УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Маја Рославцев

ГРЕБНЕРОВЕ БАЗЕ ЗА КОНАЧНО ГЕНЕРИСАНЕ ИДЕАЛЕ НАД НЕКИМ КЛАСАМА НЕНЕТЕРИНИХ ПРСТЕНА

докторска дисертација

Београд, 2021.

UNIVERSITY OF BELGRADE
FACULTY OF MATHEMATICS

Maja Roslavcev

GRÖBNER BASES FOR FINITELY GENERATED IDEALS OVER SOME CLASSES OF NON-NOETHERIAN RINGS

Doctoral Dissertation

Belgrade, 2021.

Ментор:

др Зоран Петровић, редовни професор
Универзитет у Београду, Математички факултет

Чланови комисије:

др Зоран Петровић, редовни професор
Универзитет у Београду, Математички факултет

др Александар Липковски, редовни професор
Универзитет у Београду, Математички факултет

др Зоран Пуцановић, ванредни професор
Универзитет у Београду, Грађевински факултет

др Марко Радовановић, доцент
Универзитет у Београду, Математички факултет

Датум одбране: ____________________

Захвалница

Велику захвалност дугујем свом ментору, професору Зорану Петровићу, на свом труду, знању и стрпљењу које је уложио у раду са мном и који за резултат имају ову тезу. Захваљујем се и осталим члановима комисије. Пуно ми је значило њихово пажљиво читање такста, као и сви коментари и сугестије које су ми упутили.

Маја Рославцев

Наслов дисертације: Гребнерове базе за коначно генерисане идеале над неким класама ненетериних прстена

Rезиме: У овој тези бавимо се испитивањем постојања Гребнерових база за коначно генерисане идеале у прстенима полинома над неким класама прстена који нису Нетерини. Теорија Гребнерових база је врло развијена и позната за случај прстена полинома над пољима или над Нетериним прстенима. Случај када је базни прстен ненетерин је мање заступљен. У том смислу, прстени којима ћемо се овде бавити су валуациони прстени Круловe димензије 0, валуациони домени Крулове димензије 1, као и генерализација ових последњих, Приферови домени Крулове димензије 1. Такође су предмет изучавања фон Нојман регуларни комутативни прстени као и $(p-1)$-нил-чисти комутативни прстени. Добијене закључке можемо применити и на Безуове и Булове прстене, као поткласе Приферових и фон Нојман регуларних прстена, редом. Теза се већински фокусира на прстене полинома са једном неодређеном.

Кључне речи: Гребнерова база, валуациони домен, валуациони прстен, Приферов домен, фон Нојман регуларни комутативни прстен, $(p-1)$-нил-чисти комутативни прстен.

Научна област: Математика

Ужа научна област: Алгебра

УДК број: 512.713(043.3),512.714(043.3)

Dissertation title: Gröbner bases for finitely generated ideals over some classes of non-Noetherian rings

Abstract: In this thesis we deal with the existence of Gröbner bases for finitely generated ideals in rings of polynomials over some classes of rings which are not Noetherian. The theory of Gröbner bases is highly developed when we observe the ring of polynomials over a field or over a Noetherian ring. The case when the base ring is non-Noetherian is less examined. In that sense, the rings which will be of interest here are valuation rings of Krull dimension zero, valuation domains of Krull dimension one, also the generalization of the last: Prüfer domains of Krull dimension one. Von Neumann regular commutative rings and $(p-1)$-nil-clean commutative rings will also be a matter of discussion. The conclusions of the thesis can be applied to Bezout and Boolean rings, as these form the subclasses of Prüfer and von Neumann regular rings, respectively. The thesis is mostly focused on rings of polynomials with one indeterminate.

Keywords: Gröbner basis, valuation domain, valuation ring, Prüfer domain, von Neumann regular commutative ring, $(p-1)$-nil-clean commutative ring.

Research area: Mathematics

Research sub-area: Algebra

Садржај

Увод

Пуно се може рећи о значају и применама Гребнерових база. Један од базичних проблема, који звучи једноставно а од велике је важности и који можемо решавати помоћу ове теорије јесте проблем припадности идеалу. Друге примене укључују проблеме решавања система полиномијалних једначина, димензије објекта и разне примене у алгебарској геометрији. Такође имамо и мноштво примена ван области комутативне алгебре одакле је сама теорија поникла, а то су теорија графова, одређени проблеми оптимизације, као и у рачунарству и примењеној науци.

Сам појам увео је 1965. године Бруно Бухбергер у својој докторској дисертацији [13]. Од тада се литература која се бави овом темом непрестано богати. За теорију која се тиче Гребнерових база у овом тексту ће највише бити коришћене књиге [1] и [9]. Када је у питању полиномијални прстен над пољем, ова теорија је детаљно изучена. Резултати постоје и у случају када је базни прстен Нетерин, специјално Дедекиндов домен (видети [2]), а ако је прстен главноидеалски домен, тада је, као и у случају поља, могуће користити S-полиноме. Природно је онда питање како се теорија Гребнерових база развија у случају прстена који нису Нетерини и то је тема која ће овде бити заступљена.

