3

Zatigarritasuna eta faktorizazioa eraztunetan

3.1. Elementu irreduzibleak eta elementu lehenak

Gai honetan zehar eraztun guztiak integritate-domeinuak izango dira. Normalean baldintza hori esplizituki emango da baina, agertzen ez bada ere, betetzen dela ulertuko dugu.

3.1. Definizioa. Izan bitez A integritate-domeinua eta $a, b \in A$. Orduan, *a-k b zatitzen duela* esango dugu b a-ren multiploa bada, hau da, existitzen bada $q \in A$ non $b = qa$ baita. Hori adierazteko $a \mid b$ idatziko dugu.

Ondorengo propietateak nabariak dira.

3.2. Proposizioa. *Izan bedi A integritate-domeinua. Orduan zatigarritasunak propietate hauek betetzen ditu:*

(i) $0 \mid b$ *bada, orduan* $b = 0$ *dugu.*
(ii) $a \mid 0$ *da* $a \in A$ *guztietarako.*
(iii) $u \in A^\times$ *bada, orduan*

$$a \mid b \iff ua \mid b \iff a \mid ub.$$

(iv) $a \mid b$ *dugu baldin eta soilik baldin* $(b) \subseteq (a)$ *bada.*

Garbi dago $a, b \in \mathbb{Z}$ bi zenbakik elkar zatitzen dutela baldin eta soilik baldin $a = \pm b$ bada. Jarraian ikusten dugunez, antzeko zerbait gertatzen da integritate-domeinu guztietan.

3.3. Proposizioa. *Izan bitez A integritate-domeinua eta $a, b \in A$. Orduan, baliokideak dira:*

(i) $a \mid b$ *eta* $b \mid a$.
(ii) $(a) = (b)$.
(iii) *Existitzen da* $u \in A^\times$ *non* $b = ua$ *baita.*

FROGA. Lehenengo eta behin, ohartu (i) eta (ii) baliokideak direla, 3.2 proposizioaren (iv) atala aplikatuz. Bestalde, garbi dago (iii)-k (i) inplikatzen duela. Azkenik, (i) $\Rightarrow$ (iii) inplikazioa 2.18 teoreman ikusi dugu. $\square$

3.4. Definizioa. Izan bitez A integritate-domeinua eta $a, b \in A$. Orduan, a eta b A-n *elkartuak* direla esango dugu, eta $a \sim b$ idatziko dugu, existitzen bada $u \in A^\times$ non $b = ua$ baita.

3.5. Adibideak. 1) $\mathbb{Z}$-n, $5 \sim 5$ eta $5 \sim -5$ dugu, baina $5 \not\sim b$ dugu $b \neq \pm 5$ denean.

2) $\mathbb{Q}$-n, berriz, $5 \sim b$ dugu $b \neq 0$ guztietarako. Horrek erakusten du elkartuak izateko propietatea ez dela elementuen propietatea hutsa, eta garrantzitsua dela elementuak zein eraztunen barruan hartzen ditugun.

3) $\mathbb{R}[X]$ polinomioen eraztunean $X + 1 \sim \lambda(X + 1)$ dugu $\lambda \in \mathbb{R}^\times$ guztietarako, eta $X + 1$ ez da beste inongo elementuren elkartua.

Ondorengo propietatea begi-bistakoa da.

3.6. Proposizioa. *Elkartuak izateko erlazioa baliokidetasun-erlazioa da.*

3.7. Definizioa. Izan bitez A integritate-domeinua eta $a, b \in A$. Orduan, $d \in A$ elementua a-ren eta b-ren *zatitzaile komunetako handien* bat dela esango dugu bi baldintza hauek betetzen baditu:

(i) $d \mid a$ eta $d \mid b$.
(ii) $d' \mid a$ eta $d' \mid b$ bada, $d' \in A$ izanik, orduan $d' \mid d$ dugu.

3.8. Adibidea. Argi dago a-ren eta 0-ren zatitzaile komunetako handien bat a elementua bera dela.

Aurrerago ikusiko dugunez, A integritate-domeinu batean gerta daiteke bi elementuk ez izatea zatitzaile komunetako handienik. Existitzen bada, bat baino gehiago egon daiteke baina, ondorengo proposizioak erakusten duenez, erlazio hertsia dago zatitzaile komunetako handien guztien artean.

3.9. Proposizioa. *Izan bitez A integritate-domeinua eta demagun $a, b \in A$ elementuek d_1 zatitzaile komunetako handien bat dutela A-n. Orduan, $d_2 \in A$ beste elementu bat a-ren eta b-ren zatitzaile komunetako handien bat da baldin eta soilik baldin $d_1 \sim d_2$ bada.*

FROGA. "Baldin" zatia tribiala da, kontuan hartzen badugu zatigarritasuna ez dela aldatzen unitate batez biderkatzean. Frogatu dezagun, bada, "soilik baldin" zatia: d_2 ere a-ren eta b-ren zatitzaile komunetako handien bat bada, d_1 eta d_2 A-n elkartuak direla ikusi behar dugu. Alde batetik, d_1-ek zatitzaile komunetako handienaren definizioko (i) baldintza betetzen du, hau da, $d_1 \mid a$ eta $d_1 \mid b$ dugu. Orain, d_2-k definizioko (ii) baldintza betetzen duenez, $d_1 \mid d_2$ dela ondorioztatzen dugu. Simetriagatik, $d_2 \mid d_1$ ere betetzen da. Beraz, 3.3 proposizioa aplikatuz, existitzen da $u \in A^\times$ non $d_2 = ud_1$ baita, eta d_1 eta d_2 elkartuak dira A-n. $\square$

Aurreko proposizioaren arabera, bi elementuren zatitzaile komunetako handien bat existitzen bada, orduan zatitzaile komunetako handien guztiek elementu elkartuen baliokidetasun-klase bat osatzen dute. Hori dela eta, anbiguoa izan daiteke $\text{zkh}(a,b)$ bezalako notazioa erabiltzea, ez baitago garbi baliokidetasun-klase horretatik zein elementu aukeratzen ari garen ikur horren bitartez adierazteko. Hala ere, bi kasu hauetan badago ohikoa den aukera bat:

(i) $\mathbb{Z}$-n, baliokidetasun-klase horretan dagoen zenbaki ez-negatibo bakarra aukeratzen da.
(ii) $K[X]$-n, K gorputza izanik, baliokidetasun-klase horretan dagoen polinomio moniko bakarra aukeratzen da.

Beste alde batetik, elementu elkartu guztiek ideal bera sortzen dutenez, ez dago anbiguotasunik zatitzaile komunetako handien batek sortzen duen idealari dagokionez. Horrela, notazioaz abusatuz, batzuetan $(\text{zkh}(a,b))$ idatziko dugu, nahiz eta $\text{zkh}(a,b)$ ikurrak, solte, esanahi garbirik ez izan.

3.10. Definizioa. Izan bitez A integritate-domeinua eta $a,b \in A$. Orduan, $d \in A$ elementua a-ren eta b-ren *multiplo komunetako txikien* bat dela esango dugu bi baldintza hauek betetzen baditu:

(i) $a \mid m$ eta $b \mid m$.
(ii) $a \mid m'$ eta $b \mid m'$ bada, $m' \in A$ izanik, orduan $m \mid m'$ dugu.

3.11. Adibidea. Argi dago a-ren eta 0-ren multiplo komunetako txikien bakarra 0 dela.

Gerta daiteke bi elementuren multiplo komunetako txikienik ez existitzea, baina zatitzaile komunetako handienaren kasuan bezala, ondorengo emaitza lor dezakegu.

3.12. Proposizioa. *Izan bitez A integritate-domeinua eta demagun $a,b \in A$ elementuek m_1 multiplo komunetako txikien bat dutela A-n. Orduan, $m_2 \in A$ beste elementu bat a-ren eta b-ren multiplo komunetako txikien bat da baldin eta soilik baldin $m_1 \sim m_2$ bada.*

Berriro ere, $\text{mkt}(a,b)$ soilik idaztea anbiguoa izan daiteke, baina garbi dago $(\text{mkt}(a,b))$ ideala zein den.

3.13. Definizioa. Izan bitez A integritate-domeinua eta $a \in A$. Orduan, a elementua A-n *irreduziblea* dela esango dugu, baldintza hauek betetzen badira:

(i) $a \neq 0$.
(ii) a ez da unitatea A-n.
(iii) $a = bc$ bada, $b,c \in A$ izanik, orduan b eta c elementuetako bat unitatea da A-n.

