zirkuitua begizta izango da. Zikloetan, gutxienez hiru ertz desberdin daudela pentsatuko dugu.

5.23 Adibidea. 5.7-2 Adibideko grafoan,
x_1, x_2, x_3 katea eta bidea da;
x_1, x_3, x_2, x_4, x_3 katea da, baina ez da bidea;
x_1, x_2, x_3, x_1 zirkuitua eta zikloa da.

Grafo zuzenduetan *zuzendu* adjektiboa erabiliko dugu: *ibilaldi zuzenduak*, *bide zuzenduak*, *ziklo zuzenduak*, etab.

5.24 Teorema. *Izan bedi $G = (V, E)$ grafo ez-zuzendua eta izan bitez $x, y \in V$, $x \neq y$. Orduan,*

$x - y$ ibilaldi bat badago baldin eta soilik baldin $x - y$ bide bat badago.

Froga.

Demagun $x - y$ ibilaldiren bat dagoela. x eta y-ren arteko ibilaldi guztien artean, har dezagun luzera txikieneko ibilaldia:

$$x = x_0, x_1, \ldots, x_{k-1}, x_k = y.$$

Ibilaldi hori ez bada bidea, $\exists p, q \ / \ 0 \leq p < q \leq k$ eta $x_p = x_q$. Baina, orduan,

$$x = x_0, x_1, \ldots, x_{p-1}, x_q, x_{q+1}, \ldots, x_k = y$$

x eta y-ren arteko beste ibilaldi bat da, eta k baino luzera txikiagokoa da.

Azken ibilaldi hori ez balitz bidea, berdin egingo genuke: errepikatzen den erpinaren bi agerpenen arteko zatia kendu eta luzera txikiagoko ibilaldi berri bat lortuko genuke. Horrela segi daiteke erpinak errepikatzen ez diren arte, hots, bide bat lortu arte.

Elkarrekikoa berehalakoa da; izan ere, bide bat ibilaldi bat da. □

5.25 Definizioa. $G = (V, E)$ *grafo ez-zuzendua* konexua *da edozein x eta y bi erpin desberdinetarako $x - y$ ibilaldi bat badago.*

$G = (V, E)$ *grafo zuzendua* konexu *da grafo ez-zuzendu elkartua konexua bada.*

Grafo bat ez bada konexua, diskonexua *da.*

Aurreko teoremaren arabera, horrek esan nahi du grafo ez-zuzendua konexua dela edozein x eta y bi erpin desberdinetarako $x - y$ bide bat badago.

5.26 Adibidea. 5.19 Adibideko grafoa konexua da.

5.7-1 Adibideko grafoak konexuak dira.

5.2 Adibideko grafoa eta 5.7-2 Adibideko grafo elkartua diskonexuak dira, ez dagoelako, esaterako, $x_1 - x_5$ biderik.

5.27 Teorema. *Izan bedi $G = (V, E)$ grafo ez-zuzendua; $\mathcal{R}$ erlazioa,*

$$x\mathcal{R}y \iff x - y \text{ bide bat badago},$$

baliokidetasun-erlazioa da V multzoaren gainean.

Froga.

- $\mathcal{R}$ bihurkorra da. Hau frogatu behar dugu:

$$(\forall x \in V) \quad x\mathcal{R}x.$$

$\forall x \in V$, $x - x$ ibilaldi nabaria dago; hortaz, $x\mathcal{R}x$.

- $\mathcal{R}$ simetrikoa da. Hau frogatu behar dugu:

$$(\forall x, y \in V) \quad x\mathcal{R}y \implies y\mathcal{R}x.$$

$x, y \in V$ badira,

$$\begin{aligned} &x\mathcal{R}y \implies x = x_0, x_1, \ldots, x_{p-1}, x_p = y \text{ ibilaldia badago} \implies \\ &\implies y = x_p, x_{p-1}, \ldots, x_1, x_0 = x \text{ ibilaldia badago} \implies y\mathcal{R}x. \end{aligned}$$

- $\mathcal{R}$ iragankorra da. Hau frogatu behar dugu:

$$(\forall x, y, z \in V) \quad x\mathcal{R}y \wedge y\mathcal{R}z \implies x\mathcal{R}z.$$

$x, y, z \in V$ badira,

$$\begin{aligned} &x\mathcal{R}y \wedge y\mathcal{R}z \implies \\ &\implies x = x_0, \ldots, x_p = y \ \wedge \ y = y_0, \ldots, y_q = z \text{ ibilaldiak badadaude} \implies \\ &\implies x = x_0, \ldots, x_p = y = y_0, y_1, \ldots, y_q = z \text{ ibilaldia badago} \implies x\mathcal{R}z. \end{aligned}$$

□

5.28 Definizioa. *5.27 Teoreman definitutako baliokidetasun-erlazioak erpinen V multzoa $V_1, \ldots, V_q$ baliokidetasun-klasetan banatzen du. $G_1 = (V_1, E_1)$, ..., $G_q = (V_q, E_q)$ grafoei, non E_i, $i = 1, \ldots, q$, V_i multzoaren erpinekin intzidenteak diren ertzen multzoak diren, G grafoaren* osagai konexu *deituko diegu.*

G grafoaren osagai konexuen kopurua $\kappa(G)$ adieraziko dugu.

Ondorioa. G grafoa konexua da baldin eta soilik baldin $\kappa(G) = 1$ bada.

5.29 Adibidea. 5.7-2 Adibideko grafoak 2 osagai konexu ditu, $\kappa(G) = 2$:

$G_1 = (V_1, E_1)$, non

$$V_1 = \{x_1, x_2, x_3, x_4\},\ E_1 = \{\{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_2, x_4\}, \{x_3, x_4\}, \{x_4, x_4\}\} \text{ diren;}$$

eta $G_2 = (V_2, E_2)$, non

$$V_2 = \{x_5\},\ E_2 = \emptyset \text{ diren.}$$

5.5 Grafo baten auzokidetasun-matrizea

5.30 Definizioa. *Izan bedi $G = (V, E)$ grafo bakun ez-zuzendua, begiztarik gabea eta n erpinekin, non $V = \{x_1, \ldots, x_n\}$ den. G grafoari dagokion* auzokidetasun-matrizea *honela definituko dugu: $A = (a_{ij})$, $i, j = 1, ..., n$,*

$$a_{ij} = \begin{cases} 1, & x_i \text{ eta } x_j \text{ auzokideak badira,} \\ 0, & x_i \text{ eta } x_j \text{ ez badira auzokideak.} \end{cases}$$

A matrizea simetrikoa da eta diagonal nagusiko elementu guztiak 0 dira. G grafoaren egituraren informazio osoa du, eta G adierazteko erabil dezakegu.

$x_i \in V$ erpin bakoitzeko hau betetzen da:

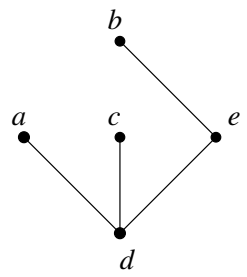
$$d(x_i) = \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} a_{ji}.$$

5.31 Adibideak.

1. 5.7-2 Adibideko grafoaren auzokidetasun-matrizea (begizta kenduta) hau da:

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

2. Hona hemen grafo bakun ez-zuzendu bat, begiztarik gabea:



Grafoaren auzokidetasun-matrizea (erpinak ordena alfabetikoan hartuta) hau da:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Bosgarren errenkadako edo zutabeko elementuen batura 2 da; hau da, $d(e) = 2$.

5.32 Teorema. *Izan bitez $G = (V, E)$ grafo bakun ez-zuzendua, begiztarik gabea, $V = \{x_1, \ldots, x_n\}$ erpinak eta grafoari dagokion A auzokidetasun-matrizea. A^p matrizearen (i, j) elementua p luzerako $x_i - x_j$ ibilaldien kopurua da.*

Froga.

p-ren gaineko indukzioaren bidez frogatuko dugu.

$p = 1$ bada, $A^p = A$ izango da; eta 1 luzerako $x_i - x_j$ ibilaldien kopurua hau da:

$$\begin{cases} 1, & \{x_i, x_j\} \in E \text{ bada,} \\ 0, & \{x_i, x_j\} \notin E \text{ bada;} \end{cases}$$

hau da, A matrizearen (i, j) elementua.

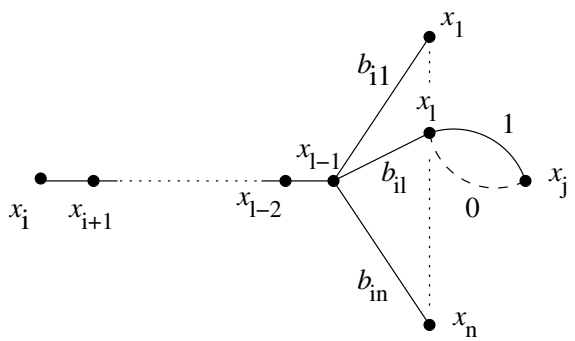
Demagun Teorema betetzen dela $p = k$ denean, hau da, A^k matrizearen (i, j) elementua k luzerako $x_i - x_j$ ibilaldien kopurua dela; ikus dezagun $p = k + 1$ denean ere betetzen dela. Hau da, A^{k+1} matrizearen (i, j) elementua $k + 1$ luzerako $x_i - x_j$ ibilaldien kopurua dela frogatu behar dugu.

Izan bitez $A^k = (b_{ij})$ eta $A^{k+1} = (c_{ij})$.

Orduan, $A^{k+1} = A^k A$ denez, hau beteko da:

$$c_{ij} = \sum_{l=1}^{n} b_{il} a_{lj}.$$

$k + 1$ luzerako $x_i - x_j$ ibilaldi bakoitza k luzerako $x_i - x_l$ ibilaldi batek eta, jarraian, $\{x_l, x_j\}$ ertz batek osatuko dute, non x_l erpina ($l \in \{1, \ldots, n\}$) edozein erpin den.



- $\{x_l, x_j\} \in E$ bada, $a_{lj} = 1$ izango da A matrizean; beraz, $k+1$ luzerako eta $x_i = y_0, y_1, \ldots, y_k = x_l, y_{k+1} = x_j$ itxurako $x_i - x_j$ ibilaldien kopurua k luzerako $x_i - x_l$ ibilaldien kopurua izango da, hots, $b_{il} = b_{il}a_{lj}$.

- Ordea, $\{x_l, x_j\} \notin E$ bada, $a_{lj} = 0$ izango da A matrizean; beraz, $k+1$ luzerako eta $x_i = y_0, y_1, \ldots, y_k = x_l, y_{k+1} = x_j$ itxurako ibilaldien kopurua $0 = b_{il}a_{lj}$ izango da.

Hortaz, $k+1$ luzerako $x_i - x_j$ ibilaldi guztien kopurua hau da:

$$\sum_{l=1}^{n} b_{il}a_{lj} = c_{ij}.$$

□

5.33 Adibidea. 5.31-2 Adibideko grafoaren auzokidetasun-matrizerako hau dugu:

$$A^3 = \begin{pmatrix} 0 & 1 & 0 & 3 & 0 \\ 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 3 & 0 \\ 3 & 0 & 3 & 0 & 4 \\ 0 & 2 & 0 & 4 & 0 \end{pmatrix}$$

Ez dago 3 luzerako $a - c$ ibilaldirik a eta c artean; badaude 3 luzerako lau ibilaldi d eta e artean:

$$d, a, d, e; \quad d, c, d, e; \quad d, e, d, e; \quad \text{eta} \quad d, e, b, e.$$

5.6 Azpigrafoak. Grafo osagarria

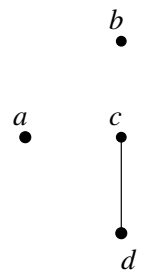
5.34 Definizioa. *Izan bedi $G = (V, E)$ grafo bat (zuzendua edo ez). $G_1 = (V_1, E_1)$ grafoa G grafoaren* azpigrafo *bat da bi baldintza hauek betetzen baditu:*

- $\emptyset \neq V_1 \subseteq V$ *eta*

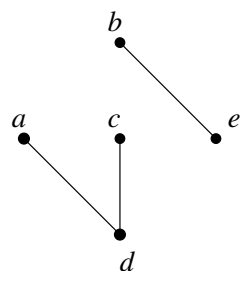
- $E_1 \subseteq E$ *eta E_1 multzoaren ertz bakoitzak intzidente izan behar du V_1 multzoaren erpinekin soilik.*

5.35 Adibidea. 5.31-2 Adibideko grafoa izanik, grafo hauek bere azpigrafoak dira:

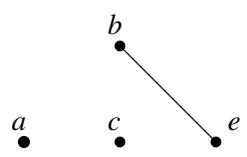
G_1



G_2



G_3



5.36 Definizioa. *$G_1 = (V_1, E_1)$ grafoa $G = (V, E)$ grafoaren azpigrafoa bada eta $V_1 = V$ bada, G_1 grafoa G grafoaren* azpigrafo sortzailea *dela esango dugu.*

Ertzen azpimultzo bakoitzeko azpigrafo sortzaile bat lortuko dugu. Beraz, $G = (V, E)$ grafoan $|E| = m$ bada, 2^m azpigrafo sortzaile izango ditu.

5.37 Adibidea. 5.35 Adibidean, G grafoaren G_2 azpigrafo sortzailea da; baina, G_1 eta G_3 ez dira azpigrafo sortzaileak.

G grafoak $2^4 = 16$ azpigrafo sortzaile ditu.

5.38 Definizioa. *Izan bitez $G = (V, E)$ grafo bat (zuzendua edo ez) eta $\emptyset \neq U \subset V$ multzo bat. U multzoak G grafoan honela definitzen duen azpigrafoari* azpigrafo induzitu *deituko diogu:*

- *erpinen multzoa U da eta*
- *ertzen multzoa $E \cap (U \times U)$ da (hots, U multzoaren erpinekin soilik intzidenteak diren E multzoaren ertzak).*

Azpigrafo induzitua $< U >$ adieraziko dugu.

5.39 Adibidea. 5.35 Adibidean, G_3 azpigrafo induzitua da, $V_3 = \{a, b, c, e\}$ multzoak induzitutakoa hain zuzen.

$$G_3 =< V_3 > .$$

G_1 ez da $V_1 = \{a, b, c, d\}$ multzoak induzitutako azpigrafoa, $\{a, d\}$ ertza ez dago eta.

Ikus ditzagun, orain, beste bi azpigrafo mota, erpin bat edo ertz bat kentzean sortutakoak.

5.40 Definizioa. *Izan bedi $G = (V, E)$ grafo bat (zuzendua edo ez).*

- *$x \in V$ izanik, $G - x$ idatziko dugu $G - x = (V_1, E_1)$ azpigrafoa adierazteko, non:*
  - *$V_1 = V \setminus \{x\}$ den eta*
  - *E_1 multzoan E multzoaren ertz guztiak dauden, x erpinarekin intzidenteak direnak izan ezik.*

  Hortaz, $G - x =< V_1 >$ grafo induzitua dugu.

- *$e \in E$ izanik, $G - e$ idatziko dugu $G - e = (V_1, E_1)$ azpigrafoa adierazteko, non:*
  - *$V_1 = V$ den eta*
  - *$E_1 = E \setminus \{e\}$ den.*

5.41 Adibidea. 5.35 Adibidean, $G_3 = G - d$ eta $G_2 = G - \{d, e\}$ dira.

Grafo baten grafo osagarria definitu ahal izateko grafo osotuaren kontzeptua behar dugu.

5.42 Definizioa. *Izan bedi $V = \{x_1, \ldots, x_n\}$ erpinen multzoa. V multzoaren gaineko* grafo osotua *grafo bakun, ez-zuzendu eta begiztarik gabea da, non*

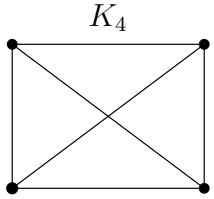
$$(\forall x, y \in V) \quad x \neq y \implies \{x, y\} \text{ ertza ezistitzen den.}$$

n erpineko grafo osotua K_n adieraziko dugu.

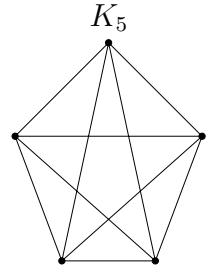
Ohar gaitezen K_n grafoak n erpin eta $\binom{n}{2}$ ertz dituela, eta erpin bakoitzaren gradua $n - 1$ dela.