Наредни текст је организован на следећи начин. У првој глави су представљене основне дефиниције и тврђења која су неопходна да би се дефинисао појам Гребнерове базе и јаке Гребнерове базе за идеал у прстену полинома над прстеном R. Дефинисани су и неки појмови из теорије комутативних прстена који се појављују у читавом тексту, као и неопходне ознаке. Потом, свака од наредних глава почиње дефиницијама, основним особинама или потребним теоремама које се односе на конкретне прстене над којима ће се разматрати питање постојања Гребнерове базе. После тог уводног дела, свака од глава садржи оригиналне резултате, од којих ће најбитнији бити споменути у наставку увода.

У другој глави уводимо појам валуационог домена. Представљен је доказ да над једнодимензионим валуационим доменом V сваки коначно генерисани идеал у $V[X]$ има минималну јаку Гребнерову базу (теорема 35). Резултати који претходе овој теореми омогућавају и одређивање те базе (леме 31 и 34), што је и илустровано на једном детаљно разрађеном примеру ненетериног валуационог домена.

У трећој глави бавимо се уопштењем прстена из претходне главе, валуационим прстенима. У теореми 39 доказано је да постоји минимална јака Гребнерова база за сваки коначно генерисани идеал у $V[X]$, где је V нуладимензиони валуациони прстен у коме је анулатор сваког елемента коначно генерисан. Такође је представљен пример који приказује како се тражена база може и одредити, у чему значајну улогу имају леме 37 и 38.

У четвртој глави описује се појам Приферовог домена, представљају неке од многих еквивалентних дефиниција и наводе неки примери. Такође се уводи потребна теорија која омогућава доказивање чињенице да постоји Гребнерова база за сваки коначно генерисни идеал у $R[X]$, где је R Приферов домен димензије један (теорема 49). У наредном одељку се дефинишу потребни појмови везани за Гребнерове базе коначно генерисаних подмодула у $R[X]^m$, за прстен R. Доказано је да постоји Гребнерова база за коначно генерисан подмодул у $R[X]^m$, где је R једнодимензиони Приферов домен и где је фиксиран мономни поредак POT (теорема 52), а у случају да је R валуациони домен, споменута база је и јака (теорема 55).

Фон Нојман регуларни комутативни прстени су приказани у петој глави, заједно са доказом о постојању јаке Гребнерове базе за коначно генерисани идеал у $R[X]$ (теорема 68). Дат је и пример на коме се показују технике одређивања те базе, а које се базирају на теореми 66 и леми 67.

У шестој глави представљамо $(p-1)$-нил-чисте комутативне прстене, као и неке примере прстена са овом особином који нису Нетерини. Потом је у теореми 74 дат доказ да је могуће решити проблем припадности радикалском идеалу у $R[X]$, где је R комутативан $(p-1)$-нил-чист прстен.

У седмој глави дата је дискусија о решавању претходних проблема у случају прстена полинома са више неодређених. Доказано је, на пример, да је идеал свих водећих коефицијената идеала I (теорема 75), као и идеал водећих коефицијената полинома који имају фиксирани степен уз неодређену X_n (теорема 77), коначно генерисан, при чему је I коначно генерисан идеал у $R[X_1, \dots, X_n]$ и R Приферов домен димензије један. Постављена су и нека питања, чије би решавање додатно обогатило теорију прстена полинома над ненетериним прстенима.

Глава 1

Основни појмови

Сви прстени који се појављују у тексту су комутативни и са јединицом. Неки од њих ће бити интегрални домени, а неки са делитељима нуле, што ће увек бити наглашено.

1.1 О Гребнеровим базама

Споменути проблем припадности коначно генерисаном идеалу лако се решава када је у питању прстен полинома над пољем K са једном неодређеном X. Знамо да је такав прстен $K[X]$ главноидеалски домен и ако је $I = \langle f_1, \ldots, f_k \rangle \triangleleft K[X]$, тада је

$$f \in I \qquad \Longleftrightarrow \qquad d \,|\, f,$$

где је $d = \text{нзд}(f_1, \ldots, f_k)$. Полином d можемо одредити помоћу Еуклидовог алгоритма. Са друге стране, ако имамо више неодређених или неки прстен уместо поља K, ситуација постаје доста сложенија.

У наредним дефиницијама и теоремама ћемо се ослањати на [1] и [9], при чему се леп приказ може наћи и у [40]. Уведимо прво појам мономног поретка. У случају једне неодређене, мономи су природно поређани тако да

$$1 < X < X^2 < X^3 < \cdots$$

Означимо скуп свих производа од n неодређених $X_1, \ldots, X_n$ са

$$\mathbb{T}^n = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \,|\, \alpha_i \geq 0,\, i \in \{1, \ldots, n\}\}.$$

Потребно је увести уређење на овом скупу које проширује релацију дељивости. Наиме, хоћемо да

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} \,|\, X_1^{\beta_1} \cdots X_n^{\beta_n} \qquad \Longrightarrow \qquad X_1^{\alpha_1} \cdots X_n^{\alpha_n} \leq X_1^{\beta_1} \cdots X_n^{\beta_n}.$$

Дефиниција 1. *Мономни поредак скупа $\mathbb{T}^n$ је линеарно уређење $\leq$ на том скупу при чему важи:*

1. *За све $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \neq 1$ важи да $1 < X_1^{\alpha_1} \cdots X_n^{\alpha_n}$;*
2. *За све $\alpha_i, \beta_i, \gamma_i \geq 0$, где $1 \leq i \leq n$, важи да*

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} < X_1^{\beta_1} \cdots X_n^{\beta_n} \Rightarrow X_1^{\alpha_1} \cdots X_n^{\alpha_n} X_1^{\gamma_1} \cdots X_n^{\gamma_n} < X_1^{\beta_1} \cdots X_n^{\beta_n} X_1^{\gamma_1} \cdots X_n^{\gamma_n}.$$

Може се доказати да је мономни поредак добро уређење на $\mathbb{T}^n$, што значи да у том скупу не постоји бесконачни опадајући низ елемената. Наведимо сада дефиниције лексикографског и степенастог лексикографског поретка.

