eman ta zabal zazu
UPV EHU
ZIENTZIA ETA TEKNOLOGIA FAKULTATEA
FACULTAD DE CIENCIA Y TECNOLOGÍA

50 URTE AÑOS 1968 - 2018
Biba Zientzia! Ciencia Viva

Trukatze probabilitatea taldeetan

Gradu Amaierako Lana
Matematikako Gradua

Iñigo Expósito Castro

Leire Legarreta Solaguren
Irakasleak zuzendutako lana

Leioa, 2026ko otsailaren 4a

Aurkibidea

Eskerrak

Eskerrak eman nahi dizkiot Leireri, memoria hau zuzendu didan irakasleari, bere laguntza, pazientzia, esfortzu eta inplikazioagatik. Hasieratik, arazo bat eduki dudan bakoitzean, ni laguntzeko prest egon delako. Bukatzeko, eskerrik beroenak eman nahi dizkiet nire familiari eta nire lagun guztiei. Lan hau ez nuke aurrera aterako zuen laguntzarik gabe.

Sarrera

Trukatze propietatea betetzen duten taldeei talde abeldar deritzegu. Aljebran talde hauen garrantzia nabaria da, honi esker elementuen arteko operaketak errazak direlako. Alabaina, talde guztiak ez dira abeldarrak, baina beti azter dezakegu zein gertu dagoen talde bat abeldarra izatetik. Propietate hauek aztertzeko tresna desberdinak erabiltzen dira. Alde batetik, abelinizazioa eta kommutadorearen propietateak erabilgarriak izan ohi dira. Bestalde, trukatze probabilitatearen kontzeptua aipatzea ezinbestekoa izango litzateke, kuantitatiboki neurtzen baitu talde baten abeldartasun maila.

Inolako zalantzarik gabe, talde teoria Aljebraren arlo aberatsa da. Are gehiago, Matematikako beste adar batzuen tresnak erabiliz, emaitza ugari frogatzea lortzen ditu ikuspuntu desberdinak erabiliz. Honen adibide dira konbinatoria eta grafo teoria, lan honetan zehar maiz erabiliko direnak.

Trukatze probabilitatearen kontzeptua taldearen egiturari buruzko emaitzak lortzeko erabili izan da, eta alderantziz, taldearen egitura ere erabili daiteke trukatze probabilitatearen behe eta goi borneak lortzeko. Adibidez, baldin eta G taldea, trinkoa bada, Gustafson-ek [9] lanean, G taldea abeldarra edo $P(G) = cp(G) \leq \frac{5}{8}$ dela frogatu zuen. Bestalde, baldin eta G taldea finitua bada, errepresentazio teoria erabiliz, [10]-n Lescot-ek, $P(G) > \frac{1}{2}$ izateak, G taldea nilpotentea eta G' azpitaldea gehienez 2 ordenakoa dela frogatu zuen. Matematikari berdinak [11] lanean, talde finitu bakunen teoria erabili gabe, $P(G) > \frac{1}{12}$ izateak, G taldea ebazgarria dela frogatu zuen.

Ondoren lana nola dagoen antolatuta azalduko da. Lehenengo kapituluan, lanean zehar beharrezkoak izango diren kontzeptu batzuen deskribapena aurkeztu da. Abelinizazio prozesua laburki azaltzen da, kommutadorearen definizioa eta oinarrizko propietateak aztertuz. Honekin erlazionatuta, talde nilpotenteak eta ebazgarriak definitzen dira, eta hauekin harreman estua duten serie zentral beherakorrak eta hitz deribatuak. Behin kommutadoreek abelinizazio prozesuan duten garrrantzia aztertuta, G', G-ren azpitalde deribatua aurkezten da, talde abeldarrekin duen harremana azpimarratuz.

Bigarren kapitulu osoa talde finitu baten trukatze probabilitateari dedikatuta dago, eta horri lotutako borneak aztertuko dira, adibide desberdinak direla medio. Trukatze probabilitatea kalkulatzeko adierazpen esplizitu bat lor-

tuko da, probabilitate teoriako Laplacen formulan oinarrituz. Praktikan, adierazpen hori kalkulatzea zaila izan daitekeenez, goi eta behe borne ez tribial batzuk aurkezten dira, ikerketa sakonagoa egiteko asmoz. Era berean, trukatze probabilitatearen kontzeptua hedatzen da, bai azpitalde bai biderkadura kartesiar eta zatidura taldeetara aplikatuz. Gainera, lortutako propietateak konjugazio klaseei buruzko emaitza ezberdinak frogatzeko erabiliko dira.

Bestalde, hirugarren kapituluan grafo teoria aljebraikoan murgilduko gara eta Neumannek izendatutako teorema bat frogatuko da. Horretarako, talde baten trukatze grafoa definitzen da eta talde zehatz batzuen trukatze grafoak irudikatuko ditugu. Prozesu hau orokortuz, trukatze grafo orokortua aurkezten da, eta talde diedriko zein semidiedrikoetara aplikatuko da.

Azkenik, A Eranskinean lanari lotutako ariketa batzuk aurkezten dira. Alde batetik, memoria garatzeko erabili diren ariketak ebazten dira. Bestetik, teoriako emaitzak berresten dituzten ariketak ere agertzen dira, praktikan jartzeko memorian zehar landutako teorema eta proposizio batzuk. Horregatik, talde diedriko eta simetrikoaren trukatze probabilitateak kalkulatzen edo bornatzen dira, beharrezkoak izan diren konbinatoriako emaitzak gogoratuz. Bukatzeko, kalkulu gehiegi dituzten teoremen kasu partikularrak ariketa moduan ebatzi dira, enuntziatutako teoremen emaitzak betetzen direla berresteko asmoz.

Notazioa

Sinboloa	Esanahia
$\|\ \|$	multzo (finitu)/ talde baten kardinala (ordena).
$\|G : H\|$	G-ren gaineko H-ren indizea.
$Z(G)$	G-ren zentrua.
x^g	x-ren konjugatua g-ren bidez.
$C_G(x)$	x-ren zentralizatzailea G-n.
$Stab_G(x)$	x-ren estabilizatzailea G-n.
$Cl_G(x)$	x-ren konjugazio klasea G-n.
$Orb_G(x)$	x-ren orbita G-n.
k_G	G-ren konjugazio klase kopurua.
$[x, y]$	x eta y elementuen kommutadorea.
G'	G-ren azpitalde deribatua.
$w(G)$	G-ren azpitalde berbala.
$\gamma_n(x_1, \ldots, x_n)$	$x_1, ..., x_n$ hitzen n. behe hitz zentrala.
$\delta_n(x_1, \ldots, x_{2^n})$	$x_1, ..., x_{2^n}$ hitzen n. hitz deribatua.
C_n	n ordenako talde ziklikoa.
D_{2n}	$2n$ kardinaleko talde diedrikoa.
SD_{2^n}	2^n kardinaleko talde semidiedrikoa.
Q_8	8 ordenako koaternioien taldea.
S_n	n mailako talde simetrikoa.
$H_3(A)$	A eraztunaren gaineko Heisenbergen taldea.
$\mathbb{Z}$	zenbaki osoen multzoa.
$p(n)$	n-ren partiketa kopurua.
$\mathbb{P}(A)$	A gertaera betetzeko probabilitatea.
$L(G)$	$G \times G$-n trukatzen diren bikoteen multzoa.
$cp(G)$	G taldearen trukatze probabilitatea.
$P(K, G)$	K-ri G-n dagokion trukatze probabilitate erlatiboa.
V	grafo baten erpinen multzoa.
E	grafo baten ertzen multzoa.
$\rho(X, G)$	X-ri elkartutako G-ren trukatze grafoa.
K_n	n erpinetako grafo betea.
$\Gamma_\Omega^{\mathrm{GC}}$	G-ri elkartutako trukatze grafo orokortua.

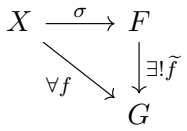
1. kapitulua

Talde teoriako oinarrizko kontzeptuak

1.1 Talde librea eta azpitalde berbala

Atal honetan, talde teoria konbinatorian maiz agertzen den azpitalde berbalaren kontzeptua azalduko da. Horretarako, lehenik gogora ditzagun talde librearen definizioa eta honi lotutako hitzen propietate nagusiak.

Definizioa 1.1.1. Izan bitez F eta G taldeak, X multzo ez hutsa eta baita $\sigma : X \to F$ aplikazioa. Esango dugu (F, σ) X-ren gaineko talde librea dela, $f : X \to G$ aplikazio bakoitzerako, existitzen bada $\widetilde{f} : F \to G$ homomorfismo bakarra zeinentzat $f = \sigma\widetilde{f}$ den; hau da, ondorengo diagrama trukakorra egiten duen homomorfismo bakarra.



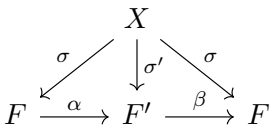
Propietate honi *talde librearen propietate unibertsala* deitzen zaio.

Behin definizio hau emanda, ondoko proposizioan talde librearen existentzia frogatuko da.

Notazioa. Idazkera errazteko, hemendik aurrera elementuen arteko . eragiketa justaposizio bidez denotatuko da, eta $(G, .)$ taldeko elementu neutroa 1 bidez. Taldeko eragiketa konposizioa denean, $g \circ f = fg$ bidez denotatuko da, eta $(G, \circ)$ taldeko elementu neutroa 1 edo id_G bidez.

Proposizioa 1.1.1. X multzo bakoitzerako, X-ren gaineko (F, σ) talde libre bakarra existitzen da, isomorfismoak salbu.

Froga. Bakartasuna frogatzen hasiko gara. Demagun (F, σ) eta (F', σ') taldeak X-ren gaineko bi talde libre direla. Orduan, definizioaren arabera ondorengo diagrama trukakorra izango litzateke:



non α, F-tik F'-ra doan eta $\sigma' = \sigma\alpha$ baldintza betetzen duen talde homomorfismo bakarra, eta β, F'-tik F-ra doan eta $\sigma = \sigma'\beta$ baldintza betetzen duen talde homomorfismo bakarra diren. Berriro ere definizioz, existitzen da homomorfismo bakarra, γ deiturikoa, F-tik F-ra doana non $\sigma = \sigma\gamma$ den. Halabeharrez, γ, F-ko identitate aplikazioa da. Bestalde, $\alpha\beta$ homomorfismoak, $\sigma = \sigma\alpha\beta$ baldintza betetzen duenez, $\alpha\beta = id_F$ dela ondorioztatzen da. Analogoki argudiatuta, $\beta\alpha = id_{F'}$ berdintza lortzen da. Beraz, F-tik F'-ra doan isomorfismo bakarra dago, α denotatuko duguna.

Orain eraki dezagun X-ren gaineko talde librea. Horretarako, kontsidera dezagun X^{-1} multzoa, hots, X-ren kopia bat: $X^{-1} = \{x^{-1} \mid x \in X\}$ sinboloez osatua. Esango dugu w, X-ren *gaineko hitza* dela $X \cup X^{-1}$-ren sinboloen kate bat bada, hau da,

$$w = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$$

non $x_i \in X$ eta $\epsilon_i = \pm 1$ diren, edozein $i \in \{1, \ldots, n\}$-rako, $n \geq 0$ izanik.

Baldin eta $n = 0$ bada, w-ri *hitz hutsa* esango diogu eta $w = 1$ bidez denotatuko dugu. Gainera, emanda $w_1 = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ eta $w_2 = y_1^{\nu_1} \cdots y_m^{\nu_m}$, X-ren gaineko bi hitz, $w_1 = w_2$ dela diogu baldin eta soilik baldin $n = m$, $x_i = y_i$ eta $\epsilon_i = \nu_i$ badira, edozein $i \in \{1, \ldots, n\}$ balioetarako.

Bestalde, X-ko bi elementu biderkatzeko kateaketa erabiliko dugu. Hain zuzen ere, baldin eta $w_1 = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ eta $w_2 = y_1^{\nu_1} \cdots y_m^{\nu_m}$ badira, bi hitz horien arteko biderketa ondorengo moduan definitzen da:

$$w_1 w_2 = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} y_1^{\nu_1} \cdots y_m^{\nu_m},$$

hitzarmenez, $1w = w = w1$ delarik. Azkenik, w *hitzaren alderantzizkoa* $w^{-1} = (x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})^{-1} = x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1}$ bidez definitzen da.

Orain kontsidera dezagun $\widetilde{F}$, X-ren gaineko hitz guztien multzoa, eta bertan defini dezagun ondorengo erlazioa: esango dugu w_1 eta w_2 hitzak baliokideak direla, $w_1 \sim w_2$ bidez adieraziko duguna, w_1-tik abiatuz w_2 hitza lortu ahal badugu, kopuru finitu aldiz ondorengo bi eragiketa motak aplikatuz:

(i) xx^{-1} edo $x^{-1}x$ gehitzea, hitzaren tokiren batean, $x \in X$ izanik.

(ii) xx^{-1} edo $x^{-1}x$ ezabatzea, hitzaren tokiren batean, $x \in X$ izanik.

w hitz laburtua dela esaten da bere garapenean ezin badaiteke (ii) motako eragiketak aplikatu beste hitz baliokide bat aurkitzeko.

Alde batetik, erraz froga daiteke $\sim$ baliokidetasun erlazioa dela.

Bestetik, dei diezaiogun F, $\widetilde{F}/\sim$ multzoari, bertako baliokidetasun klaseak $[w]$ bidez denotatuz. Lehenik, ohar gaitezen F-ri talde egitura eman diezaiokegula. Horretarako, defini dezagun F-n ondoko eragiketa:

$$[w][v] = [wv]$$

Hasteko, argi dago eragiketa hori ondo definituta dagoela, $w_1 \sim w_2$ eta $v_1 \sim v_2$ izanik, $w_1v_1 \sim w_2v_2$ delako. Gainera, $[w][1] = [w] = [1][w]$ eta $[w][w^{-1}] = [ww^{-1}] = [1]$ erlazioak betetzen dira. Azkenik, argi dago F-n eragiketa hori elkarkorra dela, $\widetilde{F}$-n ere biderketa elkarkorra delako. Ondorioz, F-k aurreko $\sim$ eragiketarekin talde egitura du.

Defini dezagun orain $\sigma : X \longrightarrow F$ aplikazioa, $\sigma(x) = [x]$ erregelaren bidez, eta froga dezagun (F, σ), X-ren gaineko talde librea dela. Horretarako, har dezagun edozein G talde eta kontsidera dezagun edozein $f : X \to G$ aplikazioa. Defini dezagun X-ren gaineko hitzen multzotik, hau da, $\widetilde{F}$-tik, G taldera doan ondoko f^* aplikazioa:

$$\begin{aligned} f^* : \quad & \widetilde{F} \longrightarrow G \\ & w = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mapsto f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n} \end{aligned}$$

Baldin eta $w \sim v$ bada, $f^*(w) = f^*(v)$ betetzen da, G taldean edozein g elementurako $gg^{-1} = g^{-1}g = 1$ delako. Beraz, zentzua du ondorengo $\widetilde{f}$ aplikazioa definitzea:

$$\begin{aligned} \widetilde{f} : F &\longrightarrow G \\ [w] &\mapsto f^*(w) \end{aligned}$$

Gainera, $\widetilde{f}$ talde homorfismoa da, edozein $[w], [v]$, F-ko elementuetarako,

$$\widetilde{f}([wv]) = f^*(wv) = f^*(w)f^*(v) = \widetilde{f}([w])\widetilde{f}([v])$$

delako, eta halabeharrez edozein $x \in X$ elementurako, $\widetilde{f}(\sigma(x)) = \widetilde{f}([x]) = f^*(x) = f(x)$ betetzen da. Hots, $f = \widetilde{f} \circ \sigma = \sigma\widetilde{f}$ betetzen da. $\square$

Behin talde librearen eta hitzen kontzeptuak aurkeztu ditugula, ondoren aztertuko dugu zein den G talde batean hitz baten balioa.

Izan bitez $k \in \mathbb{N}$ eta F, $\{x_1, x_2, \ldots\}$ multzo zenbakigarri infinituen gaineko talde librea. Demagun, $w = x_1^{\epsilon_1}x_2^{\epsilon_2} \cdots x_k^{\epsilon_k} = w(x_1, x_2, \ldots, x_k)$ ez hutsa den

hitz laburtua dela. Emanda G taldea, G-ko edozein elementuen $(g_1, g_2, \ldots, g_k)$ k-kotearentzat bertan w hitzak duen balioa definituko dugu ondoko eran:

$$w(g_1, g_2, \ldots, g_k) = g_1^{\epsilon_1} g_2^{\epsilon_2} \cdots g_k^{\epsilon_k} \in G.$$

Hain zuzen ere, ondoko definizio formala aurkezten da:

Definizioa 1.1.2. Izan bitez G taldea eta $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_k^{\epsilon_k}$ arestian definituriko F-ko hitz laburtua. Defini dezagun, $\overbrace{G \times \cdots \times G}^{k}$-tik G-ra doan ondoko aplikazioa:

$$\begin{aligned} w^* : \overbrace{G \times \cdots \times G}^{k} &\to G \\ (g_1, \ldots, g_k) &\mapsto w^*(g_1, \ldots, g_k) = w(g_1, \ldots, g_k) = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k} \end{aligned}$$

$w(g_1, \ldots, g_k)$, G-ko w-balioa $(g_1, \ldots, g_k)$-n deituz.

Gainera, G taldeko w-balioen multzoa G_w bidez adierazten da:

$$G_w = \{w(g_1, g_2, \ldots, g_k) \mid g_1, g_2, \ldots, g_k \in G\}.$$

Bestalde, G_w multzoko elementu guztiek sortutako azpitaldea, $w(G)$ bidez denotatzen dena, w hitzari dagokion *azpitalde berbala* deitzen da. Hau da, $w(G) = \langle G_w \rangle \leq G$ eta G-ren azpitalde karakteristikoa da.

Ondoren, w hitz desberdinei dagozkien azpitalde berbalekin arituko gara lanean, eta arreta berezia jarriko diogu *kommutadore hitzari*. Hain zuzen ere, atal berezi bat (hurrengoko 1.2 atala) garatuko dugu hitz horren ezaugarriak eta bertatik sortzen diren beste hainbat berezitasun aztertzeko.

Adibideak. Izan bedi G taldea.

- Demagun $n \in \mathbb{N}$ eta $w = x^n$ hitza ditugula. Orduan, hitz honi dagokion azpitalde berbala $w(G) = \langle G_w \rangle = \langle g^n \mid g \in G \rangle$ da, eta G^n bidez adierazten da. Gainera, esango dugu G taldeak *esponente* finitua duela baldin eta existitzen bada $m \in \mathbb{N}$ non $G^m = 1$ den.

- Demagun $[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$ *kommutadore hitza* dugula. Orduan, $G_w = \{[g_1, g_2] \mid g_1, g_2 \in G\}$ da, eta hitz horri dagokion azpitalde berbala, $w(G) = \langle G_w \rangle$, G' bidez denotatuko da eta G-ren azpitalde deribatua deitzen da.

- Hitz kommutadore multilinealak: definizioz, w hitz kommutadore multilineal bat, aldagai desberdinak erabiliz hitz kommutadore desberdinak ahokatzean lortzen den hitza da. Adibidez, $[[x_1, x_2], [x_3, x_4]]$ hitz kommutadore multilineala da. Honen beste adibide bat, *behe hitz zentralak* dira (1.1.3 definizioan aurkezten direnak).

Definizioa 1.1.3. Izan bitez $x_1, \ldots, x_n \in G$. $n \geq 2$ den kasurako behe hitz zentralak errekurtsiboki definitzen dira ondoko eran:

$$\gamma_n(x_1, ..., x_n) = [\gamma_{n-1}(x_1, ..., x_{n-1}), x_n]$$

non $\gamma_1(x_1) = [x_1] = x_1$ den.

γ_n hitzari dagokion azpitalde berbala $\gamma_n(G)$ bidez denotatuko da. Gainera, baldin eta m zenbaki arrunten baterako $\gamma_{m+1}(G) = 1$ eta $\gamma_m(G) \neq 1$ badira, orduan G taldea m nilpotentzia klaseko *talde nilpotentea* dela esaten da, eta $c(G) = m$ bidez denotatuko da G taldearen nilpotentzia klasea.

Definizio honi lotuta G talde baten *serie zentral beherakorraren* definizioa aurkeztuko dugu.

Definizioa 1.1.4. Izan bedi G taldea. G-ren serie zentral beherakorra errekurtsiboki definitzen da ondoko eran: $\gamma_1(G) = G$, eta edozein $i \geq 2$ indizeetarako $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

Ohartu $\gamma_2(G) = G'$ dela eta edozein $i \geq 1$ indizeetarako $\gamma_i(G)$ azpitaldeak karakteristikoak direla G-n eta bereziki normalak G-n. Beranduago, 1.2.1. korolarioan aurki daiteke honen froga.

Definizioa 1.1.5. Edozein $n \in \{0\} \cup \mathbb{N}$ zenbakirako, δ_n *hitz deribatuak* definitzen dira errekurtsiboki ondoko eran:

$$\delta_0(x_1) = x_1, \text{ eta edozein } n \text{ arruntarako,}$$
$$\delta_n(x_1, \ldots, x_{2^n}) = [\delta_{n-1}(x_1, ..., x_{2^{n-1}}), \delta_{n-1}(x_{2^{n-1}+1}, \ldots, x_{2^n})].$$

δ_n hitzari dagokion azpitalde berbalari, G-ren n. *azpitalde deribatua* deitzen zaio eta $G^{(n)}$ bidez denotatzen da. Ondorengo 1.2 atalean (hain zuzen ere, 1.2.3 definizioan) kontzeptu hau modu sakonago batean aztertuko da.

