Мастер рад

Гребнерове базе

Аутор: Јелена Јовичић
Број индекса: 1033/2008

Ментор: Доцент др Зоран Петровић

Математички факултет
Београд 2010.

Резиме

Рад пред вама је мастер рад студента Математичког факултета у Београду, у којем је обрађена тема „Гребнерове базе“. Цео рад се састоји из шест целина (1-6), а у оквиру четврте целине издвојено је осам одељака. (§1-§8)

У првом делу упознаћемо се са *полиномима n променљивих* $x_1,\dots,x_n$ чији су коефицијенти у произвољном пољу k и дефинисаћемо *афини простор*. У другом и трећем делу дефинисаћемо један од основних геометријских објеката *афини варијетет* и један од основних алгебарских објеката *идеал*.

У четвртом делу, искористићемо све што је изложено у првом, другом и трећем делу да би описали метод *Гребнерових база*. (скр. ГБ)

Одељак §1, четвртог дела се бави формулацијом проблема које ћемо покушати да решимо уз помоћ метода ГБ:

А. Проблем описа идеала

Б. Проблем припадности идеалу

В. Проблем решавања полиномских једначина

Г. Импликацијски проблем

У §2 одељку дефинисаћемо *мономијални поредак* и дати неке примере уређења $n-$торки (*лексикографски поредак, градирани лексикографски поредак, градирани обрнути лексикографски поредак)*. Одељак §3 садржи опис *алгоритма за дељење полинома у* $k[x_1,\dots,x_n]$. Алгоритам смо добили на тај начин што смо проширили алгоритам дељења за $k[x]$. Циљ је да поделимо полином $f\in k[x_1,\dots,x_n]$ са $f_1,\dots,f_\xi\in k[x_1,\dots,x_n]$, односно f треба да добијемо у облику $f=a_1f_1+\dots+a_\xi f_\xi+r$ где „количници“ $a_1,\dots,a_\xi$ и остатак r леже у $k[x_1,\dots,x_n]$. У §4 даћемо решење *Проблема описа идеала* за специјалан случај мономијалних идеала. Одељак §5 се бави доказом важног тврђења *Основне Хилбертове теореме о бази*, дефинисањем ГБ и комплетним решењем *Проблема описа идеала.* У §6 видећемо која све својства има ГБ и како да за дату базу проверимо да ли је ГБ. У §7 видећемо како да конструишемо ГБ за дати идеал. Одељак §8 је један од битнијих. У оквиру њега ћемо се позабавити решавањем преостала три проблема и видети у којој мери можемо да их решимо уз помоћ ГБ. За *Импликацијски проблем* ГБ неће дати комплетно решење.

У петом делу применићемо ГБ на решавање проблема у роботици.(*Да ли робот конобар може да послужи кафу на датом месту*?)

Последњи, шести део садржи описан на конкретном задатку, начин рачунања ГБ и проверу припадности идеалу.

Желим да искажем своју захвалност ментору доценту др Зорану Петровићу на многобројним сугестијама, примедбама и саветима, који су ми помогли у изради овог рада и његовом што бољем изгледу.

Математички факултет, Београд
19.март 2010. Јелена Јовичић

Садржај

ГРЕБНЕРОВЕ БАЗЕ

1 Полиноми и афини простор

ПОЛИНОМИ ВИШЕ ПРОМЕНЉИВИХ

У овом одељку, упознаћемо се са полиномима n променљивих $x_1,\ldots,x_n$ са коефицијентима у произвољном пољу k. Прво ћемо дефинисати шта су мономи.

Дефиниција 1. Моном *у* $x_1,\ldots,x_n$ *је производ облика*

$$x_1^{\alpha_1}\cdot x_2^{\alpha_2}\ldots x_n^{\alpha_n},$$

код кога су сви експоненти $\alpha_1,\ldots,\alpha_n$ *ненегативни цели бројеви.*
Укупан степен *монома је сума* $\alpha_1+\ldots+\alpha_n$.

Писање монома може се поједноставити: нека је $\alpha=(\alpha_1,\ldots,\alpha_n)$ n-торка ненегативних целих бројева. Онда ћемо писати

$$x^{\alpha}=x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\ldots x_n^{\alpha_n}.$$

Када је $\alpha=(0,\ldots,0)$, писаћемо $x^{\alpha}=1$. Укупан степен монома x^{α}, означаваћемо и са $|\alpha|=\alpha_1+\ldots+\alpha_n$.

Дефиниција 2. Полином f у $x_1,\ldots,x_n$ *са коефицијентима у* k *је коначна линеарна комбинација* (*са коефицијентима у* k) *монома. Полином* f *писаћемо у облику*

$$f=\sum_{\alpha}a_{\alpha}x^{\alpha},a_{\alpha}\in k,$$

где је f *сума преко коначног броја* $n-$*торки* $\alpha=(\alpha_1,\ldots,\alpha_n)$.
Скуп свих полинома у $x_1,\ldots,x_n$ *са коефицијентима у* k *означаваћемо са* $k[x_1,\ldots,x_n]$.

Када будемо радили са полиномима који имају мали број променљивих, најчешће ћемо изостављати индексе. На пример,

$$f=2x^3y^2z+\frac{3}{2}y^3z^3-3xyz+y^2$$

је полином у $Q[x,y,z]$.
За означавање полинома често ћемо користити слова f,g,h,p,q,r.

Дефиниција 3. *Нека је* $f = \sum_{\alpha} a_\alpha x^\alpha$ *полином у* $k[x_1,\ldots,x_n]$.

(*i*) **Коефицијентом** *монома* x^α *зваћемо* a_α.

(*ii*) *Ако је* $a_\alpha \neq 0$ *,онда ћемо* $a_\alpha x^\alpha$ *звати* **чланом** *од* f.

(*iii*) **Укупан степен** *од* f ***је максимум*** *од* $|\alpha|$ *где су коефицијенти* a_α *различити од нуле и означаваћемо га са* $deg(f)$.

Пример. Полином $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ има четири члана и његов укупан степен је 6. Приметимо да два члана имају исти максималан укупан степен, $\left(2x^3y^2z, \frac{3}{2}y^3z^3\right)$, овај случај никада не може да се догоди код полинома једне променљиве.

Сума и производ два полинома је такође полином. Полином f дели полином g ако постоји полином $h \in k[x_1,\ldots,x_n]$ такав да $g = fh$. У односу на сабирање и множење, $k[x_1,\ldots,x_n]$ задовољава све аксиоме поља, осим постојања инверза за множење (на пример, $\frac{1}{x_1}$ није полином).

На основу претходно изложеног, закључујемо да је $k[x_1,\ldots,x_n]$ ***прстен полинома.***

ПОЛИНОМИ ЈЕДНЕ ПРОМЕНЉИВЕ

Дефиниција 1. *Дат је полином различит од нуле* $f \in k[x]$, *нека је*

$$f = a_0x^m + a_1x^{m-1} + \ldots + a_m \ ,$$

где је $a_l \in k$ и $a_0 \neq 0$ (дакле, $m = deg(f)$). **Водећим чланом** *од* f *зваћемо* a_0x^m *и писаћемо* $LT(f) = a_0x^m$.

На пример, ако је $f = 2x^3 - 4x + 3$, онда је $LT(f) = 2x^3$.

Приметимо да ако су f и g полиноми различити од нуле, онда је

$$deg(f) \leq deg(g) \Leftrightarrow LT(f) \text{ дели } LT(g).$$

Став 2. (Алгоритам дељења). *Нека је* k *поље и нека је* g *полином различит од нуле у* $k[x]$. *Онда сваки* $f \in k[x]$ *може бити записан у облику*

$$f = qg + r \ ,$$

где су $g, r \in k[x]$, *и* $r = 0$ *или* $deg(r) < deg(g)$. *Даље,* q *и* r *су јединствено одређени.*

Помоћу следећег алгоритма написаног у псеудокоду могу се израчунати q *и* r *:*

Input: g, f
Output: q, r
$q = 0;\ r = f$
WHILE $r \neq 0$ **AND** $LT(g)$ **divides** $LT(r)$ **DO**
$$q = q + \frac{LT(r)}{LT(g)}$$
$$r = r - \frac{LT(r)}{LT(g)} g$$

АФИНИ ПРОСТОР

Даље, дефинисаћемо афини простор.

Дефиниција 4. *Нека је дато поље* k *и* n *позитиван цео број, дефинисаћемо* $n-$*димензионални* **афини простор** *над* k *као скуп*

$$k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}.$$

За пример афиног простора, размотрићемо случај када је $k = \boldsymbol{R}$. Добићемо познати простор из линеарне алгебре $\boldsymbol{R^n}$. Генерално, $k^1 = k$ звaћемо *афином линијом, а* k^2 *афином равни*.

2 Афини варијетет

Афини варијетет је један од основних геометријских објеката.

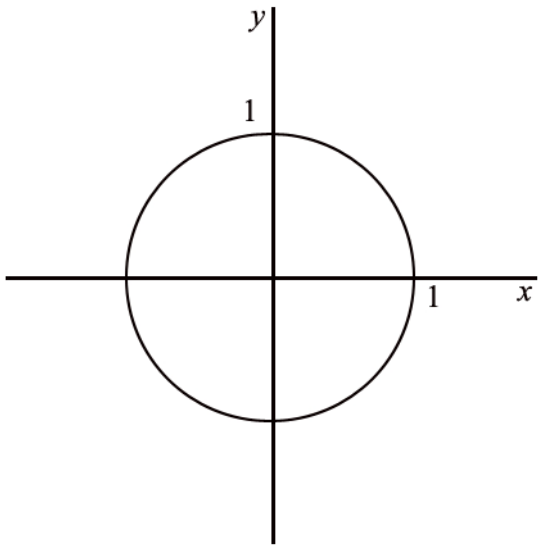
Дефиниција 1. *Нека је* k *поље, и нека су* $f_1, \ldots, f_\xi$ *полиноми у* $k[x_1, \ldots, x_n]$. *Нека је*

$$V(f_1, \ldots, f_\xi) = \{(a_1, \ldots, a_n) \in k^n : f_l(a_1, \ldots, a_n) = 0, \text{ за све } l = \overline{1, \xi}\}.$$

Афиним варијететом дефинисаним са $f_1, \ldots, f_\xi$ звaћемо $V(f_1, \ldots, f_\xi)$.

Према томе, афини варијетет $V(f_1, \ldots, f_\xi) \subset k^n$ је скуп свих решења система једначина $f_1(x_1, \ldots, x_n) = \ldots = f_\xi(x_1, \ldots, x_n) = 0$. Афине варијетете често ћемо означавати словима V, W. Користићемо да је $k = R$, тако да ћемо моћи да цртамо и слике.

Пример. У равни $\boldsymbol{R}^2$ варијетет $V\left(x^2+y^2-1\right)$, је круг пречника 1, са центром у координатном почетку.



3 Идеали

Идеал је један од основних алгебарских објеката.

Дефиниција 1. *Подскуп* $I \subseteq k\left[x_1,\ldots,x_n\right]$ *је* **идеал** *ако задовољава следеће услове:*

(*i*) $0 \in I$.

(*ii*) *Ако је* $f, g \in I$, *онда* $f+g \in I$.

(*iii*) *Ако је* $f \in I$ *и* $h \in k\left[x_1,\ldots,x_n\right]$, *онда* $hf \in I$.

Пример. Први природан пример идеала, је идеал генерисан коначним бројем полинома.

Дефиниција 2. *Нека су* $f_1,\ldots,f_\xi$ *полиноми у* $k\left[x_1,\ldots,x_n\right]$. *Нека је*

$$\left\langle f_1,\ldots,f_\xi \right\rangle = \left\{ \sum_{l=1}^{\xi} h_l f_l : h_1,\ldots,h_\xi \in k\left[x_1,\ldots,x_n\right] \right\}.$$

Ово је идеал.

Лема 3. *Ако је* $f_1,\ldots,f_\xi \in k[x_1,\ldots,x_n]$, *онда* је $\langle f_1,\ldots,f_\xi\rangle$ *идеал од* $k[x_1,\ldots,x_n]$. *Зваћемо* $\langle f_1,\ldots,f_\xi\rangle$ **идеалом генерисаним са** $f_1,\ldots,f_\xi$**.**

Доказ. Прво, $0\in\langle f_1,\ldots,f_\xi\rangle$, јер је $0=\sum_{l=1}^{\xi}0\cdot f_l$. Претпоставимо да је $f=\sum_{l=1}^{\xi}p_l f_l$ и $g=\sum_{l=1}^{\xi}q_l f_l$ и нека $h\in k[x_1,\ldots,x_n]$. Онда на основу једначина

$$f+g=\sum_{l=1}^{\xi}(p_l+q_l)f_l$$

$$hf=\sum_{l=1}^{\xi}(hp_l)f_l$$

видимо да је $\langle f_1,\ldots,f_\xi\rangle$ идеал.□

Кажемо да је идеал I ***коначно генерисан*** ако постоје $f_1,\ldots,f_\xi\in k[x_1,\ldots,x_n]$ *такви да је* $I=\langle f_1,\ldots,f_\xi\rangle$, и кажемо да је $f_1,\ldots,f_\xi$ ***база*** од I.

У §5 показаћемо важно тврђење, да је сваки *идеал од* $k[x_1,\ldots,x_n]$ коначно генерисан. (Ово тврђење је познатије као Хилбертова теорема о бази). Приметимо да дати идеал може имати различите базе. Показаћемо да од свих база које се могу одабрати, постоји погодан тип база, које се зову ***Гребнерове базе***.

4 Гребнерове базе

Волфганг Гребнер (енгл. *Wolfgang Groebner*; 2. фебруар 1899 - 20. август 1980.) био је аустријски математичар. Најпознатији је по Гребнеровој бази, која се користи у израчунавањима у алгебарској геометрији.

Рођен је у Госенсасу (садашњи Госенсас-Коле Исарко), у Доломитима, тада у Аустрији, сада у Италији.

Гребнер је првобитно студирао инжењерство на Технолошком универзитету у Грацу, али се пребацио на математику 1929. године.

Написао је дисертацију *Ein Beitrag zum Problem der Minimalbasen* 1932. године на Универзитету у Бечу; његов ментор за докторат био је Филип Фуртевенглер. После докторирања, наставио је студије у Гетингену код Еми Нетер, на пољу које је данас познато као комутативна алгебра.

Његов ученик, **Бруно Бухбергер**, увео је Гребнерове базе у својој докторској тези из 1965. и назвао их је по свом ментору.

За своју теорију Гребнерових база, Бухбергер је добио *2007 ACM Paris Kenellakis Theory and Practice Award*. Такође му је додељена *Златна медаља части* од стране аустријске владе.

§1 Проблеми

Почев од овог одељка, па надаље бавићемо се проучавањем метода Гребнерових база (скр. ГБ). Оне нам омогућавају решавање проблема везаних за полиномске идеале који се могу решавати алгоритамски или проблеме везане за разна друга израчунавања. Метод Гребнерових база се такође користи у моћним, компјутерским, алгебарским системима за проучавање идеја везаних за полиноме које се јављају у применама.
Фокусираћемо се на решавање само четири проблема.

Формулација проблема:

а. Проблем описа идеала: Да ли сваки идеал $I \subseteq k\left[x_1, x_2, \ldots, x_n\right]$ има коначан генераторски скуп?
Односно, да ли можемо да напишемо $I = \left\langle f_1, \ldots, f_\xi \right\rangle$ за неке $f_1, \ldots, f_\xi \in k\left[x_1, \ldots, x_n\right]$?

б. Проблем припадности идеалу: Нека је дат $f \in k\left[x_1, \ldots, x_n\right]$ и нека је идеал $I = \left\langle f_1, \ldots, f_\xi \right\rangle$, треба утврдити да ли $f \in I$?
Геометријски, то је повезано са проблемом утврђивања да ли је $V\left(f_1, \ldots, f_\xi\right)$ подскуп варијетету $V\left(f\right)$.

