

Гребнерове базе и примене

Марко Радовановић

Семинар за алгебру, математичку логику и теорију бројева

Београд, март-април 2026.

Дељење са остатком

Нека је K поље и $f, g \in K[X]$, $g \neq 0$. Тада постоје јединствени полиноми $q, r \in K[X]$ такви да је

$$f = qg + r \quad \text{и} \quad \deg(r) < \deg(g).$$

Шта можемо рећи у $K[x_1, \dots, x_n]$?

Нека је R комутативни прстен са јединицом.

Подседник. $\emptyset \neq I \subseteq R$ је идеал у R (пишемо $I \triangleleft R$) ако важи:

- (i) ако $x, y \in I$, тада $x + y \in I$;
- (ii) ако $a \in R$, $x \in I$, тада $ax \in I$.

Идеал генерисан са $\mathcal{G} = \{g_1, \dots, g_m\}$ у $K[x_1, \dots, x_n]$ дефинишемо као

$$\langle g_1, \dots, g_m \rangle = \{f_1 g_1 + \dots + f_m g_m : f_1, \dots, f_m \in K[x_1, \dots, x_n]\}.$$

Хилбертова теорема о бази

Сваки идеал у $K[x_1, \dots, x_n]$ је коначно генерисан.

Подседник. За $I \triangleleft R$ је $R/I = \{a+I : a \in R\}$, где је $a \in R$ за $a+I = \{a+x : x \in I\}$, при чему су операције дефинисане са:

$$(a+I) + (b+I) = (a+b) + I, \quad (a+I) \cdot (b+I) = ab + I.$$

Такође, $a+I = b+I$ ако и само ако $a-b \in I$.

Пример. Нека је $S := K[x_1, \dots, x_n]$. За $g \in S$ је $I := \langle g \rangle$ скуп полинома дељивих са g . Такође, за $f \in S$ је $f+I = r+I$, где је r остатак при дељењу f са g .

Ознаке

У наставку је K поље, а S ознака за $K[x_1, x_2, \dots, x_n]$

За $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{N}_0^n$ и $f \in K[x_1, \dots, x_n]$ користимо ознаке:

(1) $\mathbf{x}^{\mathbf{a}} := x_1^{a_1} \cdots x_n^{a_n}$ су **чланови**, а $c\mathbf{x}^{\mathbf{a}}$ су **мономи** ($c \in K$);

(2) $|\mathbf{a}| = \sum a_i$;

(3) $\text{supp}(f) = \{\mathbf{x}^{\mathbf{a}} : c_{\mathbf{a}} \neq 0\}$, где $f = \sum_{\mathbf{a} \in \mathbb{N}_0^k} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$;

(4) $\deg \mathbf{x}^{\mathbf{a}} = |\mathbf{a}|$ и $\deg f = \max\{\deg \mathbf{x}^{\mathbf{a}} : \mathbf{x}^{\mathbf{a}} \in \text{supp}(f)\}$.

Пример

За

$$f = 2x_1^2x_3 + x_2^4 - x_2x_3 \in \mathbb{R}[x_1, x_2, x_3]$$

је

$$\text{supp}(f) = \{\mathbf{x}^{(2,0,1)}, \mathbf{x}^{(0,4,0)}, \mathbf{x}^{(0,1,1)}\} \text{ и } \deg f = 4.$$

Мономијални поредак

Нека је \mathbb{T} скуп чланова алгебре $K[x_1, \dots, x_n]$ (K је поље).

Мономијални поредак

Мономијални поредак је тотално уређење $<$ на \mathbb{T} такво да:

- за свако $t \in \mathbb{T}$, $1 \leq t$;
- за све $r, s, t \in \mathbb{T}$, $t \leq s$ повлачи $r \cdot t \leq r \cdot s$.

Примери

Нека је фиксирани поредак променљивих $x_1 > x_2 > \dots > x_k$.

(1) **Лексикографски поредак** $<_{lex}$:

$$\mathbf{x}^{\mathbf{a}} <_{lex} \mathbf{x}^{\mathbf{b}} \quad \text{акко} \quad a_l < b_l, \text{ где је } l = \min\{i \mid a_i \neq b_i\}.$$

(2) **Градирано лексикографски поредак** $<_{grlex}$:

$$\mathbf{x}^{\mathbf{a}} <_{grlex} \mathbf{x}^{\mathbf{b}} \quad \text{акко} \quad |\mathbf{a}| < |\mathbf{b}|, \text{ или } |\mathbf{a}| = |\mathbf{b}| \text{ и } a_l < b_l, \text{ где је } l = \min\{i \mid a_i \neq b_i\}.$$

(3) За одређене проблеме можемо конструисати погодне мономијалне поретке (више речи касније).

Иницијални (водећи) члан и идеал

Дефиниција.

Нека је $S := K[x_1, \dots, x_n]$ и $<$ мономијални поредак на S .

(1) За $f \in S \setminus \{0\}$ дефинишемо *иницијални члан* $\text{in}_<(f)$ као највећи моном из скупа $\text{supp}(f)$ у односу на $<$.

(2) За $I \triangleleft S$ дефинишемо *иницијални идеал од I* са

$$\text{in}_<(I) = \langle \text{in}_<(f) : f \in I \setminus \{0\} \rangle.$$

Пример

Нека је $S = \mathbb{Q}[x_1, x_2, x_3, x_4]$ и $<$ градирани лексикографски поредак.

За

$$f = x_1x_2 - x_3x_4 \text{ и } g = -x_2^2 + x_3^2 \text{ је } \text{in}_<(f) = x_1x_2 \text{ и } \text{in}_<(g) = x_2^2.$$

Ако је $I := \langle f, g \rangle$, приметимо да важи

$$h = x_2f + x_1g = x_1x_3^2 - x_2x_3x_4 \in I, \text{ а } \text{in}_<(h) = x_1x_3^2 \notin \langle \text{in}_<(f), \text{in}_<(g) \rangle,$$

па $\langle \text{in}_<(f), \text{in}_<(g) \rangle \subsetneq \text{in}_<(I)$.

Иницијални (водећи) члан и идеал

Нека је $S := K[x_1, \dots, x_n]$.