Hemendik aurrera integritate-domeinuekin baino ez gara arituko eta, horregatik, elementu irreduziblearen definizioa testuinguru horretan eman dugu. Hala ere,

definizioak zentzua du eraztun orokor batean; ikusi 3.2, 3.3 eta 3.4 ariketak adibide batzuk ikusteko integritate-domeinuak ez diren eraztunen gainean.

3.14. Adibideak. 1) $\mathbb{Z}$ eraztunean, elementu irreduzibleak zenbaki lehenak dira, eta zenbaki lehenen negatiboak.

2) Harrigarria badirudi ere, $A[X]$ polinomioen eraztun batean, gerta daiteke X indeterminatua ez izatea irreduziblea. Adibidez, $\mathbb{Z}/6\mathbb{Z}[X]$ eraztunean, $X = (\overline{2}X + \overline{3})(\overline{3}X + \overline{2})$ faktorizazioa dugu, eta $\overline{2}X + \overline{3}$ eta $\overline{3}X + \overline{2}$ ez dira unitateak. (Kontuan izan, oro har, $f(X) = a_0 + \cdots + a_nX^n$ polinomio bat $A[X]$-n unitatea izanez gero, a_0 gai askeak A-ren unitatea izan behar duela.)

3) Hala ere, aurreko ataleko egoera ezin da gertatu A integritate-domeinua bada. Izan ere, $X = f(X)g(X)$ bada, orduan $\deg f + \deg g = 1$ dugu, eta f eta g polinomioetako batek konstantea izan behar du. Demagun, adibidez, $f(X) = a_0$ dela, eta idatz dezagun $g(X) = b_0 + \cdots + b_mX^m$. Orduan, $a_0b_1 = 1$ denez, a_0 unitatea da. Horrela, X-ren faktorizazioan polinomioetako bat unitatea da eta, hortaz, X irreduziblea da.

Irreduziblea izateko propietatea ez da elementuaren propietate absolutua, erlatiboa baizik: lanean ari garen eraztunaren araberakoa izan daiteke. Adibidez, $X^2 + 1$ polinomioa irreduziblea da $\mathbb{R}[X]$-n, baina ez da irreduziblea $\mathbb{C}[X]$-n, $X^2 + 1 = (X + i)(X - i)$ faktorizazioa baitugu. Bestalde, 2 zenbakia irreduziblea da $\mathbb{Z}$-n, baina ez da irreduziblea $\mathbb{Q}$-n, bigarren kasu horretan unitatea baita.

3.15. Oharra. Izan bitez $a, b \in A$ elementu elkartuak. Orduan, garbi dago a irreduziblea dela baldin eta soilik baldin b irreduziblea bada.

Terminologiari dagokionez, $A[X]$ moduko eraztunen kasuan, f polinomioa $A[X]$-n irreduziblea dela esateko beste modu bat da *A-ren gainean irreduziblea* dela esatea.

3.16. Definizioa. Izan bitez A integritate-domeinua eta $a \in A$. Orduan, a elementua A-n *lehena* dela esango dugu, baldintza hauek betetzen badira:

(i) $a \neq 0$.
(ii) a ez da unitatea A-n.
(iii) $a \mid bc$ bada, $b \in A$ eta $c \in A$ izanik, orduan $a \mid b$ edo $a \mid c$ dugu.

Nabaria da, faktoreen kopuruaren gaineko indukzioa aplikatuz, elementu lehenek propietate orokorrago hau betetzen dutela: $a \mid b_1 \dots b_n$ bada, orduan existitzen da $i \in \{1, \dots, n\}$ non $a \mid b_i$ baita.

Ondorengo proposizioak garbi erakusten du elementu lehenaren izenaren arrazoia.

3.17. Proposizioa. *Izan bitez A integritate-domeinua eta $a \in A$. Orduan,*

$$(a) \text{ ideal lehena} \iff a = 0 \text{ edo } a \text{ lehena.}$$

FROGA. $\Rightarrow$) Demagun (a) ideal lehena eta $a \neq 0$ dela, eta frogatu dezagun a lehena dela. Lehenengo eta behin, (a) A-ren ideal lehena izateagatik, $(a) \neq A$ dugu eta, hortaz, a ez da unitatea. Beraz, bakarrik falta zaigu elementu lehenaren definizioko (iii) baldintza egiaztatzea. Horretarako, demagun $a \mid bc$ dela. Orduan, $bc \in (a)$ eta (a) ideal lehena denez, $b \in (a)$ edo $c \in (a)$ dugu. Horrela, $a \mid b$ edo $a \mid c$, eta frogaturik gelditzen da a lehena dela.

$\Leftarrow$) Hasteko, $a = 0$ bada, ohartu $(a) = \{0\}$ A-ren ideal lehena dela, A integritate-domeinua izateagatik. Demagun orain a lehena dela, eta bc biderkadura (a)-n dagoela. Orduan, $a \mid bc$ dugu eta, a lehena denez, $a \mid b$ edo $a \mid c$. Horrela $b \in (a)$ edo $c \in (a)$ lortzen dugu. Bestalde, a lehena izateagatik, a ez da unitatea. Beraz, $(a) \neq A$ dugu eta frogaturik gelditzen da (a) ideal lehena dela. □

Definitu berri ditugun bi kontzeptuak oso estuki lotuta daude. Hasteko, hurrengo emaitza dugu.

3.18. Proposizioa. *Izan bitez A integritate-domeinua eta $a \in A$ elementu lehena. Orduan, a irreduziblea da.*

FROGA. Bakarrik egiaztatu behar dugu a-k elementu irreduziblearen definizioko (iii) baldintza betetzen duela. Horretarako, demagun $a = bc$ dela, $b, c \in A$ izanik, eta ikus dezagun b eta c elementuetako bat unitatea dela A-n. Bereziki, $a \mid bc$ dugu eta, a elementu lehena denez, $a \mid b$ edo $a \mid c$ lortzen dugu. Orokortasuna galdu gabe, $a \mid b$ den kasuan arituko gara. Orduan, existitzen da $u \in A$ non $b = au$ baita eta, beraz, $a = auc$. Kontuan hartzen badugu A integritate-domeinua dela eta $a \neq 0$ dela, $1 = uc$ lortzen dugu, eta c unitatea da. □

Ikusiko dugunez, aurreko proposizioaren alderantzizkoa ez da egia integritate-domeinu guztietan. Hala ere, bai beteko da hurrengo atalean sartuko ditugun eraztun berezi batzuetan.

3.19. Korolarioa. *Izan bitez A integritate-domeinua eta $a \in A$, $a \neq 0$. Baldin eta (a) ideal nagusia lehena bada, orduan a irreduziblea da.*

3.2. Faktorizazio bakarreko domeinuak

3.20. Definizioa. Izan bedi A integritate-domeinua. Orduan, A *faktorizazio bakarreko domeinua* (laburkiago *F.B.D.*) dela diogu bi baldintza hauek betetzen badira:

(i) $a \in A$ elementua ez bada nulua eta ez bada unitatea, orduan $a = p_1 \dots p_n$ idatz dezakegu, $p_1, \dots, p_n \in A$ elementu irreduzibleak izanik.

(ii) Betetzen bada $p_1 \dots p_n = q_1 \dots q_m$, p_i eta q_j elementu guztiak A-n irreduzibleak izanik, orduan $n = m$ dugu, eta existitzen da $\pi \in S_n$ permutazio bat non $p_i \sim q_{\pi(i)}$ baita $i = 1, \dots, n$ guztietarako. Bestela esanda, bi faktorizazioak berdinak dira, faktoreen ordena eta unitateak salbu.

3.21. Adibideak. 1) Ezaguna da $\mathbb{Z}$ faktorizazio bakarreko domeinua dela.

2) Gorputz bat faktorizazio bakarreko domeinua da modu tribialean.

3) Laugarren gaian frogatuko dugunez, A faktorizazio bakarreko domeinua bada, orduan $A[X]$ ere faktorizazio bakarreko domeinua da. Emaitza hori behin eta berriz aplikatuz, $A[X_1, \dots, X_n]$ faktorizazio bakarreko domeinua da $n \in \mathbb{N}$ guztietarako. Bereziki, K gorputza bada, orduan $K[X_1, \dots, X_n]$ faktorizazio bakarreko domeinua da. Gai honen amaieran $K[X]$-ren kasurako froga zuzen bat emango dugu, hurrengo gaiko emaitza erabili gabe.