Дефиниција 2. *Нека су $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ и $X_1^{\beta_1}\cdots X_n^{\beta_n}$ различити производи у $\mathbb{T}^n$. За поредак променљивих $X_1 < X_2 < \cdots < X_n$ дефинишимо лексикографски поредак са:*

$$X_1^{\alpha_1}\cdots X_n^{\alpha_n} < X_1^{\beta_1}\cdots X_n^{\beta_n} \iff \exists i \in \{1,\ldots,n\}(\alpha_i < \beta_i \text{ и } \alpha_j = \beta_j, j > i).$$

Често се овај поредак у литератури означава са $\preccurlyeq_{lex}$, а наредни са $\preccurlyeq_{grlex}$.

Дефиниција 3. *Нека су $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ и $X_1^{\beta_1}\cdots X_n^{\beta_n}$ различити производи у $\mathbb{T}^n$. За поредак променљивих $X_1 < X_2 < \cdots < X_n$ дефинишимо степенасти лексикографски поредак са:*

$$X_1^{\alpha_1}\cdots X_n^{\alpha_n} < X_1^{\beta_1}\cdots X_n^{\beta_n} \iff \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{или} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ и } X_1^{\alpha_1}\cdots X_n^{\alpha_n} \prec_{lex} X_1^{\beta_1}\cdots X_n^{\beta_n}. \end{cases}$$

Може се показати да $\preccurlyeq_{lex}$ и $\preccurlyeq_{grlex}$ задовољавају све услове дефиниције 1. Приметимо да се мономни поредак мења са променом поретка на неодређеним $X_1,\ldots,X_n$.

Уведимо сада важну нотацију.

Дефиниција 4. *Нека је R прстен и нека је задат мономни поредак $>$ на $R[X_1,\ldots,X_n]$. Нека је полином $f \in R[X_1,\ldots,X_n]$. Ако је*

$$f(X_1,\ldots,X_n) = a_1X_1^{\alpha_{11}}\cdots X_n^{\alpha_{1n}} + a_2X_1^{\alpha_{21}}\cdots X_n^{\alpha_{2n}} + \cdots + a_kX_1^{\alpha_{k1}}\cdots X_n^{\alpha_{kn}},$$

где су $a_1,\ldots,a_k$ различити од нуле и тако да

$$X_1^{\alpha_{11}}\cdots X_n^{\alpha_{1n}} > X_1^{\alpha_{21}}\cdots X_n^{\alpha_{2n}} > \cdots > X_1^{\alpha_{k1}}\cdots X_n^{\alpha_{kn}},$$

тада се водећи производ, водећи коефицијент и водећи члан (или водећи моном) полинома f редом дефинишу са:

$$\begin{aligned} &\mathrm{LP}(f) = X_1^{\alpha_{11}}\cdots X_n^{\alpha_{1n}} \\ &\mathrm{LC}(f) = a_1 \\ &\mathrm{LT}(f) = a_1X_1^{\alpha_{11}}\cdots X_n^{\alpha_{1n}}. \end{aligned}$$

У случају прстена полинома са једном неодређеном, ако је $f = a_0 + a_1X + \cdots + a_kX^k$ елемент у $R[X]$, где је $a_k \neq 0$, тада су водећи производ, водећи коефицијент и водећи члан полинома f редом једнаки

$$\mathrm{LP}(f) = X^k, \qquad \mathrm{LC}(f) = a_k, \qquad \mathrm{LT}(f) = a_kX^k.$$

Такође, од значаја је следећи појам.

Дефиниција 5. *Нека је I ненула идеал у прстену $R[X_1, \ldots, X_n]$, са задатим мономним поретком. Нека је*

$$\mathcal{LT}(I) = \{\mathrm{LT}(f) \mid f \in I \setminus \{0\}\}.$$

Тада је

$$\mathrm{LT}(I) = \langle \mathcal{LT}(I) \rangle$$

идеал водећих чланова идеала I. Такође, за било који подскуп $S \subset R[X_1, \ldots, X_n]$, идеал водећих чланова за S је

$$\mathrm{LT}(S) = \langle \mathrm{LT}(f) \mid f \in S \setminus \{0\} \rangle.$$

У случају прстена полинома $K[X]$, где је K поље и ако су $f, g \in K[X]$, где је $g \neq 0$, тада постоје полиноми $q, r \in K[X]$ тако да је $f = qg + r$ и $\deg(r) < \deg(g)$. Полином r називамо остатком при дељењу полинома f са g. Када уместо поља K имамо прстен, није увек могуће извршити наведено дељење. У случајевима када јесте, у наставку овог текста, ознака за остатак при дељењу полинома f са g је

$$\rho(f, g).$$

Када имамо прстен полинома са више неодређених, уводимо појам редукције полинома f у односу на неки коначни скуп полинома. Прво представимо појам редукције полинома f у једном кораку.

