Gröbnerove baze

Tepeš, Tatjana

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:118171

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Tatjana Tepeš

GRÖBNEROVE BAZE

Diplomski rad

Voditelj rada:
prof. dr. sc. Ozren Perše

Zagreb, 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu pokazat ćemo da se i algoritam dijeljenja i Euklidov algoritam mogu generalizirati na polinome više varijabli. Iako su ovi rezultati elementarni, otkriveni su tek nedavno, 1965. od strane B. Buchbergera. Algebra se uvijek bavila algoritmima, ali moć i sva ljepota aksiomatske metode dominira od Cayleya i Dedekinda, to jest od druge polovice devetnaestog stoljeća. Nakon izuma tranzistora 1948. brzo računanje je postalo realnost. Stari, kompliciranji algoritmi kao i novi mogli su se implementirati, budući da je računanje višeg reda ušlo u algebru. Najvjerojatnije, razvoj računalne znanosti jest ogroman razlog zbog kojeg su generalizacije klasičnih algoritama, od polinoma jedne varijable do polinoma više varijabli, tek sada otkrivene. Ovo je dramatična ilustracija utjecaja vanjskih ideja na matematiku.

Cilj ovog rada je upoznati se s pojmom Gröbnerovih baza, te proučiti njihova korisna svojstva. Gröbnerove baze su baze ideala u prstenu polinoma koje imaju neka korisna svojstva potrebna u algebarskoj geometriji pri određivanju jednadžbi afine algebarske mnogostrukosti.

Kako bismo uopće mogli definirati Gröbnerove baze, u prvom poglavlju ćemo navesti pojmove i rezultate koji će nam biti potrebni. U odjeljku 1.1. prisjetit ćemo se osnovnih algebarskih struktura koje ćemo koristiti, a to su grupe, komutativni prsteni, polja, te ideali. U odjeljku 1.2. pomno uvodimo polinome, prsten polinoma, te čitatelja prisjećamo na algoritam dijeljenja polinoma u jednoj varijabli. Slijedeći kratki odjeljak posvećen je Noetherinim prstenima, te Hilbertovom teoremu o bazi. U odjeljku 1.4. pobliže opisujemo monome, monomijalne uređaje, leksikografski uređaj, te rezultate vezane uz njih. Također, u ovom odjeljku navodimo algoritam dijeljenja u $k[x]$.

Drugo poglavlje, odjeljak 2.1. konačno sadrži definiciju Gröbnerove baze, te nekoliko rezultata vezanih za njih. Glavni rezultat odjeljka 2.2. je Buchbergerov teorem koji daje kriterij za određivanje je li neka baza ideala Gröbnerova baza, te Buchbergerov algoritam za izračunavanje Gröbnerove baze. Ideja algoritma koja se prirodno nameće jest da pokušamo proširiti polaznu bazu ideala do Gröbnerove baze dodavanjem novih elemenata. To činimo tako da bazi B dodajemo ostatke pri dijeljenju S-polinoma $S(g, g')$ sa B, $g, g' \in B$ različiti od 0. Bazu proširujemo sve dok za sve parove g, g' iz baze ostatak pri dijeljenju $S(g, g')$ sa B ne bude jednak nuli. Tada je dobivena baza Gröbnerova.

Poglavlje 1

Komutativni prsteni

1.1 Grupe

U ovom odjeljku uvest ćemo pojmove grupe, prstena, polja, te ideala u prstenu.

Definicija 1.1.1. *Uređeni par* $(G, \cdot)$*, koji se sastoji od nepraznog skupa* G *i binarne operacije*

$$\cdot : G \times G \to G$$

nazivamo ***grupa****, ako su ispunjeni slijedeći uvjeti:*

(i) binarna operacija je asocijativna, to jest vrijedi

$$(ab)c = a(bc), \text{ za svaki } a, b, c \in G;$$

(ii) za binarnu operaciju postoji i jednoznačno je određen neutralni element, to jest $e \in G$ *takav da vrijedi*

$$ea = ae = a, \text{ za svaki } a \in G;$$

(iii) svaki element je invertibilan, to jest za svaki $a \in G$ *postoji i jednoznačno je određen* $a^{-1} \in G$ *sa svojstvom*

$$aa^{-1} = a^{-1}a = e.$$

Ako još vrijedi

(iv) binarna operacija je komutativna, to jest vrijedi

$$ab = ba, \text{ za svaki } a, b \in G,$$

onda kažemo da je $(G, \cdot)$ ***komutativna*** *ili* ***Abelova*** *grupa.*

Napomenimo još da se grupoid s asocijativnom binarnom operacijom zove *polugrupa*. Pogledajmo sad neke primjere grupa.

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$ su komutativne grupe.
2. Neka je $k \in \mathbb{Z}$ dani broj, te $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$. $(k\mathbb{Z}, +)$ je komutativna grupa.
3. Skup svih uređenih n-torki realnih brojeva $\mathbb{R}^n$, uz uobičajeno koordinatno zbrajanje, je komutativna grupa.
   Isto vrijedi i za $\mathbb{Z}^n$, $\mathbb{Q}^n$ i $\mathbb{C}^n$.
4. Familija permutacija skupa X, u oznaci S_X je grupa obzirom na kompoziciju, te se naziva *simetrična grupa* na X. Kada je $X = \{1, 2, ..., n\}$, tada S_X označavamo sa S_n i nazivamo simetrična grupa na n slova.

Definicija 1.1.2. *Polugrupa koja ima (jedinstven) neutralni element naziva se* ***monoid****.*

Primjer 1.1.3. $\mathbb{N}^n$*, skup svih n-torki* $\alpha = (\alpha_1, ..., \alpha_n)$ *prirodnih brojeva, je monoid uz operaciju zbrajanja:*

$$\alpha + \beta = (\alpha_1, ..., \alpha_n) + (\beta_1, ..., \beta_n) = (\alpha_1 + \beta_1, ..., \alpha_n + \beta_n)$$

Sljedeća algebarska struktura koju ćemo definirati je prsten.

Definicija 1.1.4. ***Komutativni prsten*** *R je skup sa dvije binarne operacije, zbrajanje i množenje, takve da*

(i) R je u odnosu na zbrajanje komutativna (Abelova) grupa;

*(ii) (****komutativnost****) $ab = ba$, za svaki $a, b \in R$;*

*(iii) (****asocijativnost****) $a(bc) = (ab)c$, za svaki $a, b, c \in R$;*

(iv) postoji element $1 \in R$ takav da $1a = a$, za svaki $a \in R$;

*(v) (****distributivnost****) $a(b + c) = ab + bc$, za svaki $a, b, c \in R$.*

Grupa $(R, +)$ zove se aditivna grupa prstena, a monoid $(R, \cdot)$ multiplikativni monoid prstena. Neutralni element aditivne grupe naziva se nula prstena i označava se s 0.

Nabrojimo nekoliko primjera prstena.
Na primjer, skupovi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ su uz standardno zbrajanje i množenje prstenovi.

Sada ćemo uvesti pojam ideala u prstenu. Definirajmo prvo pojam potprstena.

Definicija 1.1.5. *Podskup S komutativnog prstena R je **potprsten** od R ako vrijedi:*

(i) $1 \in S$ *;*

(ii) ako su $a, b \in S$*, tada je i* $a - b \in S$*;*

(iii) ako su $a, b \in S$*, onda je i* $ab \in S$*.*

Iduća algebarska struktura koju ćemo koristiti u daljnjim razmatranjima je polje. Da bismo definirali pojam polja, moramo navesti i sljedeće definicije.

Definicija 1.1.6. ***Integralna domena*** *je komutativni prsten R koji zadovoljava dodatna dva aksioma: prvi,*

$$1 \neq 0 \text{ ;}$$

*drugi, **zakon poništavanja** za množenje: za sve* $a, b, c \in R$*,*

$$\text{ako je } ca = cb \text{ i } c \neq 0\text{, tada je } a = b.$$

Već navedeni primjeri komutativnih prstenova $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su integralne domene.

Definicija 1.1.7. *Neka su a i b elementi komutativnog prstena R. Tada kažemo da a **dijeli** b u R (ili a je **djelitelj** od b, odnosno b je **višekratnik** od a), u oznaci $a|b$, ako postoji element $c \in R$ takav da je $b = ca$.*

Definicija 1.1.8. *Element u u komutativnom prstenu R nazivamo **jedinica** ako $u|1$, to jest ako postoji $v \in R$ takav da je $uv = 1$. Element v tada nazivamo **inverz** od u i v se često označava sa u^{-1}.*

Sada možemo definirati pojam polja.

Definicija 1.1.9. ***Polje*** *F je komutativni prsten u kojem je $1 \neq 0$ i u kojem svaki nenul element a je jedinica, to jest postoji $a \in F$ takav da je $a^{-1}a = 1$.*

Klasični primjeri polja su $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Skup $\mathbb{Z}$ jest integralna domena, no nije polje.

Definicija 1.1.10. ***Ideal*** *u komutativnom prstenu R je podskup I od R takav da je:*

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

(ii) ako su $a, b \in I$*, tada je i* $a + b \in I$

(iii) ako je $a \in I$ *i* $r \in R$*, tada je* $ra \in I$*.*

Prsten R i podskup 0 su uvijek ideali u komutativnom prstenu R. Ideal $I \neq R$ nazivamo **pravi ideal**.

Primjer 1.1.11. *Ako se* $b_1, b_2, ..., b_n$ *nalaze u R, tada je skup svih linearnih kombinacija*

$$I = \{r_1 b_1 + r_2 b_2 + ... + r_n b_n : r_i \in R \text{ za sve } i\}$$

ideal u R. U tom slučaju pišemo $I = (b_1, b_2, ..., b_n)$ *i I zovemo* ***ideal generiran s*** $b_1, b_2, ..., b_n$*.*

Posebno, ako je $n = 1$*, tada je*

$$I = (b) = \{rb : r \in R\}$$

ideal u R; (b) *sadrži sve višekratnike od b i nazivamo ga* ***glavni ideal*** *generiran s b. Primijetimo da su R i* $\{0\}$ *uvijek glavni ideali:* $R = (1)$ *i* $\{0\} = (0)$*.*

1.2 Polinomi

Iako pretpostavljamo da je čitatelj upoznat s pojmom polinoma, u ovom odjeljku ga uvodimo aksiomatski.

Definicija 1.2.1. *Ako je R komutativni prsten, tada* ***niz*** σ *u R je*

$$\sigma = (s_0, s_1, ..., s_i, ...) \text{ ;}$$

gdje su $s_i \in R$ *za svaki* $i \geq 0$ *i nazivamo ih* ***koeficijenti*** *od* σ*.*

Da bi odredili kada su dva niza jednaka trebamo prepoznati da je niz σ doista funkcija $\sigma : \mathbb{N} \longrightarrow \mathbb{R}$, gdje je $\mathbb{N}$ skup prirodnih brojeva, takva da je $\sigma(i) = s_i$ za svaki $i \geq 0$. Prema tome, ako je $\tau = (t_0, t_1, ..., t_i, ...)$ niz, tada je $\sigma = \tau$ ako i samo ako je $\sigma(i) = \tau(i)$ za svaki $i \geq 0$, to jest $\sigma = \tau$ ako i samo ako je $s_i = t_i$ za svaki $i \geq 0$.

Definicija 1.2.2. *Niz* $\sigma = (s_0, s_1, ..., s_i, ...)$ *u komutativnom prstenu R naziva se* ***polinom*** *ako postoji neki cijeli broj* $m \geq 0$ *takav da* $s_i = 0$ *za sve* $i > m$*, to jest*

$$\sigma = (s_0, s_1, ..., s_m, 0, 0, ...).$$

Polinom ima samo konačno mnogo nenul koeficijenata. **Nul polinom**, u oznaci $\sigma = 0$, je niz $\sigma = (0, 0, ...)$.

Definicija 1.2.3. *Ako je* $\sigma = (s_0, s_1, ..., s_m, 0, 0, ...) \neq 0$ *polinom, tada postoji* $s_n \neq 0$ *takav da je* $s_i = 0$ *za svaki* $i > n$. s_n *nazivamo* ***vodeći koeficijent*** *od* σ, *a* n *je* ***stupanj*** *od* σ, *u oznaci* $Deg(\sigma)$.

