Eötvös Loránd Tudományegyetem
Természettudományi Kar

Szakdolgozat

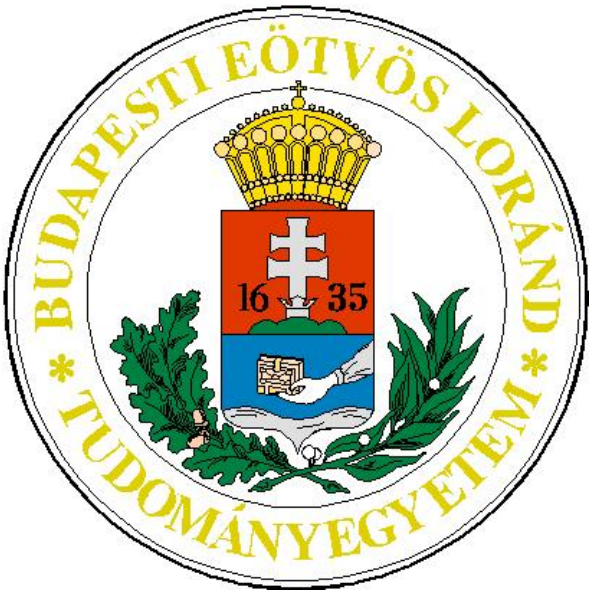
Elimináció Gröbner-bázisokkal

Szalai Gábor

Matematika BSc, elemző szakirány

Témavezető: Károlyi Gyula, egyetemi docens

Algebra és Számelmélet Tanszék



Budapest, 2010

Tartalomjegyzék

1. fejezet

Bevezetés

A szakdolgozatom témájául a Gröbner-bázisok segítségével megvalósítható eliminiációk leírását választottam.

Ez a mintegy fél évszázada létező módszer – melynek hatékonyságát különösen a nagy teljesítményű számítógépek elterjedése óta lehet kihasználni – új utakat nyitott az összetett egyenletrendszerek megoldásában. A többhatározatlanú polinomális egyenletrendszerek megoldása gyakori feladat, sokszor adják fel magasabb szintű középiskolás matematikai versenyek résztvevőinek is. Általános esetben azonban a magasabb fokú, többváltozós egyenletrendszerek analitikusan nem megoldhatóak, kivéve néhány speciális esetet, mikor intuitív módszerek alkalmazásával elvégezhetőek az egyszerűbb alakra vezető átalakítások. A Gröbner-bázisok egyik fontos gyakorlati tulajdonsága, hogy a többhatározatlanú polinomális egyenletrendszereket bizonyos feltételek teljesülése esetén visszavezeti az egyismeretlenes egyenletekre, így végül egy általános eljárást kapunk. Mindazonáltal a Gröbner-bázisok elmélete egyelőre még nem számít hangsúlyos területnek az itthoni egyetemi matematika-alapképzésben.

Munkám célja ennek a módszernek az alapszintű bemutatása gyakorlati példákon keresztül, mely egyfajta hiánypótlásként is szolgálhat a rendelkezésre álló, kevés magyar nyelvű forrás között.

A dolgozat második fejezetében ismertetem a téma megértéséhez szükséges algebrai fogalmakat és összefüggéseket. A következő részben részletesen tárgyalom a főtémául szolgáló Gröbner-bázisokkal kapcsolatos ismereteket, külön hangsúlyt fektetve az eliminációs eljárások részletes bemutatására. Az utolsó fejezetben pedig konkrét alkalmazásokra is mutatok példákat.

A Gröbner-bázisokkal kapcsolatos tanulmányaimat az angol nyelvű könyvből [1.], illetve Felszeghy Bálint internetes jegyzete [2.] alapján készítettem, az alapismereteket Freud Róbert: Lineáris algebra [3.] és Kiss Emil: Bevezetés az algebrába [6.] c. művekből dolgoztam fel, a Gauss-eliminációhoz pedig Gergó Lajos írását [7.] használtam.

2. fejezet

Alapismeretek

Ebben a fejezetben a főtéma könnyebb megértéséhez összegyűjtöttem az algebrai tanulmányaimból a fontosabb definíciókat és tételeket.

2.1. Egyhatározatlanú polinom

A szakdolgozatban végig komplex együtthatós polinomokat vizsgálok, azaz $f(x) \in \mathbb{C}[x]$.

Egyhatározatlanú polinom: Az $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ alakú formális kifejezés, ahol $n \geq 0$ egész szám és $a_0, \ldots, a_n$ komplex számok. Ha $a_j \neq 0$, akkor a_jx^j a polinom egy tagja, ahol az x^j együtthatója az a_j. Az $a_0 = a_0x^0$ a polinom konstans tagja.

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek.

Nullpolinom: Olyan polinom, amelynek minden együtthatója nulla.

Konstans polinom: Minden c komplex számot polinomnak tekintünk.

Fok: Ha $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, ahol $a_n \neq 0$, akkor f foka n. Jele: $\mathrm{gr}(f)$. Az $f(x)$ főtagja a_nx^n, főegyütthatója a_n. A nullpolinomnak nincsen foka.

Normált polinom: Az $f(x)$ polinom normált, ha a főegyütthatója 1.

Szorzásnál a fokok összeadódnak: $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$

Következmény: Két polinom szorzata csak akkor lehet 0, ha az egyik polinom 0.

Egy f polinomnak pontosan akkor van reciproka a polinomok között, ha nem nulla konstans polinom.

Két polinom összegének a foka legfeljebb akkora, mint a két polinom fokai közül a nem kisebb: $\mathrm{gr}(f+g) \leq \max(\mathrm{gr}(f), \mathrm{gr}(g))$. Ha a két polinom foka különböző, akkor egyenlőség áll fenn.

Műveletek polinomok között:

Legyen $f(x) = \sum_{k=0}^{n} a_k x^k$ és $g(x) = \sum_{k=0}^{n} b_k x^k$.

Polinomok összege: $(f+g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$.

Polinomok különbsége: $(f-g)(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_n - b_n)x^n$.

Polinom ellentetje: $f \in \mathbb{C}[x]$ ellentetje h, ha $f + h = 0$. Jele: $h = -f$.

Tehát $h(x) = \sum_{k=0}^{n} (-a_k)x^k$.

Polinomok szorzatata: $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j$-ban az x^k együtthatója $c_k = \sum_{l=0}^{k} a_l b_{k-l}$.

Megjegyzés: Az x^k-os tag akkor jön létre az $(a_i x^i)(b_j x^j)$-ből, ha $i + j = k$. A szorzat együtthatóinak kiszámolása pedig úgy értendő, hogy amelyik tag nem értelmes, azt 0-nak vesszük, vagyis $a_{n+1} = a_{n+2} = \ldots = b_{m+1} = b_{m+2} = \ldots = 0$.

2.2. Maradékos osztás, oszthatóság polinomok között

Egész számok maradékos osztása: Minden $a, b \in \mathbb{Z}$ esetén, ahol $b \neq 0$, létezik olyan $q, r \in \mathbb{Z}$, hogy $a = bq + r$ és $|r| < |b|$.

Polinomok maradékos osztása: Minden $f, g \in \mathbb{C}[x]$ esetén, ahol $g \neq 0$, létezik olyan $q, r \in \mathbb{C}[x]$, hogy $f = gq + r$ és $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$. A q és r egyértelműen meghatározott. A q és r együtthatói a négy alapművelettel kaphatók. Az eljárás során csak g főegyütthatójával osztunk.

Oszthatóság: Azt mondjuk, hogy a $g \in \mathbb{C}[x]$ polinom osztója $f \in \mathbb{C}[x]$-nek $\mathbb{C}[x]$-ben, ha létezik olyan $h \in \mathbb{C}[x]$ polinom, hogy $f(x) = g(x)h(x)$.
Jelölés: $g \mid f$.
Megjegyzés: $g \mid f \iff r = 0$.
Példa: $x + i \mid x^2 + 1$, mert $x^2 + 1 = (x+i)(x-i)$ és $x + i \in \mathbb{C}[x]$.

Egység: Azt mondjuk, hogy a $g \in \mathbb{C}[x]$ polinom egység $\mathbb{C}[x]$-ben, ha minden $\mathbb{C}[x]$-beli polinomnak osztója $\mathbb{C}[x]$-ben. $\mathbb{C}[x]$ egységei a nem nulla konstans polinomok.

Kitüntetett közös osztó: Azt mondjuk, hogy $h(x)$ az $f, g \in \mathbb{C}[x]$ polinomok kitüntetett közös osztója $\mathbb{C}[x]$-ben, ha közös osztójuk, azaz $h \mid f$ és $h \mid g$, továbbá h az f és g minden közös osztójának többszöröse, azaz tetszőleges k polinomra $k \mid f$ és $k \mid g$ esetén $k \mid h$.
A kitüntetett közös osztó egységszeres erejéig egyértelműen meghatározott.

Az f és g kitüntetett közös osztója $\mathbb{C}$ fölött az euklideszi algoritmussal[1] számítható ki, és felírható $f(x)u(x) + g(x)v(x)$ alakban alkalmas u, v polinomokkal.

2.3. Többhatározatlanú polinom

A többhatározatlanú polinomok definicióját rekurzívan visszavezethetjük az egyhatározatlanú polinomokra.

Monom: Az n változós monom alakja: $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots \cdot x_n^{\alpha_n}$, ahol az összes kitevő nemnegatív egész szám. A kifejezés fokszáma a kitevők összege. Jelölés: $\mathbf{x}^\alpha$.

Többhatározatlanú polinom: Általában az $x_1, x_2, \dots, x_n$ polinomjai az $f(x) = a_0 + a_1 x_n + a_2 x_n^2 + \dots + a_m x_n^m$ formális kifejezések, ahol $a_0, a_1, \dots, a_m \in \mathbb{C}[x_1, x_2, \dots, x_{n-1}]$. Ezek halmazát $\mathbb{C}[x_1, x_2, \dots, x_n] = \mathbb{C}[\mathbf{x}]$ jelöli.
Példa: $x_1 + \pi x_3,\ x_1^2 + i x_2 x_3 + \sqrt{2} x_1 x_3^3 \in \mathbb{C}[x_1, x_2, x_3]$.

Polinom főtagja: Egy $f(x) \in \mathbb{C}[\mathbf{x}],\ f \neq 0$ polinom főtagja a benne szereplő legnagyobb[2] tag, amelynek az együtthatója nem 0. Jelölés: $\mathrm{lm}(f)$. A főtag együtthatójának a jele: $\mathrm{lc}(f)$.

$\mathbb{C}[\mathbf{x}]$ **nullosztómentes**: Két polinom szorzata csak akkor lehet 0, ha az egyik polinom 0.

Algebrai varietás: Algebrai varietásnak nevezzük egy polinomiális egyenletekből álló rendszer megoldáshalmazát.

Fok: Legyen $f(x_1, \dots, x_n) = \sum r_{m_1,\dots,m_n} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$.
Az $r_{m_1,\dots,m_n} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$ tag foka $\sum_{i=1}^{n} m_i$. Az f foka a nem nulla tagok fokai közül a legnagyobb. Jele: $\mathrm{gr}(f)$.
Példa: $f(x_1, x_2) = i x_1^3 + \pi x_1^2 x_2 - 5 x_2^4 + 6 x_1 x_2^3$ Foka: 4.[3]

Homogén k-adfokú: Egy polinom homogén k-adfokú, ha minden tagjának foka k.

