Zuhaitz infinituak eta beren simetriak: kontradibideen iturburua talde-teorian

Gustavo A. Fernández Alcober eta *Amaia Zugadi Reizabal*

Matematika Saila, Euskal Herriko Unibertsitatea
48080 Bilbao
gustavo.fernandez@ehu.es, azugadi001@ikasle.ehu.es

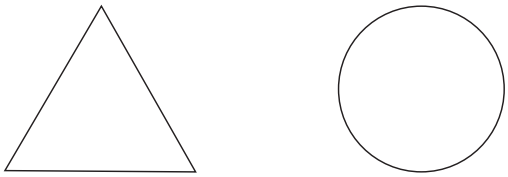
Laburpena: Taldearen kontzeptu matematikoa definitzen dugu, simetriaren ideia intuitiboa neurtzeko tresna modura. Zuhaitz erregular infinituen simetria handia erabiliz, Burnsideren Problema Orokorraren kontradibide bat ematen dugu, *Gupta-Sidkiren taldea* delakoa. Talde hori finituki sortua da, bere elementu guztiak ordena finitukoak dira, baina, hala ere, talde infinitua da. Emaitza hori frogatzeko behar diren taldeen propietate guztiak garatzen ditugu, hutsetik hasita.

Abstract: We introduce the mathematical concept of a group, which is a means of measuring the intuitive notion of symmetry. Using the high symmetry of infinite regular trees, we exhibit a counterexample to the General Burnside Problem, the so-called *Gupta-Sidki group*. This is a finitely generated group in which all elements have finite order, but it is nevertheless infinite. We develop from scratch all properties of groups which are necessary to prove this fact.

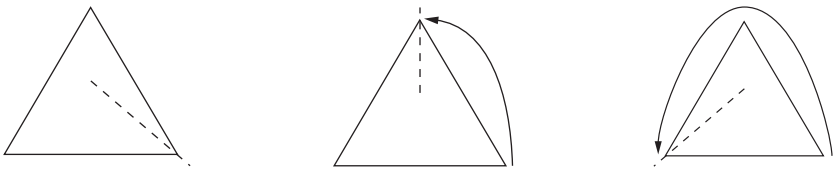
1. TALDEAK SIMETRIAREN NEURRI MODURA

Matematika zenbakiekin batera jaio zen eta, dudarik gabe, zenbakien sorrera eta arrakasta gizakiaren neurtzeko beharrari zor dizkiogu. Luzerak, azalerak edo bolumenak zenbaki bat emanez zehazten ditugu, eta zenbakien erabilerarik oinarrizkoena, kontatzea, neurtzeko modu bat baino ez da. Beste neurketa batzuetarako ordea, zenbakiak ez dira nahikoak eta objektu matematiko korapilatsuagoak asmatu behar ditugu. Hori gertatzen da *simetria* neurtu nahi dugunean. Simetria denok barneraturik dugun kontzeptua da; garbi dugu, adibidez, aurpegi bat simetrikoa dela[1] edo zirkunferentzia bat triangelu bat baino simetrikoagoa dela.

[1] Egia esan, gainetik begiratuta bakarrik. Izan ere, aurpegi bat eta aurpegi berdinaren erdiarekin ispilu eginez lortzen den irudia alderatzen baditugu, ezustekoak har ditzakegu. Ikusi adibidez [1], pertsonaia famatu batzuen asimetriaz jabetzeko, edo [2] norberarena ikusteko.



Baina, nola eman diezaiekegu gorpuzkera matematikoa ideia intuitibo horiei? Horretarako, honako ohar hau funtsezkoa da: objektu batean simetria nabaritzen dugunean, sumatzen ari gara mugimendu bat, objektuaren itxuraren gainean batere eraginik ez duena. Horrelako mugimendu bat objektuaren *simetria* bat dela esango dugu. Adibidez, aurpegi bat simetrikoa iruditzen zaigu aurpegiaren eskuinaldea eta ezkerraldea elkarrekin trukatuz gero funtsean irudi bera lortzen dugulako. Antzera, triangelu ekilatero bat bere erdiko puntuaren (barizentroaren) inguruan biratzen badugu, orduan triangelua bere horretan mantenduko da, baldin eta biraketaren angelua 120 edo 240 gradukoa bada, eta ez beste inoiz. Beraz, bi biraketa horiek triangeluaren simetriak dira.



Zehatz hitz eginda, zero graduko biraketa ere triangeluaren simetria da. Mugimendu honek puntu guztiak beren lekuan uzten dituenez, *identitatea* deitzen diogu. Ohartu bedi, bestetik, biraketa barizentroa ez den beste puntu baten inguruan eginez gero, triangelua aldatuta agertuko dela beti. Laburbilduz, planoko biraketa posible guztien artean, hiru baino ez dira triangelu ekilateroaren simetriak. Zer gertatzen da, ordea, zirkunferentziarekin? Kasu honetan ere biraketa zirkunferentziaren zentroaren inguruan egin behar dugu, baina alde nabarmena dago triangeluarekin alderatuta: orain biraketa guztiak dira simetriak! Beraz, biraketetara murrizten bagara, triangeluak hiru simetria baino ez dituen bitartean, zirkunferentziak infinitu simetria ditu (egia esan, kopuru ez-kontagarri bat). Biraketez gain, bai triangeluak bai zirkunferentziak badituzte simetria gehiago, *erreflexioak* deitutakoak, alegia. Baina erreflexioetan ere zirkunferentziak «∞ eta 3» irabazten dio triangeluari. Horrela, zirkunferentzia triangelua baino askoz ere simetrikoagoa den ideia intuitiboa formulazio matematiko baten bitartez azaltzea lortu dugu.

Zer gertatzen da objektu baten bi simetria, f eta g, hartzen baditugu eta horien *konposizioa* egiten badugu, hau da, bata bestearen atzetik aplikatzen baditugu? Konposizio hori fg idatziz adieraziko dugu. Simetriaren

definizioagatik, *f*-k eta *g*-k ez dute objektuaren itxura aldatzen eta, beraz, garbi dago *fg*-k ere ez duela ezer aldatuko. Hau da, *f* eta *g* objektu baten simetriak badira, orduan *fg* konposizioa ere simetria da. Adibidez, triangeluaren kasuan, 120 eta 240 graduko simetrien konposizioa 360 graduko biraketa da, eta hau identitatea baino ez da, beste simetria bat alegia. Bestetik, *f* simetria bakoitzak badu alderantzizko bat, f^{-1} ikurraren bidez adieraziko duguna. Alderantzizko honek *f*-k egin duena desegiten du: f^{-1} *f*-ren atzetik konposatzerakoan puntu bakoitza bere lekura itzultzen da, hau da, identitatea lortzen dugu. Adibidez, 120 graduko biraketaren alderantzizkoa –120 graduko biraketa da (hots, 120 gradu biratzea erlojuko orratzen norantzan).

Simetrien propietate hauek behin «distilaturik», taldearen kontzeptu abstraktua eman dezakegu. Artikulu honen ardatza taldeen propietate batzuen azterketa izango da, hain zuzen ere.

1.1. **Definizioa**

Izan bedi G multzoa, eragiketa batez hornitua: $g, h \in G$ bi edozein elementu izanik, definiturik dago bien arteko eragiketaren emaitza, gh modura idatziko duguna. (Hori dela-eta, talde orokor batekin ari garenean, eragiketari biderketa deituko diogu.) Demagun eragiketa honek propietate hauek betetzen dituela:

(i) Elkartze-propietatea: $(fg)h = f(gh)$ dugu, $f, g, h \in G$ guztietarako.
(ii) Identitatearen existentzia: Existitzen da $1 \in G$ non $g1 = g = 1g$ den $g \in G$ guztietarako.
(iii) Alderantzizkoen existentzia: $g \in G$ bakoitzeko, existitzen da $g^{-1} \in G$ non $gg^{-1} = 1 = g^{-1}g$.

Orduan, emandako eragiketarekiko *G taldea* dela esango dugu.

Esate baterako, definizioaren aurretik argudiatutakoaren arabera, irudi baten simetriek talde bat osatzen dute. Horrela, tresna egoki bat aurkitu dugu irudien simetria neurtzeko: taldeak. Zenbat eta elementu gehiago izan irudiaren simetrien taldeak, orduan eta simetrikoagoa da irudia. Hala ere, simetrien taldeak ez dira taldeen adibide bakarrak. Zenbakien bitartez ere talde asko lor daitezke; esaterako, zenbaki osoek, arrazionalek, errealek edo konplexuek taldea osatzen dute batuketarekiko. Beste adibide garrantzitsu bat *permutazioen taldea* da: *n* zenbaki arrunt bat finkaturik, talde hau $\{1, \ldots, n\}$ multzoaren permutazio (aplikazio bijektibo) guztiek osatzen dute; edo bestela esanda, zenbaki hauek berrordenatzeko modu guztiek. Talde hau S_n ikurraren bidez adierazten dugu. Adibideen aniztasun honetan datza kontzeptu abstraktua definitzearen abantaila: egoera asko eta zerikusi handirik gabekoak lantzeko gai izan gaitezke, teoria bakar bat garatuz.