Nul polinom 0 nema stupnja jer nema nenul koeficijenata.

Ako je R komutativni prsten, tada skup polinoma s koeficijentima iz R označavamo sa $R[x]$.

Propozicija 1.2.4. *Ako je* R *komutativni prsten, tada je* $R[x]$ *komutativni prsten koji sadrži* R *kao potprsten.*

Dokaz. Definiramo zbrajanje i množenje polinoma: ako su $\sigma = (s_0, s_1, ...)$ i $\tau = (t_0, t_1, ...)$ polinomi, tada je

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, ..., s_n + t_n, ...)$$

i

$$\sigma\tau = (c_0, c_1, c_2, ...),$$

gdje je $c_k = \sum_{i+j=k} s_i t_j = \sum_{i=0}^{k} s_i t_{k-i}$. Provjera aksioma iz definicije komutativnog prstena je rutina i ostavljamo je čitatelju. Podskup $\{(r, 0, 0, ...) : r \in R\}$ je potprsten od $R[x]$ kojeg identificiramo s R. □

Lema 1.2.5. *Neka je* R *komutativni prsten i neka su* $\sigma, \tau \in R[x]$ *nenul polinomi.*

(i) Ili je $\sigma\tau = 0$ *ili* $Deg(\sigma\tau) \leq Deg(\sigma) + Deg(\tau)$.

(ii) Ako je R *integralna domena, tada je* $\sigma\tau \neq 0$ *i*

$$Deg(\sigma\tau) = Deg(\sigma) + Deg(\tau).$$

(iii) Ako je R *integralna domena, tada je i* $R[x]$ *integralna domena.*

Definicija 1.2.6. *Ako je* R *komutativni prsten, tada* $R[x]$ *nazivamo* ***prsten polinoma*** *na* R.

Definicija 1.2.7. *Element* $x \in R[x]$ *definiramo sa*

$$x = (0, 1, 0, 0, ...).$$

Lema 1.2.8. *(i) Ako je* $\sigma = (s_0, s_1, ...)$, *tada*

$$x\sigma = (0, s_0, s_1, ...).$$

(ii) Ako je $n \geq 1$*, tada polinom* x^n *ima na svim mjestima* 0*, osim na n-toj koordinati.*

(iii) Ako je $r \in R$*, tada je*

$$(r, 0, 0, ...)(s_0, s_1, ..., s_j, ...) = (rs_0, rs_1, ..., rs_j, ...).$$

Ako identificiramo $(r, 0, 0, ...)$ s r, tada tvrdnju (iii) iz Leme 1.2.8. možemo zapisati kao

$$r(s_0, s_1, ..., s_i, ...) = (rs_0, rs_1, ..., rs_i, ...).$$

Sada dobivamo uobičajen zapis polinoma.

Propozicija 1.2.9. *Ako je* $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$*, tada je*

$$\sigma = s_0 + s_1x + s_2x^2 + ... + s_nx^n,$$

gdje se svaki element $s \in R$ *identificira polinomom* $(s, 0, 0, ...)$.

Dokaz.

$$\begin{aligned}\sigma &= (s_0, s_1, ..., s_n, 0, 0, ...) \\ &= (s_0, 0, 0, ...) + (0, s_1, 0, ...) + ... + (0, 0, ..., s_n, 0, ...) \\ &= s_0(1, 0, 0, ...) + s_1(0, 1, 0, ...) + ... + s_n(0, 0, ..., 1, 0, ...) \\ &= s_0 + s_1x + s_2x^2 + ... + s_nx^n.\end{aligned}$$

□

Koristit ćemo ovu standardnu notaciju, dakle pisat ćemo

$$f(x) = s_0 + s_1x + s_2x^2 + ... + s_nx^n$$

umjesto $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$.

Navedimo standardni vokabular vezan za polinome. Ako je $f(x) = s_0 + s_1x + s_2x^2 + ... + s_nx^n$, gdje je $s_n \neq 0$, tada s_0 nazivamo **konstantni član**, i kao što smo već naveli s_n nazivamo **vodeći koeficijent**. Ako je vodeći koeficijent $s_n = 1$, tada kažemo da je $f(x)$ **normiran**. Svaki polinom osim nulpolinoma ima stupanj. **Konstantan polinom** je ili nul polinom ili polinom stupnja 0. Polinomi stupnja 1, $a + bx$, $b \neq 0$ nazivaju se **linearni**, polinomi stupnja 2 nazivaju se **kvadratni**, stupnja 3 **kubični** i tako dalje.

Korolar 1.2.10. *Polinomi* $f(x) = s_0 + s_1x + s_2x^2 + ... + s_nx^n$ *i* $g(x) = t_0 + t_1x + t_2x^2 + ... + t_mx^m$ *stupnja n i m, respektivno, su jednaki ako i samo ako je* $n = m$ *i* $s_i = t_i$ *za svaki i.*

Spomenimo još da se $R[x]$ često naziva prsten svih polinoma nad R u jednoj varijabli. Označimo li sa $A = R[x]$ tada polinomijalni prsten $A[y]$ nazivamo prsten svih polinoma nad k u dvije varijable, x i y, u oznaci $R[x, y]$.

Na primjer, kvadratni polinom $ax^2 + bxy + cy^2 + dx + ey + f$ možemo zapisati kao $cy^2 + (bx+e)y+(ax^2+dx+f)$ polinom u varijabli y s koeficijentima u $R[x]$. Induktivno, možemo formirati komutativni prsten $R[x_1, x_2..., x_n]$ svih polinoma u n varijabli s koeficijentima u R. Lema 1.2.5.(*iii*) sada se može generalizirati, indukcijom po n. Dakle, ako je R integralna domena, tada je i $R[x_1, x_2, ..., x_n]$ također integralna domena.

Spomenimo još i algoritam dijeljenja u $R[x]$.

Teorem 1.2.11 (**Algoritam dijeljenja**). *Pretpostavimo da je k polje, te da su $f(x), g(x) \in k[x]$ i $f(x) \neq 0$. Tada postoje jedinstveni polinomi $q(x), r(x) \in k[x]$ takvi da je*

$$g(x) = q(x)f(x) + r(x)$$

te vrijedi da ili je $r(x) = 0$ ili $Deg(r) < Deg(f)$.

Dokaz. Prvo dokazujemo egzistenciju takvih q i r. Ako $f|g$, tada $g = qf$ za neki q; definiramo ostatak $r = 0$ i gotovi smo. Ako $f \nmid g$, tada uzimamo u obzir (nužno nenul) polinome oblika $g - qf$ dok q varira nad $k[x]$. Aksiom najmanjeg cijelog broja osigurava da postoji polinom $r = g - qf$ koji ima najmanji stupanj među svim takvim polinomima. Budući da je $g = qf + r$, dovoljno je pokazati da je $\mathrm{Deg}(r) < \mathrm{Deg}(f)$. Pišemo $f(x) = s_n x^n + ... + s_1 x + s_0$ i $r(x) = t_m x^m + ... + t_1 x + t_0$. Sada $s_n \neq 0$ implicira da je s_n jedinica, jer je k polje, pa s_n^{-1} postoji u k. Ako je $\mathrm{Deg}(r) \geq \mathrm{Deg}(f)$, definiramo

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x);$$

to jest, ako je $\mathrm{LT}(f) = s_n x^n$, gdje LT označava **vodeći član**, tada je

$$h = r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f;$$

primijetimo da $h = 0$ ili $\mathrm{Deg}(h) < \mathrm{Deg}(r)$. Ako je $h = 0$, tada $r = [\mathrm{LT}(r)/\mathrm{LT}(f)]f$ i

$$\begin{aligned} g &= qf + r \\ &= qf + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f \\ &= [q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}]f, \end{aligned}$$

što je u kontradikciji sa $f \nmid g$. Ako je $h \neq 0$, tada je $\mathrm{Deg}(h) < \mathrm{Deg}(r)$ i

$$g - qf = r = h + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f.$$

Prema tome, $g - [q + \mathrm{LT}(r)/\mathrm{LT}(f)]f = h$, što je u kontradikciji sa tim da je r polinom tog oblika najmanjeg stupnja. Stoga, $\mathrm{Deg}(r)<\mathrm{Deg}(f)$.

Da bi dokazali jedinstvenost od $q(x)$ i $r(x)$, pretpostavimo da je $g = q'f + r'$, gdje je $\mathrm{Deg}(r')<\mathrm{Deg}(f')$. Tada je

$$(q - q')f = r' - r.$$

Ako je $r' \neq r$, tada obje strane imaju stupanj. Ali $\mathrm{Deg}((q-q')f)=\mathrm{Deg}(q-q')+\mathrm{Deg}(f) \geq \mathrm{Deg}(f)$, dok je $\mathrm{Deg}(r - r') \leq \max\{\mathrm{Deg}(r'), \mathrm{Deg}(r)\} < \mathrm{Deg}(f)$, što je kontradikcija. Dakle, $r' = r$ i $(q - q')f = 0$. Budući da je $k[x]$ integralna domena i $f \neq 0$, slijedi da je $q - q' = 0$ i $q = q'$. □

Definicija 1.2.12. *Ako su $f(x)$ i $g(x)$ polinomi u $k[x]$, gdje je k polje, tada se polinomi $q(x)$ i $r(x)$, koji se pojavljuju u algoritmu dijeljenja nazivaju **kvocijent** i **ostatak** nakon dijeljenja $g(x)$ s $f(x)$.*

Definicija 1.2.13. *Ako su $f(x)$ i $g(x)$ polinomi u $k[x]$, gdje je k polje, tada definiramo **zajednički djeljitelj** kao polinom $c(x) \in k[x]$ takav da $c(x)|f(x)$ i $c(x)|g(x)$. Ako je barem jedan od $f(x), g(x) \in k[x]$ različit od 0, definiramo njihov **najveći zajednički djelitelj**, u oznaci **nzd**, kao normiran zajednički djelitelj koji ima najveći stupanj. Ako je $f(x) = 0 = g(x)$, definiramo njihov nzd=0.*

1.3 Noetherini prsteni

Za ideal I u komutativnom prstenu R kažemo da je **konačno generiran** ako postoje $b_1, ..., b_s \in R$ takvi da je

$$I = (b_1, ..., b_s).$$

U tom slučaju $b_1, ..., b_s$ zovemo **baza ideala** I.

U ovom odjeljku navodimo zanimljivo svojstvo prstena $k[x_1, ..., x_n]$, pri čemu je k polje, da je svaki ideal u tom prstenu konačno generiran. Primijetimo da za dani ideal postoji više različitih baza. Cilj ovog rada je upoznati se s bazama koje imaju posebna svojstva, a to su upravo Gröbnerove baze.

Definicija 1.3.1. *Komutativni prsten R zadovoljava **uvjet rastućeg lanca** ako se svaki rastući lanac ideala*

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$$

zaustavlja, to jest niz postaje konstantan od nekog mjesta nadalje; postoji prirodan broj N takav da vrijedi $I_N = I_{N+1} = I_{N+2} = ...$.

Lako se pokaže sljedeća propozicija:

Propozicija 1.3.2. *Sljedeće tvrdnje su ekvivalentne za komutativni prsten R:*

(i) R zadovoljava uvjet rastućeg lanca.

(ii) R zadovoljava uvjet maksimuma: Svaka neprazna familija F ideala u R ima maksimalan element.

(iii) Svaki ideal u R je konačno generiran.

Sada možemo imenovati komutativan prsten koji zadovoljava bilo koju od tri tvrdnje iz prethodne propozicije.

Definicija 1.3.3. *Komutativni prsten R nazivamo* ***Noetherin*** *ako je svaki ideal u R konačno generiran.*

Sljedeći teorem navodimo bez dokaza.