1.2 Kommutadorea eta azpitalde deribatua

Talde abeldarretan elementuen arteko eragiketak erraz kalkulatzen dira elementuak elkar trukatzen direlako. Alabaina, orokorrean aztertuko diren taldeak ez dira abeldarrak izango, baina zentzu batean neurtu daiteke zenbat urrundu gaitezkeen aurreko propietate horretatik. Urrunketa hau neurtzeko erabilgarria izango da arestian definitutako kommutadorearen kontzeptua erabiltzea.

Hori dela eta, atal honetan *kommutadorearen* kontzeptuarekin arituko gara. Bereziki, G talde baten $G' = [G, G]$ azpitalde deribatuarekin lan egingo dugu, horren propietate esanguratsuenak aztertuz. Aipatutako kontzeptu hori taldearen *abelinizazioarekin* erlazionatuta dago. Abelinizazio prozesua, egitura aljebraiko bat abeldarra bihurtzean datza. Bereziki taldeen kasuan, G taldearen *abelinizazioa* $G/G' = G/[G, G]$ zatidura taldea da.

Definizioa 1.2.1. Izan bitez G taldea eta $x, y \in G$. Deitzen diogu x eta y elementuen *kommutadorea*, $[x, y]$ moduan denotatuko duguna, ondorengo moduan definitzen den G-ko elementuari:

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y = (y^{-1})^x y \in G.$$

Demagun orain G taldeko n elementu ditugula, hots, $x_1, x_2, \ldots, x_n$. Orduan, n luzerako kommutadorea errekurtsiboki ondoko eran kalkulatzen da:

$$[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n] = \cdots = [\ldots[[x_1, x_2], x_3], \ldots].$$

Behin kommutadorearen kontzeptua definituta, bere propietate nagusienak aztertuko ditugu, taldeko eragiketarekin, elementuen alderantzizkoekin eta konjugazioarekin dituen harremanak aztertuz.

Notazioa. Edozein $g \in G$ elementurako, konjugazio homomorfismoa ondorengo moduan definitzen da:

$$\begin{aligned} \rho_g : G &\to G \\ x &\mapsto x^g = g^{-1}xg \end{aligned} \tag{1.1}$$

Bestalde, baldin eta $N \trianglelefteq G$ bada, G eta G/N zatidura taldearen arteko epimorfismo kanonikoa defini daiteke:

$$\begin{aligned} \pi : G &\to G/N \\ x &\mapsto \overline{x} \end{aligned} \tag{1.2}$$

$\overline{x}$ elementuak xN elementuak izanik.

Teorema 1.2.1. Izan bitez G taldea, $N \trianglelefteq G$ eta $x, y, z \in G$. Ondorengo propietateak betetzen dira:

(i) x eta y elkar trukatzen dira baldin eta soilik baldin $[x, y] = 1$.

(ii) $[y, x] = [x, y]^{-1}$.

(iii) Baldin eta f, G-ren gainean definituriko talde homomorfismoa bada, orduan $f([x, y]) = [f(x), f(y)]$ betetzen da. Bereziki, edozein $g \in G$ elementurako, $[x, y]^g = [x^g, y^g]$ betetzen da.

(iv) G/N zatidura taldean, $\overline{[x, y]} = [\overline{x}, \overline{y}]$.

(v) $[xy, z] = [x, z]^y[y, z]$.

Froga. (i) Kommutadorearen definizioa erabiliz, baldin eta $[x, y] = 1$ bada, orduan $x^{-1}y^{-1}xy = 1$ dugu. Hurrenez hurren, elementuen alderantzizkoengatik egoki biderkatuz, $xy = yx$ dugu, hau da, x eta y elkar trukatzen dira. Alderantzizkoa ere berehalakoa da.

(ii) Kommutadorearen definizioagatik, ondorengo garapena lortzen dugu:

$$[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x].$$

(iii) f homomorfismoa denez,

$$\begin{aligned} f([x,y]) &= f(x^{-1}y^{-1}xy) = f(x^{-1})f(y^{-1})f(x)f(y) \\ &= f(x)^{-1}f(y)^{-1}f(x)f(y) = [f(x),f(y)]. \end{aligned}$$

Bereziki, (1.1) konjugazio aplikazioa, talde homomorfismoa denez, edozein $g \in G$ elementurako, $[x,y]^g = [x^g, y^g]$ dugu.

(iv) Orain (1.2) epimorfismo kanonikoari (*iii*) atala aplikatuz, $\overline{[x,y]} = [\overline{x},\overline{y}]$ betetzen da.

(v) Berdintzaren bi gaiak garatuko ditugu. Alde batetik,

$$[xy,z] = (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz,$$

eta bestetik,

$$\begin{aligned} [x,z]^y[y,z] &= (x^{-1}z^{-1}xz)^y y^{-1}z^{-1}yz \\ &= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz \\ &= y^{-1}x^{-1}z^{-1}xyz. \end{aligned}$$

□

Behin, G taldeko elementuen kommutadorea aurkeztu dugula, azpitaldeen arteko kommutadorea definitzen da.

Definizioa 1.2.2. Izan bitez G taldea eta $H, K \leq G$ azpitaldeak. H eta K azpitaldeen azpitalde kommutadorea, $[H,K]$ moduan denotatuko duguna, ondoko eran definitzen da:

$$[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle$$

Era berean, baldin eta $X_1, X_2, \ldots, X_n$, G-ren azpitaldeak badira, orduan, n azpitalderen kommutadorea errekurtsiboki definitzen da:

$$[X_1,\ldots,X_n] = [[X_1,\ldots,X_{n-1}],X_n] = \cdots = [\ldots[[X_1,X_2],X_3],\ldots]$$

Aurreko 1.2.2 definizioa G-ko edozein A, B azpimultzoetarako ere eman daiteke:

$$[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle.$$

Teorema 1.2.2. Izan bitez G taldea eta $H, K \leq G$. Orduan,

(i) H-k K normalizatzen du baldin eta soilik baldin $[H,K] \leq K$ bada. Are gehiago, H-k K zentralizatzen du baldin eta soilik baldin $[H,K] = 1$ bada.

(ii) $[H,K] = [K,H]$.

(iii) Baldin eta f, G-ren gainean definituriko talde homomorfismoa bada, orduan $f([H,K]) = [f(H), f(K)]$ betetzen da. Bereziki, edozein $g \in G$ elementurako, $[H,K]^g = [H^g, K^g]$ dugu.

(iv) Baldin eta $N \trianglelefteq G$ bada, orduan $[HN/N, KN/N] = [H,K]N/N$.

Froga. (i) Lehenik eta behin, ohartu ondorengo adierazpena ematen dela:

$$[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle = \langle (k^{-1})^h k \mid h \in H, k \in K \rangle.$$

Alde batetik, $\Rightarrow$) inplikaziorako, H-k K normalizatzen duenez, orduan edozein $h \in H, k \in K$ elementuetarako, $(k^{-1})^h k = [h,k] \in K$ betetzen da, eta bereziki $[H,K] \leq K$.

Bestetik, $\Leftarrow$) inplikaziorako, demagun $[H,K] \leq K$ dela. Beraz, bereziki edozein $h \in H, k \in K$ elementuetarako $[h,k] = (k^{-1})^h k \in K$, eta hemendik H-k K normalizatzen duela ondorioztatzen da.

Bereziki, $[H,K] = 1$ bada, edozein $h \in H, k \in K$ elementuetarako $[h,k] = (k^{-1})^h k = 1$ betetzen da, eta hemendik berehalakoa da, H-k K zentralizatzen duela ohartzea. Alderantzizkoa ere berehalakoa da.

(ii) 1.2.1 teoremako (ii) atala erabiliz, $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle = \langle [k,h]^{-1} \mid h \in H, k \in K \rangle = \langle [k,h] \mid h \in H, k \in K \rangle = [K,H]$ dugu.

(iii) Kontuan izanik talde baten sortzaileen irudiak, talde horren irudiaren sortzaileak direla, eta 1.2.1 teoremako (iii) atala erabiliz, ondorengo garapena lortzen da:

$$\begin{aligned} f([H,K]) &= f(\langle [h,k] \mid h \in H, k \in K \rangle) \\ &= \langle f([h,k]) \mid h \in H, k \in K \rangle \\ &= \langle [f(h), f(k)] \mid h \in H, k \in K \rangle \\ &= [f(H), f(K)]. \end{aligned}$$

Bereziki, (1.1) konjugazio homorfismoa erabilita, edozein $g \in G$ elementurako, $[H,K]^g = [H^g, K^g]$ dugu.

(iv) Nahikoa da 1.2.1 teoremako (iv) atala erabiltzea.

□

Arestian erabilitako antzeko arrazonamenduak erabiliz, erraz ikus daiteke $H \trianglelefteq G$ baldin eta soilik baldin $[H, G] \leq H$ bada, eta $H \leq Z(G)$ betetzen dela baldin eta soilik baldin $[H, G] = 1$ betetzen bada.

Jarraian azter dezagun kommutadorearen propietateak, azpitalde normalekin eta karakteristikoekin lan egiterako orduan. Gogoratu G-ren H azpitaldea G-n karakteristikoa dela baldin eta bere irudia G gaineko edozein automorfismoaren bidez H-ren azpitaldea bada.

1.2.1. korolarioa. Izan bitez G taldea eta $H, K \leq G$.

(i) Baldin eta H eta K, G-ren azpitalde karakteristikoak badira, orduan $[H, K]$ G-ren azpitalde karakteristikoa da.

(ii) Baldin eta $H, K \trianglelefteq G$ badira, orduan $[H, K] \trianglelefteq G$ dugu.

Teorema 1.2.3. Izan bitez G taldea eta $H, K \leq G$. Orduan, $[H, K] \trianglelefteq \langle H, K \rangle$.

Froga. Lehenik ikus dezagun H-k $[H, K]$ normalizatzen duela. Horretarako, froga dezagun edozein $h, h' \in H$ eta $k \in K$ elementuetarako, $[h, k]^{h'} \in [H, K]$ dela. 1.2.1 teoremako (v) propietatea erabiliz, $[hh', k] = [h, k]^{h'}[h', k]$ betetzen da, eta halabeharrez, $[h, k]^{h'} \in [H, K]$ ondorioztatzen da, $[hh', k]$, $[h', k] \in [H, K]$ direlako. Analogoki, K-k $[H, K]$ normalizatzen duelakoan ohar gaitezke. Ondorioz, $[H, K] \trianglelefteq \langle H, K \rangle$ da. □

Azpitalde kommutadoreen artean, edozein G talderentzat, $[G, G]$ motatako azpitaldea garrantzitsua da. Azpitalde honetan oinarrituz, G taldearen serie deribatua eraiki daiteke. (Jadanik 1.2.3 definizioan eman da, serie honetako azpitaldeen aurkezpen baliokide bat.)

Definizioa 1.2.3. Izan bedi G taldea.

(i) G-ren azpitalde deribatua, G' bidez denotatuko duguna, $[G, G]$ azpitalde kommutadorea da, hau da:

$$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle.$$

(ii) Defini dezagun $G^{(0)} = G$ eta errekurtsiboki, edozein $i \geq 1$ baliorako, kontsidera dezagun $G^{(i)} = (G^{(i-1)})'$. Orduan, G-ren serie deribatua ondorengo azpitaldeen seriea da:

$$G = G^{(0)} \geq G' = G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(i)} \geq \cdots .$$

Baldin eta $G^{(m)} = 1$ eta $G^{(m-1)} \neq 1$ badira, orduan G, m luzerako *talde ebazgarria* dela esaten da, eta $l(G) = m$ bidez denotatuko da G taldearen serie deribatuaren luzera.

Erraz ikus dezakegu G talde abeldarra izateko baldintza beharrezkoa eta nahikoa $[G,G]=1$ izatea dela. Are gehiago, propietate hori hedatuz ondoko emaitza dugu.

Teorema 1.2.4. Izan bedi G taldea. Orduan,

(i) G/G' talde abeldarra da.

(ii) $N \trianglelefteq G$ izanik, baldin eta G/N zatidura taldea abeldarra bada, orduan $G' \leq N$ da.

Froga. (i) Har ditzagun edozein $\overline{x},\overline{y} \in G/G'$. Orduan, 1.2.1 teoremako (iv) atala erabiliz, $[\overline{x},\overline{y}] = \overline{[x,y]} = \overline{1}$ dugu, $[x,y] \in G'$ delako.

(ii) Baldin eta G/N talde abeldarra bada, $[xN,yN] = [\overline{x},\overline{y}] = \overline{1} = N$ dugu, edozein $\overline{x},\overline{y} \in G/N$ elementuetarako. Ondorioz, G-ko edozein x,y elementuetarako, $[x,y] \in N$ dago. Halabeharrez, $G' \leq N$ dugu. □

Ondorioz, G' da G-ren azpitalde normal txikiena zeinentzat berarekiko G-ren zatidura talde abeldarra den.

Adibidea 1.2.1. Izan bedi D_{2n}, $2n$ kardinaleko talde diedrikoa ondoko aurkezpenarekin: $D_{2n} = \langle x,y \mid x^n = y^2 = 1, x^y = x^{-1}\rangle$. Azter dezagun D_{2n}-ren abelinizazioa eta bere serie deribatua.

Alde batetik, badakigu $[x,y] = x^{-1}x^y = x^{-1}x^{-1} = x^{-2}$ dela, eta halabeharrez, $\langle x^{-2}\rangle = \langle (x^2)^{-1}\rangle = \langle x^2\rangle \leq D'_{2n}$ dugu. Bestalde, argi ikusten da $\langle x^2\rangle$ azpitaldea normala dela D_{2n}-n. Beraz, eraiki daiteke $D_{2n}/\langle x^2\rangle$ zatidura taldea. Orain, azter dezagun $\langle x^2\rangle$ taldearen kardinala.

Alde batetik $|\langle x^2\rangle| = o(x^2)$ da. Bereiz ditzagun bi kasu: a) n bakoitia den kasua, eta b) n bikoitia den kasua. a) kasuan, $o(x^2) = o(x) = n$ da eta $D_{2n}/\langle x^2\rangle$, 2 kardinaleko taldea denez, argi dago zatidura taldea 2 kardinaleko talde zikliko abeldarra dela. Bestalde, bigarren kasuan (b kasuan), $o(x^2) = \frac{n}{2}$ da, eta kasu honetan $D_{2n}/\langle x^2\rangle$ 4 kardinaleko taldea, ere abeldarra da; hain zuzen ere, $C_2 \times C_2$ motatakoa. Izan ere, kasu honetan,

$$D_{2n}/\langle x^2\rangle = \langle \overline{x} = x\langle x^2\rangle,\ \overline{y} = y\langle x^2\rangle\rangle$$

da, eta $\overline{x}^{\overline{y}} = \overline{x^{-1}} = \overline{x}$ betetzen da, $x^{-1}x^{-1} \in \langle x^2\rangle$ delako.

Beraz, edozein kasutan $D_{2n}/\langle x^2\rangle$ zatidura taldea abeldarra denez, 1.2.4 teorema erabiliz, $D'_{2n} \leq \langle x^2\rangle$ izango genuke, eta ondorioz $D'_{2n} = \langle x^2\rangle$.

Azkenik D'_{2n} talde ziklikoa denez, bereziki talde abeldarra da, eta ondorioz $D''_{2n} = \{1\}$ dugu. Hots, bere serie deribatua ondokoa da:

$$D_{2n} = {D_{2n}}^{(0)} \geq D'_{2n} = {D_{2n}}^{(1)} = \langle x^2\rangle \geq D''_{2n} = {D_{2n}}^{(2)} = \{1\}.$$

2. kapitulua

Trukatze probabilitatea

Talde teoria probabilistikoak estatistika eta probabilitateko teknika ezberdinak erabiltzen ditu arloko emaitza desberdinak frogatzeko. Horietako tresna batzuei esker adibidez, azter daiteke zein gertu dagoen talde bat abeldarra izatetik. Horretarako, bai taldearen zentruaren, bai zentralizatzaileen kardinalak aztertzen dira, abelinizazioaren eta kommutadorearen propietateei erreparatuz. Alderdi guzti horiek, *trukatze probabilitatea* izeneko kontzeptuarekin harreman estua dute.

Hain zuzen ere, trukatze probabilitateak talde bateko edozein bi elementu hartuta, elementu horiek elkar trukatzeko probabilitatea neurtzen du. Beste modu batean esanda, trukatze probabilitateak talde ez abeldar baten abeldartasun maila neurtzen duela esan genezake zentzu batean. Atal hau garatzeko gehienbat [16] eta [17] artikuluak erabili dira.

2.1 Testuinguru probabilistikoa

Has gaitezen hasierako definizio batzuk aurkezten. Horretarako, demagun $(G, .)$ talde finitu batekin lanean ari garela. Bertako probabilitate neurri naturalena, taldeko elementuak zoriz uniformeki aukeratzea litzateke. Kasu honetan, gure eredu probabilistikoa zorizko eredu klasiko diskretua izango litzateke.

Notazioa. Idazkera errazteko, hemendik aurrera Ω lagin espazio bateko A gertaera baten probabilitatea $\mathbb{P}(A)$ bidez denotatuko da.

Demagun orduan, n tamainuko $\Omega = G \times G$ lagin espazioari banaketa diskretu uniformea egokitzen diogula, non Ω-ko oinarrizko $\overline{w_i}$ gertaera guztiak ekiprobableak diren. Hau dela eta, oinarrizko gertaeren probabilitatea $\mathbb{P}(\overline{w_i}) = \frac{1}{n}$ izango genuke. Beraz, baldin eta A edozein gertaera konposatua bada, hau da, baldin eta $A = \bigcup_{j=1}^{k} \{\overline{w_j}\}$ bada, $\{\overline{w_j}\} \in \Omega$ eta $k \leq n$ izanik, A gertatzeko probabilitatea Laplaceren formularen bidez emanda dago ondoko

eran:

$$\mathbb{P}(A) = \sum_{j=1}^{k} \mathbb{P}(\overline{w_j}) = \frac{k}{n} = \frac{\text{aldeko kasuak}}{\text{kasu posibleak}}.$$

Egoera honetan, demagun $G \times G$-ko elkar trukatzen diren elementu bikoteen multzoa kontsideratzen dugula; halaber, ondoko $L(G) \subseteq G \times G$ multzoa:

$$L(G) = \{(x, y) \in G \times G \mid xy = yx\}.$$

Hemendik, G taldearen *trukatze probabilitatea*, intuitiboki, $L(G)$ gertaeraren probabilitatea izan beharko lukeela uler genezake.

Definizioa 2.1.1. Izan bedi G talde finitua. Definizioz G-ren trukatze probabilitatea deitzen zaio Laplaceren erregelaren bidez emanda dagoen ondoko adierazpenari:

$$cp(G) = \mathbb{P}(\{xy = yx \mid x, y \in G\}) = \frac{|L(G)|}{|G \times G|} = \frac{|L(G)|}{|G|^2},$$

non $L(G)$-k edozein $G \times G$-ko elkar trukatzen diren osagaiak dituen elementuen gertaera islatzen duen.

Bestalde, G talde finitu bateko elementu guztiak elkar trukatzen direnean, hau da, G taldea abeldarra denean, nabaria da $cp(G) = 1$ dela. Hori dela eta, hemendik aurrera G taldea ez abeldarra dela suposatuko dugu.

Edozein kasuan $cp(G)$-ren azterketarekin aurrera joan baino lehen, defini dezagun modu labur batean, hurrengo kapituluan ere (3 kapituluan) erabiliko dugun talde baten azpitalde bati dagokion trukatze probabilitate erlatiboa.

Definizioa 2.1.2. Izan bitez G talde finitua eta $K \leq G$. Definizioz deitzen zaio G-n, K-ri dagokion trukatze probabilitate erlatiboa ondoko zenbakiari:

$$P_G(K) = P(K, G) = \frac{|\{(x, y) \in K \times G \mid xy = yx\}|}{|K||G|}.$$

Argi dago, $P_G(G) = P(G, G) = cp(G)$ dela. Bestalde, aurreko definizioak mota askotako aldaerak onar ditzake; adibidez, azpitalde baten ordez multzo bereziak hartuz gero. Askotan, $cp(G)$, $P(G)$ bidez ere denotatzen da.

2.2 Trukatze probabilitatearen bornaketa sinpleak

Atal honen helburua $cp(G)$-ren borne batzuk aurkitzea da. Nabaria da 1-a beti dela $cp(G)$-ren goi bornea eta 0-a behe bornea. Kasu tribialak alde

batera utzita, ikerketa sakonagoa burutzen dugun heinean talde finitu desberdinen $cp(G)$-ren balio zehatzak ere aurkeztuko ditugu. Has gaitezen, talde finitu baten $cp(G)$-ren behe borne sinple bat aurkezten.

Proposizioa 2.2.1. Izan bedi G talde finitu ez tribiala eta ez abeldarra. Orduan, $cp(G) \geq \frac{3|G|-2}{|G|^2}$. Gainera, baldin eta $|G| \geq 3$ bada, $cp(G) \geq \frac{3}{|G|}$ betetzen da.

Froga. Nabaria da G-ko edozein g elementurako $(1,g),(g,1)$ eta (g,g) elementuak $L(G)$-n daudela. Baldin eta $g = 1$ bada, $(1,g),(g,1),(g,g)$ bikoteak $(1,1)$ bikotearen berdinak dira. Bestalde, G taldea ez tribiala denez, existitzen da $g \neq 1$ den G-ko elementuren bat. Orain, $|L(G)| \geq 3|G| - 2$ da. Hau da, $cp(G) = \frac{|L(G)|}{|G\times G|} \geq \frac{3|G|-2}{|G|^2}$ desberdintza egiaztatzen da.

