5

Gröbnerren oinarriak

5.1. Ordena monomialak

Indeterminatu bakar bateko polinomioak erabiltzen ditugunean, era natural batean ordenatzen ditugu: monomioen mailaren arabera. Adibidez, $f(X) = X^5 + 2X^3 + X^2 - 1$ idatzi ohi dugu, eta ez $f(X) = X^2 + 2X^3 - 1 + X^5$. Monomioak horrela ordenatzea funtsezkoa da zatiketaren algoritmoa aplikatzen dugunean. Indeterminatu batekin baino gehiagorekin aritu nahi badugu, ordea, ez dago hain garbi zein prozedura jarraitu behar genuke monomioak ordenatzeko. Hori izango da hurrengo definizioaren helburua. Aurretik, notazio apur bat finkatuko dugu.

Hemendik aurrera, $X_1, \ldots, X_n$ indeterminatuekin eratu daitezkeen monomio guztien multzoa adierazteko $\mathrm{Mon}(X_1, \ldots, X_n)$ ikurra erabiliko dugu. Hau da,

$$\mathrm{Mon}(X_1, \ldots, X_n) = \{X_1^{\alpha_1} \ldots X_n^{\alpha_n} \mid \alpha_i \in \mathbb{N} \cup \{0\},\ i = 1, \ldots, n \text{ guztietarako}\}.$$

Bereziki, 1 polinomio konstantea monomio modura ikusten ari gara, $\alpha_1 = \cdots = \alpha_n = 0$ aukeratuz. Bestetik, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ zenbaki oso ez-negatiboen tupla bat bada, $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ monomioa laburkiago idazteko, $\boldsymbol{X^\alpha}$ ikurra erabiliko dugu. Ohartu notazio horrekin $\boldsymbol{X^\alpha X^\beta} = \boldsymbol{X^{\alpha+\beta}}$ dugula.

5.1. Definizioa. Izan bedi $>$ $\mathrm{Mon}(X_1, \ldots, X_n)$ multzoaren gainean definituriko ordena-erlazio bat. Orduan, $>$ ordena monomiala dela esaten dugu, hiru baldintza hauek betetzen badira:

(OM1) Ordena osoa da: $\boldsymbol{X^\alpha}$ eta $\boldsymbol{X^\beta}$ bi edozein monomio desberdin izanik, $\boldsymbol{X^\alpha} > \boldsymbol{X^\beta}$ edo $\boldsymbol{X^\beta} > \boldsymbol{X^\alpha}$ dugu.

(OM2) Ordena ez da aldatzen monomio batez biderkatzean: $\boldsymbol{X^\alpha} > \boldsymbol{X^\beta}$ betetzen bada, eta $\boldsymbol{X^\gamma}$ beste monomio bat bada, orduan $\boldsymbol{X^\alpha X^\gamma} > \boldsymbol{X^\beta X^\gamma}$ dugu.

(OM3) Ordena ona da: monomioen edozein azpimultzo ez-hutsek elementu minimo bat du.

Nabaria da, $>$ ordena-erlazioa iragankorra izateagatik, (OM2)-ren bertsio orokorrago hau betetzen dela: $\boldsymbol{X^\alpha} > \boldsymbol{X^\beta}$ eta $\boldsymbol{X^\gamma} > \boldsymbol{X^\delta}$ bada, orduan $\boldsymbol{X^\alpha X^\gamma} > \boldsymbol{X^\beta X^\delta}$ dugu.

Adibidez, X indeterminatu bakar batekin lan egiten ari bagara, orduan X^α monomioak α mailaren arabera ordenatzea ordena monomiala da.

5.2. Notazioa. Multzo batean $>$ ordena-erlazio bat badugu, orduan:

(i) $a < b$ idatziko dugu, $b > a$ dela beste modu batean adierazteko.
(ii) $a \geq b$ idatziko dugu, $a > b$ edo $a = b$ dela adierazteko.
(iii) $a \leq b$ idatziko dugu, $a < b$ edo $a = b$ dela adierazteko.

5.3. Lema. *Izan bedi $>$ ordena monomiala. Orduan:*

(i) $\boldsymbol{X^\alpha \geq 1}$ *dugu,* $\boldsymbol{X^\alpha}$ *monomio guztietarako.*
(ii) *Baldin eta $\alpha_i \geq \beta_i$ bada, $i = 1, \ldots, n$ guztietarako, orduan $\boldsymbol{X^\alpha \geq X^\beta}$ dugu.*

Froga. (i) Ordena monomialaren (OM3) propietateagatik, $\mathrm{Mon}(X_1, \ldots, X_n)$ multzoak $\boldsymbol{X^\beta}$ elementu minimo bat du. Garbi dago nahikoa dela $\boldsymbol{X^\beta \geq 1}$ frogatzea. Absurdora eramanez, demagun ez dela $\boldsymbol{X^\beta \geq 1}$ betetzen. Horrek esan nahi du, (OM1) kontuan hartuz, $\boldsymbol{X^\beta < 1}$ dela. Orduan, desberdintza hori $\boldsymbol{X^\beta}$ monomioaz biderkatuz, eta (OM2) propietatea erabiliz, $\boldsymbol{X^{2\beta} < X^\beta}$ lortzen dugu. Hori kontraesan bat da, $\boldsymbol{X^\beta}$ monomiorik txikiena da eta.

(ii) Jarri $\gamma_i = \alpha_i - \beta_i \geq 0$, i guztietarako. Aurreko atalaren arabera, $\boldsymbol{X^\gamma \geq 1}$ dugu. Desberdintza hori $\boldsymbol{X^\beta}$ monomioaz biderkatuz, $\boldsymbol{X^\alpha \geq X^\beta}$ ondorioztatzen dugu. □

Ohartu (ii) frogatzeko bakarrik erabili ditugula (OM2) propietatea eta monomio guztietarako $\boldsymbol{X^\alpha \geq 1}$ betetzen dela.

5.4. Proposizioa. *Indeterminatu bakarra badugu, orduan ordena monomial bakarra dago, mailaren araberakoa, alegia. Hau da, $\alpha, \beta \in \mathbb{N} \cup \{0\}$ badugu, orduan $X^\alpha > X^\beta$ dugu baldin eta soilik baldin $\alpha > \beta$ bada.*

Froga. Izan bedi $>$ ordena monomiala $\mathrm{Mon}(X)$ multzoaren gainean. Aurreko lemaren arabera, $\alpha \geq \beta$ bada, $X^\alpha \geq X^\beta$ dugu. Beraz, $>$ mailaren araberako ordena monomiala da. □

Emandako ordena-erlazio bat ordena monomiala dela frogatzean, zailena (OM3) ziurtatzea izaten da. Ondorengo teorema bereziki erabilgarria da, esaten baitigu nahikoa dela askoz baldintza errazago bat egiaztatzea.

5.5. Teorema. *Ordena monomialaren definizioan, (OM3) baldintza beste honekin ordezka daiteke:*

(OM3)′ $\boldsymbol{X^\alpha \geq 1}$ *betetzen da,* $\boldsymbol{X^\alpha}$ *monomio guztietarako.*

Froga. Alde batetik, 5.3 lemaren arabera, badakigu (OM3)′ betetzen dela ordena monomial bat dugunean. Beraz, nahikoa da ikustea (OM3) propietatea (OM1), (OM2) eta (OM3)′ baldintzen ondorioa dela. Hori indeterminatuen kopuruaren gaineko indukzioa erabiliz frogatuko dugu. Hasi baino lehen, kontuan izan 5.3

lemako (ii) propietatea egiazkoa dela ari garen baldintzetan (ikusi lemaren frogaren osteko oharra). Erreferentziak errazteko asmoz, dei diezaiogun (P) propietate horri froga honetan zehar.

Lehenengo eta behin, demagun X indeterminatu bakarra dugula. Orduan, (P) propietateagatik, $\alpha \geq \beta$ bada $X^\alpha \geq X^\beta$ dugu, eta $>$ erlazioa mailaren araberako ordena monomiala da.

Azter dezagun orain kasu orokorra. Ohartu $>$ erlazioa $\mathrm{Mon}(X_1, \ldots, X_{n-1})$ multzoaren gainean ere definiturik dagoela eta, indukzio-hipotesiagatik, multzo horretan ordena monomiala dela. Ikusteko (OM3) betetzen dela, har dezagun $S \subseteq \mathrm{Mon}(X_1, \ldots, X_n)$ azpimultzo orokor bat. Defini ditzagun

$$\begin{array}{rccc} \varphi: & \mathrm{Mon}(X_1, \ldots, X_n) & \longrightarrow & \mathrm{Mon}(X_1, \ldots, X_{n-1}) \\ & X_1^{\alpha_1} \ldots X_n^{\alpha_n} & \longmapsto & X_1^{\alpha_1} \ldots X_{n-1}^{\alpha_{n-1}} \end{array}$$

eta

$$\begin{array}{rccc} \psi: & \mathrm{Mon}(X_1, \ldots, X_n) & \longrightarrow & \mathrm{Mon}(X_n) \\ & X_1^{\alpha_1} \ldots X_n^{\alpha_n} & \longmapsto & X_n^{\alpha_n} \end{array}$$

aplikazioak. Orduan, $\varphi(S)$ multzoak elementu minimo bat du, $X_1^{\gamma_1} \ldots X_{n-1}^{\gamma_{n-1}}$. Monomio hori S-ko monomio batetik dator; demagun $q = X_1^{\gamma_1} \ldots X_n^{\gamma_n}$ dela monomio hori. Laburtzeagatik, jarri $k = \gamma_n$. Orain, $0 \leq i \leq k-1$ bakoitzeko, izan bedi $S_i = \psi^{-1}(X_n^i) \cap S$. Bestela esanda, X_n-ren berretura X_n^i-ren berdina duten S-ko monomioek osatzen dute S_i multzoa. Izan bedi $p_i \in \mathrm{Mon}(X_1, \ldots, X_{n-1})$ monomioa $\varphi(S_i)$ multzoko minimoa, eta jarri $q_i = p_i X_n^i$. Orduan, $>$ erlazioa ordena osoa denez, $\{q_0, \ldots, q_{k-1}, q\}$ multzo finituak m monomio minimo bat du.

Ikus dezagun m S-ko minimoa dela. Horretarako, hartu edozein monomio $s = X_1^{\alpha_1} \ldots X_n^{\alpha_n} \in S$. Jarri $i = \alpha_n$. Baldin eta $i \leq k-1$ bada, orduan S_i multzoa definiturik dago eta $s \in S_i$ dugu. Orduan, $\varphi(s) \geq p_i$ betetzen da eta, (OM2) propietatea erabiliz, $s = \varphi(s) X_n^i \geq p_i X_n^i = q_i \geq m$ dugu. Demagun orain $i \geq k$ dela. Orduan, (P) propietateagatik, $X_n^i \geq X_n^k$ dugu. Desberdintza hori eta $X_1^{\alpha_1} \ldots X_{n-1}^{\alpha_{n-1}} \geq X_1^{\gamma_1} \ldots X_{n-1}^{\gamma_{n-1}}$ biderkatuz (horretarako (OM2) baino ez dugu behar), $s \geq q \geq m$ lortzen dugu. Laburbilduz, edozein kasutan $s \geq m$ dugu, eta horrek m S-ko monomio minimoa dela frogatzen du. □

Teorema horren arabera, ordena monomialaren definizioa (OM1), (OM2) eta (OM3)′ propietateak eskatuz ere eman ahal genuen. Hala ere, (OM3) propietatea esplizituki eskura izatea oso garrantzitsua da, horrek ziurtatuko baitu ondorengo orrialdeetan garatuko ditugun algoritmoak amaitu egingo direla. Horretarako, proposizio hau behar dugu.

5.6. Proposizioa. *Izan bedi $>$ ordena monomiala. Orduan, ez da existitzen monomioen kate hertsiki beherakor infiniturik.*

Froga. Demagun $\{\boldsymbol{X}^{\boldsymbol{\alpha}_i}\}_{i \geq 1}$ monomioen kate hertsiki beherakor infinitu bat dela. Orduan, ordena monomialaren definizioko (OM3) propietatearen arabera, existitzen da elementu minimo bat kate horretan, demagun $\boldsymbol{X}^{\boldsymbol{\alpha}_m}$ dela. Hori kontraesan bat da, $\boldsymbol{X}^{\boldsymbol{\alpha}_m} > \boldsymbol{X}^{\boldsymbol{\alpha}_{m+1}}$ da eta. □

Orain, ordena monomialen adibide nagusiak emateko moduan gaude.

5.7. Adibideak. 1) *Ordena lexikografikoa* (lex; ingelesez, *lexicographic order*):

$$\boldsymbol{X^{\alpha}} > \boldsymbol{X^{\beta}} \iff \exists i \in \{1,\dots,n\} \text{ non } \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

Bestela esanda, bi monomio konparatzeko, ezkerraldetik hasten gara begiratzen X_i bakoitzaren berretzailea bi monomioetan, eta berretzaile desberdinak lehenengo aldiz topatzen ditugunean, berretzaile handienekoa besteari inposatzen zaio. Esplizituki adierazi nahi dugunean lex ordena erabiltzen ari garela, $>_{\text{lex}}$ idatziko dugu $>$ ikurraren ordez.

2) *Ordena lexikografiko mailakatua* (grlex; ingelesez, *graded lexicographic order*). Kasu honetan, bi monomio konparatzeko honela jokatzen dugu:

(i) Lehenengo, monomioen maila osoari begiratzen diogu: desberdinak badira, maila osorik altuena duena handiagoa da.
(ii) Bi monomioek maila oso bera dutenean, lex ordena erabiltzen dugu monomioak ordenatzeko.

Esplizituki adierazi nahi dugunean grlex ordena erabiltzen ari garela, $>_{\text{grlex}}$ idatziko dugu $>$ ikurraren ordez.

3) *Alderantzizko ordena lexikografiko mailakatua* (grevlex; ingelesez, *graded reverse lexicographic order*). Kasu honetan, bi monomio konparatzeko honela jokatzen dugu:

(i) Lehenengo, monomioen maila osoari begiratzen diogu: desberdinak badira, maila osorik altuena duena handiagoa da.
(ii) Bi monomioek maila oso bera dutenean, honela desegiten dugu berdinketa:

$$\boldsymbol{X^{\alpha}} > \boldsymbol{X^{\beta}} \iff \exists i \in \{1,\dots,n\} \text{ non } \alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i.$$

Bestela esanda, bi monomio konparatzeko, eskuinaldetik hasten gara begiratzen X_i bakoitzaren berretzailea bi monomioetan, eta berretzaile desberdinak lehenengo aldiz topatzen ditugunean, berretzaile txikienekoa besteari inposatzen zaio.

Esplizituki adierazi nahi dugunean grevlex ordena erabiltzen ari garela, $>_{\text{grevlex}}$ idatziko dugu $>$ ikurraren ordez.

Adibide horietan, zein monomio den handiagoa erabakitzeko, eskuinaldetik edo ezkerraldetik irakurtzen ditugu eta, hortaz, garrantzitsua da monomioak $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ moduan idazten ditugula: X_1-en berretura lehenengo, gero X_2-rena, eta horrela jarraituz, azkenik X_n-rena. Bereziki, aurreko ordena monomial guztietarako $X_1 > X_2 > \cdots > X_n$ dugu. Monomioak idazteko orduan indeterminatuak beste modu batean ordenatzen baditugu, hau da, indeterminatuen arteko ordena aldatzen badugu, orduan lex, grlex eta grevlex ordenen beste aldera batzuk lortzen ditugu. Kontuan izanik n indeterminatuak ordenatzeko $n!$ aukera ditugula, beste horrenbeste posibilitate ditugu lex, grlex edo grevlex ordenak definitzeko orduan.

5.8. Adibideak. 1) Hartzen badugu $X > Y > Z$, orduan

$$XZ >_{\text{lex}} Y^2, \quad XZ >_{\text{grlex}} Y^2, \quad Y^2 >_{\text{grevlex}} XZ,$$
$$XZ >_{\text{lex}} Y^3, \quad Y^3 >_{\text{grlex}} XZ, \quad Y^3 >_{\text{grevlex}} XZ.$$

2) Hala ere, $Y > Z > X$ hartuz gero, $Y^2 > XZ$ eta $Y^3 > XZ$ dugu beti, $>$ ordena lex, grlex edo grevlex denean.