5.43 Adibideak.

K_4



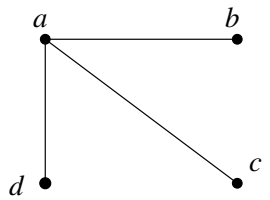
K_5



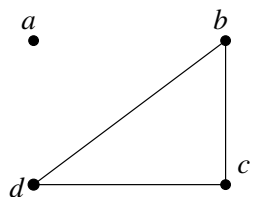
5.44 Definizioa. *Izan bedi $G = (V, E)$ grafo bakuna, ez-zuzendua, begiztarik gabea eta n erpin dituena, $V = \{x_1, \ldots, x_n\}$ izanik. G grafoaren* grafo osagarria *K_n grafo osotuaren $\overline{G} = (V, \overline{E})$ azpigrafoa da, non $\overline{E}$ multzoan E multzoan ez dauden K_n grafo osotuaren ertzak dauden.*

$G = K_n$ bada, $\overline{G}$ grafoak n erpin eta 0 ertz izango ditu; grafo nulu *deitzen da.*

5.45 Adibidea. G grafo hau bada:



$\overline{G}$ grafo osagarria beste hau izango da:



5.46 Definizioa. $G = (V, E)$ zatibiko grafoa *da grafo bakuna, ez-zuzendua eta begiztarik gabea bada eta*

- *V_1, V_2 badaude, non $V_1 \cup V_2 = V$ eta $V_1 \cap V_2 = \emptyset$ diren eta*
- *G grafoaren $\{x, y\}$ ertz bakoitzean $x \in V_1$ eta $y \in V_2$ badira.*

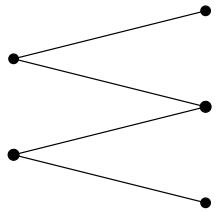
Horrez gain,

$$(\forall x \in V_1,\ \forall y \in V_2) \quad \{x, y\} \text{ ertza badago,}$$

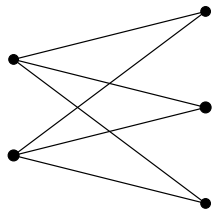
G zatibiko grafo osotua *da, eta K_{n_1,n_2} idatziko dugu, $|V_1| = n_1$ eta $|V_2| = n_2$ izanik.*

5.47 Adibideak.

1. Grafo hau zatibiko grafo da (ez osotua):



2. Grafo hau $K_{2,3}$ zatibiko grafo osotua da:



5.7 Grafoen arteko isomorfismoak

5.48 Definizioa. *Izan bitez $G_1 = (V_1, E_1)$ eta $G_2 = (V_2, E_2)$ bi grafo ez-zuzendu. Grafoen arteko $f : V_1 \longrightarrow V_2$ funtzioa* isomorfismoa *da hau betetzen badu:*

- *f bijektiboa da eta*
- $(\forall x, y \in V_1) \quad \{x, y\} \in E_1$ *baldin eta soilik baldin* $\{f(x), f(y)\} \in E_2$.

Horrelako funtzio bat badago, G_1 eta G_2 grafo isomorfoak *dira eta $G_1 \cong G_2$ idatziko dugu.*

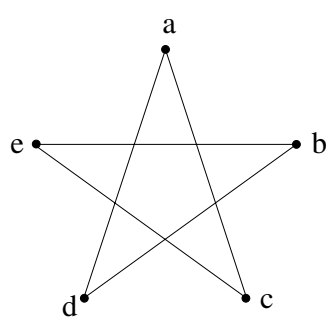
Grafoen arteko isomorfiak baliokidetasun-erlazio bat definitzen du grafoen multzoan. G_1 eta G_2 grafo isomorfoak badira, funtsean berdinak dira:

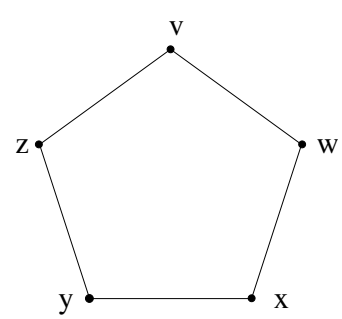
- erpinen kopuru bera dute;
- ertzen kopuru bera dute;
- gradu bera duten erpinen kopuru bera dute;
- zikloen kopuru bera dute;
- etab.

5.49 Adibideak.

1. Har ditzagun grafo hauek:

$G_1 = (V_1, E_1)$ $\qquad\qquad$ $G_2 = (V_2, E_2)$





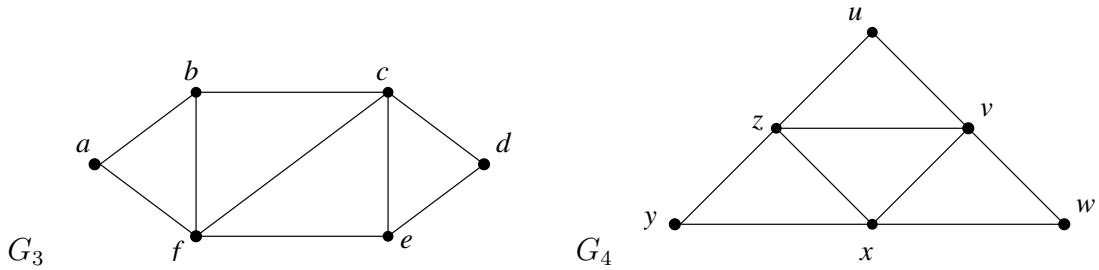
$f : V_1 \longrightarrow V_2$ funtzioa, non

$$f(a) = v, \quad f(b) = y, \quad f(c) = w, \quad f(d) = z, \quad f(e) = x \quad \text{diren,}$$

isomorfismoa da. Hau da, $G_1 \cong G_2$.

$$\begin{array}{l}
\{a, c\} \leftrightarrow \{f(a), f(c)\} = \{v, w\} \\
\{c, e\} \leftrightarrow \{f(c), f(e)\} = \{w, x\} \\
\{e, b\} \leftrightarrow \{f(e), f(b)\} = \{x, y\} \\
\{b, d\} \leftrightarrow \{f(b), f(d)\} = \{y, z\} \\
\{d, a\} \leftrightarrow \{f(d), f(a)\} = \{z, v\}
\end{array}$$

2. Ikus ditzagun, orain, grafo hauek:



Bi grafoek 6na erpin eta 9na ertz dituzte. Baina ez dira isomorfoak.

$$d(a) = d(d) = 2, \quad d(b) = d(e) = 3, \quad d(c) = d(f) = 4,$$

$$d(u) = d(w) = d(y) = 2, \quad d(v) = d(x) = d(z) = 4;$$

gradu bereko erpinen kopuruak desberdinak dira.

5.8 Kate eta zirkuitu eulertarrak

5.50 Definizioa. *Izan bedi $G = (V, E)$ grafo ez-zuzendua eta erpin isolaturik gabea. G grafoaren ertz guztiak erabiltzen dituen zirkuituari* zirkuitu eulertar *deituko diogu.*

G grafoaren ertz guztiak erabiltzen dituen kate irekiari kate eulertar *deituko diogu.*

G grafoa eulertarra *da zirkuitu eulertar bat badauka.*

5.51 Adibideak.

1. 5.49-2 Adibideko G_4 grafoan zirkuitu eulertar hau aurki dezakegu:

$$u, v, z, x, v, w, x, y, z, u.$$

Zirkuitu eulertarra da, grafoaren ertz guztiak zeharkatzen dituelako, bakoitza behin bakarrik, eta hasitako erpinean amaitzen delako. Beraz, grafo eulertarra da.

2. 5.49-2 Adibideko G_3 grafoan kate eulertar hau aurki dezakegu:

$$b, a, f, b, c, d, e, c, f, e.$$

Kate eulertarra da, grafoaren ertz guztiak zeharkatzen dituelako, bakoitza behin bakarrik, eta ez delako hasitako erpinean amaitzen. Ezin da, ordea, zirkuitu eulertar bat ere aurkitu.

5.52 Teorema. *Izan bedi $G = (V, E)$ grafo ez-zuzendua eta erpin isolaturik gabea. Orduan,*

G eulertarra da $\Longleftrightarrow$ G konexua bada eta G grafoaren erpin guztiek gradu bikoitia badute.

Froga.

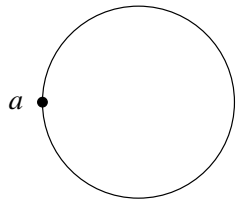
$\underline{\Longrightarrow}$: Demagun G eulertarra dela, hots, C zirkuitu eulertar bat duela.

Ikus dezagun G konexua dela: G grafoak erpin isolaturik ez duenez, V multzoaren erpin guztiak behin gutxienez agertuko dira C zirkuituan. $x, y \in V$ bi erpin desberdin izanik, x erpinean hasten den eta y erpinean bukatzen den C zirkuituaren zatia $x - y$ ibilaldi bat da. Beraz, G konexua da.

Ikus dezagun, orain, erpin guztiek gradu bikoitia dutela. Izan bedi x edozein erpin. C zirkuitua x erpinera ertz batetik "heltzen" denean, x erpinetik ertz desberdin batetik "aterako" da. Beraz, C zirkuituak x erpinarekin intzidenteak diren bi ertz desberdin, edo begizta berri bat, erabiltzen ditu. Bi kasuetan, C zirkuitua x erpinetik pasatzen den bakoitzean, bi unitate eransten dio x erpinaren graduari; hortaz, $d(x)$ bikoitia da.

$\underline{\Longleftarrow}$: Demagun G konexua dela eta G grafoaren erpin guztiek gradu bikoitia dutela. G eulertarra dela frogatu behar dugu. G grafoaren ertzen m kopuruaren gaineko indukzioz egingo dugu.

$m = 1$ bada, G grafoa hau da:



eta zirkuitu eulertarra nabaria da.

Pentsa dezagun, $m < p$ denean, zirkuitu eulertarra eraiki dezakegula. $m = p$ denean, zirkuitu eulertarra eraiki ahal izango dugula frogatuko dugu.

Hasteko, $x \in V$ erpin bat izanik, x erpina duen zirkuitu bat dagoela frogatuko dugu. Izan bedi

$$x = y_0, f_1, y_1, \ldots, f_k, y_k$$

x erpinean hasten den ibilaldirik luzeena, y_i erpinak eta f_i ertzak izanik, $i \in \{1, \cdots, k\}$.

- $i \in \{1, \cdots, k\}$ baterako $y_i = x$ bada,

  $$x = y_0, f_1, \ldots, f_i, y_i = x$$

  x erpina duen ibilaldi itxi bat da.

- $i \in \{1, \cdots, k\}$ guztietarako $y_i \neq x$ bada, y_k erpina hartuko dugu.

  - $y_k = y_i$ bada $i \in \{1, \cdots, k-1\}$ baterako, y_k erpina ibilaldiaren tartean eta amaieran agertuko da. Tartean agertzen den bakoitzean, graduari 2 erantsiko dio, eta amaieran agertzean 1 erantsiko dio; beraz, guztira gradu bakoitia emango du. Hipotesiz, erpin guztiek gradu bikoitia dutenez, ibilaldian erabili ez den ertz bat, gutxienez, intzidentea da y_k erpinarekin. Horrek esan nahi du ibilaldia luza dezakegula, esan dugunaren kontra, hau da, ibilaldia luzeena izatearen kontra.

– $y_k \neq y_i$ bada $i \in \{1, \cdots, k-1\}$ guztietarako, y_k erpina ibilaldiaren amaieran bakarrik agertuko da. y_k erpinaren gradua bikoitia denez eta y_k erpinarekin intzidentea den ertz bat bakarrik erabili dugunez, ibilaldian ez dagoen beste ertz bat egon behar da. Berriro ere, horrek esan nahi du ibilaldia luzatu ahal genukeela, ibilaldia luzeena izatearen kontra.

Horrela, x erpinetik pasatzen den ibilaldi itxi bat dagoela frogatu dugu. 5.24 Teoremaren arabera, ibilaldi bat badago, bide bat dago; beraz, x erpinetik pasatzen den C bide itxi (ziklo) bat dago. Eta ziklo hori x erpinetik pasatzen den zirkuitua da, erpinak ez badira errepikatzen ertzak ere ezin direlako errepikatu.

C zirkuitu horretan G grafoaren ertz guztiak badaude, zirkuitu eulertarra da.

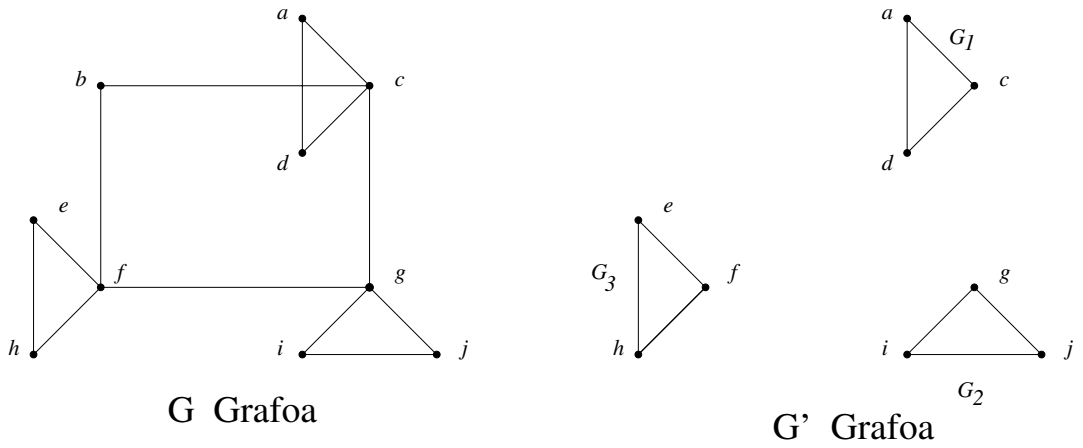
G grafoaren ertz guztiak ez badaude, G grafotik C zirkuitua ezabatuko dugu, eta, horrekin batera, isolaturik gera daitezkeen erpinak ere bai. Horrela, G' grafo bat lortuko dugu, zeinak $\{G_1, G_2, \ldots, G_l\}$ osagai konexuak izan ditzakeen. Osagai bakoitzak erpin komun bat izango du C zirkuituarekin. Horrez gain, osagai konexu bakoitza p baino ertz gutxiago dituen grafo konexua da, eta erpin guztiek gradu bikoitia izanik; hortaz, indukzio-hipotesiaren arabera, osagai konexu bakoitzerako zirkuitu eulertar bat izango dugu.

G grafoaren zirkuitu eulertarra lortzeko, C zirkuitutik ibiliko gara, edozein erpinetatik hasita. Osagai konexuren batekin komunean duen erpin batera heltzean, C zirkuitutik aterako gara eta osagai konexuaren zirkuitu eulertarra ibiliko dugu erpin komunera itzuli arte; osagaitik atera eta C zirkuitutik segituko dugu. Horrela, osagai konexu guztietatik pasatu eta gero, C zirkuitura itzuliko gara eta hasi garen erpinean bukatuko dugu. Hori izango da G grafoaren zirkuitu eulertarra.

Prozesu honek bukaera izango du, ertzen kopurua finitua delako. □

5.53 Adibideak.

1. Irudiko grafoan, b erpinetik pasatzen den C zirkuitua hartuko dugu: $C = bcgfb$. Gero, G grafoari C zirkuituaren ertzak eta isolaturik geratu den b erpina kenduko dizkiogu; G_1, G_2 eta G_3 osagai konexuek osatzen duten G' grafoa geratuko zaigu.



G grafoaren zirkuitu eulertarra lortzeko, b erpinetik (esaterako) hasiko gara:

$$bcG_1cgG_2gfG_3fb;$$

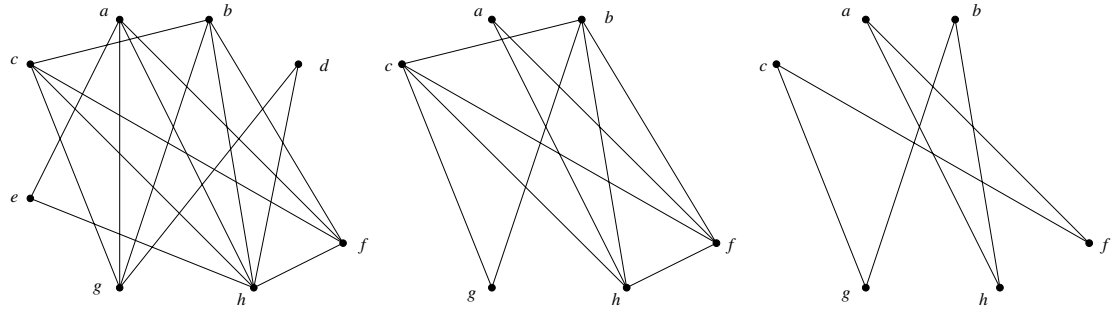
edo erpin guztiak idatziz:

$$bc\underline{adcg}\underline{ijg}f\underline{ehf}b.$$

2. Irudiko G graforako, bi graduko d eta e erpinetatik pasatzen den C zirkuitu bat hartuko dugu: $C = dheagd$. Gero, G grafoari C zirkuituaren ertzak eta isolaturik geratzen diren d eta e erpinak kenduko dizkiogu; G' lortuko dugu. G' grafoan, $C' = bchfb$ zirkuitua hartuko dugu. Orain, G' grafoari C' zirkuitua kenduz gero (ez da erpin isolaturik geratzen), G'' grafoa lortuko dugu. G'' grafoan erpin guztiek bi gradua dute, eta erraz aurki dezakegu zirkuitu eulertar bat: $E'' = afcgbha$.

   G' grafoaren zirkuitu eulertarra eratuko dugu. C' zirkuituaren edozein erpin hartuko dugu, esaterako, b. b erpina G'' grafoan dagoenez, G'' grafoan sartuko gara eta bere zirkuitu eulertarra ibiliko dugu, b erpinean bukatuz. Orain, C' zirkuitutik segituko dugu. Horrela zirkuitu eulertar hau lortuko dugu: $E' = b\underline{hafcgb}chfb$.

