1

Eraztunei buruzko orokortasunak

1.1. Eraztunak

Aljebra trukakorra izeneko alorra identitatedun eraztun trukakorraren kontzeptuaren inguruan antolaturik dago. Eraztun batek bi eragiketa ditu, eta eragiketa horiek propietate batzuk bete behar dituzte. Zorionez, propietate horiek ezagunak zaizkigu, txikitatik zenbakiekin erabili ditugun berberak baitira.

1.1. Definizioa. Izan bitez A multzoa eta $+$ eta $\cdot$ A-ren gainean definiturik dauden bi eragiketa. Orduan, $(A, +, \cdot)$ *eraztuna* dela diogu propietate hauek betetzen badira:

(i) $(A, +)$ talde trukakorra da.
(ii) Biderketa elkarkorra da.
(iii) Banatze-propietateak betetzen dira: $a(b+c) = ab+ac$ eta $(b+c)a = ba+ca$ dugu $a, b, c \in A$ guztietarako.

1.2. Definizioa. Izan bedi A eraztuna. Orduan:

(i) A *trukakorra* dela diogu biderketa trukakorra bada.
(ii) A *identitateduna* dela diogu biderketak elementu neutroa badu, eta elementu horri A-ren *identitatea* deitzen zaio.

1.3. Definizioa. Izan bedi A identitatedun eraztuna. Orduan, $a \in A$ elementuak alderantzizkoa baldin badu biderketarekiko, A-ren *unitatea* dela diogu.

Eraztun batean, batuketarekiko neutroa bakarra da (taldeetan hala gertatzen baita), eta 0 ikurraren bitartez adierazten dugu. Ohikoa da elementu horri *elementu nulu* deitzea. Era berean, eraztuna identitateduna bada, orduan identitatea ere bakarra da, eta 1 ikurra erabiltzen dugu hori adierazteko. Berez, $0 = 1$ gerta liteke baina, beranduago ikusiko dugunez, eraztun gehienetan $0 \neq 1$ dugu. Bestalde, $a \in A$ elementu baten alderantzizkoa batuketarekiko bakarra da eta $-a$ deitzen diogu. Era berean, a unitatea bada, orduan biderketarekiko duen alderantzizkoa bakarra da, eta a^{-1} gisa idazten dugu.

1.4. Adibideak. 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ eta $\mathbb{C}$ eraztunak dira ohiko batuketarekiko eta biderketarekiko, are gehiago identitatedunak eta trukakorrak dira. Bestalde, $\mathbb{N}$ ez da eraztuna, ez baita egia elementu guztiek batuketarekiko alderantzizkoa dutenik.

2) Izan bedi $n \in \mathbb{N}$ zenbaki finkoa. Orduan, $\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}$ identitatedun eraztun trukakorra da,

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \text{eta} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

eragiketekiko. Gogoratu $\overline{a} = \overline{b}$ dela baldin eta soilik baldin $a \equiv b \pmod{n}$ bada. Bereziki, $\overline{a} = \overline{0}$ dugu zehatz-mehatz a n-ren multiploa denean. Gainera, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ dugu, errepikapenik gabe.

3) Berriro ere $n \in \mathbb{N}$ zenbaki finkoa bada, orduan $n\mathbb{Z}$ eraztun trukakorra da. Hala ere, ez da identitateduna $n \geq 2$ bada.

4) Izan bedi $A = \{\overline{0}, \overline{3}\} \subseteq \mathbb{Z}/6\mathbb{Z}$. Orduan, $\overline{0}+\overline{0} = \overline{3}+\overline{3} = \overline{0}$, $\overline{0}+\overline{3} = \overline{3}+\overline{0} = \overline{3}$, $\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{3} = \overline{3} \cdot \overline{0} = \overline{0}$ eta $\overline{3} \cdot \overline{3} = \overline{3}$ denez, A identitatedun eraztun trukakorra da, identitatea $\overline{3}$ izanik.

5) $M_n(\mathbb{R})$ identitatedun eraztuna da matrizeen ohiko batuketarekiko eta biderketarekiko, baina ez da trukakorra $n \geq 2$ bada.

6) Eraztunik sinpleena $A = \{0\}$ multzoa da, $0 + 0 = 0$ eta $0 \cdot 0 = 0$ eragiketez hornitua. Horri *eraztun tribial* deitzen zaio. Identitatedun eraztun trukakorra da, eta kasu honetan $0 = 1$ berdintza betetzen da.

7) Eraztunen adibide nagusi bat polinomioen eraztunak dira. Izan bitez A eraztuna eta X indeterminatua. Orduan, X indeterminatua erabiltzen duten eta koefizienteak A-ren gainean dituzten polinomioen multzoa $A[X]$ ikurraren bidez adierazten dugu. Honelakoak dira $A[X]$-ren elementuak:

$$f(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n,$$

non $n \in \mathbb{N} \cup \{0\}$ baita eta $a_i \in A$ baita $i = 0, \ldots, n$ guztietarako. Bestela,

$$f(X) = \sum_{i \geq 0} a_i X^i$$

moduan ere idatz ditzakegu polinomioak, $a_i \in A$ koefiziente guztiak, kopuru finitu bat izan ezik, 0 diren baldintzapean. Idazkera hori erabiliz, gogoraraz dezagun nola dauden definituta $f(X) = \sum_{i \geq 0} a_i X^i$ eta $g(X) = \sum_{i \geq 0} b_i X^i$ bi polinomioren batura eta biderkadura:

$$f(X) + g(X) = \sum_{i \geq 0} (a_i + b_i) X^i$$

eta

$$f(X) \cdot g(X) = \sum_{i \geq 0} \Big(\sum_{j+k=i} a_j b_k \Big) X^i.$$

Erraz ikusten da $A[X]$ eraztuna dela eragiketa horiekiko (A eraztuna izateagatik), eta $A[X]$ identitatedun edo trukakorra dela A identitatedun edo trukakorra den arabera. Ohartu A $A[X]$-ren azpimultzoa dela; $A[X]$-ren barruan, A-ko elementuei *konstante* deituko diegu.

8) Oro har, $X_1, \ldots, X_n$ indeterminatuak badira, orduan $A[X_1, \ldots, X_n]$ ikurraz adierazten dugu indeterminatu horiek erabiltzen dituzten eta koefizienteak A-n dituzten polinomioen eraztuna. Kasu honetan, $A[X_1, \ldots, X_n]$-ren polinomio orokor bat honela idatz daiteke:

$$f(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}, \tag{1.1}$$

$a_{i_1,\ldots,i_n} \in A$ koefiziente guztiak 0 izanik, kopuru finitu bat izan ezik. Indeterminatuen arteko biderkadurei, hau da, $X_1^{i_1} \ldots X_n^{i_n}$ moduko adierezpenei *monomio* deitzen zaie. Orduan, (1.1) berdintzak dio $A[X_1, \ldots, X_n]$-ren polinomioak monomioen "konbinazio linealak" direla, koefizienteak A-n izanik. Kontuan izan 1 identitatea ere monomio bat dela, $i_1 = \cdots = i_n = 0$ berretzaileak aukeratuz lortzen dena, hain zuzen ere. Monomio horri dagokion batugaiari, hau da, $a_{0,\ldots,0}$ elementuari, f-ren *gai askea* deitzen zaio, hori baita f polinomioan indeterminaturik gabeko batugai bakarra. Orain, demagun

$$g(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} b_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$$

beste polinomio bat dela. Orduan, erraz deskriba ditzakegu $f + g$ batura eta fg biderkadura monomioen bidez:

(i) Batuketa egiteko, monomio bakoitzak bi polinomioetan dituen koefizienteak batzen dira:

$$(f+g)(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} (a_{i_1, \ldots, i_n} + b_{i_1, \ldots, i_n}) X_1^{i_1} \ldots X_n^{i_n}.$$

Beraz, batuketa "osagaiz osagai" egiten dela esan genezake.

(ii) Biderkadura lortzeko, lehenengo eta behin monomioak biderkatzeko modua definitzen dugu:

$$X_1^{i_1} \ldots X_n^{i_n} \cdot X_1^{j_1} \ldots X_n^{j_n} = X_1^{i_1 + j_1} \ldots X_n^{i_n + j_n},$$

eta orduan polinomioak biderkatzeko banatze-propietatearekin bezala jokatzen dugu:

$$(fg)(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} \Big(\sum_{\substack{j_1 + k_1 = i_1, \ldots, \\ j_n + k_n = i_n}} a_{j_1, \ldots, j_n} b_{k_1, \ldots, k_n} \Big) X_1^{i_1} \ldots X_n^{i_n}.$$

9) Polinomioen eraztunak infinitu indeterminaturekin ere defini daitezke; egia esan, edozein multzo erabil daiteke indeterminatuak indexatzeko. Izan bedi I multzo bat, eta har ditzagun $\{X_i \mid i \in I\}$ indeterminatuak, I multzoarekin indexaturik. Orduan, indeterminatu horiekin biderkadura *finituak* eginez, monomiak sor ditzakegu. Zehazkiago, $J \subseteq I$ finitua aukeratzen badugu, eta $\{i_j \mid j \in J\}$ zenbaki oso ez-negatiboak hartzen baditugu, orduan

$$\prod_{j \in J} X_j^{i_j}$$

monomioa eraikitzen dugu (indeterminatuak zein ordenatan biderkatzen diren ez dio axola, hau da, indeterminatuak elkarrekin trukatzen direla ulertzen dugu).