Ez da pentsatu behar grevlex, alderantzizko ordena lexikografiko mailakatua, grlex ordena mailakatuarekin bat datorrela, indeterminatuak alderantzizko ordenan (hau da, $X_n > \cdots > X_1$) jarriz gero. Adibidez, $X > Y > Z$ hartuta, $Y^2 >_{\text{grevlex}} XZ$ dugu, eta $Z > Y > X$ hartuta, berriz, $XZ >_{\text{grlex}} Y^2$.

Ordena monomial bat behin ezarrita, polinomio bat osatzen duten monomioak ordena horren arabera idatz ditzakegu eta, horrela, zentzua du polinomio baten gai nagusiari buruz edo antzeko kontzeptuei buruz hitz egiteak.

Hemendik aurrera, gai honetan K gorputza izango da.

5.9. Definizioa. Izan bitez $>$ ordena monomiala eta $f \in K[X_1, \ldots, X_n]$, $f \neq 0$. Orduan:

(i) f-ren adierazpenean koefiziente ez-nulua duten monomio guztietatik handiena f-ren *monomio nagusia* da. (Ingelesez, *leading monomial.*) Hori adierazteko $\text{LM}(f)$ idatziko dugu.

(ii) f-ren monomio nagusiaren koefizientea f-ren *koefiziente nagusia* da eta $\text{LC}(f)$ ikurraren bidez adieraziko dugu. (Ingelesez, *leading coefficient.*)

(iii) f-ren *gai nagusia* bere koefiziente nagusiaren eta bere monomio nagusiaren biderkadura da. (Ingelesez, *leading term.*) Hori adierazteko $\text{LT}(f)$ idatziko dugu.

(iv) f-ren monomio nagusia $\boldsymbol{X}^{\boldsymbol{\alpha}}$ bada, orduan $\boldsymbol{\alpha}$ tuplari f-ren *multimaila* deitzen zaio eta $\text{multideg}(f)$ ikurraren bidez adieraziko dugu. (Ingelesez, *multidegree.*)

Azpimarratu nahi badugu $>$ ordena monomiala erabiltzen ari garela, orduan $\text{LM}_>(f)$, $\text{LC}_>(f)$, $\text{LT}_>(f)$ eta $\text{multideg}_>(f)$ idatziko dugu.

Adibidez, lex ordenarekiko ari bagara, $X > Y > Z$ harturik, orduan $f = Y^4 - 2X^2Z + XYZ - Z^4$ polinomioaren kasuan, $\text{LM}(f) = X^2Z$, $\text{LC}(f) = -2$, $\text{LT}(f) = -2X^2Z$ eta $\text{multideg}(f) = (2, 0, 1)$ dugu.

Ondorengo propietatea nabaria da.

5.10. Teorema. *Izan bitez $f, g \in K[X_1, \ldots, X_n]$ bi polinomio ez-nulu. Orduan, ordena monomial bat finkatzen badugu:*

(i) $\text{LM}(fg) = \text{LM}(f)\text{LM}(g)$, $\text{LC}(fg) = \text{LC}(f)\text{LC}(g)$ *eta* $\text{LT}(fg) = \text{LT}(f)\text{LT}(g)$ *dugu.*

(ii) $\mathrm{LM}(f) > \mathrm{LM}(g)$ *bada, orduan* $\mathrm{LM}(f+g) = \mathrm{LM}(f)$, $\mathrm{LC}(f+g) = \mathrm{LC}(f)$ *eta* $\mathrm{LT}(f+g) = \mathrm{LT}(f)$ *dugu.*

Polinomioen maila osoaren propietateak 1.34 teoreman eman ditugu. Jarraian, multimailak propietate berak dituela ikusten dugu; horien froga aurreko teoremaren ondorio berehalakoa da. Enuntziatua eman baino lehen, azpimarratu nahi dugu ordena monomial bakoitzak zenbaki oso ez-negatiboen tuplen ordena bat dakarrela: nahikoa da $\boldsymbol{\alpha} > \boldsymbol{\beta}$ definitzea baldin eta soilik baldin $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$ bada. Hori da tuplen arteko desberdintzen esanahia hurrengo teoreman.

5.11. Teorema. *Izan bitez* $f, g \in K[X_1, \ldots, X_n]$ *bi polinomio ez-nulu. Orduan, ordena monomial bat finkatzen badugu:*

(i) $f+g \neq 0$ *bada,* $\mathrm{multideg}(f+g) \leq \max\{\mathrm{multideg}(f), \mathrm{multideg}(g)\}$ *dugu eta, gainera,* $\mathrm{multideg}(f)$ *eta* $\mathrm{multideg}(g)$ *desberdinak badira, berdintza dugu.*

(ii) $\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$ *dugu.*

5.2. Zatiketaren algoritmo orokortua

Indeterminatu bakar batekin ari garenean, polinomioak zatitzeko algoritmoa guztiz ezaguna da. Hau da erabiltzen den prozedura:

(ZA1) Zatitu behar ditugun bi polinomioak, zatikizuna eta zatitzailea, mailaren arabera ordenaturik idazten dira.

$$\begin{array}{rcrcrcr|l} X^3 & + & X^2 & + & X & + & 1 & X^2 + 1 \\ \hline \end{array}$$

(ZA2) Zatitzailearen gai nagusiak zatikizunaren gai nagusia zatitzen badu, orduan zatitzailea faktore egoki batez biderkatuz eta lortutako emaitza zatikizunari kenduz, zatikizunaren gai nagusia desagertzea lortzen dugu. Faktore hori zatidurara pasatzen da.

$$\begin{array}{rcrcrcr|l} X^3 & + & X^2 & + & 2X & + & 1 & X^2 + 1 \\ X^3 & & & + & X & & & X \\ \hline & & X^2 & + & X & + & 1 & \end{array}$$

(ZA3) Prozedura hori errepikatzen dugu, harik eta zatikizunaren maila zatitzailearena baino txikiagoa den. (Zatikizunaren maila gero eta txikiagoa denez, garbi dago une hori helduko dela.) Orduan gelditzen den polinomioa zatiketaren hondarra da.

$$\begin{array}{rcrcrcr|l} X^3 & + & X^2 & + & 2X & + & 1 & X^2 + 1 \\ X^3 & & & + & X & & & X + 1 \\ \hline & & X^2 & + & X & + & 1 & \\ & & X^2 & + & & + & 1 & \\ \hline & & & & X & & & \end{array}$$

Hasierako polinomioak f (zatikizuna) eta g (zatitzailea) badira, amaieran lortzen ditugun q zatidurak eta r hondarrak honako erlazio hau betetzen dute: $f = qg + r$ eta $\deg r < \deg g$ dugu.

Indeterminatu batez baino gehiagoz zatitu nahi baditugu polinomioak, ikusi dugu posibilitate bat dela indeterminatuetako bati rol nagusia ematea eta horrekiko egitea zatiketa, gainerako indeterminatuak konstanteak balira bezala. Zoritxarrez, hori bakarrik egin daiteke indeterminatu horren koefiziente nagusia unitate bat denean, hau da, K gorputzeko elementu ez-nulu bat denean. Oztopo hori gainditzeko, pentsa genezake indeterminatu bateko algoritmoa egokitzea indeterminatu anitzekin lan egiteko, baina indeterminatuetako bat bereizi gabe, indeterminatu guztiak indeterminatu gisa hartuz. Azken batean, *ordena monomial bat ezartzen badugu hasieratik*, orduan indeterminatu anitzeko polinomioak ordena horren arabera idatz ditzakegu. Beraz, ez dago problemarik (ZA1) pausoa egiteko. Aurrera jarraituz, (ZA2) ere egin dezakegu behin eta berriz, monomio nagusien arteko zatigarritasuna aztertuz. Hala ere, indeterminatu anitzekin diferentzia bat aurkitzen dugu, hurrengo adibideak erakusten duen bezala. Zatitu dezagun $f = X^2 + Y^2$ polinomioa $g = X + 1$-ez, grlex ordena erabiliz eta $X > Y$ harturik:

$$\begin{array}{rcl|l} X^2 & + & Y^2 & X + 1 \\ \cline{4-4} X^2 & + & + X & X \\ \cline{1-3} & & Y^2 - X & \end{array}$$

Momentu honetan, konturatzen gara zatikizunaren gai nagusia, Y^2, ez dela zatitzailearen gai nagusiaz zatigarria. Beraz, pentsa genezake (ZA3) pausora heldu garela eta zatiketa bukatutzat eman behar dugula. Hala ere, konturatzen gara zatikizunaren beste gai bat, $-X$, badela zatigarria zatitzailearen gai nagusiaz. Ohartu fenomeno hori ezin dela inola ere gertatu indeterminatu bakar baten kasuan. Izan ere, (ZA2) pausoko momenturen batean X^n zatikizunaren monomio nagusia ez bada X^k zatitzailearen gai nagusiaz zatigarria, horrek esan nahi du $n < k$ dela. Orduan, zatikizunaren beste edozein monomio X^m modukoa denez, $m \leq n$ izanik, hori ere ez da izango X^k-z zatigarria.

Hori dela eta, prozedura aldatu behar dugu momentu honetan: Y^2 gai nagusia hondarrera eramaten dugu, baina $-X$ zatikizunean mantentzen dugu. Zatiketa egiteko erabiltzen dugun eskeman, Y^2 kentzen diogu zatikizunari, eta Y^2 hori lauki baten barruan sartzen dugu, jakiteko kendura hori ez datorrela zatiduraren gai

batetik. Hori egin eta gero, zatitzen jarraitzen dugu:

$$\begin{array}{rcrcrcrcr|l}
X^2 & + & Y^2 & & & & & & & X + 1 \\
\cline{10-10}
X^2 & + & & + & X & & & & & X - 1 \\
\cline{1-5}
 & & Y^2 & - & X & & & & & \\
 & & \boxed{Y^2} & & & & & & & \\
\cline{3-5}
 & & & - & X & & & & & \\
 & & & - & X & - & 1 & & & \\
\cline{4-7}
 & & & & & & & 1 & & \\
 & & & & & & & \boxed{1} & & \\
\cline{8-8}
 & & & & & & & 0 & &
\end{array}$$

Hondarra: $Y^2 + 1$

Dakusagunez, -1 batugai berria agertzen zaigu zatiduran, eta orduan zatikizuna 1 besterik ez da. Hori ez da zatitzailearen gai nagusiaz zatigarria eta, beraz, hondarrera doa. Horrenbestez, 0 baino ez da gelditzen zatikizunean eta zatiketa bukatutzat ematen dugu: zatidura $X + 1$ da eta hondarra, berriz, $Y^2 + 1$. Aplikatzen dugun prozedura aztertuz, garbi dago kasu honetan ere betetzen dela "zatikizuna berdin zatidura bider zatitzailea gehi hondarra" erregela, indeterminatu baten kasuan ezagutzen dugun berbera:

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

Hala ere, hondarraren maila osoa zatitzailearen maila baino handiagoa da adibide honetan, indeterminatu bakar batekin ez bezala. Zein da orduan hondarra karakterizatzen duen propietatea? Berriro ere prozedurak berak ematen digu erantzuna: *hondarraren gai bat ere ez da zatitzailearen gai nagusiaz zatigarria* (bestela gai hori ez genuen hondarrera eramango!).

Behin ulertuta hondarra lortzeko modua desberdina dela, erraz eman genitzake indeterminatu anitzeko zatiketaren algoritmoaren pausoak, aurretik (ZA1), (ZA2) eta (ZA3) deskribatu ditugun moduan. Hala ere, nahiago dugu apur batean itxaron hori egiteko, laster askoz ere zatiketa orokorragoak egiteko gai izango gara eta. Horiek ikusitakoan emango dugu zatiketaren algoritmoaren deskribapen formala.

Indeterminatu bakar batekin ari garenean, zatiketaren algoritmoa erabil dezakegu f polinomio bat $\mathfrak{a}$ ideal baten barruan dagoen edo ez jakiteko. Izan ere, $K[X]$ ideal nagusietako domeinua denez, $\mathfrak{a} = (g)$ idatz dezakegu g polinomio baterako. Orduan, $f \in \mathfrak{a}$ dugu baldin eta soilik baldin f g-ren multiploa bada. Hori betetzen den erabakitzeko, f g-rekin zatitzen dugu. Horrela, $f = qg + r$ lortzen dugu, q zatiketaren zatidura eta r hondarra izanik, eta orduan $f \in \mathfrak{a}$ dugu baldin eta soilik baldin $r = 0$ bada. Jarraian ikusten dugunez, propietate hori indeterminatu baten baino gehiagoren kasura hedatzen da.

5.12. Teorema. *Izan bitez $f \in K[X_1, \ldots, X_n]$ eta $\mathfrak{a} = (g)$ $K[X_1, \ldots, X_n]$-ren ideal nagusia. Orduan, $f \in \mathfrak{a}$ dugu baldin eta soilik baldin f g-rekin zatitzeko hondarra 0 bada.*

Froga. Lehenago esan dugun bezala, indeterminatu anitzekin ere $f = qg + r$ dugu, q zatiketaren zatidura eta r hondarra izanik. Horrela, $r = 0$ bada, orduan $f = qg \in \mathfrak{a}$ dugu. Alderantzizko inplikazioa ikusteko, demagun $f \in \mathfrak{a}$ dela eta, absurdora eramanez, $r \neq 0$ dela. Orduan, $r = f - qg \in \mathfrak{a}$ ere badugu eta, hortaz, existitzen da $h \in K[X_1, \ldots, X_n]$, non $r = hg$ baita. Orain, 5.10 teorema erabiliz, $\mathrm{LT}(r) = \mathrm{LT}(h)\mathrm{LT}(g)$ dugu. Beraz, r polinomioaren gai bat (gai nagusia, alegia) g-ren gai nagusiaren multiploa da. Hori ezinezkoa da, zatiketaren hondarraren karakterizazioagatik. Horrela, $r = 0$ izan behar dugu, nahi bezala. □

Zoritxarrez, $K[X_1, \ldots, X_n]$-ren idealak ez dira oro har nagusiak. Nola erabaki dezakegu orduan $f \in \mathfrak{a}$ den, $\mathfrak{a} = (f_1, \ldots, f_s)$ ideala ez bada nagusia? Ideia zatiketaren algoritmoa orokortzea da, polinomio batez baino gehiagoz zatitu ahal izateko, idealaren sortzaileekin alegia. Algoritmo orokortu horrek dagoeneko ikusi dugun prozeduraren pauso berak jarraituko ditu, baina zatikizunaren gai nagusia zatitzailearen gai nagusiaz zatigarria den aztertu behar dugunean, proba bat baino gehiago egin beharko dugu, zatitzaile bat baino gehiago baititugu. Algoritmoaren pausoak deskribatu baino lehen, adibide batekin argituko dugu: zatitu dezagun $f = Y^3 + X^2Y + XY^2 + X$ polinomioa, $f_1 = XY - 1$-ez eta $f_2 = Y^2 - 1$-ez, lex ordena monomiala aukeratuta, $X > Y$ izanik. Lehenengo eta behin, ohartzen gara f polinomioa ez dagoela ondo ordenatuta hartu dugun ordena monomialarekiko. Hori konpontzeko, Y^3 amaieraraino eraman behar dugu eta $f = X^2Y + XY^2 + X + Y^3$ idatzi behar dugu. Orain zatiketa egiten has gaitezke. Konturatzen gara X^2Y, f-ren gai nagusia, f_1-en gai nagusiaz zatigarria dela; hori dela eta, honelakoa da lehen pausoa:

$$\begin{array}{rcrcrcrc|rcr}
X^2Y & + & XY^2 & + & X & + & Y^3 & & XY & + & 1 \\
\cline{10-12}
X^2Y & + & & + & X & & & & X & & \\
\cline{1-7}
 & & XY^2 & & & + & Y^3 & & Y^2 & - & 1 \\
\cline{10-12}
\end{array}$$

Gelditzen zaigun gai nagusi berria XY^2 da, eta hori ere f_1-en gai nagusiaz zatigarria da. Beraz, f_1-ez zatitzen jarraitzen dugu:

$$\begin{array}{rcrcrcrcr|rcr}
X^2Y & + & XY^2 & + & X & + & Y^3 & & & XY & + & 1 \\
\cline{11-13}
X^2Y & + & & + & X & & & & & X & + & Y \\
\cline{1-9}
 & & XY^2 & & & + & Y^3 & & & Y^2 & - & 1 \\
\cline{11-13}
 & & XY^2 & & & & & + & Y & & & \\
\cline{2-9}
 & & & & & & Y^3 & - & Y & & & \\
\end{array}$$

Orain, zatikizunaren gai nagusia Y^3 da, ez dena f_1-en gai nagusiaz zatigarria. Bai zatitzen du, ordea, f_2-ren gai nagusiak. Beraz, hurrengo pausoan f_2 erabiliko dugu:

$$\begin{array}{rcrcrcrcrcr|l}
X^2Y & + & XY^2 & + & X & + & Y^3 & & & & & XY + 1 \\
\cline{12-12}
X^2Y & + & & + & X & & & & & & & X + Y \\
\cline{1-11}
 & & XY^2 & & & + & Y^3 & & & & & Y^2 - 1 \\
\cline{12-12}
 & & XY^2 & & & & & + & Y & & & Y \\
\cline{2-9}
 & & & & & & Y^3 & - & Y & & & \\
 & & & & & & Y^3 & - & Y & & & \\
\cline{6-9}
 & & & & & & & & 0 & & &
\end{array}$$

Horrenbestez, zatiketa bukatuta dago. Kasu honetan hondarra 0 da, baina momenturen batean gertatu izan balitz gai nagusia ez izatea zatigarria ez f_1-en ez f_2-ren gai nagusiaz, orduan gai hori hondarrera eramango genuen. Hondarra 0 denez, deskonposizio hau dugu:

$$X^2Y + XY^2 + X + Y^3 = (X + Y)(XY + 1) + Y(Y^2 - 1).$$

Bereziki, $X^2Y + XY^2 + X + Y^3 \in (XY + 1, Y^2 - 1)$ lortzen dugu.

