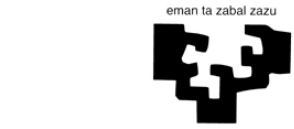


ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Talde Teoria orokorrean murgilduz

Gradu Amaierako Lana
Matematikako Gradua

Nagore Capa Calvo

Leire Legarreta Solaguren
Irakasleak zuzendutako lana

Leioa, 2014ko ekainaren 23a

Aurkibidea

Eskerrak

Nire ibilbide akademikoaren etapa honen amaieran eskerrak adierazi nahi dizkiot Leireri, memoria hau zuzendutako irakasleari, bere laguntzari, parte hartzeari eta pazientziari esker esperientzia hau oso aberatsa eta eramangarria bihurtu duelako. Hasieratik eskuzabaltasuna adierazi izan du, entzuteko eta nire buruhausteei konponbidea emateko prest egon baita. Honekin amaitzeko lau urte hauetan nire etorkizuneko xedea gertutik jarraitu duten pertsonei ere eskerrak eman nahi dizkiet.

Sarrera

Talde finituen teoriaren xedea talde finitu guztiak bilatzea da, hau da, edozein motatako talde finituak nola eraiki eta prozedura eraginkor bat nola ezarri, emandako bi talde finitu mota berdinekoak diren ala ez zehazteko. Edozein kasutan ideia honen lorpena, lan honetan garatuko den teoriatik hurrunago doa, baina momentu honetan interesgarria iruditzen zaigu bere garrantzia adieraztea. Hala ere, lehenago aipatutakoari buruz, talde abeldar finituei dagokiena duela ehun urte lortu zen.*

Jakina da G talde finitu bakoitzak $|G|$ zenbaki oso positibo bat duela elkartuta. Ohartu, n zenbaki oso positibo bakoitzeko, gutxienez beti n ordenako mota berezi bateko talde bat dagoela, hain zuzen ere, $X = \{z \in \mathbb{C} : z^n = 1\} = \{e^{\frac{2\pi i}{n}} : i \in \{0, 1, \ldots, n-1\}\}$, hau da, unitatearen n-garren erro konplexuen multzoa. Aipatutako multzoa, n ordenako taldea da ohiko biderketarekiko. Gainera, n zenbaki oso positibo bakoitzeko, n ordenako mota desberdinetako taldeen kopurua finitua dela ikustea erreza da. Izan ere, edozein n ordenako G taldearentzako eta edozein X, n elementu dituen multzoarentzako, X-k G taldearen isomorfoa den egituraren bat eman dezake. Horretarako, $\varphi\colon G \longrightarrow X$ aplikazio bijektibo bat aukeratu eta X-n edozein $g_1, g_2 \in G$, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ erregelaren bidez biderketa definitzea da egin beharreko guztia. Erraz frogatzen da horrela, X-n definitutako biderketak talde egitura duela eta ondorioz φ isomorfismo bat dela. Honek esan nahi du, n tamainako X multzo berezi bati lotutako $X \times X \longrightarrow X$ esleipen posible guztien artean, aurkitzen direla n ordenako talde mota desberdin guztiak. Baina, aipatutako esleipenen kopurua n^{n^2} da. Honela gehienez n ordenako mota desberdinen talde kopurua n^{n^2} da. Beraz, n^{n^2}, n ordenako talde kopuru desberdinen goi borne finitu bat da.

Hemendik aurrera, n zenbaki oso positibo bakoitzeko, n ordenako mota desberdinetako taldeen kopurua $v(n)$ bidez denotatuko da, eta hauetatik talde abeldarren kopurua $v_a(n)$ bidez. Argi dago, $v_a(n) \leq v(n)$ dela. Lagrangeren teoremagatik, jakina da p ordena leheneko edozein talde, talde ziklikoa dela. Gainera, ordena bereko edozein bi talde zikliko isomorfoak

*1. Kapituluko 1.3 atala ikusi.

dira; ondorioz, isomorfismo salbu p ordena leheneko talde zikliko bakarra existitzen da, C_p alegia. Beraz, baldin eta p zenbaki lehena bada, $v(p) = 1$ da. Hala eta guztiz ere, existitzen dira lehenak ez diren n zenbaki oso positiboak zeinentzat $v(n) = 1$ den. Adibidez, $n = 15$ den kasuan, froga daiteke ordena horretako edozein talde abeldarra eta ziklikoa dela, hain zuzen ere C_{15}-ren isomorfoa.

Bestalde, n zenbaki lehenen berreturen biderkadura gisa deskonposatzen bada, hau da, $n = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$ bada $s, m_1, \dots, m_s$ zenbaki oso positiboak eta $p_1, \dots, p_s$ zenbaki lehen desberdinak izanik, orduan $v(n) = 1$ da baldin eta soilik baldin $m_1, \dots, m_s$ berretzaile guztiak berdin 1 badira, eta $i, j \in \{1, \dots, s\}$ guztientzat $p_i - 1$ ez bada p_j-gatik zatigarria. Ondorengo galdera, n ordenako mota desberdinetako talde abeldarren kopuruarekin zer gertatzen den izan daiteke. Erraz ikus daiteke $v_a(n) = v_a(p_1^{m_1}) \dots v_a(p_s^{m_s})$ dela, non $j \in \{1, \dots, s\}$ bakoitzeko $v_a(p_j^{m_j})$ adierazpenak m_j zenbakia, zenbaki oso positiboen batura bezala adierazteko dauden modu desberdinen kopurua adierazten duen, osagaien ordena kontuan hartu gabe. Bereziki, $v_a(p_j^{m_j}) \geq m_j$. Honek, $v_a(n)$-rentzako n-ren menpekoa ez den goi bornerik ez dagoela erakusten du. Ondorioz, ezta $v(n)$-rentzako ere.

Talde finitu berriak eraikitzeko problemaren hurbilketa naturala taldeen ordenaren menpekoa den metodo induktibo bat bilatzea da. Beraz, talde finitu bakoitza ordena txikiagoko taldeen arabera deskribatzen saiatu behar gara. Honela, hasiera batean, zenbait oinarrizko talderekin hastea espero genezake eta honela, urratsez-urrats mota guztietako talde finituen adierazpenera hurbiltzea. Gainera, modu naturalean azpitaldeetan pentsa genezake. Baina, zein nolako azpitalde eta zenbat azpitalde ditu n ordenako talde batek? Lagrangeren Teoremagatik, jakina da G-ren edozein azpitalderen ordenak G taldearen ordena zatitzen duela. Hala ere, ez da egia G taldearen ordena n izanik, m, n-ren zatitzaile bakoitzeko G taldeak behintzat m ordenako azpitalde bat duenik. Baina, ordea, G, n ordenako talde finitua izanik, n zatitzen duen p-ren p^m berretura bakoitzeko, p zenbaki lehena izanik, G taldeak badu p^m ordenako azpitalderen bat (Sylow-en 1go Teorema). Emaitza honek, ordena zenbaki lehen baten berretura duten taldeak aztertzera eramaten gaitu. Talde hauek propietate bereziak dituzte eta talde finituen ikerketan garrantzi handia dute ere.

Edozein G taldearen azpitaldeen artean G-ri buruz informazioa lortzeko erabilgarriak diren azpitalde berezi batzuk daude, adibidez, azpitalde normalak. Baldin eta K, G-ren azpitalde normala bada, $K \trianglelefteq G$ idazkera ohikoa da. Eta kasu horretan, G/K eran denotatzen dugun, G-ren azpitaldea ez den beste talde egitura bat defini dezakegu, hain zuzen ere, G-ren zatidura taldea. Zentzu batean, G taldea K eta G/K taldeen bitartez eraiki daitekeela pentsa genezake. Bereziki, baldin eta G talde finitua bada, orduan

K eta G/K ere finituak dira eta $|G| = |K| \cdot |G/K|$ erlazioa betetzen da. Bestalde, edozein G taldek beti ditu bi azpitalde normal: G bera eta $\{1\}$ azpitalde tribiala. Honela, $G/G \cong \{1\}$ eta $G/\{1\} \cong G$ dira. Baina benetan, existitzekotan, interesgarriak diren azpitalde normalak talde osoa eta tribiala ez direnak dira. Baldin eta K, G-n azpitalde normala baina $K \neq G$ bada, $K \lhd G$ idazten dugu, eta azpitalde normal propioa dela deritzogu. Horregatik, baldin eta G finitua bada eta $K \lhd G$, G taldea, K eta G/K, G taldearen ordena baino txikiagoko talde bien menpeko deskribapena lor daitekeela aipatu da arinago. Baina ezin dezakegu esan deskribapen hori guztiz osatua denik; orokorrean K eta G/K taldeen motak ezagutzea ez baita nahikoa G taldearen mota bakartasunez zehazteko. Beraz, honek "hedapen problema" dakar: emanda edozein K eta Q bi talde, $K \trianglelefteq G$ eta $G/K \cong Q$ baldintzak betez, G talde guztien motak zehaztea. Ohartu, baldin eta K eta Q talde finituak badira, orduan talde horien mota desberdinen kopurua ere finitua dela, zeren eta talde mota horiek $|K||Q|$ ordena dute, eta mota horien kopurua gehienez $v(|K||Q|)$ da.

Nahiz eta jakitun egon "hedapen problema" gogorra dela, problema honi aurre egin diezaiokegula suposatuz momentu honetan, hurrengoa egitera anima gaitezke. Edozein G talde finiturako berfindu ezin daitekeen hurrengo azpitaldeen katea kontuan har dezakegu: $1 = K_0 \lhd K_1 \lhd \ldots \lhd K_{s-1} \lhd K_s = G$. Hau da, ezin dugu H beste azpitalde bat $K_{j-1} \lhd H \lhd K_j$ baldintza betetzen duenik aurkitu, edozein $j \in \{1, \ldots, s\}$-rako. Berfindu ezin daitezkeen kate horiei G-ren konposizio serieak deritzegu. Orduan, G taldea $K_1/K_0, K_2/K_1, \ldots, K_s/K_{s-1}$ zatidura taldeen bidez deskribatzen saia gaitezke. Nabaria da ere, $|K_1/K_0| \cdot |K_2/K_1| \cdots |K_s/K_{s-1}| = |G|$ dela. Bestalde, ezaguna da G talde finitu guztiek, gutxienez konposizio serie bat izango dutela. Aurrekoa frogatzeko, G-ren ordenaren gaineko indukzioa erabiliko da ondoren adieraziko den moduan. Baldin eta G-ren ordena 1 bada, orduan, $1 = K_0 = G$, G-ren konposizio seriea da. Hau da, hemendik aurrera $|G| > 1$ dela suposa dezakegu. Har dezagun $K \lhd G$, $|K|$ ahal den handiena izanik (gerta daiteke $K = 1$ izatea). Beraz, $|K| < |G|$ eta hipotesi induktiboa erabiliz, K azpitaldeak konposizio serie bat du: $1 = K_0 \lhd K_1 \lhd \ldots \lhd K_{s-1} = K$ non s zenbaki oso positiboa den. Orduan, $1 = K_0 \lhd K_1 \lhd \ldots \lhd K_{s-1} = K \lhd K_s = G$, G-ren konposizio seriea da. Definizioz, G talde baten edozein bi serie,

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = G$$

baliokideak direla esaten da baldin eta $s = r$ bada, eta existitzen bada σ, $\{1, 2, \ldots, s\}$ multzoaren gaineko permutazioa zeinarentzat $G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i)-1}$ den, edozein $i \in \{1, 2, \ldots, s\}$ baliotarako. Argi dago, G-ren serieen multzo gainean, aurreko definizioak baliokidetasun erlazioa definitzen

duela. Sarrera honetan ematen hasi berri garen "pintzelkadak" edo ideia intutiboak seriei buruz, oso erabilgarriak izango dira lanaren Laugarren Kapituluan. Aurreko edukiekin jarraituz, konposizio serieri buruzko emaitza garrantzitsuena ondoko Jordan-Hölderen baieztapena da: baldin eta G talde batek konposizio serie bat onartzen badu, orduan alde batetik, G-ren edozein serie propioak, G-ren konposizio seriea den berfindutako serie bat onartzen du, eta bestalde, G-ren edozein bi konposizio seriek baliokideak dira. Bereziki, baldin eta G talde finitua bada eta,

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G,$$

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_t = G,$$

G-ren bi konposizio serie badira, orduan $s = t$ da, eta $G_1/G_0, G_2/G_1, \ldots, G_s/G_{s-1}$ eta $H_1/H_0, H_2/H_1, \ldots, H_s/H_{s-1}$, s zatidura taldeen ondoz ondoko bi segidek, mota berdineko taldeak onartzen dituzte, eta horietariko bakoitza anizkoiztasun berdinarekin agertzen da aurreko bi segidetan, ordena salbu. Definizioz, G-ren konposizio luzerari s deitzen zaio eta, G_1/G_0, $G_2/G_1, \ldots, G_s/G_{s-1}$, G-ren konposizio faktoreak deitzen dira. Talde batzuen konposizio luzera batekoa da. Talde horiei talde bakunak (edo sinpleak) deritzegu. Hain zuzen ere, edozein G talde (finitua zein infinitua) bakuna da baldin eta $G \neq 1$ bada, eta G-ren azpitalde normal bakarrak tribiala eta bera badira. Erraz ohar gaitezke talde finitu ez-tribial baten edozein konposizio faktorea talde bakuna dela. Talde finitu bakunak, zentzu batean, zenbaki lehenen "papera" joka dezaketeela pentsa genezake. Hain zuzen ere, talde bakun abeldar bakarrak ordena leheneko taldeak dira. Bestalde, existizen dira infinitu kantitate talde bakun finitu ez abeldarrak direnak.

Hurrengoko interesa izan daiteke zehaztea nola azter daitezkeen talde bakun ez-abeldarren egiturak. Kasu honetan ere, nahiz eta taldeak azpitalde normal propiorik ez izan, talde osoaren egitura ordena txikiagoko taldeen arabera aztertzea izango genuke gustoko. Beraz, azpitalde ez normalekin aritu beharko gara. Honekin hasteko, beharrezkoa da W. Feit eta J.G. Thompson-en (1963an) [5] ikerkuntza modernoan aipagarrienetarikoa den ondoko emaitza eskura izatea: edozein talde finitu bakun ez abeldarraren ordena bikoitia da. Aurreko emaitzaren garrantzia, talde finitu bakun ez abeldarraretan 2 ordenako elementuren baten existentzian datza. Bestalde, Sylow-en 1go Teoremaren ondorio gisa, erraz lortzen da edozein ordena bikoitiko talde finitu batek gutxienez 2 ordenako elementu bat duela, hau da, inboluzioren bat. (Edozein kasutan lan honen A Eranskineko 5garren ariketan, aipatutako azken emaitza horren beste oinarrizko froga bat aurkeztuko da ariketa gisa.)

Lan honen helburua ez da ezertan ere, talde finitu bakun ez abeldarren karakterizazioarekin aritzea, baina puntu honetara helduta, zein garrantzia

duen talde batek inboluzio bat onartzea egokia dirudi, zeren eta azkeneneko urteetako ikerkuntza matematikoan asko aztertu da inboluzioen zentralizatzaileen inguruan. Istorio honekin bukatzeko, (1955ean) R. Brauer-ek eta K.A. Fowler-rek [6] lortutako ondoko emaitza enuntziatuko dugu: baldin eta G talde finitu bakun ez abeldarra bada, eta t, G-ren inboluzioa bada, orduan G taldean, t-ren zentralizatzailea propioa da, eta horren ordena m bidez denotatzen bada, G-ren ordena ere bornatuta dago $(\frac{1}{2}m(m+1))!$ zenbakiagatik. (Ohartu kasu honetan G-ren ordena baino txikiagoko talde ez-normal batekin lan egiten dela, hain zuzen ere, inboluzioaren zentralizatzailearekin.)

Sarrera honen azken zatian, aurkezten den memoriaren laburpen txiki bat ematea gustatuko litzaiguke. Hasteko, lehenengo Kapituluan Talde Teoriako oinarrizko kontzeptuak gogoratuko ditugu. Baita, garrantzi handia duen finituki sortuak diren talde abeldarren egitura teorema estudiatuko da. Bestalde, aipatzekoa da, Matematika Graduko Laugarren mailako lehenengo lauhilabetean garatutako "Taldeak eta Adierazpenak" irakasgaian, p-talde finituen eta Sylow-en Teoremen oinarriak jadanik aztertu direla. Edozein kasuan, memoria honen Bigarren Kapituluan, Sylow-en Teoremen ezagutza aztertuko da. Lanaren Bigarren Kapituluari amaiera emateko, Sylow-en Teoremen ondorio interesgarri bat guztiz garatuta aurkeztuko da, aplikazio gisa. Orain, Hirugarren Kapituluan guretzat guztiz berria den gai bat aztertuko da: talde nilpotenteak, hain zuzen ere. Azkenik, lanaren Laugarren Kapituluan, arinago aipatu den bezala, edozein talderen serie berezi batzuk estudiatuko dira. Preseski, Laugarren Kapitulu hori hiru zatitan banatuko dugu: alde batetik, talde ebazgarrien oinarriak, π-taldeak eta azkenik, talde ebazgarri finituen Hall-en π-azpitaldeak, eta Hall-en Teoremak. Aurkezten den lan hau estudiatzen eta osatzen egon garen bitartean, hainbat ariketa burutu ditugu. Memoria honeri eranskin bat (A Eranskina) gehituko diogu, eta bertan guretzat interesgarrienak diren ariketak agertuko dira. Argi dago, ariketa zerrenda hori ez dagoela zailtasunaren araberan guztiz orekatuta, baizik eta premiaren arabera, une batzuetan beharrezkoak izan ditugulako horiek egitea, kontzepturen bat menperatzeko.

1. Kapitulua

Talde finituen teoriako sarrera

1.1 Hasierako definizioak

Definizioa. Izan bitez G multzoa eta $*$, G-n definitutako eragiketa. Orduan, $*$ eragiketak ondoko oinarrizko propietateak bete ditzake:

(i) $*$ eragiketa elkarkorra da baldin eta,

$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ betetzen bada, $g_1, g_2, g_3 \in G$ guztietarako.

Bereziki, $*$ eragiketa elkarkorra denean, $g_1 * g_2 * \ldots * g_n$ adierazpena parentesirik gabe idaztea zentzuzkoa da.

(ii) $*$ eragiketa trukakorra da baldin eta,

$$g_1 * g_2 = g_2 * g_1 \text{ betetzen bada, } g_1, g_2 \in G \text{ guztietarako.}$$

(iii) Existitzen bada $e \in G$ non

$$g * e = g = e * g \text{ den, } g \in G \text{ elementu guztientzako,}$$

orduan e, G-n $*$-ren elementu neutroa dela diogu.

(iv) Baldin eta $*$ eragiketak e elementu neutroa badu G-n, orduan $g \in G$ elementua alderanzgarria dela diogu, existitzen bada $g' \in G$ non

$$g * g' = e = g' * g \text{ den.}$$

Kasu honetan, g' elementua g-ren alderantzizkoa dela esango dugu.

Ohartu, $*$ eragiketak elementu neutroa badu G-n, neutroa bakarra dela. Gainera, elementu bat alderanzgarria izanez gero, bere alderantzizkoa ere bakarra da.

Definizioa. Izan bitez G multzoa eta $*$, G-n definitutako eragiketa. Orduan, $(G, *)$ taldea dela esaten da ondoko hiru propietateak betetzen badira:

(i) $*$ elkarkorra da G-n.

(ii) $*$ eragiketak elementu neutroa du G-n.

(iii) G-ko elementu guztiak alderanzgarriak dira $*$-rekiko.

Gainera, baldin eta $*$ trukakorra bada G-n, orduan G taldea abeldarra edo trukakorra dela diogu.

Hemendik aurrera, notazioa arintzeko $*$ eragiketa adierazteko normalean $\cdot$ ikurra edo juxtaposizioa erabiliko dugu, hau da, orokorrean notazio biderkakorra erabiliko dugu. Gainera, orokorrean G-ko elementu neutroa 1 bidez adieraziko da eta $g \in G$, elementuaren alderantzizkoa g^{-1} bidez.

Bestalde, interesgarria izan daiteke talde batek dituen elementuen kopurua ezagutzea; honi taldearen ordena deritzogu eta $|G|$ bidez denotatuko da. Printzipioz kardinal hori finitua zein infinitua izan daiteke.

Definizioa. Izan bitez $(G, \cdot)$ taldea eta $H \subseteq G$ azpimultzoa. Orduan, H, G-ren azpitaldea dela esaten da ondoko bi baldintzak betetzen badira:

(i) $\cdot$ eragiketa da H-n, hau da, $h_1, h_2 \in H$ guztietarako, $h_1 \cdot h_2 \in H$ bada.