Orain, A eraztuna bada, $A[X_i \mid i \in I]$ polinomioen eraztuna defini dezakegu. Horren elementuak monomioen konbinazio lineal *finituak* dira, koefizienteak A-n izanik. Hortaz, hau da $A[X_i \mid i \in I]$ eraztuneko polinomio orokor baten itxura:

$$\sum_{\substack{J \subseteq I \\ J \text{ finitua}}} a_J \prod_{j \in J} X_j,$$

non $a_J \in A$ koefiziente guztiak zero baitira, kopuru finitu bat izan ezik. Polinomio horiek biderkatzeko, aurreko ataleko erregelak erabiltzen dira: batuketa "osagaiz osagai" egiten da, eta biderkadura lortzeko, banatze-propietatea aplikatzen da eta monomioak modu naturalean biderkatzen dira (pentsatu nola eman formula bat horretarako).

10) Izan bitez A eta B eraztunak. Orduan, $A \times B$ biderkadura cartesiarra ere eraztuna da, batuketa eta biderketa osagaiz osagai definitzen baditugu. Gainera, $A \times B$ trukakorra da baldin eta soilik baldin A eta B trukakorrak badira, eta identitateduna da baldin eta soilik baldin A eta B identitatedunak badira. Zehazkiago, $A \times B$-ren identitatea $(1, 1)$ bikotea da, lehenengo 1-a A-ren identitatea eta bigarrena B-ren identitatea izanik. Antzera, $A_1, \ldots, A_n$ eraztunak badira, orduan

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ da } i = 1, \ldots, n \text{ guztietarako}\}$$

biderkadura cartesiarra ere eraztuna da.

11) Oro har, $\{A_i\}_{i \in I}$ eraztun-familia bat bada, I indize-multzoa edozein izanik, orduan $\prod_{i \in I} A_i$ biderkadura cartesiarra ere eraztuna da osagaiz osagaiko eragiketekin. Gogoratu biderkadura horretako elementuak $(a_i)_{i \in I}$ moduko tuplak direla, $a_i \in A_i$ izanik $i \in I$ guztietarako. Elementu horiek ulertzeko beste modu bat hau da: $f : I \longrightarrow \cup_{i \in I} A_i$ moduko funtzioak dira, non $f(i) \in A_i$ baita $i \in I$ guztietarako. Baldin eta A_i guztiak A eraztun bera badira, orduan biderkadura cartesiar hori adierazteko A^I ikurra erabiltzen dugu. Adibidez, $\mathbb{R}^{\mathbb{N}}$ biderkadura cartesiarra zenbaki errealen segida guztien multzoa da, eraztuna dena osagaiz osagai egiten badira eragiketak.

1.5. Oharra. Polinomioen eraztun batean indeterminatu bat baino gehiago badugu, ohikoa da indeterminatuetako bati rol nagusia ematea eta besteak konstantetzat hartzea. Horrela, eraztun hori indeterminatu bakarreko polinomioen eraztun gisa ikustea lortzen dugu. Adibidez, $A[X, Y]$ eraztuna $A[X][Y]$ moduan zein $A[Y][X]$ moduan ikus dezakegu, komeni zaigun bezala.

Hemendik aurrera identitatedun eraztun trukakorrak baino ez zaizkigu interesatuko. Horregatik, "eraztun" esaten dugunean, automatikoki trukakorra eta identitateduna dela ulertuko dugu.

1.6. Oharra. Eraztuna trukakorra bada, 1.1 definizioko (iii) baldintza ahuldu daiteke, eta nahikoa da banatze-propietateetako bat eskatzea, bata bestearen ondorioa baita.

Une honetan, komenigarria da ondorengo notazioa finkatzea. Ohartu bat datorrela zenbakiekin lan egiterakoan normalean erabiltzen dugun notazioarekin.

1.7. Notazioa. Izan bitez A eraztuna eta $a \in A$. Orduan:

(i) $n \in \mathbb{Z}$ bada, $na \in A$ elementua honela definitzen dugu:

$$na = \begin{cases} \overbrace{a + \cdots + a}^{n}, & n > 0 \text{ bada}, \\ 0, & n = 0 \text{ bada}, \\ \overbrace{(-a) + \cdots + (-a)}^{-n}, & n < 0 \text{ bada}. \end{cases}$$

(ii) $n \in \mathbb{N} \cup \{0\}$ bada, $a^n \in A$ elementua honela definitzen dugu:

$$a^n = \begin{cases} \overbrace{a \cdot \ldots \cdot a}^{n}, & n > 0 \text{ bada}, \\ 1, & n = 0 \text{ bada}. \end{cases}$$

(iii) a A-ren unitatea bada, orduan a^n berretura $n \in \mathbb{Z}$ negatiboa denean ere definitzen da, honako modu honetan:

$$a^n = \overbrace{(a^{-1}) \cdot \ldots \cdot (a^{-1})}^{-n}.$$

Notazio horrek ohiko formula guztiak betetzen ditu. Adibidez:

(i) $ma + na = (m+n)a$, $m(na) = (mn)a$, $n(a+b) = na + nb$ eta $n(ab) = (na)b = a(nb)$ dugu, $m, n \in \mathbb{Z}$ eta $a, b \in A$ guztietarako.

(ii) $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ eta $(ab)^n = a^n b^n$ dugu, $m, n \in \mathbb{N} \cup \{0\}$ eta $a, b \in A$ guztietarako.

(iii) Newtonen binomioaren formula betetzen da, hots,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

dugu, $n \in \mathbb{N}$ eta $a, b \in A$ guztietarako.

Kontuan izan na ez dela ulertu behar, oro har, n-ren eta a-ren biderkadura balitz bezala, A eraztunaren barruan. Izan ere, n zenbaki osoa da, eta $\mathbb{Z}$-k (ezta $\mathbb{Z}$-ren kopia batek ere) ez du zertan A-ren barruan egon. Badago, hala ere, na elementua A-ko bi elementuren biderkadura gisa jartzeko modu bat:

$$na = n(1 \cdot a) = n1 \cdot a,$$

eta orain bai $n1$ bai a A-ko elementuak dira. (Hemen 1 A-ren identitatea da.)

Hurrengo teoreman eraztunaren definizioko axiomen ondorio batzuk ateratzen ditugu. Ikusten denez, zenbaki errealekin lan egitean ezagunak ditugun propietate batzuk edozein eraztunetan betetzen dira.

1.8. Teorema. *Izan bedi A eraztuna. Orduan, berdintza hauek betetzen dira $a, b, c \in A$ guztietarako:*

(i) $a \cdot 0 = 0$.

(ii) $(-a)b = a(-b) = -ab$.

(iii) $(-a)(-b) = ab$.
(iv) $a(b-c) = ab - ac$.

FROGA. Frogatu dezagun (i); beste atalak irakurleari utziko dizkiogu. Ohartu

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

dugula, 0 batuketarekiko neutroa dela eta banatze-propietatea erabiliz. Orain, $(A, +)$ taldea denez, elementu guztiak sinplifikagarriak dira $+$-ekiko. Orduan, goiko berdintzan $a \cdot 0$ sinplifikatuz, $a \cdot 0 = 0$ lortzen dugu. □

Hala ere, $a \cdot b = 0$ baldintzatik ezin da ondorioztatu $a = 0$ edo $b = 0$ denik. Adibidez, $\mathbb{Z}/6\mathbb{Z}$ eraztunean $\overline{2} \cdot \overline{3} = \overline{0}$ dugu, baina $\overline{2} \neq \overline{0}$ eta $\overline{3} \neq \overline{0}$. Aurrerago, 1.3 atalean, lasaiago hitz egingo dugu fenomeno horretaz.

1.9. Proposizioa. *Demagun A eraztuna ez dela tribiala. Orduan, $1 \neq 0$ dugu.*

FROGA. Izan ere, $1 = 0$ balitz, orduan $a \in A$ guztietarako $a = a \cdot 1 = a \cdot 0 = 0$ izango genuke. Hori kontraesana da, $A \neq \{0\}$ baita. □

1.10. Korolarioa. *Demagun A eraztuna ez dela tribiala. Orduan, 0 elementua ez da unitatea.*

FROGA. Ohartu $a \cdot 0 = 0 \neq 1$ betetzen dela $a \in A$ guztietarako, aurreko bi emaitzak erabiliz. □

1.11. Teorema. *Demagun A eraztuna dela. Orduan, A-ren unitateek talde bat osatzen dute biderketarekiko. Hori adierazteko $A^\times$ edo $\mathcal{U}(A)$ idatziko dugu.*

FROGA. Hasteko, ohartu biderketa eragiketa dela $A^\times$ multzoan. Izan ere, $a, b \in A^\times$ bada, orduan existitzen dira $x, y \in A$ non $ax = by = 1$ baita. Ondorioz, $(ab)(yx) = 1$ eta $ab \in A^\times$, nahi bezala. Orain, eraztun baten biderketa elkarkorra denez, bakarrik frogatu behar dugu $A^\times$-en neutroa dagoela biderketarekiko eta $a \in A^\times$ elementu baten alderantzizkoa berriro ere $A^\times$-en dagoela. Bi propietate horiek begi-bistakoak dira. □

Ondoren, unitateen beste ezaugarri garrantzitsu bat emango dugu.

1.12. Proposizioa. *Izan bitez A eraztuna eta $u \in A^\times$. Orduan, u sinplifikagarria da biderketarekiko, hau da, $ua = ub$ berdintza badugu, $a, b \in A$ izanik, $a = b$ dela ondorioztatzen da.*

FROGA. Nahikoa da $ua = ub$ berdintza u^{-1} alderantzizkoaz biderkatzea. □

1.13. Adibideak. 1) $\mathbb{Z}^\times = \{1, -1\}$ eta $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid (a, n) = 1\}$ dugu.
2) $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ eta $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ dugu.