Izan bedi A faktorizazio bakarreko domeinua, eta aukeratu dezagun elementu irreduzible elkartuen baliokidetasun-klase bakoitzeko ordezkari bat. Dei diezaiogun Π ordezkari horien multzoari. Adibidez, $\mathbb{Z}$-ren kasuan zenbaki lehen positiboen multzoa izan liteke Π multzoa, baina baita ere zenbaki lehen negatiboena, eta $K[X]$-ren kasuan, berriz, polinomio irreduzible monikoen multzoa har genezake. Orduan, edozein $a \in A$, $a \neq 0$, modu honetan jar daiteke:

$$a = up_1^{m_1} \dots p_r^{m_r}, \tag{3.1}$$

u unitatea izanik, eta $p_i \in \Pi$ eta $m_i \in \mathbb{N}$ izanik $i = 1, \dots, r$ guztietarako. Gainera, erraz ikusten da idazkera hori bakarra dela. Batzuetan, $a, b \in A$ bi elementuren faktorizazioak batera erabili nahi izango ditugu. Orduan, argudioak erraztearren, (3.1) adierazpenean 0 diren berretzaileak onartuko ditugu, eta horrela bi elementuen faktorizazioetan elementu irreduzible berberak agertzen direla pentsatu ahal izango dugu. Hau da,

$$a = up_1^{m_1} \dots p_r^{m_r} \qquad \text{eta} \qquad b = vp_1^{n_1} \dots p_r^{n_r}$$

idatziko dugu, $u, v \in A^\times$ izanik eta m_i, n_i guztiak zenbaki oso ez-negatiboak izanik. Antzera egin dezakegu bi elementu baino gehiagorekin arituz gero.

Faktorizazio bakarra erabiliz, erraz frogatu dezakegu zenbaki osoekin oso ezaguna dugun emaitza hau.

3.22. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta $a, b, c \in A$. Baldin eta $a \mid bc$ eta $\operatorname{zkh}(a, b) = 1$ bada, orduan $a \mid c$ dugu.*

Ikus dezagun faktorizazio bakarreko domeinuetan egiazkoa dela 3.18 proposizioaren alderantzizkoa.

3.23. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta $a \in A$ elementu irreduziblea. Orduan, a lehena da.*

Froga. Nahikoa dugu elementu lehenaren definizioko (iii) baldintza egiaztatzea. Demagun, bada, $a \mid bc$ dela, $b, c \in A$ izanik. Orduan, existitzen da $q \in A$ non $qa = bc$ baita. Alde batetik, b eta c ezin dira 0 izan, bestela $a = 0$ ere litzatekeelako. Bestetik, b unitatea bada, orduan zuzenean $a \mid c$ lortzen dugu, eta antzera $a \mid b$ dugu c unitatea bada. Beraz, b eta c ez-nuluak eta ez-unitateak diren kasuan jar gaitezke.

Orduan, A faktorizazio bakarreko domeinua denez, $b = p_1 \dots p_n$ eta $c = p'_1 \dots p'_m$ jar dezakegu, p_i eta p'_j guztiak A-n irreduzibleak izanik. Beraz,

$$qa = p_1 \dots p_n p'_1 \dots p'_m$$

dugu. Orain, q elementua ere deskonposatzen badugu, aurreko berdintzaren bi aldeetan irreduzibleen biderkadurak ikusiko ditugu. Kontuan hartuz A faktorizazio bakarreko domeinua dela eta a irreduziblea dela, a elementuak eta beste aldeko irreduzibleren batek elkartuak izan behar dute. Betetzen bada $a \sim p_i$ dela $i \in \{1, \dots, n\}$ izanik, orduan $a \mid b$ lortzen dugu; bestela, $a \sim p'_j$ bada $j \in \{1, \dots, m\}$ izanik, orduan $a \mid c$ dugu. □

Aurreko proposizioa eta 3.18 proposizioa konbinatuz, ikusten dugu elementu irreduzibleak eta elementu lehenak bat datozela faktorizazio bakarreko domeinu batean. Ondorioz, 3.17 proposizioa aplikatuz, emaitza hau dugu.

3.24. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta $a \in A$. Orduan,*

$$(a) \text{ ideal lehena} \iff a = 0 \text{ edo } a \text{ irreduziblea.}$$

Ondoren, faktorizazio bakarreko domeinuetan zatitzaile komunetako handienak eta multiplo komunetako handienak beti existitzen direla ikusiko dugu. Horretarako, lema begi-bistako bat behar dugu.

3.25. Lema. *Izan bitez A faktorizazio bakarreko domeinua eta $a, b \in A$, $a, b \neq 0$. Finka dezagun elementu irreduzible elkartuen ordezkarien multzo bat, Π, eta idatz dezagun*

$$a = up_1^{m_1} \dots p_r^{m_r} \qquad \text{eta} \qquad b = vp_1^{n_1} \dots p_r^{n_r},$$

u eta v unitateak izanik, $p_i \in \Pi$ izanik, eta m_i, n_i zenbaki oso ez-negatiboak izanik. Orduan,

$$a \mid b \iff m_i \leq n_i \text{ bada } i = 1, \dots, r \text{ guztietarako.}$$

3.26. Teorema. *Izan bitez A faktorizazio bakarreko domeinua eta $a, b \in A$. Orduan, existitzen dira a-ren eta b-ren zatitzaile komunetako handiena eta multiplo komunetako txikiena. Are gehiago, $a, b \neq 0$ bada, orduan finkatzen badugu elementu irreduzible elkartuen ordezkarien multzo bat, Π, eta idazten badugu*

$$a = up_1^{m_1} \dots p_r^{m_r} \qquad \text{eta} \qquad b = vp_1^{n_1} \dots p_r^{n_r},$$

u eta v unitateak izanik, $p_i \in \Pi$ izanik, eta m_i, n_i zenbaki oso ez-negatiboak izanik, orduan

$$\operatorname{zkh}(a, b) = p_1^{\min\{m_1, n_1\}} \dots p_r^{\min\{m_r, n_r\}} \tag{3.2}$$

eta

$$\operatorname{mkt}(a, b) = p_1^{\max\{m_1, n_1\}} \dots p_r^{\max\{m_r, n_r\}} \tag{3.3}$$

jar dezakegu.

FROGA. Alde batetik, a eta b elementuetako bat 0 bada, badakigu zatitzaile komunetako handiena eta multiplo komunetako txikiena existitzen direla, 3.8 eta 3.11 adibideetan ikusi dugun bezala. Hemendik aurrera, bada, $a, b \neq 0$ hartuko ditugu.

Berehala egiaztatzen da, 3.25 lemaren laguntzaz,

$$p_1^{\min\{m_1,n_1\}} \dots p_r^{\min\{m_r,n_r\}}$$

elementuak zatitzaile komunetako handienaren definizioko bi baldintzak betetzen dituela, eta

$$p_1^{\max\{m_1,n_1\}} \dots p_r^{\max\{m_r,n_r\}}$$

elementuak, berriz, multiplo komunetako txikienaren definiziokoak. □

3.27. Oharrak. 1) Aurretik esan dugu $\operatorname{zkh}(a, b)$ ikurraren erabilera anbiguoa izan daitekeela, zatitzaile komunetako handien guztiek elementu elkartuen baliokidetasun-klase bat osatzen baitute. Antzera gertatzen da $\operatorname{mkt}(a, b)$-rekin. Ikur horiei esanahi zehatza emateko, modu bat adierazi behar dugu baliokidetasun-klase horietatik elementu bakar bat aukeratzeko. Hori da, hain zuzen ere, aurreko teoreman lortzen dena, (3.2) eta (3.3) formulen bitartez. Kontuan izan horretarako Π multzoa zehaztu behar dela, hau da, elementu irreduzible elkartuen baliokidetasun-klase bakoitzetik elementu bat aukeratu behar dugula.

2) Zatitzaile komunetako handienaren eta multiplo komunetako txikienaren definizioak erraz egokitzen dira bi elementu baino gehiagoren kasura hedatzeko. Baldin eta A faktorizazio bakarreko domeinua bada eta $a_1, \dots, a_n \in A$ bada, orduan aurreko teoreman bezala argudiatuz, frogatu dezakegu elementu horien zatitzaile komunetako handien bat eta multiplo komunetako txikien bat existitzen direla. Gainera, Π elementu irreduzibleen ordezkarien multzoa finkatuz gero, $\operatorname{zkh}(a_1, \dots, a_n)$ eta $\operatorname{mkt}(a_1, \dots, a_n)$ ikurrak erabil ditzakegu, eta (3.2) eta (3.3) formulen antzeko adierazpenen bidez emanda daude. Erraz frogatzen dira errekurrentzia-erlazio hauek:

$$\operatorname{zkh}(a_1, \dots, a_n) = \operatorname{zkh}(\operatorname{zkh}(a_1, \dots, a_{n-1}), a_n) \tag{3.4}$$

eta

$$\operatorname{mkt}(a_1, \dots, a_n) = \operatorname{mkt}(\operatorname{mkt}(a_1, \dots, a_{n-1}), a_n). \tag{3.5}$$

3.28. Korolarioa. *Izan bitez A faktorizazio bakarreko domeinua eta $a, b \in A$. Orduan,* $\operatorname{zkh}(a, b) \operatorname{mkt}(a, b) \sim ab$.

