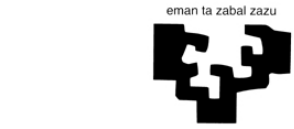


ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Eraikuntza geometrikoen eta Galoisen teoriaren arteko erlazioa

Gradu Amaierako Lana
Matematikako Gradua

Aitor Huizi Izagirre

Leire Legarreta Solaguren
Irakasleak zuzendutako lana

Leioa, 2016ko uztailak 11

Aurkibidea

Sarrera

Gaur egun, erregela eta konpasa egunerokotasunean ondo sartuta ditugun bi tresna dira. Txiki-txikitatik ikasten ditugu erabiltzen, eta modu naturalean erabiltzeko gai gara helduaroan. Alabaina, hau ez da beti horrela izan, antzinako greziar zibilizazioa (K. A. 500 urte inguruan) izan baitzen erregela eta konpas bitartezko eraikuntza geometrikoak modu sistematikoan aztertu zituen lehen giza-taldea. Zuzen paralelo nahiz perpendikularren eraikuntza, hexagono erregularraren eraikuntza... hainbat eta hainbat izan ziren geometriaren arlo honetan greziarrek egindako lorpenak. Hala ere, antzinako greziarren geometriak bazituen bere hutsuneak ere. Esate baterako, edozein zirkunferentzia emanik ez zekiten nola eraiki emandako zirkunferentziaren azalera berdina izango zuen karratu bat (erregela eta konpasa bakarrik erabiliz). Saiatuaren saiatuaz ezer lortzen ez zutenez, greziarrek ondokoa susmatu zuten: esku artean zerabilten eraikuntza, hau da, emandako zirkunferentzia baten azalera bereko karratu bat eraikitzea, ezinezko eraikuntza bat zela. Susmo historiko hau da gure lan honen abiapuntua.

Lan honek, nolabait ere, greziarrek aztertu eta garatu zuten marrazketa teknikoari mugak jartzea du helburutzat. Izan ere, erregela eta konpasa soilik erabiliz egin zitezkeen gauzak greziarrek ondo asko ezagutzen zituzten, baina ez zuten irizpiderik tresna hauekin egin ezin zitekeena aztertzeko. Horregatik, eraikuntza geometrikoak aztertzeko guk erabiliko dugun baliabidea oso modernoa izango da greziarrekin alderatuta: Galoisen teoria. Teoria honek eraikuntza geometrikoekin duen harremana izango da lan honen ardatz nagusia.

Lehenengo kapituluan, erregela eta konpas bitartez eraiki daitezken planoko puntuetan jarriko dugu enfasia. Puntu hauek zeintzuk diren guztiz karakterizatuko dituen irizpide batekin bukatuko dugu gure garapen teorikoa, eta kapitulua bukatzeko greziarrak ebazteko gai izan ez ziren hiru problema aztertu eta ebatziko ditugu: angelua hirutan zatitzearen problema, zirkuluaren koadraturaren problema eta kuboaren bikoizketaren problema.

Bigarren kapituluan, Galoisen teoria modu sakonago batean garatu ondoren, aurreko kapituluan garatutako teoria guztia poligono erregularren eraikuntzarekin lotuko dugu. Horretarako, Karl Friedrich Gauss (1777 - 1855) matematikari handiak eman zituen pausuak jarraituko ditugu oro har. Eraikuntza mota hauen inguruan, greziarren bazekiten esaterako hexagono

erregular bat nola eraiki erregela eta konpasa erabiliz, baina ez zekiten nola eraiki heptagono erregular bat. Kapitulu honetako gure helburua eraiki daitezkeen eta eraiki ezin daitezkeen poligono erregularrak guztiz zehaztea izango da.

Azkenik, hirugarren kapituluan antzinako greziarren geometriatik aterako gara, eta ekialde hurrunera egingo dugu jauzi. Izan ere, orain dela ehunka urtetik hona Japoniako *origami*-a edo papiroflexia tradizio handiko denbora-pasa bat izan da, eta gure xedea origamia gure lanean txertatzea izango da. Hain zuzen ere, origamia erabilita eraikuntza geometrikoak egiteko beste modu bat definituko dugu, eta honela antzinako greziarrek zituzten mugak zabaltzea lortuko dugu. Zehatzago esanda, greziarrentzat egiteko ezinezkoak izan ziren eraikuntza batzuk egiteko gai izango gara origamia erabiliz: esate baterako, poligono erregular gehiago eraikitzea edo edozein ekuazio kubiko origamiaren bitartez ebaztea.

Azkenik, lanaren amaieran A eranskina egongo da atxikita. Bertan, atal teorikoak garatu ahal izateko beharrezkoak diren emaitza batzuk ikusiko dira. Ariketak atalka sailkatuta egongo dira, eta atal bakoitzean dagokion kapituluan erabiltzen diren ariketak ebatziko dira.

Lan hau behar bezala ulertu ahal izateko, eta batez ere Galoisen teoriaren ikuspuntua, beharrezkoa izango da talde-teoria nahiz eraztun-teoriako oinarrizko ikastaroren bat aurretiaz emanda izatea. Era berean, polinomioen eraztunen teoria eta gorputz-teoria funtsezkoak izango dira lan osoan zehar, eta bereziki gorputz-hedadura finituen teoriari dagozkion emaitzak. Azkenik, Galoisen korrespondentzia ere oso erabilia izango da. Halaber, ariketetan eta orokorrean lan osoan zehar irudiak aurkituko dira nonahi, erregela, konpasa nahiz origamia erabilita egin beharreko eraikuntzak pausuz-pausu azaltzeko helburuarekin. Irudi hauek behar bezala ulertzeko, "semaforo" notazioa aurrez ezagutu beharko da: eraikuntzaren hasieran ematen zaizkigun puntuak gorriak izango dira, eraikuntzan zehar eraikitakoak naranjak eta eraikuntzak helburutzat zituen puntuak, berriz, berdeak.

Hau honela eta azalpen guztiak emanda, irakurlea lanean murgil dadin itxarotea besterik ez da geratzen.

1. kapitulua

Zenbaki eraikigarriak

Galoisen teoriaren ikuspuntutik azter daitezkeen eraikuntza geometriko sinpleenak erregela eta konpas bitartez egiten diren eraikuntza geometrikoak dira. Horregatik, eraikuntza geometriko hauexek izango dira lehenengo kapitulu honetan aztertuko ditugunak. Kapitulu osoan zehar erregela eta konpasa etengabe aipatuko ditugunez, irakurleak bi tresna hauek erabiltzen badakiela suposatu beharko dugu, eta beraz, lanaren ildoa behar bezala jarraitzeko, lehenik eta behin terminologia apur bat zehaztuko dugu, eta baita irakurleari aurrebaldintza batzuk eskatu ere.

1.1 Aurrebaldintzak

Oro har lan guztian zehar, *erregela* hitzez inongo neurririk edo markarik ez duen erregela izendatuko dugu, eta erregelak distantzia jakin batez banaturiko bi puntu markatuak baldin baditu, *erregela markatua* dela esango dugu. Terminologia honetaz baliatuz, irakurleak erregela eta konpas bitartezko marrazketa teknikoko oinarrizko maila bat duela suposatuko dugu. Horregatik, hemendik aurrera jakintzat emango dira nola egin ondorengo eraikuntza hauek, erregela eta konpasa erabiliz:

- Bi puntu ezberdin emanda, bien arteko erdiko puntua eraikitzea.
- Bi puntu ezberdin emanda, puntu batekiko bestearen erreflexioa eraikitzea.
- Angelu ezagun bat emanda, angeluaren erdia eta bikoitza eraikitzea.
- Zuzen bat eta bertako puntu bat emanda, puntutik igarotzen den zuzen perpendikular bat eraikitzea.
- Zuzen bat eta zuzenetik kanpo dagoen puntu bat emanda, puntutik igarotzen den zuzen paralelo bat eraikitzea.

- Egoera berean, puntutik igarotzen den eta zuzena perpendikularki ebakitzen duen beste zuzen bat eraikitzea.

Eraikuntza hauek etengabe erabiliko dira lan osoan zehar, eta bigarren hezkuntzako marrazketa teknikoko edozein liburutan aurki daiteke hauek nola egin. Behin irakurleak aurrebaldintza hauek betetzen dituela suposatuta, has gaitezen zenbaki eraikigarri bat zer den definitzen.

1.2 Zenbaki bat eraikitzea

Eraikuntza geometrikoen inguruko teoremak frogatzeko, lehenik eta behin eraikuntza geometriko bat zer den kontu handiz definitu beharko dugu, eta azaldu ere bai zer den zenbaki bat eraikitzea, erregela eta konpasa erabiliz. Jakina denez,

E1: $p_1 \neq p_2$ puntuetatik abiatuta, biak lotzen dituen l zuzena erregela bitartez marraz daiteke
E2: $p_1 \neq p_2$ eta q puntuetatik abiatuta, q zentruko eta $p_1$etik $p_2$rako distantzia erradiotzat duen Z zirkunferentzia erregela eta konpas bitartez marraz daiteke

Zerrendatze honetan E letraz *eraiki daitekeena* adierazi nahi izan dugu. E1 eta E2 pausuak emanez marraztu daitezken zuzen eta zirkunferentzia hauetatik abiatuta planoko puntu berriak lortu ditzakegu:

P1: aurreko eran eraikitako l_1 eta l_2 bi zuzen ezberdin ebakitzen diren puntua
P2: aurreko eran eraikitako l zuzena eta Z zirkunferentzia ebakitzen diren puntua
P3: aurreko eran eraikitako Z_1 eta Z_2 bi zirkunferentzia ezberdin ebakitzen diren puntua

Puntu guztiak dauden planoa guretzat $\mathbb{C}$ plano konplexua izango da, eta gure eraikuntza geometriko guztiak 0 eta 1 zenbakietatik hasiko dira.

Definizioa 1.2.1. Izan bedi $\alpha \in \mathbb{C}$ zenbaki konplexua. α zenbakia **eraikigarria** dela esango dugu erregela eta konpas bitarteko E1, E2, P1, P2 eta P3 pausuen segida finitu bat existitzen bada, 0 eta 1 puntuekin hasi eta α puntuan amaitzen dena.

Jarraian zenbaki eraikigarriei buruzko funtsezko propietate batzuk azalduko ditugu.

Proposizioa 1.2.2. *Izan bitez $\alpha, \beta \in \mathbb{C}$ zenbaki eraikigarriak. Orduan,*

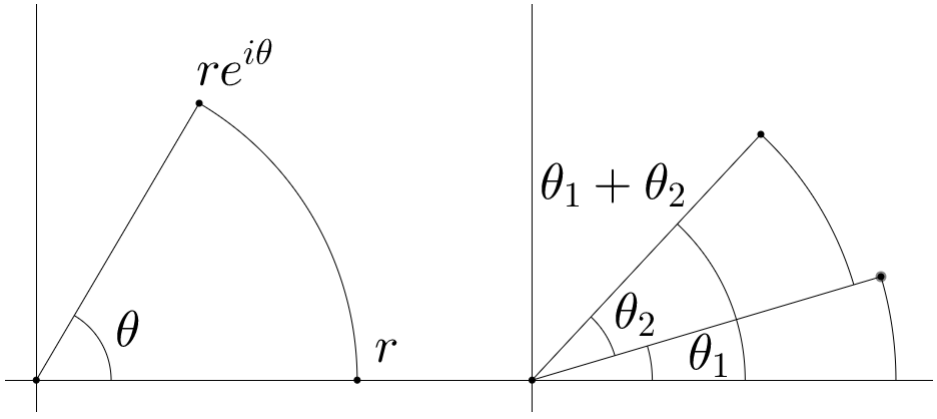
(i) $-\alpha$ *eta* $\alpha+\beta$ *eraikigarriak dira.*

(ii) $\alpha\beta$ *eraikigarria da, eta baita* α^{-1} *ere* $\alpha \neq 0$ *bada.*

Froga. Ohartu $\alpha \neq 0 \neq \beta$ kasurako proposizioa frogatzea nahikoa dela. 1.1 aurrebaldintzetan jartzen duenez, $0 \neq \alpha$ puntuak emanda badakigu α-ren erreflexioa kalkulatzen 0-rekiko. Erreflexioari γ deitzen badiogu, 0 puntuarekiko α-ren erreflexioa denez beren arteko erdiko puntua hain zuzen ere 0 izan beharko da. Hau da, $\frac{\alpha+\gamma}{2} = 0$ izan beharko da. Baina orduan $\gamma = -\alpha$ izango da, eta beraz $-\alpha$ eraikigarria da. Aldiz, $\alpha+\beta$ zenbakia eraikigarria dela A eranskineko 1 ariketan frogatzen da.

Bi zenbakiren arteko biderketa eraikitzeko, erabil dezagun notazio polarra. Edozein $\alpha, \beta \in \mathbb{C}$ izanik, batetik $|\alpha| = r_1$ eta $|\beta| = r_2$ eta bestetik Arg $\alpha = \theta_1$ eta Arg $\beta = \theta_2$ hartzen baditugu erraz ikusten da bi zenbaki konplexu hauek notazio polarrean idatzita hain zuzen ere $\alpha = r_1 e^{i\theta_1}$ eta $\beta = r_2 e^{i\theta_2}$ direla.

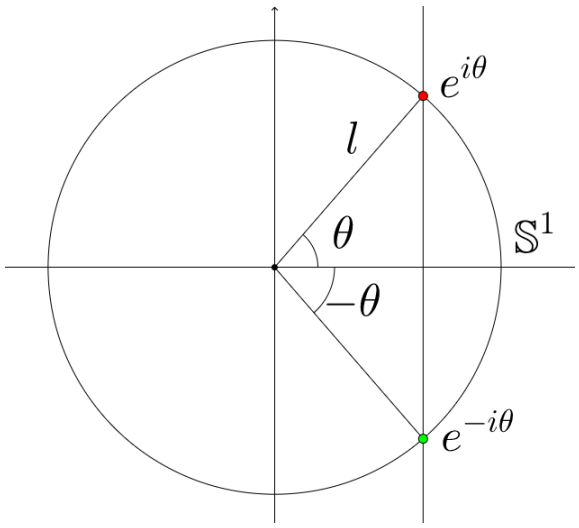
Edozein zenbaki konplexu $re^{i\theta}$ eraikigarria baldin bada, argi dago r zenbaki erreal eraikigarria izango dela. Izan ere, aski da jatorrian zentraturiko zirkunferentzia bat egitea, $re^{i\theta}$-rainoko distantzia erradiotzat izango duena. Zirkunferentzia honek OX ardatza r puntuan ebakiko du, 1.1. irudiko lehen eraikuntzan azaltzen den bezala, eta beraz P2 pausuagatik r eraikigarria izango da. Eta $re^{i\theta}$ eta r zenbaki eraikigarrien arteko angelua hain zuzen ere θ da, eta beraz posible da eraikitzea. Hau honela, gure $\alpha = r_1 e^{i\theta_1}$ eta $\beta = r_2 e^{i\theta_2}$ puntuetatik abiatuta metodo hau aplikatu daiteke, θ_1 eta θ_2 angeluak eraikitzeko. Bi angelu hauen batura eraikitzea berehalakoa da, angelu baten "gainean" bestea eraikitzea aski baita, 1.1. irudiko bigarren eraikuntzan egiten den bezala. Ondorioz, $\theta_1 + \theta_2$ angelua eraiki dezakegu erregela eta konpas bitartez.



1.1. irudia. Ezkerrean, zenbaki konplexu baten argumentua eraikitzea. Eskuinean, bi angeluren arteko batura eraikitzea.

Jarraitzeko, A eranskineko 2 ariketan bi zenbaki erreal eraikigarriren arteko biderkadura eraikitzen da, eta beraz bereziki r_1 eta r_2 eraikitzen badakigunez (P2 pausuagatik), ariketa horretan egiten dena jarraituz $r_1 r_2$ eraikita izango dugu. Erradio honetako eta jatorrian zentraturiko Z zirkunferentzia OX ardatzarekin $\theta_1 + \theta_2$ angelua osatzen duen l zuzenarekin ebakitzen badugu, berriro ere P2 pausuagatik ebakidura eraikigarria izango da. Baina ebakidura honen argumentua $\theta_1 + \theta_2$ denez eta erradioa $r_1 r_2$, halabeharrez ebakidura hau $r_1 r_2 e^{i(\theta_1+\theta_2)} = r_1 e^{i\theta_1} r_2 e^{i\theta_2} = \alpha\beta$ izan beharko da. Hemendik $\alpha\beta$ eraikigarria dela ondorioztatu dugu.

Bukatzeko, edozein $\alpha \in \mathbb{C} - \{0\}$ hartuta α^{-1} eraikitzeko, idatz dezagun α notazio polarrean: $\alpha = re^{i\theta}$. Jatorrian zentratutako eta 1 erradioko $\mathbb{S}^1$ unitate-zirkunferentzia eraiki ostean OX ardatzarekin θ angelua osatzen duen l zuzena eraikiko dugu ondoren, eta biak ebaki 1.2. irudian egiten den bezala. Ebakidura eraikigarria izango da, P2 pausuagatik, eta puntu hau hain justu $e^{i\theta}$ izango da. 1.1 aurrebaldintzetan eskatzen zenez, badakigu $e^{i\theta}$ puntutik igarotzen den zuzen bertikal bat eraikitzen (OY-rekiko paraleloa), eta zuzen bertikal honen ekuazioa $X = \cos\theta$ denez $\mathrm{Re}\, e^{i\theta} = \cos\theta$ delako, zuzenak $\mathbb{S}^1$ unitate-zirkunferentzia $e^{\pm i\theta}$ puntuetan ebakiko du (ikus 1.2. irudia).



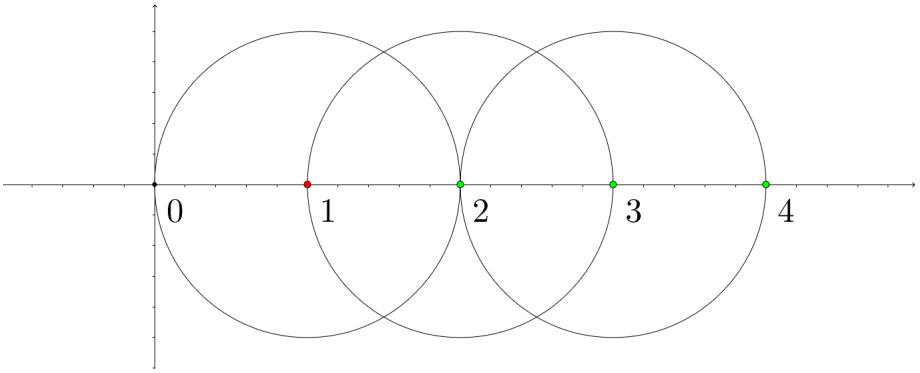
1.2. irudia.

Ondorioz, $e^{\pm i\theta}$ puntuak eraikigarriak izango dira berriro ere P2 pausuagatik, eta bereziki $e^{-i\theta}$ eraikigarria izango da. Gainera, $r = |\alpha| \neq 0$ hartuta A eranskineko 3 ariketan r^{-1} nola eraiki azaltzen da. Beraz, r^{-1} eta $e^{-i\theta}$ eraikigarriak direnez, frogatu berri dugu beraien biderkadura, $r^{-1}e^{-i\theta} = \left(re^{i\theta}\right)^{-1} = \alpha^{-1}$ ere eraikigarria izango dela.

□

Korolarioa 1.2.3. *Zenbaki arrazionalak eraikigarriak dira.*

Froga. Ohar gaitezen 0 eta 1 zenbakietatik abiatuz, oso erraz eraiki ditzakegula zenbaki osoak: lehenik eta behin 1 puntua zentrotzat hartuta, konpasaz 0-rainoko distantzia erradiotzat duen zirkunferentzia eraiki behar da. Zirkunferentzia honek OX ardatza 2 puntuan ebakiko du, eta beraz 2 eraikigarria izango da. Pausu hau errepikatuz zenbaki oso guztiak eraiki ditzakegu, 1.3. irudian eraikitzen diren bezala.



1.3. irudia. Zenbaki osoen eraikuntza. Zenbaki oso negatiboak eraikitzeko prozedura bera erabiltzen da, baina beste aldera.

Ondorioz, zenbaki oso guztiak eraikigarriak dira. Gainera, bi zenbaki eraikigarriren arteko zatiketa ere eraikigarria da 1.2.2 proposizioagatik, eta beraz zenbaki arrazionalak zenbaki eraikigarriak dira. □

1.3 Zenbaki eraikigarrien gorputza

Hemendik aurrera, zenbaki eraikigarri guztiek osatzen duten multzoari $\mathcal{C}$ deituko diogu, hots, $\mathcal{C} = \{\alpha \in \mathbb{C} \mid \alpha \textit{ eraikigarria}\}$. Aurreko atalean ikusi dugunez, zenbaki eraikigarrien arteko eragiketek portaera ona dute eraikigarritasunarekiko. Ondorioz, $\mathbb{C}$ plano konplexuko eragiketak $\mathcal{C}$ multzora murriztu ditzakegu, 1.2.2 proposizioak iradokitzen digun bezala. Proposizio honen eta 1.2.3 korolarioaren ondorio berehalakoa da jarraian datorren funtsezko emaitza hau, zenbaki eraikigarriak Galoisen teoriaren bitartez aztertzea justifikatzen duena.