(ii) $(H, \cdot)$ taldea da.

Kasu honetan, $H \leq G$ eran adieraziko dugu. Gainera, G-ko elementu neutroa eta H-koa bat datoz, eta $h \in H$ elementu bakoitzaren alderantzizkoa berdina da H-n zein G-n.

Bestalde, taldearen elementu neutrotaz baino ez, osatuta dagoen azpitaldeari, azpitalde tribiala deitzen zaio.

Hain zuzen ere, $H \leq G$ dela ikusteko definizioa ez ezik, hurrengo teorema ere erabilgarria da.

Teorema 1.1. *Izan bitez G taldea eta $H \subseteq G$ azpimultzo ez hutsa. Orduan baliokideak dira ondoko hiru baieztapenak:*

(i) *H, G-ren azpitaldea da.*

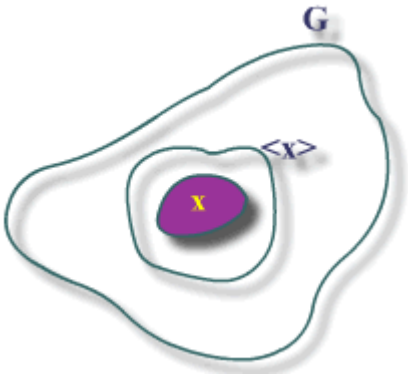
(ii) *Edozein $h_1, h_2 \in H$ elementutarako, $h_1 \cdot h_2 \in H$ eta $h_1^{-1} \in H$.*

(iii) *Edozein $h_1, h_2 \in H$ elementutarako, $h_1 \cdot h_2^{-1} \in H$.*

Orokorrean, G-ren bi azpitalde H eta K baditugu, HK-k ez du zertan beti azpitaldea izan behar. Hala ere, $HK = KH$ denean HK azpitaldea da. Bereziki, argi dago G talde abeldarren kasuan HK beti izango dela azpitaldea.

Ohar gaitezen ere G taldearen X azpimultzo bat hartuta honek ez duela, zertan beti azpitaldea izan behar. Hala ere, X multzoak G-ren azpitalde bat sor dezake ondoren azalduko dugun bezala.

Definizioa. Izan bitez G taldea eta $X \subseteq G$ azpimultzoa. Orduan, X-k sortutako azpitaldea, $\langle X \rangle$ ikurraren bitartez denotatzen dena, X barruan duen G-ren azpitalderik txikiena da. Edo beste era batera esanda, X barruan duten G-ren azpitalde guztien ebakidura da. Honen adierazpena $\langle X \rangle = \{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} : x_i \in X, \epsilon_i = \pm 1, n \in \mathbb{N} \cup \{0\}\}$ da. Gainera, baldin eta $G = \langle X \rangle$ bada, X multzoa G-ren sistema sortzaile bat dela esaten da. Honez gain, G taldea elementu kopuru finitu batez sor daitekenean, G taldea finituki sortua dela esaten da.



1.1. irudia. $\langle X \rangle$, X barruan duen G-ren azpitalderik txikiena.

Oharrak. (i) $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ biderkaduran, baldin eta $n = 0$ bada, biderkaduraren balioa berdin 1 dela suposatuko da.

(ii) Bereziki, HK, G-ren azpitalde finitua den kasuan, $HK = \langle H, K \rangle$ da. Eta, kasu honetan HK-ren kardinala edo ordena ondoko formularen bidez kalkulatzen da, $|HK| = \frac{|H||K|}{|H \cap K|}$.

Azpimultzo batek sortutako azpitaldeen artean, sinpleenak elementu bakar batez sortutakoak dira. Ondoko definizioan horien karakterizazioa ematen da.

Definizioa. Izan bitez G taldea eta $g \in G$. Orduan, g-k sortutako azpitaldea $\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$ eran definitzen da.

Gogoratu emandako azken definizio honetan G taldearen eragiketa $\cdot$ dela. Berriz, G talde batukorra denean, $\langle g \rangle = \{ig : i \in \mathbb{Z}\}$ da.

Definizioa. Izan bitez G taldea eta $g \in G$. Orduan, g elementuaren ordena ondoko moduan definitzen da,

$$o(g) = \begin{cases} n, & \text{baldin eta } \exists n \in \mathbb{N} \text{ non } g^n = 1 \text{ den eta,} \\ & n \text{ baldintza hori betetzen duen baliorik txikiena.} \\ \infty, & \text{bestelako kasuetan.} \end{cases}$$

Proposizioa 1.2. *Baldin eta G talde finitua bada, orduan $o(g)$, $|G|$-ren zatitzailea da eta $g^{|G|} = 1$ da, edozein $g \in G$ elementutarako. Bestalde, g-ren ordena finitua denean, $g^{o(g)} = 1$ da.*

Definizioak. Izan bedi G taldea.

(i) G ziklikoa dela deritzogu baldin eta existitzen bada $g \in G$ elementua non $G = \langle g \rangle$ den. Hau da, taldeko elementu bakar batez G talde osoa sor daitekenean. (Ohartu, G talde finitu bat ziklikoa dela baldin eta soilik baldin existitzen bada $g \in G$ non $o(g) = |G|$ den.)

(ii) Gainera, $G = \langle g \rangle$ talde ziklikoaren ordena n zenbaki finitua bada, orduan $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ da. Aldiz, $G = \langle g \rangle$ talde ziklikoa ordena infinitukoa denean, $G = \langle g \rangle = \{g^i : i \in \mathbb{Z}\}$ da.

(iii) Talde ziklikoek duten propietate garrantzitsu bat talde abeldarrak direla da; izan ere elementu baten berretura desberdinak elkarrekin trukatzen dira. Kontrakoa, aldiz ez da egia, hau da, talde abeldar guztiek ez dute zertan talde ziklikoak izan behar.

(iv) Talde zikliko finituen kasuan, sortzaileaz gain beste elementuen ordena kalkulatzea ere oso erreza da ondoko formula erabiliz, $o(g^r) = \frac{o(g)}{\text{zkh}(o(g),r)}$, edozein $r \in \mathbb{Z}$-rentzat.

Definizioa. Izan bitez G talde finitua, $H \leq G$ eta $g \in G$ elementu finkoa. Orduan, H-ko elementu guztiak g-rekin operatzen baditugu, ondoko bi multzo lortzen dira:

(i) g-ren H-rekiko ezker-koklasea, $gH = \{gh : h \in H\}$.

(ii) g-ren H-rekiko eskuin-koklasea, $Hg = \{hg : h \in H\}$.

Argi dago, $|gH| = |Hg|$ betetzen dela. Gainera, $\{gH : g \in G\}$ koklaseen multzoak $\frac{|G|}{|H|}$ beste elementu ditu, eta honi G-ko H-ren indizea deitzen zaio eta $|G : H|$ bidez denotatzen da. Bestalde, edozein bi ezker-koklase berdinak edo disjuntuak dira eta berdin eskuin-koklaseen kasuan.

Teorema 1.3 (Lagrangeren Teorema)**.** *Izan bitez G taldea eta $H \leq G$. Orduan ondoko baieztapenak betetzen dira:*

(i) $|G| = |G : H||H|$.

(ii) *Baldin eta G finitua bada, orduan $|G : H| = |G|/|H|$ da. Bereziki $|H|$-k $|G|$ zatitzen du.*

Bereziki, ondoko baldintza oso erabilgarria da: izan bitez G talde finitua eta $H, K \leq G$. Orduan:

(i) $|G : H \cap K| \leq |G : H||G : K|$ da, eta aurreko desberdintza berdintza da baldin eta soilik baldin $G = HK$ bada.

(ii) Baldin eta $|G : H|$ eta $|G : K|$ elkarrekiko lehenak badira, i) ataleko desberdintza berdintza bihurtzen da.

Definizioa. Izan bitez G taldea, H eta K, G-ren bi azpitalde eta $g \in G$ elementu finkoa. Orduan, H eta K-rekiko g-ren koklase bikoitza ondoko eran definitzen da: $HgK = \{hgk : h \in H, k \in K\}$. Kasu honetan, HgK koklase bikoitzak H-rekiko $|K : K \cup H^g|$ eskuin koklase ditu.
Koklase sinpleekin gertatzen den moduan, H eta K-rekiko bi koklase bikoitz berdinak dira, edo bestalde disjuntuak.

Definizioa. Izan bitez G taldea eta x, g G-ko bi elementu. Orduan, x-ren konjokatua g-ren bidez $g^{-1}xg$ elementuari deitzen zaio, eta x^g bidez denotatzen da. Nabaria da G talde abeldar batean $x^g = x$ dela, edozein $x, g \in G$ elementutarako.

Definizioa. Izan bitez G taldea eta $N \leq G$. Orduan, N, G-n azpitalde normala dela esaten dugu, ondoko baliokideak diren baldintzaren bat betetzen denean:

(i) $gN = Ng$ da, $g \in G$ guztietarako.

(ii) $N^g = N$ da, $g \in G$ guztietarako.

(iii) $n^g \in N$ da, $n \in N$ eta $g \in G$ guztietarako.

Kasu honetan, $N \trianglelefteq G$ bidez adierazten da.

Bereziki, G talde ez tribial baten azpitalde normal bakarrak tribiala eta talde bera direnean, G taldea *talde sinplea edo bakuna* dela esaten da.

Ondoren, aipagarria da aztertzea noiz H,$K \leq G$ izanik, HK azpitaldeen biderkadura ere G-ren azpitaldea den. Erraz froga daiteke horietariko bat G-n normala denean, horien biderkadura G-ko azpitaldea dela. Hurrengo galdera logikoa izan daiteke: jakinda HK, G-ko azpitaldea dela, noiz ziurta genezake biderkadura hori ere G-n normala den. Bereziki, baldin eta H eta K azpitalde biak, G-n azpitalde normalak badira, orduan HK ere G-n azpitalde normala da.

Definizioa. Izan bitez G taldea eta $N \trianglelefteq G$. Orduan, N-rekiko koklaseen multzoan $(gN)(g'N) = (gg')N$ eragiketa definituz gero, N-rekiko koklaseen multzoak talde egitura du eta talde berri hori G/N bidez denotatzen dena, G-ren zatidura taldea deitzen da. Bereziki, N azpitalde normala izateagatik, $G/N = \{gN : g \in G\} = \{Ng : g \in G\}$ da. Bestalde, G-ren zatidura taldearen ordena, G-n N azpitalde normalaren indizea da, hau da $|G/N| = |G : N|$.

Ohartu, N, G-ren azpitalde normala denean, $gN = Ng$ koklasea adierazteko $\bar{g}$ ikurra erabiliko dugula. Honela, $G/N = \{\bar{g} : g \in G\}$ da, eta eragiketa $\overline{g_1}\ \overline{g_2} = \overline{g_1 g_2}$ bidez adieraziko dugu. Gainera, $\overline{g_1} = \overline{g_2}$ dugu baldin eta soilik baldin g_1 eta g_2 elementuetakoren bat bestearen alderantzizkoagatik biderkatzean (biderketa edozein ordenatan eginda) N-ko elementua bada.

Proposizioa 1.4. *Izan bedi $N \trianglelefteq G$. Orduan, zentzu batean, N eta G/N bi taldeetatik G talde osoa eraiki dezakegu. Bereziki, G finitua bada, orduan N eta G/N ere finituak dira, eta $|G| = |N||G/N|$ da.*

Proposizioa 1.5. *Izan bedi $H \leq G$ non H ordena finitu zehatz bateko G-ren azpitalde bakarra den. Orduan, $H \trianglelefteq G$ da.*

Proposizioa 1.6. *Izan bedi $H \leq G$ non $|G : H| = 2$ den. Orduan, $H \trianglelefteq G$ da.*

Teorema 1.7 (Isomorfismoaren Bigarren Teorema)**.** *Izan bitez $H \leq G$ eta $K \trianglelefteq G$. Orduan, $H \cap K \trianglelefteq H$ eta $H/(H \cap K) \cong HK/K$ dira.*

Definizioak. Izan bitez G taldea eta $H \subseteq G$.

(i) Baldin eta $H \leq G$ eta $H \neq G$ badira, H, G-ren azpitalde propioa dela esaten da, eta $H < G$ bidez adierazten da.

(ii) Baldin eta $H < G$ bada, H, G-n azpitalde maximala dela esaten dugu, $H \leq L \leq G$ adierazpenetik $L = H$ edo $L = G$ ondorioztatzen bada, L guztietarako. Beste era batera esanda, H, G-ko azpitalde propioa G-n maximala da, ezin badaiteke L azpitalderik aurkitu non $H < L < G$ den.

Definizioa. Izan bedi $H \leq G$. Orduan, H azpitaldea G-n *karakteristikoa* dela diogu eta $H \operatorname{char} G$ bidez denotatuko da, G-ren edozein α automorfismorentzako $\alpha(H) = H$ denean.

Ohartu, aurreko definizioan, H, G-ko automorfismo guztien bitartez inbariantea gelditzeak ez duela esan nahi $\alpha(h) = h$ denik, $h \in H$ elementu guztietarako; baizik eta $\alpha(h)$ berriro ere H-ko elementu bat dela eta ez derrigorrez h elementu bera.

Jakina da, $N \trianglelefteq H \trianglelefteq G$ adierazpenetik, ezin dugula ziurtatu $N \trianglelefteq G$ denik, hau da, normaltasunak ez duela iragankortasun propietatea betetzen. Baina, aldiz, baldin eta honez gain $N \operatorname{char} H$ bada, orduan emaitza bete egiten da. Hau da, $N \operatorname{char} H \trianglelefteq G$ erlaziotik, $N \trianglelefteq G$ ondorioztatzen da.

Definizioak. Izan bitez G taldea eta $X \subseteq G$ azpimultzo bat. Orduan, G-ren azpitaldeak diren ondoko azpitalde berriak definitzen dira:

(i) G-n X-ren normalizatzailea,

$$N_G(X) = \{g \in G : X^g = X\} = \{g \in G : x^g \in X, x \in X \text{ guztietarako}\}.$$

(ii) G-n X-ren zentralizatzailea,

$$\begin{aligned} C_G(X) &= \{g \in G : x^g = x, x \in X \text{ guztietarako}\} \\ &= \{g \in G : xg = gx, x \in X \text{ guztietarako}\}. \end{aligned}$$

(iii) G-ren zentrua,

$$Z(G) = \{g \in G : gg' = g'g,\ g' \in G \text{ guztietarako}\}.$$

Nabaria da $C_G(X) \subseteq N_G(X)$ dela eta $X = \{x\}$ kasu berezian, $N_G(x) = C_G(x)$ dugu. Honez gain, $N_G(G) = G$ eta $C_G(G) = Z(G)$ direnez, $N_G(G) = C_G(G)$ berdintza bakarrik betetzen da, G talde abeldarra denean. Bestalde, baldin eta $H \leq G$ bada, $H \trianglelefteq N_G(H)$ da. Are gehiago, $N_G(H)$, H normalizatzen duen G-ren azpitalderik handiena da.

Proposizioa 1.8. *Baldin eta $K \trianglelefteq G$ eta $|K| = 2$ badira, orduan $K \leq Z(G)$ da.*

1.2 Biderkadura zuzenak eta erdizuzenak

Ondoren talde batzuk eskura izanik gure helburua, talde berri handiagoak eraikitzen saiatzea izango da. Honela justifikatuko dugu emandako talde batzuen biderkadura zuzenak, erdizuzenak, etab.

Emanda X eta Y edozein bi multzo, horien biderkadura cartesiarra, $X \times Y$ deituko duguna, $\{(x, y) : x \in X, y \in Y\}$ bidez definitzen da, hau da, (x, y) bikote ordenatu guztien multzoa da, $x \in X$ eta $y \in Y$ izanik. Azter dezagun zer gertatzen den X eta Y, G talde baten azpitaldeak direnean.

Dakigunez, H eta N bi edozein talde emanda, beren biderkadura zuzena $H \times N$ eraiki dezakegu: elementuak (h, n) bikoteak dira eta eragiketa osagaiz osagai egiten da. Oso erraza da $H \times N$-ren barruan H-ren eta N-ren kopia

bana aurkitzea: $H^* = H \times \{1\} = \{(h,1) : h \in H\}$ eta $N^* = \{1\} \times N = \{(1,n) : n \in N\}$ multzoak $H \times N$-ren azpitaldeak dira, eta garbi dago $H^* \cong H$ eta $N^* \cong N$ betetzen dela $(h,1) \to h$ eta $(1,n) \to n$ aplikazioen bitartez. Gainera, H^* eta N^*, $H \times N$-ren azpitalde normalak dira, $H^* \cap N^*$ azpitalde tribiala da eta $H^*N^* = H \times N$ dugu.

Oharra. Hemendik aurrera biderkadura cartesiarrari kanpoko biderkadura zuzena esango zaio.

Definizioa. Demagun G taldeak H eta N bi azpitalde dituela. Orduan, G taldea H eta N azpitaldeen barruko biderkadura zuzena dela esaten da, ondoko hiru baldintzak betetzen badira:

(i) $H, N \trianglelefteq G$, hau da, H eta N azpitaldeak G-n normalak dira.

(ii) $H \cap N = \{1\}$.

(iii) $G = HN$.

Kasu honetan, $G = H \times N$ idazten dugu.

Teorema 1.9. *Izan bitez H eta N bi talde. Orduan, $H \times N$ kanpoko biderkadura zuzena $H^* = \{(h,1) : h \in H\}$ eta $N^* = \{(1,n) : n \in N\}$ azpitaldeen barruko biderkadura zuzena da, eta azpitalde hauek H-ren eta N-ren isomorfoak dira, hain zuzen ere.*

Teorema 1.10. *Demagun G taldea H eta N azpitaldeen barruko biderkadura zuzena dela. Orduan:*

(i) *$G = \{hn : h \in H, n \in N\}$, errepikapenik gabe.*

(ii) *H-ko elementuak N-koekin trukatzen dira eta, beraz, h_1n_1 eta h_2n_2, G-ko bi elementu orokorren biderkadura honela egiten da: $(h_1n_1)(h_2n_2) = (h_1h_2)(n_1n_2)$.*

Ondorioz, $hn \to (h,n)$ erregelaren bitartez definituta dagoen $f\colon G \to H \times N$ aplikazioa talde isomorfismoa da. Hau da, G taldea H-ren eta N-ren kanpoko biderkadura zuzenaren isomorfoa da.

Aurreko guztiaren frogapenak detailera aztertuz kontura gaitezke barruko biderkadura zuzenaren definiziotik baldintza bat kendu ahal dugula, H-ren normaltasuna hain zuzen ere, eta oraindik ere G taldea guztiz deskribatzeko gai izango garela. Hau ikusirik, ondorengo definizioa ematen dugu.

Definizioa. Izan bitez H eta N, G-ren bi azpitalde. Orduan, G taldea H eta N azpitaldeen barruko biderkadura erdizuzena da, ondoko hiru baldintzak betetzen badira:

(i) $N \trianglelefteq G$.

(ii) $H \cap N = \{1\}$.

(iii) $G = HN$.

Kasu honetan, $G = H[N]$ idazten dugu.

Teorema 1.11. *Izan bedi $G = H[N]$ barruko biderkadura erdizuzena. Orduan, hurrengoak betetzen dira:*

(i) *$G = \{hn : h \in H, n \in N\}$ da, errepikapenik gabe.*

(ii) *Aurreko moduan idatzitako G-ko bi elementuen biderketa $(h_1n_1)(h_2n_2) = h_1h_2n_1^{h_2}n_2$ formula bidez emanda dago.*

Froga. (i) Erraza da G taldea, barruko biderkadura erdizuzena izanik, teoremako (ii) ataletik $h_1h_2n_1^{h_2}n_2$ elementua G-koa dela ikustea. Izan ere, $n_1^{h_2} \in N$ da, N azpitalde normala baita. Beraz, $h_1h_2 \in H$ eta $n_1^{h_2}n_2 \in N$ dira. Bestalde, $h_1n_1 = h_2n_2$ bada, $h_2^{-1}h_1n_1 = n_2$ da. Hortaz, $h_2^{-1}h_1 = n_2n_1^{-1}$, non ezkerreko aldeko gaia H-koa den eta eskuinekoa, aldiz, N-koa. Nola $H \cap N = \{1\}$ eta $h_2^{-1}h_1 \in H \cap N$ eta $n_2n_1^{-1} \in H \cap N$ diren, $h_2^{-1}h_1 = 1$ eta $n_2n_1^{-1} = 1$ direla ondorioztatzen da, eta ondorioz $h_2 = h_1$ eta $n_2 = n_1$ dira, hau da, $G = \{hn : h \in H, n \in N\}$-n ez dago errepikapenik. □

Teorema 1.12. *Izan bitez H eta N bi talde eta $\theta\colon H \to \mathrm{Aut}(N)$ talde homomorfismo bat. Orduan,*

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, [\theta(h_2)](n_1)n_2)$$

eragiketak talde egitura ematen dio $H \times N$ biderkadura cartesiarrari. Talde honetan, elementu neutroa $(1, 1)$ bikotea da eta (h, n)-ren alderantzizkoa $(h^{-1}, [\theta(h^{-1})](n^{-1}))$ da.