Ondorengo teoreman, zatiketaren algoritmo orokortua ematen dugu. Algoritmo hori bi zentzutan da "orokortua": alde batetik, indeterminatu baterako baino gehiagorako balio duelako; bestetik, polinomio batez baino gehiagoz zatitzen uzten digulako.

5.13. Teorema (Zatiketaren algoritmo orokortua)**.** *Demagun* $\mathrm{Mon}(X_1, \ldots, X_n)$ *multzoan ordena monomial bat finkaturik dagoela, eta izan bitez* $f \in K[X_1, \ldots, X_n]$*, eta* $F = (f_1, \ldots, f_s)$ $K[X_1, \ldots, X_n]$*-ko polinomio ez-nuluen tupla bat. Orduan,* f *polinomioa* F *tuplaz zatitzeko, ondorengo pausoak jarraitzen ditugu:*

(ZAO1) *Polinomio guztiak, hau da,* f *zatikizuna eta* $f_1, \ldots, f_s$ *zatitzaileak, emandako ordena monomialaren arabera ordenaturik idazten dira.*

(ZAO2) *Zatitzaileen gai nagusiek zatikizunaren gai nagusia zatitzen duten aztertzen dugu,* $F = (f_1, \ldots, f_s)$ *tuplan zatitzaileak agertzen diren ordenari jarraituz: lehenengo* f_1*-ekin saiatzen gara, gero* f_2*-rekin, eta abar. Aurkitzen dugun bezain pronto* f_i *polinomio bat, non* f_i*-ren gai nagusiak zatikizunaren gai nagusia zatitzen baitu, orduan* f_i *faktore egoki batez biderkatuz eta lortutako emaitza zatikizunari kenduz, zatikizunaren gai nagusia desagertzea lortzen dugu. Faktore hori* f_i*-ri dagokion zatidurari gehitzen zaio.*

(ZAO3) *Ez badugu* $F = (f_1, \ldots, f_s)$ *tuplan horrelako polinomiorik aurkitzen, orduan zatikizunaren gai nagusia hondarrera eramaten dugu eta zatikizunari bere gai nagusia kentzen diogu.*

(ZAO4) *Prozedura hori errepikatzen dugu, harik eta zatikizuna* 0 *bihurtu arte.*

Algoritmoa bukatzen denean, f_i *bakoitzaren zatidurari* q_i *deitzen badiogu eta hondarrari* r *deitzen badiogu, orduan* f*-ren deskonposizio hau lortzen dugu:*

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Gainera:

(i) *r hondarrak propietate hau betetzen du: r osatzen duten gaietatik, bat ere ez da* $\mathrm{LT}(f_i)$ *gai nagusietako batez zatigarria, $i = 1, \ldots, s$ denean. Batzuetan,* $\overline{f}^F$ *idatziko dugu hondar hori adierazteko.*

(ii) *Baldin eta $q_i f_i \neq 0$ bada (hau da, $q_i \neq 0$ bada), orduan* $\mathrm{multideg}\, f \geq \mathrm{multideg}(q_i f_i)$ *dugu.*

Froga. Hiru gauza baino ez dira frogatu behar: $f = q_1 f_1 + \cdots + q_s f_s + r$ deskonposizioa dugula, (i) eta (ii) propietateak betetzen direla, eta *algoritmoa bukatu egingo dela*, hau da, momenturen batean zatikizuna 0 bihurtuko dela.

Lehenengo eta behin, $f^{(j)}$, $q_i^{(j)}$ $(i = 1, \ldots, s)$, eta $r^{(j)}$ polinomioen segida bat definituko dugu, halako moduan non

$$f = f^{(j)} + q_1^{(j)} f_1 + \cdots + q_s^{(j)} f_s + r^{(j)} \tag{5.1}$$

baita j guztietarako. Polinomio horien esanahia hau da: zatiketaren j. iterazioan, $f^{(j)}$ momentu horretako zatikizuna izango da; $q_i^{(j)}$, f_i-ri dagokion zatidura; eta $r^{(j)}$, berriz, orduko hondarra.

Hasteko, jarri $f^{(0)} = f$, $q_i^{(0)} = 0$ eta $r^{(0)} = 0$. Orduan, nabaria da (5.1) betetzen dela. Orain, (ZAO2) edo (ZAO3) pausoetako bat aplikatzen dugunean, $f^{(j)}$, $q_i^{(j)}$ eta $r^{(j)}$ polinomioetatik abiatuz, $f^{(j+1)}$, $q_i^{(j+1)}$ eta $r^{(j+1)}$ polinomio berriak definitzen ditugu, honako modu honetan:

(a) (ZAO2) pausoa aplikatu badugu, eta f_k bada $\mathrm{LT}(f_k) \mid \mathrm{LT}(f^{(j)})$ betetzen duen F tuplako lehenengo polinomioa, orduan

$$f^{(j+1)} = f^{(j)} - \frac{\mathrm{LT}(f^{(j)})}{\mathrm{LT}(f_k)} f_k, \quad q_k^{(j+1)} = q_k^{(j)} + \frac{\mathrm{LT}(f^{(j)})}{\mathrm{LT}(f_k)},$$

$$q_i^{(j+1)} = q_i^{(j)},\ i \neq k \text{ bada}, \quad r^{(j+1)} = r^{(j)}$$

jartzen dugu.

(b) (ZAO3) pausoa aplikatu badugu, orduan

$$f^{(j+1)} = f^{(j)} - \mathrm{LT}(f^{(j)}), \quad q_i^{(j+1)} = q_i^{(j)},\ i \text{ guztietarako},$$

$$r^{(j+1)} = r^{(j)} + \mathrm{LT}(f^{(j)})$$

jartzen dugu.

Orduan, j-ren gaineko indukzioaren bidez, garbi dago $f^{(j+1)}$, $q_i^{(j+1)}$ eta $r^{(j+1)}$ polinomioek (5.1) betetzen dutela: azken batean, leku batean kentzen duguna, beste leku batean batuz orekatzen dugu. Gainera, bi kasuetan $f^{(j+1)} = f^{(j)} - h^{(j)}$ dugu, $\mathrm{LT}(h^{(j)}) = \mathrm{LT}(f^{(j)})$ izanik. Beraz, $\{\mathrm{LT}(f^{(j)})\}$ monomioen segida hertsiki beherakorra da. Orain, 5.6 proposizioaren arabera, hori bakarrik gerta daiteke segida hori finitua bada. Horrek frogatzen du algoritmoa pauso kopuru finitu batean bukatuko dela. Beste alde batetik, algoritmoa bukatzeko modu bakarra da $f^{(m)} = 0$ izatea m-ren baterako. Orduan, (5.1) aplikatuz,

$$f = q_1^{(m)} f_1 + \cdots + q_s^{(m)} f_s + r^{(m)}$$

lortzen dugu, eta enuntziatuko deskonposizioa frogaturik gelditzen da, $q_i = q_i^{(m)}$ eta $r = r^{(m)}$ jarriz.

Beste alde batetik, hondarrera eramaten diren gai guztiak ez direnez $\mathrm{LT}(f_i)$ gai nagusiez zatigarriak, garbi dago enuntziatuko (i) propietatea betetzen dela.

Azkenik, ikus dezagun enuntziatuko (ii) propietatea ere betetzen dela. Hori ere j-ren gaineko indukzioa erabiliz frogatuko dugu, kontuan hartuz $q_i = q_i^{(m)}$ dela $i = 1, \ldots, s$ guztietarako. Beraz, $\mathrm{multideg}(q_i^{(j)} f_i) \leq \mathrm{multideg}\, f$ egiatzat hartuta, $\mathrm{multideg}(q_i^{(j+1)} f_i) \leq \mathrm{multideg}\, f$ dela ikusi behar dugu. Argi eta garbi, bakarrik kezkatu behar dugu (a) kasuaz, eta $i = k$ den kasuaz. Orduan,

$$q_k^{(j+1)} f_k = q_k^{(j)} f_k + \frac{\mathrm{LT}(f^{(j)})}{\mathrm{LT}(f_k)} f_k$$

dugu. Orain,

$$\mathrm{multideg}(q_k^{(j)} f_k) \leq \mathrm{multideg}\, f$$

eta

$$\begin{aligned} \mathrm{multideg}\left(\frac{\mathrm{LT}(f^{(j)})}{\mathrm{LT}(f_k)} f_k\right) &= \mathrm{multideg}\left(\frac{\mathrm{LT}(f^{(j)})}{\mathrm{LT}(f_k)}\right) + \mathrm{multideg}\, f_k \\ &= \mathrm{multideg}(\mathrm{LT}(f^{(j)})) - \mathrm{multideg}(\mathrm{LT}(f_k)) + \mathrm{multideg}\, f_k \\ &= \mathrm{multideg}(\mathrm{LT}(f^{(j)})) = \mathrm{multideg}\, f^{(j)} \leq \mathrm{multideg}\, f \end{aligned}$$

denez, emaitza bete egiten da. □

Algoritmo bat aplikatzen dugunean, oso zorrotz jokatu behar dugu, eta algoritmoak agintzen dituen pausoak dauden bezala jarraitu behar ditugu. Bereziki, ezin dugu pausoen ordena aldatu. Zatiketaren algoritmo orokortuaren kasuan, azpimarratzekoa da nola aztertzen dugun zatikizunaren gai nagusia zatitzaileen gai nagusiez zatigarria den (ZAO2) pausoan: lehenengo, f_1-ekin saiatzen gara; horrekin ez bada betetzen, f_2-rekin saiatzen gara eta, horrela jarraituz, beharrezkoa bada, f_s-raino iritsi arte. Beraz, garrantzitsua da zein ordenatan hartu ditugun $f_1, \ldots, f_s$ polinomioak $F = (f_1, \ldots, f_s)$ tuplan zatiketa egiteko orduan. Ikus dezagun, esate baterako, zer gertatzen den aurreko adibidean f_1 eta f_2-ren ordena aldatzen badugu. Hasteko, X^2Y ez da Y^2-rekin zatigarria, baina bai ordea XY-rekin. Beraz, lehenengo pausoa aurreko bera da:

$$\begin{array}{rcrcrcr|l} X^2Y & + & XY^2 & + & X & + & Y^3 & Y^2 - 1 \\ \cline{8-8} X^2Y & + & & + & X & & & \\ \cline{1-7} & & XY^2 & & & + & Y^3 & XY + 1 \\ \cline{8-8} & & & & & & & X \end{array}$$

Orain, XY^2 da koefiziente nagusi berria, eta hori bai Y^2-rekin bai XY-rekin zatigarria da. Hala ere, kasu honetan $Y^2 - 1$ polinomioa $XY + 1$-en aurretik jarri

dugunez, horrekin egingo dugu zatiketa (aurreko zatiketan ez bezala):

$$\begin{array}{rcl|l}
X^2Y + XY^2 + X + Y^3 & & & Y^2 - 1 \\
\cline{4-4}
X^2Y + \quad + X & & & X \\
\cline{1-3}
XY^2 + Y^3 & & & XY + 1 \\
\cline{4-4}
XY^2 - X & & & X \\
\cline{1-3}
Y^3 + X & & &
\end{array}$$

Orain, ohartu $Y^3 + X$ zatikizuna ez dagoela ondo ordenatuta: $X + Y^3$ idatzi behar dugu zatiketarekin aurrera segitzeko. Orduan, X koefiziente nagusia ez da zatitzaileen gai nagusiez zatigarria eta, ondorioz, hondarrera eraman behar dugu:

$$\begin{array}{rcl|l}
X^2Y + XY^2 + X + Y^3 & & & Y^2 - 1 \\
\cline{4-4}
X^2Y + \quad + X & & & X \\
\cline{1-3}
XY^2 + Y^3 & & & XY + 1 \\
\cline{4-4}
XY^2 - X & & & X \\
\cline{1-3}
Y^3 + X & & & \\
\boxed{X} & & & \\
\cline{1-1}
Y^3 & & &
\end{array}$$

Oraindik ere jarraitu dezakegu zatitzen, Y^3 Y^2-ren multiploa da eta:

$$\begin{array}{rcl|l}
X^2Y + XY^2 + X + Y^3 & & & Y^2 - 1 \\
\cline{4-4}
X^2Y + \quad + X & & & X + Y \\
\cline{1-3}
XY^2 + Y^3 & & & XY + 1 \\
\cline{4-4}
XY^2 - X & & & X \\
\cline{1-3}
Y^3 + X & & & \\
\boxed{X} & & & \\
\cline{1-1}
Y^3 & & & \\
Y^3 - Y & & & \\
\cline{1-3}
Y & & &
\end{array}$$

Bukatzeko, garbi dago Y hondarrera eraman behar dugula:

$$\begin{array}{rcrcrcrcrcl|rcl}
X^2Y & + & XY^2 & + & X & + & Y^3 & & & & & Y^2 & - & 1 \\
X^2Y & + & & + & X & & & & & & & X & + & Y \\
\hline
 & & XY^2 & & & + & Y^3 & & & & & XY & + & 1 \\
 & & XY^2 & & & & & - & X & & & X & & \\
\hline
 & & & & & & Y^3 & + & X & & & & & \\
 & & & & & & & & \boxed{X} & & & & & \\
\hline
 & & & & & & Y^3 & & & & & & & \\
 & & & & & & Y^3 & - & Y & & & & & \\
\hline
 & & & & & & & & Y & & & & & \\
 & & & & & & & & \boxed{Y} & & & & & \\
\hline
 & & & & & & & & 0 & & &
\end{array}$$

Hondarra: $X + Y$

Horrela, oso fenomeno bitxia dugu: badakigu, aurretik egin dugun zatiketaren arabera, $X^2Y+XY^2+X+Y^3$ polinomioa $(XY+1, Y^2-1)$ idealaren barruan dagoela; hala ere, zatiketa berri honetan, zatitzaileak alderantziz jarri ditugunean, hondarra 0-ren desberdina da. Beraz, indeterminatu bakar bateko zatiketekin ez bezala, *zatiketaren algoritmo orokortuarekin, gerta daiteke zatiketaren hondarra* 0 *ez izatea, baina zatikizuna zatitzaileek sortzen duten idealaren barruan egotea.* Horrela, zatiketaren algoritmo orokortuak ez digu irizpide bat ematen polinomio bat ideal baten barruan dagoen edo ez jakiteko. Zorionez, hurrengo atalean ikusiko dugun bezala, irtenbide bat aurkituko dugu problema horretatik ateratzeko.