Orain, ikus dezagun nola lor daitekeen ideal nagusien ebakidura faktorizazio bakarreko domeinu batean.

3.29. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta $a, b \in A$. Orduan, $(a) \cap (b) = (\operatorname{mkt}(a, b))$ dugu.*

FROGA. Nahikoa da baliokidetasun-kate hau kontuan hartzea:

$$x \in (a) \cap (b) \iff a \mid x \text{ eta } b \mid x \iff \operatorname{mkt}(a, b) \mid x \iff x \in (\operatorname{mkt}(a, b)).$$

Ohartu A faktorizazio bakarreko domeinua izateko baldintza multiplo komunetako txikienaren existentziarako behar dugula. □

Azkenik, faktorizazio bakarreko domeinu baten zatikien gorputzaren propietate pare bat emango ditugu, dagoeneko $\mathbb{Q}$-n ezagunak ditugunak.

3.30. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta K A-ren zatikien gorputza. Orduan, A-ren elementu irreduzible elkartuen ordezkarien Π multzo bat finkatzen badugu, K-ren elementu bakoitza*

$$up_1^{n_1} \dots p_r^{n_r}$$

moduan idatz daiteke, $u \in A^\times$, $p_i \in \Pi$ eta $n_i \in \mathbb{Z} \setminus \{0\}$ izanik. Gainera, idazkera hori bakarra da.

Froga. Izan bedi $a/b \in K$ edozein. Orduan, $a = u_1 p_1^{k_1} \dots p_r^{k_r}$ eta $b = u_2 p_1^{\ell_1} \dots p_r^{\ell_r}$ idatz dezakegu, $u_1, u_2 \in A^\times$, $p_i \in \Pi$ eta $k_i, \ell_i \in \mathbb{N} \cup \{0\}$ izanik. Beraz,

$$\frac{a}{b} = up_1^{n_1} \dots p_r^{n_r}$$

dugu, $u = u_1 u_2^{-1} \in A^\times$ izanik, eta $n_i = k_i - \ell_i \in \mathbb{Z}$ izanik. Jakina, $n_i = 0$ bada i-ren batentzat, orduan $p_i^{n_i}$ berretura ezaba dezakegu. Beraz, orokortasuna galdu gabe $n_i \in \mathbb{Z} \setminus \{0\}$ den kasura mugatu gaitezke.

Ikus dezagun orain adierazpenaren bakartasuna. Horretarako, demagun a/b-ren beste adierazpen bat dugula. Bi adierazpenetan zero diren berretzaileak onartzen baditugu, orduan

$$\frac{a}{b} = up_1^{n_1} \dots p_r^{n_r} = vp_1^{m_1} \dots p_r^{m_r}$$

dela jar dezakegu, $u, v \in A^\times$ eta $m_i, n_i \in \mathbb{Z}$ izanik. Izan bitez

$$s_i = \begin{cases} n_i - m_i, & n_i > m_i \text{ bada,} \\ 0, & \text{bestela,} \end{cases} \qquad \text{eta} \qquad t_i = \begin{cases} m_i - n_i, & n_i < m_i \text{ bada,} \\ 0, & \text{bestela.} \end{cases}$$

Orduan,

$$up_1^{s_1} \dots p_r^{s_r} = vp_1^{t_1} \dots p_r^{t_r}$$

berdintza dugu A-ren barruan, ez K-ren barruan, berretzaile guztiak ez-negatiboak baitira. Orain, A faktorizazio bakarreko domeinua denez, $u = v$ eta $s_i = t_i$ lortzen dugu, $i = 1, \dots, r$ guztietarako. Hortik, nahitaez $n_i = m_i$ dugu $i = 1, \dots, r$ guztietarako. □

3.31. Definizioa. Izan bitez A faktorizazio bakarreko domeinua. Orduan, a/b zatiki bat, $a, b \in A$ izanik, *laburtezina* dela diogu $\operatorname{zkh}(a, b) = 1$ bada.

3.32. Proposizioa. *Izan bitez A faktorizazio bakarreko domeinua eta K A-ren zatikien gorputza. Orduan, $x \in K$ elementu bakoitza a/b zatiki laburtezin modura idatz daiteke, eta idazkera hori bakarra da zentzu honetan: $x = a'/b'$ badugu, hori ere zatiki laburtezina izanik, orduan existitzen da $u \in A^\times$ non $a' = ua$ eta $b' = u^{-1}b$ baita.*

FROGA. Idatzi $x = a_0/b_0$, $a_0, b_0 \in A$ izanik, eta jarri $d = \text{zkh}(a_0, b_0)$. Orduan, $a = a_0/d$ eta $b = b_0/d$ elementuak A-n daude, eta $x = a/b$ dugu, zatiki hori laburtezina izanik.

Ikus dezagun orain bakartasunari buruzko baieztapena. Demagun $x = a/b = a'/b'$ dugula, bi zatikiak laburtezinak izanik. Orduan, $ab' = ba'$ da eta, bereziki, $a \mid ba'$ dugu. Orain, 3.22 proposizioa erabiliz, $\text{zkh}(a, b) = 1$ izateagatik $a \mid a'$ izan behar du. Era berean, $a' \mid a$ izan behar dugu eta, 3.3 proposizioa aplikatuz, existitzen da $u \in A^\times$ non $a' = ua$. Antzera argudiatuz, existitzen da $v \in A^\times$ non $b' = vb$ baita. Orain, $ab' = ba'$ bete behar denez, $v = u^{-1}$ izan behar dugu. □

3.3. Ideal nagusietako domeinuak

3.33. Definizioa. Izan bedi A integritate-domeinua. Orduan, *A ideal nagusietako domeinua* (laburkiago *I.N.D.*) dela esango dugu A-ren ideal guztiak nagusiak badira.

3.34. Adibideak. 1) Badakigu $\mathbb{Z}$-ren ideal guztiak $n\mathbb{Z}$ motakoak direla, $n \in \mathbb{N} \cup \{0\}$ izanik. Orain, $n\mathbb{Z} = (n)$ ideal nagusia denez, $\mathbb{Z}$ ideal nagusietako domeinua dela ondorioztatzen dugu.

2) Hurrengo atalean ikusiko dugunez, K gorputza bada, orduan $K[X]$ ideal nagusietako domeinua da.

3) $K[X, Y]$ ez da ideal nagusietako domeinua. Adibidez, (X, Y) ideala ez da nagusia. Izan ere, demagun absurdora eramanez $(X, Y) = (f)$ dela $f \in K[X, Y]$ polinomioren batentzat. Orduan, $f \mid X$ eta $f \mid Y$ lortzen dugu. Orain, $f \mid X$ izateagatik, f polinomioan ez da Y-rik agertzen (bestela esanda, $\deg_Y f = 0$ dugu). Antzera, f-n ez da X-rik agertzen $f \mid Y$ izateagatik. Ondorioz, f polinomio konstantea da. Hori kontraesana da: alde batetik, 0 konstanteak $\{0\}$ ideala sortzen du, eta bestetik konstante ez-nulu bat unitatea da, eta beraz $K[X, Y]$ eraztun osoa sortzen du. Baina gure kasuan $(f) = (X, Y) \neq \{0\}, K[X, Y]$ dugu.

4) Aurreko argudio berak frogatzen du $K[X_1, \ldots, X_n]$ ez dela ideal nagusietako domeinua $n \geq 2$ denean.

5) $\mathbb{Z}[X]$ ez da ideal nagusietako domeinua. Adibidez, $(2, X)$ ideala ez da nagusia.

Ideal nagusietako domeinu batean, erraz erabaki dezakegu ideal bat (sortzaile bakar baten bidez emanda badago) maximala edo lehena den.