Definizioa. Aurreko teoremaren baldintzetan bagaude, lortzen dugun taldeari θ-rekiko H-ren eta N-ren kanpoko biderkadura erdizuzena deritzogu eta $H \ltimes_\theta N$ edo $N \rtimes_\theta H$ ikurren bitartez adierazten dugu. (Batzuetan $H[N]_\theta$ notazioa ere erabiltzen da.) Gainera, θ-ri H-ren N gaineko ekintza deitzen diogu.

1.3 Finituki sortuak diren talde abeldarren egitura teorema

Finituki sortuak diren talde abeldarren egitura teorema aztertu baino lehen gogora ditzagun erraz froga daitezkeen ondoko bi emaitzak,

Teorema 1.13. *Izan bitez G taldea eta $G_1, G_2, \ldots, G_n$ emandako G taldearen n azpitalde, n zenbaki oso positiboa izanik. Orduan baliokideak dira ondoko hiru baieztapenak:*

(i) $G = \mathrm{Dr}\prod_{i=1}^{n} G_i$ *(biderkadura zuzena).*

(ii) *Edozein G-ko g elementuk $g = g_1 g_2 \dots g_n$ adierazpen bakarra onartzen du, $g_i \in G_i$ izanik, $i \in \{1, \dots, n\}$ balio guztietarako.*

(iii) $G = \prod_{i=1}^{n} G_i$ *eta edozein $1 < m \leq n$ baliotarako*

$$\Big(\prod_{i=1}^{m-1} G_i\Big) \cap G_m = 1.$$

Lema 1.14. *Izan bedi H finituki sortua den talde abeldarra. Demagun $\{x_1, x_2, \dots, x_s\}$ talde honen sistema sortzaile bat dela, s zenbaki oso positiboa izanik. Izan bitez ere, $m_1, m_2, \dots, m_s$ zenbaki oso ez negatiboak, ez guztiak aldi berean nuluak, eta $\mathrm{zkh}(m_1, m_2, \dots, m_s) = 1$ baldintza betetzen dutelarik. Orduan, existitzen da H-ren $\{y_1, y_2, \dots, y_s\}$ beste sistema sortzaile bat zeinentzat $y_1 = \prod_{i=1}^{s} x_i^{m_i}$ den.*

Teorema 1.15. Finituki sortuak diren talde abeldarren egitura teorema. *Izan bitez r zenbaki oso positiboa, eta G taldea r sortzaileez sortua den talde abeldarra (edo r-sortua den talde abeldarra). Orduan existitzen dira G-n, $x_1, x_2, \dots, x_r$ elementuak zeinentzat*

$$G = \mathrm{Dr}\prod_{i=1}^{r}\langle x_i\rangle = \langle x_1\rangle \times \langle x_2\rangle \times \ldots \times \langle x_r\rangle$$

moduan adieraz daitekeen. Hau da, G taldea azpitalde zikliko zehatz batzuen biderkadura zuzen gisa deskonposa daiteke.

Froga. Baldin eta $r = 1$ bada, G talde ziklikoa da eta ez dago ezer frogatzeko. Demagun orain $r > 1$ dela. Kontsidera dezagun, G-ko elementuetaz osatutako $(x_1, x_2, ..., x_r)$ r-koteek, aldi berean,

$$o(x_1) \leq o(x_2) \leq \ldots \leq o(x_r)$$

eta $G = \langle x_1, x_2, \dots, x_r\rangle$ baldintzak betetzen dituzten multzo ordenatu guztien $\mathfrak{R}$ multzoa. (Ohartu aurreko eraikuntzan $x_1, x_2, \dots, x_r$ elementuak ez direla zertan desberdinak izan behar, eta goian aipatutako desberdintzan ∞ "zenbakia" edozein zenbaki oso positibo baino handiagoa dela suposa daiketeela.) Argi dago, G-ren edozein r-sistema sortzaile ordena daitekeela, agian modu batetan baino gehiagotan, eta hemendik r-sistema sortzaile hori $\mathfrak{R}$ -ko elementua dela ondorioztatzen da. Bereziki $\mathfrak{R} \neq \emptyset$ dugu.

Orain G-ko elementuen ordenetan minimaltasun baldintza batzuk betetzen duen $\mathfrak{R}$-ko elementu bat aukeratzen dugu. Hain zuzen ere, $\mathfrak{R}$-ko $(x_1, \ldots, x_r)$ elementu guztietarako, finka dezagun N_1, $o(x_1)$ guztien baliorik txikiena (ohartu N_1 zenbakia osoa eta positiboa, edo infinitua izan daitekeela). Ondoren, $o(x_1) = N_1$ baldintza betetzen duten $\mathfrak{R}$-ko $(x_1, \ldots, x_r)$ elementu guztien artean, finka dezagun N_2, $o(x_2)$ guztien baliorik txikiena. Eta modu berdinean, $N_1 = o(x_1)$ eta $N_2 = o(x_2)$ baldintzak betetzen dituzten $\mathfrak{R}$-ko $(x_1, \ldots, x_r)$ elementu guztien artean, finka dezagun N_3, $o(x_3)$ guztien baliorik txikiena. Modu berdinean, ondoz ondoren jarraituz, aukera genezake $\mathfrak{R}$-ko $(x_1, \ldots, x_r)$ elementu bat zeinentzat $o(x_i) = N_i$ den, edozein $i \in \{1, \ldots, r\}$ baliotarako. Orduan, G-ko aukeratutako $\{x_1, \ldots, x_r\}$ r-sistema sortzaileak ondoko propietatea betetzen du: baldin eta $\{y_1, \ldots, y_r\}$ G-ren beste r-sistema sortzailea eta j zenbaki oso positiboa badira, non $j > 1$ eta $i < j$ diren kasuetarako $o(x_i) = o(y_i)$ betetzen den, orduan hasieran emandako r-sistema sortzaileak edozein $i \geq j$ balioetarako, $o(x_j) \leq o(y_i)$ beteko du.

Bestalde G talde abeldarra denez, nabaria da G-ko edozein elementuk $\prod_{i=1}^{r} x_i^{n_i}$ adierazpena onartzen duela, egokiak diren n_i zenbaki osoentzako eta hau, edozein $i \in \{1, \ldots, r\}$ baliotarako. Honez gain, edozein $i \in \{1, \ldots, r\}$ baliotarako, $\langle x_i \rangle \trianglelefteq G$ dugu. Beraz, $G = \prod_{i=1}^{r} \langle x_i \rangle$ betetzen da. Ondoren, froga dezagun aurreko biderketa, benetan biderkadura zuzen bat dela, hau da, $G = \mathrm{Dr} \prod_{i=1}^{r} \langle x_i \rangle$ dela. Argudioa absurdura eramanez egingo dugu. Arinago aipatutako 1.13 Teoremagatik horrek esan nahi du, behintzat existitzen direla zenbaki oso batzuk $n_1, \ldots, n_r$ zeintzuentzat,

$$\textstyle\prod_{i=1}^{r} x_i^{n_i} = 1 \text{ eta } x_i^{n_i} \neq 1 \text{ diren, } i\text{-ren balioren batetarako.}$$

Orokortasuna galdu gabe suposa genezake $n_1, \ldots, n_r$ zenbaki guztiak ez negatiboak direla: baldin eta $n_j < 0$ balitz, nahikoa izango litzateke aurreko argudioan, x_j elementua x_j^{-1}-gatik eta n_j zenbakia $-n_j$-gatik ordezkatzea (ohartu $o(x_j^{-1}) = o(x_j)$ berdintza betetzen denez, aipatutako ordezkapenek ez dituztela arinago definitutako propietateak aldatzen). Defini ditzagun orain, ondoko $l_1, \ldots, l_r$ zenbaki osoak, zeintzurentzat $0 \leq l_i < o(x_i)$ eta $x_i^{l_i} = x_i^{n_i}$, edozein $i \in \{1, \ldots, r\}$ baliotarako. Aipatutako zenbaki osoen existentzia ziurtatuta dago ondoko argudioagatik: **(i)** baldin eta $o(x_i) < \infty$ bada, orduan zatiketaren algoritmoa erabiliz existitzen dira q_i eta s_i zenbaki osoak, non $n_i = q_i o(x_i) + s_i$ eta $0 \leq s_i < o(x_i)$ diren. Hau da, $x_i^{n_i} = x_i^{s_i}$ eta $l_i = s_i$ eran definitzen da. **(ii)** Bestalde, baldin eta $o(x_i) = \infty$ bada, $l_i = n_i$ eran definitzen dugu (ohartu orain n_i zenbaki ez negatiboa dela erabiltzen

dugula).

Baina hasieratik suposatu dugu i indizeren batetarako $x_i^{n_i} \neq 1$ eta $l_i > 0$ direla. Izan bedi j zenbaki oso positibo txikiena non $l_j > 0$ den. Honela, $j > 1$ bada, $l_k = 0$ da edozein $k < j$-rako.

Orain, izan bitez $d = \text{zkh}(l_1, l_2, \ldots, l_r)$ eta edozein $i \in \{1, \ldots, r\}$ baliotarako $m_i = \frac{l_i}{d}$. Orduan, $m_1, m_2, \ldots, m_r$ zenbaki oso ez negatiboak dira non $\text{zkh}(m_1, \ldots, m_r) = 1$ den. Gainera, $l_i = 0$ direnez $i < j$ guztietarako, $m_i = 0$ da $i < j$ guztietarako. Ondorioz, $\text{zkh}(m_j, m_{j+1}, \ldots, m_r) = 1$ da $i < j$ guztietarako.

Izan bedi $H = \langle x_j, x_{j+1}, \ldots, x_r \rangle$, G talde abeldarraren azpitaldea. Bereziki H talde abeldarra finituki sortua da. Orain, 1.14 Lemaren emaitza erabiliz, jakina da existitzen dela H-ren sortzaileen beste multzo bat $\{y_j, y_{j+1}, \ldots, y_r\}$ non $y_j = \prod_{i=j}^{r} x_i^{m_i}$ den, m_i balio batzuentzako. Honela, $y_j^d = \prod_{i=j}^{r} x_i^{m_i d} = \prod_{i=j}^{r} x_i^{l_i}$ da. Gainera, $l_i = 0$ direnez $i < j$ balioetarako, $y_j^d = \prod_{i=1}^{r} x_i^{l_i}$ da. Orain, $l_1, \ldots, l_r$ definitu ditugun modua kontuan harturik, $y_j^d = \prod_{i=1}^{r} x_i^{n_i} = 1$ da. Baina, orain $G = \langle x_1, \ldots, x_{j-1}, y_j, y_{j+1}, \ldots, y_r \rangle$ eta $o(y_j) \leq d \leq l_j < o(x_j)$ dira, eta hauxe $(x_1, x_2 \ldots, x_r)$-ren aukeraren kontrakoa da. Beraz, $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \ldots \times \langle x_r \rangle$ dela ondorioztatzen dugu. □

2. Kapitulua

Sylow-en Teoremak

2.1 p-talde finituak eta Sylow-en Teoremak

Atal honetan zehar ordena finituko taldeekin lan egingo da. Lehenengo eta behin kontzeptu batzuk definitu behar dira, Sylow-en Teoremetara heldu baino lehen.

Definizioa. Talde bat p-taldea dela deritzogu baldin eta bere ordena p^a bada, $a \geq 0$ batentzako, p zenbaki lehena izanik. Gainera, baldin eta p-talde bat G talde baten barnean badago, orduan G-ren p-azpitaldea dela deritzogu.

Gainera, p-taldeei buruzko emaitza garrantzitsu bat ondokoa da: p-talde ez tribialen zentrua beti dela ez-tribiala.

Definizioa. Izan bitez G talde finitua eta p zenbaki lehena. Idatz dezagun $|G| = p^a \cdot m$, $a \geq 0$ eta, p eta m elkarrekiko lehenak izanik. Orduan, P, G-ren Sylow-en p-azpitaldea edo p-Sylow-en azpitaldea da baldin eta ordena maximoko G-ren p-azpitaldea bada. Hau da, $P \leq G$ non $|P| = p^a$ bada.

Beste era batera esanda, $P \leq G$, G-ren Sylow-en p-azpitaldea da baldin eta soilik baldin P, p-taldea bada eta, $|G : P|$ eta p elkarrekiko lehenak badira.

Hemendik aurrera, notazioa arintzeko, p zenbaki lehen batentzako, P azpitaldea G taldearen Sylow-en p-azpitaldea denean, $P \in \mathrm{Syl}_p(G)$ idatziko dugu. Hau da, $\mathrm{Syl}_p(G)$ multzoak G-ren p-Sylow-en azpitaldeen multzoa adierazten du. Gainera, $\nu_p(G)$ erabiliko da, $\mathrm{Syl}_p(G)$ multzo horren ordena adierazteko, hau da, $\nu_p(G) = |\mathrm{Syl}_p(G)|$.

Ohartu, n ordenako mota desberdinetako ez-isomorfoak diren taldeen kopurua adierazteko $v(n)$ erabiltzen dela. Aldiz, kasu honetan, ν letra grekoa erabiltzen da.

Orain, Sylow-en teoremak enuntziatuko dira, hauek talde finituen teoriako teorema garrantzitsuenetarikoak baitira, baina ez dugu orokorki frogapenik emango. Nahi izanez gero irakurleak Talde Teoriako Oinarrizko edozein liburutan aurki ditzake frogapen horiek. Esandakoaren arabera, Sylow-en Teoremak frogatzea ez da gure helburua, baina edozein kasutan ere emaitza batzuk azpimarratuko ditugu.

Teorema 2.1 (Sylow-en Teoremak)**.** *Izan bitez G talde finitua eta p zenbaki lehen bat non $|G| = p^a \cdot m$ den, $a \geq 0$ eta $\text{zkh}(p, m) = 1$ izanik. Orduan, hurrengo lau baieztapenak betetzen dira:*

(i) *G taldeak p-Sylow-en azpitalde bat du. (Sylow-en 1go Teorema)*

(ii) *Edozein bi p-Sylow-en azpitalde konjokatuak dira G-n.*

(iii) *$P \in \text{Syl}_p(G)$ eta Q, G-ren edozein p-azpitalde izanda, existitzen da $g \in G$ non $Q \leq P^g$ den, hau da, G-ren p-azpitalde guztiak G-ren p-Sylow-en azpitalderen batetan sartuta daude. (Sylow-en 2garren Teorema)*

(iv) *Baldin eta $P \in \text{Syl}_p(G)$ bada, $\nu_p(G) = |G : N_G(P)|$ da. Bestalde, $\nu_p(G)$-k, $|G|$ zatitzen du eta $\nu_p(G)$ batarekin kongruentea da modulo p. Hau da, $\nu_p(G) \Big| |G|$ eta $\nu_p(G) \equiv 1 \pmod{p}$. (Sylow-en 3garren Teorema)*

(Aurreko Sylow-en Teoremako (iv) atalean $\nu_p(G) \Big| |G|$ baldintza baino askoz gogorragoa den beste hau dugu: $\nu_p(G)$-k, m zatitzen du, hau da, $\nu_p(G)|m$.)

Aipatzekoa da ondorengo Cauchy-ren emaitza garrantzitsua. Izan bitez G talde finitua eta p zenbaki lehena. Orduan, p-k $|G|$ zatitzen badu, G-k p ordenako elementua du: hartu G talde finitua. Hipotesiagatik, $p \Big| |G|$ betetzen denez, idatz dezagun $|G| = p^a \cdot m$ non $a \geq 1$ eta $(p, m) = 1$ diren. Izan bedi P, G-ren p-Sylow-ren bat (bere existentzia ziurtatuta dago Sylow-en 1go Teoremagatik), hau da, $|P| = p^a \neq 1$. Orduan, $P \neq \{1\}$ eta argi dago $\forall x \in P \setminus \{1\}$ elementurentzat $o(x) \Big| |P| = p^a$ eta $o(x) \neq 1$ direla. Orduan, idatz dezagun $o(x) = p^b$ non $0 < b \leq a$. Honela, $o(x^{p^{b-1}}) = \frac{o(x)}{(o(x), p^{b-1})} = \frac{p^b}{(p^b, p^{b-1})} = \frac{p^b}{p^{b-1}} = p$. Beraz, $x^{p^{b-1}}$, p ordenako elementua da G-n.

Kontuan hartu emaitza honek A Eranskineko 5garren eta 6garren ariketetako baieztapenak orokortzen dituela.

Proposizioa 2.2. *Izan bedi G, n ordeneko talde finitua. Orduan, n zatitzen duen p^m, p-ren berretura bakoitzeko, p lehena izanik, G-k badu p^m ordenako azpitalde bat.*

Orain, galdera logikoa Sylow-en p-azpitalde desberdinen kopurua noiz den bakarra izan daiteke. Galdera honen erantzuna hurrengo emaitzak emango digu: izan bitez G talde finitua, p zenbaki lehena eta $P \in \mathrm{Syl}_p(G)$. Orduan, $\nu_p(G) = 1$ da baldin eta soilik baldin $P \trianglelefteq G$ bada.

Orain, $P \in \mathrm{Syl}_p(G)$ hartuta, P eta G talde osoan bere normalizatzailearen artean zein erlazio dagoen pentsa dezakegu. Jadanik jakina da, $N_G(P)$, P normalizatzen duen G-ren azpialderik handiena dela. Hori da hurrengo lematik ondorioztatzen dena.

Lema 2.3. *Demagun G talde finitua, p zenbaki lehena eta $P \in \mathrm{Syl}_p(G)$ direla. Orduan, P, $N_G(P)$-ren p-Sylow-en azpitalde bakarra da. Beraz, $P \trianglelefteq N_G(P)$ da.*

Teorema 2.4 (G. Frattini)**.** *Baldin eta N, G talde finituaren azpitalde normala bada eta P, N-ren p-Sylow-ren bat bada, hau da, $P \in \mathrm{Syl}_p(N)$, orduan $G = N_G(P)N$ betetzen da.*

Korolarioa 2.5. *Izan bitez G talde finitua eta $P \in \mathrm{Syl}_p(G)$. Orduan, $N_G(P)$ barruan duen G-ren edozein H azpitalderentzat, $N_G(H) = H$ da.*

Lema 2.6. *Izan bitez G taldea eta $P \in \mathrm{Syl}_p(G)$. Orduan, G-ren edozein K azpitalderentzako, existitzen da $x \in G$ elementua non $K \cap P^x \in \mathrm{Syl}_p(K)$ den.*

Teorema 2.7. *Izan bedi G talde finitua, p zenbaki lehena eta $N \trianglelefteq G$. Orduan:*

(i) $\mathrm{Syl}_p(N) = \{P \cap N : P \in \mathrm{Syl}_p(G)\}$.

(ii) $\mathrm{Syl}_p(G/N) = \{PN/N : P \in \mathrm{Syl}_p(G)\}$.

Teorema 2.8. *Izan bitez G tribiala ez den talde finitua, eta $p_1, \ldots, p_s$ $|G|$-ren zatitzaile lehen desberdin guztiak, $s \geq 1$ izanik. Demagun $i = 1, \ldots, s$ bakoitzerako, G-k, P_i, p_i-Sylow normal bat duela. Orduan, $G = P_1 \times P_2 \times \cdots \times P_s = \mathrm{Dr}\prod_{i=1}^{s} P_i$ da.*

2.2 Sylow-en Teoremen aplikazio bat

Sylow-en Teoremak garrantzi handikoak dira talde teoria finituan eta horien aplikazio ugari ezagutzen dira. Ondoren, Sylow-en Teoremen aplikazio zehatz batekin arituko gara. Aipatutako aplikazioa garatu baino lehen, erraz froga daitezkeen hiru emaitza gogoratuko ditugu.