   G grafoaren E zirkuitu eulertarra eratzeko, C zirkuituaren edozein erpinetan hasiko gara, adibidez, d erpinean. C zirkuitutik ibiliko gara G' grafoarekin erpin komun bat aurkitu arte, adibidez, h. h erpinetik G' grafoan sartuko gara eta E' zirkuitu eulertarra berridatziko dugu: $E' = hafcgbchfbh$. Horrela, G' grafo osoa ibili dugu, eta C zirkuitura aterako gara h erpinetik, eta hortik segituko dugu d erpineraino. Bukaeran zirkuitu eulertar hau osatu dugu: $E = d\underline{hafcgb\underline{chfb}heagd}$.



G Grafoa G' Grafoa G'' Grafoa

5.54 Korolarioa. *Izan bedi $G = (V, E)$ grafo ez-zuzendu eta erpin isolaturik gabe bat. Orduan,*

G grafoak kate eulertar bat du $\Longleftrightarrow$ G konexua bada eta zehazki bi erpinek gradu bakoitia badute.

Froga.

$\underline{\Longrightarrow}$: Demagun G grafoak R kate eulertar bat duela (ez zirkuitua): $a - b$, $a \neq b$ izanik.

Izan bedi G' grafoa G grafoari $\{a, b\}$ ertza eranstean sortzen den grafoa. Orduan, $R \cup \{a, b\}$ G' grafoaren zirkuitu eulertarra da. 5.52 Teorema G' grafoari aplikatuz gero, G' grafoaren erpin guztiek gradu bikoitia izango dute. $x \in V$ izanik, $d(x)$ bada x erpinaren gradua G grafoan, eta $d'(x)$ bada x erpinaren gradua G' grafoan,

$$\begin{aligned} d(x) &= d'(x), \qquad x \neq a, x \neq b \text{ bada,} \\ d(a) &= d'(a) - 1, \\ d(b) &= d'(b) - 1. \end{aligned}$$

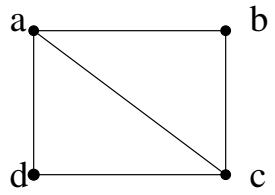
$\forall x \in V$, $d'(x)$ bikoitia denez, G grafoak gradu bakoitiko bi erpin bakarrik izango ditu, a eta b.

$\underline{\Longleftarrow}$: Demagun G konexua dela eta zehazki bi erpinek gradu bakoitia dutela, $a \neq b$.

Izan bedi G' grafoa G grafoari $\{a, b\}$ ertza eranstean sortzen den grafoa. G' konexua da eta G' grafoaren erpin guztiek gradu bikoitia badute. 5.52 Teorema aplikatuz, G' grafoak C zirkuitu eulertar bat dauka. C zirkuitutik $\{a, b\}$ ertza ezabatuz, kate eulertar bat lortuko dugu G graforako. Kate eulertar hori gradu bakoitiko erpin batean hasiko da eta bestean bukatuko da. □

5.55 Adibideak.

1.



grafoan, $K = acbadc$ kate eulertar bat da. Ez dago zirkuitu eulertarrik.

2. Königsbergeko zubien problemaren grafoan (5.5 Adibidea), lau erpinek gradu bakoitia dute:
$$d(A) = 5, d(B) = d(C) = d(D) = 3;$$
beraz, ezin da kate eulertarrik, ezta zirkuitu eulertarrik ere, osatu. Ondorioz, ezin da halako ibilaldirik egin zubiak behin bakarrik pasatzen.

Aurreko kontzeptuak eta emaitzak grafo zuzenduetara zabal ditzakegu.

5.56 Definizioa. *Izan bedi $G = (V, E)$ grafo zuzendu eta erpin isolaturik gabea. G grafoaren ertz guztiak erabiltzen dituen zirkuitu zuzenduari* zirkuitu eulertar zuzendu *deituko diogu.*

G grafoa eulertar zuzendua *da zirkuitu eulertar zuzendu bat badauka.*

5.57 Teorema. *Izan bedi $G = (V, E)$ grafo zuzendu eta erpin isolaturik gabea. Orduan,*

G grafoak zirkuitu eulertar zuzendua du $\Longleftrightarrow$ G grafo konexua bada eta $x \in V$ erpin guztietarako $d^+(x) = d^-(x)$ betetzen bada.

5.9 Bide eta ziklo hamiltondarrak

5.58 Definizioa. *Izan bedi $G = (V, E)$ grafo ez-zuzendua, $|V| = n \geq 3$ izanik. G grafoaren erpin guztiak dituen ziklo bati* ziklo hamiltondar *deituko diogu.*

G grafoaren erpin guztiak dituen bide ireki bati bide hamiltondar *deituko diogu.*

G grafoa hamiltondarra *da ziklo hamiltondar bat badu.*

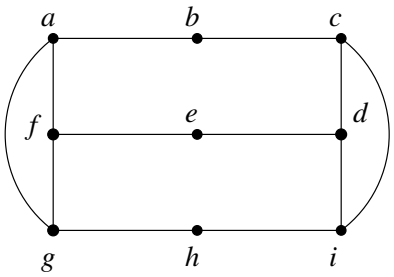
Oharrak.

1. Ziklo hamiltondar batetik ertz bat ezabatuz gero, bide hamiltondar bat lortuko dugu.

2. Grafo batek bide hamiltondar bat badu, konexua da.

3. Zirkuitu eta kate eulertarrekin ez bezala, ez dago baldintza nahikorik, ezta beharrezkorik ere, ziklo edo bide hamiltondarren bat dagoela ziurtatzeko. Teorema batzuek baldintza beharrezkoak ematen dituzte, eta beste batzuek baldintza nahikoak.

5.59 Adibidea.



G grafoan,

$$a, b, c, d, e, f, g, h, i$$

bide hamiltondarra da. Ikus dezagun ea G grafoan ziklo hamiltondarren bat dagoen.

G grafoak bederatzi erpin dituenez, ziklo hamiltondar bat balego, bederatzi ertz izango lituzke. Has gaitezen b erpinean eta saia gaitezen ziklo hamiltondar bat eratzen. Grafoaren simetria kontuan izango dugu. b erpinetik c erpinera joango gara; gero, edo d edo i erpinetara joan gaitezke. d erpinera bagoaz, $\{c, i\}$ ertza ezin da zikloan sartu, ezin garelako itzuli c erpinera. Orain, edo e edo i erpinetara joan gaitezke. e erpinera bagoaz, $\{d, i\}$ ertza ezin da zikloan sartu; beraz, i erpinera heltzen garenean ezin izango dugu segitu. Baina i erpinera bagoaz, $\{e, d\}$ ertza ezin da zikloan sartu; beraz, e erpinera heltzen garenean ezin izango dugu segitu.

Ondorioz, grafo horrek ez du ziklo hamiltondarrik.

Adibide horri begira, iradokizun batzuk eman ditzakegu $G = (V, E)$ grafoan ziklo hamiltondar bat aurkitzeko.

- G hamiltondarra bada, $x \in V$ erpin guztietarako $d(x) \geq 2$ da.

- $a \in V$ eta $d(a) = 2$ bada, a erpinarekin intzidenteak diren ertzek G grafoaren edozein ziklo hamiltondarretan agertu behar dute.

- $a \in V$ eta $d(a) > 2$ bada, G grafoaren edozein ziklo hamiltondar eraikitzeko, a erpinetik behin pasatu eta gero, a erpinarekin intzidenteak diren eta erabili ez ditugun ertzak baztertuko ditugu.

- G grafoaren edozein ziklo hamiltondar eraikitzean, ezin izango dugu ziklo bat osatu G grafoaren azpigrafo baterako, ez bada G grafoaren erpin guztiak hartzen dituela.

Ikus ditzagun grafo batek bide edo ziklo hamiltondar bat izateko baldintza nahikoak ematen dituzten teorema batzuk.

5.60 Teorema. *Izan bedi $G = (V, E)$ grafoa, begiztarik gabea eta $n \geq 3$ erpin dituena.*

$$\forall x, y \in V \quad (x \neq y) \quad d(x) + d(y) \geq n - 1$$

betetzen badu, G grafoak bide hamiltondarra izango du.

5.61 Korolarioa. *Izan bedi $G = (V, E)$ grafoa, begiztarik gabea eta $n \geq 3$ erpin dituena.*

$$\forall x \in V \quad d(x) \geq \frac{n-1}{2}$$

betetzen badu, G grafoak bide hamiltondarra izango du.

5.62 Adibidea. Zazpi azterketa zazpi egunetan antolatu nahi ditugu, irakasle batek bi azterketa jarraian ez ditzan izan. Ezein irakaslek ez du lau baino azterketa gehiago. Ikusiko dugu beti dela posible azterketak antolatzea.

Har dezagun G grafoa, non erpinak azterketak diren; bi erpinen artean ertz bat marraztuko dugu bi azterketak irakasle desberdinenak badira. Orduan, erpin bakoitzaren gradua gutxienez 3 $(7 - 4 = 3)$ da.

Horrela definitutako G grafoak $\forall x \in V \quad d(x) \geq \dfrac{7-1}{2} = 3$ betetzen du; beraz, bide hamiltondar bat badu.

5.63 Teorema. *Izan bedi $G = (V, E)$ grafoa, begiztarik gabea eta $n \geq 3$ erpin dituena.*

$$\forall x, y \in V \quad (x, y \ \textit{ez-auzokideak}) \quad d(x) + d(y) \geq n$$

betetzen badu, G grafo hamiltondarra izango da.

5.64 Korolarioa. *Izan bedi $G = (V, E)$ grafoa, begiztarik gabea eta $n \geq 3$ erpin dituena.*

$$\forall x \in V \quad d(x) \geq \frac{n}{2}$$

betetzen badu, G grafo hamiltondarra izango da.

5.65 Adibidea. Hogei laguneko talde batean, bakoitzak gutxienez hamar lagun ezagutzen ditu. Ikus dezagun mahai biribil baten inguruan eser daitezkeela, eta ziurtatu mahaikide bakoitzak bi lagun ezagun izango dituela alde banatan.

G grafoan erpinak lagunak izango dira; eta elkar ezagutzen duten lagunen artean ertzak marraztuko ditugu.

Grafo horretan erpin bakoitzaren gradua $d(x) \geq \dfrac{20}{2} = 10$ izango da. Hortaz, G grafo hamiltondarra izango da.

Baldintza horietan mahaiaren inguruan esertzeko era bakoitza ziklo hamiltondar bat izango da.

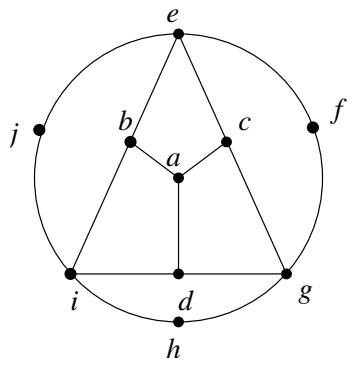
Ikus ditzagun grafo batek bide edo ziklo hamiltondar bat izateko baldintza beharrezkoak ematen dituzten teorema batzuk. Lehenengoa zatibiko grafo bati dagokio.

5.66 Teorema. *$G = (V, E)$ zatibiko grafoa izanik, non $V = V_1 \dot{\cup} V_2$ den, G grafoa hamiltondarra bada, $|V_1| = |V_2|$ izango da.*

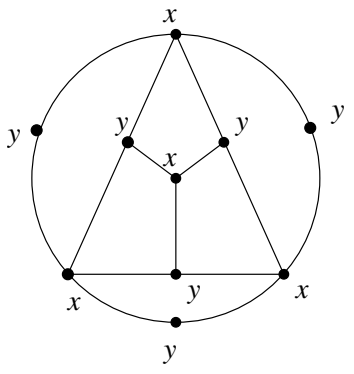
Aurreko teoremak esaten digu, $G = (V, E)$ zatibiko grafoa izanik, non $V = V_1 \dot{\cup} V_2$ den, $|V_1| \neq |V_2|$ bada, G grafoa ez dela hamiltondarra.

Adibide honek frogabidearen ideia emango digu.

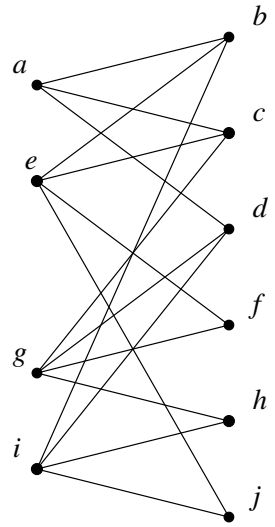
5.67 Adibidea. Har dezagun G grafo hau:



Grafo hori zatibikoa da. Hori ikusteko erpinak bi multzotan banatuko ditugu honela: a erpina x izendatuko dugu; gero, x erpinarekin auzokide diren erpin guztiak (b, c eta d) y izendatuko ditugu. Ondoren, y erpinekin auzokide diren eta izendatu gabe dauden erpinak x izendatuko ditugu; eta horrela ondoz ondo eginez gero, grafoa honela geratuko da:



Orain, x erpin guztiak alde batera eta y erpin guztiak beste aldera eramanez gero, grafoa zatibikoa dela nabarmen geratuko da:



G grafoaren erpinak bi multzotan banatuko ditugu:

$$V = V_1 \dot{\cup} V_2, \quad V_1 = \{a, e, g, i\}, \quad V_2 = \{b, c, d, f, h, j\}$$

$|V_1| \neq |V_2|$ denez, G grafoa ez da hamiltondarra.

Bide hamiltondar bat izanez gero, bidean txandakaturik agertuko lirateke bosna aldiz x eta y letrak; baina, x letra lau aldiz eta y letra sei aldiz dauzkagu. Hortaz, horrelako bide bat osatzea ezinezkoa da. Ondorioz, grafoak ez du bide hamiltondarrik.

Idazkera. $G = (V, E)$ grafoa izanik, eta $V' \subset V$ erpinen azpimultzo bat, $G - V'$ idatziko dugu $G - V' = (V_1, E_1)$ grafoa adierazteko, non $V_1 = V \setminus V'$ den eta E_1 multzoan E multzoaren ertzak dauden, V' multzoaren erpinekin intzidenteak direnak izan ezik.

5.68 Teorema. *$G = (V, E)$ grafo hamiltondarra bada, edozein $V' \subset V$ azpimultzotarako, $\emptyset \neq V' \neq V$ izanik,*

$$\kappa(G - V') \leq |V'|.$$

5.69 Korolarioa. *$G = (V, E)$ grafoa izanik, $V' \subset V$ azpimultzo bat badago, $\emptyset \neq V' \neq V$ izanik, non*

$$\kappa(G - V') > |V'|$$

betetzen den, G grafoa ez da hamiltondarra izango.

5.70 Adibidea. 5.67 Adibideko grafoan, x izendatutako erpinak kenduz gero, y izendatutako erpinak isolaturik geratuko lirateke. Beraz, $\kappa(G - V') = 6$ eta $|V'| = 4$ dira. Ondorioz, G grafoa ez da hamiltondarra.

5.10 Zuhaitzak

5.10.1 Sarrera

Zuhaitz bat grafo mota berezi bat da. Gustav Robert Kirchhoff-ek (1824-1887) erabili zituen lehenengo aldiz elektronikan. Beranduago, Arthur Cayley-k (1821-1895) berriro definitu eta garatu zituen Kimika arloan (1857).

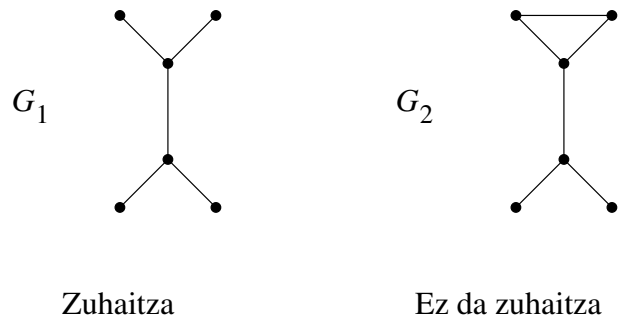
Zuhaitz berezi batzuk oso garrantzitsuak dira datuen egiturak eta ordenamenduak aztertzeko, kodeketa-teorian eta optimizazio-problema batzuen soluzioan.

5.10.2 Definizioak eta propietateak

5.71 Definizioa. *Izan bedi $T = (V, E)$ grafo ez-zuzendua eta begiztarik gabea. T grafoa* zuhaitza *da konexua bada eta ez badu ziklorik.*

Grafo baten erpin guztiak dituen eta zuhaitz den edozein azpigrafo sortzaileri zuhaitz sortzaile *deituko diogu.*

5.72 Adibidea.



G_1 grafoa G_2 grafoaren zuhaitz sortzailea da.

5.73 Teorema. *a eta b zuhaitz baten bi erpin desberdin badira, $a - b$ bide bakarra egongo da.*

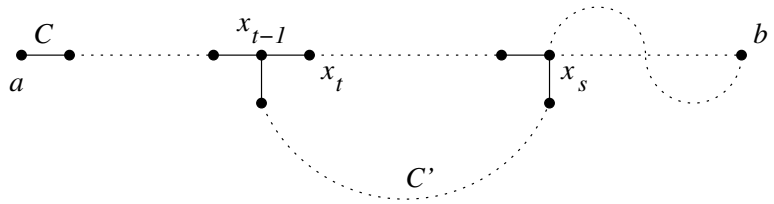
Froga.

Izan bitez $T = (V, E)$ zuhaitz bat eta $a, b \in V, \quad a \neq b$.

