Ariketak

5.1. Erabaki ondorengo ordena-erlazioak ordena monomialak diren $\mathrm{Mon}(X_1, \dots, X_n)$ multzoaren gainean. Baiezkoan, ikusi ea dagoeneko ezagutzen ditugun ordena monomialetako bat den.

(i) $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$ baldin eta soilik baldin $\boldsymbol{\alpha}-\boldsymbol{\beta}$-ren lehenengo koordenatu ez-nulua, eskuinaldetik hasita, positiboa bada.

(ii) $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$ baldin eta soilik baldin $\boldsymbol{\alpha}-\boldsymbol{\beta}$-ren lehenengo koordenatu ez-nulua, eskuinaldetik hasita, negatiboa bada. (Ordena horri revlex dei diezaiokegu. Zergatik?)

(iii) $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$ baldin eta soilik baldin $\boldsymbol{\alpha}-\boldsymbol{\beta}$-ren koordenatu guztiak ez-negatiboak badira, eta gutxienez horietariko bat positiboa bada. (Monomioekin pentsatuta, ohartu zatigarritasun-ordena dela.)

(iv) Emanda $\boldsymbol{\gamma}$ bektore finkoa, koordenatu osoak eta ez-negatiboak dituena, $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$ baldin eta soilik baldin $\boldsymbol{\gamma}\cdot\boldsymbol{\alpha} > \boldsymbol{\gamma}\cdot\boldsymbol{\beta}$ bada edo, bestela, $\boldsymbol{\gamma}\cdot\boldsymbol{\alpha} = \boldsymbol{\gamma}\cdot\boldsymbol{\beta}$ eta $\boldsymbol{X}^{\boldsymbol{\alpha}} >_{\mathrm{lex}} \boldsymbol{X}^{\boldsymbol{\beta}}$ bada. (Hemen $\boldsymbol{\gamma}\cdot\boldsymbol{\alpha}$-ren esanahia $\boldsymbol{\gamma}$ eta $\boldsymbol{\alpha}$ bektoreen ohiko biderkadura eskalarra da.)

5.2. Frogatu ordena lexikografikoa, indeterminatuak $X_1 > X_2 > \cdots > X_n$ ordenatuta, ondorengo propietatearen bidez karakteriza daitekeela: $f \in K[X_1, \dots, X_n]$ polinomiak $\mathrm{LT}(f) \in K[X_\ell, \dots, X_n]$ betetzen badu, $1 \leq \ell \leq n$ izanik, orduan $f \in K[X_\ell, \dots, X_n]$ dugu. (Beraz, alde batetik, lex ordenak propietate hori betetzen duela ikusi behar da, eta bestetik, ordena batek propietate hori betetzen badu, lex ordena dela.)

5.3. Frogatu ondorengo baieztapenak:

(i) Edozein ordena monomialekin, $\mathrm{LT}(f)$ konstantea bada, orduan f ere konstantea da.

(ii) Edozein ordena monomialekin, $\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{X}^{\boldsymbol{\beta}}$ zatigarritasun-baldintza betetzen bada, orduan $\boldsymbol{X}^{\boldsymbol{\alpha}} \leq \boldsymbol{X}^{\boldsymbol{\beta}}$ dugu. Egia al da alderantzizkoa?

(iii) Baldin eta $\mathfrak{a}$ $K[X_1, \dots, X_n]$-ren ideala bada, orduan $\mathfrak{a}$ ideal monomiala da baldin eta soilik baldin $\mathfrak{a} = (\mathrm{LT}(\mathfrak{a}))$ bada.

(iv) Ideal nagusi batean, Gröbnerren oinarri minimalak elementu bakar bateko sistema sortzaileak dira.

5.4. Izan bedi $\mathfrak{a}$ $K[X_1, \dots, X_n]$-ren ideala.

(i) Demagun lehenengo $\mathfrak{a}$ ideal monomiala dela. Izan bedi G $\mathfrak{a}$-ren sistema sortzailea, monomioek osatua. Frogatu G $\mathfrak{a}$-ren Gröbnerren oinarria dela $K[X_1, \dots, X_n]$-ren edozein ordena monomialekiko. Gainera, G Gröbnerren oinarri minimala da (izan ere, laburtua) baldin eta soilik baldin $\boldsymbol{X}^{\boldsymbol{\alpha}} \nmid \boldsymbol{X}^{\boldsymbol{\beta}}$ bada $\boldsymbol{X}^{\boldsymbol{\alpha}}, \boldsymbol{X}^{\boldsymbol{\beta}} \in G$ monomio desberdin guztietarako. Beraz, $\mathfrak{a}$-k Gröbnerren oinarri laburtu bera dauka ordena monomial guztietarako.

