2

Idealak eta homomorfismoak

2.1. Idealak eta zatidura eraztunak

Geldi gaitezen une batez pentsatzeko nola eraikitzen diren $\mathbb{Z}/n\mathbb{Z}$ eraztunak (infinitu eraztun desberdin) $\mathbb{Z}$ eraztun bakarretik. Horretarako, behin $n \in \mathbb{N}$ finkaturik, n moduluarekiko kongruentzia hartzen dugu, zeina $\mathbb{Z}$-ren gainean baliokidetasun-erlazioa baita. Erlazio horrekiko $a \in \mathbb{Z}$ elementu baten baliokidetasun-klasea $\overline{a}$ bada, orduan baliokidetasun-klase desberdinen multzoa $\mathbb{Z}/n\mathbb{Z}$ ikurraren bidez adierazten dugu eta klaseen arteko eragiketak ordezkariak erabiliz definitzen dira. Atal honetan ikusiko dugunez, ideia hori eraztun guztietara eraman daiteke, idealaren kontzeptua erabiliz.

2.1. Definizioa. Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren azpimultzoa. Orduan, $\mathfrak{a}$ A-ren *ideala* dela esaten dugu, baldintza hauek betetzen badira:

(i) $\mathfrak{a}$ A-ren azpitaldea da batuketarekiko.
(ii) $x \in \mathfrak{a}$ eta $a \in A$ bada, orduan $ax \in \mathfrak{a}$.

Demagun $\mathfrak{a}$ A-ren ideala dela. Orduan, $(A, +)$ talde abeldarra denez, $\mathfrak{a}$ A-ren azpitalde normala da batuketarekiko. Beraz, $A/\mathfrak{a}$ zatidura talde batukorra eraiki dezakegu. Haren elementuak

$$a + \mathfrak{a} = \{a + x \mid x \in \mathfrak{a}\}$$

koklaseak dira, eta testuinguruagatik garbi badago $\mathfrak{a}$ zein den, $a + \mathfrak{a}$ -ren ordez $\overline{a}$ idatziko dugu koklasea sinpleago adierazteko. Koklaseen arteko berdintza

$$\overline{a} = \overline{b} \qquad \Longleftrightarrow \qquad \exists x \in \mathfrak{a} : a = b + x \qquad \Longleftrightarrow \qquad a - b \in \mathfrak{a}$$

baliokidetasunen bidez kontrolatzen da; bereziki,

$$\overline{a} = \overline{0} \qquad \Longleftrightarrow \qquad a \in \mathfrak{a}$$

dugu. Bestalde, batuketa

$$\overline{a} + \overline{b} = \overline{a + b}$$

erregelaren bitartez definitzen da $A/\mathfrak{a}$ zatiduran.

Orain, $A/\mathfrak{a}$-ri eraztun-egitura eman nahi genioke. Horretarako, koklaseen arteko biderketa definitu beharko genuke. Modurik naturalena

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

jartzea da, baina arazo bat sortzen zaigu: ba al dago ondo definiturik biderketa hori? Jarraian ikusten dugunez, hori da idealaren definizioko bigarren baldintzaren zergatia.

2.2. Teorema. *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan, $\overline{a} \cdot \overline{b} = \overline{ab}$ biderketa ondo definiturik dago $A/\mathfrak{a}$ zatidura taldean, eta $(A/\mathfrak{a}, +, \cdot)$ eraztuna da.*

Froga. Ikus dezagun $\overline{a} \cdot \overline{b} = \overline{ab}$ biderketa ondo definiturik dagoela. Horretarako, demagun $\overline{a'} = \overline{a}$ eta $\overline{b'} = \overline{b}$ dela, eta ikus dezagun $\overline{a'b'} = \overline{ab}$ dela. Izan ere, existitzen dira $x, y \in \mathfrak{a}$ non $a' = a + x$ eta $b' = b + y$ baita eta, orduan,

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy,$$

eta $ay + xb + xy \in \mathfrak{a}$ dugu, idealaren definizioko bigarren baldintzagatik. Hortaz, $\overline{a'b'} = \overline{ab}$ dugu, nahi bezala.

Orain, erraz ikusten da $(A/\mathfrak{a}, +, \cdot)$ eraztuna izateko baldintza guztiak betetzen direla, dagoeneko A-n betetzen direlako. Ikus dezagun, adibidez, $\overline{1}$ $A/\mathfrak{a}$-ren identitatea dela: $\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}$ dugu $\overline{x} \in A/\mathfrak{a}$ guztietarako. Gainerako propietateak antzera egiaztatzen dira. □

2.3. Definizioa. Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan, $A/\mathfrak{a}$ eraztuna *zatidura eraztun* bat dela esaten dugu.

Batzuetan, $A/\mathfrak{a}$ zatidura eraztunean $\overline{a} = \overline{b}$ betetzen dela adierazteko, $a \equiv b \pmod{\mathfrak{a}}$ idatziko dugu. Beraz,

$$a \equiv b \pmod{\mathfrak{a}} \iff \exists x \in \mathfrak{a} : a = b + x \iff a - b \in \mathfrak{a}.$$

Orduan, $A/\mathfrak{a}$ eraztunaren batuketa eta biderketa ondo definituta egoteagatik, era horretako kongruentziak batu eta biderka daitezke (zenbaki osoen arteko kongruentziekin egiten dugun modura):

$$a \equiv b \pmod{\mathfrak{a}}, \quad c \equiv d \pmod{\mathfrak{a}} \implies a+b \equiv c+d \pmod{\mathfrak{a}}, \quad ab \equiv cd \pmod{\mathfrak{a}}.$$

Eman dezagun azpimultzo bat ideala den edo ez erabakitzeko modu azkarrago bat.

2.4. Proposizioa. *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren azpimultzo ez-hutsa. Orduan, $\mathfrak{a}$ A-ren ideala da baldin eta soilik baldin bi baldintza hauek betetzen badira:*

(i) *$x, y \in \mathfrak{a}$ bada, orduan $x + y \in \mathfrak{a}$.*
(ii) *$x \in \mathfrak{a}$ eta $a \in A$ bada, orduan $ax \in \mathfrak{a}$.*

Froga. Talde-teorian ikusten denez, baliokideak dira $\mathfrak{a}$ $(A, +)$-en azpitaldea izateko baldintza eta $x - y \in \mathfrak{a}$ izatea $x, y \in \mathfrak{a}$ guztietarako. Beraz, $\mathfrak{a}$ A-ren ideala da baldin eta soilik baldin baldintza hauek betetzen badira:

(i′) $x, y \in \mathfrak{a}$ bada, orduan $x - y \in \mathfrak{a}$.
(ii′) $x \in \mathfrak{a}$ eta $a \in A$ bada, orduan $ax \in \mathfrak{a}$.

Orain, $x - y = x + (-1)y$ denez, garbi dago (i) eta (ii) baldintzak eta (i′) eta (ii′) baliokideak direla, eta proposizioa frogaturik gelditzen da. □

2.5. Adibideak. 1) A edozein eraztunetan, $\{0\}$ eta A idealak dira. Ohartu $A/\{0\} = \{\overline{a} \mid a \in A\}$ dela, $\overline{a}$ guztiak desberdinak izanik, eta beraz A-rekin bijekzioan dago. Beranduago argituko dugu bijekzio horren esanahia, isomorfismoei buruz hitz egiten dugunean. Bestalde, $A/A = \{\overline{0}\}$ eraztun tribiala da.

2) $\mathbb{Z}$-ren azpitaldeak $n\mathbb{Z}$ modukoak dira, $n \in \mathbb{N} \cup \{0\}$ izanik. Horiek guztiak idealak dira; beraz, horiek dira $\mathbb{Z}$-ren ideal guztiak. Dagozkien zatidurak $\mathbb{Z}/n\mathbb{Z}$ moduko eraztunak dira, hau da, ohiko kongruentzien bitartez eraikitzen diren berberak.

3) Izan bedi

$$\mathfrak{a} = \{f \in \mathbb{R}[X] \mid f \ X^2 + 1\text{-en multiploa}\}.$$

Erraz egiaztatzen da $\mathfrak{a}$ $\mathbb{R}[X]$-ren ideala dela. Orduan, $\mathbb{R}[X]/\mathfrak{a}$ zatiduran,

$$\overline{X+1}^2 = \overline{X^2 + 2X + 1} = \overline{2X}$$

dugu, $X^2 + 1 \in \mathfrak{a}$ baita, eta

$$\overline{X}^2 = \overline{X^2} = \overline{-1},$$

nahiz eta $\mathbb{R}[X]$-n ez egon karratura jasorik -1 ematen duen elementurik.

4) Aurreko adibidea orokortu daiteke, eta edozein eraztunetan, elementu finko baten multiploek ideal bat osatzen dute.

5) $\mathbb{R}[X]$-ren barruan, $\mathbb{R}$ (polinomio konstanteen multzoa) azpitaldea da batuketarekiko, baina argi eta garbi ez da ideala.

6) A edozein eraztun bada, $A[X_1, \ldots, X_n]$ polinomioen eraztunean gai askerik gabeko polinomioek ideal bat osatzen dute.

Talde-teorian, zatidura taldeak eraiki ahal izateko azpitalde normalak behar ditugu, eta horiek azpitalde berezi batzuk dira. Eraztun-teorian, berriz, zatidura eraztunak eraikitzeko idealak behar ditugu, baina horiek ez dira azpieraztun berezi batzuk, oro har ez baitira azpieraztunak. Izan ere, $\mathfrak{a}$ ideala azpieraztuna bada, orduan $1 \in \mathfrak{a}$ izan behar duenez, $a \cdot 1 = a \in \mathfrak{a}$ dugu $a \in A$ guztietarako. Beraz, A eraztun osoa da aldi berean ideala eta azpieraztuna den azpimultzo bakarra.

Azken argudioan ikusi dugunez, ideal batean 1 identitatea badago, orduan ideal hori eraztun osoa da. Berehala frogatzen da bertsio osatuago hau.

2.6. Proposizioa. *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan, baliokideak dira:*

(i) $\mathfrak{a} = A$.
(ii) $1 \in \mathfrak{a}$.
(iii) $\mathfrak{a}$-*n unitateren bat dago.*

Eraztun baten idealak azpimultzoak direnez, eragiketa natural batzuk ditugu idealei aplikatzeko. Jarraian ikusten dugun bezala, batzuetan idealak lortzen ditugu berriro eta, horrela ez denean, konponbide erraza dugu ideal bat lortzeko.

2.7. Teorema. *Izan bitez A eraztuna eta $\mathfrak{a}$, $\mathfrak{b}$ A-ren bi ideal. Orduan:*

(i) $\mathfrak{a} \cap \mathfrak{b}$ *ere A-ren ideala da. (Orokorkiago, ideal kopuru* orokor *baten ebakidura ideala da berriro.)*

(ii) $\mathfrak{a} \cup \mathfrak{b}$ *ideala da baldin eta soilik baldin $\mathfrak{a} \subseteq \mathfrak{b}$ edo $\mathfrak{b} \subseteq \mathfrak{a}$ bada. (Kasu horietan $\mathfrak{a} \cup \mathfrak{b}$ bi idealetatik handiena baino ez da.)*

(iii) $\mathfrak{a}$ *eta* $\mathfrak{b}$ *(hau da, $\mathfrak{a} \cup \mathfrak{b}$) barruan dituen idealik txikiena*

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$$

multzoa da. (Orokorkiago, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideal kopuru finitu *bat emanda, ideal horiek barruan dituen A-ren idealik txikiena $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ batura da, hots, ideal horietan elementu bana harturik eta batuz lortzen dugun azpimultzoa.)*

(iv) $\mathfrak{a}$*-ko eta* $\mathfrak{b}$*-ko elementuen arteko biderkadura guztiak barruan dituen A-ren idealik txikiena, $\mathfrak{ab}$ gisa idazten duguna, honako hau da:*

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{k} a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b},\ k \in \mathbb{N} \right\},$$

hau da, biderkadura horien batura guztien multzoa. (Antzera gertatzen da ideal kopuru finitu *batekin.)*

Froga. Baieztapen guztiak erraz frogatzen dira, 2.4 proposizioan oinarrituz. □

Partekotasun hauek betetzen dira:

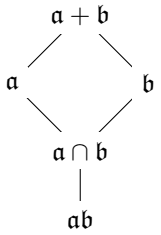

Diagrama horretan agertzen diren partekotasun guztiak hertsiak izan daitezke. Adibidez, $\mathfrak{a} = 6\mathbb{Z}$ eta $\mathfrak{b} = 10\mathbb{Z}$ $\mathbb{Z}$-ren idealak hartzen baditugu, orduan $\mathfrak{a} + \mathfrak{b} = 2\mathbb{Z}$, $\mathfrak{a} \cap \mathfrak{b} = 30\mathbb{Z}$ eta $\mathfrak{ab} = 60\mathbb{Z}$ dugu.