T konexua denez, gutxienez $a - b$ bide bat dago: $C(a = x_0, x_1, \ldots, x_p = b)$.

Demagun beste $a - b$ bide bat dagoela, C'.

Izan bedi x_t erpina C' bidean ez dagoen C bidearen lehen erpina ($1 \leq t \leq p - 1$); eta izan bedi x_s erpina bi bideetan dagoen C bidearen hurrengo erpina ($t < s \leq p$).



Orduan, C eta C' bideen zatiek, x_{t-1} eta x_s erpinen artean, ziklo bat osatuko lukete, T zuhaitza izatearen kontra doana. □

5.74 Lema. *Izan bedi $G = (V, E)$ grafo ez-zuzendua, begiztarik gabea eta konexua, eta izan bedi $e \in E$ G grafoaren ertz bat. Orduan,*

$$e \text{ ertza ziklo batean dago} \iff G - e \text{ grafoa konexua bada.}$$

Froga.

Izan bedi $e = \{a, b\}$.

$\underline{\Longrightarrow:}$

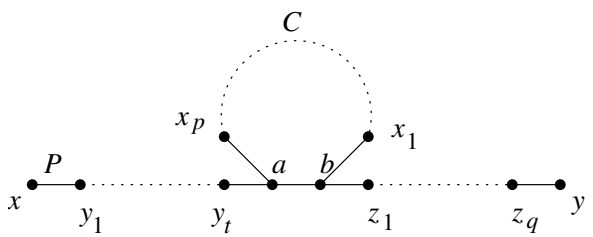
Demagun e ertza C ziklo batean dagoela: $C = a, b, x_1, x_2, \ldots, x_p, a$.

$G-e$ grafoa konexua dela frogatzeko, edozein $x, y \in V$ bi erpin desberdin izanik, $G-e$ grafoan $x-y$ bide bat dagoela frogatu behar dugu.

Izan bitez $x, y \in V$ desberdinak. G grafoa konexua denez, $x-y$ bide bat dago G grafoan (P).

P bideak ez badu e ertza, P bidea da $G-e$ grafoan.

P bideak e ertza badu, $P : x, y_1, \ldots, y_t, a, b, z_1, \ldots, z_q, y$ izango da.



Orduan, P bidea eta C zikloa e ertzean lotuz eta e ertza bietatik kenduz, $x-y$ bide bat lortuko dugu:

$$(P-e) \cup (C-e) : x, y_1, \ldots, y_t, a, x_p, \ldots, x_1, b, z_1, \ldots, z_q, y.$$

$x-y$ bide bat da $G-e$ grafoan.

$\underline{\Longleftarrow:}$

Demagun $G-e$ grafoa konexua dela.

$G-e$ grafoan $a-b$ bide bat dago, $P : a, x_1, \ldots, x_p, b$. Hortaz, $P \cup e : a, x_1, \ldots, x_p, b, a$ ziklo bat da G grafoan. □

5.75 Teorema. *Izan bedi G grafo ez-zuzendu bat.*

$$G \text{ konexua da} \iff G \text{ grafoak zuhaitz sortzailea badu.}$$

Froga.

$\underline{\Longleftarrow:}$

Demagun G grafoak T zuhaitz sortzaile bat duela.

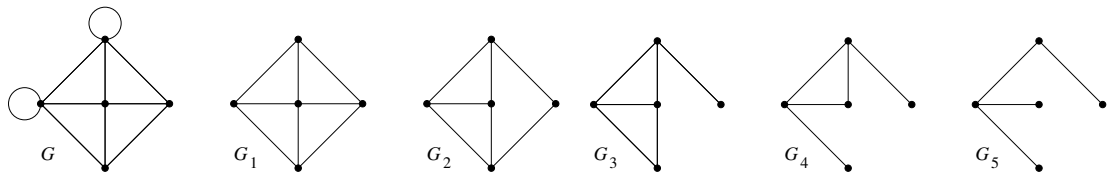
G grafoaren erpinen x, y bikote bakoitzeko $x-y$ bide bat dago T zuhaitzean. T zuhaitzaren ertzak G grafoaren ertzak direnez, bide hori G grafoan egongo da eta, beraz, G grafoa konexua da.

$\underline{\Longrightarrow:}$

Demagun G konexua dela. Eraiki dezagun zuhaitz sortzaile bat.

G ez bada zuhaitza, begizta guztiak ezabatuko ditugu. Geratzen den G_1 azpigrafoa konexua eta begiztarik gabea da eta G grafoaren erpin guztiak ditu. Zuhaitza balitz, G grafoaren zuhaitz sortzailea izango litzateke. Ez bada zuhaitza, gutxienez C_1 ziklo bat dauka. Orduan, C_1 ziklotik e_1 ertz bat ezabatuko dugu; izan bedi $G_2 = G_1 - e_1$ grafoa. 5.74 Lemaren arabera, G_2 grafoa konexua eta begiztarik gabea da eta G grafoaren erpin guztiak ditu. Zuhaitza balitz, G grafoaren zuhaitz sortzailea izango litzateke. Ez bada zuhaitza, gutxienez C_2 ziklo bat dauka. Orduan, C_2 ziklotik e_2 ertz bat ezabatuko dugu; izan bedi $G_3 = G_2 - e_2$ grafoa. Zuhaitza balitz, G grafoaren zuhaitz sortzailea izango litzateke. Ez bada zuhaitza, prozesu horrekin segituko genuke urrats kopuru finitu aldiz, G grafoaren zuhaitz sortzaile bat lortu arte. □

5.76 Adibidea.



G_5 grafoa G grafoaren zuhaitz sortzaile bat da.

5.77 Lema. *Izan bedi $T = (V, E)$ zuhaitz bat eta izan bedi e T zuhaitzaren edozein ertz. Orduan, $T - e$ ez-konexua da eta zuhaitzak diren bi osagai konexu ditu.*

Froga.

Izan bedi $e = \{a, b\}$.

Demagun $T - e$ konexua dela. Orduan, $T - e$ grafoan $a - b$ bide bat dago: C.

Hortaz, T grafoan $a - b$ bi bide daude, C bidea eta e ertza; hori T zuhaitza izatearen kontra doa, zuhaitz batean bi erpin lotzen dituen bide bakarra baitago (5.73 Teorema).

Hortaz, $T - e$ ez-konexua da eta bi osagai konexu ditu,

$$V_1 = \{a\} \cup \{x \in V \,/\, a - x \text{ bide bat dago } T - e \text{ grafoan}\}$$

eta

$$V_2 = \{b\} \cup \{x \in V \,/\, b - x \text{ bide bat dago } T - e \text{ grafoan}\}$$

erpinen multzoek induzitutako azpigrafoak hain zuzen.

Osagai konexu horiek zuhaitzak dira, begizta edo ziklo bat izanez gero, T grafoan ere egongo litzatekeelako. □

5.78 Teorema. *Izan bedi T n erpin eta m ertz dituen zuhaitz bat. Orduan,*

$$n = m + 1.$$

Froga.

Ertzen m kopuruaren gaineko indukzioz frogatuko dugu.

$m = 0$ bada, zuhaitza erpin isolatu batek osatuko du. Kasu horretan, $n = 1 = m + 1$ beteko da.

Demagun teorema betetzen dela $m \leq k$ denean, eta izan bedi $m = k + 1$.

T zuhaitzetik ertz bat ezabatuz gero, 5.77 Lemaren arabera, T_1 eta T_2 bi azpizuhaitz lortuko ditugu. Izan bitez n_1, n_2 eta m_1, m_2 T_1 eta T_2 azpizuhaitzen erpinen eta ertzen kopuruak, hurrenez hurren.

Orduan, $n = n_1 + n_2$ eta $m = m_1 + m_2 + 1 = k + 1$ izango dira. $0 \leq m_1 \leq k$ eta $0 \leq m_2 \leq k$ direnez, indukzio-hipotesiaren arabera, $n_1 = m_1 + 1$ eta $n_2 = m_2 + 1$ beteko dira. Hortaz,

$$n = n_1 + n_2 = (m_1 + 1) + (m_2 + 1) = (m_1 + m_2 + 1) + 1 = m + 1.$$

□

5.79 Adibidea. 5.72 Adibideko G_1 zuhaitzean, $n = 6$ eta $m = 5$ dira.

5.80 Teorema. *Izan bedi $T = (V, E)$ n erpin dituen zuhaitz bat. $n \geq 2$ bada, T zuhaitzak gutxienez bi erpin zintzilikatu izango ditu.*

Froga.

Izan bedi m T zuhaitzaren ertzen kopurua. 5.78 Teoremaren arabera, $m = n - 1$ beteko da. Hortaz, 5.14 Teoremaren arabera, ondoko hau beteko da:

$$\sum_{x \in V} d(x) = 2(n-1).$$

T zuhaitza konexua denez, $d(x) \geq 1$ izango da $x \in V$ guztietarako.

T zuhaitzak ez balu erpin zintzilikaturik, $d(x) \geq 2$ beteko litzateke $x \in V$ guztietarako eta, beraz, $2(n-1) = \sum_{x \in V} d(x) \geq 2n$ ere beteko litzateke, eta hori ezinezkoa da.

T zuhaitzak a erpin zintzilikatu bakarra izango balu, $d(a) = 1$ eta $d(x) \geq 2$ beteko litzateke $x \in V$ guztietarako, $x \neq a$ izanik. Orduan, $2(n-1) = \sum_{x \in V} d(x) \geq 1 + 2(n-1)$ beteko litzateke, eta hori ere ezinezkoa da.

Ondorioz, T zuhaitzak gutxienez bi erpin zintzilikatu izango ditu. □

5.81 Adibidea. 5.72 Adibideko G_1 grafoak 4 erpin zintzilikatu ditu.

5.76 Adibideko G_5 grafoak 3 erpin zintzilikatu ditu.

5.82 Teorema. *Izan bedi $G = (V, E)$ n erpin eta m ertz dituen grafo ez-zuzendua eta begiztarik gabea Hiru baieztapen hauek baliokideak dira:*

i) *G zuhaitza da.*

ii) *G grafoak ez du ziklorik, eta $n = m + 1$.*

iii) *G grafoa konexua da, eta $n = m + 1$.*

Froga.

i) $\Longrightarrow$ ii):

Demagun i) betetzen dela, hots, G zuhaitza dela.

5.78 Teorema erabiliz, $n = m + 1$ izango dugu.

G grafoak ez du ziklorik zuhaitza delako.

ii) $\Longrightarrow$ iii):

Demagun ii) betetzen dela.

Izan bedi $\kappa(G) = r$ eta izan bitez $G_1 = (V_1, E_1)$, ..., $G_r = (V_r, E_r)$ G grafoaren osagai konexuak (zuhaitzak direnak ziklorik ez dutelako).

$i = 1, \ldots, r$ bakoitzeko, $v_i \in V_i$ erpin bat aukeratuko dugu eta G grafoari $r - 1$ ertz hauek erantsiko dizkiogu, $\{v_1, v_2\}$, $\{v_2, v_3\}$, ..., $\{v_{r-1}, v_r\}$. Horrela lortuko dugun $G' = (V, E')$ grafoa zuhaitza da, eta n erpin eta $m + r - 1$ ertz ditu.

5.78 Teoremaren arabera, $n = (m + r - 1) + 1 = m + r$ eta, ii) hipotesiz $n = m + 1$ denez, $r = 1$ lortuko dugu; hau da, G konexua da.

iii) $\Longrightarrow$ i):

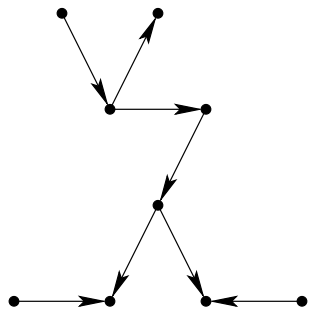
Demagun iii) betetzen dela.

5.75 Teoremaren arabera, G grafoak $T = (V, E')$ zuhaitz sortzaile bat du. Izan bedi m' T zuhaitzaren ertzen kopurua. 5.78 Teoremaren arabera, $m' = n + 1$ izango da; baina iii) hipotesiz, $n + 1 = m$ da. Hortaz, $m' = m$ da, eta hortik $G = T$ aterako dugu. □

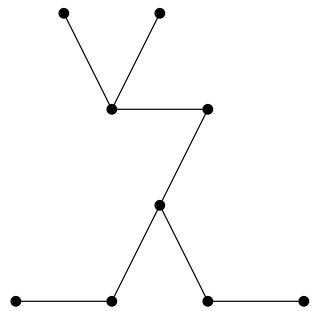
5.10.3 Zuhaitz errodunak. Zuhaitz bitarrak

5.83 Definizioa. *Izan bedi G grafo zuzendua. G grafoa* zuhaitz zuzendua *dela esango dugu G grafoaren grafo ez-zuzendu elkartua zuhaitza bada.*

5.84 Adibidea.



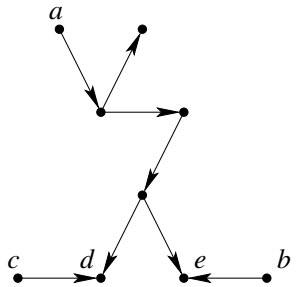
Zuhaitz zuzendua



Zuhaitz ez–zuzendu elkartua

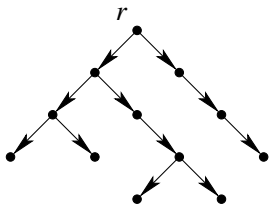
5.85 Definizioa. *G zuhaitz zuzendua bada, G zuhaitza* zuhaitz erroduna *dela esango dugu r erpin bakarra badago (*erro *deituko duguna), non $d^-(r) = 0$ den eta gainerako x erpinetarako $d^-(x) = 1$ den. Bestela,* zuhaitz erro gabea *dela esango dugu.*

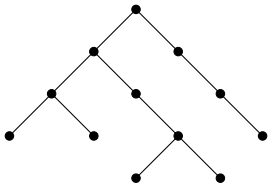
5.86 Adibidea.



Zuhaitz erro gabea

$d^-(a) = d^-(b) = d^-(c) = 0$; $d^-(e) = d^-(d) = 2$.





Zuhaitz erroduna

Ezkerreko zuhaitz erroduna geziak irudikatu gabe adieraz daiteke, ertzen noranzkoa goitik behera doala onartzen badugu.

5.87 Definizioa. *Izan bedi T zuhaitz erroduna:*

$d^+(v) = 0$ *betetzen duen edozein v erpini* hosto *edo* bukaerako erpin *deituko diogu. Gainerako erpinei* barne-erpin *edo* adarkatze-adabegi *deituko diegu.*

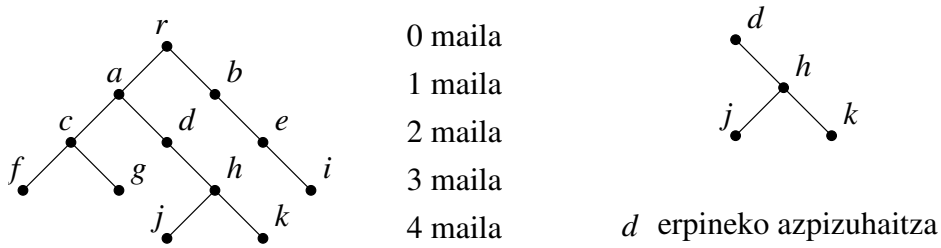
v erpina erroarekin lotzen duen bide bakarraren luzera l bada, v erpina l mailan *dagoela edo l* maila-zenbakia *duela esango dugu.*

v_1 eta v_2 erpinak izanik, v_1 erpinetik v_2 erpinera bide bat badago, v_1 erpina v_2 erpinaren arbasoa *edo v_2 erpina v_1 erpinaren* ondorengoa *dela esango dugu. Bidea* 1 *luzerakoa bada, v_1 erpina v_2 erpinaren* gurasoa *edo v_2 erpina v_1 erpinaren* umea *dela esango dugu.*

Bi erpinek guraso bera badute, senideak *direla esango dugu.*

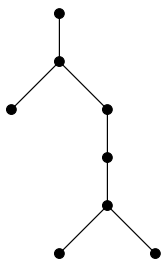
v erpinak eta bere ondorengo guztiek (baldin baditu) induzitutako azpigrafoari v erpineko azpizuhaitz *deituko diogu.*

5.88 Adibidea. Zuhaitz honetan, f, g, i, j eta k hostoak dira. a erpina k erpinaren arbasoa da. k erpina a erpinaren ondorengoa da. d erpina h erpinaren gurasoa da. h erpina d erpinaren umea da. c eta d senideak dira.



5.89 Definizioa. *Izan bedi $T = (V, E)$ zuhaitz erroduna. T zuhaitzaren hostoen maila-zenbaki handienari T zuhaitzaren* altuera *deituko diogu.*

5.90 Adibidea.

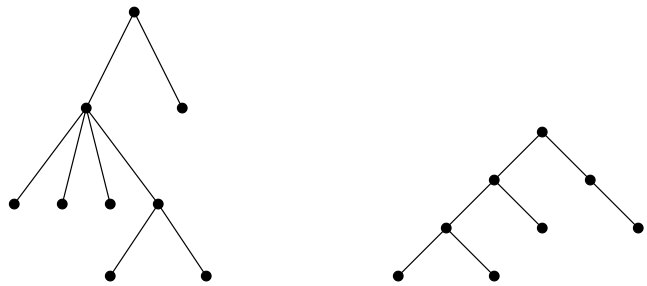


zuhaitzak $a = 5$ altuera du.