Особине

$$(1) \operatorname{in}_<(fg) = \operatorname{in}_<(f)\operatorname{in}_<(g);$$

$$(2) \operatorname{in}_<(f+g) \leq \max\{\operatorname{in}_<(f), \operatorname{in}_<(g)\}.$$

Запажање

Идеал $\operatorname{in}_<(I)$ је мономијални идеал (генерисан је мономима). За мономијални идеал $J = \langle m_1, \dots, m_k \rangle$ и моном $f \in S$ важи: $f \in J$ ако и само ако $m_i \mid f$ за неко i .

Диксонова лема

Сваки непразан скуп монома из S има коначно много минималних елемената у односу на релацију дељивости.

Дељење полинома

Дељење са остатком

Нека су $f, g_1, \dots, g_m \in S$, $g_i \neq 0$, а $<$ мономијални поредак на S . Тада постоје $q_1, \dots, q_m, r \in S$ такви да је

$$f = q_1 g_1 + \dots + q_m g_m + r$$

и важи:

- (i) елементи скупа $\text{supp}(r)$ нису садржани у $\langle \text{in}_<(g_1), \dots, \text{in}_<(g_m) \rangle$;
- (ii) $\text{in}_<(f) \geq \text{in}_<(q_i g_i)$ за $1 \leq i \leq m$.

Коментари:

Запис $f = q_1 g_1 + \dots + q_m g_m + r$ је **стандардни запис** полинома f , а r **остатак** при дељењу f са $\{g_1, \dots, g_m\}$.

Остатак није увек јединствен!

Презентовани доказ даје алгоритам за одређивање (једног) остатка.

Гребнерова база

Гребнерова база

Нека је I идеал у S , $\mathcal{G} = \{g_1, \dots, g_m\}$ скуп различитих елемената из $I \setminus \{0\}$, а $<$ мономијални поредак на S . Тада је G **Гребнерова база** идеала I у односу на $<$ ако је

$$\text{in}_<(I) = \langle \text{in}_<(g_1), \dots, \text{in}_<(g_m) \rangle.$$

Теорема

Нека је \mathcal{G} Гребнерова база идеала I . Тада важи:

- (i) сваки полином из S има јединствен остатак при дељењу са \mathcal{G} ;
- (ii) за свако $f \in S$ важи: $f \in I$ ако остатак при дељењу f са \mathcal{G} је 0.

Проблем припадности идеалу

За дати полином $f \in S$ и идеал I прстена S испитати да ли је $f \in I$.

Једно решење

Можемо користити Гребнерову базу (претходна теорема).

Бухбергеров критеријум

S -полином ненула полинома $f, g \in S$ је:

$$S(f, g) = \frac{\text{НЗС}(\text{in}_<(f), \text{in}_<(g))}{c \text{in}_<(f)} f - \frac{\text{НЗС}(\text{in}_<(f), \text{in}_<(g))}{d \text{in}_<(g)} g,$$

где су c и d коефицијенти уз $\text{in}_<(f)$ и $\text{in}_<(g)$ у f и g , редом.

Пример

Нека је $S := \mathbb{Q}[x_1, x_2, x_3, x_4]$, $<$ градирани лексикографски поредак и

$$f = x_1x_2 - x_3x_4 \text{ и } g = -x_2^2 + x_3^2.$$

Важи $\text{in}_<(f) = x_1x_2$ и $\text{in}_<(g) = x_2^2$, па је

$$S(f, g) = \frac{x_1x_2^2}{x_1x_2}(x_1x_2 - x_3x_4) - \frac{x_1x_2^2}{-x_2^2}(-x_2^2 + x_3^2) = x_1x_3^2 - x_2x_3x_4.$$

Теорема (Бухбергер)

Нека је $<$ мономијални поредак на прстену S , а $I = \langle g_1, \dots, g_m \rangle$ идеал овог прстена, при чему $g_i \neq 0$. Тада је следеће еквивалентно:

- (i) $\mathcal{G} = \{g_1, \dots, g_m\}$ је Гребнерова база за I у односу на $<$;
- (ii) за све $i \neq j$ је остатак при дељењу $S(g_i, g_j)$ са \mathcal{G} једнак 0.

Бухбергеров алгоритам

Бухбергеров алгоритам

Улаз: Идеал I прстена S и коначан генераторски скуп \mathcal{G} за I .

Корак 1: За свака два различита полинома из \mathcal{G} израчунати S -полином.

Корак 2: Ако су остаци при дељењу са \mathcal{G} свих S -полиноми из Корака 1 једнаки 0, тада се алгоритам завршава и \mathcal{G} је Гребнерова база за I .
Иначе, додајемо један ненула остатак у \mathcal{G} и враћамо се на Корак 1.

Пример

Одредимо Гребнерову базу за $I = \langle f, g \rangle$, где је $f = x_1x_2 - x_3x_4$ и $g = -x_2^2 + x_3^2$ ($<$ је градиран и лексикографски поредак). Важи

$S(f, g) = x_1x_3^2 - x_2x_3x_4 =: h$. Како $\text{supp}(h) \cap \langle \text{in}_<(f), \text{in}_<(g) \rangle = \emptyset$, то је остатак при дељењу $S(f, g)$ са $\{f, g\}$ баш $S(f, g)$, па скупу $\{f, g\}$ додајемо полином h .

Даље, рачунамо $S(f, h)$ и $S(g, h)$:

$$S(f, h) = x_2^2x_3x_4 - x_3^3x_4 = -x_3x_4(-x_2^2 + x_3^2)$$

$$S(g, h) = -x_1x_3^4 + x_2^3x_3x_4 = -x_3^2(x_1x_3^2 - x_2x_3x_4),$$

па је по Бухбергеровом критеријуму $\{f, g, h\}$ Гребнерова база за I .

Меколијева теорема

Теорема (Меколи)

Нека је $<$ мономијални поредак на S и $I \triangleleft S$. Тада косети чланова из S који нису у $\text{in}_<(I)$ чине K -базу за S/I .

Теорема

Нека је $\mathcal{G} \subset S \setminus \{0\}$ коначан скуп полинома и I идеал генерисан са \mathcal{G} . Тада је следеће еквивалентно:

- (i) \mathcal{G} је Гребнерова база за I ;
- (ii) скуп косета чланова из S који нису дељиви водећим чланом нити једног полинома из \mathcal{G} чини K -базу за S/I .