Emaitzak. (i) Nabaria da G talde batetan edozein a eta b elementuk elkar trukatzen badira, eta horien ordenak ondoz ondoko n eta m badira, orduan ab elementuaren ordena nm zenbakiaren zatitzailea dela. Gainera, n eta m elkarrekiko lehenak badira, $o(ab) = nm$ dugu.

(ii) p zenbaki lehena izanik, p^2 ordenako edozein talde, abeldarra da.

(iii) Baldin eta G talde baten H eta K bi azpitaldek, $H \cap K = 1$, $H \subseteq N_G(K)$ eta $K \subseteq N_G(H)$ baldintzak betetzen badituzte, orduan H-ko edozein elementu K-ko edozein elementurekin trukatzen da.

Nahiz eta talde ebazgarriaren definizioa Laugarren Kapituluan garatuko dugun, gogora dezagun orain bere oinarrizko esanahia ondoko aplikazioa ondo ulertzeko: G talde bat ebazgarria dela esaten da existitzen baldin bada G-ren serie (subnormal) abeldar bat, hau da, existitzen bada $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ non G_{i-1}/G_i konposizio faktoreak abeldarrak diren, edozein $i = 1, \ldots, n$-rentzako.

Aplikazioa. Izan bitez p eta q bi zenbaki lehen. Orduan, pq ordenako G taldea, ebazgarria da. Gainera frogapen honen arabera G taldeari buruzko propietate interesgarri batzuk lortuko ditugu.

Froga. Baldin eta $p = q$ bada, arinago aipatutako emaitzetatik taldea abeldarra dela ondorioztatzen da, eta beraz ebazgarria. Orduan, orokortasuna galdu gabe, demagun adibidez $p > q$ dela. Orain, Sylow-en Teoremetatik G taldearen Sylow-en p-azpitaldeen kopurua, hau da, $\nu_p(G)$, G taldearen ordenaren zatitzailea izan behar da, eta aldi berean, $\nu_p(G) \equiv 1 \pmod{p}$, edo beste modu batera esanda, $\nu_p(G) = 1 + kp$ motatakoa izan behar da, $k \geq 0$ zenbaki osoa izanik. Ondorioz, aukera bakarra $\nu_p(G) = 1$ da, eta hemendik, G-n p-Sylow bakarra dagoela, eta orduan hori bera G-n normala dela lortzen da. Dei diezaiogun G-ko p-Sylow horri P. Gainera, P-ren ordena derrigorrez p izan behar du, eta hemendik P ziklikoa dela ondorioztatzen da. Azkenik, kontuan harturik ondoko G-ren konposizio seriea $1 \trianglelefteq P \trianglelefteq G$, non bere konposizio faktoreak G/P eta $P/1$, ondoz ondoko q eta p ordenako talde ziklikoak diren, ohar gaitezke G taldea, pq ordenako talde ebazgarria dela. □

Ondoren eraikitako pq ordenako G talde ebazgarriaren ezaugarri gehiago aztertuko ditugu, $p \not\equiv 1 \pmod{q}$ edo $p \equiv 1 \pmod{q}$ baldintzapetan. Lehenik, suposa dezagun $p > q$ eta $p \not\equiv 1 \pmod{q}$ direla. Kasu honetan, Sylow-en 1go Teorema erabiliz, $\nu_q(G)$-k, $|G| = pq$-ren zatitzailea, eta bereziki p-ren zatitzailea izan behar duela ondorioztatzen da. Orduan, $\nu_q(G)$-ren aukerak 1 edo p dira, eta nola honez gain, $\nu_q(G) \equiv 1 (\mathrm{mod}\ q)$ izan behar duen, lortzen den aukera bakarra $\nu_q(G) = 1$ da. Dei diezaiogun G-ren q-Sylow horri Q. Lehen bezala argudiatuz, Q, G-n normala eta Q, q ordenako talde ziklikoa direla lortzen dugu. Orain arinago aipatutako (iii) emaitza aplikatzeko baldintzetan gaude, eta ondorioz G-ko p ordenako edozein elementu G-ko edozein q ordenako elementu batekin elkar trukatzen dela ondorioztatzen da. Beraz, bereziki P eta Q azpitaldeetako sortzaileak ere elkar trukatzen dira. Honez gain, aipatutako bi sortzaile horien biderketa, (i) emaitzagatik G-ko pq ordenako elementu bat da. Hau da, G taldea

pq ordenako talde ziklikoa dela lortu dugu.

Orain demagun $p \equiv 1 \pmod{q}$ eta $\nu_q(G) \neq 1$ baldintzapetan gaudela, hau da, demagun orain $\nu_q(G) = p$ dela. Gure helburua, behintzat pq ordenako talde ez abeldarren isomorfismo klaseren bat existitzen dela frogatzea da. Froga hau ondo ulertzeko oinarrizko zenbakizko teoriaren ondoko emaitzak kontuan hartu behar ditugu: p modulo hondar koklaseen multzoak (p zenbakiarekin elkarrekiko lehenak diren elementu zehatz batzuetaz osatutakoa) $p-1$ ordenako talde egitura du biderketarekiko, eta aipatutako talde hau, p elementuko gorputz finituaren, ziklikoa den $\mathbb{F}_p^*$ talde biderkakorraren isormorfoa da. Beraz, gure kasuan q zenbakiak $p-1$ zenbakia zatitzen duenez, existitzen dela r zenbaki oso bat zeinentzat $r \not\equiv 1 \pmod{p}$, baina $r^q \equiv 1 \pmod{p}$, ondorioztatzen da. Hemendik aurrera gure garapenean r hori finkatuta dugula suposatuko dugu. Bestalde, ohartu $x^q \equiv 1 \pmod{p}$ kongruentzia orokorrak zehatz-mehatz q emaitza desberdin dituela, eta horietariko emaitza bakoitza $\{1, r, r^2, \ldots, r^{q-1}\}$ multzoko zenbaki oso desberdin baten kongruentea dela.

Berriro ere gure egoerara bueltatuz, demagun G, pq ordenako talde ez abeldarra dela, $p \equiv 1 \pmod{q}$ izanik, eta finka ditzagun P, G-ren p-Sylow bakarra eta Q, G-ren q-Sylow-ren bat. Argi dago $PQ \leq G$ dela, $P \trianglelefteq G$ eta $Q \leq G$ direlako, eta baita $PQ = G$ dela, ezker eta eskuin aldeetan dauden bi taldeek ordena berdina dutelako. Bestalde, G-ko g elementu bakoitzak $g = uv$ biderkadura adierazpen bakarra onartzen du, $u \in P$ eta $v \in Q$ izanik. Baldin eta $x \in P - \{1\}$ eta $y \in Q - \{1\}$ badira, P, G-n normala izateagatik, orduan $x^y \in P - \{1\}$ dela ondorioztatzen da (ohartu $x^y \neq 1$ dela, zeren eta kontrako kasuan $xy = y1 = y$ litzateke eta hori $x \neq 1$-ren kontrakoa da). Beraz $x^y = x^a$ da, a zenbaki oso positiboren batentzat. Honez gain, x eta y ez direnez elkar trukatzen (ohartu G ez abeldarra eta G taldea x eta y elementuek sortutakoa dela), orduan $a \not\equiv 1 \pmod{p}$ ondorioztatzen da. Orain edozein n zenbaki osorentzat, $(x^a)^n = (x^y)^n = (x^n)^y = y^{-1}x^n y$, eta bereziki, $y^{-2}xy^2 = y^{-1}(x^y)y = (x^a)^y = x^{a^2}$. Orokorrean, $y^{-m}xy^m = x^b$ non $b = a^m$ den. Nola $y^q = 1$ den, argi dago y^q eta x elkar trukatzen direla, eta honek $a^q \equiv 1 \pmod{p}$ ondorioztatzen du. Hau da, a, $x^q \equiv 1 \pmod{p}$ kongruentziaren soluzio bat da. Orduan, $a \equiv r^c \pmod{p}$ da, $c \in \{0, 1, \ldots, q-1\}$ zenbaki osoren batentzako. Bestalde, existitzen da d zenbaki oso bat zeinentzat $cd \equiv 1 \pmod{q}$ den, eta ondorioz $a^d \equiv (r^{cd}) \equiv r \pmod{q}$ da.

Aurreko eztabaida ondoko eran laburbiltzen da. Izan bitez $P = \langle x \rangle$ eta $Q = \langle y \rangle$ non $y^{-1}xy = x^a$ den, $a \equiv r^c \pmod{q}$ izanik c-ren batentzako. Egokiro aukeratuz Q-ren sortzailea, orokortasuna galdu gabe suposa genezake $c = 1$ dela. Arinago aipatu den bezala, $r \not\equiv 1 \pmod{p}$ eta $r^q \equiv 1 \pmod{p}$ baldintzak betetzen dituen r zenbaki osoa finkatuta dago. Ondoren G-ko

edozein bi elementuren biderketa, $y^{-1}xy = x^r$ formulagatik guztiz zehaztuta dagoela frogatuko da. Nola G-ko edozein elementu $y^i x^j$ eran idatz daitekeen, $(y^i x^j)(y^k x^l) = y^i y^k y^{-k} x^j y^k x^l = y^{i+k}(x^j)^{y^k} x^l = y^{i+k}(x^{r^k})^j x^l = y^{i+k} x^{jr^k+l}$ dugu.

Azkenik r finkatuta dagoenez, goian aipatutako erlazioak, G-ko edozein bi elementuren biderketa, $x^p = y^q = 1$ eta $y^{-1}xy = x^r$ erlazioengandik guztiz zehaztuta dagoela adierazten du. Hain zuzen ere, erlazio horiek G-ko x eta y sortzaileen arteko *definizio erlazioak* deitzen dira.

3. Kapitulua

Talde nilpotenteak

3.1 Kommutadoreak eta azpitalde kommutadoreak

Jakina da taldea abeldarra denean, elementuen arteko operaketak erraz kalkula daitezkeela. Orokorrean, erabiltzen ditugun taldeak ez dute zertan abeldarrak izan behar, baina zentzuren batean zenbat urrundu gaitezkeen propietate horretatik neur daiteke.

Definizioa. Izan bitez G taldea eta $x, y \in G$ bi elementu. Orduan, x eta y-ren kommutadorea honela definitzen da:

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

Argi dago x eta y elkar trukatzen direla baldin eta soilik baldin x eta y-ren kommutadorea berdin 1 bada.

Bi elementuen kommutadorea ez ezik, elementu gehiagoen kommutadorea ere defini daiteke ondoko eran:

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

Hurrengo urratsa, azpitaldeen arteko kommutadorea definitzea izan daiteke. Izan bitez $H, K \leq G$ bi azpitalde. Orduan, bi azpitaldeen azpitalde kommutadorea ondoko eran definitzen da:

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

Ohartu, $[H, K]$ taldea G-ren azpitaldea dela.

Azpimarratzekoa da, H eta K azpitalde propioak hartu beharrean, G talde bera hartzen badugu, $[G, G]$ azpitalde kommutadorea eraiki dezakegula, G' bidez adierazten duguna. Bereziki, G', G-ren *azpitalde deribatua* deitzen da eta $G' = [G, G] = \langle [g_1, g_2] : g_1, g_2 \in G \rangle$ da.

Ondoren, kommutadorearen zenbait propietate enuntziatuko dira.

Teorema 3.1. *Izan bitez G taldea, $x, y, z \in G$ eta $H, K \leq G$.*

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

(ii) $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ *betetzen da,* $\sigma \colon G \longrightarrow G^* = G - \{0\}$ *edozein homomorfismorako.*

(iii) $[xy, z] = [x, z][x, z, y][y, z]$ *eta* $[x, yz] = [x, z][x, y][x, y, z]$.

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

(v) $\sigma([H, K]) = [\sigma(H), \sigma(K)]$ *betetzen da,* $\sigma \colon G \longrightarrow G^*$ *edozein homomorfismorako. Bereziki, G-ren edozein bi azpitalde karakteristikoen (edo normalen) azpitalde kommutadorea, karakteristikoa (edo normala) izaten jarraitzen du.*

(vi) *Baldin eta N, G-ren azpitalde normala bada, orduan* $[HN/N, KN/N] = [H, K]N/N$ *da.*

Froga. Lehenengo propietatea bi elementuen kommutadorearen definizioa erabiliz frogatzen da, $[y, x] = y^{-1}x^{-1}yx$ eta $[x, y] = x^{-1}y^{-1}xy$. Orduan, $[x, y]^{-1} = y^{-1}x^{-1}yx = [y, x]$ betetzen da.

Bigarren propietatearen kasuan, kommutadorearen definizioa eta σ homomorfismoa dela erabiliz,

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

dugu. Bestalde, $[\sigma(x), \sigma(y)] = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y)$ da, eta $[\sigma(x), \sigma(y)] = \sigma([x, y])$ berdintza begibistakoa da.

Hirugarrena frogatzeko, $[xy, z] = [x, z][x, z, y][y, z]$ erlazioa frogatuko dugu. Definizioak behin eta berriro, bi aldeetako gaiei aplikatuz berdintza lortzen dugu: $[xy, z] = (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz$ eta $[x, z][x, z, y][y, z]$
$= [x, z][[x, z], y][y, z] = (x^{-1}z^{-1}xz)([x, z]^{-1}y^{-1}[x, z]y)(y^{-1}z^{-1}yz)$
$= (x^{-1}z^{-1}xz)(z^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xzy)(y^{-1}z^{-1}yz) = y^{-1}x^{-1}z^{-1}xyz$.
Antzeko moduan froga daiteke $[x, yz] = [x, z][x, y][x, y, z]$ erlazioa.

Laugarren propietatearen kasuan, bi azpitaldeen azpitalde kommutadorearen definizioa aplikatuz eta (i) atala erabiliz, ohartu $[H, K] = \langle [h, k] : h \in H, k \in K \rangle = \langle [h, k]^{-1} : h \in H, k \in K \rangle = \langle [k, h] : h \in H, k \in K \rangle = [K, H]$ dela.

Orain, ohartu bosgarren propietatea bigarren propietatearen ondorioa dela.

Azkenik, seigarren propietatea ere berehalakoa da, bosgarren ataletik ondorioztatzen baita, $\sigma\colon G \longrightarrow G/N$ epimorfismo naturala erabiltzen badugu. □

3.2 Talde nilpotenteak

Orain G talde baten garrantzi handiko bi serie definituko ditugu.

Definizioa. Izan bedi G taldea. Orduan, G taldearen serie zentral beherakorra induktiboki ondoko eran definitzen da: $\gamma_1(G) = G$, eta $i \geq 2$ indizeetarako $\gamma_{i+1}(G) = [\gamma_i(G), G]$. (Ohartu, $\gamma_2(G) = G'$ dela, eta edozein i-rentzako $\gamma_i(G)$ azpitaldea G-n karakteristikoa dela, eta bereziki normala ere G-n.) Bestalde G taldearen serie zentral gorakorra errekurtsiboki ondoko eran definitzen da: $Z_0(G) = 1$ eta $i \geq 1$ indizeetarako $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. (Ohartu G-ren edozein H azpitalderentzat, $[H, G] \leq Z_i(G)$ dela baldin eta soilik baldin $H \leq Z_{i+1}(G)$ bada.)

Ondoren arinago aipatutako bi serien oinarrizko propietate batzuk ikusiko ditugu. Horretarako lehenago *Hiru Azpitaldeen Lema* izeneko emaitza gogoratuko dugu. Hain zuzen ere, edozein G talde eta $H, K, L \leq G$ eta $N \trianglelefteq G$ azpitalderentzat, $[H, K, L] \leq N$ eta $[K, L, H] \leq N$ betetzen baldin badira, orduan $[L, H, K]$ ere N-ren azpitaldea da.

Teorema 3.2. *Izan bedi G taldea, orduan $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ da.*

Froga. Froga i indizearen gaineko indukzioz garatzen da. Argi dago $i = 1$ kasuan, emaitza serie zentral beherakorraren definizioaren ondorio zuzena dela. Orain $i \geq 2$ diren kasuetan, $[\gamma_{i-1}(G), \gamma_j(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$ eta $[\gamma_j(G), G, \gamma_{i-1}(G)] = [\gamma_{j+1}(G), \gamma_{i-1}(G)] \leq \gamma_{i+j}(G)$ desberdintzak betetzen dira, teoreman frogatu beharreko emaitza $i-1$ kasuetarako egitzat suposatzen dugulako. Azkenik *Hiru Azpitaldeen Lema* aplikatuz, nahi genuen $[G, \gamma_{i-1}(G), \gamma_j(G)] = [\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ desberdintza lortzen da. □

Teorema 3.3. *Izan bitez G taldea eta N, G-ren azpitalde normala. Orduan, $\gamma_i(G/N) = \gamma_i(G)N/N$ betetzen da edozein $i \geq 1$ baliotarako. (Bereziki $i = 2$ denean, $\gamma_2(G/N) = \gamma_2(G)N/N = G'N/N$ dugu.)*

Froga. Emaitza 3.1 Teoremako (vi) atalaren ondorio zuzena da. □

Bereziki existitzen baldin bada c zenbaki arrunten bat zeinentzat $\gamma_{c+1}(G)$ talde tribiala den, hau da, $\gamma_{c+1}(G) = 1$ den, orduan G taldea *nilpotentea* dela esaten da, eta baldintza hori betetzen duen c-ren balio txikienari G taldearen *nilpotentzia klasea* deitzen zaio. Argi dago, $c = 1$ nilpotentzia klasea duten taldeak, hain zuzen ere, talde abeldarrak direla, eta zentzu batean talde nilpotente batean, zenbat eta nilpotentzia klasea altuagoa izan, orduan eta

urrunago dago taldea abeldarra izatetik.

Ondoren ikus dezagun nola karakteriza daitekeen ere, nilpotentea izatearen ezaugarria, taldeari dagokion serie zentral gorakorraren bidez.

Lema 3.4. *Izan bedi G, c nilpotentzia klaseko talde nilpotente bat. Orduan edozein $0 \leq i \leq c$ baliotarako, $\gamma_{c+1-i}(G) \leq Z_i(G)$ betetzen da.*

Froga. Froga i indizearean gaineko indukzioz garatzen da. Baldin eta $i = 0$ bada, orduan G-ren nilpotentzia klasea c denez, definizioz $\gamma_{c+1}(G) = 1 = Z_0(G)$ dugu, eta kasu honetan ($i = 0$ kasuan) emaitza betetzen da. Bestalde, $i \geq 1$ denean hipotesi induktiboa erabiliz, teoremaren emaitza $i - 1 \geq 0$ kasurako egia dela suposatuz, $\gamma_{c+1-(i-1)}(G) = \gamma_{c+1-i+1}(G) = [\gamma_{c+1-i}(G), G] \leq Z_{i-1}(G)$ dugu eta ondorioz, serie gorakorraren definizioan aipatutako ezaugarri bategatik $\gamma_{c+1-i} \leq Z_{(i-1)+1}(G) = Z_i(G)$ dugu, nahi genuen bezala. □

Teorema 3.5. *Izan bedi G taldea. Orduan G taldearen nilpotentzia klasea c da baldin eta soilik baldin $Z_c(G) = G$ eta $Z_{c-1}(G) \neq G$ badira.*

Froga. Lehenik eta behin, ohar gaitezen $Z_c(G) = G$ baldintzatik $\gamma_2(G) = [G, G] = [Z_c(G), G] \leq Z_{c-1}(G)$, eta $\gamma_3(G) \leq [Z_{c-1}(G), G] \leq Z_{c-2}(G)$ ondorioztatzen direla, eta baita $\gamma_{c+1}(G) \leq Z_0(G) = 1$ ere. Hau da, kasu honetan, G nilpotentea eta bere nilpotentzia klasea $\leq c$ direla lortzen da. Bestalde, aurreko 3.4 Lema erabilita, baldin eta G taldearen nilpotentzia klasea c bada, orduan $G = \gamma_1(G) \leq Z_c(G) \leq G$ dugu, eta ondorioz $Z_c(G) = G$. Orain teoremaren froga osoa, aurreko aipamen bi horiek kontuan hartzetik ondorioztatzen da. □

Beraz talde nilpotente baten nilpotentzia klasea bere serie zentral gorakorraren eta beherakorraren luzerekin bat dator. Azkenik, aipagarria den emaitza bat enuntziatuko dugu: edozein p-talde finitu talde nilpotentea da. Honen frogapena 3.5 Teoremaren, eta p-talde finitu ez-tribial baten zentrua beti talde ez tribiala izatearen ondorio zuzena da.

