# 1

# Aljebra trukakorraren oinarriak

## 1.1. Eraztunak eta gorputzak

Geometria aljebraikoa ikasten hasi aurretik, hainbat egitura aljebraiko ezagutu behar ditu irakurleak: espazio bektorialak, taldeak, gorputzak, eraztunak. Kapitulu honetan kontzeptu horiek berrikusiko ditugu eta *aljebra* izena daraman "superegitura" berria sartuko dugu, betiere ondoren beharko ditugun puntuetan enfasi berezia jarriz. Lehenengo ataletan, gai ezagunak jorratuko ditugu gehienbat; hori dela eta, emaitza batzuk frogarik gabe emango ditugu.

Goian aipatutako egituretatik sinpleena taldearena da, eragiketa bakar bat behar baitu. Has gaitezen talde bat zer den gogoraraziz.

**1.1. Definizioa.** Izan bitez $G$ multzoa eta $\cdot$ $G$-ren gainean definiturik dagoen eragiketa. Orduan, $(G, \cdot)$ *taldea* dela diogu hiru baldintza hauek betetzen badira:

(i) $\cdot$ elkarkorra da: $(xy)z = x(yz)$ dugu $x, y, z \in G$ guztietarako.
(ii) $\cdot$-ek neutroa du: existitzen da $e \in G$, non $xe = ex = x$ baita $x \in G$ guztietarako.
(iii) Elementu guztiek alderantzizkoa dute: $x \in G$ guztietarako, existitzen da $y \in G$, non $xy = yx = e$ baita.

Horrez gain $\cdot$ trukakorra bada, hau da, $xy = yx$ badugu $x, y \in G$ guztietarako, orduan $G$ *talde trukakorra* (edo *abeldarra*) dela diogu.

**1.2. Adibideak.** 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ eta $(\mathbb{C}, +)$ talde trukakorrak dira, baina $(\mathbb{N}, +)$ ez da taldea, ez baitu elementu neutrorik. (Ohartu ez dugula 0 zenbakia $\mathbb{N}$-ren barruan sartzen; sartuko bagenu ere, berriro ere $(\mathbb{N}, +)$ ez litzateke taldea, 0 izan ezik gainerako elementuek ez baitute alderantzizkorik +-ekiko.)

2) Izan bedi $n \in \mathbb{N}$. Orduan, $\{1, \ldots, n\}$ multzoaren permutazioek talde bat osatzen dute konposizioarekiko. Horri $n$ mailako *talde simetriko* deritzo eta $S_n$ ikurraren bidez adierazten dugu. Talde hori $n = 1$ edo 2 denean baino ez da abeldarra.

3) $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ matrizeen multzoa taldea da biderketarekiko, eta ez da trukakorra, $n \geq 2$ bada.

Aljebra trukakorra izeneko alorra eraztunaren kontzeptuaren inguruan antolaturik dago. Eraztunek bi eragiketa behar badituzte ere, ezin da esan taldeak baino konplikatuagoak direnik. Izan ere, eraztunek bete behar dituzten propietateak guztiz ezagun zaizkigu, txikitatik zenbakiekin erabili ditugun berberak baitira.

**1.3. 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, neutroa du eta trukakorra da.
(iii) Banatze-propietatea betetzen da: $a(b+c) = ab+ac$ dugu $a, b, c \in A$ guztietarako.

Baldin eta $a \in A$ elementuak alderantzizkoa badu $\cdot$-ekiko, $a$ *unitatea* dela diogu.

Eraztun batean, batuketarekiko eta biderketarekiko neutroak bakarrak dira, eta 0 eta 1 ikurren bitartez adierazten ditugu, hurrenez hurren. Berez, $0 = 1$ gerta liteke baina, beranduago ikusiko dugunez, eraztun gehienetan $0 \neq 1$ dugu. Ohikoa da 1 elementua $A$-ren *identitatea* dela esatea. 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.

2) Izan bedi $n \in \mathbb{N}$ zenbaki finkoa. Orduan, $\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}$ eraztuna 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) Matrizeen biderketa ez denez trukakorra, $M_n(\mathbb{R})$ ez da eraztuna definizio horrekin (bai, ordea, beste definizio batzuen arabera).

4) Izan bitez $A$ eraztuna eta $X$ indeterminatua. Orduan, koefizienteak $A$-ren gainean dituzten polinomioen multzoa $A[X]$ ikurraren bidez adierazten dugu. Erraz ikusten da $A[X]$ berriro ere eraztuna dela. Orokorkiago, $X_1, \ldots, X_n$ indeterminatuak badira, $A[X_1, \ldots, X_n]$ da indeterminatu horiek erabiltzen dituzten eta koefizienteak $A$-n dituzten polinomioen eraztuna.

5) Izan bitez $A$ eta $B$ eraztunak. Orduan, $A \times B$ biderkadura cartesiarra ere eraztuna da, batuketa eta biderketa osagaiz osagai definitzen baditugu. Adibidez, identitatea $(1, 1)$ bikotea da (hor, lehenengo 1-ak $A$-ren identitatea adierazten du eta bigarrenak, berriz, $B$-rena).

Ohartu $a \cdot 0 = 0$ betetzen dela eraztun guztietan. Hala ere, $a \cdot b = 0$ baldintzatik ezin da ondorioztatu $a = 0$ edo $b = 0$ denik. Adibidez, $\mathbb{Z}/6\mathbb{Z}$-n $\overline{2} \cdot \overline{3} = \overline{0}$ dugu, baina

$\overline{2} \neq \overline{0}$ eta $\overline{3} \neq \overline{0}$. Betetzen bada $a \cdot b = 0$ eta $a, b \neq 0$, orduan $a$ eta $b$ *zeroren zatitzaileak* direla esaten dugu.

Eraztunik sinpleena $A = \{0\}$ multzoa da, *eraztun tribial* deitutakoa. Eraztuna tribiala ez bada, orduan $1 \neq 0$ dugu. Izan ere, $1 = 0$ balitz, orduan $a \in A$ guztietarako $a = a \cdot 1 = a \cdot 0 = 0$ izango genuke, eta hori kontraesan bat da. Ohartu eraztun ez-tribial batean 0 elementua ezin dela unitatea izan, $a \cdot 0 = 0 \neq 1$ betetzen baita $a \in A$ guztietarako.

**1.5. 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 $A^\times$-en biderketa eragiketa bat dela. 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. □

Adibidez, $\mathbb{Z}^\times = \{1, -1\}$ eta $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ dugu.

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

Adibidez, $\mathbb{Z}$ $\mathbb{Q}$-ren azpieraztuna da, eta $\mathbb{Q}$, berriz, $\mathbb{C}$-ren azpieraztuna da. Gainera, $A$ eraztuna edozein izanik, $A$ $A[X]$-ren azpieraztuna da. Bestetik, $A \times \{0\}$ 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 hori $(1, 1)$ $A \times A$-ren identitatearen desberdina dela.

**1.7. Definizioa.** Izan bedi $A$ eraztuna. Orduan:

(i) $A$ *integritate-domeinua* dela diogu (laburkiago *I.D.*), ez bada eraztun tribiala eta zeroren zatitzailerik ez badu: $ab = 0$ bada, orduan nahitaez $a = 0$ edo $b = 0$.

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

Integritate-domeinuek oso ezaugarri interesgarri bat dute: elementu bat ez bada 0, sinplifikagarria da biderketarekiko. Izan ere, $a \neq 0$ bada:

$$ab = ac \implies ab - ac = 0 \implies a(b - c) = 0 \overset{a \neq 0}{\implies} b - c = 0 \implies b = c.$$

Gorputz batean, biderketak eragiketa bati normalean eskatzen zaizkion baldintza guztiak betetzen ditu, 0-k alderantzizkoa izatekoa kenduta: elkarkorra eta trukakorra da, neutroa du eta $a \neq 0$ guztiek alderantzizkoa dute. Beraz, gorputzak "eraztunik hoberenak" direla esan dezakegu. Ohartu gorputzak integritate domeinuak direla bereziki: $ab = 0$ badugu eta $a \neq 0$ bada, orduan $a^{-1}$ biderkatuz $b = 0$ lortzen dugu.

**1.8. Adibideak.** 1) $\mathbb{Z}$ I.D. da, baina ez gorputza. Beste alde batetik, $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{R}$ eta $\mathbb{C}$ gorputzak dira.

2) $A$ I.D. bada, orduan $\{a/b \mid a, b \in A,\ b \neq 0\}$ multzoa gorputza da. Gorputz horri $A$-ren *zatikien gorputz* deitzen zaio. Adibidez, $\mathbb{Q}$ $\mathbb{Z}$-ren zatikien gorputza da. Ondo ulertu behar da zatikien gorputzaren eraikuntza guztiz formala dela, bi puntu hauetan oinarriturik:

(i) Alde batetik, $a/b$ elementu bat *zer den* argitzea baino garrantzitsuagoa da horrelako bi elementu noiz diren berdinak/desberdinak ulertzea. Erregela zatiki arrazionalekin erabiltzen den berbera da:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc. \tag{1.1}$$

Behin jakinda hori betetzea nahi dugula, ez da hain zaila $a/b$ elementuari izaera bat ematea. Azkenean, $a/b$ baliokidetasun klase bat izango da $A \times (A \smallsetminus \{0\})$ multzoaren gainean, baliokidetasun-erlazioaren definizioa (1.1) formulatik harturik.

(ii) Bestetik, $a/b$ eta $c/d$ bi elementu nola batu eta nola biderkatu jakin behar dugu. Hemen, berriro ere zenbaki arrazionalen ereduari jarraitzen diogu:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{eta} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

3) $p$ zenbaki lehena bada, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gorputza da. Bestalde, $n$ konposatua bada, $\mathbb{Z}/n\mathbb{Z}$ ez da I.D. Izan ere, $n = r \cdot s$ bada, $1 < r, s < n$ izanik, orduan $\overline{r} \cdot \overline{s} = \overline{0}$ dugu, baina $\overline{r}, \overline{s} \neq \overline{0}$.

4) $K$ gorputza bada, $K[X]$ I.D. da baina ez da gorputza, $K[X]^\times = K \smallsetminus \{0\}$ (polinomio konstante ez-nuluak) baitugu. Dagokion zatikien gorputzari *funtzio arrazionalen gorputz* deitzen zaio eta $K(X)$ gisa idazten dugu. Beraz,

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

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.

**1.9. Definizioa.** Izan bedi $A$ eraztuna. Existitzen bada $n \in \mathbb{N}$, halakoa non $1 + \overset{n}{\cdots} + 1 = 0$ 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.

Adibidez, $\operatorname{char}\mathbb{Z} = \operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$ 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.

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

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

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

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

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

$$a^n = \begin{cases} a \mathrel{\therefore}^{n} a, & n > 0 \text{ bada}, \\ 1, & n = 0 \text{ bada}. \end{cases}$$

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

$$a^n = (a^{-1}) \mathrel{\therefore}^{-n} (a^{-1}).$$

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.

Aurreko notazioa erabiliz, $A$ eraztunaren karakteristika $n > 0$ bada, $n1 = 0$ dugu bereziki. Jarraian, hori bera $A$-ko elementu guztiekin gertatzen dela ikusten dugu.

**1.11. 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. □

Aurretik esan 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.

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

FROGA. Demagun $n = \operatorname{char} K > 0$ 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, $A$ I.D. 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.

**1.13. 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 1.11 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.

## 1.2. 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.

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

(i) $a, b \in \mathfrak{a}$ bada, orduan $a + b \in \mathfrak{a}$.
(ii) $a \in \mathfrak{a}$ eta $x \in A$ bada, orduan $xa \in \mathfrak{a}$.

Demagun $\mathfrak{a}$ $A$-ren ideala dela. Orduan, $x \in A$ bada, $x$-ren *koklasea*

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

multzoa da. Garbi badago $\mathfrak{a}$ zein den, $\overline{x}$ idatziko dugu koklasea sinpleago adierazteko.

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

(i) *Definitzen badugu $\sim$ erlazioa $A$-ren gainean erregela honen bitartez:*

$$x \sim y \iff x - y \in \mathfrak{a},$$

*orduan $\sim$ baliokidetasun-erlazioa da.*
(ii) *Aurreko ataleko erlazioarekiko, $x \in A$ elementu baten baliokidetasun-klasea $\overline{x}$ koklasea da. Beraz, $\overline{x} = \overline{y}$ dugu baldin eta soilik baldin $x - y \in \mathfrak{a}$ bada. Bereziki, $\overline{x} = \overline{0}$ dugu, hain zuzen ere, $x \in \mathfrak{a}$ denean.*
(iii) *$A/\mathfrak{a} = \{\overline{x} \mid x \in A\}$ koklaseen multzoa eraztuna da $\overline{x}+\overline{y} = \overline{x+y}$ eta $\overline{x}\cdot\overline{y} = \overline{xy}$ eragiketekiko. Hori $A$-ren* zatidura-eraztun *bat dela esaten dugu.*

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

$$x \equiv y \pmod{\mathfrak{a}} \iff x - y \in \mathfrak{a}.$$

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):

$$x \equiv y \pmod{\mathfrak{a}},\ z \equiv t \pmod{\mathfrak{a}} \implies x+y \equiv z+t \pmod{\mathfrak{a}},\ xy \equiv zt \pmod{\mathfrak{a}}.$$

**1.16. Adibideak.** 1) $A$ eraztuna bada, $\{0\}$ eta $A$ idealak dira, eta horiek dira $A$-k dituen ideal bakarrak baldin eta soilik baldin $A$ gorputza bada ($A \neq \{0\}$ harturik). Ohartu $A/A = \{\overline{0}\}$ dela, hau da, eraztun tribiala.

2) $n\mathbb{Z} = \{\lambda n \mid \lambda \in \mathbb{Z}\}$ $\mathbb{Z}$-ren ideala da eta dagokion zatidura $\mathbb{Z}/n\mathbb{Z}$ da, kongruentzien bitartez eraiki genuen eraztun bera.

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.

**1.17. 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*

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

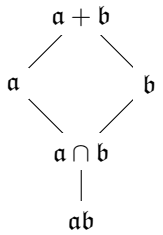
*multzoa da. (Orokorkiago, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideal kopuru* finitu *bat emanda, ideal horiek barruan dituen $A$-ren idealik txikiena $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ batura da, hots, ideal horietan elementu bana harturik eta batuz lortzen dugun azpimultzoa.)*

(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.)*

Partekotasun hauek betetzen dira:




Aurrerago ikusiko dugunez, diagrama horretan agertzen diren partekotasun guztiak hertsiak izan daitezke.

**1.18. 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.

**1.19. 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.

**1.20. 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.)

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

$$(S)=\{x_1a_1+\cdots+x_ka_k \mid x_1,\dots,x_k\in A,\ a_1,\dots,a_k\in S,\ k\in\mathbb{N}\}$$

*berdintza dugu. Bestela esanda, $S$-k sortzen duen ideala $S$-ko elementuekin egin ditzakegun konbinazio guztiek osatzen dute, konbinazio horien "koefizienteak" $A$ eraztunean izanik. Bi kasu berezi hauek azpimarratu nahi ditugu:*

(i) *$S=\{a_1,\dots,a_n\}$ finitua bada, konbinazio horietan $S$-ko elementu guztiak agertzen direla pentsa dezakegu (elementu bat agertzen ez bada, beti uler dezakegu $0$ koefizientearekin agertzen dela); ondorioz,*

$$(a_1,\dots,a_n)=\{x_1a_1+\cdots+x_na_n \mid x_1,\dots,x_n\in A\}.$$

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

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

**1.22. 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, $A=(a)$ betetzen da baldin eta soilik baldin $a$ $A$-ren unitatea bada.

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: $(f_1(X), \dots, f_n(X))$ idealeko elementuak ez dira $f_1(X), \dots, f_n(X)$ polinomioen konbinazio linealak ($K$ gorputzaren gainean), baizik eta polinomio horien multiploen baturak beste polinomio batzuekin biderkatzen ditugunean.

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.

**1.23. 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. □

**1.24. Korolarioa.** *Izan bitez $A$ eraztuna eta $\mathfrak{a} = (a_1, \dots, a_n)$ $A$-ren ideala. Orduan, $i \in \{1, \dots, n\}$ indize bakoitzeko:*

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

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

Froga. Frogatzen badugu $(a, S) \subseteq (b, S)$ partekotasuna, orduan, simetriagatik, berdintza izango dugu. Kontuan izanik 1.23 teorema, nahikoa da $a \in (b, S)$ frogatzea. Baina, $a \equiv b \pmod{(S)}$ izateagatik, $x = a - b$ elementua $(S)$ idealean dago eta, ondorioz, $a = b + x \in (b, S)$ lortzen dugu. □

**1.26. 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,

$$Y^3 + YZ^2 + Z^4 \equiv X^6 + X^2X^3 - X^6 \equiv X^5 \pmod{\mathfrak{b}}$$

dugu eta, azken korolarioa aplikatuz, $\mathfrak{a} = (Y - X^2, Z^2 - X^3, X^5)$ dugu. Hori 1.24 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.

Ondoren ikusten dugunez, 1.24 korolarioaren (i) atalaren alderantzizkoa egiazkoa da integritate-domeinuetan.

**1.27. Teorema.** *Izan bedi $A$ I.D. Orduan, $(a) = (b)$ dugu baldin eta soilik baldin existitzen bada $u \in A^\times$, non $b = ua$ baita.*

Froga. Ezkerralderako norabidean emaitza ezaguna da. Ikus dezagun, beraz, alderantzizko inplikazioa. Lehenengo eta behin, $a$ eta $b$ 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 $a \neq 0$ eta $b \neq 0$ dela. Ohartu, $(a) = (b)$ baldintza betetzeagatik, $a$ $b$-ren multiploa dela eta $b$ $a$-ren multiploa dela. Beraz, $a = xb$ eta $b = ya$ dugu $x, y \in A$ izanik eta, bi berdintza horiek konbinatuz, $a = xya$ lortzen dugu. Hortik, $a \neq 0$ eta $A$ I.D. izateagatik, $1 = xy$ ondorioztatzen dugu eta $y \in A^\times$. Orain, $b = ya$ 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.

**1.28. 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) $\mathfrak{ab} = (ab \mid a \in S,\ b \in T)$.

*Bereziki, $\mathfrak{a} = (a_1, \ldots, a_m)$ eta $\mathfrak{b} = (b_1, \ldots, b_n)$ finituki sortuak badira, orduan*

$$\mathfrak{a} + \mathfrak{b} = (a_1, \ldots, a_m, b_1, \ldots, b_n) \quad \text{eta} \quad \mathfrak{ab} = (a_ib_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n)$$

*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,

$$x = x_1a_1 + \cdots + x_ka_k \qquad \text{eta} \qquad y = y_1b_1 + \cdots + y_\ell b_\ell \tag{1.2}$$

dugu, $x_i, y_i \in A$, $a_i \in S$ eta $b_i \in T$ izanik.

(i) Bakarrik ikusi behar dugu $x + y \in (S \cup T)$ betetzen dela, eta hori garbi dago (1.2)-ko bi berdintzak batuz gero.

(ii) Biderkatzen baditugu (1.2)-ko bi berdintzak, garbi dago $xy \in (ab \mid a \in S,\ b \in T)$ 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, $\mathfrak{ab} \subseteq (ab \mid a \in S,\ b \in T)$ lortzen dugu, 1.23 teorema erabiliz. □

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

## 1.3. Ideal nagusietako domeinuak eta faktorizazio bakarreko domeinuak

Atal honetan integritate-domeinuen bi klase nagusiak sartzen ditugu, ideal nagusietako domeinuak eta faktorizazio bakarreko domeinuak. Bi eraztun mota horiek oso propietate onak betetzen dituzte, eraztun orokorragoekin konparatuta, eta horregatik bereziki interesgarria da horiekin lan egitea.

**1.29. Definizioa.** Eraztun bat *ideal nagusietako domeinua* (laburkiago *I.N.D.*) dela esaten dugu integritate-domeinua bada eta bere ideal guztiak nagusiak badira.

**1.30. Adibideak.** 1) $\mathbb{Z}$ I.N.D. da. Aurretik ikusi dugu $(4, 6) = (2)$ betetzen dela eta, oro har, $\mathfrak{a} = (S)$ $\mathbb{Z}$-ren ideala bada, orduan $\mathfrak{a} = (d)$ dugu, $d$ $S$-ko zenbaki guztien zatitzaile komunetako handiena izanik.