По претходној теорему, ако је I идеал генерисан хомогеним полиномима, из Гребнерове базе можемо наћи Хилбертов ред за S/I . Заиста, ако је $M_i = \{\mathbf{x}^{\mathbf{a}} + I : \deg(\mathbf{a}) = i\}$, тада је **Хилбертов ред** за S/I :

$$\text{Hilb}_{S/I}(t) = \sum_{t \geq 0} \dim_K M_t t^i.$$

По Меколијевој теорему: $\text{Hilb}_{S/I}(t) = \text{Hilb}_{S/\text{in}_<(I)}(t)$.

Меколијева теорема – пример

Нека је $S := \mathbb{Q}[x_1, x_2, x_3, x_4]$, $<$ градирани лексикографски поредак и $I = \langle f, g \rangle$, где је:

$$f = x_1x_2 - x_3x_4 \text{ и } g = -x_2^2 + x_3^2.$$

Тада је $\{f, g, h\}$ Гребнерова база за I , где је

$$h := x_1x_3^2 - x_2x_3x_4,$$

па је $\text{in}_<(I) = \langle x_1x_2, x_2^2, x_1x_3^2 \rangle$.

По Меколијевој теорему је \mathbb{Q} -база векторског простора S/I скуп:

$$\{x_1^i x_3 x_4^j + I : i, j \geq 0\} \cup \{x_1^i x_4^j : i, j \geq 0\} \cup \{x_2 x_3^i x_4^j : i, j \geq 0\} \cup \{x_3^i x_4^j : i, j \geq 0\},$$

па је

$$\text{Hilb}_{S/I}(t) = 1 + 4 \sum_{d \geq 1} dt^d = \frac{(1+t)^2}{(1-t)^2}.$$

Редукована Гребнерова база

Дефиниција

Нека је I идеал прстена S , а $<$ мономијални поредак на S . Тада је $\mathcal{G} = \{g_1, \dots, g_m\}$ **редукована Гребнерова база** за I у односу на $<$, ако је \mathcal{G} Гребнерова база за I у односу на $<$ и додатно:

- (i) водећи коефицијент полинома g_i , $1 \leq i \leq m$, је 1;
- (ii) за све $i \neq j$, мономи из $\text{supp}(g_j)$ нису дељиви са $\text{in}_{<}(g_i)$.

Теорема (редукована Гребнерова база)

Нека је I идеал прстена S , а $<$ мономијални поредак на S . Тада постоји јединствена редукована Гребнерова база за I у односу на $<$.

Запажање:

Редукована Гребнерова база за I даје идентитете који „задају” множење за елементе K -базе за S/I (из Меколијеве теореме).

Универзална Гребнерова база

Теорема

Сваки идеал I прстена S има само коначно много различитих иницијалних идеала.

Забелешка:

\mathcal{G} Гребнерова база за I и $\mathcal{G}' \subset \mathcal{G}$ коначан $\implies \mathcal{G}'$ Гребнерова база за I .

Теорема (универзална Гребнерова база)

За сваки идеал I прстена S постоји коначан скуп \mathcal{G} који је Гребнерова база у односу на произвољан мономијални поредак на S . За такво \mathcal{G} кажемо да је **универзална Гребнерова база** за I .

Решавање система алгебарских једначина

Подсетник, $S := K[x_1, \dots, x_n]$.

Нека су дати $f_1, \dots, f_m \in S$. Разматрамо систем једначина:

$$f_1(x_1, \dots, x_n) = 0$$

...

$$f_m(x_1, \dots, x_n) = 0.$$

Јасно, $\mathbf{a} \in K^n$ је решење ако $f(\mathbf{a}) = 0$ за све $f \in \langle f_1, \dots, f_m \rangle$.

Разматрамо **алгебарски скуп**:

$$V(I) = \{\mathbf{a} \in K^n : f(\mathbf{a}) = 0 \text{ за све } f \in I\}.$$

(Слаба) Хилбертова теорема о положају нула

Нека је K алгебарски затворено поље и I идеал прстена S . Тада је $V(I) = \emptyset$ ако и само ако је $I = \langle 1 \rangle$.

Последица

Нека је K алгебарски затворено поље и I идеал прстена S . Тада је $V(I) = \emptyset$ ако и само ако је редукована Гребнерова база идеала I једнака $\{1\}$.

Решавање система алгебарских једначина – пример

Посматрајмо систем једначина:

$$x^2 + y + z = 1$$

$$x + y^2 + z = 1$$

$$x + y + z^2 = 1.$$

Користимо Гребнерове базе и лексикографски поредак.

Гребнерова база идеала $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$ се састоји од полинома:

$$g_1 = x + y + z^2 - 1$$

$$g_2 = y^2 - y - z^2 + z$$

$$g_3 = 2yz^2 + z^4 - z$$

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

Нови систем решавамо „одоздо нагоре”. Решења су:

$$(1, 0, 0), (0, 1, 0), (-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}), (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}).$$

Приметимо да смо у g_2 и g_3 елиминисали променљиву x , а у g_4 променљиве x и y .

Забаван пример – бојење графова

Нека је $G = (V, E)$ граф. Тада је n -бојење графа G пресликавање $c: V \rightarrow \{1, 2, \dots, n\}$ такво да важи:

ако је $\{u, v\} \in E$, тада $c(u) \neq c(v)$.

(Утврдити да ли граф има n -бојење је NP-тежак проблем.)

Бајер (1982) је приказао следећи приступ. Нека је $V = \{1, \dots, m\}$. Радимо у $\mathbb{C}[x_1, \dots, x_m]$, при чему темену i „додељујемо” променљиву x_i . За свако теме имамо n опција за боју, што моделујемо једначинама

$$x_1^n - 1 = 0, x_2^n - 1 = 0, \dots, x_m^n - 1 = 0.$$

Услов да су за $\{i, j\} \in E$ боје чворова i и j различите записујемо:

$$x_i^{n-1} + x_i^{n-2}x_j + \dots + x_ix_j^{n-2} + x_j^{n-1} = 0.$$

Ако је I идеал генерисан полиномима који одговарају овим релацијама, тада је јасно:

G је n -обојив акко $\mathbf{V}(I) \neq \emptyset$,

што можемо утврдити уз помоћ Гребнерових база, 

Елиминациони поредак

Елиминациони поредак

Елиминациони поредак на S за променљиве x_1, \dots, x_t је мономијални поредак $<$ на S такав да за свака два монома $u, v \in S$ важи:

ако $x_j \mid u$ за неко $j \leq t$, а $x_j \nmid v$ за све $j \leq t$, тада $u > v$.