5.3. Gröbnerren oinarriak

5.14. Definizioa. Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideala. Orduan, $\mathfrak{a}$ *ideal monomiala* dela esaten dugu monomioen bidez sor badaiteke, hau da, existitzen bada $\{\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A\}$ monomioen familia bat, halakoa non $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A)$ baita.

Hala ere, $\mathfrak{a} = (f_1, \ldots, f_s)$ ideal monomiala bada, horrek ez du esan nahi $f_1, \ldots, f_s$ polinomioek monomioak izan behar dutenik.

Ideal monomialen kasuan, ideal-barnekotasunaren problemak oso soluzio erraza du, jarraian ikusten dugun bezala.

5.15. Teorema. *Izan bedi* $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A)$ *ideal monomiala. Orduan:*

(i) $\boldsymbol{X}^{\boldsymbol{\beta}}$ *monomio bat* $\mathfrak{a}$*-n dago baldin eta soilik baldin monomio sortzaile baten multiploa bada, hau da, existitzen bada* $\boldsymbol{\alpha} \in A$ *non* $\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{X}^{\boldsymbol{\beta}}$ *baita.*

(ii) *Polinomio bat* $\mathfrak{a}$*-n dago baldin eta soilik baldin hori osatzen duten monomio guztiak* $\mathfrak{a}$*-n badaude.*

FROGA. Bi ataletan, garbi dago bakarrik frogatu behar dugula "soilik baldin" zatia, hau da, $\Longrightarrow$ inplikazioa.

(i) Izan bedi $\boldsymbol{X}^{\boldsymbol{\beta}} \in \mathfrak{a}$. Orduan, existitzen dira $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s \in A$ eta polinomioak $q_1, \ldots, q_s \in K[X_1, \ldots, X_n]$, halakoak non

$$\boldsymbol{X}^{\boldsymbol{\beta}} = q_1 \boldsymbol{X}^{\boldsymbol{\alpha}_1} + \cdots + q_s \boldsymbol{X}^{\boldsymbol{\alpha}_s} \tag{5.2}$$

baita. Orain, $q_1, \ldots, q_s$ polinomioak monomioen konbinazio lineal modura idazten baditugu, orduan (5.2) berdintzaren eskuinaldean monomioen konbinazio lineal bat lortuko dugu, agertzen diren monomio guztiak $\boldsymbol{X}^{\boldsymbol{\alpha}_i}$-ren baten multiploa izanik. Jakina, konbinazio lineal horretan gai gehienak elkarrekin deuseztatuko dira, eta bakarrik geldituko da $\boldsymbol{X}^{\boldsymbol{\beta}}$. Gelditzen den bakar hori ere $\boldsymbol{X}^{\boldsymbol{\alpha}_i}$-ren baten multiploa denez, $\boldsymbol{X}^{\boldsymbol{\alpha}_i} \mid \boldsymbol{X}^{\boldsymbol{\beta}}$ dugu, nahi bezala.

(ii) Horretarako, argudio bera erabiltzen da. Bakarrik pentsatu behar dugu (5.2) berdintzaren ezkerraldean polinomio bat agertuko dela, eta ez bakarrik monomio bat. Edozein kasutan, polinomio hori osatzen duten monomio guztiak $\boldsymbol{X}^{\boldsymbol{\alpha}_i}$-ren baten multiploak izango dira eta, beraz, $\mathfrak{a}$ idealean egongo dira. □

5.16. Adibidea. Azter dezagun $f = X^4 + 2X^2Y^2 + Y^4$ eta $g = X^4 - X^3Y + XY^3$ polinomioak $\mathfrak{a} = (X^3, Y^3)$ ideal monomialean dauden edo ez. Horretarako, azken teoremaren arabera, polinomio horiek osatzen duten monomioak X^3 eta Y^3 sortzaileen multiploak diren ikusi behar dugu. Orduan, garbi dago $f \notin \mathfrak{a}$ eta $g \in \mathfrak{a}$ dela.

Hilberten oinarriaren teoremaren arabera, polinomioen eraztunaren edozein ideal polinomio kopuru finitu baten bidez sor daiteke. Ondorengo galdera naturala da: sor daiteke ideal monomial bat *monomio* kopuru finitu baten bidez? Hurrengo teoremak erakusten duenez, hori baino gehiago betetzen da.

5.17. Teorema. *Izan bedi* $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A)$ *ideal monomiala. Orduan, existitzen da* $B \subseteq A$ *finitua, halakoa non* $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\beta}} \mid \boldsymbol{\beta} \in B)$ *baita. Hau da,* emandako $\mathfrak{a}$-ren sortzaileen artean *sistema sortzaile finitu bat aurki dezakegu.*

FROGA. Hilberten oinarriaren teorema aplikatuz, $\mathfrak{a} = (f_1, \ldots, f_s)$ dugu polinomio batzuetarako. Finka dezagun $i \in \{1, \ldots, s\}$ indize bat. Orduan, $f_i \in \mathfrak{a}$ denez, f_i-ren adierazpenean agertzen den monomio bakoitza $\{\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A\}$ sistema sortzaileko monomio baten multiploa da, 5.15 teoremaren arabera. Zatitzaile horiek bilduz, f_i osatzen duten monomio guztietarako eta $i = 1, \ldots, s$ guztietarako, hasierako sistema sortzailearen azpimultzo finitu bat lortzen dugu, $\{\boldsymbol{X}^{\boldsymbol{\beta}} \mid \boldsymbol{\beta} \in B\}$. Frogatu dezagun $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\beta}} \mid \boldsymbol{\beta} \in B)$ dela. Alde batetik, $\supseteq$ partekotasuna nabaria da, hartutako monomio guztiak $\mathfrak{a}$-n baitaude. Alderantziz, $\subseteq$ frogatzeko, ohartu f_i guztiak $\{\boldsymbol{X}^{\boldsymbol{\beta}} \mid \boldsymbol{\beta} \in B\}$ multzoko monomioen multiploen baturak direla. □

5.18. Definizioa. Izan bedi $S \subseteq K[X_1, \ldots, X_n]$. Orduan, $\mathrm{Mon}(X_1, \ldots, X_n)$ multzoan ordena monomial bat ezartzen badugu, $\mathrm{LM}(S)$ eta $\mathrm{LT}(S)$ multzoak honela

definitzen ditugu:

$$\mathrm{LM}(S) = \{\mathrm{LM}(f) \mid f \in S,\ f \neq 0\} \quad \text{eta} \quad \mathrm{LT}(S) = \{\mathrm{LT}(f) \mid f \in S,\ f \neq 0\}.$$

Horrela, polinomioen S edozein multzok ideal monomial bat sortzen du: $(\mathrm{LM}(S))$, alegia. Kontuan izan $(\mathrm{LM}(S)) = (\mathrm{LT}(S))$ betetzen dela, bi ideal horien sortzaileen arteko diferentzia bakarra faktore konstante ez-nuluak baitira.

Ohartu $\mathrm{LM}(S)$ eta $\mathrm{LT}(S)$ ez direla idealak, nahiz eta S ideala izan. Arrazoia da multzo horiek monomioek edo gaiek bakarrik osatzen dituztela, eta bi monomio edo bi gairen batura ez dela ia inoiz berriro ere mota berekoa. Horregatik, kanpoko parentesiak beharrezkoak dira $(\mathrm{LM}(S))$ edo $(\mathrm{LT}(S))$ idazten dugunean, ideal bat lortu nahi badugu.

Orain, naturala da hau galdetzea: $\mathfrak{a} = (f_1, \ldots, f_s)$ bada, betetzen da $(\mathrm{LT}(\mathfrak{a})) = (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s))$ berdintza? Ez da zaila kontradibide bat ematen.

5.19. Adibidea. Izan bedi $\mathfrak{a} = (XY + 1, Y^2 - 1)$. Aukeratzen badugu lex ordena monomiala, $X > Y$ harturik, orduan $\mathrm{LT}(XY + 1) = XY$ eta $\mathrm{LT}(Y^2 - 1) = Y^2$ dugu. (Egia esan, horiek dira gai nagusiak edozein ordena monomial aukeratuta ere: kontuan izan 5.3 lema.) Ikus dezagun ez dela $(\mathrm{LT}(\mathfrak{a})) = (XY, Y^2)$ berdintza betetzen. Horretarako, ohartu

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

dela. Beraz, $X = \mathrm{LT}(X + Y) \in (\mathrm{LT}(\mathfrak{a}))$ dugu. Hala ere, 5.15 teoremaren arabera, $X \notin (XY, Y^2)$ dugu.

Beste alde batetik, $\mathfrak{a}$ polinomioen ideal ez-nulua bada, 5.17 teorema $(\mathrm{LT}(\mathfrak{a})) = (\mathrm{LT}(f) \mid f \in \mathfrak{a},\ f \neq 0)$ idealari aplikatzen badiogu, existitzen dira $g_1, \ldots, g_t \in \mathfrak{a}$ polinomio ez-nuluak, halakoak non $(\mathrm{LT}(\mathfrak{a})) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t))$ baita. Horrela, Gröbnerren oinarriaren kontzeptua sortzen da.

5.20. Definizioa. Demagun $\mathrm{Mon}(X_1, \ldots, X_n)$ multzoan $>$ ordena monomial bat finkaturik dagoela, eta izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal ez-nulua. Orduan, $G = \{g_1, \ldots, g_t\}$ polinomio ez-nuluen multzoa $\mathfrak{a}$-ren *Gröbnerren oinarria* da $>$ ordenarekiko, baldintza hauek betetzen badira:

(i) $G \subseteq \mathfrak{a}$.
(ii) $(\mathrm{LT}(\mathfrak{a})) = (\mathrm{LT}(G))$.

Definizioaren aurreko argudioak erakusten du $K[X_1, \ldots, X_n]$-ren ideal ez-nulu guztiek Gröbnerren oinarriak dituztela. Bestalde, hurrengo atalean garbi geldituko da, Gröbnerren oinarrien adibideak ikusten ditugunean, kontzeptu hori aukeratutako ordena monomialaren menpekoa dela: gerta daiteke $\mathfrak{a}$ idealaren azpimultzo bat bera Gröbnerren oinarria izatea ordena monomial batekiko, eta ez izatea beste ordena batekiko.

Jarraian, Gröbnerren oinarriaren definizioko (ii) baldintza modu ulergarriago batean jarriko dugu.

5.21. Proposizioa. *Izan bitez $>$ ordena monomiala eta $\mathfrak{a}$ $K[X_1,\dots,X_n]$-ren ideal ez-nulua. Orduan, $G=\{g_1,\dots,g_t\}$ polinomio ez-nuluen multzoa $\mathfrak{a}$-ren Gröbnerren oinarria da $>$ ordenarekiko baldin eta soilik baldin bi baldintza hauek betetzen badira:*

(i) $G\subseteq\mathfrak{a}$.
(ii) $f\in\mathfrak{a}$ *polinomio ez-nulua bada, existitzen da* $i\in\{1,\dots,t\}$, *halakoa non* $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$ *baita.*

Froga. Lehenengo eta behin, demagun G $\mathfrak{a}$-ren Gröbnerren oinarria dela $>$ ordenarekiko, eta izan bedi $f\in\mathfrak{a}$, $f\neq 0$. Orduan, $\mathrm{LT}(f)\in(\mathrm{LT}(\mathfrak{a}))=(\mathrm{LT}(G))=(\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t))$ dugu eta, 5.15 teoremaren arabera, existitzen da i non $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$ baita.

Orain, demagun enuntziatuko (i) eta (ii) baldintzak betetzen direla, eta ikus dezagun G Gröbnerren oinarria dela. Horretarako, $(\mathrm{LT}(\mathfrak{a}))=(\mathrm{LT}(G))$ berdintza frogatu behar dugu. Alde batetik, $G\subseteq\mathfrak{a}$ denez, $(\mathrm{LT}(G))\subseteq(\mathrm{LT}(\mathfrak{a}))$ dugu. Alderantzizko partekotasuna frogatzeko, har dezagun $(\mathrm{LT}(\mathfrak{a}))$ idealaren sortzaile bat, hau da, $\mathrm{LT}(f)$ moduko gai bat, $f\in\mathfrak{a}$ eta $f\neq 0$ izanik. Orduan, (ii) erabiliz, $\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$ dugu $g_i\in G$ polinomioren baterako. Beraz, $\mathrm{LT}(f)\in(\mathrm{LT}(G))$ lortzen dugu. Horrek $(\mathrm{LT}(\mathfrak{a}))\subseteq(\mathrm{LT}(G))$ partekotasuna ematen digu. □

Gröbnerren oinarriaren izenean, "oinarri" hitza emandako idealaren sistema sortzailea dela adierazteko erabiltzen da. Propietate hori hurrengo teoreman frogatuko dugu, Gröbnerren oinarrien beste ezaugarri garrantzitsu batzuekin batera. Edonola ere, ez da gomendagarria "oinarri" hitza sistema sortzailearen sinonimo gisa erabiltzea. Izan ere, Aljebran, espazio bektorialen kasuan ere hitz egiten dugu oinarriei buruz. Orain, $K[X_1,\dots,X_n]$-ren $\mathfrak{a}$ ideal bat azpiespazio bektoriala da bereziki, eta horrela ikusita, $\mathfrak{a}$-ren oinarri bat $\mathfrak{a}$-ren sistema sortzailea da. Hala ere, $\mathfrak{a}$-ren sistema sortzaile bat ez da, oro har, $\mathfrak{a}$ azpiespazioaren oinarria. Hori dela eta, nahasketa sor daiteke ideal baten sistema sortzaileei oinarri deitzen badiegu eta, Gröbnerren oinarrien salbuespenarekin, ez dugu terminologia hori erabiliko.

5.22. Teorema. *Izan bitez $\mathfrak{a}$ $K[X_1,\dots,X_n]$-ren ideal ez-nulua, eta $G=\{g_1,\dots,g_t\}$, $\mathfrak{a}$-ren Gröbnerren oinarri bat finkatutako ordena monomial batekiko. Orduan:*

(i) $f\in K[X_1,\dots,X_n]$ *zatitzen badugu, zatiketaren algoritmo orokorra erabiliz, $g_1,\dots,g_t$ polinomioekin, orduan hondarra ez da polinomio horiek tupla gisa zerrendatzeko moduaren menpekoa. Hondar bakar hori $\overline{f}^G$ ikurraz adieraziko dugu. (Ohartu G multzo bat dela, eta ez tupla bat.)*
(ii) $f\in K[X_1,\dots,X_n]$ *bada, orduan $f\in\mathfrak{a}$ dugu baldin eta soilik baldin $g_1,\dots,g_t$ polinomioekin (tupla gisa edozein modutan zerrendaturik) zatitzeko hondarra* 0 *bada.*
(iii) G $\mathfrak{a}$*-ren sistema sortzailea da.*

FROGA. (i) Demagun r eta r^* hondarrak lortzen ditugula, $g_1, \ldots, g_t$ polinomioak bi modu desberdinetan zerrendatzen ditugunean tupla modura. Gure helburua $r = r^*$ frogatzea da. Absurdora eramanez, demagun $r \neq r^*$ dela. Badakigu, 5.13 teoremaren arabera,

$$f = q_1 g_1 + \cdots + q_t g_t + r \quad \text{eta} \quad f = q_1^* g_1 + \cdots + q_t^* g_t + r^*$$

moduko deskonposizioak ditugula. Kenketa eginez,

$$r - r^* = (q_1^* - q_1)g_1 + \cdots + (q_t^* - q_t)g_t \in \mathfrak{a}$$

dugu. Orain, gogoratu zatiketaren algoritmo orokortuko hondarrak propietate hau betetzen duela: bere gaietako bat ere ez da zatigarria $\mathrm{LT}(g_i)$ gai nagusiekin. Ondorioz, $r - r^*$ kendurak propietate bera du eta, bereziki, $\mathrm{LT}(r - r^*)$ gai nagusia ez da $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ gai nagusiekin zatigarria. Baina, $r - r^* \neq 0$ denez, hori kontraesan bat da 5.21 proposizioaren argitan, $G = \{g_1, \ldots, g_t\}$ Gröbnerren oinarria baita. Beraz, $r = r^*$ izan behar dugu.