Edozein kasutan, artikulu honetan gehienetan erabiliko ditugun taldeak simetriarekin lotuta agertuko dira.

Triangeluaren hiru biraketak 120 graduko biraketatik (dei diezaiogun f) lor daitezke konposizioaren bitartez. Izan ere, $f^2 = ff$ konposizioa 240 graduko biraketa da eta $f^3 = f^2 f$ identitatea da. Horregatik, f-k biraketa horien taldea sortzen duela esaten dugu. Oro har, G taldea bada, S azpimultzo batek G *sortzen duela* (edo S G-ren *sistema sortzailea* dela) esango dugu G-ko elementu guztiak lor badaitezke S-ko elementuen eta beren alderantzizkoen biderkadura gisa. Hau da, G-ko elementuak itxura honetako biderkadurak badira:

$$x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}, \quad x_i \in S \quad \text{eta} \quad \varepsilon_i \in \{1, -1\} \text{ izanik.} \tag{1}$$

Hemen, n, faktoreen kopurua, edozein izan daiteke. Taldea *finituki sortua* dela esango dugu azpimultzo finitu baten bidez sor badaiteke. Hori da triangeluaren biraketen kasua: talde hori elementu bakar baten bidez sor daiteke. Hala ere, zirkunferentziaren biraketen taldea ez da finituki sortua. Hori ikusteko, ohartu bedi alde batetik finituki sortutako talde bat zenbakigarria dela beti, (1)etik ondorioztatzen den bezala, eta bestetik zirkunferentziaren biraketen kopurua jarraikiaren kardinala dela, [0, 360) tarteko angeluei dagozkien biraketa guztiak desberdinak baitira.

Dakusagunez, sortzaileen kopuruak badu zerikusia taldearen tamainarekin. Hala ere, sortzaileen kopuruak ez du determinatzen taldea finitua den edo ez. Adibidez, triangeluaren biraketen taldea elementu bakar baten bidez sor daiteke eta finitua da. Aitzitik, $\mathbb{Z}$ zenbaki osoen multzoa, infinitua da, nahiz eta hau ere elementu bakar batek sortzen duen (adibidez, 1 zenbakiak; ohartu kasu honetan eragiketa batuketa dela). Oro har, G taldea g elementuak sortzen badu, orduan (1) aplikatuz,

$$G = \{g^n \mid n \in \mathbb{Z}\}$$

dugu eta G finitua den edo ez jakiteko, $g^n = g^m$ noiz gertatzen den zehaztu behar dugu. Horretarako, funtsezkoa da ondoren definitzen dugun kontzeptua.

1.2. **Definizioa**

Izan bitez G taldea eta $g \in G$. Existitzen bada $n \geq 1$ non $g^n = 1$ den, berretzaile horien arteko txikienari g-ren ordena deituko diogu. Bestela, g-ren ordena infinitua dela esango dugu.

Horrela, 120 graduko biraketaren ordena 3 da, baina α irrazionala bada, α graduko biraketa ordena infinitukoa da. Izan ere, azken horren berreturak $n\alpha$ graduko biraketak dira ($n \in \mathbb{N}$ izanik), eta $n\alpha$ ez denez inoiz 360ren

multiploa, berretura horiek ezin dira identitatea izan. Beste alde batetik, $\sigma \in S_n$ permutazioa erregela honen bitartez emanda badago,

$$1 \longmapsto 2 \longmapsto \ldots \longmapsto n-1 \longmapsto n \longmapsto 1,$$

orduan σ-ren ordena n da. Hemendik aurrera, permutazio hau adierazteko, $(1 \ldots n)$ idatziko dugu.

1.3. **Teorema**

Izan bitez G taldea eta g ∈ *G,* k *ordenakoa. Orduan,*

(i) k *finitua bada,* g^n *edozein berretura* $\{1, g, \ldots, g^{k-1}\}$ *multzoko elementu baten berdina da. Zehazkiago,* n k*-rekin zatitzen badugu eta* r *bada lortzen dugun hondarra, orduan* $g^n = g^r$ *dugu. Ondorioz,* $g^n = 1$ *dugu baldin eta soilik baldin* n k*-ren multiploa bada, eta* $g^m = g^n$ *berdintza dugu baldin eta soilik baldin* m – n *diferentzia* k*-ren multiploa bada.*

(ii) k *infinitua bada,* $g^m = g^n$ *berdintza dugu baldin eta soilik baldin* m = n *bada.*

Frogapena

(i) Zatitzen badugu n k-rekin, orduan $n = qk + r$ deskonposizioa lortzen dugu, $0 \leq r < k$ izanik. Beraz,

$$g^n = g^{qk+r} = (g^k)^q g^r = g^r$$

dugu. Orduan, $g^n = 1$ eta $g^r = 1$ baldintzak baliokideak dira. Baina, ordenaren definizioagatik eta $0 \leq r < k$ izateagatik, $g^r = 1$ gertatzeko modu bakarra $r = 0$ izatea da, hots, $n = qk$ izatea. Ondorioz, $g^n = 1$ dugu baldin eta soilik baldin n k-ren multiploa bada. Azkenik, $g^m = g^n$ dugu baldin eta soilik baldin $g^{m-n} = 1$ bada eta, ikusi berri dugun bezala, hau $m - n$ k-ren multiploa denean gertatzen da.

(ii) Ordenaren definizioagatik, k infinitua bada, $g^n = 1$ gertatzeko modu bakarra $n = 0$ izatea da. Beraz, $g^m = g^n$ dugu baldin eta soilik baldin $m = n$ bada.

1.4. **Korolarioa**

Izan bedi G = ⟨g⟩ *elementu bakar baten bidez sor daitekeen taldea. Orduan,* G*-ren kardinala g-ren ordenaren berdina da.*

1.5. **Korolarioa**

Izan bitez G *taldea eta* g ∈ G. *Demagun* $g^{p^n} = 1$ *dela,* p *zenbaki lehena eta* n ≥ 0 *zenbaki osoa izanik. Orduan,* g*-ren ordena* p*-ren berretura da. Bereziki,* $g^p = 1$ *eta* g ≠ 1 *bada, orduan* g*-ren ordena* p *da.*

Frogapena

Izan bedi k g-ren ordena. Orduan, $g^{p^n} = 1$ baldintzak k finitua dela ziurtatzen du eta, 1.3 teorema erabiliz, p^n k-ren multiploa da. Beraz, g-ren ordena p-ren berretura da.

Askotan, G talde baten barruan beste talde batzuk aurkituko ditugu. Adibidez, biraketei baino ez badiegu begiratzen, triangeluaren hiru simetriak zirkunferentziaren simetria berezi batzuk dira. Ideia hau formalizatzea interesatzen zaigu.

1.6. **Definizioa**

Izan bitez G taldea eta H G-ren azpimultzo bat. Orduan, H G-ren *azpitaldea* dela diogu H G-ren eragiketarekiko taldea baldin bada. Hala bada, $H \leq G$ idatziko dugu propietate hau adierazteko.

Azpimultzo bat azpitaldea den edo ez ikusteko, taldearen definizioko baldintza batzuk ez ditugu zertan egiaztatu, ondorengo teoremak erakusten duen bezala.

1.7. **Teorema**

Izan bitez G *taldea eta* H G*-ren azpimultzo ez-hutsa. Orduan,* H G*-ren azpitaldea da baldin eta soilik baldin bi propietate hauek betetzen badira:*

(i) h, k ∈ H *badugu, orduan* hk ∈ H.
(ii) h ∈ H *badugu, orduan* h^{-1} ∈ H.

Honen frogapena erraz eman dezake irakurleak berak. Sarrerako atal hau bukatzeko, elementuen ordenak gordetzen dituen eragiketa bat definituko dugu, konjugazioa alegia.

1.8. **Definizioa**

Izan bitez G taldea eta x, $g \in G$. Orduan $x^g = g^{-1}xg$ elementua x-ren *konjugatua* dela esaten dugu, g-ren bitartez.

1.9. **Teorema**

Elementu batek eta bere konjugatu batek ordena bera dute.

Frogapena

Izan bitez G taldea eta $x,\ g \in G$, eta ikus dezagun x^g-ren ordena x-ren ordena bera dela. Horretarako, ohartu

$$(x^g)^n = (g^{-1}xg)\ .\overset{n}{.}.\ (g^{-1}xg) = g^{-1}x^ng$$

dela $n \in \mathbb{N}$ guztietarako. Beraz, $(x^g)^n = 1$ dugu baldin eta soilik baldin $g^{-1}x^ng = 1$ bada, eta berdintza hau, ezkerraldean g-z eta eskuinaldean g^{-1}-ez biderkatuz, baliokidea da $x^n = 1$ izatearekin. Beraz, 1 ematen duten x^g-ren lehenengo berretura eta x-ren lehenengo berretura berretzaile berberarekin lortzen dira.