Korolarioa 1.3.1. *Zenbaki eraikigarrien multzoa gorputza da ohiko batuketa eta biderketarekiko. Ondorioz,*

$$\mathbb{Q} \subseteq \mathcal{C} \subseteq \mathbb{C}$$

gorputz-hedaduren katea dugu.

Zenbaki eraikigarriei buruzko propietate batzuk emango ditugu ondoren, $\mathcal{C}$ gorputzaren propietate aljebraikoak aztertzeko baliagarriak izango direnak.

Teorema 1.3.2. *Izan bedi $\mathcal{C}$ zenbaki eraikigarrien gorputza. Orduan,*

(i) *$\alpha = a + ib \in \mathbb{C}$ bada (a eta b errealak), $\alpha \in \mathcal{C}$ baldin eta soilik baldin $a, b \in \mathcal{C}$*

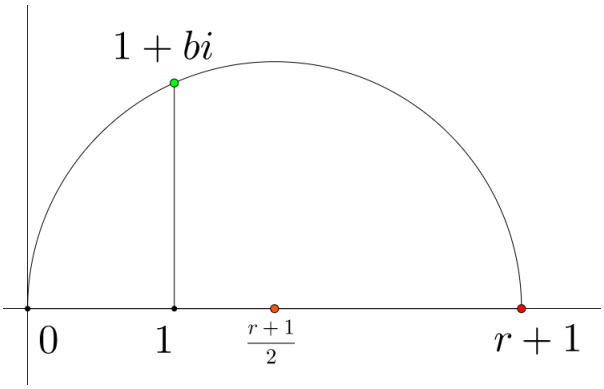
(ii) *$\alpha \in \mathcal{C}$ bada, orduan $\sqrt{\alpha} \in \mathcal{C}$*

Froga. (i) Har dezagun $\alpha = a + ib \in \mathcal{C}$. Gure α-tik OX eta OY ardatzetara zuzen perpendikularrak marraz ditzakegu, eta ondorioz $a, ib \in \mathcal{C}$ dugu. Gainera, jatorrian zentraturiko eta $|ib|$ erradioko zirkunferentziak OX ardatza b puntuan ebakitzen duenez, $b \in \mathcal{C}$ da. Ikustagun beste inplikazioa: 0-n zentratutako eta 1 erradioko zirkunferentziak OY ardatza i puntuan ebakitzen duenez, $i \in \mathcal{C}$ da. Gainera, hipotesiz $a, b \in \mathcal{C}$ dira. Ondorioz, 1.2.2 proposizioa aplikatuz halakoa da $a + ib = \alpha$ ere.

(ii) Ikustagun α eraikigarria bada $\sqrt{\alpha}$ ere eraikigarria dela ($\alpha \neq 0$ suposa dezakegu). Polarretako idazkera hartuz $\alpha = re^{i\theta}$ da, non $r = |\alpha| > 0$ eta $\theta = \text{Arg } \alpha$ diren. Nahikoa da $\sqrt{r}e^{i\theta/2}$ eraikigarria dela ikustea. Horretarako, ohar gaitezen α-ren eraikigarritasunak honakoa dakarrela:

- OX ardatza eta 0 eta α lotzen dituen zuzena E1 pausuagatik eraikita, beren arteko angelua hain zuzen ere θ da, eta beraz badakigu eraikitzen. Gainera, 1.1 ataleko aurrebaldintzetan jakintzat ematen da angeluak erdibitzen jakitea. Beraz, $\theta/2$ eraikigarria da.
- Jatorrian zentraturiko eta $|\alpha|$ erradiodun zirkunferentziak OX ardatza $\pm r$ puntuetan ebakitzen duenez, P2 pausuagatik r ere eraikigarria da.
- $\sqrt{r}$ ere eraikigarria balitz, jatorrian zentraturiko eta $\sqrt{r}$ erradioko zirkunferentzia eraiki ahal izango genuke E2 pausuagatik. Jarraian $\theta/2$ angeluari eta zirkunferentzia honi P2 aplikatuko bagenie $\sqrt{r}e^{i\theta/2}$ eraikigarria dela ondorioztatuko genuke, hots, $\sqrt{\alpha}$ eraikigarria dela.

Beraz, frogatu behar dugun bakarra $\sqrt{r}$ eraikigarria dela da, $r > 0$ ere eraikigarria denean. Horretarako, lehenik eta behin $r + 1$ puntua planoan kokatuko dugu, badakigulako eraikigarria dela r ere badelako. Izan ere, 1.2.3 korolarioagatik 1 eraikigarria da eta 1.2.2 proposizioko (i) atalagatik $r, 1 \in \mathcal{C}$ bada orduan $r+1 \in \mathcal{C}$ izango da. Jarraian, 0-ren eta $r+1$-en arteko erdiko puntua hartuko dugu, $\frac{r+1}{2}$. Puntu honetatik



1.4. irudia.

abiatuta, zirkunferentzia bat eraikiko dugu (E2 pausuaz baliatuz) $\frac{r+1}{2}$ zentrotzat duena, eta erradioa $\frac{r+1}{2}$ puntutik 0-rako distantzia, hau da, $|\frac{r+1}{2}|$ distantzia. Behin zirkunferentzia eraikita, 1 puntutik igarotzen den eta OY ardatzarekiko paraleloa den zuzen bat eraikiko dugu, E1 pausuarekin. Zuzen honek zirkunferentzia $1 + bi$ puntuan ebakiko duenez $b \in \mathbb{R}$ baterako, $1 + bi \in \mathcal{C}$ izango da P2 pausuagatik. Ondorioz, 1.3.2 teoremako (i) atalagatik badakigu $1 + bi \in \mathcal{C}$ bada bereziki $b \in \mathcal{C}$ dela. Baina $1 + bi$ zenbakia zirkunferentzian dagoenez, $\frac{r+1}{2}$ puntutik (zirkunferentziaren zentrotik) $|\frac{r+1}{2}|$ distantziara egon behar du, eta beraz

$$|1 + bi - \frac{r+1}{2}| = \sqrt{\left(1 - \frac{r+1}{2}\right)^2 + b^2} = \sqrt{\left(\frac{1-r}{2}\right)^2 + b^2} = \frac{r+1}{2}$$

da. Ekuazioa askatuz,

$$\left(\frac{1-r}{2}\right)^2 + b^2 = \frac{1 - 2r + r^2}{4} + b^2 = \frac{r^2 + 2r + 1}{4}$$

eta ondorioz $b^2 = r$ da. Hortaz, $b \in \mathcal{C}$ denez, $\sqrt{r} \in \mathcal{C}$ izango da, nahi genuena.

□

Ondorioa 1.3.3. Baldin eta $a, b, c \in \mathcal{C}$ badira, orduan $aX^2 + bX + c = 0$ ekuazioaren soluzio guztiak eraikigarriak dira. Izan ere, formula koadratikoak esaten digu $\alpha_1, \alpha_2 \in \mathbb{C}$ zenbakiak ekuazioaren bi soluzioak badira, orduan

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ eta } \alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

betetzen dela. Hortaz, $b^2 - 4ac \in \mathcal{C}$ denez 1.3.2 teoremako (ii) atalagatik $\sqrt{b^2 - 4ac} \in \mathcal{C}$ da, eta beraz $\alpha_1, \alpha_2 \in \mathcal{C}$ dira beti.

Jarraian, zenbaki eraikigarriekin lan egiteko Galoisen teoria aplikatu nahi badugu, $\mathcal{C}$-ren egitura zehaztu beharko dugu $\mathbb{Q}$-ren gorputz-hedadura bezala. Horretarako, lehenik eta behin lema tekniko baten laguntza beharko dugu.

Lema 1.3.4. *Izan bitez K, $\mathcal{C}$-ren azpigorputz bat eta $\alpha = a + ib \in \mathcal{C}$ puntua (a eta b errealak). Baldin eta α pausu bakar batean eraiki baldin badaiteke K gorputzeko elementuetatik, orduan $[K(a,b) : K] = 1$ edo 2 da.*

Froga. Pausu bakar bat nahikoa denez $\alpha = a + ib$ puntua K-tik abiatuta eraikitzeko, hiru aukera dauzkagu: α zenbakia P1 pausuaren bitartez eraikia izatea, P2 pausuaren bitartez eraikia izatea edo P3 pausuaren bitartez eraikia izatea. Azter dezagun kasu bakoitza:

- Demagun α eraikitzerakoan emandako pausua P1 dela, hau da, α puntua l_1 eta l_2 zuzenen ebakidura dela. Zuzen hauetako bakoitza koefizienteak K-n dituen ekuazio lineal batek definitzen du:

$$l_1 \equiv AX + BY + C = 0,$$

$$l_2 \equiv A'X + B'Y + C' = 0$$

  non $A, B, C, A', B', C' \in K$ diren. $\alpha = a + ib$ puntuak bi zuzenen ekuazioak aldi berean betetzen dituenez, bi zuzen hauek ezingo dira paraleloak izan (α-n ebakitzen direlako). Eta paraleloak izango ez direnez, $AB' - A'B \neq 0$ da. Hau honela izanik, $\alpha = a + ib$ puntua ekuazio-sistemaren soluzio bat izan behar denez ekuazio-sistemetarako Cramerren erregelak erakusten du $a, b \in K$ direla. Beraz, $K(a,b) = K$ dugu.

- Demagun ordea α eraikitzeko emandako pausua P2 dela, hau da, α puntua l zuzen baten eta Z zirkunferentzia baten arteko ebakidura dela. Zuzenaren eta zirkunferentziaren ekuazioak idatziz,

$$l \equiv AX + BY + C = 0,$$

$$Z \equiv X^2 + Y^2 + A'X + B'Y + C' = 0$$

  dira, $A, B, C, A', B', C' \in K$ izanik. Baldin eta $A = 0$ bada, orduan $\alpha = a + ib$ puntuak l-ren ekuazioa betetzen duenez $b = \frac{-C}{B} \in K$ da. Aldiz $A \neq 0$ bada, orduan arrazoi beragatik $a = \frac{-Bb-C}{A}$ dugu. Bi kasuetan b edo a zirkunferentziaren ekuazioan ordezkatuta, a edo b hurrenez hurren bigarren mailako $p(X) \in K[X]$ polinomio baten erroak direla ohartzen gara. Ondorioz a eta b zenbakiak K-n edo K-ren hedadura koadratiko baten barruan egongo dira, polinomioaren irreduzibilitatearen arabera. Beraz $[K(a,b) : K] = 1$ edo 2 izango da, nahi genuena.

- P3 baldin bada emandako pausua, α puntua Z_1 eta Z_2 zirkunferentzien ebakidura izango da, non

$$Z_1 \equiv X^2 + Y^2 + AX + BY + C = 0,$$

$$Z_2 \equiv X^2 + Y^2 + A'X + B'Y + C' = 0$$

diren zirkunferentziak definitzen dituzten ekuazioak, $A, B, C, A', B', C' \in K$ izanik. Ohar gaitezen aurreko kasura eraman dezakegula kasu hau ekuazio bati bestea kenduz. Izan ere, α puntua C_1 zirkunferentziaren eta

$$(A - A')X + (B - B')Y + C - C' = 0$$

ekuazioak definitzen duen l zuzenaren arteko ebakiduraz eraikitzen dugu. Beraz aurreko kasuan gaude eta ondorioz $[K(a, b) : K] = 1$ edo 2 da, nahi genuena.

□

Lema tekniko honen ondoren, benetan prest gaude $\mathcal{C}$ gorputzaren egitura Galoisen teoriaren ikuspuntutik aztertzeko.

Teorema 1.3.5 (Egitura-teorema)**.** *Izan bedi α zenbaki konplexua. Orduan, $\alpha \in \mathcal{C}$ baldin eta soilik baldin $F_0, F_1, \ldots, F_n$ gorputzak existitzen badira halakoak non*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_{n-1} \subset F_n \subset \mathbb{C},$$

$\alpha \in F_n$ delarik eta $[F_i : F_{i-1}] = 2$, $1 \leq i \leq n$ izanik.

Froga. Lehenik eta behin demagun $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{C}$ ondoz-ondoko gorputz-hedaduren katea daukagula, $[F_i : F_{i-1}] = 2$ delarik $i \in \{1, \ldots, n\}$ guztietarako. A eranskinean garatutako 4 ariketarengatik badakigu $\alpha_{i-1} \in F_{i-1}$ existitzen dela $F_i = F_{i-1}(\sqrt{\alpha_{i-1}})$ izanik. Hortaz, i-ren gaineko indukzio bidez $F_i \subset \mathcal{C}$ frogatzea izango da gure helburua. $F_0 = \mathbb{Q} \subset \mathcal{C}$ kasua 1.2.3 korolarioak baieztatzen du, eta beraz demagun orain $F_{i-1} \subset \mathcal{C}$ betetzen dela. Orduan $\alpha_{i-1} \in F_{i-1}$ eraikigarria da, eta ondorioz $\sqrt{\alpha_{i-1}}$ ere bai 1.3.2 teoremagatik. Hortaz $F_{i-1}\left(\sqrt{\alpha_{i-1}}\right) = F_i \subset \mathcal{C}$ betetzen da, nahi genuena. Beraz, indukzioa aplikatuz $F_n \subset \mathcal{C}$ dela lortu dugu, eta bereziki edozein $\alpha \in F_n$ eraikigarria dela.

Elkarrekikoa frogatzeko, har dezagun $\alpha = a + ib \in \mathcal{C}$ edozein. $\mathbb{Q}$-ren ondoz-ondoko gorputz-hedaduren kate bat eraikitzea izango da gure helburua, eta horietako baten batek α barne izatea. Demagun n pausu behar izan direla α eraikitzeko. n-ren gaineko indukzioa erabiliz, batetik $n = 0$ kasua tribiala da. Demagun orain emaitza egia dela $n - 1$ kasurako. α eraikitzeko n pausu behar izan direnez, hartu eraikitze-prozesuko $n - 1$-garren pausuko puntua, $\beta \in \mathcal{C}$. Indukzioz existitzen da $\mathbb{Q} = F_0 \subset \ldots \subset F_{n-1} \subset \mathbb{C}$ ondoz-ondoko gorputz-hedaduren katea, $[F_i : F_{i-1}] = 2$ delarik $i \in \{1, \ldots, n-1\}$

guztietarako eta $\beta \in F_{n-1}$ izanik. Gainera, α eraikigarria da $\beta \in F_{n-1}$ puntutik abiatuta pausu bakar batekin, hau da, $\alpha = a + ib$ elementua F_{n-1} gorputzeko elementuetatik pausu bakar batean eraikigarria da. Ondorioz, 1.3.4 lemagatik, existitzen da $F_{n-1}(a, b)$ gorputza, $a \notin F_{n-1}$ eta $b \notin F_{n-1}$ badira F_{n-1}-ren hedadura koadratikoa izango dena, eta $F_{n-1}(a, b) = F_{n-1}$ bestela. Baldin eta $i \in F_{n-1}(a, b)$ bada, orduan $a + ib = \alpha \in F_{n-1}(a, b)$ da, eta $F_{n-1}(a, b)$ gorputza F_{n-1}-ren hedadura koadratikoa da. Honekin froga bukatu dugu. Bestalde, $i \notin F_{n-1}(a, b)$ bada, berriz, orduan $X^2 + 1 \in F_{n-1}(a, b)[X]$ polinomioak ez du errorik $F_{n-1}(a, b)$-n eta beraz irreduziblea da gorputz horretan. Ondorioz, $Irr(i, F_{n-1}(a, b)) = X^2 + 1$ izango da eta beraz $[F_{n-1}(a, b)(i) : F_{n-1}(a, b)] = \deg(X^2 + 1) = 2$. Hau honela, aurkitu dugu $F_{n-1}(a, b)(i)$ gorputza, $a + ib = \alpha \in F_{n-1}(a, b)(i)$ izanik eta $[F_{n-1}(a, b)(i) : F_{n-1}] = 2$ edo 4 izanik, $[F_{n-1}(a, b) : F_{n-1}] = 1$ edo 2 bada, hurrenez hurren. Eta hortaz, F_{n-1} gorputzetik abiatuz hedadura koadratikoen kate bat eraiki dugu, $F_{n-1}(a, b)(i)$ gorputzean amaitzen dena eta $\alpha \in F_{n-1}(a, b)(i)$ betetzen dena, indukzioa osatuz. Honela, amaitu dugu froga. □

Korolarioa 1.3.6. *$\mathcal{C}$ gorputza erro karratuak hartzearekiko itxia den $\mathbb{C}$-ren azpigorputzik txikiena da.*

Froga. 1.3.2 teoremagatik, badakigu $\alpha \in \mathcal{C}$ bada orduan $\sqrt{\alpha} \in \mathcal{C}$ dela. Hartu orain erro karratuak hartzearekiko itxia den $\mathbb{C}$-ren edozein azpigorputz, eta dei diezaiogun F. Suposatu $\alpha \in \mathcal{C}$. Aurreko 1.3.5 teorema delaeta, badakigu existitzen dela $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{C}$ moduko gorputz-hedaduren katea $[F_i : F_{i-1}] = 2$ eta $\alpha \in F_n$ izanik. $F_n \subseteq F$ dela frogatuko bagenu, $\alpha \in F_n$ hartu dugunez $\alpha \in F$ ondorioztatuko genuke, eta beraz $\mathcal{C} \subseteq F$, frogatu nahi genuena. Beraz, froga dezagun $F_n \subseteq F$ inklusioa n-ren gaineko indukzioz. Batetik, $n = 0$ kasua tribiala da $F_0 = \mathbb{Q} \subseteq F$ baita. Bestetik, jo dezagun $n-1$ kasua egiazkotzat, hots, $F_{n-1} \subseteq F$ dela. A eranskineko 4 ariketan erakusten denez, existitzen da $\alpha_{n-1} \in F_{n-1}$ elementu bat $F_n = F_{n-1}(\sqrt{\alpha_{n-1}})$ betetzen duena. Gainera, ohartu $\alpha_{n-1} \in F_{n-1}$ denez eta hipotesi induktiboagatik $F_{n-1} \subseteq F$ ere betetzen denez, $\alpha_{n-1} \in F$ dela. Ondorioz, F gorputza hipotesiz erro karratuak hartzearekiko itxia denez eta $\alpha_{n-1} \in F$, $\sqrt{\alpha_{n-1}} \in F$ izango da, eta beraz $F_n = F_{n-1}(\sqrt{\alpha_{n-1}}) \subseteq F$ beteko da, nahi genuen bezala. □

Zenbaki eraikigarrien gorputzaren egitura 1.3.5 teoreman aztertu dugunez, gai gara zenbaki konplexu bat eraikigarria den edo ez erabakitzeko. Teorema horrek zenbaki eraikigarriak guztiz karakterizatzen dituen arren, kasu gehienetan ez da batere eraginkorra izango zenbaki konplexu baten eraikigarritasuna aztertzerako orduan. Jarraian datorren korolarioari esker, oso modu errazean argudiatu ahal izango dugu zenbaki konplexu bat **ez** dela eraikigarria.

Korolarioa 1.3.7. *Baldin eta $\alpha \in \mathcal{C}$ bada orduan existitzen da $m \geq 0$ non $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ den. Ondorioz, zenbaki eraikigarri guztiak aljebraikoak dira $\mathbb{Q}$ gainean eta beren polinomio irreduziblearen maila 2-ren berretura bat da.*

Froga. Baldin $\alpha \in \mathcal{C}$ bada, orduan 1.3.5 teoremagatik existitzen da $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{C}$ moduko gorputz-hedaduren katea $[F_i : F_{i-1}] = 2$ eta $\alpha \in F_n$ izanik. Hortaz dorrearen teoremagatik

$$[F_n : \mathbb{Q}] = [F_n : F_0] = [F_n : F_{n-1}] \ldots [F_1 : F_0] = 2^n$$

dugu. Gainera $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq F_n$, eta ondorioz berriro ere dorrearen teoremagatik $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ mailak $[F_n : \mathbb{Q}] = 2^n$ zatituko du. Bereziki $\mathbb{Q}(\alpha)/\mathbb{Q}$ hedadura finitua denez aljebraikoa izango da, eta bertako edozein elementuren polinomio irreduziblearen mailak hedaduraren maila zatituko duenez 2-ren berretura bat izango da. □

Adibideak 1.3.8. (i) Badakigunez π eta e zenbakiak traszendenteak direla $\mathbb{Q}$ gainean, 1.3.7 korolarioagatik ez dira eraikigarriak izango: $\pi, e \notin \mathcal{C}$.

(ii) Badakigu $\sqrt[3]{2}$ zenbakia aljebraikoa dela $\mathbb{Q}$ gainean, eta $Irr(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ dela. Honen maila ez denez 2-ren berretura bat, berriro ere 1.3.7 korolarioagatik $\sqrt[3]{2} \notin \mathcal{C}$ izango da.