2) Era berean, $K$ gorputza bada, $K[X]$ I.N.D. da. $\mathbb{Z}$-ren kasuko metodo bera erabil dezakegu ideal baten sortzaile bat lortzeko: emandako sortzaileen zatitzaile komunetako handienak balio du.

3) Aitzitik, $K[X, Y]$ ez da I.N.D. Ikus dezagun $(X, Y)$ ideala ez dela nagusia. Absurdora eramanez, demagun $(X, Y) = (f(X, Y))$ dela $f$ polinomio baterako. Jakina, $f \neq 0$ bete behar da. Ohartu, gainera, $f$ ezin dela konstantea izan, kasu horretan $(X, Y) = K[X, Y]$ bailitzateke, eta hori faltsua da (azken batean, $(X, Y)$-ko elementuak gai askerik gabeko polinomioak dira). Bestalde, $(X, Y) = (f(X, Y))$ betetzeagatik, existitzen dira bi polinomio $p, q \in K[X, Y]$, non

$$X = p(X, Y)f(X, Y) \qquad \text{eta} \qquad Y = q(X, Y)f(X, Y)$$

baita. Orain, bi polinomioren biderkadura $X$ baino ez bada, posibilitate bakarra da polinomio horietako bat $\lambda$ konstante ez-nulu bat izatea eta beste polinomioa $\lambda^{-1}X$ izatea. Beraz, $X = p(X, Y)f(X, Y)$ berdintza erabiliz, $f$-k konstante bat bider $X$ izan behar duela lortzen dugu. Baina $Y = q(X, Y)f(X, Y)$ faktorizazioarekin argudiatzen badugu, $f$-k konstante bat bider $Y$ ere izan behar luke. Hori kontraesan bat da eta, ondorioz, $(X, Y)$ ideala ez da nagusia. Era berean, $K[X_1, \ldots, X_n]$ polinomioen eraztunean, bi edozein indeterminatuk (edo gehiagok) sortzen duten ideala ez da nagusia.

4) Antzera ikus daiteke $\mathbb{Z}[X]$ ez dela I.N.D.: $p$ lehena bada, $(p, X)$ ideala ez da nagusia.

Aritmetikaren Oinarrizko Teoremak esaten du $\mathbb{Z}$-ko edozein zenbaki positibo zenbaki lehenen biderkadura gisa deskonposa daitekeela eta faktorizazio hori bakarra dela faktoreen ordena ez badugu kontuan hartzen. Zenbaki negatiboak lortzeko, nahikoa da zenbaki positiboak $-1$-ez biderkatzea; ohartu $-1$ unitatea dela $\mathbb{Z}$-n. Jarraian ematen ditugun definizioek $\mathbb{Z}$-ren ezaugarri hori hartzen dute motibazio gisa.

**1.31. Definizioa.** Izan bitez $A$ eraztuna eta $a \in A$. Elementu hori *irreduziblea* dela diogu bi baldintza hauek betetzen badira:

(i) $a$ ez da $A$-ren unitatea.
(ii) $a$ ezin da faktorizatu unitaterik erabili gabe. Hau da, $a = xy$ badugu, $x, y \in A$ izanik, orduan $x \in A^\times$ edo $y \in A^\times$.

Ohartu 0 ez dela inoiz elementu irreduziblea $A$ eraztun batean: $A$ eraztun tribiala bada, 0 unitatea delako; eta $A$ ez bada tribiala, $0 = 0 \cdot 0$ delako, 0 unitatea izan gabe. Bestalde, $\mathbb{Z}$-ko elementu irreduzibleak zenbaki lehenak dira *eta zenbaki lehenen negatiboak*. Azkenik, $K[X]$-ko elementu irreduzibleak polinomio irreduzibleekin bat datoz.

**1.32. Definizioa.** Izan bedi $A$ integritate-domeinua. Orduan, $A$ *faktorizazio bakarreko domeinua* (laburkiago *F.B.D.*) dela esaten dugu $a \in A$ bakoitza, $a \neq 0$ eta $a$ ez-unitatea izanik, irreduzibleen biderkadura gisa jar badaiteke, funtsean modu bakar batean. Zehazkiago,

$$a = p_1 \dots p_m = q_1 \dots q_n$$

badugu, $p_i$ eta $q_j$ guztiak irreduzibleak izanik, orduan $m = n$ eta, elementuak berrordenatuz, $p_i = u_i q_i$ dugu, $u_i \in A^\times$ izanik.

Integritate-domeinu guztiak ez dira faktorizazio bakarreko domeinuak. Adibidez, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ I.D. da, baina ez F.B.D. Ohartu $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ dela eta faktore guztiak irreduzibleak direla $\mathbb{Z}[\sqrt{-5}]$-en. (Hori ez da zaila frogatzen $\mathbb{Z}[\sqrt{-5}]$-eko normaren propietate biderkakorra erabiltzen badugu; $a + b\sqrt{-5}$ elementuaren norma $a^2 + 5b^2$ da.) Zatidura-aljebrak definitu eta gero, erraz lortuko dugu adibide gehiago. Bestalde, faktorizazio bakarreko domeinuen adibide tipikoak $\mathbb{Z}$ eta $K[X]$ dira. Oro har, honako emaitza hau dugu.

**1.33. Teorema.** *Ideal nagusietako domeinu guztiak faktorizazio bakarreko domeinuak dira.*

Horren alderantzizkoa ez da egiazkoa. Adibidez, hurrengo teoremak ziurtatzen du $K[X_1, \dots, X_n]$ moduko eraztunak faktorizazio bakarreko domeinuak direla, baina, hala ere, ez dira ideal nagusietako domeinuak, $n \geq 2$ bada. (Kontuan izan 1.30 adibideetako hirugarren atala.)

**1.34. Teorema.** *Izan bitez $A$ faktorizazio bakarreko domeinua eta $X$ indeterminatua. Orduan, $A[X]$ ere faktorizazio bakarreko domeinua da.*

Orain ez gara luzatuko bi teorema horien frogak ematen.

Jarraian ikusiko dugunez, faktorizazio bakarreko domeinuetan zatitzaile komunetako handiena eta multiplo komunetako txikiena defini ditzakegu, $\mathbb{Z}$-n edo $K[X]$-n egiten den modura. Definizio horiek eman baino lehen, ohartu F.B.D. batean $a$ eta $b$ bi elementu beti faktoriza daitezkeela irreduzible *berberak* erabiliz, hau da, $a = p_1^{m_1} \dots p_r^{m_r}$ eta $b = p_1^{n_1} \dots p_r^{n_r}$ moduan, $p_i$ guztiak irreduzibleak izanik. Jakina, $m_i$ eta $n_j$ berretzaileetako batzuk 0 izateko aukera onartu behar dugu horretarako.

**1.35. Definizioa.** Izan bedi $A$ F.B.D. eta demagun $a, b \in A$ elementuak honela faktorizatzen direla irreduzibleen biderkadura gisa:

$$a = p_1^{m_1} \dots p_r^{m_r} \quad \text{eta} \quad b = p_1^{n_1} \dots p_r^{n_r}. \tag{1.3}$$

Orduan:

(i) $a$-ren eta $b$-ren *zatitzaile komunetako handiena*, $\operatorname{zkh}(a, b)$ edo $(a, b)$ gisa idazten dena, $A$-ren honako elementu hau da:

$$\operatorname{zkh}(a, b) = p_1^{\min\{m_1, n_1\}} \dots p_r^{\min\{m_r, n_r\}}. \tag{1.4}$$

(ii) $a$-ren eta $b$-ren *multiplo komunetako txikiena*, $\operatorname{mkt}(a, b)$ edo $[a, b]$ gisa idazten dena, $A$-ren honako elementu hau da:

$$\operatorname{mkt}(a, b) = p_1^{\max\{m_1, n_1\}} \dots p_r^{\max\{m_r, n_r\}}. \tag{1.5}$$

Eman dugun definizioarekin zatitzaile komunetako handiena eta multiplo komunetako txikiena ez dira bakarrak. Izan ere, (1.3)-ko faktorizazioetan $p_i$ irreduzibleak ez dira bakarrak, irreduzible horiek unitate batzuez biderkatuz beste faktorizazio batzuk lor baititzakegu. Horrek esan nahi du (1.4) eta (1.5) formuletan ematen ditugun balioak ere ez direla bakarrak eta unitate batez biderkaturik ager daitezkeela. Esate baterako, $\mathbb{Z}$-n unitateak 1 eta $-1$ direnez, zatitzaile komunetako handiena $d$ zenbakia bada, $-d$ dela esatea ere zuzena da. Beraz, $\operatorname{zkh}(4, 6) = 2$ edo $\operatorname{zkh}(4, 6) = -2$ idatz dezakegu. Era berean, $K[X_1, \dots, X_n]$-n unitateak konstante ez-nuluak direnez, horietaz biderkatuz zatitzaile komunetako handienaren balio posible guztiak lortuko ditugu. Adibidez, $(2X^2 - 2, 2X - 2) = 2X - 2$ zein $(2X^2 - 2, 2X - 2) = X - 1$ idatz dezakegu. Hala ere, eraztun horietan baditugu irizpideak zatitzaile komunetako handien guztien artean bakar bat hobesteko: $\mathbb{Z}$-n positiboa den bakarra nahiago izaten dugu eta $K[X_1, \dots, X_n]$-n, berriz, monikoa den polinomio bakarra (hau da, koefiziente nagusia 1 duena).

Ondorengo teoremak argitzen du zergatik erabiltzen diren zatitzaile komunetako handienaren eta multiplo komunetako txikienaren izenak. Froga definizioen eta faktorizazioaren bakartasunaren ondorio berehalakoa da.

**1.36. Teorema.** *Izan bitez $A$ F.B.D. eta $a, b \in A$. Orduan, $\operatorname{zkh}(a, b)$ $a$-ren eta $b$-ren zatitzaile bat da eta $\operatorname{mkt}(a, b)$ $a$-ren eta $b$-ren multiplo bat da. Gainera, $x \in A$ edozein elementutarako:*

(i) *$x$-k $a$ eta $b$ zatitzen ditu baldin eta soilik baldin $\operatorname{zkh}(a, b)$ zatitzen badu.*

(ii) *$x$ $a$-ren eta $b$-ren multiploa da baldin eta soilik baldin $\operatorname{mkt}(a, b)$-ren multiploa bada.*

Adibidez, orain badaukagu modu azkarrago bat ikusteko $(X,Y)$ ideala ez dela nagusia. Izan ere, $(X,Y)=(f(X,Y))$ balitz, orduan $f$-k $X$ eta $Y$ zatituko lituzke. Beraz, $f$-k $\mathrm{zkh}(X,Y)=1$ ere zatituko luke eta, nahitaez, unitate bat izan behar luke. Orduan, $(X,Y)=(f(X,Y))=K[X,Y]$ lortuko genuke, baina hori faltsua da.

**1.37. Teorema.** *Izan bitez $\mathfrak{a}=(a)$ eta $\mathfrak{b}=(b)$ $A$ eraztunaren bi ideal nagusi. Orduan:*

(i) $\mathfrak{ab}=(ab)$ *dugu.*
(ii) *$A$ F.B.D. bada,* $\mathfrak{a}\cap\mathfrak{b}=(\mathrm{mkt}(a,b))$ *dugu.*
(iii) *$A$ I.N.D. bada,* $\mathfrak{a}+\mathfrak{b}=(\mathrm{zkh}(a,b))$ *dugu.*

Froga. (i) Hori 1.28 teoreman ikusi genuen.

(ii) Ohartu $x\in(a)\cap(b)$ dela baldin eta soilik baldin $x$ $a$-ren eta $b$-ren multiploa bada aldi berean. Aurreko teoremagatik, hori gertatzen da $x$ $\mathrm{mkt}(a,b)$-ren multiploa denean, hau da, $x\in(\mathrm{mkt}(a,b))$ denean. Hortik, $(a)\cap(b)=(\mathrm{mkt}(a,b))$ berdintza lortzen dugu.

(iii) $A$ I.N.D. denez, badakigu badagoela $d$ elementu bat, non $(a,b)=(d)$ baita. Orduan, $d$-k $a$ eta $b$ zatitzen ditu eta, beraz, $\mathrm{zkh}(a,b)$ ere bai. Beste alde batetik, $d\in(a,b)$ izateagatik, $d=ax+by$ idatz dezakegu, $x,y\in A$ izanik. Ondorioz, $\mathrm{zkh}(a,b)$-k $d$ zatitzen du, $a$ eta $b$ zatitzen baititu. Beraz, $d$ eta $\mathrm{zkh}(a,b)$ elementuek elkar zatitzen dute eta, horrenbestez, $(d)=(\mathrm{zkh}(a,b))$ berdintza dugu, nahi bezala. □

Oro har, ezin da baieztatu $\mathfrak{a}+\mathfrak{b}=(\mathrm{zkh}(a,b))$ formula betetzen denik F.B.D. batean, ez bada I.N.D. Adibidez, $K[X,Y]$-n, $(X)+(Y)$ ideala ez da nagusia.

**1.38. Adibideak.** 1) Izan bitez $\mathfrak{a}=10\mathbb{Z}$ eta $\mathfrak{b}=15\mathbb{Z}$, $\mathbb{Z}$-ren idealak. Orduan, $\mathfrak{a}+\mathfrak{b}=5\mathbb{Z}$, $\mathfrak{a}\cap\mathfrak{b}=30\mathbb{Z}$ eta $\mathfrak{ab}=150\mathbb{Z}$ dugu.

2) Izan bitez $\mathfrak{a}=(X^2-1)$ eta $\mathfrak{b}=(X^2-X)$, $\mathbb{Q}[X]$-ren idealak. Orduan, $\mathfrak{a}+\mathfrak{b}=(X-1)$, $\mathfrak{a}\cap\mathfrak{b}=(X^3-X)$ eta $\mathfrak{ab}=(X^4-X^3-X^2+X)$ dugu.

3) Izan bitez $\mathfrak{a}=(XY)$ eta $\mathfrak{b}=(XZ)$, $\mathbb{Q}[X,Y,Z]$-ren idealak. Orduan, $\mathfrak{ab}=(X^2YZ)$ eta $\mathfrak{a}\cap\mathfrak{b}=(XYZ)$ dugu. Hala ere, ikus daiteke $\mathfrak{a}+\mathfrak{b}=(XY,XZ)$ ez dela nagusia.

## 1.4. Ideal maximalak, lehenak eta erradikalak

Atal honetan hiru ideal mota garrantzitsu ikusiko ditugu, ideal maximalak, lehenak eta erradikalak, alegia.

**1.39. 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 honako propietate hau betetzen badu:

$$xy \in \mathfrak{a} \quad \Longrightarrow \quad x \in \mathfrak{a} \text{ edo } y \in \mathfrak{a}.$$

(iii) $\mathfrak{a}$ *ideal erradikala* dela diogu honako propietate hau betetzen badu:

$$x^n \in \mathfrak{a}, \quad n \in \mathbb{N} \text{ izanik} \quad \Longrightarrow \quad x \in \mathfrak{a}.$$

Ohartu ideal erradikalaren definizioan ez dela eskatzen propioa izatea.

Hurrengo emaitza Zorn-en Lemaren ondorio erraza da.

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

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

**1.41. 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 $A/\mathfrak{a}$ I.D. bada.*
(iii) *$\mathfrak{a}$ $A$-ren ideal erradikala da baldin eta soilik baldin $A/\mathfrak{a}$-k ez badu elementu nilpotenterik, $\overline{0}$ izan ezik. (Eraztun batean, $a$ elementua* nilpotentea *da $a$-ren berreturaren bat $0$ 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:

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

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,

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

(iii) Aurreko kasuan bezala argudiatuz lortzen da. □

**1.42. Korolarioa.** *Ideal maximalak lehenak dira eta ideal lehenak erradikalak dira.*

**1.43. Korolarioa.** *Izan bedi $A$ eraztuna. Orduan, $\{0\}$ ideal lehena da baldin eta soilik baldin $A$ I.D. bada.*

Badago modu garbiago bat 1.41 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.

**1.44. 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, badugu*

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

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

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

*aplikazioa bijektiboa da.*

(ii) *Aurreko atalaren baldintzetan,*

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

*isomorfismoa dugu.*

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

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.)

**1.45. 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 $6\mathbb{Z}/6\mathbb{Z} = \{\overline{0}\}$, denak erradikalak. Horietatik, $2\mathbb{Z}/6\mathbb{Z}$ eta $3\mathbb{Z}/6\mathbb{Z}$ maximalak dira.

2) Hauek dira $K[X]/(X^n)$-ren idealak: $(X^m)/(X^n)$, non $0 \leq m \leq n$. Ez dira erradikalak $m \geq 2$ bada, eta $(X)/(X^n)$, ordea, maximala da.

Hurrengo teoreman ikusten dugunez, faktorizazio bakarreko domeinu batean erraz ikus daiteke ideal nagusi bat lehena edo erradikala den, sortzaile baten faktorizazioari begiratuta. Bereziki, ideal nagusietako domeinu baten ideal guztiei aplikatzen zaie. Lema bat behar dugu aurretik.

**1.46. Lema.** *Izan bitez $A$ F.B.D. eta $a \in A$ elementu irreduzible bat. Orduan, $a$-k biderkadura bat zatitzen badu, faktoreetako bat zatitu behar du.*

Froga. Demagun $a$-k $x_1 \dots x_n$ zatitzen duela. Orduan, $x_1 \dots x_n = ay$ dugu $y \in A$ elementuren baterako. Berdintza horretan $x_1, \dots, x_n, y$ elementuen ordez beren irreduzibleetako faktorizazioak idazten baditugu, eta $a$ dagoen bezala uzten badugu ($a$ irreduziblea da), orduan bi aldeetan faktorizazio bera ikusi behar dugu. Horrek esan nahi du $a$ elementu irreduzibleak $x_i$ elementu baten faktorizazioan agertu behar duela. Ondorioz, $a$-k $x_i$ zatitzen duela baiezta dezakegu, nahi bezala. □

**1.47. Teorema.** *Izan bitez $A$ F.B.D. eta $a \in A$, $a \neq 0$.*

(i) *($a$) $A$-ren ideal lehena da baldin eta soilik baldin $a$ irreduziblea bada.*
(ii) *($a$) $A$-ren ideal erradikala da baldin eta soilik baldin $a$* karratugabea *bada, hau da, irreduzibleetako bere faktorizazioan ez bada karraturik agertzen.*

Froga. (i) Demagun lehenengo $(a)$ ideal lehena dela. Orduan, $(a) \neq A$ dugu eta $a$ ez da unitatea. Bestetik, $a = xy$ faktorizazio bat badugu, ikus dezagun $x$ edo $y$ unitatea dela. Ohartu $xy \in (a)$ dugula eta, beraz, $x \in (a)$ edo $y \in (a)$ dela. Simetriagatik, $x \in (a)$ dela pentsa dezakegu. Orduan $x = az$ dugu, $z \in A$ izanik, eta hortik $a = azy$. Orain, $A$ I.D. dela eta $a \neq 0$ dela erabiliz, $1 = zy$ dela ondorioztatzen dugu eta $y$ unitatea da $A$-n.

Alderantziz, demagun $a$ irreduziblea dela. Orduan, $a$ ez da unitatea eta, ondorioz, $(a) \neq A$. Orain, demagun $xy \in (a)$ dela. Horrek esan nahi du $a$-k $xy$ zatitzen duela eta, aurreko lema erabiliz, $a$-k $x$ edo $y$ zatitu behar du. Hortaz, $x \in (a)$ edo $y \in (a)$ dugu eta $(a)$ $A$-ren ideal lehena da.

(ii) Antzera ikus daiteke. □

Eraztun gehienetan, ideal nagusi bat ezin da maximala izan. Bai, jakina, $A$ I.N.D. batean. Jarraian frogatuko dugunez, kasu horretan ideal maximalak eta ideal lehenak bat datoz, $\{0\}$ ideal tribialaren salbuespenarekin. Hori ideal lehena da, baina $A$ gorputza denean baino ez da maximala.