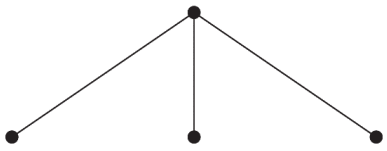
Azpitaldeen artean, interes berezia dute konjugazioaren bidez finko gelditzen direnek.

1.10. **Definizioa**

Izan bitez G taldea eta $N \leq G$. Orduan, N G-ren *azpitalde normala* dela esango dugu, eta $N \lhd G$ idatziko dugu, $x^g \in N$ bada $x \in N$ eta $g \in G$ guztietarako.

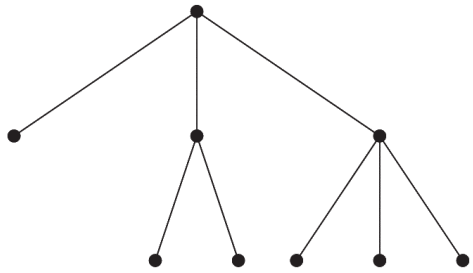
2. ZUHAITZAK ETA BEREN AUTOMORFISMOAK

Atal honetan zuhaitz batzuen simetriak aztertuko ditugu. Zer adierazi nahi dugu matematikariok «zuhaitz» esaten dugunean? Definizio formala eman beharrean, zuhaitzaren eraikuntza-prozedura deskribatuko dugu. Zuhaitza irudi geometriko lau bat da, bi osagai mota dituena: alde batetik, *erpinak,* planoko puntuak direnak, eta bestetik, *ertzak,* erpin batzuk lotzen dituzten zuzenkiak. Eraikuntzaren abiapuntua erpin bat da, zuhaitzaren *erroa* deituko dioguna. Horretatik ertz batzuk aterako dira beherantz, nahi beste, baina kopuru finitu bat. Ertz horien beheko muturretan zuhaitzaren beste erpin batzuk izango ditugu, eta horiek osatuko dute zuhaitzaren *lehenengo maila.*



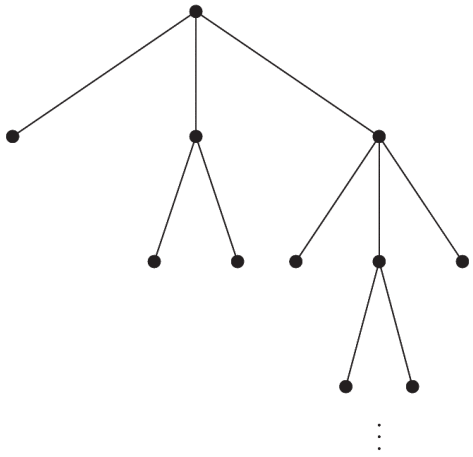
Erroa eta lehenengo maila.

Ondoren, gauza bera egingo dugu lehenengo mailako erpinekin: ertzak aterako ditugu, eta horrela zuhaitzaren bigarren mailako erpinak lortuko ditugu. Ez dugu zertan ertz kopuru bera jarri lehenengo mailako erpin guztietan, eta onargarria da erpin batzuetatik ertz bat ere ez ateratzea. Horrela, ez badugu ertzik jartzen inongo erpinetan, orduan zuhaitza bukatutzat emango dugu. Bestela, zuhaitzaren bigarren mailan erpinen bat izango dugu eta erpin horietan ertzak jartzen jarraituko dugu, hirugarren mailara pasatuz. Prozedura hau behin eta berriz errepikatuz, gelditzen garen unean zuhaitz bat izango dugu, mailaz maila osatua.



Zuhaitz finitu bat.

Litekeena da inoiz gelditu nahi ez izatea, eta orduan zuhaitz infinitu bat lortuko dugu. Hori da kasua, adibidez, beheko irudian:

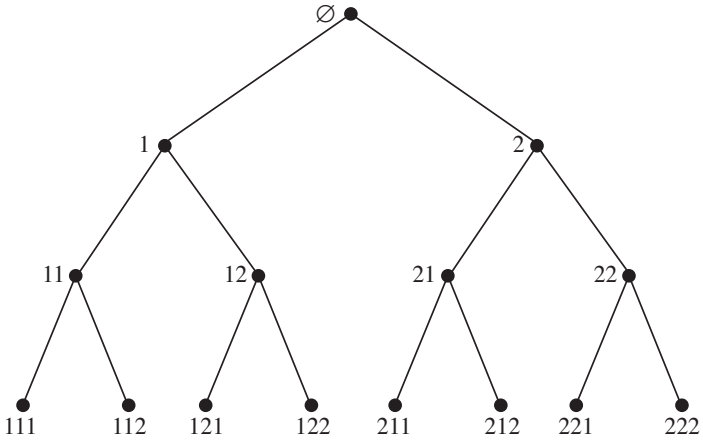


Zuhaitz infinitu bat.

Beraz, zuhaitz matematikoek naturako zuhaitzen itxura dute, baina bi diferentzia nagusi ditugu: lehenengoa, garrantzitsuena, infinituak izan daitezkeela; bigarrena, estetiko hutsa, beherantz hazten direla, gorantz egin beharrean. Baina, tira, beti pentsa dezakegu antipodetako zuhaitz bat ikusten ari garela!

Artikulu honetan interesatzen zaizkigun zuhaitzak ahal den simetrikoenak dira: erpin guztietatik ertz kopuru bera ateratzen da, infinituraino. Kopuru hori d bada, *zuhaitz d-adikoa* deituko diogu zuhaitz berezi horri, eta $\mathcal{T}_d$ ikurraren bidez adieraziko dugu. Ez badago zalantzarik d-ren balioari buruz, edo ez bazaigu bereziki interesatzen d-ren balioa azpimarratzea, $\mathcal{T}$ erabiliko dugu besterik gabe zuhaitz hau izendatzeko.

Zuhaitz d-adikoekin lan egiterakoan, komenigarria da erpinak izendatzeko sistema bat ezartzea. Horretarako, erroa $\varnothing$ ikurraren bitartez adieraziko dugu, eta horretatik eskegitzen diren erpinak 1-etik d-raino zenbakituko ditugu, ezkerretik eskuinera. Ondoren, 1 erpinetik ateratzen diren erpinei $11, \ldots, 1d$ etiketak ezarriko dizkiegu, eta hau bera errepikatuko dugu erpin guztiekin: v erpin batetik eskegitzen diren erpinak v-ri 1-etik d-rako zenbakiak atzizki modura jarriz izendatuko ditugu, hau da, $v1, \ldots, vd$ deituko diegu.



Zuhaitz d-adikoaren ezaugarri nagusi bat bere autoantzekotasuna da. Izan bedi v zuhaitzeko edozein erpin. Orduan, v-tik eskegita zuhaitz infinitu bat dugu, eta hau berriro ere zuhaitz d-adikoa da. Lehenengo mailako erpinetatik ateratzen diren zuhaitzei, bereziki, *azpizuhaitz nagusiak* deituko diegu. Ohartu i. azpizuhaitz nagusiko erpinak iv motakoak direla, $v \in \mathcal{T}_d$ izanik.

Zuhaitz d-adikoaren simetriak definitzeko orduan, plano osoaren mugimenduak hartu beharrean (zuhaitz d-adikoa ez da ia inoiz finko gelditzen biraketa baten edo erreflexio baten bidez), erpinen mugimenduak hartuko ditugu, hau da, erpinak erpinetara eramaten dituzten aplikazioak. Erpinen mugimendu bat, f, zuhaitzaren simetria dela esango dugu bi propietate hauek betetzen baditu:

(i) f bijektiboa da, hots, banan-banan lotzen ditu erpin guztiak erpin guztiekin.

(ii) Bi erpin, u eta v, ertz baten bitartez konektaturik badaude zuhaitzean, orduan $f(u)$ eta $f(v)$ irudiak ere ertz baten bidez konektaturik daude.

Aljebran, ohikoagoa da f zuhaitzaren *automorfismo* bat dela esatea, eta terminologia honi lotuko gatzaizkio hemendik aurrera. Aurreko atalean irudien simetriekin argudiatu dugun moduan, ikus daiteke zuhaitzaren automorfismoek talde bat osatzen dutela konposizioarekiko. Talde hori izendatzeko $\mathrm{Aut}\mathcal{T}$ ikurra erabiliko dugu. Ohartu, automorfismoek taldea osatzen dutenez, baduela zentzua automorfismo baten ordenari buruz hitz egiteak.

Ondorengo teoreman, zuhaitz d-adikoaren automorfismoen oinarrizko propietate batzuk biltzen ditugu.