Bukatzeko, zenbaki konplexu bat eraikigarria dela guztiz karakterizatzeko irizpide berri bat emango dugu, orain arteko irizpideak baino errazagoa izango dena kalkuluak egiterakoan. Horretarako, lehenik eta behin Galoisen teoriako nozio bat definitu beharko dugu.

Definizioa 1.3.9. Izan bedi K gorputza, $\mathbb{C}/\mathbb{Q}$ hedaduraren tarteko gorputza. K-ren *itxidura normala* deituko zaio K barne duen N/K hedadura normal txikienari. Baliokideki,

$$N/K \text{ hedadura } K\text{-ren itxidura normala} \iff N = \bigcap_{M/K \text{ normala}} M$$

Oharra 1.3.10. Ohartu beti existituko dela K-ren itxidura normala, $\mathbb{C}/K$ hedadura normala baita beti.

Adibideak 1.3.11. (i) Jakina da $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ez dela hedadura normala, $X^3 - 2 \in \mathbb{Q}[X]$ polinomio irreduziblearen erro bat, $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ baita, baina beste bi erroak ez, konplexuak baitira eta $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Bere itxidura normala $\mathbb{Q}(\sqrt[3]{2}, \omega)$ da, $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ izanik.

(ii) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ez da hedadura normala; bere itxidura normala $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ da.

Itxidura normalak erabiliz, eman dezagun zenbaki eraikigarriak karakterizatuko dituen irizpide bat.

Teorema 1.3.12. *Izan bedi $\alpha \in \mathbb{C}$ aljebraikoa $\mathbb{Q}$ gainean eta L gorputza $Irr(\alpha, \mathbb{Q})$ polinomioaren deskonposizio-gorputza $\mathbb{Q}$ gainean. Orduan α eraikigarria da baldin eta soilik baldin $[L : \mathbb{Q}]$ zenbakia 2-ren berretura bada.*

Froga. Batetik, suposatu $[L : \mathbb{Q}]$, gure hedaduraren maila 2-ren berretura dela. $L/\mathbb{Q}$ Galoisen hedadura denez $|G| = |\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$, 2-ren berretura da. Beraz Galoisen taldea 2-talde bat da (p-talde bat, $p = 2$ izanik), eta ondorioz existitzen da azpitaldeen kate bat halakoa non

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = \mathrm{Gal}(L/\mathbb{Q})$$

eta indize bakoitza, $|G_i : G_{i-1}| = 2$ delarik. $\mathrm{Gal}(L/\mathbb{Q})$ taldearen G_i azpitalde bakoitzari dagokion azpigorputz finkoari $\mathcal{F}(G_i)$ deitzen badiogu, aurreko azpitaldeen katean azpigorputz finkoak hartuz ondoko gorputz-hedaduren katea lortzen dugu:

$$\mathbb{Q} = \mathcal{F}(G_n) \subseteq \mathcal{F}(G_{n-1}) \subseteq \ldots \subseteq \mathcal{F}(G_0) = L,$$

non $[\mathcal{F}(G_{i-1}) : \mathcal{F}(G_i)] = |G_i : G_{i-1}| = 2$ den i guztietarako. Ondorioz, 1.3.5 teoremagatik $\alpha \in L$ eraikigarria da.

Bestetik, ikustagun lehenik eta behin $\mathcal{C}/\mathbb{Q}$ hedadura normal bat dela. Horretarako, hartu $\alpha \in \mathcal{C}$ eta f bere polinomio irreduziblea $\mathbb{Q}$ gainean. Hipotesiz $\alpha \in \mathcal{C}$ denez, 1.3.5 teoremagatik existitzen da $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{C}$ moduko gorputz-hedaduren katea $[F_i : F_{i-1}] = 2$ eta $\alpha \in F_n$ izanik. Hartu $N/\mathbb{Q}$, $F_n/\mathbb{Q}$ hedaduraren itxidura normala.

Ohartu f guztiz banatzen dela N gainean, N normala baita $\mathbb{Q}$ gainean. Gainera f irreduziblea da $\mathbb{Q}$-n, eta $\alpha \in F_n \subseteq N$ bere erro bat da. Gure f-ren beste edozein erro, β, hartuz gero, badakigu existitzen dela $\sigma \in \mathrm{Gal}(N/\mathbb{Q})$ non $\sigma(\alpha) = \beta$ den. Jarraitzeko, $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset N$ dorreari σ aplikatzen badiogu,

$$\mathbb{Q} = \sigma(\mathbb{Q}) = \sigma(F_0) \subseteq \ldots \subseteq \sigma(F_n)$$

lortzen dugu, $[\sigma(F_i) : \sigma(F_{i-1})] = 2$ izanik edozein i indizerako. Baina orduan 1.3.5 teoremagatik $\beta = \sigma(\alpha) \in \sigma(F_n)$ eraikigarria da. Hortaz, f guztiz banatzen da $\mathcal{C}$ gainean.

Ondorioz L, f-ren $\mathbb{Q}$ gaineko deskonposizio-gorputza $\mathcal{C}$-ren barruan dago, eta Jatorrizko Elementuaren Teoremagatik badakigu existitzen dela $\gamma \in L$ (jatorrizko elementua) halakoa non $L = \mathbb{Q}(\gamma)$ den. Badakigunez $L \subseteq \mathcal{C}$ izateagatik $\gamma \in \mathcal{C}$ dela, 1.3.7 korolarioarengatik $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ 2-ren berretura bat da. □

1.4 Antzinaroko hiru problema

Plutarko (46 - 120) filosofo eta moralista greziarrak kontatzen zuenez, antzinako Greziako Delos hiriko biztanleak kezkatuta zeuden Apolo jainkoak bidali zien izurrite batengatik. Delfosko orakuluari galdezka joan ostean, hau izan omen zen orakuluak eman zien irtenbidea: Apoloren omenez Delosen zegoen aldarea, harrizko aldare kubiko handi bat, bikoiztu egin beharko zuten, jainkoaren haserrea baretzea nahi bazuten. Delostarrak txundituta geratu omen ziren orakuluak esandakoarekin, eta Platon filosofo handiari laguntza eskatu omen zioten aldare kubikoa bikoizteko modu bat eman ziezaien.

Ez Platon eta ezta bere ondorengoak ere ez ziren problema hau matematikoki ebazteko gai izan, eta mendeetan zehar ebatzi gabeko problema bat izan zen, angelua hirutan zatitzearen problemarekin eta zirkuluaren koadraturaren problemarekin batera. Alabaina, 1837 urtean Pierre Wantzel (1814 - 1848) matematikari frantziarrak zenbaki eraikigarrien teoria guk darabilgun ikuspuntu modernotik garatu zuen, eta honi esker hiru problema hauek behin-betiko erantzunda gelditu ziren. Hona hemen hiru problema klasiko hauek.

1 Angelua hirutan zatitzea

Problema honen helburua edozein angelu emanik hiru zati berdinetan zatitzea da. 1.1 aurrebaldintzetan jakintzat ematen da badakigula edozein angelu bitan zatitzen erregela eta konpasa erabiliz. Edozein angelu hirutan zatitzea ezinezkoa dela frogatuko dugu jarraian, eta horretarako nahikoa izango da hirutan zatitu ezin den angelu bat aurkitzea. Hartu $2\pi/3$ radianeko angelua, hots, $120°$ dituen angelua, eta suposatu 3-tan zatitu daitekela: honek esan nahi du $40°$ eraikigarria dela. Angelu hau $\mathbb{S}^1$ unitate-zirkunferentziarekin ebakitzen badugu, unitatearen 9-garren erroa, $\zeta_9 = e^{2\pi i/9}$ eraikigarria dela ondorioztatzen dugu ($40° = 2\pi/9$ rad delako).

Unitatearen 9-garren erroa $X^9 - 1$-ren erroa da era nabarian. Ohartu $X^3 - 1$ polinomioaren erro guztiak $X^9 - 1$-en erroak ere badirela, $\omega \in \mathbb{C}$ zenbakia $X^3 - 1$-en erroa bada $\omega^3 = 1$ delako, eta ondorioz $\omega^9 = (\omega^3)^3 = 1$. Beraz, $X^3 - 1$ polinomioak $X^9 - 1$ zatitzen du, eta zatiketa eginez, ζ_9 errotzat duen polinomioa $X^6 + X^3 + 1$ dela ondorioztatzen dugu. $X = Y + 1$ aldagai-aldaketa eginda,

$$(Y+1)^6 + (Y+1)^3 + 1 = Y^6 + 6Y^5 + 15Y^4 + 21Y^3 + 18Y^2 + 9Y + 3$$

dugu. Eisensteinen irizpidea aplikatzen badugu $p = 3$ hartuta, $X^6 + X^3 + 1$ polinomioa $\mathbb{Q}$ gainean irreduziblea dela ikus dezakegu. Hau dela eta, $Irr(\zeta_9, \mathbb{Q}) = X^6 + X^3 + 1$ da. Baina 1.3.7 korolarioa aplikatzen badugu, $\deg(Irr(\zeta_9, \mathbb{Q})) = 6$ ez denez 2-ren berretura bat, ζ_9 ez dela eraikigarria ondorioztatzen dugu, kontraesana dena. Beraz ezinezkoa da $120°$ angelua hirutan zatitzea, eta hortaz *angelua hirutan zatitzea* orokorrean ezinezko

eraikuntza geometriko bat dela frogatu dugu, orain dela 2000 urte egindako galdera bati erantzunez.

2 Zirkuluaren koadratura

Problema hau azalera jakin bateko zirkulu bat emanda azalera berdineko karratu bat eraikitzean datza. Aurreko kasuan bezala, gure unitateak moldatu egiten baditugu zirkuluaren erradioa 1 izan dadin, bere azalera π unitate-karratukoa izango da. Beraz, π unitate-karratuko karratu bat eraikitzea da gure helburua, hots, $\sqrt{\pi}$ aldea duen karratu bat eraikitzea. Gainera zirkuluaren erradioa 1 denez 0tik eta 1etik eraikitzen hasi garela onar dezakegu, eta beraz gure helburua lortzeko $\sqrt{\pi} \in \mathcal{C}$ izan beharko litzateke. Baina absurdura eramanez, $\sqrt{\pi} \in \mathcal{C}$ bada, orduan $(\sqrt{\pi})^2 = \pi \in \mathcal{C}$ ondorioztatzen dugu, eta 1.3.8 (i) adibidean frogatu dugunez $\pi \notin \mathcal{C}$ da. Absurdura iritsi garenez, *zirkuluaren koadratura* orokorki ezinezko problema bat da.

3 Kuboaren bikoizketa

Problema honen helburua bolumen jakin bateko kubo bat izanik, bolumen bikoitzeko kuboa eraikitzea da. Orokortasun-galerarik gabe, gure kuboaren aldeen luzera 1 dela suposa dezakegu. Ondorioz kuboaren bolumena 1 da, eta beraz 2 unitateko bolumena duen kubo bat eraikitzea da helburua.

Absurdura eramanez, demagun posible dugula kuboa bikoiztea: kuboaren aldea s bada bolumena $s^3 = 2$ izan beharko da, eta beraz 2 bolumen-unitateko kuboa eraikitzea lortu badugu $s = \sqrt[3]{2}$ zenbakia eraikitzea lortu dugu, s kuboaren aldearen luzera delako. Kubo zaharraren aldeak denak 1 luzerakoak zirenez, 0 eta 1 puntuetatik eraikitzen hasi garela onar dezakegu, eta ondorioz $\sqrt[3]{2} \in \mathcal{C}$ da. Baina hau kontraesanean dago 1.3.8 (ii) adibidean frogatutakoarekin. Hortaz, *kuboaren bikoizketa* ere orokorrean egin ezin den eraikuntza geometriko bat da.

2. kapitulua

Poligono erregularren eraikuntza

Bigarren hezkuntzako marrazketa teknikoko edozein liburutan aurki daitezke hexagono erregularra eraikitzeko metodoak. Pixka bat zailxeagoa den arren, pentagono erregularraren eraikuntzak ere ez du lan gehiegirik eskatzen, eta eskola-liburutan agertzen ez bada ere Gaussek heptadekagono erregularra eraikitzeko metodo bat aurkitu zuen 19 urte besterik ez zituela. Ez da ezagutzen, ordea, heptagono edo eneagono erregularra eraikitzeko modurik, hurbiltze-metodo oso onak baldin badaude ere.

Egoera honetan, bigarren hezkuntzako ikasle bati ere bururatuko litzaioke galdera natural hau: metodorik ezagutzen ez dugun arren, teorikoki posible al da heptagonoa edo eneagonoa eraikitzea? Eta edozein aldeko poligono erregularrak eraikitzea? Ezezkoan, zeintzuk dira eraiki daitezken poligono erregularrak, eta zeintzuk ez? Galdera hauek guztiak erantzungo dira kapitulu honetan.

2.1 Sarrera

Poligono erregularren eraikigarritasuna Galoisen teoriaren bitartez aztertuko dugu kapitulu honetan. Zenbaki eraikigarrien kapituluko emaitza batzuk erabili beharko dira, eta baita unitateen erroen teoria ere. Azken teoria hau kapitulu honetan behar bezala garatuko badugu ere, horretarako lehenik eta behin zenbakien teoriako oinarrizko emaitza batzuk gogorarazi beharko ditugu:

Definizioa 2.1.1. Izan bedi $n \in \mathbb{N}$ zenbaki arrunta. *Eulerren φ funtzioa* deitzen zaio $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ funtzioari non $\varphi(1) = 1$ den eta

$$\varphi(n) := |\{a \in \mathbb{N} | (a, n) = 1\}|,$$

baldin eta $n \geq 2$ bada.

Hau da, Eulerren φ funtzioak, n-n aplikatuta, n baino txikiagoak eta n-rekin elkarrekiko lehenak diren zenbat zenbaki dauden esaten du. Jarraian, Eulerren φ funtzioaren propietate interesgarri batzuk aipatuko ditugu.

Teorema 2.1.2. *Izan bedi Eulerren φ funtzioa, orain definitu dugun bezala. Orduan,*

(i) *Bi zenbaki arrunt, n eta m, elkarrekiko lehenak badira, $\varphi(nm) = \varphi(n)\varphi(m)$ da.*

(ii) *Baldin eta $n > 1$ zenbaki arrunta bada,*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

da, biderkadura hori n zatitzen duten p zenbaki lehen guztien artekoa izanik. Bereziki $n = p^m$ bada, p zenbaki lehena eta m zenbaki arrunta izanik,

$$\varphi(p^m) = p^m \left(1 - \frac{1}{p}\right) = p^m - p^{m-1}$$

dugu. Hortaz, $m = 1$ den kasu berezia hartuta, p zenbaki lehenaren φ funtzioaren balioa

$$\varphi(p) = p - 1$$

dela ondorioztatzen dugu.

(iii) *Edozein $n \in \mathbb{N}$ izanik,*

$$\sum_{d|n} \varphi(d) = n$$

Hurrengo emaitza *Fermaten teorema txikia* izenaz ezaguna da.

Proposizioa 2.1.3. *Izan bedi p zenbaki lehena. Orduan, edozein a zenbaki osorako*

$$a^{p-1} \equiv 1 \bmod p$$

Azkenik, *binomioaren teorema* aipatuko dugu, karakteristika p zenbaki lehena duten eraztunetarako.

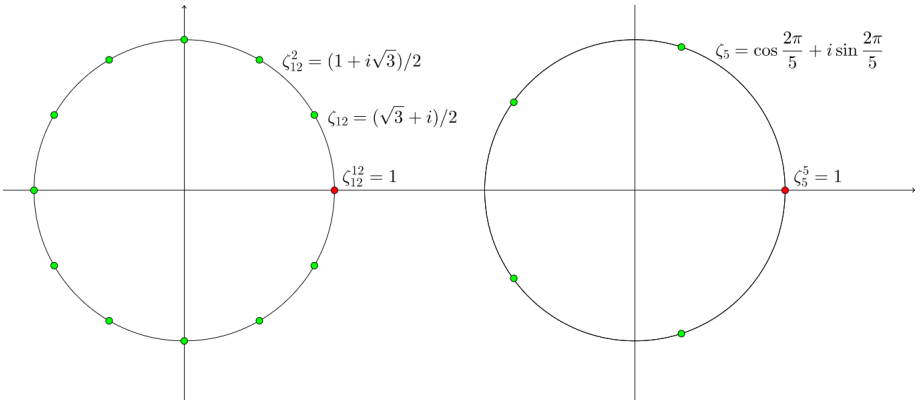
Proposizioa 2.1.4. *Izan bedi p zenbaki lehena eta p karakteristikadun A eraztuna. Edozein $a, b \in A$ izanik,*

$$(a + b)^p = a^p + b^p$$

betetzen da. Berreketa hau n aldiz errepikatuz, edozein $n \in \mathbb{N}$ hartuta, berehala ondorioztatzen da

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

emaitza ere betetzen dela.



2.1. irudia. Unitatearen 12-garren eta 5-garren erroak, $\mathbb{S}^1$ unitate-zirkunferentzia 12 eta 5 zatitan banatzen dutenak, hurrenez hurren.

2.2 Unitatearen erroak

Izan bedi $n \in \mathbb{N}$ zenbaki arrunta. Definizioz, *unitatearen n-garren erro* deitzen zaie $X^n - 1$ polinomioaren erroak diren zenbaki konplexuei. Notazio polarra erabiltzen badugu, hauek dira $X^n - 1$-en n erro desberdin (eta ondorioz erro guztiak):

$$\mathcal{R}_n = \{e^{\frac{2\pi ik}{n}}\}_{k=1}^{n} = \{e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}, 1\}$$

Ohartu zenbaki konplexu horien argumentuak $\{\frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2\pi(n-1)}{n}, 2\pi\}$ direla, eta beraz zenbaki hauek $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ unitate-zirkunferentzia n zati berdinetan banatzen dutela (ikusi goiko 2.1. irudia). Funtsezko emaitza hau da poligono erregularren eraikuntza aztertzeko unitatearen erroak erabiltzearen arrazoia.

Definizioa 2.2.1. Izan bedi $n \in \mathbb{N}$ zenbaki arrunta eta $\zeta_n \in \mathcal{R}_n$, unitatearen n-garren erroa. Honela definitzen da *n-garren polinomio ziklotomikoa*:

$$\Phi_n(X) := \prod_{\substack{0 \le i < n \\ (n,i)=1}} (X - \zeta_n^i)$$

Gauza jakina da $(\mathcal{R}_n, \cdot)$ talde zikliko bat dela, eta hemendik aurrera $\mathcal{R}_n$-ren sortzaileei unitatearen *jatorrizko n*-garren erro deituko diegu. Baldin eta $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathcal{R}_n$ bada, orduan argi dago $\langle \zeta_n \rangle = \mathcal{R}_n$ dela, hau da, ζ_n taldeko sortzaile bat dela eta ondorioz unitatearen *jatorrizko* n-garren erro bat. Talde-teoriagatik badakigu beste sortzaile guztiak ζ_n^i motakoak izango direla, i eta n elkarrekiko lehenak direnean. Honek polinomio ziklotomikoak definitzeko beste era baliokide bat emango digu.

Proposizioa 2.2.2. *Izan bedi $n \in \mathbb{N}$ zenbaki arrunta. Orduan, $\Phi_n(X)$ polinomioa n-garren polinomio ziklotomikoa da baldin eta soilik baldin*

$$\Phi_n(X) = \prod_{\substack{0 \leq i < n \\ \zeta_n^i \ jatorrizkoa}} (X - \zeta_n^i)$$

Adibideak 2.2.3. (i) *$n = 1$ denean kasu tribiala da, $\Phi_1(X) = X - 1$ baita.*

(ii) *$n = 2$ bada, unitatearen jatorrizko 2-garren erro bakarra -1 denez $\Phi_2(X) = X + 1$.*

(iii) *$n = 4$ kasuan, $X^n - 1 = X^4 - 1 = (X^2 + 1)(X + 1)(X - 1)$ da. Gainera, 4-rekin elkarrekiko lehenak diren zenbakiak 1 eta 3 direnez, unitatearen jatorrizko 4-garren erroak i eta $i^3 = -i$ dira. Ondorioz, $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$ da.*

Adibideko hiru polinomio ziklotomikoak biderkatzen baditugu $X^4 - 1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)$ faktorizazioa lortzen dugu. Edozein $n \in \mathbb{N}$ kasura orokortzen saiatzen bagara, ohartu unitatearen jatorrizko n-garren erro guztiak $X^n - 1$ polinomioaren erroak direla. Izan ere, unitatearen jatorrizko n-garren erroak unitatearen n-garren erro berezi batzuk besterik ez dira. Beraz, $\Phi_n(X)$ polinomioaren erro guztiak $X^n - 1$-en erroak direnez, $\Phi_n(X)$ polinomioak $X^n - 1$ zatituko du beti. Hauxe litzateke jarraian burura etorriko litzaigukeen galdera: zein da orokorrean $X^n - 1$-en faktorizazioa?