Szorzásnál a fokok összeadódnak: $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$.

Műveletek polinomok között:

Az n-határozatlanú polinomok összegét, különbségét, szorzatát ugyanúgy definiáljuk, mint az egyhatározatlanúakét, csak most az együtthatók $\mathbb{C}[x_1, x_2, \dots, x_{n-1}]$ elemei.

Példa: Legyen $f(x_1, x_2) = 5x_1^3 + 4\pi x_1 x_2^2 + 2i$, $g(x_1, x_2) = 6x_1^3 - 5x_1 x_2^2 + x_2^6$.

[1] Ez egy számelméleti algoritmus, mellyel két szám legnagyobb közös osztója határozható meg. Az eljárás maradékos osztások sorozatából áll, melyet polinomok esetén is alkalmazhatunk.

[2] Értelmezése a 2.5. alfejezetben.

[3] $\mathrm{gr}(x_2^4) = \mathrm{gr}(x_1 x_2^3) = 4$ és $\mathrm{gr}(x_1^3) = \mathrm{gr}(x_1^2 x_2) = 3$.

A két polinom összege:
$(f+g)(x_1,x_2) = 11x_1^3 + x_2^6 + (4\pi - 5)x_1x_2^2 + 2i$.
A két polinom szorzata:
$(f \cdot g)(x_1,x_2) = 30x_1^6 + 24\pi x_1^4x_2^2 + 12ix_1 3 - 25x_1^4x_2^5 - 20\pi x_1^2x_2^4 - 10ix_1x_2^2 + 5x_1^3x_2^6 + 4\pi x_1x_2^8 + 2ix_2^6$.

2.4. Polinomfüggvény, polinomok gyökei

Polinomfüggvény: Legyen b komplex szám. Az $f(x) = a_0 + a_1x + \ldots + a_nx^n$ polinom b helyen felvett helyettesítési értéke $f^*(b) = a_0 + a_1b + \ldots + a_nb^n$. Az f-hez tartozó f^* polinomfüggvény az az $f^* : \mathbb{C} \mapsto \mathbb{C}$ függvény, mely minden $b \in \mathbb{C}$-hez $f(b)$-t rendel.

Gyök: Legyen $f \in \mathbb{C}[x]$, $b \in \mathbb{C}$. A b szám gyöke az f polinomnak, ha $f^*(b) = 0$.

Ha $f, g \in \mathbb{C}[x]$ és $b \in \mathbb{C}$, akkor $(f+g)^*(b) = f^*(b) + g^*(b)$ és
$(fg)^*(b) = f^*(b)g^*(b)$.

Algebra alaptétele: Minden nem konstans, komplex együtthatós polinomnak van gyöke a komplex számok körében.

Páratlan fokú valós együtthatós polinomnak van valós gyöke.

Gyöktényezős alak: Minden n-edfokú komplex együtthatós f polinom felírható $c(x-b_1)\ldots(x-b_n)$ alakban, ahol a c az f főegyütthatója. Ez az f polinom gyöktényezős alakja. A b szám gyöke az f polinomnak $\iff$ van olyan q polinom, hogy $f(x) = (x-b)q(x)$.

Gyök multiplicitása: Legyen $f(x) = c(x-d_1)^{k_1}(x-d_2)^{k_2}\cdots(x-d_n)^{k_n}$, ahol a $d_1, \ldots, d_n$ már páronként különbözőek. A k_i szám a d_i gyök multiplicitása.

k-szoros gyök: Az $f \in \mathbb{C}[x]$ polinomnak a $b \in \mathbb{C}$ szám k-szoros gyöke, ha $f(x) = (x-b)^k q(x)$, ahol a $q \in \mathbb{C}[x]$ polinomnak b már nem gyöke. A k szám éppen a b gyök multiplicitása.

Minden polinomnak legfeljebb annyi különböző gyöke van, mint amekkora a foka.
Minden komplex együtthatós polinomnak pontosan annyi gyöke van multiplicitással számolva, mint amennyi a foka.

Azonossági tétel: Ha két, legfeljebb n-edfokú polinom több mint n helyen megegyezik, akkor egyenlők.

2.5. Lexikografikus elrendezés

Legyen $f(x_1,\dots,x_n)=\sum r_{m_1,\dots,m_n}x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$. Az általános tag $m_1\dots m_n$ "telefonszáma" n-jegyű, "számjegye" bármilyen nagy lehet.

Lexikografikus sorrend: A telefonszámokat úgy rakjuk sorba, ahogy a telefonkönyvben, vagyis növekvő sorrendben. Jelölés: *lex*.

Példa:$f(x_1,x_2,x_3)=13x_1^2x_3^2+ix_1^3+\pi x_1^2x_2-5x_2^3+6x_1x_2^3$.
Lex elrendezés: $f(x_1,x_2,x_3)=-5x_2^3+6x_1x_2^3+\pi x_1^2x_3+13x_1^2x_3^2+ix_1^3$.[4]

A pontos definíció a következő. Tekintsük a polinom két tagját, ezek legyenek:
$P=rx_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ és $Q=sx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$. A telefonszámok: $m_1\dots m_n$ és $k_1\dots k_n$.
Azt mondjuk, hogy P *lex* kisebb Q-nál, ha van olyan $1\le j\le n$, hogy $m_1=k_1$, $m_2=k_2,\dots,m_{j-1}=k_{j-1}$, de $m_j<k_j$.

$P\prec Q$ jelentése: P lexikografikusan kisebb, mint Q.

$P\preceq Q$ jelentése: $P\prec Q$, vagy P és Q az r,s együtthatóktól eltekintve megegyezik.

Főtag: Egy polinom főtagja a lexikografikusan legnagyobb tagja, azaz a *lex* elrendezésben a legutolsó tag (amelynek nem 0 az együtthatója).

Példa:$f(x_1,x_2,x_3)=13x_1^2x_3^2+ix_1^3+\pi x_1^2x_2-5x_2^3+6x_1x_2^3$. Főtag: ix_1^3.

Szorzat főtagja a főtagok szorzata.

2.6. Ideál

Ez az alfejezet az egyik legfontosabb egység, ugyanis a dolgozatban a $\mathbb{C}[x_1,\dots,x_n]$ polinomgyűrű ideáljaié lesz a főszerep.

Gyűrű: Egy $\mathcal{R}$ nemüres halmazt gyűrűnek nevezünk, ha
(i) értelmezve van $\mathcal{R}$-en két művelet - az egyiket összeadásnak, a másikat szorzásnak hívjuk;
(ii) az összeadás asszociatív és kommutatív, létezik nullelem, és minden elemnek létezik ellentettje;
(iii) a szorzás asszociatív;
(iv) bármely $a,b,c\in\mathcal{R}$-re $a(b+c)=ab+ac$ és $(b+c)a=ba+bc$ teljesül.

Szokásos gyűrű: $\mathcal{R}$ szokásos gyűrű, ha kommutatív, egységelemes és nullosztómentes.

Ideál: Egy $\mathcal{R}$ gyűrűben egy nemüres $I\subseteq\mathcal{R}$ részhalmazt az $\mathcal{R}$ ideáljának nevezzük, ha

[4] $x_1^2x_3^2:202,\ x_1^3:300,\ x_1^2x_3:201,\ x_2^3:030,\ x_1x_2^3:130\to 030<130<201<202<300$

(i) I zárt az ($\mathcal{R}$-beli) összeadásra és ellentettképzésre, azaz

$$i, j \in I \Longrightarrow i + j \in I, -i \in I;$$

(ii) bármely I-beli elemet egy tetszőleges $\mathcal{R}$-beli elemmel akármelyik oldalról megszorozva ismét I-beli elemet kapunk, azaz

$$i \in I, r \in \mathcal{R} \Longrightarrow ri \in I, ir \in I.$$

Kommutatív gyűrűben természetesen elég az egyik feltételt megkövetelni.
Jelölés: $I \lhd \mathcal{R}$.

Példa: $\mathcal{R} = \mathbb{Z}$-ben az n-nel osztható számok: ${}_n\mathbb{Z} = \{nk | k \in \mathbb{Z}\} \lhd \mathbb{Z}$.

Triviális ideál: Bármely gyűrűben ideál a csak 0-ból álló részhalmaz és maga a gyűrű, ezeket hívjuk triviális ideáloknak. Testben csak ez a két ideál létezik.

Főideál: Legyen a az $\mathcal{R}$ szokásos gyűrű tetszőleges eleme. Ekkor az $\{ra | r \in \mathcal{R}\}$ halmazt az a által generált főideálnak nevezzük, és $< a >$-val jelöljük.

Az $< a >$ főideál az a elemet tartalmazó **legszűkebb ideál**, azaz
(i) $< a >$ ideál $\mathcal{R}$-ben;
(ii) $a \in < a >$;
(iii) ha I ideál $\mathcal{R}$-ben és $a \in I$, akkor $< a > \subseteq I$.

Főideálgyűrű: Ha az $\mathcal{R}$ szokásos gyűrűben minden ideál főideál, akkor a gyűrű főideálgyűrű. Például: $\mathbb{Z}, T[x]$. A $\mathbb{C}[x, y]$ gyűrű viszont nem főideálgyűrű.

Generált ideál: Legyenek $a_1, \ldots, a_k$ az $\mathcal{R}$ szokásos gyűrű tetszőleges elemei. Ekkor a $\{\sum_{j=1}^{k} r_j a_j | r_j \in \mathcal{R}\}$ halmazt az $a_1, \ldots, a_k$ által generált ideálnak nevezzük, jelölése $< a_1, \ldots, a_k >$. A főideálok tehát az egyetlen elem által generált ideálok.

Végesen generált: Egy I ideál végesen generált, ha léteznek olyan $a_1, \ldots, a_k$ elemek, amelyekre $I = < a_1, \ldots, a_k >$.

Az $< a_1, \ldots, a_k >$ ideál az a_j elemeket tartalmazó **legszűkebb ideál**, azaz
(i) $< a_1, \ldots, a_k >$ ideál $\mathcal{R}$-ben;
(ii) $a_j \in < a_1, \ldots, a_k >$ minden $j = 1, 2, \ldots, k$ esetén;
(iii) ha I ideál $\mathcal{R}$-ben és $a_j \in I$, akkor $< a_1, \ldots, a_k > \subseteq I$.

Radikálideál: Az $\mathcal{R}$ szokásos gyűrű egy I ideáljának $\sqrt{I}$ radikálja alatt azon gyűrűelemek halmazát értjük, amelyeknek van olyan pozitív egész kitevős hatványa, amely I-be esik.

Legyen I ideál az $\mathcal{R}$ gyűrűben. Ekkor az I szerinti $a+I = \{a+i | i \in I\}$ **maradékosztályok** az $\mathcal{R}$ gyűrű diszjunkt részhalmazai, melyek egyesítése $\mathcal{R}$, és ezek az $[a+I]+[b+I] = [a+b]+I$ és $[a+I][b+I] = ab+I$ módon definiált összeadásra és szorzásra nézve gyűrűt alkotnak. Ezt a gyűrűt az $\mathcal{R}$-nek az I szerinti maradékosztálygyűrűjének vagy **faktorgyűrű**jének nevezzük, és $\mathcal{R}/I$-vel jelöljük.

2.7. Gauss-elimináció

Főminor: $D_k = \det \begin{pmatrix} a_{1,1} & \dots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{k,1} & \dots & a_{k,k} \end{pmatrix}$ determinánsok az $A = (a_{i,j})$ mátrix úgynevezett főminorai.