2.1. **Teorema**

Izan bedi f *zuhaitz* d*-adikoaren automorfismoa. Orduan,*

(i) $\mathrm{f}(\emptyset) = \emptyset$.
(ii) f*-k mailak gordetzen ditu; hau da,* υ *erpina* m. *mailan badago, orduan* $\mathrm{f}(\upsilon)$ *ere* m. *mailan dago. Beraz,* f*-k* m. *mailako* d^{m} *erpinen permutazio bat zehazten du.*

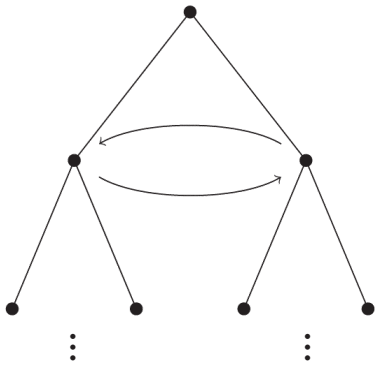
Frogapena

(i) Automorfismoaren definizioagatik, v edozein erpin izanik, v eta $f(v)$ erpin kopuru berarekin konektaturik daude. Orain, zuhaitz d-adikoan, erroa izan ezik, gainontzeko erpin guztiak $d + 1$ erpinekin konektaturik daude: d azpitik eta beste bat gainetik. Hori dela eta, $f(\emptyset) = \emptyset$ dugu nahitaez.
(ii) Hau m-ren gaineko indukzioaren bidez ikusiko dugu. Lehenengo eta behin, $m = 0$ denean (i) ataletik lortzen dugu emaitza. Orain, demagun m baino txikiagoak diren mailetarako betetzen dela, eta izan bedi v m. mailako erpin bat. Dei diezaiogun u zuhaitzaren $m - 1$. mailan eta v-ren gainean dagoen erpinari. Orduan, u eta v lotuta daudenez, $f(u)$ eta $f(v)$ ere konektaturik daude, f automorfismoa izateagatik. Indukzio hipotesiagatik, $f(u)$ zuhaitzaren $m - 1$. mailan dago eta, beraz, $f(v)$-rentzat bi aukera baino ez daude: m. mailan edo $m - 2$. mailan egotea. Absurdora eramanez, demagun azken aukera dugula. Berriro indukzio hipotesiagatik, f-k $m - 2$. mailako erpinen permutazio bat zehazten du; ondorioz, $m - 2$. mailan badago w erpin bat non $f(w) = f(v)$ den. Automorfismoaren (i) propietateagatik, hemendik $w = v$ lortzen dugu. Hau kontraesan bat da, v eta w maila desberdinetan baitaude. Beraz, $f(v)$-k m. mailan egon behar du.

Zuhaitz d-adikoaren automorfismo bat deskribatzeko, hasiera batean behintzat, erpin guztien irudiak eman behar ditugu. Aurreko teoremaren (i) atala ikusita, $\varnothing$ erroaren irudia zehazteko beharrik ez dago.

2.2. **Adibideak**

1) Zuhaitz 2-adikoaren kasuan, defini dezagun f mugimendua $f(0v) = 1v$ eta $f(1v) = 0v$ erregelen bitartez, $v \in \mathcal{T}$ guztietarako. Garbi dago f-k bi azpizuhaitz nagusiak elkartrukatu besterik ez duela egiten eta, ondorioz, f automorfismoa dela.



Ohartu f^2-k erpin bakoitza bere burura eramaten duela. Beraz, f^2 identitatea da eta f-ren ordena 2 da.

2) Aurreko adibidea erraz orokortu daiteke edozein zuhaitz d-adikotarako eta azpizuhaitz nagusiak berrordenatzeko edozein modutarako. Izan ere, $\sigma \in S_d$ $\{1, \ldots, d\}$ multzoaren permutazioa bada, orduan $f(iv) = \sigma(i)v$ definituz $i = 1, \ldots, d$ eta $v \in \mathcal{T}$ guztietarako, $\mathcal{T}$-ren automorfismo bat lortzen dugu. Automorfismo honek i. azpizuhaitz nagusia $\sigma(i)$.era eramaten du, eta mugimendu hau zurruna da: azpizuhaitzaren barruan ez dago inolako aldaketarik, azpizuhaitz batek beste baten lekua hartzen baitu pieza bakar bat balitz bezala. Horregatik, honelako automorfismoei *automorfismo zurrunak* deituko diegu. Erraz ikus daiteke, f bere buruarekin behin eta berriz konposatuz, f-ren ordena σ-ren ordenarekin bat datorrela. Automorfismo zurrunen artean, kasu hau interesatuko zaigu bereziki: $d = p$ zenbaki lehena denean eta $\sigma = (1 \ldots p)$ permutazioa denean. Artikulu honen lehenengo atalean ikusitakoaren arabera, automorfismo zurrun hau p ordenakoa da.

Zuhaitz d-adikoaren f eta g automorfismoek v erpina finkatzen badute, orduan garbi dago fg-k eta f^{-1}-ek ere v finko uzten dutela. Beraz, S erpin multzo bat bada, orduan S-ko erpinak finkatzen dituzten automorfismo guztiek Aut$\mathcal{T}$-ren azpitalde bat osatzen dute.

2.3. **Definizioa**

Izan bedi $m \geq 1$. Orduan, m. mailako erpin guztiak finkatzen dituzten automorfismoen multzoari m. mailaren *egonkortzailea* deituko diogu eta Stab(m) ikurraren bidez adieraziko dugu.

2.4. **Teorema**

Stab(m) Aut$\mathcal{T}$-ren azpitalde normala da $m \geq 1$ guztietarako.

Frogapena

Izan bitez $f \in$ Stab(m) eta $g \in$ Aut$\mathcal{T}$. Orain, v erpina m. mailan badago, orduan $g^{-1}(v)$ ere m. mailan dago eta, hori dela eta, $f(g^{-1}(v)) = g^{-1}(v)$ dugu. Beraz,

$$(f^g)\,(v) = (g^{-1}fg)(v) = g(f(g^{-1}(v))) = g(g^{-1}(v)) = v.$$

Ondorioz, f^g konjugatua Stab(m)-n dago eta Stab(m) Aut$\mathcal{T}$-ren azpitalde normala da.

Izan bedi $f \in$ Stab(1) eta finka dezagun erpin bat zuhaitzaren lehenengo mailan, hau da, $i \in \{1, \ldots, d\}$. Hartzen badugu $v \in \mathcal{T}$ erpin orokor bat, orduan $f(i) = i$ izateagatik, $f(iv) = iw$ dugu w erpin baterako. Orain, f $\mathcal{T}$-ren automorfismoa denez, $f_i(v) = w$ erregelak $f_i \in$ Aut$\mathcal{T}$ definitzen du. Horrela, f-ri elkartuta badugu $(f_1, \ldots, f_d)$ tupla bat, eta tupla honek guztiz deskribatzen du f automorfismoa: izan ere, $f(iv) = if_i(v)$ denez $i \in \{1, \ldots, d\}$ eta $v \in \mathcal{T}$ guztietarako, zuhaitzeko erpin guztien irudiak ezagutzen ditugu. Hau dela eta, $f = (f_1, \ldots, f_d)$ idatziko dugu. Notazio hau erabilita, nola biderkatzen dira Stab(1)-eko bi elementu?

2.5. **Teorema**

$(f_1, \ldots, f_d) \cdot (g_1, \ldots, g_d) = (f_1g_1, \ldots, f_dg_d)$ dugu. Hau da, tuplen notazioa erabiliz, Stab(1)-eko automorfismoak osagaiz osagai biderkatzen dira.

Frogapena

Ohartu gaitezen

$$(fg)\,(iv) = g(f\,(iv)) = g(if_i(v)) = ig_i(f_i(v)) = i(f_ig_i)(v)$$

dugula $i \in \{1, \ldots, d\}$ eta $v \in \mathcal{T}$ guztietarako.

Tuplen notazioaren abantaila bat da planteamenduari buelta eman diezaiokegula eta automorfismo berriak *definitzeko* erabil dezakegula. Adibidez, $\sigma = (1 \ldots d)$ bada eta $a_i \in$ Aut$\mathcal{T}$ σ^i-ri dagokion automorfismo zurruna

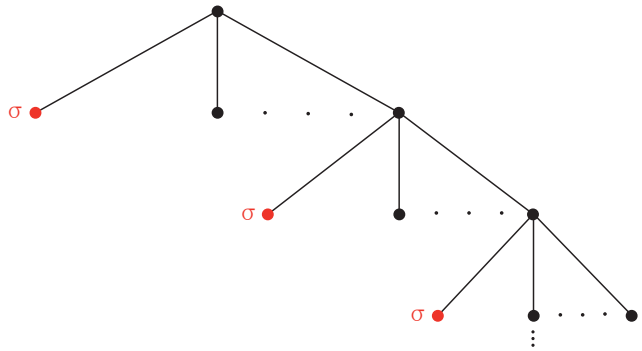
bada, orduan $f = (a_1, \ldots, a_d)$ egokitzapenak Stab(1)-eko automorfismo bat definitzen du. Ohartu f-k bigarren mailako erpinetatik eskegitzen diren d^2 azpizuhaitzak zurrunki permutatzen dituela, d-ko multzoetan, baina multzo bakoitza permutazio desberdin baten arabera.