Lema 3.6. *Izan bedi $K \lhd G$ azpitalde normal propioa. Orduan, K, G-ren azpitalde maximala da baldin eta soilik baldin G/K ordena lehenekoa bada.*

Froga. Nola K azpitalde normal propioa den G-n, $|G/K| > 1$ da. Orain, K, G-ren azpitalde maximala da baldin eta soilik baldin G/K-k ez badu azpitalde propio ez tribialik. Eta aurrekoa gertatzen da baldin eta soilik baldin G/K orden leheneko taldea ziklikoa bada. □

Lehenengo Kapituluko definizio orokorren atalean azpitalde maximal baten definizioa eman dugu. Baldin eta G taldea finitua eta ez tribiala bada, orduan G-k gutxienez azpitalde maximal bat du. Honela, zentzua du Frattiniren azpitaldea, $\Phi(G)$ bidez denotatzen dena definitzea. Frattiniren

azpitaldea, G-ren azpitalde maximal guztien ebakidura bezala definitzen da. Baldin eta G talde tribiala bada, orduan $\Phi(G) = 1$ da.

Teorema 3.7. *Izan bedi G talde finitua. Orduan, hurrengo zazpi baieztapenak baliokideak dira:*

(i) *G talde nilpotentea da.*

(ii) *G-ren edozein azpitalde G-n subnormala da, hau da, edozein H, G-ren azpitalderako existitzen da, H-tik G-ra, azpitalde normalen kate bat.*

(iii) *Baldin eta $H < G$ bada, orduan $H < N_G(H)$.*

(iv) *G-ren edozein azpitalde maximala G-n normala da.*

(v) *$G' \leq \Phi(G)$ da.*

(vi) *G-ren edozein Sylow-en azpitalde normala da G-n.*

(vii) *G, ordena lehenen berreturen azpitaldeen biderkadura zuzena da.*

Froga. Orokortasuna galdu gabe, $G \neq 1$ dela suposa dezakegu, $G = 1$ den kasuan zazpi baliokidetasunak tribialak direlako.

$(i) \Rightarrow (ii)$ Izan bedi G talde nilpotentea. Demagun G-ren nilpotentzia klasea c dela. Orduan, jakina da G-ren edozein H azpitaldek, c luzerako serie bat duela H-tik G-ra. Bereziki, G-ren edozein azpitalde subnormala da G-n.

$(ii) \Rightarrow (iii)$ Izan bedi $H < G$. (ii) propietateagatik suposatzen ari gara, H-tik G-ra serie bat dagoela. Bereziki, kasu honetan, H-tik G-rako serie propio bat dago; adibidez, $H = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$. Gainera, $H < G$ denez, $n \geq 1$ da. Beraz, $H < H_1 \leq N_G(H)$, eta bereziki $H < N_G(H)$.

$(iii) \Rightarrow (iv)$ Izan bedi M, G-ren azpitalde maximala. (iii) ataletik, $M < N_G(M) \leq G$ da. Baina, M maximala izateagatik, $N_G(M) = G$ da. Beraz, $M \lhd G$ da.

$(iv) \Rightarrow (v)$ Izan bedi M, G-ren azpitalde maximal bat. (iv) ataletik $M \lhd G$ da. Orduan, 3.6 Lema erabiliz, G/M orden leheneko talde zikliko a eta bereziki abeldarra da, eta ondorioz $G' \leq M$ da. Aurrekoa G-ren azpitalde maximal guztietarako egia denez, $\Phi(G)$-ren definizioa erabilita, $G' \leq \Phi(G)$ da.

$(v) \Rightarrow (iv)$ Izan bedi M, G-ren azpitalde maximal bat. Orain, (v) ataletik $G' \leq M$ dugu. Honela, M/G', G/G' talde abeldarraren azpitaldea da, eta bereziki, $M/G' \lhd G/G'$ da. Honen ondorioz, $M \lhd G$ da.

$(iv) \Rightarrow (vi)$ Izan bedi P, G-ren p-Sylow-ren bat. Absurdura eramanez, suposa dezagun $P \not\trianglelefteq G$ dela, hau da, $N_G(P) < G$ dela. Orduan, $N_G(P)$ barruan duen G-ren M azpitalde maximal bat dago. Bestalde, 2.5 Korolarioa erabiliz $N_G(M) = M$ ondorioztatzen da, eta hau (iv) atalaren emaitzaren kontrakoa da. Beraz, $N_G(P) = G$ eta hemendik $P \trianglelefteq G$ dugu.

$(vi) \Rightarrow (vii)$ Izan bitez $p_1, \ldots, p_s$ $|G|$-ren zatitzaile lehen desberdin guztiak, s zenbaki oso positiboa izanik. (vi) propietateagatik, G-ren P_i, p_i-Sylow-ak normalak dira G-n, eta hau $i = 1, \ldots, s$ guztientzako. Orain, 2.8 teorema erabiliz, $G = P_1 \times P_2 \times \cdots \times P_s$ da, nahi genuen bezala.

$(vii) \Rightarrow (i)$ Izan bedi $G = P_1 \times P_2 \times \cdots \times P_s$ non P_i, p_i-taldeak diren, p_i zenbaki lehenak izanik $i = 1, \ldots, s$ guztietarako. Orduan, jakina da P_i bakoitza nilpotentea dela, p_i-taldea izateagatik. Azkenik, nola talde nilpotente biren biderkadura zuzena ere nilpotentea den, G nilpotentea dela ondorioztatzen da. □

4. Kapitulua

Talde ebazgarrien oinarriak eta Hall-en π-azpitaldeak

4.1 Talde ebazgarriak

Definizioa. Izan bedi G taldea. Orduan, G taldearen konposizio seriea G-ren azpitaldeen hurrengo kate finitu bat da:

$$G = G_0 \trianglerighteq \ldots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$$

non $G_i \trianglelefteq G_{i-1}$ diren eta G_{i-1}/G_i talde sinpleak diren $i \in \{1, \ldots, n\}$ indizeetarako. Lortutako zatidura talde horiek seriearen *konposizio faktoreak* deitzen dira.

Definizioa. Izan bedi $H \leq G$. Orduan, H, G-ren azpitalde subnormala dela esaten da H-tik G-ra doan serie bat badago, hau da, $H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$ serie bat badago.

Bereziki, G-ren edozein azpitalde normala, G-n azpitalde subnormala da, baina aldiz, kontrakoak ez du zertan egia izan behar.

Definizioa. G talde bat ebazgarria dela esaten da existitzen baldin bada G-ren serie (subnormal) abeldar bat, hau da, existitzen bada $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ non G_{i-1}/G_i konposizio faktoreak abeldarrak diren, edozein $i = 1, \ldots, n$-rentzako.

Definizioa. Baldin eta G taldea bada, definitzen dira $G^{(0)} = G$ eta $G^{(i)} = \left(G^{(i-1)}\right)'$ edozein $i \geq 1$ balio arruntetarako. Orain G taldearen *serie deribatua* $G = G^{(0)} \geq G^{(1)} = G' \geq G'' = G^{(2)} \geq \ldots \geq G^{(i)} \geq \ldots$ serieari deitzen zaio. (Argi dago serie deribatuaren ondoz-ondoko zatidura taldeak talde abeldarrak direla.)

Teorema 4.1. *Izan bedi G taldea. Orduan G ebazgarria da baldin eta soilik baldin G taldearen serie deribatua $\{1\}$-an bukatzen bada.*

Froga. Lehenengo eta behin G taldea ebazgarria denez badakigu G taldeak serie abeldar bat onartzen duela. Adibidez, $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$. Orduan, $G^{(0)} = G = G_0$ da. Bestalde, G_0/G_1 talde abeldarra izateagatik, $G_0' = G^{(1)} \leq G_1$ ondorioztatzen da, eta G_1/G_2 abeldarra izateagatik, $G_1' \leq G_2$ dugu. Lortutako lehenengo adierazpenean deribatuak aplikatuz, $(G^{(1)})' \leq G_1'$ dugu, eta bigarren adierazpena ere erabiliz $(G^{(1)})' = G^{(2)} \leq G_2$ dela ondorioztatzen da. Prozedura horri jarraituz, $G^{(n)} \leq G_n = \{1\}$ dugu, hau da, G-ren serie deribatua momenturen batean $\{1\}$-an bukatzen da.

Azkenik, G taldearen serie deribatuaren ondoz-ondoko zatidurak abeldarrak direnez eta hipotesiagatik serie deribatu hori $\{1\}$-an bukatzen dela suposatzen baldin badugu, jadanik badugu G taldearen serie subnormal abeldar bat, eta hemendik G taldea ebazgarria dela lortzen da. □

Aurreko 4.1 Teoremaren frogan ere ikusi duguna zera da, baldin eta talde bat ebazgarria bada, orduan taldearen serie deribatua gai posible gutxienengo duen serie abeldar bat dela. Definizioz, kasu horretan, G taldearen serie deribatuaren ℓ kate-maila kopuruari, G-ren *deribatu luzera* deitzen zaio, eta $\mathrm{dl}(G) = \ell$ bidez denotatzen da. Ohartu ℓ balioa $G^{(\ell)} = 1$ eta $G^{(\ell-1)} \neq 1$ baldintzengandik zehaztuta dagoela.

Adibideak. G talde bakarra zeinentzat $\mathrm{dl}(G) = 0$ den, talde tribiala $G = 1$ da, eta $\mathrm{dl}(G) = 1$ baldintza betetzen duten taldeak, talde abeldar ez tribialak dira. Bestalde, edozein G talderen serie zentral (gorakorra edo beherakorra) serie abeldarra denez, edozein talde nilpotentea, ere talde ebazgarria da. Bereziki, p-talde finituak talde ebazgarriak dira. Baina ordea, kontrakoak ez du zertan egia izan behar, hau da, existitzen dira talde ebazgarri ez nilpotenteak. Hartu adibidez S_3, zeinentzat bere serie deribatua ondokoa den,

$$S_3 \geq S_3' = \langle (123) \rangle \geq S_3'' = 1 \text{ eta } \mathrm{dl}(S_3) = 2.$$

Jakina da, S_3 ez dela talde nilpotentea, erraz ikus daitekeelako S_3-ren Sylowen 2-azpitaldeak ez direla normalak S_3-n.

Orain, G taldea bakuna eta ez abeldarra bada, $G = G' = G'' = \cdots \neq 1$ dugu eta hemendik G ez dela ebazgarria ondorioztatzen da. Bereziki, aurrekoa S_n taldeari aplikatuz, $n \geq 5$ denean, ondokoa dugu: lehenengo eta behin, jakina da edozein $n \geq 5$ baliotarako $S_n' = A_n$ dela, eta A_n talde alternatua kasu horietan talde bakuna (eta ez abeldarra) dela ere; beraz, edozein $i \geq 1$ balio arruntarako, ${S_n}^{(i)} = A_n \neq 1$ dugu, eta hemendik S_n taldea ez dela ebazgarria ondorioztatzen da. (Azkenik, ohartu ordea, S_4 taldea ebazgarria dela, $S_4 \geq S_4' = A_4 \geq S_4'' = A_4' = \langle (12)(34), (13)(24) \rangle \geq S_4''' = 1$ bere serie deribatua baita, eta ondorioz $\mathrm{dl}(S_4) = 3$ da.)

Teorema 4.2. *Baldin eta G talde ebazgarria bada, orduan G-ren edozein azpitalde, eta edozein zatidura taldea ere ebazgarriak dira.*

Froga. Hipotesiagatik G ebazgarria denez, existitzen da ℓ zeinentzat $G^{(\ell)} = 1$ den. Baldin eta $H \leq G$ bada, orduan $H^{(\ell)} \leq G^{(\ell)}$, eta ondorioz $H^{(\ell)} = 1$ dugu, eta H ebazgarria da. Orain hartu edozein $N \trianglelefteq G$, eta ohartu $(G/N)^{(\ell)} = G^{(\ell)}N/N = \overline{1}$ dela, hau da, G/N talde ebazgarria dela. □

Teorema 4.3. *Izan bitez G taldea eta $N \trianglelefteq G$. Orduan G ebazgarria da baldin eta soilik baldin N eta G/N ebazgarriak badira. Gainera, kasu honetan* $\mathrm{dl}(G) \leq \mathrm{dl}(G/N) + \mathrm{dl}(N)$ *betetzen da.*

Froga. Aurreko 4.2 Teoremagatik norabide bat nabaria da. Bestalde, demagun orain N eta G/N ebazgarriak direla, hau da, existitzen direla ℓ eta k zeinentzat $N^{(l)} = 1$ eta $(G/N)^{(k)} = \overline{1}$ diren. Orduan $G^{(k)} \leq N$ eta ondorioz $G^{(k+\ell)} = 1$, hau da, G ebazgarria dela ondorioztatzen da. □

Honen ondorio gisa, talde baten bi azpitalde ebazgarrien biderkadura, horietariko azpitalde bat normala bada talde osoan, ere ebazgarria dela lortzen da.

Korolarioa 4.4. *Izan bitez G taldea, $H \leq G$ eta $N \trianglelefteq G$ bi azpitalde ebazgarriak. Orduan HN ebazgarria da. Partikularki, edozein bi azpitalde ebazgarrien biderkadura erdizuzena (eta zuzena ere) ebazgarria da.*

Froga. Ohartu lehenik eta behin $H \cap N \trianglelefteq H$ dela, N normala izateagatik G-n. 4.3 Teorema aplikatuz H talde ebazgarriari, $H/(H \cap N)$ taldea ebazgarria dela lortzen da. Orain Isomorfismoaren Bigarren Teorema kontuan izanik, $H/(H \cap N) \cong HN/N$ dugu, eta ondorioz HN/N ebazgarria da. Azkenik, berriro ere 4.3 Teorema aplikatuz HN taldearen, N azpitalde eta HN/N zatidura talde ebazgarri biei, HN ebazgarria dela lortzen da. □

Aurreko korolarioan beharrezkoa izan da horietariko azpitalde bat normala izatea talde osoan. Orokorki, bi azpitalde ebazgarrien biderkadurak, nahiz eta biderkadura azpitaldea izan, ez du zertan ebazgarria izan behar. Hartu adibidez, S_4 eta $K = \langle(12345)\rangle$. Biak dira S_5-ko azpitalde ebazgarriak. Gainera $S_4K = S_5$ da, baina ordea S_5 ez da ebazgarria.

Azkenik, zentzua du G talde finitu baten *erradikal ebazgarria* definitzea G taldearen azpitalde normal ebazgarri guztien biderkadura gisa.

Ondoren talde ebazgarri baten azpitalde normal minimalaren ezaugarri batzuk aztertuko ditugu.

Teorema 4.5. *Izan bitez G talde ebazgarria eta N, G-ren azpitalde normal minimal bat. Orduan ondoko baieztapenen bat betetzen da,*

(i) *Existitzen da p zenbaki lehen bat zeinentzat N, p-talde abeldar elementala den, hau da, N, C_p-ren kopien biderkadura zuzen murriztua da.*

(ii) *Bestalde N, $\mathbb{Q}$-ren kopien biderkadura zuzen murriztua da, hau da, N, $\mathbb{Q}$-espazio bektorial baten talde batukorraren isomorfoa da.*

Froga. Lehenik eta behin, ohartu N-ren azpitalde karakteristiko bakarrak 1 eta N direla. Orain $N' \operatorname{char} N$ denez, printzipioz N'-ren aukera posibleak 1 eta N dira. Baina $N' = N$ balitz, edozein $i \geq 1$ baliotarako $N^{(i)} = N \neq 1$ litzateke, eta hau, N ebazgarria izatearen kontrakoa da. Beraz $N' = 1$ da, hau da, N abeldarra da. Defini dezagun edozein p zenbaki lehenerako $K_p = \{x \in N : x^p = 1\}$ multzoa. Orain N abeldarra denez, K_p, N-ren azpitaldea da, eta honez gain, N-n karakteristikoa. Ondorioz berriro ere K_p-rentzako bi aukera baino ez daude. Baldin eta p zenbaki lehenen batetarako $K_p = N$ bada, orduan N, p-talde abeldar elementala izango litzateke eta (i) atala lortzen da. Bestalde, demagun edozein p zenbaki lehenerako $K_p = 1$ dela. Orduan, N taldeak ez du ordena leheneko elementurik, eta ezta ordena finituko elementurik ere. Edozein $m \in \mathbb{N}$ zenbakirako, definitzen dira $L_m = \{x^m : x \in N\}$ multzoak. Berriro ere N abeldarra izateagatik, L_m multzoak N-ren azpitaldeak dira eta N-n karakteristikoak. Orain N-ren azpitalde karakteristikoen aukerak kontuan harturik, eta baita kontuan harturik N-k ez duela ordena finituko elementurik, edozein $m \in \mathbb{N}$ zenbakirako $L_m = N$ dela ondorioztatzen da. Hemendik, $m \in \mathbb{N}$ zenbaki bat finkatuta, edozein $n \in N$ elementurentzat existitzen da $x \in N$ zeinentzat $n = x^m$ den. Gainera, $n \in N$ bakoitzarentzat x-ren aukera bakarra da. Bestalde, $n = y^m$ balitz, $y \in N$ izanik, $n = x^m = y^m$ adierazpenetik $(xy^{-1})^m = 1$ litzatekete, eta hemendik $xy^{-1} = 1$ lortuko genuke, aztertzen ari garen kasuan, N-k ez duelako ordena finituko elementurik. Hau da, $x = y$ litzateke, nahi genuen bezala. Kasu honetan, x, n-ren m-garren erro bakarra dela esaten da, eta $x = n^{1/m}$ bidez adierazten da. Horrela edozein $a/b \in \mathbb{Q}$ zenbaki arrazionalarentzat zentzua du $x^{a/b}$ adieraztea. Azkenik, ohartu aurrekotik N, $\mathbb{Q}$-espazio bektoriala dela lortzen dela. □

Bereziki G taldea ebazgarri finitua bada, orduan bere azpitalde normal minimalak derrigorrez p-talde abeldar elementalak izan behar dira.

Teorema 4.6. *Izan bitez G talde ebazgarria eta $M \max G$. Orduan M-ren indizea G-rekiko zenbaki lehen baten berretura da edo bestalde infinitua da.*

Froga. Lehenik eta behin ohartu G ebazgarria, eta M azpitaldea G-n propioa izateagatik, existitzen dela i balioren bat zeinentzat $G^{(i)} \not\leq M$, baina bai ordea $G^{(i+1)} \leq M$. Zatidura $G^{(i+1)}$ azpitaldeagatik eginez, hau da, $G^{(i+1)}$ azpitaldeagatik moztuz, orokortasuna galdu gabe suposa dezakegu, existitzen dela $A \trianglelefteq G$ azpitalde abeldarra zeinentzat $A \not\leq M$. Orduan, $M < MA \leq G$, eta hemendik $G = MA$ lortzen da, $M \max G$ delako. Bestalde, A normala denez G-n, $A \cap M$ ere normala da M-n. Are gehiago, A abeldarra denez, orduan $A \cap M$ ere normala da A-n. Azkenik, $G = MA$, $A \cap M \trianglelefteq M, A \cap M \trianglelefteq A$ hiru baldintzetatik, $A \cap M \trianglelefteq G$ lortzen da. Orain

$A \cap M$, G-ko azpitalde normalagatik zatituz, suposa dezakegu orokortasuna galdu gabe $G = M[A]$ biderkadura erdizuzena dela (hau da, $A \cap M = 1$ dela). Azkenik, ikus dezagun egoera honetan A, G-ko azpitalde normal minimal bat dela. Absurdura eramanez, azken baieztapen hori egia izango ez balitz, existituko litzateke $B \trianglelefteq G$ zeinentzat $1 < B < A$ den. Bestalde, nola $G = M[A]$ den, $M < MB < MA = G$ azpitaldeen katea lortuko genuke, eta hori $M \max G$ izatearen kontrakoa da. Ondorioz, A, G-ko azpitalde normal minimala da. Orain 4.5 Teorema erabilita eta kontuan harturik ere, $|G : M| = |A|$ dela, teorema honen froga bukatutzat eman genezake. □

Bereziki, G talde ebazgarri finitua eta $M \max G$ bada, $|G : M|$ zenbaki lehen baten berretura da.