3) $\mathcal{U}(\mathbb{R}[X]) = \mathbb{R} \setminus \{0\}$ dugu eta, oro har, $\mathcal{U}(\mathbb{R}[X_1, \ldots, X_n]) = \mathbb{R} \setminus \{0\}$. Izan ere, konstantea ez den polinomio erreal bat beste edozein polinomioz biderkatzean ezin dugu 1 konstantea lortu. Ikusita zer gertatzen den $\mathbb{R}$-ren kasuan, pentsa genezake $\mathcal{U}(A[X]) = \mathcal{U}(A)$ berdintza beteko dela A eraztun guztietarako, baina hori ez da beti egia. Adibidez, $\overline{2}X + \overline{1} \in \mathbb{Z}/4\mathbb{Z}[X]$ polinomioa unitatea da, bere buruaren alderantzizkoa baita. Aurrerago, 1.37 teoreman, A eraztunaren gaineko baldintza nahiko bat emango dugu, $\mathcal{U}(A[X]) = \mathcal{U}(A)$ berdintza ziurtatzeko.

1.2. Azpieraztunak

1.14. Definizioa. Izan bitez A eraztuna eta $B \subseteq A$. Betetzen bada B ere eraztuna dela A-ren eragiketekiko, eta B-ren identitatea A-ren identitatearekin bat badator, orduan B A-ren *azpieraztuna* dela esango dugu.

1.15. Adibideak. 1) Edozein eraztun bere buruaren azpieraztuna da.

2) $\mathbb{Z}$ $\mathbb{Q}$-ren azpieraztuna da, eta $\mathbb{Q}$, berriz, $\mathbb{C}$-ren azpieraztuna da.

3) Baldin eta $n \in \mathbb{N}$ eta $n \geq 2$ bada, $n\mathbb{Z}$ ez da $\mathbb{Z}$-ren azpieraztuna, ez baitu identitaterik. Egia esan, $\mathbb{Z}$-ren azpieraztun bakarra $\mathbb{Z}$ bera da. Izan ere, B $\mathbb{Z}$-ren azpieraztuna bada, orduan $0 \in B$ eta $1 \in B$ dugu. Orain, B eraztuna izateagatik, $-1 \in B$ ere izan behar du. Ondorioz, $n = 1 + \overset{n}{\cdots} + 1 \in B$ eta $-n = (-1) + \overset{n}{\cdots} + (-1) \in B$ dugu $n \in \mathbb{N}$ guztietarako. Horrenbestez, $B = \mathbb{Z}$ frogatu dugu. Argudio horrek berak frogatzen du $\mathbb{Z} \subseteq B$ partekotasuna betetzen dela $\mathbb{C}$-ren azpieraztuna den edozein B-rentzat. Beraz, $\mathbb{Z}$ $\mathbb{C}$-ren azpieraztunik txikiena da.

4) A eraztuna bada, orduan A $A[X]$-ren azpieraztuna da eta $A[X]$ $A[X, Y]$-ren azpieraztuna da.

5) A eraztun ez-tribiala bada, $B = \{0\}$ eraztun tribiala A-ren barruan dago, baina ez da A-ren azpieraztuna: kontuan izan B-ren identitatea eta A-rena ez datozela bat. Hori dela eta, ez da hitz egiten eraztun baten azpieraztun tribialari buruz, talde baten azpitalde tribialaren kasuan ez bezala.

6) A eraztun ez-tribiala bada, orduan $A \times \{0\}$ ez da $A \times A$-ren azpieraztuna, nahiz eta eraztuna izan $A \times A$-ren eragiketekiko. Arrazoia da $A \times \{0\}$-ren identitatea $(1, 0)$ dela eta $A \times A$-rena, berriz, $(1, 1)$.

7) $B = \{\overline{0}, \overline{3}\}$ eraztuna ez da $\mathbb{Z}/6\mathbb{Z}$-ren azpieraztuna, identitate desberdinak dituztelako. Egia esan, 3) atalean bezala argudiatuz, $\mathbb{Z}/n\mathbb{Z}$-ren azpieraztun bakarra $\mathbb{Z}/n\mathbb{Z}$ bera dela ikus daiteke.

Jarraian, eraztun baten azpimultzo bat azpieraztuna den edo ez erabakitzeko irizpide azkar bat ematen dugu.

1.16. Teorema. *Izan bitez A eraztuna eta $B \subseteq A$. Orduan, B A-ren azpieraztuna da baldin eta soilik baldin hiru propietate hauek betetzen badira:*

(i) *$x, y \in B$ bada, orduan $x - y \in B$.*
(ii) *$x, y \in B$ bada, orduan $x \cdot y \in B$.*
(iii) *$1 \in B$.*

FROGA. Hasteko, garbi dago (i), (ii) eta (iii) baldintzak betetzen direla B A-ren azpieraztuna bada. Frogatu dezagun orain alderantzizkoa. Alde batetik, B ezhutsa izateagatik eta (i) baldintza betetzeagatik, badakigu B A-ren azpitaldea dela batuketarekiko. Bereziki, $(B,+)$ taldea da. Bestalde, (ii) propietatearen arabera, biderketa eragiketa da B-n. Gainera, biderketa A-ren gainean elkarkorra eta trukakorra denez, eta banatze-propietatea betetzen denez, beste horrenbeste gertatzen da B-n. Azkenik, $1 \in B$ denez, B-k badu elementu neutroa biderketarekiko. Horrenbestez, frogaturik gelditzen da B identitatedun eraztun trukakorra dela, eta A-ren identitate bera duenez, A-ren azpieraztuna da. □

Azken teoremaren ondorio berehalakoa da honako emaitza hau.

1.17. Korolarioa. *Izan bedi A eraztuna. Orduan, A-ren azpieraztunen ebakidura A-ren azpieraztuna da.*

Izan bitez A eraztuna eta S A-ren azpimultzo orokor bat. Normalean ez da gertatuko S A-ren azpieraztuna izatea; adibidez, $1 \notin S$ bada, guztiz ezinezkoa da. Hala ere, pentsa genezake S-rekin azpieraztun bat sortzea, talde-teorian azpitaldeak edo aljebra linealean azpiespazioak sortzen ditugun bezala. Horretarako, aukera bat da konturatzea S barruan duen azpieraztun txikien bat dagoela, S barruan duten azpieraztun guztien ebakidura, alegia. (Kontuan izan aurreko korolarioa.)

1.18. Definizioa. Izan bitez A eraztuna eta $S \subseteq A$. Orduan, *S-k sortutako azpieraztuna* S barruan duten A-ren azpieraztun guztien ebakidura da. Hori adierazteko $\mathbb{Z}[S]$ ikurra erabiliko dugu.

1.19. Notazioa. Baldin eta $S = \{a_1, \dots, a_n\}$ finitua bada, normalean $\mathbb{Z}[a_1, \dots, a_n]$ idatziko dugu $\mathbb{Z}[\{a_1, \dots, a_n\}]$-ren ordez.

1.20. Oharra. Aurretik esandakoaren arabera, $\mathbb{Z}[S]$ da S barruan duen A-ren azpieraztunik txikiena. Ondorioz, maiz erabiliko dugun propietate hau betetzen da: B A-ren azpieraztuna bada eta $S \subseteq B$ bada, orduan $\mathbb{Z}[S] \subseteq B$ partekotasuna dugu.

Aurreko definizioak desabantaila bat du: ez digu erakusten nolakoak diren $\mathbb{Z}[S]$-ko elementuak. Segidan konpontzen dugu arazo hori.

1.21. Teorema. *Izan bitez A eraztuna eta $S \subseteq A$. Orduan,*

$$\begin{aligned}\mathbb{Z}[S] &= \Big\{ \sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} a_1^{i_1} \dots a_n^{i_n} \mid \lambda_{i_1,\dots,i_n} \in \mathbb{Z},\ a_1, \dots, a_n \in S,\ n \in \mathbb{N} \cup \{0\} \Big\} \\ &= \big\{ f(a_1, \dots, a_n) \mid f \in \mathbb{Z}[X_1, \dots, X_n],\ a_1, \dots, a_n \in S,\ n \in \mathbb{N} \big\}\end{aligned}$$

dugu. Bestela esanda, S-k sortzen duen azpieraztuna S-ko elementuen konbinazio polinomiko guztiek osatzen dute, koefizienteak $\mathbb{Z}$-n izanik. Bereziki, hau da $a \in A$

elementu batek sortzen duen azpieraztuna:

$$\begin{aligned}\mathbb{Z}[a] &= \left\{\lambda_0\,1+\lambda_1 a+\cdots+\lambda_n a^n \mid \lambda_i\in\mathbb{Z},\ n\in\mathbb{N}\cup\{0\}\right\}\\ &= \big\{f(a)\mid f\in\mathbb{Z}[X]\big\}.\end{aligned}$$

Froga. Izan bedi

$$B=\big\{f(a_1,\dots,a_n)\mid f\in\mathbb{Z}[X_1,\dots,X_n],\ a_1,\dots,a_n\in S,\ n\in\mathbb{N}\big\}.$$

Orduan, $\mathbb{Z}[S]=B$ berdintza frogatu behar dugu. Horretarako, ohartu lehenengo eta behin B A-ren azpieraztuna dela. Erraz egiaztatzen da hori 1.16 teorema erabiliz. Konturatzen bagara $S\subseteq B$ dela, zuzenean lortzen dugu $\mathbb{Z}[S]\subseteq B$ partekotasuna, 1.20 oharra kontuan hartuz. Alderantzizko partekotasuna ikusteko, hartu B-ko elementu orokor bat, hau da, $f(a_1,\dots,a_n)$ moduko konbinazio polinomiko bat, $a_1,\dots,a_n\in S$ izanik. Konbinazio polinomiko hori $a_1,\dots,a_n$ elementuekin batuketak eta biderketak eginez lortzen da. Orain, $S\subseteq\mathbb{Z}[S]$ denez eta $\mathbb{Z}[S]$ eraztuna denez, $f(a_1,\dots,a_n)\in\mathbb{Z}[S]$ dela ondorioztatzen dugu. Horrenbestez, frogaturik gelditzen da $B\subseteq\mathbb{Z}[S]$ dela. □

1.22. Adibideak. 1) Aurreko teorema aplikatuz, hau da 1/3-ek $\mathbb{Q}$-n sortzen duen azpieraztuna:

$$\mathbb{Z}[1/3]=\left\{\lambda_0+\lambda_1\frac{1}{3}+\cdots+\lambda_n\left(\frac{1}{3}\right)^n \mid \lambda_i\in\mathbb{Z},\ n\in\mathbb{N}\cup\{0\}\right\}.$$

Orain, garbi dago

$$\mathbb{Z}[1/3]=\left\{\frac{a}{3^n}\mid a\in\mathbb{Z},\ n\in\mathbb{N}\cup\{0\}\right\}$$

dela.