**1.48. Teorema.** *Izan bitez $A$ I.N.D. eta $a \in A$, $a \neq 0$. Orduan, $(a)$ maximala da baldin eta soilik baldin lehena bada.*

FROGA. Nahikoa da frogatzea, $(a)$ lehena den baldintzapean, $(a)$ maximala dela. Aurreko teoremaren arabera, badakigu $a$ irreduziblea dela. Demagun orain $(a) \subsetneq \mathfrak{b} \subseteq A$ dela, $\mathfrak{b}$ $A$-ren ideala izanik, eta ikus dezagun $\mathfrak{b} = A$ dela. Hipotesiagatik, $A$ I.N.D. da eta, beraz, $\mathfrak{b} = (b)$ idatz dezakegu. Orduan, $(a) \subseteq (b)$ izateagatik, $a = bc$ dugu $c$ elementuren baterako. Orain, $a$ irreduziblea denez, $b$ edo $c$ unitatea da. Lehenengo kasuan, $(b) = A$ lortzen dugu, nahi bezala. Ordea, $c$ unitatea balitz, orduan $b = ac^{-1}$ izango genuke eta, hortik, $b \in (a)$. Orduan $(a) = (b)$ lortuko genuke, eta hori kontraesan bat da. □

**1.49. Adibideak.** 1) $\mathbb{Z}$-n, $3\mathbb{Z}$ maximala da eta $15\mathbb{Z}$ erradikala da, baina ez lehena.

2) $(X^3 + X + 1)$ maximala da $\mathbb{Q}[X]$-n, baina ez $\mathbb{R}[X]$-n ezta $\mathbb{C}[X]$-n, orduan erradikala baino ez da. (Ohartu $(X^3+X+1)$ multzoa desberdina dela hiru eraztun horietan.)

3) $(X^2 + 1)$ maximala da $\mathbb{R}[X]$-n, baina ez $\mathbb{C}[X]$-n.

4) $(f(X))$ maximala da $\mathbb{C}[X]$-n baldin eta soilik baldin $f(X)$ lehenengo mailakoa bada. Ondorioz,

$$\{(X - a) \mid a \in \mathbb{C}\}$$

multzoan $\mathbb{C}[X]$-ren ideal maximal guztiak agertzen dira, errepikapenik gabe. Emaitza hori, $\mathbb{C}$-rekin ez ezik, edozein gorputz aljebraikoki itxirekin ere betetzen da.

5) $K$ edozein gorputz izanik, $(X + Y)$ ideal lehena da $K[X, Y]$-n, baina ez maximala. Adibidez, $(X + Y) \subsetneq (X, Y) \subsetneq K[X, Y]$ dugu.

6) $K$ edozein gorputz izanik, $(X, Y)$ ideal maximala da $K[X, Y]$-n (eta ez nagusia). Izan ere, $(X, Y)$ multzoa gai askerik gabeko polinomioek osatzen dute. Orain, $(X, Y) \subsetneq \mathfrak{b} \subseteq K[X, Y]$ bada, aukeratu polinomio bat $f \in \mathfrak{b} \setminus (X, Y)$. Orduan, $f$-ren gai askea ez da zero eta $f = \lambda + g$ idatz dezakegu, $\lambda \in K^\times$ eta $g \in (X, Y)$ izanik. Hortik $\lambda \in \mathfrak{b}$ lortzen dugu eta, $\lambda$ $K[X, Y]$-ren unitatea denez, $\mathfrak{b} = K[X, Y]$ ondorioztatzen dugu.

7) Oro har, $(X_1, \ldots, X_n)$ maximala da $K[X_1, \ldots, X_n]$-n. (Aurreko adibideko argudio berak balio du.)

? Nolakoa izan behar du $f(X)$ polinomioak $(f(X))$ maximala izateko $\mathbb{R}[X]$-n?

## 1.5. Lokalizatuak

$A$ integritate-domeinua bada, ikusi dugu $K$ gorputz baten barruan sar daitekeela, zatikien gorputz deitutakoa. Eskuarki, eraztun asko topa daitezke $A$-ren eta

$K$-ren artean. Adibidez, $\mathbb{Z}$-ren eta $\mathbb{Q}$-ren artean eraztun familia infinitu bat lortzen dugu, $p$ zenbaki lehen bakoitzeko

$$\left\{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \text{ ez da } p\text{-ren multiploa}\right\}$$

hartuz. Eraztun horien eraikuntza $A$ edozein eraztunen kasura orokortu nahi dugu atal honetan, eta lortzen diren eraztun berrien propietate nagusiak estudiatu.

**1.50. Definizioa.** Izan bitez $A$ I.D. eta $\mathfrak{p}$ $A$-ren ideal lehena. Orduan,

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

multzoa definitzen dugu, $A$-ren zatikien gorputzaren barruan. Hori $\mathfrak{p}$ idealarekiko $A$-ren *lokalizatua* dela esaten dugu.

$A_{\mathfrak{p}}$-ren definizioan, jakiteko $a/b$ zatiki bat multzo horren barruan dagoen edo ez, zatikiaren $b$ izendatzaileari begiratzen diogu, $\mathfrak{p}$ ideal lehenetik kanpo egoteko eskatuz. Dakigunez, zatiki baten adierazpena ez da bakarra, eta horregatik pentsatu beharko genuke zatiki horren beraren beste adierazpen bat, adibidez $x/y$, hartuz gero, ea $y$ ere $\mathfrak{p}$-tik kanpo egongo den. Hau da, $a/b = x/y$ bada, $b \notin \mathfrak{p}$ izanik, izan behar du $y \notin \mathfrak{p}$? Laster konturatzen gara propietate hori ez dela egiazkoa. Adibidez, $\mathbb{Z}$-n $(2)$ ideal lehena hartuz gero, orduan $1/3 = 2/6$ dugu eta $3 \notin (2)$, baina hala ere $6 \in (2)$. Orduan, zer egin behar dugu: $1/3$ elementua $\mathbb{Z}_{(2)}$ lokalizatuan sartu behar dugu edo ez? Edo $\mathbb{Z}_{(2)}$ ondo definiturik ez dagoela esan beharko genuke besterik gabe? Problema horri soluzioa emateko, zehaztu behar dugu nola ulertzen dugun $A_{\mathfrak{p}}$ lokalizatuaren definizioa: zatiki bat $A_{\mathfrak{p}}$-n dagoela esango dugu *existitzen bada* elementu horren adierazpen bat, $a/b$, non $b \notin \mathfrak{p}$ den. Beraz, $1/3 \in \mathbb{Z}_{(2)}$ dela esan dezakegu.

$A$ F.B.D. izanez gero, orduan $A$-ren zatikien gorputzeko edozein elementuk $a/b$ moduko adierazpen laburtezin bakar bat du, hau da, $\text{zkh}(a, b) = 1$ izanik. Orduan, erraz egiazta daiteke adierazpen horrek erabakitzen duela elementua $A_{\mathfrak{p}}$-n dagoen edo ez: elementu horren zatiki moduko adierazpen baten izendatzailea $\mathfrak{p}$-tik kanpo egongo da baldin eta soilik baldin $b \notin \mathfrak{p}$ bada.

**1.51. Teorema.** *Izan bitez $A$ I.D. eta $\mathfrak{p}$ $A$-ren ideal lehena. Orduan, $A_{\mathfrak{p}}$ multzoa $A$-ren zatikien gorputzaren azpieraztuna da. Gainera, $A \subseteq A_{\mathfrak{p}}$ partekotasuna dugu, ohikoa den bezala $a \in A$ elementu bakoitza $a/1$ zatikiarekin identifikatzen badugu.*

Froga. Bakarrik frogatu behar dugu, $a/b$ eta $c/d$ $A_{\mathfrak{p}}$-n egonez gero, $a/b + c/d$ eta $a/b \cdot c/d$ ere $A_{\mathfrak{p}}$-n daudela. Hori berehalakoa da, $b, d \notin \mathfrak{p}$ baldintzatik $bd \notin \mathfrak{p}$ ondorioztatzen baitugu, $\mathfrak{p}$ $A$-ren ideal lehena izateagatik. □

Eraztun baten lokalizatu bat *ideal lehen batekiko* hartu behar da beti, eta ez ideal orokor batekiko, aurreko frogak argi erakusten duen bezala.

Pasatzen garenean $\mathbb{Z}$-tik $\mathbb{Q}$-ra, helburua da zenbaki oso ez-nulu guztiak unitate bihurtzea. Zein zenbaki oso bihurtzen dira unitate, adibidez, $\mathbb{Z}_{(2)}$ lokalizatura

pasatzean? Badugunez

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

dela, $\mathbb{Z}$-ko zenbaki bakoiti guztiak unitate bihurtzen dira $\mathbb{Z}_{(2)}$-n, eta horiek baino ez. Ondorioz, 3-ak $\mathbb{Z}_{(2)}$ osoa sortzen du, nahiz eta $\mathbb{Z}$-n 3-ak ez duen eraztun osoa sortzen. Oro har, hori da lokalizatuaren ideia: $\mathfrak{p}$-tik kanpoko elementu guztiak unitate bihurtzen dira $A$-tik $A_\mathfrak{p}$-ra pasatzean (eta beraz $A_\mathfrak{p}$ osoa sortzen dute), eta horiek baino ez.

$\mathbb{Z}_{(2)}$-ren adibidearekin jarraituta, zein da $(a/b)$ ideal nagusi orokor bat? Hori ikusteko, idatzi $a = 2^n c$ moduan, $c$ bakoitia izanik. Zenbaki bakoitiak unitateak direnez $\mathbb{Z}_{(2)}$-n, $(a/b) = (2^n c/b) = (2^n)$ dugu. Beraz, ideal guztiak (2)-ren barruan daude eta (2) da $\mathbb{Z}_{(2)}$-ren ideal maximal bakarra. Hurrengo teoremetan ikusiko dugunez, $\mathbb{Z}_{(2)}$-ren propietate horiek ez dira kasualitateak.

**1.52. Teorema.** *Izan bitez $A$ eraztuna eta $\mathfrak{p}$ $A$-ren ideal lehena. Orduan:*

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

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

*$A_\mathfrak{p}$-ren ideala da. Zehazkiago, hau da $\mathfrak{a}$-k $A_\mathfrak{p}$-n sortzen duen ideala.*

(ii) *Alderantziz, $\mathfrak{A}$ $A_\mathfrak{p}$-ren ideala bada eta $\mathfrak{a} = \mathfrak{A} \cap A$ definitzen badugu, orduan $\mathfrak{A} = \mathfrak{a}A_\mathfrak{p}$ dugu. Beraz, $A_\mathfrak{p}$ lokalizatuaren ideal guztiak (i) atalekoak bezalakoak dira.*

(iii) *$a/b \in A_\mathfrak{p}$ unitatea da baldin eta soilik baldin $a \notin \mathfrak{p}$ bada.*

(iv) *$\mathfrak{a}A_\mathfrak{p} \neq A_\mathfrak{p}$ desberdintza dugu baldin eta soilik baldin $\mathfrak{a} \subseteq \mathfrak{p}$ bada.*

Froga. (i) Berehalakoa da $\mathfrak{a}A_\mathfrak{p}$ $A_\mathfrak{p}$-ren ideala dela,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{eta} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

formuletan oinarrituz. Bestalde, $\mathfrak{a}$-ko elementuekin konbinazioak egiten baditugu $A_\mathfrak{p}$-ko elementuekin biderkaturik, garbi dago $\mathfrak{a}A_\mathfrak{p}$ lortzen dela, $\mathfrak{a}$ $A$-ren ideala izateagatik. Hortaz, $\mathfrak{a}A_\mathfrak{p}$ $\mathfrak{a}$-k $A_\mathfrak{p}$-n sortzen duen ideala da.

(ii) Oro har, $A \subseteq B$ bi eraztun badira eta $\mathfrak{b}$ $B$-ren ideala bada, argi dago $\mathfrak{b} \cap A$ $A$-ren ideala dela. Beraz, gure kasuan, $\mathfrak{a} = \mathfrak{A} \cap A$ $A$-ren ideala da. Orain, $\mathfrak{a}$ $\mathfrak{A}$-ren barruan dago, eta azken hori $A_\mathfrak{p}$-ren ideala da. Beraz, $\mathfrak{a}$-k $A_\mathfrak{p}$-n sortzen duen ideala, $\mathfrak{a}A_\mathfrak{p}$ alegia, $\mathfrak{A}$-ren barruan dago. Ikus dezagun alderantzizko partekotasuna ere betetzen dela. Horretarako, hartu $a/b$ elementu orokor bat $\mathfrak{A}$-n. Orduan, $b$-z biderkatuz, $a \in \mathfrak{A}$ lortzen dugu eta, ondorioz, $a \in \mathfrak{a}$. Beraz $a/b \in \mathfrak{a}A_\mathfrak{p}$ lortzen dugu, nahi bezala.

(iii) Demagun, lehenengo eta behin, $a/b$ $A_\mathfrak{p}$-ren unitatea dela. Orduan, existitzen da $x/y \in A_\mathfrak{p}$ non $a/b \cdot x/y = 1$ den, hau da, $ax = by$. Gorago aipatu dugun bezala, $a/b, x/y \in A_\mathfrak{p}$ izateagatik eta $\mathfrak{p}$ ideal lehena izateagatik, $by \notin \mathfrak{p}$ dugu. Beraz, $ax \notin \mathfrak{p}$ dugu eta, $\mathfrak{p}$ $A$-ren ideala denez, $a \notin \mathfrak{p}$ ondorioztatzen dugu. Alderantziz, $a \notin \mathfrak{p}$ bada, orduan $b/a$ zatikia $A_\mathfrak{p}$-n dago eta, ondorioz, $a/b$ $A_\mathfrak{p}$-ren unitatea da.

(iv) Hori aurreko atalaren ondorioa da: kontuan izan ideal bat eraztun osoaren berdina dela baldin eta soilik baldin eraztunaren unitate bat badu. □

Ohartu $\mathfrak{a}A_{\mathfrak{p}}$-ren definizioa ere ondo ulertu behar dugula: elementu bat $\mathfrak{a}A_{\mathfrak{p}}$-n dago hori adierazteko balio duen $a/b$ zatikiren batek (ez guztiek) betetzen badu $a \in \mathfrak{a}$, $b \notin \mathfrak{p}$. Beraz, $x/y \in \mathfrak{a}A_{\mathfrak{p}}$ izateagatik ezin dugu besterik gabe esan $x \in \mathfrak{a}$ izango denik, baizik eta existitzen dela $a/b$ non $x/y = a/b$ eta $a \in \mathfrak{a}$, $b \notin \mathfrak{p}$ den. Adibidez, $\mathbb{Z}$-n $\mathfrak{p} = 2\mathbb{Z}$ eta $\mathfrak{a} = 3\mathbb{Z}$ hartzen baditugu, orduan $1/5 \in 3\mathbb{Z}_{(2)}$ dugu, nahiz eta $1 \notin 3\mathbb{Z}$. Izan ere, $1/5 = 3/15$ dugu, $3 \in 3\mathbb{Z}$ eta $15 \notin 2\mathbb{Z}$ izanik. (Edo bestela, gogoratu $3\mathbb{Z}_{(2)} = \mathbb{Z}_{(2)}$ dela, 3-a $\mathbb{Z}_{(2)}$-n unitatea izateagatik.) Hala eta guztiz ere, hurrengo teoreman ikusiko dugun bezala, $\mathfrak{a} \subseteq \mathfrak{p}$ ideal lehena bada, orduan egia da $a/b \in \mathfrak{a}A_{\mathfrak{p}}$ izatetik $a \in \mathfrak{a}$ ondorioztatzen dela.

Aurreko teoremaren arabera, $A_{\mathfrak{p}}$-ren ideal propioak ezagutu nahi baditugu, nahikoa da $\mathfrak{p}$-ren barruan $A$-ren idealak bilatzea. Hortik dator lokalizatuaren izena eraztun horretarako. Hain zuzen ere, $A$-tik $A_{\mathfrak{p}}$-ra pasatzean $\mathfrak{p}$-tik kanpoko elementu guztiak unitate bihurtzen dira eta, idealei dagokienez, bakarrik du garrantzia $\mathfrak{p}$-ren barruan gertatzen denak: eraztunaren estudioa $\mathfrak{p}$-ren barruan lokalizatu egiten dugu.

Orain honako galdera hau azaltzen zaigu: $\mathfrak{a}A_{\mathfrak{p}}$ idealak dira, $\mathfrak{a} \subseteq \mathfrak{p}$ izanik, $A_{\mathfrak{p}}$-ren ideal propio guztiak bai, baina ba al dira desberdinak $A$-ren ideal desberdinetatik abiatzen bagara? Erraz ikus dezakegu hori ez dela horrela. Adibidez, (2) eta (6) $\mathbb{Z}$-ren idealak (2) ideal lehenaren barruan daude eta desberdinak dira, baina $\mathbb{Z}_{(2)}$-n sortzen dituzten idealak berdinak dira, $6 = 2 \cdot 3$ delako eta 3-a $\mathbb{Z}_{(2)}$-ren unitatea delako. Oro har, $2\mathbb{Z}_{(2)} = 2 \cdot 3^n\mathbb{Z}_{(2)}$ berdintza dugu $n \geq 0$ guztietarako. Hala ere, ondorengo teoreman ikusten dugun bezala, problema hori desagertu egiten da $\mathfrak{p}$-ren barruan ideal lehenetara mugatzen bagara. Teorema horren froga ez dugu hemen azalduko.

**1.53. Teorema.** *Izan bitez $A$ eraztuna eta $\mathfrak{p}$ $A$-ren ideal lehena. Orduan:*

(i) *$\mathfrak{q}$ $A$-ren ideal lehena bada, $\mathfrak{q} \subseteq \mathfrak{p}$ izanik, orduan $a/b \in \mathfrak{q}A_{\mathfrak{p}}$ dugu baldin eta soilik baldin $a \in \mathfrak{q}$ bada.*

(ii) *Badugu bikjekzio bat*

$$\begin{array}{ccc} \{\mathfrak{q} \mid \mathfrak{q} \text{ } A\text{-ren ideal lehena eta } \mathfrak{q} \subseteq \mathfrak{p}\} & \longrightarrow & \{A_{\mathfrak{p}}\text{-ren ideal lehenak}\} \\ \mathfrak{q} & \longmapsto & \mathfrak{q}A_{\mathfrak{p}}. \end{array}$$

(iii) *$A_{\mathfrak{p}}$ lokalizatuak ideal maximal bakarra du, $\mathfrak{p}A_{\mathfrak{p}}$, alegia.*

Adibidez, $p \in \mathbb{Z}$ lehena bada, $\mathbb{Z}_{(p)}$ lokalizatuak bi ideal lehen baino ez ditu, $\{0\}$ eta $p\mathbb{Z}_{(p)}$, eta azken hori maximala da. Antzera gertatzen da $K[X]_{(p(X))}$-n, $p(X)$ polinomio irreduziblea bada.

Demagun $\mathfrak{a}A_{\mathfrak{p}}$ $A_{\mathfrak{p}}$-ren ideal lehena dela, $\mathfrak{a} \subseteq \mathfrak{p}$ izanik. Orduan, *azken teoremak ez dio $\mathfrak{a}$-k $A$-ren ideal lehena izan behar duenik*, baizik eta badagoela $\mathfrak{b}$ $A$-ren ideal lehena, halakoa non $\mathfrak{b}A_{\mathfrak{p}} = \mathfrak{a}A_{\mathfrak{p}}$ baita. Adibidez, $18\mathbb{Z}_{(2)} = 2\mathbb{Z}_{(2)}$ ideal lehena da $\mathbb{Z}_{(2)}$-n, baina $18\mathbb{Z}$ ez da lehena $\mathbb{Z}$-n.

Zer esan dezakegu $A_{\mathfrak{p}}$ lokalizatuaren ideal erradikalei buruz? Ez da zaila frogatzen, $\mathfrak{a}$ $A$-ren ideal erradikala izanez gero, $\mathfrak{a}A_{\mathfrak{p}}$ $A_{\mathfrak{p}}$-ren ideal erradikala dela. Gainera, modu horretan $A_{\mathfrak{p}}$-ren ideal erradikal guztiak lor daitezke. Hala ere, $\mathfrak{p}$-ren barruan dauden bi ideal erradikal desberdinek $A_{\mathfrak{p}}$-ren ideal bera eman diezagukete: $2\mathbb{Z}_{(2)} = 6\mathbb{Z}_{(2)}$ dugu, nahiz eta $2\mathbb{Z} \neq 6\mathbb{Z}$ izan.

## 1.6. Polinomioak

Orain arte polinomioen eraztunak behin baino gehiagotan agertu bazaizkigu ere, gehienbat koefizienteak gorputz batean izanik, atal honetan polinomioen teoriaren garapen sistematikoago bat egingo dugu, oinarrizko kontzeptu guztiak definituz.

**1.54. Definizioa.** Izan bitez $A$ eraztuna eta $X_1, \ldots, X_n$ indeterminatuak.

(i) *Monomio* bat $X_1^{i_1} \ldots X_n^{i_n}$ moduko adierazpen bat da, $i_j \geq 0$ zenbaki osoak izanik. (Hor, $i_j$ berretzaile guztiak 0 badira, monomioa 1 dela ulertzen da.) Monomioaren *maila osoa* $i_1 + \cdots + i_n$ batura da eta $X_j$*-rekiko maila* $i_j$ berretzailea da.