Дефиниција 6. *За дате полиноме f и h и скуп ненула полинома $G = \{g_1, \ldots, g_r\}$ који су садржани у $R[X_1, \ldots, X_n]$ кажемо да се f редукује до h по модулу G у једном кораку ако је*

$$h = f - (c_1 \mathcal{X}^{\alpha_1} g_1 + \cdots + c_r \mathcal{X}^{\alpha_r} g_r),$$

где су $c_1, \ldots, c_r \in R$, $\mathcal{X}^{\alpha_1}, \ldots, \mathcal{X}^{\alpha_r} \in \mathbb{T}^n$ и тако да важи:

$$\mathrm{LP}(f) = \mathcal{X}^{\alpha_i} \mathrm{LP}(g_i) \text{ за све } i \text{ где } c_i \neq 0,$$

$$\mathrm{LT}(f) = c_1 \mathcal{X}^{\alpha_1} \mathrm{LT}(g_1) + \cdots + c_r \mathcal{X}^{\alpha_r} \mathrm{LT}(g_r).$$

У том случају, пишемо

$$f \xrightarrow{G} h.$$

Можемо одмах приметити да у овом случају важи и да је $\mathrm{LP}(h) < \mathrm{LP}(f)$.

Дефиниција 7. *За дате полиноме f и h и скуп ненула полинома $G = \{g_1, \ldots, g_r\}$ који су садржани у $R[X_1, \ldots, X_n]$ кажемо да се f редукује до h по модулу G ако постоје полиноми $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ тако да*

$$f \xrightarrow{G} h_1 \xrightarrow{G} h_2 \xrightarrow{G} \cdots \xrightarrow{G} h_t \xrightarrow{G} h.$$

У том случају, пишемо

$$f \xrightarrow{G}_+ h.$$

Уведимо појам полинома који је минималан у односу на коначан скуп полинома и једну карактеризацију тог појма.

Дефиниција 8. *Кажемо да је полином $p \in R[X_1, \ldots, X_n]$ минималан у односу на коначан скуп ненула полинома G ако се не може редуковати по модулу G.*

Лема 9. *Нека је* $p \in R[X_1, \dots, X_n] \setminus \{0\}$*. Тада је* p *минималан у односу на скуп ненула полинома* $G = \{g_1, \dots, g_r\}$ *ако и само ако* $\mathrm{LT}(p) \notin \mathrm{LT}(G)$.

Доказ. Ако p није минималан, може се редуковати по модулу G, па је

$$\mathrm{LT}(p) = c_1\mathcal{X}^{\alpha_1}\mathrm{LT}(g_1) + \cdots + c_r\mathcal{X}^{\alpha_r}\mathrm{LT}(g_r), \text{ где су } c_i \in R,\ \mathcal{X}^{\alpha_i} \in \mathbb{T}^n,\ 1 \le i \le r.$$

Одмах следи да $\mathrm{LT}(p) \in \mathrm{LT}(G)$.

Са друге стране, претпоставимо да је $\mathrm{LT}(p) \in \mathrm{LT}(G)$. Тада је

$$\mathrm{LT}(p) = h_1\mathrm{LT}(g_1) + \cdots + h_r\mathrm{LT}(g_r), \qquad \text{за } h_1, \dots, h_r \in R[X_1, \dots, X_n].$$

Овде се може претпоставити да су h_i мономи, то јест, да су облика $h_i = c_i\mathcal{X}^{\alpha_i}$, за $1 \le i \le r$. Ово управо значи да се p може редуковати до $p - (c_1\mathcal{X}^{\alpha_1}g_1 + \cdots + c_r\mathcal{X}^{\alpha_r}g_r)$, па p није минималан. □

Представимо сада важну теорему која представља аналогон појму дељења са остатком у $K[X]$.

Теорема 10. *Нека је* $f \in R[X_1, \dots, X_n] \setminus \{0\}$ *и* $G = \{g_1, \dots, g_r\}$ *скуп ненула полинома у* $R[X_1, \dots, X_n]$*. Тада постоји полином* p *који је минималан у односу на* G *и за који важи да* $f \xrightarrow{G}_+ p$*. Такође, постоје полиноми* $h_1, \dots, h_r \in R[X_1, \dots, X_n]$ *тако да*

$$f = h_1g_1 + \cdots + h_rg_r + p \qquad и \qquad \mathrm{LP}(f) = max(max_{1\le i\le r}(\mathrm{LP}(h_i)\mathrm{LP}(g_i)), \mathrm{LP}(p)).$$

Доказ. Ако је f минималан у односу на G, тада је јасно тврђење теореме. Ако није, онда се f може редуковати до p_1 и тада је $\mathrm{LP}(f) > \mathrm{LP}(p_1)$. Слично, или је p_1 минималан у односу на G или се може редуковати до p_2. На овај начин добијамо низ редукција

$$f \xrightarrow{G} p_1 \xrightarrow{G} p_2 \xrightarrow{G} \cdots \qquad \text{где важи} \qquad \mathrm{LP}(f) > \mathrm{LP}(p_1) > \mathrm{LP}(p_2) > \cdots$$

Овај процес се мора завршити јер је $<$ добро уређење, што значи да се f редукује до неког полинома p који је минималан у односу на G.