Примери елиминационих поредака

(1) Лексикографски поредак је елиминациони поредак за свако t .

(2) **Производ поредака** на $K[x_1, \dots, x_r]$ и $K[y_1, \dots, y_s]$. Ако је $<_1$ поредак на $K[x_1, \dots, x_r]$ и $<_2$ поредак на $K[y_1, \dots, y_s]$, тада је њихов производ поредак $<$ на $K[x_1, \dots, x_r, y_1, \dots, y_s]$ дат са:

$$\mathbf{x}^a \mathbf{y}^b > \mathbf{x}^c \mathbf{y}^d \quad \text{ако} \quad \mathbf{x}^a >_1 \mathbf{x}^c, \text{ или } \mathbf{a} = \mathbf{c} \text{ и } \mathbf{y}^b >_2 \mathbf{y}^d.$$

(3) **Тежински поредак** $<_{\mathbf{w}}$ са тежином $\mathbf{w} = (1, \dots, 1, 0, \dots, 0)$ (t јединица). Ако је $<$ на S , тада је за $\mathbf{w} \in \mathbb{R}_{\geq 0}^n$ **тежински поредак** $<_{\mathbf{w}}$ дат са:

$$\mathbf{x}^a >_{\mathbf{w}} \mathbf{x}^b \quad \text{ако} \quad \mathbf{w} \cdot \mathbf{a} > \mathbf{w} \cdot \mathbf{b}, \text{ или } \mathbf{w} \cdot \mathbf{a} = \mathbf{w} \cdot \mathbf{b} \text{ и } \mathbf{x}^a > \mathbf{x}^b.$$

Елиминација и Гребнерове базе

Елиминациони идеали

Нека је I идеал прстена S и $1 \leq t \leq n$. Тада је

$$I_t := I \cap K[x_{t+1}, \dots, x_n]$$

t -ти елиминациони идеал за I .

Теорема

Нека је I идеал у S и $1 \leq t \leq n$. Ако је \mathcal{G} Гребнерова база за I у односу на неки елиминациони поредак $<$ за x_1, \dots, x_t , тада је $\mathcal{G}_t := \mathcal{G} \cap K[x_{t+1}, \dots, x_n]$ Гребнерова база за идеал I_t у односу на индуковани поредак на $K[x_{t+1}, \dots, x_n]$. Специјално,

$$\text{in}_<(I \cap K[x_{t+1}, \dots, x_n]) = \text{in}_<(I) \cap K[x_{t+1}, \dots, x_n].$$

Пример

Посматрајмо систем једначина:

$$x^2 + y + z = 1$$

$$x + y^2 + z = 1$$

$$x + y + z^2 = 1.$$

У односу на лексикографски поредак, Гребнерова база идеала $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$ се састоји од полинома:

$$g_1 = x + y + z^2 - 1$$

$$g_2 = y^2 - y - z^2 + z$$

$$g_3 = 2yz^2 + z^4 - z$$

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

Одавде је:

$$I_2 = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle$$

$$I_1 = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z, z^6 - 4z^4 + 4z^3 - z^2 \rangle.$$

Неке примене

Теорема (пресек идеала)

Нека су I и J идеали у S . Тада је $I \cap J = (tI + (1-t)J) \cap S$.

Теорема (припадност радикалу)

Нека је I идеал у S и $f \in S$. Тада је $f \in \sqrt{I}$ ако и само ако $\langle I, 1 - ft \rangle \cap S = S$.
(Подсетник: $\sqrt{I} = \{g \in S : g^k \in I \text{ за неко } k \geq 0\}$.)

Теорема

Нека је $S = K[x_1, \dots, x_n]$, $S' = K[y_1, \dots, y_m]$ и $\varphi : S \rightarrow S'$ хомоморфизам K -алгебри задат са $\varphi(x_i) = f_i$ (за неке $f_i \in S'$). Нека је $J = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subset K[x_1, \dots, x_n, y_1, \dots, y_m]$.

(1) Важи: $\text{Ker}(\varphi) = J \cap S$.

(2) Нека је \mathcal{G} Гребнерова база за J у односу на неки елиминациони поредак за y_1, \dots, y_m . Ако је $g \in S'$ и h његов остатак у односу на \mathcal{G} , тада важи:

- (i) $g \in \text{Im}(\varphi)$ ако и само ако је $h \in S$;
- (ii) ако је $g \in \text{Im}(\varphi)$, тада је $g = h(f_1, \dots, f_n)$.

Параметризација

Нека је дат систем параметарских једначина:

$$u_1 = f_1(y_1, \dots, y_m)$$

...

$$u_n = f_n(y_1, \dots, y_m).$$

Желимо да елиминишемо параметре y_1, \dots, y_m .

Одређујемо Гребнерову базу за $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subset K[y_1, \dots, y_m, x_1, \dots, x_n]$ у односу на неки елиминациони поредак $<$ за y_1, \dots, y_m .

Пример.

Нека је $e_1 = x_1 + x_2 + x_3$, $e_2 = x_1x_2 + x_1x_3 + x_2x_3$, $e_3 = x_1x_2x_3$ и $I = \langle t_1 - e_1, t_2 - e_2, t_3 - e_3 \rangle \subset \mathbb{Q}[x_1, x_2, x_3, t_1, t_2, t_3]$. Гребнерова база у односу на производ градираних обрнутих лексикографских поредака на $\mathbb{Q}[x_1, x_2, x_3]$ и $\mathbb{Q}[t_1, t_2, t_3]$ је

$$\mathcal{G} = \{x_1 + x_2 + x_3 - t_1, x_2^2 - x_1x_3 - x_2t_1 + t_2, x_3^3 - x_2^2t_1 + x_3t_2 - t_3\}.$$

По претходном, ако желимо да представимо неки полином из $\mathbb{Q}[x_1, x_2, x_3]$ преко e_1, e_2, e_3 довољно је да нађемо његов остатак по модулу \mathcal{G} .