(ii) Bakarrik frogatu behar dugu "soilik baldin" zatia. Demagun zatiketaren hondarra $r \neq 0$ dela. Orain, $f = q_1 g_1 + \cdots + q_t g_t + r$ deskonposizioa erabiliz eta $f \in \mathfrak{a}$ dela kontuan hartuz, $r \in \mathfrak{a}$ lortzen dugu. Aurreko atalean bezala, hori kontraesan bat da.

(iii) Hori (ii) atalaren ondorio berehalakoa da: $f \in \mathfrak{a}$ polinomioa $g_1, \ldots, g_t$-rekin zatituz, $f = q_1 g_1 + \cdots + q_t g_t$ lortzen dugu. Beraz, $\mathfrak{a}$-ko edozein polinomio $(g_1, \ldots, g_t)$ idealean dago, hau da, $\mathfrak{a} \subseteq (g_1, \ldots, g_t)$ dugu. Alderantzizko partekotasuna begibistakoa da, $G \subseteq \mathfrak{a}$ izateagatik. Horrela, $\mathfrak{a} = (g_1, \ldots, g_t)$ dugu, eta G $\mathfrak{a}$-ren sistema sortzailea da. □

Dakusagunez, $G = \{g_1, \ldots, g_t\}$ Gröbnerren oinarri batekin zatitzean, 5.2 atalean topatu ditugun arazoak desagertu egiten dira: alde batetik, $g_1, \ldots, g_t$ elementuak tupla gisa edozein modutan zerrendatuta ere, beti lortuko dugu hondar bera; beste alde batetik, polinomio bat $\mathfrak{a}$-n badago, G-ko polinomioekin zatitzean, beti lortuko dugu 0 hondarra. Bereziki, horrek ideal-barnekotasunaren problema ebazteko metodo bat ematen digu; jakin nahi badugu f polinomioa $\mathfrak{a}$ idealean dagoen, honela jokatuko dugu:

(i) $\mathfrak{a}$ idealaren G Gröbnerren oinarri bat aurkituko dugu (nahi dugun ordena monomialarekiko; ez du garrantzirik ordena monomiala zein den).
(ii) f polinomioa G-ko polinomioekin zatituko dugu (horiek edozein modutan zerrendaturik), eta r hondarra 0 den edo ez ikusiko dugu: $r = 0$ bada, orduan $f \in \mathfrak{a}$ dugu, eta $r \neq 0$ bada, orduan $f \notin \mathfrak{a}$ dugu.

Prozedura horretan, punturik korapilatsuena $\mathfrak{a}$ idealaren Gröbnerren oinarri bat aurkitzea da. Hori lortzeko algoritmo bat ematea izango da, hain zuzen ere, hurrengo atalaren helburua.

5.4. S-irizpidea eta Buchbergerren algoritmoa

Aurreko atalean ikusi dugunez, $K[X_1,\dots,X_n]$-ren $\mathfrak{a}$ ideal batek dituen sistema sortzaile guztietatik, Gröbnerren oinarriak hobestekoak dira. Eskuarki, $\mathfrak{a}$ ideala sistema sortzaile baten bidez emango digute. Horrela, honako bi galdera hauek sortzen dira:

(i) Emandako sistema sortzailea, ba al da $\mathfrak{a}$-ren Gröbnerren oinarria?
(ii) Sistema sortzaile hori ez bada Gröbnerren oinarria, nola alda dezakegu Gröbnerren oinarri bat lortzeko?

Lehenengo galderari erantzuteko, irizpide bat garatuko dugu, *S-irizpidea*, sistema sortzaile bat Gröbnerren oinarria den edo ez esango diguna, kalkulu erraz batzuk eginez. Bestetik, *Buchbergerren algoritmoak* bigarren galderari erantzuna emango dio. Hori izango da normalean erabiliko dugun prozedura Gröbnerren oinarriak eraikitzeko.

Has gaitezen S-irizpidearekin. Horren atzean dagoen ideia hobeto ulertzeko, azter dezagun kasu berezi bat. Demagun $\mathfrak{a}=(f,g)$ bi polinomioren bidez sortuta dagoela. Orduan, 5.21 proposizioaren arabera, $\{f,g\}$ multzoa $\mathfrak{a}$-ren Gröbnerren oinarria da baldin eta soilik baldin, $0\neq h\in\mathfrak{a}$ guztietarako, $\mathrm{LT}(f)\mid\mathrm{LT}(h)$ edo $\mathrm{LT}(g)\mid\mathrm{LT}(h)$ badugu. Orain, $h\in\mathfrak{a}$ bada, $h=pf+qg$ idatz dezakegu, $p,q\in K[X_1,\dots,X_n]$ izanik. Hiru kasu ditugu:

(i) $\mathrm{LM}(pf)>\mathrm{LM}(qg)$. Orduan, 5.10 teorema erabiliz, $\mathrm{LT}(h)=\mathrm{LT}(pf)=\mathrm{LT}(p)\mathrm{LT}(f)$ dugu eta, beraz, $\mathrm{LT}(f)\mid\mathrm{LT}(h)$.
(ii) $\mathrm{LM}(pf)<\mathrm{LM}(qg)$. Orduan, $\mathrm{LT}(h)=\mathrm{LT}(qg)=\mathrm{LT}(q)\mathrm{LT}(g)$ dugu eta, beraz, $\mathrm{LT}(g)\mid\mathrm{LT}(h)$.
(iii) $\mathrm{LM}(pf)=\mathrm{LM}(qg)$.

Azken kasuan, beste bi posibilitate daude:

(iii-a) $\mathrm{LT}(pf)+\mathrm{LT}(qg)\neq 0$, hau da, pf-ren eta qg-ren gai nagusiak ez dira elkarrekin deuseztatzen. Orduan, h-ren monomio nagusia $\mathrm{LM}(pf)=\mathrm{LM}(qg)$-ren berdina da. Beraz, bai $\mathrm{LT}(f)$-k bai $\mathrm{LT}(g)$-k $\mathrm{LT}(h)$ zatitzen dute.
(iii-b) $\mathrm{LT}(pf)+\mathrm{LT}(qg)=0$, hau da, pf-ren eta qg-ren monomio nagusiak elkarrekin deuseztatzen dira. Orduan, h-ren monomio nagusia $\mathrm{LM}(pf)=\mathrm{LM}(qg)$ baino txikiagoa da, eta ez dago garbi $\mathrm{LT}(f)$-k edo $\mathrm{LT}(g)$-k $\mathrm{LT}(h)$ zatituko duten. Idazten badugu

$$h=\mathrm{LT}(p)f-\mathrm{LT}(q)g+(p-\mathrm{LT}(p))f+(q-\mathrm{LT}(q))g,$$

orduan gai nagusien deuseztatzea $\mathrm{LT}(p)f-\mathrm{LT}(q)g$ zatian gertatzen da.

Dakusagunez, (iii-b) kasuan f eta g polinomioen gai nagusiak elkarrekin deuseztatzea lortzen dugu, gai egoki batzuekin biderkatu eta gero. Zein da hori lortzeko modurik errazena? Demagun, adibidez, $f=2X^3Y+Y^2$ eta $g=3X^2Y^3-2XY$ dela, eta lex ordena erabiltzen ari garela, $X>Y$ harturik. Orduan, $\mathrm{LT}(f)=2X^3Y$ eta $\mathrm{LT}(g)=3X^2Y^3$ dugu, eta

$$\frac{1}{2}\,Y^2\,\mathrm{LT}(f)-\frac{1}{3}\,X\,\mathrm{LT}(g)=X^3Y^3-X^3Y^3=0.$$

Horrela,

$$\frac{1}{2}\,Y^2 f - \frac{1}{3}\,Xg$$

konbinazioarekin f-ren eta g-ren gai nagusiak elkarrekin deuseztatzea lortzen dugu. Azter dezagun nola lortu dugun deuseztatze hori:

(i) f Y^2-rekin eta g X-rekin biderkatzen baditugu, lortzen diren biderkadurek X^3Y^3 monomio nagusi bera dute. Ohartu X^3Y^3 monomioa $\mathrm{LM}(f)$-ren eta $\mathrm{LM}(g)$-ren multiplo komunetako txikiena dela, f-ri $X^3Y^3/\mathrm{LM}(f)$ biderkatzen diogula, eta g-ri, berriz, $X^3Y^3/\mathrm{LM}(g)$.

(ii) Behin biderkadura horietan monomio bera eskuraturik, bakarrik doitu behar ditugu koefizienteak, gai nagusien deuseztatzea lortzeko. Hori erraz konpontzen da: nahikoa da f polinomioa $\mathrm{LC}(f)$ koefiziente nagusiaz zatitzea eta g, berriz, $\mathrm{LC}(g)$-z zatitzea. Horrela, 1 koefizientea lortuko dugu bi kasuetan eta, kenketa eginez, gai nagusiak elkarrekin deuseztatuko dira.

Beraz, f polinomioa $X^3Y^3/\mathrm{LM}(f)$-rekin biderkatu dugu, eta $\mathrm{LC}(f)$-rekin zatitu dugu. Hau da, f $X^3Y^3/\mathrm{LT}(f)$-rekin biderkatu dugu. Antzera, g $X^3Y^3/\mathrm{LT}(g)$-rekin biderkaturik agertzen da. Hori ikusita, ondorengo definizioa ematen dugu.

5.23. Definizioa. Izan bitez $f, g \in K[X_1, \ldots, X_n]$, eta izan bedi $\boldsymbol{X}^{\boldsymbol{\gamma}}$ $\mathrm{LM}(f)$-ren eta $\mathrm{LM}(g)$-ren multiplo komunetako txikiena. (Ordena monomial bat emanda dago inplizituki.) Orduan, f-ren eta g-ren *S-polinomioa*, $S(f,g)$ ikurraren bidez adieraziko duguna, honela definitzen da:

$$S(f,g) = \frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\mathrm{LT}(f)}\,f - \frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\mathrm{LT}(g)}\,g. \tag{5.3}$$

Ohartu S-polinomioa f-ren eta g-ren multiploen kendura bat dela; beraz, (f,g) idealean dago. Bestetik, garbi dago $S(g,f) = -S(f,g)$ dela. Definizioko formula buruz ikastea baino, hobe da aipatu ditugun bi ideiak gogoratzea S-polinomioa kalkulatzeko: lehenengo, f-ren eta g-ren monomio nagusien multiplo komunetako txikiena bilatu behar da, eta gero koefizienteak konpondu behar dira gai nagusien deuseztatzea lortzeko.

5.24. Adibidea. Izan bitez $f = X^2YZ - Y^4$ eta $g = 2XYZ^2 - Y^2Z^2$, eta har dezagun $\mathrm{Mon}(X,Y,Z)$ multzoan grevlex ordena monomiala, $X > Y > Z$ izanik. Orduan, $\mathrm{LT}(f) = -Y^4$ eta $\mathrm{LT}(g) = 2XYZ^2$ dugu, eta monomio nagusien multiplo komunetako txikiena XY^4Z^2 da. Beraz,

$$\begin{aligned} S(f,g) &= -XZ^2 f - \frac{1}{2}Y^3 g = (-X^3YZ^3 + XY^4Z^2) - (XY^4Z^2 - \frac{1}{2}Y^5Z^2) \\ &= -X^3YZ^3 + \frac{1}{2}Y^5Z^2. \end{aligned}$$

Orain 117. orrialdeko (iii-b) atalean esaten ari ginenaren ildotik jarraituko dugu. Hor $h = pf + qg$ polinomioa genuen eta $\mathrm{LT}(p)f + \mathrm{LT}(q)g$ konbinazioan f-ren gai nagusia g-ren gai nagusiarekin deuseztatzen zen. Jarraian ikusten dugunez, deuseztatze hori S-polinomioarekin lortzen denaren ondorioa da.

5.25. Proposizioa. *Izan bitez f eta g bi polinomio, eta a eta b bi gai. Baldin eta $af + bg$ konbinazioan f-ren eta g-ren gai nagusiak elkarrekin deuseztatzen badira, orduan $af + bg = cS(f, g)$ dugu, c gai bat izanik.*

FROGA. Hipotesiaren arabera, $a\mathrm{LT}(f) + b\mathrm{LT}(g) = 0$ dugu. Orduan,

$$\begin{aligned} af + bg &= \frac{a\,\mathrm{LT}(f)}{\mathrm{LT}(f)}\,f + \frac{b\,\mathrm{LT}(g)}{\mathrm{LT}(g)}\,g = \frac{a\,\mathrm{LT}(f)}{\mathrm{LT}(f)}\,f + \frac{-a\,\mathrm{LT}(f)}{\mathrm{LT}(g)}\,g \\ &= a\,\mathrm{LT}(f)\left(\frac{f}{\mathrm{LT}(f)} - \frac{g}{\mathrm{LT}(g)}\right) \end{aligned} \tag{5.4}$$

dugu. Bestalde, $a\mathrm{LT}(f) = -b\mathrm{LT}(g)$ biderkadura bai $\mathrm{LM}(f)$-ren bai $\mathrm{LM}(g)$-ren multiploa da. Beraz, $\boldsymbol{X}^{\boldsymbol{\gamma}}$ bada $\mathrm{LM}(f)$-ren eta $\mathrm{LM}(g)$-ren multiplo komunetako txikiena, orduan $\boldsymbol{X}^{\boldsymbol{\gamma}}$-k $a\mathrm{LT}(f)$ zatitzen du. Idatz dezagun $a\mathrm{LT}(f) = c\boldsymbol{X}^{\boldsymbol{\gamma}}$. Balio hori (5.4) berdintzan ordezkatuz,

$$af + bg = c\left(\frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\mathrm{LT}(f)}\,f - \frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\mathrm{LT}(g)}\,g\right) = c\,S(f, g)$$

lortzen dugu, eta $af + bg$ S-polinomioaren multiploa da. □

Orain, $af+bg$ konbinazioan f-ren eta g-ren gai nagusiak elkarrekin deuseztatzen direla esateko beste modu bat $\mathrm{multideg}(af) = \mathrm{multideg}(bg) = \delta$ eta $\mathrm{multideg}(af + bg) < \delta$ baldintzak eskatzea da. Hori dela eta, hurrengo teoremak aurreko proposizioa orokortzen du, gai nagusien deuseztatzea bi polinomioren baino gehiagoren konbinazio batean gertatzen den kasura.

5.26. Teorema. *Izan bitez $f_1, \ldots, f_s$ polinomioak, eta $a_1, \ldots, a_s$ gaiak. Demagun* $\mathrm{multideg}(a_i f_i) = \delta$ *multimaila guztiak berdinak direla $i = 1, \ldots, s$ guztietarako, eta* $\mathrm{multideg}(a_1 f_1 + \cdots + a_s f_s) < \delta$ *dela. Orduan, existitzen dira c_i gaiak, halakoak non*

$$a_1 f_1 + \cdots + a_s f_s = \sum_{i=1}^{s-1} c_i S(f_i, f_{i+1})$$

baita. Gainera, $\mathrm{multideg}(c_i S(f_i, f_{i+1})) < \delta$ *dugu i guztietarako.*

FROGA. Teorema s-ren gaineko indukzioa erabiliz frogatuko dugu. Ohartu $s = 2$ den kasua 5.25 proposizioko emaitza dela.