2) Antzera, 1/2-ak eta 1/3-ak sortzen duten $\mathbb{Q}$-ren azpieraztuna

$$\mathbb{Z}[1/2,1/3]=\left\{\frac{a}{2^m3^n}\mid a\in\mathbb{Z},\ m,n\in\mathbb{N}\cup\{0\}\right\}$$

zatikien multzoa da.

3) Bestalde, erraz ikus daiteke i zenbakiak sortzen duen $\mathbb{C}$-ren azpieraztuna

$$\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$$

dela: nahikoa da ohartzea $i^n\in\{\pm1,\pm i\}$ dela $n\in\mathbb{N}\cup\{0\}$ guztietarako. Ohikoa da $\mathbb{Z}[i]$-ko elementuei *zenbaki oso gaussiar* deitzea, Carl Friedrich Gauss izan baitzen zenbaki horiek sistematikoki aztertu zituen lehenengo matematikaria. Hirugarren gaian ikusiko dugunez, zenbaki oso gaussiarrek eta ohiko zenbaki osoek ezaugarri komun asko dituzte.

4) Hau da $\mathbb{Z}[X]$ eraztunean X^2-k sortzen duen azpieraztuna:

$$\mathbb{Z}[X^2]=\big\{a_0+a_1X^2+a_2X^4+\cdots+a_nX^{2n}\mid a_i\in\mathbb{Z},\ n\in\mathbb{N}\cup\{0\}\big\}.$$

Bestela esanda, berretzaile bikoitiko gaiak besterik ez duten polinomioek osatzen dute X^2-k sortzen duen azpieraztuna.

1.23. Korolarioa. *Izan bedi A eraztuna. Orduan,*

$$\mathbb{Z}[1] = \{n1 \mid n \in \mathbb{Z}\}$$

A-ren azpieraztunik txikiena da.

FROGA. Izan bedi B A-ren azpieraztuna. Orduan, $1 \in B$ dugu eta, 1.20 oharra aplikatzen badugu, $\mathbb{Z}[1] \subseteq B$ partekotasuna ondorioztatzen dugu. Horrek $\mathbb{Z}[1]$ A-ren azpieraztunik txikiena dela frogatzen du. □

Aurreko korolarioan, ez da gomendagarria $n1$-en ordez n idaztea. Izan ere, 1.7 puntuaren ondoren azpimarratu dugun bezala, $n1$ ikur bat besterik ez da, eta ez "n bider 1". Horrela, n positiboa bada, $n1 = 1 + \overset{n}{\cdots} + 1$ dugu. Lanean ari garen A eraztunak $\mathbb{Z}$ baldin badu bere barruan, orduan A-ren 1 identitatea 1 zenbaki osoa izango da. Ondorioz, $n1$-en balioa kalkulatzean n zenbaki osoa lortzen dugu, eta egiazkoa da $n1 = n$ berdintza. Baina $\mathbb{Z}$ ez badago A-ren barruan, ez du zentzurik $n1 = n$ idazteak. Adibidez, $A = \mathbb{Z}/m\mathbb{Z}$ bada $m \in \mathbb{N}$ batentzat, orduan A-ren identitatea $\overline{1}$ da eta $n1 = n\overline{1} = \overline{n}$ dugu. Beraz, $\mathbb{Z}/m\mathbb{Z}$-ren azpieraztunik txikiena $\{\overline{n} \mid n \in \mathbb{Z}\}$ dugu, hau da, $\mathbb{Z}/m\mathbb{Z}$ osoa. Ohartu emaitza hori bat datorrela 1.15 adibideetako 7) atalean esandakoarekin.

1.24. Definizioa. Izan bedi A eraztuna. Orduan, $\mathbb{Z}[1]$ eraztunari A-ren *azpieraztun lehen* deritzo.

1.3. Integritate-domeinuak eta gorputzak. Zatikien eraztunak

Ikusi dugunez, zenbaki errealekin erabiltzen ditugun identitate aljebraiko gehienak baliozkoak dira, oro har, eraztunetan. Badago, hala ere, aipatu dugun salbuespen garrantzitsu bat: $a \cdot b = 0$ izan daiteke a eta b elementuak zero izan gabe. Horrelako elementuek izen berezi bat merezi dute.

1.25. Definizioa. Izan bitez A eraztuna eta $a \in A$, $a \neq 0$. Existitzen bada $b \in A$, $b \neq 0$, halakoa non $ab = 0$ baita, orduan a *zeroren zatitzailea* dela esaten dugu.

Jakina, definizioko b elementua ere zeroren zatitzailea da. Jarraian bi eraztun mota nagusi definitzen ditugu.

1.26. Definizioa. Izan bedi A eraztuna. Orduan:

(i) A *integritate-domeinua* dela diogu (laburkiago *I.D.*), ez bada eraztun tribiala eta ez badu zeroren zatitzailerik.

(ii) A *gorputza* dela diogu, ez bada eraztun tribiala eta $A^\times = A \setminus \{0\}$ bada.

Integritate-domeinuaren definizioan, zeroren zatitzailerik ez izateko baldintza modu hauetariko batean jar daiteke, nahiago dugun bezala:

(ID) $ab = 0$ bada, orduan $a = 0$ edo $b = 0$ dugu.
(ID′) $ab = 0$ eta $a \neq 0$ bada, orduan $b = 0$ dugu.
(ID″) $a \neq 0$ eta $b \neq 0$ bada, orduan $ab \neq 0$ dugu.

Bestalde, 1.10 korolarioaren arabera, eraztun bat ez bada tribiala, orduan 0 elementua ez da unitatea. Beraz, eragiketei normalean eskatzen zaizkien propietateak kontuan hartzen baditugu, gorputz bateko biderketak ahal diren propietate guztiak betetzen ditu: elkarkorra eta trukakorra da, neutroa du, eta $a \neq 0$ guztiek alderantzizkoa dute. Alde horretatik, gorputzak "eraztunik hoberenak" direla esan dezakegu. Ohikoa da gorputzak K letraz adieraztea.

Ondorengo emaitzak erakusten duenez, integritate-domeinuaren eta gorputzaren kontzeptuak elkarrekin lotuta daude.

1.27. Proposizioa. *Izan bedi K gorputza. Orduan, K integritate-domeinua da.*

Froga. Badakigunez K eraztun ez-tribiala dela, nahikoa da (ID′) baldintza egiaztatzea. Demagun $ab = 0$ dela, $a, b \in K$ izanik, eta $a \neq 0$ izanik. Kontuan hartuz K gorputza dela, badakigu a elementuak baduela alderantzizkoa K-n, a^{-1}. Orain, $ab = 0$ berdintza a^{-1}-ez biderkatzen badugu, $b = 0$ dela lortzen dugu, nahi bezala. □

Eman ditzagun orain integritate-domeinuen eta gorputzen adibideak.

1.28. Adibideak. 1) $\mathbb{Z}$ integritate-domeinua da, baina ez da gorputza, $\mathbb{Z}^\times = \{1, -1\}$ baita. Beraz, integritate-domeinu batek ez du zertan gorputza izan.

2) $\mathbb{Q}$, $\mathbb{R}$ eta $\mathbb{C}$ gorputzak dira.

3) Erraz ikus daiteke $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ multzoa gorputza dela. Ohartu

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i \in \mathbb{Q}(i)$$

dela $a + bi \neq 0$ denean (hau da, $a \neq 0$ edo $b \neq 0$ denean). Horrexegatik ere, $\mathbb{Z}[i]$ ez da gorputza, integritate-domeinua den arren.