За $f = x_1^4 + x_2^4 + x_3^4 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2$ добијамо остатак $h = t_1^4 - 4t_1^2t_2 + t_2^2 + 6t_1t_3$

$$f = e_1^4 - 4e_1^2e_2 + e_2^2 + 6e_1e_3.$$

Коначни алгебарски скупови

За скуп $V \subseteq K^n$ дефинишемо:

$$\mathbf{I}(V) = \{f \in S : f(\mathbf{a}) = 0 \text{ за све } \mathbf{a} \in V\}.$$

Хилбертова теорема о положају нула

Ако је K алгебарски затворено поље и I идеал у S , тада важи $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Теорема

Нека је K алгебарски затворено поље. Следеће је еквивалентно:

- (1) $\mathbf{V}(I)$ је коначан;
- (2) димензија векторског простора S/I је коначна;
- (3) за сваки мономијални поредак $<$ на S , Гребнерову базу \mathcal{G} за I у односу на $<$ и $1 \leq i \leq n$ постоји $g \in \mathcal{G}$, такво да је $\text{in}_<(g) = x_i^{\mu_i}$ за неко $\mu_i \geq 0$.

Алгебарски скуп мономијалног идеала

Нека је $I = \langle x_2^2 x_3^2, x_1^5 x_3^4, x_1 x_2 x_3^3 \rangle$. Тада важи:

$$\begin{aligned} \mathbf{V}(I) &= \mathbf{V}(x_2^2 x_3^2) \cap \mathbf{V}(x_1^5 x_3^4) \cap \mathbf{V}(x_1 x_2 x_3^3) \\ &= (\mathbf{V}(x_2) \cup \mathbf{V}(x_3)) \cap (\mathbf{V}(x_1) \cup \mathbf{V}(x_3)) \cap (\mathbf{V}(x_1) \cup \mathbf{V}(x_2) \cup \mathbf{V}(x_3)) \\ &= \mathbf{V}(x_3) \cup \mathbf{V}(x_1, x_2). \end{aligned}$$

Теорема-дефиниција

Алгебарски скуп мономијалног идеала је коначна унија координатних потпростора од K^n .

Димензија овог алгебарског скупа је највећа међу димензијама ових потпростора.

Теорема

Нека је J мономијални идеал генерисан мононимима m_1, \dots, m_k . Тада је димензија $\mathbf{V}(J)$ једнака максималној кардиналности скупа променљивих \mathcal{P} таквог да нити један од монома m_i није производ променљивих само из \mathcal{P} .

Димензија

Дефиниција

Алгебарски скуп $V \subseteq K^n$ је **иредуцибилан** ако важи: из $V = V_1 \cup V_2$ за нека два алгебарска скупа V_1 и V_2 следи $V_1 = V$ или $V_2 = V$.

Алгебарски скуп $V \subseteq K^n$ је **димензије m** ако је m дужина најдужег строго опадајућег низа иредуцибилних алгебарских скупова у V :

$$V = V_0 \supset V_1 \supset \cdots \supset V_m.$$

Пример

- (1) Координатни потпростори од K^n су иредуцибилни. Њихова димензија је иста као димензија одговарајућег векторског простора.
- (2) Алгебарски скуп $\mathbf{V}(x_3) \cup \mathbf{V}(x_1, x_2)$ није иредуцибилан.

Димензију можемо да прочитамо из Хилбертов реда.

Теорема

Нека је K алгебарски затворено поље. Тада је димензија $\mathbf{V}(I)$ једнака димензији $\mathbf{V}(\text{in}_{<}(I))$ за произвољан градуисани поредак $<$.

Аутоматско доказивање теорема (пример)

Задатак. Доказати да се дијагонале паралелограма полове.

Посматрамо паралелограм $ABCD$ у \mathbb{R}^2 . Овај паралелограм је јединствено одређен тачкама A , B и D . Нека је $A(0,0)$, $B(u_1,0)$ и $D(u_2,u_3)$. Тачку $C(x_1,x_2)$ налазимо из услова $AB \parallel CD$ и $BC \parallel AD$:

$$0 = \frac{x_2 - u_3}{x_1 - u_2} \quad \text{и} \quad \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1},$$

што даје

$$h_1 = x_2 - u_3 = 0, \quad h_2 = (x_1 - u_1)u_3 - x_2u_2 = 0.$$

Тачку пресека дијагонала AC и BD , тачку $X(x_3,x_4)$, дефинишемо једначинама:

$$\frac{x_4}{x_3} = \frac{x_2}{x_1} \quad \text{и} \quad \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1},$$

из чега добијамо

$$h_3 = x_4x_1 - x_3x_2 = 0, \quad h_4 = x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0.$$

Једнакости $AH = HC$ и $BH = HD$ (које желимо да докажемо) записујемо:

$$f_1 = x_3^2 + x_4^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 = 0$$

$$f_2 = (x_3 - u_1)^2 + x_4^2 - (x_3 - u_2)^2 - (x_4 - u_3)^2 = 0.$$

Аутоматско доказивање теорема (пример)

Желимо да важи $f_1, f_2 \in \mathbf{I}(\mathbf{V}(I))$, где је
 $I = \langle h_1, h_2, h_3, h_4 \rangle \subseteq \mathbb{R}[x_1, x_2, x_3, x_4, u_1, u_2, u_3]$.

Први проблем. Лепо би било да запишемо $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, јер: $f \in \sqrt{I}$ ако је $\langle I, 1 - ft \rangle \cap S = S$ ако је $\{1\}$ редукована Гребнерова база за $\langle I, 1 - ft \rangle$. Међутим, \mathbb{R} није алгебарски затворено! Ипак, важи

$$\text{из } f \in \sqrt{I} \text{ следи } f \in \mathbf{I}(\mathbf{V}(I)).$$

Међутим, у нашем случају $f_1 \notin \sqrt{I}$!