Reguláris mátrix: Az A mátrix reguláris, ha $\det(A) \neq 0$.

Diagonális mátrix: $\mathcal{D} = \{A \in \mathbb{R}^{n \times n} \ | a_{i,j} = 0, \text{ha } i \neq j \ , \ n \in N\}$.

Felső háromszögmátrix: $\mathcal{U} = \{A \in \mathbb{R}^{n \times n} \ | a_{i,j} = 0, \text{ha } i > j \ , \ n \in N\}$.

Alsó háromszögmátrix: $\mathcal{L} = \{A \in \mathbb{R}^{n \times n} \ | a_{i,j} = 0, \text{ha } i < j \ , \ n \in N\}$.

Részleges főelemkiválasztás: Az elimináció j. lépésében sorcserével úgy határozzuk meg az $a_{k,k}^{(j-1)}$ főelemet, hogy $|a_{k,k}^{(j-1)}| = \max\limits_{i=k,k+1,\dots,n} |a_{i,k}^{(j-1)}|$ teljesüljön.

Teljes főelemkiválasztás: Az elimináció j. lépésében sor-, és oszlopcserével úgy határozzuk meg az $a_{k,k}^{(j-1)}$ főelemet, hogy $|a_{k,k}^{(j-1)}| = \max\limits_{k \leq i,l \leq n} |a_{i,l}^{(j-1)}|$ teljesüljön.

Alapfeladatunk:

$$A \in \mathbb{R}^{n \times n}, \ \det(A) \neq 0, \ b \in \mathbb{R}^n, \ Ax = b, \ x = ?$$

Ennek a feladatnak egy gyors megoldása a Gauss-elimináció. Az algoritmus lényege, hogy először átalakítjuk a mátrixunkat felső háromszögmátrixszá, majd második lépésben rekurzív módon visszahelyettesítünk:

I. lépés: $Ax = b \iff Ux = r, \text{ ahol } U \in \mathcal{U}$.

II. lépés: $x_n = \frac{r_n}{u_{n,n}} \ , x_k = \frac{1}{u_{k,k}}(r_k - \sum_{j=k+1}^{n} u_{k,j} x_j) \ , k = n-1, \dots, 2, 1$.

Az I. részben szereplő átalakítást a következő módon írhatjuk le:
$a_{i,j}^{(k)} = a_{i,j}^{(k-1)} - \dfrac{a_{i,k}^{(k-1)}}{a_{k,k}^{(k-1)}} a_{k,j}^{(k-1)}$, ahol $k = 1, 2, \dots, n \ , \ i = k+1, \dots, n \ ,$
$j = k, \dots, n+1$.

A II. rész az előzőek szerint:

$$x_n = \frac{a_{n,n+1}^{(n-1)}}{a_{n,n}^{(n-1)}}\ , x_k = \frac{1}{a_{k,k}^{(k-1)}}\left(a_{k,n+1}^{(k-1)} - \sum_{j=k+1}^{n} a_{k,j}^{(k-1)} x_j\right)\ , k = n-1, \ldots, 2, 1.$$

Az $Ax = b\ ,\ A \in \mathbb{R}^{n\times n}\ ,\ b \in \mathbb{R}^n\ ,\ \det(A) \neq 0$ LER[5] esetén
a Gauss-elimináció végrehajtható $\iff$ $a_{k,k}^{(k-1)} \neq 0,\ k = 1, 2, \ldots, n-1.$

Az $Ax = b\ ,\ A \in \mathbb{R}^{n\times n}\ ,\ b \in \mathbb{R}^n\ ,\ \det(A) \neq 0$ LER esetén
$D_k \neq 0,\ k = 1, 2, \ldots, n-1 \iff a_{k,k}^{(k-1)} \neq 0,\ k = 1, 2, \ldots, n-1.$

Az $Ax = b\ ,\ A \in \mathbb{R}^{n\times n}\ ,\ b \in \mathbb{R}^n\ ,\ \det(A) \neq 0$ LER esetén a GE+RF[6] algoritmusa végrehajtható.

Lássuk, hogyan néz ez ki a gyakorlatban:

Példa:[7]

Legyen: $A = \begin{pmatrix} -2 & 3 & 8 \\ 9 & -5 & -8 \\ 0 & 1 & 2 \end{pmatrix}\ ,\ b = \begin{pmatrix} 3 \\ 10 \\ 2 \end{pmatrix}$

A tanult tétel miatt először le kell ellenőrizni, hogy a mátrixunkon lefut-e a Gauss-elimináció. Ehhez arra van szükség, hogy a főminorok ne legyenek nullák.

$A := matrix(3, 3, [-2, 3, 8, 9, -5, -8, 0, 1, 2]);$
$b := vector(3, [3, 10, 2]);$
$f := (i, j) \to A[i, j];$
$for\ i\ to\ 3\ do$
$DD[i] := det(matrix(i, i, f));$[8]
$od;$

Itt azt kapjuk, hogy $D_1 = -2$, $D_2 = -17$ és $D_3 = 22$, tehát alkalmazható az algoritmus. A $D_3 \neq 0$, azaz a mátrixunk determinánsa nem 0, ennélfogva a feltételeknek megfelel a példánk.

I. lépés: Végrehajtjuk a mátrixunk felső háromszögmátrixszá való átalakítását. Ritkán előfordulhat, hogy elakad a program, annak ellenére, hogy az algoritmus megvalósítható. Ez akkor következik be, ha a főátlóban 0 szerepel. Ekkor 0-val kellene osztanunk, ami nem lehetséges. Ezt főelemkiválasztással tudjuk orvosolni. A főelemkiválasztásnak az a lényege, hogy a számunkra rossz sort - ahol 0 szerepel a főátlóban - kicseréli olyan

[5] Lineáris egyenletrendszer
[6] Gauss-elimináció+részleges főelemkiválasztás
[7] A számoláshoz a Maple nevű programot használtam. A példához a linalg csomagot alkalmaztam.
[8] Itt a DD[i] jelentése az i. főminor.

sorral, hogy a csere után a főátlóban 0-tól különböző szám álljon. Ezt mindig meg fogjuk tudni csinálni, ugyanis ha nem tudnánk kicserélni, akkor a feldolgozásra váró blokkmátrixunk determinánsa 0 lenne, ez pedig ellentmond a feltevésünknek, hogy az alapmátrixunk determinánsa 0.

$GE := proc(A, b);$
$n := rowdim(A);$
$AA := augment(A, b);$
$for\ k\ to\ n-1\ do$
$\quad for\ i\ from\ k+1\ to\ n\ do$
$\quad s := -AA[i,k]/AA[k,k];$
$\quad for\ j\ from\ k\ to\ n+1\ do$
$\quad AA[i,j] := AA[i,j] + s * AA[k,j]$
$\quad od;$
$\quad od;$
$od;$
$evalm(AA);$
$end;$

A programmal a következő megoldás jön ki:

$$U = \begin{pmatrix} -2 & 3 & 8 \\ 0 & \frac{17}{2} & 28 \\ 0 & 0 & -\frac{22}{17} \end{pmatrix} \quad \text{és} \quad r = \begin{pmatrix} 3 \\ 10 \\ -\frac{13}{17} \end{pmatrix}$$

II. lépés: Miután megkaptuk az U mátrixot és az r vektort, rekurzív módon visszahelyettesítve ki lehet számolni a keresett x vektort.

$GE2 := proc(A, b);$
$n := rowdim(A);$
$AA := augment(A, b);$
$for\ k\ to\ n-1\ do$
$\quad for\ i\ from\ k+1\ to\ n\ do$
$\quad s := -AA[i,k]/AA[k,k];$
$\quad for\ j\ from\ k\ to\ n+1\ do$
$\quad AA[i,j] := AA[i,j] + s * AA[k,j]$
$\quad od;$
$\quad od;$
$od;$
$x := vector(n, 0);$
$x[n] := AA[n, n+1]/AA[n, n];$

$for\ l\ from\ n-1\ by\ -1\ to\ 1\ do$
$x[l] := (AA[l, n+1] - (sum(AA[l, p] * x[p], p = l+1..n)))/AA[l, l]$
$od;$
$evalm(x);$
$end;$

Így a végső megoldás: $x = \begin{pmatrix} \frac{23}{11} \\ \frac{9}{11} \\ \frac{13}{22} \end{pmatrix}$.[9]

Megyjegyzés I.: A Gauss-elimináció megbízhatóságának egyik fontos kritériuma a közelítő adatokkal történő számolások esetén a hibanövekedés kontrollálása. A gyakorlatban a különböző mérésekhez felírt lineáris egyenletrendszerekhez használhatjuk a GE eljárást. Ekkor már azonban megjelennek a mérési hibák. Az elimináció során arra kell figyelnünk, hogy egy hibanövekedés ne legyen túl nagy.
Főelemkiválasztás előnye: Mivel mindig az adott oszlop (sor) legnagyobb abszolút értékű elemével osztunk, így a hiba kicsi lesz, nem fog nagyra nőni. Ez a veszély akkor állna fenn, ha egy kis számmal osztanánk. Például a hiba értéke jobban nő, ha 0,2 helyett 0,1-gyel osztunk, mintha 10,2 helyett 10,1-gyel.[10]

A részleges főelemkiválasztás előnye a teljessel szemben, hogy az előző eredményesség megtartása mellett nem jár a munkaigény megduplázásával, mint a teljes változatban.

Megjegyzés II.: Természetesen nemcsak négyzetes mátrixokra tudjuk alkalmazni a Gauss-eliminációt, azonban ott sokkal bonyolultabbá válhat az eljárás.

[9] Természetesen a Maple program fejlettségének köszönhetően tartalmaz alapalgoritmusokat, mint például a Gauss-elimináció. Ezáltal használhatjuk a gausselim ill. a linsolve parancsot a felső háromszögmátrix és a megoldást adó vektor kiszámolásához. Előfordulhat, hogy a felső háromszögmátrixunk nem egyezik meg a beépített programmal kijövő mátrixszal. Ennek oka, hogy utóbbi főelemkiválasztást hajt végre az algoritmus közben, így a lehető legegyszerűbb eredményt adja. A megoldó vektor persze a két fajta számolással mindig megegyezik.

[10] Az egy tizedes eltérések mérési hibák.

3. fejezet

Gröbner-bázis

3.1. Történelem

A Gröbner-bázisok eredete:

A múlt évszázad matematikájának egyik célja a nemlineáris többváltozós egyenletrendszerek zárt megoldásainak megtalálása volt. 1949-ben W. Gröbner[1] tett erre egy javaslatot, amit 1965-ben tanítványa, **Bruno Buchberger**[2] dolgozott ki részletesen Ph.D. dolgozatának keretében. Buchberger a témavezetője tiszteletére az alkalmazott formulát Gröbner-bázisnak nevezte el. Munkásságáért 2007-ben elnyerte a "Paris Kanellakis Elmélet és Gyakorlat"[3] díjat.
Tőlük függetlenül hasonló koncepciót fejlesztett ki Heisuke Hironaka[4] 1964-ben. Ő a formulát standard bázisnak keresztelte el.
Említésre méltó még A.I. Shirshov[5] neve, aki 1962-ben dolgozott ki egy analóg teóriát, sajnos azonban munkája a Szovjetunión kívül szinte teljesen ismeretlen maradt.

3.2. Bevezetés

A főtémánk elkezdése előtt érdemes még bevezetni néhány fogalmat.