4) Noiz dira $\mathbb{Z}/n\mathbb{Z}$ eraztunak integritate-domeinuak edo gorputzak? Ezaguna da $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid (a, n) = 1\}$ dela. Beraz,

$$\mathbb{Z}/n\mathbb{Z} \text{ gorputza} \iff (\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} \iff n \text{ zenbaki lehena.}$$

Ohikoa da $\mathbb{F}_p$ idaztea $\mathbb{Z}/p\mathbb{Z}$-ren ordez p lehena denean; F letra erabiltzearen arrazoia da gorputzei ingelesez "field" deitzen zaiela. Horrela, p zenbaki lehen bakoitzeko, p elementu dituen $\mathbb{F}_p$ gorputz finitua dugu. Beste alde batetik, n zenbaki konposatua bada, orduan $n = r \cdot s$ idatz dezakegu, $1 < r, s < n$ izanik. Orduan, $\overline{r} \cdot \overline{s} = \overline{0}$ dugu $\mathbb{Z}/n\mathbb{Z}$-n, baina $\overline{r}, \overline{s} \neq \overline{0}$. Horrek erakusten du $\mathbb{Z}/n\mathbb{Z}$ ez dela integritate-domeinua n konposatua denean. Ondorioz,

$$\mathbb{Z}/n\mathbb{Z} \text{ integritate-domeinua} \iff \mathbb{Z}/n\mathbb{Z} \text{ gorputza}$$

baliokidetasuna dugu. Horren zergatia hobeto ulertuko da **??** problema egin eta gero.

1.29. Oharra. Nabaria da integritate-domeinu baten edozein azpieraztun integritate-domeinua dela berriro ere. Hala ere, gorputz baten azpieraztun batek ez du zertan gorputza izan. Adibidez, $\mathbb{Q}$ gorputza da eta $\mathbb{Z}$ $\mathbb{Q}$-ren azpieraztuna da, baina $\mathbb{Z}$ ez da gorputza.

Ondorengo proposizioan ikusten dugun bezala, integritate-domeinuek familiarra egiten zaigun propietate bat dute, ez dena eraztun guztietan betetzen.

1.30. Proposizioa. *Izan bitez A eraztuna eta $a \in A$, $a \neq 0$, zeroren zatitzailea ez den elementua. Orduan, a sinplifikagarria da biderketarekiko, hau da, $ab = ac$ berdintza badugu, $b, c \in A$ izanik, $b = c$ dela ondorioztatzen da. Bereziki, A integritate-domeinua bada, orduan elementu ez-nulu guztiak sinplifikagarriak dira biderketarekiko.*

Froga. Izan ere,

$$ab = ac \implies ab - ac = 0 \implies a(b-c) = 0 \implies b - c = 0 \implies b = c.$$

Ohartu azkenaurreko inplikazioa a zeroren zatitzailea ez izateagatik eta $a \neq 0$ izateagatik betetzen dela. □

Jarraian $A[X]$ eraztunaren propietate batzuk frogatu nahi ditugu, A integritate-domeinua denean. Horien froga polinomioen mailaren kontzeptuan oinarritzen da.

1.31. Definizioa. Izan bitez A eraztuna eta $f \in A[X]$. Orduan:

(i) $f = 0$ bada, f-ren *maila* $-\infty$ da.
(ii) $f \neq 0$ bada, eta $f(X) = a_0 + \cdots + a_n X^n$ idazten badugu, $a_n \neq 0$ izanik, orduan f-ren *maila* n da. Gainera, a_n f-ren *koefiziente nagusia* dela diogu, eta $a_n = 1$ bada, f *polinomio monikoa* dela diogu.

Edozein kasutan, f-ren maila adierazteko $\deg f$ ikurra erabiltzen dugu.

Ohartu $A[X]$-ko konstanteak $\deg f \leq 0$ betetzen duten polinomioak direla eta konstante ez-nuluak, berriz, $\deg f = 0$ betetzen dutenak.

Mailaren kontzeptua $A[X_1, \ldots, X_n]$ bezalako eraztunetan ere defini daiteke, baina orduan maila osoa eta indeterminatu batekiko mailak bereizi behar dira.

1.32. Definizioa. Izan bitez A eraztuna eta $X_1, \ldots, X_n$ indeterminatuak. Orduan:

(i) $X_1^{i_1} \ldots X_n^{i_n}$ monomioaren *maila osoa* $i_1 + \cdots + i_n$ batura da eta X_j*-rekiko maila* i_j berretzailea da.

Izan bedi orain $f \in A[X_1, \ldots, X_n]$. Orduan:

(ii) $f = 0$ bada, haren maila osoa eta X_j indeterminatu batekiko maila $-\infty$ dira.

(iii) $f \neq 0$ bada, f-ren *maila osoa* haren adierazpenean koefiziente ez-nulua duten monomioen maila osorik handiena da. Antzera definitzen da f-ren *maila X_j indeterminatuarekiko*,

Edozein kasutan, f-ren maila osoa adierazteko $\deg f$ idazten dugu, eta X_j-rekiko maila adierazteko, berriz, $\deg_{X_j} f$.

Adibidez, $f(X,Y) = X^3+X^2Y^2+Y^3$ polinomioaren kasuan, $\deg_X f = \deg_Y f = 3$ eta $\deg f = 4$ dugu.

1.33. Oharra. Azken definizioan eman ditugun indeterminatu batekiko mailak benetan 1.31 definizioan sartutako mailaren kasu bereziak dira. Izan ere, $A[X_1,\dots,X_n]$ eraztunean X_j indeterminatuari rol nagusia ematen badiogu, gainerako indeterminatuak konstantetzat hartuz, hau da, polinomioen eraztun hori $A[X_1,\dots,X_{j-1},X_{j+1},\dots,X_n][X_j]$ moduan ikusten badugu, orduan f polinomio baten maila $\deg_{X_j} f$ besterik ez da.

Ondorengo emaitza nabaria da.

1.34. Teorema. *Izan bitez A eraztuna eta $f,g \in A[X_1,\dots,X_n]$ bi polinomio. Orduan:*

(i) $\deg(f+g) \leq \max\{\deg f, \deg g\}$ *dugu eta, gainera,* $\deg f$ *eta* $\deg g$ *desberdinak badira, berdintza dugu.*

(ii) $\deg(fg) \leq \deg f + \deg g$ *dugu eta, gainera, A integritate-domeinua bada, orduan berdintza dugu.*

Emaitza berak betetzen dira $\deg_{X_j}$ *erabiltzen badugu* deg *maila osoaren ordez.*

Froga. Emaitza guztiak berehalakoak dira. Propietate hau besterik ez dugu frogatuko: A integritate-domeinua denean, $\deg(fg) = \deg f + \deg g$ dela. Ohartu emaitza hori begi-bistakoa dela f eta g polinomioetako bat 0 denean. Demagun, beraz, $f,g \neq 0$ dela. Izan bitez $\deg f = \ell$ eta $\deg g = m$. Orduan, f-ren adierazpenean badago $aX_1^{i_1}\dots X_n^{i_n}$ batugai bat, hiru propietate hauek betetzen dituena:

(i) $a \in A$, $a \neq 0$.
(ii) $i_1 + \dots + i_n = \ell$.
(iii) f-n agertzen diren gainerako monomioen maila gehienez ℓ da.

Antzera gertatzen da g-ren kasuan, eta haren adierazpenean badago $bX_1^{j_1}\dots X_n^{j_n}$ batugai bat non:

(i′) $b \in A$, $b \neq 0$.
(ii′) $j_1 + \dots + j_n = m$.
(iii′) g-n agertzen diren gainerako monomioen maila gehienez m da.

Orduan, fg biderkadura kalkulatzean, monomio guztien maila gehienez $\ell+m$ izango da, eta batugaietako bat $abX_1^{i_1+j_1}\dots X_n^{i_n+j_n}$ da. Orain, A integritate-domeinua eta $a,b \neq 0$ izateagatik, $ab \neq 0$ dugu, eta bestalde $(i_1+j_1)+\dots+(i_n+j_n) = \ell+m$ dugu. Horrek guztiak $\deg(fg) = \ell+m = \deg f + \deg g$ dela frogatzen du. □

A eraztuna integritate-domeinua ez bada, orduan $\deg(fg) = \deg f + \deg g$ propietatea ez da beti betetzen. Hori ikusteko, aukeratu ditzagun bi elementu $a, b \in A$ halakoak non $ab = 0$ eta $a, b \neq 0$ baita. Orduan, a eta b koefiziente nagusiak dituzten f eta g bi edozein polinomio hartzen baditugu $A[X]$ eraztunean, $\deg(fg) < \deg f + \deg g$ betetzen da.

1.35. Proposizioa. *Izan bedi A eraztuna. Orduan, baliokideak dira:*

(i) *A integritate-domeinua da.*
(ii) *$A[X]$ integritate-domeinua da.*

Froga. Lehenengo eta behin, demagun A integritate-domeinua dela, eta ikus dezagun $A[X]$ ere integritate-domeinua dela. Horretarako (ID$''$) propietatea egiaztatuko dugu: $f, g \in A[X]$ polinomio ez-nuluak badira, $fg \neq 0$ dela ikusiko dugu. Alde batetik, $f, g \neq 0$ izateagatik, $\deg f \geq 0$ eta $\deg g \geq 0$ dugu. Orain, 1.34 teorema aplikatzen badugu, $\deg(fg) \geq 0$ lortzen dugu eta, hortaz, $fg \neq 0$ dugu.

Alderantzizkoa errazagoa da: integritate-domeinu baten azpieraztunak ere integritate-domeinuak direnez, $A[X]$ integritate-domeinua den kasuan, A ere izango da. □

Ez da inola ere egia $K[X]$ gorputza denik K gorputza denean. Izan ere, $A[X]$ motako eraztun bat ez da inoiz gorputza, X indeterminatuak ez baitu alderantzizkorik. Edozein kasutan, aurreko proposizioa erabiliz, badakigu $K[X]$ integritate-domeinua dela K gorputza denean. Hirugarren gaian ikusiko dugun bezala, gorputza ez den arren, $K[X]$ integritate-domeinu mota hoberenetarikoa da.