3.35. Teorema. *Izan bitez A ideal nagusietako domeinua eta $a \in A$. Orduan:*

(i) *(a) maximala da baldin eta soilik baldin a irreduziblea bada.*
(ii) *(a) lehena da baldin eta soilik baldin $a = 0$ edo a irreduziblea bada.*

FROGA. Badakigu $\{0\}$ ideala lehena dela, A integritate-domeinua izateagatik. Beraz, teorema frogatzeko nahikoa da hiru propietate hauek baliokideak direla frogatzea, $a \neq 0$ den baldintzapean:

(P1) (a) maximala da.
(P2) (a) lehena da.
(P3) a irreduziblea da.

Ezaguna dugu ideal maximal guztiak lehenak direla; beraz, (P1)-ek (P2) inplikatzen du. Bestalde, integritate-domeinuetan (P2)-k (P3) inplikatzen duela 3.19 korolarioan ikusita daukagu (gogoratu $a \neq 0$ dela). Beraz, nahikoa dugu (P3)-tik (P1) ondorioztatzen dela frogatzea. Demagun, bada, a irreduziblea dela, eta ikus dezagun (a) A-ren ideal maximala dela. Alde batetik, $(a) \neq A$ dugu, a ez baita unitatea. Orain, $(a) \subseteq \mathfrak{b} \subseteq A$ betetzen duen $\mathfrak{b}$ ideal bat emanda, $\mathfrak{b} = (a)$ edo $\mathfrak{b} = A$ dela ikusiko dugu. Kontuan hartzen badugu A ideal nagusietako domeinua dela, $\mathfrak{b} = (b)$ idatz dezakegu, $b \in A$ elementuren batentzat. Orduan, $(a) \subseteq (b)$ partekotasuna dugu eta, hortaz, $a = qb$ dugu, $q \in A$ izanik. Orain, a irreduziblea denez, q eta b elementuetako bat unitatea da. Baldin bada q unitatea, orduan $\mathfrak{b} = (b) = (qb) = (a)$ lortzen dugu. Bestela, b unitatea bada, $\mathfrak{b} = (b) = A$ dugu. □

Bereziki, ideal nagusietako domeinu batean, ideal lehen guztiak lortzeko nahikoa da ideal maximalei $\{0\}$ ideal nulua gehitzea.

Definizioei begiratuta, ez dirudi lotura zuzenik dagoenik ideal nagusietako domeinuen eta faktorizazio bakarreko domeinuen artean. Hala ere, konturatzen gara aurreko teoremaren (ii) atala frogatua genuela dagoeneko faktorizazio bakarreko domeinuen kasuan (ikusi 3.24 proposizioa). Egia esan, gure hurrengo teoremak erakutsiko duenez, ideal nagusietako domeinu guztiak faktorizazio bakarrekoak dira. Emaitza hori frogatzeko, lema pare bat behar ditugu. Lehenengoa 3.17 proposizioaren eta 3.35 teoremaren ondorio berehalakoa da.

3.36. Lema. *Izan bitez A ideal nagusietako domeinua eta $a \in A$ elementu irreduziblea. Orduan, a lehena da.*

Gogoratu aurreko lema faktorizazio bakarreko domeinuetan ere betetzen dela, 3.23 proposizioan ikusi dugun bezala.

3.37. Lema. *Izan bedi A ideal nagusietako domeinua, eta demagun ideal nagusien kate gorakor infinitu bat dugula,*

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots .$$

Orduan kate hori gelditu egiten da, hau da, existitzen da $n_0 \in \mathbb{N}$ non $(a_n) = (a_{n_0})$ baita $n \geq n_0$ guztietarako. Bestela esanda, zatigarritasun baldintzen kate infinitu beherakor bat badugu,

$$\cdots \mid a_n \mid \cdots \mid a_2 \mid a_1,$$

orduan existitzen da $n_0 \in \mathbb{N}$ non $a_n = u_n a_{n_0}$ baita $n \geq n_0$ guztietarako, u_n unitatea izanik.

Froga. Izan bedi $\mathfrak{a} = \cup_{n \geq 1} (a_n)$. Berehala egiaztatzen da $\mathfrak{a}$ A-ren ideala dela. Orain, A ideal nagusietako domeinua denez, existitzen da $a \in A$ non $\mathfrak{a} = (a)$ baita.

Baina, $\mathfrak{a}$-ren definizioaren arabera, $a \in (a_{n_0})$ dugu n_0-ren batentzat. Beraz, $n \geq n_0$ denean,

$$\mathfrak{a} = (a) \subseteq (a_{n_0}) \subseteq (a_n) \subseteq \mathfrak{a}$$

dugu. Ondorioz, aurreko partekotasun guztiak berdintzak dira eta, bereziki, $(a_n) = (a_{n_0})$ dugu $n \geq n_0$ guztietarako. □

3.38. Teorema. *Izan bedi A ideal nagusietako domeinua. Orduan, A faktorizazio bakarreko domeinua da.*

Froga. Ikus dezagun faktorizazio bakarreko domeinuaren definizioko bi baldintzak betetzen direla. Hasteko, frogatu dezagun $a \in A$ edozein elementu, ez bada nulua eta ez bada unitatea, irreduzibleen biderkadura gisa deskonposatzen dela. Jakina, a bera irreduziblea bada, orduan emaitza tribiala da. Bestela, $a = bc$ moduan faktorizatzen da, $b, c \in A$ ez-unitateak (eta ez-nuluak) izanik. Bereziki, $b \mid a$ eta $c \mid a$ dugu. Baldin eta b eta c irreduzibleak badira, berriro bukatu dugu. Ez bada horrela, orduan jarraitu faktorizatzen b eta/edo c. Argudio hori errepikatuz, bi posibilitate ditugu:

(i) Momenturen batean, agertzen diren azpikasu guztietan faktore irreduzibleak baino ez lortzea. Orduan, hasierako a elementua faktore horien biderkadura denez, a irreduzibleen biderkadura gisa adierazita gelditzen da, nahi bezala.

(ii) Zatigarritasun baldintzen kate infinitu bat lortzea, eta $a_{n+1} \mid a_n$ pauso bakoitzean, a_n ez da a_{n+1} bider unitate bat. Baina, 3.37 lemaren arabera, hori ezinezkoa da.

Frogatu dezagun orain faktorizazioen bakartasuna. Demagun $p_1 \dots p_n = q_1 \dots q_m$ dela, p_i eta q_j guztiak irreduzibleak izanik. Orain, 3.36 lemaren arabera, p_1 elementua lehena da. Horrela, $p_1 \mid q_1 \dots q_m$ denez, existitzen da $r \in \{1, \dots, m\}$ non $p_1 \mid q_r$ baita. Baina p_1 eta q_r irreduzibleak direnez, nahitaez $q_r = u_1 p_1$, u_1 unitatea izanik, eta $p_1 \sim q_r$ dugu. Ordezkatzen badugu q_r-ren balioa $p_1 \dots p_n = q_1 \dots q_m$ faktorizazioan eta p_1 sinplifikatzen badugu, orduan $p_2 \dots p_n = u_1 q_1 \dots q_{r-1} q_{r+1} \dots q_m$ berdintza lortzen dugu. Orain, p_2-rekin argudiatzen badugu p_1-ekin egin dugun bezala, badago $s \in \{1, \dots, m\}$, $s \neq r$, non $p_2 \sim q_s$ baita. Horrela jarraituz, azkenean $m = n$ dela lortuko dugu, eta badago $\pi \in S_n$ permutazio bat non $p_i \sim q_{\pi(i)}$ baita $i = 1, \dots, n$ guztietarako. □

Aurreko teoremaren alderantzizkoa ez da egiazkoa: adibidez, $K[X_1, \dots, X_n]$ faktorizazio bakarreko domeinua da beti, baina ez da ideal nagusietako domeinua $n \geq 2$ denean.

Azkenik, ikus dezagun nola egiten diren idealen arteko ohiko eragiketak ideal nagusietako domeinu baten kasuan, ideal horiek sortzaile bakar baten bidez emanda badaude.

3.39. Teorema. *Izan bitez A ideal nagusietako domeinua eta $a, b \in A$. Orduan:*

(i) $(a) + (b) = (\mathrm{zkh}(a, b))$.

(ii) $(a) \cap (b) = (\mathrm{mkt}(a, b))$.

(iii) $(a) \cdot (b) = (ab)$.

FROGA. Badakigu, 3.29 proposizioaren arabera, (ii) faktorizazio bakarreko edozein domeinutan betetzen dela. Bestalde, (iii) askoz ere orokorragoa den emaitza baten kasu berezi bat besterik ez da. Beraz, nahikoa dugu (i) frogatzea.