Tagsorrend: A $\prec$ reláció egy tagsorrend a monomokon, ha egy olyan teljes rendezés, melynek minimális eleme 1, és szorzásra nézve monoton, azaz ha bármely két tagot megszorzunk egy azonos elemmel, a sorrend nem változik.

A három leggyakrabban használt tagsorrend:

[1] Wolfgang Gröbner, osztrák matematikus, 1899-1980.
[2] Bruno Buchberger, osztrák matematikus, 1942-.
[3] Paris Christos Kanellakis, görög informatikus, 1953-1995.
[4] Heisuke Hironaka, japán matematikus, 1931- .
[5] AI Shirshov, orosz matematikus, 1921-1981.

- a **lexikografikus elrendezés**[6]

- a **fok-kompatibilis lexikografikus elrendezés:** Jelölés: *grlex*. Azt mondjuk, hogy P *grlex* kisebb Q-nál, ha P foka kisebb, mint Q foka, azonos fokszám esetén pedig P lexikografikusan kisebb, mint Q.
Azaz először a fokszám szerint rendezünk, majd az azonos fokúkat *lex* szerint.
Példa:$f(x_1, x_2, x_3) = 13x_1^2x_3^2 + ix_1^3 + \pi x_1^2x_2 - 5x_2^3 + 6x_1x_2^3$.
Grlex elrendezés: $f(x_1, x_2, x_3) = -5x_2^3 + \pi x_1^2x_3 + ix_1^3 + 6x_1x_2^3 + 13x_1^2x_3^2$.[7]

- a **fok-kompatibilis fordított lexikografikus elrendezés:** Jelölés: *grevlex*. Legyen $P = rx_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ és $Q = sx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$. Azt mondjuk, hogy P *grevlex* kisebb Q-nál, ha P foka kisebb, mint Q foka, azonos fokszám esetén pedig P kisebb, mint Q, ha a legnagyobb i indexre - $i \in \{1, \ldots, n\}$ -, ahol $m_i \neq k_i$, ott $m_i > k_i$.
Példa:$f(x_1, x_2, x_3) = 13x_1^2x_3^2 + ix_1^3 + \pi x_1^2x_2 - 5x_2^3 + 6x_1x_2^3$.
Grevlex elrendezés: $f(x_1, x_2, x_3) = \pi x_1^2x_3 - 5x_2^3 + ix_1^3 + 13x_1^2x_3^2 + 6x_1x_2^3$. [8]

Ideál varietása: $V(I)$-t az I ideálhoz tartozó varietásnak nevezzük:

$$V(I) = \{u \in \mathbb{C}[\mathbf{x}] : f(u) = 0, \forall f \in I\}.$$

Példa: Legyen $I =< x^2 - x, y^2 - y >$. Ekkor $V(I)$ azok a pontok, amelyek igazzá teszik ezt a két egyenletet: $x^2 - x = 0$ és $y^2 - y = 0$. Ez alapján:

$$V(I) = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Legyen $I =< x^2 + y^2 - 1 >$. Ekkor $V(I) = \{$Az origó középpontú 1 sugarú kör$\}$.

Nézzük meg, hogyan tudjuk értelmezni az előbbieket a lineáris egyenletrendszernél:

$$\text{Általános eset: } Ax = b, \text{ ahol } A \in \mathbb{R}^{n\times k},\ x \in \mathbb{R}^k,\ b \in \mathbb{R}^n.$$

(1) Nincs megoldás: $\longrightarrow$ $V(I) = \emptyset$.

(2) Van megoldás:
(a) homogén[9] az egyenletrendszer, azaz:
$Ax = 0$ $\longrightarrow$ $V(I)$ elemei az $\mathbb{R}^k$-nak egy alterét alkotják.

---

[6] Lásd 2.5. alfejezet.

[7] (Fokszámok, telefonszámok): $x_1^2x_3^2 : (4, 202)$, $x_1^3 : (3, 300)$, $x_1^2x_3 : (3, 201)$, $x_2^3 : (3, 030)$, $x_1x_2^3 : (4, 130)$. $\rightarrow$ $(3, 030) < (3, 201) < (3, 300) < (4, 130) < (4, 202)$

[8] (Fokszámok, telefonszámok): $x_1^2x_3^2 : (4, 202)$, $x_1^3 : (3, 300)$, $x_1^2x_3 : (3, 201)$, $x_2^3 : (3, 030)$, $x_1x_2^3 : (4, 130)$. $\rightarrow$ $(3, 20\mathbf{1}) < (3, 0\mathbf{30}) < (3, 3\mathbf{0}0) < (4, 20\mathbf{2}) < (4, 13\mathbf{0})$

[9] Egy lineáris egyenletrendszer homogén, ha mindegyik b_j $(j = 1, \ldots, n)$ nullával egyenlő. Triviális a megoldás, ha az összes ismeretlen nulla.

(b) nem homogén az egyenletrendszer:
Mivel az általános esetnek létezik megoldása: $Ax_0 = b$.
$\longrightarrow \quad A(x - x_0) = b - b = 0$. A 2a, miatt a megoldások egy U egy alteret fognak alkotni $\mathbb{R}^k$-ban: $x - x_0 \in U \quad \longrightarrow \quad V(I) = \{x = x_0 + u \mid u \in U\} = x_0 + U$.

Állítás: $V(I)$ egy affin varietás. Nevezetesen, ha $I =< f_1, \ldots, f_n >$, akkor $V(I) = V(f_1, \ldots, f_n)$.

Ideál főtagja: Legyen $I \lhd \mathbb{C}[\mathbf{x}]$ egy ideál. Ekkor

$$\mathrm{Lm}(I) = \{\mathrm{lm}(f) : \ f \in I, \ f \neq 0\},$$

azaz I főtagjainak Lm(I) halmaza az I-ben szereplő nem nulla polinomok főtagjaiból áll.

Standard monom: Az I ideál standard monomjai azoknak a monomoknak halmazai, amelyekre teljesül, hogy semelyik $f \in I$ polinomnak sem főtagja, azaz

$$\mathrm{Sm}(I) = \{\mathbf{x}^\alpha \in \mathbb{C}[\mathbf{x}]\} \setminus \mathrm{Lm}(I) = \{\mathbf{x}^\alpha : \nexists f \in I, \text{amelyre } \mathrm{lm}(f) = \mathbf{x}^\alpha\}.$$

3.3. Maradékos osztás

A maradékos osztás értelmezése a többhatározatlanú polinomok rendszerére:

Az egyhatározatlanú polinomok oszthatóságát ki tudjuk terjeszteni a többhatározatlanú polinomokra, azonban itt már korántsem egyértelmű megoldásokat kapunk.

Definíció: Legyen egy adott tagsorrendünk, és legyen egy s-elemű polinomhalmazunk, $F = (f_1, \ldots, f_s) \in \mathbb{C}[\mathbf{x}]$. Ekkor minden $f \in \mathbb{C}[\mathbf{x}]$ polinomot fel tudunk írni úgy, hogy

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

ahol $a_i, r \in \mathbb{C}[\mathbf{x}]$, és $r = 0$ vagy r egy olyan polinom, amelynek főtagja, és ennek következtében egyik tagja sem osztható semelyik f_i főtagjával. Az r-t az f polinom F rendszer szerinti osztási maradékának hívjuk, és ez általában nem egyértelmű. Jelölés: $f \ rem \ F$. Továbbá, ha $a_i f_i \neq 0$, akkor fennáll

$$\mathrm{multigr}(f) \geq \mathrm{multigr}(a_i f_i).$$

Ilyen előállítást kaphatunk a következő **eljárással**[10]. Vesszük az osztandó és osztó polinom főtagját. Ha osztható, akkor a hányadossal megszorozzuk az osztót, és a szorzatot kivonjuk az osztandó polinomból. A kapott hányadosokból épülnek fel az a_i együtthatós polinomok. Ha már nem tudunk tovább osztani, akkor a megmaradó eredmény az r osztási maradék lesz.

Példa I.: $F = (f_1, f_2),\ f = f_{(0)} = xy^2 + 1,\ f_1 = xy + 1,\ f_2 = y + 1$ és $x \succ y$.
$\rightarrow\ \mathrm{lm}(f) = xy^2,\ \mathrm{lm}(f_1) = xy,\ \mathrm{lm}(f_2) = y.$
$\mathrm{lm}(f)$ osztható $\mathrm{lm}(f_1)$-gyel $\rightarrow\ \mathrm{lm}(f)/\mathrm{lm}(f_1) = y\ \rightarrow\ a_1 = y.$
$\rightarrow\ f_{(1)} = f - yf_1 = xy^2 + 1 - y(xy + 1) = -y + 1\ \rightarrow \mathrm{lm}(f_{(1)}) = -y.$
$\mathrm{lm}(f_{(1)})$ nem osztható $\mathrm{lm}(f_1)$-gyel, de $\mathrm{lm}(f_2)$-vel igen:
$\rightarrow\ \mathrm{lm}(f_{(1)})/\mathrm{lm}(f_2) = -1\ \rightarrow\ a_2 = -1.$
$\rightarrow\ f_{(2)} = f_{(1)} - (-1)f_2 = -y + 1 - ((-1)(y + 1)) = 2.$
Mivel $\mathrm{lm}(f_{(2)}) = 0$, ezért $f_{(2)} = 2 = r$.

$f = a_1f_1 + a_2f_2 + r = y(xy + 1) + (-1)(y + 1) + 2 = xy^2 + 1.$

Példa II.(a): $F = (f_1, f_2),\ f = f_{(0)} = xy^2 - x,\ f_1 = xy + 1,\ f_2 = y^2 - 1,\ x \succ y.$
$\rightarrow\ \mathrm{lm}(f) = xy^2,\ \mathrm{lm}(f_1) = xy,\ \mathrm{lm}(f_2) = y^2.$
$\mathrm{lm}(f)$ osztható $\mathrm{lm}(f_1)$-gyel $\rightarrow\ \mathrm{lm}(f)/\mathrm{lm}(f_1) = y\ \rightarrow\ a_1 = y.$
$\rightarrow\ f_{(1)} = f - yf_1 = xy^2 - x - y(xy + 1) = -x - y\ \rightarrow \mathrm{lm}(f_{(1)}) = -x.$
$\mathrm{lm}(f_{(1)})$ nem osztható sem $\mathrm{lm}(f_1)$-gyel, sem $\mathrm{lm}(f_2)$.
$\rightarrow f(1) = -x - y = r.$

$f = a_1f_1 + r = y(xy + 1) + (-x - y) = xy^2 - x.$

Példa II.(b): $F = (f_2, f_1),\ f = f_{(0)} = xy^2 - x,\ f_1 = xy + 1,\ f_2 = y^2 - 1,\ x \succ y.$
$\rightarrow\ \mathrm{lm}(f) = xy^2,\ \mathrm{lm}(f_1) = xy,\ \mathrm{lm}(f_2) = y^2.$
$\mathrm{lm}(f)$ osztható $\mathrm{lm}(f_2)$-gyel $\rightarrow\ \mathrm{lm}(f)/\mathrm{lm}(f_2) = x\ \rightarrow\ a_2 = x.$
$\rightarrow\ f_{(1)} = f - xf_2 = xy^2 - x - x(y^2 - 1) = 0\ \rightarrow \mathrm{lm}(f_{(1)}) = 0$ és $r = 0.$

$f = a_2f_2 + r = x(y^2 - 1) + 0 = xy^2 - x.$

Példa III.: $F = (f_1, f_2),\ f = f_{(0)} = x^2y + xy^2 + y^3,\ f_1 = xy - 1,$
$f_2 = y^2 - 1$ és $x \succ y$.
$\rightarrow\ \mathrm{lm}(f) = x^2y,\ \mathrm{lm}(f_1) = xy,\ \mathrm{lm}(f_2) = y^2.$
$\mathrm{lm}(f)$ osztható $\mathrm{lm}(f_1)$-gyel $\rightarrow\ \mathrm{lm}(f)/\mathrm{lm}(f_1) = x\ \rightarrow\ a_1 = x.$
$\rightarrow\ f_{(1)} = f - xf_1 = x^2y + xy^2 + y^3 - x(xy - 1) = xy^2 + x + y^3\ \rightarrow \mathrm{lm}(f_{(1)}) = xy^2.$
$\mathrm{lm}(f_{(1)})$ osztható $\mathrm{lm}(f_1)$-gyel $\rightarrow\ \mathrm{lm}(f_{(1)})/\mathrm{lm}(f_1) = y\ \rightarrow\ a_1 = x + y.$

[10] A precíz meghatározást lásd a 3.5. alfejezetben.