Proposizioa 2.2.4. *Izan bedi $n \in \mathbb{N}$. Orduan, n-garren polinomio ziklotomikoa $\varphi(n)$ mailako polinomio monikoa da. Gainera, polinomio hauek faktorizazio hau betetzen dute:*

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Froga. Hartu $n \in \mathbb{N}$ edozein. Definizioagatik argi dago $\Phi_n(X)$ monikoa dela. Jatorrizkoak diren unitatearen n-garren erroak hain justu ζ_n^i motakoak direnez, i eta n elkarrekiko lehenak izanik, guztira horrelako $\varphi(n)$ erro daudela ere argi dago. Beraz, $\Phi_n(X)$-k lehen mailako $\varphi(n)$ faktore izango dituenez berehalakoa da bere maila $\varphi(n)$ dela. Har dezagun frogatu nahi dugun berdintzako eskuin aldeko polinomioaren erro bat: $\zeta \in \mathbb{C}$ non

$$\prod_{d|n} \Phi_d(\zeta) = 0$$

betetzen den. Hortaz ζ biderkadura horretako polinomioren baten erroa da, eta ondorioz existitzen da n zatitzen duen d_0 zenbaki arrunta non $\Phi_{d_0}(\zeta) = 0$ den. Beraz ζ unitatearen jatorrizko d_0-garren erroa da, eta ondorioz $\zeta^{d_0} = 1$

da. Baina $d_0|n$ denez existitzen da $m \in \mathbb{N}$ non $d_0 m = n$ den, eta ondorioz $1 = 1^m = (\zeta^{d_0})^m = \zeta^n$, eta hemendik ζ unitatearen n-garren erroa ere badela ondorioztatzen dugu. Beraz

$$\prod_{d|n} \Phi_d(X) | X^n - 1$$

da, aurreko biderkadura horren erro guztiak $X^n - 1$-en erroak direlako. Gainera, frogatu berri dugunez $\deg(\Phi_d(X)) = \varphi(d)$ dela, 2.1.2 teoremako (iii) atala kontuan hartuta

$$\deg\left(\prod_{d|n} \Phi_d(X)\right) = \sum_{d|n} \deg\left(\Phi_d(X)\right) = \sum_{d|n} \varphi(d) = n$$

dugu, eta ondorioz polinomio batek bestea zatitzeaz gain biek maila bera dute. Azkenik, biak definizioz monikoak dira, eta beraz berdinak direla ondorioztatzen dugu, frogatu nahi genuena. □

Gure hurrengo helburua $\Phi_n(X)$ polinomioaren irreduzibilitatea frogatzea izango da. Horretarako, gorputz finituen gaineko polinomioen inguruko propietate berezi bat frogatu beharko dugu lehenik eta behin.

Lema 2.2.5. *Izan bedi p zenbaki lehena eta $f(X) \in \mathbb{F}_p[X]$. Kasu horretan $f(X^p) = f(X)^p$ betetzen da.*

Froga. Idatz dezagun lehenik eta behin $f(X) \in \mathbb{F}_p[X]$ polinomioaren garapena. f-ren maila n bada, badakigu existituko direla $\{\overline{a}_i\}_{i=0}^n \subset \mathbb{F}_p$ zenbakiak

$$f(X) = \sum_{i=0}^{n} \overline{a}_i X^i$$

izanik. $\mathbb{F}_p[X]$ eraztunaren karakteristika p denez, 2.1.4 proposizioagatik

$$f(X)^p = \left(\sum_{i=0}^{n} \overline{a}_i X^i\right)^p = \sum_{i=0}^{n} \overline{a}_i^p X^{pi}$$

dugu. Gainera, 2.1.3 proposizioagatik edozein a zenbaki osorako $a^{p-1} \equiv 1 \mod p$ denez, klaseak hartuta $\overline{a}^{p-1} = \overline{1}$ izango da $\mathbb{F}_p$ gorputzean, eta beraz $\overline{a}^p = \overline{a}$. Emaitza hau f polinomioaren koefizienteei aplikatzen badiegu, edozein $i = 1, \ldots, n$ izanik, $\overline{a}_i^p = \overline{a}_i$ izango da. Ondorioz

$$\sum_{i=0}^{n} \overline{a}_i^p X^{pi} = \sum_{i=0}^{n} \overline{a}_i X^{pi} = f(X^p),$$

frogatu nahi genuena. □

Teorema 2.2.6. *Izan bedi $n \in \mathbb{N}$. Orduan $\Phi_n(X) \in \mathbb{Z}[X]$, eta irreduziblea da $\mathbb{Q}$ gainean.*

Froga. Ikustagun lehenik eta behin $\Phi_n(X) \in \mathbb{Z}[X]$ dela, n-ren gaineko indukzioz. Tribiala da $n = 1$ kasua, $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$ delako. Gainera, 2.2.4 proposizioagatik

$$X^n - 1 = \Phi_n(X) \cdot \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$$

dugu. Biderketa hau koefiziente osoak dituen polinomio moniko baten eta $\Phi_n(X)$-ren arteko biderketa da, hipotesi induktiboagatik $\Phi_d(X) \in \mathbb{Z}[X]$ baita, $d < n$ guztietarako. Beraz, argi dago $\Phi_n(X) \in \mathbb{Z}[X]$ dela.

Irreduzibilitatea frogatzeko, har dezagun $f(X) = Irr(\zeta_n, \mathbb{Q})$ polinomioa eta ikustagun $\Phi_n(X)$-ren berdina dela. Badakigu ζ_n zenbakia n-garren polinomio ziklotomikoaren erroa dela, eta ondorioz $f(X)|\Phi_n(X)$ betetzen dela. Gainera ohar gaitezen biak monikoak direla, eta ondorioz nahikoa dela $\Phi_n(X)|f(X)$ betetzen dela frogatzea. Hori frogatzea lortzeko, $\Phi_n(X)$-ren edozein erro hartuko dugu, eta f-ren erroa dela ikusiko dugu. Horretarako:

- Ikustagun baldin eta n zatitzen ez duen p zenbaki lehena badugu, eta $\alpha \in \mathbb{C}$ zenbakia f-ren erro bat bada, orduan α^p ere f-ren erroa dela. Horretarako, absurdura eramanez demagun existitzen dela $\alpha \in \mathbb{C}$ zenbakia f-ren erroa dena, α^p f-ren erroa ez delarik. Badakigu $f(X)|X^n - 1$ dela, eta beraz existitzen dela $g(X) \in \mathbb{Q}[X]$ polinomioa non

  $$X^n - 1 = f(X)g(X)$$

  den. Gauss-en lemagatik, badakigu existituko direla $\lambda, \mu \in \mathbb{Q}$ zenbakiak, $\lambda \cdot f(X) = \tilde{f}(X)$ eta $\mu \cdot g(X) = \tilde{g}(X)$ harturik $\tilde{f}(X)\tilde{g}(X) = X^n - 1$ eta $\tilde{f}(X), \tilde{g}(X) \in \mathbb{Z}[X]$ beteko dutenak. Gainera, f-ren eta $\tilde{f}$-ren erroak berdinak dira, eta baita g-renak eta $\tilde{g}$-renak ere. Ondorioz, $X^n - 1 = f(X)g(X)$ faktorizazioan, $f(X), g(X) \in \mathbb{Z}[X]$ suposa genezake hemendik aurrera.

  Hipotesiz α^p ez da $f(X)$-ren erroa, baina bai $X^n - 1$-rena. Izan ere, α hipotesiz f-ren erro bat denez eta $f(X) \mid \Phi_n(X)$, α unitatearen jatorrizko n-garren erro bat izango da. Ondorioz, α^p halabeharrez $g(X)$-ren erroa izan beharko da: $g(\alpha^p) = 0$ beteko da orduan, hau da, α zenbakia $g(X^p)$-ren erroa dela. Hortaz, f-ren erro guztiak $g(X^p)$-renak ere badirenez $f(X) \mid g(X^p)$ betetzen da. Zatiketa hau koefiziente osoak dituzten polinomioen artekoa denez, existitzen da $h(X) \in \mathbb{Z}[X]$ polinomioa non

  $$g(X^p) = f(X)h(X)$$

  den. Badakigu $f(X)$ monikoa dela, eta beraz hala dira $g(X^p)$ eta $h(X)$ ere. Har ditzagun polinomio guzti horiek orain $\mathbb{F}_p[X]$ polinomioen

eraztunean (koefiziente bakoitzaren klaseak hartuta). 2.2.5 lemagatik $\overline{g}(X^p) = \overline{g}(X)^p$ da, eta ondorioz $\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$ dugu.

Hortaz, $\overline{f}(X)$-ren $\overline{q}(X)$ faktore irreduzible bat hartzen badugu, honek $\overline{g}(X)^p$ zatituko du eta beraz $\overline{g}(X)$ ere bai. Orduan, $\overline{q}(X)|\overline{f}(X)$ eta $\overline{q}(X)|\overline{g}(X)$ dugunez, $\overline{q}(X)^2|\overline{f}(X)\overline{g}(X) = X^n - \overline{1}$ lortuko dugu.

Har dezagun $X^n - \overline{1}$ polinomioaren deskonposizio-gorputza $\mathbb{F}_p$-n, eta dei diezaiogun F. $\overline{q}(X)^2|\overline{f}(X)\overline{g}(X) = X^n - \overline{1}$ denez, $\overline{q}(X)$ polinomioaren F gaineko erro guztiak $X^n - \overline{1}$-ek gutxienez bi aldiz errepikatuak izango ditu. Beraz, $X^n - \overline{1}$ polinomioak erro anizkoitzen bat izango du bere deskonposizio-gorputzean, eta beraz definizioz ez da polinomio banangarria izango. Alabaina, A eranskineko 5 ariketak esaten digu kasu honetan $X^n - \overline{1}$ eta bere deribatu formala, $\overline{n}X^{n-1}$, ez direla elkarrekiko lehenak izango. Baina hau absurdua da, $p \nmid n$ denez $\overline{n}X^{n-1}$ polinomio ez-nulua baita, $X = \overline{0}$ bere erro bakarra izanik. $\overline{0}$ ez denez $X^n - \overline{1}$-en erroa, bi polinomio hauek ez dute erro komunik. Ondorioz, $X^n - \overline{1}$ eta bere deribatua elkarrekiko lehenak dira, eta hau kontraesana da.

- Orain badakigu $\alpha \in \mathbb{C}$ zenbakia $f(X) = Irr(\zeta_n, \mathbb{Q})$-ren erroa bada α^p ere izango dela, $p \nmid n$ baldin bada. Erro guzti hauek unitatearen jatorrizko n-garren erroak direnez, $f(X) \mid \Phi_n(X)$ delako, halakoak izango dira α eta α^p ere.

  Badakigu unitatearen jatorrizko n-garren erroak hain justu $\mathcal{R}_n = \{e^{\frac{2\pi ik}{n}}\}_{k=1}^n$ talde zikliko biderkakorraren sortzaileak direla. Talde horretako sortzaile bat, $\zeta \in \mathcal{R}_n$ finkatzen badugu, beste sortzaile guztiak ζ^m motakoak izango dira, $m \in \mathbb{Z}$ zenbakia n-rekin elkarrekiko lehena den zenbaki osoa izanik. Gure kasu partikularrean, α unitatearen jatorrizko n-garren erro bat denez, unitatearen beste jatorrizko n-garren erro guztiak α^m motakoak izango dira, $m \in \mathbb{Z}$ eta $\text{zkh}(n, m) = 1$ izanik. m-ren faktorizazioa zenbaki lehenetan $m = p_1 \dots p_r$ bada (zenbaki lehen hauek errepikatuta egon daitezke), badakigu $\text{zkh}(n, m) = 1$ denez $p_i \nmid n$ dela, edozein $i = 1, \dots, r$ izanik. Honenbestez, aurreko puntuan frogatu duguna aplikatuz α zenbakia f-ren erroa denez, α^{p_1} ere f-ren erroa izango da. Baina α^{p_1} zenbakia f-ren erroa bada, orduan $(\alpha^{p_1})^{p_2} = \alpha^{p_1 p_2}$ ere halakoxea izango da. r-ren gaineko indukzioa aplikatuz erraz frogatzen da honenbestez $\alpha^{p_1 \cdots p_r} = \alpha^m$ ere f-ren erroa dela.

  Ondorioz, n-rekin elkarrekiko lehena den edozein $m \in \mathbb{Z}$ hartuta α^m zenbakia f-ren erroa denez, unitatearen jatorrizko n-garren erro guztiak f-ren erroak ere izango dira. Hau da, $\Phi_n(X) \mid f(X)$ beteko da, frogatu nahi genuena.

□

2.2.4 proposiziotik eta 2.2.6 teorematik berehalako emaitza bat ondorioztatzen da.

Korolarioa 2.2.7. *Izan bedi $n \in \mathbb{N}$ eta ζ_n, unitatearen jatorrizko n-garren erroa. Orduan $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ da. Gainera, $\Phi_n(X)$-ren deskonposizio-gorputza $\mathbb{Q}$ gainean hain zuzen ere $\mathbb{Q}(\zeta_n)$ da.*

Froga. Batetik, badakigu ζ_n, unitatearen jatorrizko n-garren erroa $\Phi_n(X)$-ren erroa dela. Polinomio hau monikoa da 2.2.4 proposizioagatik eta irreduziblea da 2.2.6 teoremagatik. Beraz, $Irr(\zeta_n, \mathbb{Q}) = \Phi_n(X)$ da. Hemendik $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(Irr(\zeta_n, \mathbb{Q})) = \deg(\Phi_n(X))$ ondorioztatzen dugu, eta gainera, berriro ere 2.2.4 proposizioagatik $\deg(\Phi_n(X)) = \varphi(n)$ da. Hortaz, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ da.
Bestetik, $\Phi_n(X)$ polinomioaren erro guztien multzoa

$$\mathcal{E} = \{\zeta_n^i\}_{\substack{1 \leq i < n \\ (n,i)=1}}$$

denez ($\mathcal{E}$ multzoko elementuak errepikapenik gabe daude emanda), $\Phi_n(X)$-ren deskonposizio gorputza $\mathbb{Q}$ gainean $\mathbb{Q}(\mathcal{E})$ izango da. ζ_n zenbakiaren berreturak eginda erro guzti horiek sortzen direnez, berehalakoa da $\mathbb{Q}(\mathcal{E}) = \mathbb{Q}(\zeta_n)$ betetzen dela ikustea. □

Unitateen erroen atalarekin amaitzeko, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ hedaduraren Galoisen taldea zein den kalkulatuko dugu jarraian. Azken emaitza honen ondoren, benetan prest egongo gara poligono erregularren eraikigarritasuna aztertzeko.

Teorema 2.2.8. *Izan bedi $n \geq 2$ zenbaki arrunta eta $\zeta_n \in \mathbb{C}$ unitatearen jatorrizko n-garren erro bat. Orduan,*

(i) *$\mathbb{Q}(\zeta_n)$ gorputza $\mathbb{Q}$-ren Galoisen hedadura da.*

(ii) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

Froga. Argi dago $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ hedadura normala dela, 2.2.7 korolarioagatik $\mathbb{Q}(\zeta_n)$ baita $\Phi_n(X)$ polinomioaren deskonposizio-gorputza $\mathbb{Q}$ gainean. Gainera, $\mathrm{char}\,\mathbb{Q}(\zeta_n) = \mathrm{char}\,\mathbb{Q} = 0$ da, eta beraz $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ Galoisen hedadura izango da.
Hurrengo puntua frogatzeko, dei dezagun $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ eta hartu $\sigma \in G$ edozein. Badakigu σ guztiz zehaztuko duela $\sigma(\zeta_n)$ irudiak, berriro ere unitatearen jatorrizko n-garren erroa izan beharko dena. Beraz $\sigma(\zeta_n) = \zeta_n^k$ izan beharko da, non k eta n elkarrekiko lehenak diren. Ideia honetatik abiatuta eraiki $\psi : G \longrightarrow \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ non $\psi(\sigma) = k$ den, eta ikustagun ψ talde-monomorfismoa dela. Edozein $\sigma, \sigma' \in G$ hartuta $\sigma(\zeta_n) = \zeta_n^k$ eta $\sigma'(\zeta_n) = \zeta_n^{k'}$ izanik, orduan $(\sigma \circ \sigma')(\zeta_n) = \sigma(\zeta_n^{k'}) = \zeta_n^{kk'}$ da. Hortaz, $\psi(\sigma \circ \sigma') = kk' = \psi(\sigma)\psi(\sigma')$ denez, ψ talde-homomorfismoa da. Injektibotasuna betetzen dela ikusteko, ohartu $\psi(\sigma) = 1$ bada, zuzenean $\sigma(\zeta_n) = \zeta_n^1 = \zeta_n$ dela, eta beraz

$\sigma = 1_G$ ondorioztatzen dela, badakigulako ζ_n-ren irudiak guztiz zehazten duela σ automorfismoa. Jarraitzeko, $\mathbb{Q}(\zeta_n)$ gorputza $\mathbb{Q}$-ren Galoisen hedadura denez $|G| = |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ da. Gainera, 2.2.7 korolarioagatik $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ da. Beraz, frogarekin bukatzeko $\psi : G \longrightarrow \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ talde-homomorfismo injektiboa denez, G finitua denez eta

$$|G| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})|$$

betetzen denez, zuzenean ψ talde-isomorfismoa dela ondorioztatzen dugu, nahi genuena.

□

2.3 Poligono erregularren eraikigarritasuna

Iritsi gara kapitulu honen muinera: unitatearen erroen teoria zenbaki eraikigarrienarekin elkarturik, gai izango gara n aldeko poligono erregularra erregela eta konpas bitartez eraiki daiteken edo ez erabakitzeko, n-ren arabera. Horretarako, lehenik eta behin defini ditzagun zenbaki lehen berezi batzuk, funtsezkoak izango direnak gure teoria garatzeko.

Definizioa 2.3.1. Izan bedi n zenbaki lehen bakoitia. Orduan n *Fermaten zenbakia* dela esango dugu

$$n = 2^{2^r} + 1$$

moduan idatz baldin badaiteke, $r \geq 0$ zenbaki osoa izanik. Gainera n zenbaki lehena bada, *Fermaten lehena* deituko diogu.

Zenbaki hauek Pierre de Fermat (1601 - 1665) matematikariak erabili zituen lehen aldiz, eta hari zor diote izena. Oro har, Fermaten m-garren zenbakia esaten zaio $F_m = 2^{2^m} + 1$ zenbakiari, eta Fermaten lehenengo bost zenbakiak

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

dira. Bost hauetatik guztiak lehenak dira, eta Frematek r guztietarako F_r Fermaten zenbakia lehena izango zela susmatzen zuen. Alabaina, Leonhard Euler (1707 - 1783) matematikari handiak $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ faktorizazioa lortu zuen 1732 urtean. Are gehiago, gaur egun r berretzailea 5 eta 32 artean baldin badago ezaguna da $F_r = 2^{2^r} + 1$ zenbakia konposatua dela. Hala ere, oraindik frogatu gabe dago adibidez F_{33} zenbakia lehena den ala ez.

Eulerrek F_5 faktorizatzea lortu zuenean, Gaussek arreta apur bat jarri zien zenbaki hauei urte batzuetan zehar, eta poligono erregularren erregela eta konpas bitartezko eraikigarritasunarekin lotu zuen *Disquisitiones Arithmeticae* obra handian. Haren pausuei jarraituz, guk ere berdina egingo dugu jarraian.

Teorema 2.3.2. *Izan bedi $n > 2$ zenbaki osoa. Orduan, n aldeko poligono erregularra eraikigarria da erregela eta konpas bitartez baldin eta soilik baldin*

$$n = 2^s p_1 \dots p_r$$

bada, $s \geq 0$ zenbaki osoa eta $p_1, \dots, p_r$ zenbakiak, Fermaten r zenbaki lehen desberdin ($r \geq 0$) izanik.

Froga. A eranskineko 6 ariketan frogatzen da n aldeko poligono erregularra eraikigarria dela baldin eta soilik baldin ζ_n zenbaki eraikigarria bada. Beraz, aski dugu $\zeta_n \in \mathcal{C}$ frogatzea. Aurreko emaitzetatik abiatuta, honako hau dakigu:

- Badakigu ζ_n aljebraikoa dela $\mathbb{Q}$ gainean, eta $Irr(\zeta_n, \mathbb{Q}) = \Phi_n(X)$ dela ere bai 2.2.6 teoremagatik. Gainera, 2.2.7 korolarioagatik $\Phi_n(X)$-ren deskonposizio-gorputza $\mathbb{Q}(\zeta_n)$ da.
- Ondorioz, aurreko kapituluko 1.3.12 teoremagatik $\zeta_n \in \mathcal{C}$ izango da baldin eta soilik baldin $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ maila 2-ren berretura bada.
- Gainera, berriro ere 2.2.7 korolarioagatik $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ da, φ Eulerren funtzioa izanik.

Eta honenbestez, ζ_n eraikigarria izango da baldin eta soilik baldin $\varphi(n)$ zenbakia 2-ren berretura bada.