Bereziki, baldin eta $|G| \geq 3$ bada, erraz froga daiteke G-n badagoela g elementuren bat non $o(g) \geq 3$ den. Kontrako kasuan, G-ko elementu ez tribial guztiak bi ordenakoak izango lirateke, eta honek G talde abeldarra dela ondorioztatuko luke, hipotesiaren aurkakoa dena. Orain, kasu honetan, (g,g^2) eta (g^2,g) elementuak, goiko parrafoan kontatu ez ditugun $L(G)$-ko elementu berriak dira. Ondorioz, $|L(G)| \geq 3|G| - 2 + 2$ dugu, hots, $|L(G)| \geq 3|G|$, eta bereziki kasu honetan $cp(G) \geq \frac{3}{|G|}$.

□

Ohartu $cp(G) \geq \frac{3}{|G|}$ behe bornea ez dela oso baliogarria, G-ren kardinala (finitua) handitzen den heinean.

Edozein kasutan, beste borne bat aurkeztu baino lehen, kalkula dezagun S_3 eta Q_8 taldeen trukatze probabilitateak, eta ohartu gaitezen S_3-ren kasuan aurreko desberdintza, berdintza bat dela, hain zuzen ere. Horretarako, talde bakoitzari dagokion taula eraikiko dugu, elkar trukatzen diren elementu bikoteen kopurua zenbatzeko.

Adibidea 2.2.1. Izan bedi $(S_3,\circ)$, 3 mailako talde simetrikoa. Kontsidera dezagun $S_3 = \langle x,y \mid x^3 = y^2 = 1, x^y = x^{-1}\rangle$ aurkezpena, edo baliokideki, kontsidera dezagun $S_3 = \langle (123),(12)\rangle$. Orain, izenda ditzakegu S_3-ko elementuak $\{1,(12),(13),(23),(123),(132)\}$ bidez, edo $\{1,x,x^2,y,xy,x^2y\} = \{1,y,x^2y,xy,x,x^2\}$ moduan.

Lehendabizi, S_3 taldeko elementuen arteko konposaketa eragiketarekiko, beheko (2.1.) taula begiratuz, erraz ikus daiteke nor den $L(S_3)$ multzoa:

$$\begin{aligned} L(S_3) =& \{(\{1\}\times S_3)\}\cup\{(S_3\times\{1\})\}\cup\{(y,y),(xy,xy),(x^2y,x^2y)\} \\ & \cup\{(x^k,x^l) \mid 1\leq k,l\leq 2\}. \end{aligned}$$

Orain, $L(S_3)$ multzoko elementuen kontaketa eginez, $|L(S_3)| = 18$ dugu, eta ondorioz, $cp(S_3) = \frac{18}{36} = \frac{1}{2} = 0.5$ da.

$(S_3, \circ)$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

2.1. Taula: S_3 talde simetrikoaren taula

Adibidea 2.2.2. Izan bedi $(Q_8, \cdot)$ koaternioien taldea. Har dezagun Q_8 taldearen $\langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle$ edo $\langle i, j \mid i^4 = 1, i^2 = j^2, i^j = i^{-1} \rangle$ aurkezpenak. Orain, Q_8 taldeko elementuak, $\{1, i, i^2, i^3, j, ji, ji^2, ji^3\} = \{1, i, -1, -i, j, -k, -j, k\} = \{1, -1, i, -i, j, -j, k, -k\}$ gisa adieraz daitezke, edo baliokideki $\{1, a, a^2, a^3, b, ab, ab^2, ab^3\}$ bidez.

Lehendabizi, Q_8 taldeko elementuen arteko eragiketarekiko, beheko (2.2.) taula begiratuz, erraz ikus daiteke nor den $L(Q_8)$ multzoa:

$$\begin{aligned} L(Q_8) =& \{(\{1\} \times Q_8)\} \cup \{(Q_8 \times \{1\})\} \cup \{(\{-1\} \times\ Q_8)\} \\ & \cup \{(a, -1), (a, a), (a^{-1}, a)\} \cup \{(a^{-1}, -1), (a^{-1}, a^{-1}), (a, a^{-1})\} \\ & \cup \{(b, -1), (b, b), (b^{-1}, b)\} \cup \{(b^{-1}, -1), (b^{-1}, b^{-1}), (b, b^{-1})\} \\ & \cup \{(ab, -1), (ab, ab), ((ab)^{-1}, ab)\} \\ & \cup \{(ab)^{-1}, -1), ((ab)^{-1}, (ab)^{-1}), (ab, (ab)^{-1})\}. \end{aligned}$$

Orain, $L(Q_8)$ multzoko elementuen kontaketa eginez, $|L(Q_8)| = 40$ dugu, eta ondorioz $cp(Q_8) = \frac{40}{64} = \frac{5}{8} = 0.625 > 0.5$ da.

$(Q_8, \cdot)$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

2.2. Taula: Q_8 koaternioi taldearen taula

2.3 Trukatze probabilitatearen kalkulua

Ondorengo emaitzetan, talde baten trukatze probabilitatea, elementuen konjugazio klaseekin erlazionatzen saiatuko gara. Horretarako, gogoratu behar dugu nola definitzen den elementu baten zentralizatzailea, elementu baten konjugazio klasea eta konjugazio klaseen propietate batzuk aurkeztu behar ditugu.

Lehendabizi, G talde bateko $x \in G$ elementu baten zentralizatzailea, $C_G(x)$ denotatzen duguna, G-ko x elementuarekin trukatzen diren elementuen multzoa da, eta elementu horren konjugazio klasea, $\mathrm{Cl}_G(x)$ denotatzen duguna, $\{x^g \mid g \in G\}$ multzoa da.

Bestalde, gogora dezagun noiz esaten den talde batek multzo baten gainean eragiten duela. Definizioz, G talde batek, hutsa ez den Ω multzo baten gainean eragiten du, edozein $g \in G$ eta edozein $x \in \Omega$-rako existitzen bada Ω-ko xg elementu bakarra zeintzentzat, edozein $g_1, g_2 \in G$-rako ($x \in \Omega$ izanik) ondoko baldintzak betetzen diren:

(i) $(xg_1)g_2 = x(g_1g_2)$.

(ii) $x1 = x$.

Egoera honetan Ω-ko x elementu bakoitzaren orbita, $\mathrm{Orb}_G(x) = \mathrm{Orb}(x)$ bidez denotatzen dena: $\{xg \mid g \in G\}$, Ω-ren azpimultzoa da, eta x-ren estabilizatzailea, $\mathrm{Stab}_G(x)$ bidez denotatzen dena: $\{g \in G \mid xg = x\}$, G-ren azpitaldea da. Jakina da, $|\mathrm{Orb}_G(x)| = |G : \mathrm{Stab}_G(x)|$ dela.

Azter dezagun orain aipatutako ekintzei buruzko orbiten kopuruaren formula bat.

Lema 2.3.1. (**Cauchy Frobeniusen lema**)
Izan bitez G talde finitua eta Ω multzo finitua. Demagun G taldeak Ω-ren gainean eragiten duela. Orduan, eragina horren k_G orbiten kopurua, ondoko adierazpenaren bidez emanda dago,

$$k_G = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{fix}(g)|,$$

$\mathrm{fix}(g)$, g elementuaren bidez finko geratzen diren Ω-ko elementuek osatutako multzoa izanik.

Froga. Denota dezagun $O = \{\mathrm{Orb}_G(x) \mid x \in \Omega\}$ bidez, Ω-ren gainean eragiten duen ekintzaren orbita desberdinen multzoa, eta $|O| = k_G$.

Izan bedi $X = \{(x, g) \in \Omega \times G \mid xg = x\}$. Alde batetik ondokoa dugu,

$$X = \bigcup_{x \in \Omega} \{x\} \times \{g \in G \mid xg = x\} = \bigcup_{x \in \Omega} \{x\} \times \mathrm{Stab}_G(x),$$

eta bestetik,

$$X = \bigcup_{g\in G} \{x \in \Omega \mid xg = x\} \times \{g\} = \bigcup_{g\in G} \mathrm{fix}(g) \times \{g\}.$$

X multzoaren bi adierazpenetan kardinalak hartuz, eta kontutan harturik horietan agertzen diren bildurak disjuntuak direla, ondoko berdintzak lortzen dira. Alde batetik,

$$|X| = \sum_{x\in\Omega} |\{x\} \times \mathrm{Stab}_G(x)| = \sum_{x\in\Omega} |\mathrm{Stab}_G(x)|.$$

Bestetik,

$$|X| = \sum_{g\in G} |\mathrm{fix}(g) \times \{g\}| = \sum_{g\in G} |\mathrm{fix}(g)|.$$

Orain, arestian aipatutako estabilizatzailearen propietateagatik, jakina da Ω-ko edozein x elementurako, $|\mathrm{Orb}_G(x)| = |G : \mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$ dela, eta hemendik, $|\mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Orb}_G(x)|}$ dugu. Ondorioz,

$$\sum_{x\in\Omega} |\mathrm{Stab}_G(x)| = |G| \sum_{x\in\Omega} \frac{1}{|\mathrm{Orb}_G(x)|}.$$

Bestalde, aipatutako ekintzaren orbita desberdinek Ω multzoaren partiketa osatzen dutenez, $\sum_{x\in\Omega} \frac{1}{|\mathrm{Orb}_G(x)|} = \sum_{x\in\Omega} \frac{1}{|\mathrm{Orb}(x)|}$ adierazpenak, ondoko garapena onartzen du:

$$\begin{aligned}
\sum_{x\in\Omega} \frac{1}{|\mathrm{Orb}(x)|} &= \sum_{\mathrm{Orb}(x)\in O} \; \sum_{w\in\mathrm{Orb}(x)} \frac{1}{|\mathrm{Orb}(w)|} \\
&= \sum_{\mathrm{Orb}(x)\in O} \frac{1}{|\mathrm{Orb}(w)|} \sum_{w\in\mathrm{Orb}(x)} 1 \\
&= \sum_{\mathrm{Orb}(x)\in O} \frac{1}{|\mathrm{Orb}(w)|} |\mathrm{Orb}(w)| \\
&= \sum_{\mathrm{Orb}(x)\in O} 1 = |O| = k_G.
\end{aligned}$$

Ondorioz, $|X| = \sum_{x\in\Omega} |\mathrm{Stab}_G(x)| = |G| \cdot k_G$ ondorioztatzen da, eta hemendik $\sum_{g\in G} |\,\mathrm{fix}(g)| = |X| = |G| \cdot k_G$. Azkenik, $k_G = \frac{1}{|G|} \sum_{g\in G} |\,\mathrm{fix}(g)|$ dela ondorioztatzen da, frogatu nahi genuen bezala. □

Lema 2.3.2. Izan bedi G talde finitua. Orduan, $|L(G)| = \sum_{x \in G} |C_G(x)|$ da.

Froga. Definizioz badakigu $L(G) = \{(x, y) \in G \times G \mid xy = yx\}$ dela, eta bestalde $C_G(x) = \{g \in G \mid xg = gx\}$ denez, erraz ohar gaitezke ondoko adierazpenetaz: $L(G) = \bigcup_{x \in G} (\{x\} \times C_G(x))$, bildura berri hori disjuntua izanik. Beraz,

$$|L(G)| = |\bigcup_{x \in G} (\{x\} \times C_G(x))| = \sum_{x \in G} |\{x\} \times C_G(x)| = \sum_{x \in G} |C_G(x)|.$$

□

Teorema 2.3.1. Izan bitez G talde finitua eta k_G konjugazio klase ezberdinen kopurua. Orduan, $k_G = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|$.

Froga. Konjugazio ekintza kontsideratuz, $\mathrm{Orb}_G(x) = \{x^g \mid g \in G\} = \mathrm{Cl}_G(x)$ eta $\mathrm{fix}(g) = \{x \in G : x^g = x\} = C_G(g)$ berdintzak ditugu. Beraz, Cauchy Frobeniusen 2.3.1 Lema aplikatuz, $k_G = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)| = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|$.

□

Behin talde baten konjugazio klaseen eta zentralizatzaileen arteko erlazioa aztertuta, Cauchy Frobeniusen Leman oinarrituta, talde baten trukatze probabilitatea kalkulatzeko adierazpen esplizitu bat emango dugu.

Teorema 2.3.2. Izan bitez G talde finitua eta k_G konjugazio klase ezberdinen kopurua. Orduan, $cp(G)=\frac{k_G}{|G|}$ da.

Froga. Alde batetik Teorema 2.3.1-gatik, jakina da konjugazio klaseen kopurua: $k_G = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|$ dela. Bestalde, Lema 2.3.2-gatik G-n trukatzen diren elementu bikoteen multzoaren tamaina kalkulatzeko, nahikoa da taldearen zentralizatzaileen kardinaleei erreparatzea, hots, $|L(G)| = \sum_{g \in G} |C_G(g)|$.
Orain, trukatze probabilitatearen definizioa erabiliz, ondokoa dugu:

$$cp(G) = \frac{|L(G)|}{|G|^2} = \frac{\sum_{g \in G} |C_G(g)|}{|G|^2} = \frac{|G| \cdot k_G}{|G|^2} = \frac{k_G}{|G|}.$$

□

2.4 Trukatze probabilitatearen borne sakonagoak

Atal honetan, trukatze probabilitatearen bornaketak hedatuko ditugu. Izan ere, trukatze probabilitatearen kalkulua, familia talde zabalagoetara hedatuko dugu, hain zuzen ere, biderkadura kartesiarren eta zatidura taldeen trukatze probabilitateak kontsideratuko ditugu. Baina horretarako, arinago talde teoriaren oinarrizko emaitza batzuk gogoratuko ditugu.

Proposizioa 2.4.1. Izan bitez G eta L bi talde. Orduan, ondorengo baieztapenak betetzen dira:

(i) $G/Z(G)$ talde ziklikoa da baldin eta soilik baldin $G = Z(G)$ bada.

(ii) Edozein $(a, b) \in G \times L$ elementurako, $C_{G\times L}(a, b) = C_G(a) \times C_L(b)$ erlazioa betetzen da.

Froga. i) Has gaitezen lehenengo baieztapena frogatzen. $\Rightarrow$) inplikaziorako, ohartu $G/Z(G)$ talde ziklikoa bada, orduan $G/Z(G) = \langle xZ(G)\rangle$ dela, $x \in G$ elementuren batentzako. Ondorioz, $G = \langle x, Z(G)\rangle$ dugu. Hemendik, $Z(G)$-ren definizioagatik, nabaria da x elementua $Z(G)$-ko elementu guztiekin trukatzen dela, eta ondorioz G taldea abeldarra da, edo baliokidea dena, $G = Z(G)$ da.

Bestalde, $\Leftarrow$) inplikaziorako, baldin eta $G = Z(G)$ bada, $Z(G) \trianglelefteq G$ denez, $G/Z(G)$ zatidura taldea eraiki daiteke, hau da, eraiki daiteke $Z(G)/Z(G) = \overline{1}$ zatidura taldea. Azkenik, nabaria da azken zatidura hori ziklikoa dela.

ii) Bestalde, bi talde (ezberdinen edo berdinen) biderkadura kartesiarreko zentralizatzaileen garapena ondokoa da:
$C_{G\times L}(a, b) = \{(x, y) \in G \times L \mid (a, b)^{(x,y)} = (a, b)\} = \{(x, y) \in G \times L \mid (a^x, b^y) = (a, b)\} = \{(x, y) \in G \times L \mid a^x = a \text{ eta } b^y = b\} = \{x \in G \mid a^x = a\} \times \{y \in L \mid b^y = b\} = C_G(a) \times C_L(b)$. □

Proposizioa 2.4.2. Izan bitez G eta L talde finitu ez abeldarrak. Orduan, $cp(G \times L) = cp(G) \cdot cp(L)$

Froga. Alde batetik, 2.3.2 Teoremagatik badakigu, G eta L taldeen trukatze propietateak, $cp(G) = \frac{k_G}{|G|}$ eta $cp(L) = \frac{k_L}{|L|}$ formulen bidez adierazi daitezkeela, $k_G = \sum_{g\in G} \frac{1}{|G|}|C_G(g)|$ eta $k_L = \sum_{l\in L} \frac{1}{|L|}|C_L(l)|$ izanik, 2.3.1 Teoremako emaitzagatik. Modu berdinean, $G \times L$ biderkadura kartesiarraren trukatze probabilitatea ondorengo formula bidez kalkula daiteke:

$$cp(G \times L) = \frac{k}{|\ G \times L\ |}, \text{ non } k = \frac{1}{|G||L|} \sum_{g\in G, l\in L} C_{G\times L}(g, l),$$

$G \times L$ biderkadura kartesiarreko konjugazio klaseen kopurua den.

Orain, 2.4.1 proposizioaren (ii) atala erabiliz,

$$\begin{aligned} k =& \frac{1}{|G||L|} \sum_{(g,l)\in G\times L} |C_{G\times L}(g,l)| = \frac{1}{|G||L|} \sum_{g\in G, l\in L} |C_G(g)\times C_L(l)| \\ &= \frac{1}{|G||L|} \sum_{g\in G} |C_G(g)| \sum_{l\in L} |C_L(l)| = \sum_{g\in G} \frac{|C_G(g)|}{|G|} \sum_{l\in L} \frac{|C_L(l)|}{|L|} = k_G \cdot k_L \end{aligned}$$

Hemendik, $cp(G\times L) = \dfrac{k}{|\ G\times L\ |} = \frac{k_G}{|G|}\cdot\frac{k_L}{|L|} = cp(G)\cdot cp(L)$. □

Behin, taldeen arteko biderkadura kartesiarraren trukatze probabilitatea aztertu dugula, G talde baten azpitaldeen eta zatidura taldeen trukatze probabilitateak aztertuko ditugu. Zentzu batean, talde baten trukatze probabilitatea handia denean, orduan eta trukatzeari buruzko informazio txikiagoa dugula esan genezake, orden bateko talde abeldarrek haiei buruzko informazio gutxi islatzen dutelako, trukakortasuna dela eta. Hortaz, zentzukoa dirudi pentsatzea G talde baten azpitaldeen eta zatidura taldeen trukatzeari buruzko informazioa G-rena baino txikiagoa dela, eta ondorioz haien trukatze probabilitateak handiagoak izatea. Emaitza hauek aztertzeko, ondorengo teoremak aurkezten dira.

Teorema 2.4.1. Izan bitez G talde finitua eta $H \trianglelefteq G$. Orduan, $cp(G/H) \geq cp(G)$ dugu. Gainera, $cp(G/H) = cp(G)$ berdintza ematen da baldin eta soilik baldin $[x,y] \in H$ izateak, $[x,y] = 1$ ondorioztatzen badu. Bestalde, goiko berdintza ematen denean, $H \leq Z(G)$ egiaztatzen da.

Froga. Alde batetik, $cp(G) = \frac{|L(G)|}{|G|^2}$ eta $cp(G/H) = \frac{|L(G/H)|\cdot|H|^2}{|G|^2}$ ditugu. Bestetik, kontuan hartu $L(G/H)$, G/H zatidura taldean elkar trukatzen diren elementu bikoteen multzoa dela, hau da,

$$\begin{aligned} L(G/H) &= \{(xH,yH)\in G/H\times G/H \mid xHyH = yHxH\} \\ &= \{(xH,yH)\in G/H\times G/H \mid xyH = yxH\} \\ &= \{(xH,yH)\in G/H\times G/H \mid (yx)^{-1}xy \in H\} \\ &= \{(xH,yH)\in G/H\times G/H \mid [x,y]\in H\}. \end{aligned}$$

Gainera, $\frac{|\{(x,y)\in G\times G \mid [x,y]\in H\}|}{|H|^2} = |L(G/H)|$ betetzen da, eta hemendik

$$\begin{aligned} |H|^2|L(G/H)| &= |\{(x,y)\in G\times G \mid [x,y]\in H\}| \geq |\{(x,y)\in G\times G \mid [x,y]=1\}| \\ &= |\{(x,y)\in G\times G \mid xy=yx\}| = |L(G)| \text{ lortzen da.} \end{aligned}$$

Beraz, $cp(G/H) = \frac{|L(G/H)|\cdot|H|^2}{|G|^2} \geq \frac{|L(G)|}{|G|^2} = cp(G)$, hau da, $cp(G/H) \geq cp(G)$. Gainera, goiko desberdintzako garapena aztertuz, argi ikusten da

$cp(G/H) = cp(H)$ dela baldin eta soilik baldin edozein $(x, y) \in G \times G$ emanik, $[x, y] \in H$ izateak, $[x, y] = 1$ ondorioztatzen badu. Bereziki, aurreko berdintza betetzen bada, edozein $x \in H$ eta $g \in G$ emanik, H, G-ren azpitalde normala izanik, nabaria da $[x, g] = x^{-1}x^g \in H$ dela, eta ondorioz kasu honetan, $[x, g] = 1$ lortuko litzateke, edo baliokideki $x \in Z(G)$ izatea, $x \in H$ izanik. Hau da, kasu honetan, $H \leq Z(G)$ betetzen da. □

Oharra 2.4.1. Baina $H \leq Z(G)$ izatea ez da baldintza nahikoa, $cp(G) = cp(G/H)$ erlazioa betetzeko. Honetaz ohartzeko, ondorengo adibidea aurkezten da. Izan bitez $G = Q_8$, koaternioien taldea eta $H = Z(Q_8) = \langle -1 \rangle$ honen zentrua. Arestian (2.2.2 Adibidean) ikusi dugu, $cp(Q_8) = \frac{5}{8}$ dela. Bestalde, $Q_8/H = Q_8/\langle -1 \rangle$ zatidura taldea 4 ordenako talde abeldarra da. Beraz, $cp(Q_8/H) = 1$, baina ordea $cp(Q_8) \neq 1$.

Teorema 2.4.2. Izan bitez G talde finitua eta $H \leq G$. Orduan, ondorengo erlazioa betetzen da: $cp(G) \leq cp(H)$.