2.8. Oharra. Ideal kopuru infinitu baten batura ere defini daiteke. Zehazkiago, $\{\mathfrak{a}_i\}_{i \in I}$ A-ren idealen familia bat bada, orduan $\sum_{i \in I} \mathfrak{a}_i$ baturako elementuak ideal horietako elementuen batura *finitu* guztiak dira, hau da,

$$a_{i_1} + \cdots + a_{i_n}$$

bezalako baturak, non $a_j \in A_j$, $i_1, \ldots, i_n \in I$ eta $n \in \mathbb{N}$. Erraz egiaztatzen da $\sum_{i \in I} \mathfrak{a}_i$ A-ren ideala dela, eta hori dela $\cup_{i \in I} \mathfrak{a}_i$ bildura barruan duen idealik txikiena.

Aurreko teoremaren atal batzuetan, A-ren azpimultzo berezi batzuen kasuan, hori barruan duen idealik txikiena identifikatu dugu. Zein da azpimultzo orokor bat barruan duen idealik txikiena? Galdera horrek erantzun erraza du, hurrengo teoreman ikusiko dugun bezala. Lehenago, kontzeptu hori formalizatuko dugu.

2.9. Definizioa. Izan bitez A eraztuna eta S A-ren azpimultzoa. Orduan, *S-k sortutako ideala* S barruan duten A-ren ideal guztien ebakidura da. Bestela esanda, S barruan duen A-ren idealik txikiena da. Ideal hori (S) ikurraren bidez adieraziko dugu.

2.10. Definizioa. Ideal bat *finituki sortua* dela esango dugu elementu kopuru finitu baten bidez sor badaiteke, eta *nagusia* dela, berriz, elementu bakar baten bidez sor badaiteke.

Aurreko definizioan, "sor badaiteke" hori azpimarratu nahi dugu. Izan ere, ideal bat nagusia izan daiteke, sortzaile batekin baino gehiagorekin emanda badago ere, eta finituki sortua izan daiteke, infinitu sortzailerekin emanda ikusten badugu ere. Adibidez, $\mathbb{Z}$-n $(4,6)$ ideala nagusia da, $(4,6)=(2)$ delako. (Hurrengo teoremaren ondoren justifikatuko dugu berdintza hori.)

2.11. Teorema. *Izan bitez A eraztuna eta S A-ren azpimultzoa. Orduan,*

$$(S)=\{a_1x_1+\cdots+a_kx_k \mid a_1,\dots,a_k\in A,\ x_1,\dots,x_k\in S,\ k\in\mathbb{N}\}$$

berdintza dugu. Bestela esanda, S-k sortzen duen ideala S-ko elementuekin egin ditzakegun konbinazio guztiek osatzen dute, konbinazio horien "koefizienteak" A eraztunean izanik. Bereziki:

(i) *$S=\{x_1,\dots,x_n\}$ finitua bada,*

$$(x_1,\dots,x_n)=\{a_1x_1+\cdots+a_nx_n \mid a_1,\dots,a_n\in A\}.$$

(ii) *$S=\{x\}$ elementu bakar batek sortzen duen ideala x-ren multiplo guztien multzoa da, hau da,*

$$(x)=\{ax \mid x\in A\}.$$

Froga. Izan bedi

$$\mathfrak{a}=\{a_1x_1+\cdots+a_kx_k \mid a_1,\dots,a_k\in A,\ x_1,\dots,x_k\in S,\ k\in\mathbb{N}\}.$$

Berehala frogatzen da, 2.4 proposizioaren laguntzaz, $\mathfrak{a}$ A-ren ideala dela. Nabaria da $S\subseteq\mathfrak{a}$ partekotasuna, eta (S) denez S barruan duen A-ren idealik txikiena, $(S)\subseteq\mathfrak{a}$ dela ondorioztatzen da. Beste alde batetik, $x_1,\dots,x_k\in S$ badira, orduan (S) idealean ere badaude. Beraz, $a_1x_1+\cdots+a_kx_k\in(S)$ dugu $a_1,\dots,a_k\in A$ guztietarako. Horrela $\mathfrak{a}\subseteq(S)$ partekotasuna lortzen dugu. □

2.12. Adibideak. 1) $n\in\mathbb{Z}$ bada, $(n)=n\mathbb{Z}$ dugu.

2) $\mathbb{Z}$-n $(4,6)=(2)$ dugu. Izan ere,

$$(4,6)=\{4x+6y \mid x,y\in\mathbb{Z}\}=\{2z \mid z\in\mathbb{Z}\}=(2).$$

Erdiko berdintzan $\subseteq$ partekotasuna nabaria da eta $\supseteq$ Bézouten identitatearen ondorioa da, 2-a delako 4aren eta 6aren zatitzaile komunetako handiena.

3) A eraztun guztietarako $A = (1)$ dugu eta, oro har, $A = (x)$ betetzen da baldin eta soilik baldin x A-ren unitatea bada.

4) $\mathbb{R}[X, Y]$ polinomioen eraztunean,

$$(X, Y) = \{Xf(X, Y) + Yg(X, Y) \mid f, g \in \mathbb{R}[X, Y]\}$$

gai askerik gabeko polinomioen multzoa da.

5) Oro har, A edozein eraztun bada, orduan $A[X_1, \ldots, X_n]$ polinomioen eraztunean, $(X_1, \ldots, X_n)$ ideala gai askerik gabeko polinomioen multzoa da.

Elementu batzuek sortutako ideala elementu horien konbinazioek osatzen dutela esaten dugunean, ez ditugu adierazi nahi elementu horien *konbinazio linealak*, hau da, elementu horien multiploen baturak eskalarrez biderkatzen ditugunean, baizik eta elementu horien multiploen batura A *eraztuneko elementuez biderkatzen ditugunean*. Eraztun orokor baten kasuan ez dago posibilitate handirik akats horretan erortzeko; azken batean, zein gorputzen gainean hartuko genituzke eskalarrak? Hala ere, $K[X]$-ren kasuan (edo polinomioen eraztun orokorragoen kasuan) arrisku hori badago, K gorputza tartean delako. Beraz, argi izan: $(f_1(X), \ldots, f_n(X))$ idealeko elementuak ez dira $f_1(X), \ldots, f_n(X)$ polinomioen konbinazio linealak (K gorputzaren gainean), baizik eta polinomio horien multiploen baturak beste polinomio batzuekin biderkatzen ditugunean.

Orain, gorputzak idealen bitartez karakteriza daitezkeela ikusiko dugu.

2.13. Proposizioa. *Izan bedi A eraztun ez-tribiala. Orduan, A gorputza da baldin eta soilik baldin A-ren ideal bakarrak $\{0\}$ eta A badira.*

Froga. Demagun A gorputza dela, eta izan bedi $\mathfrak{a} \neq \{0\}$ A-ren ideala. Orduan, $x \in \mathfrak{a} \setminus \{0\}$ hartzen badugu, x unitatea da, eta 2.6 proposizioa erabiliz, $\mathfrak{a} = A$ dugu. Hortaz, A-ren ideal bakarrak $\{0\}$ eta A dira.

Demagun orain A eraztunaren ideal bakarrak $\{0\}$ eta A direla. Har dezagun $a \in A$, $a \neq 0$, eta ikus dezagun a unitatea dela. Horretarako, ohartu (a) idealak A eraztun osoa izan behar duela nahitaez. Beraz, $1 \in (a)$ dugu eta existitzen da $x \in A$ non $1 = xa$ baita, hau da, a unitatea da. □

Aurreko adibide batean ikusi dugu $(4, 6) = (2)$ berdintza betetzen dela $\mathbb{Z}$-n. Oro har, bi ideal sortzaileren bidez emanda badaude, nola jakin dezakegu berdinak diren edo ez? Horretarako, nahikoa da jakitea ideal horietariko bakoitza bestearen parte den edo ez. Hurrengo teoremak ematen digu erantzuna.

2.14. Teorema. *Izan bitez A eraztuna eta $\mathfrak{a} = (S)$ eta $\mathfrak{b} = (T)$ A-ren bi ideal. Orduan, $\mathfrak{a} \subseteq \mathfrak{b}$ dugu baldin eta soilik baldin $S \subseteq \mathfrak{b}$ bada, hau da, S-ko elementu guztiak T-ko elementuen konbinazioak badira.*

FROGA. Nabaria da $\mathfrak{a} \subseteq \mathfrak{b}$ baldintzak $S \subseteq \mathfrak{b}$ dakarrela. Alderantzizkoa ere garbi dago: definizioz, $\mathfrak{a} = (S)$ ideala S barruan duten A-ren ideal guztietatik txikiena denez, $S \subseteq \mathfrak{b}$ betetzen bada orduan $\mathfrak{a} \subseteq \mathfrak{b}$ ere bai. □

2.15. Korolarioa. *Izan bitez A eraztuna eta $\mathfrak{a} = (x_1, \dots, x_n)$ A-ren ideala. Orduan, $i \in \{1, \dots, n\}$ indize bakoitzeko:*

(i) *x_i-ren ordez ux_i jartzen badugu, $u \in A^\times$ izanik, $\mathfrak{a}$ ideala ez da aldatzen.*
(ii) *x_i-ren ordez $x_i + \sum_{j \neq i} a_j x_j$ jartzen badugu, $a_j \in A$ izanik $j \neq i$ guztietarako, $\mathfrak{a}$ ez da aldatzen.*

FROGA. Aurreko teoremaren ondorio berehalakoa da. □

Adibidez, $(X^2 + Y^2, X^2 - Y^2) = (X^2 + Y^2, 2X^2) = (X^2 + Y^2, X^2) = (Y^2, X^2)$ dugu $\mathbb{Q}[X, Y]$-n. Berdin litzateke $\mathbb{F}_2[X, Y]$-n?

2.16. Korolarioa. *Izan bitez A eraztuna eta $\mathfrak{a} = (x, S)$ A-ren ideala. Orduan, $x \equiv y \pmod{(S)}$ bada, $\mathfrak{a} = (y, S)$ ere badugu. Bestela esanda, $\mathfrak{a}$ ideal baten sistema sortzaile batean, beti jar dezakegu x elementu baten ordez y beste elementu bat, x eta y beste sortzaileek sortzen duten idealarekiko kongruenteak badira.*

FROGA. Frogatzen badugu $(x, S) \subseteq (y, S)$ partekotasuna, orduan, simetriagatik, berdintza izango dugu. Kontuan izanik 2.14 teorema, nahikoa da $x \in (y, S)$ frogatzea. Baina, $x \equiv y \pmod{(S)}$ izateagatik, $z = x - y$ elementua (S) idealean dago eta, ondorioz, $x = y + z \in (y, S)$ lortzen dugu. □

2.17. Adibidea. Izan bedi $\mathfrak{a} = (Y - X^2, Z^2 - X^3, Y^3 + YZ^2 - Z^4)$. Orduan, azken sortzailearen ordez, X bakarrik erabiltzen duen polinomio bat jar dezakegu. Izan ere, jarri $\mathfrak{b} = (Y - X^2, Z^2 - X^3)$, beste bi polinomioek sortzen duten ideala. Nabaria da $Y \equiv X^2 \pmod{\mathfrak{b}}$ eta $Z^2 \equiv X^3 \pmod{\mathfrak{b}}$ betetzen dela. Beraz,

$$Y^3 + YZ^2 + Z^4 \equiv (X^2)^3 + X^2X^3 - (X^3)^2 \equiv X^5 \pmod{\mathfrak{b}}$$

dugu eta, azken korolarioa aplikatuz, $\mathfrak{a} = (Y - X^2, Z^2 - X^3, X^5)$ dugu. Hori 2.15 korolarioa erabiliz ere lor genezake, baina lan gehiago eskatuko luke pentsatzeak $Y - X^2$ eta $Z^2 - X^3$ polinomioen zein multiplo batu behar dizkiogun $Y^3 + YZ^2 - Z^4$-ri X^5 baino ez gelditzeko.

Jarraian ikusten dugunez, 2.15 korolarioaren (i) atalaren alderantzizkoa egiazkoa da integritate-domeinuetan, ideal nagusien kasuan.

2.18. Teorema. *Izan bedi A integritate-domeinua. Orduan, $(x) = (y)$ dugu baldin eta soilik baldin existitzen bada $u \in A^\times$, non $y = ux$ baita.*

FROGA. Ezkerralderako norabidean emaitza ezaguna da. Ikus dezagun, beraz, alderantzizko inplikazioa. Lehenengo eta behin, x eta y elementuetako bat 0 bada, garbi dago besteak ere 0 izan behar duela (0 baita $\{0\}$ idealaren sortzaile bakarra) eta emaitza bete egiten da. Demagun hemendik aurrera $x \neq 0$ eta $y \neq 0$

dela. Ohartu, $(x) = (y)$ baldintza betetzeagatik, x y-ren multiploa dela eta y x-ren multiploa dela. Beraz, $x = ay$ eta $y = bx$ dugu $a, b \in A$ izanik eta, bi berdintza horiek konbinatuz, $x = abx$ lortzen dugu. Hortik, $x \neq 0$ eta A integritate-domeinua izateagatik, $1 = ab$ ondorioztatzen dugu. Beraz, $b \in A^\times$ dugu. Orain, $y = bx$ dela gogoratuz, nahi genuen emaitza frogaturik gelditzen da. □

Azkenik, ikus dezagun nola lor ditzakegun $\mathfrak{a}$ eta $\mathfrak{b}$ bi idealen baturaren eta biderkaduraren sortzaileak, $\mathfrak{a}$-ren eta $\mathfrak{b}$-ren sortzaileak ezagutuz gero.