Demagun orain $s > 2$ dela. Alde batetik, $\mathrm{multideg}(a_i f_i) = \delta$ denez $i = 1, \ldots, s$ guztietarako,

$$\mathrm{LM}(a_1 f_1) = \mathrm{LM}(a_2 f_2) = \cdots = \mathrm{LM}(a_s f_s)$$

dugu. Hori dela eta, $\mathrm{multideg}(a_1 f_1 + \cdots + a_s f_s) < \delta$ izateko modu bakarra

$$\mathrm{LT}(a_1 f_1) + \mathrm{LT}(a_2 f_2) + \cdots + \mathrm{LT}(a_s f_s) = 0 \tag{5.5}$$

betetzea da. Gainera, $\mathrm{LM}(a_1 f_1) = \mathrm{LM}(a_2 f_2)$ izategatik, existitzen da $\lambda \in K$ non $\mathrm{LT}(a_1 f_1) = -\lambda \mathrm{LT}(a_2 f_2)$ baita. Ondorioz,

$$\mathrm{LT}(a_1 f_1) + \mathrm{LT}(\lambda a_2 f_2) = 0$$

dugu eta, (5.5) erabiliz,

$$\mathrm{LT}((1-\lambda)a_2f_2) + \mathrm{LT}(a_3f_3) + \cdots + \mathrm{LT}(a_sf_s) = 0.$$

Horrek esan nahi du

$$\mathrm{multideg}(a_1f_1 + \lambda a_2f_2) < \delta$$

eta

$$\mathrm{multideg}((1-\lambda)a_2f_2 + a_3f_3 + \cdots + a_sf_s) < \delta$$

betetzen dela. Indukzio-hipotesia eta $s = 2$ den kasua erabiliz, existitzen dira $c_1, c_2, \ldots, c_s$ gaiak halakoak non

$$a_1f_1 + \lambda a_2f_2 = c_1S(f_1, f_2)$$

eta

$$(1-\lambda)a_2f_2 + a_3f_3 + \cdots + a_sf_s = \sum_{i=2}^{s-1} c_iS(f_i, f_{i+1}).$$

Bi berdintza horiek batuz, enuntziatuko emaitza lortzen dugu. □

Orain, S-irizpidea enuntziatzeko eta frogatzeko moduan gaude.

5.27. Teorema (S-irizpidea)**.** *Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal ez-nulua, eta G $\mathfrak{a}$-ren sistema sortzaile finitu bat. Orduan, ordena monomial batekiko, baliokideak dira:*

(i) *G $\mathfrak{a}$-ren Gröbnerren oinarria da.*

(ii) *$g, h \in G$ guztietarako, $S(g,h)$ polinomioaren hondarra 0 da, G-rekin zatitzean. Zatiketa hori egiteko, G-ko elementuak nahi dugun bezala zerrenda ditzakegu, eta are gehiago, zerrendatzeko modu desberdinak aukera ditzakegu S-polinomio desberdinetarako.*

Froga. (i) ⇒ (ii). Esan dugunez, $S(g,h)$ polinomioa (g,h) idealaren barruan dago eta, bereziki, $\mathfrak{a}$-ren barruan. Orduan, G $\mathfrak{a}$-ren Gröbnerren oinarria izateagatik, $\overline{S(g,h)}^{G} = 0$ dugu, 5.22 teoremaren arabera.

(ii) ⇒ (i). Izan bedi $f \in \mathfrak{a}$, $f \neq 0$, eta ikus dezagun badagoela $g \in G$, halakoa non $\mathrm{LT}(g) \mid \mathrm{LT}(f)$ baita. Orduan, 5.21 proposizioaren arabera, G $\mathfrak{a}$-ren Gröbnerren oinarria dela frogaturik gelditzuko da.

Izan bedi $G = \{g_1, \ldots, g_t\}$. Lehenengo eta behin, $f \in \mathfrak{a} = (g_1, \ldots, g_t)$ izateagatik, $f = q_1g_1 + \cdots + q_tg_t$ idatz dezakegu, $q_i \in K[X_1, \ldots, X_n]$ izanik. Orain, i-ren baterako $\mathrm{multideg}(f) = \mathrm{multideg}(q_ig_i)$ bada, orduan $\mathrm{LM}(f) = \mathrm{LM}(q_ig_i) = \mathrm{LM}(q_i)\mathrm{LM}(g_i)$ dugu eta, ondorioz, $\mathrm{LT}(g_i)$ gai nagusiak $\mathrm{LT}(f)$ zatitzen du.

Demagun, orduan, $\mathrm{multideg}(f) = \mathrm{multideg}(q_ig_i)$ berdintza ez dela inoiz betetzen, hau da, $f = q_1g_1 + \cdots + q_tg_t$ moduko deskonposizio guztietarako

$$\mathrm{multideg}(f) < \max\{\mathrm{multideg}(q_ig_i) \mid i = 1, \ldots, t\}$$

dugula. Ikusiko dugunez, horrek kontraesan batera eramango gaitu. Aukeratu dezagun f-ren deskonposizioa $\delta = \max\{\mathrm{multideg}(q_ig_i) \mid i = 1, \ldots, t\}$ balioa minimoa den moduan. (Minimo horren existentzia ordena monomialaren definizioko (OM3) baldintzak ziurtatzen du.) Orain, q_ig_i batugaien artean, batzuen multimaila δ-ren

berdina izango da, eta gainerakoena, δ baino txikiagoa. Orokortasuna galdu gabe, δ multimaila dutenak lehenengoak direla pentsa dezakegu, adibidez $q_1g_1, \dots, q_sg_s$. Orduan, $h = q_{s+1}g_{s+1} + \cdots + q_tg_t$ bada,

$$\begin{aligned} f &= q_1g_1 + \cdots + q_sg_s + h \\ &= (\mathrm{LT}(q_1) + q_1 - \mathrm{LT}(q_1))g_1 + \cdots + (\mathrm{LT}(q_s) + q_s - \mathrm{LT}(q_s))g_s + h \\ &= \mathrm{LT}(q_1)g_1 + \cdots + \mathrm{LT}(q_s)g_s + h' \end{aligned} \tag{5.6}$$

dugu, $\mathrm{multideg}(\mathrm{LT}(q_i)g_i) = \delta$ izanik $i = 1, \dots, s$ guztietarako, eta h' izanik multimaila δ baino txikiagoa duten g_i polinomioen multiplo batzuen batura. Gogoratzen badugu $\mathrm{multideg}(f) < \delta$ dela,

$$\mathrm{multideg}(\mathrm{LT}(q_1)g_1 + \cdots + \mathrm{LT}(q_s)g_s) < \delta$$

ere badela ondorioztatzen dugu. Orduan, 5.26 teorema erabiliz,

$$\mathrm{LT}(q_1)g_1 + \cdots + \mathrm{LT}(q_s)g_s = \sum_{i=1}^{s-1} c_iS(g_i, g_{i+1}) \tag{5.7}$$

idatz dezakegu, $\mathrm{multideg}(c_iS(g_i, g_{i+1})) < \delta$ izanik i guztietarako. Orain, hipotesiaren arabera, $S(g_i, g_{i+1})$ bakoitza G-rekin zatitzean 0 hondarra lortzen dugu. Hori dela eta, 5.13 teorema aplikatuz

$$S(g_i, g_{i+1}) = h_1g_1 + \cdots + h_tg_t$$

dugu, $\mathrm{multideg}(h_jg_j) \leq \mathrm{multideg}(S(g_i, g_{i+1}))$ izanik. (Ohartu deskonposizio hori lortzeko ez duela garrantzirik zein modutan zerrendatzen ditugun G-ko polinomioak zatiketa egiteko orduan.) Azken berdintza horretako balioak (5.7)-n ordezkatuz, eta gero hori (5.6)-ra eramanez,

$$f = q_1'g_1 + \cdots + q_t'g_t$$

moduko deskonposizio bat lortzen dugu, $\mathrm{multideg}(q_i'g_i) < \delta$ izanik, $i = 1, \dots, t$ guztietarako. Hori δ-ren definizioaren kontra doa, eta emaitza frogaturik gelditzen da. □

5.28. Adibidea. Izan bedi $\mathfrak{a} = (Y - X^2, Z - X^3)$ $K[X, Y, Z]$-ren ideala. Ikus dezagun ea $f = Y - X^2$ eta $g = Z - X^3$ polinomioek $\mathfrak{a}$-ren Gröbnerren oinarri bat osatzen duten. Dakigunez, kontzeptu hori erlatiboa da, eta erantzuna aukeratzen dugun ordena monomialaren araberakoa izan daiteke. Bi kasu aztertuko ditugu:

(i) Ordena monomiala lex bada, $X > Y > Z$ harturik. Orduan, $\mathrm{LM}(f) = X^2$ eta $\mathrm{LM}(g) = X^3$ dugu. Beraz,

$$S(f, g) = -Xf + g = -XY + Z.$$

Zatitu dezagun S-polinomio hau (f, g) tuplaz:

$$\begin{array}{rcl|rcl} -XY & + & Z & -X^2 & + & Y \\ \cline{4-6} \boxed{-XY} & & & & & \\ \cline{1-1} & & Z & -X^3 & + & Z \\ \cline{4-6} & & \boxed{Z} & & & \\ \cline{3-3} & & 0 & & & \end{array}$$

Beraz, zatiketaren hondarra $-XY + Z \neq 0$ da, eta $\{f, g\}$ ez da kasu honetan Gröbnerren oinarria.

(ii) Ordena monomiala lex bada, $Z > Y > X$ harturik. Kasu horretan, $\mathrm{LM}(f) = Y$ eta $\mathrm{LM}(g) = Z$ dugu. Ondorioz,

$$S(f, g) = Zf - Yg = -X^2Z + X^3Y.$$

Berriro ere, S-polinomioa (f, g) tuplaz zatitu behar dugu:

$$\begin{array}{rcl|rcl} -X^2Z & + & X^3Y & Y & - & X^2 \\ \cline{4-6} -X^2Z & & + X^5 & X^3 & & \\ \cline{1-3} & X^3Y & - X^5 & Z & - & X^3 \\ \cline{4-6} & X^3Y & - X^5 & -X^2 & & \\ \cline{2-3} & & 0 & & & \end{array}$$

Beraz, zatiketaren hondarra 0 da, eta $\{f, g\}$ Gröbnerren oinarria da aipatu dugun ordena monomialarekiko.

Dakusagunez, gerta daiteke multzo bat Gröbnerren izatea ordena monomial batekiko, eta ez izatea beste batekiko. Adibide honekin, berriro ere azpimarratu nahi dugu Gröbnerren oinarria izateko propietatea erlatiboa dela.

Dagoeneko, atal honen hasieran egindako lehenengo galderari erantzun diogu, eta badugu irizpide bat sistema sortzaile bat Gröbnerren oinarria den edo ez jakiteko. Hurrengo teoreman, bigarren galderaz arduratuko gara: sistema sortzaile hori Gröbnerren oinarria ez bada, nola lor dezakegu Gröbnerren oinarri bat emandako sistema sortzailea erabiliz? Ideia ondorengo lematik ateratzen dugu.

5.29. Lema. *Demagun f polinomioa $(f_1, \ldots, f_s)$-rekin zatitzeko hondarra r dela. Orduan, f $(f_1, \ldots, f_s, r)$-rekin zatitzen dugunean* 0 *hondarra lortzen dugu.*

Froga. Notazioa sinplifikatzearren, jarri $F = (f_1, \ldots, f_s)$. Lehenengo eta behin, beste emaitza hau frogatuko dugu: $f - r$ polinomioa F-rekin zatitzeko hondarra 0 dela. Absurdora eramanez, demagun faltsua dela. Aukera dezagun kontradibide bat, $\mathrm{LM}(f)$ monomioa minimoa den moduan. Izan bedi $r' \neq 0$, $f - r$ polinomioa F-rekin zatituz lortzen den hondarra. Orain, bi kasu bereizten ditugu:

(i) $\mathrm{LT}(f - r) = \mathrm{LT}(f)$. Hori gertatzen da baldin eta soilik baldin $\mathrm{LM}(r) < \mathrm{LM}(f)$ bada. Kontuan hartzen badugu $\mathrm{LT}(r)$ dela, f F-rekin zatitzean,

hondarrera eramaten den lehenengo gaia, ondorioztatzen dugu zatiketa horren lehenengo pausoan $\mathrm{LT}(f)$ $\mathrm{LT}(f_i)$-ren batekin zatigarria dela. Orduan, $\mathrm{LT}(f) = q_i\mathrm{LT}(f_i)$ bada, zatiketa egiten jarraituko dugu $g = f - q_i f_i$ zatikizun berriarekin. Bestalde, $\mathrm{LT}(f - r) = \mathrm{LT}(f)$ denez, $f - r$ polinomioa F-rekin zatitzeko, lehenengo pausoa berbera da eta $(f - r) - q_i f_i = g - r$ zatikizun berria lortuko dugu. Orain, g F-rekin zatitzen badugu, hondarra r da. (Azken batean, f-rekin egiten dugun zatiketa bera da, baina pauso bat geroago hasita.) Era berean, $g - r$ F-rekin zatituz $r' \neq 0$ hondarra lortzen dugu. Hori kontraesan bat da, g polinomioa ez delako frogatu nahi dugun emaitzaren kontradibide bat, $\mathrm{LM}(g) < \mathrm{LM}(f)$ izateagatik.

(ii) $\mathrm{LT}(f - r) \neq \mathrm{LT}(f)$. Hori gertatzen da baldin eta soilik baldin $\mathrm{LM}(r) = \mathrm{LM}(f)$ bada. (Gogoan izan $\mathrm{LM}(r) \leq \mathrm{LM}(f)$ dela, r izateagatik f F-rekin zatitzeko hondarra.) Orduan, f-ren zatiketan lehenengo pausoa eman eta gero, lortzen dugun zatikizun berria $g = f - \mathrm{LT}(r)$ da, $\mathrm{LT}(r)$ hondarrera doa eta. Ohartu, gainera, g F-rekin zatitzeko hondarra $r' = r - \mathrm{LT}(r)$ dela. (Hori, berriro ere, f-ren zatiketaren parte bat da.) Orain, kontuan hartuz $\mathrm{LM}(g) < \mathrm{LM}(f)$ dela eta f kontradibide minimoa dela, ondorioztatzen dugu $g - r'$-ek 0 hondarra ematen duela F-rekin zatitzean. Baina, $g - r' = (f - \mathrm{LT}(r)) - (r - \mathrm{LT}(r)) = f - r$ denez, horrek esan nahi luke f ez dela kontradibide bat.