в. Проблем решавања полиномских једначина: Наћи сва заједничка решења система полиномских једначина у k^n

$$f_1\left(x_1, \ldots, x_n\right) = \ldots = f_\xi\left(x_1, \ldots, x_n\right) = 0$$

Наравно, исто је и ако поставимо питање да ли тачке припадају афином варијетету $V\left(f_1, \ldots, f_\xi\right)$.

г. Импликацијски проблем: Нека је V подскуп од k^n задат параметарски

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m) \end{aligned}$$

Ако су g_l полиноми (или рационалне функције) који зависе променљивих t_l, онда ће V бити афини варијетет или његов део. Треба наћи систем полиномских једначина (x_l) тако да дефинишу варијетет.

§2 Мономијални пореци у $k[x_1, x_2, \ldots, x_n]$

Код алгоритма дељења у $k[x]$ битан је редослед чланова у полиномима.

На пример, када делимо полином $f(x) = x^5 - 3x^2 + 1$ полиномом $g(x) = x^2 - 4x + 7$ на стандардан начин:

- Чланове у полиномима пишемо у опадајућем поретку у односу на степен од x.
- Водећи члан (члан највећег степен) у f је $x^5 = x^3 \cdot x^2 = x^3 \cdot$(водећи члан у g). Одузимамо $x^3 \cdot g(x)$ од f да би скратили водећи члан и добијамо $x^4 - 7x^3 - 3x^2 + 1$.
- Понављамо исти поступак на $f(x) - x^3 \cdot g(x)$, све док не добијемо полином степена мањег од 2.

Код алгоритма дељења полинома једне променљиве уређују се степени монома

$$\ldots > x^{m+1} > x^m > \ldots > x^2 > x > 1. \quad (1)$$

Успех алгоритма зависиће од систематичног рада са водећим члановима у f и g.

Из горе наведеног можемо да претпоставимо да ће и код дељења произвољних полинома више променљивих у $k[x_1, \ldots, x_n]$ бити битан поредак чланова .

На основу $n-$торке експонената $\alpha = (\alpha_1, \ldots, \alpha_n) \in \boldsymbol{N^n}$, можемо да реконструишемо моном $x^\alpha = x_1^{\alpha_1} \ldots x^{\alpha_n}$ (између монома у $k[x_1, \ldots, x_n]$ и $\boldsymbol{N^n}$ је успостављено 1-1 пресликавање). Даље, уређење > дефинисано на простору $\boldsymbol{N^n}$ нам даје уређење на мономима: ако је $\alpha > \beta$, такође је $x^\alpha > x^\beta$.

Дефиниција 1. Мономијални поредак у $k[x_1, \ldots, x_n]$ *је било која релација* $>$ *на* $\boldsymbol{N^n}$*, или равноправно, било која релација на скупу монома* x^α, $\alpha \in \boldsymbol{N^n}$*,која задовољава следеће услове:*

(i) $>$ *је тотално* (*или линеарно*) *уређење на* $\boldsymbol{N^n}$

(ii) *Ако је* $\alpha > \beta$ *и* $\gamma \in \boldsymbol{N^n}$*, онда је* $\alpha + \gamma > \beta + \gamma$

(iii) $>$ *је добро-уређење на* $\boldsymbol{N^n}$*.Сваки различит од празног, подскуп од* $\boldsymbol{N^n}$ *има најмањи елемент у односу на* $>$.

Следећа лема ће нам појаснити услов (iii) из Дефиниције 1.

Лема 2. *Релација уређења* $>$ *на* $\boldsymbol{N^n}$ *је добро уређење ако и само ако је сваки строго опадајући низ у* $\boldsymbol{N^n}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

коначан.

Ову лему ћемо често користити за доказивање да се различити алгоритми морају завршити после одређеног броја корака. Завршиће се, јер неки члан строго опада (у складу са датим мономијалним поредком) у сваком кораку алгоритма.

У §4 видећемо да је услов (iii) Дефиниције 1 еквивалентан услову $\forall \alpha \in \boldsymbol{N^n}, \alpha \geq 0$.

Једноставан пример мономијалног поредка је нумерички поредак

$$\dots > m+1 > m > \dots > 3 > 2 > 1 > 0$$

елемената из $\boldsymbol{N}$.

Први пример уређења n – торки, биће лексикографски поредак.

Дефиниција 3. (Лексикографски поредак, енгл. **Lexicographic Order –** скр. **lex)** *Нека су* $\alpha = (\alpha_1, \dots, \alpha_n)$ *и* $\beta = (\beta_1, \dots, \beta_n) \in \boldsymbol{N^n}$. *Казаћемо да је* $\alpha >_{lex} \beta$, *ако је у вектору разлике* $\alpha - \beta \in \boldsymbol{N^n}$, *прва ненулта позиција са леве стране позитивна.*
Тада ћемо писати $x^{\alpha} >_{lex} x^{\beta}$ *ако је* $\alpha >_{lex} \beta$.

Пример.
а. $(1,2,0) >_{lex} (0,3,4)$, јер је $\alpha - \beta = (1,-1,-4)$
б. $(3,2,4) >_{lex} (3,2,1)$, јер је $\alpha - \beta = (0,0,3)$
в. Промењљиве $x_1, \dots, x_n$ су обично уређене лексикографским поредком
$(1,0,\dots,0) >_{lex} (0,1,0,\dots,0) >_{lex} \dots >_{lex} (0,\dots,0,1)$, тако да је $x_1 >_{lex} x_2 >_{lex} \dots >_{lex} x_n$

Напомена. Када радимо са полиномима који зависе од једне, две или три промењљиве погодније је да се користе ознаке x, y, z него са x_1, x_2, x_3.

Дефиниција 5. (Градирани лексикографски поредак, енгл. **Graded Lex Order-** скр. **grlex)** *Нека су* $\alpha = (\alpha_1, \dots, \alpha_n)$ *и* $\beta = (\beta_1, \dots, \beta_n) \in \boldsymbol{N^n}$. *Казаћемо да је* $\alpha >_{grlex} \beta$
ако је $|\alpha| = \sum_{l=1}^{n} \alpha_l > |\beta| = \sum_{l=1}^{n} \beta_l$, *или* $|\alpha| = |\beta|$ *и* $\alpha >_{lex} \beta$.

Пример.
а. $(1,2,3) >_{grlex} (3,2,0)$ јер је $|(1,2,3)| = 6 > |(3,2,0)| = 5$
б. $(1,2,4) >_{grlex} (1,1,5)$ јер је $|(1,2,4)| = |(1,1,5)|$ и $(1,2,4) >_{lex} (1,1,5)$

Још један пример монимијалног поредка је градирани обрнути лексикографски поредак. У неким случајевима ефикаснији је за рачунање.

Дефиниција 6. (Градирани обрнути лексикографски поредак, енгл. **Graded Reverse Lex Order-**скр. **grevlex)** *Нека су* $\alpha=(\alpha_1,\ldots,\alpha_n)$ *и* $\beta=(\beta_1,\ldots,\beta_n)\in \boldsymbol{N^n}$. *Казаћемо да је* $\alpha >_{grevlex} \beta$ *ако је* $|\alpha|=\sum_{l=1}^{n}\alpha_l > |\beta|=\sum_{l=1}^{n}\beta_l$, *или* $|\alpha|=|\beta|$ *и у* $\alpha-\beta\in \boldsymbol{Z^n}$, *прва ненулта позиција са десне стране негативна.*

Пример.

а. $(4,7,1) >_{grevlex} (4,2,3)$ јер је $|(4,7,1)|=12>|(4,2,3)|=9$

б. $(1,5,2) >_{grevlex} (4,1,3)$ јер је $|(1,5,2)|=|(4,1,3)|$ и $\alpha-\beta=(-3,4,-1)$

Став 4. *Лексикографски поредак на* $\boldsymbol{N^n}$ *је мономијални поредак.*

Доказ.

(i) Да је $>_{lex}$ тотални поредак следи директно из дефиниције и чињенице да је у $\boldsymbol{N}$ тотални поредак.

(ii) Ако је $\alpha >_{lex} \beta$, имамо да је $\alpha-\beta$ прва ненулта позиција са леве стране позитивна, односно $\alpha_k-\beta_k$ је позитивно.

$$x^{\alpha}\cdot x^{\gamma}=x^{\alpha+\gamma} \text{ и } x^{\beta}\cdot x^{\gamma}=x^{\beta+\gamma}$$

Онда је у $(\alpha+\gamma)-(\beta+\gamma)=\alpha-\beta$ прва ненулта позиција $\alpha_k-\beta_k>\mathbf{0}$.

(iii) Претпоставимо да $>_{lex}$ није добро уређење. Онда по Леми 2 постојаће бесконачан, строго опадајући низ

$$\alpha(1)>_{lex}\alpha(2)>_{lex}\alpha(3)>_{lex}\ldots$$

елемената $\boldsymbol{N^n}$. Показаћемо да то води до контрадикције.

Посматраћемо прве компоненте вектора $\alpha(i)\in \boldsymbol{N^n}$. По дефиницији лексикографског поредка, ове прве компоненте су у облику нерастућег низа ненегативних бројева. Како је $\boldsymbol{N}$ добро уређен, прве компоненете од $\alpha(i)$ морају се „стабилизовати“ на крају. Значи, постоји k такво да су све прве компоненте од $\alpha(i)$ једнаке за $i\geq k$.

Почев од $\alpha(k)$, друга и следеће компоненете су у игри за одређивање лексикографског поредка. Следеће компоненте од $\alpha(k),\alpha(k+1),\ldots$ *су у облику* нерастућег низа.

Из истих разлога као и раније, следеће компоненте се морају „стабилизовати“. Настављајући на исти начин, видимо да су за неко $l,\alpha(l),\alpha(l+1),\ldots$ све једнаке. Ово је котрадикција са чињеницом да је $\alpha(l)>\alpha(l+1)$. □

Напомена. На сличан начин може се доказати и да је *градирани лексикографски поредак мономијални поредак и градирани обрнути лексикографски поредак мономијални поредак.*

Пример. У следећем примеру видећемо како се мономијални поредак примењује на полиноме.

Ако је $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ полином у $k[x_1, \ldots, x_n]$ и $>$ неки мономијални поредак, онда можемо уредити мономе од f у складу са $>$.

Нека је

$$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$$

онда:

а. У складу са лексикографским поредком можемо да преуредимо чланове од f на следећи начин

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$$

б. У складу са градираним лексикографским поредком можемо да преуредимо чланове од f на следећи начин

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$$

в. У складу са обрнутим градираним лексикографским поредком можемо да преуредимо чланове од f на следећи начин

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$$

Дефиниција 7. *Нека је* $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ *полином различит од нуле у* $k[x_1, \ldots, x_n]$ *и нека је* $>$ *мономијални поредак.*

(i) **Водећи мултистепен** *од* f *је*

$$multi\,deg(f) = max\left(\alpha \in \boldsymbol{N}^{n} : a_{\alpha} \neq 0\right)$$ (*максимум је узет у складу са* $>$*)*

(ii) **Водећи коефицијент** *од* f *је*

$$LC(f) = a_{multi\,deg(f)} \in k$$

(iii) **Водећи моном** *од* f *је*

$$LM(f) = x^{multi\,deg(f)}$$ (*са коефицијентом 1).*

(iv) **Водећи члан** *од* f *је*

$$LT(f) = LC(f) \cdot LM(f)$$

Пример. Чланове датог полинома уредићемо у складу са lex, grlex, grevlex поредком и одредићемо мултистепен, водећи коефицијент, водећи моном, водећи члан.

$$f(x,y,z) = 2x^2y^8 - 3x^5y\ z^4 + xyz^3 - xy^4$$

Лексикографски поредак

$$f(x,y,z) = 2x^2y^8 - 3x^5y\ z^4 + xyz^3 - xy^4$$
$$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$$

$$multi\ deg(f) = (5,1,4)$$
$$LC(f) = -3$$
$$LM(f) = x^5yz^4$$
$$LT(f) = -3x^5yz^4$$

Градирани лексикографски поредак

$$f(x,y,z) = 2x^2y^8 - 3x^5y\ z^4 + xyz^3 - xy^4$$
$$f(x,y,z) = -3x^5y\ z^4 + 2x^2y^8 - xy^4 + xyz^3$$

$$multi\ deg(f) = (5,1,4)$$
$$LC(f) = -3$$
$$LM(f) = x^5yz^4$$
$$LT(f) = -3x^5yz^4$$

Градирани обрнут лексикографски поредак

$$f(x,y,z) = 2x^2y^8 - 3x^5y\ z^4 + xyz^3 - xy^4$$
$$f(x,y,z) = 2x^2y^8 - 3x^5yz^4 - xy^4 + xyz^3$$

$$multi\ deg(f) = (2,8,0)$$
$$LC(f) = 2$$
$$LM(f) = x^2y^8$$
$$LM(f) = 2x^2y^8$$

Лема 8. *Нека су* $f, g \in k[x_1,\ldots,x_n]$ *полиноми различити од нуле. Онда важи:*

(i) $multi\,deg(fg) = multi\,deg(f) + multi\,deg(g)$

(ii) *Ако је* $f+g \neq 0$, *онда* $multi\,deg(f+g) \leq max(multi\,deg(f), multi\,deg(g))$

Ако је код сабирања, $multi\,deg(f) \neq multi\,deg(g)$, *онда важи једнакост.*

Од сада па надаље претпоставићемо да је одабран само један мономијални поредак. Водећи чланови и остало, биће одређивани у складу са њим.

§3 Алгоритам дељења у $k[x_1,\ldots,x_n]$

Алгоритам дељења за полиноме у $k[x_1,\ldots,x_n]$ формулисаћемо на тај начин, што ћемо проширити алгоритам дељења за $k[x]$. Циљ нам је да поделимо полином $f \in k[x_1,\ldots,x_n]$ са $f_1,\ldots,f_\xi \in k[x_1,\ldots,x_n]$.
Односно f треба да добијемо у облику

$$f = a_1 f_1 + \ldots + a_\xi f_\xi + r$$

где „количници“ $a_1,\ldots,a_\xi$ и остатак r леже у $k[x_1,\ldots,x_n]$.

Основна идеја алгоритма је иста као и у случају једне променљиве. Желимо да поништимо водећи члан од f (водећи рачуна о задатом мономијалном поредку) множећи неки f_l са одговарајућим мономом и одузимајући га. После тога моном постаје члан у одговарајућем a_l.

Теорема 3. (Алгоритам дељења у $k[x_1,\ldots,x_n]$**).** *Нека је фиксиран мономијални поредак* $>$ *на* $\mathbf{N}^n$, *и нека је* $F = (f_1,\ldots,f_\xi)$ ξ*-торка полинома у* $k[x_1,\ldots,x_n]$. *Тада се сваки полином* $f \in k[x_1,\ldots,x_n]$ *може записати на следећи начин:*

$$f = a_1 f_1 + \ldots + a_\xi f_\xi + r$$

за $a_l, r \in k[x_1,\ldots,x_n]$, *при чему је или r=0 или је r нека линеарна комбинација (са коефицијентима у* k*) монома од којих ни један није дељив са било којим од* $LT(f_1),\ldots,LT(f_\xi)$.

Онда ћемо r назвати **остатком** *полинома* f *при дељењу са* F . *Осим тога, ако је* $a_l f_l \neq 0$

$$multi\,deg(f) \geq multi\,deg(a_l f_l)$$

Доказ. Доказаћемо егзистенцију $a_1,\ldots,a_\xi$ и r дајући алгоритам за њихову конструкцију. Показаћемо да алгоритам ради коректно за све улазне податке.