Teorema 4.7. *Izan bitez G talde ebazgarria eta N, G-ren azpitalde normal maximal bat. Orduan, N-ren indizea G-rekiko zenbaki lehen bat da.*

Froga. Hipotesiagatik N, G-ren azpitalde normal maximala denez, G/N talde bakuna da. Bestalde, 4.2 Teoremagatik, G ebazgarria denez, G/N ere ebazgarria da. Orain, nola G/N talde ebazgarria den, hau da, serie abeldar bat onartzen duen, eta aldi berean G/N talde bakuna den, G/N-ren serie abeldarraren aukera bakarra $\{\overline{1}\} \trianglelefteq G/N$ da, eta honek G/N abeldarra dela esan nahi du. Azkenik, talde abeldarren deskonposaketa (ikusi Lehenengo Kapituluko 1.3 atala) kontuan harturik, eta baita G/N bakuna dela, G/N-ren aukera bakarra ordena leheneko talde ziklikoa izatea da. Bereziki, $|G/N|$ zenbaki lehen bat da. □

Aurreko teoremaren ondorio zuzena, G talde ebazgarri batek, konposizio serieren bat izatearen karakterizazioa, G finitua eta bere konposizio faktore guztiak orden leheneko talde ziklikoak izatean datza. Hau da, hain zuzen ere, hurrengo teoreman azaltzen dena.

Teorema 4.8. *Izan bedi G talde ebazgarria. Orduan, G taldeak konposizio serie bat onartzen du baldin eta soilik baldin G finitua eta kasu horretan seriearen konposizio faktoreak orden lehenekoak badira.*

4.2 π-taldeak

Atal honetan zehar talde finituak zein infinituak kontsideratuko ditugu.

Definizioa. Izan bitez π finkatutako zenbaki lehenen multzoa, eta $n = p_1^{e_1} \dots p_s^{e_s} \in \mathbb{N}$ zenbaki lehenen biderkadura gisa deskonposatutako zenbakia. Orduan, n-ren zatitzaile lehen guztiak π-n badaude, hau da, $p_1, \dots, p_s \in \pi$ badaude, n, *π-zenbakia* dela deritzogu. π multzotik kanpo dauden zenbaki lehenen multzoa π' bidez denotatzen da. Bestalde, berordenaketa bat egin ondoren eta $r < s$ izanik, baldin eta $p_1, \dots, p_r \in \pi$ eta $p_{r+1}, \dots, p_s \notin \pi$, edo

$p_{r+1}, \ldots, p_s \in \pi'$ badaude, orduan n zenbakiaren π-*zatia* $p_1^{e_1} \ldots p_r^{e_r}$ adierazpenari deituko diogu eta n_π bidez denotatuko da, eta n zenbakiaren π'-zatia $p_{r+1}^{e_{r+1}} \ldots p_s^{e_s}$ adierazpena izango da, $n_{\pi'}$ bidez denotatzen dena.

Definizioz, 1a π-zenbakia da, π multzoa edozein izanik. Bereziki, π zenbaki lehen bakar batez osatuta dagoenean, hau da, $\pi = \{p\}$ denean, orduan p eta p' notazioak erabiliko dira.

Bestalde, edozein G talde baten (G finitua edo infinitua) ordena finituko g elementu bat hartuta, baldin eta g-ren ordena π-zenbakia bada, orduan g π-*elementua* dela esaten da. Honela, jadanik, π-taldeak definitzeko "tresna" guztiak eskura ditugu.

Definizioa. Izan bitez G taldea eta π zenbaki lehenen multzo bat. Orduan, G π-taldea da baldin eta G-ko elementu guztiak π-elementuak badira. Bereziki G taldea, finitua denean, π-taldea dela esaten da, $|G|$ π-zenbakia bada. Beste era batera esanda, baldin eta $|G| = p_1^{e_1} \ldots p_s^{e_s}$ bada, $p_1, \ldots, p_s \in \pi$ direnean.

Azkenengo definizio honek, p-taldeak orokortzen ditu. Bestalde, G, p'-taldea da, p zenbakiak ez badu $|G|$ zatitzen. Hemendik aurrera G taldea, finitua denean, $|G|$ zatitzen duten zenbaki lehenen multzoa $\pi(G)$ bidez adieraziko dugu. Hau da, $\pi(G) = \{p \text{ lehena } : |G| \equiv 0 \pmod{p}\}$.

Teorema 4.9. *Emanda π zenbaki lehenen multzo bat, edozein $n \in \mathbb{N}$ zenbakirako, $n = n_\pi n_{\pi'}$ eran deskonposatzen da, n_π π-zenbakia eta $n_{\pi'}$ π'-zenbakia izanik.*

Teorema 4.10. *Izan bedi g ordena finituko elementua. Orduan, g elementua $g = xy = yx$ eran deskonposa dezakegu, x, π-elementua eta y, π'-elementua izanik. Gainera, deskonposizio hau bakarra da eta deskonposizioaren faktore bakoitza g-ren berretura bat da. Are gehiago, x-ren ordena g-ren ordenaren π-zatia da, eta y-ren ordena g-ren ordenaren π'-zatia da.*

Froga. Izan bitez n, g-ren ordenaren π-zatia eta m, g-ren ordenaren π'-zatia, hau da, $n = o(g)_\pi$ eta $m = o(g)_{\pi'}$. Honela, $o(g) = nm$ da, eta n eta m elkarrekiko lehenak direnez, existitzen dira a eta b zenbaki osoak non $am + bn = 1$ den. Orain, defini ditzagun $x_0 = g^{am}$ eta $y_0 = g^{bn}$. Honela, definizioz, $g = g^{am+bn} = x_0 y_0 = y_0 x_0$ dugu. Bestalde $o(g) = nm$ denez, $x_0^n = g^{amn} = 1$ eta $y_0^m = g^{bnm} = 1$ dugu. Ohartu teoreman ezarritako deskonposizioa lortzen dela.

Orain, deskonposizoaren bakartasuna frogatuko da. Horretarako, $g = xy = yx$ ere dela suposatuko dugu, $o(x) = u$ π-zenbakia eta $o(y) = v$ π'-zenbakia izanik. Orduan, $\text{zkh}(u, v) = 1$ denez, existitzen dira c eta d zenbaki osoak non $cu + dv = 1$ den. Orduan, $g^{cu} = (xy)^{cu} = x^{cu} y^{cu} =$

$y^{cu} = y^{1-dv} = yy^{-dv} = y$ eta $g^{dv} = (xy)^{dv} = x^{dv}y^{dv} = x^{dv} = x^{1-cu} = xx^{-cu} = x$ dira. Hau da, x eta y, g-ren berreturak dira. Beraz, x_0, y_0, x eta y elkar trukatzen dira. Gainera, $x_0y_0 = g = xy$ berdintzatik, $x^{-1}x_0 = yy_0^{-1}$ ondorioztatzen da. Bestalde, azkeneko adierazpenaren ezkerreko aldea π-elementua eta eskuineko aldea π'-elementua dira. Azkenik, π eta π' multzoak osagarriak direnez, $x^{-1}x_0 = yy_0^{-1} = 1$ da. Ondorioz, $x = x_0$ eta $y = y_0$ dira. Beraz, hasieran aipatutako deskonposizioa bakarra da. □

Hemendik aurrera, x, g-ren π-zatia eta y, g-ren π'-zatia deituko dira.

Korolarioa 4.11. *Izan bedi G talde finitua zein infinitua. Orduan, G-ko ordena finituko edozein elementu, ordena zenbaki lehenen berreturen bat duten eta haien artean trukakorrak diren, elementuen biderkadura gisa idatz daiteke era bakarrean.*

Proposizioa 4.12. *Izan bedi G talde finitua eta π zenbaki lehenen multzo bat. Ondoko hiru baieztapenak baliokideak dira:*

(i) *G taldea π-taldea da.*

(ii) *$|G|$, π-zenbakia da.*

(iii) *$\pi(G) \subset \pi$.*

Froga. $(i) \Rightarrow (ii)$ Ondorioztapenaren froga absurdura eramanez egingo da. Demagun orduan $|G|$ ez dela π-zenbakia eta behintzat existitzen dela p zenbaki lehen bat zeinentzat p-k $|G|$ zatitzen duen baina $p \notin \pi$. Sylow-en Teoriako ondorio bategatik, ziurta genezake existitzen dela $g \in G$ non $o(g) = p$ den. Bereziki, g ez da π-elementua eta hemendik G ez da π-taldea, eta hau hipotesiaren kontrakoa da. Honekin, G, π-taldea izanik, $|G|$, π-zenbakia dela frogatu dugu.

$(ii) \Rightarrow (iii)$ Nabaria da.

$(iii) \Rightarrow (i)$ Jakina denez, G-ko edozein elementuren ordenak $|G|$ zatitzen du. Honela, G-ko elementu guztiak $\pi(G)$-elementuak dira, eta hipotesiagatik $\pi(G) \subset \pi$ denez, G-ko elementu guztiak π-elementuak dira, eta ondorioz G, π-taldea da. □

Emandako definizioagatik, berehalakoa da G π-talde finitu zein infinitua izanik, G-ren edozein azpitalde edo zatidura taldea ere π-taldea dela.

4.3 Hall-en π-azpitaldeak eta Hall-en Teoremak

Teorema 4.13. *G talde baten bi π-azpitaldeen biderkadurak, baldin eta azpitaldea bada, G-ren π-azpitaldea izaten jarraitzen du.*

Froga. Izan bitez H eta K, G-ren bi π-azpitalde. $HK \leq G$, G-ren π-azpitaldea dela ikusteko nahikoa da $|HK| = \frac{|H||K|}{|H\cap K|}$ ordena, π-zenbakia izaten jarraitzen duela ikustea, eta hori berehalakoa da $|H|$, $|K|$ eta $|H \cap K|$ π-zenbakiak direlako. □

Korolarioa 4.14. *Edozein talde finituk π-erradikala du, hau da, G-ren π-azpitalde normal handiena. Hauxe, $O_\pi(G)$ bidez adierazten da.*

Ohar gaitezen, π zenbaki lehenen multzoa eta G taldea badira, $O_\pi(G) = O_{\pi\cap\pi(G)}(G)$ dela. Beraz, $\pi \subseteq \pi(G)$ kasua baino ez dugu kontuan hartu behar.

Teorema 4.15. *Baldin eta G talde ebazgarri finitua eta π zenbaki lehenen multzo bat badira, orduan $O_\pi(G) \neq 1$ edo $O_{\pi'}(G) \neq 1$ dira.*

Definizioa. Izan bitez G talde finitua eta π zenbaki lehenen multzoa. Orduan, H, G-ren azpitalde bat, *G-ren Hall-en π-azpitalde* bat dela esaten da $|H|$, $|G|$-ren π-zatia bada. Beste era batera esanda, $|H|$, π-zenbakia eta $|G : H|$ π'-zenbakia badira.

Ohartu, zenbaki lehenen multzo baterako H, G-ren Hall-en azpitaldea izatea zkh$(|H|, |G : H|) = 1$ baldintzaren baliokidea dela. Adibide gisa, baldin eta $\pi = \{2, 7\}$ eta $|G| = 2^2 \cdot 5 \cdot 7^2$ badira, $|H| = 2^2 \cdot 7^2$ ordenako azpitaldea G-ren Hall-en π-azpitaldea da. Gainera, $|G : H| = 5$ π'-zenbakia da. Hemendik aurrera, G-ren Hall-en π-azpitaldeen multzoa $\mathrm{Hall}_\pi(G)$ idatziko dugu. Edozein kasutan, gerta daiteke $\mathrm{Hall}_\pi(G) = \emptyset$ izatea. Adibide gisa, A_5 talde alternatuaren kasuan, $|A_5| = 2^2 \cdot 3 \cdot 5$ da eta A_5-k ez du Hall-en $\{2, 5\}$-azpitalderik, ezta Hall-en $\{3, 5\}$-azpitalderik ere. Hala ere, A_5 taldeak baditu Hall-en $\{2, 3\}$-azpitaldeak, adibidez A_4.

Teorema 4.16. *Izan bitez G taldea eta $H \in \mathrm{Hall}_\pi(G)$. Baldin eta $N \trianglelefteq G$, ondokoak betetzen dira:*

(i) $H \cap N \in \mathrm{Hall}_\pi(N)$.

(ii) $HN/N \in \mathrm{Hall}_\pi(G/N)$.

Froga. i) $H \cap N \leq H$ denez, $|H \cap N| \Big| |H|$ da. Gainera, $H \in \mathrm{Hall}_\pi(G)$ denez, $|H|$ π-zenbakia da eta ondorioz $|H \cap N|$ ere π-zenbakia da. Bestalde, $|N : H \cap N| = \frac{|N|}{|H\cap N|} = \frac{|HN|}{|H|}$ da, eta $\frac{|HN|}{|H|}$ zenbakiak, $|G : H|$ zenbakia zatitzen du. Orain nola $|G : H|$, π' zenbakia den, $|N : H \cap N|$ π'-zenbakia dela ondorioztatzen da. Beraz, $H \cap N \in \mathrm{Hall}_\pi(N)$.

ii) $\left|\frac{HN}{N}\right| = \left|\frac{H}{H\cap N}\right|$ zenbakiak $|H|$ zatitzen du. Hortaz, $H \in \mathrm{Hall}_\pi(G)$ izateagatik $\left|\frac{HN}{N}\right|$ π-zenbakia da. Bestalde, $|G/N : HN/N| = |G : HN|$ zenbakiak $|G : H|$ zenbakia zatitzen duenez, $|G : HN|$ π'-zenbakia dela ondorioztatzen da. □

Aurreko teoremako (i) atalaren ondorio bat K, G-ren azpitalde subnormala eta $H \in \mathrm{Hall}_\pi(G)$ badira, orduan $H \cap K \in \mathrm{Hall}_\pi(K)$ dela da. Hauxe, orokorrean, edozein K azpitaldetarako ez da egia, ezta Sylow-en azpitaldeetarako ere. Adibidez, S_3 taldean, $H = \langle(12)\rangle \in \mathrm{Syl}_2(S_3)$ eta $K = \langle(13)\rangle$ hartuz, $H \cap K = 1 \notin \mathrm{Syl}_2(K)$. Ohartu, (i) ataleko frogapenean $HN \leq G$ betetzeko soilik $N \trianglelefteq G$ dela erabiltzen dela. Beraz, $|HN|$, $|G|$-ren zatitzailea dela ziurta daiteke. Hori dela eta, HN, G-ren azpitaldea den bitartean, $H \cap N \in \mathrm{Hall}_\pi(N)$ da. Bereziki, H Hall-en π-azpitalde normala bada, $H \cap K \in \mathrm{Hall}_\pi(K)$ da, edozein $K \leq G$ izanik.

Teorema 4.17. *Izan bitez G talde finitua eta H, G-ren Hall-en π-azpitalde normala. Orduan, H-k G-ren edozein π-azpitalde bere barnean du. Bereziki, H, G-ren Hall-en π-azpitalde bakarra da, eta ondorioz $H \operatorname{char} G$ da. (Argi dago kasu honetan $H = O_\pi(G)$ dela.)*

Froga. Izan bedi K, G-ren π-azpitalde bat. Hipotesiz, $H \trianglelefteq G$ denez, HK, G-ren azpitaldea da eta gainera π-azpitaldea da. Baina, H, G-ren Hall-en π-azpitaldea eta $H \leq HK$ direnez, derrigorrez $H = HK$ da, eta hemendik $K \leq H$ lortzen da. □

Teorema 4.18. *Izan bitez G talde finitua eta K, G-ren π-azpitalde normal bat. Orduan K, G-ren Hall-en π-azpitalde guztien barne dago.*

Froga. Izan bedi $H \in \mathrm{Hall}_\pi(G)$. Hipotesiz, $K \trianglelefteq G$ denez, HK ere G-ren azpitaldea da eta gainera π-azpitaldea. Bestalde, $H \leq HK$ eta H, G-ren Hall-en π-azpitaldea izateak $H = HK$ ondorioztatzen du eta hemendik $K \leq H$ dugu. □

Teorema 4.19 (Talde ebazgarrien Hall-en Lehenengo Teorema)**.** *Izan bedi G talde ebazgarri finitua eta π zenbaki lehenen multzoa. Orduan, G-k Hall-en π-azpitaldeak ditu.*

Froga. $|G|$-ren gaineko indukzioz frogatuko da. Hipotesiagatik, G talde ebazgarria denez, 4.15 Teorema erabiliz, hurrengo kasuetako bat ematen da: $O_\pi(G) \neq 1$ edo $O_{\pi'}(G) \neq 1$.

- $O_\pi(G) \neq 1$ denean, izan bedi $N = O_\pi(G)$. Orduan, G/N, $|G|$ baino kardinal txikiagoko taldeari hipotesi induktiboa aplikatuz, G/N-k Hall-en π-azpitalde bat du, dei diezaiogun H/N. Bereziki, $|G/N : H/N| = |G : H|$ π'-zenbaki bat da. Ondoko diagrama dugu:

$$\begin{array}{ll} G & \\ | & \pi'\text{-zenbakia} \\ H & \\ | & \pi\text{-zenbakia} \\ N & \\ | & \pi\text{-zenbakia} \\ 1 & \end{array}$$

Orduan, $|H| = |H/N||N|$ π-zenbakia da eta $|G : H|$ π'-zenbakia denez, hemendik $H \in \mathrm{Hall}_\pi(G)$ dugu.

- $O_\pi(G) = 1$ eta $O_{\pi'}(G) \neq 1$ direnean, izan bedi $N = O_{\pi'}(G)$. Baldin eta $N = G$ bada, G π'-taldea da eta $1 \in \mathrm{Hall}_\pi(G)$ da. Beraz, suposa dezagun orain N, G-n propioa dela. Honela, G/N-ren azpitalde normal minimal bat har dezakegu, L/N alegia. Gainera, hipotesiagatik G talde ebazgarri finitua denez, G/N ere ebazgarria da eta L/N p-talde abeldar elementala da, p zenbaki lehen baterako 4.5 Teoremagatik. Gainera, froga dezagun $p \in \pi$ dagoela. Izan ere, $p \in \pi'$ balitz, L, $N = O_{\pi'}(G)$ baino handiagoa den G-ren π'-azpitalde normala izango litzateke, eta hau kontraesana da. Orduan, $|L| = |L/N||N| = p^n|N|$ da $n \in \mathbb{N}$ batentzako, non p^n π-zenbakia eta $|N|$ π'-zenbakia diren. Izan bedi $P \in \mathrm{Syl}_p(L)$. Orduan $|P| = p^n$ da. Gainera $|PN| = \frac{|P||N|}{|P \cap N|} = p^n|N| = |L|$ da, $|P \cap N| = 1$ izanik, eta $PN \leq L$ denez, $L = PN = NP$ (kontuan hartu $N \trianglelefteq G$ dela) lortzen da. Orain, 2.4 Frattiniren argumentuko teorema erabiliz, $G = N_G(P)L = LN_G(P)$ dugu.

$$\begin{array}{ll} G = N_G(P)L & \\ \quad | & \quad \triangledown \\ \quad L & \\ \quad | & \\ \quad P & \quad \in \mathrm{Syl}_p(L) \end{array}$$

Orain, $G = LN_G(P) = NPN_G(P) = NN_G(P)$ dugu, $P \subseteq N_G(P)$ delako. Gainera, $|N|$ π'-zenbakia denez, $|G|$-ren π-zati osoa $|N_G(P)|$-k darama. Beraz, $N_G(P)$ azpitaldea G-n propioa bada, hipotesi induktiboa erabiliz, $N_G(P)$-k, badu G-ren Hall-en π-azpitalde bat eta emaitza lortu dugu. Bestalde, $N_G(P) = G$ izango balitz, P, G-n normala izango litzateke, eta bereziki P, G-ren π-azpitalde normala litzateke, eta azken emaitz hau $O_\pi(G) = 1$ izatearen kontrakoa da.