2.19. Teorema. *Izan bitez $\mathfrak{a} = (S)$ eta $\mathfrak{b} = (T)$ A-ren bi ideal. Orduan:*

(i) $\mathfrak{a} + \mathfrak{b} = (S \cup T) = (s, t \mid s \in S,\ t \in T)$.

(ii) $\mathfrak{ab} = (st \mid s \in S,\ t \in T)$.

Bereziki, $\mathfrak{a} = (x_1, \dots, x_m)$ eta $\mathfrak{b} = (y_1, \dots, y_n)$ finituki sortuak badira, orduan

$$\mathfrak{a} + \mathfrak{b} = (x_1, \dots, x_m, y_1, \dots, y_n) \quad \text{eta} \quad \mathfrak{ab} = (x_i y_j \mid i = 1, \dots, m,\ j = 1, \dots, n)$$

dugu.

Froga. Bi ataletan, garbi dago $\supseteq$ partekotasuna betetzen dela; beraz, bakarrik arduratuko gara $\subseteq$ frogatzeaz. Izan bitez $x \in \mathfrak{a}$ eta $y \in \mathfrak{b}$. Orduan,

$$x = a_1 x_1 + \cdots + a_k x_k \qquad \text{eta} \qquad y = b_1 y_1 + \cdots + b_\ell y_\ell \tag{2.1}$$

dugu, $a_i, b_j \in A$, $x_i \in S$ eta $y_j \in T$ izanik.

(i) Bakarrik ikusi behar dugu $x + y \in (S \cup T)$ betetzen dela, eta hori garbi dago (2.1)-eko bi berdintzak batuz gero.

(ii) Biderkatzen baditugu (2.1)-eko bi berdintzak, garbi dago $xy \in (st \mid s \in S,\ t \in T)$ betetzen dela. Orain, kontuan hartzen badugu $\mathfrak{ab}$ biderkaduraren definizioa, konturatzen gara $\{xy \mid x \in \mathfrak{a},\ y \in \mathfrak{b}\}$ ideal horren sistema sortzaile bat dela. Horrenbestez, $\mathfrak{ab} \subseteq (st \mid s \in S,\ t \in T)$ lortzen dugu, 2.14 teorema erabiliz. □

Oso zaila izan daiteke, ordea, $\mathfrak{a} \cap \mathfrak{b}$ ebakiduraren sortzaileak ematea.

Atal hau bukatzeko, idealaren kontzeptua K-aljebren kasuan aztertuko dugu. Lehenengo eta behin, ikus dezagun nola aldatzen definizioa (hasiera batean, behintzat) eraztun arrunten kasuarekin konparatuta. Imajinatzekoa denez, idealei azpiespazioak ere izateko eskatuko zaie.

2.20. Definizioa. Izan bitez A K-aljebra eta $\mathfrak{a} \subseteq A$. Orduan, $\mathfrak{a}$ azpimultzoa A *aljebraren ideala* dela esaten dugu A eraztunaren ideala bada eta azpiespazioa bada aldi berean, hau da, propietate hauek betetzen baditu:

$$x, y \in \mathfrak{a} \ \Rightarrow\ x + y \in \mathfrak{a}, \qquad x \in \mathfrak{a},\ a \in A \ \Rightarrow\ ax \in \mathfrak{a}, \qquad \lambda \in K,\ x \in \mathfrak{a} \ \Rightarrow\ \lambda x \in \mathfrak{a}.$$

Jakina, aljebren idealek zatidura aljebrak ematen dizkigute.

2.21. Teorema. *Izan bitez A K-aljebra eta $\mathfrak{a}$ azpimultzoa A aljebraren ideala. Orduan,*

$$\lambda \cdot \overline{a} = \overline{\lambda a}, \quad \lambda \in K \text{ eta } \overline{a} \in A/\mathfrak{a} \text{ izanik,}$$

eragiketa ondo definiturik dago. Eskalarrezko biderketa hori eta $A/\mathfrak{a}$ zatidura eraztunaren batuketa eta biderketa hartzen ditugunean, $A/\mathfrak{a}$ K-aljebra da. Hori zatidura aljebra *bat dela esaten dugu.*

Lehenengo gaian aipatu dugunez, aljebra baten azpieraztun batek ez du zertan azpialjebra izan, gerta daitekeelako azpiespazioa ez izatea. Egoera guztiz kontrakoa da idealen kasuan. Izan ere, aljebra baten barruan, "ideala aljebraren egiturarekiko" eta "ideala eraztunaren egiturarekiko" gauza bera dira. Horren arrazoia da 2.20 definizioan dagoen hirugarren baldintza beste bien ondorioa dela. Izan ere,

$$\lambda x = \lambda(1 \cdot x) = (\lambda \cdot 1)x \in \mathfrak{a}$$

dugu, $\lambda \cdot 1 \in A$ eta $x \in \mathfrak{a}$ baita. Hori dela eta, eraztunen idealetarako betetzen diren emaitzek aljebren idealetarako ere balio dute.

2.22. Adibidea. Izan bedi K gorputza. Orduan, $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideala bada, $K[X_1, \ldots, X_n]/\mathfrak{a}$ moduko zatidurak K-aljebrak dira. Nahiz eta $K[X_1, \ldots, X_n]$-ren dimentsioa infinitua izan, $K[X_1, \ldots, X_n]/\mathfrak{a}$ zatidurak dimentsio finitukoak izan daitezke. (Ikusi, adibidez, 2.6 problema.)

2.2. Homomorfismoak

2.23. Definizioa. Izan bedi $\varphi : A \longrightarrow B$ aplikazioa, A eta B eraztunak izanik. Orduan, φ *eraztun-homomorfismoa* dela esango dugu batuketa eta biderketa gordetzen baditu, eta A-ren identitatea B-ren identitatera eramaten badu, hau da, propietate hauek betetzen baditu:

(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$, $x, y \in A$ guztietarako.
(ii) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$, $x, y \in A$ guztietarako.
(iii) $\varphi(1) = 1$.

Homomorfismo mota batzuei izen bereziak ematen zaizkie:

(a) φ injektiboa bada, *monomorfismoa* dela diogu.
(b) φ supraiektiboa bada, *epimorfismoa* dela diogu.
(c) φ bijektiboa bada, *isomorfismoa* dela diogu.
(d) $A = B$ bada, φ *endomorfismoa* dela diogu.
(e) $A = B$ bada eta φ bijektiboa bada, *automorfismoa* dela diogu.

2.24. Oharra. Eraztun-homomorfismo bat bereziki talde-homomorfismoa denez batuketarekiko, orduan propietate hauek betetzen dira:

(i) $\varphi(0) = 0$.
(ii) $a \in A$ bada, orduan $\varphi(na) = n\varphi(a)$ dugu, $n \in \mathbb{Z}$ guztietarako.

Gainera, eraztun-homomorfismoaren definizioko (ii) eta (iii) baldintzetatik berehala ondorioztatzen dira beste bi propietate hauek:

(iii) $a \in A$ bada, orduan $\varphi(a^n) = \varphi(a)^n$ dugu, $n \in \mathbb{N} \cup \{0\}$ guztietarako.

(iv) a A-ren unitatea bada, orduan $\varphi(a^{-1}) = \varphi(a)^{-1}$ eta, oro har, $\varphi(a^n) = \varphi(a)^n$ dugu, $n \in \mathbb{Z}$ guztietarako.

2.25. Adibideak. 1) Konjugazioa, hau da, $z = a + bi \mapsto \overline{z} = a - bi$ aplikazioa, $\mathbb{C}$-ren automorfismoa da.

2) Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan,

$$\begin{array}{rccc} \pi & : & A & \longrightarrow & A/\mathfrak{a} \\ & & a & \longmapsto & \overline{a} \end{array}$$

aplikazioa eraztun-epimorfismoa da, eta A-tik $A/\mathfrak{a}$-rako *epimorfismo kanonikoa* deitzen zaio.

3) Izan bedi B A-ren azpieraztuna. Orduan, $\iota : B \longrightarrow A$ aplikazioa, non $\iota(b) = b$ baita $b \in B$ guztietarako, eraztun-monomorfismoa da. Horri *partekotasun monomorfismo* deitzen zaio. Bereziki, A-ren identitate aplikazioa A-ren automorfismoa da.

4) Izan bitez A eta B eraztun ez-tribialak. Orduan, $\varphi : A \longrightarrow B$ aplikazio nulua, A-ko elementu guztiak 0ra eramaten dituena, ez da eraztun-homomorfismoa. Izan ere, ez du A-ren identitatea B-ren identitatea eramaten.

Bi eraztun isomorfo ditugunean, propietate aljebraiko berberak izango dituzte. Adibidez, erraz frogatu daiteke emaitza hau.

2.26. Proposizioa. *Izan bedi $\varphi : A \longrightarrow B$ eraztun-isomorfismoa. Orduan:*

(i) *A integritate-domeinua da baldin eta soilik baldin B integritate-domeinua bada.*

(ii) *A gorputza da baldin eta soilik baldin B gorputza bada.*

Antzera definitu ahal ditugu K-aljebren arteko homomorfismoak.

2.27. Definizioa. Izan bitez K gorputza eta A, B K-aljebrak. Orduan, $\varphi : A \longrightarrow B$ aplikazioa *K-aljebra homomorfismoa* dela esango dugu propietate hauek betetzen baditu:

(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$, $x, y \in A$ guztietarako.
(ii) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$, $x, y \in A$ guztietarako.
(iii) $\varphi(\lambda x) = \lambda\varphi(x)$, $\lambda \in K$ eta $x \in A$ guztietarako.
(iv) $\varphi(1) = 1$.

Bestela esanda, φ aljebra-homomorfismoa da aldi berean eraztun-homorfismoa eta aplikazio lineala bada.

Eraztun-homomorfismoen kasuan bezala definitzen dira aljebra-monomorfismoak, epimorfismoak, eta abar.

2.28. Adibidea. Zenbaki konplexuen gorputza aldi berean $\mathbb{R}$-aljebra eta $\mathbb{C}$-aljebra modura ikus dezakegu. Orduan, konjugazioa $\mathbb{R}$-aljebra automorfismoa da, baina ez da $\mathbb{C}$-aljebra automorfismoa, azken kasu horretan ez baita aplikazio lineala.

Jarraiko teoreman ikusten denez, bereziki erraza da aljebra-homomorfismoak definitzea polinomioen aljebren gainean. Emaitza hau behin eta berriz erabiliko dugu ikastaro honetan zehar.

2.29. Teorema (Polinomioen aljebren propietate unibertsala)**.** *Izan bitez K gorputza eta B K-aljebra. Orduan, $b_1, \dots, b_n \in B$ elementuak aukeratzen baditugu, badago $\varphi : K[X_1, \dots, X_n] \longrightarrow B$ K-aljebra homomorfismo bat, eta bakar bat, non $\varphi(X_i) = b_i$ baita $i = 1, \dots, n$ guztietarako. Zehazkiago, hau da $K[X_1, \dots, X_n]$-ko polinomio orokor baten irudia φ-ren bitartez:*

$$\sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \overset{\varphi}{\longmapsto} \sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} b_1^{i_1} \dots b_n^{i_n}, \tag{2.2}$$

hau da, irudia lortzeko, nahikoa da X_i indeterminatu bakoitzaren ordez b_i elementua jartzea. Beraz, honela ere eman ditzakegu φ-ren irudiak:

$$f(X_1, \dots, X_n) \overset{\varphi}{\longmapsto} f(b_1, \dots, b_n).$$

Aplikazio hori ebaluazio-homomorfismo *bat dela esaten dugu.*

Froga. Beste edozer baino lehen, φ ondo definituta dagoela azpimarratu nahi dugu. Izan ere, $f \in K[X_1, \dots, X_n]$ polinomio baten adierazpena

$$\sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n}$$

moduan bakarra denez, ez dago zalantzarik zein den $\varphi(f)$ irudia (2.2) formularen bitartez. Behin ondo definituta dagoela ziurtatuta, berehala egiaztatzen da φ K-aljebra homomorfismoa dela, eta $\varphi(X_i) = b_i$ dela $i = 1, \dots, n$ guztietarako.