Froga. Har ditzagun edozein $h \in H$ eta edozein $g \in G$. Alde batetik, $C_H(g) = C_G(g) \cap H$, eta bereziki $C_H(h) = C_G(h) \cap H$ dira. Orain, kontuan izanik bi azpimultzoren biderketaren kardinala adierazteko formula, ondorengo bornaketa lor daiteke, $C_G(g)H \subseteq G$ delako.

$$|C_G(g) \cap H| = \frac{|C_G(g)| \cdot |H|}{|C_G(g)H|} \geq \frac{|C_G(g)| \cdot |H|}{|G|}.$$

Denota dezagun $|G : H| = m$. Talde teoriako oinarrizko emaitzengatik jakina da, edozein $g \in G$ elementurako $C_H(g) \leq C_G(g)$ dela, eta baita ere $|C_G(g) : C_H(g)| \leq m = |G : H|$ dela. Ondorioz, $|C_G(g)| \leq m|C_H(g)|$.
Orain batuketa bikoitzaren erlazioak kontuan hartuta, ondokoa lortzen da:

$$\sum_{g \in G} |C_H(g)| = |\{(g, h) \mid g \in G, h \in H, gh = hg\}| = \sum_{h \in H} |C_G(h)|.$$

Ondorioz,

$$|L(G)| = \sum_{g \in G} |C_G(g)| \leq \sum_{g \in G} m \cdot |C_H(g)| = \sum_{h \in H} m \cdot |C_G(h)| \leq \sum_{h \in H} m^2 \cdot |C_H(h)|.$$

Orain, trukatze probabilitatearen definizioa eta arestian erabilitako formulak erabiliz, emaitza frogatuta geratzen da. Hots,

$$cp(G) = \frac{|L(G)|}{|G|^2} = \frac{\sum_{g \in G} |C_G(g)|}{|G|^2} \leq \frac{\sum_{h \in H} m^2 \cdot |C_H(h)|}{|G|^2}$$
$$= \frac{\sum_{h \in H} |C_H(h)|}{|H|^2} = \frac{|L(H)|}{|H|^2} = cp(H).$$

□

Teorema 2.4.3. Izan bitez G talde finitua eta $H \trianglelefteq G$. Orduan,

$$cp(G) \leq cp(H) \cdot cp(G/H).$$

Froga. Denota dezagun $\overline{G} = G/H$. Trukatze probabilitatearen definizioa erabiliz, $cp(G) = \frac{k_G}{|G|^2}$, $cp(H) = \frac{k_H}{|H|^2}$ eta $cp(G/H) = \frac{k_{\overline{G}} \cdot |H|^2}{|G|^2}$ dira.

Orain, $cp(G) \leq cp(H) \cdot cp(G/H)$ dela frogatzeko, $k_G \leq k_H \cdot k_{\overline{G}}$ desberdintza egiaztatzea nahikoa da, edo baliokidea dena, $|L(G)| \leq |L(H)| \cdot |L(\overline{G})|$ ikustea.

2.3.2 Lema erabiliz, $|L(G)| = \sum_{g \in G} |C_G(g)|$, $|L(H)| = \sum_{h \in H} |C_H(h)|$ eta $|L(\overline{G})| = \sum_{\overline{g} \in \overline{G}} |C_{\overline{G}}(\overline{g})|$ berdintzak ditugu. Bestalde, 2.4.2 Teoremaren frogan ikusi dugun moduan, ondorengo desberdintza ere betetzen da:

$$|L(G)| = \sum_{g \in G} |C_G(g)| \leq |G : H| \cdot \sum_{g \in G} |C_H(g)|$$

Gainera, $|G : H| \leq \sum_{\overline{g} \in \overline{G}} |C_{\overline{G}}(\overline{g})|$ erlazioa berehalakoa da. Izan ere, baldin eta $|G : H| = m$ bada, $|C_{\overline{G}}(\overline{g})| \geq 1$ denez, $\sum_{\overline{g} \in \overline{G}} |C_{\overline{G}}(\overline{g})| \geq m$ beteko da. Antzeko bornaketak eginez, (hauek ikusteko kontsultatu [7] artikulua), $cp(G) \leq cp(H) \cdot cp(G/H)$ erlazioa frogatuta geratzen da. □

Bestalde, aurreko 2.4.3 Teoremak, biderkadura erdizuzenaren kasura aplikatuta, biderkadura horri lotutako trukatze probabilitatearen formula bat ematen du. Baina formula eman baino lehen gogora dezagun barruko biderkadura erdizuzenaren definizioa. Hain zuzen ere, definizioz G taldea, H eta N azpitaldeen barruko biderkadura erdizuzena dela diogu, $G = H \ltimes N$ bidez denotatuko duguna, ondorengo hiru baldintzak betetzen badira: $N \trianglelefteq G$, $G = HN$ eta $H \cap N = \{1\}$. Egoera honetan, N, biderkadura erdizuzenaren nukleoa deitzen da, eta H biderkadura erdizuzenaren osagarria.

2.4.1. korolarioa. Izan bitez $H \leq G$ eta $N \trianglelefteq G$ bi azpitalde finitu eta G horien arteko biderkadura erdizuzena, hots, $G = H \ltimes N$. Orduan,

$$cp(G) \leq cp(N) \cdot cp(H)$$

Froga. Biderkadura erdizuzenaren ezaugarriengatik, $N \trianglelefteq G$ eta $G/N \cong H$. Beraz, 2.4.3 Teorema aplikatuz,

$$cp(G) \leq cp(N) \cdot cp(G/N) = cp(N) \cdot cp(H),$$

nahi genuen bezala. □

Definizioa 2.4.1. G taldearen konposizio seriea G-ren azpitaldeen segida finitua da, hots,

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$$

moduko katea, non edozein $i \in \{1, \ldots, k\}$ baliorako G_i/G_{i-1} konposizio faktorea talde sinplea den, hau da, horietariko faktore bakoitza azpitalde normal tribialik gabeko taldea den.

Teorema 2.4.4. Izan bedi $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G$, G taldearen konposizio seriea, edozein $i \in \{1, \ldots, k\}$ baliorako i. konposizio faktorea $G_i/G_{i-1} = H_i$-ren bidez denotatuz. Orduan,

$$cp(G) \leq \prod_{i=1}^{k} cp(H_i).$$

Froga. Froga konposizio seriaren luzearen gaineko, hau da, k zenbakiaren gaineko indukzioren bidez garatuko dugu. Lehendabizi, $k = 1$ kasua aztertuko dugu. Egoera honetan, $\{1\} = G_0 \trianglelefteq G_1 = G$ konposizioa seriea dugu. Orduan, 2.4.3 Teorema erabiliz, eta kontuan izanik $G_0 \trianglelefteq G$, $G_1/G_0 = H_1$ direla, ondorengo desberdintza lortuko genuke:

$$cp(G) \leq cp(G_0) \cdot cp(G_1/G_0) = cp(\{1\}) \cdot cp(H_1) = cp(H_1), \text{ nahi genuena.}$$

Orain, demagun emaitza $k-1$ luzera duen edozein konposizio serie batentzat betetzen dela. Bereziki, enuntziatutako emaitza suposa dezakegu $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{k-1}$ konposizio seriearentzat egia dela. Beraz, $cp(G_{k-1}) \leq \prod_{j=1}^{k-1} cp(M_j)$ betetzen da edozein $j \in \{1, \ldots, k-1\}$ baliorako, $M_j = G_j/G_{j-1} \equiv H_j$ izanik. Hau da, $cp(G_{k-1}) \leq \prod_{j=1}^{k-1} cp(H_j)$.

Froga dezagun orain enuntziatuko desberdintza egia dela k kasurako. Alde batetik, $G_{k-1} \trianglelefteq G_k = G$ denez, eraiki daiteke $\bar{G} = G/G_{k-1}$ zatidura taldea. Bestetik, 2.4.3 Teorema erabiliz, $cp(G) \leq cp(G_{k-1}) \cdot cp(G/G_{k-1})$ dugu. Hasierako konposizio seriearen k. konposizio faktorea G/G_{k-1}, H_k bidez denotatzen denez, arestian lortutako desberdintza ondorengo moduan berriadtz daiteke: $cp(G) \leq cp(G_{k-1}) \cdot cp(H_k)$. Azkenik, $cp(G_{k-1}) \leq \prod_{j=1}^{k-1} cp(H_j)$ desberdintza erabiliz,

$$cp(G) \leq \prod_{j=1}^{k-1} cp(H_j) \cdot cp(H_k) = \prod_{i=1}^{k} cp(H_i) \text{ dugu,}$$

frogatu nahi genuen bezala. □

Jarraian, trukatze probabilitatea bornatzea ahalbidetzen duen Erdös-en teorema aurkezten da.

Teorema 2.4.5. [Erdös-en teorema] [9]. Izan bedi G talde finitu ez abeldarra. Orduan, $cp(G) \leq \frac{5}{8}$.

Froga. Lehendabizi, ohar gaitezen $|G : Z(G)| \geq 4$ dela. Alde batetik, ezinezkoa da $|G : Z(G)| = 1$ izatea. Kontrako kasuan, $G = Z(G)$ izango litzateke, hau da, G talde abeldarra izango litzateke, hasierako hipotesiaren kontra doana. Bestalde, $|G : Z(G)| = 2$ edo 3 badira, orduan A Eranskineko 1 ariketagatik, $G/Z(G)$ zatidura taldea 2 edo 3 ordenako talde siklikoa litzateke, hurrenez hurren, eta 2.4.1 Proposizioko (i) ataletik, berriro ere G abeldarra dela ondorioztatuko genuke, hipotesiaren aurka doana. Beraz, $|G : Z(G)| \geq 4$ edo baliokideki $\frac{|Z(G)|}{|G|} \leq \frac{1}{4}$.

Gainera, edozein $a \notin Z(G)$-rako $C_G(a) \neq G$ edo baliokideki $|G : C_G(a)| \geq 2$ betetzen da, eta ondorioz, $\frac{|C_G(a)|}{|G|} \leq \frac{1}{2}$. Orain, adibidez, Lema 2.3.2 erabiliz,

$$\begin{aligned} cp(G) &= \sum_{g\in G} \frac{|C_G(g)|}{|G|^2} = \sum_{g\in Z(G)} \frac{|C_G(g)|}{|G|^2} + \sum_{g\in G-Z(G)} \frac{|C_G(g)|}{|G|^2} \\ &\leq \sum_{g\in Z(G)} \frac{|G|}{|G|^2} + \sum_{g\in G-Z(G)} \frac{1}{2|G|} = \frac{|Z(G)|}{|G|} + \frac{|G|-|Z(G)|}{2|G|} \\ &= \frac{|Z(G)|+|G|}{2|G|} = \frac{|G|}{2|G|} + \frac{|Z(G)|}{2|G|} = \frac{1}{2} + \frac{|Z(G)|}{2|G|} \\ &\leq \frac{1}{2} + \frac{1}{2\cdot 4} = \frac{5}{8} \text{ dugu.} \end{aligned}$$

(Lehehengo bornaketa egiteko, kontuan hartu dugu edozein $g \notin Z(G)$ elementurako $C_G(g) < G$ dela, eta ondorioz $|G : C_G(g)| \geq 2$ dela. Bigarren bornaketa egiteko, aldiz, ohartu $\frac{|Z(G)|}{|G|} \leq \frac{1}{4}$ dela.) □

Ohar gaitezen aipatutako goi bornea berdintza bihurtzen dela infinitu talderentzako. Izan ere, 2.2.2 Adibideagatik jakina da $cp(Q_8) = \frac{5}{8}$ dela, eta 2.4.2 Proposizioa erabilita, ohar gaitezke edozein G talde finitu abeldarra emanik, $G \times Q_8$ taldearen trukatze probabilitatea ere $\frac{5}{8}$ dela.

Oharra 2.4.2. Aurreko 2.4.5 Teoremak, talde finitu baten trukatze probabilitatearentzako goi borne bat ematen du. Baita interesgarria izango litzateke, ez tribiala den behe borneren baten existentzia aztertzea. Alabaina, talde finitu orokor baten trukatze probabilitateak ez du (baliogarria den) behe borne ez tribial orokorrik.

Kontsidera dezagun $G_1 = S_3$, 3 kardinaleko talde simetrikoa eta defini dezagun edozein $n \geq 2$ arruntarako, $G_n = G_{n-1} \times S_3$. Jadanik, jakina dugu $cp(S_3) = 0.5$ dela eta gertaeren independentzia eta 2.4.2 Proposizioa kontutan harturik, erraz ikus daiteke $cp(G_n) = (0.5)^n$ dela. Bestalde,

$\lim_{n\to\infty}(0.5)^n = 0$ denez, hemendik ohar gaitezke ezin dugula esplizituki talde finitu orrokorrentzako ez tribiala eta baliogarria den behe borne orokor bat aurkitu.

2.4.2. korolarioa. Izan bedi G talde finitu ez abeldarra. Orduan G-k gehienez, $\lfloor\frac{5|G|}{8}\rfloor$ konjugazio klase desberdin ditu.

Froga. 2.3.2 Teoremako emaitza erabiliz, $cp(G) = \frac{k_G}{|G|}$ dugu, k_G, G taldearen konjugazio klase kopurua izanik. Bestalde, Erdös-en 2.4.5 Teorema erabiliz, $cp(G) \leq \frac{5}{8}$ dugu. Beraz, $\frac{k_G}{|G|} \leq \frac{5}{8}$ da, eta ondorioz, $k_G \leq \frac{5|G|}{8}$. Orain, talde baten konjugazio klaseen kopurua zenbaki arrunta denez, nahikoa da aurreko desberdintzari lur funtzioa aplikatzea, $k_G \leq \lfloor\frac{5|G|}{8}\rfloor$ desberdintza lortzeko. □

Definizioa 2.4.2. Izan bedi G talde finitu (ez abeldarra). $cp(G) = \frac{5}{8}$ berdintza betetzen duten G taldeei 5-8 taldeak deritze.

Erdösen 2.4.5 teoremako frogan ikusi den moduan, 5-8 taldeen deskribapena, (1) baldintza: $|G : Z(G)| = 4$, eta (2) baldintza: edozein $g \in G - Z(G)$ elementurako, $|G : C_G(g)| = 2$ betetzearen baliokidea da. Gainera, baldin eta G ez bada abeldarra, $|G : Z(G)| = 4$ baldintzak, $G/Z(G) \cong V_4 \cong C_2 \times C_2$ egitura derrigortzen du, eta hemendik berehalakoa da (2) baldintza ondorioztatzea. Beraz, hemendik aurrera G, 5-8 taldea izatea, eta $G/Z(G)$ Klein-eko 4-taldea izatea egitura baliokideak izango dira.

Bestalde, jadanik ikusi dugu $cp(Q_8) = \frac{5}{8}$ dela, eta A eranskineko 4 Ariketagatik ere jakina da $cp(D_8) = \frac{4+6}{4\cdot 4} = \frac{5}{8}$ dela. Beraz, Q_8 koaternioien taldea eta 8 kardinaleko D_8 talde diedrikoa, *5-8 taldeak* dira.

Trukatze probabilitatearen kalkuluari dagokionez, emaitza desberdinak lortzen ari gara bornaketa berriak emanez. G taldeari baldintza gehigarriak eskatuz gero, borne horiek hobe daitezke eta emaitza zehatzagoak lortu, arestian aipatutako 5-8 taldeekin gertatzen zen moduan. Horretarako, ondorengo proposizioa aurkezten da, 2 indizeko H azpitalde abeldarra duten G taldeen trukatze probabilitatea esplizituki kalkulatzea ahalbidetzen duena.

Proposizioa 2.4.3. Demagun G talde ez abeldar finitu batek 2 indizeko H azpitalde abeldarra duela. Orduan, $Z(G)$, H-ren azpitalde propioa da eta $cp(G) = \frac{n+3}{4n}$ betetzen da, $n = |H : Z(G)|$ izanik.

Froga. H, G-ren 2 indizeko azpitaldea denez, H azpitalde normala da G-n. Har dezagun $x \in G \setminus H$. Nola G talde ez abeldarra den, x ez da trukatzen behintzat $u \in H$-ko elementu batekin. Gainera, edozein $g \in G$ hartuta, $g = hx^i$ moduan idatz daiteke, $h \in H$ eta $i \in \{0, 1\}$ izanik (hau da, $g = h$ edo $g = hx$ motakoa da). Bestalde, edozein $h \in H$ elementurako, hx ez da u

elementuarekin trukatzen. Halabeharrez, $Z(G) \subseteq H \setminus \{u\}$ eta $Z(G)$, H-ren azpitalde propioa direla ondorioztatzen da.

Denota ditzagun $n = |H : Z(G)|$ eta $m = |Z(G)|$. Nola $|G : H| = 2$ den, $|G| = 2nm$ dela ondorioztatzen da.

Bestalde, orbita estabilitzailearen teorema aplikatuz, badakigu $y \in G$ elementu bakoitzarentzat $|\mathrm{Cl}_G(y)| = |G : \mathrm{C}_G(y)|$ dela. Hasteko, bereiztu ditzagun hiru kasu: a) $y \in Z(G)$; b) $y \in H \setminus Z(G)$ eta c) $y \in G \setminus H$. Lehenengo (a) kasuan, y elementuak konjugatu bakarra du; bigarren (b) kasuan, y elememtuak bi konjugatu desberdin ditu, eta hirugarren (c) kasuan A Eranskineko Ariketa 2-gatik badakigu y elementuak n konjugatu desberdin dituela. Ondorioz,

$$\begin{aligned} k_G &= |Z(G)| + \frac{|H| - |Z(G)|}{2} + \frac{|G| - |H|}{n} \\ &= m + \frac{nm - m}{2} + \frac{nm}{n} = 2m + \frac{nm - m}{2} = \frac{(n+3)m}{2} \end{aligned}$$

eta 2.3.2 Teorema erabiliz, $cp(G) = \frac{k_G}{|G|} = \frac{(n+3)m}{2.2nm} = \frac{n+3}{4n}$ dugu, frogatu nahi genuen bezala. □

Egoera honen kasu partikularra, A Eranskineko Ariketa 4-an topa dezakegu. Hain zuzen ere, kontsidera dezagun D_{2n}, $2n$ kardinaleko talde diedrikoa non n zenbaki bakoitia den, $\langle x, y \mid x^n = y^2 = 1, x^y = x^{-1} \rangle$ aurkezpena duelarik. Kasu honetan, $Z(D_{2n}) = 1$ da eta $H = \langle x \rangle$, D_{2n}-ren 2 indizeko talde ziklikoa (eta ondorioz, abeldarra) da, $|H : Z(D_{2n})| = n$ izanik. Beraz, 2.4.3 Proposiziagatik, $cp(D_{2n}) = \frac{n+3}{4n}$ dela baieztatzen da, Ariketa 4-an frogatu den modura.

Ikusten den bezala, praktikan zaila izaten da G talde baten trukatze probabilitatea kalkulatzea. Horregatik, hemendik aurrera goi eta behe borne hobeagoak aurkitzen saiatuko gara.

Teorema 2.4.6. Izan bitez G talde finitu ez abeldarra eta p, $|G|$ zatitzen duen zenbaki lehenik txikiena. Orduan, $cp(G) \leq \frac{1}{p} + \frac{(p-1)}{p|G:Z(G)|} \leq \frac{p^2+p-1}{p^3}$.

Froga. Alde batetik, edozein $a \notin Z(G)$ elementurako $C_G(a) \neq G$ da, eta emandako p-ren definizioagatik, edozein $a \notin Z(G)$-rako $|G : C_G(a)| \geq p$ dela ondorioztatzen da, edo baliokideki $\frac{|C_G(a)|}{|G|} \leq \frac{1}{p}$ dela. Orain, 2.3.2 Lema erabiliz, ondokoa dugu:

$$\begin{aligned} cp(G) &= \sum_{g\in G} \frac{|C_G(g)|}{|G|^2} = \sum_{g\in Z(G)} \frac{|C_G(g)|}{|G|^2} + \sum_{g\in G-Z(G)} \frac{|C_G(g)|}{|G|^2} \\ &\leq \sum_{g\in Z(G)} \frac{|G|}{|G|^2} + \sum_{g\in G-Z(G)} \frac{1}{p\cdot|G|} = \frac{|Z(G)|}{|G|} + \frac{|G|-|Z(G)|}{p\cdot|G|} \\ &= \frac{(p-1)\cdot|Z(G)|+|G|}{p\cdot|G|} = \frac{(p-1)\cdot|Z(G)|}{p\cdot|G|} + \frac{1}{p} \\ &= \frac{1}{p} + \frac{(p-1)}{p\cdot|G:Z(G)|}. \end{aligned}$$

Azkenik, froga dezagun egoera honetan, $|G:Z(G)| \geq p^2$ dela. Alde batetik, argi dago, $|G:Z(G)|$ ezin daitekeela ez 1 ez q zenbaki lehen bat izan; bestalde, G taldea abeldarra izango litzateke (erabili 2.4.1 Proposizioaren (i) atala, eta hori hipotesiaren aurka doa). Beraz, $|G:Z(G)| = m(= m_1\cdot m_2)$ zenbaki konposatua litzatekete, non $m \in \mathbb{N}$ den, eta m_1, m_2 zenbaki arruntak $|G|$-ren zatitzaileak diren. Orain, enuntziatuko p-ren definizioagatik, argi dago $m_1 \geq p$, $m_2 \geq p$ direla, eta ondorioz, $|G:Z(G)| \geq p^2$ da, edo baliokideki, $\frac{1}{|G:Z(G)|} \leq p^2$.

Ondorioz, $cp(G) \leq \frac{1}{p} + \frac{p-1}{p|G:Z(G)|} \leq \frac{1}{p} + \frac{p-1}{p^3} = \frac{p^2+p-1}{p^3}$. □

Arestian aipatu den moduan, orokorki ezin da esplizituki talde finitu orrokorrentzako ez tribiala eta baliogarria den behe borne orokorra aurkitu. Alabaina, G taldearen propietateak aztertuta, batzuetan, trukatze probabilitatearen ez tribialak diren behe borne hobeagoak eman daitezke. Honi lotuta, ondorengo teorema aurkezten da.