Према дефиницији редукције, важи да

$$f - p_1 = c_1\mathcal{X}^{\alpha_1}g_1 + \cdots + c_r\mathcal{X}^{\alpha_r}g_r, \text{ за } c_i \in R,\ \mathcal{X}^{\alpha_i} \in \mathbb{T}^n,\ 1 \le i \le r.$$

Такође је $\mathrm{LP}(f) = \mathcal{X}^{\alpha_i}\mathrm{LP}(g_i)$ за све индексе i где је c_i ненула, при чему важи једнакост $\mathrm{LT}(f) = c_1\mathcal{X}^{\alpha_1}\mathrm{LT}(g_1) + \cdots + c_r\mathcal{X}^{\alpha_r}\mathrm{LT}(g_r)$. Ако је p_1 минималан, тврђење је доказано. У супротном, имамо да се p_1 редукује до p_2, па је

$$p_1 - p_2 = d_1\mathcal{X}^{\beta_1}g_1 + \cdots + d_r\mathcal{X}^{\beta_r}g_r, \text{ за } d_i \in R,\ \mathcal{X}^{\beta_i} \in \mathbb{T}^n,\ 1 \le i \le r,$$

при чему је $\mathrm{LP}(p_1) = \mathcal{X}^{\beta_i}\mathrm{LP}(g_i)$ за све индексе i где је d_i ненула и где важи једнакост $\mathrm{LT}(p_1) = d_1\mathcal{X}^{\beta_1}\mathrm{LT}(g_1) + \cdots + d_r\mathcal{X}^{\beta_r}\mathrm{LT}(g_r)$. Следи да је

$$f - p_2 = (c_1\mathcal{X}^{\alpha_1} + d_1\mathcal{X}^{\beta_1})g_1 + \cdots + (c_r\mathcal{X}^{\alpha_r} + d_r\mathcal{X}^{\beta_r})g_r.$$

Настављајући на овај начин добијамо тражену репрезентацију за полином f. □

Представимо сада теорему која ће нам омогућити да уведемо појам Гребнерове базе за идеал.

Теорема 11. *Нека је I идеал у $R[X_1, \ldots, X_n]$ и $G = \{g_1, \ldots, g_r\}$ подскуп ненула елемената у I. Тада су следећа тврђења еквивалентна:*

1. $\mathrm{LT}(G) = \mathrm{LT}(I)$;

2. *За било који полином $f \in R[X_1, \ldots, X_n]$ важи да*

$$f \in I \qquad \Longleftrightarrow \qquad f \xrightarrow{G}_+ 0;$$

3. *За сваки полином $f \in I$ важи да је $f = h_1 g_1 + \cdots + h_r g_r$, за неке полиноме $h_1, \ldots, h_r \in R[X_1, \ldots, X_n]$ при чему је $\mathrm{LP}(f) = max_{1 \le i \le r}(\mathrm{LP}(h_i)\mathrm{LP}(g_i))$.*

Доказ. (1) $\Rightarrow$ (2): Ако је $f \xrightarrow{G}_+ 0$, из саме дефиниције редукције видимо да се f може написати помоћу полинома из G, а како је $G \subset I$, следи да $f \in I$.

Са друге стране, претпоставимо да је $f \in I$. Према претходној теореми, $f \xrightarrow{G}_+ p$ и p је минималан у односу на G. Такође, из чињенице да $f, f - p \in I$ следи да $p \in I$, па и $\mathrm{LT}(p) \in \mathrm{LT}(I)$. Ако је $p \neq 0$, тада из леме 9 следи да $\mathrm{LT}(p) \notin \mathrm{LT}(G)$. Ово је контрадикција јер је по претпоставци $\mathrm{LT}(G) = \mathrm{LT}(I)$.

(2) $\Rightarrow$ (3): Следи директно из теореме 10.

(3) $\Rightarrow$ (1): Довољно је доказати да $\mathrm{LT}(f) \in \mathrm{LT}(G)$, за $f \in I$. Из (3) имамо репрезентацију елемента f тако да је $\mathrm{LP}(f) = max_{1 \le i \le r}(\mathrm{LP}(h_i)\mathrm{LP}(g_i))$. Нека је $J \subseteq \{1, \ldots, r\}$ скуп индекса i за које је $\mathrm{LP}(f) = \mathrm{LP}(h_i)\mathrm{LP}(g_i)$. Тада важи да је $\mathrm{LT}(f) = \sum_{i \in J} \mathrm{LT}(h_i)\mathrm{LT}(g_i)$, па $\mathrm{LT}(f) \in \mathrm{LT}(G)$. □

Дефиниција 12. *Скуп ненула полинома $G = \{g_1, \ldots, g_r\}$ је Гребнерова база идеала I у $R[X_1, \ldots, X_n]$ ако важи неки од еквивалентних услова теореме 11.*

Ако се у дефиницији 6 редукција може извршити коришћењем само једног елемента скупа G, тада говоримо о јакој редукцији.