Bakartasuna ikusteko, har dezagun $\psi(X_i) = b_i$ baldintza $i = 1, \dots, n$ guztietarako betetzen duen $\psi : K[X_1, \dots, X_n] \longrightarrow B$ beste K-aljebra homomorfismo bat. Orduan, eraztun-homomorfismoa eta aplikazio lineala denez,

$$\begin{aligned}
\psi\Big(\sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \Big) &= \sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} \psi(X_1)_1^{i_1} \dots \psi(X_n)_n^{i_n} \\
&= \sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} b_1^{i_1} \dots b_n^{i_n} \\
&= \psi\Big(\sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \Big)
\end{aligned}$$

dugu eta, horrela, $\psi = \varphi$ dela lortzen dugu. □

Beraz, $K[X_1, \dots, X_n]$-ren gainean K-aljebra homomorfismo bat definitzeko, nahikoa da indeterminatuen irudiak nahi dugun moduan aukeratzea.

2.30. Adibidea. Azken teoremaren arabera,

$$\begin{array}{rccc}
\varphi & : & \mathbb{R}[X,Y] & \longrightarrow & \mathbb{R}[Y] \\
 & & X & \longmapsto & 1 \\
 & & Y & \longmapsto & Y
\end{array}$$

irudiak emanez, ondo definituriko $\mathbb{R}$-aljebra homomorfismo bat dugu. Orduan,

$$\varphi(X^2+XY+Y^2)=1+Y+Y^2$$

dugu.

Azpimarratu behar da 2.29 teoremaren metodoak ez duela oro har funtzionatzen $K[X_1,\dots,X_n]$-ren ordez $A=K[a_1,\dots,a_n]$ beste aljebra finituki sortu bat hartzen badugu, $a_1,\dots,a_n$ elementuak ez badira indeterminatuak. Hau da, ezin da ziurtatu $a_i\mapsto b_i$ esleipenek K-aljebra homomorfismo bat definituko dutenik. Arrazoia da ezin dugula ziurtatu (2.2) formulak ondo definitutako φ aplikazioa ematen duenik. Izan ere, 1.59 teoremaren arabera $x\in K[a_1,\dots,a_n]$ elementu bakoitza

$$x=\sum_{i_1,\dots,i_n\geq 0}\lambda_{i_1,\dots,i_n}a_1^{i_1}\dots a_n^{i_n}$$

moduan idatz badaiteke ere, ezin dugu ziurtatu adierazpen hori bakarra denik. Orduan, $\varphi(x)$ kalkulatzean, gerta liteke x-ren horrelako bi adierazpenetan a_i-ren ordez b_i jartzean irudi desberdinak lortzea. Beraz, ezin dugu baieztatu φ ondo definituta egongo denik.

2.31. Adibidea. Eman dezagun azken arrisku-oharrean esandakoa konfirmatzen duen adibide bat. Izan bedi $A=\mathbb{R}[X,Y]/(X^2-Y^3)$ $\mathbb{R}$-aljebra. Orduan, $A=\mathbb{R}[\overline{X},\overline{Y}]$ dugu eta saia gaitezke A-tik $\mathbb{R}$-ra $\mathbb{R}$-aljebra homomorfismo bat definitzen $\overline{X}$-ren eta $\overline{Y}$-ren irudiak emanez. Ikus dezagun zer gertatzen den $\overline{X}\mapsto 1$ eta $\overline{Y}\mapsto -1$ esleipenekin. Egongo balitz irudi horiek dituen $\varphi:A\longrightarrow\mathbb{R}$ $\mathbb{R}$-aljebra homomorfismo bat, orduan

$$\varphi(\overline{X^2})=\varphi(\overline{X})^2=1\qquad\text{eta}\qquad\varphi(\overline{Y^3})=\varphi(\overline{Y})^3=-1$$

dugu. Orain, A aljebran $\overline{X^2}=\overline{Y^3}$ denez, horrek esan nahi du φ hori ez dagoela ondo definituta. Beraz, ez dago $\overline{X}\mapsto 1$ eta $\overline{Y}\mapsto -1$ betetzen duen aljebra-homomorfismorik. Argi ikusten da zein den homomorfismo hori lortzeko oztopoa: A-ko elementuen idazkera $\overline{X}$ eta $\overline{Y}$ sortzaileekiko ez dela bakarra.

Ikusi dugun propietate unibertsalak aljebretarako balio du, eta $K[X_1,\dots,X_n]$-ren gainean homomorfismoak definitzeko erabil dezakegu, *K gorputza den baldintzapean*. Nola egin dezakegu homomorfismoa $A[X_1,\dots,X_n]$-ren gainean definitu nahi badugu, A eraztuna bada, baina ez gorputza? Erantzuna da antzera joka daitekeela, baina B koeremuak nolakoa izan behar duen beste modu batean zehaztu beharko dugula. (Egia esan, A-aljebrak A eraztun orokor baten gainean definitu izan bagenitu, orduan B-k A-aljebra izan behar duela esan genezake; baina horretarako A-moduluen teoria garaturik izan beharko genuke, eta ez dugu eskura izango seigarren gaira iritsi arte.)

2.32. Teorema. *Izan bitez A eta B eraztunak, $A\subseteq B$ izanik. Orduan, $b_1,\dots,b_n\in B$ elementuak aukeratzen baditugu, badago $\varphi:A[X_1,\dots,X_n]\longrightarrow B$ eraztun-homomorfismo bat non $\varphi(X_i)=b_i$ baita $i=1,\dots,n$ guztietarako. Zehazkiago,*

hau da $A[X_1,\dots,X_n]$-ko polinomio orokor baten irudia φ-ren bitartez:

$$\sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n}X_1^{i_1}\dots X_n^{i_n} \overset{\varphi}{\longmapsto} \sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n}b_1^{i_1}\dots b_n^{i_n},$$

hau da, irudia lortzeko, nahikoa da X_i indeterminatu bakoitzaren ordez b_i elementua jartzea. Beraz, honela ere eman ditzakegu φ-ren irudiak:

$$f(X_1,\dots,X_n)\overset{\varphi}{\longmapsto} f(b_1,\dots,b_n).$$

Aplikazio hori ebaluazio-homomorfismo *bat dela esaten dugu. Bestalde, φ homomorfismoari A-ren gainean identitatea izateko eskatzen badiogu, orduan φ bakarra da.*

Froga. Polinomioen aljebren propietate unibertsalaren frogan bezala argudia dezakegu. □

2.33. Adibidea. Azken teoremaren arabera,

$$\begin{array}{rccc}\varphi & : & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}[i] \\ & & X & \longmapsto & i\end{array}$$

erregelak eraztun-homomorfismo bat definitzen du.

Garrantzitsua da esatea 2.29 eta 2.32 teoremetako emaitzek ez dutela funtzionatzen B koeremua ez bada izan behar duen bezalakoa. Adibidez, zentzugabekeria hutsa da $\varphi:\mathbb{R}[X]\longrightarrow\mathbb{F}_3$ eraztun-homomorfismo bat saiatzea definitzen $X\mapsto\overline{2}$ esleipenaren bitartez. Izan ere, hala egingo bagenu, orduan $\varphi(f(X))=f(\overline{2})$ izango genuke $f(X)\in\mathbb{R}[X]$ guztietarako eta, adibidez,

$$\varphi(\sqrt{2}X+\pi)=\sqrt{2}\cdot\overline{2}+\pi$$

litzateke. Baina azken adierazpen horrek ez du batere zentzurik, $\overline{2}\in\mathbb{F}_3$ ezin baita batu edo biderkatu osoak ez diren zenbaki errealekin.

Jarraitzeko, eman ditzagun homomorfismoen oinarrizko propietate batzuk.

2.34. Proposizioa. *Izan bedi $\varphi:A\longrightarrow B$ eraztun-homomorfismoa. Orduan:*

(i) *A' A-ren azpieraztuna bada, orduan $\varphi(A')$ B-ren azpieraztuna da. Bereziki,* $\operatorname{im}\varphi$ *B-ren azpieraztuna da.*
(ii) *B' B-ren azpieraztuna bada, orduan $\varphi^{-1}(B')$ A-ren azpieraztuna da.*
(iii) *$\mathfrak{a}$ A-ren ideala bada, orduan $\varphi(\mathfrak{a})$* $\operatorname{im}\varphi$*-ren ideala da, baina ez du zertan B-ren ideala izan.*
(iv) *$\mathfrak{b}$ B-ren ideala bada, orduan $\varphi^{-1}(\mathfrak{b})$ A-ren ideala da.*

Froga. Bakarrik frogatuko ditugu (ii) eta (iii), beste bi atalen froga antzekoa da eta.

(ii) Hemen 1.16 teoreman oinarrituko gara. Izan bitez $x,y\in\varphi^{-1}(B')$. Orduan, $\varphi(x),\varphi(y)\in B'$ dugu eta, B' B-ren azpieraztuna izateagatik,

$$\varphi(x-y)=\varphi(x)-\varphi(y)\in B' \quad \text{eta} \quad \varphi(xy)=\varphi(x)\varphi(y)\in B'$$

dugu. Ondorioz, $x-y, xy \in \varphi^{-1}(B')$ da. Bestalde, $\varphi(1)=1\in B'$ denez, $1\in \varphi^{-1}(B')$. Beraz, $\varphi^{-1}(B')$ A-ren azpieraztuna da.

(iii) Honetarako, 2.4 proposizioa erabiliko dugu. Hasteko, ohartu $\varphi(\mathfrak{a})$ ez dela hutsa, $\mathfrak{a}$ ez-hutsa izateagatik. Orain, izan bitez $z,t\in\varphi(\mathfrak{a})$ eta $b\in \operatorname{im}\varphi$. Orduan, existitzen dira $x,y\in\mathfrak{a}$ eta $a\in A$ non $z=\varphi(x)$, $t=\varphi(y)$, eta $b=\varphi(a)$ baita. Orduan, $\mathfrak{a}$ A-ren ideala denez,

$$z+t=\varphi(x)+\varphi(y)=\varphi(x+y)\in\varphi(\mathfrak{a}) \quad \text{eta} \quad bz=\varphi(a)\varphi(x)=\varphi(ax)\in\varphi(\mathfrak{a})$$

dugu. Horrela, $\varphi(\mathfrak{a})$ $\operatorname{im}\varphi$-ren ideala dela frogatu dugu. □

Azken proposizioan esan dugun bezala, $\varphi: A\longrightarrow B$ eraztun-homomorfismoa bada eta $\mathfrak{a}$ A-ren ideala bada, orduan $\varphi(\mathfrak{a})$-k ez du zertan B-ren ideala izan. Adibidez, $\iota:\mathbb{Z}\longrightarrow\mathbb{Q}$ partekotasun monomorfismoa bada, orduan $\mathbb{Z}$ $\mathbb{Z}$-ren ideala da, baina $\iota(\mathbb{Z})=\mathbb{Z}$ ez da $\mathbb{Q}$-ren ideala. Hobeto ulertu nahi badugu zergatik huts egin dezakeen propietate horrek, nahikoa dugu 2.34 proposizioko (iii) atalaren froga aztertzea. Arazoa bz biderkadurarekin dugu: $z=\varphi(x)$ dugu, baina $b=\varphi(a)$ idazteko aukerarik ez badago, orduan ezin dugu zt $\mathfrak{a}$-rekin erlazionatu φ-ren bitartez, eta ez dugu $\mathfrak{a}$ A-ren ideala dela erabiltzeko posibilitaterik.

2.35. Proposizioa. *Izan bedi $\varphi: A\longrightarrow B$ eraztun-homomorfismo supraiektiboa. Orduan:*

(i) *$\mathfrak{a}$ A-ren ideala bada, orduan $\varphi(\mathfrak{a})$ B-ren ideala da.*
(ii) *$\mathfrak{a}=(a_1,\dots,a_n)$ A-ren ideala bada, orduan $\varphi(\mathfrak{a})=(\varphi(a_1),\dots,\varphi(a_n))$ dugu.*

Froga. (i) Hori 2.34 proposizioaren ondorio hutsa da, $\operatorname{im}\varphi=B$ baita, φ supraiektiboa izateagatik.

(ii) Alde batetik, $\varphi(a_1),\dots,\varphi(a_n)\in\varphi(\mathfrak{a})$ dugu eta $\varphi(\mathfrak{a})$ B-ren ideala da. Beraz, $(\varphi(a_1),\dots,\varphi(a_n))\subseteq\varphi(\mathfrak{a})$ partekotasuna lortzen dugu.

Alderantzizko partekotasuna frogatzeko, hartu $x\in\mathfrak{a}$ elementu orokor bat. Orduan, $\mathfrak{a}=(a_1,\dots,a_n)$ izateagatik, $x=q_1a_1+\cdots+q_na_n$ idatz dezakegu, $q_1,\dots,q_n\in A$ izanik, eta

$$\varphi(x)=\varphi(q_1)\varphi(a_1)+\cdots+\varphi(q_n)\varphi(a_n)\in(\varphi(a_1),\dots,\varphi(a_n)).$$

Horrela, $\varphi(\mathfrak{a})\subseteq(\varphi(a_1),\dots,\varphi(a_n))$ lortzen dugu. □

2.36. Definizioa. Izan bedi $\varphi: A\longrightarrow B$ eraztun-homomorfismoa. Orduan,

$$\ker\varphi=\{a\in A\mid \varphi(a)=0\}$$

multzoa φ-ren *nukleoa* dela esaten dugu.