INPUT: $f_1,\ldots,f_\xi,f$

OUTPUT: $a_1,\ldots,a_\xi,r$

$a_1=0;\ldots;a_\xi=0;r=0$

$p=f$

WHILE $p\neq 0$ **DO**

$l=1$

divisionoccurred *=false*

WHILE $l\leq\xi$ **AND** ***divisionoccurred****=false* **DO**

IF $LT(f_l)$ **DIVIDES** $LT(p)$ **THEN**

$$a_l=a_l+LT(p)/LT(f_l)$$
$$p=p-\left(LT(p)/LT(f_l)\right)f_l \quad (*)$$

divisionoccurred*=true*

ELSE

$l=l+1$

IF ***divisionoccurred****=false* **THEN**

$$r=r+LT(p)$$
$$p=p-LT(p) \quad (**)$$

Напомена. Логичка променљива „*divisionoccurred*“ нам говори кад неки од $LT(f_l)$ дели $LT(p)$.

Сваки пут када прођемо главну **WHILE...DO** петљу, догодиће се тачно један од следећа два случаја:

Корак дељења :

Ако неки $LT(f_l),l=1,\ldots,\xi$ дели $LT(p)$, алгоритам се своди на случај једне променљиве.

Корак остатка :

Ако $LT(f_l)$ не дели $LT(p)$, онда алгоритам додаје $LT(p)$ остатку r .

Да би доказали да алгоритам функционише, прво ћемо показати да једнакост

$$f=a_1f_1+\ldots+a_\xi f_\xi+p+r \quad (2)$$

важи у сваком кораку. Очигледно је да важи за почетне вредности $a_1,\ldots,a_\xi,p,r$.

Сада претпоставимо да (2) важи у неком кораку алгоритма. Ако је следећи корак **Корак дељења**, онда неки $LT(f_l),l=\overline{1,\xi}$ дели $LT(p)$, и из једнакости

$$a_lf_l+p=\left(a_l+LT(p)/LT(f_l)\right)f_l+\left(p-\left(LT(p)/LT(f_l)\right)f_l\right)$$

се види да је $a_l f_l + p$ непромењено. Како и остале променљиве нису промењене, једнакост (2) је тачна.
У другом случају , ако је следећи корак **Корак остатка**, онда ће p и r бити промењени, али сума $p+r$ остаје непромењена:

$$p+r=\left(p-LT\left(p\right)\right)+\left(r+LT\left(p\right)\right)$$

Видимо да је (2) још увек непромењена.
Алгоритам се завршава када је $p=0$. У овом случају, (2) постаје

$$f=a_1 f_1+\ldots+a_\xi f_\xi+r.$$

Када се алгоритам заврши $a_1,\ldots,a_\xi,r$ имају жељене особине, јер су чланови додавани r само ако нису дељиви са $LT\left(f_l\right), l=\overline{1,\xi}$.

Остало је да покажемо да ће се алгоритам завршити. Приметимо, да сваки пут када променимо вредност променљиве p, мултистепен се смањује или постаје 0. Да би видели како се мултистепен смањује, претпоставимо да је Кораку дељења p постало

$$p^{'}=p-\frac{LT\left(p\right)}{LT\left(f_l\right)}f_l$$

На основу Леме 8 из §2, имамо

$$LT\left(\frac{LT\left(p\right)}{LT\left(f_l\right)}f_l\right)=\frac{LT\left(p\right)}{LT\left(f_l\right)}LT\left(f_l\right)=LT\left(p\right).$$

тако да p и $\left(LT\left(p\right)/LT\left(f_l\right)\right)f_l$ имају исти водећи члан. Разлика p' мора имати строго мањи мултистепен када је $p^{'}\neq 0$. Даље, претпоставимо да је током Корака остатка, p постало

$$p^{'}=p-LT\left(p\right).$$

Овде је , очигледно $multi\,deg\left(p^{'}\right)<multi\,deg\left(p\right)$ када је $p^{'}\neq 0$. Дакле, мултистепен се мора смањити у сваком случају .
Ако се алгоритам никада не заврши, добили би смо бесконачни, опадајући низ мултистепена. Ово се не може догодити (Лема 2 из §2). Дакле, у једном тренутку је $p=0$ и алгоритам се завршава после коначног броја корака.

Остало је да одредимо везу између $multi\,deg\left(f\right)$ и $multi\,deg\left(a_l f_l\right)$. Сваки члан у a_l је облика $LT\left(p\right)/LT\left(f_l\right)$, за неку вредност p. Алгоритам почиње са $p=f$, и мултистепен од p опада. На основу тога је $LT\left(p\right)\leq LT\left(f\right)$, и лако се доказује (користећи услов (ii) дефиниције мономијалног поредка) да је $multi\,deg\left(f\right)\geq multi\,deg\left(a_l f_l\right)$ када је $a_l f_l\neq 0$. □

На крају се поставља питање да ли алгоритам у $k\left[x_1,\ldots,x_n\right]$ има исте особине као и алгоритам у $k\left[x\right]$? Алгоритам је на жалост далеко је од савршеног, тек када се повеже са Гребнеровим базама достиже свој максимум. (§5 и §6)

Једна од битнијих особина алгоритма дељења у $k[x]$, је да је остатак јединствено одређен. У следећем примеру видећемо да ли ово важи код алгоритма у $k[x_1,\ldots,x_n]$.

Пример. Нека је дат полином $f = x^2y + xy^2 + y^2$ и уређени пар полинома $F = (f_1, f_2) = (xy-1, y^2-1)$ у лексикографском поредку $(x >_{lex} y)$. Према алгоритму дељења имамо следеће кораке:

$$(x^2y + xy^2 + y^2) : (xy-1) = x + y$$
$$\underline{(-)\,x^2y - (+)\,x}$$
$$xy^2 + x + y^2$$
$$\underline{(-)\,xy^2 - (+)\,y}$$
$$x + y^2 + y$$

$$(x + y^2 + y) : (y^2 - 1) = 1$$
$$\underline{(-)\,y^2 - (+)1}$$
$$x + y + 1$$

$$x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1\cdot(y^2-1) + (x+y+1) \quad (1)$$

Посматрамо исти полином $f = x^2y + xy^2 + y^2$ као у претходном случају и исти уређени пар полинома. Једино ћемо заменити њихова места $F = (g_1, g_2) = (f_2, f_1) = (y^2-1, xy-1)$ $(x >_{lex} y)$. Према алгоритму имамо следеће кораке:

$$(x^2y + xy^2 + y^2) : (y^2 - 1) = x + 1$$
$$\underline{xy^2 - x}$$
$$x^2y + x + y^2$$
$$\underline{(-)\,y^2 - (+)1}$$
$$x^2y + x + 1$$

$$(x^2y + x + 1) : (xy - 1) = x$$
$$\underline{(-)\,x^2y - (+)\,x}$$
$$2x + 1$$

$$x^2y+xy^2+y^2=(x+1)(y^2-1)+x\cdot(xy-1)+(2x+1) \quad (3)$$

Ако се упореде изрази (1) и (3) видимо да се разликују добијени остаци при дељењу. Из тога закључујемо да остатак није јединствено одређен и да је уређење ξ-торка полинома $F=(f_1,\ldots,f_\xi)$ битно.

Уз помоћ алгоритма дељења у $k[x]$ се решава и проблем припадности идеалу. Једна од последица Теореме 3 је, ако после дељења f са $F=(f_1,\ldots,f_\xi)$ добијемо остатак $r=0$, онда је $f=a_1f_1+\ldots+a_\xi f_\xi$ и $f\in\langle f_1,\ldots f_\xi\rangle$. Дакле $r=0$ је довољан услов за припадност идеалу, а да ли је и потребан видећемо у следећем примеру.

Пример 5. Нека је $f_1=xy+1, f_2=y^2-1\in k[x,y]$ (lex). Када делимо $f=xy^2-x$ са $F=(f_1,f_2)$ добијамо

$$xy^2-x=y(xy+1)+0\cdot(y^2-1)+(-x-y).$$

А када делимо са $F=(f_2,f_1)$, добијамо

$$xy^2-x=x\cdot(y^2-1)+0\cdot(xy+1)+0.$$

Из друге једнакости видимо да $f\in\langle f_1,f_2\rangle$,а ипак је могуће добити остатак који се разликује од нуле када се дели са $F=(f_1,f_2)$.

§4 Мономијални идеали и Диксонова лема

У овом одељку разматраћемо ***Проблем описа идеала из §1 за специјалан случај мономијалних идеала***. Прво ћемо дефинисати моноимијалне идеале у $k[x_1,\ldots,x_n]$.

Дефиниција 1. *Идеал $I\subseteq k[x_1,\ldots,x_n]$ је **мономијални идеал** ако постоји подскуп $A\subset \mathbf{N}^n$ (који може бити бесконачан) такав да се I састоји од свих полинома који су коначне суме облика $\sum_{\alpha\in A}h_\alpha x^\alpha$, где је $h_\alpha\in k[x_1,\ldots,x_n]$.*

У том случају писаћемо $I=\langle x^\alpha:\alpha\in A\rangle$.

Другим речима, идеал I у прстену полинома $k[x_1,\ldots,x_n]$ генерисан неким скупом монома је мономијални идеал.

Пример. Мономијални идеал је $I=\langle x^4y^2,x^3y^4,x^2y^5\rangle\subseteq k[x,y]$.

Описаћемо све мономе који леже у датом мономијалном идеалу.

Лема 2. *Нека је* $I = \langle x^{\alpha} : \alpha \in A \rangle$ *мономијални идеал. Онда моном* x^{β} *лежи у* I *ако и само ако је* x^{β} *дељиво са* x^{α} *за неко* $\alpha \in A$.

Доказ. Ако је x^{β} умножак од x^{α} за неко $\alpha \in A$, онда $x^{\beta} \in I$ у складу са дефиницијом идеала.

Супротно, ако $x^{\beta} \in I$, онда $x^{\beta} = \sum_{l=1}^{s} h_l x^{\alpha(l)}$, где је $h_l \in k[x_1, \ldots, x_n]$ и $\alpha(l) \in A$. Ако проширимо свако h_l као линеарну комбинацију монома, видећемо да је сваки члан са десне стране једнакости дељив са неким $x^{\alpha(l)}$. И лева страна x^{β} има ту особину. □

Приметимо да је x^{β} дељиво са x^{α} када је $x^{\beta} = x^{\alpha} \cdot x^{\gamma}$, за неко $\gamma \in \boldsymbol{N^n}$. Ово је еквивалентно са $\beta = \alpha + \gamma$. Дакле, скуп

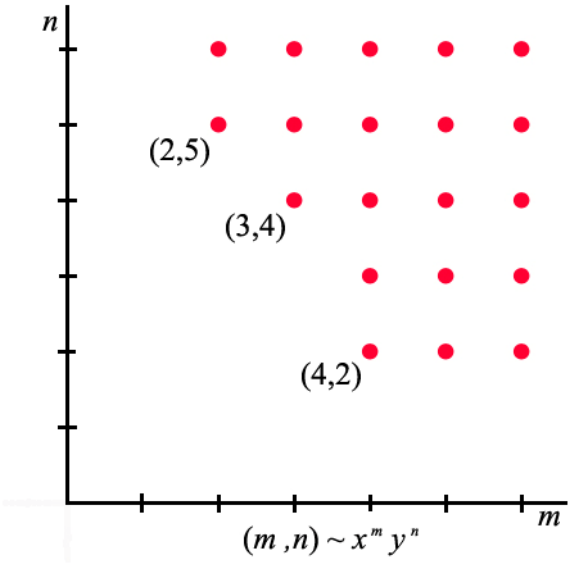
$$\alpha + \boldsymbol{N^n} = \{\alpha + \gamma : \gamma \in \boldsymbol{N^n}\}$$

се састоји од експонената свих монома дељивих са x^{α}. Овај закључак и Лема 2 омогућавају нам да нацртамо слике монома у датом мономијалном идеалу.

На пример, ако је $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, онда су експоненти монома у I у облику скупа

$$((4,2) + \boldsymbol{N^2}) \cup ((3,4) + \boldsymbol{N^2}) \cup ((2,5) + \boldsymbol{N^2}).$$

Визуелно можемо да прикажемо овај скуп као унију целобројних тачака кроз три транслације првог квадранта у равни:



Следећа леми нам говори о томе да се посматрањем монома полинома f, може утврдити да ли f припада мономијалном идеалу .

Лема 3. *Нека је I мономијални идеал, и нека је $f \in k[x_1,\ldots,x_n]$. Онда су следећа тврђења еквивалентна:*
(i) $f \in I$.
(ii) *Сваки члан од f лежи у I.*
(iii) *f је k-линеарна комбинација монома у I.*

Директна последица ставке (iii) Леме 3, је да је мономијални идеал једнистевено одређен са својим мономима.

Последица 4. *Два мономијална идеала су иста ако и само ако садрже исте мономе.*

Једно од важних тврђења је да су сви мономијални идеали у $k[x_1,\ldots,x_n]$ коначно генерисани.

Теорема 5. (Диксонова лема) *Мономијални идеал $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1,\ldots,x_n]$ може бити написан у облику $I = \langle x^{\alpha(1)},\ldots,x^{\alpha(\xi)} \rangle$, где $\alpha(1),\ldots,\alpha(\xi) \in A$. Специјално, I има коначну базу.*

Доказ. (Индукцијом по n, где је n број променљивих)
Ако је $n=1$, онда је I генерисан са мономима x_1^α, где је $\alpha \in A \subseteq \boldsymbol{N}$. Нека је β најмањи елемент од $A \subseteq \boldsymbol{N}$.
Онда је $\beta \le \alpha$ за свако $\alpha \in A$, такво да x_1^β дели све остале генераторе x_1^α. Одатле следи да је $I = \langle x_1^\beta \rangle$.
Претпоставимо да је $n>1$ и да је теорема тачна за $n-1$. Променљиве ћемо означити као $x_1,\ldots,x_{n-1},y$, тако да се мономи у $k[x_1,\ldots,x_{n-1},y]$ могу записати у облику $x^\alpha y^m$, где је $\alpha = (\alpha_1,\ldots,\alpha_{n-1}) \in \boldsymbol{N^{n-1}}$ и $m \in \boldsymbol{N}$.

Претпоставимо да је $I \subseteq k[x_1,\ldots,x_{n-1},y]$ мономијални идеал. Да би пронашли генераторе за I, узмемо да је J мономијали идеал у $k[x_1,\ldots,x_{n-1}]$ генерисан мономима x^α, таквим да $x^\alpha y^m \in I$, за неко $m \ge 0$. Како је J мономијални идеал у $k[x_1,\ldots,x_{n-1}]$,по индуктивној хипотези коначно много x^α генерише J, па је $J = \langle x^{\alpha(1)},\ldots,x^{\alpha(\xi)} \rangle$. Идеал J може бити схваћен као „пројекција“ од I на $k[x_1,\ldots,x_{n-1}]$.

За свако i између 1 и ξ, начин на који је дефинисан J, нам говори да $x^{\alpha(i)}y^{m_i} \in I$ за неко $m_i \geq 0$. Нека је m највеће од свих m_i. Онда за свако k између 0 и $m-1$, конструишемо идеал $J_k \subseteq k\left[x_1,\ldots,x_{n-1}\right]$ генерисан мономима x^{β} таквим да $x^{\beta}y^k \in I$. О J_k можемо да размишљамо као о „делу“ од I који је генерисан мономима који садрже y тачно степена k. На основу индуктивне хипотезе, J_k има коначан генераторски скуп монома, и $J_k = \left\langle x^{\alpha_k(1)},\ldots,x^{\alpha_k(\xi_k)}\right\rangle$.
Тврдимо да је I генерисан следећим мономима:

из $J : x^{\alpha(1)}y^m,\ldots,x^{\alpha(\xi)}y^m$,
из $J_0 : x^{\alpha_0(1)},\ldots,x^{\alpha_0(\xi_0)}$,
из $J_1 : x^{\alpha_1(1)}y,\ldots,x^{\alpha_1(\xi_1)}y$
.....
из $J_{m-1} : x^{\alpha_{m-1}(1)}y^{m-1},\ldots,x^{\alpha_{m-1}(\xi_{m-1})}y^{m-1}$.