$\rightarrow\ f_{(2)} = f_{(1)} - xf_1 = xy^2 - x + y^3 - y(xy-1) = x + y + y^3\ \rightarrow \mathrm{lm}(f_{(2)}) = x.$
Tegyük be x-et az osztási maradékok közé, majd folytassuk az eljárást: $\rightarrow\ f_{(2)} = y + y^3$ és $\rightarrow \mathrm{lm}(f_{(2)}) = y^3$.
$\mathrm{lm}(f_{(2)})$ nem osztható $\mathrm{lm}(f_1)$-gyel, de $\mathrm{lm}(f_2)$-vel már igen:
$\rightarrow\ \mathrm{lm}(f_{(2)})/\mathrm{lm}(f_2) = y\ \rightarrow\ a_2 = y.$
$\rightarrow\ f_{(3)} = f_{(2)} - yf_2 = y + y^3 - y(y^2-1) = 2y.$
Miután $\rightarrow \mathrm{lm}(f_{(3)}) = 2y$, ezért $\mathrm{lm}(f_{(3)})$ nem osztható $\mathrm{lm}(f_2)$-vel sem, így $f_{(3)}$ is osztási maradék lesz.

$f = a_1f_1 + a_2f_2 + r = (x+y)(xy-1) + y(y^2-1) + x + 2y = x^2y + xy^2 + y^3.$

A 2. példánk jól mutatja, hogy a többhatározatlanú polinom osztásánál nagyon fontos, hogy milyen sorrendben osztunk. Arra törekszünk, hogy az osztási maradék 0 legyen, ha $f \in < F >$.
Az F csak akkor lesz jó generátorrendszere az I ideálnak, ha F Gröbner-bázisa az f-nek.

3.4. Gröbner-bázis

Monomiális ideál: Egy ideál monomiális, ha van monomokból álló generátorrendszere. Azaz az $I \lhd \mathcal{R}$ ideált monomiális ideálnak nevezzük, ha létezik olyan $A \subseteq \mathbb{N}^n$, amelyre

$$I =< \mathbf{x}^A >=< \{\mathbf{x}^\alpha \in \mathbb{C}[\mathbf{x}] : \alpha \in A\} >$$

Két monomiális ideál akkor és csak akkor azonos, ha ugyanazokat a monomokat tartalmazzák.

Legyen $I =< \mathbf{x}^\alpha : \alpha \in A >$ egy monomiális ideál. Ekkor az $\mathbf{x}^\beta$ monom pontosan akkor van benne az I ideálban, ha $\mathbf{x}^\beta$ osztható $\mathbf{x}^\alpha$-val valamely $\alpha \in A$-ra.

Dickson-lemma: Minden monomiális ideál végesen generálható, más szóval minden $A \subseteq \mathbb{N}^n$ esetén létezik olyan $B \subseteq A$ véges halmaz, amelyre $< \mathbf{x}^A >=< \mathbf{x}^B >$.

Legyen $I \subseteq \mathbb{C}[\mathbf{x}]$.
(i) $< \mathrm{Lm}(I) >$ egy monomiális ideál.
(ii) Létezik $g_1, \ldots, g_n \in I$, úgy hogy $< \mathrm{Lm}(I) >=< \mathrm{Lm}(g_1), \ldots, \mathrm{Lm}(g_n) >$ teljesül.

Hilbert-féle bázistétel: Minden $I \subseteq \mathbb{C}[\mathbf{x}]$ ideál végesen generálható. Azaz létezik $G = \{g_1, \ldots, g_n\} \in I$, amelyre teljesül, hogy $I =< G >$.

A Gröbner-bázist többféleképpen tudjuk definiálni:

A tételben szereplő G véges halmazt az I ideál $\prec$ rendezésre vonatkozó Gröbner-bázisának nevezzük, ha a következő, egymással ekvivalens tulajdonságok bármelyike teljesül.

(I.) **Gröbner-bázis:** Legyen $I =< G >$. Az I ideál Gröbner-bázisának olyan véges $G \subseteq I$ halmazt nevezünk, amelyre teljesül, hogy minden $f \in I,\ f \neq 0$ polinomhoz létezik $g \in G$, amelyre $\mathrm{lm}(g)$ osztója $\mathrm{lm}(f)$-nek. Azaz $G \subseteq I$ véges halmaz I Gröbner-bázisa, ha $\mathrm{Lm}(I) = \mathrm{Lm}(G)$.

(II.) **Gröbner-bázis:** Legyen $G = \{g_1, \ldots, g_n\}$ Gröbner bázisa egy $I \in \mathbb{C}[\mathbf{x}]$ ideálnak és $f \in I$. Ekkor egyértelműen létezik $r \in \mathbb{C}[\mathbf{x}]$ a következő tulajdonságokkal:
(i) Létezik $g \in I$, hogy $f = g + r$, és
(ii) r-nek nincs olyan tagja, amely osztható bármelyik $\mathrm{lm}(g_i)$-vel.

A gyakorlatban r-t az f polinom G szerinti osztási maradékának hívjuk, nem számít, hogy milyen sorrendben használjuk G elemeit az osztási algoritmus során.

(III.) **Gröbner-bázis:** Legyen $G = \{g_1, \ldots, g_n\}$ részhalmaza egy $I \in \mathbb{C}[\mathbf{x}]$ ideálnak és $f \in \mathbb{C}[\mathbf{x}]$. Ekkor G pontosan akkor lesz Gröbner-bázis, ha $f \in I$, azaz ha f polinom G szerinti osztási maradéka 0.

(IV.) **Gröbner-bázis:** Legyen $G = \{g_1, \ldots, g_n\}$ nemnulla polinomok halmaza. G csak akkor Gröbner-bázisa a $< G >$ ideálnak, ha $\forall\ g_i, g_j \in G$ esetén $S(g_i, g_j)$[11]-nek G-vel vett redukáltja[12] 0.

Fontos megjegyzés: A Gröbner-bázis általában függ a tagsorrendtől, ugyanis egy polinom főtagját nagyon befolyásolja a választott tagsorrend.[13]

Példa I.: Legyen $I =< f_1, f_2 >,\ f_1 = x^3 - 2xy,\ f_2 = x^2y - 2y^2 + x$. Használjunk *grlex* rendezést. Ekkor $G = \{f_1, f_2\}$ Gröbner-bázis-e?
Új tagsorrend: $f_1 = -2xy + x^3$ és $f_2 = x - 2y^2 + x^2y$.
$\rightarrow\ \mathrm{lm}(f_1) = x^3,\ \mathrm{lm}(f_2) = x^2y$. Vegyük a következő tagot: $yf_1 - xf_2$.
$y(-2xy + x^3) - x(x - 2y^2 + x^2y) = -2xy^2 + x^3y - x^2 + 2y^2x - x^3y = -x^2$.
Így $-x^2 \in I$. Azonban az x^2 nem osztható se $\mathrm{lm}(f_1)$-gyel, se $\mathrm{lm}(f_2)$-vel.
Tehát $-x^2 \notin < \mathrm{lm}(f_1), \mathrm{lm}(f_2) >$. Ezért az G nem Gröbner-bázis.

Példa II.: Legyen $I =< f_1, f_2 >,\ f_1 = x_1 + x_2,\ f_2 = x_1 - x_2$ és $x_2 \succ x_1$.
$\mathrm{lm}(f_1) = x_2$ és $\mathrm{lm}(f_2) = x_2$. $G = \{f_1, f_2\}$ Gröbner-bázis-e?
Ekkor $(f_1 + f_2)/2 = x_1 \in I$. De x_1 nem osztható se $\mathrm{lm}(f_1)$-gyel, se $\mathrm{lm}(f_2)$-vel.
Tehát G nem Gröbner-bázis.
Legyen $g_1' = x_1$ és $g_2' = x_2$. $G' = \{g_1', g_2'\}$ Gröbner-bázis-e?

[11] Lásd a 3.6. alfejezetben.
[12] Lásd a 3.5. alfejezetben.
[13] Lásd a 3.6. alfejezetben a Gröbner-bázis (IV.) féle definíciójára alkalmazazott példát.

Kell: $G' \subseteq I$. Mivel $\frac{f_1 + f_2}{2} = x_1$ és $\frac{f_1 - f_2}{2} = x_2$. Azaz $G' \subseteq I$.
Kell: $\forall f \in I,\ f \neq 0$ polinomhoz $\exists g' \in G'$, amelyre $\mathrm{lm}(g')$ osztója $\mathrm{lm}(f)$-nek.
Ha $\mathrm{lm}(g')$ nem osztója $\mathrm{lm}(f)$-nek, akkor $\mathrm{lm}(f) = 1 \to f$ konstans $c \neq 0$.
Kell $c \notin I$. Ez igaz, mert ha x_1 és x_2 is 0, akkor a két generátorelem 0-t ad, és ennek I minden elemére teljesülnie kell. $\longrightarrow G'$ Gröbner-bázis.

Kérdés, hogy tetszőleges ideálnak létezik-e Gröbner-bázisa?

A Hilbert-féle bázistétel hasznos következménye:

$\mathbb{C}[\mathbf{x}]$ minden I ideáljának van Gröbner-bázisa.

3.5. Redukció

Ebben az alfejezetben áttekintjük a maradékos osztás egyik lépésének a pontos megfogalmazását.

Redukció: Legyen $f, g \in \mathbb{C}[\mathbf{x}]$. Ekkor

$$\tilde{f}(\mathbf{x}) = f(\mathbf{x}) - \frac{c_f \cdot \mathbf{x}^\alpha}{c_g \cdot \mathrm{lm}(g)} \cdot g(\mathbf{x}),$$

ahol $\mathbf{x}^\alpha$ f egy monomja, ami osztható $\mathrm{lm}(g)$-vel, c_f $\mathbf{x}^\alpha$ együtthatója, c_g pedig g főegyütthatója.

Ekkor $\mathbf{x}^\alpha$ kiesik, és $\tilde{f}$-ben $\mathbf{x}^\alpha$ helyett nála csak szigorúan kisebb monomok lesznek.