(ii) *Polinomio* bat $A$-ren gainean, monomio kopuru finitu baten konbinazio lineal bat da, koefizienteak $A$-n izanik. Baldin eta $f$ polinomioak $X_1, \ldots, X_n$ indeterminatuak erabiltzen baditu, askotan $f(X_1, \ldots, X_n)$ idatziko dugu hori adierazteko. Definizioaren arabera, hau da polinomio orokor baten itxura:

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

$a_{i_1, \ldots, i_n} \in A$ koefizienteen artean bakarrik kopuru finitu bat izanik zeroren desberdina.

(iii) $f$ polinomioa ez bada 0, orduan $f$-ren *maila osoa*, $\deg f$ ikurraren bidez adieraziko duguna, koefiziente ez-nulua duten monomioen maila osorik handiena da. Koefiziente guztiak zero badira, hau da, 0 polinomio konstantearen kasuan, honela definitzen dugu maila osoa: $\deg 0 = -\infty$. Antzera definitzen da $f$-ren *maila* $X_j$ *indeterminatuarekiko*, $\deg_{X_j} f$.

(iv) $A[X_1, \ldots, X_n]$ koefizienteak $A$-n dituzten eta $X_1, \ldots, X_n$ indeterminatuak erabiltzen dituzten polinomio guztien multzoa da.

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.

Era natural batean, $A[X_1, \ldots, X_n]$ polinomioen multzoari eraztun-egitura eman diezaiokegu, bi eragiketa hauek kontuan hartuz:

(i) Batuketa: Bi polinomioren batura lortzeko, batu monomio bakoitzaren koefizienteak bi polinomioetan.

(ii) Biderketa: Bi monomio biderkatzeko berretzaileak batzen ditugu, hau da,

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

eta horretan oinarrituz bi polinomioren biderkadura definitzen dugu, propietate banakorra bete dadin eskatuz.

Ohartu $A[X_1,\dots,X_n]$ eta $A[X_1,\dots,X_{n-1}][X_n]$ eraztunak identifika daitezkeela. Adibidez $K[X,Y]$ eraztuna, komenigarria bada, $K[X][Y]$ edo $K[Y][X]$ gisa ikus dezakegu. Hiru ikuspuntu horien arteko diferentzia indeterminatu bakoitzari ematen diogun garrantzian datza. Lehenengo aukeran, $K[X,Y]$-ren kasuan, $X$ eta $Y$ indeterminatuak berdin ikusten ditugu; $K[X][Y]$-ren kasuan, berriz, $Y$ indeterminatuari ematen diogu rol nagusia eta $X$ konstantetzat hartzen dugu; eta $K[Y][X]$-ren kasuan, alderantziz egiten dugu.

Hurrengo teoremaren froga berehalakoa da.

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

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

(ii) $\deg(fg)\le\deg f+\deg g$ *dugu eta, gainera, $A$ I.D. bada, orduan berdintza dugu.*

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

$A$ ez bada I.D., ezin da beti ziurtatu $\deg(fg)=\deg f+\deg g$ izango denik. Izan ere, $A$ I.D. ez izateagatik, badaude $ab=0$ betetzen duten bi elementu ez-nulu, $a$ eta $b$. Orain, hartzen baditugu $f$ eta $g$ bi polinomio $A[X]$-n, $f$-ren koefiziente nagusia $a$ eta $g$-rena $b$ izanik, orduan $\deg(fg)<\deg f+\deg g$ dugu. Adibidez, $f(X)=g(X)=\overline{2}X$ har ditzakegu $\mathbb{Z}/4\mathbb{Z}[X]$-n. Kasu horretan bi polinomioen biderkadura 0 da, polinomioak 0 izan gabe; horrek erakusten du, bide batez, $\mathbb{Z}/4\mathbb{Z}[X]$ ez dela I.D.

Baldin badakigu $A$ eraztuna zein motatakoa den, zer esan dezakegu $A[X_1,\dots,X_n]$ eraztunari buruz? Honako propietate hauek ditugu:

(i) $A$ I.D. bada, orduan $A[X_1,\dots,X_n]$ ere I.D. da.

(ii) $A$ F.B.D. bada, orduan $A[X_1,\dots,X_n]$ ere F.B.D. da. (Hau 1.34 teoremaren ondorioa da.)

(iii) $A$ I.N.D. bada, $A[X]$-k ez du zertan I.N.D. izan: hartu adibidez $A=\mathbb{Z}$ edo $K[Y]$.

(iv) $K$ gorputza bada, $K[X]$ ez da gorputza, bere unitateak konstante ez-nuluak baino ez baitira. Hala ere, $K[X]$-ko zatiketaren algoritmoari esker, $K[X]$ I.N.D. dela frogatu daiteke. Zehazkiago, $\mathfrak{a}\neq\{0\}$ $K[X]$-ren ideala bada, orduan $\mathfrak{a}$-ren sortzaile bat lortzeko nahikoa da maila txikieneko polinomio ez-nulu bat hartzea $\mathfrak{a}$-ren barruan.

Ondoren, polinomioen eraztun baten unitateak zein diren determinatzen dugu, koefizienteak integritate-domeinu baten gainean badaude.

**1.56. Teorema.** *Izan bedi $A$ I.D. Orduan, $A[X_1, \ldots, X_n]$-ren unitateak $A$-ren unitateekin bat datoz. Bereziki, $K$ gorputza bada, orduan $K[X_1, \ldots, X_n]$-ren unitateak konstante ez-nuluak dira.*

FROGA. Hori biderkaduraren maila mailen batura izateagatik gertatzen da. Izan ere, $f, g \in A[X_1, \ldots, X_n]$ eta $fg = 1$ bada, orduan $\deg f + \deg g = \deg(fg) = \deg 1 = 0$ eta, halabeharrez, $\deg f = \deg g = 0$ izan behar du. Beraz, $fg = 1$ betetzen bada, orduan $f$ eta $g$ konstanteak dira, hau da, $A$-n daude. Horrek esan nahi du $A[X_1, \ldots, X_n]$-ren unitateak $A$-ren unitateak direla. □

Aurreko teorema ez da betetzen $A$ eraztun guztietarako. Adibidez, $A = \mathbb{Z}/4\mathbb{Z}$ bada, orduan $(\overline{2}X + \overline{1})^2 = \overline{4}X^2 + \overline{4}X + \overline{1} = \overline{1}$ dugu eta, ondorioz, $\overline{2}X + \overline{1}$ unitatea da $\mathbb{Z}/4\mathbb{Z}[X]$-n. Hala ere, horrek ez gaitu kezkatu behar, guk erabiliko ditugun polinomio guztiek koefizienteak integritate-domeinu batean izango baitituzte.

Polinomioen eraztunen propietate garrantzitsuenetako bat Hilbert-en oinarriaren teorema da. Horren enuntziatua emateko, Noether-en eraztunaren kontzeptua behar dugu.

**1.57. Definizioa.** Izan bedi $A$ eraztuna. Orduan, *$A$ Noether-en eraztuna* dela esaten dugu $A$-ren ideal guztiak finituki sortuak badira, hau da, elementu kopuru finitu baten bidez sor badaitezke.

Adibidez, ideal nagusietako domeinuak (bereziki, gorputzak) Noetherren eraztunak dira. Oso emaitza garrantzitsua da Noetherren eraztunak kate-baldintza baten bidez karakteriza daitezkeela.

**1.58. Teorema.** *Izan bedi $A$ eraztuna. Orduan, baliokideak dira:*

(i) *$A$ Noetherren eraztuna da.*

(ii) *Ezin da eraiki $A$-ren idealen kate hertsiki gorakor infiniturik. Bestela esanda,*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_i \subseteq \cdots$$

*$A$-ren idealen kate gorakor infinitu bat bada, orduan gelditzen da, hau da, existitzen da $m \in \mathbb{N}$, non $\mathfrak{a}_i = \mathfrak{a}_m$ baita $i \geq m$ guztietarako.*

**1.59. Teorema** (Hilberten oinarriaren teorema)**.** *Izan bedi $A$ Noetherren eraztuna. Orduan, $A[X]$ ere Noetherren eraztuna da.*

**1.60. Korolarioa.** *Izan bitez $K$ gorputza eta $n \in \mathbb{N}$. Orduan, $K[X_1, \ldots, X_n]$-ren ideal guztiak finituki sortuak dira.*

Geometria aljebraikoko ikastaro honetan, askotan ebatzi beharko dugu honako problema hau: $K[X_1, \ldots, X_n]$-ren $\mathfrak{a}$ ideal bat emanda, erabakitzea ideal lehena den edo ez. Teorian behintzat, kasurik errazena da $\mathfrak{a} = (f)$ ideal nagusia denean. Orduan, 1.47 teoremaren arabera, $f$ polinomioaren irreduzibilitatea aztertu behar dugu. Orain arte, irreduzibilitaterako ezagutzen ditugun irizpide guztiek $f \in K[X]$

polinomio baterako balio dute, hau da, gorputz baten gainean eta indeterminatu bakar baten kasurako, baina oraingo honetan $f \in K[X_1, \ldots, X_n]$ dugu. Irtenbide bat indeterminatuetako bati rol nagusia ematea izan daiteke, adibidez $X_n$-ri. Horrek esan nahi du $K[X_1, \ldots, X_n]$ eraztuna $K[X_1, \ldots, X_{n-1}][X_n]$ gisa ikusten ari garela, hau da, $X_n$ balitz bezala indeterminatu bakarra eta polinomioen koefizienteak $K[X_1, \ldots, X_{n-1}]$-eko polinomioak balira bezala. Bestela esanda, $f \in A[X]$ idatz dezakegu, $X = X_n$ eta $A = K[X_1, \ldots, X_{n-1}]$ izanik. Baina orain konturatzen gara $A$ ez dela gorputza eta ez dakigula $K[X]$-n ezagutzen genituen metodoek $A[X]$-n ere balio izango duten. Edonola ere, $A$ F.B.D. denez, "eraztun ona" dela pentsa dezakegu, eta beharbada $A[X]$-n irreduzibilitatearen azterketa ez dela oso desberdina izango, $K[X]$-ren kasuarekin alderatuta. Horregatik guztiagatik, ondorengo problema orokor hau estudiatuko dugu atal honetako gainerako zatian.

**1.61. Problema.** *$A$ F.B.D. bada, zein puntutaraino balio dute $A[X]$-n gorputz baten gaineko koefizienteen kasuan ezagutzen ditugun irreduzibilitaterako irizpideek?*

Lehenengo eta behin, gogora ditzagun oinarrizko emaitza batzuk, koefizienteak gorputz batean daudenean balio dutenak. Izan bitez $K$ gorputza eta $f \in K[X]$. Orduan:

(P1) $\deg f = 1$ bada, $f$ irreduziblea da $K[X]$-n.
(P2) $\deg f \geq 2$ bada eta $f$-k erro bat badu $K$-n, $f$ ez da irreduziblea $K[X]$-n.
(P3) $\deg f = 2$ edo 3 bada eta $f$-k ez badu errorik $K$-n, $f$ irreduziblea da $K[X]$-n.

Ikus dezagun, adibide batzuen bitartez, zer gertatzen den gorputz baten ordez faktorizazio bakarreko domeinu bat jarriz gero.

**1.62. Adibideak.** 1) $f(X) = 2X+2$ ez da irreduziblea $\mathbb{Z}[X]$-n, lehenengo mailakoa den arren. Izan ere, $f(X) = 2(X + 1)$ dugu, eta ez 2 ez $X + 1$ ez dira unitateak $\mathbb{Z}[X]$-n. Jakina, faktorizazio horrek ez du gezurtatzen $f(X)$-ren irreduzibilitatea $\mathbb{Q}$-ren gainean,* 2-a unitatea baita $\mathbb{Q}[X]$-n.

2) Izan bedi $f(X, Y) = XY + Y \in K[X, Y]$. Ikusten badugu $K[X, Y]$ eraztuna $K[Y][X]$ gisa, hau da, polinomioak $X$-rekiko bakarrik ikusiz, orduan $f$ lehenengo mailakoa da, baina ez da irreduziblea. Izan ere, $f(X, Y) = Y(X + 1)$ dugu eta $Y$ ez da unitatea $K[Y][X]$-n. Hala ere, $f(X, Y)$ irreduziblea da $K[Y][X]$-ren ordez $K(Y)[X]$ erabiltzen badugu. Kasu horretan, koefizienteak $K(Y)$ gorputzean hartzen ditugu, eta horretan $Y$ unitatea da. Beraz, $f(X, Y) = Y(X + 1)$ faktorizazioa ez dugu kontuan hartu behar beste kasu horretan, faktoreetako bat unitatea baita.

Aurreko adibideek erakusten duten bezala, (P1) propietatea ez da betetzen $A$ F.B.D. bada. Gainera, $K$ $A$-ren zatikien gorputza bada, orduan $f(X) \in A[X]$ polinomio batek portaera desberdinak izan ditzake $A[X]$-n eta $K[X]$-n irreduzibilitateari dagokionez. Garbi dago nondik datorren diferentzia hori: $f$-k $A$-n dagoen

*Oharra terminologiaren aldetik: *$f$ $A[X]$-n irreduziblea dela adierazteko beste modu bat $f$ $A$-ren gainean* irreduziblea dela esatea da. Ez nahasi bi aukera horiek eta ez esan mesedez polinomio bat $A[X]$-ren gainean edo $A$-n irreduziblea denik.

faktore konstante bat izan dezake, $A$-n unitatea ez dena, baina jakina $K$-n unitatea izango dena edonola ere.

Azter dezagun orain zer gertatzen den (P2) propietatearekin. Demagun $f \in A[X]$ polinomioak $a$ erroa duela $A$-n. Zatiketaren algoritmoa erabiltzen badugu $f(X)$ $X-a$-z zatitzeko, orduan $f(X) = q(X)(X-a)+r$ lortzen dugu, $r$ konstantea izanik. Berdintza horretan $X = a$ ordezkapena eginez, $r = f(a) = 0$ lortzen dugu. Beraz, $f(X) = q(X)(X-a)$ dugu eta $f$ ez da irreduziblea. Horrek erakusten du (P2) propietatea edozein eraztunen gainean balio duela (ez dugu behar $A$ F.B.D. ezta I.D. izaterik).

Zatiketaren algoritmoak, berez, $K[X]$-n funtzionatzen du, $K$ gorputza izanik. $A$ ez bada gorputza ezin dira zatiketa guztiak $A[X]$-n egin, baina batzuk bai, zehazkiago $f(X)$ $g(X)$-z zatitu dezakegu $g$-ren koefiziente nagusia $A$-ren unitatea bada. Horren zergatia ikusteko, bakarrik gogoratu behar dugu zein prozedura erabiltzen den zatiketaren algoritmoan gorputz baten gainean: zatitu nahi badugu $f(X) = a_nX^n + \cdots + a_0$ polinomioa $g(X) = b_mX^m + \cdots + b_0$ beste polinomio batez, orduan $a_nb_m^{-1}X^{n-m}$ monomioaz biderkatzen dugu $g(X)$ eta lortutako emaitza $f(X)$-ri kentzen diogu. Gero kendurarekin errepikatzen dugu prozedura. Ikusten dugunez, $b_m$-ren alderantzizkoa behar dugu eta, horregatik, zatiketaren algoritmoa aplikatu ahal izango dugu gorputza ez den beste eraztun baten gainean, $g$-ren koefiziente nagusia unitatea den bitartean. Bereziki, $f(X)$ edozein polinomio beti zatitu daiteke $X - a$ moduko polinomio batez eta, beraz, aurreko paragrafoan egindako zatiketa ondo justifikaturik dago. Baina, adibidez, $\mathbb{Z}[X]$-n ezin da $X^3+1$ $2X+1$-ez zatitu, 2-a ez bada unitatea $\mathbb{Z}$-n. Oraindik ere, zatiketa $\mathbb{Q}[X]$-ren barruan egin dezakegu baina, orduan, zatidura eta hondarra $\mathbb{Q}[X]$-n egongo dira eta ez derrigorrean $\mathbb{Z}[X]$-n. Era berean, $K[X,Y] = K[Y][X]$ hartuz, ezin da $X^3+Y^3$ $YX^2+Y^2$-z zatitu, $Y$ ez baita unitatea $K[Y]$-n. Bai egin daiteke, ordea, $K(Y)[X]$-n. Ohartu, baita ere, badagoela $X^3+Y^3$ $YX^2+Y^2$-z zatitzea $K[X,Y] = K[X][Y]$ ikusiz gero, kasu horretan koefiziente nagusia 1 delako.

Aipa dezagun, azkenik, (P3) propietatea ere faltsua dela F.B.D. baten gainean. Adibidez, $f(X) = 2X^2+2 = 2(X^2+1)$ ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta bigarren mailakoa izan eta $\mathbb{Z}$-n errorik ez izan. Baina, (P3) propietateagatik, $f$ irreduziblea da $\mathbb{Q}[X]$-n. Era berean, $f(X,Y) = YX^2 + Y = Y(X^2+1)$ ez da irreduziblea $\mathbb{R}[Y][X]$-n, $\mathbb{R}(Y)[X]$-n bada ere. Ohartu, $X$-rekiko polinomio gisa begiratuta, $f$-k ez duela errorik $\mathbb{R}(Y)$-n (eta, beraz, are gutxiago $\mathbb{R}[Y]$-n). Hori egiaztatzeko, $X$-ren ordez $\mathbb{R}(Y)$-ko elementu orokor bat jarri behar dugu, hau da, $g(Y)/h(Y)$ moduko zatiki bat, eta ikusi behar dugu emaitza ezin dela 0 izan. Baina

$$Y\left(\frac{g(Y)}{h(Y)}\right)^2 + Y = 0 \iff Y\left(\frac{g(Y)^2}{h(Y)^2} + 1\right) = 0 \iff g(Y)^2 + h(Y)^2 = 0$$

dugu, eta hori ezinezkoa da $g$-k eta $h$-k koefiziente errealak dituztelako eta $h \neq 0$ delako. Berriro ere, kontradibideak unitatea ez den konstante bat erabiliz eman

ditugu. Ondorengo teoreman ikusiko dugunez, hori da horrelako adibideak lortzeko modu bakarra.

**1.63. Definizioa.** Izan bitez $A$ F.B.D. eta $f \in A[X]$. Orduan, $f$ *jatorrizkoa* dela esango dugu bere koefizienteen zatitzaile komunetako handiena 1 bada.

**1.64. Lema** (Gaussen Lema)**.** *Jatorrizko polinomioen biderkadura jatorrizkoa da.*

Gaussen Lema aplikatuz, funtsezko emaitza hau frogatu daiteke, polinomio baten irreduzibilitatea F.B.D. baten gainean eta bere zatikien gorputzaren gainean erlazionatzen dituena.

**1.65. Teorema.** *Izan bitez $A$ F.B.D., $K$ $A$-ren zatikien gorputza eta $f \in A[X]$. Orduan, baliokideak dira:*

(i) *$f$ irreduziblea da $A[X]$-n.*
(ii) *$f$ irreduziblea da $K[X]$-n eta jatorrizkoa da.*

Ondorioz, (P1) eta (P3) propietateak konpontzeko modua lortzen dugu.

**1.66. Korolarioa.** *Izan bitez $A$ F.B.D. eta $f \in A[X]$ jatorrizkoa. Orduan:*

(i) *$\deg f = 1$ bada, $f$ irreduziblea da $A[X]$-n.*
(ii) *$\deg f = 2$ edo 3 bada eta $f$-k ez badu errorik $A$-ren zatikien gorputzean, orduan $f$ irreduziblea da $A[X]$-n.*

Oso inportantea da, aurreko korolarioaren (ii) atalean, $f$-k ez duela errorik izan behar *$A$-ren zatikien gorputzean*, eta ez bakarrik $A$-n. Adibidez, $f(X) = 4X^2 - 1 \in \mathbb{Z}[X]$ polinomioa jatorrizkoa da eta ez du errorik $\mathbb{Z}$-n, baina faktorizatu egiten da: $f(X) = (2X + 1)(2X - 1)$. Arazoa da ez duela errorik $\mathbb{Z}$-n, baina bai $\mathbb{Q}$-n. Antzeko adibide bat eman dezakegu bi indeterminaturekin. Jarri $f(X, Y) = Y^2X^2 - 1 \in K[Y][X]$, jatorrizkoa dena. Ohartu $f$-k, $X$-rekiko begiratuta, ez duela errorik $K[Y]$-n; bestela, existituko litzateke $g(Y) \in K[Y]$ non $Y^2g(Y)^2 = 1$ den, eta hori ezinezkoa da. Hala ere, $f(X, Y) = (YX + 1)(YX - 1)$ faktorizatu egiten da. Problema dator $f$-k $K(Y)$-n erroak dituelako, $\pm 1/Y$ alegia.