2.37. Proposizioa. *Izan bedi $\varphi: A\longrightarrow B$ eraztun-homomorfismoa. Orduan, $\ker\varphi$ A-ren ideala da, eta φ injektiboa da baldin eta soilik baldin $\ker\varphi=\{0\}$ bada.*

Froga. Ikusteko $\ker\varphi$ A-ren ideala dela, nahikoa da $\ker\varphi=\varphi^{-1}(\{0\})$ dela ohartzea eta 2.34 proposizioaren (iv) atala erabiltzea.

Demagun φ injektiboa dela. Orduan, $a \in \ker\varphi$ badugu, $\varphi(a) = 0 = \varphi(0)$ denez, $a = 0$ dela ondorioztatzen dugu. Hortaz, $\ker\varphi = \{0\}$ da, eta enuntziatuko baliokidetasunaren inplikazioetako bat dugu. Alderantzizkoa ikusteko, demagun $\ker\varphi = \{0\}$ dela, eta $\varphi(a) = \varphi(b)$ dela. Orduan, $\varphi(a-b) = 0$ eta $a - b \in \ker\varphi$. Beraz, $a - b = 0$ dugu, hau da, $a = b$. Horrek φ injektiboa dela frogatzen du. □

2.38. Teorema (Lehenengo isomorfismo-teorema)**.** *Izan bedi $\varphi : A \longrightarrow B$ eraztun-homomorfismoa. Orduan,*

$$\begin{array}{rccc} \overline{\varphi} & : & A/\ker\varphi & \longrightarrow & \operatorname{im}\varphi \\ & & \overline{a} & \longmapsto & \varphi(a) \end{array}$$

aplikazioa ondo definiturik dago eta eraztun-isomorfismoa da. Beraz,

$$\frac{A}{\ker\varphi} \cong \operatorname{im}\varphi.$$

Froga. Ikus dezagun $\overline{\varphi}$ ondo definituta dagoela:

$$\begin{array}{ccccc} \overline{a} = \overline{a'} & \Longrightarrow & a - a' \in \ker\varphi & \Longrightarrow & \varphi(a-a') = 0 \\ & \Longrightarrow & \varphi(a) - \varphi(a') = 0 & \Longrightarrow & \varphi(a) = \varphi(a'). \end{array}$$

Orain, begi-bistakoa da $\overline{\varphi}$ homomorfismoa dela, φ izateagatik, eta $\overline{\varphi}$ supraiektiboa dela, haren koeremua $\operatorname{im}\varphi$ izateagatik. Ikus dezagun, azkenik, $\overline{\varphi}$ injektiboa dela. Horretarako, 2.37 proposizioaren arabera, nahikoa da $\ker\overline{\varphi} = \{\overline{0}\}$ dela frogatzea. Ikus dezagun hala dela:

$$\overline{a} \in \ker\overline{\varphi} \quad \Longrightarrow \quad \overline{\varphi}(\overline{a}) = 0 \quad \Longrightarrow \quad \varphi(a) = 0 \quad \Longrightarrow \quad a \in \ker\varphi \quad \Longrightarrow \quad \overline{a} = \overline{0}.$$

□

2.39. Oharra. Jakina, lehenengo isomorfismo-teoremaren bertsio bera dugu aljebra-homomorfismoetarako, "eraztun" agertzen den leku guztietan "aljebra" jartzen badugu.

Lehenengo isomorfismo-teorema oso tresna egokia da isomorfismoak frogatzeko. Ikus ditzagun adibide pare bat.

2.40. Adibideak. 1) Izan bedi $\varphi : \mathbb{R}[X,Y] \longrightarrow \mathbb{R}[Y]$ 2.31 adibidean eman dugun $\mathbb{R}$-aljebra homomorfismoa, $X \mapsto 1$ eta $Y \mapsto Y$ esleipenen bidez definituta. Alde batetik, $f \in K[Y]$ bada, orduan $\varphi(f) = f$ dugu eta, hortaz, φ supraiektiboa da. Ikus dezagun orain $\ker\varphi = (X-1)$ dela. Partekotasunetako bat nabaria da: $\varphi(X-1) = 0$ denez eta $\ker\varphi$ ideala denez, $(X-1) \subseteq \ker\varphi$ dugu. Alderantzizko partekotasuna ikusteko, har dezagun $f \in \ker\varphi$ eta zatitu dezagun $X-1$ polinomioaz, X indeterminatuarekiko (horretarako, Y konstantetzat hartu behar dugu, hau da, $\mathbb{R}[X,Y]$ eraztuna $\mathbb{R}[Y][X]$ gisa ikusten ari gara). Orduan, $f = q(X-1)+r$ lortzen dugu, $q, r \in K[X,Y]$ eta $\deg_X r < \deg_X(X-1)$ izanik. Horrek esan nahi du $\deg_X r \leq 0$ dela, eta r polinomioan ez dago X-rik. Beraz, $r \in K[Y]$ dugu. Orduan,

$$0 = \varphi(f) = \varphi(q(X-1)+r) = \varphi(q)\varphi(X-1) + \varphi(r) = r$$

lortzen dugu. Ondorioz, $f = q(X-1)$ besterik ez da, eta $f \in (X-1)$ dugu. Horrenbestez, $\ker\varphi = (X-1)$ dela frogatu dugu. Orain, lehenengo isomorfismo-teorema aplikatzen badugu,

$$\frac{\mathbb{R}[X,Y]}{(X-1)} \cong \mathbb{R}[Y]$$

isomorfismoa lortzen dugu.

2) Aurreko adibidean ez dago ezer berezirik $\mathbb{R}$ gorputzari eta 1 balioari buruz. Beraz, K edozein gorputz bada eta $a \in K$ edozein elementu bada, orduan isomorfismo hau dugu:

$$\frac{K[X,Y]}{(X-a)} \cong K[Y].$$

3) Guztiz era berean (are gehiago, errazagoa da) frogatu daiteke beste isomorfismo hau, K edozein gorputz izanik, eta $a \in K$ edozein elementu izanik:

$$\frac{K[X]}{(X-a)} \cong K.$$

4) Berriro ere polinomioen aljebren propietate unibertsala erabiliz,

$$\begin{array}{rccc} \varphi & : & \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ & & X & \longmapsto & i \end{array}$$

erregelaren bidez $\mathbb{R}$-aljebra homomorfismo bat definitzen dugu. Ohartu φ supraiektiboa dela, $\varphi(a+bX) = a+bi$ baita, $a, b \in \mathbb{R}$ guztietarako. Ikus dezagun oraingoan $\ker\varphi = (X^2+1)$ dela. Alde batetik, $\varphi(X^2+1) = 0$ denez eta $\ker\varphi$ ideala denez, $(X^2+1) \subseteq \ker\varphi$ dugu. Bestetik, $f \in \ker\varphi$ bada, orduan X^2+1 polinomioaz zatituz, $f = q(X^2+1)+r$ lortzen dugu, $\deg r \leq 1$ izanik. Orain, $r(X) = a+bX$ idazten badugu, eta f-ren deskonposizioari φ aplikatzen badiogu,

$$0 = \varphi(f) = \varphi(q(X^2+1)+r) = \varphi(q)\varphi(X^2+1)+\varphi(r) = a+bi$$

lortzen dugu. Ondorioz, $a = b = 0$ izan behar du, eta $r = 0$ dugu. Horrela, $f = q(X^2+1) \in (X^2+1)$ dugu. Beraz, $\ker\varphi = (X^2+1)$ dela frogatu dugu. Lehenengo isomorfismo-teorema aplikatuz,

$$\frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}$$

isomorfismoa dugu, zenbaki konplexuen gorputza $\mathbb{R}[X]$-ren zatidura modura adierazten duena.

5) Guztiz era berean, 2.33 adibidean eman dugun eraztun-homomorfismoa erabiltzen badugu,

$$\frac{\mathbb{Z}[X]}{(X^2+1)} \cong \mathbb{Z}[i]$$

isomorfismoa lortzen dugu.

Atal hau bukatzeko, hondarraren teorema txinatarra deitutakoa aurkezten dugu. Bi bertsio emango ditugu: lehenengoak, bertsio klasikoak, zenbaki osoen gaineko kongruentzia-sistema linealak askatzeko balio du; bigarrena, orokorragoa, edozein eraztunetan aplika daiteke.

2.41. Teorema (Hondarraren teorema txinatarra: bertsio klasikoa)**.** *Izan bitez $m_1, \dots, m_r \in \mathbb{Z}$ binaka elkarrekiko lehenak diren zenbakiak. Orduan, $a_1, \dots, a_r \in \mathbb{Z}$ guztietarako,*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases} \tag{2.3}$$

kongruentzia-sistemak soluzioa du, eta soluzio guztiek hondar-klase bakarra osatzen dute $m_1 \dots m_r$ moduluarekiko.

Froga. Demagun

$$\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \quad \vdots \\ x \equiv 0 \pmod{m_r} \end{cases} \quad \begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv 1 \pmod{m_2} \\ \quad \vdots \\ x \equiv 0 \pmod{m_r} \end{cases} \quad \dots \quad \begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \quad \vdots \\ x \equiv 1 \pmod{m_r} \end{cases} \tag{2.4}$$

sistema laguntzaileak askatzen dakigula, eta izan bitez $x_1, \dots, x_r$ sistema horien soluzioak, hurrenez hurren. Orduan, garbi dago $x = a_1x_1 + \dots + a_rx_r$ zenbakia (2.3) sistemaren soluzioa dela.

Azaldu dezagun, bada, nola askatu sistema laguntzaileak. Erraztasunez, lehenengoaren kasuan egingo dugu. Hipotesiaren arabera,

$$\operatorname{zkh}(m_1, m_2) = \dots = \operatorname{zkh}(m_1, m_r) = 1$$

dugu eta, ondorioz, $\operatorname{zkh}(m_1, m_2 \dots m_r) = 1$ ere bai. Bézouten identitatea aplikatuz, existitzen dira $\lambda, \mu \in \mathbb{Z}$ non

$$\lambda m_1 + \mu m_2 \dots m_r = 1$$

baita. Orduan,

$$x_1 = 1 - \lambda m_1 = \mu m_2 \dots m_r$$

hartzen badugu, garbi dago lehenengo sistema laguntzailearen soluzioa dela.

Azkenik, ikus dezagun (2.3) sistemaren soluzioek hondar-klase bakarra osatzen dutela $m_1 \dots m_r$ moduluarekiko. Finka dezagun sistemaren soluzio bat, x. Orduan, y zenbaki osoa ere soluzioa izango da baldin eta soilik baldin

$$\begin{cases} x \equiv y \pmod{m_1} \\ \quad \vdots \\ x \equiv y \pmod{m_r} \end{cases}$$

bada. Ohartu kongruentzia horiek betetzen direla baldin eta soilik baldin

$$m_1 \mid x - y, \ \dots \ , m_r \mid x - y$$

bada, edo gauza bera dena, $\operatorname{mkt}(m_1, \dots, m_r) \mid x - y$ bada. Orain, $m_1, \dots, m_r$ binaka elkarrekiko lehenak direnez, haien multiplo komunetako txikiena $m_1 \dots m_r$ biderkadura da eta, ondorioz,

$$\begin{aligned} y \text{ (2.3) sistemaren soluzioa da} &\iff m_1 \dots m_r \mid x - y \\ &\iff x \equiv y \pmod{m_1 \dots m_r}. \end{aligned}$$

Beraz, sistemaren soluzio guztiek hondar-klase bakarra osatzen dute $m_1 \dots m_r$ moduluarekiko. □

2.42. Oharra. Teoremaren frogak erakusten du praktikan zein prozedura jarraitu behar den (2.3) bezalako sistemak askatzeko: sistema laguntzaileen $x_1, \dots, x_r$ soluzioak lortu Bézouten identitatearen laguntzaz, eta $x = a_1x_1 + \cdots + a_rx_r$ konbinazioa egin.

Orain, hondarraren teorema txinatarraren bertsio orokortua emango dugu. Horretarako, ohartu $x \equiv a \pmod{m}$ kongruentzia bat $x \equiv a \pmod{m\mathbb{Z}}$ moduan ere jar daitekeela, moduluan ideal bat jarrita. Hori da ideia edozein eraztunetan balio duen bertsio bat emateko: moduluetan idealak erabiltzea. Aurretik, kontzeptu bat sartu behar dugu, eta lema bat eman behar dugu.