Izan bedi $c \in A$ non $(a) + (b) = (c)$ baita. Orduan, $a \in (c)$ eta $b \in (c)$ denez, $c \mid a$ eta $c \mid b$ dugu. Ondorioz, $c \mid \text{zkh}(a, b)$ lortzen dugu. (Hemen zatitzaile komunetako handienaren existentzia erabiltzen ari gara, A faktorizazio bakarreko domeinua ere izateagatik betetzen dena: gogoratu 3.26 teorema.) Bestela jarrita, $(\text{zkh}(a, b)) \subseteq (c)$ dugu. Bestalde, $c \in (a) + (b)$ denez, $c = xa + yb$ idatz dezakegu, non $x, y \in A$ baita. Orain, $\text{zkh}(a, b) \mid a$ eta $\text{zkh}(a, b) \mid b$ baldintzetatik $\text{zkh}(a, b) \mid c$ ondorioztatzen dugu. Hortaz, $(c) \subseteq (\text{zkh}(a, b))$ partekotasuna lortzen dugu. Beraz, $(c) = (\text{zkh}(a, b))$ eta (i) atala frogaturik gelditzen da. □

Nahiz eta (ii) eta (iii) berdintzak faktorizazio bakarreko domeinu guztietan bete, (i) ez da oro har egiazkoa. Adibidez, $K[X, Y]$ faktorizazio bakarreko domeinua da, eta $\text{zkh}(X, Y) = 1$ dugu. Beraz, $(X) + (Y) \neq (\text{zkh}(X, Y))$ dugu. Hala ere, aurreko frogak erakusten duenez, A faktorizazio bakarreko domeinua bada *eta* $(a) + (b)$ *ideala nagusia bada*, orduan bai betetzen da $(a) + (b) = (\text{zkh}(a, b))$ berdintza.

3.40. Oharra. Aurreko teoremak idealen arteko eragiketak deskribatzen ditu integritate-domeinu batean, *ideal horiek ideal nagusi modura idatzita badaude*. Beraz, idealen bat sortzaile bat baino gehiagorekin emanda badago, lehenengo pausoak izan behar du ideal hori sortzaile bakar baten bidez adieraztea. Egia esan, horretarako bidea 3.39 teoremak berak ematen digu. Izan ere, $a_1, \ldots, a_n \in A$ badira, orduan

$$(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n) = (\text{zkh}(a_1, \ldots, a_n))$$

dugu, teorema horren (i) atala behin eta berriz erabiliz (kontuan izan (3.4) erlazioa). Orain, emaitza hori aplikatu ahal izateko, inportanteena da zatitzaile komunetako handienak kalkulatzeko modu eraginkor bat izatea lan egiten ari garen eraztunean.

3.41. Korolarioa (Bézouten identitatea)**.** *Izan bitez A ideal nagusietako domeinua eta $a, b \in A$. Orduan, existitzen dira $x, y \in A$ non* $\text{zkh}(a, b) = xa + yb$ *baita.*

Oro har, ez du zentzurik Bézouten identitateari buruz hitz egiteak faktorizazio bakarreko domeinu batean, ez bada ideal nagusietako domeinua. Adibidez, $K[X, Y]$-n $\text{zkh}(X, Y) = 1$ dugu, baina 1 ezin da $f(X, Y)X + g(X, Y)Y$ moduan jarri (ohartu horrelako konbinazio batek ez duela gai askerik).

3.4. Domeinu euklidearrak

Nola frogatu daiteke integritate-domeinu bat ideal nagusietako domeinua dela? Momentuz, bakarrik justifikatu dugu $\mathbb{Z}$ ideal nagusietako domeinua dela. Nola egingo dugu beste kasu batzuetan, adibidez, $K[X]$-ren kasuan, K gorputza izanik?

Atal honetan ikusten dugunez, aukera bat da zatiketak hondarrarekin egiteko posibilitatea egotea eraztun horretan ($\mathbb{Z}$-n eta $K[X]$-n gertatzen den bezala). Ideia hori domeinu euklidearraren kontzeptuan gorpuzten da.

3.42. Definizioa. Izan bedi A integritate-domeinua. Orduan:

(i) $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ funtzio bat, *funtzio euklidearra* dela esaten dugu propietate hau betetzen badu: $a, b \in A$ eta $b \neq 0$ guztietarako, existitzen dira $q, r \in A$ non $a = qb + r$ baita, $r = 0$ izanik edo $r \neq 0$ eta $\varphi(r) < \varphi(b)$ izanik.

(ii) A *domeinu euklidearra* dela esaten dugu funtzio euklidear bat definitu ahal bada $A \setminus \{0\}$-ren gainean.

Batzuetan, A domeinu euklidearra dela frogatzeko erabiliko dugun φ funtzioa A osoaren gainean definiturik egongo da. Kasu horietan, $a, b \in A$, $b \neq 0$ emanda, aurkitzen baditugu q eta r non $a = qb + r$ eta $\varphi(r) < \varphi(b)$ baita ($r = 0$ eta $r \neq 0$ den kasuak bereizi gabe), frogaturik gelditzuko da φ funtzio euklidearra dela.

3.43. Teorema. *Izan bedi A domeinu euklidearra. Orduan, A ideal nagusietako domeinua da.*

Froga. Izan bedi $\mathfrak{a}$ A-ren ideala. Baldin eta $\mathfrak{a} = \{0\}$ bada, orduan tribiala da $\mathfrak{a}$ nagusia dela. Demagun orduan $\mathfrak{a} \neq \{0\}$ dela, eta hartu $a \in \mathfrak{a} \setminus \{0\}$ elementu bat non

$$\varphi(a) = \min\{\varphi(x) \mid x \in \mathfrak{a} \setminus \{0\}\}$$

baita. Ikus dezagun $\mathfrak{a} = (a)$ dela. Nabaria da $(a) \subseteq \mathfrak{a}$ partekotasuna, $a \in \mathfrak{a}$ izateagatik. Alderantzizko partekotasuna frogatzeko, har dezagun $b \in \mathfrak{a}$ eta ikus dezagun $b \in (a)$ dela. Domeinu euklidearraren definizioaren arabera, existitzen dira $q, r \in A$ non $b = qa + r$ baita, $r = 0$ izanik edo $r \neq 0$ eta $\varphi(r) < \varphi(a)$ izanik. Baina, $r = b - qa \in \mathfrak{a}$ denez, bigarren kasua a-ren aukeraketaren kontra joango litzateke. Beraz nahitaez $r = 0$ eta $b = qa \in (a)$, nahi bezala. □

Aurreko teoremaren alderantzizkoa ez da egia: badaude domeinu euklidearrak ez diren ideal nagusietako domeinuak. Hala ere, eman daitezkeen adibide sinpleenek ere lana eskatzen dute frogatzeko. Irakurlearen jakin-mina asetzeko, esan dezagun

$$\mathbb{Z}[(1 + \sqrt{-19})/2] = \left\{ a + b\,\frac{1 + \sqrt{-19}}{2} \mid a, b \in \mathbb{Z} \right\}$$

eraztuna dela horren adibide bat.

3.44. Proposizioa. *$\mathbb{Z}$ domeinu euklidearra da, $\varphi(n) = |n|$ funtzio euklidearrarekin.*

Froga. Ikus dezagun $\varphi(n) = |n|$ funtzio euklidearra dela. Horretarako, aukeratu $a, b \in \mathbb{Z}$, $b \neq 0$. Lehenengo eta behin, demagun $b > 0$ dela. Aukeratu $q \in \mathbb{Z}$ non $qb \leq a < (q + 1)b$ baita, eta jar dezagun $r = a - qb$. Orduan, $a = qb + r$ dugu eta

$$\varphi(r) = |r| = |a - qb| = a - qb < b = |b| = \varphi(b),$$

nahi bezala. Bestalde, $b < 0$ bada, orduan $-b > 0$ dugu eta, aurreko kasua aplikatuz, existitzen dira $q, r \in \mathbb{Z}$ non $a = q(-b) + r$ eta $\varphi(r) < \varphi(-b)$ baita. Orduan, $a = (-q)b + r$ eta $\varphi(r) < \varphi(-b)$ dugu, $|-b| = |b|$ da eta. Horrenbestez, froga biribildurik dago. □

Domeinu euklidearraren definizioan ez da esaten q eta r elementuak bakarrak izan behar dutenik. Adibidez, aztertu berri dugun $\mathbb{Z}$-ren kasuan, $10 = 3 \cdot 3 + 1$ eta $10 = 3 \cdot 4 - 2$ bi deskonposizioek definizioko baldintza betetzen dute, $\varphi(n) = |n|$ funtzio euklidearrarekin. Beste kontu bat da prozedura edo algoritmo bat egotea q eta r elementu egokiak lortzeko. (Hori da aurreko frogan egin duguna.) Hala bada, *algoritmoa aplikatzean* beti ematen direnez pauso berberak, orduan hasierako a eta b balioak behin aukeratuta, q eta r bakarrak lortuko ditugu.