Ondoren datozen bi emaitzak ezagunak ditugu dagoeneko $\mathbb{Z}$-ren gainean, baina kasu horretan ez ezik, faktorizazio bakarreko domeinu guztietarako ere balio dute.

**1.67. Teorema.** *Izan bitez $A$ F.B.D., $K$ $A$-ren zatikien gorputza eta $f \in A[X]$. Orduan:*

(i) *$a/b \in K$ $f$-ren erroa bada, orduan $a$-k $f$-ren gai askea zatitzen du eta $b$-k, berriz, $f$-ren koefiziente nagusia zatitzen du.*
(ii) *$f$ monikoa bada (hau da, $f$-ren koefiziente nagusia 1 bada), orduan $f$-k $K$-n dituen erro guztiak $A$-n daude.*

Teorema horretako (i) atalak $f$ polinomioaren $K$-ren gaineko balizko erroak mugatu egiten ditu. Adibidez, $f(X) = 4X^7 + X + 1 \in \mathbb{Z}[X]$ hartuz gero, bere erro

arrazional *posibleak* $\pm 1$, $\pm 1/2$ eta $\pm 1/4$ balioetara mugatzen ditu. Horiekin proba eginez, ikusten dugu ez direla $f$-ren erroak eta, horrenbestez, baiezta dezakegu $f$-k ez duela erro arrazionalik. Argudio horrek berak erakusten du nola lor ditzakegun $f \in \mathbb{Z}[X]$ polinomio orokor baten erro *arrazional* guztiak. (Beste problema bat da erro konplexu guztiak ematea, ez dena oro har posible.) Bestetik, (ii) atala oso interesgarria da 1.66 korolarioaren (ii) atalarekin batera erabiltzeko. Hain zuzen ere, bi emaitza horiek konbinaturik, honako hau lortzen dugu.

**1.68. Korolarioa.** *Izan bitez $A$ F.B.D. eta $f \in A[X]$* monikoa, *$\deg f = 2$ edo 3 izanik. Orduan, $f$-k ez badu errorik $A$-n, irreduziblea da $A$-ren gainean.*

Ondorengo teorema honek polinomio berezi batzuen irreduzibilitatea ziurtatzen du F.B.D. baten gainean.

**1.69. Teorema** (Eisenstein-en irizpidea)**.** *Izan bitez $A$ F.B.D. eta $f(X) = a_n X^n + \cdots + a_0 \in A[X]$. Demagun badagoela $p \in A$ irreduziblea, baldintza hauek betetzen dituena:*

(i) $p \mid a_0$, $p^2 \nmid a_0$.
(ii) $p \mid a_1, \ldots, p \mid a_{r-1}$, $p \nmid a_r$, *non $r \leq n$ baita.*

*Orduan, $A$-ren gaineko $f$-ren faktorizazioan badago $r$ maila edo handiagoa duen faktore irreduzible bat. Bereziki, $r = n$ bada eta $f$ jatorrizkoa bada, orduan $f$ irreduziblea da $A[X]$-n.*

Eisensteinen irizpidea aplikatzean, kontuan izan ohar sinple hau: edozein elementuk 0 zatitzen duenez, konprobatzen dugunean $p$ irreduzibleak polinomioaren zein koefiziente zatitzen dituen, bakarrik erreparatu behar diegu 0 ez diren koefizienteei (hau da, polinomioa idaztean agertzen diren koefizienteei).

**1.70. Adibideak.** 1) Izan bedi $f(X) = X^4 + 2X^3 + 4X + 2 \in \mathbb{Z}[X]$. Eisensteinen irizpidea erabiltzen badugu, $p = 2$ hartuta, $f$ $\mathbb{Z}$-ren gainean irreduziblea dela ondorioztatzen dugu. Ez da gauza bera gertatzen $g(X) = 3X^5 + 6X^2 + 12X + 30$ polinomioarekin, nahiz eta $p = 2$ zenbaki lehenarekin Eisensteinen irizpidearen baldintza guztiak bete. Baiezta dezakegu $g$-k $\mathbb{Z}[X]$-n bosgarren mailako faktore irreduzible bat duela, baina horrek ez du esan nahi $g$ $\mathbb{Z}$-ren gainean irreduziblea denik, $g$ ez baita jatorrizkoa. Izan ere, $g(X) = 3(X^5 + 2X^2 + 4X + 10)$ da $g$-ren faktorizazioa $\mathbb{Z}$-ren gainean (ohartu bosgarren mailako faktorea dugula, Eisensteinen irizpideak ziurtatzen duen bezala). Bestalde, $g$ irreduziblea da $\mathbb{Q}$-ren gainean.

2) Izan bedi $f(X, Y) = X^5Y + X^5 + Y^5 + Y \in K[X, Y]$. Polinomio hori $X$-rekiko ikusten badugu, hau da, koefizienteak $K[Y]$-n hartuz, orduan $f(X, Y) = (Y + 1)X^5 + Y^5 + Y \in K[Y][X]$ idazten dugu. Eisensteinen irizpidea aplikatu nahi badugu, $Y^5 + Y$ gai askearen zatitzaile irreduzible bat behar dugu (irreduziblea $K[Y]$-n, jakina), karratura jasorik $Y^5 + Y$ zatitzen ez duena. Aukera bat $Y$ indeterminatua bera hartzea da. Orduan, $f$-k $K[Y][X] = K[X, Y]$-n $X$-rekiko bosgarren mailakoa den faktore irreduzible bat duela ondorioztatzen dugu. Hori

dela eta, $f$ $K[X,Y]$-n irreduziblea den edo ez jakiteko, $K[Y][X]$-n jatorrizkoa den aztertu behar dugu. Horretarako, $\operatorname{zkh}(Y+1, Y^5+Y)$ kalkulatu behar dugu. Hori $Y+1$ izango da $Y+1$-ek $g(Y)=Y^5+Y$ zatitzen badu, eta 1 bestela. Badakigunez, $Y+1$-ek $g(Y)$ zatitzen du baldin eta soilik baldin $g(-1)=0$ bada. Kasu honetan $g(-1)=-2$ denez,

$$\begin{cases} g(-1)=0, & \operatorname{char} K = 2 \text{ bada;} \\ g(-1)\neq 0, & \operatorname{char} K \neq 2 \text{ bada.} \end{cases}$$

Ondorioz,

$$\operatorname{zkh}(Y+1, Y^5+Y) = \begin{cases} Y+1, & \operatorname{char} K = 2 \text{ bada;} \\ 1, & \operatorname{char} K \neq 2 \text{ bada.} \end{cases}$$

Horrela, bi kasu hauek ditugu:

(i) $\operatorname{char} K \neq 2$ bada, $f$ jatorrizkoa da $K[Y][X]$-n eta, hortaz, irreduziblea $K[X,Y]$-n.

(ii) $\operatorname{char} K = 2$ bada, orduan $f$ ez da jatorrizkoa $K[Y][X]$-n eta, beraz, ez da irreduziblea $K[X,Y]$-n. Kasu honetan $Y^5+Y = Y(Y^4+1) = Y(Y+1)^4$ dugu eta honako hau da $f$-ren faktorizazioa $K[X,Y]$-ren irreduzibleetan:

$$f(X,Y) = (Y+1)(X^5+Y(Y+1)^3).$$

3) Azter dezagun $f(X)=X^4-X^3+2X+2$ polinomioaren irreduzibilitatea $\mathbb{Z}$-ren gainean. Eisensteinen irizpidea aplikatzen badugu $p=2$ hartuta, badakigu $f$-k hirugarren mailako edo maila altuagoko faktore irreduzible bat duela $\mathbb{Z}[X]$-n. Bestalde, $f$ jatorrizkoa denez, ez du faktore konstanterik (unitateez aparte). Beraz, bi aukera baino ez daude:

(i) $f(X)$ irreduziblea da $\mathbb{Z}$-ren gainean.

(ii) $f(X)=g(X)h(X)$, non $g(X), h(X)\in\mathbb{Z}[X]$, $\deg g = 1$ eta $\deg h = 3$ baita.

Azken kasua beteko balitz, $f$-k $\mathbb{Q}$-n erro bat izango luke. Orain, 1.67 teoremaren arabera, $f$-k $\mathbb{Q}$-n izan ditzakeen erro bakarrak $\pm 1$ eta $\pm 2$ dira. Horiekin probatuz, ikusten dugu ez direla $f$-ren erroak eta, horrenbestez, $f$ $\mathbb{Z}$-ren gainean irreduziblea dela ondorioztatzen dugu.

Beste batzuetan, $A$-ren gaineko irreduzibilitatea lortzeko, koefizienteak $A$-ren zatidura batera pasatzen ditugu, hurrengo teorema hau erabiliz.

**1.71. Teorema** (Koefizienteen laburketa ideal batekiko)**.** *Izan bitez $A$ F.B.D. eta $\mathfrak{a}$ $A$-ren ideala. Baldin eta $f(X)=a_nX^n+\cdots+a_0\in A[X]$ bada, idatz dezagun $\overline{f}(X)=\overline{a}_nX^n+\cdots+\overline{a}_0\in A/\mathfrak{a}[X]$. Demagun bi baldintza hauek betetzen direla:*

(i) *$f$ jatorrizkoa da.*

(ii) $\deg \overline{f} = \deg f$.

*Orduan, $\overline{f}$ irreduzible bada $A/\mathfrak{a}[X]$-n, halabeharrez $f$ irreduziblea da $A[X]$-n.*

Oro har, teorema hori $\mathfrak{m}$ ideal maximal batekin erabiliko dugu, orduan $A/\mathfrak{m}$ gorputza baita eta, beraz, $A$-ren gainean irreduzibilitatea aztertzeko, gorputz baten gaineko kasura pasa gaitezke.

**1.72. Oharra.** Azken teoremaren baldintzak beharrezkoak dira, erraz ikus dezakegun bezala. Adibideak $A = \mathbb{Z}$ eta $\mathfrak{a} = 2\mathbb{Z}$ hartuz emango ditugu. Alde batetik, $f(X) = 3X + 3$ ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta $\overline{f}(X) = X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ irreduziblea den eta $\deg \overline{f} = \deg f$ den. Beraz, polinomioa jatorrizkoa izateko baldintza ezinbestekoa da. Bestetik, $g(X) = 2X^2 + X$ polinomio jatorrizkoa ez da irreduziblea $\mathbb{Z}[X]$-n, nahiz eta $\overline{g}(X) = X$ irreduziblea den $\mathbb{Z}/2\mathbb{Z}[X]$-n. Kasu horretan, arazoa da $\deg \overline{g} < \deg g$ dugula.

**1.73. Adibidea.** Izan bedi $f(X) = X^4 - X + 1 \in \mathbb{Z}[X]$. Polinomio hori modulo 2 laburtzen badugu, orduan $\overline{f}(X) = X^4 + X + \overline{1} \in \mathbb{F}_2[X]$ lortzen dugu. Azken polinomio hori irreduziblea da $\mathbb{F}_2$ gorputzaren gainean. Izan ere, $\overline{f}$-k ez du errorik $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ multzoan eta, ondorioz, faktorizatuko balitz, bigarren mailako bi irreduzibleren biderkadura litzateke. Orain, erraz ikusten da $\mathbb{F}_2[X]$-n bigarren mailako irreduzible bakarra dagoela, $X^2 + X + \overline{1}$ alegia. Beraz, $\overline{f}$ faktorizatuko balitz,

$$\overline{f}(X) = (X^2 + X + \overline{1})^2 = X^4 + X^2 + \overline{1}$$

izango genuke, eta hori ez da egia. Horrela, $\overline{f}$ irreduziblea da, eta 1.71 teoremaren baldintzak betetzen direnez, $f$ irreduziblea da $\mathbb{Z}$-ren gainean.

Hurrengo atalean, polinomioen eraztunen arteko isomorfismoak lortzeko metodoak hobeto ezagutzen ditugunean, 1.71 teorema indeterminatu bat baino gehiagoko polinomioei ere aplikatuko diegu.

Polinomioen irreduzibilitateari eskainitako zati hau bukatzeko, emaitza negatibo bat emango dugu, polinomio berezi batzuk beti faktorizatzen direla ziurtatzen baitu. Enuntziatua eman baino lehen, polinomio homogeneoak definitu behar ditugu. Polinomio horiek oso rol garrantzitsua izango dute, geometria aljebraikoa espazio proiektiboaren gainean garatu nahi dugunean.

**1.74. Definizioa.** Polinomio bat *homogeneoa* dela diogu bere monomio guztien maila osoa berdina bada.

Adibidez, $f(X, Y) = X^2 + 3XY + 2Y^2$ homogeneoa da eta $g(X, Y) = X^2 + 3X^2Y^2 + 2Y^2$ ez da homogeneoa. Ikus dezagun $f(X, Y)$ faktore linealetan deskonposatzen dela. Izan ere,

$$f(X, Y) = X^2 + 3XY + 2Y^2 = Y^2 \left( \left( \frac{X}{Y} \right)^2 + 3 \left( \frac{X}{Y} \right) + 2 \right) = Y^2 h \left( \frac{X}{Y} \right)$$

dugu, $h(T) = T^2 + 3T + 2$ izanik. (Ohartu $h(T) = f(T, 1)$ dela.) Orain, $h(T)$ polinomioak $T = -1$ eta $T = -2$ erroak dituenez, $h(T) = (T + 1)(T + 2)$ faktorizazioa dugu. Beraz,

$$f(X, Y) = Y^2 \left( \frac{X}{Y} + 1 \right) \left( \frac{X}{Y} + 2 \right) = (X + Y)(X + 2Y)$$

deskonposizioa lortzen dugu. Era berean argudiatuz, ondorengo teorema frogatu daiteke. Gogoratu $h(T) \in K[T]$ polinomio bat $K$-ren gainean *banatzen dela* esaten

dugula faktore linealen biderkadura gisa deskonposatzen bada. Bestela esanda, $\deg h = n$ bada, $h$ $K$-ren gainean banatzen da baldin eta soilik baldin $h$-k $n$ erro baditu $K$ gorputzean, erro bakoitza bere anizkoiztasuna beste aldiz kontatuz gero.

**1.75. Teorema.** *Izan bedi $f(X,Y) \in K[X,Y]$ polinomio homogeneoa eta jarri $h(T) = f(T,1) \in K[T]$. Orduan:*

(i) *$f(X,Y)$ $K$-ren gainean faktorizatzen da baldin eta soilik baldin $h(T)$ $K$-ren gainean faktorizatzen bada.*

(ii) *$f(X,Y)$ faktore linealen biderkadura gisa deskonposatzen da $K$-ren gainean baldin eta soilik baldin $h(T)$ $K$-ren gainean banatzen bada. Hala bada, eta $h$-ren erroak $K$-n $\lambda_1, \dots, \lambda_n$ badira (bakoitza bere anizkoiztasuna beste aldiz errepikaturik), orduan*

$$f(X,Y) = (X - \lambda_1 Y) \dots (X - \lambda_n Y)$$

*dugu. (Ohartu faktore guztiak homogeneoak direla.)*

Teorema hori ez da egiazkoa polinomioek hiru edo indeterminatu gehiago erabiltzen badituzte. Adibidez, $\operatorname{char} K \neq 2$ bada, $f(X,Y,Z) = X^2 + Y^2 + Z^2$ irreduziblea da (1.11 ariketan ikusiko dugu hori) eta, beraz, ezin da faktore linealetan deskonposatu.

Gogoratu $K$ gorputza *aljebraikoki itxia* dela polinomio ez-konstante guztiek erroren bat badute $K$-n. Horren ondorioz, $K[X]$-ko polinomio guztiak faktore linealetan deskonposatzen dira (hau da, $K$-ren gainean banatzen dira) eta lehenengo mailako polinomioak dira $K[X]$-ko irreduzible bakarrak. Aljebraren Oinarrizko Teorema delakoak baieztatzen du $\mathbb{C}$, zenbaki konplexuen gorputza, aljebraikoki itxia dela.

**1.76. Korolarioa.** *$K$ gorputz aljebraikoki itxia bada, orduan $K[X,Y]$-ko polinomio homogeneo guztiak faktore linealetan deskonposatzen dira, horiek ere homogeneoak izanik.*

Emaitza hori ez da betetzen polinomioa ez bada homogeneoa. Adibidez, $f(X,Y) = X^3 + Y^2 + 1$ irreduziblea da $K[X,Y]$-n, $K$ edozein gorputz izanik, eta beraz ezin da faktore linealetan deskonposatu.

Nola faktorizatzen da $X^n - Y^n$ polinomio homogeneoa? Ikusita 1.75 teoremako emaitza, erantzuna $h(T) = T^n - 1$ polinomioaren deskonposizioak emango digu. Polinomio horren erroak, hau da, $\zeta^n = 1$ betetzen duten $\zeta$ elementuak, *unitatearen $n$. erroak* dira. Erraz egiazta daiteke unitatearen erroek talde bat osatzen dutela biderketarekiko. Talde hori, finitua denez, ziklikoa da. (Oro har, $K$ gorputza bada, $K^\times$-ren azpitalde finitu guztiak ziklikoak dira.) Horrek esan nahi du unitatearen erro guztiak erro bakar baten berretura gisa jar daitezkeela.

Oro har, ez dago garbi unitatearen zenbat $n$. erro izango dituen gorputz batek. Adibidez, $\mathbb{R}$-k unitatearen bi erro karratu ditu, 1 eta $-1$, baina unitatearen erro kubiko bakarra, 1 erro tribiala. Orokorkiago, $n$ bikoitia bada, $\mathbb{R}$-k unitatearen bi $n$.

erro ditu eta, $n$ bakoitia bada, bakar bat. Bestalde, $K$ gorputzaren karakteristika $p$ zenbaki lehena bada, orduan $n = p^m$ $p$-ren berretura bada, $K$-n dagoen unitatearen $n$. erro bakarra 1 da,

$$T^n - 1 = T^{p^m} - 1 = (T-1)^{p^m}$$

baitugu.

Unitatearen erro ez-tribialak egotea ziurtatu nahi badugu, $K$ gorputza aljebraikoki itxia har dezakegu, eta horrela egingo dugu hemendik aurrera. Orduan, unitatearen $n$ erro daude $K$-n, anizkoiztasunak kontuan hartuz gero. Horrez gain $\operatorname{char} K \nmid n$ baldintza badugu (adibidez, $\operatorname{char} K = 0$ bada), orduan erro horiek guztiak desberdinak dira. Kasu horretan, $\zeta$ unitatearen $n$. erroen taldearen sortzailea bada, $\zeta$ unitatearen *jatorrizko $n$. erroa* dela esaten dugu.* Orduan, unitatearen erro guztiak $1, \zeta, \ldots, \zeta^{n-1}$ dira eta

$$T^n - 1 = (T-1)(T-\zeta)\ldots(T-\zeta^{n-1})$$

dugu. Beraz, 1.75 teoremaren arabera, honako hau da $X^n - Y^n$ polinomioaren faktorizazioa:

$$X^n - Y^n = (X-Y)(X-\zeta Y)\ldots(X-\zeta^{n-1}Y).$$

Hori da faktorizazioa, adibidez, $\mathbb{C}$-ren gainean. Kasu horretan,

$$\zeta = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\,\sin\frac{2\pi}{n}$$

unitatearen jatorrizko $n$. erroa har dezakegu. Adibidez, $\omega = -1/2 + i\sqrt{3}/2$ unitatearen jatorrizko erro kubikoa da eta $i$, jatorrizko laugarren erroa. Ondorioz,

$$\begin{aligned} X^3 - Y^3 &= (X-Y)(X-\omega Y)(X-\omega^2 Y) \\ &= (X-Y)\left(X-\left(-\frac{1}{2}+i\,\frac{\sqrt{3}}{2}\right)Y\right)\left(X-\left(-\frac{1}{2}-i\,\frac{\sqrt{3}}{2}\right)Y\right) \end{aligned}$$

eta

$$X^4 - Y^4 = (X-Y)(X+Y)(X-iY)(X+iY)$$

faktorizazioak ditugu $\mathbb{C}$-ren gainean.