Teorem 1.3.4 (Hilbertov teorem o bazi). *Ako je R komutativni Noetherin prsten, tada je* $R[x]$ *također Noetherin.*

Sljedeća tvrdnja slijedi indukcijom iz Teorema 1.3.4.:

Korolar 1.3.5. *Ako je k polje,* $k[x_1, ..., x_n]$ *je Noetherin.*

1.4 Generalizirani algoritam dijeljenja

U ovom odjeljku proučavamo prsten polinoma, $k[x_1, ..., x_n]$, pri čemu je k polje.

Prisjetimo se da je najvažnije svojstvo algoritma dijeljenja u $k[x]$ da je ostatak $r(x)$ malog stupnja. Bez nejednakosti $\mathrm{Deg}(r) < \mathrm{Deg}(g)$, rezultat bi bio praktično neupotrebljiv. Želimo poopćiti algoritam dijeljenja na $k[x_1, ..., x_n]$.

Prvo ćemo definirati pojam monoma.

Definicija 1.4.1. ***Monom*** *u varijablama* $x_1, ..., x_n$ *je produkt oblika*

$$cx_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

gdje je $c \in k$*, te su svi eksponenti* $\alpha_1, ..., \alpha_n$ *nenegativni cijeli brojevi.*

Sada je polinom f u više varijabli suma monoma

$$f = \sum c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Definicija 1.4.2. ***Multistupanj monoma***

$$cx_1^{\alpha_1} \cdots x_n^{\alpha_n} \in k[x_1, ..., x_n],$$

gdje $0 \neq c \in k$ *i* $\alpha_i \geqslant 0$ *za sve i, jest n-torka* $\alpha = (\alpha_1, ..., \alpha_n)$ *čija* ***težina*** *je suma* $\mid \alpha \mid = \alpha_1 + ... + \alpha_n$.

Kada dijelimo $f(x)$ s $g(x)$ u $k[x]$, obično se monomi u $f(x)$ rasporede silazno po stupnjevima:

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_2 x^2 + c_1 x + c_0.$$

Polinom u više varijabli,

$$f(X) = f(x_1, ..., x_n) = \sum c_{(\alpha_1,...,\alpha_n)} x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

možemo zapisati kompaktno kao

$$f(X) = \textstyle\sum_\alpha c_\alpha X^\alpha$$

ako skratimo $(\alpha_1, ..., \alpha_n)$ u α i $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ u X^α.

Monomi uključeni u $f(X)$ bit će poredani po njihovim multistupnjevima.

U Primjeru 1.1.3. vidjeli smo da je $\mathbb{N}^n$, skup svih n-torki $\alpha = (\alpha_1, ..., \alpha_n)$ prirodnih brojeva, monoid uz operaciju zbrajanja:

$$\alpha + \beta = (\alpha_1, ..., \alpha_n) + (\beta_1, ..., \beta_n) = (\alpha_1 + \beta_1, ..., \alpha_n + \beta_n).$$

Ova operacija monoida povezana je s množenjem monoma:

$$X^\alpha X^\beta = X^{\alpha+\beta}.$$

Prisjetimo se da je parcijalno uređen skup skup X sa relacijom $\preceq$ koja je refleksivna, antisimetrična i tranzitivna. Naravno, možemo pisati $x \prec y$ ako je $x \preceq y$ i $x \neq y$, a možemo umjesto toga pisati i $y \succeq x$ (odnosno $y \succ x$).

Parcijalno uređen skup X je *dobro uređen* ako svaki neprazan podskup $S \subseteq X$ sadrži najmanji element; tj. postoji $s_0 \in S$ takav da $s_0 \preceq s$ za svaki $s \in S$. Na primjer, skup prirodnih brojeva $\mathbb{N}$ sa uobičajenom nejednakosti $\leq$ je dobro uređen.

Može se dokazati da svaki strogo padajući niz u dobro uređenom skupu mora biti konačan. Ovo svojstvo dobro uređenih skupova može se upotrijebiti da bi se pokazalo

da neki algoritam nakon nekog vremena staje. Na primjer, u dokazu algoritma dijeljenja polinoma jedne varijable za svaki korak smo vezali prirodne brojeve: to je bio stupanj ostatka. Nadalje, ako algoritam ne stane u danom koraku, tada je prirodni broj vezan za slijedeći korak- stupanj njegovog ostatka- strogo manji. Budući da su prirodni brojevi dobro uređeni po uobičajenoj nejednakosti $\leq$, taj strogo padajući niz prirodnih brojeva mora biti konačan, to jest algoritam mora stati nakon konačnog broja koraka.

Zanimaju nas uređaji multistupnjeva koji su kompatibilni s množenjem monoma- to jest sa zbrajanjem u monoidu $\mathbb{N}^n$.

Definicija 1.4.3. ***Monomijalni uređaj*** *je dobar uređaj na* $\mathbb{N}^n$ *takav da*

$$\alpha \preceq \beta \Longrightarrow \alpha + \gamma \preceq \beta + \gamma$$

za sve $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Monomijalni uređaj koristit ćemo na slijedeći način. Ako je $X = (x_1, ..., x_n)$, tada definiramo $X^\alpha \preceq X^\beta$ u slučaju da je $\alpha \preceq \beta$; to jest monomi su poredani prema njihovim multistupnjevima.

Lema 1.4.4. *Neka je* $\preceq$ *monomijalni uređaj na* $\mathbb{N}^n$*, te neka su* $f(X), g(X) \in k[X] = k[x_1, ..., x_n]$ *različiti od* 0*.*

(i) Ako je $f + g \neq 0$*, tada* $Deg(f + g) \preceq max\ \{\ Deg\ (f),\ Deg(g)\ \}$ *; stroga nejednakost vrijedi samo ako je* $Deg\ (f) = Deg(g)$*.*

(ii) $Deg(fg) = Deg\ (f) + Deg\ (g)$ *i* $Deg\ (f^m) = m\ Deg\ (f)$ *za sve* $m \geq 1$*.*

Definicija 1.4.5. *Ako je* $\mathbb{N}^n$ *snabdjevan monomijalnim uređajem, tada svaki*

$$f(X) \in k[X] = k[x_1, ...x_n]$$

možemo zapisati kao sumu najvećeg člana i nižih članova u padajućem poretku:

$$f(X) = c_\alpha X^\alpha + \text{niži članovi.}$$

Definira se njegov ***vodeći član*** $LT(f) = c_\alpha X^\alpha$ *, te njegov* ***stupanj*** $Deg(f) = \alpha$*.*
$f(X)$ *zovemo* ***normiran*** *ako je* $LT(f) = X^\alpha$*; to jest ako je* $c_\alpha = 1$*.*

$\mathrm{Deg}(f)$ i $\mathrm{LT}(f)$ ovise o monomijalnom uređaju. Dva najpoznatija primjera monomijalnih uređaja su: leksikografski uređaj i stupanj-leksikografski uređaj.

Definicija 1.4.6. ***Leksikografski uređaj*** *na* $\mathbb{N}^n$ *definiran je sa*

$$\alpha \preceq_{lex} \beta$$

ako je ili $\alpha = \beta$ *ili ako je prva koordinata različita od nule u* $\beta - \alpha$ *pozitivna.*[1].

Napomena 1.4.7. *Izraz leksikografski odnosi se na standardni poredak riječi u rječniku. Na primjer, slijedeće njemačke riječi "rastu" u leksikografskom smislu (slova su poredana ovako:* $a < b < ... < z$*):*

ausgehen
ausladen
auslagen
auslegen
bedeuten

Ako je $\alpha \prec_{lex} \beta$ *tada se oni podudaraju na prvih* $i - 1$ *koordinata (za neki* $i \geq 1$ *) , to jest,* $\alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1}$*, i postoji stroga nejednakost:* $\alpha_i < \beta_i$.

Propozicija 1.4.8. *Leksikografski uređaj* $\preceq_{lex}$ *je monomijalni uređaj na* $\mathbb{N}^n$.

Dokaz. Prvo pokažimo da je leksikografski uređaj parcijalni uređaj.

Relacija $\preceq_{lex}$ je refleksivna; zbog same njene definicije vrijedi $\alpha \preceq_{lex} \alpha$. Za antismetričnost pretpostavimo da je $\alpha \preceq_{lex} \beta$ i $\beta \preceq_{lex} \alpha$. Ako je $\alpha \neq \beta$, tada je prva koordinata npr. i na kojoj se ne podudaraju. Za notaciju, pretpostavimo da je $\alpha_i < \beta_i$. No, to je u kontradikciji s $\beta \preceq_{lex} \alpha$.

Da bi dokazali tranzitivnost, pretpostavimo $\alpha \prec_{lex} \beta$ i $\beta \prec_{lex} \gamma$ (dovoljno je promatrati strogu nejednakost). Sada je $\alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1}$ i $\alpha_i < \beta_i$. Neka je γ_p prva koordinata za koju je $\beta_p < \gamma_p$. Ako je $p < i$, tada je

$$\gamma_1 = \beta_1 = \alpha_1, \ ..., \gamma_{p-1} = \beta_{p-1} = \alpha_{p-1}, \ \alpha_p = \beta_p < \gamma_p \ ;$$

ako je $p \geqslant i$, tada je

$$\gamma_1 = \beta_1 = \alpha_1, \ ..., \gamma_{i-1} = \beta_{i-1} = \alpha_{i-1}, \ \alpha_i < \beta_i = \gamma_i.$$

U oba slučaja, prva koordinata od $\gamma - \alpha$ različita od nule je pozitivna; tj. $\alpha \prec_{lex} \gamma$.

Nadalje, pokažimo da je leksikografski uređaj dobar uređaj. Ako je S neprazan podskup od $\mathbb{N}^n$, definiramo

[1] Razlika $\beta - \alpha$ možda ne leži u $\mathbb{N}^n$, ali leži u $\mathbb{Z}^n$.

$$C_1 = \{ \text{ sve prve koordinate } n\text{-torki u } S \},$$

i definiramo δ_1 da bude najmanji broj u C_1 (C_1 je neprazni podskup dobro uređenog skupa $\mathbb{N}$).

Definiramo

$$C_2 = \{ \text{ sve druge koordinate } n\text{-torki } (\delta_1,\ \alpha_2,\ ...,\ \alpha_n) \in S \}.$$

Kako je $C_2 \neq \emptyset$, on sadrži najmanji broj δ_2.

Slično, za svaki $i < n$, definiramo C_{i+1} kao sve $(i+1)$-ve koordinate od onih n-torki iz S, čijih prvih i koordinata su $(\delta_1, ..., \delta_i)$, te definiramo δ_{i+1} da bude najmanji broj u C_{i+1}. Po konstrukciji, n-torka $\delta = (\delta_1,\ ...,\ \delta_n)$ leži u S. Nadalje, ako $\alpha = (\alpha_1,\ ...,\ \alpha_n) \in S$, tada

$$\alpha - \delta = (\alpha_1 - \delta_1,\ \alpha_2 - \delta_2,\ ...,\ \alpha_n - \delta_n)$$

ima prvu ne nul koordinatu, ako postoji, pozitivnu, te je $\delta \prec_{lex} \alpha$. Dakle, leksikografski uređaj je dobar uređaj.

Sada pretpostavimo da je $\alpha \preceq_{lex} \beta$; te tvrdimo da je

$$\alpha + \gamma \preceq_{lex} \beta + \gamma$$

za sve $\gamma \in \mathbb{N}$. Ako je $\alpha = \beta$, tada $\alpha + \gamma = \beta + \gamma$. Ako je $\alpha \prec_{lex} \beta$, tada je prva ne nul koordinata od $\beta - \alpha$ pozitivna. No,

$$(\beta + \gamma) - (\alpha + \gamma) = \beta - \alpha$$

i tako je $\alpha + \gamma \prec_{lex} \beta + \gamma$.

Dakle, $\preceq_{lex}$ je monomijalni uređaj.

□

U leksikografskom uređaju $x_1 \succ x_2 \succ x_3 \succ ...$, zato što je

$$(1,\ 0,\ ...,\ 0) \succ (0,\ 1,\ 0,\ ...,\ 0) \succ ... \succ (0,\ 0,\ ...,\ 1).$$

Svaka permutacija varijabli $x_{\sigma(1)},\ ...,\ x_{\sigma(n)}$ daje različiti leksikografski uređaj na $\mathbb{N}^n$.