Suposatu $n = 2^s p_1 \dots p_r$ dela, $p_1, \dots, p_r$ Fermaten lehen ezberdinak izanik. 2.1.2 teoremako (ii) puntuagatik,

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

da, eta $2^s, p_1, \dots, p_r$ guztiak binaka elkarrekiko lehenak direnez, 2.1.2 teoremako (i) puntuagatik

$$\varphi(n) = \varphi\left(2^s p_1 \dots p_r\right) = \varphi(2^s)\varphi(p_1) \dots \varphi(p_r)$$

da. Are gehiago, teorema bereko (ii) puntuagatik $\varphi(2^s) = 2^s - 2^{s-1} = 2^{s-1}$ da eta $p_1, \dots, p_r$ guztiak zenbaki lehenak direnez,

$$\varphi(2^s)\varphi(p_1) \dots \varphi(p_r) = \begin{cases} 2^{s-1}(p_1 - 1) \dots (p_r - 1), s > 0 \text{ bada,} \\ (p_1 - 1) \dots (p_r - 1), s = 0 \text{ bada} \end{cases}$$

Ondorioz, p_i guztiak Fermaten lehenak direnez, zuzenean $\varphi(n)$ zenbakia 2-ren berretura bat da. Izan ere, $p_i = 2^{2^i} + 1$ denez, $p_i - 1$ zenbakia 2-ren berretura izango da, edozein $i = 1, \dots, r$ izanik. Beraz, $\zeta_n \in \mathcal{C}$ izango da.

Beste inplikazioa frogatzeko, suposatu $\varphi(n)$ hipotesiz 2-ren berretura dela. Suposa dezagun n-ren faktorizazioa $n = q_1^{a_1} \dots q_s^{a_s}$ dela, $q_1, \dots, q_s$

zenbaki lehen ezberdinak eta $a_1, \ldots, a_s$ berretzaileak denak $a_i \geq 1$ izanik, $\forall i = 1, \ldots, s$. Berriro ere 2.1.2 teoremako (ii) atalagatik,

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{q_i}\right) = n \left(\frac{q_1 - 1}{q_1}\right) \cdots \left(\frac{q_s - 1}{q_s}\right) =$$

$$= q_1^{a_1 - 1}(q_1 - 1) \ldots q_s^{a_s - 1}(q_s - 1)$$

Izan bedi $i = 1, \ldots, s$ edozein. Harturik q_i lehena, nahikoa da 2-ren ezberdina den kasuan, Fermaten lehena dela ondorioztatzea. Bestalde, baldin eta q_i zenbaki lehen bakoitia bada, $a_i = 1$ izan beharko da, hipotesiz $\varphi(n)$ zenbakia 2-ren berretura delako. Eta berriro ere $\varphi(n)$ zenbakia 2-ren berretura delako, $q_i - 1$ zenbakia ere 2-ren berretura izan beharko da, eta ondorioz $q_i = 2^{m_i} + 1$ motakoa, $m_i \in \mathbb{N} \cup \{0\}$ izanik. Baina A eranskineko 7 ariketan frogatu dugunez, zenbaki lehen bat mota horretakoa denean, halabeharrez m_i zenbakia 2-ren berretura bat da. Beraz, q_i zenbaki lehena Fermaten lehena izan beharko da, frogatu nahi genuena. □

Adibideak 2.3.3. (i) Kapituluaren hasierara joz, pentagono eta hexagono erregularra eraikitzeko moduak ezagunak direla aipatu dugu. Kontrasta dezagun lehendik genekiena aurreko 2.3.2 teoremak esaten digunarekin. Ohar gaitezen 5 zenbakia Fermaten lehena dela eta $6 = 2^1 \cdot 3$ dela, 3 ere Fermaten lehena izanik. Ondorioz, aurreko teoremako baldintzak betetzen direnez bai pentagono eta bai hexagono erregularra poligono eraikigarriak dira. Beraz, 2.3.2 teorema bat dator lehenagotik *a priori* genekienarekin.

(ii) Gaussek bazuen teorema honen berri, eta $F_2 = 17$ Fermaten zenbakia denez, heptadekagono erregularra eraikigarria dela baieztatu zuen. Horrekin nahikoa ez, eta metodo esplizitu bat ere eman zuen.

(iii) Kapituluaren hasieran esan dugun bezala, ez da ezagutzen heptagono eta eneagono erregularrak eraikitzeko metodorik. 2.3.2 teorema aplikatuz, ohar gaitezen 7 eta 9 ez direla 2-ren berretura baten eta Fermaten lehenen arteko biderkadura. Ondorioz, **heptagono eta eneagono erregularrak ezin dira eraiki erregela eta konpasa erabiliz**, eta beraz ez da harritzekoa hauek eraikitzeko metodorik inork aurkitu ez izana.

(iv) 65537 zenbakia Fermaten lehena da, $F_4 = 2^{2^4} + 1 = 65537$ baita. Beraz, teorikoki posible da 65537 aldeko poligono erregularra eraikitzea erregela eta konpasa erabiliz. Lehenengo begiratuan, dena den, honetarako metodo bat aurkitzeak izugarrizko lan astuna eta ia ezinezkoa ematen du. Hala ere, Johann Gustav Hermes (1846 - 1912) matematikariak metodo esplizitu bat ematea lortu zuen 1894 urtean. Ez zitzaion oso erraza suertatu, 10 urte eman baitzituen 200 orri baino gehiagoko eskuizkribua osatzen.

Oharra 2.3.4. Fermaten lehenen ezagutzak badu zer esana eraikuntza geometrikoen inguruan. Frogarik oraindik argitaratu ez bada ere, matematikari batzuek uste dute Fermaten lehen bakarrak, hain zuzen ere, Fermatek ezagutzen zituen bostak zirela, hau da, F_0, F_1, F_2, F_3 eta F_4. Hau egia balitz, 2.3.2 teoremak ondokoa ere inplikatuko luke: n aldeko poligono erregularra eraikigarria da baldin eta soilik baldin

$$n = 2^s \cdot 3^a \cdot 5^b \cdot 17^c \cdot 257^d \cdot 65537^e$$

bada, $s \geq 0$ eta a, b, c, d, e guztiak 0 edo 1 izanik. Argi dago emaitza hau 2.3.2 teorema baino askoz ere gogorragoa dela.

3. kapitulua

Origami zenbakiak

Orain arte eraikigarritasunaz hitz egin dugun guztietan, erregela eta konpasa erabiliz eraiki daitezken objektu geometrikoetaz hitz egin dugu. Zehazki, 1 kapituluan zenbaki eraikigarriak zein diren aztertu dugu, erregela eta konpasa bakarrik erabili daitezkeen kasuan. Kapitulu honetan, beste baliabide bat ere sartuko dugu jokoan: "papera tolestea" edo *origami*-a.

Origamia (edo papiroflexia) japoniar jatorria duen artea da: guraize eta kolarik erabili gabe papera tolestean datza, hainbat formatako paperezko irudiak lortzeko. Origamiaren ideian oinarrituta plano konplexuan puntuak eraikitzeko modu berri bat plantea daiteke, hain zuzen ere planoa "tolestearen" ideia.

Jarraian, puntu berriak eraikitzeko erregela eta konpasaz gain origamia ere erabiltzeak emango digun abantailetako bat aurkeztuko dugu, origamirik gabe edukiko ez genukeena.

3.1 Angelua hirutan zatitzea

1 kapituluko 1.4 atalean ikusi dugunez, ezinezkoa da edozein angelu hirutan banatzea erregela eta konpasa erabiliz. Alabaina, atal honetan ikusiko dugu hau posible izango dela, erregela eta konpasaz gain origamiaz ere baliatzen bagara.

Ohar gaitezen lehenik eta behin $\theta \in [0, 2\pi)$ edozein angelu hartuta badakigula θ erdibitzen eta bikoizten, 1.1 aurrebaldintzetan hala eskatzen baita. Beraz, nahikoa izango dugu $\theta \in [\frac{\pi}{4}, \frac{\pi}{2})$ tartean dagoenean, angelua hirutan nola zatitu jakitea. Hona hemen zergatia.

- $\theta \in (0, \frac{\pi}{4})$ baldin bada ($\theta = 0$ kasua tribiala da), har dezagun $n = \min\{m \in \mathbb{N} \mid 2^m\theta \geq \frac{\pi}{4}\}$. Alegia, θ angelua behin eta berriro bikoiztuko dugu, $\frac{\pi}{4}$ radian edo gehiagokoa izan arte. n minimoa hartu dugunez,

$$2^{n-1}\theta < \frac{\pi}{4} \leq 2^n\theta$$

izango da. Absurdura eramanez $\frac{\pi}{2} \leq 2^n\theta$ balitz, orduan erdibituz $\frac{\pi}{4} \leq 2^{n-1}\theta$ litzateke, absurdua dena. Beraz, $2^n\theta < \frac{\pi}{2}$ da.

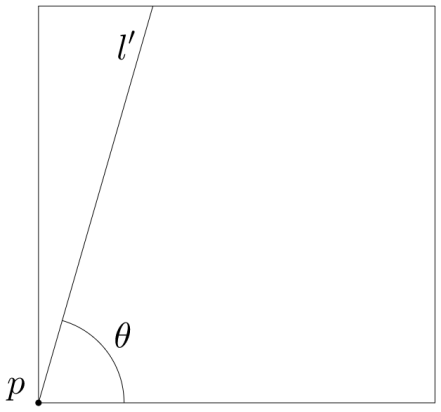
Honenbestez, angelua n aldiz bikoiztuz $2^n\theta \in [\frac{\pi}{4}, \frac{\pi}{2})$ lortu dugu. Aipatutako tarte honetan angeluak hirutan zatitzen jakingo bagenu, $\frac{2^n\theta}{3}$ eraikiko genuke eta jarraian angelu hau n aldiz erdibitu. Honela, $\frac{\theta}{3}$ eraikitzea lortuko genuke.

- $\theta \in [\frac{\pi}{2}, \pi)$ baldin bada, ordea, bitan zatituko dugu eta horrela $\frac{\theta}{2} = \tilde{\theta} \in [\frac{\pi}{4}, \frac{\pi}{2})$ izango da. Hemen angelua hirutan zatitu baldin badezakegu, orduan $\frac{\tilde{\theta}}{3}$ eraiki eta ondoren bikoiztu egingo dugu. Beraz, $\frac{2\tilde{\theta}}{3} = \frac{\theta}{3}$ eraikita izango dugu.

- $\theta \in [\pi, 2\pi)$ baldin bada, estrategia berdina erabiliz $\tilde{\theta} = \frac{\theta}{2}$ eraikiko dugu lehenik eta behin, eta $\tilde{\theta} \in [\frac{\pi}{2}, \pi)$ izango da. Orain aurreko kasuan gaude, eta beraz $\frac{\tilde{\theta}}{3}$ eraiki ondoren bikoiztu egingo dugu. Horrela, $\frac{2\tilde{\theta}}{3} = \frac{\theta}{3}$ eraikita izango dugu.

Ondorioz, esan bezala $\theta \in [\frac{\pi}{4}, \frac{\pi}{2})$ kasurako, θ hirutan zatitzen jakitea nahikoa izango da.

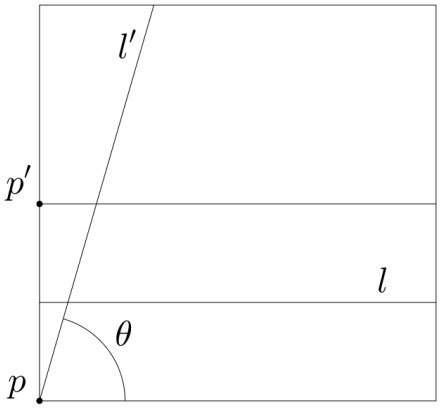
Har dezagun beraz planoko eremu karratu bat, origamia egiteko gure paper-orria izango dena, eta oinarritik abiatuta eraiki dezagun $[\frac{\pi}{4}, \frac{\pi}{2})$ tartean egongo den θ angelua, angeluaren erpina karratuaren oinarriko ezkerreko punta izanik.



3.1. irudia.

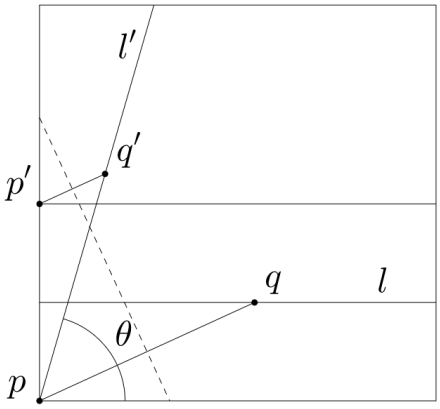
Jarraitzeko, karratuaren oinarria "gorantz" tolestuko dugu bi aldiz, oinarriarekiko paraleloak diren bi zuzen lortzeko. Gure paper-orriaren behealdea hartuko dugu, eta karratuaren oinarriarekiko paraleloa den zuzen batekiko tolestuko dugu. Orria behin tolestu ondoren, berriro ere tolestuko dugu

distantzia berdina erabiliz, tolestuta dagoen paperaren zatia berriro ere "barrurantz" sartuz (oinarriaren eta bi tolesturen arteko distantziak berdinak izatea garrantzitsua da). Tolesten dugun zatiaren albo-luzera zoriz aukera daiteke, eta 3.2. irudiko egoera izango da lortuko duguna.



3.2. irudia.

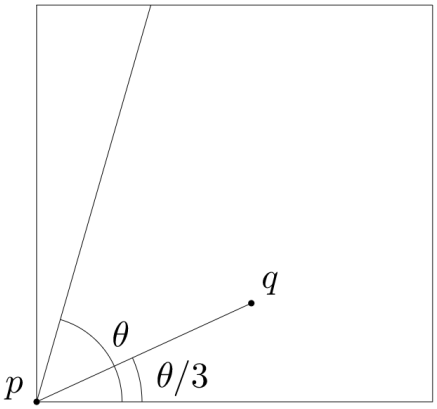
Jarraian, oinarria bigarren aldiz tolestean lortutako zuzenak orriaren ezkerraldea ebakitzen duen puntua hartu, eta deitu p' puntua. Oraingoan orria berriro tolestuko dugu, p' puntua oinarriarekin θ angelua osatzen duen l' zuzenera eramateko, eta angeluaren erpina lehen lortutako l zuzenera. Emaitza 3.3. irudikoa izango da.



3.3. irudia.

Bukatzeko, p eta q puntuetatik igarotzen den zuzena hartuko dugu. A eranskineko 8 ariketan frogatuko dugunez, zuzen honek karratuaren oinarriarekin osatzen duen angelua, hain zuzen ere, $\theta/3$ izango da, 3.4. irudian

azaltzen den bezala.



3.4. irudia.

Ondorioz, edozein $\theta \in [\frac{\pi}{4}, \frac{\pi}{2})$ angelutarako $\theta/3$ angelua origamia erabiliz eraikitzea posible dela frogatu dugu. Are gehiago esan genezake: kasu orokorra frogatzeko gure kasu partikularra frogatzea nahikoa denez, origamiaren bitartez edozein angelu hirutan zatitzea posible dela frogatu dugula.

3.2 Ekuazio kubikoak ebaztea

Badakigu erregela eta konpasa bakarrik erabilita ezin dugula edozein ekuazio kubiko ebatzi. Izan ere, absurdura eramanez hau hala balitz, bereziki $X^3 - 2 = 0$ ekuazioaren soluzioak plano konplexuan marrazteko gai izango ginateke. Hortaz, $\sqrt[3]{2}$ zenbaki eraikigarria izango litzateke, baina hau 1.3.8 (ii) adibidearekin kontraesanean dago. Honenbestez, orokorrean ezinezkoa da ekuazio kubiko bat erregela eta konpas bitartez bakarrik ebaztea.

Alabaina, jarraian ikusiko dugu hau neurri batean posible izango dela, erregela eta konpasaz gain origamia ere erabiltzen badugu. Horretarako, lehenik eta behin 3.1 atalean angelua hirutan zatitzeko erabiltzen den teknika sakonago aztertuko dugu, eta parabolen zuzen ukitzaileak eraikitzearekin lotuko dugu.

Gogora dezagun zein den parabolaren definizioa. Parabola bat $\mathbb{R}^2$ planoko leku geometriko bat da, $p \in \mathbb{R}^2$ puntua eta l zuzena emanik (parabolaren *fokua* eta *zuzentzailea* deitzen dira, hurrenez hurren), p puntura eta l zuzenera distantzia berera dauden puntuez osatua dagoena. Hots, $P \subseteq \mathbb{R}^2$ parabola

$$P = \{q \in \mathbb{R}^2 \mid d(p,q) = d(l,q)\}$$

betetzen duen leku geometrikoa izango da, d distantzia $\mathbb{R}^2$-ko ohiko distantzia euklidearra izanik. Orokortasunik galdu gabe, ohartu l zuzena ho-

rizontala dela suposa dezakegula. Izan ere, beti aplikatu ahal izango dugu biraketa egoki bat, zuzena horizontala bihur dadin. Gainera, horren ondoren translazio bat ere aplika dezakegu, parabolaren erpina $(0,0)$ puntua izan dadin. Beraz, ez dugu orokortasunik galtzen $p=(0,a)$ dela suposatzen badugu, $a>0$ izanik. Gainera, $(0,0)\in P$ denez, distantzia berera dago p-tik eta l-tik, eta hortaz l zuzenaren ekuazioa $Y=-a$ da halabeharrez.

Behin hau jakinik parabolaren ekuazioa sinplifikatzen zaigu. Edozein $q=(X,Y)\in P$ hartuta, l gaineko bere proiekzioa $p'=(X,-a)$ izango da,

$$d(q,p')^2=(X-X)^2+(Y+a)^2=(Y+a)^2$$

berdintza beteko duelarik. Gainera, q puntutik p-rako distantziaren karratua

$$d(p,q)^2=(0-X)^2+(a-Y)^2=X^2+(Y-a)^2$$

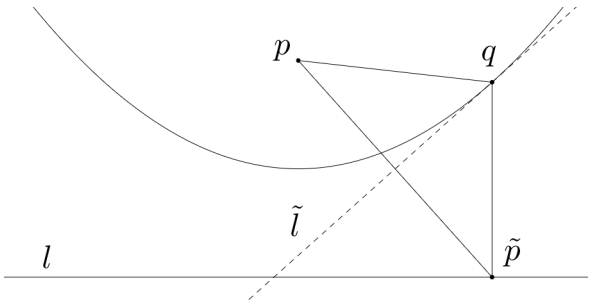
da. Badakigunez bi distantzia hauek berdinak direla, $X^2+(Y-a)^2=(Y+a)^2$ beteko dute $(X,Y)\in P$ puntu guztiek. Berdintza garatzen badugu, parabolaren ekuazioa $X^2=4aY$ dela ondorioztatzen dugu.

Oharra 3.2.1. Baldin eta eraikuntza berdina egiten badugu l zuzentzailea bertikala eta $p=(a,0)$ izanik, $a>0$ balio baterako, orduan parabolaren ekuazioa $Y^2=4aX$ dela froga daiteke modu berean.

Jarraitzeko, ikus dezagun geometria euklidearreko lema bat. Lema hau funtsezkoa da origamiaz ekuazio kubikoak ebaztearen teknika justifikatzeko.

Lema 3.2.2. *Plano euklidearrean, izan bedi l zuzenean ez dagoen p puntu bat. Orduan, beste $\tilde{l}$ zuzen bat emanik, $\tilde{l}$-ren gaineko p puntuaren erreflexioa l zuzenean egongo da baldin eta soilik baldin $\tilde{l}$ zuzena p fokutzat eta l zuzentzailetzat duen parabolaren zuzen ukitzailea bada.*

Froga. Badakigu edozein parabola emanda suposa dezakegula parabolaren ekuazioa $X^2=4aY$ dela, fokua $p=(0,a)$ eta zuzentzailea $l\equiv Y=-a$ izanik $a>0$ baterako. Hau honela izanik, ikusi 3.5. irudia.



3.5. irudia.

Batetik, $\tilde{l}$ zuzenaren bitartez $p = (0, a)$ puntuaren erreflexioa, $\tilde{p}$ deituko dioguna, $l \equiv Y = -a$ zuzenean egongo dela suposatuko dugu. Ondorioz, $\tilde{p} = (X_0, -a)$ beteko da $X_0 \in \mathbb{R}$ baterako. Gainera, 3.5. irudiko q puntuaren koordenatuak $q = (X_0, \frac{X_0^2}{4a})$ izango dira. Izan ere, $\tilde{p} = (X_0, -a)$ puntua dagoen zuzen bertikal berean dagoenez q puntua, X osagaia berdina izango dute, eta horrez gain q parabolan dagoenez parabolaren ekuazioa ere bete beharko duelako, hau da, $X^2 = 4aY$. Jarraitzeko, eraikita dagoen moduagatik, $\tilde{l}$ zuzena p eta bere erreflexioa $\tilde{p}$ lotzen dituen zuzenarekiko perpendikularra izango da. Kalkuluak egiten baditugu, $\tilde{l}$ zuzenaren norabide bektore bat $\overrightarrow{d} = (2a, X_0)$ dela erraz ikus daiteke, eta beraz gai gara $\tilde{l}$ zuzenaren ekuazioa ateratzeko. Hain zuzen ere,

$$\tilde{l} \equiv \begin{cases} X = X_0 + 2at \\ Y = \frac{X_0^2}{4a} + X_0 t \end{cases}$$

izango da $\tilde{l}$ zuzenaren ekuazio parametrikoa. Hemendik erraza da

$$\tilde{l} \equiv Y = \frac{X_0}{2a} X - \frac{X_0^2}{4a}$$

ekuazio esplizitua ateratzea, eta ondorioz $\tilde{l}$ zuzenaren malda $\frac{X_0}{2a}$ dela lortzen dugu. Gainera, parabolaren ekuazioa era esplizituan idazten badugu, hots, $Y = \frac{X^2}{4a}$ erara, deribatua eginez argi ikusten da parabolaren malda $q = (X_0, \frac{X_0^2}{4a})$ puntuan $\frac{X_0}{2a}$ dela. Ondorioz, $\tilde{l}$ zuzena parabolaren ukitzailea izango da q puntuan.