Zer gertatzen da $K$ aljebraikoki itxia eta $\operatorname{char} K \mid n$ bada? Orduan, halabeharrez, $\operatorname{char} K = p$ zenbaki lehena da. Idatz dezagun $n = mp^t$, $p \nmid m$ izanik. Orduan,

$$T^n - 1 = T^{mp^t} - 1 = (T^m - 1)^{p^t}$$

dugu. Kontuan izanik $K$-ren karakteristikak ez duela $m$ zatitzen, orduan aurreko atalaren arabera, $K$-k badu unitatearen jatorrizko $m$. erro bat, dei diezaiogun $\zeta$, eta hori erabiliz, badakigu nola faktorizatzen den $T^m - 1$ polinomioa. Beraz, kasu horretan,

$$T^n - 1 = (T-1)^{p^t}(T-\zeta)^{p^t}\ldots(T-\zeta^{m-1})^{p^t}$$

---

*$K$ gorputza aljebraikoki itxia bada eta $\operatorname{char} K \nmid n$ bada, $K$-k unitatearen $\varphi(n)$ jatorrizko $n$. erro ditu, $n$ ordenako talde zikliko batek $\varphi(n)$ sortzaile baititu. Hor $\varphi(n)$ Eulerren funtzioa da. Zehazkiago, $\zeta$ jatorrizko $n$. erroa bada, orduan gainerako jatorrizko erro guztiak $\zeta^k$ modukoak dira, $1 \le k \le n$ eta $\operatorname{zkh}(k,n) = 1$ izanik.

dugu eta, ondorioz,

$$X^n - Y^n = (X-Y)^{p^t}(X-\zeta Y)^{p^t}\dots(X-\zeta^{m-1}Y)^{p^t}.$$

Horrela, guztiz erabakita gelditzen da $X^n-Y^n$ polinomioaren faktorizazioa gorputz aljebraikoki itxi baten gainean.

## 1.7. $K$-aljebrak

Atal honetan zehar, $K$ gorputza izango da beti.

**1.77. 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, honako zentzu honetan:

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

**1.78. Adibideak.** 1) $K$-aljebrarik garrantzizkoenak $K[X_1,\dots,X_n]$ polinomioen aljebrak dira.

2) $K(X_1,\dots,X_n)$ funtzio arrazionalen gorputza ere $K$-aljebra da.

3) $K$ gorputza bera $K$-aljebra da. Oro har, $K \subseteq F$ gorputz-hedadura bat badugu, orduan $F$ $K$-aljebra da. Adibidez, $\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}$-aljebra da 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.)

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.

**1.79. Definizioa.** Izan bedi $A$ $K$-aljebra. Orduan:

(i) $B \subseteq A$ $A$-ren *azpialjebra* da azpieraztuna eta azpiespazioa bada aldi berean, hau da, propietate hauek betetzen baditu:

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

(ii) $\mathfrak{a} \subseteq A$ $A$-ren *ideala* da eraztunaren ideala bada eta azpiespazioa bada aldi berean, hau da, propietate hauek betetzen baditu:

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

Aljebra baten idealak definitzean eman dugun hirugarren baldintza ez da beharrezkoa, beste bietatik ondorioztatzen baita. 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. Ondorioz, aljebra baten barruan, "ideala aljebraren egiturarekiko" eta "ideala eraztunaren egiturarekiko" gauza bera dira. Hori dela eta, eraztunen idealetarako eman ditugun emaitzek (besteak beste, korrespondentziaren teorema) aljebren idealetarako ere balio dute.

**1.80. Teorema.** *Izan bitez $A$ aljebra eta $\mathfrak{a}$ $A$-ren ideala. Orduan, $A/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in A\}$ aljebra bat da.*

**1.81. Definizioa.** Izan bedi $f : A \longrightarrow B$ aplikazioa, $A$ eta $B$ $K$-aljebrak izanik (biak $K$ gorputz beraren gainean). Orduan, $f$ *aljebra-homomorfismoa* dela diogu aldi berean eraztun-homomorfismoa eta aplikazio lineala bada, hau da, baldintza hauek betetzen baditu:

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

Horrez gain $f$ bijektiboa bada, orduan $f$ *isomorfismoa* dela eta $A$ eta $B$ *isomorfoak* direla esaten dugu, eta $A \cong B$ idatziko dugu.

Hurrengo teoreman ikusten dugunez, edozein homomorfismotatik isomorfismo bat lor daiteke.

**1.82. Teorema** (Isomorfiaren lehenengo teorema)**.** *Izan bedi $f : A \longrightarrow B$ aljebra-homomorfismoa. Orduan:*

(i) $\operatorname{im} f = \{f(a) \mid a \in A\}$ *$B$-ren azpialjebra da, $f$-ren* irudia *deitutakoa, eta $f$ supraiektiboa da baldin eta soilik baldin* $\operatorname{im} f = B$ *bada.*
(ii) $\ker f = \{a \in A \mid f(a) = 0\}$ *$A$-ren ideala da, $f$-ren* nukleoa *deitutakoa, eta $f$ injektiboa da baldin eta soilik baldin* $\ker f = \{0\}$ *bada.*
(iii) $A/\ker f \cong \operatorname{im} f$ *isomorfismoa dugu, $\overline{x} \mapsto f(x)$ erregelaren bitartez.*

Zergatik dira hain interesgarriak isomorfismoak? Erantzuna da bi aljebra isomorfok egitura bera dutela, eta alde batean ditugun propietate aljebraikoak beste aldean islaturik ikusiko ditugula. Adibidez, honako emaitza hau dugu.

**1.83. Teorema.** *Izan bedi $\varphi : A \longrightarrow B$ aljebra isomorfismoa. Orduan:*

(i) *$a$ $A$-ren unitatea da baldin eta soilik baldin $\varphi(a)$ $B$-ren unitatea bada.*
(ii) *$a$ $A$-ko elementu irreduziblea da baldin eta soilik baldin $\varphi(a)$ $B$-ko irreduziblea bada.*
(iii) *$\mathfrak{a}$ $A$-ren ideal erradikala, lehena edo maximala da baldin eta soilik baldin $\varphi(\mathfrak{a})$ $B$-ren tipo bereko ideala bada.*

Isomorfismoen garrantziaren beste arrazoietako bat ondorengoa da: batzuetan, itxuraz konplikatua den aljebra bat beste aljebra sinpleago edo ezagunago batekin identifikatzeko erabil ditzakegu. Ikus dezagun horren adibide bat.

**1.84. Adibidea.** Badakigu $(X-a)$ $K[X]$-ren ideal maximala dela, $X-a$ sortzailea irreduziblea baita. Ondorioz, $K[X]/(X - a)$ gorputza da. Ikus dezagun gorputz hori $K$-ren isomorfoa dela. Horretarako, definitu honako aplikazio hau:

$$\begin{array}{rccc} \varphi & : & K[X] & \longrightarrow & K \\ & & f(X) & \longmapsto & f(a). \end{array}$$

Erraz ikus daiteke $\varphi$ aljebra-homomorfismoa dela. Isomorfiaren lehenengo teorema aplikatzeko asmoz, azter dezagun zein diren $\varphi$-ren irudia eta nukleoa. Alde batetik,

$$\varphi(\lambda) = \varphi(\lambda \cdot 1) = \lambda\varphi(1) = \lambda \cdot 1 = \lambda^*$$

denez $\lambda \in K$ guztietarako, $\operatorname{im} f = K$ dugu. Ikus dezagun orain $\ker\varphi = (X-a)$ dela. Lehenengo eta behin, $\varphi(X-a) = 0$ denez, $X - a \in \ker\varphi$ dugu. Kontuan hartuz $\ker\varphi$ $K[X]$-ren ideala dela, $(X-a) \subseteq \ker\varphi$ lortzen dugu. Alderantzizko partekotasuna frogatzeko, har dezagun $f(X) \in \ker\varphi$. Orduan $f(a) = 0$ dugu eta, ondorioz, $X - a$ polinomioak $f(X)$ zatitzen du. (Gogoan izan hori zatiketaren algoritmoaren ondorioa dela.) Bestela esanda, $f(X)$ $X-a$-ren multiploa da eta $f(X) \in (X-a)$ lortzen dugu, nahi bezala. Bukatzeko, isomorfiaren lehenengo teoremaren arabera $K[X]/\ker\varphi \cong \operatorname{im}\varphi$ dugunez, isomorfismo hau lortzen dugu:

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

Ikus dezagun aurreko adibideko isomorfismoaren aplikazio bat, polinomio baten irreduzibilitatea frogatzeko.

**1.85. Adibidea.** Izan bedi $f(X,Y) = X^4 + X^3Y^4 + 3X^3 + Y^2 + 2Y + 1$. Ba al da lehena $(f(X,Y))$ ideala $\mathbb{Q}[X,Y]$-n? Hau da, ba al da irreduziblea $f(X,Y)$ $\mathbb{Q}[X,Y]$-n? Eman diezaiogun $X$-ri rol nagusia. Orduan, $f(X,Y) = X^4 + (Y^4+3)X^3 + (Y+1)^2$ $X$-rekiko polinomio gisa idazten dugu, koefizienteak $\mathbb{Q}[Y]$-n izanik. Horrela ikusita, polinomioa jatorrizkoa da. Ohartu $f$-ri ezin diezaiokegula Eisensteinen irizpidea aplikatu, $(Y+1)^2$ gai askea karratu bat delako. Saia gaitezen 1.71 teorema erabiltzen, $f$ polinomioaren koefizienteen laburketa $(Y)$ idealarekiko eginez. Ohartu $(Y)$ $\mathbb{Q}[Y]$-ren (hau da, koefizienteen eraztunaren) ideal lehena dela. Orduan, $\overline{f}$ polinomio bat lortzen dugu, $X$ indeterminatua erabiltzen duena eta koefizienteak $\mathbb{Q}[Y]/(Y)$-n dituena. Kontuan izanik $\overline{Y} = \overline{0}$ dela $\mathbb{Q}[Y]/(Y)$ zatiduran,

$$\overline{f}(X) = X^4 + \overline{3}X^3 + \overline{1}$$

dela ondorioztatzen dugu. Ikusita $\deg\overline{f} = \deg f$ dela, $\overline{f}$ irreduziblea bada orduan $f$ ere irreduziblea dela frogaturik gelditzen da. Horretarako isomorfismoen indarra erabiltzeko aukera dugu. Aurreko adibidearen arabera, $\mathbb{Q}[Y]/(Y) \cong \mathbb{Q}$ dugu eta, ondorioz, $\mathbb{Q}[Y]/(Y)[X] \cong \mathbb{Q}[X]$. Horrek esan nahi du $\overline{f}$ polinomioa $\mathbb{Q}$-ren gainean definituta balego bezala ikus dezakegula. Zehazkiago, $g(X) = X^4 + 3X^3 + 1 \in \mathbb{Q}[X]$ bada, orduan 1.83 teoremaren arabera, $\overline{f}$ irreduziblea da baldin eta soilik baldin $g$ irreduziblea bada $\mathbb{Q}$-ren gainean.

Orain, $g$-ren koefizienteak osoak direnez, berriro ere koefizienteen laburketa aplikatuko dugu, oraingo honetan 2 moduluarekiko. Horrela, $\overline{g}(X) = X^4 + X^3 + \overline{1} \in \mathbb{F}_2[X]$ polinomioa lortzen dugu. Erraz ikus dezakegu polinomio hori irreduziblea

*Oro har, $A \neq \{0\}$ $K$-aljebra bada, orduan $K \cdot 1 = \{\lambda \cdot 1 \mid \lambda \in K\}$ multzoa $A$-ren azpialjebra da, eta $K$-ren isomorfoa da $\lambda \cdot 1 \mapsto \lambda$ aplikazioaren bitartez. Hori dela eta, eskuarki $K \cdot 1$ eta $K$ identifikatu egingo ditugu, eta $K$ $A$-ren barruan dagoela ulertuko dugu. Orduan, $K$ gorputzeko elementuak finko gelditzen dira $\varphi : A \to B$ edozein aljebra-homomorfismoren bitartez: $\varphi(\lambda) = \lambda$ dugu, $\lambda \in K$ guztietarako.

dela, 1.73 adibidean bezala argudiatuz. Hortaz, $g$ irreduziblea da $\mathbb{Z}$-ren gainean eta, ondorioz, $\mathbb{Q}$-ren gainean ere bai. Horregatik guztiagatik, $f(X,Y)$ $\mathbb{Q}[X,Y]$-n irreduziblea dela ziurta dezakegu.

Isomorfiaren lehenengo teoremaren arabera, homomorfismo batetik isomorfismo bat lor dezakegu, eta horregatik ondorengo galdera naturalki azaltzen da: nola defini dezakegu aljebra-homomorfismo bat? Aukera bat erregela bat edo "formula" bat ematea da. Adibidez, definitzen baditugu $\varphi, \psi : A \longrightarrow A$ aplikazioak $\varphi(a) = -a$ eta $\psi(a) = a^2$ formulen bidez, ba al dira homomorfismoak? Erraz ikus daiteke $\varphi$ aplikazioa $\operatorname{char} K = 2$ denean baino ez dela homomorfismoa eta $\psi$, berriz, $K = \mathbb{F}_2$ denean baino ez. Jakina, formula bat ematen digutenean, beti ikus dezakegu, lan gehiagorekin edo gutxiagorekin, homomorfismo bat definitzen duen. Askoz ere interesgarriagoa litzateke, hala ere, aldez aurretik jakitea zein formulek emango dizkiguten homomorfismoak. Zoritxarrez, hori ez dago batere garbi.

Beste ikuspegi bat espazio bektorialen teoriatik har dezakegu. Izan bitez $V$ eta $W$ bi $K$-espazio bektorial, $V$ dimentsio finitukoa izanik, eta har dezagun $\mathcal{B} = \{v_1, \ldots, v_n\}$ $V$-ren oinarri bat. Lehenengo eta behin, demagun badugula $\varphi : V \longrightarrow W$ aplikazio lineal bat eta ezagutzen ditugula $\mathcal{B}$-ko bektoreen irudiak; jar dezagun $w_i = \varphi(v_i)$, $i = 1, \ldots, n$ guztietarako. Orduan, informazio hori nahikoa da $v \in V$ bektore orokor baten irudia emateko. Egin behar dugun guztia da $v$ bektorea $\mathcal{B}$ oinarriarekiko deskonposatzea,

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n, \quad \lambda_i \in K \text{ izanik,}$$

eta $\varphi$ aplikatzea, kontuan izanik $\varphi$ lineala dela:

$$\varphi(v) = \lambda_1 \varphi(v_1) + \cdots + \lambda_n \varphi(v_n).$$

Azkenik, $\varphi(v_i)$ bakoitzaren ordez $w_i$ jarriz, $v$-ren irudia lortzen dugu:

$$\varphi(v) = \lambda_1 w_1 + \cdots + \lambda_n w_n. \tag{1.6}$$

Orain, interesgarriena da argudio horri buelta eman diezaiokegula eta erabil dezakegula, ez emandako aplikazio lineal baten irudiak kalkulatzeko, baizik eta aplikazio lineal berriak *eraikitzeko*. Izan ere, $V$-tik $W$-ra aplikazio lineal bat definitu nahi badugu, nahikoa da $v_i \in \mathcal{B}$ bakoitzaren irudia *nahi dugun moduan* aukeratzea $W$-ren barruan. Irudi horri $w_i$ deitzen badiogu, orduan (1.6) erregelaren bitartez definitzen den $\varphi : V \longrightarrow W$ aplikazioa beti da lineala, ez dugu inolako egiaztapenik egin behar. (Hobeto esanda, teorema batek ziurtatzen du horrela izango dela beti, eta horren frogan emandako argudio orokorrak kasuz kasu egiaztatuz joatea aurrezten digu.) Ideia horrek askatasun handia ematen digu aplikazio linealak definitzeko orduan. Jarraian ikusten dugunez, $\varphi : A \longrightarrow B$ aljebra-homomorfismo bat definitzeko, antzeko zerbait egin dezakegu $A = K[X_1, \ldots, X_n]$ den kasu berezian.

**1.86. Teorema** ($K[X_1, \ldots, X_n]$-ren propietate unibertsala)**.** *Izan bedi $B$ $K$-aljebra. Orduan:*

(i) *$\varphi : K[X_1, \ldots, X_n] \longrightarrow B$ aljebra-homomorfismo bat guztiz zehazturik geldi-tzen da $X_1, \ldots, X_n$ indeterminatuen irudiak ezagututa. Zehazkiago, $\varphi(X_i) =$*

*$b_i$ bada $i = 1, \dots, n$ denean, orduan honako hau da polinomio orokor baten irudia:*

$$\varphi\Big(\sum_{i_1,\dots,i_n\geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n}\Big) = \sum_{i_1,\dots,i_n\geq 0} \lambda_{i_1,\dots,i_n} b_1^{i_1} \dots b_n^{i_n}. \tag{1.7}$$

(ii) *Alderantziz, $\varphi : K[X_1, \dots, X_n] \longrightarrow B$ aljebra-homomorfismo bat definitzeko, nahikoa da $X_1, \dots, X_n$ indeterminatuen irudiak, $b_1, \dots, b_n \in B$* nahi dugun moduan *aukeratzea. Orduan, $\varphi$ (1.7) formularen bitartez definitzen da edozein polinomioren gainean.*

Aurreko teoremaren frogan, (i) atalerako behar dugun guztia da edozein polinomio indeterminatuak konbinatuz idazten dela, baturak, biderkadurak eta eskalarrezko biderkadurak erabiliz. Bigarren atalerako, ordea, zerbait gehiago behar dugu: deskonposizio hori bakarra dela. Hori da arrazoia (ii) ez izateko egiazkoa $K[X_1, \dots, X_n]$-ren ordez aljebra orokor bat jarriz gero. Aurrerago emango dugu propietate horrek huts egiten duen adibide bat.

**1.87. Adibideak.** 1) Aurreko teoremaren arabera,

$$\begin{array}{rccc} \varphi & : & K[X,Y] & \longrightarrow & K[X,Y] \\ & & X & \longmapsto & X-1 \\ & & Y & \longmapsto & Y+2 \end{array}$$

esleipenak aljebra-homomorfismo bat definitzen du. Orduan, $f(X, Y)$ polinomio orokor baten irudia $f(X - 1, Y + 2)$ da. Adibidez,

$$\varphi(X^2 + Y + 1) = (X - 1)^2 + (Y + 2) + 1 = X^2 - 2X + Y + 4.$$

Ikus dezagun $\varphi$ isomorfismoa dela. Horretarako, 1.82 teoremaren arabera, nahikoa litzateke $\operatorname{im}\varphi = K[X, Y]$ eta $\ker\varphi = \{0\}$ dela ikustea. Oraingoan beste modu batean ikusiko dugu, $\varphi$-ren alderantzizko aplikazioa esplizituki emanez. Izan bedi

$$\begin{array}{rccc} \psi & : & K[X,Y] & \longrightarrow & K[X,Y] \\ & & X & \longmapsto & X+1 \\ & & Y & \longmapsto & Y-2. \end{array}$$

Orduan, $(\psi \circ \varphi)(X) = (\varphi \circ \psi)(X) = X$ eta $(\psi \circ \varphi)(Y) = (\varphi \circ \psi)(Y) = Y$ denez, $(\psi\circ\varphi)(f(X, Y)) = (\varphi\circ\psi)(f(X, Y)) = f(X, Y)$ dela ondorioztatzen dugu $f(X, Y) \in K[X, Y]$ guztietarako. Horrek esan nahi du $\psi\circ\varphi$ eta $\varphi\circ\psi$ identitate aplikazioarekin bat datozela eta, hortaz, $\varphi$ bijektiboa dela. Emaitza horren aplikazio modura, kontuan izanik $(X, Y)$ $K[X, Y]$-ren ideal maximala dela eta 1.83 teorema, $(X - 1, Y + 2)$ ere $K[X, Y]$-ren ideal maximala dela ondorioztatzen dugu.*

2) Aurreko adibidean emandako argudio bera erabiliz, orokorkiago frogatu dezakegu $(X - a, Y - b)$ ideala maximala dela $K[X, Y]$-n $a, b \in K$ guztietarako.

*Hor, inplizituki, emaitza hau erabiltzen ari gara, 1.2 ariketan frogatuko duguna: $\varphi : A \longrightarrow B$ aljebra-homomorfismo supraiektiboa bada eta $\mathfrak{a} = (a_1, \dots, a_r)$ $A$-ren ideala bada, orduan $\varphi(A)$ $B$-ren ideala da eta $\varphi(A) = (\varphi(a_1), \dots, \varphi(a_r))$ dugu. Emaitza hori ez da oro har betetzen $\varphi$ ez bada supraiektiboa.