2.43. Definizioa. Izan bitez A eraztuna eta $\mathfrak{a}$ eta $\mathfrak{b}$ A-ren idealak. Orduan, $\mathfrak{a}$ eta $\mathfrak{b}$ *komaximalak* direla esango dugu $\mathfrak{a} + \mathfrak{b} = A$ bada.

2.44. Adibidea. Zenbaki osoen eraztunean, $m\mathbb{Z}$ eta $n\mathbb{Z}$ idealak komaximalak dira baldin eta soilik baldin $\operatorname{zkh}(m, n) = 1$ bada.

2.45. Lema. *Izan bitez A eraztuna eta $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ A-ren idealak, binaka komaximalak. Orduan:*

(i) *$\mathfrak{a}_i$ eta $\mathfrak{a}_1 \dots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \dots \mathfrak{a}_r$ komaximalak dira $i = 1, \dots, r$ guztietarako, hau da,*

$$\mathfrak{a}_i + \mathfrak{a}_1 \dots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \dots \mathfrak{a}_r = A$$

dugu.

(ii) *$\mathfrak{a}_1 \dots \mathfrak{a}_r = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ dugu.*

Froga. (i) Erraztasunez, $i = 1$ den kasuan baino ez dugu frogatuko. Alde batetik, $\mathfrak{a}_1$ eta $\mathfrak{a}_i$ komaximalak direnez, existitzen dira $x_i \in \mathfrak{a}_1$ eta $y_i \in \mathfrak{a}_i$ non $x_i + y_i = 1$ baita $i = 2, \dots, r$ guztietarako. Berdintza horiek guztiak biderkatuz,

$$1 = (x_2 + y_2) \dots (x_r + y_r) = x + y_2 \dots y_r$$

lortzen dugu, $x \in \mathfrak{a}_1$ izanik ($\mathfrak{a}_1$-ean faktore bat duten biderkaduren batura baita) eta $y_2 \dots y_r \in \mathfrak{a}_2 \dots \mathfrak{a}_r$ izanik. Ondorioz, 1 identitatea $\mathfrak{a}_1 + \mathfrak{a}_2 \dots \mathfrak{a}_r$ idealean dago, eta $\mathfrak{a}_1 + \mathfrak{a}_2 \dots \mathfrak{a}_r = A$ dugu, nahi bezala.

(ii) Emaitza hori r-ren gaineko indukzioaz frogatuko dugu. Lehenengo eta behin, ikus dezagun $r = 2$ den kasua, hau da, frogatu dezagun $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$ dela. Gogoratu $\subseteq$ partekotasuna beti betetzen dela. Har dezagun orain $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$. Badakigunez $\mathfrak{a}_1$ eta $\mathfrak{a}_2$ komaximalak direla, $1 = z_1 + z_2$ idatz dezakegu, $z_1 \in \mathfrak{a}_1$ eta $z_2 \in \mathfrak{a}_2$ izanik. Berdintza hori x-rekin biderkatuz, $x = xz_1 + xz_2 \in \mathfrak{a}_1\mathfrak{a}_2$ lortzen dugu. Horrela frogatua dugu $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$ berdintza, indukzioaren oinarria dena.

Demagun orain $r \geq 3$ dela, eta emaitza $r - 1$ idealekin betetzen dela. Aurreko atalaren arabera, $\mathfrak{a}_1$ eta $\mathfrak{a}_2 \dots \mathfrak{a}_r$ idealak komaximalak dira. Beraz, bi idealen kasuan

emaitza frogatuta dagoenez,

$$\mathfrak{a}_1\mathfrak{a}_2\dots\mathfrak{a}_r = \mathfrak{a}_1 \cap \mathfrak{a}_2\dots\mathfrak{a}_r$$

dugu. Bestalde, indukzio-hipotesia aplikatuz,

$$\mathfrak{a}_2\dots\mathfrak{a}_r = \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_r$$

dugu. Azken bi berdintzak konbinatuz, froga biribildurik dago. □

2.46. Teorema (Hondarraren teorema txinatarra: bertsio orokortua)**.** *Izan bitez A eraztuna eta $\mathfrak{a}_1,\dots,\mathfrak{a}_r$ A-ren idealak, binaka komaximalak. Orduan, $a_1,\dots,a_r \in A$ guztietarako,*

$$\begin{cases} x \equiv a_1 \pmod{\mathfrak{a}_1} \\ \quad\vdots \\ x \equiv a_r \pmod{\mathfrak{a}_r} \end{cases}$$

kongruentzia-sistemak soluzioa du, eta soluzio guztiek koklase bakarra osatzen dute $\mathfrak{a}_1\dots\mathfrak{a}_r$ moduluarekiko.

Froga. Nahikoa da, $\mathbb{Z}$-ren kasuan bezala, sistema laguntzaile hauek askatzea:

$$\begin{cases} x \equiv 1 \pmod{\mathfrak{a}_1} \\ x \equiv 0 \pmod{\mathfrak{a}_2} \\ \quad\vdots \\ x \equiv 0 \pmod{\mathfrak{a}_r} \end{cases} \quad \begin{cases} x \equiv 0 \pmod{\mathfrak{a}_1} \\ x \equiv 1 \pmod{\mathfrak{a}_2} \\ \quad\vdots \\ x \equiv 0 \pmod{\mathfrak{a}_r} \end{cases} \quad \dots \quad \begin{cases} x \equiv 0 \pmod{\mathfrak{a}_1} \\ x \equiv 0 \pmod{\mathfrak{a}_2} \\ \quad\vdots \\ x \equiv 1 \pmod{\mathfrak{a}_r} \end{cases}$$

Ohartu sistema horiek soluzioa dutela ziurtatzeko nahikoa dela 2.45 lemaren (i) atala aplikatzea: horren arabera, existitzen dira $x_i \in \mathfrak{a}_1\dots\mathfrak{a}_{i-1}\mathfrak{a}_{i+1}\dots\mathfrak{a}_r$ eta $y_i \in \mathfrak{a}_i$ non $x_i + y_i = 1$ baita, eta orduan garbi dago x_i $i$garren sistema laguntzailearen soluzioa dela.

Ikusteko sistemaren soluzioek koklase bakar bat osatzen dutela $\mathfrak{a}_1\dots\mathfrak{a}_r$ moduluarekiko, finka dezagun sistemaren soluzio bat, x. Orduan, $y \in A$ ere soluzioa izango da baldin eta soilik baldin

$$\begin{cases} x \equiv y \pmod{\mathfrak{a}_1} \\ \quad\vdots \\ x \equiv y \pmod{\mathfrak{a}_r} \end{cases}$$

bada. Ohartu kongruentzia horiek betetzen direla baldin eta soilik baldin

$$x - y \in \mathfrak{a}_1,\ \dots\ , x - y \in \mathfrak{a}_r$$

bada, edo gauza bera dena, $x - y \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_r$ bada. Orain, 2.45 lemaren (ii) atala aplikatuz, $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_r = \mathfrak{a}_1\dots\mathfrak{a}_r$ dugu eta, ondorioz,

$$y \text{ sistemaren soluzioa da} \iff x-y \in \mathfrak{a}_1\dots\mathfrak{a}_r \iff x \equiv y \pmod{\mathfrak{a}_1\dots\mathfrak{a}_r},$$

nahi genuen bezala. □

2.3. Ideal mota nagusiak

2.47. Definizioa. Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan:

(i) $\mathfrak{a}$ A-ren *ideal maximala* dela diogu propioa bada eta ezin bada sartu beste ideal propio handiago batean. Sinbolikoki jarrita:

$$\mathfrak{a} \subseteq \mathfrak{b} \subseteq A \quad \Longrightarrow \quad \mathfrak{b} = \mathfrak{a} \text{ edo } \mathfrak{b} = A.$$

(ii) $\mathfrak{a}$ A-ren *ideal lehena* dela diogu propioa bada eta propietate hau betetzen badu:

$$ab \in \mathfrak{a} \quad \Longrightarrow \quad a \in \mathfrak{a} \text{ edo } b \in \mathfrak{a}.$$

2.48. Adibideak. 1) Argi eta garbi, $\{0\}$ ideal lehena da baldin eta soilik baldin A integritate-domeinua bada.

2) $\mathbb{Z}$-ren ideal maximalak $p\mathbb{Z}$ modukoak dira, p lehena izanik, eta ideal lehenak horiek berak dira, $\{0\}$ ideal nuluarekin batera.

3) Izan bedi K gorputza. Orduan, (X) ideala maximala da $K[X]$-n. Hori ikusteko, demagun $(X) \subsetneq \mathfrak{b} \subseteq K[X]$ dela, $\mathfrak{b}$ $K[X]$-ren ideala izanik, eta frogatu dezagun $\mathfrak{b} = K[X]$ dela. Alde batetik, (X)-ko elementuak gai askerik gabeko polinomioak direnez, existitzen da $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathfrak{b}$ non $a_0 \neq 0$ baita. Orain, $(X) \subseteq \mathfrak{b}$ denez, $a_1X + \cdots + a_nX^n \in \mathfrak{b}$ dugu eta, ondorioz,

$$a_0 = f(X) - (a_1X + \cdots + a_nX^n) \in \mathfrak{b}.$$

Horrela, $\mathfrak{b}$ idealaren barruan konstante ez-nulu bat aurkitu dugu, eta hori unitatea da $K[X]$-n. Beraz, $\mathfrak{b} = K[X]$ dugu.

4) Beste alde batetik, A eraztuna ez bada gorputza, orduan (X) ez da $A[X]$-ren ideal maximala. Izan ere, $a \in A$ elementua aukeratzen badugu, ez-nulua eta ez-unitatea dena, orduan $(X) \subsetneq (a, X) \subsetneq A[X]$ dugu.

5) Hirugarren adibidean bezala argudiatuz, K gorputza bada, $(X_1, \ldots, X_n)$ ideala $K[X_1, \ldots, X_n]$-n maximala dela ikus dezakegu.

Hurrengo emaitza Zornen Lemaren ondorio erraza da.

2.49. Teorema. *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideal propioa. Orduan, $\mathfrak{a}$ ideal maximal baten barruan sar daiteke. Bereziki, A-k ideal maximalak ditu.*

2.50. Oharra. Ideal maximalen existentzia eraztunen propietate berezi bat da, eta beste egitura aljebraikoetan ez dugu antzeko emaitzarik. Adibidez, talde batean ez dugu zertan azpitalde maximalik izan, ezta azpitalde normal maximalik ere. Hori da kasua, adibidez, $\mathbb{Q}$ talde batukorrarekin.

Hurrengo teoreman ikusten dugun bezala, $\mathfrak{a}$ ideala maximala edo lehena den jakiteko, $A/\mathfrak{a}$ zatidura erabil dezakegu.

2.51. Teorema. *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan:*

(i) *$\mathfrak{a}$ A-ren ideal maximala da baldin eta soilik baldin $A/\mathfrak{a}$ gorputza bada.*

(ii) $\mathfrak{a}$ *A-ren ideal lehena da baldin eta soilik baldin* $A/\mathfrak{a}$ *integritate-domeinua bada.*

FROGA. Teorema hori frogatzeko, bakarrik gogoratu behar dugu $A/\mathfrak{a}$ zatidura eraztunean $\overline{a} = \overline{0}$ dugula baldin eta soilik baldin $a \in \mathfrak{a}$ bada.

(i) Baliokidetasun hauek ditugu:

$$\begin{aligned} A/\mathfrak{a} \text{ gorputza} &\iff \left\{ \begin{array}{l} A/\mathfrak{a} \neq \{\overline{0}\} \\ \overline{x} \neq \overline{0} \ \Rightarrow \ \exists\, \overline{a} : \overline{a} \cdot \overline{x} = \overline{1} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \mathfrak{a} \neq A \\ x \notin \mathfrak{a} \ \Rightarrow \ \exists\, a : 1 - ax \in \mathfrak{a} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \mathfrak{a} \neq A \\ x \notin \mathfrak{a} \ \Rightarrow \ \exists\, a \in A,\ \exists\, y \in \mathfrak{a} : 1 = ax + y \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \mathfrak{a} \neq A \\ x \notin \mathfrak{a} \ \Rightarrow \ (x) + \mathfrak{a} = A. \end{array} \right\} \end{aligned}$$

Orain, demagun $A/\mathfrak{a}$ gorputza dela eta frogatu dezagun $\mathfrak{a}$ A-ren ideal maximala dela. Aurrekoagatik, badakigu $\mathfrak{a}$ A-ren ideal propioa dela. Har dezagun $\mathfrak{b}$ beste ideal bat, non $\mathfrak{a} \subsetneq \mathfrak{b} \subseteq A$ baita, eta ikus dezagun $\mathfrak{b} = A$ dela. Horretarako, aukeratu elementu bat $x \in \mathfrak{b} \setminus \mathfrak{a}$. Goian ikusi bezala, $(x) + \mathfrak{a} = A$ dugu. Baina (x) eta $\mathfrak{a}$ idealak $\mathfrak{b}$-ren barruan daude, eta hortik $\mathfrak{b} = A$ dela ondorioztatzen dugu.