5.91 Definizioa. *Izan bedi $T = (V, E)$ zuhaitz erroduna, eta p zenbaki oso positiboa.*

Esango dugu T zuhaitz p-tarra *dela $d^+(x) \leq p$ bada $x \in V$ guztietarako. ($p = 2$ bada,* zuhaitz bitarra *da).*

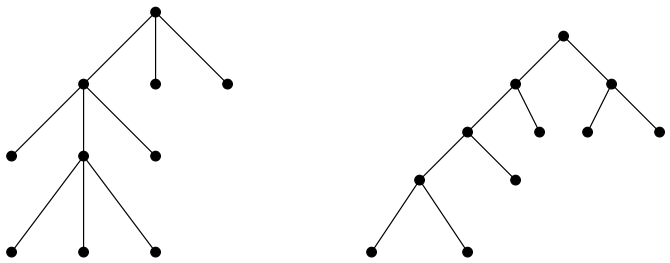
5.92 Adibidea.



Zuhaitz 4–tarra Zuhaitz bitarra

5.93 Definizioa. $T = (V, E)$ *zuhaitz erroduna* zuhaitz p-tar osotua *da* $d^+(x) = 0$ *edo* $d^+(x) = p$ *bada* $x \in V$ *guztietarako. (*$p = 2$ *bada,* zuhaitz bitar osotua *da).*

5.94 Adibidea.



Zuhaitz 3–tar osotua Zuhaitz bitar osotua

5.95 Teorema. *Izan bedi* $T = (V, E)$ n *erpin dituen zuhaitz* p*-tar osotua,* i *barne-erpinak eta* h *hostoak izanik. Orduan,*

(a) $n = pi + 1$ *da.*

(b) $h = (p - 1)i + 1$ *da.*

(c) $i = \dfrac{h-1}{p-1} = \dfrac{n-1}{p}$ *da.*

Froga.

(a) Izan bedi a T zuhaitzaren altuera.

$k = 0, 1, \ldots, a$ bakoitzeko, n_k eta i_k k mailan dauden erpin guztien kopuruak eta barne-erpinen kopuruak izango dira, hurrenez hurren. Orduan, $n_0 = 1$ da eta

$$n_k = i_{k-1}p, \quad k = 1, \ldots, a.$$

Hortaz,

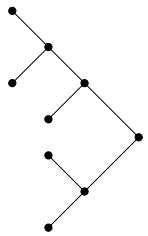
$$n = \sum_{k=0}^{a} n_k = 1 + \sum_{k=1}^{a} i_{k-1}p = 1 + p\sum_{k=1}^{a} i_{k-1} = 1 + pi.$$

(b) $pi + 1 = n = i + h$ da. Beraz, $h = pi - i + 1 = (p - 1)i + 1$ izango da.

(c) (a) eta (b) ataletatik ondorioztatuko dugu. □

5.96 Adibidea. 5.94 Adibideko zuhaitz 3-tar osotuan, $p = 3$, $h = 7$, $i = 3$ eta $n = 10$ dira. Eta, beraz, (a) $10 = 3 \cdot 3 + 1$, (b) $7 = 2 \cdot 3 + 1$ eta (c) $3 = \frac{6}{2} = \frac{9}{3}$ betetzen dira.

5.97 Adibidea. Bost bikotek mus txapelketa batean parte hartzen dute, non bikote bat kanporatzen den partida bat galtzen duenean. Txapelketa 5 hosto dituen zuhaitz bitar osotu baten bidez adieraz daiteke:



Txapeldunak izendatzeko jokatu behar diren partida-kopurua barne-erpinen kopurua da. 5.95 Teoremaren arabera, $i = \frac{h-1}{p-1} = \frac{5-1}{2-1} = 4$.

Oro har, bikoteen kopurua h bada, partiden kopurua $i = \frac{h-1}{p-1} = h - 1$ izango da.

5.98 Adibidea. Laborategi bateko ordenagailuak 4 irteera dituen hormako entxufe batean konektatu behar ditugu. Konexioak 4 irteerako luzapen-kableen bidez egingo ditugu. 7 luzapen-kable baditugu, zenbat ordenagailu konekta ditzakegu?

Hormako entxufea zuhaitz 4-tar osotu baten erroa bezala har dezakegu. Kable bakoitza barne-erpina izango da, eta ordenagailu bakoitza hosto bat. Barne-erpinen kopurua, beraz, $i = 7 + 1$ da (luzapen-kableak eta hormako entxufea).

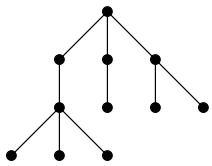
5.95 Teoremaren arabera, ordenagailuen kopurua $h = (p-1)i + 1 = (4-1)8 + 1 = 25$ da.

5.99 Definizioa. *Izan bedi T a altuerako zuhaitz bat. T* zuhaitz orekatua *dela esango dugu hosto bakoitzaren maila-zenbakia a edo $a - 1$ denean.*

5.100 Adibideak.

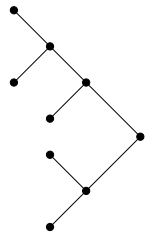
1. 5.90 Adibideko zuhaitza ez da orekatua, hosto bat 2 mailan eta beste bi 5 mailan dauzkalako.

2. Zuhaitz hau $a = 3$ altuerako zuhaitz orekatua da:



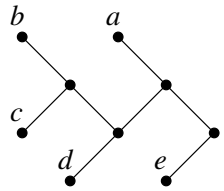
5.101 Adibidea. 5.97 Adibideko zuhaitzak orekatua izan behar du, txapelketa ahalik eta zuzenena izan dadin. Ez bada orekatua, bikoteren batek aukera bat baino gehiago izango du hurrengo fasera pasatzeko partida gutxiago jokatuz.

Txapelketaren zuhaitza hau bada



$a = 3$ altuerako zuhaitz orekatua da. Bikote batek, txapeldun izateko, bi edo hiru partida jokatu beharko ditu.

Txapelketaren zuhaitza, aldiz, hau bada



ez da orekatua. Irabazteko, b eta c bikoteek 4 partida jokatu beharko dituzte, d bikoteak 3 partida, a bikoteak 2 partida eta e bikoteak partida 1 bakarrik.

Idazkera. $x \in \mathbb{R}$ izanik, $\lceil x \rceil$ (x-ren sabaia) x baino handiagoa edo berdina den zenbaki oso txikiena da.

5.102 Adibidea. $\lceil 3.2 \rceil = 4$, $\lceil -5.7 \rceil = -5$, $\lceil 8 \rceil = 8$.

5.103 Teorema. *Izan bedi $T = (V, E)$ a altuerako eta h hostoko zuhaitz p-tar osotua ($p > 1$). Orduan, $h \leq p^a$ eta $a \geq \lceil \log_p h \rceil$ beteko dira.*

Froga.

$h \leq p^a$ a-ren gaineko indukzioaz frogatuko dugu.

$a = 0$ bada, $n = h = 1$ eta $p^a = p^0 = 1$ izango dira; orduan, $h = p^a$ betetzen da.

Demagun emaitza zuzena dela $a \leq k$ denean, eta izan bedi $a = k + 1$.

T zuhaitzaren h hostoen maila-zenbaki posibleak $1, \ldots, a$ dira, eta, gutxienez, p hosto daude a mailan.

Har ditzagun erroaren p umeak, eta izan bitez $T_1, \ldots, T_p$ erroak erpin horietan dituen azpizuhaitzak (zuhaitz p-tar osotuak dira). T_i zuhaitzaren hosto-kopurua h_i eta altuera a_i badira, $i = 1, \ldots, p$ izanik, $a_i \leq a - 1$, $i = 1, \ldots, p$, eta $h = h_1 + \ldots + h_p$ izango dira.

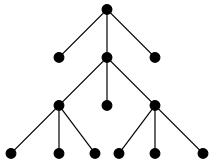
$a_i \leq a - 1 = k$ denez, $i = 1, \ldots, p$ izanik, indukzio-hipotesiaren arabera,

$h_i \leq p^{a_i} \leq p^{a-1}$ izango dugu, $i = 1, \ldots, p$. Hortaz, $h = h_1 + \ldots + h_p \leq p(p^{a-1}) = p^a$.

Ondorioz, $h = p^a$ betetzen da a guztietarako.

$h \leq p^a$ denez, $\log_p h \leq \log_p(p^a) = a$ izango dugu, eta $a \in \mathbb{Z}$ denez, $a \geq \lceil \log_p h \rceil$ aterako dugu. □

5.104 Adibidea. Zuhaitz honetan



$p = 3$, $a = 3$, $h = 9$ dira. Orduan, $9 \leq 3^3$ eta $3 \geq \lceil \log_3 9 \rceil = \lceil 2 \rceil = 2$ betetzen dira.

5.105 Korolarioa. *Izan bedi $T = (V, E)$ a altuerako eta h hostoko zuhaitz p-tar osotu orekatua ($p > 1$). Orduan, $a = \lceil \log_p h \rceil$ beteko da.*

Froga.

$a = 0$ bada, $h = 1$ eta $\lceil \log_p h \rceil = \lceil \log_p 1 \rceil = \lceil 0 \rceil = 0 = a$ izango dira.

$a > 0$ bada, $a - 1$ mailan, gutxienez, barne-erpin bat dago ($i_{a-1} > 0$). $k = 0, 1, \ldots, a$ balioetarako n_k, i_k eta h_k k mailan dauden erpin guztien kopurua, barne-erpinen kopurua eta hostoen kopurua dira, hurrenez hurren. Orduan, $n_0 = 1$ eta

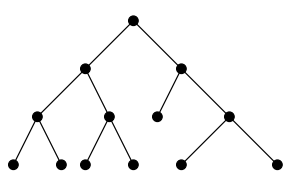
$$n_k = i_{k-1}p, \quad k = 1, \ldots, a.$$

Horrez gain, orekatua izateagatik, $h_k = 0$ eta $n_k = i_k$, $k = 0, \ldots, a - 2$ dira. Hortaz, $n_{a-1} = n_{a-2}p = n_{a-3}p^2 = \ldots = n_0 p^{a-1} = p^{a-1}$ eta $h = h_{a-1} + h_a = h_{a-1} + i_{a-1}p =$ $= h_{a-1} + i_{a-1} + i_{a-1}(p-1) > h_{a-1} + i_{a-1} = n_{a-1} = p^{a-1}$.

Hau da, $h > p^{a-1}$ betetzen da. Hortik, $\log_p h > \log_p(p^{a-1}) = a - 1$ izango dugu. Gainera, 5.103 Teoremaren arabera, $\log_p h \leq a$ betetzen da.

Hortaz, $a = \lceil \log_p h \rceil$. □

5.106 Adibidea.



$p = 2$, $a = 3$, $h = 7$ dira. Eta $3 = \lceil \log_2 7 \rceil = \lceil 2' \ldots \rceil = 3$ betetzen da.

6. Kapitulua

Konbinatoria

6.1 Sarrera

Konbinatoriaren helburua konfigurazioak aztertzea da. *Konfigurazio* bat objektuen antolaketa jakin bat da. Konfigurazio bat bilatzen da objektu batzuk aldez aurretik finkatutako murriztapen batzuk errespetatuz jarri nahi diren bakoitzean.

Adibidez, O eta X objektuak eta K_1 eta K_2 kaxak baditugu, bi objektuak bi kaxetan sartzeko modu bakoitza konfigurazio bat da.

K_1	K_2
O, X	

K_1	K_2
X	O

K_1	K_2
O	X

K_1	K_2
	O, X

Demagun, orain, bidaiari batek 50 herri bisitatu behar dituela, eta abiapuntura itzuli. Behin bakarrik bisitatu nahi du herri bakoitza. Ibilbide posible bakoitza konfigurazio bat da.

Konbinatorian lau alderdi hartu behar dira kontuan: existentzia, deskribapena, zenbaketa eta optimizazioa.

<u>Existentzia</u>. Konfigurazio ezezagun baten bilaketaren problema da. Horrelako konfiguraziorik egongo al da?

Adibidez, bidaiariaren probleman, herri bakoitzetik behin pasatzen den ibilbiderik ba al dago?

Beste kasu batean, osa daiteke zenbaki oso positiboen 3×3 matrize bat, haren errenkada, zutabe eta diagonal guztien batura 15 izan dadin?

<u>Deskribapena</u>. Konfigurazio guztien deskribapena konfigurazio guztien zerrenda egitean datza.

Ikus dezagun zein diren bi objektu hiru kaxatan sartzeko moduak:

K_1	K_2	K_3
O, X		

K_1	K_2	K_3
	O, X	

K_1	K_2	K_3
		O, X

K_1	K_2	K_3
X	O	

K_1	K_2	K_3
X		O

K_1	K_2	K_3
O	X	

K_1	K_2	K_3
	X	O

K_1	K_2	K_3
O		X

K_1	K_2	K_3
	O	X

Bidaiariaren probleman, ibilbide guztien zerrenda egitea da.

Zenbaketa. Konfigurazio guztien zenbaketaren problema konfigurazio posible guztien kopurua lortzen saiatzea da. Konbinatoriaren alderdirik ezagunena da. Gu alderdi horretaz baino ez gara arduratuko.

Adibidez, zenbat modu daude mahai baten inguruan 6 lagun esertzeko?

Bi objektu bi kaxatan sartzeko, 4 modu daude. Hiru kaxatan bi objektu sartzeko, 9 modu daude. Bidaiariaren probleman, ibilbide kopurua zehaztea da.

Optimizazioa. x konfigurazio bakoitzari $f(x)$ balio bat esleitzen zaio eta $f(x)$ minimoa egiten duen konfigurazioa bilatuko da. Hau da, x_0 konfigurazio bat bilatuko da, non $f(x_0) \leq f(x)$ beteko den x konfigurazio guztietarako.

Bidaiariaren problemari dagokionez, x ibilbide bakoitzari $f(x) = x$-ren kilometro kopurua esleitzen zaio. Ibilbiderik laburrena bilatuko da.

6.2 Baturaren eta biderkaduraren arauak

Esperimentu deituko diogu hainbat emaitza behagarri dituen prozesu bati. Adibidez, dado bat jaurti (6 emaitza posible), txanpon bat eta dado bat batera jaurti (12 emaitza posible), bi objektu bi kaxatan sartu (4 emaitza posible), 300 ikasleren artean ordezkari bat aukeratu (300 emaitza posible).

Esperimentu baten emaitza posibleen kopurua zenbatzeko, oinarrizko bi printzipio erabiliko ditugu: *baturaren araua* eta *biderkaduraren araua*. Problema konplexuak oinarrizko ideia horien bidez ebatz daitezkeen problema sinpleagoetan banatzen dira.

Problema horiek deskonposatzeko eta gure soluzio partzialak egokitzeko gaitasuna garatu nahi dugu, azken erantzunera iristeko.

Baturaren araua: Esperimentu batek m emaitza posible baditu eta beste esperimentu batek n emaitza posible baditu, bi esperimentuetako edozein egiten dugunean (ez biak batera) $m + n$ emaitza posible daude.

Oharra. Esperimentu batek m emaitza posible dituela diogunean, m emaitza horiek desberdinak direla pentsatuko dugu, kontrakoa adierazten ez bada behintzat.

Biderkaduraren araua: Esperimentu batek m emaitza posible baditu eta beste esperimentu batek n emaitza posible baditu, bi esperimentuak egiten ditugunean, $m \cdot n$ emaitza posible daude.

6.1 Adibidea. Enpresa batean bi atal daude: A atala 50 langilerekin eta B atala 30 langilerekin. Zenbat aukera daude:

a) enpresaren ordezkari bat hautatzeko? $50 + 30 = 80$ forma daude.

b) atal bakoitzeko ordezkari bat hautatzeko? $50 \cdot 30 = 1.500$ forma daude.

Arauak bi esperimentu baino gehiagotan aplika daitezke.

6.2 Adibidea. Akademia batek Logikako 3 ikastaro, Konbinatoriako 5 ikastaro eta Aljebrako 2 ikastaro eskaintzen ditu. Zenbat aukera ditu pertsona batek

a) ikastaro batean izena emateko? $3 + 5 + 2 = 10$ aukera daude.

b) gai bakoitzeko ikastaro batean izena emateko? $3 \cdot 5 \cdot 2 = 30$ aukera daude.

Batzuetan, bi arauak konbinatu behar izaten dira problema bat ebazteko.

6.3 Adibidea. Matrikula-plaka batek 6 digitu ditu edo 2 letra eta jarraian 4 digitu. Zenbat matrikula-plaka daude

a) letrak eta digituak ezin badira errepikatu? $10\cdot9\cdot8\cdot7\cdot6\cdot5+26\cdot25\cdot10\cdot9\cdot8\cdot7 = 3.427.200$ plaka daude.

b) letrak ezin badira errepikatu, baina digituak bai? $10^6 + 26 \cdot 25 \cdot 10^4 = 7.500.000$ plaka daude.

6.3 Aldakuntzak. Permutazioak

Biderkaduraren araua erabiliz, ordena edo diseinu jakin baten arabera jarritako objektuen antolamenduak zenbatuko dira.