Bestetik, errekurrentziak beste bide bat ematen digu automorfismoak definitzeko, zuhaitzaren autoantzekotasuna erabiliz. Ikus dezagun adibide bat. Izan bedi a, $\sigma = (1 \ldots d)$ permutazioari dagokion automorfismo zurruna eta defini dezagun $f = (a, 1, \ldots, 1, f)$. (Hemen, $d = 2$ bada, ulertuko dugu tarteko 1ak ez direla agertzen.) Hasiera batean, pentsa dezakegu f-ren definizioak ez duela zentzurik; azken batean, f definitzeko f bera erabiltzen ari gara! Hala ere, segituan erakutsiko dugun bezala, emandako informazioa nahikoa da f-ren irudia $\mathcal{T}$-ko edozein erpinen gainean ezagutzeko eta, horrenbestez, f guztiz determinaturik gelditzen da goiko definizioaren bitartez eta horrelako definizio errekurrenteak zentzuzkoak dira.

Har dezagun, bada, $v \in \mathcal{T}$ erpin orokor bat. Erpin hau lehenengo azpizuhaitz nagusiaren barruan badago, orduan $f = (a, 1, \ldots, 1, f)$ egokitzapenaren arabera, v-ren irudia a-k determinatzen du. Era berean, v bigarren, hirugarren, . . ., $(d - 1)$-garren azpizuhaitz nagusietako batean badago, orduan dagokion osagaian identitatea aurkitzen dugu $(a, 1, \ldots, 1, f)$ tuplan eta, ondorioz, $f(v) = v$ dugu. Arazo bakarra v azken azpizuhaitz nagusian dagoenean topatzen dugu, orduan f irakurtzen baitugu definizioko tuplan, eta f oraindik ere guztiz zehaztu gabe baitago. Ikus dezagun, hala ere, jakin dezakegula zein den $f(v)$. Alde batetik, $v = d$ lehenengo mailan badago, orduan $f \in$ Stab(1) definitu dugunez, $f(v) = v$ dugu nahitaez. Bestetik, $v \neq d$ bada, orduan $v = dw$ idatz dezakegu, $w \in \mathcal{T}$ izanik. Orain, $f = (a, 1, \ldots, 1, f)$ notazioaren esanahia aplikatuz, $f(v) = df(w)$ dugu eta w-ri aurretik esandako guztia aplika diezaiokegu; beraz, w ez badago azken azpizuhaitz nagusian, $f(w)$ ezaguna da. Horrela, erpin guztien irudia lortzen dugu f-ren bitartez, dd erpinetik eskegitzen den azpizuhaitzekoak kenduta. Baina, $f(dd) = df(d) = dd$ ere kalkula dezakegu, hau da, dd erpina finko gelditzen da. Gainera, $w \in \mathcal{T}$ bada, $f(ddw) = df(dw) = ddf(w)$ dugu eta aurreko argudioa errepika dezakegu. Orain, garbi dago prozedura honek edozein erpinen irudia emango digula. Laburbilduz,

(i) $v = d \ldots d$ motako erpina bada, orduan $f(v) = v$.
(ii) v ez bada mota horretakoa, idatz dezagun $v = d \ldots diw$, $i \in \{1, \ldots, d - 1\}$ eta $w \in \mathcal{T}$ izanik (litekeena da hasieran d-rik ez egotea). Orduan, $i = 1$ bada, $f(v) = d \ldots d1a(w)$ dugu eta $i \neq 1$ bada, berriz, $f(v) = v$.

Beheko irudian adierazten dugu f-ren ekintza zuhaitzaren gainean:



3. BURNSIDEREN PROBLEMA ETA GUPTA-SIDKIREN TALDEA

Izan bedi G talde finituki sortua, hau da, $G = \langle S \rangle$ jar dezakegu, $S = \{g_1, \ldots, g_r\}$ finitua izanik. Orduan, G-ko elementuen deskribapena (1) formulan eman dugu eta itxura honetakoak dira: $g = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$, non $x_i \in S$ eta $\varepsilon_i \in \{1, -1\}$ den. Orain, G taldea abeldarra baldin bada, orduan x_i eta x_j berdinak direnean, aukera dugu bi elementu hauek elkarrekin jartzeko. Ahal diren elementu guztiak biltzen baditugu, azkenean honelako adierazpen bat lortuko dugu:

$$g = g_1^{n_1} \ldots g_r^{n_r}, \qquad n_i \in \mathbb{Z} \text{ izanik.} \tag{2}$$

Ondorioz, honako emaitza hau lortzen dugu.

3.1. Teorema

Izan bedi G *talde abeldar finituki sortua eta demagun sistema sortzaile finitu baten elementu guztiak ordena finitukoak direla. Orduan,* G *finitua da.*

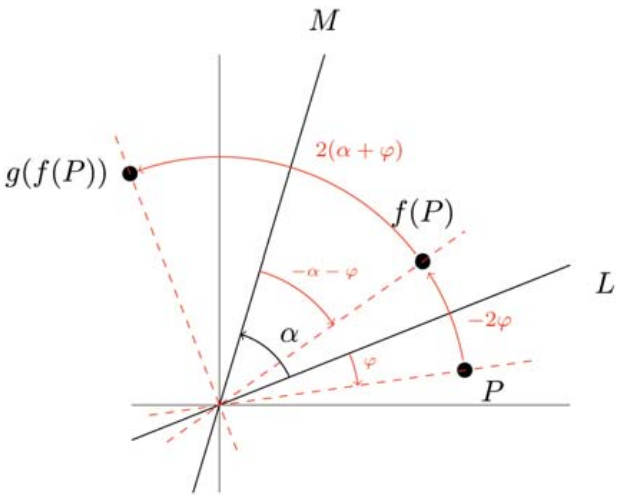
Frogapena

Demagun $S = \{g_1, \ldots, g_r\}$ enuntziatuko G-ren sistema sortzailea dela, eta izan bedi k_i g_i-ren ordena, $i = 1, \ldots, r$ guztietarako. Hartu $g \in G$ elementu orokor bat eta deskonposatu (2) adierazpenean bezala. Orduan, 1.3 teorema erabiliz, $g_i^{n_i}$ berreturak k_i balio desberdin har ditzake. Ondorioz, g-rentzako aukera desberdinak $k_1 \ldots k_r$ biderkadurak mugatzen ditu eta G finitua da.

Zein puntutaraino da egiazkoa aurreko teoremako propietatea, taldea abeldarra izateko baldintza kentzen badugu?

3.2. **Adibidea**

Izan bitez L eta M $\mathbb{R}^2$-ko jatorritik igarotzen diren bi zuzen eta demagun zuzen hauen arteko α angelua irrazionala dela. Zuzen hauek bi erreflexio zehazten dituzte, f eta g, eta hauek zirkunferentziaren simetriak dira. Ikus dezagun fg konposizioa 2α angeluko biraketa dela. Horretarako, P puntu orokor bat hartzen dugu planoan eta $(fg)(P)$ irudia zein den aztertzen dugu. Eman diezaiogun φ izena L zuzenak P puntuarekin osatzen duen angeluari.[2] Orduan, $f(P)$ lortzeko -2φ angeluaren arabera mugitu behar dugu P puntua. (Ohartu angelu hau P-ren menpekoa dela, f ez baita biraketa.) Orain, M zuzenak $-(\alpha + \varphi)$ angelua osatzen du $f(P)$-rekin eta, ondorioz, $(fg)(P) = g(f(P))$ puntua lortzeko $2(\alpha + \varphi)$ angeluaren arabera mugitu behar dugu $f(P)$. Horrenbestez, $(fg)(P)$ lortzeko P puntua 2α angeluaren arabera mugitu behar dugu. Angelu hau ez da P-ren menpekoa eta, hortaz, fg konposizioa 2α angeluko biraketa da.



Orain, $G = \{f, g\}$ jartzen badugu, orduan G taldea 2 ordenako bi elementuren bidez sortuta dago, baina hala ere G infinitua da. Izan ere, $fg \in G$ ordena infinituko biraketa da, 2α irrazionala izateagatik.

Aurreko adibidean, G taldea infinitua da ordena infinituko elementu bat duelako. Planteamendua pixka bat aldatuz, sortzaileak ordena finitukoak izateaz gain, eska genezake taldeko elementu guztiak ordena finitukoak izatea. Horrela, ondorengo problema azaltzen da.

---

[2] Honekin, L zuzenaren eta P puntua jatorriarekin lotzen duen zuzenaren arteko angelua adierazi nahi dugu.

Burnsideren Problema Orokorra

Izan bedi G talde finituki sortua eta demagun taldeko elementu guztiak ordena finitukoak direla. Ba al da finitua G taldea?

Problema honek William Burnside matematikari britainiarraren izena darama, bera izan baitzen esplizituki proposatu zuen lehenengoa, 1902 urtean (ikusi [4] erreferentzia). Honela zioen Burnsidek: «A still undecided point in the theory of discontinuous groups is whether the group order of a group may be not finite, while the order of every operation it contains is finite.» Hemen, inplizituki, taldea finituki sortua dela ulertzen da.