Alderantziz, $\mathfrak{a}$ A-ren ideal maximala bada, frogatu dezagun $A/\mathfrak{a}$ gorputza dela. Aurreko baliokidetasunen arabera, bakarrik ikusi behar dugu $(x) + \mathfrak{a} = A$ betetzen dela $x \notin \mathfrak{a}$ guztietarako. Hori berehalakoa da ideal maximalaren definizioan oinarrituz, $(x) + \mathfrak{a}$ A-ren ideala baita eta $\mathfrak{a} \subsetneq (x) + \mathfrak{a}$ baita, $x \notin \mathfrak{a}$ izateagatik.

(ii) Kasu honetan,

$$\begin{aligned} A/\mathfrak{a} \text{ I.D.} &\iff \left\{ \begin{array}{l} A/\mathfrak{a} \neq \{\overline{0}\} \\ \overline{x} \cdot \overline{y} = \overline{0} \ \Rightarrow \ \overline{x} = \overline{0} \text{ edo } \overline{y} = \overline{0} \end{array} \right\} \\ &\iff \left\{ \begin{array}{l} \mathfrak{a} \neq A \\ xy \in \mathfrak{a} \ \Rightarrow \ x \in \mathfrak{a} \text{ edo } y \in \mathfrak{a} \end{array} \right\} \\ &\iff \mathfrak{a} \ A\text{-ren ideal lehena.} \end{aligned}$$

□

2.52. Korolarioa. *Edozein eraztunetan, ideal maximalak lehenak dira.*

2.53. Adibideak. 1) Izan bedi K gorputza. Kontuan hartzen baditugu 2.40 adibideetan emandako isomorfismoak, eta 2.51 teorema aplikatzen badugu, esan dezakegu $(X - a)$ $K[X]$-ren ideal maximala dela, eta $(X - a)$ $K[X, Y]$-ren ideal lehena dela, baina ez maximala.

2) Era berean, $(X^2 + 1)$ $\mathbb{R}[X]$-ren ideal maximala da, eta $(X^2 + 1)$ $\mathbb{Z}[X]$-ren ideal lehena da, baina ez maximala.

Badago modu garbiago bat 2.51 teoremaren (i) ataleko baliokidetasuna zergatik betetzen den ulertzeko. Horretarako zatidura baten idealak nolakoak diren ezagutu behar dugu. Emaitza hori oso maiz erabiltzen da, eta jarraian enuntziatuko dugu.

2.54. Teorema (Korrespondentziaren teorema)**.** *Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala. Orduan:*

(i) *$\mathfrak{b}$ A-ren ideala bada, $\mathfrak{a} \subseteq \mathfrak{b}$ izanik,*

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \{x + \mathfrak{a} \mid x \in \mathfrak{b}\}$$

multzoa $A/\mathfrak{a}$-ren ideala da, eta horrela agertzen dira $A/\mathfrak{a}$-ren ideal guztiak. Zehazkiago,

$$\begin{array}{ccc} \{\mathfrak{b} \mid \mathfrak{b} \text{ } A\text{-ren ideala eta } \mathfrak{a} \subseteq \mathfrak{b}\} & \longrightarrow & \{A/\mathfrak{a}\text{-ren idealak}\} \\ \mathfrak{b} & \longmapsto & \mathfrak{b}/\mathfrak{a} \end{array}$$

aplikazioa bijektiboa da.

(ii) *Aurreko atalaren baldintzetan,*

$$\frac{A/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}} \cong A/\mathfrak{b}$$

isomorfismoa dugu. Emaitza horri zatidura bikoitzaren teorema *edo* bigarren isomorfismo-teorema *deitzen zaio.*

(iii) *$\mathfrak{b}/\mathfrak{a}$ $A/\mathfrak{a}$-ren ideal maximala edo lehena da baldin eta soilik baldin $\mathfrak{b}$ A-ren ideal maximala edo lehena bada, hurrenez hurren.*

Froga. (i) Batuketari besterik ez badiogu begiratzen, orduan talde-teoriako korrespondentziaren teoremagatik, badakigu bijekzio bat dagoela $\mathfrak{a}$ barruan duten A-ren azpitaldeen eta $A/\mathfrak{a}$-ren azpitaldeen artean, $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ erregelaren bidez emanda. Beraz, nahikoa dugu frogatzea $\mathfrak{b}$ ideala dela baldin eta soilik baldin $\mathfrak{b}/\mathfrak{a}$ ideala bada, $\mathfrak{a} \subseteq \mathfrak{b}$ den baldintzapean. Hori erraz ikusten da 2.4 proposizioan oinarrituz.

(ii) Definitu

$$\begin{array}{rccc} \varphi & : & A/\mathfrak{a} & \longrightarrow & A/\mathfrak{b} \\ & & x + \mathfrak{a} & \longmapsto & x + \mathfrak{b} \end{array}$$

aplikazioa. Ohartu φ ondo definituta dagoela, $\mathfrak{a} \subseteq \mathfrak{b}$ izateagatik:

$$x + \mathfrak{a} = y + \mathfrak{a} \implies x - y \in \mathfrak{a} \implies x - y \in \mathfrak{b} \implies x + \mathfrak{b} = y + \mathfrak{b}.$$

Orduan, nabaria da φ homomorfismoa eta supraiektiboa dela, eta erraz ikus daiteke $\ker \varphi = \mathfrak{b}/\mathfrak{a}$ dela. Horrela, lehenengo isomorfismo-teorema aplikatuz,

$$\frac{A/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}} \cong \frac{A}{\mathfrak{b}}$$

isomorfismoa ondorioztatzen dugu.

(iii) Ikus dezagun ideal maximalen kasua, ideal lehenena guztiz era berean justifikatzen baita. Horretarako, 2.51 teoreman emandako karakterizazioa erabiliko

dugu, (ii) atalarekin eta 2.26 proposizioarekin batera:

$$\mathfrak{b}/\mathfrak{a}\ A/\mathfrak{a}\text{-ren ideal maximala} \iff \frac{A/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}} \text{ gorputza} \iff A/\mathfrak{b} \text{ gorputza}$$
$$\iff \mathfrak{b}\ A\text{-ren ideal maximala.}$$

□

Izan bedi $\mathfrak{a}$ A-ren ideala. Hartzen badugu $\mathfrak{b}$ A-ren beste ideal bat, $\mathfrak{a} \not\subseteq \mathfrak{b}$ izanik, egia da oraindik ere

$$I = \{x + \mathfrak{a} \mid x \in \mathfrak{b}\}$$

multzoa $A/\mathfrak{a}$ zatiduraren ideala dela. Ohiko akatsa da orduan $I = \mathfrak{b}/\mathfrak{a}$ moduan idaztea, konturatu gabe $\mathfrak{a}$ ez dagoela $\mathfrak{b}$-ren barruan. Ideal hori zatidura gisa idazteko modu zuzena

$$I = \frac{\mathfrak{a} + \mathfrak{b}}{\mathfrak{a}}$$

da. (Ohartu $\overline{a + x} = \overline{x}$ dela $a \in \mathfrak{a}$ bada.)

2.55. Adibideak. 1) Hauek dira $\mathbb{Z}/6\mathbb{Z}$-ren idealak: $\mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}\}$, $3\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{3}\}$ eta $6\mathbb{Z}/6\mathbb{Z} = \{\overline{0}\}$. Horietatik, $2\mathbb{Z}/6\mathbb{Z}$ eta $3\mathbb{Z}/6\mathbb{Z}$ maximalak eta lehenak dira.

2) Eman ditzagun $K[X]/(X^n)$ zatiduraren ideal lehenak. Korrespondentziaren teoremaren arabera, $\mathfrak{p}/(X^n)$ motakoak dira, $\mathfrak{p}$ $K[X]$-ren ideal lehena izanik, eta $(X^n) \subseteq \mathfrak{p}$ izanik. Beraz, $X^n \in \mathfrak{p}$ dugu eta, $\mathfrak{p}$ ideal lehena denez, $X \in \mathfrak{p}$ ondorioztatzen dugu. Horrela, $(X) \subseteq \mathfrak{p}$ partekotasuna dugu. Orain, badakigu (X) ideala $K[X]$-n maximala dela eta, hortik, $\mathfrak{p} = (X)$ lortzen dugu. Laburbilduz, $K[X]/(X^n)$ eraztunak ideal lehen bakarra du, eta beraz ideal maximal bakarra ere bai: $(X)/(X^n)$ alegia. (Hirugarren gaian, $K[X]$-ren ideal guztiak nagusiak direla jakingo dugu, eta azkarrago egingo dugu adibide hau. Are gehiago, zuzenean ondorioztatuko dugu $K[X]/(X^n)$-ren ideal guztiak $(X^m)/(X^n)$ modukoak direla, $0 \leq m \leq n$ izanik.)

Eman dezagun orain 2.51 teoremaren (i) ataleko baliokidetasuna frogatzeko ordezko argudioa. Badakigu, 2.13 proposizioaren arabera, eraztun ez-tribial bat gorputza dela baldin eta soilik baldin bere ideal bakarrak ideal tribiala eta eraztun osoa besterik ez badira. Emaitza hori korrespondentziaren teoremaren (i) atalarekin konbinatzen badugu, $A/\mathfrak{a}$ gorputza da baldin eta soilik baldin $\mathfrak{a}$ ideal propioa bada eta ez badago beste idealik $\mathfrak{a}$-ren eta A-ren artean, hau da, baldin eta soilik baldin $\mathfrak{a}$ A-ren ideal maximala bada.

2.4. Zatikien eraztunen idealak

Atal labur honetan zatikien eraztunen idealak deskribatzen ditugu. Ikusiko dugunez, emaitza bereziki ona da ideal lehenen kasuan.

2.56. Definizioa. Izan bitez A integritate-domeinua, S A-ren azpimultzo biderkakorra, eta $\mathfrak{a}$ A-ren ideala. Orduan,

$$S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a},\ s \in S \right\} \subseteq S^{-1}A$$

definitzen dugu.

Merezi du momentu batez gelditzea $S^{-1}\mathfrak{a}$ multzoaren definizioa behar bezala azaltzeko. Lehenengo gaian $S^{-1}A$ definitzean esan genuen bezala, kasu honetan ere ez da oro har egia a/b zatiki bat $S^{-1}\mathfrak{a}$-n egoteko derrigorrean $a \in \mathfrak{a}$ eta $b \in S$ bete behar denik, baizik eta elementu hori zatiki moduan dituen adierazpen guztietatik badagoela gutxienez aukera bat definizioko baldintzak betetzen dituena. Eman dezagun adibide bat: hartu $S^{-1}\mathbb{Z}$ zatikien eraztuna, $S = \{3^n \mid n \in \mathbb{N} \cup \{0\}\}$ izanik, eta $\mathfrak{a} = 6\mathbb{Z}$. Orduan, $10/15 \in S^{-1}\mathfrak{a}$ dugu, $10 \notin \mathfrak{a}$ eta $15 \notin S$ den arren. Izan ere, $10/15 = 6/9$ ere idatz daiteke, eta oraingo honetan $6 \in \mathfrak{a}$ eta $9 \in S$. Ohartu elementua zatiki laburtezin modura idazten badugu, oraindik ere ez dituela $S^{-1}\mathfrak{a}$-n egoteko baldintzak betetzen kasu honetan: $10/15 = 2/3$ dugu, baina $2 \notin \mathfrak{a}$. Beraz, oso inportantea da ez ibiltzea arinegi zatiki bat $S^{-1}\mathfrak{a}$ bezalako multzo batean dagoen edo ez erabakitzeko.

2.57. Proposizioa. *Izan bitez A integritate-domeinua, S A-ren azpimultzo biderkakorra, eta $\mathfrak{a}$ A-ren ideala. Orduan, $S^{-1}\mathfrak{a}$ $S^{-1}A$-ren ideala da, eta $S^{-1}\mathfrak{a} = S^{-1}A$ berdintza dugu baldin eta soilik baldin $\mathfrak{a} \cap S \neq \varnothing$ bada.*

Froga. Oso erraz egiaztatzen da $S^{-1}\mathfrak{a}$ $S^{-1}A$-ren azpieraztuna dela. Ikus dezagun $S^{-1}A$ zatikien eraztun osoaren berdina dela baldin eta soilik baldin $\mathfrak{a} \cap S \neq \varnothing$ bada. Demagun $S^{-1}\mathfrak{a} = S^{-1}A$ dela. Orduan, $1 \in S^{-1}\mathfrak{a}$ dugu, eta existitzen dira $a \in \mathfrak{a}$ eta $s \in S$ non $1 = a/s$ baita. Ondorioz, $a = s$ eta $\mathfrak{a} \cap S \neq \varnothing$ dugu. Alderantziz, x elementu bat $\mathfrak{a}$-n eta S-n badago, orduan $1 = x/x \in S^{-1}\mathfrak{a}$ dugu, eta $S^{-1}\mathfrak{a} = S^{-1}A$. □

Hurrengo teoremak dioenez, $S^{-1}A$-ren ideal guztiak $S^{-1}\mathfrak{a}$ motakoak dira.