6.4 Definizioa. *n objektu dituen bilduma bat izanik, r tamainako* aldakuntza *deituko diogu n objektuen artetik aukeratutako r objekturen ordenazio bakoitzari.*

n objektuko bilduma bateko errepikapenik gabeko r tamainako aldakuntzen kopurua $V(n,r)$ adieraziko dugu. Kasu horretan, $0 \leq r \leq n$ izan behar du.

n objektuko bilduma bateko r tamainako errepikatuzko aldakuntzen kopurua $VR(n,r)$ adieraziko dugu. Kasu horretan, $0 \leq r$ izan behar du.

6.5 Adibidea. a, b, c hiru objektuak baditugu:

a) 2 tamainako aldakuntzak:

- errepikapenik ez badago: ab, ac, ba, bc, ca, cb.

- errepikapenak onartzen badira: $aa, ab, ac, ba, bb, bc, ca, cb, cc$.

b) 3 tamainako aldakuntzak:

- errepikapenik ez badago: $abc, acb, bac, bca, cab, cba$.

- errepikapenak onartzen badira: $aaa, aab, aac, aba, abb, abc, \ldots$.

Aldakuntzen kopuruak kalkulatzen.

10 objektu baditugu, $A, B, C, D, E, F, G, H, I$ eta J, 4 tamainako aldakuntza kopurua zenbatzeko, posizioak eta posizio bat okupatzeko aukeratu daitezkeen objektuen kopurua hartuko ditugu kontuan. Posizio bat okupatzea esperimentu bat da.

- Errepikapenik onartzen ez bada: lehen posiziorako 10 emaitza posible daude. Bigarren posiziorako 9 daude, hirugarrenerako 8 daude, eta laugarrenerako 7. Biderkaduraren arauaren arabera, 4 tamainako aldakuntza kopurua hau da: $V(10,4) = 10\cdot9\cdot8\cdot7 = 5.040$. (Emaitza bera lortzen da posizioak beste ordena batean betetzen badira)

- Errepikapenak onartzen badira: posizio bakoitzean 10 emaitza posible daude. Biderkaduraren arauaren arabera, 4 tamainako errepikatuzko aldakuntzen kopurua, orain, $VR(10,4) = 10 \cdot 10 \cdot 10 \cdot 10 = 10.000$ da.

Oro har, n objektu $a_1, \ldots, a_n$ baldin baditugu, r tamainako aldakuntza kopurua modu berean kalkulatzen da:

- Errepikapenik gabe ($r \leq n$ izan behar du): lehen posiziorako n emaitza posible daude; bigarrenerako $n-1$ daude; hirugarrenerako $n-2$ daude; eta r. posiziorako $n-r+1$

daude. Biderkaduraren arauaren arabera, n objektuko bilduma bateko errepikapenik gabeko r tamainako aldakuntza kopurua hau da:

$$\boxed{V(n,r) = n \cdot (n-1) \cdots (n-r+1), \quad 1 \leq r \leq n.}$$

$r = 0$ bada, errepikapenik gabeko 0 tamainako aldakuntza kopurua $\boxed{V(n,0) = 1}$ da.

- Errepikapenekin ($r > n$ ere izan daiteke): posizio bakoitzean n emaitza posible daude. Biderkaduraren arauaren arabera, n objektuko bilduma bateko r tamainako *errepikatuzko aldakuntza* kopurua honako hau da:

$$\boxed{VR(n,r) = n^r, \quad 0 \leq r.}$$

6.6 Definizioa. *$n \geq 0$ zenbaki oso bat izanik, n-ren* faktoriala*, $n!$, honela definitzen da:*

$$\begin{aligned} &0! = 1, \\ &n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1, \quad n \geq 1. \end{aligned}$$

Ondorio gisa, edozein n zenbaki osotarako: $(n+1)! = (n+1) \cdot n!$.

Faktorialen idazkera erabiliz, aurreko emaitzak honela idatziko ditugu:

$$V(n,r) = n \cdot (n-1) \cdots (n-r+1) = \frac{n \cdot (n-1) \cdots (n-r+1) \cdot (n-r) \cdots 3 \cdot 2 \cdot 1}{(n-r) \cdots 3 \cdot 2 \cdot 1} =$$

$$= \frac{n!}{(n-r)!}, \quad 1 \leq r \leq n.$$

$r = 0$ kasuan, $V(n,0) = \dfrac{n!}{n!} = 1$.
Hau da,

$$\boxed{V(n,r) = \frac{n!}{(n-r)!}, \quad 0 \leq r \leq n.}$$

6.7 Definizioa. *$r = n$ denean, n tamainako aldakuntzei n objektuen* permutazio *esaten zaie. Hau da, n objektu desberdineko permutazioa n objektuen antolamendua da.*

6.8 Adibidea. a, b eta c hiru objektu desberdinen permutazioak abc, acb, bac, bca, cab eta cba dira.

n objektu desberdinen permutazio kopurua objektu horien ordenazio kopurua da, eta $P(n)$ adieraziko dugu:

$$\boxed{P(n) = V(n,n) = n!.}$$

6.9 Adibideak.

1. 10 laguneko talde bati argazkia atera nahi diogu eserleku batean.

   a) Zenbat modutara eser daitezke? $P(10) = 10! = 3.628.800$.

   b) 10 lagunetatik 4ren argazkia atera nahi badugu, zenbat aukera daude?

   $V(10,4) = \dfrac{10!}{6!} = 10 \cdot 9 \cdot 8 \cdot 7 = 5.040$.

2. (*Permutazio zirkularrak*) 5 pertsona, A, B, C, D eta E, mahai borobil baten inguruan esertzen badira, zenbat ordenazio zirkular desberdin egin daitezke?

   Bi ordenazio zirkular berdinak dira horietako bat beste baten biraketa denean. Adibidez, $ABCDE = BCDEA = CDEAB = DEABC = EABCD$.

   Ordenazio (permutazio) zirkular bakoitzeko 5 permutazio lineal daude. Beraz, permutazio zirkularren kopuruari $PC(n)$ deitzen badiogu, hau izango dugu:

   $$P(5) = 5 \cdot PC(5)$$

   eta hortik, $PC(5) = \dfrac{P(5)}{5} = \dfrac{5!}{5} = 4! = 24$.

   Kalkulatzeko beste modu bat A posizioa finkatzea izango litzateke. Kasu horretan, $PC(5) = P(4) = 4!$.

   Orokorrean, esan dezakegu $\boxed{PC(n) = P(n-1) = (n-1)!}$ dela.

3. Zenbat modutan eser daitezke 5 lagun, A, B, C, D eta E, mahai borobil baten inguruan, C lagunak B-ren eskuinean eseri nahi badu?

   Bi posizio finkatzen dira; beraz, erantzuna $P(3) = 3! = 6$ da.

4. Zenbat modutan ordena daitezke $LAPIKO$ hitzaren letrak? $P(6) = 6! = 720$.

Errepikatuzko permutazioen kopuruak kalkulatzen.

Demagun, orain, n objekturen ordenazioen kopurua kalkulatu nahi dugula, eta horietako batzuk errepikatuta daudela: lehen motako n_1 objektu daude, bigarren motako n_2, ..., eta r. motako n_r, non $n_1 + n_2 + \cdots + n_r = n$ baita. Ordenazio kopurua $PR_{n_1,n_2,\ldots,n_r}(n)$ adieraziko dugu.

6.10 Adibideak.

1. Zenbat modutan ordena daitezke AMA hitzaren letrak?

   A letrak bereizten baditugu A_1 eta A_2, $P(3) = 3! = 6$ forma izango dugu: A_1MA_2, A_2MA_1, A_1A_2M, A_2A_1M, MA_1A_2 eta MA_2A_1.

   A letrak bereizten ez baditugu, $A_1MA_2 = A_2MA_1 = AMA$, $A_1A_2M = A_2A_1M = AAM$ eta $MA_1A_2 = MA_2A_1 = MAA$ izango ditugu. Beraz, A letrak bereizten ez dituen permutazio bakoitzari A letrak bereizten dituen bi permutazio dagozkio. Hortaz,

$$P(3) = 2 \cdot PR_{2,1}(3).$$

$$PR_{2,1}(3) = \frac{P(3)}{2} = \frac{3!}{2} = 3.$$

2. Zenbat modutan ordena daitezke $ATAZA$ hitzaren letrak?

   Letrak bereizita, $(A_1TA_2ZA_3)$: $P(5)$; eta letrak bereizi gabe, $(ATAZA)$: $PR_{3,1,1}(5)$. Hortaz,

$$P(5) = 3! \cdot PR_{3,1,1}(5).$$

$$PR_{3,1,1}(5) = \frac{P(5)}{3!} = \frac{5!}{3!} = 20.$$

3. Zenbat modutan ordena daitezke $OROKOR$ hitzaren letrak?

   Letrak bereizita, $(O_1R_1O_2KO_3R_2)$: $P(6)$; R letrak bereizi gabe $(O_1RO_2KO_3R)$: $PR_{2,1,1,1,1}(6)$; eta O letrak bereizi gabe, $(OROKOR)$: $PR_{2,3,1}(6)$. Hortaz,

$$P(6) = 2! \cdot PR_{2,1,1,1,1}(6) = 2! \cdot 3! \cdot PR_{2,3,1}(6).$$

$$PR_{2,3,1}(6) = \frac{P(6)}{2!3!} = \frac{6!}{2!3!} = 60.$$

Oro har, n objektu badaude, lehenengo motako n_1, bigarren motako n_2, ..., r. motako n_r, non $n_1 + n_2 + \cdots + n_r = n$ baita, n objektuen *errepikatuzko permutazio* kopurua honako hau da:

$$\boxed{PR_{n_1,\ldots,n_r}(n) = \frac{n!}{n_1! \cdots n_r!}, \qquad n_1 + n_2 + \cdots + n_r = n.}$$

6.11 Adibideak.

1. Zenbat mezu desberdin sor daitezke Morse kodeko 3 marratxo eta 2 puntu erabiliz?

$$PR_{3,2}(5) = \frac{5!}{3!2!} = 10.$$

2. Zenbat modutan margotu ditzakegu 12 gela 3 gela berde, 2 gela arrosa, 2 gela hori eta gainerakoak zuriak izateko moduan?

$$PR_{3,2,2,5}(12) = \frac{12!}{3!2!2!5!} = 166.320.$$

6.4 Konbinazioak

6.12 Definizioa. Errepikapenik gabeko r tamainako konbinazio *deituko diogu, n objekturen artean r objektu aukeratzeko modu bakoitzari, zein ordenatan aukeratzen diren kontuan hartu gabe.*

n objekturen errepikapenik gabeko r tamainako konbinazioen kopurua $C(n,r)$ adieraziko dugu.

6.13 Adibidea. 10 kideko erakunde batean, $A, B, C, D, E, F, G, H, I$ eta J, lehendakaria, idazkaria eta diruzaina aukeratu behar baditugu, ordenazio kopurua honako hau izango da: $V(10,3) = 10 \cdot 9 \cdot 8 = 720$. Kontuan hartzen dugu ez dela gauza bera lehendakaria izatea, diruzaina izatea edo idazkaria izatea.

Baina 3 pertsonako batzorde bat aukeratzen badugu, kargu desberdinik ez badago, hautaketa-ordenak ez du axola. Izan ere, ABC, ACB, BAC, BCA, CAB eta CBA hirukoteek A, B eta C kideak batzorderako hautatuak izan direla adierazten dute; hots, $ABC = ACB = BAC = BCA = CAB = CBA$ dira. Beraz,

$$V(10,3) = 3! \cdot C(10,3).$$

$$C(10,3) = \frac{V(10,3)}{3!} = \frac{10!}{3!7!} = 120.$$

Konbinazioen kopuruak kalkulatzen.

Oro har, n objektuko bilduma bat izanik, r tamainako konbinazio bakoitzeko (ordenak ez du axola) r tamainako $P(r) = r!$ aldakuntza (ordenak garrantzia du) izango ditugu. Beraz, oro har, hau dugu:

$$\boxed{V(n,r) = P(r) \cdot C(n,r),}$$

eta hortik:

$$\boxed{C(n,r) = \frac{V(n,r)}{P(r)} = \frac{n!}{r!(n-r)!}, \quad 0 \leq r \leq n.}$$

$C(n,r)$ balioa $\binom{n}{r}$ eran ere idatzi ohi da eta n gain r *zenbaki* (edo *koefiziente*) *binomial* deitzen zaio.

$$\boxed{C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}, \quad 0 \leq r \leq n.}$$

6.14 Adibidea. Pertsona batek 20 lagun ditu eta 5 gonbidatu nahi ditu afaltzera. Zenbat modutan egin dezake hautaketa?

Ordena garrantzitsua ez denez, $C(20,5) = \binom{20}{5} = \frac{20!}{5!15!} = 15.504.$

Edozein zenbaketa-problemarekin aritzean, ordenak probleman duen garrantzia aztertu behar da. Ordenak garrantzia badu, aldakuntzak edo permutazioak hartu behar dira kontuan eta, bestela, konbinazioak.

6.15 Adibideak.

1. Azterketa batean, 12 galderako sorta batetik 8 galderari erantzun behar die ikasle batek. Zenbat modutan erantzun diezaioke azterketari?

   a) Murrizketarik gabe:

$$C(12,8) = \binom{12}{8} = \frac{12!}{8!4!} = 495.$$

   b) Lehenengo 5 galderetatik 2 erantzun behar baditu, eta azken 7 galderetatik 6:

$$C(5,2)C(7,6) = \binom{5}{2}\binom{7}{6} = \frac{5!}{2!3!}\frac{7!}{6!1!} = 10 \cdot 7 = 70.$$

   c) Lehenengo 5 galderetatik gutxienez 2 erantzun behar baditu (eta guztira 8):

   - lehenengo 5 galderetatik 2 erantzuten baditu: $\binom{5}{2}\binom{7}{6}$.

   - lehenengo 5 galderetatik 3 erantzuten baditu: $\binom{5}{3}\binom{7}{5}$.

   - lehenengo 5 galderetatik 4 erantzuten baditu: $\binom{5}{4}\binom{7}{4}$.

   - lehenengo 5 galderetatik 5 erantzuten baditu: $\binom{5}{5}\binom{7}{3}$.

   Guztira, $\binom{5}{2}\binom{7}{6} + \binom{5}{3}\binom{7}{5} + \binom{5}{4}\binom{7}{4} + \binom{5}{5}\binom{7}{3} = 70+210+165+35 = 490.$

   Oharra. c) kalkulatzeko, lehenengo 5 galderen artean 2 galdera hartzen baditugu, eta, gero, aukeratu ez diren 10 galderen artean 6 galdera hartzen baditugu, $\binom{5}{2}\binom{10}{6} = 2.100$, zenbait aukera hainbat aldiz zenbatzen ari gara. Adibidez, p_1 eta p_2 aukeratzen baditugu lehenengo 5 artean, eta gainerako 10en artean p_4, p_6, p_7, p_8, p_9 eta p_{10} azterketa hau izango dugu: $p_1, p_2, p_4, p_6, p_7, p_8, p_9, p_{10}$. Baina, lehenengo 5 galderen artean p_1 eta p_4 aukeratzen baditugu, eta p_2, p_6, p_7, p_8, p_9 eta p_{10} gainerako 10en artean, berriro ere $p_1, p_4, p_2, p_6, p_7, p_8, p_9, p_{10}$ azterketa izango dugu.

2. 3 digituko zenbat zenbaki daude?

   1 Digitu errepikaturik ez badute: $V(10,3) = 10 \cdot 9 \cdot 8 = \frac{10!}{7!} = 720.$

   2 Digitu errepikatuak izan baditzakete: $VR(10,3) = 10^3 = 1.000.$

   3 Digitu errepikaturik ez badute eta 5 zenbakiaz hasten badira:
   $V(9,2) = 9 \cdot 8 = \frac{9!}{7!} = 72.$

   4 Digitu errepikaturik ez badute eta 0 zenbakiaz ez badira hasten:
   $V(10,3) - V(9,2) = 10 \cdot 9 \cdot 8 - 9 \cdot 8 = 648.$

5 Digitu errepikatuak izan baditzakete eta 5 zenbakiaz hasten badira: $VR(10,2) = 10^2 = 100$.

6 Digitu errepikatuak izan baditzakete eta 0 zenbakiaz ez badira hasten: $VR(10,3) - VR(10,2) = 10^3 - 10^2 = 900$.

Problema batzuk bi ikuspuntutatik azter daitezke, permutazioenak edo konbinazioenak.

6.16 Adibidea. 21 laguneko talde batetik 7 laguneko 3 batzorde eratu behar dira (A, B eta C). Zenbat modutan egin daiteke?

Lehenengo batzorderako: $C(21,7) = \binom{21}{7}$ aukera.

Bigarren batzorderako: $C(14,7) = \binom{14}{7}$ aukera.

Hirugarren batzorderako: $C(7,7) = \binom{7}{7}$ aukera.

Guztira, $\binom{21}{7}\binom{14}{7}\binom{7}{7} = \frac{21!}{7!14!}\frac{14!}{7!7!}\frac{7!}{7!0!} = \frac{21!}{7!7!7!} = 399.072.960.$

Kalkulua honela ere egin genezakeen: 21 pertsonak lerroan jartzen ditugu, eta bakoitzaren azpian dagokion batzordea:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & \dots & 21 \\ A & A & B & B & \dots & B \end{array}$$

Horrela, A, B eta C letrak zazpina aldiz agertuko dira antolamendu bakoitzean. Hortaz, guztira izango ditugun antolamenduak hauek dira:

$$PR_{7,7,7}(21) = \frac{21!}{7!7!7!} = 399.072.960.$$

Problema batzuk ebazteko, permutazio eta konbinazio kontzeptuak behar dira.