Приметимо да је сваки моном у I дељив са неким од горе наведених. Нека $x^{\alpha}y^p \in I$. Ако је $p \geq m$, онда је $x^{\alpha}y^p$ дељив са неким $x^{\alpha(i)}y^m$ због начина конструкције J. Ако је $p \leq m-1$, онда је $x^{\alpha}y^p$ дељиво са неким $x^{\alpha_p(i)}y^p$ због конструкције J_p. (На основу Леме 2 горе описани мономи генеришу идеал који има исте мономе као I). На основу Последице 4, наше тврђење је доказано.

Да би комплетирали доказ теореме, потребно је да покажемо да коначан скуп генератора може бити изабран из датог скупа генератора за идеал. У односу на променљиве $x_1,\ldots,x_n$, наш мономијални идеал је $I = \left\langle x^{\alpha} : \alpha \in A\right\rangle \subseteq k\left[x_1,\ldots,x_n\right]$. Треба показати да је идеал I генерисан са коначно много x^{α}, где $\alpha \in A$. Знамо да је $I = \left\langle x^{\beta(1)},\ldots,x^{\beta(\xi)}\right\rangle$ за неке мономе $x^{\beta(i)}$ у I. Како $x^{\beta(i)} \in I = \left\langle x^{\alpha} : \alpha \in A\right\rangle$, на основу Леме 2 сваки $x^{\beta(i)}$ је дељив са $x^{\alpha(i)}$ за неко $\alpha(i) \in A$. Лако је показати да је $I = \left\langle x^{\alpha(1)},\ldots,x^{\alpha(\xi)}\right\rangle$. □

Теорема 5 решава Проблем описа мономијалних идеала, говори нам да идеал има коначну базу. Такође решава и проблем припадности за мономијалне идеале. Ако је $I = \left\langle x^{\alpha(1)},\ldots,x^{\alpha(\xi)}\right\rangle$, лако може да се покаже да дати полином f припада I, ако и само ако је остатак дељења f са $x^{\alpha(1)},\ldots,x^{\alpha(\xi)}$ нула.
Диксонова лема се користи и за доказ битног тврђења везаног за мономијалне поредке у $k\left[x_1,\ldots,x_n\right]$.

Последица 6. Нека је $>$ релација на $\boldsymbol{N^n}$ која задовољава следећа својства:
(i) $>$ *је тотални поредак на* $\boldsymbol{N^n}$.
(ii) *ако је* $\alpha > \beta$ *и* $\gamma \in \boldsymbol{N^n}$, *онда* $\alpha + \gamma > \beta + \gamma$.
Онда је $>$ *добро уређење ако и само ако је* $\alpha \geq 0$ *за свако* $\alpha \in \boldsymbol{N^n}$.

Последица 6. нам омогућава да поједноставимо Дефиницију 1 из §2 (Дефиниција мономијалог поредка). Услови (i) и (ii) не могу бити промењени, али услов (iii) можемо заменити са једноставнијим условом да је $\alpha \geq 0$ за свако $\alpha \in \boldsymbol{N^n}$. Ово ће знатно олакшати проверу да ли је дати поредак мономијалан.

§5 Хилбертова теорема о бази и Гребнерова база

Све што смо изложили до сада, омогућава нам да у овом одељку дамо комплетно решење ***Проблема описа идеала*** **из §1**. Видећемо и на који начин да добијемо базу идеала са „добрим“ својствима, повезаном са алгоритмом дељења описаним у §3. Кључна идеја коју ћемо користити, је да за одабрани мономијални поредак , сваки $f \in k[x_1,\ldots,x_n]$ има јединствени водећи члан $LT(f)$.
За било који идеал I можемо дефинисати *идеал водећих чланова*.

Дефиниција 1. *Нека је* $I \subseteq k[x_1,\ldots,x_n]$ ***идеал*** *различит од* $\{0\}$.
(*i*) *Означимо са* $LT(I)$ *скуп водећих чланова елемената од* I *.Тако да,*

$$LT(I) = \left\{ cx^{\alpha} : \exists f \in I, LT(f) = cx^{\alpha} \right\}$$

(*ii*) *Означимо са* $\langle LT(I) \rangle$ *идеал генерисан елементима од* $LT(I)$.

Напомена: Ако је дат коначан, генераторски скуп за I, $I = \langle f_1,\ldots,f_{\xi} \rangle$, онда $\langle LT(f_1),\ldots,LT(f_{\xi}) \rangle$ и $\langle LT(I) \rangle$ могу бити *различити* идеали.
По дефиницији је, $LT(f_l) \in LT(I) \subseteq \langle LT(I) \rangle, l = \overline{1,\xi}$ из чега следи да је $\langle LT(f_1),\ldots,LT(f_{\xi}) \rangle \subseteq \langle LT(I) \rangle$.Следећи пример показује да је $\langle LT(I) \rangle$ прави надскуп.

Пример 2. Нека је $I = \langle f_1, f_2 \rangle$, где је $f_1 = x^3 - 2xy$ и $f_2 = x^2y - 2y^2 + x$, grlex задат мономијални поредак на $k[x, y]$**.** Онда

$$x\left(x^2y - 2y^2 + x\right) - y \cdot \left(x^3 - 2xy\right) = x^2,$$

тако да $x^2 \in I$. Дакле, $x^2 = LT\left(x^2\right) \in \left\langle LT\left(I\right)\right\rangle$. Међутим x^2 није дељиво са $LT\left(f_1\right) = x^3$ или $LT\left(f_2\right) = x^2 y$, тако да $x^2 \notin \left\langle LT\left(f_1\right), LT\left(f_2\right)\right\rangle$ по Леми 2 из §4.

Сада ћемо показати да је $\left\langle LT\left(I\right)\right\rangle$ мономијални идеал. То ће нам омогућити коришћење добијених резултата у §4. Специјално, следиће да је $\left\langle LT\left(I\right)\right\rangle$ генерисан са коначно много водећих чланова.

Став 3. *Нека је* $I \subseteq k\left[x_1,\ldots,x_n\right]$ *идеал.*
(i) $\left\langle LT\left(I\right)\right\rangle$ *је мономијални идеал.*
(ii) *Постоје* $g_1,\ldots,g_\psi \in I$ *такви да је* $\left\langle LT\left(I\right)\right\rangle = \left\langle LT\left(g_1\right),\ldots,LT\left(g_\psi\right)\right\rangle$.

Доказ. (i) Водећи мономи $LM\left(g\right)$ елемената $g \in I - \left\{0\right\}$ генеришу мономијални идеал $\left\langle LM\left(g\right) : g \in I - \left\{0\right\}\right\rangle$. Како се $LM\left(g\right)$ и $LT\left(g\right)$ разликују за константу различиту од нуле, овај идеал је једнак $\left\langle LT\left(g\right) : g \in I - \left\{0\right\}\right\rangle = \left\langle LT\left(I\right)\right\rangle$. Дакле, $\left\langle LT\left(I\right)\right\rangle$ је мономијални идеал.

(ii) Пошто је $\left\langle LT\left(I\right)\right\rangle$ генерисан мономима $LM\left(g\right)$ за $g \in I - \left\{0\right\}$, на основу Диксонове леме је $\left\langle LT\left(I\right)\right\rangle = \left\langle LM\left(g_1\right),\ldots,LM\left(g_\psi\right)\right\rangle$ за коначно много $g_1,\ldots,g_\psi \in I$. Пошто се $LM\left(g_l\right)$ разликује од $LT\left(g_l\right), l = \overline{1,\psi}$, за константу различиту од нуле, следи да је $\left\langle LT\left(I\right)\right\rangle = \left\langle LT\left(g_1\right),\ldots,LT\left(g_\psi\right)\right\rangle$. □

Користећи Став 3 и алгоритам дељења доказаћемо постојање коначног генераторског скупа *сваког* полиномског идеала. Нека је $I \subseteq k\left[x_1,\ldots,x_n\right]$ било који идеал и идеал $\left\langle LT\left(I\right)\right\rangle$ као у Дефиницији 1. Изабраћемо неки мономијални поредак, који ћемо користити приликом алгоритма дељења и рачунања водећих чланова.

Теорема 4. (Хилбертова теорема о бази) *Сваки идеал има коначан генераторски скуп. Тако да је,* $I = \left\langle g_1,\ldots,g_\psi\right\rangle$, *за неке* $g_1,\ldots,g_\psi \in I$.

Доказ. Ако је $I = \left\{0\right\}$, нека је генераторски скуп $\left\{0\right\}$. Он је сигурно коначан.
Ако I садржи полином различит од нуле, онда ћемо генераторски скуп $g_1,\ldots,g_\psi$ за I конструисати на следећи начин. На основу Става 3, постоје $g_1,\ldots,g_\psi \in I$ такви да је $\left\langle LT\left(I\right)\right\rangle = \left\langle LT\left(g_1\right),\ldots,LT\left(g_\psi\right)\right\rangle$.

Тврдимо да је $I=\langle g_1,\ldots,g_\psi\rangle$.

Очигледно је да $\langle g_1,\ldots,g_\psi\rangle\subseteq I$ јер $g_l\in I, l=\overline{1,\psi}$. Супротно, нека је $f\in I$ било који полином. Ако применимо алгоритам дељења из §3 да би поделили f са $\langle g_1,\ldots,g_\psi\rangle$, тада добијамо израз облика

$$f=a_1g_1+\ldots+a_\psi g_\psi+r$$

где сваки члан у r није дељив ни са једним од $LT(g_1),\ldots,LT(g_\psi)$. Тврдимо да је $r=0$.

Да би ово доказали, треба да имамо у виду

$$r=f-a_1g_1-\ldots-a_\psi g_\psi\in I.$$

Ако је $r\neq 0$, онда $LT(r)\in\langle LT(I)\rangle=\langle LT(g_1),\ldots,LT(g_\psi)\rangle$, на основу Леме 2 из §4, следи да $LT(r)$ мора бити дељиво са неким $LT(g_l)$**.** Ово је контрадикција са дефиницијом остатка , због тога r мора бити нула. Дакле,

$$f=a_1g_1+\ldots+a_\psi g_\psi+0\in\langle g_1,\ldots,g_\psi\rangle,$$

што значи да је $I\subset\langle g_1,\ldots,g_\psi\rangle$. □

База $\{g_1,\ldots,g_\psi\}$ коришћена у доказу Теореме 4, даје одговор на **Проблем описа идеала** и има специјално својство $\langle LT(I)\rangle=\langle LT(g_1),\ldots,LT(g_\psi)\rangle$.

Ако погледамо Пример 2, видимо да се све базе идеала не понашају на овај начин. Ови посебним базама даћемо име.

ВАЖНО!!!

Дефиниција 5. *Фиксирајмо мономијални поредак. За коначан подскуп* $G=\{g_1,\ldots,g_\psi\}$ *идеала* I *кажемо да је* **Гребнерова база** (*или* **стандардна база,** *означаваћемо је са* **ГБ)** ако је

$$\langle LT(I)\rangle=\langle LT(g_1),\ldots,LT(g_\psi)\rangle.$$

ВАЖНО!!!

Неформално, скуп $\{g_1,\ldots,g_\psi\}\subseteq I$ је Гребнерова база за I ако и само ако је водећи члан било ког елемента из I дељив са неким од $LT(g_l), l=\overline{1,\psi}$.

Из доказа Теореме 4 добијамо и следећу последицу.

Последица 6. *Фиксирајмо мономијални поредак. Онда сваки идеал* $I\subseteq k[x_1,\ldots,x_n]$ *различит од* $\{0\}$ *има Гребнерову базу. Осим тога, било која Гребнерова база за идеал* I *је база за* I.

Доказ. Нека је дат идеал различит од нуле, скуп $G=\{g_1,\ldots,g_\psi\}$ конструисан у доказу Теореме 4 је Гребнерова база на основу дефиниције. За други део последице, приметимо да ако је $\langle LT(I)\rangle=\langle LT(g_1),\ldots,LT(g_\psi)\rangle$, онда је на основу доказа Теореме 4 $I=\langle g_1,\ldots,g_\psi\rangle$,па је G ГБ за I.□

У одељку §6 видећемо још нека својства ГБ и решење Проблема припадности идеалу из §1.

Пример. Идеал I из Примера 2, има базу $\{f_1,f_2\}=\{x^3-2xy,x^2y-2y^2+x\}$.Скуп $\{f_1,f_2\}$ *није* ГБ за I у односу на grlex поредак. На основу Примера 2, $x^2\in\langle LT(I)\rangle$, али $x^2\notin\langle LT(f_1),LT(f_2)\rangle$. У одељку §7 показаћемо како се проналази ГБ за I.

Завршићемо овај одељак са два облика Хилбертове теореме о бази.

(а) Први је алгебарско тврђење о идеалима у $k[x_1,\ldots,x_n]$.

Растући ланац идеала је

$$I_1\subseteq I_2\subseteq I_3\subseteq\ldots$$

На пример, низ облика

$$\langle x_1\rangle\subseteq\langle x_1,x_2\rangle\subseteq\ldots\subseteq\langle x_1,\ldots,x_n\rangle \quad (1)$$

је (коначан) растући ланац идеала. Ако пробамо да *проширимо* ланац додајући идеал са генераторима , имаћемо једну од две могућности. Посматраћемо идеал $\langle x_1,\ldots,x_n,f\rangle$ где је $f\in k[x_1,\ldots,x_n]$. Ако је $f\in\langle x_1,\ldots,x_n\rangle$, онда поново добијамо $\langle x_1,\ldots,x_n\rangle$ и ништа се није променило. Ако $f\notin\langle x_1,\ldots,x_n\rangle$, онда тврдимо да је $\langle x_1,\ldots,x_n,f\rangle=k[x_1,\ldots,x_n]$.Објашњење:

$$f=a_0+p,a_0\neq 0,p\in\langle x_1,\ldots,x_n\rangle$$
$$Тада\ a_0\in\langle x_1,\ldots,x_n,f\rangle,a_0\neq 0\Rightarrow$$
$$a_0\neq 0,1\in\langle x_1,\ldots,x_n,f\rangle\Rightarrow$$
$$\langle x_1,\ldots,x_n,f\rangle=k[x_1,\ldots,x_n]$$

Као резултат наведеног, растући ланац (1) може бити настављен на два начина, или понављањем последњег идеала *до бесконачности* или додавањем $k[x_1,\ldots,x_n]$ и понављањем њега до бесконачности. У сваком случају, растући ланац ће се „стабилизовати“ после коначног броја корака, сви идеали после одређеног броја корака ће бити једнаки. Теорема 7 показује да се исто догађа у *сваком* растућем ланцу идеала у $k[x_1,\ldots,x_n]$.

Теорема 7. (Услов растућег ланца – енгл. **Ascending Chain condition,** скр. **ACC)** *Нека је*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

растући ланац идеала у $k[x_1,\dots,x_n]$. *Онда постоји* $\boldsymbol{N} \geq 1$ *такво да*

$$I_N = I_{N+1} = I_{N+2} = \dots$$

Доказ. Дат је растући ланац $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$, нека ја скуп $I = \bigcup_{l=1}^{\infty} I_l$. Показаћемо прво да је I идеал у $k[x_1,\dots,x_n]$**.** Прво, $0 \in I$ јер $0 \in I_l$ за свако l.
Даље, ако $f, g \in I$, по дефиницији, $f \in I_l$, и $g \in I_j$ за неке l и j (могу да буду и различити). Међутим, пошто су идеали I_l из растућег ланца, ако их поново означимо тако да је $l \leq j$, онда су и f и g у I_j. Како је I_j идеал, сума $f+g \in I_j$, дакле, $\in I$.Слично, ако $f \in I$ и $r \in k[x_1,\dots,x_n]$, онда $f \in I_l$ за неко l, и $r \cdot f \in I_l \subset I$.Дакле, I је идеал.