Napomena 1.4.9. *Ako je X neki dobro uređen skup s uređajem $\preceq$, tada leksikografski uređaj na X^n možemo definirati sa $a = (a_1,\ ...,\ a_n) \preceq_{lex} b = (b_1,\ ...,\ b_n)$ u slučaju $a = b$ ili ako se ne poklapaju prvo na i-toj koordinati i $a_i \prec b_i$. Tada je jednostavno generalizirati prethodnu Propoziciju 1.4.8. tako da se $\mathbb{N}$ zamijeni s X.*

Nadalje, za svaki skup X konstruiramo monoid W(X): njegovi elementi su prazn riječ zajedno sa svim riječima $x_1^{e_1} \cdots x_p^{e_p}$ na skupu X, gdje $p \geqslant 1$ i $e_i = \pm 1$, za svaki i. Za razliku od $\mathbb{N}^n$, gdje su sve riječi duljine n, monoid $W(X)$ ima riječi različitih duljina.

Od većeg značaja ovdje je submonoid $W^+(X)$ od $W(X)$ koji sadrži sve "pozitivne" riječi na X:

$$W^+(X) = \{x_1 \cdots x_p \in W(X) : x_i \in X \; i \; p \geqslant 0\}.$$

Korolar 1.4.10. *Ako je X dobro uređen skup,tada je $W^+(X)$ dobro uređen u leksikografskom uređaju (u oznaci $\preceq_{lex}$).*

Dokaz. Dokaz da je to dobar uređaj ostavljamo čitatelju.

Prvo, definiramo $1 \preceq_{lex} w$ za sve $w \in W^+(X)$.

Nadalje, u danim riječima $u = x_1 \cdots x_p$ i $v = y_1 \cdots y_p$ u W^+, kraću dopunjujemo jedinicama da bi se dobile iste duljine riječi, i preimenujemo ih u $u^{'}$ i $v^{'}$ u W^+.

Ako je $m \geq max\{p, q\}$, možemo smatrati $u^{'}, \; v^{'} \in X^m$, i definiramo $u \preceq_{lex} v$ ako $u^{'} \preceq_{lex} v^{'}$ u X^m. (Ovo je red riječi obično korišten u riječnicima). □

Lema 1.4.11. *Neka je dan monomijalni uređaj na $\mathbb{N}^n$, tada svaki niz koraka oblika $f(X) \longrightarrow f(X) - c_\beta X^\beta + g(X)$, gdje je $c_\beta X^\beta$ nenul član od $f(X)$ i $Deg(g) \prec \beta$ je konačan.*

Dokaz. Svaki polinom

$$f(X) = \Sigma_\alpha c_\alpha X^\alpha \in k[X] = k[x_1, ..., x_n]$$

možemo zapisati tako da su multistupnjevi njegovih članova u silaznom poretku:

$\alpha_1 \succ \alpha_2 \succ ... \succ \alpha_p$.

Definiramo

$$\text{multiriječ } (f) = \alpha_1 \cdots \alpha_p \in W^+(\mathbb{N}^n).$$

Neka je $c_\beta X^\beta$ nenul član u $f(X)$, te $g(X) \in k[X]$ takav da je $\text{Deg}(X) \prec \beta$ i

$$f(X) = h(X) + c_\beta X^\beta + l(X) \, ,$$

gdje je $h(X)$ suma svih članova od $f(X)$ multistupnja $\succ \beta$, a $l(X)$ je suma svih članova od $f(X)$ multistupnja $\prec \beta$.

Tvrdimo da je

$$\begin{aligned} \text{multiriječ}(f(X) - c_\beta X^\beta + g(X)) &\preceq_{lex} \text{multiriječ}(h + l + g) \\ &\prec_{lex} \text{multiriječ}(f) \text{ u } W^+(X). \end{aligned}$$

Suma članova u $f(X) - c_\beta X^\beta + g(X)$ multistupnja $\succ \beta$ je $h(X)$, dok je suma nižih članova $l(X) + g(X)$. No, $\mathrm{Deg}(l + g) \prec \beta$, prema Lemi 1.4.4. Stoga se početni članovi od $f(X)$ i $f(X) - c_\beta X^\beta + g(X)$ podudaraju, dok sljedeći član u $f(X) - c_\beta X^\beta + g(X)$ ima multistupanj $\prec \beta$, i to dokazuje tvrdnju.

Budući da je $W^+(\mathbb{N}^n)$ dobro uređen, slijedi da bilo koji niz koraka oblika $f(X) \longrightarrow f(X) - c_\beta X^\beta + g(X)$ mora biti konačan.

□

Sada navodimo drugi najpopularniji monomijalni uređaj. Prisjetimo se da ako je $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, tada $|\alpha| = \alpha_1 + ... + \alpha_n$ označava njegovu težinu.

Definicija 1.4.12. ***Stupanj-leksikografski uređaj*** *na $\mathbb{N}^n$ definiran je s $\alpha \preceq_{dlex} \beta$ ako je ili $\alpha = \beta$ ili*

$$|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|,$$

ili ako je $|\alpha| = |\beta|$, tada ja prva nenul koordinata u $\beta - \alpha$ pozitivna.

Drugim riječima, za dane $\alpha = (\alpha_1, ..., \alpha_{n)}$ i $\beta = (\beta_1, ..., \beta_n)$ prvo provjerimo težinu; ako je $|\alpha| < |\beta|$, tada $\alpha \preceq_{dlex} \beta$; ako su iste, dakle ako α i β imaju istu težinu, poredamo ih leksikografski.

Na primjer, $(1, 2, 3, 0) \prec_{dlex} (0, 2, 5, 0)$ i $(1, 2, 3, 4) \prec_{dlex} (1, 2, 5, 2)$.

Propozicija 1.4.13. *Stupanj-leksikografski uređaj $\preceq_{dlex}$ je monomijalni uređaj na $\mathbb{N}^n$.*

Dokaz. Lagano se pokazuje da je $\preceq_{dlex}$ parcijalni uređaj na $\mathbb{N}^n$.

Nadalje, da bi pokazali da je $\preceq_{lex}$ dobro uređen, neka je S neprazan podskup od $\mathbb{N}^n$. Težine elemenata u S tvore neprazan podskup od $\mathbb{N}$, pa postoji najmanji takav, oznake t.

Neprazan podskup svih $\alpha \in S$ težine t ima najmanji element, jer se stupanj-leksikografski uređaj $\preceq_{dlex}$ podudara s leksikografskim uređajem $\preceq_{lex}$ na tom podskupu.

Stoga, postoji najmanji element u S u stupanj-leksikografskom uređaju.

Pretpostavimo da je

$$\alpha \preceq_{dlex} \beta \text{ i } \gamma \in \mathbb{N}^n.$$

Sada je $|\alpha + \gamma| = |\alpha| + |\gamma|$, tako da $|\alpha| = |\beta|$ povlači

$$|\alpha + \gamma| = |\beta + \gamma|$$

i $|\alpha| < |\beta|$ povlači

$$|\alpha + \gamma| < |\beta + \gamma|;$$

u potonjem slučaju Propozicija 1.4.8. pokazuje da je $\alpha + \gamma \preceq_{dlex} \beta + \gamma$.

□

Sljedeća propozicija pokazuje, uvažavajući monomijalni uređaj, da se polinomi više varijabli ponašaju kao polinomi jedne varijable.

Propozicija 1.4.14. *Neka je $\preceq$ monomijalni uređaj na $\mathbb{N}^n$ i neka su*

$$f(X),\ g(X),\ h(X) \in k[x_1, ..., x_n],$$

gdje je k polje.

(i) Ako je Deg (f) = Deg (g), tada je LT (g) | LT (f).

(ii) LT (hg) = LT (h) LT (g).

(iii) Ako je Deg (f) = Deg (hg), tada LT (g) | LT (f).

Dokaz.

(i) Ako je Deg $(f) = \alpha =$ Deg (g), tada je LT $(f) = cX^\alpha$ i LT $(g) = dX^\alpha$.

Stoga, LT (g) | LT (f), jer $c \neq 0$ i c je jedinica u k (primijetimo, također je LT (f) | LT (g)).

(ii) Neka je $h(X) = cX^\gamma +$ niži članovi, te $g(X) = bX^\beta +$ niži članovi, pa je LT $(h) = cX^\gamma$ i LT $(g) = bX^\beta$.

Očito, $cbX^{\gamma+\beta}$ je nenul član od $h(X)g(X)$. Da bi pokazali da je to vodeći član, neka je $c_\mu X^\mu$ član od $h(X)$ sa $\mu \preceq \gamma$, te neka je $b_\nu X^\nu$ član od $g(X)$ sa $\nu \preceq \beta$ (s barem jednom strogom nejednakosti).

Sada Deg$(c_\mu X^\mu b_\nu X^\nu) = \mu + \nu$; budući da je $\preceq$ monomijalni uređaj, imamo $\mu + \nu \prec \gamma + \nu \prec \gamma + \beta$.

Prema tome, $cbX^{\gamma+\beta}$ je član od $h(X)g(X)$ s najvećim multistupnjem.

(iii) Kako je Deg (f) = Deg (hg) dio (i) daje LT (hg) | LT (f) i LT (h) LT (g) = LT (hg) po (ii); stoga, LT (g) | LT (f).

□

Definicija 1.4.15. *Neka je $\preceq$ monomijalni uređaj na $\mathbb{N}^n$ i neka su $f(X),\ g(X) \in k[X]$, gdje je $k[X] = k[x_1, ..., x_n]$. Ako postoji nenul član $c_\beta X^\beta$ u $f(X)$ s $LT(g) \mid c_\beta X^\beta$ i*

$$h(X) = f(X) - \frac{c_\beta X^\beta}{LT_{(g)}} g(X)$$

tada definiramo ***redukciju*** $f \xrightarrow{g} h$ *kao zamjenu od f s h.*

Redukcija je uobičajen korak korišten u dugom dijeljenju polinoma jedne varijable. Naravno, poseban slučaj redukcije je za $c_\beta X^\beta = \mathrm{LT}(f)$.

Propozicija 1.4.16. *Neka je $\preceq$ monomijalni uređaj na $\mathbb{N}^n$, te neka su $f(X),\ g(X) \in k[X] = k[x_1, ..., x_n]$ i pretpostavimo da $f \xrightarrow{g} h$, to jest postoji nenul član $c_\beta X^\beta$ u $f(X)$ s $LT\,(g) \mid c_\beta X^\beta$ i*
$h(X) = f(X) - \frac{c_\beta X^\beta}{LT_{(g)}} g(X)$. *Tada je*

$$Deg\ (\frac{c_\beta X^\beta}{LT_{(g)}} g(X)) \preceq Deg\ (f).$$

Nadalje, ako je $\beta = Deg\ (f)$ (to jest ako $c_\beta X^\beta = LT\ (f)$) tada je ili

$$h(X) = 0 \text{ ili } Deg\ (h) \prec Deg\ (f);$$

te ako je $\beta \prec Deg\ (f)$, tada $Deg\ (h) = Deg\ (f)$.

Dokaz. Zapišimo

$$f(X) = \mathrm{LT}(f) + c_k X^k + \text{niži članovi},$$

gdje je $c_k X^k = \mathrm{LT}\ (f - \mathrm{LT}\ (f))$; budući da je $c_\beta X^\beta$ član od $f(X)$, imamo $\beta \preceq \mathrm{Deg}\ (f)$.

Slično, ako je $\mathrm{LT}\ (g) = a_\gamma X^\gamma$, tada je $\mathrm{Deg}\ (g) = \gamma$, pišemo

$$g(X) = a_\gamma X^\gamma + a_\lambda X^\lambda + \text{niži članovi},$$

gdje je $a_\lambda X^\gamma = \mathrm{LT}\ (g - \mathrm{LT}\ (g))$.