Дефиниција 13. *За дате полиноме f и h и скуп ненула полинома $G = \{g_1, \ldots, g_r\}$ који су садржани у $R[X_1, \ldots, X_n]$ кажемо да се f јако редукује до h по модулу G у једном кораку ако је*

$$h = f - c\mathcal{X}^\alpha g, \qquad \text{за } c \in R,\ \mathcal{X}^\alpha \in \mathbb{T}^n,\ g \in G$$

и тако да важи: $\mathrm{LT}(f) = c\mathcal{X}^\alpha \mathrm{LT}(g)$. У том случају, пишемо

$$f \overset{G}{\twoheadrightarrow} h.$$

Дефиниција 14. *За дате полиноме f и h и скуп ненула полинома $G = \{g_1, \ldots, g_r\}$ који су садржани у $R[X_1, \ldots, X_n]$ кажемо да се f јако редукује до h по модулу G ако постоје полиноми $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ тако да*

$$f \overset{G}{\twoheadrightarrow} h_1 \overset{G}{\twoheadrightarrow} h_2 \overset{G}{\twoheadrightarrow} \cdots \overset{G}{\twoheadrightarrow} h_t \overset{G}{\twoheadrightarrow} h.$$

У том случају, пишемо

$$f \overset{G}{\twoheadrightarrow}_+ h.$$

Представимо сада теорему која ће нам омогућити да уведемо појам јаке Гребнерове базе.

Теорема 15. *Нека је I идеал у $R[X_1, \dots, X_n]$ и G коначан подскуп ненула елемената у идеалу I. Тада су следећа тврђења еквивалентна:*

1. *За сваки полином $f \in I$ постоји $g \in G$ тако да $\mathrm{LT}(g) \,|\, \mathrm{LT}(f)$;*
2. *За било који полином $f \in R[X_1, \dots, X_n]$ важи да*
$$f \in I \qquad \iff \qquad f \overset{G}{\twoheadrightarrow}_+ 0;$$
3. *Важи да је*
$$\{c\mathcal{X}^\alpha \mathrm{LT}(g) \,|\, c \in R,\, \mathcal{X}^\alpha \in \mathbb{T}^n, g \in G\} = \{d\mathcal{X}^\beta \mathrm{LT}(f) \,|\, d \in R,\, \mathcal{X}^\beta \in \mathbb{T}^n, f \in I\}.$$

Доказ. (1) $\Rightarrow$ (2): Ако је $f \overset{G}{\twoheadrightarrow}_+ 0$, тада је свакако и $f \in I$. Са друге стране, за $f \in I$ постоји $g_{i_1} \in G$ тако да $\mathrm{LT}(g_{i_1}) \,|\, \mathrm{LT}(f)$. То значи да за $c \in R$ и $\mathcal{X}^\alpha \in \mathbb{T}^n$ важи једнакост $\mathrm{LT}(f) = c\mathcal{X}^\alpha \mathrm{LT}(g_{i_1})$. Тада је $h_1 = f - c\mathcal{X}^\alpha g_{i_1} \in I$. Свакако је $\mathrm{LP}(f) > \mathrm{LP}(h_1)$. Ако је $h_1 \neq 0$, тада постоји $g_{i_2} \in G$ тако да $\mathrm{LT}(g_{i_2}) \,|\, \mathrm{LT}(h_1)$. Дакле, $h_2 = h_1 - d\mathcal{X}^\beta g_{i_2} \in I$ и можемо наставити овај процес:

$$f \overset{G}{\twoheadrightarrow} h_1 \overset{G}{\twoheadrightarrow} h_2 \overset{G}{\twoheadrightarrow} \cdots \qquad \text{и} \qquad \mathrm{LP}(f) > \mathrm{LP}(h_1) > \mathrm{LP}(h_2) > \cdots$$

Следи да постоји природан број k тако да је $h_k = 0$ и онда имамо да је $f \overset{G}{\twoheadrightarrow}_+ 0$.

(2) $\Rightarrow$ (3): Јасно је да је лева страна садржана у десној. Ако је $f \in I$, тада се f може јако редуковати у једном кораку. Тако да постоје $c \in R$, $\mathcal{X}^\alpha \in \mathbb{T}^n$ и $g \in G$ тако да $h = f - c\mathcal{X}^\alpha g$ и $\mathrm{LT}(f) = c\mathcal{X}^\alpha \mathrm{LT}(g)$. Ово значи да је $\mathrm{LT}(f)$ садржано у скупу са леве стране.

(3) $\Rightarrow$ (1): За $f \in I$ постоји моном $c\mathcal{X}^\alpha$ тако да $\mathrm{LT}(f) = c\mathcal{X}^\alpha \mathrm{LT}(g)$, за неко $g \in G$. Тада је и $\mathrm{LT}(g) \,|\, \mathrm{LT}(f)$. □

Дефиниција 16. *Скуп ненула полинома $G = \{g_1, \dots, g_r\}$ је јака Гребнерова база идеала I у $R[X_1, \dots, X_n]$ ако важи неки од еквивалентних услова теореме 15.*

Уведимо и појам минималне јаке Гребнерове базе идела I.

Дефиниција 17. *Јака Гребнерова база $G = \{g_1, \dots, g_r\}$ за идеал I у $R[X_1, \dots, X_n]$ је минимална ако за све $i \neq j$ важи да $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$.*

Приметимо како се једноставно може доказати да за сваки идеал над Нетериним прстеном постоји Гребнерова база.