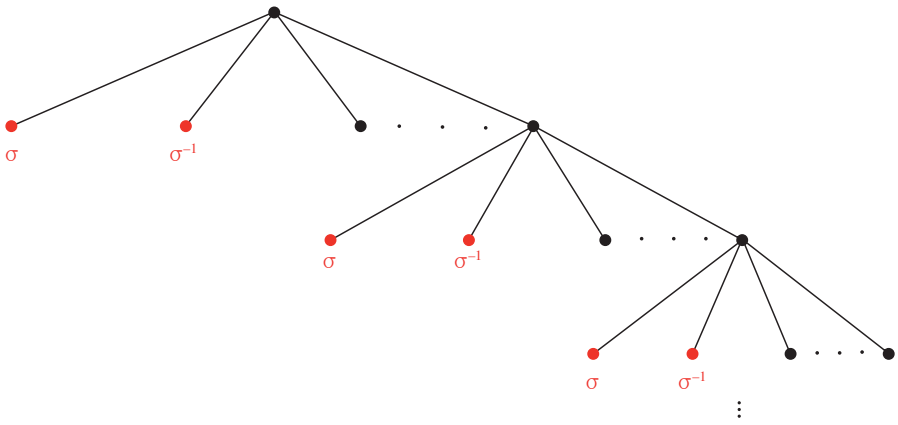
Problema honen ebazpena ez da batere tribiala, eta horren seinale da lehenengo kontradibidea ez zela eman 1964era arte, Evgeny Golod matematikari errusiarraren [5] artikuluan. Hortik aurrera adibide gehiago agertu ziren, eta horien artean nabarmena da 1983an Narain Gupta indiarrak eta Said Sidki palestinarrak eman zutena [6]. Guptaren eta Sidkiren taldea (gaur egun *Gupta-Sidkiren taldea* izenaz ezagutua) zuhaitz baten automorfismoen azpitalde bat da, eta artikulu honen gainerakoan talde honen eraikuntza aztertuko dugu eta, xehetasun guztiekin, Burnsideren Problema Orokorraren kontradibide bat dela frogatuko dugu.

3.3. **Definizioa**

Izan bedi $p > 2$ zenbaki lehena eta definitu zuhaitz p-adikoaren honako bi automorfismo hauek:

(i) a, $\sigma = (1 \ldots p)$ zikloari dagokion automorfismo zurruna.
(ii) b, errekurrentziaz emanda $b = (a, a^{-1}, 1, \ldots, 1, b)$ erregelaren bitartez. (Hemen, $p = 3$ bada, batak ez dira agertzen.)

Orduan, $G = \langle a, b \rangle$ taldeari *Gupta-Sidkiren taldea* deitzen zaio.



Ohartu bedi a eta b automorfismoak p ordenakoak direla. Hau garbi dago a-ren kasuan, σ zikloa p ordenakoa baita. Ikusteko b-ren ordena ere p dela, gogoan izan tuplen notazioa erabiltzen dugunean eragiketa osagaiz osagai egiten dela. Ondorioz,

$$b^p = (a^p, a^{-p}, 1, \ldots, 1, b^p) = (1, 1, \ldots, 1, b^p)$$

dugu eta errekurrentzia hau betetzeko $b^p = 1$ izan behar dugu nahitaez. Kontuan izanik $b \neq 1$ dela, 1.5 korolarioa aplikatuz b-ren ordena p dela lortzen dugu.

Hemendik aurrera, $p > 2$ zenbaki lehena finkatu egingo dugu, $\mathcal{T}$-k zuhaitz p-adikoa adieraziko du, eta agertuko diren automorfismo guztiak zuhaitz p-adikoarenak izango dira. Gainera, a eta b goian definituriko automorfismoak izango dira beti.

3.4. **Teorema** (Gupta-Sidkiren teorema)

Gupta-Sidkiren taldeko elementu guztien ordena finitua da, zehazkiago p*-ren berretura bat, baina hala ere taldea infinitua da.*

Teorema hau frogatzeko, lehenengo Gupta-Sidkiren taldea hobeto ezagutu behar dugu. Jar dezagun

$$\mathrm{Stab}_G(1) = G \cap \mathrm{Stab}(1).$$

Garbi dago $\mathrm{Stab}_G(1)$ G-ren azpitalde normala dela eta $\mathrm{Stab}_G(1)$-en barruan dagoen a-ren berretura bakarra 1 dela; edo bestela esanda, $\langle a \rangle \cap \mathrm{Stab}_G(1) = \{1\}$ dela.

3.5. **Lema**

Izan bedi G *Gupta-Sidkiren taldea. Orduan,* g ∈ G *elementu bakoitza* g = hn *moduan deskonposa daiteke, era bakar batean gainera,* h ∈ ⟨a⟩ *eta* n ∈ ⟨b, b^{a}, . . ., $\mathrm{b}^{\mathrm{a}^{p-1}}$⟩ *izanik.*

Frogapena

Sistema sortzailearen definizioagatik, $G = \langle a, b \rangle$ taldeko elementuak a, a^{-1}, b eta b^{-1} elementuekin egin daitezkeen biderkadura guztiak dira. Kasu honetan, a eta b automorfismoak p ordenakoak izateagatik, $a^{-1} = a^{p-1}$ eta $b^{-1} = b^{p-1}$ dugu. Beraz, alderantzizkoak ez ditugu behar. Horrela, $g \in G$ bakoitza lortzeko, a eta b elementuak hainbat aldiz hartu behar ditugu eta, modu zehatz batean tartekaturik, biderkatu behar ditugu. Honenbestez,

$$g = ababaabbab \tag{3}$$

bezalako adierazpenak dituzte G-ko elementuek.

Teoremak ziurtatzen duen deskonposizioaren existentzia frogatzeko, nahikoa da $ba = ab^a$ berdintza betetzen dela ohartzea eta, oro har,

$$b^{a^i} a = ab^{a^{i+1}} \tag{4}$$

dugula. Izan ere, (4) berdintzari esker, $g \in G$ elementu baten adierazpenean a-ren agerraldi guztiak ezkerraldera mugi ditzakegu, baina horretarako, b batzuen tokian b-ren konjugatuak jarri beharko ditugu, a-ren berreturen bitartez. Horrela, $g = hn$ deskonposizio bat lortuko dugu, h a-ren berretura izanik eta n, berriz, b^{a^i} moduko konjugatuen biderkadura bat izanik. Adibidez, goian (3) emandako g elementuaren kasuan, honela lortzen dugu deskonposizioa:

$$g = ababaabbab = a^2b^abaabbab = a^2b^aab^aabbab = a^3b^{a^2}b^aabbab = \\ = a^3b^{a^2}ab^{a^2}bbab = a^4b^{a^3}b^{a^2}bbab = \ldots = a^5b^{a^4}b^{a^3}b^ab^ab.$$

Azkenik, ohartu n-ren adierazpenean nahikoa dela $b, b^a, \ldots, b^{a^{p-1}}$ konjugatuak erabiltzea: a-ren ordena p denez, a^i edozein berretura $\{1, a, \ldots, a^{p-1}\}$ multzoaren barruan aurkitzen dugu beti, 1.3 teorema erabiliz.

Ikus dezagun orain deskonposizioaren bakartasuna. Horretarako, demagun $g = h_1n_1 = h_2n_2$ dela, $h_1, h_2 \in \langle a \rangle$ eta $n_1, n_2 \in \langle b, b^a, \ldots, b^{a^{p-1}} \rangle$ izanik. Orduan,

$$h_2^{-1} h = n_2n_1^{-1} \in \langle a \rangle \cap \langle b, b^a, ..., b^{a^{p-1}} \rangle \leq \langle a \rangle \cap \mathrm{Stab}_G(1) = \{1\}$$

dugu eta, ondorioz, $h_1 = h_2$ eta $n_1 = n_2$. Beraz, g-ren deskonposizioa bakarra da.

Aurreko lema dela eta, Gupta-Sidkiren taldean lan egiteko, funtsezkoa da b-ren konjugatuak ezagutzea a-ren berreturen bitartez. Ondorengo emaitzak esaten digu nola konjugatzen den, oro har, Stab(1)-eko elementu bat a automorfismoarekin.

3.6. **Lema**

Izan bedi $\mathrm{f} = (\mathrm{f}_1, \mathrm{f}_2, ..., \mathrm{f}_p) \in$ *Stab(1). Orduan,*

$$\mathrm{f}^a = (\mathrm{f}_p, \mathrm{f}_1, \ldots, \mathrm{f}_{p-1})$$

dugu.

Frogapena

Har dezagun erroaren desberdina den erpin bat, v, eta ikus dezagun enuntziatuko berdintzaren bi automorfismoek irudi bera dutela v-ren gai-

nean. Idatz dezagun $v = iw$, $i \in \{1, \ldots, p\}$ eta $w \in \mathcal{T}$ izanik. Orduan, $i \geq 2$ bada,

$$(f^a)(v) = (a^{-1}f\,a)(iw) = (f\,a)(i-1w) = a(i-1\,f_{i-1}(w)) = if_{i-1}(w)$$

dugu eta, bestetik, $i = 1$ bada,

$$(f^a)(v) = (a^{-1}f\,a)(1w) = (f\,a)(pw) = a(pf_p(w)) = 1f_p(w).$$

Bi berdintza hauek frogatzen dute f^a konjugatuak eta $(f_p, f_1, \ldots, f_{p-1})$ tuplak irudi bera dutela v-ren gainean.