Други проблем. Гребнерова база за $I \subseteq \mathbb{R}[x_1, x_2, x_3, x_4, u_1, u_2, u_3]$ у односу на лексикографски поредак се састоји од:

$$\begin{aligned} g_1 &= x_1x_4 + x_4u_1 - x_4u_2 - u_1u_3, & g_2 &= x_1u_3 - u_1u_3 - u_2u_3 \\ g_3 &= x_2 - u_3, & g_4 &= x_3u_3 + x_4u_1 + x_4u_2 - u_1u_3, \\ g_5 &= x_4u_1^2 - x_4u_1u_2 - \frac{1}{2}u_1^2u_3 + \frac{1}{2}u_1u_2u_3, & g_6 &= x_4u_1u_3 - \frac{1}{2}u_1u_3^2. \end{aligned}$$

Одавде се може добити разлагање $\mathbf{V}(I) = V' \cup U_1 \cup U_2 \cup U_3$ на иредуцибилне компоненте, где је $V' = \mathbf{V}(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2})$,

$$U_1 = \mathbf{V}(x_2, x_4, u_3), \quad U_2 = \mathbf{V}(x_1, x_2, u_1 - u_2, u_3), \quad U_3 = \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1).$$

Међутим, u_1, u_2, u_3 су „зависне” на U_1, U_2 и U_3 !

Аутоматско доказивање теорема

Нека је I идеал у $K[u_1, \dots, u_m, x_1, \dots, x_n]$, такав да је алгебарски скуп $V := \mathbf{V}(I)$ иредуцибилан. Тада кажемо да су u_1, \dots, u_m **алгебарски независне на V** ако нити један ненула полином ових променљивих није нула за све тачке из V .

Нека $h_1, \dots, h_k \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$, $I = \langle h_1, \dots, h_k \rangle$, $V := \mathbf{V}(I)$ и V' унија иредуцибилних компоненти V на којима су u_1, \dots, u_m алгебарски независне. Кажемо да f **генерички следи** из h_1, \dots, h_k ако је $f \in \mathbf{I}(V')$.

Теорема

Уз претходне ознаке, f генерички следи из h_1, \dots, h_k увек када постоји полином $c \in \mathbb{R}[u_1, \dots, u_m]$ такав да је

$$c \cdot f \in \sqrt{I},$$

што је еквивалентно са $f \in \sqrt{\tilde{I}}$, где је \tilde{I} идеал генерисан са h_1, \dots, h_k у $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$.

Наравно, $f \in \sqrt{\tilde{I}}$ тестирамо уз помоћ Гребнерових база. Над \mathbb{C} имамо еквиваленцију.

Торусни идеали

Нека је $\{\mathbf{h}_1, \dots, \mathbf{h}_m\} \subseteq \mathbb{Z}^n$. Посматрамо **афину полугрупу**

$$H = \mathbb{N}\mathbf{h}_1 + \dots + \mathbb{N}\mathbf{h}_m = \{a_1\mathbf{h}_1 + \dots + a_m\mathbf{h}_m : a_1, \dots, a_m \in \mathbb{N}\}$$

и додељујемо јој потпрстен $K[H]$ прстена $K[x_1, x_1^{-1}, \dots, x_n, x_n^{-1}]$ генерисан члановима $f_i = \mathbf{x}^{\mathbf{h}_i}$.

Посматрамо пресликавање $\varphi : K[t_1, \dots, t_m] \rightarrow K[H]$, такво да $t_i \mapsto f_i$. Тада је $P_H := \text{Ker } \varphi$ **торусни идеал** од H и важи $K[H] \cong K[t_1, \dots, t_m]/P_H$.

Идеал P_H је прост, па је алгебарски скуп $\mathbf{V}(P_H)$ иредуцибилан

Торусни идеали

Нека је $\{\mathbf{h}_1, \dots, \mathbf{h}_m\} \subseteq \mathbb{Z}^n$. Посматрамо **афину полугрупу**

$$H = \mathbb{N}\mathbf{h}_1 + \dots + \mathbb{N}\mathbf{h}_m = \{a_1\mathbf{h}_1 + \dots + a_m\mathbf{h}_m : a_1, \dots, a_m \in \mathbb{N}\}$$

и додељујемо јој потпрстен $K[H]$ прстена $K[x_1, x_1^{-1}, \dots, x_n, x_n^{-1}]$ генерисан члановима $f_i = \mathbf{x}^{\mathbf{h}_i}$.

Посматрамо пресликавање $\varphi : K[t_1, \dots, t_m] \rightarrow K[H]$, такво да $t_i \mapsto f_i$. Тада је $P_H := \text{Ker } \varphi$ **торусни идеал** од H и важи $K[H] \cong K[t_1, \dots, t_m]/P_H$.

Идеал P_H је прост, па је алгебарски скуп $\mathbf{V}(P_H)$ иредуцибилан и садржи тачке $(\mathbf{a}^{\mathbf{h}_1}, \dots, \mathbf{a}^{\mathbf{h}_m})$ за $\mathbf{a} \in (K^*)^m$, тј. један (алгебарски) торус. Алгебарски скупови $\mathbf{V}(P_H)$ су управо **афини алгебарски торуси**.

Теорема

Идеал I је биномни (генерисан биномима) и прост ако и само ако је торусни идеал.

Торусни идеали (пример)

Пример 1.

Нека је $n = 3$, $m = 4$ и $\mathbf{h}_1 = (1, 0, 0)$, $\mathbf{h}_2 = (0, 1, 0)$, $\mathbf{h}_3 = (0, 0, 1)$, $\mathbf{h}_4 = (1, 1, -1)$.

Тада је $\varphi : K[t_1, t_2, t_3, t_4] \rightarrow K[x_1^\pm, x_2^\pm, x_3^\pm]$ задато са

$$t_1 \mapsto x_1, \quad t_2 \mapsto x_2, \quad t_3 \mapsto x_3, \quad t_4 \mapsto x_1 x_2 x_3^{-1},$$

па је $\varphi(t_1 t_2 - t_3 t_4) = x_1 x_2 - x_3 x_1 x_2 x_3^{-1} = 0$, тј. $t_1 t_2 - t_3 t_4 \in P_H$.