Példa: $f(\mathbf{x}) = x_1^3 + x_1x_2 - x_2^2,\ g(\mathbf{x}) = 2x_1^2 - x_2$.
$\frac{c_f \cdot \mathbf{x}^\alpha}{c_g \cdot \mathrm{lm}(g)} \cdot g(\mathbf{x}) = (x_1^3/2x_1^2) \cdot (2x_1^2 - x_2) = x_1^3 - \frac{x_1x_2}{2}$.
Így: $\tilde{f}(\mathbf{x}) = x_1^3 + x_1x_2 - x_2^2 - (x_1^3 - \frac{x_1x_2}{2}) = \frac{x_1x_2}{2} - x_2^2$.

Ha G polinomok egy véges halmaza és $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$, akkor azt mondjuk, hogy f redukált G-re nézve, amennyiben f semelyik monomját sem osztja semelyik $g \in G$ vezető tagja.

Ezek alapján $f(\mathbf{x})$ felbontható a következőképpen:

$$f(\mathbf{x}) = \sum_{i=1}^{n} g_i(\mathbf{x})h_i(\mathbf{x}) + \tilde{f}(\mathbf{x}),$$

ahol $\tilde{f}$ redukált polinom G-re nézve, $G = \{g_1, \ldots, g_n\},\ h_1, \ldots, h_n \in \mathbb{C}[\mathbf{x}]$, továbbá igaz, hogy $\mathrm{lm}(g_ih_i) \preceq \mathrm{lm}(f)$.

Állítás: Ha G az I ideál Gröbner-bázisa, akkor tetszőleges $f \in \mathbb{C}[\mathbf{x}]$ polinom G redukáltja egyértelmű, és $f \in I$ csak akkor, ha a redukált 0.

Bizonyítás: Legyen $\tilde{f}_1$ és $\tilde{f}_2$ redukáltja G-nek. Ekkor a különbségük is benne lesz az I ideálban, azonban a $\tilde{f}_1 - \tilde{f}_2$ standard monomok lineáris kombinációja, ezért $\tilde{f}_1 - \tilde{f}_2 = 0$. Az f és 0 redukáltja egyenlő, mivel f és 0 mod I megegyezik. Ezenfelül 0 már redukált, ebből következik, hogy az f redukáltja 0.

A megfordítás is igaz:
Ha $G \subseteq I$ véges, és $\forall f \in I$ polinom G-vel redukálható 0-ra,
akkor G Gröbner-bázis.
Ha $G \subseteq I$ véges, $< G >= I$ és $\forall f \in \mathbb{C}[\mathbf{x}]$ polinom G szerinti redukáltja egyértelmű, akkor G Gröbner-bázis.

3.6. Buchberger-algoritmus

Egy ideál Gröbner-bázisának meghatározásához általános módszert ad a Buchberger-algoritmus.

Definíció: Legyen $f, g \in \mathbb{C}[\mathbf{x}]$ nemnulla polinomok.
(i) Ha multigr$(f) = \alpha$ és multigr$(g) = \beta$, akkor legyen $\gamma = (\gamma_1, \ldots, \gamma_n)$,
ahol $\gamma_i = \max(\alpha_i, \beta_i)$ $\forall i$-re. Ekkor nevezzük $\mathbf{x}^\gamma$-t az f és g főtagjának legkisebb közös többszörösének. Az f és g polinomok főegyütthatójai a c_f ill. c_g.
(ii) Legyen az f és g S-polinomja:

$$S(f,g) = \frac{\mathbf{x}^\gamma}{c_f \cdot \mathrm{lm}(f)} \cdot f(\mathbf{x}) - \frac{\mathbf{x}^\gamma}{c_g \cdot \mathrm{lm}(g)} \cdot g(\mathbf{x}).$$

Megfigyelhető, hogy a kisebbítendő és a kivonandó legmagasabb fokú tagja megegyezik, ami egyenlő $\mathbf{x}^\gamma$-val, így $S(f,g)$-ből kiesik $\mathbf{x}^\gamma$, ezáltal
$\mathrm{lm}(S(f,g)) \prec \mathbf{x}^\gamma$.

Példa: $f(x_1, x_2) = x_1^3 x_2^2 - x_1^2 x_2^3 + x_1$, $g(x_1, x_2) = 3x_1^4 x_2 + x_2^2$ és legyen grlex rendezés.
Ekkor $\mathrm{lm}(f) = x_1^3 x_2^2$ és $\mathrm{lm}(g) = x_1^4 x_2 \implies \gamma = (4,2)$. Így

$$S(f,g) = \frac{x_1^4 x_2^2}{x_1^3 x_2^2} \cdot f - \frac{x_1^4 x_2^2}{3x_1^4 x_2} \cdot g = x_1 \cdot f - \frac{1}{3} \cdot x_2 \cdot g = -x_1^3 x_2^3 + x_1^2 - \frac{1}{3} x_1^3,$$

$\implies \mathrm{lm}(S(f,g)) = x_1^3 x_2^3 \prec \mathbf{x}^\gamma = x_1^4 x_2^2$.

Lemma: Legyenek $f_1, \ldots, f_s$ közös $\mathbf{x}^\gamma$ főtagú és 1 főegyütthatójú polinomok. Feltesszük, hogy $f = \sum_{i=1}^{s} c_i f_i$ valamilyen $c_i \in \mathbb{C}$ együtthatókkal.

Ha $\mathrm{lm}(f) \prec x^\gamma$, akkor f előáll $f = \sum_{i=1}^{s-1} c_i^* S(f_i, f_{i+1})$ alakban, ahol $c_i^* \in \mathbb{C}$.

Nézzünk egy példát a Gröbner-bázis (IV.) féle definíciójának alkalmazására:

Legyen $I =< x_2 - x_1^2, x_3 - x_1^3 >$ ideál. Ekkor $G = \{x_2 - x_1^2, x_3 - x_1^3\}$
Gröbner-bázis $x_2 \succ x_3 \succ x_1$ lex rendezés mellett, ugyanis:

$$S(x_2 - x_1^2, x_3 - x_1^3) = \frac{x_2 x_3}{x_2}(x_2 - x_1^2) - \frac{x_2 x_3}{x_3}(x_3 - x_1^3) = -x_3 x_1^2 + x_2 x_1^3.$$

A maradékos osztási algoritmust használva találunk olyan felbontást, hogy

$$-x_3 x_1^2 + x_2 x_1^3 = x_1^3 \cdot (x_2 - x_1^2) + (-x_1^2) \cdot (x_3 - x_1^3) + 0.$$

Így $S(x_2 - x_1^2, x_3 - x_1^3)\ rem\ G = 0$.

$\Longrightarrow$ G Gröbner-bázisa az I ideálnak.

Figyeljük meg, hogy ezzel szemben az $x_1 \succ x_2 \succ x_3$ rendezés mellett G nem lesz Gröbner-bázis. Ekkor

$$S(x_2 - x_1^2, x_3 - x_1^3) = \frac{x_1^3}{-x_1^2}(x_2 - x_1^2) - \frac{x_1^3}{-x_1^3}(x_3 - x_1^3) = -x_1 x_2 + x_3.$$

Mivel sem $\mathrm{lm}(g_1) = x_1^2$, sem $\mathrm{lm}(g_2) = x_1^3$ nem osztója a fent kapott polinom főtagjának, ezért $S(x_2 - x_1^2, x_3 - x_1^3)\ rem\ G = x_1 x_2 + x_3 \neq 0$, tehát G nem Gröbner-bázis.

Buchberger-algoritmus: Legyen $I =< f_1, \ldots, f_s >\in \mathbb{C}[\mathbf{x}]$ ideál és $F \subseteq I$ egy tetszőleges véges generátorrendszere. Adott $\prec$ monomiális rendezés mellett a következő eljárás véges számú lépésben véget ér, és az alábbi algoritmus megadja az I ideál egy $G \subseteq I$ Gröbner-bázisát.

Bemenet: $F = G = \{f_1, \ldots, f_s\}$

A pszeudokódos[14] algoritmus:

```
1   G ← {f_1, ..., f_s}
2   P ← {(f_i, f_j)[15] | f_i, f_j ∈ G, i < j, f_i ≠ f_j}
3    while P ≠ 0
4      do (f, g) ← egy tetszőleges pár P-ből
5         P ← P \ (f, g)
6         r ← S(f, g) rem G
7         if r ≠ 0
8           then G ← G ∪ {r}
```

[14] A pszeudokód az algoritmusok és általában az eljárások leírására használt olyan mesterséges formális nyelv, mely változókból és néhány állandó jelentésű szóból áll, és hasonlít a számítógépes programozási nyelvekre.

[15] Itt a zárójel egy rendezett párt jelöl.

9 $\quad P \leftarrow P \cup \{(f,r) \mid f \in G\}$

10 **return** G

Nézzük meg ezt egy konkrét **példán**:
Az algoritmus akkor ér véget, amikor P az üres halmaz lesz valamely teljes ciklus után. Az ekkor kapott G-t fogjuk Gröbner-bázisnak hívni.

$I =< f_1, f_2 >,\ f_1 = x^3 - 2xy,\ f_2 = xy^2 - 2y^2 + x$ és legyen *grlex* rendezés.

$\longrightarrow\ G = \{f_1, f_2\}$ és $P = \{(f_1, f_2)\},\ lm(f_1) = x^3,\ \mathrm{lm}(f_2) = x^2y.$

I. Először megvizsgáljuk az (f_1, f_2) párt[16]. Ekkor $P = \{\emptyset\}$.
$S(f_1, f_2) = -x^2$.
$\rightarrow r = f_3 = S(f_1, f_2)\ rem\ G = -x^2$.
Így $G = \{f_1, f_2, f_3\}$ és $P = \{(f_1, f_3), (f_2, f_3)\}$.
$\rightarrow S(f_1, f_2)\ rem\ G = 0$.

II. Ezután következzen az (f_1, f_3). $P = \{(f_2, f_3)\}$.
$S(f_1, f_3) = \frac{x^3}{x^3}(x^3 - 2xy) - \frac{x^3}{-x^2}(-x^2) = -2xy$.
$\rightarrow r = f_4 = S(f_1, f_3)\ rem\ G = -2xy$.
$G = \{f_1, f_2, f_3, f_4\}$ és $P = \{(f_2, f_3), (f_1, f_4), (f_2, f_4), (f_3, f_4)\}$.
$\rightarrow S(f_1, f_3)\ rem\ G = 0$.

III. A következő (f_2, f_3), és $P = \{(f_1, f_4), (f_2, f_4), (f_3, f_4)\}$.
$S(f_2, f_3) = \frac{x^2y}{x^2y}(xy^2 - 2y^2 + x) - \frac{x^2y}{-x^2}(-x^2) = -2y^2 + x$.
$\rightarrow r = f_5 = S(f_2, f_3)\ rem\ G = -2y^2 + x$.
$G = \{f_1, f_2, f_3, f_4, f_5\}$
és $P = \{(f_1, f_4), (f_2, f_4), (f_3, f_4), (f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.
$\rightarrow S(f_1, f_3)\ rem\ G = 0$.

IV. (f_2, f_3) és $P = \{(f_2, f_4), (f_3, f_4), (f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.
$S(f_1, f_4) = \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{-2xy}(-2xy) = -2xy^2$.
Mivel $S(f_1, f_4) = yf_4\ \rightarrow\ r = S(f_1, f_4)\ rem\ G = 0$.
$G = \{f_1, f_2, f_3, f_4, f_5\}$
és $P = \{(f_2, f_4), (f_3, f_4), (f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

[16]Ezt a 3.4. alfejezetben már megtettük.