Stoga,

$$\begin{aligned} h(X) &= f(X) - \frac{c_\beta X^\beta}{LT(g)} g(X) \\ &= f(X) - \frac{c_\beta X^\beta}{LT(g)} [LT(g) + a_\lambda X^\lambda + ...] \\ &= [f(X) - c_\beta X^\beta] - \frac{c_\beta X^\beta}{LT(g)} [a_\lambda X^\lambda + ...]. \end{aligned}$$

Sada $\mathrm{LT}(g) \mid c_\beta X^\beta$ povlači da je $\beta - \gamma \in \mathbb{N}^n$.
Tvrdimo

$$\mathrm{Deg}(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}[a_\lambda X^\lambda + ...]) = \lambda + \beta - \gamma; \text{to jest}$$
$$\lambda + \beta - \gamma = \mathrm{Deg}(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)} a_\lambda X^\lambda)$$

je najveći multistupanj koji se pojavljuje.
Pretpostavimo da je $a_\eta X^\eta$ niži član u $g(X)$, (tj.,$\eta < \lambda$).
Budući da je $\preceq$ monomijalni uređaj,

$$\eta + (\beta - \gamma)\gamma + (\lambda - \gamma) = \lambda.$$

Sada $\lambda < \gamma$ povlači $\lambda + (\beta - \gamma) \prec \gamma + (\beta - \gamma) = \beta$, pa je

$$\mathrm{Deg}(-[\frac{c_\beta X^\beta}{\mathrm{LT}(g)}]g(X)) \prec \beta \preceq \mathrm{Deg}(f). \tag{1.1}$$

Zbog toga, ako je $h(X) \neq 0$, tada je prema Lemi 1.4.4. :

$$\mathrm{Deg}(h) \preceq \max\{\mathrm{Deg}(f(X) - c_\beta X^\beta),\ \mathrm{Deg}(-[\tfrac{c_\beta X^\beta}{\mathrm{LT}(g)}]g(X)\}.$$

Sada, ako je $\beta = \mathrm{Deg}(f)$, tada $c_\beta X^\beta = \mathrm{LT}(f)$,

$$f(X) - c_\beta X^\beta = f(X) - \mathrm{LT}(f) = c_k X^k + \text{niži članovi}$$

i stoga,

$$\mathrm{Deg}(f(X) - c_\beta X^\beta) = k \prec \mathrm{Deg}(f)$$

u ovom slučaju.
Ako je $\beta \prec \mathrm{Deg}(f)$, tada $\mathrm{Deg}(f(X) - c_\beta X^\beta) = \mathrm{Deg}(f)$, dok iz (1.1) slijedi

$$\mathrm{Deg}(-[\tfrac{c_\beta X^\beta}{\mathrm{LT}_{(g)}}]g(X)) \prec \mathrm{Deg}(f)\ ,$$

pa je $\mathrm{Deg}(h) = \mathrm{Deg}(f)$ u ovom slučaju.

Zadnja nejednakost (iz iskaza teorema) je očita; jer

$$\tfrac{c_\beta X^\beta}{\mathrm{LT}_{(g)}} g(X) = c_\beta X\beta + \tfrac{c_\beta X^\beta}{\mathrm{LT}_{(g)}}[a_\lambda X^\lambda + ...].$$

Budući da potonji dio polinoma ima stupanj $\lambda + \beta - \gamma \prec \beta$, vidimo da je

$$\mathrm{Deg}(\tfrac{c_\beta X^\beta}{\mathrm{LT}_{(g)}} g(X)) = \beta \preceq \mathrm{Deg}(f).$$

□

Definicija 1.4.17. *Neka je $\{g_1(X_1), ..., g_m(X_m)\}$ skup polinoma u $k[X]$. Kažemo da je polinom $r(X)$* ***reduciran mod*** *$\{g_1, ..., g_m\}$ ako je ili $r(X) = 0$ ili nijedan od $LT(g_i)$ ne dijeli nijedan ne nul član od $r(X)$.*

Slijedi algoritam dijeljenja za polinome u više varijabli.

Budući da su za algoritam dijeljenja potrebni polinomi djelitelji $\{g_1, ..., g_m\}$ korišteni u posebnom poretku (uostalom, algoritam mora dati eksplicitne upute), koristit ćemo se n-torka polinoma umjesto podskup polinoma.

Označimo m-torku čiji i-ti ulaz je g_i sa $[g_1, ..., g_m]$ jer bi uobičajena notacija $(g_1, ..., g_m)$ bila zamijenjena s idealom $(g_1, ..., g_m)$ generiranim s g_i.

Teorem 1.4.18. *(**Algoritam dijeljenja u** $k[X]$) Neka je $\preceq$ monomijalni uređaj na $\mathbb{N}^n$, te neka je $k[X] = k[x_1, ..., x_n]$.*

Ako je $f(X) \in k[X]$ i $G = [g_1(X), ..., g_m(X)]$ je n-torka polinoma u $k[X]$, tada postoji algoritam koji daje polinome $r(X),\ a_1(X),\ ...,\ a_m(X) \in k[X]$ s

$$f = a_1 g_1 + ... + a_m g_m + r,$$

gdje je r reducirani mod $\{g_1, ..., g_m\}$ i

$$Deg(a_i g_i) \preceq Deg(f),\ za\ svaki\ i.$$

Dokaz. Jednom kad je monomijalni uređaj izabran, tako da su vodeći članovi definirani, algoritam je direktna generalizacija algoritma dijeljenja u jednoj varijabli.

Prvo, reduciramo *mod* g_1 koliko god puta je moguće, zatim reduciramo *mod* g_2 koliko puta je moguće, nakon čega ponovo reduciramo *mod* g_1.

Općenitije, jednom kad je polinom reduciran *mod* $[g_1,\ ...,\ g_i]$, za bilo koji i, tada reduciramo *mod*$[g_1,\ ...\ , g_i,\ g_{i+1}]$.

Pseudokod koji opisuje algoritam preciznije:

$Ulaz : f(X) = \sum_{\beta} c_\beta X^\beta,\ [g_1, ..., g_m]$

$Izlaz : r,\ a_1, ..., a_m$

$r := f;\ a_i = 0$

DOK f nije reduciran *mod*$[g_1, ..., g_m]$ RADI

  izaberi najmanji i s $\mathrm{LT}(g_i)|c_\beta X^\beta$ za neki β

  $f - [c_\beta X^\beta/\mathrm{LT}(g_i)]g_i := f$

  $a_i + [c_\beta X^\beta/\mathrm{LT}(g_i)] := a_i$

ZAVRŠI PETLJU

Za svaki korak $h_j \xrightarrow{g_i} h_{j+1}$ algoritma, imamo

$$\text{multiriječ } (h_j) \succ_{lex} \text{multiriječ } (h_{j+1})$$

u $W^+(\mathbb{N}^n)$ po Propoziciji 1.4.11., i zato algoritam staje, jer je $\prec_{lex}$ dobar uređaj na $W^+(\mathbb{N}^n)$.

Očito, izlaz $r(X)$ je reducirani *mod* $\{g_1, ..., g_m\}$, jer ako sadrži član djeljiv s nekim $\mathrm{LT}(g_i)$, tada se može reducirati još jednom.

Napokon, svaki član od $a_i(X)$ ima oblik $c_\beta X^\beta/\mathrm{LT}(g_i)$ za neki srednji izlaz $h(X)$. Sada iz Propozicije 1.4.16. slijedi da vrijedi $\mathrm{Deg}(a_i g_i) \preceq \mathrm{Deg}(f)$.

□

Definicija 1.4.19. *Dan je monomijalni uređaj na* $\mathbb{N}^n$*, polinom* $f(X) \in k[X]$ *i m-torka* $G = [g_1, ..., g_m]$.

Izlaz $r(X)$ *algoritma dijeljenja zovemo* ***ostatak*** *od* $f(X)$ *mod* G.

Primijetimo, ostatak r od f *mod* G je reduciran *mod* $\{g_1, ..., g_m\}$ i

$$f - r \in I = (g_1, ..., g_m).$$

Za algoritam je potrebno da G bude m-torka, zbog naredbe

"izaberi najmanji i za koji $\mathrm{LT}(g_i) \mid c_\beta X^\beta$"

za neki β koja određuje redoslijed redukcije.

Sljedeći primjer pokazuje da ostatak ne ovisi samo o skupu polinoma $\{g_1, ..., g_m\}$, nego i o redoslijedu koordinata u m-torki $G = [g_1, ..., g_m]$. To jest, ako je $\sigma \in S_m$ permutacija, i $G_\sigma = [g_{\sigma(1)}, ..., g_{\sigma(m)}]$, tada ostatak r_σ od $f \ mod \ G_\sigma$ nije nužno isti kao ostatak r od $f \ mod \ G$.

Čak štoviše, moguće je da $r \neq 0$ i $r_\sigma = 0$, tako da ostatak *mod* G nije prepreka da f bude u idealu $(g_1, ..., g_m)$.

Ovaj fenomen ilustrirat ćemo u sljedećem primjeru, i podrobnije ćemo ga opisati u sljedećem poglavlju.

Primjer 1.4.20. *Neka je $f(x, y, z) = x^2y^2 + xy$, te neka je $G = [g_1, g_2, g_3]$, gdje su*

$$\begin{aligned} g_1 &= x^2 + z^2 \\ g_2 &= x^2y + yz \\ g_3 &= z^3 + xy. \end{aligned}$$

Koristi se stupanj leksikografski uređaj na $\mathbb{N}^3$.

Sada, $y^2 = LT(g_i) \mid LT(f) = x^2y^2$, pa $f \xrightarrow{g_1} h$, gdje je

$$h = f - \tfrac{x^2y^2}{y^2}(y^2 + z^2) = -x^2z^2 + xy.$$

Polinom $-x^2z^2 + xy$ je reduciran mod G, jer ni $-x^2z^2$ ni xy nije djeljiv ni s jednim od vodećih članova $LT(g_1) = y^2$, $LT(g_2) = x^2y$, $LT(g_3) = z^3$.

Primijenimo sada algoritam dijeljenja koristeći trojku $G' = [g_2, g_1, g_3]$.

Prva redukcija daje $f \xrightarrow{g_2} h'$, gdje

$$h' = f - \tfrac{x^2y^2}{x^2y}(x^2y + yz) = -y^2z + xy.$$

Sada h' nije reduciran i reduciranjem mod g_1 daje

$$h' - \tfrac{-y^2z}{y^2}(y^2 + z^2) = z^3 + xy.$$

Ali $z^3 + xy = g_3$, pa $z^3 + xy \xrightarrow{g_3} 0$. Dakle, ostatak ovisi o poretku djelitelja polinoma g_i u m-torci.

Poglavlje 2

Gröbnerove baze

2.1 Gröbnerove baze

U ovom poglavlju pretpostavljamo da je $\mathbb{N}^n$ snabdjeven monomijalnim uređajem (npr. stupanj-leksikografski uređaj), tako da je LT(f) definiran i da algoritam dijeljenja ima smisla.

Vidjeli smo da ostatak od $f\ mod[g_1, ..., g_m]$, dobiven iz algoritma dijeljenja, može ovisiti o poretku u kojem su izlistani g_i.

Neformalno, Gröbnerova baza $\{g_1, ..., g_m\}$ ideala $I = (g_1, ..., g_m)$ je generirajući skup takav da, za svaku m-torku $G_\sigma = [g_{\sigma(1)}, ..., g_{\sigma(m)}]$ formiranu iz g_i, gdje je $\sigma \in S_m$ permutacija, ostatak od $f\ mod\ G_\sigma$ je točno prepreka tome da li f leži u I.

Definirat ćemo Gröbnerove baze koristeći svojstvo koje se lakše provjeri, i tada pokazati (u Propoziciji 2.1.2.), da su one karakterizirane s upravo spomenutim zanimljivijim svojstvom.

Definicija 2.1.1. *Skup polinoma* $\{g_1, ..., g_m\}$ *je* ***Gröbnerova baza*** *ideala* $I = (g_1, ..., g_m)$ *ako za svaki nenul* $f \in I$, *postoji* g_i *sa svojstvom* $LT(g_i) \mid LT(f)$.

Primjetimo da Gröbnerova baza je skup polinoma, ne m-torka polinoma. Prethodni primjer pokazuje da

$$\{y^2 + z^2, x^2y + yz, z^3 + xy\}$$

nije Gröbnerova baza ideala $(y^2 + z^2, x^2y + yz, z^3 + xy)$.