3.45. Proposizioa. *Izan bedi K gorputza. Orduan, $K[X]$ domeinu euklidearra da $\varphi(f) = \deg f$ funtzio euklidearrarekin.*

Froga. Izan bitez $f, g \in K[X]$, $g \neq 0$, eta ikus dezagun nola lortu q eta r polinomioak funtzio euklidearraren baldintza betetzeko. Ohartu oraingo φ funtzioa, balioak $\mathbb{N} \cup \{0\}$ multzoan hartu behar dituenez, bakarrik dagoela definituta $K[X] \setminus \{0\}$ multzoan, eta ez $K[X]$ osoan.

Froga deg f-ren gaineko indukzioaz egingo dugu. Indukzio hori berezi samarra da, ez delako zehatz-mehatz $\mathbb{N}$-ren edo $\mathbb{N} \cup \{0\}$-ren gaineko indukzio bat. Izan ere, polinomio baten maila $-\infty$ ere izan daiteke, eta orduan indukzioa beste multzo ordenatu honen gainean aplikatuko dugu:

$$-\infty < 0 < 1 < 2 < \cdots < n < \cdots .$$

Edozein kasutan, froga arretaz aztertzen bada, ikusiko da indukzioak arazorik gabe funtzionatzen duela. Indukzioaren oinarria $\deg f = -\infty$ kasua da, hau da, $f = 0$ den kasua. Orduan, nahikoa dugu $q = r = 0$ hartzea. Demagun orain $f \neq 0$ dela. Baldin eta $\deg g > \deg f$ bada, orduan $q = 0$ eta $r = f$ har ditzakegu. Bestalde, $\deg g \leq \deg f$ bada, idatz dezagun $f(X) = a_n X^n + \cdots + a_0$ eta $g(X) = b_m X^m + \cdots + b_0$, a_n eta b_m ez-nuluak izanik. Orduan, $\deg(f(X) - a_n b_m^{-1} X^{n-m} g(X)) < \deg f$ dugu eta, indukzio-hipotesia aplikatuz, existitzen dira $q', r \in K[X]$ non

$$f(X) - a_n b_m^{-1} X^{n-m} g(X) = q'(X) g(X) + r(X),$$

$r = 0$ izanik edo $r \neq 0$ eta $\deg r < \deg g$ izanik. Orduan, $q(X) = q'(X) + a_n b_m^{-1} X^{n-m}$ hartzen badugu, $f = qg + r$ betetzen da eta proposizioa frogaturik dago. □

Frogan ezkutuan gelditu badaiteke ere, arretaz aztertzen badugu azken momentuan eman dugun argudioa, konturatuko gara hori dela polinomioak zatitzean egiten den gauza bera: $a_n b_m^{-1} X^{n-m}$ monomioa zatiduran jartzen dugu, $g(X)$ zatitzaileaz biderkatzen dugu, emaitza $f(X)$ zatikizunari kentzen diogu, eta jarraitzen dugu zatitzen. Prozedura hori da "zatiketaren algoritmoaren" izenaz ezagutzen dena.

Zatiketaren algoritmoak, berez, $K[X]$-n funtzionatzen du, K *gorputza izanik*. Ohartu goian emandako prozeduran K gorputza izatea funtsezkoa dela, $b_m \neq 0$ elementuaren alderantzizkoa, b_m^{-1}, erabili behar dugu eta. Beraz, A eraztuna ez bada gorputza, ezin dugu ziurtatu $f, g \in A[X]$ bi polinomioren arteko zatiketa $A[X]$-n bertan burutu daitekeenik. Hala ere, batzuetan zatiketaren algoritmoak bai funtzionatuko du $A[X]$-ren barruan: hori izango da kasua f g-rekin zatitu nahi badugu eta g*-ren koefiziente nagusia* A*-ren unitatea bada*. Bereziki, $f \in A[X]$ edozein polinomio beti zatitu daiteke $X - a$ moduko polinomio batez. Baina, adibidez, $\mathbb{Z}[X]$-n ezin da $X^3 + 1$ $2X + 1$-ez zatitu, 2-a ez baita 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, $K[X, Y]$ eraztuna $K[Y][X]$ moduan ikusten badugu, X-ri rol nagusia emanez, ezin da $X^3 + Y^3$ polinomioa $YX^2 + Y^2$-z zatitu, Y ez baita unitatea $K[Y]$-n. Bai egin daiteke zatiketa, ordea, $K(Y)[X]$ eraztunean, $K(Y)$-n Y unitatea baita. Ohartu, baita ere, badagoela $X^3 + Y^3$ polinomioa $YX^2 + Y^2$-z zatitzea $K[X, Y] = K[X][Y]$ ikusiz gero, kasu horretan koefiziente nagusia 1 delako. Bosgarren gaian $K[X_1, \ldots, X_n]$ eraztunean (K gorputza eta $n \geq 2$ izanik) zatiketak egiteko beste aukera batzuk aztertuko ditugu eta *zatiketaren algoritmo orokortua* deitutakoa garatuko dugu.

3.46. Korolarioa. $\mathbb{Z}$ *eta* $K[X]$ *(K gorputza bada) ideal nagusietako domeinuak dira.*

Bukatzeko, eman dezagun benetan berria den adibide bat.

3.47. Proposizioa. $\mathbb{Z}[i]$*, zenbaki oso gaussiarren eraztuna, domeinu euklidearra da,*

$$\varphi(a + bi) = |a + bi| = a^2 + b^2$$

funtzio euklidearrarekin. Bereziki, $\mathbb{Z}[i]$ *ideal nagusietako domeinua da.*

Froga. Izan bitez $a + bi, c + di \in \mathbb{Z}[i]$, $c + di \neq 0$ izanik. Orduan,

$$\frac{a + bi}{c + di} = e + fi$$

jar dezakegu, $e, f \in \mathbb{Q}$ izanik, $\mathbb{Q}(i) = \{x + yi \mid x, y \in \mathbb{Q}\}$ gorputza da eta. Izan bitez u eta v e-tik eta f-tik gertuen dauden zenbaki osoak, hurrenez hurren. Orduan, $|e - u| \leq 1/2$ eta $|f - v| \leq 1/2$ dugu. Ondorioz,

$$\frac{|(a + bi) - (u + vi)(c + di)|^2}{|c + di|^2} = |(e + fi) - (u + vi)|^2 = (e - u)^2 + (f - v)^2 \leq \frac{1}{2}.$$

Beraz, $q = u + vi$ eta $r = (a + bi) - q(c + di)$ jartzen badugu, orduan $a + bi = q(c + di) + r$ eta $\varphi(r) \leq \frac{1}{2}\varphi(c + di) < \varphi(c + di)$ dugu. Beraz, φ funtzio euklidearra da. □

3.5. Hilberten oinarriaren teorema

Aurreko atalean $K[X]$ domeinu euklidearra dela ikusi dugu, K gorputza bada. Ondorioz, $K[X]$ ideal nagusietako domeinua da, eta bere ideal guztiak sortzaile bakar baten bidez sor daitezke. Emaitza hori ez da hedatzen indeterminatu bat baino gehiagoren kasura; izan ere, aurretik ikusi dugu (X, Y) ideala ez dela nagusia $K[X, Y]$-n. Hala ere, David Hilbert matematikari aleman ospetsuak ondorengo teorema frogatu zuen 1890ean.

3.48. Teorema (Hilberten oinarriaren teorema)**.** *Izan bedi K gorputza. Orduan, $K[X_1, \dots, X_n]$-ren ideal guztiak finituki sortuak dira.*

Ohartu teoremaren izeneko "oinarriak" sistema sortzailea esan nahi duela benetan. Terminologia zaharkitua da hori.