Beste inplikazioa frogatzeko, suposa dezagun $\tilde{l}$ zuzena parabolaren ukitzailea dela q puntu orokor batean. Puntu horren koordenatuak $q = (X_0, \frac{X_0^2}{4a})$ izango dira $X_0 \in \mathbb{R}$ baterako, q puntua parabolan dagoenez bere ekuazioa bete behar duelako. Bestalde, $\tilde{l}$ zuzenaren malda halabeharrez $\frac{X_0}{2a}$ izango da, badakigulako hipotesiz $\tilde{l}$ zuzena parabolaren zuzen ukitzailea dela q puntuan. Beraz, $b \in \mathbb{R}$ baterako $\tilde{l}$ zuzenak

$$Y = \frac{X_0}{2a} X + b$$

ekuazioa beteko du. Alabaina, q puntua $\tilde{l}$ zuzenean ere badagoenez, bereziki zuzenaren ekuazioa bete beharko du, eta beraz

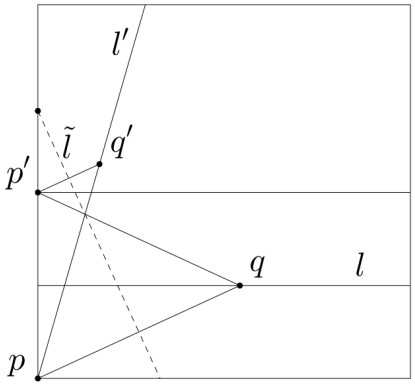
$$\frac{X_0^2}{4a} = \frac{X_0}{2a} X_0 + b$$

berdintza bete beharko da. Hemendik $b = -\frac{X_0^2}{4a}$ ondorioztatzen dugu, eta beraz

$$Y = \frac{X_0}{2a} X - \frac{X_0^2}{4a}$$

izango da $\tilde{l}$ zuzenaren ekuazioa. Oinarrizko geometria euklidearreko eragiketak eginez, $p = (0, a)$ puntuaren erreflexioa $\tilde{l}$ zuzenarekiko $\tilde{p} = (X_0, -a)$ dela lor daiteke. Ondorioz, $\tilde{l}$-ren gaineko p puntuaren erreflexioa l zuzenean dago, nahi genuen bezala. □

Ondorioa 3.2.3. Aurreko lema honek origamiarekin zer lotura duen ikusteko, jar dezagun arreta 3.6. irudian.



3.6. irudia.

Irudi horretako notazioa mantenduz, ohar gaitezen p puntua $q \in l$ puntura eta p' puntua $q' \in l'$ puntura eramaten dela papera $\tilde{l}$ zuzenetik tolesten denean. Ondorioz, $\tilde{l}$ gaineko p-ren erreflexioa l zuzenean dago. Baina 3.2.2 lemagatik, baliokideki $\tilde{l}$ zuzena p fokutzat eta l zuzentzailetzat duen parabolaren zuzen ukitzailea dela esan dezakegu. Arrazoi beragatik, $\tilde{l}$ zuzena p' fokutzat eta l' zuzentzailetzat duen parabolaren zuzen ukitzailea ere izango da. Honenbestez, edozein bi parabola emanik (p eta p' fokudunak eta l eta l' zuzentzailedunak, hurrenez hurren), bi parabolek duten zuzen ukitzaile komun bat lortu dezakegu 3.6. irudian egiten den bezalako tolestura bat eginez. Hain zuzen ere, p puntua l zuzenera eta p' puntua l' zuzenera eramaten dituen tolestura eginez lortzen den $\tilde{l}$ zuzena izango da bila gabiltzan ukitzaile komuna.

3.2 atalaren hasieran aipatu dugun bezala, erregela eta konpasaz gain origamia erabilita ekuazio kubikoak ebazteko gai gara, neurri batean. Izan ere, origamiaz baliatuz gai izango gara koefiziente errealetako edozein ekuazio kubikoren erro **errealak** eraikitzeko. Hori nola egin azaltzen da jarraian, 3.2.3 ondorioa ekuazio kubikoetara aplikatuz.

Adibidea 3.2.4. Badakigu edozein ekuazio kubikotarako aldagai-aldaketa egoki bat existitzen dela, Tschirnhausen transformazioa deitua, aplikatu eta gero bigarren mailako monomioa ez agertzea eragiten duena. Beraz, ez

dugu orokortasunik galtzen koefiziente errealetako edozein ekuazio kubiko hartzerako orduan $X^3 + aX + b = 0$ motakoa dela suposatzen badugu, $a, b \in \mathbb{R}$ izanik. Gainera, ohartu ekuazio kubiko horretako soluzio erreal bat aurkitzea nahikoa dela, beste bi soluzio errealak (existitzen badira) bigarren mailako ekuazio baten erroak izango direlako. Eta 1.3.3 ondorioagatik beti izango gara gai soluzio hauek eraikitzeko, a eta b zenbakietatik abiatuta.

Beraz, aurki dezagun $X^3 + aX + b = 0$ ekuazio kubikoaren erro erreal bat origamia erabiliz, $a, b \in \mathbb{R}$ eta $b \neq 0$ izanik ($b = 0$ kasuan bila gabiltzan erro erreal bat 0 da). Har ditzagun bi parabola plano euklidearrean, hain zuzen ere

$$\left(Y - \frac{1}{2}a\right)^2 = 2bX \text{ eta } Y = \frac{1}{2}X^2$$

ekuazioek definitzen dituztenak. 3.2.3 ondorioa aplikatuz, har dezagun aldi berean bi parabolei ukitzailea den l zuzen bat, lehenengo parabola (X_1, Y_1) puntuan eta bigarrena (X_2, Y_2) puntuan ukitzen dituelarik. Halaber, l zuzenaren maldari m deituko diogu. A eranskineko 9 ariketan erakusten denez, lehenengo parabolaren zuzen ukitzailearen malda (X_1, Y_1) puntuan

$$m = \frac{b}{Y_1 - \frac{1}{2}a}$$

da. Beraz, bereziki $m \neq 0$ eta $Y_1 - \frac{1}{2}a = \frac{b}{m}$ da. Azken emaitza hau eta parabolaren ekuazioa erabilita,

$$X_1 = \frac{\left(Y - \frac{1}{2}a\right)^2}{2b} = \frac{\left(\frac{b}{m}\right)^2}{2b} = \frac{b}{2m^2} \text{ eta } Y_1 = \frac{b}{m} + \frac{a}{2}$$

emaitzak lortzen dira. Era berean, berriro ere A eranskineko 9 ariketak dionez bigarren parabolaren zuzen ukitzailearen malda (X_2, Y_2) puntuan $m = X_2$ da. Ondorioz, parabolaren ekuaziotik berehala ondorioztatzen da $Y_2 = \frac{m^2}{2}$ dela.

Bestalde, badakigu (X_1, Y_1) eta (X_2, Y_2) puntuak l zuzenean daudela. Honenbestez, zuzen bateko bi puntu hauek ezagututa, badakigu zuzenaren m malda, hain zuzen ere,

$$m = \frac{Y_2 - Y_1}{X_2 - X_1}$$

dela. Baina aurretik (X_1, Y_1) eta (X_2, Y_2) koordenatuak m balioaren arabera kalkulatu ditugunez, ordezkapena egiten badugu

$$m = \frac{Y_2 - Y_1}{X_2 - X_1} = \frac{\frac{m^2}{2} - \left(\frac{b}{m} + \frac{a}{2}\right)}{m - \frac{b}{2m^2}} = \frac{m^4 - 2bm - am^2}{2m^3 - b}$$

lortzen dugu. Azkenik, $m \neq 0$ denez, sinplifikazio batzuk egin daitezke eta m maldak

$$m^3 + am + b = 0$$

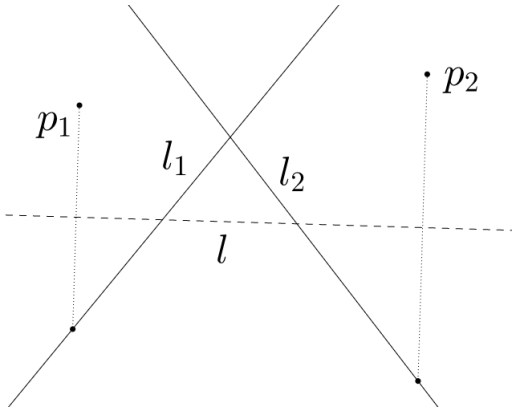
ekuazioa betetzen duela lortzen da. Badakigu A eranskineko 10 ariketagatik m zenbakia l zuzenetik abiatuta eraiki daitekela erregela, konpasa eta origamiarekin, eta beraz adibidearen hasierako ekuazio kubikoaren erro erreal bat eraikitzea lortu dugu erregela, konpasa eta origamia erabiliz.

3.3 Origami zenbakien gorputza

Kapitulu honen zati nagusira iritsi gara. 1 kapituluan, erregela eta konpas bitartez eraiki daitezken zenbaki konplexuen multzoaren propietateak aztertu ditugu. Baina eraikitzeko teknika horiei origamia gehitzen badiegu, zeintzuk izango dira orain eraiki ahal izango ditugun zenbaki konplexuak? Horretarako pausu berri hau sartuko dugu gure eraikuntzetan, zenbaki eraikigarrien kasuko E1 eta E2 pausuez gain:

E3: $p_1 \neq p_2$ puntuetatik eta $l_1 \neq l_2$ zuzenetatik abiatuta, $p_1 \notin l_1$ eta $p_2 \notin l_2$ izanik hurrenez hurren, erreflexio bidez p_1 puntua l_1 zuzenera eta p_2 puntua l_2 zuzenera eramango dituen l zuzena eraiki daiteke.

Adibidea 3.3.1. E3 pausua kasu konkretu batean nola aplikatzen den azaltzen du jarraian datorren irudiak. Bertan l zuzena eraikitzen da, eta zuzen horrek erreflexio bidez p_1 puntua l_1 zuzenera eta p_2 puntua l_2 zuzenera eramaten ditu.



3.7. irudia.

Eraikuntza geometrikoak egiteko modu berri bat definitu dugunez, E3 pausua, hain zuzen ere, pausu berri honekin eraiki daitezkeen zenbakiak definitzea da jarraian egingo duguna.

Definizioa 3.3.2. Izan bedi $\alpha \in \mathbb{C}$ zenbaki konplexua. α zenbakia **origami zenbakia** dela esango dugu E1, E2, E3, P1, P2 eta P3 pausuen segida finitu bat existitzen bada, 0 eta 1 puntuekin hasi eta α puntuan amaitzen dena.

Dei diezaiogun hemendik aurrera $\mathcal{O} = \{\alpha \in \mathbb{C} \mid \alpha \textit{ origami zenbakia}\}$ multzoari. Ohar gaitezen $\mathcal{C} \subseteq \mathcal{O}$ inklusioa betetzen dela era nabarian. Frogatuko ez dugun arren, gure lan honetan funtsezkoa izango da jarraian datorren emaitza (froga bibliografiako [7] liburuko 10. kapituluan aurki daiteke).

Teorema 3.3.3. *Izan bedi $\mathcal{O}$ origami zenbakien multzoa. Orduan $\mathcal{O}$ gorputza da ohiko batuketa eta biderketarekiko. Gainera,*

$$\mathbb{Q} \subseteq \mathcal{O} \subseteq \mathbb{C}$$

gorputz-hedaduren katea dugu.

Badirudi $\mathcal{O}$ eta $\mathcal{C}$ multzoen propietateen artean halako paralelismo bat dagoela. Noraino orokor ditzakegu $\mathcal{C}$ gorputzak dituen berezitasunak $\mathcal{O}$ gorputzera? Mantenduko al dira berezitasun hauek? Hona hemen erantzunaren zati bat.

Teorema 3.3.4. *Izan bedi $\mathcal{O}$, origami zenbakien gorputza, eta $\alpha \in \mathbb{C}$.*

(i) *$\alpha = a + ib$ bada $(a, b \in \mathbb{R})$, orduan $\alpha \in \mathcal{O}$ baldin eta soilik baldin $a, b \in \mathcal{O}$*

(ii) *Baldin eta $\alpha \in \mathcal{O}$ bada, orduan $\sqrt{\alpha}, \sqrt[3]{\alpha} \in \mathcal{O}$*

Froga. (i) $a, b \in \mathcal{O}$ badira, 1.3.2 teoremako (i) atalaren frogan azaltzen den modu berean, $a + ib$-tik abiatuta a eta ib eraiki daitezke erregela eta konpasa erabiliz. Ondorioz, $a, ib \in \mathcal{O}$ izango da. Gainera, 1.3.2 teoremako (i) atalagatik $i \in \mathcal{C}$ dela ere badakigunez, bereziki $i \in \mathcal{O}$ izango da. Hortaz, $ib \in \mathcal{O}$ denez, $b \in \mathcal{O}$ ere izango da (3.3.3 teoremagatik $\mathcal{O}$ gorputza delako). Beste inplikazioa are errezagoa da: $\mathcal{O}$ gorputza denez eta $a, b, i \in \mathcal{O}$, zuzenean $a + ib = \alpha \in \mathcal{O}$ baita.

(ii) Har dezagun $\alpha \in \mathcal{O}$. 1.3.2 teoremako (ii) ataleko frogapenean azaltzen den modura, α zenbakia plano konplexuan eraikita baldin badago badakigu erregela eta konpasaz $\sqrt{\alpha}$ eraikitzen. Beraz, $\sqrt{\alpha} \in \mathcal{O}$ izango da berehala.

Erro kubikoa eraikitzeko, lehenik eta behin idatz dezagun α bere forma polarrean: $\alpha = re^{i\theta}$ izango da, $r = |\alpha|$ eta $\theta = \text{Arg } \alpha$ izanik. Hasteko, gogoratu 3.1 atalagatik badakigula Arg $\alpha = \theta$ angelua hirutan zatitzen origamia erabiliz. Beraz, $e^{i\theta/3} \in \mathcal{O}$ izango da. Jarraitzeko, ohar gaitezen $r \in \mathcal{O}$ dela, jatorrian zentraturiko eta $|\alpha|$ erradiodun zirkunferentziak $\pm r$ puntuetan ebakitzen baitu OX ardatza, eta ondorioz P2 pausuagatik $r \in \mathcal{O}$ baita. $\sqrt[3]{r} \in \mathcal{O}$ frogatuko bagenu, 3.3.3 teoremagatik $\sqrt[3]{r}e^{i\theta/3} = \sqrt[3]{\alpha} \in \mathcal{O}$ izango litzateke. $\sqrt[3]{r}$ eraikitzeko hartu 3.2.4 adibideko bi parabolak, $a = 0$ eta $b = -r$ diren kasu berezian. 3.2

atalak eta 3.2.1 oharrak erakusten dutenez, $X^2 = 4aY$ eta $Y^2 = 4bX$ ekuazioen bitartez definituak dauden bi parabolen fokuak $(0, a)$ eta $(b, 0)$ dira, hurrenez hurren, eta zuzentzaileak berriz $Y = -a$ eta $X = -b$. Gure kasuan, ditugun bi parabolak

$$Y^2 = -2rX \text{ eta } Y = \frac{1}{2}X^2$$

ekuazioek definitzen dituzte. Beraz, fokuak $p_1 = (-\frac{r}{2}, 0)$ eta $p_2 = (0, \frac{1}{2})$ izango dira, hurrenez hurren, eta zuzentzaileak berriz $l_1 \equiv X = \frac{r}{2}$ eta $l_2 \equiv Y = -\frac{1}{2}$ zuzenak. $r \in \mathcal{O}$ denez, aurreko bi puntu eta bi zuzen hauek erregela, konpas eta origamiaren bitartez eraiki daitezke. Orain E3 pausua aplikatzen badiegu bi puntu eta bi zuzen hauei (bistakoa delako $p_1 \notin l_1$ eta $p_2 \notin l_2$ betetzen dela), l zuzen berri bat eraiki daiteke origamia erabiliz, p_1 puntua l_1 zuzenera eta p_2 puntua l_2 zuzenera eramango dituelarik erreflexio bidez. 3.2.4 adibidean erakusten denez, l zuzen honen m maldak $m^3 + am + b = 0$ ekuazioa beteko du, eta beraz gure kasuan $m^3 = r$ izango da. Honenbestez, l zuzenaren malda $\sqrt[3]{r}$ izango da, eta ondorioz A eranskineko 10 ariketak erakusten du $\sqrt[3]{r} \in \mathcal{O}$ dela, frogatu nahi genuena.

□

Zenbaki eraikigarrien gorputzaren kasuan 1.3.5 egitura-teorema dagoen bezala, origami zenbakien gorputzarentzat ere ezagutzen da egitura-teorema bat, funtsezkoa izango dena gorputz hau Galoisen teoriaren ikuspuntutik aztertzeko. Teoremaren froga [1] liburuko 10. kapituluan aurkitu daiteke.

Teorema 3.3.5 (Egitura-teorema)**.** *Izan bedi α zenbaki konplexua. Orduan, $\alpha \in \mathcal{O}$ baldin eta soilik baldin $F_0, F_1, \ldots, F_n$ azpigorputzak existitzen badira halakoak non*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

betetzen den $\alpha \in F_n$ izanik, eta $[F_i : F_{i-1}] = 2$ edo 3 den, edozein $1 \leq i \leq n$ baliotarako.

Erregela eta konpas bitartez soilik eraiki daitezkeen zenbakien kasuan bezala, badago origami zenbakiak karakterizatzen dituen irizpide bat, kalkuluak egiterako orduan aurreko egitura-teorema baino errazagoa izango dena. Hala ere, emaitza hau frogatu ahal izateko lehenik eta behin talde-teoriako oinarrizko nozio bat definitu beharko dugu, eta beharrezkoak izango zaizkigun emaitza batzuk eman.

Definizioa 3.3.6. *Izan bedi G talde finitua. G taldea ebazgarria dela esango dugu*

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = G$$

moduko azpitaldeen kate bat existitzen bada, G_{i+1}/G_i talde abeldarra izanik edozein $0 \leq i \leq r - 1$ baliotarako.

Lema 3.3.7. *Izan bitez $p, q, a, b \in \mathbb{N} \cup \{0\}$ zenbaki arruntak, p eta q zenbaki lehenak eta G talde finitu abeldarra, bere ordena $|G| = p^a q^b$ izanik. Orduan existitzen da*

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

azpitaldeen kate bat halakoa non $|G_{i+1} : G_i| = p$ edo q den, edozein $0 \leq i \leq s-1$ baliotarako.

Froga. G talde tribiala bada emaitza berehalakoa da. G ez bada tribiala, orokortasunik galdu gabe $a \neq 0$ suposatuko dugu, eta ondorioz $p \mid |G|$ dugula. Hortaz, hartu $P \in \mathrm{Syl}_p(G)$, Sylow-en p-azpitalde bat. Badakigu G abeldarra dela, eta beraz $P \trianglelefteq G$ dugu. Zatidura-taldea eginez, G/P talde tribiala edo q-talde bat izango da, $b = 0$ edo $b \neq 0$ bada, hurrenez hurren.

Baldin eta $b = 0$ bada $G = P$ izango da, eta beraz p-talde bat. Ondorioz, existituko da azpitaldeen kate bat,

$$\{1_G\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_t = P$$

motakoa, $|H_{i+1} : H_i| = p$ izanik edozein $0 \leq i \leq t-1$ baliotarako. Honekin, amaitu dugu froga.

Baldin eta $b \neq 0$ bada, orduan G/P zatidura-taldea q-talde bat izango da. Beraz, existituko da P barne duten G-ren azpitaldeen kate bat,

$$P = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_{t'} = G$$

motakoa, halakoa non

$$\{1_{G/P}\} = K_0/P \trianglelefteq K_1/P \trianglelefteq \ldots \trianglelefteq G/P$$

den eta $|K_{i+1}/P : K_i/P| = |K_{i+1} : K_i| = q$, edozein $0 \leq i \leq t'-1$ baliotarako.