Приметимо да $\mathbf{V}(P_H)$ садржи скуп тачака $(a_1, a_2, a_3, a_1 a_2 a_3^{-1}) \in \mathbb{C}^4$, $a_i \neq 0$, које чине торус (изоморфан са $(\mathbb{C}^*)^3$).

Пример 2.

Нека је $m = 3$, $n = 1$ и $\mathbf{h}_1 = 5$, $\mathbf{h}_2 = 7$, $\mathbf{h}_3 = 11$. Тада је

$$H = \{5a + 7b + 11c : a, b, c \in \mathbb{N}\},$$

а $\varphi : K[t_1, t_2, t_3] \rightarrow K[x^\pm]$ задато са

$$t_1 \mapsto x^5, \quad t_2 \mapsto x^7, \quad t_3 \mapsto x^{11},$$

па је нпр. $\varphi(t_1^2 t_3 - t_2^3) = x^{10} x^{11} - x^{21} = 0$, тј. $t_1^2 t_3 - t_2^3 \in P_H$.

Нека занимљива питања:

Одредити највеће $n \in \mathbb{N}$ такво да $n \notin H$. (**Проблем новчића**)

За дато $n \in \mathbb{N}$ наћи најмање $a + b + c$ такво да је $n = 5a + 7b + 11c$, $a, b, c \in \mathbb{N}$.

Торусни идеали

Нека је $\pi : \mathbb{N}^m \rightarrow H$, $\pi(u_1, \dots, u_m) = u_1 \mathbf{h}_1 + \dots + u_m \mathbf{h}_m$. Тада је $\varphi(\mathbf{t}^{\mathbf{u}}) = \mathbf{x}^{\pi(\mathbf{u})}$.

Теорема

Скуп $\{\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}} : \pi(\mathbf{u}) = \pi(\mathbf{v})\}$ је генератриса K -векторског простора P_H .

За $\mathbf{v} \in \mathbb{Z}^m$ су \mathbf{v}^+ и \mathbf{v}^- такви да $v_i^+ = \begin{cases} v_i, & v_i \geq 0 \\ 0, & \text{иначе} \end{cases}$ и $v_i^- = \begin{cases} 0, & v_i > 0 \\ -v_i, & \text{иначе} \end{cases}$.

Последица

Важи $P_H = \langle \mathbf{t}^{\mathbf{u}^+} - \mathbf{t}^{\mathbf{u}^-} : \mathbf{u} \in \text{Ker}(\pi) \rangle$, где је $\text{Ker}(\pi) = \{\mathbf{u} \in \mathbb{Z}^n : \pi(\mathbf{u}^+) = \pi(\mathbf{u}^-)\}$. Такође, за сваки мономијални поредак $<$ постоји коначан скуп $G \subset \text{Ker}(\pi)$ такав да је редукована Гребнерова база за P_H у односу на $<$ једнака $\{\mathbf{t}^{\mathbf{u}^+} - \mathbf{t}^{\mathbf{u}^-} : \mathbf{u} \in G\}$.

Нека је \mathcal{U}_H универзална Гребнерова база за P_H која је унија свих редукованих Гребнерових база за P_H . За бином $\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}} \in P_H$ кажемо да је **примитиван** ако не постоји бином $\mathbf{t}^{\mathbf{r}} - \mathbf{t}^{\mathbf{s}} \in P_H$ такав да $\mathbf{t}^{\mathbf{r}} \mid \mathbf{t}^{\mathbf{u}}$ и $\mathbf{t}^{\mathbf{s}} \mid \mathbf{t}^{\mathbf{v}}$.

Теорема

Сви биноми у \mathcal{U}_H су примитивни.

Желимо да одредимо Гребнерову базу за $P_H \subset K[t_1, \dots, t_m]$ за дате $\mathbf{h}_1, \dots, \mathbf{h}_m \in \mathbb{Z}^n$. Посматрамо прстен $K[x_0, x_1, \dots, x_n, t_1, \dots, t_m]$. Нека је $<$ неки елиминациони поредак за x_0, x_1, \dots, x_n у овом прстену. Тада је

$$P_H = \langle x_0 x_1 \dots x_n - 1, t_1 \mathbf{x}^{\mathbf{h}_1^-} - \mathbf{x}^{\mathbf{h}_1^+}, \dots, t_m \mathbf{x}^{\mathbf{h}_m^-} - \mathbf{x}^{\mathbf{h}_m^+} \rangle \cap K[t_1, \dots, t_m],$$

па ако је \mathcal{G} Гребнерова база идеала $\langle x_0 x_1 \dots x_n - 1, t_1 \mathbf{x}^{\mathbf{h}_1^-} - \mathbf{x}^{\mathbf{h}_1^+}, \dots, t_m \mathbf{x}^{\mathbf{h}_m^-} - \mathbf{x}^{\mathbf{h}_m^+} \rangle$, добијамо да је

$$\mathcal{G} \cap K[t_1, \dots, t_m],$$

Гребнерова база идеала P_H .

Проблем новчића (Фробениусов проблем)

Нека су $h_1, \dots, h_m \in \mathbb{N}$. Означимо са $g(h_1, \dots, h_m)$ највећи природан d број такав да не постоје $a_1, \dots, a_m \in \mathbb{N}$ такви да је $a_1 h_1 + \dots + a_m h_m = d$, тј. највећи природан број који није у H . Ако је $\text{нзд}(h_1, \dots, h_m) = 1$ он постоји.

Примери

(1) $g(6, 10, 15) = 29$.

(2) $g(h_1, h_2) = h_1 h_2 - h_1 - h_2$ (за $\text{нзд}(h_1, h_2) = 1$).

(3) За $m > 2$ није позната формула за $g(h_1, \dots, h_m)$.

Посматрајмо сада општи проблем. Елементе из H можемо „видети” у формалном ред

$$\sum_{d \in H} x^d,$$

а ово је управо Хилбертов ред за $K[H]$. Како је $K[H] \cong K[t_1, \dots, t_m]/P_H$ изоморфизам градуисаних прстена (при чему је $\deg(t_i) = h_i$), то је ово и Хилбертов ред за $K[t_1, \dots, t_m]/P_H$, а њега можемо добити уз помоћ Гребнерових база.