V. (f_2, f_4) és $P = \{(f_3, f_4), (f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

$S(f_2, f_4) = \dfrac{x^2y}{x^2y}(xy^2 - 2y^2 + x) - \dfrac{x^2y}{-2xy}(-2xy) = -2y^2 + x.$

Amiért $S(f_2, f_4) = yf_5 \ \rightarrow \ r = S(f_2, f_4)\ rem\ G = 0.$

$G = \{f_1, f_2, f_3, f_4, f_5\}$ és $P = \{(f_3, f_4), (f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

VI. (f_3, f_4) és $P = \{(f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

$S(f_3, f_4) = \dfrac{x^2y}{-x^2}(-x^2) - \dfrac{x^2y}{-2xy}(-2xy) = 0.$

$\rightarrow \ r = S(f_3, f_4)\ rem\ G = 0.$

$G = \{f_1, f_2, f_3, f_4, f_5\}$ és $P = \{(f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

VII. (f_1, f_5) és $P = \{(f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

$S(f_1, f_5) = \dfrac{x^3y^2}{x^3}(x^3 - 2xy) - \dfrac{x^3y^2}{-2y^2}(-2y^2 + x) = \dfrac{x^4}{2} - 2xy^3.$

Itt ránézésre nem tudjuk eldönteni, ezért szükségünk van a maradékos osztásra:

$$\begin{array}{r} \dfrac{x^4}{2} - 2xy^3 \\ \underline{-\dfrac{x}{2}(x^3 - 2xy)} \\ x^2y - 2xy^3 \\ \underline{-(x^2y - 2y^2 + x)} \\ -2xy^3 + 2y^2 - x \end{array}$$

Így $S(f_1, f_5) = \dfrac{x}{2}f_1 + f_2 - y^2f_4 - f_5 \ \longrightarrow \ r = S(f_1, f_5)\ rem\ G = 0.$

$G = \{f_1, f_2, f_3, f_4, f_5\}$ és $P = \{(f_2, f_5), (f_3, f_5), (f_4, f_5)\}$.

VIII. (f_2, f_5) és $P = \{(f_3, f_5), (f_4, f_5)\}$.

$S(f_2, f_5) = \dfrac{x^2y^2}{x^2y}(x^2y - 2y^2 + x) - \dfrac{x^2y^2}{-2y^2}(-2y^2 + x) = \dfrac{x^3}{2} - 2y^3 + xy.$

Ismét maradékosan osztunk:

$$\begin{array}{r} \dfrac{x^3}{2} - 2y^3 + xy \\ \underline{-\dfrac{1}{2}(x^3 - 2xy)} \\ -2y^3 + 2xy \\ \underline{-y(-2y^2 + x} \\ xy \end{array}$$

Így $S(f_2, f_5) = \dfrac{1}{2}f_1 + yf_5 - \dfrac{f_4}{2} \ \longrightarrow \ r = S(f_2, f_5)\ rem\ G = 0.$

$G = \{f_1, f_2, f_3, f_4, f_5\}$ és $P = \{(f_3, f_5), (f_4, f_5)\}$.

IX. (f_3, f_5) és $P = \{(f_4, f_5)\}$.

$S(f_3, f_5) = \dfrac{x^2y^2}{-x^2}(-x^2) - \dfrac{x^2y^2}{-2y^2}(-2y^2 + x) = \dfrac{x^3}{2}$.

Mivel $S(f_3, f_5) = \dfrac{f_1}{2} - \dfrac{f_4}{2} \ \rightarrow \ r = S(f_3, f_5)\ rem\ G = 0$.

$G = \{f_1, f_2, f_3, f_4, f_5\}$ és $P = \{(f_4, f_5)\}$.

X. (f_4, f_5) és $P = \{\emptyset\}$.

$S(f_4, f_5) = \dfrac{xy^2}{-2xy}(-2xy) - \dfrac{xy^2}{-2y^2}(-2y^2 + x) = \dfrac{x^2}{2}$.

Miután $S(f_4, f_5) = -\frac{1}{2}x^2 \ \rightarrow \ r = S(f_4, f_5)\ rem\ G = 0 \ \rightarrow P = \{\emptyset\}$.

Végeztünk az algoritmussal, azaz:

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

Redukált Gröbner-bázis:

Egy I ideál Gröbner-bázisa nem egyértelmű és egy adott Gröbner-bázis általában nem minimális.

Lemma: Ha G az $I \subseteq \mathbb{C}[\mathbf{x}]$ ideál egy Gröbner-bázisa és
$\mathrm{lm}(g) \in < \mathrm{Lm}(G \backslash \{g\}) >$, akkor $G \setminus \{g\}$ is egy Gröbner-bázisa I-nek.

Minimális Gröbner-bázis: Azt mondjuk, hogy a $G \subseteq \mathbb{C}[\mathbf{x}]$ halmaz az $I =< G >$ ideál minimális Gröbner-bázisa, ha Gröbner-bázis és $\forall g \in G$ esetén:
(i) $\mathrm{lc}(g) = 1$,
(ii) $\mathrm{lm}(g) \notin < \mathrm{Lm}(G \backslash \{g\}) >$.

Most visszatérek az előző **példámhoz**:

Az $I =< x^3 - 2xy, xy^2 - 2y^2 + x >$ ideálnak *grlex* rendezés mellett
$G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$ egy Gröbner-bázisa volt.

Ekkor $\mathrm{lm}(f_1) = x^3,\ \mathrm{lm}(f_2) = x^2y,\ \mathrm{lm}(f_3) = -x^2,\ \mathrm{lm}(f_4) = -2xy,\ \mathrm{lm}(f_5) = -2y^2$.

Először, ahol a főtagok együtthatója nem 1, ott átalakítjuk a polinomokat úgy, hogy teljesítse az előző definícióban leírt első feltételt:

$\{\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \tilde{f}_4, \tilde{f}_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, x^2, xy, -2y^2 + x\}$.

Második lépésben a fenti lemma szerint csökkentjük a Gröbner-bázisunkat:

$\mathrm{lm}(f_1) = x^3 = -x \cdot \mathrm{lm}(f_3) = x \cdot x^2 \ \longrightarrow$ az f_1 polinom elhagyható.

$\mathrm{lm}(f_2) = x^2y = -y \cdot \mathrm{lm}(f_3) = y \cdot x^2 \ \longrightarrow$ az f_2 polinom is elhagyható.

Ennélfogva az I ideálnak egy minimális Gröbner-bázisa:

$G = \{\tilde{f}_1, \tilde{f}_2, \tilde{f}_3\} = \{x^2, xy, y^2 - \frac{1}{2}x\}$.

Sajnos az adott ideálunknak végtelen sok minimális Gröbner-bázisa van.
Például: $G = \{\tilde{f}_1, \tilde{f}_2, \tilde{f}_3\} = \{x^2 + axy, xy, y^2 - \frac{1}{2}x\}$, ahol a egy bármilyen konstans.
Szerencsére mindig lesz egy minimális bázis, ami jobb, mint a többi.

Redukált Gröbner-bázis: Ha az I ideál G Gröbner-bázisára teljesül, hogy $\forall g \in G$ redukált $G\backslash\{g\}$-re nézve és főegyüttható 1, akkor G az I redukált Gröbner-bázisa.
Azaz G Gröbner-bázis csak akkor redukált, ha $\forall g \in G$-ben $\mathrm{lm}(g)$-t leszámítva csak standard monom tagok szerepelnek, és g főegyüttható 1.

A **példánk** folytatása:
Ebben az esetben csak akkor lesz a Gröbner-bázis redukált, ha $a = 0$.

Tehát a keresett minimális, redukált Gröbner-bázis:
$G = \{\tilde{f}_1, \tilde{f}_2, \tilde{f}_3\} = \{x^2, xy, y^2 - \frac{1}{2}x\}$.[17]

Tétel: Tetszőleges I ideálhoz egy rögzített tagsorrend mellett egyértelműen létezik redukált Gröbner-bázis.

Minimális generátor: A redukált Gröbner-bázis elemeinek főtagjai az $\mathrm{Lm}(I)$ minimális generátorai.

Megjegyzés: A tapasztalatok azt mutatják, hogy általában a *grevlex* rendezés lesz a legjobb számunkra.

[17] Szerencsére nincs szükség mindig ilyen hosszas számolásokra, ugyanis a Maple program segítségével könnyen lehet redukált Gröbner-bázist találni:

$with(Groebner)$;
$F := [x^3 - 2 * x * y, x^2 * y - 2 * y^2 + x]$;
$Basis(F, tord, grlex(x, y))$;

$$[x^2, xy, 2y^2 - x]$$

4. fejezet

Alkalmazás

4.1. Ideál tagjainak problémája

A Gröbner-bázis segítségével válszolni tudunk olyan alapvető kérdésre, hogy egy adott polinomot tartalmaz-e egy adott ideál.

Legyen $I =< f_1, \ldots, f_n >$, és $f \in \mathbb{C}[\mathbf{x}]$. Ekkor ki tudjuk számolni az I ideál egy $G = \{g_1, \ldots, g_s\}$ Gröbner-bázisát.
A Gröbner-bázis (III.) féle definíciójából pedig jól látszik, hogy

$$f \in I \quad \Longleftrightarrow \quad f \; rem \; G = 0.$$

Példa I.: $I =< f_1, f_2 >,\ f_1 = xz - y^2,\ f_2 = x^3 - z^2$ és legyen *grlex* rendezés.

Legyen $f = -4x^2y^2z^2 + y^6 + 3z^5$. Kérdés: $f \in I$?

Ránézésre megállapítható, hogy $< f_1, f_2 >$ nem lesz Gröbner-bázis, ugyanis:

$\longrightarrow \quad S(f_1, f_2) = \dfrac{x^3z}{xz}(xz - y^2) - \dfrac{x^3z}{x^3}(x^3 - z^2) = x^2y^2 - z^3.$

$\longrightarrow \quad \mathrm{lm}(S(f_1, f_2)) = x^2y^2$-t nem osztja se $\mathrm{lm}(f_1) = xz$, se $\mathrm{lm}(f_1) = x^3$.

Ezért a Maple program segítségével[1] meghatározzuk a redukált Gröbner-bázist:

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Ezután például maradékos osztással le tudjuk teszteni a polinomunkat:
A *grlex* rendezés miatt[2] legyen $G = \{f_5, f_4, f_3, f_2, f_1\}$. Így azt kapjuk, hogy:

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

[1] Lásd a 3.6. alfejezetet.
[2] Mindig az aktuális legnagyobb főtagú polinommal osztunk.

Mivel az osztási maradék 0, ezáltal $f \in I$.

Példa II.: Néhány esetben még gyorsabban el lehet dönteni a kérdést. Az előző példa folytatásaként vizsgáljuk meg az $h = xy - 5z^2 + x$ polinomot.

Ekkor $h \notin I$, ugyanis:
$\mathrm{lm}(h) = xy \notin < G >$. Ezt onnan tudjuk, hogy a h polinomunk főtagját nem osztja a Gröbner-bázist alkotó polinomok egyik főtagja sem.

$\longrightarrow$ $h \; rem \; G \neq 0$.

Állítás: Két ideál pontosan akkor lesz egyenlő, ha a redukált Gröbner-bázisok megegyeznek.