1.36. Korolarioa. *Izan bedi A integritate-domeinua bada. Orduan, $A[X_1, \ldots, X_n]$ ere integritate-domeinua da.*

Orain $A[X]$ polinomioen eraztun baten unitateak interesatzen zaizkigu. Dakusagunez, emaitza bereziki sinplea da A integritate-domeinua denean.

1.37. Teorema. *Izan bedi A integritate-domeinua. Orduan, $\mathcal{U}(A[X]) = \mathcal{U}(A)$ dugu.*

Froga. Garbi dago $\mathcal{U}(A) \subseteq \mathcal{U}(A[X])$ betetzen dela. Alderantzizko partekotasuna frogatzeko, har dezagun $f \in \mathcal{U}(A[X])$, eta ikus dezagun A-n dagoela. Lehenengo eta behin, f unitatea izateagatik, existitzen da $g \in A[X]$ non $fg = 1$ baita. Berdintza horretan mailak hartzen baditugu eta 1.34 teorema aplikatzen badugu, $\deg f + \deg g = 0$ dela lortzen dugu. Hortik, nahitaez $\deg f = 0$ izan behar duela ondorioztatzen dugu eta, beraz, $f \in A$ dugu. □

Aurreko teoremaren alderantzizkoa ez da egiazkoa: gerta daiteke $\mathcal{U}(A[X]) = \mathcal{U}(A)$ berdintza betetzea A integritate-domeinua izan gabe. Hori da kasua, adibidez, $A = \mathbb{Z}/n\mathbb{Z}$ hartzen badugu, n karratugabea izanik (hau da, n-ren faktorizazioan agertzen den zenbaki lehen bakoitzaren berretzailea 1 bada). Ikusi **??** problema emaitza horren frogaren eskema ikusteko.

1.38. Korolarioa. *Izan bedi K gorputza. Orduan, $K[X_1, \dots, X_n]$-ren unitateak konstante ez-nuluak dira.*

Gorputz guztiak integritate-domeinuak badira ere, badakigu alderantzizkoa ez dela egia. Hala ere, A integritate-domeinu bat emanda, badago modu bat horretatik gorputz bat eraikitzeko, kopiatzen duena zenbaki arrazionalen eraikuntza zenbaki osoetatik abiatuz. Jar dezagun

$$K = \left\{ \frac{a}{b} \mid a, b \in A,\ b \neq 0 \right\}.$$

Hemen, $\frac{a}{b}$ (a/b moduan ere idatziko duguna) ikur bat besterik ez da; beranduago justifikatuko dugu a/b *zer den*. Elementu horiek A-ko elementuen *zatikiak* direla esango dugu. Momentuz, garrantzitsuena da jakitea horrelako bi ikur noiz diren berdinak, eta nola batzen diren eta biderkatzen diren. Hori guztia zenbaki arrazionalekin bezala egingo dugu. Alde batetik,

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad = bc \tag{1.2}$$

dugu. Bestetik, batuketa eta biderketa formula hauen bidez emanda daude:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{1.3}$$

eta

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{1.4}$$

1.39. Definizioa. Izan bedi A integritate-domeinua. Orduan, A-ren *zatikien gorputza*

$$\left\{ \frac{a}{b} \mid a, b \in A,\ b \neq 0 \right\}$$

multzoa da, non elementuen arteko berdintza (1.2) formularen araberakoa baita, eta batuketa eta biderketa (1.3) eta (1.4) formulen bidez emanda baitaude.

1.40. Oharra. Zatikien gorputzaren eraikuntza formalagoa egin nahi badugu, argi erakusten duena zatikiak zer diren, honela joka dezakegu. Definitu $A \times (A \setminus \{0\})$ multzoaren gainean $\sim$ erlazioa modu honetan:

$$(a, b) \sim (c, d) \quad \Longleftrightarrow \quad ad = bc.$$

Orduan, $\sim$ baliokidetasun-erlazioa da, eta (a, b) elementuari dagokion baliokidetasun-klasea da a/b moduan idazten dugun zatikia. Erraz ikus daiteke orduan (1.3) eta (1.4) eragiketak ondo definituta daudela zatikien multzoaren gainean, hau da, ez direla a, b, c eta d balioen menpekoak, baizik eta baliokidetasun-klaseen menpekoak.

Erraz egiazta daiteke ondorengo emaitza.

1.41. Teorema. *Izan bitez A integritate-domeinua eta K A-ren zatikien gorputza. Orduan, K gorputza da.*

Ohartu zatikien gorputzaren barruan hasierako integritate-domeinuaren kopia bat dugula: $a \mapsto a/1$ aplikazioa bijektiboa da, eta batuketa eta biderketa gordetzen ditu (horren esanahia garbiago geldituko da 2. gaian, eraztun-isomorfismoei buruz hitz egiten dugunean). Hori dela eta, normalean $a/1$ zatikiaren ordez a besterik ez dugu idatziko.

1.42. Adibideak. 1) $\mathbb{Z}$-ren zatikien gorputza $\mathbb{Q}$ da.

2) K gorputza bada, badakigu $K[X]$ integritate-domeinua dela, da baina ez gorputza. Dagokion zatikien gorputzari *funtzio arrazionalen gorputza* deitzen zaio, X indeterminatuarekiko, eta $K(X)$ ikurraz adierazten dugu. Beraz,

$$K(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in K[X],\ g(X) \neq 0 \right\}.$$

3) Antzera definitzen da $K(X_1, \ldots, X_n)$ funtzio arrazionalen gorputza $X_1, \ldots, X_n$ indeterminatuetan. Hori $K[X_1, \ldots, X_n]$ integritate-domeinuaren zatikien gorputza da, eta haren elementuak $K[X_1, \ldots, X_n]$-ko polinomioen zatikiak dira.

4) Espero genezakeen bezala, gorputz baten zatikien gorputza gorputz hori bera da. Izan ere, A gorputza bada, orduan $a/b = ab^{-1}/1$ dugu (zuzenean egiaztatzen da hala dela (1.2) erabiliz). Beraz, zatiki guztiak A-ko elementuekin bat datoz.

Atal honekin bukatzeko, zatikien gorputzaren azpieraztunak "fabrikatzeko" modu bat emango dugu. Horretarako, kontzeptu hau behar dugu.

1.43. Definizioa. Izan bitez A eraztuna eta $S \subseteq A$. Orduan, S *azpimultzo biderkakorra* dela esango dugu hiru baldintza hauek betetzen badira:

(i) S itxia da biderketarekiko: $x, y \in S$ bada, orduan $xy \in S$ dugu.
(ii) $1 \in S$.
(iii) $0 \notin S$.

1.44. Adibideak. 1) Izan bedi A integritate-domeinua. Orduan, $A \setminus \{0\}$ multzoa biderkakorra da.

2) Izan bedi A integritate-domeinua eta aukeratu dezagun $a \in A$ elementu bat, $a \neq 0$. Orduan, $\{a^n \mid n \in \mathbb{N} \cup \{0\}\}$ berreturek azpimultzo biderkakor bat osatzen dute.

3) Oro har, A integritate-domeinua bada eta $T \subseteq A \setminus \{0\}$ bada, orduan T-k S azpimultzo biderkakor bat sortzen du: S-ren elementuak T-ko elementuen arteko biderkadura guztiak dira (horien artean faktorerik gabeko biderkadura sartzen da, definizioz 1 dena). Orduan, aurreko adibidean elementu batek sortzen duen azpimultzo biderkakorra eman dugu, eta adibidez, 2ak eta 3ak sortzen duten $\mathbb{Z}$-ren azpimultzo biderkakorra $\{2^m 3^n \mid m, n \in \mathbb{N} \cup \{0\}\}$ multzoa da.

4) Izan bedi $p \in \mathbb{Z}$ zenbaki lehena. Orduan, $S = \{a \in \mathbb{Z} : p \nmid a\}$ $\mathbb{Z}$-ren azpimultzo biderkakorra da. Ohartu aurreko adibideko kategorian sartzen dela: aukeratu T gisa zenbaki lehen guztien multzoa, p kenduta.

1.45. Teorema. *Izan bitez A integritate-domeinua eta S A-ren azpimultzo biderkakorra. Orduan,*

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

multzoa A-ren zatikien gorputzaren azpieraztuna da, eta A $S^{-1}A$-ren azpieraztuna da.

FROGA. Ariketa erraza da, 1.16 teorema aplikatuz. □

1.46. Definizioa. Izan bitez A integritate-domeinua eta S A-ren azpimultzo biderkakorra. Orduan, $S^{-1}A$ S-ri dagokion *zatikien eraztuna* dela diogu.

Beraz, A-ren zatikien gorputza zatikien eraztunen kasu berezi bat da, $S = A \setminus \{0\}$ azpimultzo biderkakorra aukeratzen dugunean, alegia. Ikus ditzagun beste adibide batzuk.

1.47. Adibideak. 1) $\mathbb{Z}$ eraztunean $S = \{3^n \mid n \in \mathbb{N} \cup \{0\}\}$ azpimultzo biderkakorra aukeratzen badugu, orduan

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

dugu eta, beraz, $S^{-1}\mathbb{Z} = \mathbb{Z}[1/3]$. Ohartu $\mathcal{U}(S^{-1}\mathbb{Z}) = \{\pm 3^n \mid n \in \mathbb{Z}\}$ dela.

2) Antzera, 2ak eta 3ak sortzen duten azpimultzo biderkakorra aukeratzen badugu $\mathbb{Z}$-n, hau da, $S = \{2^m 3^n \mid m, n \in \mathbb{N} \cup \{0\}\}$ hartzen badugu, orduan $S^{-1}\mathbb{Z} = \mathbb{Z}[1/2, 1/3]$ dugu.