Bereziki, hauexek dira b-ren konjugatuak a-ren berreturen bitartez:

$$\begin{aligned} b &= (a, a^{-1}, 1, 1, \ldots, 1, b), \\ b^a &= (b, a, a^{-1}, \ldots, 1, 1), \\ b^{a^2} &= (1, b, a, a^{-1}, \ldots, 1, 1), \\ &\vdots \\ b^{a^{p-1}} &= (a^{-1}, 1, 1, 1, \ldots, b, a). \end{aligned} \tag{5}$$

Ohartu konjugatu hauek guztiak p ordenakoak direla, 1.9 teorema aplikatuz. Notazioa sinplifikatzearren, hemendik aurrera b_i idatziko dugu b^{a^i}-ren ordez, $i \in \mathbb{Z}$ guztietarako. Kontuan izanik 1.3 teorema, i p-rekin zatitzearen hondarra r bada, orduan $b_i = b_r$ dugu eta, bestetik, $b_i = b_j$ dugu baldin eta soilik baldin $i - j$ diferentzia p-ren multiploa bada. Beraz, b_i automorfismo guztien artean, $b_0, \ldots, b_{p-1}$ dira posibilitate desberdin guztiak, eta hauek goian (5) emandako tuplak dira zehatz-mehatz. Hala ere, interesgarria da b_i ikurra eskuragarri izatea $i \in \mathbb{Z}$ guztietarako: horrela, (5)eko automorfismoak a-ren berreturekin konjugatu behar ditugunean,

$$b_i^{a^j} = (b^{a^i})^{a^j} = b^{a^{i+j}} = b_{i+j}$$

erlazioa erabil dezakegu, kezkatu gabe $i + j$ balioa $\{0, 1, \ldots, p-1\}$ multzotik ateratzen den edo ez.

Gupta-Sidkiren taldea infinitua dela frogatzeko, emaitza honetan oinarrituko gara.

3.7. **Lema**

Izan bitez A *multzoa eta* B A*-ren azpimultzo bat,* B ≠ A *izanik. Demagun existitzen dela* φ*:* B → A *aplikazio supraiektibo bat (hau da,* A*-ko elementu guztiak* B*-ko elementuen irudiak direla* φ*-ren bitartez). Orduan,* A *infinitua da.*

Frogapena

Absurdora eramanez, demagun A finitua dela. Orduan, B ere finitua da eta, B-ko elementu bakoitzak irudi bakar bat duenez, $\varphi : B \to A$ aplikazioaren irudien kopurua B-ren kardinala da gehienez jota. Baina, A finitua denez eta $B \neq A$ denez, kopuru hau A-ren kardinala baino txikiagoa da. Beraz, A-ko elementu guztiak ezin dira irudiak izan φ-ren bitartez. Honek A infinitua dela frogatzen du.

3.8. **Teorema**

Gupta-Sidkiren taldea infinitua da.

Frogapena

Izan bedi $N = \langle b_0, b_1, \ldots, b_{p-1} \rangle$. Orduan, $N \leq \mathrm{Stab}_G(1)$ dugu eta N-ko elementuak tupla modura ikus daitezke; hain zuzen ere, (5)eko tuplen biderkadura gisa. Izan bedi φ tuplen lehenengo osagaiari dagokion proiekzioa. Tuplak osagaiz osagai biderkatzen direnez, φ-ren irudiak (5)eko lehenengo osagaien biderkadura posible guztiak dira, hau da, a, b, 1 eta a^{-1}-ekin egin daitezkeen biderkadura guztiak. Kontuan izanik $G = \langle a, b \rangle$ dela, $\varphi : N \to G$ supraiektiboa dela ondorioztatzen dugu. Bestalde, N ez da G talde osoaren berdina, $a \in G$ ez baitago lehenengo mailaren egonkortzailean. Aurreko lema aplikatuz, G-k infinitua izan behar du.

Izan bedi $g \in G$ eta idatz dezagun, 3.5 leman bezala, $g = hn$, $h \in \langle a \rangle$ eta $n \in \langle b_0, \ldots, b_{p-1} \rangle$ izanik. Orduan, n elementua b_i automorfismoen biderkadura gisa jar daiteke, beharbada modu bat baino gehiagotan. Biderkadura horietan faktoreen kopuruari begiratzen badiogu eta ahal den txikiena aukeratzen badugu, zenbaki horri g-ren *luzera* esaten zaio eta $\ell(g)$ ikurraren bidez adierazten dugu. Ohartu $\ell(g) = 0$ dugula baldin eta soilik baldin $g \in \langle a \rangle$ bada. Ikus ditzagun luzeraren propietate batzuk.

3.9. **Lema**

Izan bitez $g_1, g_2 \in G$. *Orduan,* $\ell(g_1 g_2) \leq \ell(g_1) + \ell(g_2)$ *dugu.*

Frogapena

Jarri $r = \ell(g_1)$ eta $s = \ell(g_2)$, eta idatzi

$$g_1 = a^i b_{i_1} \ldots b_{i_r} \quad \text{eta} \quad g_2 = a^j b_{j_1} \ldots b_{j_s}.$$

Orduan, 3.5 lemaren frogapenean erabilitako argudioa errepikatuz,

$$g_1 g_2 = a^{i+j} b_{i_1}^{a^j} \ldots b_{i_r}^{a^j} b_{j_1} \ldots b_{j_s} = a^{i+j} b_{i_1+j_1} \ldots b_{i_r+j} b_{j_1} \ldots b_{j_s}$$

dugu eta, ondorioz, $\ell(g_1 g_2) \leq r + s$.

3.10. **Lema**

Izan bedi $n \in \langle b_0, \ldots, b_{p-1} \rangle$, $n \neq 1$, *eta idatz dezagun* $n = (n_1, \ldots, n_p)$ *tupla modura. Orduan, bi aukera hauetako bat betetzen da:*

(i) n *elementua* b_i *automorfismo baten berretura da.*
(ii) $\ell(n_i) < \ell(n)$, $i = 1, \ldots, p$ *guztietarako.*

Frogapena

Jarri $r = \ell(n)$ eta ohartu $r \geq 1$ dela, $n \neq 1$ izateagatik. Orduan, $n = x^{(1)} \ldots x^{(r)}$ dugu, $x^{(j)} \in \{b_0, \ldots, b_{p-1}\}$ izanik $j = 1, \ldots, r$ guztietarako. Idatzi $x^{(j)} = (x_1^{(j)}, \ldots, x_p^{(j)})$ tupla bezala. Finka dezagun i indize bat 1-etik p-ra bitartean eta azter dezagun $\ell(n_i)$ balioa. Tuplak osagaiz osagai biderkatzen direnez, $n_i = x_i^{(1)} \ldots x_i^{(r)}$ berdintza dugu eta, 3.9 lema erabiliz,

$$\ell(n_i) \leq \ell(x_i^{(1)}) + \ldots + \ell(x_i^{(r)}). \tag{6}$$

Orain, begiratzen badiogu (5)eko automorfismoen i. osagaiari, bi aukera ditugu:

a) Osagai hori a, a^{-1} edo 1 da eta, beraz, 0 luzerakoa da.
b) Osagai hori b da eta, beraz, 1 luzerakoa da. Hau automorfismoa b_i denean baino ez da gertatzen.

Honen arabera, eta (6) desberdintza ikusita, $\ell(n_i) < r$ ez betetzeko posibilitate bakarra $x^{(j)}$ guztiak b_i-ren berdinak izatea da. Azken kasu honetan n b_i-ren berretura da eta teorema frogaturik gelditzen da.

Azkenik, zenbakien teoriako oinarrizko emaitza hau behar dugu.

3.11. **Lema**

Izan bitez p *zenbaki lehena eta* i *eta* j *bi zenbaki oso finko. Orduan,* j *ez bada* p*-rekin zatigarria, {*i, i + j, i + 2j, . . ., i + *(*p – *1)*j*} multzoko elementuak* p*-rekin zatitzerakoan, {0, 1, 2, . . .,* p *– 1} hondar posible guztiak lortzen dira (ez halabeharrez ordena berean).*

Frogapena

Hondarrak 0 eta $p - 1$ artean daudenez beti, nahikoa da frogatzea $i + \lambda j$ eta $i + \mu j$ zenbakien hondarrak desberdinak direla $0 \leq \lambda < \mu \leq p - 1$ denean. Absurdora eramanez, demagun $i + \lambda j = qp + r$ eta $i + \mu j = q'p + r$ dela, $0 \leq r \leq p - 1$ izanik. Kendura eginez, $(\mu - \lambda)j = (q' - q)p$ lortzen dugu. Hemendik, p lehena denez eta j ez denez p-ren multiploa, p-k $\mu - \lambda$ zatitzen duela lortzen dugu. Hau ez da posible, $0 < \mu - \lambda \leq p - 1$ baita.