4.2. Polinomiális egyenletrendszerek megoldása

A Gröbner-bázisok legfontosabb alkalmazási területe kétségkívül a többváltozós polinomiális egyenletrendszerek megoldása.
A polinomális egyenletek meghatároznak egy $I \in \mathbb{C}[\mathbf{x}]$ ideált a következőképpen: először az egyenleteket úgy rendezzük át, hogy a jobb oldalon csak 0 szerepeljen, tehát kapunk egy homogén egyenletrendszert, amelyben a bal oldalon álló polinomok már egy ideált generálnak. Ennek az ideálnak ki tudjuk számolni a Gröbner-bázisát. A tagsorrendet ezekben az esetekben mindig *lex*nek[3] választjuk. Ekkor ugyanis az esetek nagy részében jelentősen egyszerűsödő polinomokat kapunk a bázisunkban. Ez a gyakorlatban úgy jelenik meg, hogy a bázis polinomjaiban fokozatosan csökken a változók száma a rendezés szerint. Azaz először x_1, majd x_2, ... eliminálódik. Szerencsés esetben ekkor az utolsó polinomban már csak egy ismeretlen, az x_n fog szerepelni. Ennek a megoldása már jóval egyszerűbb. A kapott eredményt visszahelyettesítve pedig az összes 0-ad fokú megoldást ki tudjuk számolni.[4] Előfordulhat[5], hogy az utolsó polinomban is több ismeretlen marad, ilyenkor különböző alakzatú magasabb fokú megoldást kapunk legvégül.
Fontos szerepe lesz egy korábbi állításunknak is: $V(I)$ egy affin varietás, ahol I egy ideál.[6]

Most nézzük ezt meg két konkrét esetben:

[3] Részletes algebrai bizonyítással belátható a döntésünk helyessége.
[4] Az eljárás nagy hasonlóságot mutat a Gauss-eliminiációval.
[5] Például ha több ismeretlenünk van, mint egyenlet. Ekkor annyival több változó marad, mint amenynyivel több az ismeretlenek száma.
[6] Lásd a 3.2. alfejezetben.

Példa I.:

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

Ezek az egyenletek definiálják az
$I =< x^2+y^2+z^2-1, x^2+z^2-y, x-z >\in \mathbb{C}[x,y,z]$ ideált.
Feladat: $V(I)$ összes pontját megtalálni.

Először is számoljuk ki az ideálunk Gröbner-bázisát! Tagsorrendünk legyen *lex*, és használjuk ismét a Maple programot:

$$G := \{f_1, f_2, f_3\} = \{x-z, -y+2z^2, z^4+\frac{1}{2}z^2-\frac{1}{4}\}.$$

Az f_3 polinomunk már csak egy ismeretlent tartalmaz, ilyenkor speciális esetekben már meg tudjuk határozni a gyököket.[7]
Legyen $z^2=s \longrightarrow f_3 = s^2+\frac{1}{2}s-\frac{1}{4}$. Alkalmazzuk a másodfokú megoldóképletet[8]:
$\longrightarrow \quad s = \dfrac{-\frac{1}{2} \pm \sqrt{\frac{1}{4}+1}}{2} = \dfrac{\pm\sqrt{5}-1}{4}.$ Mivel $z=\sqrt{s}$, ezért:
$\longrightarrow \quad z = \pm\sqrt{\dfrac{\pm\sqrt{5}-1}{4}} = \pm\dfrac{1}{2}\sqrt{\pm\sqrt{5}-1}.$
Kaptunk négy megoldást z-re. Ezeket a megoldásokat behelyettesítve az $f_2=0$ és $f_1=0$, egyenletbe egyértelműen meg tudjuk határozni az x és y értékeket:
$f_2 = -y+2z^2 = 0 \ \rightarrow \ 2z^2 = y.$
$f_1 = x-z = 0 \ \rightarrow \ z = x.$
A kapott négy megoldás:

$$\begin{aligned} x &= \frac{1}{2}\sqrt{\sqrt{5}-1} & y &= \sqrt{5}-1 & z &= \frac{1}{2}\sqrt{\sqrt{5}-1}, \\ x &= -\frac{1}{2}\sqrt{\sqrt{5}-1} & y &= -(\sqrt{5}-1) & z &= -\frac{1}{2}\sqrt{\sqrt{5}-1}, \\ x &= \frac{1}{2}i\sqrt{\sqrt{5}+1} & y &= -\sqrt{5}-1 & z &= -\frac{1}{2}i\sqrt{\sqrt{5}+1}, \\ x &= -\frac{1}{2}i\sqrt{\sqrt{5}+1} & y &= -(-\sqrt{5}-1) & z &= -\frac{1}{2}i\sqrt{\sqrt{5}+1}. \end{aligned}$$

[7] Negyedfokú egyenletekig létezik megoldóképlet, magasabb fokúakra azonban már nem, így ha ezeket nem tudjuk visszavezetni alacsonyabb fokszámú egyenletekre, akkor csak közelítő megoldásokat kapunk.

[8] Az $ax^2+bx+c=0$ alakú másodfokú egyenlet megoldóképlete: $x_{1,2} = \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$

Mivel $V(I) = V(f_1, f_2, f_3)$, ezért megtaláltuk az eredeti egyenletrendszerünk összes megoldását.

Példa II.:

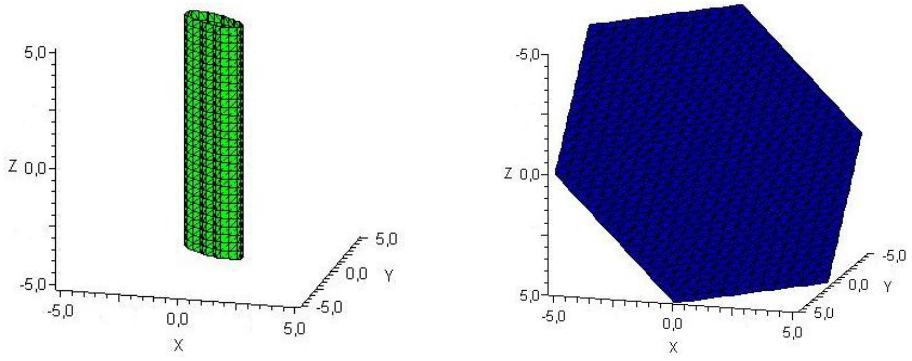
$$\begin{aligned} (y-1)^2 + (z-1)^2 &= 1, \\ x + y &= z. \end{aligned}$$

Ezek az egyenletek meghatározzák az
$I =< (y-1)^2 + (z-1)^2 - 1, x + y - z > \in \mathbb{C}[x, y, z]$ ideált.
Feladat: $V(I)$ összes pontját megtalálni.

Mivel kevesebb egyenletünk van, mint ismeretlenünk, ezért most nem 0. fokú megoldást fogunk kapni, hanem ebben az esetben a megoldások egy "egy dimenziós" alakzatot, egy térbeli görbét alkotnak. Meghatározzuk az ideálunk Gröbner-bázisát Maple programmal, *lex* tagsorrend mellett:

$$G := \{f_1, f_2\} = \{1 - 2y - 2z + y^2 + z^2, y - z + x\}.$$

Az f_1-et kicsit átalakítjuk: $1 - 2y - 2z + y^2 + z^2 = -1 + 2 - 2y - 2z + y^2 + z^2 = (y-1)^2 + (z-1)^2 - 1$.
Láthatjuk, hogy most nem maradt olyan egyenletünk, amiben csupán egy ismeretlen szerepel.
Így az ideálunk varietása geometriailag az $(y-1)^2 + (z-1)^2 - 1$ egyenletű henger[9] és a $z = y + x$ egyenletű síkunk[10] metszete lesz:[11]



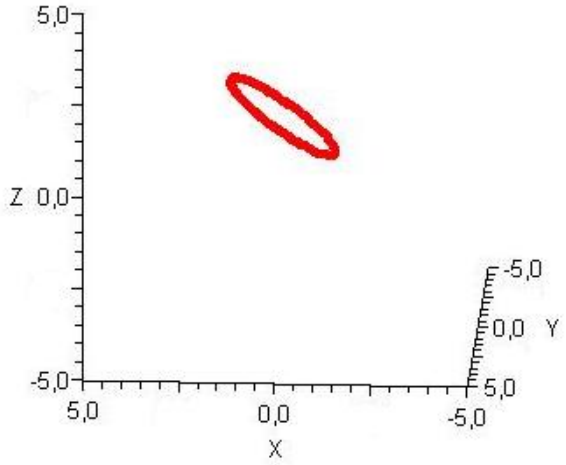
(a) f_1 (b) f_2

4.1. ábra. Gröbner-bázis polinomjai

[9] implicitplot3d($(y-1)^2 + (x+y-1)^2 - 1$, x = -5 .. 5, y = -5 .. 5, view = -5 .. 5, numpoints = 20000)

[10] implicitplot3d(x+y-z, x = -5 .. 5, y = -5 .. 5, z = -5 .. 5, view = -5 .. 5, scaling = constrained, numpoints = 10000)

[11] A Maple-ben az ábrázoláshoz a plots és az intersectplot csomagot használtam.



4.2. ábra. Az ideálunk varietása

Ezek alapján: $V(I)$[12]={Az $(y-1)^2+(z-1)^2=1$ egyenletű henger azon pontjai, amelyekre teljesül, hogy $x=z-y$}, azaz egy ellipszis lesz az alakzat.

[12]intersectplot$((y-1)^2+(z-1)^2=1, z-y=x$, x = -5 .. 5, y = -5 .. 5, z = -5 .. 5, thickness = 3)

Összefoglalás

A dolgozatom elején összefoglaltam azokat a főbb ismereteket, amelyek később nélkülözhetetlenek a téma feldolgozásához. Hosszabban foglalkoztam az ideálokkal, mivel ez adja a Gröbner-bázis alapját, illetve a Gauss-eliminációval, amellyel egyfokú többismeretlenes polinomiális egyenleteket tudunk megoldani.
A harmadik fejezetben bevezettem a Gröbner-bázis fogalmát, a kiszámításához pedig mutattam egy algoritmust, egy konkrét példán pedig megnéztem, hogy működik ez a gyakorlatban.
A negyedik fejezetben kétféle alkalmazást mutattam a Gröbner-bázis használatára. A második alkalmazásban végül a bevezetőben felvetett téma általános módszerét is vázoltam.

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Károlyi Gyulának a diplomamunkám témájának kijelöléséért, valamint a dolgozat elkészítésében nyújtott folyamatos segítségéért, hasznos tanácsaiért és útmutatásaiért.
A dolgozat átnézéséért köszönetet mondok bátyámnak, Szalai Tamásnak és évfolyamtársamnak, Madarász Évának.

Felhasznált irodalom

1. David Cox, John Little and Donald O'Shea: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra (Springer-Verlag, New York, 1992)

2. Felszeghy Bálint: Bevezetés a Gröbner-bázisok elméletébe, internetes jegyzet:
http://www.math.bme.hu/∼fbalint/publ/grobner_jegyzet.pdf

3. Freud Róbert: Lineáris algebra (ELTE Eötvös Kiadó, Budapest, 1996)

4. Freud Róbert és Gyarmati Edit: Számelmélet (Nemzeti Tankönyvkiadó, Budapest, 2000)

5. Iványi Antal: Informatikai algoritmusok I. (ELTE Eötvös Kiadó, Budapest, 2004)

6. Kiss Emil: Bevezetés az algebrába (Typotex, Budapest, 2007)

7. Gergó Lajos: Numerikus módszerek - kidolgozott példák, feladatok (egyetemi jegyzet, ELTE Eötvös Kiadó, Budapest, 2000)

8. Stoyan Gisbert és Takó Galina: Numerikus módszerek I. (Typotex, Budapest, 1993)