Ondorioz, bi kateak elkartuz

$$\{1_G\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_t = P = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_{t'} = G$$

azpitaldeen katea lortu dugu, ondoz-ondoko edozein bi azpitalderen indizea p edo q izanik, frogatu nahi genuena. □

Proposizioa 3.3.8. *Izan bitez $p, q, a, b \in \mathbb{N} \cup \{0\}$ zenbaki arruntak, p eta q zenbaki lehenak eta G talde finitua, bere ordena $|G| = p^a q^b$ izanik. Orduan G ebazgarria da baldin eta soilik baldin*

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

azpitaldeen kate bat existitzen bada halakoa non $|G_{i+1} : G_i| = p$ edo q den, edozein $0 \leq i \leq s-1$ baliotarako.

Froga. Batetik, suposatu G talde ebazgarria dela. Ondorioz, existitzen da $\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = G$ azpitaldeen kate bat halakoa non i guztietarako G_{i+1}/G_i talde abeldarra den. G_{i+1}/G_i talde abeldar hauetako bakoitzari 3.3.7 lema aplikatzen badiogu, zatidura-taldeen korrespondentzia teoremagatik emaitza berehalakoa da. Bestalde, demagun orain

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

azpitaldeen kate bat existitzen dela, i-ren edozein baliorako $|G_{i+1} : G_i| = p$ edo q izanik. Orain i edozein indize hartuta, $|G_{i+1}/G_i| = p$ edo q denez, bereziki zenbaki lehenak direnak, G_{i+1}/G_i zatidura-talde bakoitza ziklikoa da, eta ondorioz abeldarra. Hemendik berehalakoa da G ebazgarria dela ondorioztatzea. □

Jarraian datorren teorema oso ezaguna da, eta orain arte ezagutzen diren frogapen guztiak, berriz, oso konplexuak. Hemen ez dugu frogarik emango, baina talde-adierazpenak erabiliz egindako frogapena [6]-n topa daiteke.

Teorema 3.3.9 (Burnside)**.** *Izan bitez $p, q, a, b \in \mathbb{N} \cup \{0\}$ zenbaki arruntak, p eta q zenbaki lehenak eta G talde finitua, bere ordena $|G| = p^a q^b$ izanik. Orduan G ebazgarria da.*

Teorema hau 3.3.8 proposizioari aplikatuz gero, berehalakoa da ondorengo korolario hau.

Korolarioa 3.3.10. *Izan bitez $p, q, a, b \in \mathbb{N} \cup \{0\}$ zenbaki arruntak, p eta q zenbaki lehenak eta G talde finitua, bere ordena $|G| = p^a q^b$ izanik. Orduan*

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

azpitaldeen kate bat existitzen da halakoa non $|G_{i+1} : G_i| = p$ edo q den, edozein $0 \leq i \leq s-1$ baliotarako.

Azken emaitza honekin, benetan prest gaude origami zenbakiak guztiz karakterizatuko dituen modu praktiko eta erraz bat frogatzeko.

Teorema 3.3.11. *Izan bedi $\alpha \in \mathbb{C}$ zenbaki aljebraikoa $\mathbb{Q}$ gainean eta L gorputza $Irr(\alpha, \mathbb{Q})$ polinomioaren deskonposizio-gorputza $\mathbb{Q}$ gainean. Orduan α origami zenbakia da baldin eta soilik baldin $[L : \mathbb{Q}] = 2^a 3^b$ bada, $a, b \in \mathbb{N} \cup \{0\}$ izanik.*

Froga. Demagun lehenik eta behin $\alpha \in \mathbb{C}$ zenbakia $\mathbb{Q}$ gainean aljebraikoa dela, eta L gorputza $Irr(\alpha, \mathbb{Q})$ polinomioaren deskonposizio-gorputza dela $\mathbb{Q}$ gainean. 1.3.12 teoremaren frogan $\mathcal{C}/\mathbb{Q}$ hedadura normala dela ikusten da, eta pausu berdinak jarraituz erraz ikus daiteke $\mathcal{O}/\mathbb{Q}$ ere hedadura normala dela. Ondorioz, $\alpha \in \mathcal{O}$ denez, definizioz $Irr(\alpha, \mathbb{Q})$ polinomioaren beste erro guztiak ere $\mathcal{O}$ gorputzean egongo dira. Beraz, $L \subseteq \mathcal{O}$ inklusioa beteko da.

Jatorrizko Elementuaren Teoremagatik, existitzen da $\gamma \in L$ (jatorrizko elementua) $L = \mathbb{Q}(\gamma)$ beteko duena. γ elementu honi 3.3.5 teorema aplikatzen badiogu, berehala lortzen da emaitza $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ mailarentzat, eta beraz existitzen dira $a, b \in \mathbb{N} \cup \{0\}$ halakoak non $[L : \mathbb{Q}] = 2^a 3^b$ den.

Beste inplikazioa frogatzeko, demagun $[L : \mathbb{Q}] = 2^a 3^b$ dela. $L/\mathbb{Q}$ hedadura normala denez eta char $\mathbb{Q} = 0$ denez, $L/\mathbb{Q}$ Galoisen hedadura izango da. Galoisen korrespondentzia aplikatuz, badakigu $|\mathrm{Gal}(L/\mathbb{Q})| = 2^a 3^b$ izango dela, eta ondorioz 3.3.10 korolarioagatik existitzen da

$$\{1_{\mathrm{Gal}(L/\mathbb{Q})}\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = \mathrm{Gal}(L/\mathbb{Q})$$

moduko azpitaldeen kate bat, halakoa non $|G_{i+1} : G_i| = 2$ edo 3 den, edozein $0 \leq i \leq s-1$ baliotarako. $\mathrm{Gal}(L/\mathbb{Q})$ taldearen azpitalde horien azpigorputz finkoak hartzen baditugu, berriro ere Galoisen korrespondentzia aplikatuz

$$\mathbb{Q} = \mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = \mathcal{F}(G_s) \subseteq \ldots \subseteq \mathcal{F}(G_0) = \mathcal{F}(\{1_{\mathrm{Gal}(L/\mathbb{Q})}\}) = L$$

gorputz-hedaduren kate bat topatu dugu, $[\mathcal{F}(G_i) : \mathcal{F}(G_{i+1})] = |G_{i+1} : G_i| =$ 2 edo 3 izanik, edozein $0 \leq i \leq s-1$ baliotarako. Orain 3.3.5 teorema aplikatzea besterik ez da geratzen, eta $\alpha \in \mathcal{O}$ dela ondorioztatzen da zuzenean. Beraz, amaitu dugu froga. □

Teorema hau oso praktikoa da zenbaki konplexu bat origami zenbakia den edo ez erabakitzeko.

Adibideak 3.3.12. (i) Demagun $\alpha \in \mathcal{C}$ dela, zenbaki eraikigarri bat. 1.3.12 teoremagatik, L gorputza $Irr(\alpha, \mathbb{Q})$ polinomioaren deskonposizio-gorputza bada $\mathbb{Q}$ gainean, orduan $[L : \mathbb{Q}]$ zenbakia 2-ren berretura bat da. Ondorioz, existituko da $a \in \mathbb{N}$ zenbakia $[L : \mathbb{Q}] = 2^a = 2^a 3^0$ betetzen duena, eta beraz 3.3.11 teoremagatik $\alpha \in \mathcal{O}$ izango da. Honenbestez, $\mathcal{C} \subseteq \mathcal{O}$ inklusioa beste modu batera frogatu dugu.

(ii) Har dezagun ζ_7, unitatearen jatorrizko 7-garren erro bat. 2.2.6 teoremagatik $Irr(\zeta_7, \mathbb{Q}) = \Phi_7(X)$ da, eta 2.2.7 korolarioagatik $\mathbb{Q}$ gaineko bere deskonposizio-gorputza $\mathbb{Q}(\zeta_7)$ da, $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \varphi(7) = 6$ izanik. $6 = 2^1 3^1$ denez, 3.3.11 teoremagatik $\zeta_7 \in \mathcal{O}$ da. Alabaina, 2.3.3 (iii) adibideagatik $\zeta_7 \notin \mathcal{C}$ da. Ondorioz, $\mathcal{C} \subset \mathcal{O}$ inklusioa propioa da, hau da, bi multzoak ez dira berdinak, $\zeta_7 \in \mathcal{O} - \mathcal{C}$ baita.

(iii) Oraingoan ζ_9 hartzen badugu, aurreko adibideko justifikazio beragatik $Irr(\zeta_9, \mathbb{Q})$ polinomioaren deskonposizio-gorputza $\mathbb{Q}$ gainean $\mathbb{Q}(\zeta_9)$ da eta $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$ da. Ondorioz, berriro ere 3.3.11 teoremagatik $\zeta_9 \in \mathcal{O}$ da. Honenbestez, 2.3.3 (iii) adibidean esaten den arren erregela eta konpasaz ezin direla heptagono eta eneagono erregularrak eraiki, hau posible izango da origamiaz ere baliatzen bagara.

Lan honi bukaera borobil bat emateko, 3.3.11 teoremaren korolario oso sinple eta ulerterraz bat emango dugu jarraian.

Korolarioa 3.3.13. *Izan bedi $f(X) \in \mathbb{Q}[X]$ polinomioa, deg $f \leq 4$ izanik. Orduan, $f(X)$ polinomioaren erroak origami zenbakiak dira. Hau da, origamia erabilita $f(X) = 0$ ekuazioa aska dezakegu.*

Froga. Enuntziatuko notazioa mantenduz, hartu $\alpha \in \mathbb{C}$ zenbakia, $f(X)$-ren edozein erro. $Irr(\alpha, \mathbb{Q})$ polinomioak $f(X)$ zatituko duenez, $\deg(Irr(\alpha, \mathbb{Q})) \leq 4$ izango da era nabarian. Baina $Irr(\alpha, \mathbb{Q})$ polinomioari A eranskineko 11 ariketa aplikatzen badiogu, badakigu $[L : \mathbb{Q}] \mid \deg(Irr(\alpha, \mathbb{Q}))!$ izango dela, L gorputza $Irr(\alpha, \mathbb{Q})$ polinomioaren deskonposizio-gorputza izanik $\mathbb{Q}$ gainean. $\deg(Irr(\alpha, \mathbb{Q})) \in \{1, 2, 3, 4\}$ denez, $\deg(Irr(\alpha, \mathbb{Q}))! \in \{1, 2, 6, 24\}$ izango da. Gainera, $6 = 2^1 3^1$ eta $24 = 2^3 3^1$ betetzen denez, kasu guztietan $[L : \mathbb{Q}]$ zenbakiak $2^a 3^b$ motako zenbaki bat zatituko du, eta beraz $[L : \mathbb{Q}]$ ere mota honetakoa izango da. Honenbestez, 3.3.11 teoremak esaten digu $\alpha \in \mathcal{O}$ izango dela. □

A. eranskina

Ariketak

A.1 Zenbaki eraikigarriak

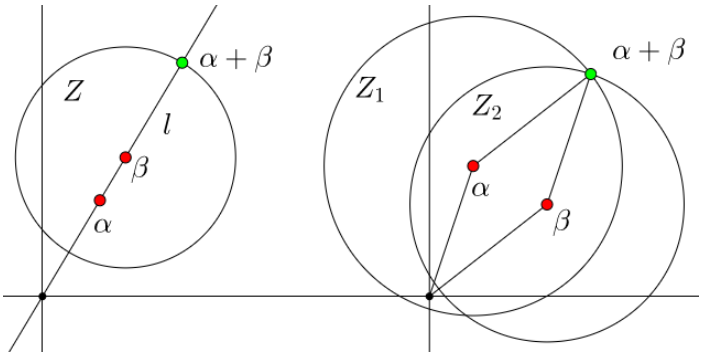
Ariketa 1. Frogatu bi zenbaki eraikigarriren arteko batuketa eraikigarria dela.

Ebazpena. Hartu $\alpha, \beta \in \mathcal{C}$ edozein.

- α, β eta 0 puntua lerrokatuta badaude, orduan α eta β zuzen berean daude (dei diezaiogun l zuzen honi) eta beraz linealki menpekoak dira. Hortaz, existitzen da $\lambda \in \mathbb{R}$ halakoa non $\beta = \lambda\alpha$ den. β-n zentraturiko eta $|\alpha|$ erradioko Z zirkunferentzia definitu dezakegu E2 pausuagatik (ikusi A.1. irudietako ezkerrekoa), eta zirkunferentzia hau hain zuzen ere
$$Z = \{\gamma \in \mathbb{C} \mid |\gamma - \beta| = |\alpha|\}$$
izango da. Eta argi dago ondorioz $\alpha + \beta \in Z$ betetzen dela. Gainera $\alpha+\beta = \alpha+\lambda\alpha = (\lambda+1)\alpha$ denez $\alpha+\beta$ puntua l zuzenean ere egongo da. Eta Z zirkunferentziaren eta l zuzenaren arteko ebakidura eraikigarria izango denez P2 pausuagatik, $\alpha + \beta \in \mathcal{C}$ izango da, nahi genuena.

- α, β eta 0 puntuak ez badaude lerrokatuta, eraiki Z_1 eta Z_2, bi zirkunferentzia, jarraian azaltzen den moduan (ikus A.1. irudietako eskuineko kasua).
$$Z_1 = \{\gamma \in \mathbb{C} \mid |\gamma - \alpha| = |\beta|\},$$
$$Z_2 = \{\gamma \in \mathbb{C} \mid |\gamma - \beta| = |\alpha|\}$$
Argi dago $\alpha+\beta \in Z_1 \cap Z_2$ dela, bi zirkunferentzietan egoteko baldintzak era tribialean betetzen dituelako. Beraz, P3 pausuagatik $\alpha + \beta$ bi zirkunferentziren ebakidura denez eraikigarria izango da, hots, $\alpha+\beta \in \mathcal{C}$, frogatu nahi genuena.

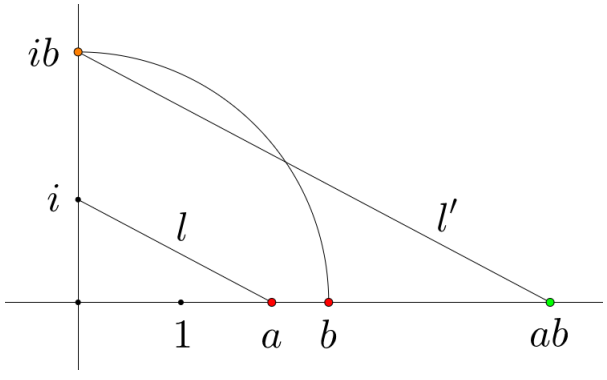
□



A.1. irudia. $\alpha+\beta$ eraikitzea: α, β eta 0 puntuak lerrokatuta dauden kasua ezkerrean, eta lerrokatuta ez dauden kasua eskuinean.

Ariketa 2. Frogatu bi zenbaki erreal eraikigarriren biderkadura ere eraikigarria dela.

Ebazpena. Har ditzagun edozein $a, b \in \mathcal{C} \cap \mathbb{R}$. Definizioz 0 eta 1 eraikigarriak direnez, 0-n zentraturiko eta 1 erradioko zirkunferentzia eraiki daiteke, eta OY ardatza i puntuan ebakitzen duenez P2 pausuagatik $i \in \mathcal{C}$ da, hau da, eraikigarria da. Modu berean, b ere eraikigarria denez jatorrian zentratutako zirkunferentzia bat eraiki daiteke, OY ardatza ib puntuan ebakiko duena. Beraz, $ib \in \mathcal{C}$ ere izango da. i eraikigarria denez, eta hipotesiz a ere bai, a-tik i-rako zuzena eraiki dezakegu E1 pausuagatik, eta dei diezaiogun honi l (ikusi A.2. irudia). Plano konplexua $\mathbb{R}^2$ plano euklidearrarekin identifikatzen badugu, l zuzena $(0,1)$ puntutik ($i \in \mathbb{C}$ puntutik) eta $(a,0)$ puntutik ($a \in \mathbb{C}$ puntutik) igaroko da. Gainera, bere norabide-bektorea $(a,0) - (0,1) = (a,-1)$ izango da. ib eraikigarria denez, 1.1 aurrebaldintzengatik badakigu ib-tik igarotzen den eta l-rekiko paraleloa den l' zuzena eraikitzen.



A.2. irudia.

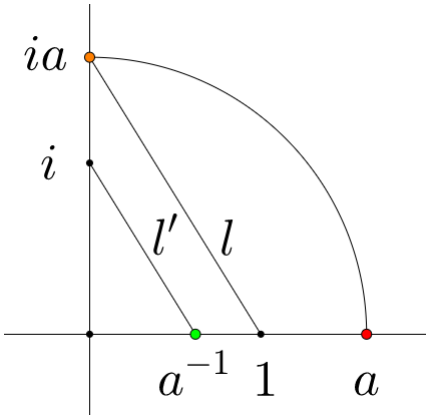
Zuzen honen norabide-bektorea l-ren berdina edo proportzionala) izango da. Beraz, orokortasunik galdu gabe suposa dezakegu l'-ren norabide bektorea $(a, -1)$ izango dela. Bestalde, l' zuzena $(0, b)$ puntutik pasako denez ($ib \in \mathbb{C}$ puntutik), bere ekuazio parametrikoa

$$l' \equiv \begin{cases} X = 0 + at \\ Y = b - t \end{cases}$$

izango da. Kalkuluak eginez, ekuazio inplizitua $l' \equiv X + aY = ab$ izango da, eta l' zuzena eta OX ardatza ebakitzen diren puntua eraikigarria izango da, P1 pausuarengatik. Alabaina, OX ardatzaren ekuazioa $Y = 0$ denez, l'-ren ekuazioan ordezkatuz, aipatutako ebaki-puntua hain zuzen ere $X = ab$ betetzen duen puntua dela ondorioztatzen dugu. Baina hau $(ab, 0)$ puntua da, hain justu, bila genbiltzan biderkadura. Beraz, ab eraikigarria da. □

Ariketa 3. Frogatu zenbaki erreal ez-nulu eta eraikigarri baten alderantzizkoa eraikigarria dela.

Ebazpena. Hartu edozein $a \in \mathcal{C} \cap \mathbb{R} - \{0\}$. Eraikigarria denez, jatorrian zentraturiko eta a erradioko zirkunferentzia eraiki daiteke E2 pausuagatik. OY ardatza ia puntuan ebakitzen duenez, P2 pausuagatik $ia \in \mathcal{C}$ izango da, hau da, eraikigarria. Eta 1 definizioz eraikigarria denez, ia-tik 1-era doan l zuzena eraiki dezakegu E1 pausuagatik (ikusi A.3. irudia). Aurreko ariketan bezala plano konplexua $\mathbb{R}^2$ plano euklidearrarekin identifikatzen badugu, l zuzena $(0, a)$ eta $(1, 0)$ puntuetatik igaroko da eta bere norabide-bektore bat $(-1, a)$ izango da. Ohartu 2 ariketan erakutsi dugula $i \in \mathcal{C}$ dela. Beraz, eraiki dezagun i puntutik igarotzen den eta l-rekiko paraleloa den l' zuzena (badakigu l' zuzena eraikitzen, 1.1 aurrebaldintzengatik).



A.3. irudia.

Aipatutako azken zuzen hau $(0,1)$-tik igaroko denez eta bere norabide-bektore bat $(-1,a)$ izango denez, bere ekuazio parametrikoa

$$l' \equiv \begin{cases} X = 0 - t \\ Y = 1 + at \end{cases}$$

izango da. Hemendik erraza da l'-ren ekuazio inplizitua ateratzea, hain zuzen ere, $l' \equiv aX + Y - 1 = 0$ izango dena. P1 pausuagatik, OX ardatzaren eta l' zuzenaren arteko ebakidura eraikigarria izango da. Baina OX ardatzeko puntuek $Y = 0$ ekuazioa betetzen dutenez, berdintza hau l'-ren ekuazioan ordezkatuz aipatutako ebakidurako puntu honek $aX = 1$ beteko duela ondorioztatzen dugu. a hipotesiz nulua ez denez, puntu honek $X = a^{-1}$ ere beteko du. Beraz, a^{-1} puntua izango da eraiki berri dugun puntua, eta honenbestez $a^{-1} \in \mathcal{C}$ izango da, nahi genuena. □

Ariketa 4. Izan bedi F/K gorputz-hedadura, $[F : K] = 2$ eta char $K \neq 2$ izanik. Frogatu K-ren edozein hedadura koadratiko, bakuna dela eta erro karratu bat gehituz lortzen dela.

Ebazpena. $[F : K] \neq 1$ denez, $K \subsetneq F$ da eta ondorioz hartu edozein $\alpha \in F - K$, badakigulako $F - K \neq \varnothing$ dela. Ohar gaitezen

$$K \subseteq K(\alpha) \subseteq F$$

betetzen dela, eta $\alpha \notin K$ denez $K \neq K(\alpha)$ dela. Ondorioz, mailaren teoremagatik aukera bakarra $K(\alpha) = F$ izatea da, $[K(\alpha) : K]$ mailak $[F : K] = 2$ zatitu behar baitu. Honenbestez, K-ren mota honetako edozein hedadura bakuna izango da.