2.58. Teorema. *Izan bitez A integritate-domeinua eta S A-ren azpimultzo biderkakorra. Orduan:*

(i) *$S^{-1}A$-ren ideal guztiak $S^{-1}\mathfrak{a}$ modukoak dira, A-ren $\mathfrak{a}$ idealen batentzat (ez derrigorrean bakarra).*

(ii) *Ideal lehenetara mugatzen bagara, orduan*

$$\begin{array}{ccc} \{S \text{ ebakitzen ez duten } A\text{-ren ideal lehenak}\} & \longmapsto & \{S^{-1}A\text{-ren ideal lehenak}\} \\ \mathfrak{p} & \longrightarrow & S^{-1}\mathfrak{p} \end{array}$$

aplikazioa bijektiboa da.

Froga. (i) Izan bedi $\mathfrak{A}$ $S^{-1}A$-ren ideala, eta jarri $\mathfrak{a} = \mathfrak{A} \cap A$. Berehala egiaztatzen da $\mathfrak{a}$ A-ren ideala dela. Ikus dezagun $S^{-1}\mathfrak{a} = \mathfrak{A}$ dela. Alde batetik, $a \in \mathfrak{a}$ eta $s \in S$

bada, orduan

$$\frac{a}{s} = \frac{1}{s} \cdot a \in \mathfrak{A}$$

dugu, eta horrek $S^{-1}\mathfrak{a} \subseteq \mathfrak{A}$ dela frogatzen du. Alderantzizko partekotasuna ikusteko, hartu $a/s \in \mathfrak{A}$, non $s \in S$ baita. Orduan,

$$a = s \cdot \frac{a}{s} \in \mathfrak{A}$$

dugu, eta beraz, $a \in \mathfrak{a}$. Ondorioz, $a/s \in S^{-1}\mathfrak{a}$ dugu eta frogaturik gelditzen da $\mathfrak{A} \subseteq S^{-1}\mathfrak{a}$ partekotasuna.

(ii) Dei diezaiogun Φ enuntziatuko aplikazioari. Hasteko, ikus dezagun Φ-k benetan $S^{-1}A$-ren ideal lehenen multzoan hartzen dituela irudiak. Beraz, $\mathfrak{p}$ A-ren ideal lehena bada, $\mathfrak{p} \cap S = \varnothing$ izanik, $S^{-1}\mathfrak{p}$ $S^{-1}A$-ren ideal lehena dela ikusiko dugu. Alde batetik, 2.57 proposizioaren arabera, $S^{-1}\mathfrak{p}$ ideal propioa da. Orain, demagun

$$\frac{x}{s} \cdot \frac{x'}{s'} = \frac{x''}{s''} \in S^{-1}\mathfrak{p}$$

dela, $s, s', s'' \in S$ eta $x'' \in \mathfrak{p}$ izanik. Orduan, $xx's'' = x''ss' \in \mathfrak{p}$. Orain, $\mathfrak{p}$ A-ren ideal lehena da, eta $s'' \notin \mathfrak{p}$ dugu, $\mathfrak{p} \cap S = \varnothing$ baita. Beraz, $x \in \mathfrak{p}$ edo $x' \in \mathfrak{p}$ dugu, eta hemendik, $x/s \in S^{-1}\mathfrak{p}$ edo $x'/s' \in S^{-1}\mathfrak{p}$. Horrenbestez, frogaturik gelditzen da $S^{-1}\mathfrak{p}$ $S^{-1}A$-ren ideal lehena dela.

Erraz ikus dezakegu Φ supraiektiboa dela. Izan ere, $\mathfrak{P}$ $S^{-1}A$-ren ideal lehena bada, jar dezagun $\mathfrak{p} = \mathfrak{P} \cap A$. Orduan, (i) atalean frogatu den bezala, $\Phi(\mathfrak{p}) = \mathfrak{P}$ dugu.

Azkenik, ikus dezagun Φ injektiboa dela. Baldin eta $S^{-1}\mathfrak{p}_1 = S^{-1}\mathfrak{p}_2$ bada, $\mathfrak{p}_1$ eta $\mathfrak{p}_2$ A-ren ideal lehenak izanik eta $\mathfrak{p}_1 \cap S = \mathfrak{p}_2 \cap S = \varnothing$ izanik, orduan $\mathfrak{p}_1 = \mathfrak{p}_2$ dela frogatu behar dugu. Horretarako, nahikoa da emaitza hau frogatzea: $\mathfrak{p}$ A-ren ideal lehena bada eta $\mathfrak{p} \cap S = \varnothing$ bada, orduan $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$ dela. Ohartu $\supseteq$ partekotasuna tribiala dela. Alderantzizko partekotasuna ikusteko, izan bedi $a \in S^{-1}\mathfrak{p} \cap A$. Orduan, $a = x/s$ idatz dezakegu, $x \in \mathfrak{p}$ eta $s \in S$ izanik. Beraz, $as = x \in \mathfrak{p}$ dugu eta, $\mathfrak{p}$ A-ren ideal lehena denez eta $s \notin \mathfrak{p}$ denez, nahitaez $a \in \mathfrak{p}$. Horrela, bigarren partekotasuna lortzen dugu. □

Ez bagara ideal lehenetara mugatzen, $\mathfrak{a} \longmapsto S^{-1}\mathfrak{a}$ aplikazioak ez du zertan injektiboa izan, nahiz eta S ebakitzen ez duten idealak baino ez hartu. Eman dezagun adibide bat: hartu $S^{-1}\mathbb{Z}$ zatikien eraztuna, $S = \{3^n \mid n \in \mathbb{N} \cup \{0\}\}$ izanik. Orduan, $\mathfrak{a} = 6\mathbb{Z}$ idealak ez du S ebakitzen, eta

$$S^{-1}\mathfrak{a} = \left\{ \frac{6k}{3^n} \mid k \in \mathbb{Z},\ n \in \mathbb{N} \cup \{0\} \right\} = \left\{ \frac{2\ell}{3^n} \mid \ell \in \mathbb{Z},\ n \in \mathbb{N} \cup \{0\} \right\}$$

dugu. Beraz, $\mathfrak{b} = 2\mathbb{Z}$ bada (horrek ere ez du S ebakitzen), orduan $S^{-1}\mathfrak{a} = S^{-1}\mathfrak{b}$ dugu.

Egokiro ulertu behar da aurreko teoremaren (ii) atalaren esanahia. Ez du esaten $S^{-1}\mathfrak{a}$ ideal lehena denean $\mathfrak{a}$ idealak S ebakitzen ez duen A-ren ideal lehena izan behar duenik. Egia da $\mathfrak{a}$-k ez duela S ebakiko: bestela $S^{-1}\mathfrak{a} = S^{-1}A$ izango genuke eta ez litzateke $S^{-1}A$-ren ideal lehena izango. Baina ezin dugu ziurtatu $\mathfrak{a}$ lehena denik. Teoremak dioena da $\mathfrak{p}$ ideal lehen bat (zehazkiago, bakar bat)

aurki dezakegula A-n, S ebakitzen ez duena, eta $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{a}$ betetzen duena. Badaukagu egoera horren adibide bat dagoeneko emanda: aurreko arrisku-oharrean $S^{-1}\mathfrak{a} = S^{-1}\mathfrak{b}$ berdintza dugu, eta $\mathfrak{b} = 2\mathbb{Z}$ lehena bada ere (eta, beraz, $S^{-1}\mathfrak{b}$ ere lehena da, 2.58 teoremaren arabera), $\mathfrak{a} = 6\mathbb{Z}$ ez da lehena.

Aurreko teorema bereziki interesgarria da lokalizatuak deitzen diren zatikien eraztunetarako. Lehenengo eta behin, eman dezagun lokalizatuen definizioa, lema begi-bistako honetan oinarritzen dena.

2.59. Lema. *Izan bitez A integritate-domeinua eta $\mathfrak{p}$ A-ren ideal lehena. Orduan, $A \setminus \mathfrak{p}$ multzoa biderkakorra da.*

2.60. Definizioa. Izan bitez A integritate-domeinua eta $\mathfrak{p}$ A-ren ideal lehena. Orduan, A-ren *lokalizatua* $\mathfrak{p}$ idealarekiko, $A_{\mathfrak{p}}$ ikurraz adierazten dena, $A \setminus \mathfrak{p}$ azpimultzo biderkakorrari dagokion zatikien eraztuna da. Hau da,

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} \mid a, b \in A,\ b \notin \mathfrak{p} \right\}.$$

Ideal lehen batekiko lokalizatua egiten dugunean, ideal horrekiko *lokalizatzen dugula* ere esaten da.

2.61. Adibidea. Zenbaki osoen kasuan, (2) ideal lehena denez, horrekiko lokaliza dezakegu, eta

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \text{ bakoitia} \right\}$$

dugu.

Lokalizatuen kasuan, ohikoa da $\mathfrak{a}A_{\mathfrak{p}}$ idaztea $S^{-1}\mathfrak{a}$-ren ordez ($S = A \setminus \mathfrak{p}$ izanik, jakina). Beraz,

$$\mathfrak{a}A_{\mathfrak{p}} = \left\{ \frac{a}{b} \mid a \in \mathfrak{a},\ b \notin \mathfrak{p} \right\}.$$

2.62. Korolarioa. *Izan bitez A integritate-domeinua eta $\mathfrak{p}$ A-ren ideal lehena. Orduan,*

$$\mathfrak{q} \longrightarrow \mathfrak{q}A_{\mathfrak{p}}$$

bikjekzioa dugu $\mathfrak{p}$-ren barruan dauden ideal lehenen eta $A_{\mathfrak{p}}$-ren ideal lehenen artean. Ondorioz, $A_{\mathfrak{p}}$-k ideal maximal bakarra du, $\mathfrak{p}A_{\mathfrak{p}}$ alegia.

Froga. Aurreko teoremaren ondorio berehalakoa da: ohartu $A \setminus \mathfrak{p}$ azpimultzo biderkakorra ebakitzen ez duten ideal lehenak $\mathfrak{p}$-ren barruan daudenak direla. □

2.63. Oharra. Eraztun bat *lokala* dela esaten da ideal maximal bakarra duenean. Beraz, azken korolarioaren arabera, $A_{\mathfrak{p}}$ motako eraztun guztiak lokalak dira. Hortik dator "lokalizatuaren" izena ematea.

2.64. Adibidea. $\mathbb{Z}_{(2)}$-ren ideal lehen bakarrak $\{0\}$ eta

$$(2)\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a \in (2),\ b \text{ bakoitia} \right\} = \left\{ \frac{2k}{b} \mid k \in \mathbb{Z},\ b \text{ bakoitia} \right\}$$

dira, $\{0\}$ eta (2) baitira (2)-ren barruan dauden $\mathbb{Z}$-ren ideal lehen bakarrak. Ohartu azken ideal hori (2) gisa jar daitekeela $\mathbb{Z}_{(2)}$-ren barruan, haren elementuak $2x$ motakoak baitira, $x \in \mathbb{Z}_{(2)}$ izanik. Bestalde, $\mathbb{Z}_{(2)}$ lokalizatuari 2.58 teoremaren (i) atala aplikatzen badiogu, orduan haren ideal guztiak $\mathfrak{a}\mathbb{Z}_{(2)}$ motakoak direla lortzen dugu, $\mathfrak{a} \subseteq (2)$ $\mathbb{Z}$-ren ideala izanik. Jar dezagun $\mathfrak{a} = (a)$, $a \in \mathbb{Z}$ izanik. Orduan, ideal lehenen kasuan bezala, $\mathfrak{a}\mathbb{Z}_{(2)} = (a)$ dugu (sortutako ideal hori $\mathbb{Z}_{(2)}$-n ulertuta). Idatz dezagun $a = 2^n k$ moduan, $n \in \mathbb{N} \cup \{0\}$ eta k bakoitia izanik, eta ohartu k unitatea dela $\mathbb{Z}_{(2)}$-n, $1/k \in \mathbb{Z}_{(2)}$ baita. Ondorioz, $\mathfrak{a}\mathbb{Z}_{(2)} = (2^n)$ dugu, eta hauek dira $\mathbb{Z}_{(2)}$-ren ideal guztiak:

$$(2^n) = \left\{ \frac{a}{b} \mid a \text{ } 2^n\text{-ren multiploa},\ b \text{ bakoitia} \right\},$$

non $n \in \mathbb{N} \cup \{0\}$. Garbi dago ideal horiek guztiak desberdinak direla n-ren balio desberdinetarako, eta kate beherakor bat osatzen dutela:

$$\mathbb{Z}_{(2)} \supsetneq (2) \supsetneq (2^2) \supsetneq \cdots \supsetneq (2^n) \supsetneq \cdots .$$