Теорема 18. *Нека је I ненула идеал у $R[X_1, \dots, X_n]$, где је домен R Нетерин. Тада постоји Гребнерова база за I.*

Доказ. Како је и $R[X_1, \dots, X_n]$ Нетерин прстен, идеал I је коначно генерисан. Нека је $G = \{g_1, \dots, g_r\}$ скуп тих генератора. Ако је $\mathrm{LT}(G) = \mathrm{LT}(I)$, према теореми 11, G је Гребнерова база за I. У супротном је $\mathrm{LT}(G) \subset \mathrm{LT}(I)$. Ако би било $\mathrm{LT}(f) \in \mathrm{LT}(G)$, за свако $f \in I$, тада би ови скупови били заправо једнаки. Тако да постоји $f \in I$ при чему је $\mathrm{LT}(f) \notin \mathrm{LT}(G)$. Нека је $g_{r+1} = f$. Посматрајмо скуп $G_1 = G \cup \{g_{r+1}\}$. Због претходног услова важи да је

$$\mathrm{LT}(G) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_r) \rangle \subset \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_{r+1}) \rangle = \mathrm{LT}(G_1).$$

Ако је $\mathrm{LT}(G_1) = \mathrm{LT}(I)$, тада је G_1 Гребнерова база за I. У супротном можемо наставити овај поступак. На овај начин добићемо строго растући низ идеала у $R[X_1, \ldots, X_n]$ који мора бити стационаран. Дакле, постоји $s \geq 1$ тако да је $\mathrm{LT}(G_s) = \mathrm{LT}(I)$, па је скуп $G \cup \{g_{r+1}, \ldots, g_{r+s}\}$ Гребнерова база за I. □

За крај овог одељка, можемо представити терминологију која се појављује у литератури везано за Гребнерове базе над прстенима (видети [43]).

Дефиниција 19. *Прстен R је n-Гребнеров, где је $n \geq 1$, ако за сваки коначно генерисани идеал I у $R[X_1, \ldots, X_n]$ и сваки мономни поредак на прстену полинома, идеал водећих чланова $\mathrm{LT}(I)$ је коначно генерисан. Прстен R је Гребнеров, ако је n-Гребнеров за свако $n \geq 1$.*

Постављена је хипотеза, на пример, да је сваки једнодимензиони валуациони домен Гребнеров. Аутор у [42] спомиње да је у претходној дефиницији довољно разматрати лексикографки поредак и поставља хипотезу да се за одређене класе прстена из доказа за лексикографски поредак може закључити да наведени услов важи за сваки мономни поредак. Више о овој теми биће представљено у глави 7.

Користећи споменуту терминологију, у главама 2, 3, 4 и 5, представљени су докази да су једнодимензиони валуациони домен, нуладимензиони валуациони прстен у коме је анулатор сваког елемента коначно генерисан, једнодимензиони Приферов домен и фон Нојман регуларни прстен 1-Гребнерови прстени.

1.2 Остали појмови и дефиниције

Идеалу I у прстену $R[X]$ можемо придружити модуле над R који добро описују водеће чланове елемената идеала у одређеном степену.

Дефиниција 20. *Нека је $R[X]_k$ ознака за R-подмодул у $R[X]$ који је генерисан са $1, X, X^2, \ldots, X^k$. Тада је R-подмодул*

$$I_k = I \cap R[X]_k, \qquad \text{за } k \geq 0,$$

асоцирани модул идеала I.

За идеал I у $R[X]$ асоцирани R-модул I_k садржи све полиноме из I који су степена највише k. Овај појам биће нарочито користан у главама 2, 3 и 5. У глави 4 појавиће се појам асоцираног идеала, али неће бити конфузије око ова два појма.

Представимо дефиниције НЗД и Безуовог домена (видети [16]).

Дефиниција 21. *Интегрални домен R је НЗД домен ако свака два елемента у R имају највећи заједнички делилац.*

У терминима идеала, може се рећи да је домен НЗД ако за свака два елемента постоји минимални главни идеал који садржи идеал генерисан са та два елемента. За сваки НЗД домен, важи да је и $R[X_1, \ldots, X_n]$ НЗД домен (видети [3]). За случај једне неодређене и валуационог домена V, у глави 2 представићемо и доказ ове чињенице.

Дефиниција 22. *Интегрални домен R је Безуов домен ако је у њему сваки коначно генерисани идеал главни.*

Сваки Безуов домен је и НЗД домен. У Безуовом домену, сем највећег заједничког делиоца елемената a и b, постоји и релација: $ax + by = \text{нзд}(a, b)$.

Подсетимо се сада дефиниције Крулове димензије прстена, као и појмова екстензије и контракције идеала (видети, на пример, [7]).

Дефиниција 23. *Нека је R прстен и*

$$P_0 \subset P_1 \subset \cdots \subset P_n$$

строго растући низ простих идеала у R. Кажемо да овакав ланац има дужину n. Крулова димензија прстена R је супремум дужина свих ланаца простих идеала у овом прстену.

У овом тексту под димензијом прстена увек ћемо мислити на Крулову димензију. Да је Крулова димензија прстена нула, значи да је сваки прости идеал и максималан. Ако је D интегрални домен, важи да је димензија за D нула ако и само ако је D поље. За интегрални домен D важи и да је $\langle 0 \rangle$ прост идеал у D. Ако је D димензије један, тада такође важи да је сваки ненула прости идеал у D и максималан.

Нека је $A \subseteq B \subseteq C$ низ раширења интегралних домена и нека је I идеал у B. Користићемо стандардну нотацију за контракцију и екстензију идеала I. Наиме, контракција за I је $I^c = I \cap A$, а екстензија $I^e = CI$.