(ii) Alderantziz, $\mathfrak{a}$-ren Gröbnerren oinarri laburtuak bat badatoz $K[X_1, \ldots, X_n]$-ren ordena monomial guztietarako, izan behar du $\mathfrak{a}$-k ideal monomiala? (Kontuan izan aurreko ariketaren (iv) atala.)

(iii) Izan bedi $d \in \mathbb{N}$ finkoa. Definitu

$$\mathfrak{a} = \{f \in K[X_1, \ldots, X_n] \mid f \text{ osatzen duten monomio guztien maila osoa} \geq d \text{ da}\}.$$

Frogatu $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideal monomiala dela eta eman $\mathfrak{a}$-ren Gröbnerren oinarri laburtua.

5.5. Izan bitez $\mathfrak{a}$ ideal monomiala eta $\{\boldsymbol{X}^{\boldsymbol{\alpha_1}}, \ldots, \boldsymbol{X}^{\boldsymbol{\alpha_r}}\}$ $\mathfrak{a}$-ren Gröbnerren oinarri laburtua.

(i) Erabil dezagun notazio hau: A matrizearen elementuak $K[X_1, \ldots, X_n]$-ko polinomioak badira, orduan polinomio bakoitza bere gai askearekin ordezkatuz lortzen den matrizea $\widetilde{A}$ ikurraz adieraziko dugu. (Beraz, $\widetilde{A}$-ren elementuak K gorputzean daude. Ohartu $A \mapsto \widetilde{A}$ aplikazioa eraztun-homomorfismoa dela.) Baldin eta $(\boldsymbol{X}^{\boldsymbol{\alpha_1}} \ \ldots \ \boldsymbol{X}^{\boldsymbol{\alpha_r}})A = (\boldsymbol{X}^{\boldsymbol{\alpha_1}} \ \ldots \ \boldsymbol{X}^{\boldsymbol{\alpha_r}})$ bada, frogatu $\widetilde{A} = I_r$ dela.

(ii) Demagun orain $\mathfrak{a} = (f_1, \ldots, f_s)$ dugula, f_i guztiak polinomioak izanik, ez derrigorrean monomioak. Frogatu $s \geq r$ dela. (Iradokizuna: Badaude P eta Q matrizeak $K[X_1, \ldots, X_n]$-ren gainean, $r \times s$ eta $s \times r$ tamainakoak, halakoak non $(\boldsymbol{X}^{\boldsymbol{\alpha_1}} \ \ldots \ \boldsymbol{X}^{\boldsymbol{\alpha_r}})P = (f_1 \ \ldots \ f_s)$ eta $(f_1 \ \ldots \ f_s)Q = (\boldsymbol{X}^{\boldsymbol{\alpha_1}} \ \ldots \ \boldsymbol{X}^{\boldsymbol{\alpha_r}})$ baita. Aplikatu orduan (i) atala.) Beraz, ideal monomial baten sortzaile-kopuru minimoa monomioak diren sortzaileak aukeratuz lortzen da, eta kopuru hori bat dator Gröbnerren oinarri laburtuaren kardinalarekin.

(iii) Aurreko ariketa erabiliz, ondorioztatu $r \in \mathbb{N}$ guztietarako existitzen direla r sortzaile behar dituzten idealak $K[X, Y]$ eraztunaren barruan. Horrek erakusten du ez dela posible Hilberten oinarriaren teoremaren bertsio kuantitatibo bat ematea, $K[X_1, \ldots, X_n]$-ren ideal guztien sortzaile-kopuru minimoa n-ren funtzioan bornatzen duena.

(iv) Buchbergerren algoritmoa erabiliz, kalkulatu $\mathfrak{b} = (X^2 + Y^2, X^3)$ idealaren Gröbnerren oinarri laburtua ordena lexikografikoarekiko, $X > Y$ hartuta. Ondorioztatu ideal ez-monomialen kasuan ezin dela ziurtatu Gröbnerren oinarri laburtu baten kardinala idealaren sortzaile kopuru minimoarekin bat datorrenik.