Orain emaitza horren froga alternatibo bat emango dugu, esango diguna gainera $K[X,Y]/(X-a,Y-b)$ zatidura $K$ gorputzaren isomorfoa dela. Horretarako, definitu

$$\begin{array}{rccc} \varphi & : & K[X,Y] & \longrightarrow & K \\ & & X & \longmapsto & a \\ & & Y & \longmapsto & b \end{array}$$

aljebra-homomorfismoa. Lehenengo eta behin, ohartu $\operatorname{im}\varphi = K$ dugula, 1.84 adibidean bezala argudiatuz. Ikus dezagun orain $\ker\varphi = (X-a,Y-b)$ dela. Alde batetik,

$$\varphi(X-a) = \varphi(X) - \varphi(a) = a - a = 0$$

eta

$$\varphi(Y-b) = \varphi(Y) - \varphi(b) = b - b = 0$$

denez, $X-a$ eta $Y-b$ $\varphi$-ren nukleoan daude eta, $\ker\varphi$ ideala denez, $(X-a,Y-b) \subseteq \ker\varphi$ lortzen dugu. Alderantzizko partekotasuna ikusteko, har dezagun $f \in \ker\varphi$ eta frogatu dezagun $f \in (X-a,Y-b)$ dela. Horretarako, zatitu dezagun $f$ polinomioa $X-a$-z, $X$ indeterminatuarekiko. (Zatiketa hori $K[Y][X]$-n egiten dugu. Ohartu zatiketaren algoritmoa erabil daitekeela, $X-a$ monikoa delako.) Orduan, $f$-ren deskonposizio hau dugu:

$$f = q(X-a) + r, \quad r \in K[X,Y] \text{ eta } \deg_X r < 1 \text{ izanik.} \tag{1.8}$$

Beraz, $r$-k ez du $X$-rik, eta $r \in K[Y]$ dela ondorioztatzen dugu. Orain, $r$ polinomioa $Y-b$-z zatitzen dugu $K[Y]$-n ($Y$-rekiko, jakina, kasu honetan ez dago beste aukerarik). Horren ondorioz,

$$r = q^*(Y-b) + r^*, \quad r^* \in K[Y] \text{ eta } \deg r^* < 1 \text{ izanik,} \tag{1.9}$$

lortzen dugu. Orduan, $r^*$ hondarrak $K$ gorputzeko konstantea izan behar du. Laburbilduz, $f$-ren beste deskonposizio hau lortzen dugu:

$$f = q(X-a) + q^*(Y-b) + r^*, \quad q, q^* \in K[X,Y] \text{ eta } r^* \in K \text{ izanik.} \tag{1.10}$$

Orain, berdintza horri $\varphi$ aplikatzen badiogu, $f$, $X-a$ eta $Y-b$ $\varphi$-ren nukleoan daudela kontuan hartuz,

$$0 = \varphi(f) = \varphi(q)\varphi(X-a) + \varphi(q^*)\varphi(Y-b) + \varphi(r^*) = \varphi(r^*)$$

dugu. Baina, $r^*$ konstantea denez, $\varphi(r^*) = r^*$ dugu eta, hortaz, $r^* = 0$. Bukatzeko, balio hori (1.10)-era eramanez, $f = q(X-a) + q^*(Y-b) \in (X-a,Y-b)$ dugu, nahi bezala.

3) Azken adibideko argudioa errepikatuz, ondorengo isomorfismo hau frogatu dezakegu:

$$\frac{K[X_1,\ldots,X_n]}{(X_1-a_1,\ldots,X_n-a_n)} \cong K, \qquad a_1,\ldots,a_n \in K \text{ guztietarako.}$$

Ondorioz, $(X_1-a_1,\ldots,X_n-a_n)$ $K[X_1,\ldots,X_n]$-ren ideal maximala da.

4) Beste alde batetik, $(X_1-a_1)$ ideala lehena da $K[X_1,\ldots,X_n]$ eraztunean, $X_1-a_1$ polinomioa irreduziblea baita. Ondorioz, $K[X_1,\ldots,X_n]/(X_1-a_1)$ zatidura

I.D. da. Ba al da ezagutzen dugun I.D. baten isomorfoa? Ikus dezagun baietz. Definitu

$$\begin{array}{rccc} \varphi & : & K[X_1,\dots,X_n] & \longrightarrow & K[X_2,\dots,X_n] \\ & & X_1 & \longmapsto & a_1 \\ & & X_2 & \longmapsto & X_2 \\ & & \vdots & \vdots & \vdots \\ & & X_n & \longmapsto & X_n. \end{array}$$

Ikusten badugu $\varphi$ supraiektiboa dela eta $\ker\varphi = (X_1 - a_1)$ dela, orduan

$$\frac{K[X_1,\dots,X_n]}{(X_1-a_1)} \cong K[X_2,\dots,X_n]$$

isomorfismoa ondorioztatuko dugu. Alde batetik, $X_2,\dots,X_n \in \operatorname{im}\varphi$ dugu eta $K \subseteq \operatorname{im}\varphi$ ere bai (gogoratu, aurretik ikusi dugun bezala, konstante baten irudia konstante hori bera dela). Orain, $\operatorname{im}\varphi$ azpialjebra denez, elementu horiekin egin ditzakegun batura eta biderkadura guztiak ere $\operatorname{im}\varphi$-n daude eta, beraz, $\operatorname{im}\varphi = K[X_2,\dots,X_n]$ da. Bestetik, nabaria da $X_1 - a_1 \in \ker\varphi$ dela. Alderantzizko partekotasuna lortzeko, hartu $f \in \ker\varphi$ eta zatitu $X_1 - a_1$ polinomioaz $X_1$-ekiko. Orduan,

$$f = q(X_1 - a_1) + r, \qquad \deg_{X_1} r < 1 \text{ izanik},$$

deskonposizioa dugu, hau da, $r \in K[X_2,\dots,X_n]$ izanik. Berdintza horri $\varphi$ aplikatuz,

$$0 = \varphi(f) = \varphi(q)\varphi(X_1 - a_1) + \varphi(r) = r$$

lortzen dugu eta, beraz, $f = q(X_1 - a_1) \in (X_1 - a_1)$. Horrek $\ker\varphi = (X_1 - a_1)$ dela frogatzen du.

5) Azken adibideetako ideiak konbinatuz, isomorfismo hau frogatu dezakegu:

$$\frac{K[X_1,\dots,X_n]}{(X_1-a_1,\dots,X_r-a_r)} \cong K[X_{r+1},\dots,X_n], \qquad a_1,\dots,a_r \in K \text{ guztietarako.}$$

Ondorioz, $(X_1 - a_1,\dots,X_r - a_r)$ $K[X_1,\dots,X_n]$-ren ideal lehena da.

6) Azter dezagun orain $(X^2+1, Y)$ ideala $\mathbb{R}[X,Y]$-n lehena den edo ez. Lehenengo eta behin, $(Y) \subseteq (X^2+1, Y)$ partekotasuna izateagatik, korrespondentziaren teoremak ondokoa ziurtatzen du:

$$(X^2+1,Y) \text{ lehena } \mathbb{R}[X,Y]\text{-n} \iff \frac{(X^2+1,Y)}{(Y)} \text{ lehena } \frac{\mathbb{R}[X,Y]}{(Y)}\text{-n}$$

Orain, aurreko adibide baten arabera, $\mathbb{R}[X,Y]/(Y)$ eta $\mathbb{R}[X]$ isomorfoak dira. Ohartu, gainera, isomorfismo esplizitu bat ezagutzen dugula bi aljebra horien artean, isomorfiaren lehenengo teoremak dioen bezala. Izan ere, isomorfismoa $X \mapsto X$, $Y \mapsto 0$ esleipenen bidez emanda dagoen homomorfismotik datorrenez, karakterizaturik gelditzen da $\overline{X} \mapsto X$ eta $\overline{Y} \mapsto 0$ erregelen bitartez. Orduan, eskema hau

irudika dezakegu:

$$\begin{array}{ccccc} \mathbb{R}[X,Y] & \longrightarrow & \dfrac{\mathbb{R}[X,Y]}{(Y)} & \longrightarrow & \mathbb{R}[X] \\ (X^2+1,Y) & \longmapsto & \dfrac{(X^2+1,Y)}{(Y)} & \longmapsto & (X^2+1) \\ (Y) & \longmapsto & \dfrac{(Y)}{(Y)} = \{\overline{0}\} & \longmapsto & \{0\} \end{array}$$

Hor, lehenengo geziak epimorfismo kanonikoa adierazten du eta bigarrena, berriz, aipatutako isomorfismoa da. Aljebra bakoitzaren azpian agertzen den ideala bere irudiarekin lotuta dago. Aurretik argudiatu dugu $(X^2+1,Y)$ ideal lehena dela $\mathbb{R}[X,Y]$-n baldin eta soilik baldin $(X^2+1,Y)/(Y)$ lehena bada $\mathbb{R}[X,Y]/(Y)$-n. Bestalde, 1.83 teoremaren arabera, isomorfismo batek gorde egiten ditu ideal lehenak eta, beraz, azken ideal hori lehena da baldin eta soilik baldin $(X^2+1)$ lehena bada $\mathbb{R}[X]$-n. Orain, $X^2+1$ irreduziblea denez $\mathbb{R}$-ren gainean, $(X^2+1)$ ideal lehena da $\mathbb{R}[X]$-n eta, beraz, $(X^2+1,Y)$ $\mathbb{R}[X,Y]$-n lehena dela baiezta dezakegu. Are gehiago, $(X^2+1)$ $\mathbb{R}[X]$-n maximala izateagatik, era berean ondorioztatzen dugu $(X^2+1,Y)$ $\mathbb{R}[X,Y]$-n maximala dela.

Dakusagunez, kasu honetan, nagusia ez zen ideal bat lehena den edo ez aztertzeko orduan, erabili dugun prozedura ideal nagusi baten kasura eramatea izan da, baina beste aljebra batean.

7) Guztiz era berean ikus dezakegu $(X^2+1,Y)$ ideala ez dela maximala ezta lehena ere $\mathbb{C}[X,Y]$-n. Arrazoia da ideal horren azterketa $\mathbb{C}[X]$-n $(X^2+1)$ ideala estudiatzera eramango dugula, eta azken ideal hori ez dela lehena, $X^2+1=(X-i)(X+i)$ faktorizatzen baita $\mathbb{C}$-ren gainean.

Izan bitez $f,g \in K[X_1,\ldots,X_n]$. Badakigu $(f)$ ideal lehena dela baldin eta soilik baldin $f$ irreduziblea bada, baina ez da pentsatu behar $(f,g)$ moduko ideal bat lehena dela baldin eta soilik baldin $f$ eta $g$ irreduzibleak badira.

Alde batetik, $\mathfrak{a}=(X^2+1,Y^2+1)$ ideala ez da lehena $\mathbb{R}[X,Y]$-n, nahiz eta emandako bi sortzaileak irreduzibleak izan. Demagun, absurdora eramanez, $\mathfrak{a}$ ideal lehena dela. Orduan,

$$(X-Y)(X+Y)=X^2-Y^2=(X^2+1)-(Y^2+1)\in\mathfrak{a}$$

izateagatik, $X-Y\in\mathfrak{a}$ edo $X+Y\in\mathfrak{a}$ izango genuke. Ikus dezagun $X-Y$ ez dagoela $\mathfrak{a}$-n. Egongo balitz, idatzi ahal izango genuke

$$X-Y=f(X,Y)(X^2+1)+g(X,Y)(Y^2+1).$$

Hor $X=i$ eta $Y=-i$ ordezkatuz, $2i=0$ kontraesana lortzen dugu. Antzera frogatzen da $X+Y$ ez dagoela $\mathfrak{a}$-n eta bilatzen ari ginen absurdoa lortu dugu.

Beste alde batetik, azken adibidean ikusi dugun bezala, $(X^2+1,Y)$ ideal lehena da $\mathbb{R}[X,Y]$-n. Orain, erraz alda dezakegu ideal horren sortzaileetako bat irreduziblea ez izateko. Adibidez,

$$(X^2+1,Y)=(X^2+1,Y-(X^2+1)Y)=(X^2+1,-X^2Y)=(X^2+1,X^2Y)$$

dugu. Beraz, sortzaileetako bat irreduziblea ez bada ere, ideala lehena izan daiteke.

Izan bitez $A$ $K$-aljebra bat eta $a_1, \ldots, a_n \in A$. Orduan, 1.86 teoremaren arabera, $X_1 \mapsto a_1, \ldots, X_n \mapsto a_n$ erregelek $K[X_1, \ldots, X_n] \longrightarrow A$ aljebra-homomorfismo bat definitzen dute, *ebaluazio homomorfismo* deitutakoa. Homomorfismo horren bitartez, $f(X_1, \ldots, X_n)$ polinomio baten irudia $f(a_1, \ldots, a_n)$ ikurraren bidez adierazten dugu, eta balio hori $a_1, \ldots, a_n$ elementuen *konbinazio polinomiko* bat dela esaten dugu. 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

$$f(a_1, \ldots, a_n) = \sum_{i_1,\ldots,i_n \geq 0} \lambda_{i_1,\ldots,i_n} a_1^{i_1} \ldots a_n^{i_n} \tag{1.11}$$

dugu. Jarraian ikusten dugunez, konbinazio polinomikoek azpimultzo batek sortzen duen azpialjebrarekin lotura zuzena dute.

**1.88. Teorema.** *Izan bitez $A$ $K$-aljebra eta $S \subseteq A$. Orduan, $S$-ko elementuen konbinazio polinomikoek $A$-ren azpialjebra bat osatzen dute, eta hori da $S$ barruan duen $A$-ren azpialjebrarik txikiena. Horri $S$-k* sortutako azpialjebra *deitzen diogu eta $K[S]$ ikurraren bidez adierazten dugu. Beraz,*

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

Baldin eta $S = \{a_1, \ldots, a_n\}$ finitua bada, orduan $K[a_1, \ldots, a_n]$ idatziko dugu sinpleago $K[\{a_1, \ldots, a_n\}]$-ren ordez.

**1.89. 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:

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

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, (1.11) 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 ez duten polinomioen multzoa da.

4) Izan bedi $K \subseteq L$ gorputz-hedadura. Orduan, $u \in L$ bada, Galoisen teorian $K[u]$ eta $K(u)$ azpimultzoak definitzen dira honako modu honetan:

$$K[u] = \{f(u) \mid f \in K[X]\}$$

eta

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

Ohartu $K[u]$ $u$-k sortzen duen azpialjebra dela eta, beraz, notazio aldetik ez dagoela nahasteko posibilitaterik. Bestalde, $K(u)$ $K[u]$-ren zatikien gorputza da, eta hori da $K$ eta $u$ barruan dituen $L$-ren azpigorputzik txikiena. Bestela esanda, $K(u)$ da $u$ elementuak $K \subseteq L$ hedaduran sortzen duen tarteko gorputza.

Nabaria da $K[u] \subseteq K(u)$ dugula eta $K[u]$ gorputza dela baldin eta soilik baldin $K[u] = K(u)$ bada. Ezaguna da $K[u] = K(u)$ dela zehatz-mehatz $u$ *aljebraikoa* denean $K$-ren gainean, hau da, existitzen bada $f \in K[X]$, $f \neq 0$, non $f(u) = 0$ baita. Garbi dago $f$ monikoa har dezakegula nahi izanez gero. Orduan, badago polinomio moniko horien artean maila txikieneko bakar bat, irreduziblea dena gainera. Polinomio hori adierazteko $\mathrm{Irr}(u, K)$ idazten dugu eta orduan isomorfismo hau dugu:

$$K[u] \cong \frac{K[X]}{(\mathrm{Irr}(u, K))}. \tag{1.12}$$

Ez bada aljebraikoa, $u$ $K$-ren gainean *transzendentea* dela esaten dugu. Orduan, $K[u] \neq K(u)$ dugu eta bi isomorfismo hauek betetzen dira:

$$K[u] \cong K[X] \qquad \text{eta} \qquad K(u) \cong K(X). \tag{1.13}$$

Ohartu (1.12) eta (1.13) isomorfismoak 1.86 teoremaren ondorioz lor daitezkeela, $K[X]$-tik $K[u]$-ra homomorfismo bat definituz $X \mapsto u$ erregelaren bitartez, eta isomorfiaren lehenengo teorema erabiliz.

Azken adibidean ikusi dugun (1.12) isomorfismoa erraz orokortu daiteke beste aljebra askotarako. Horretarako, kontzeptu hau behar dugu.

**1.90. 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.

**1.91. Teorema.** *Izan bedi $A = K[a_1, \ldots, a_n]$ $K$-aljebra finituki sortua. Orduan, existitzen da $K[X_1, \ldots, X_n]$-ren ideal bat, $\mathfrak{a}$, halakoa non*

$$A \cong \frac{K[X_1, \ldots, X_n]}{\mathfrak{a}}$$

*baita.*

Froga. Polinomioen aljebren propietate unibertsalaren arabera, $X_1 \mapsto a_1$, …, $X_n \mapsto a_n$ erregelek $\varphi : K[X_1, \ldots, X_n] \longrightarrow A$ homomorfismo bat definitzen dute. Orduan, $\operatorname{im}\varphi$ irudia $a_1, \ldots, a_n$ elementuen konbinazio polinomikoek osatzen dute. Hau da, $\operatorname{im}\varphi = K[a_1, \ldots, a_n] = A$ dugu. Orain, $\mathfrak{a} = \ker\varphi$ hartuz gero, isomorfiaren lehenengo teoremak erakusten du $K[X_1, \ldots, X_n]/\mathfrak{a} \cong A$ dela. □

Bestela esanda, $K$-aljebra finituki sortuak polinomioen aljebren zatidurak baino ez dira. Horregatik baieztatu dugu lehenago aljebrarik garrantzizkoenak polinomioen aljebrak direla.

Polinomioen aljebren propietate unibertsala ikusita, pentsa genezake hori aljebra guztietara orokortzea honako modu honetan: $A$-ren $S$ sistema sortzaile bat hartzen badugu, orduan $\varphi : A = K[S] \longrightarrow B$ aljebra-homomorfismo bat definitzeko, nahikoa da $S$-ko elementuen irudiak nahi dugun moduan aukeratzea. Hori faltsua da, hurrengo adibidean erakusten dugun bezala. Egia da, *behin $\varphi$ homomorfismo bat izanda*, $S$-ko elementuen irudiak jakitea nahikoa dela $A$-ko elementu orokor baten irudia ezagutzeko. Azken batean, $A = K[S]$ izateagatik, $A$-ko elementuak $S$-ko elementuen konbinazio polinomikoak dira eta nahikoa dugu erabiltzea $\varphi$-k baturak, biderkadurak eta eskalarrezko biderkadurak gordetzen dituela. Hau da, propietate unibertsalaren (i) atala bete egiten da. Huts egiten duena (ii) atala da, homomorfismoak eraikitzeko balio duena (eta bi ataletatik inportanteena dena). Arazoa da $a \in A$ elementu baten adierazpena, $S$-ko elementuen konbinazio polinomiko modura, ez dela oro har bakarra; $a$-ren irudia kalkulatzean adierazpen desberdinak erabiliz gero, emaitza desberdinak lor genitzake. Bestela esanda, $S$-ko elementuen irudiak emanez definitu nahi dugun homomorfismoa ez dago oro har ondo definituta.

**1.92. Adibidea.** Izan bedi $A = K[X,Y]/(X^3 - Y^2)$ zatidura. Garbi dago $A$-ko edozein elementu $\overline{X}$ eta $\overline{Y}$ elementuen konbinazio polinomikoa dela eta, beraz, $A = K[\overline{X}, \overline{Y}]$ dela. Saia gaitezen $\varphi : A \longrightarrow K$ aljebra-homomorfismo bat definitzen $\varphi(\overline{X}) = 1$ eta $\varphi(\overline{Y}) = 0$ erregelen bidez. Orduan,

$$\varphi(\overline{X}^2) = \varphi(\overline{X})^2 = 1$$

dugu baina, beste alde batetik, $\overline{X}^2 = \overline{Y}^3$ denez zatidura horretan,

$$\varphi(\overline{X}^2) = \varphi(\overline{Y}^3) = \varphi(\overline{Y})^3 = 0.$$

Kontraesan horrek $\varphi$ ez dagoela ondo definiturik frogatzen du. Ez dago problemarik, hala ere, $\varphi : K[X,Y] \longrightarrow K$ definitzeko $\varphi(X) = 1$ eta $\varphi(Y) = 0$ esleipenen bitartez.