Teorema 2.4.7. Izan bitez G talde finitua, eta p, $|G|$ zatitzen duen zenbaki lehenik txikiena. Denota dezagun $m = |G:Z(G)|$. Orduan, ondorengo behe bornea betetzen da:

$$cp(G) \geq \frac{(p+1)\cdot m - p}{m^2}.$$

Gainera, berdintza betetzen da baldin eta soilik baldin edozein $g \in G-Z(G)$ elementurako, $|C_G(g):Z(G)| = p$ bada.

Froga. Lehendabizi, ohartu edozein $g \in G - Z(G)$ elementua hartuta, $g \in C_G(g) = C_G(\langle g\rangle)$ eta $Z(G) \leq C_G(\langle g\rangle)$ direnez, orduan nabaria dela $Z(G) < C_G(\langle g\rangle)$ partekotasuna. Bestalde, p-ren definizioagatik $|C_G(\langle g\rangle):Z(G)| \geq p$. Ondorioz, $p\cdot|Z(G)| \leq |C_G(g)|$. Orain, 2.3.2 Lema erabiliz eta kontutan

izanda edozein $g \in Z(G)$ elementurako $C_G(g) = G$ dela, ondorengoa dugu:

$$\begin{aligned}|L(G)| &= \sum_{g\in G}|C_G(g)| = \sum_{g\in Z(G)}|C_G(g)| + \sum_{g\in G-Z(G)}|C_G(g)| \\ &= |G|\cdot|Z(G)| + \sum_{g\in G-Z(G)}|C_G(g)| \geq |G|\cdot|Z(G)| + \sum_{g\in G-Z(G)} p|Z(G)| \\ &\geq |G|\cdot|Z(G)| + p\cdot(|G|-|Z(G)|)\cdot|Z(G)|.\end{aligned}$$

Azkenik, trukatze probabilitatearen definizioa erabiliz,

$$\begin{aligned}cp(G) = \frac{|L(G)|}{|G|^2} &\geq \frac{|G|\cdot|Z(G)| + p\cdot(|G|-|Z(G)|)\cdot|Z(G)|}{|G|^2} \\ &= \frac{|G|\cdot|Z(G)| + p\cdot|G|\cdot|Z(G)|}{|G|^2} - \frac{p\cdot|Z(G)|^2}{|G|^2} \\ &= \frac{|Z(G)|\cdot(1+p)}{|G|} - \frac{p}{m^2} \\ &= \frac{p+1}{m} - \frac{p}{m^2} \\ &= \frac{(p+1)\cdot m - p}{m^2}.\end{aligned}$$

Gainera, aurreko garapenik nabaria da aurreko desberdintza berdintza dela baldin eta soilik baldin edozein $g \notin Z(G)$ elementurako $|C_G(g) : Z(G)| = p$ bada. □

2.4.3. korolarioa. Izan bitez G, n kardinaleko talde ez abeldar finitua eta p, n zatitzen duen zenbaki lehenik txikiena non $|G : Z(G)| = m$ den. Orduan, G-k gutxienez, $p\cdot|Z(G)|+1$ konjugazio klase ditu. Are gehiago, G taldeak $(p-1)\cdot|Z(G)|+1 \geq p$ konjugazio klase ez tribial ditu.

Froga. 2.4.7 Teoremaren baieztapenagatik, badakigu $cp(G) \geq \frac{(p+1)\cdot m-p}{m^2}$ desberdintza betetzen dela. Bestalde, $m = |G : Z(G)|$, $|G|$-ren zatitzailea izateagatik, $|G : Z(G)|$ zenbaki ez lehena izateagatik (G talde ez abeldarra delako) eta p-ren definizioagatik, nabaria da $m \geq p^2 > p$ betetzen dela. Beraz, ondorengo bornaketak ditugu:

$$cp(G) \geq \frac{(p+1)\cdot m - p}{m^2} > \frac{(p+1)\cdot m - m}{m^2} \geq \frac{m\cdot(p+1-1)}{m^2} \geq \frac{p}{m},$$

eta bereziki $cp(G) > \frac{p}{m}$. Bestalde, 2.3.2 Teorema erabiliz, $cp(G)=\frac{k}{|G|}$ dugu. Ondorioz, $\frac{k}{|G|} > \frac{p}{m}$ edo baliokidea dena, $k > \frac{p\cdot|G|}{m} = p\cdot|Z(G)|$ ondorioztatzen da. Beraz, $k > p\cdot|Z(G)|$, hau da, G-k gutxienez $p\cdot|Z(G)|+1$ konjugazio klase ditu, eta zentroko elementuen konjugazio klase tribialak alde batera utzita, G taldeak $(p-1)\cdot|Z(G)|+1 \geq p$ konjokazio klase ez tribial ditu. □

Goiko 2.4.3. Korolarioan baldintza bereziak betetzen dituen G talde ez abeldar baten konjugazio klaseen kopuruaren erlazio bat lortu da, taldearen trukatze probabilitatea erabiliz. Ildo honetako ondorio gehiago eman baino lehen, aipa dezagun ondoko emaitza.

Oharra 2.4.3. Demagun G talde batek Ω multzo baten gainean eragiten duela. Orduan, edozein $g \in G$ elementurako $w \to w \cdot g$ aplikazioa, Ω-tik Ω-ra doan aplikazioa da, hau da, Ω multzoko permutazioak ematen dituena. Edozein $g \in G$ elementurako defini dezagun:

$$\begin{aligned} \Theta : G &\to \mathcal{S}_\Omega \\ g &\mapsto \Theta_g : w \mapsto w \cdot g \end{aligned}$$

Goiko Θ aplikazioa, Ω gaineko G-ren permutazio bidezko adierazpena deiturikoa, talde homomorfismoa da. Gainera, nabaria da

$$\operatorname{Ker}\Theta = \{g \in G \mid w \cdot g = w, \text{ edozein } w \in \Omega\} = \bigcap_{w \in \Omega} Stab_G(w) \text{ dela.}$$

Proposizioa 2.4.4. Izan bedi G talde finitu bakuna eta ez abeldarra non $|G| = n \geq k!$ den, $k, n \in \mathbb{N}$ izanik. Orduan, ez da existitzen $H < G$ non $|G : H| \leq k$ betetzen den. Beraz, G taldearen konjugazio klase ez tribial bakoitza gutxienez $k + 1$ tamainukoa da.

Froga. Emaitza k-ren gaineko indukzio matematikoa erabiliz frogatuko da.

$k = 1$ denean, orduan $|G| \geq 1!$ dugu eta G-ko H azpitalde bakarra non $|G : H| \leq 1$ den, $H = G$ talde osoa da, hau da, azpitalde ez propioa. Ondorioz, emaitza betetzen da.

Bereziki $k = 2$ bada, $|G| \geq 2!$ izanik, frogatu beharko litzateke ez dagoela H, G-ren azpitalde propiorik non $|G : H| \leq 2$ den. Baina aurreko kasuan oinarrituta, $|G| \geq 2! \geq 1!$ izanik, eta jakinda ez dagoela H, G-ren azpitalde propioa non $|G : H| \leq 1$ den, orduan egoera honetan nahikoa litzateke ikustea ez dela existitzen $H < G$ non $|G : H| = 2$ den. Gainera, $k = 2$ kasurako arrazoitutako azken argudioa, orokorki edozein $k \geq 2$ kasurako isla daiteke.

Horregatik, $k \geq 2$ izanik, demagun orain $|G| \geq (k-1)!$ kasurako emaitza betetzen dela, hau da, ez dela existitzen $H < G$ non $|G : H| \leq k - 1$ den, eta k kasua frogatzeko, nahikoa da ikustea ez dela existitzen $H < G$ non $|G : H| = k$ den.

Orain, aipatutako azken emaitza hori absurdura eramanez arrazoituko dugu. Hau da, demagun existitzen dela $H < G$ non $|G : H| = k$ den. Har dezagun Ω, H azpitalde horren eskuin koklaseen multzoa, hau da, har dezagun $\Omega = \{Hx \mid x \in G\}$ zeintzentat $|\Omega| = k$ den.

Kontsidera dezagun 2.4.3 Oharreko $G \to \Omega$ ekintza, edo baliokidea dena, $\Theta : G \to \mathcal{S}_\Omega$ talde homomorfismoa, non $\mathcal{S}_\Omega$, k mailako talde simetrikoa eta $\Theta_g(Hx) = Hx \cdot g$ diren. Alde batekik, jakina da Ker $\Theta \trianglelefteq G$ dela, eta bestetik, G talde bakuna denez, bi aukera baino ez daude: Ker $\Theta = \{1\}$ edo Ker $\Theta = G$. Gainera,

$$\text{Ker } \Theta = \bigcap_{w \in \Omega} \text{Stab}_G(w = Hx) \text{ da,}$$

eta Ω-ko w elementu bakoitzarentzat $\text{Stab}_G(w = Hx)$:

$$= \{g \in G \mid Hx.g = Hx\} = \{g \in G \mid xgx^{-1} \in H\} = \{g \in G \mid g \in H^x\},$$

hau da, Ker $\Theta = \bigcap_{x \in G} H^x = H_G$, hots, Ker Θ, G-n H-ren *core* deituriko azpitaldea da, azpitalde hori H barne dagoen G-ren azpitalde normal handiena izanik. Beraz, Ker $\Theta \neq G$ eta Ker $\Theta = \{1\}$, hots, Θ injektiboa da.

Hau da, $\Theta : G \to \mathcal{S}_\Omega$ aplikazio injektiboa dela frogatu da. Ondorioz, $|G| = n \leq k!$ eta $|\mathcal{S}_\Omega| = k!$ direnez, $|G| = k!$ ondorioztatzen da, eta bereziki Θ aplikazioa talde isomorfismoa dela, hau da, G eta $\mathcal{S}_\Omega$ talde isomorfoak dira (orokortasunik galdu gabe $k \geq 3$ dela suposa genezake; hasieran argudiatu dugun modura, bestalde suposatutakoa kontraesan bat litzatekeelako.)

Orain, $k \geq 3$ izanik, jakina da k mailako talde simetrikoak ez direla bakunak, talde horiek bi indizeko azpitalde normalak dituztelako. Hau da, kontraesan orokor batera heldu gara, eta ondorioz hasieran suposatukoa ez da betetzen.

Beraz, orokorki $k \geq 2$ kasurako esan genezake ez dela existitzen $H < G$ non $|G : H| = k$ den, eta ondorioz ez dela existitzen $H < G$ non $|G : H| \leq k$ den.

Bestalde, enuntziatuaren bigarren zatia berehalakoa da, edozein $g \in G$ elementurako $|\,\text{Cl}_G(g)| = |G : C_G(g)|$ delako, $C_G(g) \leq G$ izanik. □

3. kapitulua

Grafo teoria. Talde baten trukatze grafoa

3.1 Motibazioa

Izan bedi G taldea. G taldeari grafo bat elkartu ahal zaio, adibidez, grafoaren V erpinen multzo gisa, G taldeko elementuen multzoa hartzen bada, eta E ertzen multzo gisa, G taldeko elkar trukatzen diren edozein bi elementu lotzen dituzten bikoteen multzoa. Definizio honek aldaerak izan ditzake grafoaren begistak baimentzen edo baimentzen ez diren arabera, edota V erpinen multzoa, G-ko elementu guztien ordez, G taldeko zentroan ez dauden elementuen multzoa hartzen bada, edota beste hainbat faktoreen araberako aldaerak.

Hasteko, gogora dezagun (V, E) grafoa izanik, erpinen multzoaren kardinala, grafoaren maila dela eta ertzen multzoaren kardinala, grafoaren tamaina. Bestetik, edozein bi erpin auzokideak direla esango dugu erpin horiek ertz baten bidez konektatuta badaude. Gainera, $\{v_1, v_2 \ldots, v_{k-1}, v_k\}$ erpinen familia emanda, baldin eta edozein $i \in \{1, \ldots, k-1\}$ indizerako, $v_i v_{i+1} \in E$ bada, orduan $\{v_1, v_2, \ldots, v_{k-1}, v_k\}$ erpinen segidari, v_1 eta v_k erpinen arteko *paseoa* deitzen zaio. Honez gain, erpin guztiak desberdinak dituen paseoari *bidea* esaten zaio.

Esango dugu grafo bat *konexua* dela baldin eta grafoko edozein bi erpin desberdin, bide baten bidez lotu badaitezke. Zentzu honetan, grafo baten osagai konexuak, emandako grafoaren azpigrafo konexu maximalak dira, hau da, (V', E'), (V, E)-ren *osagai konexua* dela esango dugu baldin eta soilik baldin (V', E') grafo konexua bada, eta ez bada existitzen (V, E)-ren beste azpigrafo konexurik (V', E') azpigrafo gisa duenik.

Kapitulu honen hurrengo atalean edozein G talde finitu ez abeldarrentzat, berari dagokion trukatze grafoaren eta trukatze grafo orokortuaren kontzeptuak definituko ditugu, eta ondoren talde ezagun batzuen trukatze grafoak aztertuko ditugu.

Hirugarren atalean, Peter M. Neumann-ek [12] lanean, arlo honekin erlazionatuta dagoen talde bati elkartukako grafoaren emaitza interesgarri bat aurkeztuko da. Emaitza hori aurkeztearen helburua ikerkuntza sakonagoko pintzelkada bat ematea izan da. Hain zuzen ere, artikulu horretako emaitza ulertzea izan da lan zorrotzagoa eskatu duen zatia.

3.2 Talde baten trukatze grafoa

Definizioa 3.2.1. Izan bitez G talde finitua eta X, G-ren azpimultzoa. Deitzen zaio X-ri elkartutako trukatze grafo, $\Gamma = \Gamma(G) = \rho(X, G)$ denotatuko dena, $V(\Gamma)$ erpin multzo gisa: X, eta x, y desberdinak diren bi erpin auzokideak direla esaten denean, baldin eta $xy = yx$ bada.

Garapen honetan, hemendik aurrera, baldin eta G talde finitu ez abeldarra bada, $X = G - Z(G)$ multzoa hartuko dugu, eta berari elkartutako $\rho(X, G)$ grafoa, $\Gamma(G) = \Gamma$ bidez denotatuko dugu. Gure kasuan, grafo ez norabideratua, erpin anizkoitzik gabekoa eta begista gabekoa kontsideratuko da. Azkenik, gogora dezagun v erpinaren maila deitzen zaiola v-ren auzokideak diren erpin desberdinen kopuruari eta grafoko erpin guztiak maila berdina dutenean, grafoa *erregularra* dela esaten dugula.

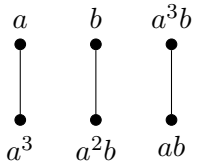
3.2.1 Talde ezagun batzuen trukatze grafoak

Has gaitezen Q_8 koaternioiaren taldea aztertzen.

Adibidea 3.2.1. Har dezagun Q_8 taldearen ondorengo aurkezpena:

$$\langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle.$$

Orduan, Q_8-ko elementuak errepikapenik gabe: $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ dira, eta berezeki $Z(Q_8) = \{1, a^2\}$. Beraz, $\rho(X, Q_8)$ grafoaren erpinen multzoa: $V(\Gamma) = \{a, a^3, b, ab, a^2b, a^3b\}$ da, eta berari dagokion trukatze grafoa:



3.1. irudia: Q_8 taldearen trukatze grafoa

(3.1.) irudiari erreparatuz, ikus dezakegu grafoaren maila 6 dela, erpin bakoitzaren maila 1 eta grafo ez konexua dela. Gainera, 3 osagai konexu ditu.

Ondoren 2. kapituluan, 2.1.2 Definizioan aurkeztutako kontzeptuarekin lotuta dauden definizio aldaera batzuk aztertuko ditugu:

Definizioa 3.2.2. Izan bedi G taldea eta $X \subseteq G$ ez-hutsa. G taldeko elementuek, X-ko elementuak finkatzeko probabilitatea ondoko eran definitzen da:

$$P_G(X) = \frac{|\{(x,g) \in X \times G \mid xg = gx, \forall g \in G \text{ eta } \forall x \in X\}|}{|X||G|}$$

Definizioa 3.2.3. Izan bitez G talde finitua eta S, $G \times G$-ko ondoko azpimultzoa: $S = \{(a,b) \in G \times G \mid ab = ba\}$. Izan bedi Ω, S-ren azpimultzoa, non G taldeak Ω-ren gainean konjokazioaren bidez eragiten duen. Definizioz, ausazko G-ko elementu batek Ω multzoa finkatzearekiko trukatze maila ondoko eran definitzen da:

$$P_G(\Omega) = \frac{|\{(g, w = (w_1, w_2)) \in G \times \Omega : g(w_1, w_2) = (w_1, w_2)g, \forall g \in G, \forall w \in \Omega\}|}{|\Omega||G|}$$

edo

$$P_G(\Omega) = \frac{|\{(g, w = (w_1, w_2)) \in G \times \Omega : (w_1, w_2)^g = (w_1, w_2), \forall g \in G, \forall w \in \Omega\}|}{|\Omega||G|}$$

edo modu laburrean

$$P_G(\Omega) = \frac{|\{(g,w) \in G \times \Omega : w^g = w, \forall g \in G, \forall w \in \Omega\}|}{|\Omega||G|}.$$

Teorema 3.2.1. Aurreko definizioaren baldintzetan, $P_G(\Omega) = \frac{k}{|\Omega|}$ betetzen da, $k = k_G$, Ω-n, G taldearen eraginpean dauden konjugazio klase kopurua izanik.

Froga. Lehenik, kontuan har dezagun 2. kapituluan, 2.3.1 Cauchy Frobeniusen leman erabilitako ondoko berdintza:

$$\sum\nolimits_{w \in \Omega} |\mathrm{Stab}_G(w)| = |G| \cdot k.$$

Orain, goiko $P_G(\Omega)$ definizioa erabiliz,

$$P_G(\Omega) = \frac{|\{(g,w) \in G \times \Omega : w^g = w, \forall g \in G, \forall w \in \Omega\}|}{|\Omega||G|} \text{ dugu.}$$

Bestetik,

$$\begin{aligned}|\{(g,w) \in G \times \Omega : w^g = w, \forall g \in G, \forall w \in \Omega\}| &= \sum\nolimits_{w\in\Omega} |\{g \in G : w^g = w\}| \\ &= \sum\nolimits_{w\in\Omega} |\mathrm{Stab}_G(w)| \\ &= |G| \cdot k.\end{aligned}$$

Beraz,

$$P_G(\Omega) = \frac{|G| \cdot k}{|\Omega| \cdot |G|} = \frac{k}{|\Omega|}.$$

□

Argi dago $P_G(\Omega) = 1$ dela baldin eta soilik baldin G taldea abeldarra bada.

Teorema 3.2.2. Izan bedi $G = D_{2n}$, $2n$ kardinaleko talde diedrikoa, n zenbaki bikoitia izanik. Kontsidera ditzagun:

$$S = \{\{a,b\}, G\text{-ko 2 tamainako azpimultzoak non } ab = ba \text{ den}\},$$

eta Ω, S-ren ondoko azpimultzoa:

$$\begin{aligned}\Omega &= \{\{a,b\} \in S \mid a \neq b \text{ eta } o(a) = o(b) = 2\} \\ &= \{\{a,b\} \subseteq G \mid ab = ba, a \neq b, o(a) = o(b) = 2\}.\end{aligned}$$

Orduan,

$$P_G(\Omega) = P_{D_{2n}}(\Omega) = \begin{cases} \frac{4}{|\Omega|}, & \frac{n}{2} \text{ bikoitia bada} \\ \frac{3}{|\Omega|}, & \frac{n}{2} \text{ bakoitia bada} \end{cases}$$

Froga. Lehenik eta behin, ohartu G taldeak Ω multzoaren gainean eragiten duela konjugazioaren bidez. Izan ere, baldin eta a, b, G-ko elementuak, elkar trukatzen badira, orduan edozein G-ko g elementurentzat, a^g eta b^g elementuak ere elkar trukatzen dira. Honez gain, $o(a) = o(a^g)$ da, edozein $a, g \in G$ elementuetarako.

Bestalde, $G = D_{2n} = \langle x, y \mid x^n = y^2 = 1, x^y = x^{-1}\rangle$-ren aurkezpena kontuan harturik, D_{2n}-ren elementuak errepikapenik gabe $\{x^i, yx^i \mid 0 \leq i \leq n-1\}$ dira. Hortik, 2 ordenako elementuen familia $\{x^{n/2}, yx^i \mid 0 \leq i \leq n-1\}$ da, eta bereziki $Z(D_{2n}) = \langle x^{\frac{n}{2}}\rangle = \{1, x^{\frac{n}{2}}\}$.

Beraz, Ω familiako azpimultzoak ondoko motakoak izan dira: n azpimultzo $\{x^{n/2}, yx^i\}$ motakoak, $i \in \{0, \ldots, n-1\}$ izanik, eta baita ere $\frac{n}{2}$ azpimultzo $\{yx^i, yx^{i+n/2}\}$ motakoak, $i \in \{0, \ldots, \frac{n}{2} - 1\}$ izanik. Ondorioz, $|\Omega| = \frac{3n}{2}$ da.

Azter dezagun orain zein den Ω-n, G taldearen eraginpean dauden k konjugazio klase kopurua. Has gaitezen, $\frac{n}{2}$ bikoitia den kasuarekin (n bikoitia izanik). Antzeko modu batean aztertuko litzateke $\frac{n}{2}$ bakoitia den kasua.