5.6. Izan bitez $\mathfrak{a} = (\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A)$ eta $\mathfrak{b} = (\boldsymbol{X}^{\boldsymbol{\beta}} \mid \boldsymbol{\beta} \in B)$ $K[X_1, \ldots, X_n]$-ren ideal monomialak. Frogatu $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$ eta $\mathfrak{a}\mathfrak{b}$ ere ideal monomialak direla, eta eman ideal horiek sortzen dituzten monomioak $\mathfrak{a}$-ren eta $\mathfrak{b}$-ren sortzaileak erabiliz. Noiz datoz bat $\mathfrak{a} \cap \mathfrak{b}$ eta $\mathfrak{a}\mathfrak{b}$?

5.7. Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideala eta demagun $\{f_1, \ldots, f_s\}$ $\mathfrak{a}$-ren sistema sortzailea dela, baina ez Gröbnerren oinarria (emandako ordena monomial batekiko). Frogatu badagoela $f \in \mathfrak{a}$ polinomio bat, hondar ez-nulua ematen duena $f_1, \ldots, f_s$-rekin zatitzean, polinomio horiek edozein modutan zerrendatuta ere. (Laguntza: Erabili Gröbnerren oinarriaren definizioa.)

5.8. Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideala.

(i) Demagun $G \subseteq \mathfrak{a}$ multzoak ondorengo propietatea betetzen duela: $f \in \mathfrak{a}$ guztiek 0 hondarra ematen dute G-rekin zatitzean (G-ko polinomioak ordena finko batean zerrendatu eta gero). Frogatu G $\mathfrak{a}$-ren Gröbnerren oinarria dela. (Egia esan, hori Buchbergerren irizpidearen ondorio zuzena da. Eman, hala ere, emaitza horren beste froga bat, Gröbnerren oinarriaren definizioan oinarrituta.)

(ii) Izan bitez G eta G' $\mathfrak{a}$-ren Gröbnerren bi oinarri, ordena monomial bera erabilita. Frogatu $\overline{f}^G = \overline{f}^{G'}$ dela $f \in K[X_1, \ldots, X_n]$ guztietarako.

5.9. Bigarren gaiko 2.6 ariketan, $K[X, Y]/(f(X, Y))$ moduko zatidura eraztun baten oinarri bat eta dimentsioa lortu ditugu. Problema honetan gure asmoa da emaitza hori $K[X_1, \ldots, X_n]$-ren zatidura eraztun guztietara hedatzea.

(i) Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_n]$-ren ideala. Frogatu $\mathrm{Mon}(X_1, \ldots, X_n) \setminus \mathrm{LM}(\mathfrak{a})$ multzoko monomioen koklaseek $K[X_1, \ldots, X_n]/\mathfrak{a}$ zatiduraren K-oinarri bat osatzen dutela. Ondorioztatu nola erabil daitekeen $\mathfrak{a}$-ren Gröbnerren oinarri bat $K[X_1, \ldots, X_n]/\mathfrak{a}$-ren K-oinarri bat lortzeko.

(ii) Aurkitu ondorengo zatiduren K-oinarriak, eta eman beren dimentsioa, finitua izanez gero (ohartu ordena monomial desberdinak erabiliz K-oinarri desberdinak lor daitezkeela):
   (a) $K[X, Y]/(X^2, Y^2)$.
   (b) $K[X, Y]/(X^2Y, XY^2)$.
   (c) $K[X, Y, Z]/(X^3 + Y^2, Y^3 + Z^2, Z^3 + X^2)$.
   (d) $K[X, Y, Z]/(X + YZ, Y + XZ, Z + XY)$.

(iii) Indeterminatu bakar baten kasuan, $g \in K[X]$ edozein polinomio izanik, badakigu nola adierazi $\overline{g} \in K[X]/(f(X))$ koklasea $\{\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}\}$ K-oinarriaren elementuen konbinazio lineal gisa. Nahikoa da g f-z zatitzea eta zatiketaren r hondarra hartzea; orduan, $\overline{g} = \overline{r}$ dugu. Esan nola ebatz daitekeen problema hori $K[X_1, \ldots, X_n]/\mathfrak{a}$ zatidura orokor baten kasuan. Baldin eta $g(X, Y, Z) = X^3 + Y^3 + Z^3$ bada, aurreko ataleko (c) eta (d) kasuetan, deskonposatu $\overline{g}$ elementua $K[X, Y, Z]/\mathfrak{a}$ zatiduran, lortutako K-oinarriarekiko.