## 1.8. Polinomioen aljebren ideal maximalak

Aurreko atalean ikusi dugunez, $K$ gorputza bada eta $a_1, \ldots, a_n \in K$ elementuak edozein modutan aukeratzen baditugu, orduan $(X_1 - a_1, \ldots, X_n - a_n)$ $K[X_1, \ldots, X_n]$-ren ideal maximala da. Gai honetako azken zati honetan, gure helburua alderantzizko partzial hau frogatzea da.

**1.93. Teorema.** *Izan bedi $\mathfrak{m}$ $K[X_1, \ldots, X_n]$-ren ideal maximala, $K$ gorputz aljebraikoki itxia izanik. Orduan, existitzen dira $a_1, \ldots, a_n \in K$, halakoak non $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ baita.*

Horrenbestez, $K$ aljebraikoki itxia bada, guztiz determinaturik gelditzen dira $K[X_1, \ldots, X_n]$-ren ideal maximalak.

Aurreko teorema ez da inola ere egiazkoa $K$ ez bada aljebraikoki itxia, eta indeterminatu bakar batekin huts egiten du jadanik. Izan ere, $K$ aljebraikoki itxia ez izateagatik, badago $p(X) \in K[X]$ polinomio irreduzible bat $\deg p(X) \geq 2$ izanik. Orduan, $(p(X))$ $K[X]$-ren ideal maximala da eta ezin da $(X - a)$ moduan jarri, $X - a$ ezin baita izan $p(X)$-ren multiploa. Adibideak indeterminatu gehiagorekin eman nahi izanez gero, hartu $\mathfrak{m} = (p(X_1), X_2, \ldots, X_n)$ ideala. Erabiltzen badugu

$$\frac{K[X_1, \ldots, X_n]}{(X_2, \ldots, X_n)} \cong K[X_1]$$

isomorfismoa, $\mathfrak{m}$ $K[X_1, \ldots, X_n]$-ren ideal maximala dela ondorioztatzen da. Hala ere, $\mathfrak{m}$ ezin da idatzi $(X_1 - a_1, \ldots, X_n - a_n)$ moduan. (Hori ere goiko isomorfismoaren ondorio berehalakoa da.)

Azken teoremaren froga beste emaitza honetan oinarritzen da.

**1.94. Teorema** (Zariskiren lema)**.** *Izan bitez $K \subseteq L$ gorputz-hedadura eta $u_1, \ldots, u_n \in L$. Orduan, $K[u_1, \ldots, u_n]$ gorputza da baldin eta soilik baldin $u_1, \ldots, u_n$ aljebraikoak badira $K$-ren gainean.*

Ohartu Zariskiren lemak lehenago aipatutako emaitza honen orokorpena dela, elementu baten baino gehiagoren kasura: $K[u]$ gorputza da baldin eta soilik baldin $u$ aljebraikoa bada $K$-ren gainean.

1.93 TEOREMAREN FROGA ZARISKIREN LEMAN OINARRITUZ. Izan bedi $L = K[X_1, \ldots, X_n]/\mathfrak{m}$ eta erabil dezagun marren notazioa $L$-ko elementuak adierazteko. Ohartu $L$ gorputza dela, $\mathfrak{m}$ $K[X_1, \ldots, X_n]$-ren ideal maximala izateagatik. Izan bedi $E = \{\overline{\lambda} \mid \lambda \in K\} \subseteq L$. Erraz egiaztatzen da $\lambda \mapsto \overline{\lambda}$ aplikazioa isomorfismo bat dela $K$-ren eta $E$-ren artean. Bereziki, $E$ aljebraikoki itxia da. Beste alde batetik,

$$\begin{aligned} L &= \left\{ \overline{f(X_1, \ldots, X_n)} \mid f \in K[X_1, \ldots, X_n] \right\} \\ &= \left\{ \sum_{i_1, \ldots, i_n \geq 0} \overline{\lambda}_{i_1, \ldots, i_n} \overline{X}_1^{i_1} \ldots \overline{X}_n^{i_n} \mid \lambda_{i_1, \ldots, i_n} \in K \right\} \\ &= E[\overline{X}_1, \ldots, \overline{X}_n] \end{aligned}$$

dugu. Horrela, $E \subseteq L$ hedadura dugu eta $L = E[\overline{X}_1, \ldots, \overline{X}_n]$ gorputza da. Zariskiren lema erabiliz, $\overline{X}_1$, …, $\overline{X}_n$ $E$-ren gainean aljebraikoak direla ondorioztatzen dugu. Orain, $E$ aljebraikoki itxia dela kontuan hartuz, $\overline{X}_1, \ldots, \overline{X}_n \in E$ lortzen dugu. Horrela, existitzen dira $a_1, \ldots, a_n \in K$, halakoak non $\overline{X}_1 = \overline{a}_1$, …, $\overline{X}_n = \overline{a}_n$ baita. Ondorioz, $X_1 - a_1, \ldots, X_n - a_n \in \mathfrak{m}$ dugu eta, $\mathfrak{m}$ ideala eta propioa izateagatik,

$$(X_1 - a_1, \ldots, X_n - a_n) \subseteq \mathfrak{m} \subsetneq K[X_1, \ldots, X_n]$$

partekotasunak ditugu. Badakigunez $(X_1 - a_1, \ldots, X_n - a_n)$ $K[X_1, \ldots, X_n]$-ren ideal maximala dela, hortik $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ berdintza ondorioztatzen da. □

Zariskiren lemaren frogan, funtsezkoa da elementu osoaren kontzeptua, jarraian definitzen duguna.

**1.95. Definizioa.** Izan bitez $A \subseteq B$ eraztun-hedadura eta $b \in B$. Orduan, $b$ $A$-ren gainean *elementu osoa* dela esaten dugu existitzen bada $f \in A[X]$ polinomio moniko bat, non $f(b) = 0$ baita.

Ikusten dugunez, definizio hori eta elementu aljebraikoarena oso antzekoak dira. Diferentzia bakarrak hauek dira:

(i) Elementu aljebraikoaren definizioa gorputz-hedadura baten kasuan ematen da, eta ez eraztun orokorren hedaduretarako.
(ii) Elementu osoa izateko, $f(b) = 0$ betetzen duen $f$ polinomioari monikoa izateko eskatzen zaio eta elementu aljebraikoa izateko, berriz, ez.

Hala ere, $K \subseteq L$ gorputz-hedadura batean, elementu osoak eta aljebraikoak gauza bera dira. Izan ere, $u \in L$ aljebraikoa bada, orduan badago $g \in K[X]$, $g \neq 0$, non $g(u) = 0$ baita. Orain, $g$-ren koefiziente nagusia $\lambda$ bada, $f = \lambda^{-1}g$ polinomioa monikoa da eta $f(u) = 0$ dugu. Hortaz, $u$ elementu osoa ere bada. Horrek esan nahi du elementu osoaren kontzeptua elementu aljebraikoaren luzapena besterik ez dela, gorputz-hedaduretatik eraztun-hedaduretara pasatzeko.

**1.96. Adibideak.** 1) Nabaria da $A$ eraztun bateko elementu guztiak $A$-ren gainean osoak direla. Azken batean, $a \in A$ elementua $X - a \in A[X]$ polinomioaren erroa da.

2) $\mathbb{Z} \subseteq \mathbb{C}$ hedaduran, $\sqrt{2}$, $\sqrt[3]{2}$ eta $i$ elementu osoak dira.

3) $\mathbb{Z} \subseteq \mathbb{Q}$ hedaduran $1/2$ ez da osoa, nahiz eta $f(X) = 2X - 1 \in \mathbb{Z}[X]$ polinomioaren erroa izan. Kontua da ezin dela izan koefiziente osoak dituen polinomio *moniko* baten erroa, hurrengo teoreman frogatzen dugun bezala. Horrek erakusten du, gorputzen kasuan ez bezala, eraztun-hedaduren kasuan polinomioa monikoa izateko baldintza funtsezkoa dela elementu bat osoa den edo ez erabakitzeko.

**1.97. Teorema.** *Izan bitez $A$ F.B.D. eta $K$ $A$-ren zatikien gorputza. Orduan, $A \subseteq K$ hedadurako elementu oso bakarrak $A$-koak dira.*

Froga. Nahikoa da 1.67 teoremaren (ii) atala irakurtzea. Horren arabera, $f \in A[X]$ polinomio moniko batek $K$-n dituen erroak $A$-n daude. □

Beraz, azken adibidean ikusitakoa ez da kasualitatea, eta $\mathbb{Z} \subseteq \mathbb{Q}$ hedaduran elementu oso bakarrak $\mathbb{Z}$-koak dira. Zariskiren lemaren frogarako, aurreko teoremaren kasu berezi hau interesatuko zaigu.

**1.98. Korolarioa.** *Izan bedi $K$ gorputza. Orduan, $K[X] \subseteq K(X)$ hedadurako elementu oso bakarrak $K[X]$-koak dira. Hau da, polinomioen zatiki bat osoa bada $K[X]$-ren gainean, orduan zatiki hori polinomio bat da benetan.*

Galoisen teorian frogatzen da elementu aljebraikoen batura, biderkadura eta zatidura berriro ere aljebraikoak direla. Hori dela eta, $K \subseteq L$ hedadura batean, elementu aljebraikoek tarteko gorputz bat osatzen dute. Elementu osoekin antzeko zerbait gertatzen da.

**1.99. Teorema.** *Izan bedi $A \subseteq B$ eraztun-hedadura. Orduan, hedadura horretako elementu osoen batura eta biderkadura elementu osoak dira berriro ere. Ondorioz, elementu osoek $R$ eraztun bat osatzen dute, $A \subseteq R \subseteq B$ betetzen duena.*

Gorputz-hedadura bat, $K \subseteq L$, aljebraikoa dela esaten dugu $L$-ko elementu guztiak aljebraikoak badira $K$-ren gainean. Hurrengo teoreman hedadura aljebraikoen oinarrizko propietate pare bat ematen ditugu.

**1.100. Teorema.** (i) *Izan bitez $K \subseteq E$ eta $E \subseteq L$ bi hedadura aljebraiko. Orduan, $K \subseteq L$ hedadura ere aljebraikoa da.* (Hedadura aljebraikoen propietate iragankorra.)

(ii) *Izan bedi $K \subseteq L$ gorputz-hedadura eta demagun $u_1, \ldots, u_n \in L$ aljebraikoak direla $K$-ren gainean. Orduan, $K \subseteq K(u_1, \ldots, u_n)$ hedadura aljebraikoa da.*

Antzera definitzen dira eraztun-hedadura osoak. Kasu horretan ere propietate iragankorra dugu eta, bestetik, $A \subseteq B$ hedadura batean $b_1, \ldots, b_n$ elementuak osoak badira $A$-ren gainean, orduan $A \subseteq A[b_1, \ldots, b_n]$ hedadura osoa da. (Hor, nahiz eta $A$ gorputza ez izan, $A[b_1, \ldots, b_n]$-ren esanahia aljebren kasukoa bezalakoa da: $b_1, \ldots, b_n$ elementuekin egin daitezkeen konbinazio polinomiko guztiak dira, koefizienteak $A$-n izanik.)

Zariskiren lemaren froga. Bi inplikazioak $n$-ren gaineko indukzioa erabiliz egingo ditugu (bakoitza bere aldetik). Ohartu $n = 1$ den kasua ezaguna dela. Beraz, $n \geq 2$ hartuko dugu hemendik aurrera.

$\Leftarrow$) Demagun $u_1, \ldots, u_n$ aljebraikoak direla $K$ gorputzaren gainean. Indukzio-hipotesiaren arabera, $L = K[u_1, \ldots, u_{n-1}]$ gorputza da. Orain, $u_n$ $L$-ren gainean aljebraikoa denez ($K$-ren gainean aljebraikoa delako eta $K \subseteq L$ delako), $L[u_n]$ gorputza da. Kontuan izanik $L[u_n] = K[u_1, \ldots, u_n]$ dela, inplikazio hori frogaturik gelditzen da.

$\Rightarrow$) Demagun orain $F = K[u_1, \ldots, u_n]$ gorputza dela. Izan bedi $E = K(u_1)$. Orduan, $F$ gorputza denez, $E \subseteq F$ dugu eta, $u_2, \ldots, u_n \in F$ denez, $E[u_2, \ldots, u_n] \subseteq F$ ere bai. Alderantzizko partekotasuna nabaria da eta, hortaz, $F = E[u_2, \ldots, u_n]$ berdintza lortzen dugu. Horrela, kate hau dugu:

$$K \subseteq K[u_1] \subseteq E = K(u_1) \subseteq F = E[u_2, \ldots, u_n].$$

Berriro ere kontuan hartuz $F$ gorputza dela, indukzio-hipotesiak ziurtatzen du $u_2, \ldots, u_n$ aljebraikoak direla $E$-ren gainean. Beraz, 1.100 teoremagatik, $E \subseteq F$

hedadura aljebraikoa da. Lortzen badugu frogatzea $u_1$ aljebraikoa dela $K$-ren gainean, orduan $K \subseteq E$ ere hedadura aljebraikoa da. Hedadura aljebraikoen propietate iragankorraga erabiliz, $K \subseteq F$ hedadura aljebraikoa dela ondorioztatzen dugu eta, bereziki, $u_1, \ldots, u_n$ elementu guztiak aljebraikoak dira $K$-ren gainean, nahi bezala.

Demagun orduan, absurdora eramanez, $u_1$ transzendentea dela $K$-ren gainean. Izan bedi $u$ edozein elementu $u_2, \ldots, u_n$-ren artean aukeratuta. Orduan, $u$ aljebraikoa da $E$-ren gainean eta, beraz, existitzen da $\alpha(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_0 \in E[X]$, non $\alpha(u) = 0$ baita. Orain, $E = K(u_1)$ dela kontuan hartuz, $\alpha$-ren koefiziente bakoitza $a_i = g_i(u_1)/h_i(u_1)$ modukoa da, $g_i, h_i \in K[X]$ eta $h_i(u_1) \neq 0$ izanik. Beraz, honako berdintza hau dugu:

$$u^k + \frac{g_{k-1}(u_1)}{h_{k-1}(u_1)}u^{k-1} + \cdots + \frac{g_1(u_1)}{h_1(u_1)}u + \frac{g_0(u_1)}{h_0(u_1)} = 0.$$

Biderkatzen badugu $h_{k-1}(u_1) \ldots h_0(u_1)$ biderkaduraz izendatzaileak eliminatzeko, orduan

$$f_k(u_1)u^k + f_{k-1}(u_1)u^{k-1} + \cdots + f_1(u_1)u + f_0(u_1) = 0$$

lortzen dugu, $f_i \in K[X]$ izanik $i$ guztietarako. Bestela esanda, azken erlazio horretako koefiziente guztiak $K[u_1]$-n daude. Horrek ez du esan nahi $u$ elementua osoa denik $K[u_1]$ eraztunaren gainean, azken berdintza horretan $u^k$-ren koefizienteak ez duelako zertan 1 izan. Hala ere, berdintza horretatik badago elementu oso bat ateratzea. Horretarako, $f_k(u_1)^{k-1}$ elementuaz biderkatzen dugu, honako adierazpen hau lortuz:

$$\big(f_k(u_1)u\big)^k + f_{k-1}(u_1)\big(f_k(u_1)u\big)^{k-1} + \cdots + f_1(u_1)f_k(u_1)^{k-2}\big(f_k(u_1)u\big) + f_0(u_1)f_k(u_1)^{k-1} = 0.$$

Hortik, $f_k(u_1)u$ elementua $K[u_1]$-en gainean osoa dela ondorioztatzen dugu.

Aurreko argudioan, $u$ gisa $u_2, \ldots, u_n$ elementuetako edozein har dezakegu. Beraz, existitzen dira $m_2, \ldots, m_n \in K[X]$, halakoak non $m_i(u_1)u_i$ biderkadura elementu osoa baita $K[u_1]$-en gainean $i = 2, \ldots, n$ guztietarako. Izan bedi $m = m_2 \ldots m_n \in K[X]$. Kontuan hartzen badugu elementu osoen biderkadura osoa dela eta $K[u_1]$-eko elementuak osoak direla $K[u_1]$-en gainean, ondorioztatzen dugu $m(u_1)u_i$ osoa dela $K[u_1]$-en gainean $i = 2, \ldots, n$ guztietarako. Jakina, $u_1$ bera osoa denez $K[u_1]$-en gainean, propietate hori $i = 1$ den kasurako ere betetzen da.

Orain, baieztatzen dugu $v \in F = K[u_1, \ldots, u_n]$ edozein izanda, badagoela $t$ berretzaile bat ($v$-ren menpekoa izango dena) non $m(u_1)^t v$ osoa den $K[u_1]$-en gainean. Hori frogatzeko, idatzi $v$ elementua $u_1, \ldots, u_n$-ren konbinazio polinomiko modura, koefizienteak $K$-n izanik. Hau da, idatzi $v = q(u_1, \ldots, u_n)$, $q \in K[X_1, \ldots, X_n]$ izanik. Orduan, $q$ polinomioaren maila osoa $t$ bada, ikus dezagun $m(u_1)^t v$ elementu osoa dela $K[u_1]$-en gainean. Ohartu $m(u_1)^t v$ honelako gaien konbinazio lineala dela, $K$ gorputzeko koefizienteekin:

$$m(u_1)^t u_1^{i_1} u_2^{i_2} \ldots u_n^{i_n},$$

$X_1^{i_1}X_2^{i_2}\dots X_n^{i_n}$ $q$-n agertzen den monomio bat izanik. Jarri $s = i_1 + i_2 + \cdots + i_n$. Maila osoaren definizioagatik, $s \leq t$ dugu. Orduan,

$$m(u_1)^t u_1^{i_1} u_2^{i_2} \dots u_n^{i_n} = m(u_1)^{t-s}(m(u_1)u_1)^{i_1}(m(u_1)u_2)^{i_2}\dots(m(u_1)u_n)^{i_n}$$

dugu, eta idazkera horrek erakusten du elementu hori osoa dela $K[u_1]$-en gainean. Beraz, $m(u_1)^t v$ ere, horien konbinazio lineala izateagatik, osoa da $K[u_1]$-en gainean. Propietate hori $v \in F$ guztietarako betetzen denez, bereziki beteko dute $K(u_1)$-eko elementu guztiek.

Kontraesana lortzeko eta, beraz, teoremaren froga bukatutzat emateko, bakarrik falta zaigu azken propietatearen "itzulpen" bat egitea. Gogoratu $u_1$ $K$-ren gainean transzendentea den baldintzapean ari garela. Orduan, $K(u_1) \cong K(X)$ dugu eta isomorfismo horren bitartez, $K[u_1] \cong K[X]$ ere badugu. Beraz, azken paragrafoko propietatea honela eman daiteke: existitzen da $m(X)$ polinomio finko bat non, $v(X) \in K(X)$ edozein funtzio arrazional harturik, $m(X)^t v(X)$ osoa baita $K[X]$-ren gainean $t$ berretzaile egoki baterako ($v(X)$-ren menpekoa izango dena). Baina, 1.98 teoremaren arabera, badakigu hori bakarrik dela posible $m(X)^t v(X)$ polinomio bat bada. Horrela, esaten ari gara badagoela $m(X)$ polinomio finko bat propietate hau betetzen duena: edozein funtzio arrazional harturik, $m(X)$-ren berretura egoki batez biderkaturik polinomio bat lor dezakegu, hau da, izendatzailea elimina dezakegu. Erraz ikus dezakegu, hala ere, hori faltsua dela. Nahikoa da $p(X) \in K[X]$ polinomio irreduzible bat aukeratzea, ez dena $m(X)$-ren faktorizazioan agertzen*, eta $v(X) = 1/p(X)$ funtzio arrazionala hartzea. Orduan, ezinezkoa da $v(X)$-ren izendatzailea eliminatzea $m(X)$-ren berretura batez biderkatuz. □

*Hori beti egin daiteke, $K[X]$ polinomioen eraztunean polinomio irreduzibleen kopurua infinitua baita. Hori ikusteko, nahikoa da infinitu zenbaki lehen daudela frogatzen duen Euklidesen argudioa errepikatzea. Ohartu, bide batez, polinomio irreduzibleen infinitutasunak beste ondorio hau duela: *gorputz aljebraikoki itxi guztiak infinituak dira.* Izan ere, nahikoa da gogoratzea gorputz aljebraikoki itxi baten gainean polinomio irreduzibleak lehenengo mailakoak baino ez direla.