Oinarrizko kontak eginez, erraz froga daiteke konjugazio klase bat definitzen dela $\{x^{n/2}, yx^i\}$ motako azpimultzoetarako (i bikoitia izanik), konjugazio klase bat $\{x^{n/2}, yx^i\}$ motako azpimultzoetarako (i bakoitia izanik), konjugazio klase bat $\{yx^i, yx^{i+\frac{n}{2}}\}$ motako azpimultzoetarako (i bikoitia izanik), eta azkenik beste konjugazio klase bat $\{yx^i, yx^{i+\frac{n}{2}}\}$ motako azpimultzoetarako (i bakoitia izanik). Hau da, $k = 4$ da.

Bestalde, n bikoitia izanik, $\frac{n}{2}$ bakoitia den kasurako, arestian aipatutako k zenbakia $k = 3$ da. Izan ere, kasu horretan konjugazio klase bat definitzen da $\{x^{n/2}, yx^{i+\frac{n}{2}}\}$ motako azpimultzoetarako (i bikoitia izanik), konjugazio klase bat $\{x^{n/2}, yx^{i+\frac{n}{2}}\}$ motako azpimultzoetarako (i bakoitia izanik), eta konjugazio klase bakarra $\{yx^i, yx^{i+\frac{n}{2}}\}$ motako azpimultzoetarako. (A eranskineko 6 eta 7 Ariketetan, hurrenez hurren, baieztatzen dira emaitza hauek).

Beraz, 3.2.1 Teorema aplikatuz, $P_G(\Omega) = \frac{4}{|\Omega|}$ edo $P_G(\Omega) = \frac{3}{|\Omega|}$ da, $\frac{n}{2}$ bikoitia edo bakoitia izatearen arabera.

□

Bestalde, n zenbaki bakoitia balitz, orduan $Z(D_{2n}) = \{1\}$ da, eta halabeharrez,

$$\Omega = \{\{a, b\} \subseteq G \mid ab = ba, a \neq b, o(a) = o(b) = 2\} = \emptyset.$$

Definizioa 3.2.4. Izan bitez G talde finitu ez abeldarra eta Ω goian definitu den azpimultzo ez hutsa: $\Omega = \{\{a, b\} \subseteq G \mid ab = ba, a \neq b, o(a) = o(b) = 2\}$. Definizioz, G-ri elkartutako trukatze grafo orokortua deituko diogu, Γ_Ω^{GC} bidez adierazten den ondoko grafoari:

$$\text{Erpinen multzoa: } V(\Gamma_\Omega^{GC}) = \Omega - A,$$

$$A = \{w = \{a, b\} \in \Omega \mid w^g = w \text{ den, } \forall g \in G\} \text{ izanik.}$$

Gainera, $V(\Gamma_\Omega^{GC})$-ko $w_1 = \{a_1, b_1\}$ eta $w_2 = \{a_2, b_2\}$ erpinak *auzokideak* direla diogu, erpin horiek elkar trukatzen direnean, hau da, $w_1.w_2 = w_2.w_1$ denean, edo baliokideki $a_1a_2 = a_2a_1$ eta $b_1b_2 = b_2b_1$ betetzen denean.

Bereziki, G taldea abeldarra bada, Γ_Ω^{GC} grafo hutsa da, $G = Z(G)$ delako eta bereziki, $\Omega = A$ delako.

Ondoren, talde diedrikoaren trukatze grafo orokortua aztertuko dugu. Azterketa hori, grafo betearen kontzeptuarekin lotu daiteke. Hori dela eta, ondoko teorema aurkeztu baino lehen, gogora dezagun grafo betearen definizioa.

Hain zuzen ere, baldin eta (V, E) n mailako grafoa bada, n erpinetako *grafo betea* dela esango da, K_n bidez denotatuko dena, baldin eta grafoko edozein bi erpin, ertz baten bidez konektatuta badaude. Argi dago, K_n grafoak $\frac{n(n-1)}{2}$ ertz dituela.

Teorema 3.2.3. Izan bitez D_{2n}, $2n$ kardinaleko talde diedrikoa (n zenbaki bikoitia izanik), eta Ω goian definitu den multzoa. Orduan,

$$\Gamma_{\Omega}^{GC} = \bigcup_{i=1}^{\frac{n}{2}} K_3.$$

Froga. Alde batetik, 3.2.2 Teoremagatik, badakigu $|\Omega| = \frac{3n}{2}$ dela. Bestetik, erraz ikus daiteke $A = \{w = \{a, b\} \in \Omega \mid w^g = w, \forall g \in D_{2n}\} = \emptyset$ dela. Hau da, talde honen trukatze grafo orokortuaren erpinen kopurua:

$$|V(\Gamma_{\Omega}^{GC})| = |\Omega - A| = \frac{3n}{2} \text{ da.}$$

Orain, azter ditzagun trukatze grafo orokortu horren erpin auzokideak. Alde batetik, edozein $0 \leq j \leq n-1$ baliorako, $\{yx^j, yx^{j+\frac{n}{2}}\}$ eta $\{yx^j, x^{\frac{n}{2}}\}$ erpin auzokideak dira. Baita ere edozein $0 \leq j \leq n-1$ baliorako, auzokideak dira $\{yx^j, yx^{j+\frac{n}{2}}\}$ eta $\{yx^{j+\frac{n}{2}}, x^{\frac{n}{2}}\}$ erpinak.

Bestetik, $yx^j yx^{j+\frac{n}{2}} = yx^{j+\frac{n}{2}} yx^j$ betetzen denez, edozein $0 \leq j \leq n-1$ baliorako baita ere auzokideak dira $\{yx^{j+\frac{n}{2}}, x^{\frac{n}{2}}\}$ eta $\{yx^j, x^{\frac{n}{2}}\}$ erpinak.

Beraz, 3-naka elkar auzokideak diren erpinen $\frac{n}{2}$ tamainako segida bat aurkitzen da, bakoitza trukatze grafo orokortuaren osagai konexu bat izanik, K_3 motatakoa. (Izan ere, demagun osagai konexuen kopurua $\frac{n}{2}$ baino handiagoa dela. Orduan, gutxienez $\frac{n}{2}$ erpin ez lirateke beste erpinekin trukatuko, eta hau absurdoa da.)

Beraz, guztira $\frac{3n}{2}$ erpin daude eta $\frac{n}{2}$ osagai konexu, K_3 motatakoak. Ondorioz,

$$\Gamma_{\Omega}^{GC} = \bigcup_{i=1}^{\frac{n}{2}} K_3,$$

frogatu nahi genuen moduan. □

Adibidea 3.2.2. Izan bedi $D_{16} = D_{2.8}$, 16 kardinaleko talde diedrikoa, ondoko aurkezpenaren bidez emandakoa: $\langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle$. Aurreko 3.2.3 Teorema aplikatuz, $n = 8$ denez, $\Gamma_{\Omega}^{GC} = \bigcup_{i=1}^{4} K_3$ dugu.

Lehenik, D_{16}-ren trukatze grafo orokortua irudikatzeko bertako erpin auzokideak zehaztu behar ditugu.

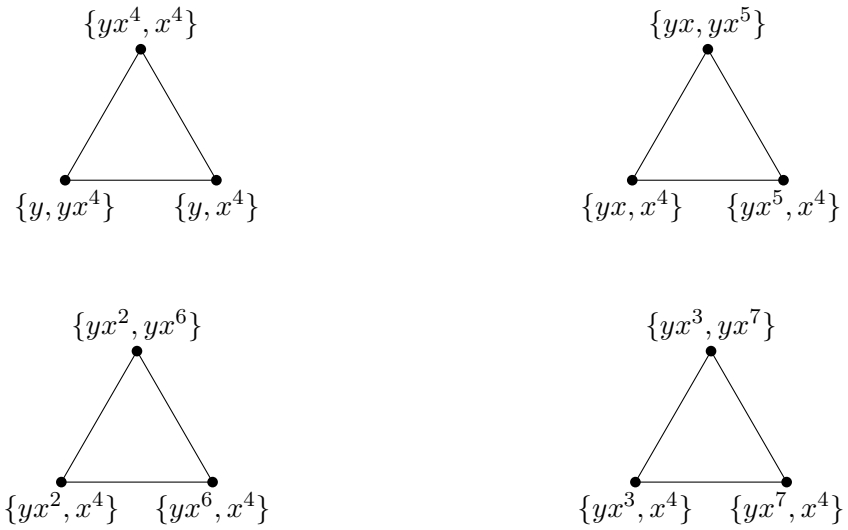
Ω multzoan $12 = \frac{3.8}{2}$ elementu daude: 8 elementu $\{yx^j, x^4\}$ motakoak eta 4 elementu $\{yx^j, yx^{j+4}\}$ motakoak ($0 \leq j \leq 7$-rako, nahikoa da $0 \leq j \leq 4-1 = 3$ hartzea); hots, $\{y, yx^4\}$, $\{yx, yx^5\}$, $\{yx^2, yx^6\}$ eta $\{yx^3, yx^7\}$ elementuak.

Hau da,

$$\Omega = \{\{yx^7, x^4\}, \{yx^6, x^4\}, \{yx^5, x^4\}, \{yx^4, x^4\}, \{yx^3, x^4\}, \{yx^2, x^4\}, \{yx, x^4\}, \{y, x^4\}, \{yx^3, yx^7\}, \{yx^2, yx^6\}, \{yx, yx^5\}, \{y, yx^4\}\}.$$

Orain 3.2.3 Teorema aplikatuz, $\frac{n}{2} = \frac{8}{2} = 4$ osagai konexu daude.

Hemen argi ikusten da, $\{y, x^4\}, \{yx^4, x^4\}, \{y, yx^4\}$ erpinek osagai konexu bat osatzen dutela; modu berdinean $\{yx, x^4\}, \{yx^5, x^4\}, \{yx, yx^5\}$ erpinek beste osagai konexu bat, $\{yx^2, x^4\}, \{yx^6, x^4\}, \{yx^2, yx^6\}$ erpinek hirugarrena, eta azkenik, $\{yx^3, x^4\}, \{yx^7, x^4\}, \{yx^3, yx^7\}$ erpinek laugarren osagai konexua osatzen dute.



3.2. irudia: D_{16} taldearen trukatze grafo orokortua

Behin talde diedrikoaren trukatze grafo orokortua aztertu dugula, talde semidiedrikoaren trukatze grafo orokortuaren propietate nagusiak aipatuko ditugu. Talde semidiedrikoak 2^n kardinala eta 2 indizeko azpitalde zikliko bat duten talde ez abeldarrak dira. Beraz, 2^n kardinaleko talde semidiedrikoa, ondoko aurkepenaren bidez eman daiteke ($n \geq 3$ izanik):

$$SD_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, x^y = x^{2^{n-2}-1} \rangle.$$

Teorema 3.2.4. [5] Izan bedi SD_{2n}, 2^n kardinaleko talde semidiedrikoa, $n \geq 3$ izanik. Har dezagun arestian definitutako Ω azpimultzo ez hutsa, zeinetan G-k eragiten duen konjokazioaren bidez. Orduan, $|\Omega| = 3.2^{n-3}$ da.

Hain zuzen ere, badaude $2^{n-2} = 2.2^{n-3}$ elementu $\{x^{2^{n-2}}, yx^i\}$ motakoak ($0 \leq i \leq 2^{n-1}$ izanik, i zenbaki bikoitia den kasurako), eta 2^{n-3} elementu $\{yx^i, yx^{i+2^{n-2}}\}$ motakoak ($0 \leq i \leq 2^{n-1}$ izanik, i zenbaki bikoitia den kasurako).

Lan honetan ez dugu teorema honen froga garatuko. Izan ere, kalkulu guztiak zehatz mehatz garatuz froga nahiko erraz egiaztatuko litzateke, 3.2.2 Teoreman egin den modura.

Teorema 3.2.5. [5] (Teorema 5). Izan bitez SD_{2^n}, 2^n kardinaleko talde semidiedrikoa, $n \geq 3$ izanik, eta arestian definitutako Ω azpimultzo ez hutsa. Orduan,

$$\Gamma_\Omega^{GC} = \bigcup_{i=1}^{2^{n-3}} K_3 \text{ da.}$$

Froga. Alde batetik, goiko 3.2.4 Teoremagatik badakigu $|\Omega| = 3.2^{n-3}$ dela. Bestetik, erraz ikus daiteke $A = \{w = \{a, b\} \in \Omega \mid w^g = w, \forall g \in SD_{2n}\} = \emptyset$ dela. Hau da, talde horren trukatze grafo orokortuaren erpinen multzoaren kardinala,

$$|V(\Gamma_\Omega^{GC})| = |\Omega - A| = |\Omega| = 3.2^{n-3} \text{ da.}$$

Orain, azter ditzagun trukatze grafo orokortuaren erpin auzokideak. Alde batetik, edozein $0 \leq i \leq 2^{n-1}$ zenbaki bikoitirako $\{yx^i, yx^{i+2^{n-2}}\}$ eta $\{yx^i, x^{2^{n-2}}\}$, baita ere $0 \leq i \leq 2^{n-1}$ balio bikoitirako, erpin auzokideak dira. Modu berdinean, edozein $0 \leq i \leq 2^{n-1}$ balio bikoitirako auzokideak dira $\{yx^i, yx^{i+2^{n-2}}\}$ eta $\{yx^{i+2^{n-2}}, x^{2^{n-2}}\}$ erpinak.

Bestetik, $yx^i yx^{i+2^{n-2}} = yx^{i+2^{n-2}} yx^i$ betetzen denez, edozein $0 \leq i \leq 2^{n-1}$ balio bikoitirako baita ere auzokideak dira $\{yx^i, x^{2^{n-2}}\}$ eta $\{yx^{i+2^{n-2}}, x^{2^{n-2}}\}$ erpinak.

Ondorioz, 3-naka auzokideak diren eta elkarrekiko disjuntuak diren erpinen multzoen segida bat lortzen da, horietariko bakoitzak K_3 azpigrafoa osatzen duelarik. Azkenik, $|V(\Gamma_\Omega^{GC})| = 3.2^{n-3}$ denez, K_3 motako 2^{n-3} osagai konexu dituen grafoa dugu.

Beraz,

$$\Gamma_\Omega^{GC} = \bigcup_{i=1}^{2^{n-3}} K_3,$$

frogatu nahi genuen moduan. □

Adibidea 3.2.3. Izan bedi SD_{2^4}, 16 kardinaleko talde semidiedrikoa, ondoko aurkezpenaren bidez emanda dagoena:

$$SD_{2^4} = \langle x, y \mid x^{2^3} = x^8 = y^2 = 1, x^y = x^{2^2-1} = x^3 \rangle.$$

3.2.5 Teorema aplikatuz, $n = 4$ denez, $\Gamma_\Omega^{GC} = \bigcup_{i=1}^{2^{4-3}} K_3 = \bigcup_{i=1}^{2} K_3$ dugu.

Gainera, 3.2.5 Teorema beraren arabera, Ω multzoan $6 = 3.2^{4-3}$ elementu daude, eta $|V(\Gamma_\Omega^{GC})| = |\Omega - A| = |\Omega| = 3.2^{4-3}$. Bestalde, SD_{2^4} taldearen trukatze grafo orokortuaren erpinak ondokoak dira:

$$\{yx^6, yx^2\}, \{yx^4, y\}, \{yx^6, x^4\}, \{yx^4, x^4\}, \{yx^2, x^4\}, \{y, x^4\}.$$

Honez gain, $2^{4-3} = 2$ osagai konexu daude; $\{yx^6, yx^2\}, \{yx^2, x^4\}, \{yx^6, x^4\}$ erpinek osagai konexu bat osatzen dute, eta $\{yx^4, y\}, \{yx^4, x^4\}, \{y, x^4\}$ erpinek beste osagai konexu bat.

3.3. irudia: SD_{16} taldearen trukatze grafo orokortua

3.3 Neumannen emaitza

Atal honetan lana bukatzeko, aztertu ditudan artikuluetatik bereziki interesgarria eta frogatzeko ez hain erreza iruditu zaidan emaitza aurkezten dut.

Demagun G taldeko trukatzen diren elementuen proportzioa α bidez denotatzen dela. Baldin eta $\alpha = 1$ bada, nabaria da G taldea abeldarra dela. Ildo honetan interesa dago jakiteko zer esan daitekeen G talde finitu bati buruz, dagokion grafoek behintzat α proportzio ertz posible onartzen dituenean.

Bereziki, 1988an, Peter M. Neumann-ek [12] lanean ondoko emaitza plazaratu zuen:

Emanda G talde finitua, edozein $\alpha > 0$ izanik, baldin eta G-ri elkartutako grafoak gutxienez $\alpha\frac{1}{2}|G|(|G|+1)$ ertz onartzen baditu, orduan beti existitzen dira $\beta > 0$ eta G taldearen G_0 sekzio abeldarra zeinentzat $|G_0| \geq \beta|G|$ betetzen den.

Orain goian aipaturiko emaitzaren baliokide den teorema aurkeztuko da.

Teorema 3.3.1. Izan bedi G talde finitua non $|L(G)| \geq \frac{|G|^2}{a}$ den, $a \geq 1$ zenbaki erreala izanik. Orduan, existitzen dira n_1 eta n_2 zenbaki errealak eta $H, K \trianglelefteq G$ non $K \leq H$, H/K talde abeldarra eta $|G : H| \leq n_1$ eta $|K| \leq n_2$ diren.

Froga. Defini dezagun $X = \{x \in G \mid |\operatorname{Cl}_G(x)| \leq a^2\}$ multzoa. Hipotesiz eta 2.3.2 Lema aplikatuz, badakigu $\frac{|G|^2}{a} \leq |L(G)| = \sum_{x\in G} |C_G(x)|$ betetzen dela. Beraz, ondorengo bornaketa dugu:

$$\frac{|G|^2}{a} \leq \sum_{x\in X} |C_G(x)| + \sum_{x\in G-X} |C_G(x)| \leq |X||G| + (|G| - |X|)\frac{|G|}{a^2}. \quad (3.1)$$

(Izan ere, baldin eta $x \in G - X$ bada, orduan $|\operatorname{Cl}_G(x)| > a^2$ da, eta orbita estabilizatzailearen erlazioa aplikatuz, $|\operatorname{C}_G(x)| = \frac{|G|}{|\operatorname{Cl}_G(x)|} < \frac{|G|}{a^2}$ lortzen dugu.) Beraz, aurreko (3.1) desberdintza berridatziz ondokoa dugu:

$$\frac{|G|^2}{a} \leq |X||G| + (|G| - |X|)\frac{|G|}{a^2} \iff |G|^2 a \leq |X||G|a^2 + (|G| - |X|)|G|$$
$$\iff |G|a \leq |X|a^2 + (|G| - |X|) \iff |G|(a-1) \leq (a^2-1)|X|.$$

Bereziki, $a = 1$ bada, G taldea, abeldarra izango litzateke, eta teoremaren emaitzak berehalakoak lirateke. Halabeharrez, demagun $a > 1$ dela. Orduan, goiko adierazpena $(a-1)$ balioagatik sinplifikatuz ondokoa dugu:

$$|G| \leq |X|(a+1), \text{ edo baliokideki, } \frac{|G|}{a+1} \leq |X|. \quad (3.2)$$

Har ditzagun G-ren $H = \langle X \rangle$ eta $K = [H, H] = H'$ azpitaldeak. Teoremaren baieztapena burutzeko nahikoa da frogatzea ondorengo baldintzak betetzen direla:

(i) $H, K \trianglelefteq G$

(ii) $K \leq H$

(iii) H/K abeldarra

(iv) existitzen direla n_1, n_2 zenbaki errealak zeinentzat $|G : H| \leq n_1$ eta $|K| \leq n_2$ diren

Has gaitezen (i) atala frogatzen. Lehenik eta behin, erraz ikus daiteke, X-ren definizioagatik $H = \langle X \rangle \trianglelefteq G$ dela. Bestalde, 1.2.1. Korolarioaren ondorioz, $H \trianglelefteq G$ denez, $K = [H, H]$ ere G-ren azpitalde normala dela ondorioztatzen da.

Bestetik, (ii) eta (iii) baldintzak ere berehalakoak dira, kommutadorearen propietateen eta K-ren definizioagatik, $K = [H, H] \leq H$ eta $H' = [H, H] = K \leq K$ direlako, eta ondorioz, $(H/K)' = H'K/K = H'/K = K/K = \overline{1}$ delako (hau da, H/K abeldarra ere delako).

Froga dezagun orain (iv) propietatea. Alde batetik, $X \subseteq H$ denez, eta (3.2) adierazpena erabiliz berehalakoa da: $|G : H| = \frac{|G|}{|H|} \leq \frac{|G|}{|X|} \leq a + 1$. Beraz, n_1 zenbaki erreal gisa $a + 1$ balioa proposatzen da. Jarraian n_2 balio erreala lortuko dugu $|K|$ modu egoki batean bornatuz.

Har ditzagun $k_0, k_1, \ldots, k_n$, H barne dauden elementuen G-konjugazio klaseen kardinal desberdinek, $1 = k_0 < k_1 < \ldots < k_n$ (*) izanik (kardinal horiek segida gorakorrean berrordenatuta). Defini dezagun edozein $i \in \{0, 1, \ldots, n\}$ baliorako $X_i = \{x \in H \mid |\operatorname{Cl}_G(x)| \leq k_i\}$ multzoak. Ohar gaitezen $i < n$ bada $X_i \neq H$ dela, $H = \langle X_n \rangle$ izanik. Izan ere, baldin eta $i < n$ bada, $X_i \neq X_n$ dugu, existitzen delako behintzat X_n-ko $x \in H$ elementuren bat zeinentzat $|\operatorname{Cl}_G(x)| = k_n \not\leq k_i$ den, eta ondorioz $x \notin X_i$. Halabeharrez, $X_i X \not\subseteq X_i$ dugu. Beraz, existitzen dira behintzat $h \in X_i$ eta $x \in X$ non $|\operatorname{Cl}_G(hx)| > k_i$ den, eta bereziki non $|\operatorname{Cl}_G(hx)| \geq k_{i+1}$ den.