5.10. $K[X, Y, Z]$-ren ondorengo idealetarako, erabaki emandako sortzaileek Gröbnerren oinarri bat osatzen duten lex, grlex eta grevlex ordena monomialekiko, hurrenez hurren, betiere $X > Y > Z$ harturik.

(i) $(X^2 + Z^2, Y + Z^2)$.
(ii) $(X^2 + Z^2, X + YZ)$.
(iii) $(X^2 + Z^2, XZ + Y^2)$.
(iv) $(Y + Z^2, XZ + Y^2)$.
(v) $(Y^3, XZ + Y^2)$.
(vi) $(X^2 + Y^3, XZ + Y^2)$.

Kasu guztietan, aurkitu ideal horien Gröbnerren oinarri laburtu bana aipatutako ordena monomialekiko.

5.11. Ariketa honetan 5.5 problemaren (iv) ataleko emaitza orokortzen dugu. Izan bedi $\mathfrak{a} = (X^n + Y^n, X^m)$, $m > n > 1$ izanik. Frogatu $\mathfrak{a}$-ren Gröbnerren oinarri

laburtuek hiruna elementu dutela $X > Y$ betetzen duten ordena monomial guztiekiko. Zer gertatzen da $m \leq n$ bada? Eta $Y > X$ hartuz gero?

5.12. Erabaki baieztapen hau egiazkoa den edo ez: "Izan bitez $f, f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, eta demagun f-ren gai guztiak $\mathrm{LT}(f_i)$-ren batez zatigarriak direla (aldez aurretik finkatutako ordena monomial batekiko). Zatiketaren algoritmoa jarraitzen badugu f polinomioa $f_1, \ldots, f_s$-rekin zatitzeko, orduan zero hondarra lortzen da beti, $f_1, \ldots, f_s$ edozein modutan zerrendatuta ere."

5.13. Problema honetan ikusten dugu batzuetan "bisualki" jakin daitekeela emandako sistema sortzaile bat ideal baten Gröbnerren oinarria den edo ez, inolako kalkulurik egin gabe. Ondorengo ataletan, ordena monomial finko batekin lan egiten dugu.

(i) Izan bedi $\mathfrak{a} = (f, g)$ $K[X_1, \ldots, X_n]$-ren ideala eta demagun $\mathrm{LT}(f)$ eta $\mathrm{LT}(g)$ monomioak elkarrekiko lehenak direla. Frogatu $\{f, g\}$ $\mathfrak{a}$-ren Gröbnerren oinarria dela. (Iradokizuna: Izan bedi $h \in \mathfrak{a}$, $h \neq 0$, eta demagun, absurdora eramanez, $\mathrm{LT}(f)$-k eta $\mathrm{LT}(g)$-k ez dutela $\mathrm{LT}(h)$ zatitzen. Idatzi $h = \alpha f + \beta g$, eta aukera ditzagun α eta β polinomioak $\mathrm{multideg}\,\alpha + \mathrm{multideg}\,\beta$ minimoa den moduan. Ikusi $\mathrm{LT}(\alpha)\mathrm{LT}(f) + \mathrm{LT}(\beta)\mathrm{LT}(g) = 0$ dela, eta ondorioztatu existitzen dela γ gai bat, non $\mathrm{LT}(\alpha) = \gamma\mathrm{LT}(g)$ eta $\mathrm{LT}(\beta) = -\gamma\mathrm{LT}(f)$ baita. Jarri $\widetilde{\alpha} = \alpha - \gamma g$ eta $\widetilde{\beta} = \beta + \gamma f$. Orduan $h = \widetilde{\alpha} f + \widetilde{\beta} g$ dugu, eta hori kontraesan bat da.)