Propozicija 2.1.2. *Skup polinoma* $\{g_1, ..., g_m\}$ *je Gröbnerova baza ideala* $I = (g_1, ..., g_m)$ *ako i samo ako za svaku m-torku* $G_\sigma = [g_{\sigma(1)}, ..., g_{\sigma(m)}]$, *gdje je* $\sigma \in S_m$, *svaki* $f \in I$ *ima ostatak* 0 *mod* G_σ.

Dokaz. Pretpostavimo da postoji neka permutacija $\sigma \in S_m$ i neki $f \in I$ čiji ostatak *mod* G_σ nije 0. Između svih takvih polinoma, izabere se f s najmanjim stupnjem. Budući da je $\{g_1, ..., g_m\}$ Gröbnerova baza,

$$\mathrm{LT}(g_i) \mid \mathrm{LT}(f),$$

za neki i. Izabere se najmanji $\sigma(i)$ za koji postoji redukcija

$$f \xrightarrow{g_{\sigma(i)}} h,$$

te primjetimo da je $h \in I$.

Kako je $\mathrm{Deg}(h) \prec \mathrm{Deg}(f)$, algoritam dijeljenja daje niz redukcija

$$h = h_0 \to h_1 \to h_2 \to ... \to h_p = 0.$$

No, algoritam dijeljenja za f pridružuje $f \to h$ na početku, pokazujući da je ostatak od f *mod* G_σ jednak 0. Kontradikcija.

Obratno, pretpostavi se da svaki $f \in I$ ima ostatak 0 *mod* G_σ, ali da $\{g_1, ..., g_m\}$ nije Gröbnerova baza od $I = (g_1, ..., g_m)$.

Ako postoji nenul $f \in I$ takav da

$$LT(g_i) \nmid LT(f)$$

za svaki i, tada u bilo kojoj redukciji $f \xrightarrow{g_i} h$ imamo $\mathrm{LT}(h) = \mathrm{LT}(f)$.

Dakle, ako je $G = [g_1, ..., g_m]$ algoritam dijeljenja daje redukcije

$$f \to h_1 \to h_2 \to ... \to h_p = r$$

u kojim $\mathrm{LT}(r) = \mathrm{LT}(f)$.

Zato, $r \neq 0$, to jest ostatak od f *mod* G nije 0, a to je kontradikcija.

□

Lema 2.1.3. *Neka je* $c_\alpha X^\alpha$ *monom različit od nule, te neka su* $f(X), g(X) \in k[X]$ *polinomi takvi da nijedan njihov član nije djeljiv s* $c_\alpha X^\alpha$. *Tada nijedan član od* $f(X) - g(X)$ *također nije djeljiv s* $c_\alpha X^\alpha$.

Korolar 2.1.4. *Ako je* $\{g_1, ..., g_m\}$ *Gröbnerova baza ideala* $I = (g_1, ..., g_m)$, *te ako je* $G = [g_1, ..., g_m]$ *bilo koja m-torka formirana iz* g_i, *tada za svaki* $f(X) \in k[X]$ *postoji jedinstveni* $r(X) \in k[X]$ *koji je reduciran mod* $\{g_1, ..., g_m\}$ *tako da* $f - r \in I$; *ustvari, r je ostatak od f mod G.*

Dokaz. Algoritam dijeljenja daje polinom r, reduciran *mod* $\{g_1, ..., g_m\}$, te polinome $a_1, ..., a_m$ za koje je $f = a_1g_1 + ... + a_mg_m + r$; očito je $f - r = a_1g_1 + ... + a_mg_m \in I$.

Da bi se pokazala jedinstvenost, pretpostavi se da su r i r' reducirani *mod*$\{g_1, ..., g_m\}$, te da $f - r$ i $f - r'$ leže u I, pa je

$$(f - r') - (f - r) = r - r' \in I.$$

Budući da su r i r' reducirani *mod* $\{g_1, ..., g_m\}$, nijedan od njihovih članova nije dijeljiv ni s jednim od LT(g_i).

Ako je $r - r' \neq 0$, tada nijedan član od $r - r'$, prema Lemi 2.1.3. nije djeljiv ni s jednim od LT(g_i); pa posebno, LT($r - r'$) nije djeljiv ni s jednim od LT(g_i), a ovo je kontradikcija s Propozicijom 2.1.2.

Dakle, $r = r'$.

□

Sljedeći korolar pokazuje da Gröbnerova baza rješava problem različitih ostataka u algoritmu dijeljenja koji proizlaze iz različitih m-torki.

Korolar 2.1.5. *Neka je* $\{g_1, ..., g_m\}$ *Gröbnerova baza ideala* $I = (g_1, ..., g_m)$*, te neka je* $G = [g_1, ..., g_m]$.

(i) Ako je $f(X) \in k[X]$ *i* $G_\sigma = [g_{\sigma(1)}, ..., g_{\sigma(m)}]$*, gdje je* $\sigma \in S_m$ *permutacija, tada je ostatak od* f *mod* G *jednak ostatku od* f *mod* G_σ.

(ii) Polinom $f \in I$ *ako i samo ako* f *ima ostatak* 0 *mod* G.

Dokaz. (i) Ako je r ostatak od f *mod* G, tada prethodni Korolar 2.1.4. kaže da je r jedinstveni polinom, reduciran *mod* $\{g_1, ..., g_m\}$, sa $f - r \in I$.

Slično, ostatak r_σ od f *mod* G_σ je jedinstven polinom, reduciran *mod* $\{g_1, ..., g_m\}$, sa $f - r_\sigma \in I$. Tvrdnja jedinstvenosti u prethodnom Korolaru 2.1.4. daje $r = r_\sigma$.

(ii) Propozicija 2.1.2. pokazuje da ako je $f \in I$, tada je ostatak jednak nuli.

Obratno, ako je r ostatak od f *mod* G, tada $f = q + r$, gdje je $q \in I$. Dakle, ako je $r = 0$, tada je $f \in I$.

□

Nameće se nekoliko očitih pitanja. Da li Gröbnerove baze postoje i, ako postoje, jesu li jedinstvene?

Ako je dan ideal $I \in k[X]$, postoji li algoritam za nalaženje Gröbnerove baze od I?

Pojam S-polinoma omogućit će nam da prepoznamo Gröbnerovu bazu, no prvo uvedimo notaciju.

Definicija 2.1.6. *Ako su* $\alpha = (\alpha_1, ..., \alpha_n)$ *i* $\beta = (\beta_1, ..., \beta_n)$ *u* $\mathbb{N}^n$*, definira se*

$$\alpha \vee \beta = \mu$$

gdje je $\mu_i = max\{\alpha_i, \beta_i\}$ *i* $\mu = (\mu_1, ..., \mu_n)$*.*

Primijetimo da je $X^{\alpha\vee\beta}$ najmanji zajednički višekratnik monoma X^α i X^β.

Definicija 2.1.7. *Neka su* $f(X)$, $g(X) \in k[X]$*, gdje je* $LT(f) = a_\alpha X^\alpha$ *i* $LT(g) = b_\beta X^\beta$*. Definiramo*

$$L(f, g) = X^{\alpha\vee\beta}.$$

S***-polinom*** *S(f,g) definiran je sa*

$$S(f, g) = \frac{L(f,g)}{LT(f)} f - \frac{L(f,g)}{LT(g)} g;$$

to jest, ako je $\mu = \alpha \vee \beta$*, tada*

$$S(f, g) = a_\alpha^{-1} X^{\mu-\alpha} f(X) - b_\beta^{-1} X^{\mu-\beta} g(X).$$

Primjetimo $S(f, g) = -S(g, f)$.

Primjer 2.1.8. *(i) Ako je* $f(x, y) = 3x^2y$ *i* $g(x, y) = 5xy^3 - y$ *(u stupanj-leksikografskom uređaju), tada je* $LT(f, g) = x^2y^3$ *i*

$$S(f, g) = \frac{x^2y^3}{3x^2y} 3x^2y - \frac{x^2y^3}{5xy^3}(5xy^3 - y) = \frac{1}{5}xy$$

(ii) Ako su $f(X)$ *i* $g(X)$ *monomi, recimo,* $f(X) = a_\alpha X^\alpha$ *i* $g(X) = b_\beta X^\beta$*, tada je*

$$S(f, g) = \frac{X^{\alpha\vee\beta}}{a_\alpha X^\alpha} a_\alpha X^\alpha - \frac{X^{\alpha\vee\beta}}{b_\beta X^\beta} b_\beta X^\beta = 0.$$

Sljedeća tehnička lema pokazuje zašto su S-polinomi važni. Kaže da ako je

$$Deg(\textstyle\sum_j a_j g_j) \prec \delta\,,$$

gdje su a_j monomi, dok $\mathrm{Deg}(a_j g_j) = \delta$ za svaki j, tada bilo koji polinom multistupnja $\prec \delta$ možemo zapisati kao linearnu kombinaciju S-polinoma,s monomijalnim koeficijentima, od kojih je svaki član multistupnja strogo manjeg od δ.

Lema 2.1.9. *Neka su dani* $g_1(X), ..., g_l(X) \in k[X]$ *i monomi* $c_j X^{\alpha(j)}$*, neka je* $h(X) = \sum_{j=1}^{l} c_j X^{\alpha(j)} g_j(X)$.

Neka je δ *multistupanj. Ako je* $Deg(h) \prec \delta$ *i* $Deg(c_j X^{\alpha(j)} g_j(X)) = \delta$ *za svaki* $j \leqslant l$*, tada postoje* $d_j \in k$ *takvi da*

$$h(X) = \sum_j d_j X^{\delta - \mu(j)} S(g_j, g_{j+1})$$

gdje je $\mu(j) = Deg(g_j) \vee Deg(g_{j+1})$*, za sve* $j < l$ *vrijedi*

$$Deg(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta.$$

Dokaz. Neka je $\mathrm{LT}(g_j) = b_j X^{\beta(j)}$, pa je

$$\mathrm{LT}(c_j X^{\alpha(j)} g_j(X)) = c_j b_j X^{\delta}.$$

Koeficijent od X^δ u $h(X)$ je prema tome $\sum_j c_j b_j$. Budući da je $\mathrm{Deg}(h) \prec \delta$, moramo imati $\sum_j c_j b_j = 0$.

Definiramo normirane polinome

$$u_j(X) = b_j^{-1} X^{\alpha(j)} g_j(X).$$

Imamo teleskopsku sumu

$$\begin{aligned} h(X) &= \sum_{j=1}^{l} c_j X^{\alpha(j)} g_j(X) \\ &= \sum_{j=1}^{l} c_j b_j u_j \\ &= c_1 b_1 (u_1 - u_2) + (c_1 b_1 + c_2 b_2)(u_2 - u_3) + ... \\ &+ (c_1 b_1 + ... + c_{l-1} b_{l-1})(u_{l-1} - u_l) \\ &+ (c_1 b_1 + ... + c_l b_l) u_l \end{aligned}$$

Zadnji izraz $(c_1 b_1 + ... + c_l b_l) u_l = 0$, jer je $\sum_j c_j b_j = 0$. Budući da je $\delta = \mathrm{Deg}(c_j X^{\alpha(j)} g_j(X))$, imamo $\alpha(j) + \beta(j) = \delta$, pa $X^{\beta(j)} \mid X^\delta$ za sve j.

Otuda, za svaki $j < l$, imamo

$$\mathrm{nzv}\{X^{\beta(j)}, X^{\beta(j+1)}\} = X^{\beta(j) \vee \beta(j+1)} \mid X^\delta,$$

to jest, ako pišemo $\mu(j) = \beta(j) \vee \beta(j+1)$, tada je $\delta - \mu(j) \in \mathbb{N}^n$.