3) K gorputza bada, har dezagun $K[X]$-ren barruan $S = \{X^n \mid n \in \mathbb{N} \cup \{0\}\}$ azpimultzoa, hau da, X indeterminatuak sortzen duen azpimultzo biderkakorra. Orduan,

$$\begin{aligned} S^{-1}K[X] &= \left\{ \frac{f(X)}{X^n} \mid f(X) \in K[X],\ n \in \mathbb{N} \cup \{0\} \right\} \\ &= \{a_{-k}X^{-k} + \cdots + a_0 + \cdots + a_n X^n \mid a_i \in K,\ k, n \in \mathbb{N} \cup \{0\}\} \end{aligned}$$

dugu. Eraztun horretako elementuak X-rekiko polinomioak bezalakoak dira, hau da, X-ren berreturen konbinazio linealak, baina oraingo honetan berretzaile negatiboko berreturak ere onartzen ditugu. Elementu horiek *Laurenten polinomiak* direla esaten da, Pierre Alphonse Laurent matematikari frantsesarengatik. Kasu honetan, $\mathcal{U}(S^{-1}K[X]) = \{\lambda X^n \mid \lambda \in K \setminus \{0\},\ n \in \mathbb{Z}\}$ dugu.

Ondo ulertu behar da $S^{-1}A$ multzoaren definizioa. Izan ere, zatikien idazkera a/b moduan ez denez bakarra, konfusioa sor daiteke erabakitzean x elementu bat $S^{-1}A$-n dagoen edo ez. Elementu hori zatiki modura eman badigute, $x = a/b$, definizioak ez du esan nahi $x \in S^{-1}A$-n izateko b-k derrigorrean S-n egon behar duenik. Esanahi zuzena da $x \in S^{-1}A$ izango dela *idatz badaiteke* $x = c/d$ zatiki moduan $d \in S$ izanik (baina beharbada c/d zatikia ez da hasierako a/b zatikia izango). Argitu dezagun egoera adibide baten bitartez. Azter dezagun $S^{-1}\mathbb{Z}$-ren kasua, $S = \{3^n \mid n \in \mathbb{N} \cup \{0\}\}$ izanik. Orduan, $2/6$ elementua $S^{-1}\mathbb{Z}$-n dago,

nahiz eta $6 \notin S$ izan. Kontua da $2/6$ adierazteko $1/3$ ere idatz dezakegula, eta kasu horretan $3 \in S$ dugu. Arazo horrek badu konponbide erraza A eraztuna faktorizazio bakarreko domeinua den kasuan, orduan zatiki laburtezinak erabil baititzakegu, baina horretarako 3. gaira arte itxaron beharko dugu.

Zatikien gorputza eraikitzean, A integritate-domeinu baten elementu ez-nulu guztiak alderanzgarri bihurtzea lortzen dugun bezala, azpimarratu nahi dugu $S^{-1}A$ bezalako zatikien eraztunetan S-ko elementuak alderanzgarri bihurtzen ditugula.

1.4. Karakteristika

Zenbaki errealen gorputzean, $2 \neq 0$ dugu, hau da, $1 + 1 \neq 0$. Oro har, $n \in \mathbb{N}$ bada, orduan $1 + \overset{n}{\cdots} + 1 \neq 0$. Bestalde, $\mathbb{Z}/2\mathbb{Z}$-n $\overline{1} + \overline{1} = \overline{0}$ dugu eta $\mathbb{Z}/3\mathbb{Z}$-n, berriz, $\overline{1} + \overline{1} \neq \overline{0}$, baina $\overline{1} + \overline{1} + \overline{1} = \overline{0}$. Dakusagunez, identitatea bere buruarekin behin eta berriz batzean, eraztun batzuetan 0 lor dezakegu (batugaien kopuruaren arabera), eta beste eraztun batzuetan, berriz, ez dugu inoiz 0 lortuko. Hori ikusita, ondorengo kontzeptua sartzen dugu.

1.48. Definizioa. Izan bedi A eraztuna. Existitzen bada $n \in \mathbb{N}$, halakoa non $n1 = 1 + \overset{n}{\cdots} + 1 = 0$ betetzen baita A eraztunean, orduan balio horien arteko txikienari A-ren *karakteristika* deitzen diogu. Horrelako n-rik ez badago, A-ren karakteristika 0 dela esango dugu. Edozein kasutan, A-ren karakteristika $\operatorname{char} A$ ikurraren bidez adieraziko dugu.

Bestela esanda, A-ren karakteristika 1 identitateak batuketarekiko duen ordenaren araberakoa da: 1aren ordena finitua bada, orduan hori bera da karakteristika; bestela, ordena infinitua bada, orduan karakteristika 0 da.

1.49. Adibideak. $\operatorname{char}\mathbb{Z} = \operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$ eta $\operatorname{char}\mathbb{Z}/n\mathbb{Z} = n$ dugu. Bestetik, A B-ren azpieraztuna bada, orduan $\operatorname{char} A = \operatorname{char} B$ dugu, A-ren eta B-ren identitateak bat datoz eta. Bereziki, $\operatorname{char} A[X] = \operatorname{char} A$ dugu, A eraztun guztietarako. Gainera, K gorputza bada, $\operatorname{char} K(X) = \operatorname{char} K$ betetzen da.

1.50. Proposizioa. *Izan bedi A eraztuna. Orduan,* $\operatorname{char} A = n$ *bada, ondorengoa da A-ren azpieraztun lehenaren kardinala:*

$$|\mathbb{Z}[1]| = \begin{cases} +\infty, & \text{if } n = 0, \\ n, & \text{if } n > 0. \end{cases}$$

Froga. Badakigu, 1.23 korolarioaren arabera, $\mathbb{Z}[1] = \{n1 \mid n \in \mathbb{Z}\}$ dela. Bestela esanda, $\mathbb{Z}[1]$ da 1 elementuak batuketarekiko sortzen duen azpitaldea. Orduan, talde-teoriak dio $\mathbb{Z}[1]$-en kardinala 1 elementuaren ordena dela. Horrela, proposizioa frogaturik gelditzen da, karakteristikaren definizioaren osteko oharra kontuan hartuz. □

Definizioaren arabera, A eraztunaren karakteristika $n > 0$ bada, $n1 = 0$ dugu. Jarraian, hori bera A-ko elementu guztiekin gertatzen dela ikusten dugu.

1.51. Proposizioa. *Izan bedi A eraztuna, eta demagun $n = \operatorname{char} A > 0$ dela. Orduan, m n-ren multiploa bada, $ma = 0$ dugu $a \in A$ guztietarako. Bereziki, $na = 0$ dugu.*

Froga. Idatzi $m = dn$, $d \in \mathbb{Z}$ izanik. Orduan, aurretik ikusitako propietateengatik, $ma = d(na)$ eta $na = n(1 \cdot a) = (n1) \cdot a = 0 \cdot a = 0$ dugu. Horrela, $ma = 0$ lortzen dugu, nahi bezala. □

Ikusi dugun bezala, $\operatorname{char} \mathbb{Z}/n\mathbb{Z} = n$ dugu $n \in \mathbb{N}$ guztietarako. Beraz, eraztun baten karakteristika edozein zenbaki positibo izan daiteke. Jarraian ikusten dugunez, ez da gauza bera gertatzen integritate-domeinuetara murriztuz gero.

1.52. Teorema. *Izan bedi A integritate-domeinua. Orduan, A-ren karakteristika 0 edo zenbaki lehen bat da.*

Froga. Demagun $n = \operatorname{char} A > 0$ dela, eta ikus dezagun n zenbaki lehena dela. Absurdora eramanez, jar dezagun $n = k\ell$, $1 < k, \ell < n$ izanik. Orduan, $0 = n1 = (k\ell)1 = (k1) \cdot (\ell 1)$ dugu eta, A integritate-domeinua denez, $k1 = 0$ edo $\ell 1 = 0$ izan behar du. Edozein kasutan, A-ren karakteristika n baino txikiagoa dela lortzen dugu, eta hori kontraesan bat da. □

Matematikan larri ibiltzen diren ikasleen artean, ohikoak izaten dira $(x+y)^2 = x^2 + y^2$ bezalako akatsak. Harrigarria bada ere, batzuetan horrelako berdintzak egiazkoak izan daitezke eraztun batean, karakteristika 0-ren desberdina bada.

1.53. Teorema. *Izan bedi A eraztuna, eta demagun $p = \operatorname{char} A$ zenbaki lehena dela. Orduan,*

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

dugu, $a, b \in A$ eta $n \in \mathbb{N}$ guztietarako.

Froga. Nahikoa da $(a+b)^p = a^p + b^p$ dela ikustea. Behin hori frogatuta, teoremako emaitza zuzenean ondorioztatzen da, n-ren gaineko indukzioa erabiliz. Newtonen binomioaren arabera,

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

dugu. Orain, p lehena denez, ezaguna da $\binom{p}{i}$ koefiziente binomiala p-ren multiploa dela $1 \leq i \leq p-1$ guztietarako. Kontuan izanik $p = \operatorname{char} A > 0$ dela, orduan 1.51 proposizioa erabiliz, $\binom{p}{i} a^{p-i} b^i = 0$ dugu i-ren balio horietarako. Horrenbestez, $(a+b)^p = a^p + b^p$ lortzen dugu. □

Azken propietate hori interesgarria da berretura batzuk arin egiteko (berretzailea egokia denean), baina kontrako norabidean ere erabil daiteke eta, esate baterako, polinomioak azkar faktorizatzeko ere balio izaten du batzuetan. Adibidez, $\mathbb{F}_2[X]$ polinomioen eraztunaren karakteristika 2 denez, $X^8 + X^4 + 1 = (X^2 + X + 1)^4$ dugu.