По Хилбертовој теореми о бази, идеал мора имати коначан генераторски скуп: $I = \langle f_1,\dots,f_\xi \rangle$. Сваки од генератора је садржан у неком од I_j, нека $f_l \in I_{j_i}$ за неки j_i, $i = 1,\dots,\xi$. Нека је $\boldsymbol{N}$ максимум од j_l. Онда по дефиницији растућег ланца $f_l \in I_N$ за свако l. Дакле,

$$I = \langle f_1,\dots,f_\xi \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \dots \subseteq I .$$

Растући ланац се стабилизује са I_N. Сви наредни идеали у ланцу су једнаки. □

Тврђење да се сваки растући ланац идеала у $k[x_1,\dots,x_n]$ стабилизује зове се **услов растућег ланца или енгл. ascending chain condition - ACC.** ACC ћемо користити у §7, када будемо описивали Бухбергеров алгоритам за конструисање ГБ.

(б) Други облик Хилбертове теореме о бази је геометријски.
До сада , афине варијетете сматрали смо скуповима решења посебних, коначних скупова полиномских једначина:

$$V(f_1,\dots,f_\xi) = \{(a_1,\dots,a_n) \in k^n : f_l(a_1,\dots,a_n) = 0, \text{ за свако } l\}$$

Хилбертова теорема о бази показује, да има смисла говорити о афином варијетету дефинисаном *идеалом* $I \subseteq k[x_1,\dots,x_n]$**.**

Дефиниција 8. *Нека је* $I \subseteq k[x_1,\dots,x_n]$ *идеал. Означићемо са* $V(I)$ *скуп*

$$V(I) = \{(a_1,\dots,a_n) \in k^n : f(a_1,\dots,a_n) = 0, \text{ за свако } f \in I\}.$$

Мада идеал I различит од нуле увек садржи бесконачно много различитих полинома, ипак се скуп $V(I)$ може записати коначаним скупом полиномских једначина.

Став 9. *$V(I)$ је афини варијетет.*

Специјално, ако је $I=\langle f_1,\dots,f_\xi\rangle$, онда је $V(I)=V(f_1,\dots,f_\xi)$.

§6 Својства Гребнерове базе

У §5 показали смо, да сваки идеал различит од нуле $I\subseteq k[x_1,\dots,x_n]$ има Гребнерову базу. Сада ћемо се упознати са својствима Гребнерове базе и видети на који начин можемо да проверимо да ли је дата база Гребнерова.
Прво ћемо показати шта се догађа када се дели елементима ГБ и да је у том случају остатак јединствено одређен.

Став 1. *Нека је $G=\{g_1,\dots,g_\psi\}$ Гребнерова база за идеал $I\subseteq k[x_1,\dots,x_n]$ и нека $f\in k[x_1,\dots,x_n]$. Онда постоји јединствено $r\in k[x_1,\dots,x_n]$ са следећим својствима:*

(i) *Ниједан члан од r није дељив са неким од $LT(g_1),\dots,LT(g_\psi)$*

(ii) *Постоји $g\in I$ такво да је $f=g+r$.*

Специјално, r је остатак приликом дељења f са G без обзира на редослед елемената од G код алгоритма дељења.

Остатак r се некада назива *нормалном формом од f*.
Као последицу Става 1, добијамо критеријум за одређивање припадности полинома идеалу.

ВАЖНО!!!

Последица 2. *Нека је $G=\{g_1,\dots,g_\psi\}$ Гребнерова база за идеал $I\subseteq k[x_1,\dots,x_n]$ и нека $f\in k[x_1,\dots,x_n]$. Онда $f\in I$ ако и само ако је остатак при дељењу f са G нула.*

ВАЖНО!!!

Својство дато у Последици 2. некада се узима и за дефиницију Гребнерове базе, јер се може показати да важи ако и само ако је $\langle LT(g_1),\dots,LT(g_\psi)\rangle=\langle LT(I)\rangle$.

У даљем раду користићемо следећу ознаку за остатак.

Дефиниција 3. *Остатак при дељењу f са уређеном ξ-торком $F=(f_1,\dots,f_\xi)$ означавамо са $\overline{f}^F$.*

Ако је F Гребнерова база за $\langle f_1,\dots,f_\xi\rangle$, онда можемо узети F као скуп (без неког одређеног поредка) по Ставу 1.

Пример. Нека је, $F=\left(x^2y-y^2,x^4y^2-y^2\right)\subseteq k\left[x,y\right]$, користећи лексикографски поредак,

$$\overline{x^5y}^F=xy^3.$$

На основу алгоритма дељења добијамо

$$x^5y=\left(x^3+xy\right)\left(x^2y-y^2\right)+0\cdot\left(x^4y^2-y^2\right)+xy^3.$$

Нека је дат генераторски скуп идеала.Треба да проверимо да ли је тај скуп Гребнерова база. „Препрека“ да скуп $\left\{f_1,\ldots,f_\xi\right\}$ да буде ГБ, је да постоји комбинација полинома f_l, чији водећи чланови не припадају идеалу генерисаном са $LT\left(f_l\right)$.

ВАЖНО!!!

Дефиниција 4. *Нека су* $f,g\in k\left[x_1,\ldots,x_n\right]$ *полиноми различити од нуле.*

(i) *Ако је* $multi\,deg\left(f\right)=\alpha$ *и* $multi\,deg\left(g\right)=\beta$, *и нека је* $\gamma=\left(\gamma_1,\ldots,\gamma_n\right)$, *где је* $\gamma_i=max\left(\alpha_i,\beta_i\right)$ *за свако* $i=\overline{1,n}$. **Најмањи заједнички садржалац** од $LM\left(f\right)$ и $LM\left(g\right)$, називамо x^γ и пишемо $x^\gamma=LCM\left(LM\left(f\right),LM\left(g\right)\right)$.

(ii) S **-полином** *од* f *и* g *је комбинација*

$$S\left(f,g\right)=\frac{x^\gamma}{LT\left(f\right)}\cdot f-\frac{x^\gamma}{LT\left(g\right)}\cdot g.$$

Пример. Нека су $f=x^3y^2-x^2y^3+x$ и $g=3x^4y+y^2$ у $R\left[x,y\right]$, у складу са градираним лексикографским поредком. Онда је $\gamma=\left(4,2\right)$ и

$$\begin{aligned}S\left(f,g\right)&=\frac{x^4y^2}{x^3y^2}\cdot f-\frac{x^4y^2}{3x^4y}\cdot g\\&=x\cdot f-\left(\frac{1}{3}\right)\cdot y\cdot g\\&=-x^3y^3+x^2-\left(\frac{1}{3}\right)\cdot y^3\end{aligned}$$

S-полином $S\left(f,g\right)$ је тако „дизајниран“ да доводи до скраћивања водећих чланова. Следећа лема показује да је свако скраћивање водећих чланова између полинома истог мултистепена резултат оваквог начина скраћивања.

Лема 5. *Претпоставимо да имамо суму* $\sum_{l=1}^{\xi} c_l f_l$, *где је* $c_l \in k$ *и* $multi\,deg\left(f_l\right) = \delta \in N^n$ *за свако* l. *Ако је* $multi\,deg\left(\sum_{l=1}^{\xi} c_l f_l\right) < \delta$, *онда* $\sum_{l=1}^{\xi} c_l f_l$ *је линеарна комбинација, са коефицијентима у* k, S*-полинома* $S\left(f_j, f_k\right)$ *за* $1 \le j,k \le \xi$. *Такође сваки* $S\left(f_j, f_k\right)$ *има мултистепен мањи од* δ.

Када $f_1,...,f_\xi$ задовољавају услове Леме 5, добијамо једнакост облика

$$\sum_{l=1}^{\xi} c_l f_l = \sum_{j,k} c_{jk} S\left(f_j, g_k\right).$$

Треба да видимо где долази до скраћивања. У суми са леве стране, сваки члан суме $c_l f_l$ има мултистепен δ, тако да до скраћивања долази пошто се саберу. У суми са десне стране, сваки члан суме $c_{jk} S\left(f_j, g_k\right)$ има мултистепен мањи од δ, тако да се скраћивање већ догодило.

Користећи S-полиноме и Лему 5, доказује се Бухбергеров критеријум за проверу да ли је база идеала ГБ.

ВАЖНО!!!

Теорема 6. *Нека је* I *полиномски идеал. Онда је база* $G = \left\{g_1,\ldots,g_\psi\right\}$ *за* I *ГБ ако и само ако је за сваки пар* $l \ne j$, *остатак при дељењу* $S\left(g_l, g_j\right)$ *са* G *(наведених у истом поретку) је нула.*

Теорема 6. се понекад зове „Бухбергеров критеријум S-парова“. Већ смо видели да ГБ има доста добрих особина. До сада, било је тешко одредити када је база идеала ГБ.
Користећи критеријум S-парова лако ћемо показати да је дата база ГБ.

Пример. Посматраћемо идеал $I = \left\langle y - x^2, z - x^3 \right\rangle$, уврнута кубика у R^3. Тврдимо да је $G = \left\{y - x^2, z - x^3\right\}$ ГБ за лексикографски поредак, $y > z > x$. Да би ово показали, израчунаћемо S-полином.

$$S\left(y - x^2, z - x^3\right) = \frac{yz}{y}\left(y - x^2\right) - \frac{yz}{y}\left(z - x^3\right) = -zx^2 + yx^3.$$

Користећи алгоритам дељења, добијамо

$$-zx^2 + yx^3 = x^3\left(y - x^2\right) + \left(-x^2\right)\cdot\left(z - x^3\right) + 0,$$

тако да је $\overline{S\left(y - x^2, z - x^3\right)}^{G} = 0$. Дакле по Теореми 6, G је ГБ за I.

§7 Бухбергеров алгоритам

Последица 6 из §5 , нам говори да сваки идеал у $k[x_1,\ldots,x_n]$ различит од $\{0\}$ има Гребнерову Базу. Међутим, доказ нам не говори како да је конструишемо. Можемо да поставимо проблем: како да конструишемо ГБ за дати идеал $I \subseteq k[x_1,\ldots,x_n]$?

Пример 1. Нека је дат прстен $k[x,y]$ са градираним лексикографским поредком, и нека је $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Већ смо показали да $\{f_1, f_2\}$ није Гребнерова база за I , јер $LT(S(f_1,f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.

Да би конструисали ГБ, покушаћемо да додавањем полинома у I, проширимо постојећи генераторски скуп до ГБ .

Поставља се питање ког облика треба да буду нови генератори које додајемо? У §6 видели смо да S-полиноми имају добре особине. Нека је $S(f_1,f_2) = -x^2 \in I$, и његов остатак при дељењу са $F = (f_1,f_2)$ је $-x^2$ (различит од нуле). Дакле, треба да укључимо остатак као нови генератор $f_3 = -x^2$ у наш скуп. Ако је $F = (f_1,f_2,f_3)$, на основу Теореме 6 из §6 можемо да проверимо да ли је нови скуп ГБ за I . Даље,

$$S(f_1,f_2) = f_3,$$
$$\overline{S(f_1,f_2)}^F = 0,$$
$$S(f_1,f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy,$$
$$\overline{S(f_1,f_3)}^F = -2xy \neq 0.$$

Дакле F није ГБ, па морамо додати $f_4 = -2xy$ нашем генераторском скупу. Ако је $F = (f_1,f_2,f_3,f_4)$, онда

$$\overline{S(f_1,f_2)}^F = \overline{S(f_1,f_3)}^F = 0,$$
$$S(f_1,f_4) = y(x^3 - 2xy) - \left(\frac{1}{2}\right)x^2(-2xy) = -2xy = yf_4,$$
$$\overline{S(f_1,f_4)}^F = 0,$$
$$S(f_2,f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x,$$
$$\overline{S(f_2,f_3)}^F = -2y^2 + x \neq 0.$$

Опет морамо да додамо нови генереатор $f_5 = -2y^2 + x$ скупу. Ако је $F = \{f_1,f_2,f_3,f_4,f_5\}$, може да се провери да је

$$\overline{\left(S_l, S_j\right)}^{F} = 0 \text{ за свако } 1 \le l \le j \le 5.$$

На основу Теореме 6 из §6, следи да је F Гребнерова база за I

$$\left\{f_1, f_2, f_3, f_4, f_5\right\} = \left\{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\right\}.$$

У примеру смо видели да се додавањем остатака $\overline{\left(S_l, S_j\right)}^{F}$ различитих од нуле, база F може проширити до Гребнерове базе. Ова идеја се може генерализовати и довести до Бухбергеровог алгоритма за рачунање ГБ.

Теорема 2. (Елементарна верзија Бухбергеровог алгоритма) *Нека је* $I = \left\langle f_1, \ldots, f_\xi \right\rangle \neq \{0\}$ *полиномски идеал. Онда се Гребнерова база за* I *може конструисати следећим алгоритмом у коначном броју корака:*

INPUT: $F = \left(f_1, \ldots, f_\xi\right)$

OUTPUT: a Groebner basis $G = \left(g_1, \ldots, g_\psi\right)$ for I, with $F \subseteq G$

$G = F$

REPEAT

$G' = G$

FOR each pair $\{p, q\}$, $p \neq q$ in G' DO

$S = \overline{S(p,q)}^{G'}$

IF $S \neq 0$ THEN $G = G \cup \{S\}$

UNTIL $G' = G$.

Доказ. Ако је $G = \left\{g_1, \ldots, g_\psi\right\}$, онда са $\langle G \rangle$ и $\langle LT(G) \rangle$ означавамо следеће идеале:

$$\langle G \rangle = \left\langle g_1, \ldots, g_\psi \right\rangle$$
$$\left\langle LT(G) \right\rangle = \left\langle LT\left(g_1\right), \ldots, LT\left(g_\psi\right) \right\rangle$$

Прво ћемо показати да $G \subseteq I$ остаје непромењено у сваком кораку алгоритма. Ово је тачно у почетку, и сваки пут кад повећамо G, ми додајемо остатак $S = \overline{S(p,q)}^{G'}$ за неке $p, q \in G$. Дакле, ако је $G \subseteq I$, онда су $p, q, S(p,q)$ у I, и како смо делили са $G' \subseteq I$, добијамо $G \cup \{S\} \subseteq I$. Приметимо да G садржи базу F од I, тако да је G уствари база од I.

Алгоритам се завршава када је $G' = G$, што значи да је $\overline{S(p,q)}^{G'} = 0$ за свако $p, q \in G$. На основу Теореме 6 из §6, G је Гребнерова база од $\langle G \rangle = I$.

Сада треба да покажемо да се алгоритам завршава. Треба видети шта се догађа приликом сваког пролазка кроз главну петљу. Скуп G се састоји од G'

(стари скуп G) заједно остацима S-полинома елемената од G', који су различити од нуле. Онда је

$$\langle LT(G')\rangle \subseteq \langle LT(G)\rangle \quad (1)$$

пошто је $G' \subseteq G$. Ако је $G' \neq G$, тврдимо да је $\langle LT(G')\rangle$ је строго мање од $\langle LT(G)\rangle$. Да би ово показали, претпоставимо да је $r \neq 0$ остатак од S-полинома, додат G. Пошто је r остатак при дељењу са $G', LT(r)$ није дељиво са водећим члановима елемената из G', па $LT(r) \notin \langle LT(G')\rangle$. Следи $LT(r) \in \langle LT(G)\rangle$.