No,

$$\begin{aligned} X^{\delta-\mu(j)} S(g_j, g_{j+1}) &= X^{\delta-\mu(j)} \left(\frac{X^{\mu(j)}}{LT(g_j)} g_j(X) - \frac{X^{\mu(j)}}{LT(g_{j+1})} g_{j+1}(X)\right) \\ &= \frac{X^{\delta}}{LT(g_j)} g_j(X) - \frac{X^{\delta}}{LT(g_{j+1})} g_{j+1}(X) \\ &= b_j^{-1} X^{\alpha(j)} g_j - b_{j+1}^{-1} X^{\alpha(j+1)} g_{j+1} \\ &= u_j - u_{j+1}. \end{aligned}$$

Supstituiranjem ove jednadžbe u teleskopsku sumu dobivamo sumu željenog oblika, gdje je $d_j = c_1 b_1 + ... + c_j b_j$:

$$\begin{aligned} h(X) = {} & c_1 b_1 X^{\delta-\mu(1)} S(g_1, g_2) + (c_1 b_1 + c_2 b_2) X^{\delta-\mu(2)} S(g_2, g_3) + ... \\ & + (c_1 b_1 + ... + c_{l-1} b_{l-1}) X^{\delta-\mu(l-1)} S(g_{l-1}, g_l). \end{aligned}$$

Konačno, budući da su oba u_j i u_{j+1} normirani s vodećim članom multistupnja δ, imamo $\mathrm{Deg}(u_j - u_{j+1}) \prec \delta$. No, pokazali smo da je $u_j - u_{j+1} = X^{\delta-\mu(j)} S(g_j, g_{j+1})$, pa je tako $\mathrm{Deg}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta$, što se i trebalo pokazati.

□

2.2 Buchbergerov algoritam

Prema Propoziciji 2.1.2., $\{g_1, ..., g_m\}$ je Gröbnerova baza od $I = (g_1, ..., g_m)$ ako svaki $f \in I$ ima ostatak 0 *mod G* (gdje je G bilo koja m-torka formirana redajući g_i).

Važnost slijedećeg teorema leži u pokazivanju da je nužno izračunati ostatke samo konačno mnogo polinoma, S-polinoma, da bi odredili je li $\{g_1, ..., g_m\}$ Gröbnerova baza.

Teorem 2.2.1 (Buchberger). *Skup $\{g_1, ..., g_m\}$ je Gröbnerova baza ideala $I = (g_1, ..., g_m)$ ako i samo ako $S(g_p, g_q)$ ima ostatak 0 mod G za sve $p,\ q,$ gdje je $G = [g_1, ..., g_m]$.*

Dokaz. Očito, $S(g_p, g_q)$ kao linearna kombinacija od g_p i g_q leži u I.

Dakle, ako je $G = \{g_1, ..., g_m\}$ Gröbnerova baza, tada $S(g_p, g_q)$ ima ostatak 0 *mod G*, po Propoziciji 2.1.2.

Obratno, pretpostavimo da $S(g_p, g_q)$ ima ostatak 0 *mod G* za sve $p,\ q$; moramo pokazati da svaki $f \in I$ ima ostatak 0 *mod G*. Po Propoziciji 2.1.2. dovoljno je pokazati da ako je $f \in I$, tada $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$ za neki i.

Budući da je $f \in I = (g_1, ..., g_m)$, možemo pisati $f = \sum_i h_i g_i$, pa tako

$$\mathrm{Deg}(f) \preceq max_i\{\mathrm{Deg}(h_i, g_i)\}.$$

Ako vrijedi jednakost, tada $\mathrm{Deg}(f) = \mathrm{Deg}(h_i g_i)$ za neki i, pa Propozicija 1.4.14. daje $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$, što smo i željeli pokazati.

Stoga, možemo pretpostaviti strogu nejednakost:

$$\mathrm{Deg}(f) \prec max_i\{\mathrm{Deg}(h_i g_i)\}.$$

Polinom f može se zapisati kao linearna kombinacija od g_i na mnogo načina.

Od svih izraza oblika

$$f = \sum_i h_i g_i$$

biramo onaj u kojem je $\delta = max_i\{\mathrm{Deg}(h_i g_i)\}$ minimalan (što je moguće jer je $\preceq$ dobar uređaj).

Ako je $\mathrm{Deg}(f) = \delta$, gotovi smo, kao što je pokazano, dakle, možemo pretpostaviti strogu nejednakost: $\mathrm{Deg}(f) \prec \delta$. Pišemo:

$$f = \sum_{j;\ \mathrm{Deg}(h_j g_j) = \delta} h_j g_j + \sum_{l;\ \mathrm{Deg}(h_l g_l) < \delta} h_l g_l. \tag{2.1}$$

Ako je $\mathrm{Deg}(\sum_j h_j g_j) = \delta$, tada je $\mathrm{Deg}(f) = \delta$, što je kontradikcija; dakle, $\mathrm{Deg}(\sum_j h_j g_j) \prec \delta$. No, koeficijent od X^δ u ovoj sumi je dobiven iz njegovih vodećih članova, pa je

$$\mathrm{Deg}(\textstyle\sum_j LT(h_j) g_j) \prec \delta.$$

Sada je $\sum_j \mathrm{LT}(h_j) g_j$ polinom koji zadovoljava pretpostavku Leme 2.1.9., pa postoje konstante d_j i multistupnjevi $\mu(j)$ takvi da

$$\sum_j \mathrm{LT}(h_j) g_j = \sum_j d_j X^{\delta - \mu(j)} S(g_j, g_{j+1}), \tag{2.2}$$

gdje je $\mathrm{Deg}(X^{\delta-\mu(j)} S(g_j, g_{j+1})) \prec \delta$.

Budući da svaki $S(g_j, g_{j+1})$ ima ostatak 0 *mod G*, algoritam dijeljenja daje $a_{ji}(X) \in k[X]$ sa

$$S(g_j, g_{j+1}) = \textstyle\sum_i a_{ji} g_i,$$

gdje je $\mathrm{Deg}(a_{ji} g_i) \preceq \mathrm{Deg}(S(g_j, g_{j+1}))$ za sve $j,\ i$.

Slijedi da je

$$X^{\delta-\mu(j)}S(g_j, g_{j+1}) = \sum_i X^{\delta-\mu(j)}a_{ji}g_i.$$

Stoga, Lema 2.1.9. daje

$$\mathrm{Deg}(X^{\delta-\mu(j)}a_{ji}g_i) \preceq \mathrm{Deg}(X^{\delta-\mu(j)}S(g_j, g_{j+1})) \prec \delta. \tag{2.3}$$

Supstitucijom u jednadžbu (2.2), imamo

$$\begin{aligned}\sum_j \mathrm{LT}(h_j)g_j &= \sum_j d_j X^{\delta-\mu(j)}S(g_j, g_{j+1}) \\ &= \sum_j d_j(\sum_i X^{\delta-\mu(j)}a_{ji}g_i) \\ &= \sum_i(\sum_j d_j X^{\delta-\mu(j)}a_{ji})g_i.\end{aligned}$$

Ako označimo $\sum_j d_j X^{\delta-\mu(j)}$ sa h_i', tada je

$$\sum_j \mathrm{LT}(h_j)g_j = \sum_i h_i' g_i, \tag{2.4}$$

gdje je, po jednadžbi (2.3) $\mathrm{Deg}(h_i' g_i) \prec \delta$ za sve i.

Konačno, supstituiramo izraz u jednadžbi (2.4) u jednadžbu (2.1):

$$\begin{aligned}f &= \sum_{j;\,\mathrm{Deg}(h_j g_j)=\delta} h_j g_j + \sum_{l;\,\mathrm{Deg}(h_l g_l)\prec\delta} h_l g_l = \\ &= \sum_{j;\,\mathrm{Deg}(h_j g_j)=\delta} \mathrm{LT}(h_j)g_j + \sum_{j;\,\mathrm{Deg}(h_j g_j)=\delta} [h_j - \mathrm{LT}(h_j)]g_j + \sum_{l;\,\mathrm{Deg}(h_l g_l)\prec\delta} h_l g_l = \\ &= \sum_i h_i' g_i + \sum_{j;\,\mathrm{Deg}(h_j g_j)=\delta} [h_j - \mathrm{LT}(h_j)]g_j + \sum_{l;\,\mathrm{Deg}(h_l g_l)\prec\delta} h_l g_l.\end{aligned}$$

Zapisali smo f kao linearnu kombinaciju od g_i u kojoj svaki član ima multistupanj strogo manji od δ, što je u kontradikciji sa minimalnosti od δ. Sada je dokaz potpun. □

Korolar 2.2.2. *Ako $I = (f_1, ..., f_s)$ u $k[X]$, gdje je svaki f_i monom (to jest, ako je I monomijalni ideal), tada je $\{f_1, ..., f_s\}$ Gröbnerova baza od I.*

Dokaz. Prema primjeru 2.1.8. (*ii*) , S-polinom bilo kojeg para monoma je 0.

□

Evo glavnog rezultata: Gröbnerova baza od $(f_1, ..., f_s)$ može se dobiti pridružujući ostatke S-polinomima.

Lema 2.2.3. *Ideal $I \in k[X]$ koji je generiran monomima, recimo $I = (X^{\alpha(1)}, ..., X^{\alpha(q)})$, nazivamo* ***monomijalni ideal****.*

(i) $f(X) \in I$ *ako i samo ako je svaki član od* $f(X)$ *djeljiv s nekim* $X^{\alpha(i)}$.

(ii) Ako je $G = [g_1, ..., g_m]$ *i* r *je reduciran mod G, tada r ne leži u monomijalnom idealu* $(LT(g_1), ..., LT(g_m))$.

Teorem 2.2.4 (**Buchbergerov algoritam**)**.** *Svaki ideal $I = (f_1, ..., f_s)$ u $k[X]$ ima Gröbnerovu bazu koja se može izračunati pomoću algoritma.*

Dokaz. Ovo je pseudokod za algoritam:

$Ulaz : B = f_1, ..., f_s \quad G = [f_1, ..., f_s]$
$Izlaz$: Gröbnerova baza $B = \{g_1, ..., g_m\}$ koja sadrži $\{f_1, ..., f_s\}$
$B := \{f_1, ..., f_s\} \;\; G := [f_1, ..., f_s]$
PONAVLJAJ
  $B' := B \;\; G' := G$
  ZA svaki par $g, \; g'$ za koji je $g \neq g' \in B'$ RADI
    $r :=$ ostatak od $S(g, g') \; mod \; G'$
    AKO $r \neq 0$
      TADA $B := B' \cup r$ i $G' = [g_1, ..., g_m, r]$
DOK $B = B'$

Sada svaka petlja algoritma povećava podskup $B \subseteq I = (g_1, ..., g_m)$ pridružujući mu ostatak *mod G* jednog od S-polinoma $S(g, g')$.

Kako su $g, \; g' \in I$, ostatak r od $S(g, g')$ leži u I, pa je veći skup $B \bigcup \{r\}$ sadržan u I.

Jedina zapreka zaustavljanju algoritma kod nekog B' je ako neki $S(g, g')$ nema ostatak $0 \; mod \; G'$.

Prema tome, ako algoritam stane, tada Teorem 2.2.1. pokazuje da je B' Gröbnerova baza.

Da bi vidjeli da algoritam ima kraj, pretpostavimo da petlja počinje s B' i završava s B.

Budući da je $B' \subseteq B$, imamo inkluziju monomijalnih ideala

$$(\mathrm{LT}(g') : g' \in B') \subseteq (\mathrm{LT}(g) : g \in B).$$

Tvrdimo da ako $B' \subsetneq B$, tada postoji također stroga inkluzija ideala.

Pretpostavimo da je r nenul ostatak nekog S-polinoma *mod* B' i da je $B = B' \bigcup \{r\}$. Prema definiciji, ostatak r je reduciran *mod* G', pa nijedan član od r nije djeljiv s $\mathrm{LT}(g')$ za bilo koji $g' \in B'$; posebno, $\mathrm{LT}(r)$ nije djeljiv ni s jednim $\mathrm{LT}(g')$.

Dakle, $\mathrm{LT}(r) \notin (\mathrm{LT}(g') : g' \in B')$, prema prethodnoj lemi. S druge strane, imamo $\mathrm{LT}(r) \in (\mathrm{LT}(g) : g \in B)$.