1.5. K-aljebrak

Atal honetan zehar, K gorputza izango da beti.

1.54. Definizioa. *A K-aljebra* dela esaten dugu (edo aljebra K-ren gainean) aldi berean eraztuna eta K-espazio bektoriala bada, bi propietate hauek betez:

(i) Eraztunaren eta espazio bektorialaren batuketak bat bera dira.
(ii) Eraztunaren biderketa eta espazio bektorialaren eskalarrezko biderketa bateragarriak dira, zentzu honetan:

$$\lambda(ab) = (\lambda a)b = a(\lambda b), \quad \lambda \in K \text{ eta } a, b \in A \text{ guztietarako.}$$

Orduan, $\dim_K A$ ikurra erabiliko dugu (edo $\dim A$ besterik gabe, garbi badago zein den K gorputza) A-ren dimentsioa adierazteko, K-espazio bektorial gisa.

1.55. Adibideak. 1) K-aljebrarik garrantzizkoenak $K[X_1, \ldots, X_n]$ polinomioen aljebrak dira. Ohartu monomioek $K[X_1, \ldots, X_n]$-ren oinarri bat osatzen dutela eta, beraz, $\dim K[X_1, \ldots, X_n] = \infty$ dugu.

2) $K(X_1, \ldots, X_n)$ funtzio arrazionalen gorputza ere K-aljebra da, hori ere dimentsio infinitukoa.

3) K gorputza bera K-aljebra da, eta $\dim_K K = 1$ dugu. Oro har, $K \subseteq F$ gorputz-hedadura bat badugu, orduan F K-aljebra da. Adibidez, $\mathbb{R}$ eta $\mathbb{Q}(i)$ $\mathbb{Q}$-aljebrak dira eta $\mathbb{C}$ $\mathbb{R}$-aljebra da. (Baina $\mathbb{R}$ ez da $\mathbb{C}$-aljebra eragiketa naturalekin, zenbaki erreal bat zenbaki konplexu batez biderkatzean ez baitugu lortzen beti zenbaki erreal bat.) Ohartu $\dim_{\mathbb{Q}} \mathbb{R} = \infty$ eta $\dim_{\mathbb{Q}} \mathbb{Q}(i) = \dim_{\mathbb{R}} \mathbb{C} = 2$ dugula.

4) X multzoa bada, $\mathcal{F}(X, K) = \{f : X \to K \text{ aplikazioa}\}$ K-aljebra da. Orokorkiago, A K-aljebra bada, $\mathcal{F}(X, A)$ K-aljebra da.

1.56. Definizioa. Izan bitez A K-aljebra eta $B \subseteq A$. Orduan, B A-ren *azpialjebra* da azpieraztuna eta azpiespazioa bada aldi berean, hau da, propietate hauek betetzen baditu:

$$1 \in B, \qquad x, y \in B \;\Rightarrow\; x + y, xy \in B, \qquad \lambda \in K,\, x \in B \;\Rightarrow\; \lambda x \in B.$$

Azpialjebra guztiak azpieraztunak dira, baina gerta daiteke azpieraztun bat ez izatea azpialjebra, ez izateagatik azpiespazioa. Adibidez, $\mathbb{R}$ $\mathbb{Q}$-aljebra da eta $\mathbb{Z}$ $\mathbb{R}$-ren azpieraztuna da, baina ez da $\mathbb{Q}$-azpialjebra. Bestalde, azpieraztunen kasuan bezala, emaitza hau dugu.

1.57. Proposizioa. *Izan bedi A K-aljebra. Orduan, A-ren azpialjebren ebakidura azpialjebra da.*

Hori dela eta, azpimultzo batek sortzen duen azpialjebra defini dezakegu.

1.58. Definizioa. Izan bitez A K-aljebra eta $S \subseteq A$. Orduan, *S-k sortutako azpialjebra* S barruan duten A-ren azpialjebra guztien ebakidura da. Hori adierazteko $K[S]$ ikurra erabiliko dugu.

Beraz, S-k sortzen duen azpialjebra S barruan duen A-ren azpialjebrarik txikiena da. Baina, nolakoak dira $K[S]$-ren elementuak? Jarraian ikusiko dugunez, antzekotasun handia dago azpieraztunen kasuarekin.

Izan bitez A K-aljebra bat, $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ polinomio bat eta $a_1, \ldots, a_n \in A$. Orduan, $X_1 \mapsto a_1$, $\ldots$, $X_n \mapsto a_n$ ordezkapenek A-ko elementu bat definitzen dute, $f(a_1, \ldots, a_n)$ ikurraren bidez adierazten duguna. Zehazkiago, polinomioa

$$f(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} \lambda_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$$

bada, orduan

$$f(a_1, \ldots, a_n) = \sum_{i_1, \ldots, i_n \geq 0} \lambda_{i_1, \ldots, i_n} a_1^{i_1} \ldots a_n^{i_n} \tag{1.5}$$

jartzen dugu. Balio hori $a_1, \ldots, a_n$ elementuen *konbinazio polinomiko* bat dela esaten dugu. Jarraian ikusten dugunez, konbinazio polinomikoek azpimultzo batek sortzen duen azpialjebrarekin lotura zuzena dute.

1.59. Teorema. *Izan bitez A K-aljebra eta $S \subseteq A$. Orduan, S-k sortzen duen azpialjebra S-ko elementuen konbinazio polinomikoek osatzen dute, hau da,*

$$K[S] = \{f(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in S,\ f \in K[X_1, \ldots, X_n],\ n \in \mathbb{N}\}.$$

Froga. Sortutako azpieraztunaren kasuan bezala argudiatzen da. □

1.60. Korolarioa. *Izan bitez A K-aljebra eta $S \subseteq A$. Orduan, S-k sortzen duen azpialjebra da S-k sortzen duen azpieraztunak sortzen duen azpiespazioa.*

1.61. Adibideak. 1) Polinomioen aljebra orokor bat adierazteko erabiltzen dugun notazioa, $K[X_1, \ldots, X_n]$, bat dator azken teoreman sartu dugun notazioarekin. Izan ere, polinomioen aljebra $X_1, \ldots, X_n$ indeterminatuek sortzen dute; azken batean, polinomioak $X_1, \ldots, X_n$ indeterminatuen konbinazio polinomikoak dira.

2) Sortutako azpialjebraren definizioa aplikatuz, garbi dago X^2-k $K[X]$-ren barruan sortzen duen azpialjebra honako hau dela:

$$K[X^2] = \Big\{ \sum_{i \geq 0} a_i X^i \mid a_i = 0 \text{ da } i \text{ bakoiti guztietarako} \Big\}.$$

3) Zein da X^2 eta X^3 elementuek $K[X]$-n sortzen duten azpialjebra, $K[X^2, X^3]$? Azpialjebra hori osatzen duten elementuak $f(X^2, X^3)$ modukoak dira, $f \in K[X, Y]$ izanik. Orain, (1.5) formularen arabera, honelako polinomioak lortzen ditugu:

$$\sum_{i,j\geq 0} \lambda_{i,j} X^{2i} X^{3j} = \sum_{i,j\geq 0} \lambda_{i,j} X^{2i+3j}, \qquad \lambda_{i,j} \in K \text{ izanik.}$$

Erraz ikusten da $2i + 3j$ berretzaileek, $i, j \geq 0$ izanez gero, zero eta zenbaki arrunt guztiak estaltzen dituztela, 1aren salbuespenarekin. Beraz,

$$K[X^2, X^3] = \{\lambda_0 + \lambda_2 X^2 + \lambda_3 X^3 + \cdots + \lambda_n X^n \mid \lambda_i \in K,\ n \in \mathbb{N} \cup \{0\}\},$$

X monomioa agertzen ez den polinomioen multzoa da.

4) Laurenten polinomioen eraztuna 1.47 adibideetan ikusi dugu. Gogoratu Laurenten polinomioak

$$a_{-k} X^{-k} + \cdots + a_0 + \cdots + a_n X^n$$

moduko adierazpenak direla, $a_i \in K$ izanik, eta $k, n \in \mathbb{N} \cup \{0\}$ izanik. Erraz ikus daiteke eraztun hori $K(X)$-ren azpialjebra dela, are gehiago $K[X, X^{-1}]$-en berdina dela.

1.62. Definizioa. Izan bedi A K-aljebra. Orduan, A *finituki sortua* dela esaten dugu existitzen badira $a_1, \ldots, a_n \in A$, non $A = K[a_1, \ldots, a_n]$ baita.

1.63. Proposizioa. *Izan bedi A K-aljebra, eta demagun A dimentsio finitukoa dela. Orduan, A finituki sortua da.*

Froga. Izan bedi $\{a_1, \ldots, a_n\}$ A-ren oinarria K-espazio bektorial gisa. Orduan, A-ren elementuak $\lambda_1 a_1 + \cdots + a_n \lambda_n a_n$ moduko konbinazio linealak dira, $\lambda_i \in K$ izanik $i = 1, \ldots, n$ guztietarako. Konbinazio linealak bereziki konbinazio polinomikoak direnez, orduan 1.59 teorema aplikatuz, $A = K[a_1, \ldots, a_n]$ lortzen dugu. Beraz, A K-aljebra finituki sortua da. □

Aurreko proposizioaren alderantzizkoa ez da egia: aljebra bat finituki sortua izan daiteke, dimentsio infinitukoa bada ere. Hori da kasua, adibidez, $K[X_1, \ldots, X_n]$ polinomioen aljebrekin.