3.12. **Teorema**

Gupta-Sidkiren taldeko elementu guztien ordena p*-ren berretura da.*

Frogapena

Har dezagun $g \in G$ elementu bat eta froga dezagun g-ren ordena p-ren berretura dela $\ell(g)$-ren gaineko indukzioaz. Baldin eta $\ell(g) = 0$ bada, orduan $g \in \langle a \rangle$ dugu. Beraz, g a-ren berretura da eta, $a^p = 1$ denez, $g^p = 1$ ere betetzen da. Orduan, 1.5 korolarioa aplikatuz, g-ren ordena 1 edo p da.

Demagun orain $\ell(g) \geq 1$ dela eta emaitza egiazkoa dela luzera txikiagoko elementuetarako. Bi kasu hauek bereiziko ditugu: $g \in N$ eta $g \notin N$.

(i) Demagun $g \in N$ dela eta idatz dezagun $g = (g_1, \ldots, g_p)$. Gogoan izan, 3.10 lemaren arabera, bi aukera ditugula. Existitzen bada $k \in \mathbb{N}$ non $g = b_i^k$ den, orduan $g^p = 1$ dugu, b_i-ren ordena p baita. Beraz, g elementua p ordenakoa da. Bigarren aukera $i = 1, \ldots, p$ guztietarako $\ell(g_i) < \ell(g)$ izatea da. Indukzio hipotesiagatik, g_i bakoitzaren ordena p-ren berretura da. Izan bedi p^k berretura horietatik handiena (edo, gauza bera dena, multiplo komunetako txikiena). Orduan,

$$g^{p^k} = (g_1^{p^k}, \ldots, g_p^{p^k}) = (1, \ldots, 1) = 1$$

dugu eta, berriro ere 1.5 korolarioa erabiliz, g-ren ordena p-ren berretura da.

(ii) Demagun orain $g \notin N$ dugula. Jarri $g = hn$, $h \in \langle a \rangle$, $h \neq 1$, eta $n \in \langle b_0, \ldots, b_{p-1} \rangle$ izanik. Orduan,

$$g^p = hn \,.\overset{p}{.}\, hn = h^p n^{hp-1} \ldots n^h n = n^{h^{p-1}} \ldots n^h n \in N$$

dugu. Orain, idatz dezagun $h = a^j$ eta $n = \mathrm{b}_{i_1} \ldots b_{i_r}$. Balio hauek aurreko berdintzara eramanez,

$$g^p = b_{i_1+j(p-1)} \ldots + b_{i_r+j(p-1)} \ldots b_{i_1+j} \ldots b_{i_r+j}\, b_{i_1} \ldots b_{i_r} \tag{7}$$

lortzen dugu. Ohartu p-k ez duela j zatitzen, a-ren ordena p baita eta $h \neq 1$ baita. Beraz, 3.11 lema aplika dezakegu eta $\{i_1 + j(p-1), \ldots, i_1 + j, i_1\}$ zenbakien hondarrak p-rekin zatitzerakoan $\{0, 1, \ldots, p-1\}$ multzokoak dira. Horrela,

$$\{b_{i_1+j(p-1)}, \ldots, b_{i_1+j}, b_{i_1}\} = \{b_0, b_1, \ldots, b_{p-1}\}$$

dugu (ez halabeharrez ordena berean). Beste horrenbeste egiten badugu $i_2, \ldots, i_r$ indizeekin, ondorioztatzen dugu (7) berdintzan $b_0, \ldots, b_{p-1}$ automorfismo guztiak agertzen direla, bakoitza r aldiz errepikaturik. Hori bai, ezin dugu aurretiaz jakin zein ordena-

tan agertzen diren. Edozein kasutan, $g^p = (f_1, \ldots, f_p)$ tupla modura idazten badugu, orduan (5)eko adierazpenak erabiliz, osagai bakoitzean a, a^{-1} eta b elementuen biderkadura bat ikusiko dugu, eta bakoitza zehatz-mehatz r aldiz agertzen da. Biderkadura horiek berrordenatzen ditugunean a-ren berretura guztiak aurretik jartzeko, azkenean a-ren eta a^{-1}-en r agerraldi horiek elkarrekin desagertzen dira eta, ondorioz, f_i bakoitza N-ko elementu bat da, r luzerakoa. Aplikatzen badugu (i) kasuan frogatutakoa, f_i guztien ordena p-ren berretura da. Hortik, $g^p = (f_1, \ldots, f_p)$-ren ordena ere p-ren berretura da eta, beraz, g-ren ordena ere p-ren berretura da.

Bukatzeko, esan dezagun Gupta-Sidkiren taldea eta antzeko kontradibideak ez direla inola ere Burnsidek azaldu zuen problemaren amaiera. Burnsidek berak 1902ko artikulu berean, beste problema «errazago» hau planteatu zuen.

Burnsideren Problema

Izan bedi G talde finituki sortua eta demagun G-ko elementu guztien ordena finitua dela eta, are gehiago, badagoela borne bat elementuen ordenetarako. (Bestela esanda, existitzen dela $n \in \mathbb{N}$ non $g^n = 1$ den $g \in G$ guztietarako.) Ba al da finitua G taldea?

Esan beharra dago Goloden adibideetan eta Gupta-Sidkiren taldean elementuen ordenak ez daudela bornaturik. Beraz, talde hauek ez dira kontradibideak Burnsideren Problemarako. Hala ere, 1968an, Sergei Adian azerbaijandarrak eta Pyotr Novikov errusiarrak ezezko erantzuna eman zioten Burnsideren Problemari [3]. Baina matematikariok ez dugu itxaropena hain erraz galtzen, eta badago oraindik ere Burnsideren Problemaren hirugarren aldaera bat. Ideia hau da: sortzaileen kopurua eta elementuen ordenetarako bornea finkatzen baditugu ere, taldea infinitua izan daiteke, baina zer esan dezakegu *aldez aurretik* eskatzen badugu taldeak *finitua* izatea?

Burnsideren Problema Murriztua

Izan bitez d eta n zenbaki finkoak. Demagun G talde *finitua* d elementuren bidez sor daitekeela eta G-ko elementu guztiek $g^n = 1$ betetzen dutela. Ba al dago bornatuta G-ren kardinala d-ren eta n-ren funtzioan?

Kasu honetan (hirugarrenean bai!) erantzuna baiezkoa da. Burnsideren Problema Murriztuaren soluzioa Zelmanov matematikari errusiarrak osatu zuen 1989an, [7] eta [8] artikuluetan. Zelmanoven lana izugarria izan zen eta, hori saritzeko, 1994ean Fields Domina ospetsua eman zioten Zürichen antolatu zen Matematikarien Nazioarteko Kongresuan. Kontuan izan Fields Dominak lau urtean behin banatzen direla, gehienez lau matematikariri, beti ere saridunak adinez berrogei urtetik beherakoak izanik. Matematika

Nobel Saririk gabe, XX. mendean Fields Domina zen matematikari bati Nobel Sariaren pareko ospea ekar ziezaiokeen sari bakarra. Duela gutxi, 2003an, Norvegiako Zientzietako eta Letretako Akademiak Abel Saria ezarri du. Hau urtero ematen da eta Nobel Sariaren antzeko diru kopuruaz horniturik dago. Artikulu honen gaiarekin lotuta, azpimarratzekoa da 2008 urtean Abel Sariaren irabazleak John Thompson estatubatuarra eta Jacques Tits frantsesa izan zirela, talde-teoriaren arloan egindako ekarpenengatik.

ERREFERENTZIAK

[1] *A Study of Asymmetry of Faces,* in www.upscale.utoronto.ca/GeneralInterest/Harrison/Parity/FaceStudy/FaceStudy. html.

[2] *Symmeter and Symface,* www.symmeter.com.

[3] S.I. ADIAN, P.S. NOVIKOV:, «On infinite periodic groups I, II, III», *Izv. Akad. Nauk SSSR Ser. Mat*. 32 (1968), 212-244; 251-524; 709-731.

[4] W. BURNSIDE: «On an unsettled question in the theory of discontinuous groups», *Quart. J. Pure Appl. Math*. 33 (1902), 230-238.

[5] E.S. GOLOD: «On nil-algebras and finitely approximable *p*-groups», *Izv. Akad. Nauk SSSR Ser. Mat*. 28 (1964), 273-276.

[6] N. GUPTA, S. SIDKI: «On the Burnside problem for periodic groups», *Math. Z.* 182 (1983), 385-388.

[7] E.I. ZELMANOV: «Solution of the restricted Burnside problem for groups of odd exponent», *Izv. Akad. Nauk SSSR Ser. Mat*. 54 (1990), 42-59.

[8] E.I. ZELMANOV: «Solution of the restricted Burnside problem for 2-groups», *Mat. Sb*. 182 (1991), 568-592.