□

Korolarioa 4.20. *Izan bitez G talde ebazgarri finitua eta $N \trianglelefteq G$. Orduan,* $\mathrm{Hall}_\pi(G/N) = \{HN/N : H \in \mathrm{Hall}_\pi(G)\}$ *da.*

Froga. Kasu honetan $\mathrm{Hall}_\pi(G/N) = \{HN/N : H \in \mathrm{Hall}_\pi(G)\}$ berdintza frogatzeko bi partekotasunak betetzen direla ikusiko dugu. Ezkerreko partekotasuna ezaguna da, 4.16 Teoremaren (ii) ataletik. Beste partekotasuna frogatzeko, har dezagun $L/N \in \mathrm{Hall}_\pi(G/N)$ eta ikus dezagun $L/N = HN/N$ motatakoa dela, $H \in \mathrm{Hall}_\pi(G)$-ren batentzako. Orduan, L, G talde finitu ebazgarriaren azpitaldea denez, L ere talde finitu ebazgarria da. Beraz, 4.19 Teorema erabiliz L-k behintzat Hall-en π-azpitalde bat du, H alegia. Bestalde, $|G : L| = |G/N : L/N|$ π'-zenbakia denez, benetan H, G-ren

Hall-en π-azpitaldea ere bada. Hau da, $H \in \mathrm{Hall}_\pi(G)$. Beraz, $H, N \leq L$ eta $N \trianglelefteq G$ direnez, $HN \leq L$ da. Bestalde, $H \in \mathrm{Hall}_\pi(G)$ izateagatik, berriro ere 4.16 Teoremaren (*ii*) ataletik $HN/N \in \mathrm{Hall}_\pi(G/N)$ da. Baina, $HN/N \leq L/N$, $HN/N \in \mathrm{Hall}_\pi(G/N)$ eta $L/N \in \mathrm{Hall}_\pi(G/N)$ dira. Ondorioz, $L/N = HN/N$ da, nahi genuen bezala. □

Lema 4.21. *Izan bedi $G = H[N]$ biderkadura erdizuzena. Baldin eta K, H-ren azpitaldea bada non $KN \trianglelefteq G$ den, orduan $K \trianglelefteq H$ da.*

Froga. Kontsidera dezagun $\rho\colon G = HN \longrightarrow G/N \cong H$ epimorfismoa. Modu honetan $\rho(hn) = h$ erregela bidez uler genezake. Orduan, $KN \trianglelefteq G$ denez, $\rho(KN) \trianglelefteq \mathrm{Im}(\rho)$ da, hau da, $KN/N \trianglelefteq HN/N$. Beraz $K \trianglelefteq H$. □

Teorema 4.22 (Talde ebazgarrien Hall-en Bigarren Teorema)**.** *Izan bedi G talde ebazgarri finitua eta $H, K \in \mathrm{Hall}_\pi(G)$. Orduan, H eta K konjokatuak dira G-n.*

Froga. Froga $|G|$-ren gaineko indukzioz egingo da. Bi kasu bereiziko dira:

- $O_\pi(G) \neq 1$ denean. Izan bedi $N = O_\pi(G)$. Orduan G/N, $|G|$ baino kardinal txikiagoko taldeari hipotesi induktiboa aplikatuz, nola HN/N, $KN/N \in \mathrm{Hall}_\pi(G/N)$ diren, HN/N eta KN/N konjokatuak direla ondorioztatzen da. Bestalde, N ere π-azpitalde normala denez G-n, $N \leq H$ eta $N \leq K$ dira. Beraz, H/N eta K/N konjokatuak dira. Hau da, existitzen da $gN \in G/N$ non $H/N = (K/N)^{gN} = K^gN/N = K^g/N$ den. Beraz, $H = K^g$ da, $g \in G$ izanik.

- $O_\pi(G) = 1$ eta $O_{\pi'}(G) \neq 1$ direnean. Izan bedi $N = O_{\pi'}(G)$. Orduan, G/N-n har dezagun L/N azpitalde normal minimal bat. Talde ebazgarrien Hall-en Lehen Teoreman, hau da, 4.19 Teoreman ikusi den moduan, L/N p-taldea da, $p \in \pi$ zenbaki lehen baterako, eta $L = P[N]$ da, $P \in \mathrm{Syl}_p(L)$ izanik. Orain, Sylow-en azpitaldeentzako Frattiniren argumentua erabiliz, $G = LN_G(P) = NPN_G(P) = NN_G(P)$ da. Beraz, $|G|$-ren π-zati osoa $|N_G(P)|$-n dago. Gainera, P, p-azpitaldea da, eta hasierako H-k G-ren p-Sylow-en azpitalderen bat barne du, Q alegia. Orduan, Sylow-en Teoremak erabiliz, existitzen da $x \in G$ elementuren bat non $P \leq Q^x \leq H^x$ den. Beraz, $L = PN \leq H^xN$ da eta bereziki PN normala da G-n, $L \trianglelefteq G$ delako. Orain H^xN biderkadura erdizuzena denez ($|H^x|$ eta $|N|$ ordenak elkarrekiko lehenak dira), 4.21 Lema erabiliz, $P \leq H^x$ azpitaldeari non $PN \trianglelefteq G$ den, orduan $P \trianglelefteq H^x$ lortzen dugu. Beraz, $H^x \leq N_G(P)$ da. Argudio berdina errepikatuz K-rentzat, H-ren ordez, existitzen da $y \in G$ non $K^y \leq N_G(P)$ den. Eta, amaitzeko nola P, ez den π-azpitalde normala G-n, $N_G(P) < G$ dugu. Orain H^x, $K^y \in \mathrm{Hall}_\pi(G)$ dira, eta baita H^x, $K^y \in \mathrm{Hall}_\pi(N_G(P))$ ere. Azkenik hipotesi induktiboa $N_G(P)$-ri aplikatuz, H^x eta K^y konjokatuak direla lortzen dugu, eta baita ere H eta K konjokatuak direla, nahi genuen bezala.

□

Korolarioa 4.23 (Frattiniren argumentua Hall-en azpitaldeentzako)**.** *Izan bitez G taldea eta $N \trianglelefteq G$ azpitalde ebazgarri finitua. Orduan, edozein $H \in \mathrm{Hall}_\pi(N)$ azpitalderentzat $G = NN_G(H)$ dugu.*

Froga. Izan bedi $g \in G$ elementu bat. Hipotesiz $H \in \mathrm{Hall}_\pi(N)$ denez, eta N, G-n azpitalde normala denez, orduan $H^g \leq N^g = N$ eta $|H| = |H^g|$ dira. Honen ondorioz, $H^g \in \mathrm{Hall}_\pi(N)$ da. Orain, 4.22 Teorema N taldeari aplikatuta, H eta H^g konjokatuak dira N-n, hau da existitzen da $n \in N$ non $H = (H^g)^n$ den. Beraz, $gn \in N_G(H)$ eta $g \in N_G(H)n^{-1} \subseteq N_G(H)N = NN_G(H)$ da. Orduan $G \subseteq NN_G(H)$ partekotasuna frogatu dugu (beste partekotasuna berehalakoa da). □

Teorema 4.24 (Talde ebazgarrien Hall-en Hirugarren Teorema)**.** *Izan bedi G talde ebazgarri finitua eta K, G-ren π-azpitalde bat. Orduan, K, G-ren Hall-en π-azpitalderen batetan sartuta dago.*

Froga. Froga $|G|$-ren indukzioz gainean egingo da. Bi kasu bereiziko dira:

- $O_\pi(G) \neq 1$ denean. Izan bedi $N = O_\pi(G)$. Orduan KN/N, G/N-ren π-azpitaldea da, $|KN/N|$, $|K|$-ren zatitzailea delako. Bestalde, KN/N, G/N-ren Hall-en π-azpitalderen baten barne dago, alegia H/N-ren barnean. Orduan, $H \in \mathrm{Hall}_\pi(G)$ eta $K \leq KN \leq H$ da, hau da, K, G-ren Hall-en π-azpitalde baten barne dugu, hain zuzen ere, H barnean.

- $O_\pi(G) = 1$ eta $O_{\pi'}(G) \neq 1$ direnean. Izan bedi $N = O_{\pi'}(G)$. Orduan, hipotesi indukiboa erabiliz, KN/N, G/N-ren Hall-en π-azpitalde baten barnean dago. 4.20 Korolarioa erabiliz, G/N-ren Hall-en π-azpitalde hori HN/N moduan idatz daiteke, $H \in \mathrm{Hall}_\pi(G)$ izanik. Orduan, $KN \leq HN$ eta Dedekind-en erregela erabiliz, $KN = KN \cap HN = (K \cap HN)N = (KN \cap H)N$ da, non K π-taldea, N π'-taldea eta $K \cap HN$ π-taldea diren. Beraz, $|K| = |K \cap HN| = |KN \cap H|$ da. Ondorioz, K zein $K \cap HN$, HN-ren Hall-en π-azpitaldeak dira. Orain, 4.22 Teorema erabiliz, hau da, talde ebazgarrien Hall-en Bigarren Teorema aplikatuz, existitzen da $x \in HN$ non $K = (KN \cap H)^x \leq H^x$ den. Bereziki K, G-ren Hall-en π-azpitalde baten barnean dago, hain zuzen ere, H^x barnean.

□

Korolarioa 4.25. *Izan bitez G talde finitu ebazgarria eta $N \trianglelefteq G$. Orduan, $\mathrm{Hall}_\pi(N) = \{H \cap N : H \in \mathrm{Hall}_\pi(G)\}$ da.*

Froga. Berdintzaren bi partekotasunak ikusiko dira. Eskumatik ezkerrerako partekotasuna ezaguna da (ikusi 4.16 Teoremako (i) atala). Beste partekotasunerako, izan bedi $K \in \mathrm{Hall}_\pi(N)$. Orduan, K, G-ren π-azpitaldea denez, aurreko 4.24 Teorema erabiliz, existitzen da $H \in \mathrm{Hall}_\pi(G)$ non $K \leq H$ den. Beraz, $K \leq H$ eta $K \leq N$ izateagatik, $K \leq H \cap N$ da. Baina, K eta $H \cap N$, N-ren Hall-en π-azpitaldeak direnenez, derrigorrez $K = H \cap N$ da. □

Teorema 4.26. *Baldin eta G talde finitu batek π zenbaki lehenen edozein multzotarako Hall-en π-azpitaldeak baditu, orduan G talde ebazgarria da.*

A. Eranskina

Ariketa ebatziak

Ariketa 1. Izan bitez m eta n zenbaki oso positiboak non n, m-gatik zatigarria den. Izan bedi σ, n luzerako S_n-ko zikloa. Frogatu, σ^m zikloa n/m luzerako m ziklo disjuntuen biderkadura dela.

Ebazpena. Izan bedi $\sigma = (a_1 a_2 \dots a_n) \in S_n$, n luzerako zikloa. m-k n zatitzen duenez, $n = m \cdot r$ da $r \in \mathbb{N}$ izanik. Ikus dezagun lehenik kasu erraz batzuk:

- $m = 2$ denean, n bikoitia da. Kasu honetan, ondoko eskeman ikusiko den moduan, azpiindizeen arteko biko saltoak daude, $\sigma^m = \sigma^2$ kalkulatzerakoan:

$$\begin{array}{l} a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \\ a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} a_4 \\ a_3 \xrightarrow{\sigma} a_4 \xrightarrow{\sigma} a_5 \\ a_4 \xrightarrow{\sigma} a_5 \xrightarrow{\sigma} a_6 \end{array}$$

  Honela,

$$\sigma^2 = \sigma \circ \sigma = (a_1 a_2 \dots a_n) \circ (a_1 a_2 \dots a_n) = \\ (a_1 a_3 a_5 \dots a_{n-1})(a_2 a_4 a_6 \dots a_n)$$

  da. Ikusten den bezala, ziklo bakoitza $n/2$ luzerakoa da lehenengo zikloan azpiindize bakoitikoak daudelarik eta bestean azpiindize bikoitikoak.

- $m = 3$ denean, ondoko eskema jarraitzen da, $\sigma^m = \sigma^3$ kalkulatzerakoan:

$$\begin{array}{l} a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} a_4 \\ a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} a_4 \xrightarrow{\sigma} a_5 \\ a_3 \xrightarrow{\sigma} a_4 \xrightarrow{\sigma} a_5 \xrightarrow{\sigma} a_6 \\ a_4 \xrightarrow{\sigma} a_5 \xrightarrow{\sigma} a_6 \xrightarrow{\sigma} a_7 \\ a_5 \xrightarrow{\sigma} a_6 \xrightarrow{\sigma} a_7 \xrightarrow{\sigma} a_8 \\ a_6 \xrightarrow{\sigma} a_7 \xrightarrow{\sigma} a_8 \xrightarrow{\sigma} a_9 \end{array}$$

Kasu honetan, ikus daitekeen bezala hiruko saltoak dira. Beraz,

$$\sigma^3 = \sigma \circ \sigma \circ \sigma = (a_1 a_2 \dots a_n) \circ (a_1 a_2 \dots a_n) \circ (a_1 a_2 \dots a_n) = (a_1 a_4 a_7 \dots)(a_2 a_5 a_8 \dots)(a_3 a_6 a_9 \dots)$$

da. Hau da, σ^3, 3 ziklo disjuntuen biderkadura da, ziklo bakoitza $n/3$ luzerakoa izanik.

Orain, ikus dezagun orokorrean m kasurako. Kasu honetan, m luzerako saltoak egongo dira, σ^m kalkulatzerakoan.

$$\sigma = (a_1 a_2 \dots a_n) = (a_1 a_2 \dots a_m a_{m+1} a_{m+2} \dots a_{2m} a_{2m+1} \dots a_{(r-1)m+1} a_{(r-1)m+2} \dots a_{(r-1)m+m} = a_{mr} = a_n)$$

Beraz, σ^m-ren adierazpena ondokoa da,

$$(a_1 a_{m+1} a_{2m+1} \dots a_{(r-1)m+1})(a_2 a_{m+2} a_{2m+2} \dots a_{(r-1)m+2}) \dots (a_m a_{2m} \dots a_n)$$

$n = m \cdot r$ izanik. Hau da, σ^m, m ziklo disjuntuen biderkadura da, ziklo bakoitza $n/m = r$ luzerakoak izanik. □

Ariketa 2. Frogatu G talde finitua eta $G/Z(G)$ ziklikoa bada, orduan G talde abeldarra dela. Beraz, $Z(G) = G$ dela.
Iradokizuna: Izan bedi $G/Z(G) = \langle gZ(G) \rangle$ non $g \in G$. Erakutsi, $x \in G$ edozein elementu, $g^r z$ eran idatz daitekeela, r zenbaki osoa eta $z \in Z(G)$ izanik.

Ebazpena. Izan bedi $G/Z(G)$ ziklikoa. Orduan, existitzen da $\bar{g} = gZ(G) \in G/Z(G)$ non $G/Z(G) = \langle gZ(G) \rangle$, $g \in G$ izanik. Bestalde, G taldearen zentrua modu honetan definitzen da: $Z(G) = \{g \in G : gg' = g'g, \forall g' \in G\} = \{g \in G : g = g^{g'}, \forall g' \in G\}$. Jakina da, $Z(G)$ talde abeldarra dela eta gainera $Z(G) \leq G$ dela. Baina, are gehigo $Z(G) \trianglelefteq G$ da. Orain, $G = \langle gZ(G), Z(G) \rangle = \langle g, Z(G) \rangle$. Izan bedi $Z(G) = \{z_1, \dots, z_k\}$. Orduan, edozein $x \in G$ emanda, $x = g^{r_1} z_1^{l_1} g^{r_2} z_2^{l_2} \dots g^{r_s} z_s^{l_s}$ eran idatz daiteke $0 \leq s \leq k$ izanik eta $l_i \in \mathbb{Z}$, $\forall i \in \{1, \dots, k\}$. Gainera, $z_1, \dots, z_s \in Z(G)$ direnez, $x = g^{r_1} g^{r_2} \dots g^{r_s} z_1^{l_1} z_2^{l_2} \dots z_s^{l_s} = g^m z$ eran adieraz daiteke, $m \in \mathbb{Z}$ eta $z \in Z(G)$ izanik. Beraz, $x \in G$ edozein elementu, $g^m z$ eran idatz daiteke .

Orain, $Z(G) = G$ dela ikusteko, bi partekotasunak ikusi behar dira. Argi dago $Z(G) \subseteq G$ dela. Beraz ikus dezagun $G \subseteq Z(G)$ partekotasuna. Izan bitez $g^m z_1$ eta $g^l z_2$, G-ko edozein bi elementu. Orduan, $(g^m z_1)(g^l z_2) = g^m g^l z_1 z_2 = g^{m+l} z_2 z_1 = g^{l+m} z_2 z_1 = g^l g^m z_2 z_1 = (g^l z_2)(g^m z_1)$ da, eta ondorioz $g^m z_1 \in Z(G)$, nahi genuen bezala. Hortaz, $Z(G) = G$ betetzen da, eta ondorioz G talde abeldarra da. □

Ariketa 3. Izan bedi $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0\}$.

(i) Frogatu G taldea $GL_2(\mathbb{R})$-ren azpitaldea dela.

(ii) Frogatu $H = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a = c = 1, b \in \mathbb{R}\} = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R}\}$, G-ren azpitaldea dela.

(iii) Ikusi $H \cong (\mathbb{R}, +)$ dela.

(iv) Aurkitu G-n bi ordenako elementu guztiak.

(v) Erakutsi bigarren ordenako bi elementuen arteko biderkadura ordena infinituko elementua izan daitekeela.

Ebazpena. (i) Gogora dezagun $GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A \neq 0\}$ ohiko biderketarekin taldea dela. Argi dago, $G \subseteq GL_2(\mathbb{R})$ betetzen dela. Izan bitez $A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ eta $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ G-ko edozein bi matrize. Orduan, $B^{-1} = \frac{adj(B)^t}{\det B} = \frac{\begin{pmatrix} c_2 & 0 \\ -b_2 & a_2 \end{pmatrix}^t}{a_2c_2} = \begin{pmatrix} 1/a_2 & -b_2/a_2c_2 \\ 0 & 1/c_2 \end{pmatrix}$ da. Beraz, $AB^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} 1/a_2 & -b_2/a_2c_2 \\ 0 & 1/c_2 \end{pmatrix} = \begin{pmatrix} a_1/a_2 & (-a_1b_2/a_2c_2) + b_1/c_2 \\ 0 & c_1/c_2 \end{pmatrix}$ da. $G \leq GL_2(\mathbb{R})$ frogatzeko, AB^{-1}, G-ko elementua dela frogatu behar dugu, eta hau, G-ko edozein A eta B-rentzako. Hau nabaria da, $\frac{a_1}{a_2}\frac{c_1}{c_2} = \frac{a_1c_1}{a_2c_2} \neq 0$ delako.

(ii) Kasu honetan, argi dago $H \subseteq G$ dela. Izan bitez $A = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}$ eta $B = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}$, H-ko edozein bi elementu. Orduan, $B^{-1} = \frac{adj(B)^t}{\det B} = \frac{\begin{pmatrix} 1 & 0 \\ -b_2 & 1 \end{pmatrix}^t}{1} = \begin{pmatrix} 1 & -b_2 \\ 0 & 1 \end{pmatrix}$ da. Eta, $AB^{-1} = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -b_2 + b_1 \\ 0 & 1 \end{pmatrix}$. Argi dago $AB^{-1} \in H$ dela, $-b_2 + b_1 \in \mathbb{R}$ baita. Beraz, $H \leq G$ azpitaldea da.

(iii) Defini dezagun H eta $\mathbb{R}$-ren arteko hurrengo aplikazioa: $f\colon (H, \cdot) \longrightarrow (\mathbb{R}, +)$, non edozein $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ matrizeari b zenbaki erreala dagokion. Izan bitez $A = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}$ eta $B = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}$, H-ko edozein bi matrize. Lehenik, ikus dezagun f talde homomorfismoa dela, hau da $f(AB) = f(A) + f(B)$ dela. Alde batetik, $AB = \begin{pmatrix} 1 & b_2 + b_1 \\ 0 & 1 \end{pmatrix}$ da. Honela,

$f(AB) = b_2 + b_1 = f(A) + f(B)$ betetzen da. Beraz, f talde homomorfismoa da. Orain, ikus dezagun f bijektiboa dela. Horretarako injektibotasuna eta suprajektibotasuna ikusiko ditugu. Izan bitez $A, B \in H$ non $f(A) = f(B)$, hau da, $b_1 = b_2$ baldintza betetzen delarik. Orduan, $A = B$ da, eta honenbestez, f injektiboa da. Izan bedi edozein $b_1 \in \mathbb{R}$, orduan existitzen da $A = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \in H$ non $f(A) = b_1$ den. Ondorioz, f ere suprajektiboa da. Beraz, f talde homomorfismo bijektiboa da, hau da, f isomorfismoa da eta $H \cong (\mathbb{R}, +)$ da.

(iv) Izan bedi $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$ non $a, b, c \in \mathbb{R}$ eta $ac \neq 0$. Azter ditzagun zeintzuk mota horretako matrizeak diren bigarren ordenakoak, hau da, $o(A) = 2$ betetzen dutenak. Horretarako, $A \cdot A = I_2$ betetzen duten matrizeak bilatu behar ditugu. Orain $A \cdot A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a^2 & ab + bc \\ 0 & c^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ da baldin eta soilik baldin $a^2 = 1, ab + bc = 0$ eta $c^2 = 1$ badira. Hau da, $a = 1$ edo $a = -1$, $c = 1$ edo $c = -1$ eta $b(a + c) = 0$ direnean. Azter ditzagun ondoko kasuak:

- $a = 1$ eta $c = 1$ direnean, $b = 0$ da. Honela, $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ dugu.
- $a = 1$ eta $c = -1$ direnean, b edozein izan daiteke. Honela, $A = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ dugu, edozein $b \in \mathbb{R}$.
- $a = -1$ eta $c = 1$ direnean, b edozein izan daiteke. Honela, $A = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ dugu, edozein $b \in \mathbb{R}$.
- $a = -1$ eta $c = -1$ direnean, $b = 0$ da. Honela, $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ dugu, edozein $b \in \mathbb{R}$.