Nahiz eta $K[X]$-ren idealak elementu bakar baten bidez sor daitezkeen, ez da egia $K[X_1, \dots, X_n]$-ren ideal guztiak n elementuren bidez sor daitezkeenik, $n \geq 2$ bada. Are gehiago, ezin da Hilberten oinarriaren bertsio kuantitatibo bat eman, hau da, ezin da bornatu n-ren funtzioan $K[X_1, \dots, X_n]$-ren idealak sortzeko behar diren elementuen kopurua. Izan ere, aurrerago 5.5 probleman ikusiko dugun bezala, $r \in \mathbb{N}$ guztietarako badaude r sortzaile behar dituzten idealak $K[X, Y]$ eraztunaren barruan. Antzeko adibideak eman daitezke $K[X_1, \dots, X_n]$ eraztunetan, $n \geq 2$ guztietarako.

Hilberten oinarriaren teoremaren froga emateko, komenigarria da ideal guztiak finituki sortuak izateko baldintza beste modu batean interpretatzea.

3.49. Lema. *Izan bedi A eraztuna. Orduan, baliokideak dira:*

(i) *A-ren ideal guztiak finituki sortuak dira.*

(ii) *A-ren idealen kate gorakor guztiak gelditzen dira, hau da,*

$$\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots$$

A-ren idealak badira, orduan existitzen da $n_0 \in \mathbb{N}$ non $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ baita $n \geq n_0$ guztietarako.

Froga. (i) $\Rightarrow$ (ii). Izan bedi $\mathfrak{a} = \cup_{n\in\mathbb{N}} \mathfrak{a}_n$, kateko ideal guztien bildura. Erraz egiaztatzen da $\mathfrak{a}$ ere A-ren ideala dela. Hipotesiaren arabera, $\mathfrak{a} = (x_1, \dots, x_k)$ finituki sortua da. Orain, $i \in \{1, \dots, k\}$ bakoitzeko existitzen da $n_i \in \mathbb{N}$ non $x_i \in \mathfrak{a}_{n_i}$ baita. Jarri $n_0 = \max\{n_1, \dots, n_k\}$. Orduan, $x_1, \dots, x_k \in \mathfrak{a}_{n_0}$ dugu eta, hortaz, $n \geq n_0$ guztietarako

$$\mathfrak{a}_{n_0} \subseteq \mathfrak{a}_n \subseteq \mathfrak{a} = (x_1, \dots, x_k) \subseteq \mathfrak{a}_{n_0}$$

da. Horrenbestez, $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ dugu $n \geq n_0$ guztietarako.

(ii) $\Rightarrow$ (i). Absurdora eramanez, demagun $\mathfrak{a}$ A-ren ideala dela, eta ez dela finituki sortua. Orduan, A-ren idealen $\{\mathfrak{a}_n\}_{n\in\mathbb{N}}$ kate hertsiki gorakor infinitu bat

lortuko dugu, hipotesiaren kontra doana. Kate hori induktiboki eraikitzen dugu: izan bedi $\mathfrak{a}_1 = (a_1)$, $a_1 \in \mathfrak{a}$ edozein elementu izanik, eta $\mathfrak{a}_n = (a_1, \dots, a_n)$ definituta badago, har dezagun $a_{n+1} \in \mathfrak{a} \setminus \mathfrak{a}_n$ (existitu behar du horrelako elementu batek, $\mathfrak{a}$ ez baita finituki sortua) eta jarri $\mathfrak{a}_{n+1} = (a_1, \dots, a_n, a_{n+1})$. Orduan, garbi dago $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$ dela n guztietarako, nahi genuen bezala. □

Ohartu 3.37 leman aurreko lemaren (i) ⇒ (ii) inplikazioaren kasu berezi bat frogatu genuela, A ideal nagusietako domeinua denean. Are gehiago, kasu horretako froga eta 3.49 lemarena konparatzen badira, ikusiko da ideia bera erabiltzen dela bietan.

3.50. Definizioa. Izan bedi A eraztuna. Orduan, A *eraztun noetherdarra* dela esango dugu A-ren ideal guztiak finituki sortuak badira (edo, baliokidea dena, A-ren idealen kate gorakor guztiak gelditzen badira).

Aurreko definizioko terminoa Emmy Noether matematikariaren izenetik hartuta dago.

3.51. Teorema. *Izan bedi A eraztun noetherdarra. Orduan, $A[X]$ ere noetherdarra da.*

Froga. Har dezagun $\mathfrak{A}$ $A[X]$-ren ideala, eta ikus dezagun finituki sortua dela. Jakina, nahikoa da $\mathfrak{A} \neq \{0\}$ den kasua aztertzea. Orduan, $n \in \mathbb{N} \cup \{0\}$ guztietarako, $\mathfrak{a}_n$ A-ren azpimultzo bat definitzen dugu. Horretan, $\mathfrak{A}$-ren barruko n-garren mailako polinomio guztien koefiziente nagusiak sartzen ditugu, 0 elementu nuluarekin batera. Erraz egiaztatzen da $\mathfrak{a}_n$ A-ren ideala dela. Gainera, $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ partekotasuna dugu n guztietarako. Izan ere, $f(X) \in \mathfrak{A}$ n-garren mailako polinomioa bada, orduan $Xf(X) \in \mathfrak{A}$ $(n+1)$-garren mailakoa da eta koefiziente nagusi bera du. Horrela, A-ren idealen kate gorakor bat dugu eta, A eraztun noetherdarra denez, existitzen da $n_0 \in \mathbb{N}$ non $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ baita $n \geq n_0$ guztietarako.

Bestalde, berriro ere A noetherdarra izateagatik, $i = 0, \dots, n_0$ guztietarako existitzen da $S_i \subseteq A \setminus \{0\}$ finitua non $\mathfrak{a}_i = (S_i)$ baita. (Ohartu $S_i = \varnothing$ hartzen dugula $\mathfrak{a}_i = \{0\}$ bada.) Orain, S_i-ko elementu bakoitzeko, har dezagun koefiziente nagusi hori duen i-garren mailako polinomio bat $\mathfrak{A}$-n, eta dei diezaiogun T_i polinomio horien multzoari. Ohartu $|T_i| = |S_i| < \infty$ dela. Azkenik, jar dezagun $T = \cup_{i=0}^{n_0} T_i$, multzo finitua dena.

Frogatu dezagun T $\mathfrak{A}$-ren sistema sortzailea dela. Horretarako, har dezagun $f \in \mathfrak{A}$ eta ikus dezagun $f \in (T)$ dela, deg f-ren gaineko indukzioa erabiliz. Hemen, 3.45 proposizioaren frogan bezala, indukzioaren oinarria deg $f = -\infty$ den kasua da, hau da, $f = 0$ polinomioa. Demagun orain f-ren maila $n \geq 0$ dela, eta izan bedi a_n f-ren koefiziente nagusia. Orduan, $a_n \in \mathfrak{a}_n$ dugu. Orain, bi kasu bereizten ditugu:

(i) $n \leq n_0$. Kasu honetan, $a_n \in (S_n)$ dugu, eta $a_n = q_1 s_1 + \cdots + q_m s_m$ idatz dezakegu, $q_i \in A$ eta $s_i \in S_n$ izanik. Aukeratu, $i = 1, \dots, m$ bakoitzeko, s_i koefiziente nagusia duen $f_i \in T_n$ polinomio bat. Orduan, $q_1 f_1 + \cdots + q_m f_m \in (T)$ polinomioa n-garren mailakoa da eta a_n koefiziente nagusia

du. Horrela, $g = f - (q_1 f_1 + \cdots + q_m f_m) \in \mathfrak{A}$ polinomioaren maila n baino txikiagoa da eta, indukzio hipotesiaren arabera, $g \in (T)$ dugu. Beraz, $f = g + q_1 f_1 + \cdots + q_m f_m \in (T)$, nahi bezala.

(ii) $n > n_0$. Kasu honetan, $\mathfrak{a}_n = \mathfrak{a}_{n_0} = (S_{n_0})$ dugu. Aurreko kasuan bezala, existitzen da n_0 mailako $q_1 f_1 + \cdots + q_m f_m \in (T)$ polinomio bat, f-ren koefiziente nagusi bera duena. Orduan, $f - X^{n-n_0}(q_1 f_1 + \cdots + q_m f_m) \in \mathfrak{A}$ polinomioaren maila n baino txikiagoa da, eta goian bezala $f \in (T)$ ondorioztatzen dugu.

□

Azken teorema behin eta berriz aplikatuz, emaitza orokorrago hau lortzen dugu.

3.52. Teorema (Hilberten oinarriaren teorema: bertsio orokortua)**.** *Izan bedi A eraztun noetherdarra. Orduan, $A[X_1, \ldots, X_n]$ ere noetherdarra da.*

3.53. Korolarioa. *$\mathbb{Z}[X_1, \ldots, X_n]$-ren ideal guztiak finituki sortuak dira.*