Horrenbestez, emaitza laguntzailea frogaturik gelditzen da. Orain, erraz ikus dezakegu enuntziatuko propietatea betetzen dela. Izan ere, demagun $\{f^{(i)}\}$ dela f-ren zatiketan agertzen diren zatikizunen segida. Orduan, $f^{(j)}$ baldin bada gai nagusia hondarrera eramaten duen lehenengo zatikizuna, konturatzen gara $f^{(j)}$ F-rekin zatituz r hondarra lortzen dugula. Aurreko paragrafoko emaitzaren arabera, $f^{(j)} - r$-k 0 hondarra ematen du F-rekin zatitzean. Ikus dezagun, beste alde batetik, zer gertatzen den f polinomioa $(f_1, \ldots, f_s, r)$ tupla luzatuaz zatitzen badugu. Orduan, lehenengo $j-1$ pausoetan f_i polinomioak erabil ditzakegu zatikizunen gai nagusiak ezabatzeko eta, beraz, j. zatikizuna $f^{(j)}$ da. Esan dugun bezala, polinomio horren gai nagusia hondarrera doa F-rekin zatitzean. Beraz, $\mathrm{LT}(f^{(j)}) = \mathrm{LT}(r)$ dugu eta zatiketaren ondorengo pausoan r polinomioa erabiliko dugu $\mathrm{LT}(f^{(j)})$ ezabatzeko. Beraz, hurrengo zatikizuna $f^{(j)} - r$ da. Ikusi dugunez, $f^{(j)} - r$-k 0 hondarra ematen du F-rekin zatitzean. Horrek esan nahi du zatiketak aurrera egin ahala, zatikizunen gai nagusiak beti izango direla $\mathrm{LT}(f_i)$-ren batez zatigarriak. Ondorioz, $f^{(j)} - r$ $(f_1, \ldots, f_s, r)$-rekin zatituz gero, inoiz ez gara helduko r erabiltzera. Horrela, tupla luzatuaz zatituz ere $f^{(j)} - r$-k 0 hondarra ematen du. Azkenik, $f^{(j)} - r$ polinomioa f-ren zatiketan zatikizun modura agertzen denez, f $(f_1, \ldots, f_s, r)$-rekin zatitzean lortzen den hondarra ere 0 da. □

5.30. Teorema (Buchbergerren algoritmoa)**.** *Izan bitez* $\mathfrak{a}$ *polinomioen ideal eznulua, eta* $\{f_1, \ldots, f_s\}$ $\mathfrak{a}$*-ren sistema sortzailea. Jarri* $G_0 = \varnothing$ *eta* $G_1 = (f_1, \ldots, f_s)$*, eta errepikatu ondorengo pausoak* $i \geq 1$ *guztietarako:*

(BA1) *Definitu* $G_{i+1} = G_i$*.*

(BA2) *$f \in G_i \setminus G_{i-1}$ eta $g \in G_i$ guztietarako, kalkulatu $S(f,g)$ polinomioa eta zatitu G_i-rekin, G_i-ko polinomioak nahi dugun bezala zerrendatuz. (Nahi izanez gero, zerrendatzeko modu desberdinak aukera ditzakegu (f,g) bikote desberdinetarako.)*

(BA3) *Aurreko ataleko zatiketaren hondarra 0 ez den kasu guztietan, birdefinitu G_{i+1} tupla, hondar hori azken posizioan gehituz.*

Orduan, existitzen da m, halakoa non $G_m = G_{m+1}$ baita (hau da, (BA2) pausoan S-polinomio guztiek 0 hondarra ematen dute), eta G_m $\mathfrak{a}$-ren Gröbnerren oinarria da.

Froga. Alde batetik, G_{i+1}-en definizioagatik, $G_i \subseteq G_{i+1}$ dugu. Kontuan izanik $G_1 = (f_1, \ldots, f_s)$ $\mathfrak{a}$-ren sistema sortzailea dela, G_i ere $\mathfrak{a}$-ren sistema sortzailea da $i \geq 1$ guztietarako.

Ikus dezagun algoritmoa gelditzen dela, hau da, badagoela m, non $G_m = G_{m+1}$ baita. Absurdora eramanez, demagun $G_i \subsetneq G_{i+1}$ dela i guztietarako. Orduan, existitzen da $S(f,g)$ polinomio bat, $f, g \in G_i$ izanik, halakoa non $h = \overline{S(f,g)}^{G_i}$ hondarra 0-ren desberdina baita. Horrela, h-ren gai nagusia ez da G_i-ko polinomioen gai nagusiaz zatigarria eta, 5.15 teoremaren arabera, $\mathrm{LT}(h) \notin (\mathrm{LT}(G_i))$ dugu. Beraz, $(\mathrm{LT}(G_i)) \subsetneq (\mathrm{LT}(G_{i+1}))$ partekotasun hertsia dugu. Orduan,

$$(LT(G_1)) \subsetneq \cdots (\mathrm{LT}(G_i)) \subsetneq (\mathrm{LT}(G_{i+1})) \subsetneq \cdots$$

idealen kate hertsiki gorakor infinitu bat dugu. Baina hori ezinezkoa da, Hilberten oinarriaren teoremaren arabera.

Azkenik, ikus dezagun G_m $\mathfrak{a}$-ren Gröbnerren oinarria dela. Aplikatzen badugu S-irizpidea, hori frogatzeko $\overline{S(f,g)}^{G_m} = 0$ dela egiaztatu behar dugu $f, g \in G_m$ guztietarako. Orain, $G_m = G_{m+1}$ izateagatik eta G_{m+1}-en eraikuntzagatik, hondarra 0 da $f \in G_m \setminus G_{m-1}$ edo $g \in G_m \setminus G_{m-1}$ denean. (Gogoratu $S(g,f) = -S(f,g)$ dela.) Beste alde batetik, $f, g \in G_{m-1}$ bada, har dezagun $i \in \{1, \ldots, m-1\}$ ahal den txikiena, non $f, g \in G_i$ baita. Beraz, polinomioetako bat $G_i \setminus G_{i-1}$-en dago. Orduan, bi kasu bereizten ditugu:

(i) $\overline{S(f,g)}^{G_i} = 0$. Orduan, $S(f,g)$ G_m-rekin zatitzeko, zerrendatu ditzagun G_m-ko elementuak modu honetan: hasieran, G_i-koak ($\overline{S(f,g)}^{G_i} = 0$ lortzen genuen ordena berean), eta gero gainerako guztiak. Horrela, zatiketaren algoritmoaren prozeduragatik, garbi dago $\overline{S(f,g)}^{G_m} = 0$ dugula.

(ii) $\overline{S(f,g)}^{G_i} \neq 0$. Beraz, G_{i+1} eraikitzen dugunean, G_i multzoari $r = \overline{S(f,g)}^{G_i}$ polinomioa gehituko diogu. Orduan, $S(f,g)$ G_m-rekin zatitzeko, zerrendatu ditzagun G_m-ko elementuak modu honetan: hasieran, G_i-koak ($S(f,g)$-k r hondarra ematen duen ordena berean), gero r, eta azkenik G_m-ko gainerako polinomio guztiak. Aurreko lemaren arabera, zatiketa $G_i \cup \{r\}$ multzoarekin (r azken posizioan izanik) bakarrik egiten badugu, orduan $S(f,g)$-k 0 hondarra ematen du. Ondorioz, zatiketaren algoritmo orokortuaren funtzionamendua kontuan izanik, $\overline{S(f,g)}^{G_m} = 0$ ere lortzen dugu.

□

Aurreko teoremaren frogan, oso garrantzitsua izan da, G_i multzoaz zatitzean, polinomioak edozein modutan zerrenda ditzakegula. Hori praktikan ere oso lagungarria da. Adibidez, $S(f,g)$ polinomioa kalkulatu eta gero, konturatzen bagara $h \in G_i$ polinomio baten multiploa dela, orduan S-polinomio horrek ez du ekarpenik izango G_{i+1} multzoan: izan ere, $S(f,g)$ G_i-rekin zatitzeko orduan h lehenengo posizioan jartzen badugu, orduan zuzenean lortzen dugu zatiketaren hondarra 0 dela.

5.31. Adibidea. Gogoratu $\{Y - X^2, Z - X^3\}$ sistema sortzailea ez dela $\mathfrak{a} = (Y - X^2, Z - X^3)$ idealaren Gröbnerren oinarria lex ordenarekiko, $X > Y > Z$ hartuz gero. Aplika diezaiogun Burchbergerren algoritmoa sistema sortzaile horri, Gröbnerren oinarri bat lortzeko. Hasteko, jarri $f_1 = -X^2 + Y$ eta $f_2 = -X^3 + Z$ (ohartu polinomioen gaiak emandako ordena monomialarekiko ordenatu ditugula), eta jarri $G_1 = \{f_1, f_2\}$. Hauek dira eman behar diren pausoak (ez ditugu kalkuluak idatziko, errazak dira eta):

(P1) $S(f_1, f_2) = -Xf_1 + f_2 = -XY + Z$ eta $f_3 = \overline{S(f_1, f_2)}^{G_1} = -XY + Z$ dugu. Jarri $G_2 = \{f_1, f_2, f_3\}$.

(P2) $S(f_1, f_3) = -Yf_1 + Xf_3 = XZ - Y^2$ eta $f_4 = \overline{S(f_1, f_3)}^{G_2} = XZ - Y^2$ dugu. Beste alde batetik, $S(f_2, f_3) = -Yf_2 + X^2 f_3 = X^2 Z - YZ = -Zf_1$ denez, badakigu S-polinomio horren hondarra 0 izango dela. Jarri $G_3 = \{f_1, f_2, f_3, f_4\}$.

(P3) $S(f_1, f_4) = -Zf_1 - Xf_4 = XY^2 - YZ = -Yf_3$ denez, S-polinomio horretatik ez dugu ezer lortzen. Beste alde batetik, $S(f_2, f_4) = -Zf_2 - X^2 f_4 = X^2 Y^2 - Z^2$ dugu eta, zatiketa eginez, $f_5 = \overline{S(f_2, f_4)}^{G_3} = Y^3 - Z^2$. Azkenik, $S(f_3, f_4) = -Zf_3 - Yf_4 = Y^3 - Z^2$ eta $\overline{S(f_3, f_4)}^{G_3} = Y^3 - Z^2$ aurreko berbera da. Jarri $G_4 = \{f_1, f_2, f_3, f_4, f_5\}$.

(P4) $S(f_1, f_5) = -Y^3 f_1 - X^2 f_5 = X^2 Z^2 - Y^4$ eta $\overline{S(f_1, f_5)}^{G_4} = 0$ dugu. Era berean, $S(f_2, f_5) = -Y^3 f_2 - X^3 f_5 = X^3 Z^2 - Y^3 Z$ eta $\overline{S(f_2, f_5)}^{G_4} = 0$ dugu. Ohartu $S(f_3, f_5) = -Y^2 f_3 - Xf_5 = XZ^2 - Y^2 Z = Zf_4$ dela; beraz, S-polinomio hori ez dugu kontuan hartu behar. Bukatzeko, $S(f_4, f_5) = Y^3 f_4 - XZf_5 = XZ^3 - Y^5$ eta $\overline{S(f_4, f_5)}^{G_4} = 0$ dugu.

Azken pausoan S-polinomio guztien hondarra 0 denez, $G_5 = G_4$ dugu eta $G_4 = \{-X^2 + Y, -X^3 + Z, -XY + Z, XZ - Y^2, Y^3 - Z^2\}$ $\mathfrak{a}$-ren Gröbnerren oinarria da.

5.5. Gröbnerren oinarri minimalak eta laburtuak

Eman dugun azken adibideak erakusten duenez, Buchbergerren algoritmoa aplikatzen dugunean, lortzen dugun Gröbnerren oinarria hasierako sistema sortzailea baino askoz luzeagoa izan daiteke. Hala ere, batzuetan, polinomio batzuk ken ditzakegu, Gröbnerren oinarria izateko propietatea galdu gabe.

5.32. Lema. *Izan bedi G $\mathfrak{a}$-ren Gröbnerren oinarria. Demagun existitzen direla $g, h \in G$ desberdinak, non $\mathrm{LT}(g) \mid \mathrm{LT}(h)$ baita. Orduan, $G \setminus \{h\}$ ere $\mathfrak{a}$-ren Gröbnerren oinarria da.*

Froga. Izan bedi $f \in \mathfrak{a}$ ez-nulua. Orduan, nahikoa da $\mathrm{LT}(f)$ gai nagusia $G \setminus \{h\}$-ko polinomio baten gai nagusiaz zatigarria dela ikustea, 5.21 teoremaren arabera. Kontuan hartzen badugu G $\mathfrak{a}$-ren Gröbnerren oinarria dela, badakigu existitzen dela $q \in G$, non $\mathrm{LT}(q) \mid \mathrm{LT}(f)$ baita. Orain bi aukera daude:

(i) $q \in G \setminus \{h\}$.

(ii) $q = h$. Orduan, $\mathrm{LT}(g) \mid \mathrm{LT}(h) \mid \mathrm{LT}(f)$ dugu, eta $g \in G \setminus \{h\}$.

Edozein kasutan, nahi genuen emaitza betetzen da. □

Esate baterako, 5.31 adibidean, $\{-X^2+Y, -X^3+Z, -XY+Z, XZ-Y^2, Y^3-Z^2\}$ Gröbnerren oinarria lortu dugu (lex ordenarekin, $X > Y > Z$ harturik), eta konturatzen gara $-X^2+Y$ polinomiaren gai nagusiak $-X^3+Z$-rena zatitzen duela. Azken lemaren arabera, $-X^3+Z$ polinomioa ezaba dezakegu eta $\{-X^2+Y, -XY+Z, XZ-Y^2, Y^3-Z^2\}$ ere emandako idealaren Gröbnerren oinarria da.

Jarraian ikusten dugunez, Gröbnerren oinarririk txikienak lortzeko, nahikoa da aurreko lema behin eta berriz aplikatzea.

5.33. Definizioa. Izan bitez $\mathfrak{a}$ polinomioen ideal ez-nulua eta G $\mathfrak{a}$-ren Gröbnerren oinarria. Orduan, G $\mathfrak{a}$-ren *Gröbnerren oinarri minimala* dela esango dugu, G-ren azpimultzo propioen artean ez badago $\mathfrak{a}$-ren Gröbnerren oinarririk.

Beste testuliburu batzuetan, Gröbnerren oinarri minimalaren definizioan, polinomio guztien koefiziente nagusia 1 izateko eskatzen da. Hala ere, guk ez dugu baldintza hori exijituko.

Hurrengo teoremak dioenez, begirada soil batekin jakin dezakegu Gröbnerren oinarri bat minimala den edo ez.

5.34. Teorema. *Izan bedi $G = \{g_1, \ldots, g_t\}$ $\mathfrak{a}$-ren Gröbnerren oinarria. Orduan, G Gröbnerren oinarri minimala da baldin eta soilik baldin propietate hau betetzen badu: $g_i, g_j \in G$ desberdinak badira, orduan $\mathrm{LT}(g_i)$-k ez du $\mathrm{LT}(g_j)$ zatitzen.*

Froga. Izan bedi G Gröbnerren oinarri minimala, eta demagun existitzen direla $g_i, g_j \in G$ desberdinak, non $\mathrm{LT}(g_i) \mid \mathrm{LT}(g_j)$ baita. Orduan, 5.32 lemaren arabera, $G \setminus \{g_j\}$ ere $\mathfrak{a}$-ren Gröbnerren oinarria da. Hori ezinezkoa da, G oinarri minimala izateagatik. Beraz, $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$ dugu $i \neq j$ guztietarako.

Orain, frogatu dezagun alderantzizko inplikazioa. Demagun G-ko polinomioen gai nagusiek enuntziatuko propietatea betetzen dutela, eta ikus dezagun G oinarri minimala dela. Horrela ez balitz, G oinarriari g_j polinomio bat ken geniezaioke, eta oraindik ere Gröbnerren oinarri bat izango genuke. Baina, orduan, 5.21 teoremaren arabera, existituko litzateke $g_i \in G \setminus \{g_j\}$, non $\mathrm{LT}(g_i) \mid \mathrm{LT}(g_j)$ baita. Hori hipotesiaren kontra doa. □

Beraz, $\{-X^2+Y, -XY+Z, XZ-Y^2, Y^3-Z^2\}$ multzoa $\mathfrak{a} = (Y-X^2, Z-X^3)$ idealaren Gröbnerren oinarri minimala da lex ordenarekiko, $X > Y > Z$ harturik.

Polinomioen ideal baten G Gröbnerren oinarri bat ez bada minimala, garbi dago G-ren barruan oinarri minimal bat topa dezakegula: nahikoa da, Gröbnerren oinarriak diren G-ren azpimultzoen artean, elementu kopururik txikiena duen bat aukeratzea. Aurreko teoremak metodo azkarrago bat ematen digu oinarri minimal hori lortzeko. Izan ere, G ez bada Gröbnerren oinarria, $h \in G$ polinomio baten gai nagusia $g \in G$ beste baten gai nagusiaz zatigarria da, eta h G-tik ken dezakegu, oraindik ere Gröbnerren oinarri bat izanik. Prozedura hori behin eta berriz errepikatuz, joango gara polinomioak banan-banan kenduz, gai nagusien arteko zatigarritasun guztiak ezabatu arte. Orduan, gelditzen zaizkigun polinomioek Gröbnerren oinarri minimal bat osatuko dute.