На основу (1), идеали $\langle LT(G')\rangle$ су из узастопних итерација петље растућег ланца од идеала у $k[x_1,\ldots,x_n]$. На основу Теореме 7 из §5 видимо да се после коначног броја итерација ланац „стабилизује“, тако да је $\langle LT(G')\rangle = \langle LT(G)\rangle$. На основу претходног $G' = G$, тако да се алгоритам завршава после одређеног броја корака. □

Критеријум S-парова (Теорема 6 из §6) и Бухбергеров алгоритам (Теорема 2) представљају алгоритамску основу за теорију Гребнерових база.

Напомена: Ако је остатак $\overline{S(p,q)}^{G'} = 0$ он се неће променити и ако будемо додали нове елементе генераторском скупу G'. Тако да нема потребе да их поново рачунамо. Ако додамо нове генераторе f_j једном, треба само проверити за $\overline{S(f_i,f_j)}^{G'}, i < j-1$.

Описани алгоритам је елементарна верзија Бухбергеровог алгоритма. Да бисмо га оптимизовали можемо да елиминишемо непотребне генераторе користећи следећу лему.

Лема 3. *Нека је G Гребнерова база за полиномски идеал I. Нека је $p \in G$ такав полином да $LT(p) \in \langle LT(G-\{p\})\rangle$. Онда је и $G-\{p\}$ Гребнерова база за I.*

Доказ. Знамо да је $\langle LT(G)\rangle = \langle LT(I)\rangle$. Ако $\langle LT(p)\rangle \in \langle LT(G-\{p\})\rangle$, онда је $LT(G-\{p\}) = LT(G)$. На основу дефиниције је $G-\{p\}$ Гребнерова база за I. □

Прилагођавањем константи тако да сви водећи коефицијенти буду 1 и елеминисањем сваког p са $LT(p) \in \langle LT(G-\{p\})\rangle$ из G, добијамо базу коју називамо **минимална** Гребнерова база.

Дефиниција 4. Минимална Гребнерова база *за полиномски идеал* I *је Гребнерова база* G *за* I *таква:*

(i) $LC(p)=1$ *за свако* $p \in G$.

(ii) *За све* $p \in G$, $LT(p) \notin \langle LT(G-\{p\}) \rangle$.

Пример. Конструисаћемо минималну ГБ за дати идеал различит од нуле. Применом алгоритма из Теореме 2 и Леме 3 елиминисаћемо непотребне генераторе. Користићемо идеал I описан у Примеру 1. Нашли смо Гребнерову базу

$$f_1 = x^3 - 2xy,$$
$$f_2 = x^2 y - 2y^2 + x,$$
$$f_3 = -x^2,$$
$$f_4 = -2xy,$$
$$f_5 = -2y^2 + x$$

Неки од водећих коефицијената су различити од 1, први корак је да помоножимо генераторе са одговарајућом константом. Приметимо да је $LT(f_1) = x^3 = -x \cdot LT(f_3)$. На основу Леме 3, можемо изоставити f_1 у минималној Гребнеровој бази. Слично, како је $LT(f_2) = x^2 y = -\left(\frac{1}{2}\right) x \cdot LT(f_4)$, можемо елиминисати f_2. Нема више случајева где водећи члан једног генератора дели водећи члан другог генератора. Дакле,

$$\overline{f_3} = x^2, \overline{f_4} = xy, \overline{f}_5 = y^2 - \left(\frac{1}{2}\right) x$$

је минимална Гребнерова база за I.

На жалост, идеал може имати више минималних Гребнерових база. За дати идеал, такође је и ово минимална Гребнерова база, где је $a \in k$ било која константа.

$$\overline{f_3} = x^2 + axy, \overline{f_4} = xy, \overline{f}_5 = y^2 - \left(\frac{1}{2}\right) x \quad (2)$$

Срећом можемо да одаберемо минималну ГБ са најбољим особинама.

Дефиниција 5. **Редукована Гребнерова база** *за идеал* I *је Гребнерова база* G *за* I *таква да*:

(i) $LC(p)=1$ *за свако* $p \in G$

(ii) *За свако* $p \in G$, *нема монома од* p *који се налазе у* $\langle LT(G-\{p\}) \rangle$.

Приметимо, да је Гребнерова база (2) у Примеру редукована за $a = 0$.

Став 6. *Нека је* $I \neq \{0\}$ *полиномски идеал. Онда, за дати мономијални поредак,* I *има* ***јединствену****, редуковану Гребнерову базу.*

Доказ. Нека је G минимална ГБ база за I. Кажемо да је $g \in G$**, *редукован*** за G под условом да ниједан моном од g не припада $\langle LT(G-\{p\})\rangle$. Наш циљ је да модификујемо G док се сви његови елементи не редукују.

Приметимо, да ако је g редуковано за G, онда је g редуковано за било коју минималну ГБ за I која садржи g и има исти скуп водећих чланова. Ово важи јер дефиниција о редуковању укључује само водеће чланове.

Даље, дат је $g \in G$ и нека је $g' = \overline{g}^{G-\{g\}}$ и скуп $G' = (G-\{g\}) \cup \{g'\}$. Тврдимо да је G' минимална Гребнерова база за I. Да би ово показали, приметимо да је $LT(g') = LT(g)$, када делимо g са $G-\{g\}$, $LT(g)$ иде у остатак јер није дељиво ни са једним од елемента од $LT(G-\{g\})$. Значи $\langle LT(G')\rangle = \langle LT(G)\rangle$. Како је G' сигурно садржано у I, G' је ГБ, и њена минималност следи.
На крају, приметимо да је g' редуковано за G' на основу његове конструкције.

Узећемо елементе од G и применићемо претходни поступак док сви не буду редуковани. ГБ се може променити сваки пут, али приметили смо да ако је један елеменат редукован, он остаје редукован јер никада не мењамо водеће чланове. Дакле, завршићемо са редукованом ГБ.

Да би доказали јединственост, претпоставимо да су G и $\overline{G}$ редуковане ГБ базе за I. Специјално, G и $\overline{G}$ су минималне ГБ.
Нека је дато $g \in G$, постоји $\overline{g} \in \overline{G}$ такво да је $LT(g) = LT(\overline{g})$. Ако покажемо да је $g = \overline{g}$, следиће да је $G = \overline{G}$, и важиће јединственост.

Да би показали да је $g = \overline{g}$, посматрамо разлику $g - \overline{g}$. Разлика припада I, и како је G ГБ, следи да је $\overline{g - \overline{g}}^{G} = 0$. Знамо да је $LT(g) = LT(\overline{g})$. Ови чланови се скраћују у $g - g'$,а преостали чланови нису дељиви ни са једним од $LT(G) = LT(\overline{G})$, G и $\overline{G}$ су редуковани. Ово показује да је $\overline{g - \overline{g}}^{G} = g - \overline{g}$, и $g - \overline{g} = 0$. □

Компјутерски, алгебарски системи користе неке од верзија Бухбергеровог алгоритма. Ови системи увек рачунају ГБ чији су елементи константни умношци елемената у редукованим ГБ. То значи да ће у суштини дати исте одговоре за дати проблем. Дакле, одговори могу бити лако проверавани са једног система на други.

Друга последица јединствености из Става 6 је **алгоритам за једнакост идеала.** Из алгоритма можемо да видимо када два скупа полинома

$\{f_1,\ldots,f_\xi\},\{g_1,\ldots,g_\psi\}$ генеришу исти идеал: једноставно фиксирамо мономијални поредак и рачунамо редуковану Гребнерову базу за $\langle f_1,\ldots,f_\xi\rangle$ и $\langle g_1,\ldots,g_\psi\rangle$.

Идеали једнаки ако и само ако су Гребнерове базе исте.

§8 Прве примене Гребнерове базе

У §1 смо описали четири проблема везана за идеале и варијетете. Први Проблем описа идеала, је решен уз помоћ Хилбертове теореме о бази у §5. Сада ћемо се позабавити са преостала три проблема и видети у којој мери можемо да их решимо уз помоћ Гребнерових база.

А. Проблем описа идеала

Да ли сваки идеал $I \subseteq k[x_1,\ldots,x_n]$ *има коначан генераторски скуп?*

Решење :Теорема 4. (Хилбертова теорема о бази) из §5
Сваки идеал $I \subseteq k[x_1,\ldots,x_n]$ има **коначан** генераторски скуп.
Значи, $I = \langle g_1,\ldots,g_\psi \rangle$ за неке $g_1,\ldots,g_\psi \in I$.

Б. Проблем припадности идеалу

Нека је дат полином $f \in k[x_1,\ldots,x_n]$ и идеал $I = \langle f_1,\ldots,f_\xi \rangle$. Да ли $f \in I$?

Решење: Ако повежемо Гребнерове Базе са алгоритмом дељења, добићемо **алгоритам за одређивање припадности идеалу.** Нека је дат идеал $I = \langle f_1,\ldots,f_\xi \rangle$. Треба да видимо у ком случају дати полином f припада I. Користићемо алгоритам сличан Теореми 2 из §7, да би пронашли Гребнерову базу $G = \{g_1,\ldots,g_\psi\}$ за I. На основу Последице 2 из §6 важи

$$f \in I \text{ ако и само ако } \overline{f}^G = 0.$$

Пример 1. Нека $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \in C[x,y,z]$, и нека је фиксиран градирани лексикографски поредак. Нека је $f = -4x^2y^2z^2 + y^6 + 3z^5$. Желимо да проверимо да ли $f \in I$.

Генераторски скуп није Гребнерова база од I, јер $L(T)$ садржи полиноме $LT(S(f_1,f_2)) = LT(-x^2y^2 + z^3) = x^2y^2$ који не припадају идеалу $\langle LT(f_1), LT(f_2) \rangle = \langle xz, x^3 \rangle$. Дакле, треба да конструишемо ГБ за I. Проналазимо да је ГБ $G = (f_1,f_2,f_3,f_4,f_5) = (xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5)$. Ово је редукована база.

Сада можемо да проверимо да ли полиноми припадају I. Када поделимо f са G, добијамо

$$f = 0 \cdot f_1 + 0 \cdot f_2 - 4z^2 f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0$$

Како је остатак нула, следи да $f \in I$.

За други пример, узмимо да је $f = xy - 5z^2 + x$. Чак и без рачунања остатка приликом дељења са G, можемо да видимо, из облика елемената у G да $f \notin I$. Зато што $LT(f) = xy$ није у идеалу $\langle LT(G) \rangle = \langle xz, x^3, x^2y^2, xy^4, y^6 \rangle$. Дакле, $\overline{f}^G \neq 0$, тако да $f \notin I$.

B. Проблем решавања полиномских једначина

Наћи сва заједничка решења у k^n система полиномских једначина

$$f_1(x_1, \ldots, x_n) = \ldots = f_\xi(x_1, \ldots, x_n) = 0.$$

Решење:
Сада ћемо начин рада са ГБ применити на решавање система полиномских једначина више променљивих.

Пример 2. Посматраћемо једначине облика

$$\begin{aligned} &x^2 + y^2 + z^2 = 1, \\ &x^2 + z^2 = y \qquad (1) \\ &x = z \end{aligned}$$

у C^3. Ове једначине одређене су идеалом $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subset C[x, y, z]$, и желимо да пронађемо све тачке у $V(I)$. На основу Става 9 из §5 можемо да израчунамо $V(I)$ користећи било коју базу од I. Видећемо шта се догађа ако будемо користили Гребнерову базу.
Рачунаћемо ГБ на I у складу са lex поредком. База је

$$\begin{aligned} g_1 &= x - z, \\ g_2 &= -y + 2z^2, \\ g_3 &= z^4 + \left(\frac{1}{2}\right) z^2 - \frac{1}{4}. \end{aligned}$$

Полином g_3 зависи само од z, и његов корен је

$$z = \pm \frac{1}{2} \sqrt{\pm\sqrt{5} - 1}.$$

Када се вредности z за замене у једначине $g_2 = 0$ и $g_1 = 0$, добијамо јединствена решења по y и x. Постоје четири решења за $g_1 = g_2 = g_3 = 0$, два реална и два

комплексна. Како је $V(I)=V(g_1,g_2,g_3)$ на основу Ставу 9 из §5, добили смо сва решења једначина (1).

Пример 3. Дат је систем полиномских једначина, добијених применом Лагранжевог метода за проналажење миниманих и максималних вредности од $x^3+2xyz-z^2$ при услову $x^2+y^2+z^2=1$:

$$\begin{aligned}
&3x^2+2yz-2x\lambda=0,\\
&2xz-2y\lambda=0,\\
&2xy-2z-2z\lambda=0,\\
&x^2+y^2+z^2-1=0.
\end{aligned}$$

Прво рачунамо ГБ за идеал у $R[x,y,z,\lambda]$ генерисан левом страном ове четири једначине, у складу са лексикографским поредком са $\lambda>x>y>z$. Гребнерова база је :

$$\begin{aligned}
&\lambda-\frac{3}{2}x-\frac{3}{2}yz-\frac{167616}{3835}z^6-\frac{36717}{590}z^4-\frac{134419}{7670}z^2\\
&x^2+y^2+z^2-1\\
&xy-\frac{19584}{3835}z^5+\frac{1999}{295}z^3-\frac{6403}{3835}z,\\
&xz+yz^2-\frac{1152}{3835}z^5-\frac{108}{295}z^3+\frac{2556}{3835}z,\\
&y^3+yz^2-y-\frac{9216}{3835}z^5+\frac{906}{295}z^3-\frac{2562}{3835}z,\\
&y^2z-\frac{6912}{3835}z^5+\frac{827}{295}z^3-\frac{3839}{3835}z,\\
&yz^3-yz-\frac{576}{59}z^6+\frac{1605}{118}z^4-\frac{453}{118}z^2,\\
&z^7-\frac{1763}{1152}z^5+\frac{655}{1152}z^3-\frac{11}{288}z
\end{aligned}\qquad (2)$$

Овај скуп полинома делује застрашујуће. (Коефицијенти елемената ГБ много су компликованији, него коефицијенти почетног скупа.). Последњи полином зависи само од променљиве z. У процесу тражења ГБ елиминисали смо остале променљиве. (Чудесно☺) једначина добијена изједначавањем овог полинома са нулом има следеће корене

$$z=0,\pm1,\pm\frac{2}{3},\pm\frac{\sqrt{11}}{8\sqrt{2}}.$$

Ако z изједначимо са сваком од ових вредности, преостале једначине можемо да решимо по y,x (и λ, његове вредности тренутно нам нису битне). Добијамо следећа решења:

$$z = 0; y = 0; x = \pm 1.$$
$$z = 0; y = \pm 1; x = 0.$$
$$z = \pm 1; y = 0; x = 0.$$
$$z = \frac{2}{3}; y = \frac{1}{3}; x = -\frac{2}{3}.$$
$$z = \frac{\sqrt{11}}{8\sqrt{2}}; y = -\frac{3\sqrt{11}}{8\sqrt{2}}; x = -\frac{3}{8}.$$
$$z = -\frac{\sqrt{11}}{8\sqrt{2}}; y = \frac{3\sqrt{11}}{8\sqrt{2}}; x = -\frac{3}{8}.$$

Одавде можемо лако да одредимо минималне и максималне вредности.

Пример 2 и Пример 3 показују да је проналажење ГБ за идеал у складу са лексикографским поредком битно поједностављује облик једначина. Добијамо једначине из којих можемо лако да елиминишемо променљиве. Редослед елиминације је повезан са поредком променљивих. У Примеру 3 је $\lambda > x > y > z$ и у (2) прво се елимише λ, затим x, и тако даље.

Систем једначина у добијеном облику лако се решава, последња једначина има само једну променљиву. За њу користимо технику решавања једначине једне променљиве. Прво нађемо њене корене и заменимо их у преостале једначине система. На тај начин проналазимо остала решења.