Beraz, G-ko bigarren ordenako elementu posible guztiak, $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$, $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $A_3 = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ eta $A_4 = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ dira, edozein $b \in \mathbb{R}$ izanik. Bestalde ohartu, $A^2 = I_2$ izateak ez duela inplikatzen $o(A) = 2$ izatea derrigorrez. Izan ere, $A^2 = I_2$ izateak $o(A)$-k 2a zatitzen duela inplikatzen du. Bereziki, $A_1 = I_2$ lehen ordenako matrize bakarra denez, A_2, A_3 eta A_4 dira bigarren ordenako matrize bakarrak.

(v) Izan bitez $A = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ eta $B = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ bigarren ordenako G-

ko matrizeak non $b \neq 0$ den. Orduan, $AB = \begin{pmatrix} -1 & 2b \\ 0 & -1 \end{pmatrix}$ da. Bila dezagun $AB = C$ matrizearen ordena:

$$C^2 = C \cdot C = \begin{pmatrix} 1 & -4b \\ 0 & 1 \end{pmatrix}$$
$$C^3 = C \cdot C \cdot C = \begin{pmatrix} -1 & 6b \\ 0 & -1 \end{pmatrix}$$
$$C^4 = C \cdot C \cdot C \cdot C = \begin{pmatrix} 1 & 8b \\ 0 & 1 \end{pmatrix}$$

Orokorrean, $C^n = \begin{pmatrix} (-1)^n & (-1)^{n+1}2nb \\ 0 & (-1)^n \end{pmatrix}$, edozein n zenbaki arruntarentzat. Argi ikus daitekeen moduan, C matrizearen ordena infinitua da, $b \neq 0$ delako.

□

Ariketa 4. (i) Idatzi A_4 taldearen elementu guztiak eta bilatu elementu bakoitzaren ordena.

(ii) Frogatu $Z(A_4) = 1$ dela.

(iii) Erakutsi A_4 taldeak lau ordenako V azpitalde bakarra duela, eta ondorioztatu $V \trianglelefteq A_4$.

(iv) Frogatu A_4-k ez duela sei ordenako azpitalderik.

Ebazpena. (i) Ezaguna denez, A_4 taldea laugarren mailako talde alternatua da, bere elementuak permutazio bikoitiak direlarik (3 luzerako zikloak edo bi trasposizioen biderkadurak). Bestalde, $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 3 \cdot 2^2$ da. Ondorioz, A_4-ko elementuak ondokoak dira:

$$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132),$$
$$(124), (142), (134), (143), (234), (243)\}.$$

Gainera, A_4 taldea S_4 talde simetriko ez abeldarraren azpitaldea da. Baina, are gehiago, $A_4 \trianglelefteq S_4$ da, eta $|S_4 : A_4| = 2$. A_4-ko elementu bakoitzaren ordena hurrengo zerrendan erakusten da:

$1 \to 1$	$(123) \to 3$
$(13)(24) \to 2$	$(124) \to 3$
$(12)(34) \to 2$	$(132) \to 3$
$(14)(23) \to 2$	$(142) \to 3$
$(134) \to 3$	$(143) \to 3$
$(234) \to 3$	$(243) \to 3$

(ii) Lehenik, gogora dezagun $Z(A_4) = \{\sigma \in A_4 : \sigma\tau = \tau\sigma, \forall \tau \in A_4\}$ dela. Absurdora eramanez, demagun $Z(A_4) \neq 1$ dela. Orduan, existitzen da $1 \neq \epsilon \in A_4$, non $\epsilon \in Z(A_4)$ den. Bestalde, bataren desberdinak diren A_4-ko elementu guztiak 2 eta 3 ordenako elementuak dira. Beraz, hurrengo bi kasuak bereizten dira:

- $o(\epsilon) = 2$ denean, $\epsilon \in Z(A_4)$ izateagatik, bereziki existitzen da $\eta \in A_4$ non $o(\eta) = 3$ eta ϵ-ekin trukatzen dena. Orduan, existitzen da $\tau = \epsilon\eta \in A_4$ non $o(\tau) = 3 \cdot 2 = 6$ den. Eta hau kontraesana da; izan ere A_4-n ez dagoelako 6 ordenako elementurik.
- $o(\epsilon) = 3$ denean, $\epsilon \in Z(A_4)$ izateagatik, bereziki existitzen da $\gamma \in A_4$ non $o(\gamma) = 2$ eta ϵ-ekin trukatzen dena. Orduan, existitzen da $\sigma = \epsilon\gamma \in A_4$ non $o(\sigma) = 3 \cdot 2 = 6$ den. Eta hau kontraesana da; izan ere A_4-n ez dagoelako 6 ordenako elementurik.

Beraz, ez da existitzen 1-aren desberdina den $\epsilon \in A_4$ elementua non $\epsilon \in Z(A_4)$ den. Ondorioz, $Z(A_4) = 1$ da.

(iii) Izan bedi V lau ordenako A_4-ren azpitaldea. Orduan, jakina da V azpitalde abeldarra dela (ikusi adibidez, Sylow-en Teoremen aplikazioaren atalaren hasieran, ikusten diren emaitzetariko bat). Gainera, V azpitalde ziklikoen biderkadura zuzena bezala deskonposa daiteke, eta $|V| = 4$ denez, hurrego aukera posible bakarrak ditugu,

$$C_4 \cong C_{2^2} \text{ edo } C_2 \times C_2.$$

Baina, $V \cong C_4$ izango balitz, A_4-n 4 ordenako elementuren bat egongo litzateke, eta hau kontraesana da (i) atalagatik. Beraz, $V \cong C_2 \times C_2$ da, non $C_2 = \langle a \rangle$ eta $C_2 = \langle b \rangle$ diren, $a, b \in A_4$ bi ordenako elementuak izanik. Honela, $V \cong C_2 \times C_2 = \langle a \rangle \times \langle b \rangle$ da, eta $V = \{1, a, b, ab\}$ litzateke. (Bereziki, $o(ab) = mkt(o(a), o(b)) = 2$ da, a eta b edozein A_4-ko bi ordenako elementu izanik). Edozein kasuan, A_4 taldeak 4 ordenako V azpitalde bakarra du, eta azpitalde hori bakarra izateagatik, $V \trianglelefteq A_4$ da.

(iv) Absurdora eramanez, demagun A_4-k 6 ordenako azpitalde bat duela: H alegia. Orduan, $|A_4 : H| = 2$ da, eta honenbestez $H \trianglelefteq A_4$. Bestalde, 6 ordenako talde isomorfo desberdinak $C_6 \cong C_2 \times C_3$ edo $S_3 \cong D_6 = \langle a, b : a^3 = 1, b^2 = 1, a^b = a^{-1} \rangle$ dira, lehenengoa abeldarra eta bigarrena ez abeldarra izanik. Orain izan bedi V, (iii) ataleko 4 ordenako azpitalde bakarra. Orduan, $H \cap V \leq H, V$ izateagatik, $|H \cap V|$-ren aukera posibleak 1 edo 2 dira.

- $|H \cap V| = 2$ denean, $|V : H \cap V| = 2$ da, hortaz $H \cap V \trianglelefteq V$ da eta baita $H \cap V \trianglelefteq A_4$ ere. Bereziki $H \cap V \leq Z(A_4)$ dugu, eta

$|H \cap V|$-k, $|Z(A_4)|$ zatitzen du. Orain, (ii) erabiliz, $|H \cap V| = 1$ dela ondorioztatzen da, hipotesiaren kontrakoa.

- $|H \cap V| = 1$ bada, orduan $V/1 \cong VH/H$ denez, $|VH/H| = |VH|/|H| = 4$ da. Ondorioz, $|VH| = 4 \cdot 6 = 24$ da, baina $VH \leq A_4$ izateagatik, $24 = |VH|$-k $|A_4| = 12$ zatitzen du, eta hau kontraesana da.

Beraz, A_4-k ez du 6 ordenako azpitalderik.

□

Ariketa 5. Ariketa honetan, lanaren sarreran aipatutako ondoko emaitzaren frogapena garatuko da oinarrizko baieztapenak erabiliz, eta Sylow-en teoriako emaitzak kontuan hartu gabe: edozein ordena bikoitiko talde finitu batek gutxienez 2 ordenako elementu bat du. (Cauchy-ren emaitzaren ondorio zuzena da.)

Froga. Izan bedi G ordena bikoitiko talde finitua. Defini ditzagun $T = \{x \in G : x^2 = 1\}$ eta $U = \{x \in G : x^2 \neq 1\}$ G taldearen bi azpimultzo. Erraz ikus daiteke $T \cap U = \emptyset$ eta $T \cup U = G$ direla. Beraz, $|G| = |T| + |U| - |T \cap U| = |T| + |U|$ da.

Orain, ondoko galderari erantzuna bilatuko diogu: zenbat elementu ditu U multzoak? Hasiera batean bi aukera ditugu. Alde batetik, baldin eta $U = \emptyset$ bada, orduan $|U| = 0$ litzateke. Hau da, U-n ez dago elementurik. Beste aldetik, baldin eta $U \neq \emptyset$ bada, orduan U-n elementuren bat dago. Har dezagun $x_1 \in U$. Orduan, definizioz $x_1^2 = x_1 x_1 \neq 1$ da, eta honela x_1-en desberdina den x_1^{-1} elementua ere U-n dago. Orain, berriro ere bi aukera ditugu. Alde batetik, gerta daiteke U-n soilik bi elementu horiek egotea, hau da, $U = \{x_1, x_1^{-1}\}$ izatea edo gehiago egotea. Lehenengo kasuan, $|U| = 2$ izango litzateke, hau da, U-k bi elementu ditu. Beste aldetik, gerta daiteke U-n x_1 eta x_1^{-1} elementuen desberdina den beste elementuren bat egotea. Kasu honetan, har dezagun $x_2 \in U$ non $x_2 \neq x_1$ eta $x_2 \neq x_1^{-1}$ den. Orduan, aurrekoan bezala definizioz, $x_2^2 = x_2 x_2 \neq 1$ da, eta honela x_2-ren desberdina den x_2^{-1} elementua ere U-n dago. Gainera, ziurta dezakegu $x_2^{-1} \neq x_1$ eta $x_2^{-1} \neq x_1^{-1}$ direla, $x_2 \neq x_1^{-1}$ eta $x_2 \neq x_1$ baitira. Orain berriro ere beste bi kasu ditugu. Alde batetik U-n soilik $x_1, x_1^{-1}, x_2, x_2^{-1}$ elementuak egotea, hau da, $U = \{x_1, x_1^{-1}, x_2, x_2^{-1}\}$ izatea, eta horrenbestez $|U| = 4$ izatea edo gehiago egotea.

Prozedura errepikatuz U multzoko elementu guztiekin bukatu arte, konturatzen gara, edozein kasuan $|U|$ bikoitia dela. Gainera, hipotesiz $|G|$ bikoitia denez, $|G| = |T| + |U|$ berdintzatik, $|T|$-k ere bikoitia izan behar duela ondorioztatzen da. Gainera, $T \neq \emptyset$, behintzat $1 \in T$ dagoelako. Honela, $|T| \geq 2$ eta bikoitia da. Beraz, existitzen da $t \in T \setminus \{1\}$ elementuren bat

non $t^2 = 1$ den. Orain $o(t)|2$ eta $o(t) \neq 1$ dira. Beraz derrigorrez, $o(t) = 2$ da, hau da, t inboluzio bat da, nahi genuen bezala. □

Ariketa 6. Frogatu ondoko propietatea $|G|$-ren gaineko indukzioa erabiliz. Baldin eta G talde abeldar finitua bada, non p zenbaki lehenak $|G|$ zatitzen duen, orduan G-k p ordeneko elementu bat du. (Ez dugu Sylow-en teoriako emaitzarik erabiliko.)

Ebazpena. Izan bedi G talde abeldar finitua non $p \Big| |G|$ den, p zenbaki lehena izanik. Hau da, $|G| = p \cdot n$ non $n \geq 1$ den. (Suposa dezakegu $n > 1$ dela. Bestalde, $|G| = p$ da, $G \cong C_p$ eta emaitza berehalakoa da). Har dezagun $K \neq 1$, G-ren azpitalde propioa. Orduan, G talde abeldarra denez, K azpitalde abeldarra da, eta bereziki $K \lhd G$ da. Beraz, bi aukera daude, p-k $|K|$ zatitzen duenean, eta p-k ez duenean $|K|$ zatitzen, baina bai p-k $|G/K|$ zatitzen duenean. Orduan,

(i) $p \Big| |K|$ denean, nola $|K| < |G|$ denez, hipotesi induktiboa erabiliz existitzen da K-n p ordenako elementua. Bereziki, elementu hori G-n ere dago.

(ii) $p \not\Big| |K|$ eta $p \Big| |G/K|$ direnean. Hasieran, K azpitaldearen aukeragatik, $K \neq 1$ denez, $|G/K| < |G|$ da, eta G/K ere abeldarra da. Beraz, hipotesi induktiboa G/K-ri aplikatuz, G/K-n existitzen da p ordenako elementu bat, $\bar{x} = xK$ non $x \in G$ den. Orain, $o(\bar{x})|o(x)$ denez, $o(x) = p \cdot a$ da $a \geq 1$ izanik. Amaitzeko, x^a elementua hartuz gero, $o(x^a) = p$ da, eta $x^a \in G$ dago.

□

Ariketa 7. G talde baten zentrua hurrengo moduan definitzen da,

$$Z(G) = \{g \in G : gx = xg, \forall x \in G\}.$$

Erakutsi $Z(G) = \operatorname{Ker} \tau$ dela, non $\tau \colon G \to \Sigma_G$ homomorfismoa honela definituta dagoen: $\tau(g) = \tau_g \colon G \to G$, non $\tau_g(x) = g^{-1}xg$ den, eta $\tau_g \in \operatorname{Aut} G$ izanik. Ondorioztatu $Z(G) \trianglelefteq G$ eta $\operatorname{Inn} G \cong \frac{G}{Z(G)}$ direla.

Ebazpena. Lehenik, $Z(G) = \operatorname{Ker} \tau$ dela ikusiko da.

$$\operatorname{Ker} \tau = \{g \in G : \tau(g) = id_G\} = \{g \in G : g^{-1}xg = x, \forall x \in G\} = \{g \in G : xg = gx, \forall x \in G\} = Z(G).$$

Orain, $\operatorname{Ker} \tau \trianglelefteq G$ eta $Z(G) = \operatorname{Ker} \tau$ direnez, $Z(G) \trianglelefteq G$ da. Amaitzeko, Isomorfiaren Lehenengo Teorema dela eta, $G/\operatorname{Ker} \tau = G/Z(G) \cong \operatorname{Im} \tau = \tau(G)$ da. Orain, $\operatorname{Im} \tau = \tau(G) = \{\tau(g) : g \in G\} = \{\tau_g : g \in G\}$ da, baina definizioz, $\operatorname{Inn} G = \{\tau_g : g \in G\} \subseteq \operatorname{Aut} G$ denez, $\frac{G}{Z(G)} \cong \operatorname{Inn} G$ da. □

Ariketa 8. Izan bitez $\alpha \in \operatorname{Aut} G$ eta G talde finitua. Orduan, definizioz α puntu finko gabekoa da baldin eta α-ren bitartez G-ren finkatutako puntuen azpimultzoa tribiala bada, hau da, $\alpha(g) \neq g$ bada, $1 \neq g \in G$ edozein elementu izanik. (Oharra: "Puntu finko gabeko" terminoa estandarra da. Agian, hizkuntza abusua da. Izan ere, edozein taldeko automorfismok identitate elementua finkatzen baitu. Automorfismo batek taldeko identitate elementua ez den beste edozein elementu ez badu finkatzen, puntu finko gabekoa dela esaten da.)

Suposa dezagun α, G talde finitu baten puntu finko gabeko automorfismoa dela. Frogatu $\{\alpha(g)g^{-1} : g \in G\} = G$ dela. Bestalde, $o(\alpha) = 2$ bada, ondorioztatu $\alpha(x) = x^{-1}$ dela, $x \in G$ guztietarako, eta G talde abeldarra dela.

Ebazpena. Defini dezagun $\phi\colon G \to G$ aplikazioa, non $g \in G$ guztietarako $\phi(g) = \alpha(g)g^{-1}$ den. Ikus dezagun ϕ aplikazioa injektiboa dela:

$$\phi(g_1) = \phi(g_2) \Rightarrow \alpha(g_1)g_1^{-1} = \alpha(g_2)g_2^{-1} \Rightarrow \alpha(g_1)g_1^{-1}g_2 = \alpha(g_2) \Rightarrow$$
$$\alpha(g_2)^{-1}\alpha(g_1)g_1^{-1}g_2 = 1_G \Rightarrow \alpha(g_2^{-1}g_1) = (g_1^{-1}g_2)^{-1} = g_2^{-1}g_1$$

dugu. Nola α puntu finko gabekoa denez, aurrekotik $g_2^{-1}g_1 = 1$ dela lortzen da, eta ondorioz, $g_1 = g_2$ dugu. Beraz, ϕ injektiboa eta $|G| < \infty$ direnez, ϕ supraiektiboa da. Hau da, ϕ bijektiboa da. Hortaz, $|G| = n < \infty$ dela suposatuz,

$$\begin{aligned} g_1 &\longrightarrow \alpha(g_1)g_1^{-1} \in G \\ g_2 &\longrightarrow \alpha(g_2)g_2^{-1} \in G \\ &\vdots \\ g_n &\longrightarrow \alpha(g_n)g_n^{-1} \in G \end{aligned}$$

dugu, eta orduan $\{\alpha(g_1)g_1^{-1}, \alpha(g_2)g_2^{-1}, \ldots, \alpha(g_n)g_n^{-1}\}$ elementu desberdinekin, berriro ere G talde osoa lortzen da, hau da, $G = \{\alpha(g)g^{-1} : g \in G\}$ da.

Orain, suposa dezagun $o(\alpha) = 2$ dela, hau da, $\alpha^2 = \alpha \circ \alpha = 1_G$ dela. Beraz, $\alpha(\alpha(x)) = x$ da, $x \in G$ guztietarako. Orain, $x \in G$ guztietarako existitzen da $g_x \in G$ non $\alpha(g_x)g_x^{-1} = x$ den. Alde batetik azken adierazpen honi α automorfismoa aplikatuz,

$$\alpha(x) = \alpha(\alpha(g_x)g_x^{-1}) = \alpha(\alpha(g_x))\alpha(g_x^{-1}) = g_x(\alpha(g_x))^{-1}$$

dugu. Eta bestalde, adierazpenari alderantzizkoa aplikatuz,

$$x^{-1} = (\alpha(g_x)g_x^{-1})^{-1} = (g_x^{-1})^{-1}(\alpha(g_x))^{-1} = g_x(\alpha(g_x))^{-1}.$$

Ondorioz, $\alpha(x) = x^{-1}$ da.

Azkenik, G talde abeldarra dela ikusiko da. Horretarako, α automorfismoa eta, $\alpha(x) = x^{-1}$ edozein $x \in G$-rako direla erabiliz,

$$\forall x, y \in G\text{-rako, } (xy)^{-1} = \alpha(xy) = \alpha(x)\alpha(y)$$

dugu. Nola $(xy)^{-1} = y^{-1}x^{-1} = \alpha(y)\alpha(x)$ den, $\alpha(x)\alpha(y) = \alpha(y)\alpha(x)$ dela ondorioztatzen da. Hau da, $x^{-1}y^{-1} = y^{-1}x^{-1}$ da, eta ondorioz G talde abeldarra da.

□

Bibliografia

[1] John S. Rose, A Course on Group Theory, Cambridge University Press, 1978.

[2] Michio Suzuki, Group Theory I, Springer-Verlag, 1982.

[3] W. R. Scott, Group Theory, Dover, 1987.

[4] Harvey E. Rose, A Course on Finite Groups, Springer, 2009.

[5] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963), 775-1029.

[6] R. Brauer and K. A. Fowler, On groups of even order, Ann. of Math. (2) 62 (1955), 565-83.