(Напомена: при градуацији $\deg(t_i) = h_i$ је P_H генерисан хомогеним полиномима.)

Нека занимљива питања

Посматрамо поново $\pi: \mathbb{N}^m \rightarrow H$ задато са: $\pi(u_1, \dots, u_m) = u_1 \mathbf{h}_1 + \dots + u_m \mathbf{h}_m$.

Нека су све координате вектора \mathbf{h}_i ненегативне. Може нас занимати:

- (1) Одредити кардиналност скупа $\pi^{-1}(\mathbf{b})$.
- (2) Изабрати случајну тачку из скупа $\pi^{-1}(\mathbf{b})$.
- (3) За дато $\mathbf{w} \in \mathbb{R}^n$ наћи тачку $\pi^{-1}(\mathbf{b})$ такву да је $\mathbf{u} \cdot \mathbf{w}$ минимално.

Нека је $<$ поредак на \mathbb{N}^n индукован поретком на $K[t_1, \dots, t_n]$ и $\mathcal{F} \subseteq \text{Ker}(\pi)$ коначан скуп.

Конструиримо усмерен граф $\pi^{-1}(\mathbf{b})_{\mathcal{F}, <}$:

- чворови су елементи $\pi^{-1}(\mathbf{b})$;
- између \mathbf{u} и \mathbf{u}' је грана ако је $\mathbf{u} - \mathbf{u}' \in \mathcal{F}$ или $\mathbf{u}' - \mathbf{u} \in \mathcal{F}$ и усмерена је од \mathbf{u} до \mathbf{u}' ако је $\mathbf{u}' < \mathbf{u}$.

Нека је $\pi^{-1}(\mathbf{b})_{\mathcal{F}}$ одговарајући (неусмерени) граф.

Теорема

- (1) Граф $\pi^{-1}(\mathbf{b})_{\mathcal{F}}$ је повезан за свако $\mathbf{b} \in H$ ако и само ако $\{\mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-} : \mathbf{v} \in \mathcal{F}\}$ генерише P_H .
- (2) Усмерен граф $\pi^{-1}(\mathbf{b})_{\mathcal{F}, <}$ има јединствен понор за свако $\mathbf{b} \in H$ ако и само ако $\{\mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-} : \mathbf{v} \in \mathcal{F}\}$ је Гребнерова база за P_H у односу на $<$.

Целобројно програмирање

Проблем (3) је један проблем целобројног програмирања.

За дато $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{R}_{\geq 0}^n$ тражимо $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{Z}^n$ тако да:

$$u_1 \mathbf{h}_1 + \dots + u_m \mathbf{h}_m = \mathbf{b}$$

и да је $\mathbf{u} \cdot \mathbf{w}$ минимално.

Примери

(1) Фабрике F_1 , F_2 и F_3 производе 120, 150 и 30 комада неког производа, а продавнице P_1 и P_2 имају потражње 100 и 200 за тим производом. Ако је позната цена транспорта једног производа од фабрике F_i до продавнице P_j желимо да одредимо оптималан начин да дистрибуирамо производе. Посматрајмо пресликавање:

$$\pi(u_1, u_2, u_3, u_4, u_5, u_6) = (u_1 + u_3 + u_5, u_2 + u_4 + u_6, u_1 + u_2, u_3 + u_4, u_5 + u_6),$$

а разматрамо $\pi^{-1}(100, 200, 120, 150, 30)$ (где $\mathbf{h}_1 = (1, 0, 1, 0, 0)$, $\mathbf{h}_2 = (0, 1, 1, 0, 0)$, $\mathbf{h}_3 = (1, 0, 0, 1, 0)$, $\mathbf{h}_4 = (0, 1, 0, 1, 0)$, $\mathbf{h}_5 = (1, 0, 0, 0, 1)$, $\mathbf{h}_6 = (0, 1, 0, 0, 1)$).

(2) Нека су $h_1, \dots, h_m \in \mathbb{N}$ и $d \in \mathbb{N}$. Тада је најмање n такво да важи $n = a_1 + \dots + a_m$ за неке $a_i \in \mathbb{N}$ и $a_1 h_1 + \dots + a_m h_m = d$ заправо:

$$\text{минимално } \mathbf{a} \cdot \mathbf{w} \quad \text{за} \quad \mathbf{a} \in \pi^{-1}(d),$$

где је $\mathbf{w} = (1, \dots, 1)$.

Теорема

Усмерен граф $\pi^{-1}(\mathbf{b})_{\mathcal{F}, <}$ има јединствен понор за свако $\mathbf{b} \in H$ ако и само ако $\{\mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-} : \mathbf{v} \in \mathcal{F}\}$ је Гребнерова база торусног идеала P_H у односу на $<$.

Нека је $<$ неки поредак на $K[t_1, \dots, t_m]$ (нпр. лексикографски) и $<_{\mathbf{w}}$ одговарајући тежински поредак. Тада претходно тврђење даје решење претходног проблема целобројног програмирања на следећи начин:

- (1) Нека је $\mathbf{v} \in \pi^{-1}(\mathbf{b})$.
- (2) Одредимо (редуковану) Гребнерову базу \mathcal{G} за P_H у односу на $<_{\mathbf{w}}$.
- (3) Нека је $\mathbf{x}^{\mathbf{u}}$ остатак при дељењу $\mathbf{x}^{\mathbf{v}}$ са \mathcal{G} .
- (4) $\mathbf{u} \cdot \mathbf{w}$ је тражена минимална вредност.

Литература

Књиге:

- (1) Ene, Herzog, *Gröbner Bases in Commutative Algebra*, AMS
- (2) Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms*, Springer
- (3) Sturmfels, *Gröbner Bases and Convex Polytopes*, AMS
- (4) Adams, Loustau, *An Introduction to Gröbner Bases*, AMS

Предавања доступна онлајн:

- (1) Federico Galetto, *Computational Methods in Commutative Algebra* (мини-курс)
Део програма: *An Introduction to Recent Trends in Commutative Algebra*
(Fields Institute)
- (2) Federico Ardila: *Combinatorial Commutative Algebra* (курс)
- (3) Mike Stillman: *Computational Commutative Algebra and Computational Algebraic Geometry* (докторски курс, Fields Institute)

Хвала на пажњи!