Jarraitzeko, badakigunez $[K(\alpha) : K] = 2$ dela, $Irr(\alpha, K)$ polinomioa bigarren mailakoa izango da. Beraz existituko dira $a, b \in K$ elementuak, $Irr(\alpha, K) = X^2 + aX + b$ izanik. Bestalde, char $K \neq 2$ denez, bigarren mailako ekuazioetarako formula koadratikoa aplika dezakegu polinomio honen erroak kalkulatzeko. Bereziki α erro bat denez, honelako adierazpen bat onartuko du:

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Hortaz, $K(\alpha) = K(\sqrt{a^2 - 4b})$ izango da, hau da, F gorputzean existitzen da $\beta = \sqrt{a^2 - 4b}$ elementua $F = K(\beta)$ izanik, frogatu nahi genuena. □

A.2 Poligono erregularren eraikuntza

Ariketa 5. Izan bedi K gorputza eta $f(X) \in K[X]$ polinomio ez-konstante eta monikoa. Frogatu f banangarria dela K gainean baldin eta soilik baldin f eta bere deribatu formala, f', elkarrekiko lehenak badira.

Ebazpena. Hartu f-ren deskonposizio-gorputza K gainean eta deitu honi F. f-ren maila n bada existitzen dira $\alpha_1, \ldots, \alpha_n \in F$ halakoak, $F[X]$ eraztunean $f(X) = (X - \alpha_1) \ldots (X - \alpha_n)$ betetzen delarik. Gainera, edozein $i \in \{1, \ldots, n\}$ hartzen badugu, defini dezagun $h_i(X) \in F[X]$ polinomioa

$$h_i(X) = \prod_{j \neq i} (X - \alpha_j)$$

biderkadura bezala. Beraz, $f(X) = (X - \alpha_i)h_i(X)$ izango da. Aurreko adierazpena deribatuz, $f'(X) = (X - \alpha_i)h_i'(X) + h_i(X)$ lortzen dugu, eta deribatu hau α_i puntuan ebaluatzen badugu,

$$f'(\alpha_i) = h_i(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$$

izango da. Absurdura eramanez f banangarria balitz baina f eta f' ez balira elkarrekiko lehenak, g faktore komun ez-konstante bat izango lukete biek, eta beraz gutxienez erro komun bat. Bereziki erro hau f-ren erroetako bat izango denez, existituko litzateke α_{i_0} zenbakia $i_0 \in \{1, \ldots, n\}$ balioren baterako, f-ren eta f'-ren erro komuna izanik. Kasu honetan,

$$0 = f'(\alpha_{i_0}) = h_{i_0}(\alpha_{i_0}) = \prod_{j \neq i_0} (\alpha_{i_0} - \alpha_j)$$

izango da, eta ondorioz $\alpha_{i_0} = \alpha_j$ beteko da, $j \neq i_0$ baterako. Hau absurdua denez, f eta f' elkarrekiko lehenak izan beharko dira.

Beste inplikazioa frogatuko dugu jarraian. Hipotesiz zkh(f,f')=1 denez, Bézouten teoremagatik existitzen dira $A(X), B(X) \in K[X]$ polinomioak non $A(X)f(X) + B(X)f'(X) = 1$ betetzen den. f-ren edozein erro α_i hartuta,

$$A(\alpha_i)f(\alpha_i) + B(\alpha_i)f'(\alpha_i) = B(\alpha_i)f'(\alpha_i) = 1$$

beteko da, eta ondorioz $f'(\alpha_i) \neq 0$. Orduan

$$\prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$$

izango da edozein $i = 1, \ldots, n$ izanik, eta honenbestez $\alpha_1, \ldots, \alpha_n$ guztiak desberdinak izango dira, f polinomioa K gainean banangarria dela baieztatuz. □

Ariketa 6. Izan bedi $n \in \mathbb{N}$ edozein zenbaki arrunt. Frogatu n aldeko poligono erregularra eraikigarria dela baldin eta soilik baldin $\zeta_n \in \mathcal{C}$ bada.

Ebazpena. Hartu $n \in \mathbb{N}$ edozein. n aldeko poligono erregularra eraikigarria bada, bereziki poligonoaren ondoz-ondoko bi erpin eraikigarriak dira. Bestalde, poligonoaren zentrutik bi erpin hauetara doazten bi zuzenkiek

$\frac{2\pi}{n}$ radianeko angelua osatzen dutenez, $\frac{2\pi}{n}$ angelua eraikigarria izango da. Beraz, horizontalarekin $\frac{2\pi}{n}$ angelua osatzen duen l zuzena eraiki dezakegu, eta baita jatorrian zentraturiko eta 1 erradioko $\mathbb{S}^1$ zirkunferentzia ere, E2 pausuagatik. Jarraitzeko, P2 pausuagatik bi eraikuntza hauen arteko ebakidura eraikigarria izango da. Baina $\zeta_n = e^{\frac{2\pi i}{n}} \in l \cap \mathbb{S}^1$ da (Arg $\zeta_n = \frac{2\pi}{n}$ eta $|\zeta_n| = 1$ betetzen delako, hurrenez hurren), eta beraz $\zeta_n \in \mathcal{C}$.

Beste inplikazioa frogatuko dugu jarraian. ζ_n eraikigarria bada, orduan bereziki 1.2.2 (ii) proposizioagatik bere berreturak ere eraikigarriak izango dira. Beraz, ζ_n^i eraikigarria izango da, edozein $1 \leq i < n$ izanik. Plano konplexuan puntu guzti hauek eraiki ondoren (eraikigarriak direlako hau posible da), ondoz-ondoko edozein bi puntu zuzenki batekin lotuko ditugu, erregela erabiliz. Horrela, n aldeko poligono erregularra eraikia izango dugu, hain zuzen ere, erpintzat ζ_n^i zenbakiak dituena, $1 \leq i < n$ guztietarako. □

Ariketa 7. Frogatu $2^n + 1$ zenbaki lehena bada, $n \in \mathbb{N}$ izanik, orduan n zenbakia 2-ren berretura bat dela.

Ebazpena. Ohartu orokorrean $k \in \mathbb{N}$ badugu, orduan

$$X^{2k+1} + 1 = (X + 1)(X^{2k} - X^{2k-1} + X^{2k-2} + \cdots - X + 1)$$

dugula. Absurdura eramanez, suposatzen badugu n zenbakia ez dela 2-ren berretura bat, orduan $n = (2k + 1)m$ motakoa izango da, $k \geq 1$ izanik eta $m < n$, biak zenbaki arruntak. Ondorioz, ikusi dugunez orokorrean $X + 1 | X^{2k+1} + 1$ dela, $X = 2^m$ kasura aplikatuz,

$$2^m + 1 | (2^m)^{2k+1} + 1 = 2^n + 1$$

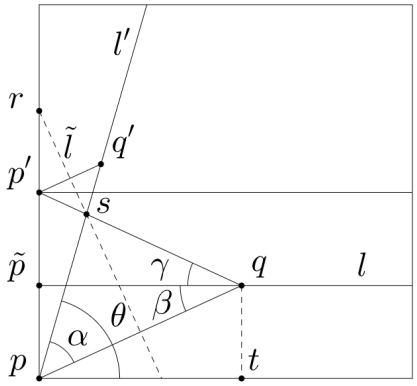
izango da. $m < n$ denez, $2^n + 1$ zenbakia lehena ez dela ondorioztatzen dugu, hipotesiaren kontra doana. Honekin amaitzen dugu froga. □

A.3 Origami zenbakiak

Ariketa 8. 3 kapituluko 3.1 ataleko notazioa mantenduz, frogatu θ angelutik abiatuta egiten den eraikuntzan lortzen den angelua benetan $\theta/3$ dela.

Ebazpena. Hasteko, definizio pare bat emango ditugu, idazkera arintzearren.

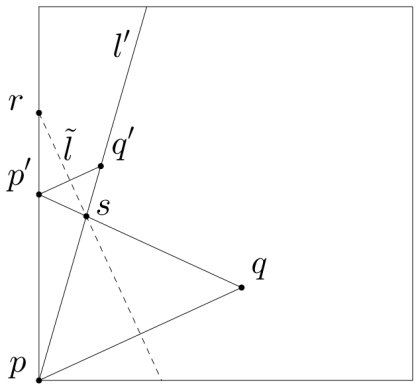
- θ_1 eta θ_2 angeluak kongruenteak direla esango dugu radianetan neurtuta berdina badira, eta $\theta_1 \sim \theta_2$ idatziko dugu.
- Planoko edozein a, b, c puntu izanda $\triangle(abc)$ deituko diogu a, b eta c puntuek definitzen duten triangeluari.
- Planoko edozein bi puntu emanda, a eta b, biak lotzen dituen zuzenkiari $\overrightarrow{ab}$ deituko diogu, eta a-tik b-ra dagoen distantziari berriz $|\overrightarrow{ab}|$.



A.4. irudia.

Froga azaltzeko 3.1 atalean erabili den irudi bat hartu eta puntu lagungarri batzuk gehitu dizkiogu (ikusi A.4. irudia). Irudi horretan oinarrituz, $\overrightarrow{pq}$ zuzenak horizontalarekin osatzen duen angelua $\theta - \alpha$ da. Angelu hau hain zuzen ere $\frac{\theta}{3}$ dela frogatzea izango da gure helburua. Has gaitezen froga puntuz-puntu lantzen.

(i) Lehenik eta behin, $\overrightarrow{pq'}$eta $\overrightarrow{p'q}$ zuzenkiak hartu (ikusi A.5. irudia).

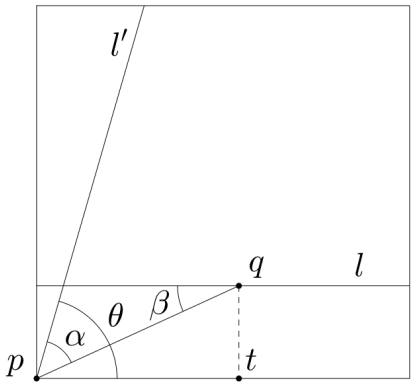


A.5. irudia.

Bien ebakidura, hots, A.4. irudiko s puntua, $\tilde{l}$ zuzenean dagoela frogatuko dugu. $\tilde{l}$ eraiki dugun moduagatik, p'-tik eta q'-tik distantzia berera dauden puntuen leku geometrikoa da. Beraz, nahikoa da $|\overrightarrow{sp'}| = |\overrightarrow{sq'}|$ dela frogatzea. $\tilde{l}$ zuzena $\overrightarrow{p'q'}$-ren erdiko puntutik igarotzen denez, $\triangle(p'q's)$ triangelua bi triangelu zuzenetan banatuko du. Bi triangelu hauek kateto bat dute komunean, eta beste katetoa, biek luzera

berekoa dute. Izan ere, bi kateto hauek p'-tik eta q'-tik erdiko puntura dagoen distantziak dira, definizioz berdinak izango direnak. Ondorioz, Pitagorasen teoremagatik bi hipotenusak guztiz zehaztuta daude eta berdinak dira, hau da, p'-tik s-ra eta q'-tik s-ra distantzia bera dago.

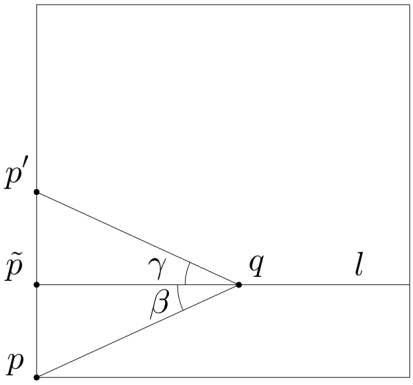
(ii) Jarraitzeko, $\theta \sim \alpha + \beta$ dela frogatuko dugu (ikusi A.6. irudia).



A.6. irudia.

$\triangle(pqt)$ triangelu zuzena hartzen badugu, ohar gaitezen q erpinari dagokion angelua $\frac{\pi}{2}-\beta$ dela. Triangelu honen hiru angeluak $\frac{\pi}{2}-\beta, \theta-\alpha$ eta $\frac{\pi}{2}$ izango dira. Beraz, $(\frac{\pi}{2}-\beta)+(\theta-\alpha)+\frac{\pi}{2} \sim \pi$ izango da, edozein triangeluren hiru angeluen arteko batura π radianekoa delako. Hemendik berehalakoa da $\theta \sim \alpha + \beta$ dela.

(iii) Ondoren, $\gamma \sim \beta$ dela frogatuko dugu (A.7. irudiko egoeran).

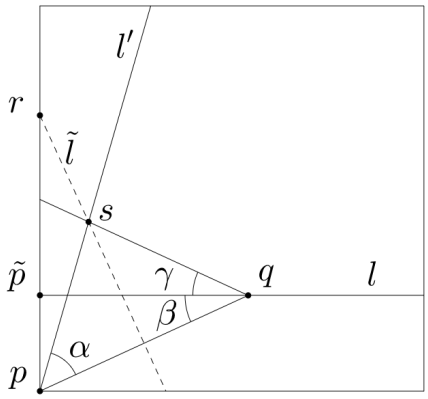


A.7. irudia.

Horretarako, lehenik eta behin $\triangle(pp'q)$ triangelua hartuko dugu. $\tilde{p}$

eraiki dugun moduagatik, $|\overrightarrow{p\tilde{p}}| = |\overrightarrow{\tilde{p}p'}|$ izango da. Eta horregatik, $\triangle(\tilde{p}p'q)$ eta $\triangle(p\tilde{p}q)$ triangelu zuzenak hartuta luzera bereko hipotenusak izango dituzte. Izan ere, kateto bat komunean dute, eta beste katetoak luzera berekoak direla ikusi dugu oraintxe. Beraz, Pitagorasen teoremagatik hipotenusak guztiz zehaztuta daude eta berdinak dira. Eta hortaz, triangelu hauek alde guztiak berdinak dituztenez, angeluak ere hala izango dituzte, hiru aldeen luzerek angeluak guztiz zehazten baitituzte. Bereziki, $\gamma \sim \beta$ izango da.

(iv) Hurrengo pausua $\alpha \sim \gamma + \beta$ frogatzea izango da (ikusi A.8. irudia).



A.8. irudia.

Badakigu s-tik p-ra eta q-ra distantzia bera egongo dela, $s \in \tilde{l}$ baita (i) puntuagatik. Bestalde, $\tilde{l}$ eraiki dugun moduagatik p eta q-ren erdiko puntutik igarotzen da. Beraz, aurreko puntuan bezala bi triangelu zuzen definiturik izango ditugu, kateto bat komunean dutena. Gainera, bi triangelu hauen beste katetoak luzera berekoak izango dira. Ondorioz, Pitagorasen teoremagatik hipotenusak ere berdinak izango direnez alde guztiak berdinak izango dituzte, eta beraz angeluak ere bai. Hemendik zuzenean $\alpha \sim \gamma + \beta$ ondorioztatzen da.

(v) Bukatzeko, froga dezagun $\theta - \alpha \sim \frac{\theta}{3}$ dela. Batetik (iv) puntuagatik $\alpha \sim \gamma + \beta$ da, eta bestetik (iii) puntuagatik $\gamma \sim \beta$ da. Beraz, $\alpha \sim 2\beta$ denez, $\beta \sim \frac{\alpha}{2}$ izango da. Baina orduan (ii) puntuagatik $\theta \sim \alpha + \beta \sim \alpha + \frac{\alpha}{2} \sim \frac{3\alpha}{2}$ beteko da, hau da, $\alpha \sim \frac{2\theta}{3}$ izango da. Beraz, $\theta - \alpha \sim \theta - \frac{2\theta}{3} = \frac{\theta}{3}$ ondorioztatzen dugu, frogatu nahi genuena.

□

Ariketa 9. Kalkulatu $\left(Y - \frac{1}{2}a\right)^2 = 2bX$ ekuazioak definitzen duen parabolaren zuzen ukitzailearen malda (X_1, Y_1) puntuan, eta egin gauza bera $Y = \frac{1}{2}X^2$ ekuazioak definitzen duen parabolarekin, (X_2, Y_2) puntuan.

Ebazpena. Lehenengo parabolaren kasuan, ohar gaitezen ekuazioa

$$X = \frac{\left(Y - \frac{1}{2}a\right)^2}{2b}$$

modura idazten badugu, hau koordenatu esplizituetan emanda dagoela. Ondorioz, malda lortzeko, ekuazioa Y aldagaiarekiko deribatu besterik ez dugu egin behar, eta ondoren Y_1 puntuan ebaluatu. Hemendik berehalakoa da malda

$$\frac{Y_1 - \frac{1}{2}a}{b}$$

dela. Baina malda hau OY ardatza abzisa bezala hartuta lortu dugunez, koordenatu-sistema irauli beharko dugu ohiko sistemara itzultzeko. Ondorioz, benetan zuzen ukitzailearen malda aurreko maldaren iraulia izango da, hots,

$$m = \frac{b}{Y_1 - \frac{1}{2}a}$$

Bigarren parabolaren kasuan, hau koordenatu esplizitutan emanda dago, OX ardatza abzisa bezala hartuta. Beraz, zuzenean ekuazioa deribatu eta X_2 puntuan ebaluatuz, m' malda $m' = X_2$ dela lortzen dugu. □

Ariketa 10. Izan bedi $m \in \mathbb{R}$. Frogatu m maldadun l zuzena erregela, konpas eta origamiaren bitartez eraiki baldin badaiteke, orduan m malda erregela, konpas eta origamiaren bitartez eraiki daitekeen zenbakia dela.

Ebazpena. Badakigu l zuzenaren ekuazioak idazkera esplizitua onartzen duela. Beraz, l zuzenaren malda m denez, existituko da $a \in \mathbb{R}$ zenbakia $l \equiv Y = mX + a$ izanik. $X = 0$ eta $X = 1$ ekuazioek definitzen dituzten bi zuzen bertikalak hartzen baditugu, bi zuzen hauek l zuzena $(0, a)$ eta $(1, m + a)$ puntuetan ebakiko dute, hurrenez hurren. Beraz, $(0, a)$ eta $(1, m + a)$ puntuak erregela, konpas eta origamiaren bitartez eraikigarriak izango dira. Jarraitzeko, 1.3.2 teoremako (i) atalaren frogan egiten den eraikuntza berdina eginez, a eta $m + a$ zenbaki errealak erregela, konpas eta origamiaren bitartez eraiki daitezkela ondorioztatzen dugu. Bukatzeko, a-tik abiatuta $-a$ eraikitzea berehalakoa denez, eranskin honetako 1 ariketaren ebazpeneko eraikuntza egingo dugu, eta $m + a + (-a) = m$ batura eraikitzea lortuko dugu. Ondorioz, m zenbakia erregela, konpas eta origamiaren bitartez eraiki daitekeen zenbaki bat izango da. □

Ariketa 11. Izan bedi K gorputza eta $f(X) \in K[X]$ polinomio moniko irreduziblea, bere maila n izanik. $f(X)$ polinomioaren deskonposizio-gorputza K gainean L bada, frogatu $[L : K] \mid n!$ betetzen dela.

Ebazpena. Indukzioa erabiliko dugu, n-ren gainean. Baldin eta $n = 1$ bada, argi dago f-ren deskonposizio-gorputza K gainean hain zuzen ere K dela,

eta ondorioz $[K : K] \mid 1!$ dela era nabarian. Jarraitzeko, suposa dezagun n baino maila txikiagoa duten polinomioetarako emaitza bete egiten dela. Hartu $\alpha \in L$, f-ren edozein erro. Badakigu $K(\alpha)$ gorputzean

$$f(X) = (X - \alpha)g(X)$$

deskonposizioa beteko dela, $g(X) \in K(\alpha)[X]$ izanik. Badakigunez deg $g = n-1$ dela, hipotesi induktiboagatik $[L : K(\alpha)] \mid (n-1)!$ izango da, L delako g-ren $K(\alpha)$ gaineko deskonposizio-gorputza. Gainera, f irreduziblea denez K gainean, $Irr(\alpha, K) = f(X)$ izango da eta ondorioz $[K(\alpha) : K] = n$ izango da. Hau honela, mailaren teoremagatik

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \mid (n-1)!n = n!$$

betetzen dela berehalakoa da. □

Oharra A.3.1. 11 ariketako emaitza oraindik egia da $f(X) \in K[X]$ polinomioa ez bada irreduziblea. Hala ere, emaitza hau ez dugu hemen frogatu, lan honetako ariketen helburua teoriaren garapena laguntzea baita, eta teorian irizpide hau kasu irreduziblean bakarrik erabili dugu.

Bibliografia

[1] D. A. Cox, *Galois Theory*, Wiley Interscience, 2004.

[2] J. P. Escofier, *Galois Theory*, Springer, 2001.

[3] C. R. Hadlock, *Field Theory and its classical problems*, The Mathematical Association of America, 1978.

[4] L. Gaal, *Classical Galois Theory with Examples*, AMS Chelsea Publishing, 1979.

[5] G. Navarro, *Un curso de números*, Universitat de València, 2007.

[6] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, 1994.

[7] G. E. Martin, *Geometric Constructions*, Springer-Verlag, 1998.

[8] W. W. Rouse Ball, *A Short Account of the History of Mathematics*, Dover Publications, 1960.