Г. Импликацијски проблем

Нека је V подскуп од k^n задат параметарски

$$\begin{aligned} x_1 &= g_1(t_1,\ldots,t_m),\\ &\vdots\\ x_n &= g_n(t_1,\ldots,t_m). \end{aligned}$$

Ако су g_l полиноми (или рационалне функције) које зависе од променљивих t_j, онда ће V бити афини варијетет или његов део. Наћи систем полиномских једначина таквих да дефинишу варијетет.

Решење:
Дате параметарске једначине

$$\begin{aligned} x_1 &= f_1(t_1,\ldots,t_m),\\ &\vdots\\ x_n &= f_n(t_1,\ldots,t_m). \end{aligned} \qquad (3)$$

дефинишу подскуп алгебарског варијетета V у k^n.

Нека су f_l полиноми и афини варијетет у k^{n+m} дефинисан горе наведеним једначинама или

$$\begin{aligned} &x_1 - f_1(t_1,\ldots,t_m) = 0,\\ &\vdots\\ &x_n - f_n(t_1,\ldots,t_m) = 0. \end{aligned}$$

Треба елиминисати променљиве $t_1,\ldots,t_m$ из једначина.На основу тога добићемо једачине за V.

Као и до сада променљиве ћемо елиминисати уз помоћ Гребнерових база. Користићемо и лексикографски поредак у $k[t_1,\ldots,t_m,x_1,\ldots,x_n]$ дефинисан са

$$t_1 > \ldots > t_m > x_1 > \ldots > x_n.$$

Нека је дата ГБ за идеал $\bar{I} = \langle x_1 - f_1,\ldots,x_n - f_n\rangle$. Како користимо лексикографски поредак, очекујемо да ГБ има полиноме који ће елиминисати променљиве и $t_1,\ldots,t_m$ ће бити први елиминисани. Они су највећи у датом мономијалном поредку. На основу тога ГБ за $\bar{I}$ садржаће полиноме који зависе од $x_1,\ldots,x_n$. Они се кандидидују за једначине од V.

Пример 4. Нека је дата параметарска крива V

$$\begin{aligned} x &= t^4,\\ y &= t^3,\\ z &= t^2 \end{aligned}$$

у C^3.Можемо да израчунамо ГБ G од $I = \langle t^4 - x, t^3 - y, t^2 - z\rangle$, у складу са лексикографским поредком у $C[t,x,y,z]$

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

Последња два полинома зависе од x,y,z. Они дефинишу афини варијетет у C^3 који садржи криву V. Интуитивно, могли би да претпоставимо да те две једначине у дефинишу криву (1- димензионални варијетет) C^3. Да ли је V пресек ове две површи ?

$$x - z^2 = 0, y^2 - z^3 = 0$$

Да ли могу друге криве (или чак површине) да буду у пресеку?
Гребнерове базе не дају комплетан одговор на ово питање.

5 Примене у роботици

Робот конобар има задатак да послужи кафу на одређеном месту. Наш задатак је да видимо да ли ће успети у томе.

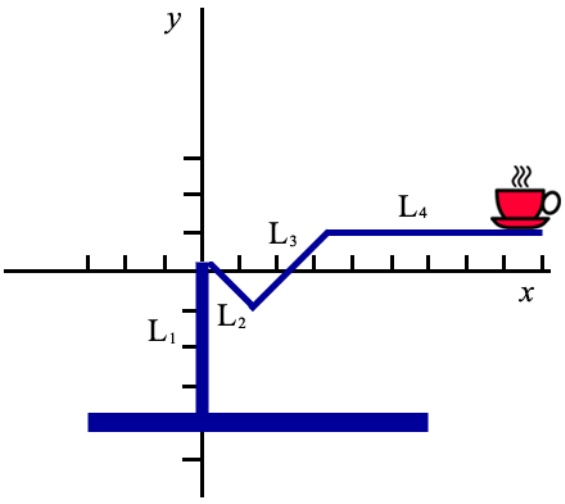
За почетак сместићемо робота у дводимензионалну раван и посматраћемо покрете његове руке. Приказ руке ће бити поједностављен. Она ће се састојати од четири равна дела дужина l_1, l_2, l_3, l_4 повезана са три зглоба. Први део l_1 је причвршћен за под (односно у нашој равни он је вертикалан и фиксиран). Крај од l_1, први зглоб, је почетак координатног система. Шољица кафе се налази на послужавнику (последњи део l_4) . Послужавник мора бити у хоризонталном положају да се не би пролила кафа.

Нека је θ_i угао који део l_i гради са позитивним делом x осе ($\theta_1 = 90°$ и $\theta_4 = 0°$). Фиксирамо дужине $l_2 = 1, l_3 = 3, l_4 = 5$.

Задатак: Да ли робот може да послужи кафу на месту (x, y) у односу на координатни почетак ?

Решење: Да би то проверили морамо да пронађемо решења следећих једначина.

$$l_2 \cos\theta_2 + l_3 \cos\theta_3 + l_4 = x$$
$$l_2 \sin\theta_2 + l_3 \sin\theta_3 = y$$



Слика 1. Конобар робот служи кафу

На први поглед не можемо да видимо како ће нам Гребнерове базе олакшати решавање једначина. Променљиве θ_i су садржане у тригонометријским функцијама. „Трик“ је да се за $\cos\theta_i, \sin\theta_i$ уведе смена c_i, s_i и да се замени у

систему са $c_i^2 + s_i^2 - 1 = 0$. Заменом ових вредности и фиксираних вредности l_i добијамо

$$c_2 + 3c_3 + 5 = x$$
$$s_2 + 3s_3 = y$$
$$c_2^2 + s_2^2 = 1$$
$$c_3^2 + s_3^2 = 1$$

Дајући партикуларне вредности за x, y желимо да одредимо c_2, s_2, c_3, s_3. (Ово је тзв. Инверзни Кинематички проблем). Поново напишемо систем користећи лексикографски поредак дефинисан са $c_2 > c_3 > s_2 > s_3$

$$\begin{aligned} c_2^2 + s_2^2 - 1 &= 0 \\ c_2 + 3c_3 + 5 - x &= 0 \\ c_3^2 + s_3^2 - 1 &= 0 \\ s_2 + 3s_3 - y &= 0 \end{aligned} \quad (1)$$

Посматраћемо неке карактеристичне тачке за послуживање кафе (x, y):

1. $(x, y) = (6, 2)$

Из система (1) за вредност $(x, y) = (6, 2)$ добијамо редуковану Гребнерову базу

$$c_3 + 3s_3 - \left(\frac{13}{6}\right)$$
$$c_2 + 6s_3 - \left(\frac{11}{2}\right)$$
$$s_3^2 - \left(\frac{26}{15}\right)s_3 + \left(\frac{133}{180}\right)$$
$$s_2 + 3s_3 - 2$$

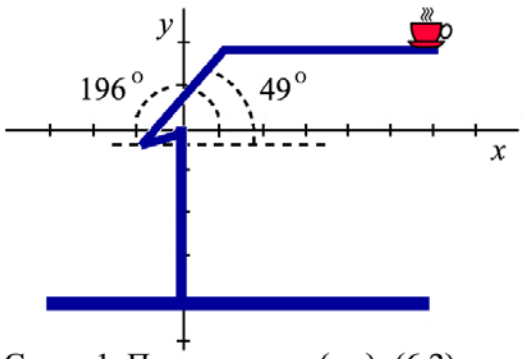
Сваки од ових полинома изједначимо са нулом , решимо једначину која зависи од једне променљиве s_3 и заменимо решења да би добили c_2, c_3, s_2. Из израза који зависе од θ_2, θ_3 добијамо два решења

(а) $(\theta_2, \theta_3) = (196°, 49°)$ (погледати Слику 2)

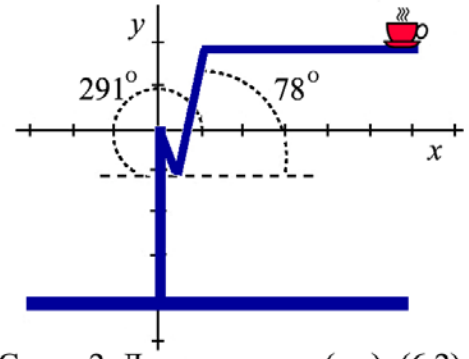
(б) $(\theta_2, \theta_3) = (291°, 78°)$ (погледати Слику 3)

Дакле, рука може бити у две положаја за $(x, y) = (6, 2)$.

Робот ће успети да послужи кафу! Добиће бакшиш.



Слика 1. Прво решење $(x,y)=(6,2)$



Слика 2. Друго решење $(x,y)=(6,2)$

2. $(x,y)=(6,-1)$

Из система (1) за вредност $(x,y)=(6,-1)$ добијамо редуковану Гребнерову базу

$$c_3 - s_3 - \left(\frac{5}{3}\right)$$
$$c_2 + 3s_3 + 4$$
$$s_3^2 + \left(\frac{5}{3}\right)s_3 + \left(\frac{8}{9}\right)$$
$$s_2 + 3s_3 + 1$$

Ако покушамо да решимо полиномску једначину која зависи од једне променљиве s_3 видећемо да се нешто чудно дешава. Једначина је облика ax^2+bx+c и њена решења су $x=\frac{\left(-b\pm\sqrt{b^2-4ac}\right)}{2a}$. Добијамо да је $b^2-4ac=-\frac{7}{9}<0$.Дакле, постоји имагинарни корен и нема реалних решења система.

Робот неће успети да послужи кафу! Остаће без бакшиша.

3. $(x,y)=(5,10)$

Из система (1) за вредност $(x,y)=(5,10)$ добијамо редуковану Гребнерову базу

$$s_3 - \left(\frac{9}{5}\right)$$
$$c_2 + 3c_3$$
$$c_3^2 + \left(\frac{56}{25}\right)$$
$$s_2 - \left(\frac{23}{5}\right)$$

Сва решења дају вредности промењљивих чији је опсег већи од један (на пример $s_2 = \frac{23}{5}, s_3 = \frac{9}{5}$). То је противречи услову да су промењљиве косинусне и синусне функције и да њихове вредности не могу бити веће од 1.

И у овом случају кафа неће бити послужена!!

4. $(x, y) = (5, 0)$

Из система (1) за вредност $(x, y) = (5, 0)$ добијамо редуковану Гребнерову базу

1

Из овога се одмах види да нема решења.

Кафа неће бити послужена!!

Напомене:

1) Претходно изложени проблем је доста поједностављен. Може се конструисати много реалнији проблем са руком робота у три димензије.

2) Уместо да служи кафу, робот може да ради и са шрафцигером. У том случају морамо задати, поред коначних координата (x, y) и орјентацију $0 \le \phi \le 2\pi$ (или смер „увртања“). Тако да глава шрафцигера заврће вијак.

3) Координатни систем може се одабрати и на други начин, тако да се добију компликованије полиномске једначине (на пример полиноми већег степена). У пракси, често се користи да је θ_i угао између l_i и l_{i-1} (θ_1 је фискиран на $90°$).

4) Ако је потребно да се одреде вредности свих промењљивих (можда једне или две), мора да се води рачуна о избору лексикографског поредка. У овом примеру имали смо $4! = 24$ могућа избора, и одабрали смо поредак који нам прво даје s_3 . У

општем случају, променљиву коју желимо прву да добијемо, стављамо лексикографски последњу.

6 Задатак

Посматрамо полиномијални прстен над пољем $\boldsymbol{Z_2}$ са три променљиве, дакле $Z_2[x,y,z]$. Да ли елеменат z^2 припада идеалу генерисаном полиномима $x^3+z, x^2y+xz+y^2, x^2z+yz$?

Решење: Ако повежемо Гребнерове Базе са алгоритмом дељења, добићемо **алгоритам за одређивање припадности идеалу.** Нека је дат идеал $I=\langle f_1,f_2,f_3\rangle$. Треба да видимо у ком случају дати полином f припада I. Користићемо алгоритам сличан Теореми 2 из §7, да би пронашли Гребнерову базу $G=\{g_1,\ldots,g_\psi\}$ за I. На основу Последице 2 из §6 важи

$$f\in I \text{ ако и само ако } \overline{f}^{G}=0.$$

Нека $I=\langle f_1,f_2,f_3\rangle=\langle x^3+z,x^2y+xz+y^2,x^2z+yz\rangle$, и нека је фиксиран лексикографски поредак. Нека је $f=z^2$. Желимо да проверимо да ли $f\in I$. Треба да конструишемо ГБ за I.

$$B=\{f_1,f_2,f_3\}$$
$$S(f_1,f_2)=\frac{x^3y}{x^3}(x^3+z)-\frac{x^3y}{x^2y}(x^2y+xz+y^2)=$$
$$y(x^3+z)-(x^2y+xz+y^2)=$$
$$x^3y+yz-x^3y-x^2z-xy^2=$$
$$-x^2z-xy^2+yz=-f_3-xy^2$$

* $f_4=-xy^2, B=\{f_1,f_2,f_3,f_4\}$
$$S(f_1,f_2)=-f_3+f_4, \overline{S(f_1,f_2)}^{B}=0$$

$$S(f_1,f_3)=\frac{x^3z}{x^3}\left(x^3+z\right)-\frac{x^3z}{x^2z}\left(x^2z+yz\right)=$$
$$z\left(x^3+z\right)-x\left(x^2z+yz\right)=$$
$$x^3z+z^2-x^3z-xyz=-xyz+z^2$$

$$* f_5=-xyz+z^2,\ B=\{f_1,f_2,f_3,f_4,f_5\}$$

$$S(f_1,f_3)=f_5,\overline{S(f_1,f_3)}^B=0$$
$$S(f_1,f_4)=\frac{x^3y^2}{x^3}\left(x^3+z\right)-\frac{x^3y^2}{-xy^2}\left(-xy^2\right)=$$
$$y^2\left(x^3+z\right)-x^3y^2=$$
$$x^3y^2+y^2z-x^3y^2=y^2z$$

$$* f_6=y^2z,\ B=\{f_1,f_2,f_3,f_4,f_5,f_6\}$$
$$S(f_1,f_4)=f_6,\overline{S(f_1,f_4)}^B=0$$

$$S(f_1,f_5)=\frac{x^3yz}{x^3}\left(x^3+z\right)-\frac{x^3yz}{-xyz}\left(-xyz+z^2\right)=$$
$$yz\left(x^3+z\right)+x^2\left(-xyz+z^2\right)=$$
$$x^3yz+yz^2-x^3yz+x^2z^2=yz^2+x^2z^2=zf_3$$
$$\overline{S(f_1,f_5)}^B=0$$

$$S(f_1,f_6)=\frac{x^3y^2z}{x^3}\left(x^3+z\right)-\frac{x^3y^2z}{y^2z}\left(y^2z\right)=$$
$$x^3y^2z+y^2z^2-x^3y^2z=y^2z^2=zf_6$$
$$\overline{S(f_1,f_6)}^B=0$$

$$S(f_2,f_3)=\frac{x^2yz}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2yz}{x^2z}\left(x^2z+yz\right)=$$
$$z\left(x^2y+xz+y^2\right)-y\left(x^2z+yz\right)=$$
$$x^2yz+xz^2+y^2z-x^2yz-y^2z=xz^2$$

$$* f_7=xz^2,\ B=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7\}$$
$$S(f_2,f_3)=f_7,\overline{S(f_2,f_3)}^B=0$$

$$S(f_1,f_7)=\frac{x^3z^2}{x^3}\left(x^3+z\right)-\frac{x^3z^2}{xz^2}xz^2=$$
$$z^2\left(x^3+z\right)-x^3z^2=z^3$$

$$*\ f_8=z^3\ ,B=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8\}$$
$$S(f_1,f_7)=f_8,\overline{S(f_1,f_7)}^B=0$$

$$S(f_1,f_8)=\frac{x^3z^3}{x^3}\left(x^3+z\right)-\frac{x^3z^3}{z^3}z^3=z^4=zf_8$$
$$S(f_1,f_8)=zf_8,\overline{S(f_1,f_8)}^B=0$$