Gainera, multzo bezala ikusita, $\operatorname{Cl}_G(hx) \subseteq \operatorname{Cl}_G(h) \operatorname{Cl}_G(x)$ partekotasuna betetzen da ($h, x \in G$ izanik). Beraz, multzo bakoitzaren kardinalak hartuta, $|\operatorname{Cl}_G(hx)| \leq |\operatorname{Cl}_G(h) \operatorname{Cl}_G(x)| = \frac{|\operatorname{Cl}_G(h)||\operatorname{Cl}_G(x)|}{|\operatorname{Cl}_G(h) \cap \operatorname{Cl}_G(x)|} \leq |\operatorname{Cl}_G(h)||\operatorname{Cl}_G(x)|$ desberdintza dugu. Orain kontuan izanik $x \in X$ eta $h \in X_i$ direla (eta bereziki multzo horien definizioak), ondorengo bornaketa dugu:

$$|\operatorname{Cl}_G(hx)| \leq |\operatorname{Cl}_G(h)||\operatorname{Cl}_G(x)| \leq |\operatorname{Cl}_G(h)| a^2 \leq a^2 k_i.$$

Beraz, $i < n$ bada, $k_{i+1} \leq a^2 k_i$ dugu.

Ondoren eraiki dezagun goiko (*) $1 = k_0 < k_1 < \ldots < k_n$ segidaren azpisegida bat ondoko eran: finka dezagun $i_0 = 0$ eta posible denean, edozein $j \geq 0$ baliorako izan bedi i_{j+1} indizerik txikiena zeintzentzat $k_{i_{j+1}} > a^4 k_{i_j}$ desberdintza betetzen den. Argi dago, honela eraikitako azpisegidarentzat $i_j < i_{j+1}$ betetzen dela. Beraz, $1 = k_0 = k_{i_0} < k_{i_1} < \ldots < k_{i_m}$.

Lehenik, azpisegidaren definizioagatik argi dago $k_{i_{j+1}-1} \leq a^4 k_{i_j}$ betetzen dela. Bestetik, hasierako (*) segidaren ezaugarriegatik, $k_{i_{j+1}} \leq a^2 k_{i_{j+1}-1}$ desberdintza ere dugu. Ondorioz, $k_{i_{j+1}} \leq a^6 k_{i_j}$ betetzen da. Azkenik, i_m indizeari lotuta, goiko desberdintza m aldiz aplikatzen badugu, $k_{i_m} \leq a^{6m}$ dugu. Are gehiago, $k_n \leq a^4 k_{i_m} \leq a^{6m+4}$.

Har dezagun orain $x_j \in H$ non $|\operatorname{Cl}_G(x_j)| = k_{i_j}$ den, eta kontsidera dezagun $Y_j = x_j X$ multzoa. Baldin eta y, Y_j-ko elementua bada, orduan $y = x_j x$

modukoa da, $x \in X$ izanik, eta baliokideki, $x_j = yx^{-1}$ da. Orain kontuan harturik $|\mathrm{Cl}_G(x_j x)| \leq |\mathrm{Cl}_G(x_j)||\mathrm{Cl}_G(x)|$ eta $|\mathrm{Cl}_G(x)| = |\mathrm{Cl}_G(x^{-1})|$ direla, ondoko desberdintzak betetzen dira:

$$\frac{|\mathrm{Cl}_G(x_j)|}{|\mathrm{Cl}_G(x)|} \leq |\mathrm{Cl}_G(y = x_j x)| \leq |\mathrm{Cl}_G(x_j)||\mathrm{Cl}_G(x)|.$$

Beraz, $\frac{k_{i_j}}{a^2} \leq \frac{k_{i_j}}{|\mathrm{Cl}_G(x)|} \leq |\mathrm{Cl}_G(y)| \leq a^2 k_{i_j}$ dugu.

Ondoren, baldin eta $j \neq j'$ bada $Y_j \cap Y_{j'} = \emptyset$ dela froga daiteke (hemen ez da froga zuzenean garatzen, baina kalkuluak egiterakoan kontutan hartu behar da, $k_{i_{j+1}} > a^4 k_{i_j}$ baldintza betez aukeratu izan direla Y_j eta $Y_{j'}$ multzoak).

Ondorioz, $|H| \geq |X| \cdot (m+1)$ desberdintza dugu. Azkenik, (3.2) ekuazioa erabiliz, $|H| \leq |G| \leq |X| \cdot (a+1)$ dugu, eta hemendik $m \leq a$ ondorioztatzen da. Beraz, $k_n \leq a^{6m+4} \leq a^{6a+4}$ lortzen dugu.

Gure kasuan G taldea finitua izateagatik, bereziki G taldea BFC motatakoa da, hau da, G taldearen konjugazio klaseen kardinalak finituki bornatuta daude borne komun batergatik, eta bereziki, G-ren H azpitaldearen konjugazio klaseen kardinalak ere bornatuta daude borne komun batergatik. Gainera, H taldearekiko, $H' = [H, H] = K$ azpitalde kommutadorearen kardinala, H-ko konjugazio klase handienaren arabera bornatuta dago. Beraz, nahikoa da n_2 gisa, aipatutako borne hori aukeratzea, $|K| \leq n_2$ dela ondorioztatzeko, eta honela froga bukatzeko.

□

Goiko 3.3.1 Teoremari lotuta, n_1 eta n_2 zenbakiak errealak izanik, baldin eta G talde finitua bada zeinentzat existitzen diren $H, K \trianglelefteq G$ non $K \leq H$, H/K zatidura taldea abeldarra, $|G : H| \leq n_1$ eta $|K| \leq n_2$ diren, orduan nahikoa da $a = n_1^2 n_2 > 1$ zenbakia hartzea teoremaren baieztapena betetzen dela egiaztatzeko.

Hau da, har dezagun edozein $x \in H$. Orduan, H/K talde abeldarra denez, $\mathrm{Cl}_H(x) = \{h^{-1}xh \mid h \in H\}$ multzoa K-ren koklase bakar batean dago. Gainera, orbita estabilizatzailearen erlazioagatik, $|\mathrm{Cl}_H(x)| = |H : \mathrm{C}_H(x)|$ da. Bestetik, $|\mathrm{Cl}_H(x)| \leq |K| \leq n_2$ denez, $|C_G(x)| \geq |C_H(x)| = \frac{|H|}{|\mathrm{Cl}_H(x)|} \geq \frac{|H|}{n_2}$.

Hemendik, 2.3.2 Lema erabiliz eta kontuan harturik $|G : H| \leq n_1$ edo baliokideki $|H|/|G| \geq 1/n_1$ dela,

$$|L(G)| = \sum_{x \in G} |C_G(x)| \geq \sum_{x \in H} |C_H(x)| \geq |H| \cdot \frac{|H|}{n_2} \geq \frac{|G|^2}{n_1^2 n_2}.$$

A. eranskina

Ariketak

A.1 Talde teoriako oinarrizko ariketak

Ondorengo emaitzak talde teoriako emaitza klasikoak dira, eta ariketa modura planteatzen ditugu, laneko emaitza askoren frogetan maiz erabiltzen direlako.

Ariketa 1. Izan bedi G talde finitua, ordena p zenbaki lehena izanik. Orduan, G talde ziklikoa da.

Ebazpena. Har dezagun G-ko edozein g elementu ez tribiala eta kontsidera dezagun g-k sortutako azpitaldea, hau da, $\langle g \rangle \leq G$. Lagrangeren teorema erabiliz, talde finitu baten edozein azpitalderen kardinalak G-ren kardinala zatitu behar du. Alabaina, $|G| = p$ denez eta $|\langle g \rangle|$ ezin daitekeenez 1 izan, hemendik $|\langle g \rangle| = p$ dela ondorioztatzen da. Beraz, $|\langle g \rangle| = p = |G|$, eta ondorioz, $\langle g \rangle = G$. Hau da, G talde ziklikoa da. □

Ariketa 2. Izan bedi G talde ez abeldar finitua eta demagun G-k 2 indizeko H azpitalde abeldarra duela. (2.4.3 Proposizioan frogatuta dago $Z(G) < H$ dela). Denotatuz $|H : Z(G)| = n$ bidez, baldin eta $y \in G \setminus H$ bada, orduan y elementuak n konjugazio klase ezberdin ditu.

Ebazpena. Denota ditzagun $m = |\mathrm{Z}(G)|$ eta $n = |H : \mathrm{Z}(G)|$. 2.4.3 Proposizioan ikusi den modura, $|G| = 2nm$ da, H, G-ren azpitalde normala da, eta G-ko edozein elementu $g = hx^i$ moduan idatz daiteke, $x \in G \setminus H$ finko batentzako, $h \in H$-ko izanik, eta $i \in \{0, 1\}$.

Har dezagun edozein $y \in G \setminus H$ eta froga dezagun $|\mathrm{C}_G(y)| = 2m$ dela. Nola $y \notin H$, $y = h_0 x$ modura idatz daiteke. Demagun orain y elementua, $h \in H$ elementu batekin trukatzen dela. Orduan, $x^{-1}{h_0}^{-1}hh_0x = h$ dugu. Baina ${h_0}^{-1}hh_0 = h$ dugu (H abeldarra delako), eta halabeharrez, $x^{-1}hx = h$ da. Aurreko berdintza hori ematen da, $h \in \mathrm{C}_H(x) = \mathrm{Z}(G)$ bada. Ondorioz, $|\mathrm{C}_G(y) \cap H| = |\mathrm{Z}(G)| = m$ dugu.

Demagun orain y elementua $g = hx$ elementuarekin trukatzen dela, $h \in H$ izanik. 1.2.1 Teoremaren (i) atala erabiliz, $[g = hx, y = h_0x] = 1$ dugu. Gainera, $[hx, h_0x] = x^{-1}wx$ dugu, $w = h^{-1}x^{-1}{h_0}^{-1}hxh_0$ izanik, eta halabeharrez, $w = 1$ dugu.

Orain, H G-ren azpitalde normala denez, $c = x^{-1}{h_0}^{-1}hx = ({h_0}^{-1}h)^x \in H$ dugu, eta $1 = w = h^{-1}ch_0 = h^{-1}h_0c = [d, x] = 1$ ondorioztatzen da, $d = h_0^{-1}h \in H$ izanik. Beraz, y elementua, $g = hx$ elementuarekin trukatzen da baldin eta soilik baldin $h_0^{-1}h \in Z(G)$ bada. Ondorioz, $g = hx \in G \setminus H$ motako $|Z(G)| = m$ elementu daude y elementuarekin trukatzen direnak.

Azkenik, $|\mathrm{C}_G(y) \cap H| = |\mathrm{Z}(G)| = m$ ere betetzen denez, $|C_G(y)| = 2m$ dela ondorioztatzen da, eta hemendik $|\,\mathrm{Cl}_G(y)| = |G : C_G(y)| = \frac{2nm}{2m} = n$, nahi genuena frogatu. □

Lehenengo kapituluan, talde nilpotenteak eta serie zentral beherakorra definitzen dira, hauetan gehiegi sakondu gabe. Ondorengo ariketan talde baten serie zentral beherakorra kalkulatzen da, definizioa praktikan jartzeko.

Ariketa 3. Izan bedi A identitatedun eraztun trukakorra. A eraztunaren gaineko Heisenbergen taldea, $H_3(A)$-ren bidez denotatuko duguna, 3×3 tamainako goi matrize triangeluarren taldea da, hau da,

$$H_3(A) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in A \right\},$$

eragiketa matrizeen biderketa izanik. Baldin eta $A = \mathbb{Z}$ bada, $H_3(\mathbb{Z})$ taldeari *Heisenbergen talde diskretua* deritzogu eta ondorengo 3 elementuek sortzen dute $H_3(\mathbb{Z})$ taldea:

$$X = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$H_3(\mathbb{Z})$ taldeko matrize sortzaile horiek, ondorengo trukatze erlazioak betetzen dituzte:

$$XY = YXZ, \quad XZ = ZX, \quad YZ = ZY$$

eta bereziki,

$$XYX^{-1}Y^{-1} = Z.$$

Gainera, $H_3(\mathbb{Z})$ taldearen zentrua ondorengo moduan adieraz daiteke:

$$Z(H_3(\mathbb{Z})) = \langle Z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : c \in \mathbb{Z} \right\}.$$

Ariketa honen helburua Heisenbergen talde diskretua 2 nilpotentzia klaseko talde nilpotentea (noski, ez abeldarra) dela ikustea da.

Ebazpena. $H_3(\mathbb{Z})$ taldearen serie zentral beherakorra eraikiko dugu 1.1.4 Definizioa jarraituz. Horretarako, matrize sortzaileen arteko kommutadoreak kalkulatuko ditugu. Has gaitezen X, Y eta Z matrizeen alderantzizkoak lortzen.

$$X^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Y^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad Z^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ondoren, haien arteko kommutadoreak kalkulatuko ditugu. Kalkulu hauek Wolfram Mathematica programaren bidez egin dira. Atal honetan, kommutadorea izeneko funtzio bat programatu da, A eta B matrizeak jasota, bi matrize horien arteko kommutadorea kalkulatzen duena.

```
kommutadorea[A_, B_] := Inverse[A].Inverse[B].A.B
X = {{1, 1, 0}, {0, 1, 0}, {0, 0, 1}};
Y = {{1, 0, 0}, {0, 1, 1}, {0, 0, 1}};
Z = {{1, 0, 1}, {0, 1, 0}, {0, 0, 1}};
kommutadorea[X,Y]
{{1, 0, 1}, {0, 1, 0}, {0, 0, 1}}
kommutadorea[X,Z]
{{1, 0, 0}, {0, 1, 0}, {0, 0, 1}}
kommutadorea[Y,Z]
{{1, 0, 0}, {0, 1, 0}, {0, 0, 1}}
```

Kommutadore funtzioa Heisenbergen taldearen sortzaileetara aplikatuz, ondorengo emaitzak lortzen dira.

$$[X, Y] = X^{-1}Y^{-1}XY = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = Z$$

$$[X, Z] = X^{-1}Z^{-1}XZ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$[Y, Z] = Y^{-1}Z^{-1}YZ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Halabeharrez, $\gamma_2(H_3(\mathbb{Z})) = [H_3(\mathbb{Z}), H_3(\mathbb{Z})] = \langle Z \rangle$ betetzen da, eta gainera $\gamma_3(H_3(\mathbb{Z})) = [H_3(\mathbb{Z}), \gamma_2(H_3(\mathbb{Z}))] = 1$ dugu, $[X, Z] = [Y, Z] = [Z, Z] = 1$ direlako.

Orain eraiki dezagun $H_3(\mathbb{Z})$ taldearen serie zentral beherakorra:

$$\gamma_1(H_3(\mathbb{Z})) = H_3(\mathbb{Z}) \geq \gamma_2(H_3(\mathbb{Z})) = Z(H_3(\mathbb{Z})) = \langle Z \rangle \geq \gamma_3(H_3(\mathbb{Z})) = 1.$$

Nola $\gamma_3(H_3(\mathbb{Z})) = 1$ eta $\gamma_2(H_3(\mathbb{Z})) \neq 1$ diren, frogatuta geratzen da Heisenbergen talde diskretua 2 klaseko talde nilpotentea dela. □

A.2 Talde berezi batzuen trukatze probabilitatea

Atal honetan edozein kardinaleko talde diedrikoaren eta talde simetrikoaren trukatze probabilitateak ariketa modura planteatu eta kalkulatuko ditugu. Kasu bakoitzean talde horien inguruko propietate esanguratsuenak ere aztertuko ditugu.

A.2.1 Talde diedrikoa

Izan bedi $n \in \mathbb{N}$, $n \geq 3$ izanik. $2n$ kardinaleko talde diedrikoa, D_{2n}-ren bidez denotatuko duguna, n alde dituen poligono erregular baten simetrien taldea da. Taldeko eragiketa konposaketa da, eta bertan bi motako elementu ezberdintzen ditugu:

- $\frac{2\pi i}{n}$ angeluko biraketak, edozein $i \in \{0, 1, 2, \ldots, n-1\}$ -rako
- erreflexioak

Bestalde, D_{2n}-ren ondorengo aurkezpena eman daiteke:

$$D_{2n} = \langle x, y \mid x^n = y^2 = 1, x^y = x^{-1} \rangle.$$

Talde diedrikoko elementuak errepikapenik gabe, ondoko adierazpenen bidez eman daitezke:

$$D_{2n} = \{y^i x^j \mid 0 \leq i \leq 1, \quad 0 \leq j \leq n-1\}.$$

Ariketa 4. Izan bedi D_{2n}, $2n$ kardinaleko talde diedrikoa, $n \geq 3$ izanik. Orduan,

$$cp(D_{2n}) = \begin{cases} \frac{n+3}{4n}, & \text{n bakoitia bada} \\ \frac{n+6}{4n}, & \text{n bikoitia bada} \end{cases}$$

Ebazpena. Lehendabizi, demagun n zenbaki arrunta bakoitia dela eta kalkula dezagun D_{2n}-ko edozein $y^i x^j$ motako elementuaren zentralizatzailearen kardinala.

Hasteko, nabaria da $C_{D_{2n}}(1) = \{g \in D_{2n} : 1^g = 1\} = D_{2n}$ dela. Jarraian, kalkula dezagun $C_{D_{2n}}(x^k) = \{g \in D_{2n} : (x^k)^g = x^k\}$, edozein $1 \leq k \leq n-1$ baliorako. Nola x^j eta x^k elementuak elkar trukatzen diren, x-ren berreketak izateagatik, orduan edozein $j \in \{0, 1, \ldots, n-1\}$ baliorako, $x^j \in C_{D_{2n}}(x^k)$. Halabeharrez, $\langle x \rangle \subseteq C_{D_{2n}}(x^k)$. Bestalde, nabaria da $C_{D_{2n}}(x^k) = C_{D_{2n}}\langle x^k \rangle$ dela.

Froga dezagun orain edozein $k \in \{1, \ldots, n-1\}$ baliorako $C_{D_{2n}}\langle x^k \rangle = \langle x \rangle$ betetzen dela. Izan ere, alde batetik, talde diedrikoaren propietateei erreparatuz, jakina da $o(x) = n$ dela, eta $|D_{2n}| = 2n$ denez, $|D_{2n} : \langle x \rangle| = 2$ dugu. Orain, indizeen propietate biderkakorra erabiliz eta kontuan harturik $\langle x \rangle \leq C_{D_{2n}}\langle x^k \rangle$ dela, printzipioz bi aukera posible daude: $C_{D_{2n}}\langle x^k \rangle = \langle x \rangle$ edo $C_{D_{2n}}\langle x^k \rangle = \langle x, y \rangle = D_{2n}$ izatea. Ikus dezagun orain bigarren aukera ez dela posible.

$$\begin{array}{c} D_{2n} = \langle x, y \rangle \\ | \\ C_{D_{2n}}\langle x^k \rangle \\ | \\ \langle x \rangle \end{array}$$

Absurdora eramanez, baldin eta $C_{D_{2n}}\langle x^k \rangle = D_{2n}$ balitz, horrek esan nahi du $y \in C_{D_{2n}}(x^k)$ dela, edo baliokidea dena, y eta x^k elkar trukatuko liratekeela, hau da, $(x^k)^y = x^k$ beteko litzatekeela. Bestalde, kontuan izanda berreketa eta konjugazioa elkar trukatzen direla, eta kontuan izanik zein den D_{2n} taldearen aurkezpena, ondorengo garapena lortzen da:

$$x^k = (x^k)^y = (x^y)^k = (x^{-1})^k.$$

Ondorioz, $x^k = x^{-k}$ izango genuke, eta hemendik x^{-k} elementuaren alderantzizkoagatik biderkatuz, $x^{2k} = 1$ lortuko genuke. Orain, ordenaren propietateak kontuan izanda, $n = o(x) \mid 2k$ dugu. Bestalde, n zenbaki bakoitia denez, hau da, $(n, 2) = 1$ denez, $n \mid k$ ondorioztatzen da, $k \in \{1, 2, \ldots, n-1\}$ izanik, eta hau ezinezkoa da. Beraz, absurdo batera iritsi gara eta ondorioz $y \notin C_{D_{2n}}\langle x^k \rangle$. Hemendik, $C_{D_{2n}}\langle x^k \rangle = \langle x \rangle$ berdintza ondorioztatzen da, edozein $k \in \{1, 2, \ldots, n-1\}$ baliorako.

Ondoren, ikus dezagun $\langle y \rangle = C_{D_{2n}}(y) = C_{D_{2n}}\langle y \rangle$ betetzen dela. Alde batetik, nabaria da $\langle y \rangle \leq C_{D_{2n}}\langle y \rangle$, eta bestetik ikusiko dugu ez dagoela D_{2n} taldean, y-rekin trukatzen duten elementu ez tribial gehiagorik. Aurretik ikusi dugun moduan, $k \in \{1, 2, \ldots, n-1\}$ izanik, x^k elementuek ez dira y-rekin trukatzen. Halabeharrez, $x^k \notin C_{D_{2n}}\langle y \rangle$. Ikus dezagun orain yx^k motako elementuek ere ez daudela $C_{D_{2n}}\langle y \rangle$ taldean. Bestalde, baldin eta $yx^k \in C_{D_{2n}}\langle y \rangle$ balego, orduan $k \in \{1, 2, \ldots, n-1\}$ balio horretarako, yx^k

motako elementua y-rekin trukatuko litzateke. Baliokideki, $(yx^k)^y = (yx^k)$ lortuko genuke. Ondoren, konjugazioaren propietateak kontutan izanda,

$$yx^k = (yx^k)^y = y^y(x^k)^y = y(x^k)^y,$$

eta hemendik $x^k = (x^k)^y$. Baina badakigu hori absurdoa dela. Beraz, $C_{D_{2n}}\langle y\rangle = \langle y\rangle$ da.