5.35. Teorema. *Izan bedi G $\mathfrak{a}$-ren Gröbnerren oinarri minimala. Orduan, G' $\mathfrak{a}$-ren Gröbnerren beste oinarri bat bada (ordena monomial berarekiko), baliokideak dira:*

(i) *G' ere Gröbnerren oinarri minimala da.*
(ii) $|G'| = |G|$.

Froga. (i) $\Rightarrow$ (ii). Kasu honetan, G eta G' oinarri minimalak dira eta, egoeraren simetriagatik, $|G| = |G'|$ dela frogatzeko, nahikoa da $|G| \leq |G'|$ desberdintza ikustea. Gogoratu, G' Gröbnerren oinarria izateagatik, $g \in G$ bakoitzerako existitzen dela $g' \in G'$, non $\mathrm{LT}(g') \mid \mathrm{LT}(g)$ baita. Ikusten badugu $g, h \in G$ bi elementu desberdini $g', h' \in G'$ desberdinak dagozkiela, orduan $|G| \leq |G'|$ lortuko dugu zuzenean. Absurdora eramanez, demagun $g' = h'$ dela. Orain, G Gröbnerren oinarria dela erabiliz, badago $f \in G$, non $\mathrm{LT}(f) \mid \mathrm{LT}(g') = \mathrm{LT}(h')$ baita. Ondorioz, $\mathrm{LT}(f)$-k bai $\mathrm{LT}(g)$ bai $\mathrm{LT}(h)$ zatitzen ditu. Kontuan hartzen badugu g eta h desberdinak direla, $f \neq g$ edo $f \neq h$ izan beharko dugu. Beraz, G-ko polinomio baten gai nagusiak G-ko beste polinomio baten gai nagusia zatitzen du. Baina, 5.34 teoremaren arabera, hori ezinezkoa da, G oinarri minimala da eta.

(ii) $\Rightarrow$ (i). Badakigu G'-en barruan G'' oinarri minimal bat aurki dezakegula. Ikus dezagun $G' = G''$ dela. Horretarako, ohartu $|G''| = |G|$ dugula, (i) atalaren arabera, eta $|G'| = |G|$ dela, hipotesiaren arabera. Ondorioz, $|G''| = |G'|$ dugu, eta G'' G'-en azpimultzoa denez, $G'' = G'$ dela ondorioztatzen dugu. □

Beraz, polinomioen ideal baten Gröbnerren oinarri minimal guztiek elementu kopuru bera dute (ordena monomial berarekiko hartzen baditugu, jakina). Adibidez, lex ordenarekiko, $X > Y > Z$ harturik, $\mathfrak{a} = (Y - X^2, Z - X^3)$ idealaren Gröbnerren oinarri guztiek launa elementu dituzte gutxienez, $\mathfrak{a}$ bi polinomiorekin sor daitekeen arren.

Ordena monomial desberdinak erabiliz gero, oinarri minimalek elementu kopuru desberdinak izan ditzakete. Aurretik ikusi dugun bezala, $\{Y-X^2, Z-X^3\}$ multzoa $\mathfrak{a} = (Y-X^2, Z-X^3)$ idealaren Gröbnerren oinarria da lex ordenarekiko, $Z > Y >$

X harturik. Garbi dago, gainera, oinarri minimala dela. Hala ere, 2 elementu baino ez ditu, eta ez 4, lex ordena $X > Y > Z$ jarrita hartzen dugun kasuan bezala.

Garrantzitsua da azpimarratzea polinomioen ideal batek ez duela, oro har, Gröbnerren oinarri minimal bakar bat (ordena monomiala finkatu eta gero), nahiz eta oinarriko polinomioei monikoak izateko eskatu. Adibide bat emateko, ondorengo lema lagungarria da.

5.36. Lema. *Izan bedi G $\mathfrak{a}$-ren Gröbnerren oinarria, eta demagun $G' \subseteq \mathfrak{a}$ multzoak $\mathrm{LM}(G') = \mathrm{LM}(G)$ betetzen duela. (Hori beteko da, bereziki, $\mathrm{LT}(G') = \mathrm{LT}(G)$ bada.) Orduan, G' ere $\mathfrak{a}$-ren Gröbnerren oinarria da.*

Froga. Izan bedi $f \in \mathfrak{a}$ ez-nulua. Orduan, G $\mathfrak{a}$-ren Gröbnerren oinarria izateagatik, existitzen da $g \in G$, non $\mathrm{LT}(g) \mid \mathrm{LT}(f)$ baita. Orain, $\mathrm{LM}(G) = \mathrm{LM}(G')$ baldintza betetzen denez, badago $g' \in G'$, non $\mathrm{LM}(g') = \mathrm{LM}(g)$ baita. Beraz, $\mathrm{LT}(g')$-en eta $\mathrm{LT}(g)$-ren arteko diferentzia bakarra faktore konstante ez-nulu bat da. Horrenbestez, $\mathrm{LT}(g') \mid \mathrm{LT}(f)$ dugu eta, 5.21 teoremaren arabera, G' ere $\mathfrak{a}$-ren Gröbnerren oinarria da. □

Adibidez, hartu lex ordena, $Z > Y > X$ izanik, eta jarri $\mathfrak{a} = (Y - X^2, Z - X^3)$. Badakigunez, $G = \{Y - X^2, Z - X^3\}$ $\mathfrak{a}$-ren Gröbnerren oinarri minimala da. Kentzen badiogu G-ko bigarren polinomioari lehenengoa bider X, orduan $G' = \{Y - X^2, Z - XY\}$ multzo berria lortzen dugu. Azken lemaren arabera, G' $\mathfrak{a}$-ren Gröbnerren oinarria da, $G' \subseteq \mathfrak{a}$ eta $\mathrm{LT}(G') = \mathrm{LT}(G)$ delako (bigarren polinomioa aldatu dugu, baina haren gai nagusia, ez). Gainera, G' oinarri minimala da, 2 elementu baititu, G oinarri minimalak beste.

Gai hau bukatzeko, Gröbnerren oinarrien artean mota bat bereiziko dugu, oinarri laburtuak. Ikusiko dugunez, ideal bakoitzak oinarri laburtu bakarra izango du, oinarri minimalekin gertatzen den ez bezala.

5.37. Definizioa. Izan bitez $\mathfrak{a}$ polinomioen ideal ez-nulua eta G $\mathfrak{a}$-ren Gröbnerren oinarria. Orduan, G $\mathfrak{a}$-ren *Gröbnerren oinarri laburtua* dela esango dugu, bi baldintza hauek betetzen badira:

(i) $h \in G$ edozein harturik, h-ren gai bat ere ez da $\mathrm{LT}(g)$ gai nagusi batez zatigarria, $g \in G$ eta $g \neq h$ izanik.
(ii) G-ko polinomio guztien koefiziente nagusia 1 da.

Garbi dago oinarri laburtuak minimalak direla, bereziki. Izan ere, polinomioen koefiziente nagusien gaineko baldintza alde batera utzirik, hau da oinarri minimal baten eta oinarri laburtu baten arteko diferentzia: lehenengo kasuan, bakarrik eskatzen dugu h-ren gai nagusia ez izatea zatigarria g beste polinomio baten gai nagusiaz; bigarrenean, berriz, h-ren gai guztiek bete behar dute baldintza hori.

5.38. Adibidea. Har dezagun lex ordena monomiala $\mathrm{Mon}(X, Y, Z)$ multzoan, $Z > Y > X$ izanik. Lehenago ikusi dugun bezala, $G = \{Y - X^2, Z - X^3\}$ eta

$G' = \{Y - X^2, Z - XY\}$ multzoak $\mathfrak{a} = (Y - X^2, Z - X^3)$ idealaren Gröbnerren oinarri minimalak dira. Orain, G laburtua da, eta G' ez da: ohartu $Z - XY$ polinomioan, $-XY$ gaia $Y - X^2$ beste polinomioaren gai nagusiaz zatigarria dela.

Orain, galdera batzuk sortzen zaizkigu. Ba al dute polinomioen ideal ez-nulu guztiek Gröbnerren oinarri laburturik? Hala bada, zein modutan lor dezakegu oinarri laburtu bat? Erantzuna hurrengo teoreman ematen dugu.

5.39. Lema. *Izan bitez G eta G' $\mathfrak{a}$-ren Gröbnerren bi oinarri minimal, ordena monomial berarekiko. Orduan,* $\mathrm{LM}(G) = \mathrm{LM}(G')$ *dugu.*

Froga. Simetriagatik, nahikoa da $\mathrm{LM}(G) \subseteq \mathrm{LM}(G')$ partekotasuna frogatzea. Izan bedi $g \in G$ edozein. Orduan, $g \in \mathfrak{a}$ denez eta G' $\mathfrak{a}$-ren Gröbnerren oinarria denez, existitzen da $g' \in G'$, non $\mathrm{LM}(g') \mid \mathrm{LM}(g)$ baita. Argudio hori alderantziz aplikatuz, existitzen da $h \in G$, non $\mathrm{LM}(h) \mid \mathrm{LM}(g')$ baita. Baina, orduan, $\mathrm{LM}(h) \mid \mathrm{LM}(g)$ ondorioztatzen dugu eta, G oinarri minimala denez, hori gertatzeko posibilitate bakarra $h = g$ izatea da. Beraz, $\mathrm{LM}(g)$ eta $\mathrm{LM}(g')$ monomioek elkar zatitzen dute eta, hortaz, $\mathrm{LM}(g) = \mathrm{LM}(g')$ dugu. □

5.40. Teorema. *Izan bedi $\mathfrak{a}$ polinomioen ideal ez-nulua. Orduan, $\mathfrak{a}$-k Gröbnerren oinarri laburtu bakar bat du ordena monomial bakoitzeko. Gainera, $G = \{g_1, \ldots, g_t\}$ $\mathfrak{a}$-ren Gröbnerren oinarri minimala bada, eta g_i' bada g_i polinomioa $G \setminus \{g_i\}$-rekin zatitzeko hondarra (polinomio horiek edozein modutan zerrendaturik), orduan $G' = \{g_1', \ldots, g_t'\}$ $\mathfrak{a}$-ren Gröbnerren oinarri laburtua da.*

Froga. Lehenengo eta behin, ikus dezagun G' oinarri laburtua dela. Hasteko, G' $\mathfrak{a}$-ren Gröbnerren oinarria dela frogatuko dugu. Kontuan izanik $G' \subseteq \mathfrak{a}$ dela, nahikoa dugu ikustea $\mathrm{LT}(g_i') = \mathrm{LT}(g_i)$ dela $i = 1, \ldots, t$ guztietarako. Ohartu $\mathrm{LT}(g_i)$ ez dela $\mathrm{LT}(g_j)$-z zatigarria $i \neq j$ denean, G oinarri minimala izateagatik. Hori dela eta, g_i polinomioa $G \setminus \{g_i\}$ multzoaz zatitzen dugunean, $\mathrm{LT}(g_i)$ koefiziente nagusia g_i' hondarrera doa zuzenean. Beraz, $\mathrm{LT}(g_i') = \mathrm{LT}(g_i)$ dugu, eta G $\mathfrak{a}$-ren Gröbnerren oinarria da. Orain, absurdora eramanez, demagun G' ez dela laburtua. Orduan, existituko da g_i' polinomio bat, halakoa non g_i'-en gaietako bat g_j' beste polinomio baten gai nagusiaz zatigarria baita. Baina, $\mathrm{LT}(g_j') = \mathrm{LT}(g_j)$ denez, g_i'-en gai hori $\mathrm{LT}(g_j)$-z zatigarria da. Gogoratu zatiketaren algoritmo orokortuan hondarrak ezaugarri hau duela: bere gaietako bat ere ez dela zatitzaileen gai nagusiez zatigarria. Gure kasuan, g_i' hondarra ematen duen zatiketan, g_j zatitzaileen artean agertzen da. Beraz, $\mathrm{LT}(g_j)$-k ezin du g_i'-en gai bat ere zatitu. Kontraesan horrek G' oinarri laburtua dela frogatzen du.

Frogatu dezagun orain oinarri laburtu bakarra dagoela. Hartzen baditugu G_1 eta G_2 bi oinarri laburtu, orduan, simetriagatik, nahikoa da $g_1 \in G_1$ polinomio bakoitza G_2-n ere badagoela ikustea. Badakigu, 5.39 lema aplikatuz, $\mathrm{LM}(G_1) = \mathrm{LM}(G_2)$ dugula. Beraz, badago $g_2 \in G_2$, non $\mathrm{LM}(g_1) = \mathrm{LM}(g_2)$ baita. Kontuan izanik g_1-en eta g_2-ren koefiziente nagusiak 1 direla, horrek esan nahi du $\mathrm{LT}(g_1) = \mathrm{LT}(g_2)$ dela. Ikus dezagun $g_1 = g_2$ dela. Horretarako, zatitu dezagun $g_1 - g_2$

kendura G_1-ekin. Alde batetik, badakigu zatiketaren hondarra 0 dela, $g_1 - g_2 \in \mathfrak{a}$ izateagatik eta G_1 $\mathfrak{a}$-ren Gröbnerren oinarria izateagatik. Beste alde batetik, $g_1 - g_2$ egitean g_1-en eta g_2-ren gai nagusiak elkarrekin deuseztatzen dira. Beraz, $g_1 - g_2$-ren monomio bat g_1-en monomio batekin edo g_2-ren monomio batekin bat dator, baina ez monomio nagusiekin bat. Horregatik, eta G_1 eta G_2 oinarri laburtuak direlako eta $\mathrm{LM}(G_1) = \mathrm{LM}(G_2)$ delako, $g_1 - g_2$ kendura G_1-ekin zatitzean, gai guztiak hondarrera doaz. Hori dela eta, zatiketaren hondarra $g_1 - g_2$ bera da. Ondorioz, $g_1 - g_2 = 0$ dugu, eta $g_1 = g_2 \in G_2$, nahi bezala. □

5.41. Adibidea. Aurretik esan dugu $G = \{Y - X^2, Z - XY\}$ multzoa $\mathfrak{a} = (Y - X^2, Z - X^3)$-ren Gröbnerren oinarri minimala dela, baina ez laburtua, lex ordena monomiala hartzen badugu, $Z > Y > X$ izanik. Eman dezagun $\mathfrak{a}$-ren oinarri laburtu bat, azken teoremako metodoa G oinarriari aplikatuz. Horretarako, $Y - X^2$ polinomioa $Z - XY$-rekin eta $Z - XY$ polinomioa $Y - X^2$-rekin zatitu behar ditugu, eta hondarrekin gelditu behar dugu. Horrela, $\{Y - X^2, Z - X^3\}$ oinarri laburtua lortzen dugu. Bagenekien hori $\mathfrak{a}$-ren oinarri laburtua dela, eta ezin genuen beste emaitzarik lortu, $\mathfrak{a}$-k oinarri laburtu bakarra du eta.

Gröbnerren oinarri batetik oinarri minimal bat lortu nahi badugu, ikusten dugunean oinarriko polinomio baten gai nagusia beste baten gai nagusiaz zatigarria dela, lehenengo polinomio hori oinarritik kentzen dugu. Oinarri minimaletik laburtua atera nahi badugu, ordea, oinarriko polinomio baten edozein gai beste polinomio baten gai nagusiaz zatigarria bada, orduan gai hori desagertzea lor dezakegu, baina ez gai hori besterik gabe ezabatuz, baizik eta polinomio hori oinarriko besteez zatituz. Azaldu dezagun hori azken adibidea erabiliz. Horretan, $G = \{Y - X^2, Z - XY\}$ $\mathfrak{a}$-ren oinarri minimala da. Konturatzen garenean $Z - XY$ polinomioaren $-XY$ gaia $Y - X^2$-ren gai nagusiaz zatigarria dela, ez da zuzena $-XY$ besterik gabe ezabatzea eta $\{Y - X^2, Z\}$ oinarri laburtua dela esatea. Izan ere, azken multzoa ezin da inola ere $\mathfrak{a}$-ren Gröbnerren oinarria izan, Z polinomioa ez baitago $\mathfrak{a}$-ren barruan. (Hori ikusteko, nahikoa da Z G-rekin zatitzea eta ikustea hondarra $X^3 \neq 0$ dela.)