(ii) Oro har, $\mathfrak{a} = (g_1, \ldots, g_t)$ bada, $(\mathrm{LT}(g_i), \mathrm{LT}(g_j)) = 1$ izanik $i \neq j$ guztietarako, egokitu aurreko ataleko argudioa $\{g_1, \ldots, g_t\}$ $\mathfrak{a}$-ren Gröbnerren oinarria dela frogatzeko. (Horrela argudiatuz, $h = \alpha_1 g_1 + \cdots + \alpha_r g_r + \alpha_{r+1} g_{r+1} + \cdots + \alpha_t g_t \in \mathfrak{a}$ polinomio bat lortuko dugu, baldintza hauek betetzen dituena: $\mathrm{LT}(h)$ ez da $\mathrm{LT}(g_i)$ batez ere zatigarria, $\sum_{i=1}^{t} \mathrm{multideg}(\alpha_i)$ minimoa da,

$$\mathrm{LM}(\alpha_1 g_1) = \cdots = \mathrm{LM}(\alpha_r g_r) > \mathrm{LM}(\alpha_{r+1} g_{r+1}), \ldots, \mathrm{LM}(\alpha_t g_t)$$

eta

$$\mathrm{LT}(\alpha_1 g_1) + \cdots + \mathrm{LT}(\alpha_r g_r) = 0.$$

Ikusi

$$\prod_{\substack{j=1 \\ j \neq i}}^{r} \mathrm{LT}(g_j) \mid \mathrm{LT}(\alpha_i)$$

dela $i = 1, \ldots, r$ guztietarako, eta idatzi

$$\mathrm{LT}(\alpha_i) = \gamma_i \prod_{\substack{j=1 \\ j \neq i}}^{r} \mathrm{LT}(g_j).$$

Jarri orduan

$$\widetilde{\alpha}_i = \alpha_i - \gamma_i \prod_{\substack{j=1 \\ j \neq i}}^{r} g_j$$

$i = 1, \ldots, r$ denean, eta $\widetilde{\alpha}_i = \alpha_i$, $i = r+1, \ldots, t$ denean.)

(iii) Erabili aurreko atala 5.10 ariketaren kasu batzuk ebazteko.

(iv) Demagun ekuazio linealen sistema bat dugula,

$$\begin{cases} a_{11}X_1 + \cdots + a_{1n}X_n - b_1 = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n - b_m = 0 \end{cases}$$

eta jarri $\mathfrak{a} = (a_{11}X_1 + \cdots + a_{1n}X_n - b_1, \ldots, a_{m1}X_1 + \cdots + a_{mn}X_n - b_m)$. Orduan, Gaussen algoritmoa jarraituz lortzen den sistema baliokidearen polinomioek $\mathfrak{a}$-ren Gröbnerren oinarri bat osatzen dute edozein ordena monomialekiko, $X_1 > \cdots > X_n$ hartzen den bitartean.

5.14. Frogatu $\mathfrak{a} = (Y - X^2, XY)$ ez dela $K[X, Y]$-ren ideal erradikala. (Iradokizuna: Aurkitu behar dugu $f \notin \mathfrak{a}$ polinomio bat, halakoa non $f^r \in \mathfrak{a}$ den r berretzaileren baterako. Horretarako, kandidatu garbi bat dago. Orduan, idealbarnekotasunaren problema baten aurrean gaude, eta hori $\mathfrak{a}$-ren Gröbnerren oinarri baten laguntzarekin erabaki daiteke. Eman froga alternatibo bat, Gröbnerren oinarririk erabili gabe.)

5.15. Izan bedi $f \in K[X_1, \ldots, X_n]$. Idatz dezagun f X_1 indeterminatuarekiko,

$$f(X_1, \ldots, X_n) = a_m(X_2, \ldots, X_n)X_1^m + \cdots + a_1(X_2, \ldots, X_n)X_1 + a_0(X_2, \ldots, X_n),$$

eta demagun $a_m(X_2, \ldots, X_n) \in K^\times$ unitatea dela. Dakigunez, kasu horretan $g \in K[X_1, \ldots, X_n]$ edozein polinomio f-rekin zatitu dezakegu, X_1 indeterminatuarekiko. Frogatu horrela lortzen diren zatidura eta hondarra bat datozela $K[X_1, \ldots, X_n]$-ren zatiketaren algoritmo orokortua aplikatuz lortzen direnekin, ordena lexikografikoa aukeratzen badugu, $X_1 > \cdots > X_n$ harturik.