$$S(f_2,f_4)=\frac{x^2y^2}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2y^2}{-xy^2}\left(-xy^2\right)=$$
$$y\left(x^2y+xz+y^2\right)-x^2y^2=x^2y^2+xyz+y^3-x^2y^2=$$
$$xyz+y^3=$$
$$-\left(-xyz+z^2\right)+\left(y^3+z^2\right)=f_5+\left(y^3+z^2\right)$$

$$*\ f_9=y^3+z^2\ ,B=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8,f_9\}$$
$$S(f_2,f_4)=f_5+f_9,\overline{S(f_2,f_4)}^B=0$$

$$S(f_1,f_9)=\frac{x^3y^3}{x^3}\left(x^3+z\right)-\frac{x^3y^3}{y^3}\left(y^3+z^2\right)=$$
$$y^3\left(x^3+z\right)-x^3\left(y^3+z^2\right)=-x^3z^2+y^3z=-x^2f_7+yf_6$$
$$\overline{S(f_1,f_9)}^B=0$$

$$S(f_2,f_5)=\frac{x^2yz}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2yz}{-xyz}\left(-xyz+z^2\right)=$$
$$z\left(x^2y+xz+y^2\right)+x\left(-xyz+z^2\right)=$$
$$x^2yz+xz^2+y^2z+\left(-x^2yz\right)+xz^2=y^2z=f_6$$
$$\overline{S(f_2,f_5)}^B=0$$

$$S(f_2,f_6)=\frac{x^2y^2z}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2y^2z}{y^2z}y^2z=$$

$$yz\left(x^2y+xz+y^2\right)-x^2y^2z=$$

$$x^2y^2z+xyz^2+y^3z-x^2y^2z=y\left(xz^2\right)+z\left(y^2z\right)=$$

$$=yf_7+yf_6$$

$$\overline{S(f_2,f_6)}^B=0$$

$$S(f_2,f_7)=\frac{x^2yz^2}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2yz^2}{y^2z}xz^2=$$

$$z^2\left(x^2y+xz+y^2\right)-x^2yz^2=$$

$$z\left(xz^2\right)+z\left(y^2z\right)=zf_7+zf_6$$

$$\overline{S(f_2,f_7)}^B=0$$

$$S(f_2,f_8)=\frac{x^2yz^3}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2yz^3}{z^3}z^3=$$

$$z^3\left(x^2y+xz+y^2\right)-x^2yz^3=xz^4+y^2z^3=z^2f_7+z^2f_6$$

$$\overline{S(f_2,f_8)}^B=0$$

$$S(f_2,f_9)=\frac{x^2y^3}{x^2y}\left(x^2y+xz+y^2\right)-\frac{x^2y^3}{y^3}\left(y^3+z^2\right)=$$

$$y^2\left(x^2y+xz+y^2\right)-x^2\left(y^3+z^2\right)=$$

$$xy^2z+y^4-x^2z^2=-yf_5-zf_3+y^4$$

$$*\ f_{10}=y^4,\ B=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8,f_9,f_{10}\}$$

$$S(f_2,f_9)=-yf_5-zf_3+f_{10},\overline{S(f_2,f_9)}^B=0$$

$$S(f_1,f_{10})=\frac{x^3y^4}{x^3}\left(x^3+z\right)-\frac{x^3y^4}{y^4}\left(y^4\right)=$$

$$y^4\left(x^3+z\right)-x^3y^4=y^4z=zf_{10}$$

$$\overline{S(f_1,f_{10})}^B=0$$

$$S(f_3,f_4)=\frac{x^2y^2z}{x^2z}\left(x^2z+yz\right)-\frac{x^2y^2z}{-xy^2}\left(-xy^2\right)=yy^2z=yf_6$$

$$\overline{S(f_3,f_4)}^B=0$$

$$S(f_3,f_5)=\frac{x^2yz}{x^2z}\left(x^2z+yz\right)-\frac{x^2yz}{-xyz}\left(-xyz+z^2\right)=y^2z+xz^2=f_6+f_7$$

$$\overline{S(f_3,f_5)}^{B}=0$$

$$S(f_3,f_6)=\frac{x^2y^2z}{x^2z}\left(x^2z+yz\right)-\frac{x^2y^2z}{y^2z}y^2z=y^3z$$

$$\overline{S(f_3,f_6)}^{B}=0$$

$$S(f_3,f_7)=\frac{x^2z^2}{x^2z}\left(x^2z+yz\right)-\frac{x^2z^2}{xz^2}xz^2=yz^2$$

* $f_{11}=yz^2$, $B=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8,f_9,f_{10},f_{11}\}$

$$S(f_1,f_{11})=\frac{x^3yz^2}{x^3}\left(x^3+z\right)-\frac{x^3yz^2}{yz^2}y^2z=yz^3=zf_{11}$$

$$\overline{S(f_1,f_{11})}^{B}=0$$

$$S(f_3,f_8)=\frac{x^2z^3}{x^2z}\left(x^2z+yz\right)-\frac{x^2z^3}{z^3}z^3=yz^2z=zf_{11}$$

$$\overline{S(f_3,f_8)}^{B}=0$$

$$S(f_3,f_9)=\frac{x^2y^3z}{x^2z}\left(x^2z+yz\right)-\frac{x^2y^3z}{y^3}\left(y^3+z^2\right)=zy^4-x^2z^3=$$

$$zf_{10}-xzf_7$$

$$\overline{S(f_3,f_9)}^{B}=0$$

$$S(f_3,f_{10})=\frac{x^2y^4z}{x^2z}\left(x^2z+yz\right)-\frac{x^2y^4z}{y^4}y^4=yzy^4=yzf_{10}$$

$$\overline{S(f_3,f_{10})}^{B}=0$$

$$S(f_3,f_{11})=\frac{x^2yz^2}{x^2z}\left(x^2z+yz\right)-\frac{x^2yz^2}{yz^2}yz^2=y^2z^2=zf_6$$

$$\overline{S(f_3,f_{11})}^{B}=0$$

$$S(f_4,f_5)=\frac{xy^2z}{-xy^2}\left(-xy^2\right)-\frac{xy^2z}{xyz}\left(-xyz+z^2\right)=yz^2$$

$$\overline{S(f_4,f_5)}^B = 0$$

$$S(f_4,f_6) = 0, \overline{S(f_4,f_6)}^B = 0$$
$$S(f_4,f_7) = 0, \overline{S(f_4,f_7)}^B = 0$$
$$S(f_4,f_8) = 0, \overline{S(f_4,f_8)}^B = 0$$
$$S(f_4,f_9) = \frac{xy^3}{-xy^2}\left(-xy^2\right) - \frac{xy^3}{y^3}\left(y^3+z^2\right) = -xz^2 = -f_7$$
$$\overline{S(f_4,f_9)}^B = 0$$

$$S(f_4,f_{10}) = \frac{xy^4}{-xy^2}\left(-xy^2\right) - \frac{xy^4}{y^4}y^4 = 0$$
$$\overline{S(f_4,f_{10})}^B = 0$$

$$S(f_4,f_{11}) = \frac{xy^2z^2}{-xy^2}\left(-xy^2\right) - \frac{xy^2z^2}{yz^2}yz^2 = 0$$
$$\overline{S(f_4,f_{11})}^B = 0$$

$$S(f_5,f_6) = \frac{xy^2z}{-xyz}\left(-xyz+z^2\right) - \frac{xy^2z}{y^2z}y^2z = -yz^2 = -f_{11}$$
$$\overline{S(f_5,f_6)}^B = 0$$

$$S(f_5,f_7) = \frac{xyz^2}{-xyz}\left(-xyz+z^2\right) - \frac{xyz^2}{xz^2}xz^2 = z^3 = f_8$$
$$\overline{S(f_5,f_7)}^B = 0$$

$$S(f_5,f_8) = \frac{xyz^3}{-xyz}\left(-xyz+z^2\right) - \frac{xyz^3}{z^3}z^3 = -z^4 = -zf_8$$
$$\overline{S(f_5,f_8)}^B = 0$$

$$S(f_5,f_9) = \frac{xy^3z}{-xyz}\left(-xyz+z^2\right) - \frac{xy^3z}{y^3}\left(y^3+z^2\right) = -y^2z^2 - xz^3 = -f_6 - zf_7$$
$$\overline{S(f_5,f_9)}^B = 0$$

$$S\left(f_5,f_{10}\right)=\frac{xy^4z}{-xyz}\left(-xyz+z^2\right)-\frac{xy^4z}{y^4}\left(y^4\right)=$$

$$-y^3\left(-xyz+z^2\right)-xy^4z=xy^4z-y^3z^2-xy^4z=-y^3z^2=-yz^2y^2=-yzf_6$$

$$\overline{S\left(f_5,f_{10}\right)}^B=0$$

$$S\left(f_5,f_{11}\right)=\frac{xyz^2}{-xyz}\left(-xyz+z^2\right)-\frac{xyz^2}{yz^2}\left(yz^2\right)=-xyz^2-z^3-xyz^2=$$

$$-z^3=-f_8$$

$$\overline{S\left(f_5,f_{11}\right)}^B=0$$

$$S\left(f_6,f_7\right)=\frac{xy^2z^2}{y^2z}y^2z-\frac{xy^2z^2}{xz^2}\left(xz^2\right)=0$$

$$\overline{S\left(f_6,f_7\right)}^B=0$$

$$S\left(f_6,f_8\right)=\frac{y^2z^3}{y^2z}y^2z-\frac{y^2z^2}{z^3}z^3=0$$

$$\overline{S\left(f_6,f_8\right)}^B=0$$

$$S\left(f_6,f_9\right)=\frac{y^3z}{y^2z}y^2z-\frac{y^3z}{y^3}\left(y^3+z^2\right)=-z^3=-f_8$$

$$\overline{S\left(f_6,f_9\right)}^B=0$$

$$S\left(f_6,f_{10}\right)=\frac{y^4z}{y^2z}y^2z-\frac{y^4z}{y^4}y^4=0$$

$$\overline{S\left(f_6,f_{10}\right)}^B=0$$

$$S\left(f_6,f_{11}\right)=\frac{y^2z^2}{y^2z}y^2z-\frac{y^2z^2}{yz^2}\left(yz^2\right)=0$$

$$\overline{S\left(f_6,f_{11}\right)}^B=0$$

$$S\left(f_7,f_8\right)=\frac{xz^3}{xz^2}xz^2-\frac{xz^3}{z^3}\left(z^3\right)=0$$

$$\overline{S\left(f_7,f_8\right)}^B=0$$

$S(f_7, f_9) = 0, \overline{S(f_7, f_9)}^B = 0$

$S(f_7, f_{10}) = 0, \overline{S(f_7, f_{10})}^B = 0$

$S(f_7, f_{11}) = 0, \overline{S(f_7, f_{11})}^B = 0$

$S(f_8, f_9) = \frac{y^3 z^3}{z^3} z^3 - \frac{y^3 z^3}{y^3}\left(y^3 + z^2\right) = -z^5 = -z^2 f_8$

$\overline{S(f_8, f_9)}^B = 0$

$S(f_8, f_{10}) = 0$

$\overline{S(f_8, f_{10})}^B = 0$

$S(f_8, f_{11}) = 0$

$\overline{S(f_8, f_{11})}^B = 0$

$S(f_9, f_{10}) = \frac{y^4}{y^3}\left(y^3 + z^2\right) - \frac{y^4}{y^4} y^4 = yz^2 = f_{11}$

$\overline{S(f_9, f_{10})}^B = 0$

$S(f_9, f_{11}) = \frac{y^3 z^2}{y^3}\left(y^3 + z^2\right) - \frac{y^3 z^2}{yz^2} yz^2 = z^4 = zf_8$

$\overline{S(f_9, f_{11})}^B = 0$

$S(f_2, f_{10}) = \frac{x^2 y^4}{x^2 y}\left(x^2 y + xz + y^2\right) - \frac{x^2 y^4}{y^4} y^4 = xyy^2 z + yy^4 =$

$xyf_6 + yf_{10}$

$\overline{S(f_2, f_{10})}^B = 0$

$S(f_2, f_{11}) = \frac{x^2 yz^2}{x^2 y}\left(x^2 y + xz + y^2\right) - \frac{x^2 yz^2}{yz^2} yz^2 = xz^3 + y^2 z^2 =$

$zf_7 + zf_6$

$\overline{S(f_2, f_{11})}^B = 0$

Проналазимо да је ГБ

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}\} =$$
$$= \left\{x^3 + z, x^2y + xz + y^2, x^2z + yz, -xy^2, -xyz + z^2, y^2z, xz^2, z^3, y^3 + z^2, y^4, yz^2\right\}.$$

Полином $f = z^2$ је моном, а он није у мономијалном идеалу који чине водећи чланови Гребнерове базе. $\langle LT(G)\rangle = \langle x^3, x^2y, x^2z, -xy^2, -xyz, y^2z, xz^2, z^3, y^3, y^4, yz^2\rangle$. Одатле следи да је остатак при дељењу са G исти тај полином, па он не припада идеалу.

Додатак: Наћи највеће n, тако да је x^n није у идеалу (такво n се зове *висина елемента*)!

$n = 3, f_1$

$x^3 : (x^3 + z) = 1$

$\underline{(-)x^3(-) + z}$

$-z$

Остатак при дељењу са G је z. (у Z_2 је -1=1)

$n = 4, f_1$

$x^4 : (x^3 + z) = x$

$\underline{(-)x^4(-) + xz}$

$-xz$

Остатак при дељењу са G је xz.

$n = 5, f_1, f_3$

$x^5 : (x^3 + z) = x^2$

$\underline{(-)x^5(-) + x^2z}$

$-x^2z$

$x^2z : (x^2z + yz) = 1$

$\underline{(-)x^2z(-) + yz}$

$-yz$

Остатак при дељењу са G је yz.

$n = 6, f_1, f_3, f_5$

$x^6 : \left(x^3 + z\right) = x^3$

$\underline{\left(-\right) x^6 \left(-\right) + x^3 z}$

$-x^3 z$

$x^3 z : \left(x^2 z + yz\right) = x$

$\underline{\left(-\right) x^3 z \left(-\right) + xyz}$

$-xyz$

$-xyz : \left(-xyz + z^2\right) = 1$

$\underline{\left(+\right) - xyz \left(-\right) + z^2}$

$-z^2$

Остатак при дељењу са G је z^2.

$n = 7, f_1, f_3, f_5, f_7$

$x^7 : \left(x^3 + z\right) = x^4$

$\underline{\left(-\right) x^7 \left(-\right) + x^4 z}$

$-x^4 z$

$x^4 z : \left(x^2 z + yz\right) = x^2$

$\underline{\left(-\right) x^4 z \left(-\right) + x^2 yz}$

$-x^2 yz$

$-x^2 yz : \left(-xyz + z^2\right) = x$

$\underline{\left(+\right) - x^2 yz \left(-\right) + xz^2}$

$-xz^2$

$xz^2 : xz^2 = 1$

$\underline{\left(-\right) xz^2}$

0

За $n = 7$, x^n ће припадати идеалу. $x^7 = x^4 f_1 + x^2 f_3 + x f_5 + f_7$

Литература

[1] http://sr.wikipedia.org, Википедија, слободна енциклопедија, *Волфганг Гребнер*

[2] http://en.wikipedia.org/wiki/Bruno_Buchberger, From Wikipedia, the free encyclopedia, *Bruno Buchberger*

[3] David Cox, John Little, Donald O'Shea, *Ideals, Varieties, and Algorithms*

[4] Др Бранко Малешевић, *Гребнерове базе и примене*,Симболичка алгебра 2008

[5] http://www.it.nuigalway.ie, Michael Mc Gettrick (NUI, Galway), *OGB (Online Grobner Bases), Verison 1.0 User Manual*