Bukatzeko, antzeko modura edozein $k \in \{1, 2, \ldots, n-1\}$ baliorako, $\langle y\rangle = C_{D_{2n}}(yx^k) = C_{D_{2n}}\langle yx^k\rangle$ dela frogatzen da.

Beraz, Lema 2.3.2 erabiliz, D_{2n} taldearen trukatze probabilitatea lortzen dugu:

$$cp(D_{2n}) = \frac{\sum\limits_{x\in D_{2n}} |C_{D_{2n}}(x)|}{|D_{2n}|^2} = \frac{1\cdot 2n + (n-1)\cdot n + n\cdot 2}{4n^2} = \frac{n^2+3n}{4n^2} = \frac{n+3}{4n}.$$

Analogoki, n zenbaki bikoitia den kasurako $cp(D_{2n}) = \frac{n+6}{4n}$ dela frogatzen da.

□

Aurreko 4 Ariketan lortutako adierazpenean limiteak hartzen baditugu n infinitura doanean, $cp(D_{2n})$-ren balioa 0.25-rantz konbergitzen duela ikusten dugu. Bereziki, $n = 3$ bada, $cp(D_6) = 0.5$ eta $n = 4$ bada $cp(D_8) = \frac{5}{8} = 0.625$ dira.

Hurrengo azpiatalean n mailako talde simetrikoaren trukatze probabilitatearen adierazpen esplizitu bat emango dugu.

A.2.2 Talde simetrikoa

Lehendabizi, fija dezagun $n \in \mathbb{N}$ eta defini dezagun nor den n mailako talde simetrikoa.

Izan bedi $X = \{1, 2, \ldots, n\}$ n tamainako multzo finitua eta kontsidera dezagun S_n deituko dugun, X-tik X-ra doazen aplikazio bijektibo guztien multzoa. Multzo berri horretan funtzioen arteko konposaketa hartzen badugu eragiketa gisa; $(S_n, \circ)$ egiturak talde egitura du. Hemendik aurrera $(S_n, \circ)$ egiturari, n mailako talde simetrikoa deituko diogu eta bertako elementuei permutazio deituko diegu. Permutazioen artean $\sigma \in S_n$, r luzerako zikloa dela diogu r letra (zenbaki, hots, $a_1, \ldots, a_r$ balioak) ziklikoki mugitzen baditu, eta gainerako $n-r$ letrak finko uzten baditu. Gainera, bi ziklo disjuntuak direla esaten da haien artean ez dituztenean letra komunik mugitzen. Bestalde, jakina da, S_n-ko edozein permutazio ziklo disjuntuen biderkadura

gisa idatz daitekeela, eta deskonposaketa hori bakarra dela, zikloen ordena salbu. Azkenik, gogoratu $|S_n| = n!$ dela.

Orain, S_n taldearen trukatze probabilitatea kalkulatzerako orduan, komenigarria da talde horren konjugazio klaseen kopurua ezagutzea.
S_n-ko bi permutazio konjugatuak dira baldin eta soilik baldin biek ziklo disjuntuen biderkadura gisa idazterakoan, biek luzera bereko ziklo kopurua berdinetan banatu daitezkenean. Deskonposaketa horretan oinarrituta, permutazio baten tipoa defini daiteke; hots, $(c_1, ..., c_n)$ moduko bektorea non c_i bakoitzak, permutazioaren deskoposaketan, i luzerako ziklo kopurua denotatzen duen, $i \in \{1, 2, \ldots, n\}$ izanik. Beraz, bi permutazio konjugatuak dira baldin eta soilik baldin tipo bera badute. Bestalde, talde simetrikoko konjugazio klase kopurua aztertzeko, partiketaren kontzeptua eta konbinatoriako emaitzak aurkeztea ezinbestekoa da.

Konbinatoriako emaitzak

Emanda n zenbaki arrunta, definizioz n-ren partiketa, $a_1, \ldots, a_l$ zenbaki arrunten bilduma da, guztien artean n batzen dutelarik. (Hemendik aurrera, n zenbakiaren partiketa kopurua $p(n)$-ren bidez denotatuko dugu.)

Talde simetrikoaren trukatze probabilitatearen borne bat emateko, konbinatoriaren oinarrizko kontzeptu batzuk berreskuratuko ditugu, [1] liburua jarraituz.

Definizioa A.2.1. Izan bedi Ω, n osagai dituen multzoa. k-naka hartutako n elementuen errepikatuzko konbinazioak, Ω-tik ateratako k osagaidun multiazpimultzoak dira, hots, k osagaidun multzoak errepikapenak onartuz, eta balio hau, ondoko zenbakiaren bidez emanda dago:

$$CR_n^k = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k! \cdot (n-1)!}$$

Era berean, gogora dezagun Newtonen binomian oinarritutako ondoko identitate binomiala: baldin eta $n \in \mathbb{N}$ bada, orduan

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n. \tag{1}$$

Jakina da $p(n)$-ren kalkulua zenbaki teorian agertzen den problema zaila izan ohi dela. Kalkulu hau Bellen (B_n) zenbakiekin erlazionatuta dago. Azken familia horrek ere, Stirlingen bigarren motako zenbaki familiarekin harreman estua du, azken familia honek $[n]$-ko k tamainako partiketa kopurua adierazten baitu. Baldin eta bigarren motako Stirlingen zenbakiak $S(n, k) =$

$\left\{ {n \atop k} \right\}$-ren bidez denotatzen badira, $B_n = \sum_{k=0}^{n} S(n,k)$ betetzen dela froga daiteke.

Alabaina, $p(n)$-ren kalkulua gai honetatik kanpo dago. Horregatik, informazio hau eraskin moduan soilik aipatzen da. Behin, $p(n)$-ren esanahi konbinatorioa aurkeztuta, $p(n)$ goitik bornatzen saiatuko gara. Horretarako, ondorengo emaitza aurkezten da.

Proposizioa A.2.1. Izan bedi n zenbaki arrunta. Orduan, $p(n) \leq 2^{n-1}$ dugu.

Froga. Kontsidera dezagun $x_1 + \cdots + x_k = n$ ekuazio diofantikoa, edozein $i \in \{1, \ldots, n\}$ baliorako, $x_i \geq 1$ izanik. Orduan, edozein n-ren partiketa aurreko ekuazioaren soluzioa da. Orain, ekuazio horren soluzio kopurua zehazteko, errepikatuzko konbinazioak erabiliko ditugu, soluzioen ordenak garrantziarik ez baitu.

Denota dezagun π_n^k-ren bidez aurreko ekuazioaren soluzio kopurua. Beraz, errepikatuzko konbinazioak erabiliz, $\pi_n^k = CR_k^{n-k} = CR_{n-1}^{k-1} = \binom{n-1}{k-1}$ dugu. Ondorioz, arestian aurkeztutako (1) identitatea erabiliz:

$$\pi_n = \sum_{k=1}^{n} \pi_n^k = \sum_{k=0}^{n-1} \binom{n-1}{k-1} = 2^{n-1}.$$

Beraz, $p(n) \leq 2^{n-1}$ dugu, frogatu nahi genuen bezala.

□

Ariketa 5. S_n taldearen trukatze probabilitatea: $cp(S_n) = \frac{p(n)}{n!}$ da.

Froga. S_n taldeko konjugazio klase kopurua, n letreekin egin daitezkeen ziklo moten konbinazio desberdinen kopurua da, eta nabaria da, kopuru hori n-ren partiketa kopuruarekin bat datorrela, hots, $p(n)$-rekin. Orain, 2.3.2 Teorema erabiliz, $cp(S_n) = \frac{k_G}{|S_n|} = \frac{p(n)}{n!}$ da. □

Ondorioz, A Eranskineko A.2.1 proposizioa erabiliz, $p(n) \leq 2^{n-1}$ denez, $cp(S_n) \leq \frac{2^{n-1}}{n!}$ goi bornea lortzen da.

Bestalde, 2 kapituluan ikusitako 2.2.1 Adibidea kontsideratuz, S_3, 3. mailako talde simetrikoaren trukatze probabilitatea $\frac{1}{2}$ da. Hain zuzen ere, $p(3) = 3$, $|S_3| = 3! = 6$ eta $\frac{p(3)}{3!} = \frac{1}{2}$ dira.

A.2.3 Ω multzoa finkatzearekiko trukatzearen kalkuluak

Ariketa 6. Izan bitez D_8, 8 kardinaleko talde diedrikoa, ondoko aurkezpenaren bidez emanda $\langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1}\rangle$, eta $\Omega = \{\{a, b\} \subset D_8 \mid ab = ba, a \neq b, o(a) = o(b) = 2\}$ multzoa. Kalkula dezagun ausazko D_8-ko elementu batek Ω multzoa finkatzearekiko trukatze maila, hots, $P_{D_8}(\Omega)$.

Ebazpena. Kasu honetan, $n = 4$ zenbaki bikoitia eta $\frac{4}{2}$ bikoitia direnez, ikus dezagun $P_{D_8}(\Omega) = \frac{4}{|\Omega|}$ dela. Lehendabizi, D_8-ko elementuak zerrendatuko ditugu, hots, $D_8 = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$. Bestalde, Ω multzoa zehazteko, D_8-ko 2 ordenako elementuak zerrendatuko ditugu, hots, $\{x^2, y, yx, yx^2, yx^3\}$.

Gainera badakigu $Z(D_8) = \langle x^2\rangle$ dela. Beraz, $\{\{x^2, y\}, \{x^2, yx\}, \{x^2, yx^2\}, \{x^2, yx^3\}\} \subseteq \Omega$. Jarraian, azter dezagun noiz $\{yx^j, yx^k\}$ motako azpimultzoak Ω multzoan dauden, hau da, noiz $yx^jyx^k = yx^kyx^j$ den, $j \in \{0, 1, 2, 3\}$ eta $k \in \{0, 1, 2, 3\}$ izanik.

Alde batetik,

$$yx^jyx^k = (x^j)^y x^k = (x^y)^j x^k = (x^{-1})^j x^k = x^{-j+k}$$

Bestetik, $yx^kyx^j = x^{-k+j}$ berdintza dugu. Beraz,

$$x^{-j+k} = x^{-k+j} \iff -j+k \equiv -k+j \pmod{n=4} \iff 2k \equiv 2j \pmod 4.$$

Ondorioz, $\{y, yx^2\}, \{yx, yx^3\}$ dira lor daitezkeen Ω-ko gainontzeko elementuak. Halabeharrez,

$$\Omega = \{\{x^2, y\}, \{x^2, yx\}, \{x^2, yx^2\}, \{x^2, yx^3\}, \{y, yx^2\}, \{yx, yx^3\}\}$$

dugu, eta $|\Omega| = 6$ da.

Behin Ω multzoa zehaztuta, orain Ω-ko elementuen konjugazio klaseak kalkulatuko dugu. Horretarako, D_8-ko elementu orokorren konjugatuak aztertuko ditugu.

Hau da, kontsidera dezagun $i \in \{0, 1\}$, $j \in \{0, 1, 2, 3\}$ eta $k \in \{0, 1, 2, 3\}$ edozein balio. Alde batetik,

$$(x^k)^{y^ix^j} = ((x^k)^{y^i})^{x^j} = (x^k)^{y^i} = (x^{y^i})^k = (x^{(-1)^i})^k$$

(kontuan hartu $(x^k)^{y^i}$ elementua x^j-rekin elkar trukatzen dela, lehenengokoa x-ren berreketa delako.)

Era berean, ondorengo berdintza ere lortzen da:

$$(yx^k)^{y^ix^j} = y^{y^ix^j}(x^k)^{y^ix^j} = y^{x^j}(x^k)^{y^i} = y^{x^j}x^{(-1)^ik} = yx^{2j+(-1)^ik}$$

(kontutan hartu, $y^{x^j} = x^{-j}yx^j = y(x^{-j})^y x^j = y(x^y)^{-j}x^j = yx^{2j}$ dela.)

Beraz, D_8-ko 2 ordenako elementuen konjugazio klaseak ondokoak dira:

$$\mathrm{Cl}_{D_8}(x^2) = \{x^2\}$$
$$\mathrm{Cl}_{D_8}(y) = \{y, yx^2\}$$
$$\mathrm{Cl}_{D_8}(yx) = \{yx, yx^3\} = \mathrm{Cl}_{D_8}(yx^3)$$

Azkenik, Ω-ko elementuen konjugazio klaseak ondokoak dira:

$$\mathrm{Cl}_\Omega(\{x^2, y\}) = \{\{x^2, y\}, \{x^2, yx^2\}\}$$
$$\mathrm{Cl}_\Omega(\{x^2, yx\}) = \{\{x^2, yx\}, \{x^2, yx^3\}\}$$
$$\mathrm{Cl}_\Omega(\{y, yx^2\}) = \{\{y, yx^2\}\}$$
$$\mathrm{Cl}_\Omega(\{yx, yx^3\}) = \{\{yx, yx^3\}\}$$

Beraz, $k = 4$ eta $|\Omega| = 6$ denez, 3.2.1 Teoremagatik $P_{D_8}(\Omega) = \frac{k}{|\Omega|} = \frac{4}{6} = \frac{2}{3}$ dugu. □

Ariketa 7. Izan bitez D_{12}, 12 kardinaleko talde diedrikoa, ondoko aurkezpenaren bidez emanda $\langle x, y \mid x^6 = y^2 = 1, x^y = x^{-1}\rangle$, eta $\Omega = \{\{a, b\} \subset D_{12} \mid ab = ba, a \neq b, o(a) = o(b) = 2\}$ multzoa. Kalkula dezagun ausazko D_{12}-ko elementu batek Ω multzoa finkatzearekiko trukatze maila, hots, $P_{D_{12}}(\Omega)$.

Ebazpena. Kasu honetan, $n = 6$ zenbaki bikoitia eta $\frac{6}{2} = 3$ bakoitia direnez, ikus dezagun $P_{D_{12}}(\Omega) = \frac{3}{|\Omega|}$ dela. Lehendabizi, D_{12}-ko elementuak zerrendatuko ditugu, hots, $D_{12} = \{1, x, x^2, x^3, x^4, x^5, y, yx, yx^2, yx^3, yx^4, yx^5\}$. Bestalde, Ω multzoa zehazteko, D_{12}-ko 2 ordenako elementuak zerrendatuko ditugu, hots, $\{x^3, y, yx, yx^2, yx^3, yx^4, yx^5\}$.

Alde batetik, badakigu $Z(D_{12}) = \langle x^3\rangle = \{1, x^3\}$ dela. Beraz,

$$\{\{x^3, y\}, \{x^3, yx\}, \{x^3, yx^2\}, \{x^3, yx^3\}, \{x^3, yx^4\}, \{x^3, yx^5\}\} \subseteq \Omega.$$

Jarraian, azter dezagun noiz $\{yx^j, yx^k\}$ motako azpimultzoak Ω multzoan dauden, hau da, noiz $yx^jyx^k = yx^kyx^j$ betetzen den, $j \in \{0, 1, 2, 3, 4, 5\}$ eta $k \in \{0, 1, 2, 3, 4, 5\}$ izanik.

Alde batetik,

$$yx^jyx^k = (x^j)^yx^k = (x^y)^jx^k = (x^{-1})^jx^k = x^{-j+k}$$

Bestetik, $yx^kyx^j = x^{-k+j}$ berdintza dugu. Beraz,

$$x^{-j+k} = x^{-k+j} \iff -j+k \equiv -k+j \pmod{n=6} \iff 2k \equiv 2j \pmod 6.$$

Ondorioz, $\{\{y, yx^3\}, \{yx, yx^4\}, \{yx^2, yx^5\}\}$ dira lor daitezkeen Ω-ko gainontzeko elementuak. Halabeharrez,

$$\begin{aligned}\Omega =&\{\{x^3, y\}, \{x^3, yx\}, \{x^3, yx^2\}, \{x^3, yx^3\}, \{x^3, yx^4\},\\ &\{x^3, yx^5\}, \{y, yx^3\}, \{yx, yx^4\}, \{yx^2, yx^5\}\}\end{aligned}$$

Behin Ω multzoa zehaztuta, orain Ω-ko elementuen konjugazio klaseak kalkulatuko dugu. Horretarako, D_{12}-ko elementu orokorren konjugatuak aztertuko ditugu. Hau da, kontsidera dezagun edozein $i \in \{0, 1\}$, $j \in \{0, 1, 2, 3, 4, 5\}$ eta $k \in \{0, 1, 2, 3, 4, 5\}$ balioak. Alde batetik,

$$(x^k)^{y^i x^j} = ((x^k)^{y^i})^{x^j} = (x^k)^{y^i} = (x^{y^i})^k = (x^{(-1)^i})^k$$

(kontuan hartu $(x^k)^{y^i}$ elementua x^j-rekin elkar trukatzen dela, lehenengokoa x-ren berreketa delako.)

Era berean, ondorengo berdintza ere lortzen da:

$$(yx^k)^{y^i x^j} = y^{y^i x^j}(x^k)^{y^i x^j} = y^{x^j}(x^k)^{y^i} = y^{x^j} x^{(-1)^i k} = yx^{2j+(-1)^i k}$$

(kontutan hartu, $y^{x^j} = x^{-j} y x^j = y(x^{-j})^y x^j = y(x^y)^{-j} x^j = yx^{2j}$ dela.)

Beraz, D_{12}-ko 2 ordenako elementuen konjugazio klaseak ondokoak dira:

$$\begin{aligned}\mathrm{Cl}_{D_{12}}(x^3) &= \{x^3\}\\ \mathrm{Cl}_{D_{12}}(y) &= \{y, yx^2, yx^4\}\\ \mathrm{Cl}_{D_{12}}(yx) &= \{yx, yx^3, yx^5\}\end{aligned}$$

Azkenik, Ω-ko elementuen konjugazio klaseak ondokoak dira:

$$\mathrm{Cl}_\Omega(\{x^3, y\}) = \{\{x^3, y\}, \{x^3, yx^2\}, \{x^3, yx^4\}\}$$

$$\mathrm{Cl}_\Omega(\{x^3, yx\}) = \{\{x^3, yx\}, \{x^3, yx^3\}, \{x^3, yx^5\}\}$$

$$\mathrm{Cl}_\Omega(\{y, yx^3\}) = \{\{y, yx^3\}, \{yx, yx^4\}, \{yx^2, yx^5\}\}$$

Beraz, $k = 3$ eta $|\Omega| = 9$ denez, 3.2.1 Teoremagatik $P_{D_{12}}(\Omega) = \frac{k}{|\Omega|} = \frac{3}{9} = \frac{1}{3}$ dugu.

□

Bibliografia

[1] J. A. Barcena-Petisco eta M. Merino, *Matematika diskretua. 2. edizioa*, 2023.

[2] S. M. Buckley eta D. Machale, "Groups with $Pr(G) = \frac{1}{3}$".

[3] M. A. El-Sanfaz, N. H. Sarmin eta S. M. S. Omer, "The Probability that an element of the Dihedral Groups fixes a set", Malasyan Journal of Foundamental and Applied Sciences, 2014, Vol. 52, No. 1 , 1-6.

[4] M.A. El-Sanfaz, S. M. S. Omer eta N. H. Sarmin, "On the probability that a group fixes a set and its generalized conjugacy class graph", International Journal of Mathematical Analysis, 2015, Vol. 9, No. 4, 161-167.

[5] M. A. El-Sanfaz, N. H. Sarmin eta S. N. A. Zamri, "Generalized Commuting Graph of Dihedral, Semi-dihedral and Quasidiedral Groups", Malasyan Journal of Foundamental and Applied Sciences, 2021, Vol. 17, No. 6, 711-719.

[6] G. Fernández-Alcober, *Teoría de Grupos. Teoría de las Representaciones Ordinarias de Grupos Finitos*, Euskal Herriko Unibertsitateko Matematika Graduko "Grupos y Representaciones" irakasgaiko apunteak, 2001.

[7] P. X. Gallagher, "The number of conjugacy classes in a finite group", Mathematische Zeitschrift, 1970, Vol. 118, 175-179.

[8] M. E. Garciarena, *Cardinality and Words in Profinite Groups*, PhD thesis, Università degli Studi di Padova, 2021.

[9] W. H. Gustafson, "What is the probability that two group elements commute?", The Americal mathematical monthly, 1973, Vol. 80, No. 9, 1031-1034.

[10] P. Lescot, "Sur certains groupes finis", Rev. Math. Spéciales, 1987, Vol. 8, 276-277.

[11] P. Lescot, "Degré de commutativité et structure d'un groupe fini (1)", Rev. Math. Spéciales, 1988, Vol. 8, 276-279.

[12] P. M. Neumann, "Two Combinatorial Problems in Group Theory", Bulletin of the London Mathematical Society, 1898, Vol. 21, No. 5, 456-458.

[13] S. M. S. Omer, N. H. Sarmin eta A. Erfanian, "The Probability that an element of a Symmetric Group fixes a set and its application in Graph Theory", World Applied Sciences Journal, 2013, Vol. 27, No.12, 1637-1642.

[14] S. M. S. Omer, N. H. Sarmin eta A. Erfanian, "The Probability that an element of a Symmetric Group fixes a set and the group act on set by conjugation", International Journal of Applied Mathematics and Statistics, 2013, Vol. 32, No. 2, 111-117.

[15] E. Romano, A. Russo eta G. Vincenzi, "Generalized FC-groups. In Procedings of the Meeting on Groups Theory and its Applications, on the occasion of Javier Otal's 60 th birthday", JM Munoz Escolano, 2011, 243-266.

[16] S. Sen. "Commuting Probability of finite Groups", Resonance, 2023, Vol. 28, No. 4, 597-612.

[17] S. Sen. "Commuting Probability of finite Groups (Extended)", Indian Statistical Institute, 2023.