6.17 Adibidea. Zenbat modutan ordena daitezke $ARABERAKOAN$ hitzaren letrak?

a) Murrizketarik gabe:

$$PR_{4,2,1,1,1,1,1}(11) = \frac{11!}{4!2!} = 831.600.$$

b) A horiek ezin badira ondoz ondoan agertu:

A gabe ($RBERKON$), $PR_{1,2,1,1,1,1}(7) = \frac{7!}{2!} = 2.520.$

A kokatzeko posizioak:

$$\begin{array}{ccccccccccccccc} & - & & - & & - & & - & & - & & - & & - & \\ \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \end{array}$$

Lau posizio aukeratu behar dira 8etatik: $C(8,4) = \binom{8}{4} = 70.$

Hortaz, guztira: $\frac{7!}{2!}\binom{8}{4} = 2520 \cdot 70 = 176.400.$

6.18 Propietateak.

Koefiziente binomialek propietate hauek betetzen dituzte:

1. $\binom{n}{0} = \binom{n}{n} = 1.$

2. $\binom{n}{r} = \binom{n}{n-r}, \quad 0 \leq r \leq n.$

3. $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}, \quad 1 \leq r \leq n-1.$

Froga.

Propietate bakoitzaren bi froga emango ditugu: lehenengoa koefiziente binomialen definizioa erabiliz; eta bigarrenean, koefiziente horiek interpretatuko ditugu.

1. a) Koefiziente binomialak

   $\binom{n}{0} = \frac{n!}{0!n!} = 1. \qquad \binom{n}{n} = \frac{n!}{n!0!} = 1.$

   b) Koefizienteen interpretazioa

   $\binom{n}{0}$ balioa n objekturen artean 0 objektu aukeratzeko moduen kopurua da. Hori modu bakarrean egin daiteke, bat ere aukeratu gabe.

   $\binom{n}{n}$ balioa n objekturen artean n objektu aukeratzeko moduen kopurua da. Hori modu bakarrean egin daiteke, denak aukeratuz.

2. a) Koefiziente binomialak

   $\binom{n}{r} = \frac{n!}{r!(n-r)!}. \qquad \binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!}.$

   b) Koefizienteen interpretazioa

   n objekturen artean r objektu hautatzeko moduen kopurua n objektuen artean $n-r$ objektu baztertzeko moduen kopuru bera da.

3. a) Koefiziente binomialak

   $\binom{n}{r} = \frac{n!}{r!(n-r)!}.$

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

   $$= \frac{(n-1)!}{(r-1)!(n-r)(n-r-1)!} + \frac{(n-1)!}{r(r-1)!(n-r-1)!} =$$

   $$= \frac{(n-1)!r + (n-1)!(n-r)}{r(r-1)!(n-r)(n-r-1)!} = \frac{(n-1)!(r+n-r)}{r!(n-r)!} = \frac{(n-1)!n}{r!(n-r)!} = \frac{n!}{r!(n-r)!}.$$

b) Koefizienteen interpretazioa

$a_1, \ldots, a_n$ n objekturen r tamainako ordenazio kopurua $\left(\binom{n}{r}\right)$ $a_2, \ldots, a_n$ objektuen $r-1$ tamainako ordenazioen kopurua $\left(\binom{n-1}{r-1}\right)$ gehi $a_2, \ldots, a_n$ objektuen r tamainako ordenazioen kopurua $\left(\binom{n-1}{r}\right)$ da. Lehenengoak a_1 dutenak dira, eta bigarrenak, berriz, a_1 ez dutenak. □

6.19 Teorema. *Teorema binomiala*
x eta y bi zenbaki erreal badira eta n zenbaki oso positibo bat bada:

$$(x+y)^n = \binom{n}{0} x^0 y^n + \binom{n}{1} x^1 y^{n-1} + \binom{n}{2} x^2 y^{n-2} + \cdots + \binom{n}{n} x^n y^0 =$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Froga.
Teorema binomiala n-ren gaineko indukzioaren bidez frogatuko dugu.
$n = 1$ denean, $(x+y)^1 = x + y$.
Bestalde, $\displaystyle\sum_{k=0}^{1} \binom{1}{k} x^k y^{1-k} = \binom{1}{0} x^0 y^1 + \binom{1}{1} x^1 y^0 = y + x = x + y$.
Demagun berdintza $n = p \geq 1$ denean betetzen dela, hau da,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \quad \text{(indukzio-hipotesia)}$$

betetzen dela.

Berdintza $n = p + 1$ baliorako ere betetzen dela frogatu behar dugu. Hau da, frogatu behar dugu:

$$(x+y)^{p+1} = \sum_{k=0}^{p+1} \binom{p+1}{k} x^k y^{p+1-k}.$$

$$(x+y)^{p+1} = (x+y)^p (x+y) = \left(\sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \right) (x+y) =$$

$$= \left(\sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \right) x + \left(\sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \right) y = \sum_{k=0}^{p} \binom{p}{k} x^{k+1} y^{p-k} + \sum_{k=0}^{p} \binom{p}{k} x^k y^{p+1-k}.$$

Alde batetik,

$$\sum_{k=0}^{p} \binom{p}{k} x^{k+1} y^{p-k} = \sum_{k=1}^{p+1} \binom{p}{k-1} x^k y^{p+1-k} = \sum_{k=1}^{p} \binom{p}{k-1} x^k y^{p+1-k} + \binom{p}{p} x^{p+1} y^0 =$$

$$= \sum_{k=1}^{p} \binom{p}{k-1} x^k y^{p+1-k} + x^{p+1}.$$

Beste aldetik,

$$\sum_{k=0}^{p} \binom{p}{k} x^k y^{p+1-k} = \binom{p}{0} x^0 y^{p+1} + \sum_{k=1}^{p} \binom{p}{k} x^k y^{p+1-k} = y^{p+1} + \sum_{k=1}^{p} \binom{p}{k} x^k y^{p+1-k}.$$

Eta biak elkartuz,

$$(x+y)^{p+1} = \sum_{k=1}^{p} \binom{p}{k-1} x^k y^{p+1-k} + x^{p+1} + y^{p+1} + \sum_{k=1}^{p} \binom{p}{k} x^k y^{p+1-k} =$$

$$= \sum_{k=1}^{p} \left[\binom{p}{k-1} + \binom{p}{k} \right] x^k y^{p+1-k} + x^{p+1} + y^{p+1}.$$

Kontuan izanik $\binom{p}{k-1} + \binom{p}{k} = \binom{p+1}{k}$ dela eta $\binom{p+1}{p+1} = \binom{p+1}{0} = 1$ dela, hau dugu:

$$(x+y)^{p+1} = \sum_{k=1}^{p} \binom{p+1}{k} x^k y^{p+1-k} + \binom{p+1}{p+1} x^{p+1} y^0 + \binom{p+1}{0} x^0 y^{p+1} =$$

$$= \sum_{k=0}^{p+1} \binom{p+1}{k} x^k y^{p+1-k}.$$

□

6.20 Adibideak.

1. $(x+y)^2 = \sum_{k=0}^{2} \binom{2}{k} x^k y^{2-k} = \binom{2}{0} x^0 y^2 + \binom{2}{1} x^1 y^1 + \binom{2}{2} x^2 y^0 = y^2 + 2xy + x^2.$

2. $(x+y)^3 = \sum_{k=0}^{3} \binom{3}{k} x^k y^{3-k} = \binom{3}{0} x^0 y^3 + \binom{3}{1} x^1 y^2 + \binom{3}{2} x^2 y^1 + \binom{3}{3} x^3 y^0 =$
   $= y^3 + 3xy^2 + 3x^2y + x^3.$

3. $(x+y)^4 =$
   $= \sum_{k=0}^{4} \binom{4}{k} x^k y^{4-k} = \binom{4}{0} x^0 y^4 + \binom{4}{1} x^1 y^3 + \binom{4}{2} x^2 y^2 + \binom{4}{3} x^3 y^1 + \binom{4}{4} x^4 y^0 =$
   $= y^4 + 4xy^3 + 6x^2y^2 + 4x^3y + x^4.$

6.21 Korolarioa. *x eta y bi zenbaki erreal badira eta n zenbaki oso positibo bat bada,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{n-k} x^k y^{n-k}.$$

Froga.

Nahikoa da kontuan izatea $\binom{n}{k} = \binom{n}{n-k}$ dela. □

6.22 Korolarioa. *Edozein n zenbaki oso positibotarako:*

a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$.

Froga.

a) $2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$.

b) $0 = (-1+1)^n = \binom{n}{0}(-1)^0 + \binom{n}{1}(-1)^1 + \binom{n}{2}(-1)^2 + \cdots + \binom{n}{n}(-1)^n =$

$= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n}$. □

6.23 Teorema. *Teorema multinomiala*

n eta t zenbaki oso positiboetarako eta $x_1, \ldots, x_t$ zenbaki errealetarako, $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ gaiaren koefizientea $(x_1 + x_2 + \cdots + x_t)^n$ garapenean hau da:

$$\frac{n!}{n_1! n_2! \cdots n_t!},$$

non n_i bakoitza zenbaki oso bat den, $0 \leq n_i \leq n$, $i = 1, \ldots, t$, eta $n_1 + n_2 + \cdots + n_t = n$ den.

Froga.

n-ren gaineko indukzioaren bidez frogatuko dugu.

$n = 1$ denean, $n_1 + n_2 + \cdots + n_t = n$ denez, $0 \leq n_i \leq 1$ izanik, $k \in \{1, \ldots, t\}$ existituko da, non $n_k = 1$ eta $n_i = 0$, $i \neq k$. Hortaz, $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t} = x_k$.

x_k gaiaren koefizientea $(x_1 + x_2 + \cdots + x_t)^1 = x_1 + x_2 + \cdots + x_t$ garapenean hau da:

$$1 = \frac{1!}{0! \cdots 1! \cdots 0!} = \frac{n!}{n_1! n_2! \cdots n_t!}.$$

Demagun $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ gaiaren koefizientea $(x_1 + x_2 + \cdots + x_t)^p$ berreturan $\dfrac{p!}{n_1! n_2! \cdots n_t!}$ dela (indukzio-hipotesia), $n_1 + n_2 + \cdots + n_t = p$ izanik.

Frogatu behar dugu $(x_1 + x_2 + \cdots + x_t)^{p+1}$ berreturan $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ gaiaren koefizientea $\dfrac{(p+1)!}{n_1! n_2! \cdots n_t!}$ dela, $n_1 + n_2 + \cdots + n_t = p + 1$ izanik.

$(x_1 + x_2 + \cdots + x_t)^{p+1} = (x_1 + x_2 + \cdots + x_t)^p (x_1 + x_2 + \cdots + x_t) =$
$= (x_1 + x_2 + \cdots + x_t)^p x_1 + (x_1 + x_2 + \cdots + x_t)^p x_2 + \cdots + (x_1 + x_2 + \cdots + x_t)^p x_t$ denez, $x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ gaiaren koefizientea $(x_1 + x_2 + \cdots + x_t)^p x_i$ batugai bakoitzean duen koefizienteen batura izango da, $i = 1, ..., t$.

$x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$ gaiaren koefizientea $(x_1 + x_2 + \cdots + x_t)^p x_i$ batugaian $x_1^{n_1} \cdots x_i^{n_i - 1} \cdots x_t^{n_t}$ gaiaren koefizientea da $(x_1 + x_2 + \cdots + x_t)^p$ berreturan. Hau da, $\dfrac{p!}{n_1! n_2! \cdots (n_i - 1)! \cdots n_t!}$.

Ondorioz, $(x_1+x_2+\cdots+x_t)^{p+1}$ berreturan $x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}$ gaiaren koefizientea hau da:

$$\sum_{i=1}^{t}\frac{p!}{n_1!n_2!\cdots(n_i-1)!\cdots n_t!}=\frac{p!}{(n_1-1)!n_2!\cdots n_t!}+\cdots+\frac{p!}{n_1!n_2!\cdots(n_t-1)!}=$$

$$=\frac{p!n_1+p!n_2+\cdots+p!n_t}{n_1!n_2!\cdots n_t!}=\frac{p!(n_1+n_2+\cdots+n_t)}{n_1!n_2!\cdots n_t!}=\frac{p(p+1)}{n_1!n_2!\cdots n_t!}=\frac{(p+1)!}{n_1!n_2!\cdots n_t!}.$$

□

6.24 Adibideak.

1. $(x+y+z)^8$ berreturan, $x^2y^3z^2$ gaiaren koefizientea $\dfrac{8!}{2!3!2!}=1.680$ da.
2. a) Aurkitu x^3y^5 gaiaren koefizientea $(x+y)^8$ berreturan.
   b) Aurkitu a^3b^5 gaiaren koefizientea $(2a-3b)^8$ berreturan.
   a) Koefizientea $\dbinom{8}{3}=56$ da.
   b) $x=2a$ eta $y=-3b$ eginez x^3y^5 gaian, hau geratuko da:
   $\dbinom{8}{3}x^3y^5=\dbinom{8}{3}(2a)^3(-3b)^5=\dbinom{8}{3}2^3(-3)^5a^3b^5=56\cdot 8\cdot(-243)a^3b^5=$
   $=-108.864a^3b^5$.
3. a) Aurkitu $x^2y^2z^4$ gaiaren koefizientea $(x+y+z)^8$ berreturan.
   b) Aurkitu a^2b^2 gaiaren koefizientea $(a+2b-3)^8$ berreturan.
   a) Koefizientea $\dfrac{8!}{2!2!4!}=420$ da.
   b) $x=a$, $y=2b$ eta $z=-3$ eginez $x^2y^2z^4$ gaian, hau geratuko da:

$$\frac{8!}{2!2!4!}x^2y^2z^4=\frac{8!}{2!2!4!}a^2(2b)^2(-3)^4=\frac{8!}{2!2!4!}2^2(-3)^4a^2b^2=$$
$$=420\cdot 4\cdot 81a^2b^2=136.080a^2b^2.$$

6.5 Errepikatuzko konbinazioak

6.25 Definizioa. *r tamainako errepikatuzko konbinazio deituko diogu n objektuen artean aukeratutako r objekturen ordenazio bakoitzari, r objektu horiek errepikatuta egon daitezkeelarik.*

6.26 Adibidea. $E=\{a,b,c,d,e,f\}$ multzoa izanik, 4 tamainako errepikatuzko konbinazioak aztertuko ditugu. Hau da, E multzotik 4 elementu hautatuko ditugu, baina aukera bakoitzean elementu errepikatuak egon daitezke.

Horrela, $aabb=abab=abba=baab=baba=bbaa\neq aaab$ daukagu.

E multzoaren elementuen artean ordena bat ezarriko dugu: $a<b<c<d<e<f$.

Ordena horri esker, 4 tamainako errepikatuzko konbinazioak ordena ditzakegu: *aaaa*, *aaab*, *aaac*, *aaad*, ...

Ordenazio kopurua zenbatzeko, beste modu batera adieraziko ditugu. Konbinazio bakoitzeko, agertzen diren letrak eta errepikatzen diren elementuak idatziko ditugu. Honela:

$aaaa$ konbinazioari $a123$ esleitzen diogu, a-k lehen posizioan a agertzen dela adierazten du, 1ak lehen elementua (a) errepikatu egiten dela adierazten du, 2ak bigarren elementua (a) errepikatu egiten dela eta 3ak hirugarren elementua (a) errepikatu egiten dela.

$$\begin{array}{ll} aaab & ab12 \\ aacc & ac13 \\ abdf & abdf \\ accc & ac23 \end{array}$$

Beraz, $\{a, b, c, d, e, f\}$ elementuen 4 tamainako errepikatuzko konbinazio bakoitzari $\{a, b, c, d, e, f, 1, 2, 3\}$ elementuen errepikapenik gabeko 4 tamainako konbinazio bat dagokio, eta alderantziz. Adibidez, $abe3$ konbinazioa $abee$ da, eta $af23$ konbinazioa $afff$.

Beraz, $\{a, b, c, d, e, f\}$ elementuen 4 tamainako errepikatuzko konbinazioen kopurua ($CR(6, 4)$) $\{a, b, c, d, e, f, 1, 2, 3\}$ elementuen errepikapenik gabeko 4 tamainako konbinazioen kopuruaren berdina da $\left(= C(6 + 3, 4) = \binom{9}{4}\right)$. Kontuan izan behar da 6 elementu ager daitezkeela eta 3 posizio errepika daitezkeela.

Oro har, n objektu ezberdin $a_1, \ldots, a_n$ izanik, objektu horien r tamainako errepikatuzko konbinazio bakoitzari $\{a_1, \ldots, a_n, 1, 2, \ldots, r-1\}$ (objektuak + posizio errepikagarriak) objektuen errepikapenik gabeko r tamainako konbinazio bat dagokio, eta alderantziz. Beraz,

$$\boxed{CR(n, r) = C(n + r - 1, r) = \binom{n + r - 1}{r}, \quad r \geq 0.}$$

(r n baino handiagoa izan daiteke errepikapenak onartzen direnean)

6.27 Adibideak.

1. Likore-denda batean 20 ardo-marka daude. 12 botila eskatu nahi baditugu, nola egin daiteke?

   Markak errepikatu daitezkeenez,

   $CR(20, 12) = C(20 + 12 - 1, 12) = \binom{31}{12} = 141.120.525.$

2. 7 txanpon desberdin banatu nahi dira 3 lagunen artean. Nola egin daiteke hori?