Dakle, ako algoritam ne stane, postoji beskonačan strogo uzlazni lanac ideala u $k[X]$, a to je kontradikcija s Hilbertovim teoremom o bazi, jer $k[X]$ zadovoljava uvjet uzlaznog lanca.

□

Primjer 2.2.5. $B' = \{y^2 + z^2, x^2y + yz, z^3 + xy\}$ *nije Gröbnerova baza jer*

$$S(y^2 + z^2, x^2y + yz) = x^2z^2 - y^2$$

nema ostatak 0 *mod* G'.

Međutim, pridruži li se $x^2z^2 - y^2z$ *dobije se Gröbnerova baza B jer svi S-polinomi u B imaju ostatak* 0 *mod* B'.

Teoretski, Buchbergerov algoritam nalazi Gröbnerovu bazu B od I, ali se postavlja pitanje praktičnosti istoga.

U mnogim slučajevima, izračuna se u razumnoj količini vremena, no s druge strane, ima primjera gdje treba puno vremena da bi završio.

Korolar 2.2.6. *(i) Ako je* $I = (f_1, ..., f_t)$ *ideal u* $k[X]$*, tada postoji algoritam koji određuje da li polinom* $h(X) \in k[X]$ *leži u I.*

(ii) Ako su $I = (f_1, ..., f_t)$ *i* $I' = (f_1', ..., f_s')$ *ideali u* $k[X]$*, tada postoji algoritam kojim se određuje da li je* $I = I'$.

Dokaz. (i) Koristimo Buchbergerov algoritam da bi našli Gröbnerova baza B od I, zatim pomoću algoritma dijeljenja izračunamo ostatak od h *mod* G (gdje je G bilo koja m-torka proizišla redajući polinome u B). Po Korolaru 2.1.5., $h \in I$ ako i samo ako $r = 0$.

(ii) Pomoću Buchbergerova algoritma nađemo Gröbnerove baze $\{g_1, ..., g_m\}$ i $\{g_1^{'}, ..., g_m^{'}\}$ od I i $I^{'}$, respektivno. Prema dijelu (i), postoji algoritam koji određuje da li je svaki $g_j^{'} \in I$ i $I^{'} \subseteq I$ ako je svaki $g_j^{'} \in I$.

Slično, postoji algoritam kojim se određuje obratna inkluzija, pa prema tome postoji algoritam kojim se određuje jednakost $I = I^{'}$.

□

Gröbnerova baza $B = \{g_1, ..., g_m\}$ može biti prevelika. Na primjer, iz same definicije Gröbnerove baze slijedi da ako je $f \in I$, tada $B \cup \{f\}$ je također Gröbnerova baza od I, stoga, mogli bi tražiti Gröbnerove baze, koje su na neki način minimalne.

Definicija 2.2.7. *Baza $\{g_1, ..., g_m\}$ ideala I je **reducirana** ako je:*

(i) svaki g_i normiran;

(ii) svaki g_i reduciran mod$\{g_1, ..., \hat{g}_i, ..., g_m\}$.

Može se dokazati da je reducirana Gröbnerova baza ideala jedinstvena. U specijalnom slučaju gdje je svaki $f_i(X)$ linearan, to jest,

$$f_i(X) = a_{i1}x_1 + ... + a_{in}n_n,$$

tada su zajedničke nultočke $(f_1, ..., f_t)$ rješenja homogenog sustava od t jednadžbi s n nepoznanica.

Ako je $A = [a_{ij}]$ $t \times n$ matrica koeficijenata, tada se može pokazati da reducirana Gröbnerova baza odgovara redu reduciranoj formi matrice A.

Još jedan specijalni slučaj pojavljuje se kad su $f_1, ..., f_t$ polinomi jedne varijable.

Reducirana Gröbnerova baza dobivena iz $\{f_1, ..., f_t\}$ pretvara se u njihov najveći zajednički djeljitelj, pa je Euklidov algoritam generaliziran na polinome više varijabli.

Korolar 2.2.6. ne počinje s "Ako je I ideal u $k[X]$"; nego specificira bazu: $I = (f_1, ..., f_t)$. Razlog je, naravno, taj što Buchbergerov algoritam zahtjeva bazu kao ulaz.

Na kraju ovog poglavlja pokazat ćemo kako naći bazu presjeka ideala.

Za dani je sustav jednadžbi polinoma u više varijabli jedan od načina za naći rješenje je eliminirati varijable.

Definicija 2.2.8. *Neka je k polje i $I \subseteq k[X, Y]$ ideal, gdje je $k[X, Y]$ polinomijalni prsten disjunktnih skupova varijabli $X \cup Y$. **Eliminacijski ideal** je*

$$I_X = I \cap k[X].$$

Na primjer, ako je $I = (x^2, xy)$ tada je Gröbnerova baza $\{x^2, xy\}$ (to su monomi, pa primijenimo Korolar 2.2.2.), pa je $I_X = (x^2) \subseteq k[X]$, dok je $I_Y = \{0\}$.

Propozicija 2.2.9. *Neka je k polje i neka $k[X] = k[x_1, ..., x_n]$ ima monomijalni uređaj za koji vrijedi $x_1 \succ x_2 \succ ... \succ x_n$ (npr. leksikografski uređaj), i za fiksni $p > 1$ neka je $Y = x_p, ..., x_n$.*

Ako $I \subseteq k[X]$ ima Gröbnerovu bazu $G = \{g_1, ..., g_m\}$, tada je $G \cap I_Y$ Gröbnerova baza za eliminacijski ideal $I_Y = I \cap k[x_p, ..., x_n]$.

Dokaz. Prisjetimo se da ako je $\{g_1, ..., g_m\}$ Gröbnerova baza od $I = (g_1, ..., g_m)$ to znači da za svaki nenul $f \in I$, postoji g_i takav da je $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.

Neka je $f(x_p, ..., x_n) \in I_Y$ neprazan. Budući da je $I_Y \subseteq I$, postoji $g_i(X)$ takav da $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$; dakle, $\mathrm{LT}(g_i)$ uključuje samo "zadnje" varijable $x_p, ..., x_n$.

Neka je $\mathrm{Deg}(\mathrm{LT}(g_i)) = \beta$. Ako g_i sadrži član $c_\alpha X^\alpha$ uključujući samo "ranije" varijable,x_i za $i < p$,tada je $\alpha \succ \beta$, zato jer je $x_1 \succ x_2 \succ ... \succ x_p \succ ... \succ x_n$.

To je kontradikcija, za β, stupanj vodećeg člana od g_i je veći nego stupanj bilo kojeg člana od g_i.

Slijedi da $g_i \in k[x_p, ..., x_n]$. Tada je $G \cap k[x_p, ..., x_n]$ Gröbnerova baza za $I_y = I \cap k[x_p, ..., x_n]$.

□

Sada možemo uvesti Gröbnerovu bazu presjeka ideala.

Propozicija 2.2.10. *Neka je k polje i neka su $I_1, ..., I_t$ ideali u $k[X]$, gdje je $X = x_1, ..., x_n$.*

(i) Promotrimo prsten polinoma $k[X, y_1, ..., y_t]$ gdje imamo novu varijablu y_j za $1 \leqslant j \leqslant t$. Ako je J ideal u $k[X, y_1, ..., y_t]$ generiran s $1 - (y_1 + ... + y_t)$ i $y_j I_j$ za svaki j, tada je $\cap_{j=1}^t I_j = J_X$.

(ii) Ako su dane Gröbnerove baze $I_1, ..., I_t$, tada možemo izračunati Gröbnerovu bazu od $\cap_{j=1}^t I_j$.

Dokaz. (i) Ako je $f = f(X) \in J_X = J \cap k[X]$, tada je $f \in J$, pa imamo jednadžbu

$$f(X) = g(X, Y)(1 - \sum y_j) + \sum_j h_j(X, y_1, ..., y_t) y_j q_j(X),$$

gdje su $g, h_j \in k[X, Y]$ i $q_j \in I_j$. Stavljajući $y_j = 1$ i ostale ipsilone na 0 daje nam $f = h_j(X, 0, ..., 1, ...0) q_j(X)$. Primijetimo da je $h_j(X, 0, ..., 1, ...0) q_j(X) \in k[X]$, pa je $f \in I_j$. Kako je j bio proizvoljan, imamo $f \in \cap I_j$, pa je $J_X \subseteq I_j$.

Za obratnu inkluziju, ako je $f \in \cap I_j$, tada jednadžba

$$f = f(1 - \sum y_j) + \sum_j y_j f$$

pokazuje da je $f \in J_X$, kako smo i željeli.

(ii) Ovo slijedi iz dijela (*i*) i Propozicije 2.2.9. ako koristimo monomijalni uređaj u kojem sve varijable u X slijede iz varijable u Y.

□

Primjer 2.2.11. *Promotrimo ideal $I = (x) \cap (x^2, xy, y^2) \subseteq k[x, y]$, gdje je k polje. Iako nije teško naći bazu od I ručno, koristit ćemo Gröbnerove baze da bi ilustrirali Propoziciju 2.2.10.*

Neka su u i v nove varijable, definiramo

$$J = (1 - u - v, ux, vx^2, vxy, vy^2) \subseteq k[x, y, u, v].$$

Prvi korak je naći Gröbnerovu bazu od J; koristimo lex monomijalni uređaj sa $x \prec y \prec u \prec v$. Budući da je S-polinom dva monoma 0*, Buchbergerov algoritam brzo daje Gröbnerovu bazu G od J:*

$$G = \{v + u - 1, x^2, yx, ux, uy^2 - y^2\}$$

Iz Propozicije 2.2.9. slijedi da Gröbnerova baza od I je $G \cap k[x, y]$: svi oni elementi od G koji ne uključuju varijable u i v.

Dakle,

$$I = (x) \cap (x^2, xy, y^2) = (x^2, xy).$$

Bibliografija

[1] J. J. Rotman, *Advanced Modern Algebra*, Prentice Hall, Upper Siddle River, NJ, 2002.

[2] B. Širola, *Algebarske strukture*,
https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf

Sažetak

U ovom radu, glavni cilj nam je proučiti pojam Gröbnerove baze. Rad se sastoji od dva poglavlja. U prvom poglavlju upoznajemo osnovne algebarske strukture koje su nam bile potrebne u daljnjim razmatranjima. Upoznajemo grupe, prstene i ideale, te nešto više pažnje posvećujemo polinomima, koji su bitni u radu. Također definiramo Noetherin prsten, te jedno poglavlje posvećujemo monomima, monomijalnim uređajima, te leksikografskom uređaju.

U drugom poglavlju smo konačno mogli definirati Gröbnerovu bazu, te navesti neka njena svojstva. Vrlo važan nam je bio Buchbergerov teorem, koji daje kriterij za određivanje je li neka baza Gröbnerova, te istoimeni algoritam za izračunavanje Gröbnerove baze.

Summary

In this diploma thesis the main goal is to study the concept of Gröbner basis. The thesis consists of two chapters. In the first chapter we introduce the basic algebraic structures which were important in further considerations. We get to know groups, rings and ideals, and more attention was devoted to polynomials which are very important in our work. We also define Noetherian ring, and one chapter is devoted to monomials, monomial order and lexicographic order.

In the second chapter we define the determine Gröbner basis, and prove some of it's properties. Buchberger's theorem was very important to us because it gives us criterion for determining whether the basis is Gröbner, and Buchberger's algorithm gives us the Gröbner basis.

Životopis

Rođena sam u Celju (Republika Slovenija), dana 16.01.1989. godine. Pohađala sam Osnovnu školu Viktora Kovačića u Humu na Sutli, a zatim upisala gimnaziju (opći smjer) u Srednjoj školi Krapina. Pohađanje dodatne nastave iz matematike i matematička natjecanja pomogla su mi pri odabiru smjera kojim želim nastaviti. Tako sam, po završetku srednjoškolskog obrazovanja, 2007. godine upisala Matematički odsjek Prirodoslovno - matematičkog fakulteta u Zagrebu. Preddiplomski studij sam završila 2013. godine, te sam iste godine upisala i diplomski studij Primijenjene matematike.