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ A & A & A & A & A & A & B \\ A & A & B & A & A & A & A \end{array}$$

   Bi banaketa horiek desberdinak dira, B lagunak jasotzen dituen 3. eta 7. txanponak desberdinak direlako.

   Beraz, hau da soluzioa: $VR(3, 7) = 3^7 = 2.187$.

3. 7 txanpon berdin 3 lagunen artean banatu nahi dira. Nola egin daiteke, baldin eta

   1 murrizketarik ez badago? (onartzen da lagun batek edo gehiagok ez dutela ezer jasotzen)

1	2	3	4	5	6	7
A	A	A	A	A	A	B
A	A	B	A	A	A	A

   Bi banaketa horiek berdinak dira, txanpon guztiak berdinak direlako.

   Beraz, hau da soluzioa: $CR(3,7) = \binom{3+7-1}{7} = \binom{9}{7} = 36.$

   2 lagun bakoitzak txanpon bat jaso behar badu gutxienez?

   Txanpon bat ematen diogu lagun bakoitzari, eta gainerakoak banatuko ditugu. Hau da,

   $$CR(3,4) = \binom{3+4-1}{4} = \binom{6}{4} = 15.$$

   3 lagun bakoitzak txanpon bat jaso behar du gutxienez, eta A lagunak 3 txanpon gutxienez?

   A-ri 3 txanpon eta B eta C-ri txanpon bana emango diegu, eta gainerakoa banatuko dugu:

   $$CR(3,2) = \binom{3+2-1}{2} = \binom{4}{2} = 6.$$

Ikusten dugunez, r objektu n hartzaileren artean banatzeko moduak hauek dira:
- objektuak desberdinak badira, $VR(n,r) = n^r$.
- objektuak berdinak badira, $CR(n,r) = \binom{n+r-1}{r}$.

6.28 Adibideak.

1. Zenbat modutan bana daitezke euro bateko 8 txanpon eta zentimo bateko 6 txanpon 4 lagunen artean, lagun bakoitzak gutxienez euro bat jaso dezan?

   Euro bana emango diegu lau lagunei, eta gainerakoa honela banatuko dugu:

   $$CR(4,4)CR(4,6) = \binom{7}{4}\binom{9}{6} = 2.940.$$

2. Zehaztu ondoko ekuazioaren soluzio osoen kopurua:

   $$x_1 + x_2 + x_3 + x_4 = 8, \quad x_i \geq 0, \quad i = 1,2,3,4.$$

   Soluzio bat, adibidez, hau da: $x_1 = 3, x_2 = 0, x_3 = 0, x_4 = 5$. Interpretazio bat izan daiteke 8 objektu berdin banatzen direla 4 hartzaileren artean (lehenak x_1 jasotzen ditu, bigarrenak x_2, ...). Hau da soluzio kopurua:

   $$CR(4,8) = \binom{11}{8} = 165.$$

Era berean,

$$x_1 + \cdots + x_n = r, \quad x_i \geq 0, \quad i = 1, \ldots, n,$$

ekuazioaren soluzio osoen kopurua r objektu berdin n hartzaile artean banatzeko modu kopuruaren berdina da, eta hau da kopuru hori:

$$CR(n, r).$$

6.29 Adibideak.

1. Zenbat soluzio oso ez-negatibo daude ondoko inekuaziorako?

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 < 10.$$

Soluzio kopurua kalkula dezakegu honako ekuaziorako soluzio kopurua kalkulatuz:

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = k, \quad 0 \leq k \leq 9.$$

Hortaz, guztira:

$$\sum_{k=0}^{9} CR(6, k).$$

Beste modu bat da

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 10, \quad x_i \geq 0, \quad i = 1, \ldots, 6, \quad 1 \leq x_7,$$

ekuazioaren soluzio osoen kopurua kalkulatzea da.

$y_7 = x_7 - 1, \quad y_7 \geq 0$ aldaketa egiten badugu, honela geratzen zaigu:

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + y_7 = 9.$$

Soluzio osoen kopurua, $x_i \geq 0, \quad i = 1, \ldots, 6, \quad 0 \leq y_7$ izanik, hau da:

$$CR(7, 9) = \binom{15}{9} = 5.005.$$

2. Zenbat gai daude $(x + y)^n$ berreturaren garapen binomialean?

Gai bakoitzak $\binom{n}{k} x^k y^{n-k}$ forma du. Beraz, gai kopurua $n_1 + n_2 = n$ ekuazioaren soluzio osoen kopurua da, $n_1, n_2 \geq 0$ izanik. Hau da,

$$CR(2, n) = \binom{2 + n - 1}{n} = \binom{n + 1}{n} = \frac{(n + 1)!}{n!1!} = n + 1.$$

3. Zenbat gai daude $(x + y + z + w)^{10}$ berreturaren garapenean?

Gai bakoitzak $\dfrac{10!}{n_1!n_2!n_3!n_4!} x^{n_1} y^{n_2} z^{n_3} w^{n_4}$ forma du, non $n_1 + n_2 + n_3 + n_4 = 10$ baita, $n_i \geq 0$, $i = 1, 2, 3, 4$, izanik.

Gai kopurua $= n_1 + n_2 + n_3 + n_4 = 10$ ekuazioaren soluzio osoen kopurua, $n_i \geq 0$, $i = 1, 2, 3, 4$ izanik.

$$CR(4, 10) = \binom{13}{10} = 286.$$

Bibliografia

Biggs, N. L. (1994). *Matemática discreta*. Vicens Vives, Barcelona.

Chang, C.-L. and Lee, R. C.-T. (1973). *Symbolic logic and mechanical theorem proving*. Computer Science and Applied Mathematics. Academic Press, New York.

Copi, I. M. (1979). *Lógica simbólica*. Compañía Editorial Continental, México.

Deaño, A. (1980). *Introducción a la lógica formal*. Alianza Universidad. Textos; 11. Alianza, Madrid.

García Merayo, F., Hernández Peñalver, G., and Nevot Luna, A. (2003). *Problemas resueltos de matemática discreta*. Paso a paso. Thomson-Paraninfo, Madrid.

Gibbons, A. (1985). *Algoritmic graph theory*. Cambridge University Press, Cambridge.

Grassmann, W. K. and Tremblay, J.-P. (1996). *Matemática discreta y lógica*. Prentice Hall, Madrid.

Grimaldi, R. P. (1997). *Matemáticas discreta y combinatoria: una introducción con aplicaciones*. Addison-Wesley Iberoamericana, Argentina.

Kleene, S. C. (1967). *Mathematical logic*. John Wiley & Sons, New York.

Lipson, M. and Lipschutz, S. (2004). *2000 problemas resuelto de matemática discreta*. McGraw-Hill, Madrid.

Liu, C. L. (1995). *Elementos de matemáticas discretas*. McGraw-Hill, México.

Ross, K. A. and Wright, C. R. (1992). *Discrete mathematics*. Prentice-Hall, Englewood Cliffs, New Jersey.

Kontzeptuen Aurkibidea

n moduluko kongruentzia, 73
-n egon, 60
    -n zeharo egon, 61

abiaburu multzo, 75
absurdora eramateko erregela, 28
adabegi, 116
    adarkatze-adabegi, 144
adarkatze-adabegi, 144
agerpen, 6, 36
    aske, 36
    lotu, 36
aldagai, 32, 34
    aske, 36
    aske x aldagairako, 53
    lotu, 36
aldakuntza, 151
errepikatuzko aldakuntza, 152
alderantzizko funtzio, 80
alfabeto, 6, 34
altuera, 144
amaiera, 116
anizkoiztasun, 117
antisimetri propietatea, 68
arau
    baturaren arau, 150
    biderkaduraren arau, 150
argumentu, 18
    baliogabe, 18, 43
    baliozko argumentu, 18, 43
    gaizki eraikita, 18
    ongi eraikita, 18
argumentu-eskema, 18
aritate, 34
aritmetikaren oinarrizko teorema, 102
arrazoibide
    baliozko, 1
    zuzen, 1
atomo, 6
átomo, 35
atzekari, 4
aurreirudi, 75
    elementu baten aurreirudi, 75
aurrekari, 4
auzokidetasun-matrize, 123
azpiformula, 6, 36
azpigrafo, 125
    induzitu, 126
    sortzaile, 126
azpimultzo, 60
    jator, 61
azpizuhaitz
    v erpineko azpizuhaitz, 144

baiezko proposizio partikularra I, 33
baiezko proposizio unibertsala A, 33
baldintzabiko, 5
baldintzazko, 4
baldintzazko frogaren erregela, 26
baliokidetasun-erlazio, 70
baliokidetasun-klase, 70
Baliokidetza material (BALIO), 14
baliozkotasunaren froga formal, 21
banatze-lege, 64
Banatze-legeak (BANA), 13
barne-erpin, 144
barruan eduki, 60
    zeharo eduki barruan, 61
begizta, 116
bide, 121
    hamiltondar, 134
    zuzendu, 121
biderkadura kartesiar, 66
bigarren osagai, 66
bihurtze-propietatea, 67
bikote (ordenatu), 66
bikote berdinak, 66
ongi definitutako bilduma, 60

bildura multzo, 63
bukaerako erpin, 144

De Morganen lege orokortuak, 65
De Morganen legeak, 64
De Morganen legeak (DeM), 14
dedukzio formal, 20
Dilema Eraikitzaile (DE), 19, 21
Dilema Suntsitzaile (DS), 19, 21
disjuntzio, 4
    esklusibo, 4, 9
    inklusibo, 4, 9
Disjuntzioaren Batuketa (DB), 20, 21

ebakidura multzo, 63
egia-balio, 8, 9, 40
egia-taula, 11
egiazko egin, 10
elementu, 59
elkartze-lege, 64
Elkartze-legea (ELKAR), 13
enuntziatu ireki, 33
enuntziatua itxi, 33
eragile logikoak, 6
eredu, 10
Eredu–teoria, 3
eremu, 37
erlazio
    antisimetriko, 68
    baliokidetasun-erlazio, 70
    bihurkor, 67
    bitar, 67
    iragankor, 68
    ordena osoko erlazio, 69
    ordena partzialeko erlazio, 69
    ordena-erlazio, 69
    simetriko, 68
erpin, 116
    arbaso, 144
    auzokide, 116
    barne-erpin, 144
    bukaerako erpin, 144
    guraso, 144
    isolatu, 116
    ondorengo, 144
    senide, 144
    ume, 144
    zintzilikatu, 118
v erpineko azpizuhaitz, 144
erregela
    absurdora eramateko erregela, 28
    baldintzazko frogaren erregela, 26
    inferentzia-erregela, 20
    ordezkapen-erregela, 23
    zenbatzaileen erregelak, 52
erro, 143
ertz, 116
    ez-zuzendu, 116
    intzidente, 116
Esportazio (ESP), 14
Euklidesen algoritmoa, 96
ezezko proposizio partikularra O, 33
ezezko proposizio unibertsala E, 33

faktorial, 152
faltsutu, 10
formula, 6
    atomiko, 35
    baliogabe, 11, 43
    baliozko, 11, 43
    inkontsistente, 11, 43
    itxi, 36
    kontsistente, 11, 43
    ongi eratutako (oef), 6, 35
formula logikoki baliokideak, 13, 47
Frogabidearen eta dedukzio naturalaren teoria, 3
funtzio, 74
    alderantzizko funtzio, 80
    bijektibo, 78
    identitate funtzio, 77
    injektibo, 78
    karakteristiko, 77
    konposatu, 80
    logiko, 38
    murrizketa funtzio, 77
    proposizio-funtzio, 32
    surjektibo, 78
funtzio berdinak, 76
funtzioen konposizioa, 80

gradu, 118
    irteera-gradu, 118
    sarrera-gradu, 118

graduerdi, 118
grafo, 76, 116
  k-erregular, 120
  k-grafo, 117
  bakun, 117
  diskonexu, 122
  erregular, 120
  eulertar, 130
  eulertar zuzendu, 134
  ez-zuzendu, 116
    elkartu, 117
  hamiltondar, 134
  konexu, 122
  nulu, 128
  osagarri, 128
  osotu, K_n, 127
  zatibiko grafo, 128
    osotu, K_{n_1,n_2}, 128
  zuzendu, 116
    konexu, 122
grafo isomorfoak, 129

hedapenaren arabera, 60
helburu multzo, 75
hondar, 90
hosto, 144

ibilaldi, 121
  ireki, 121
  itxi, 121
  nabaria, 121
  zuzendu, 121
idenpotentzia, 64
identitate funtzio, 77
inferentzia-erregela, 20
Inplikazio material (INP), 14
instantziazio, 32
interpretazio, 8, 39
Interpretazio-teoria, 3
interpretaziorako egiazkoa izan, 10
interpretaziorako faltsua izan, 10
iragate-propietatea, 68
irismen, 6, 36
irudi, 75, 77
irudi multzo, 78
isomorfismo, 129

jatorri, 116

kardinal, 60
kate, 121
  eulertar, 130
kendura multzo, 63
klase
  partiketa baten, 65
koefiziente binomial, 155
errepikatuzko konbinazio, 162
konbinazio, 155
konbinazio lineal, 87
konfigurazio, 149
kongruente modulu n, 73
konjuntzio, 4
Konjuntzioaren Konbinazio (KK), 19, 21
Konjuntzioaren Sinplifikazio (KS), 19, 21
konstante, 32, 34
kontraesan, 11, 27, 43
kuantifikatze, 33

lehen ordenako termino, 35
lehenengo osagai, 66
lengoaia
  objektu lengoaia, 2
logika
  formal, 1
logikoki deduzitu, 15, 43
lokailu, 3
lokailu logikoak, 6, 34
luzera, 121

maila, 144
maila-zenbaki, 144
matrize
  auzokidetasun-matrize, 123
metalengoaia, 2
Modus Ponens (MP), 19, 21
Modus Tollens (MT), 19, 21
multigrafo, 117
multiplo, 86
  komun, 99
multiplo komun txikiena (mkt), 99
multzo, 59
  abiaburu multzo, 75
  berdinak, 61
  bildura multzo, 63

disjuntuak, 63
ebakidura multzo, 63
erreferentzi multzo, 61
helburu multzo, 75
huts, 61
irudi multzo, 78
kendura multzo, 63
ongi ordenatu, 86
ordenatu, 69
osagarri, 62
osagarri multzo batean, 62
osoki ordenatu, 69
parteen multzo, 62
partzialki ordenatu, 69
potentzia multzo, 62
unibertsal, 61
zatidura multzo, 72
murrizketa funtzio, 77

objektu lengoaia, 2
ondorio, 18
ondorio logiko, 15, 43
ongi definitutako bilduma, 60
ordena onaren printzipioa, 86
ordena-erlazio, 69
ordezkapen-erregela, 23
ordezkapen-instantzia, 32
ordezkari, 72
orokortze, 33
osagai
bigarren osagai, 66
lehenengo osagai, 66
osagai konexu, 123

parte, 60
jator, 61
partiketa, 65
baten klase, 65
errepikatuzko permutazio, 154
permutazio, 152
zirkular, 153
Pragmatika, 2
predikatu, 3, 31, 34
Predikatu-logika, 3
premisa, 18
proposizio, 3
atomiko, 3
konposatu, 3
proposizio-funtzio, 32
Proposizio-logika, 3

RSA algoritmoa, 110

Semantika, 2
Semiotika, 2
Silogismo Disjuntibo (SD), 19, 21
Silogismo Hipotetiko (SH), 19, 21
simetri propietatea, 68
sinbolo inpropio, 35
sinbolo inpropioak, 6
Sintaxia, 2
subjektu, 31

tautologia, 11, 43
Tautologia (TAUT), 13
teorema
binomial, 159
multinomial, 161
termino, 3
lehen ordenako termino, 35
Transposizio (TRANS), 14
trukatze-lege, 64
Trukatze-legea (TRUK), 13

ukapen, 4
Ukapen bikoitza (UB), 13
ulerpenaren arabera, 60

v erpineko azpizuhaitz, 144

zatibiko grafo, 128
osotu, K_{n_1,n_2}, 128
zatidura, 90
zatidura multzo, 72
zatikizun, 90
zatitzaile, 86, 90
komun, 91
komun handien (zkh), 91
zenbaki
konposatu, 88
lehen, 88
zenbaki
arrazional, 60
arrunt, 60
binomial, 155

erreal, 60
konplexu, 60
lehen, 85
oso, 60
zenbaki lehen erlatiboak, 95
zenbatzaile
existentzial, 33, 34
unibertsal, 33, 34
zenbatzaileen erregelak, 52
ziklo, 121
hamiltondar, 134
zuzendu, 121
zirkuitu, 121
eulertar, 130
eulertar zuzendu, 134
zuhaitz, 139
p-tar, 144
osotu, 145
bitar, 144
osotu, 145
erro gabea, 143
errodun, 143
orekatu, 146
sortzaile, 139
zuzendu, 143