За крај споменимо неке ознаке које ће бити коришћене у тексту. Џејкобсонов радикал и нилрадикал прстена R биће означени са $\mathrm{J}(R)$ и $\mathrm{Nil}(R)$, редом. Скуп инвертибилних елемената прстена R је $\mathrm{U}(R)$. Анулатор R-модула M је $\mathrm{Ann}(M)$, а нарочито ћемо користити ознаку за анулатор елемента a у прстену R:

$$\mathrm{Ann}(a) = \{b \in R \mid ab = 0\}.$$

Глава 2

Валуациони домени димензије 1

2.1 Дефиниција и основне особине

О валуационим доменима се често говори као о полазној тачки при изучавању нетериних домена. Разлог томе је што су најједноставнији за изучавање од свих класа домена који нису Нетерини. Иако је појам валуације уведен раније, као валуациони домени спомињу се у [28], док се исцрпна теорија може наћи у [18] и [19].

Уведимо прво сам појам валуационог домена. Постоји више начина на које се може дефинисати овај појам, а у случају резултата који ће бити представљени, најоперативнија дефиниција је наредна.

Дефиниција 24. *Прстен V је валуациони ако за све $a, b \in V \setminus \{0\}$ важи да*

$$a \mid b \qquad \textit{или} \qquad b \mid a.$$

Интегрални домен који је валуациони прстен се назива валуациони домен.

Еквивалентно, домен V је валуациони ако

$$a \in V \qquad \text{или} \qquad a^{-1} \in V,$$

где је a било који елемент поља разломака K за V. Оваква дефиниција омогућава да се при одређеним рачунима формирају две гране, за две могуће релације, и да се потом рачун настави засебно. То је посебно корисно у неким динамичким техникама које се користе у конструктивној алгебри (видети, на пример, [43] и [23]). Валуациони домен се може дефинисати и преко одређеног пресликавања v, валуације, али овде се нећемо бавити том терминологијом (видети [18]). Можемо само рећи да ће за два елемента a и b валуационог домена важити да $a \mid b$ ако и само ако је $v(a) \leq v(b)$. За специјално дефинисано v добијамо дискретне валуационе домене, који заправо представљају Нетерине валуационе домене и чешће се срећу у литератури.

Наведимо неке од важних особина валуационих домена. Интегрално су затворени и сваки натпрстен од V који је садржан у пољу разломака за V је такође валуациони домен. Важи и следеће: ако је R интегрални домен и K његово поље разломака, тада је интегрално затворење $\bar{R}$ једнако

$$\bar{R} = \bigcap_{R \subseteq V \subseteq K} V,$$

где су V валуациони домени. Затим, идеали од V су тотално уређени инклузијом. Имамо и једну важну карактеризацију: домен V је валуациони ако и само ако је локални и Безуов прстен.

Нека је $A = \{a_1, \ldots, a_s\}$ коначан скуп елемената валуационог прстена V. Примењујући претходну дефиницију индуктивно на овај скуп, можемо закључити да постоји индекс $i \in \{1, \ldots, s\}$ такав да a_i дели све елементе датог скупа A. Ову чињеницу ћемо често користити. Важно је напоменути и да одавде једноставно следи да је у валуационом прстену сваки коначно генерисани идеал главни.

Следећа три тврђења су добро позната, али ћемо укључити њихове доказе ради комплетности.

Тврђење 25. *Сваки валуациони прстен је локални.*

Доказ. Нека је M неки максимални идеал. Докажимо да је тада M једини максимални идеал у V. Ако је $a \in V \setminus M$, тада је $\langle M, a\rangle = V$. Следи да постоје елементи $m \in M$ и $b \in V$ тако да $m + ab = 1$. Ако би за елемет m важило да $m \,|\, a$, тада би m био инвертибилан. Следи да $a \,|\, m$ и тада је a инвертибилан. □

Максимални идеал у V ћемо означавати са M. Дефинишимо прво појам примитивног полинома.

Дефиниција 26. *Нека је R прстен. Полином $p \in R[X]$ је примитиван ако има бар један инвертибилан коефицијент.*

За два примитивна полинома над валуационим доменом важи следећа лема.

Лема 27. *Нека је V валуациони домен. Производ примитивних полинома у $V[X]$ је примитивни полином.*

Доказ. Нека су f и g примитивни полиноми у $V[X]$. Како и f и g имају коефицијент који је инвертибилан, следи да $f, g \notin M[X]$. Идеал $M[X]$ је прост у $V[X]$, што повлачи да $fg \notin M[X]$. Ово значи да је неки коефицијент полинома fg инвертибилан, па је fg примитиван. □

Очигледно је да је валуациони домен и НЗД домен, па се може доказати следећа теорема.

Теорема 28. *Нека је V валуациони домен. Тада је $V[X]$ НЗД домен.*

Доказ. Нека су $f, g \in V[X]$ и K је поље разломака за V. Пошто су сви елементи у V међусобно упоредиви, постоји коефицијент a полинома f који дели све његове коефицијенте. Следи да је $f = af_1$, где је f_1 полином са једним коефицијентом једнаким 1. На сличан начин је $g = bg_1$, где g_1 има један коефицијент једнак 1.

Можемо прво одредити највећи заједнички делилац за полиноме f_1 и g_1. Како је $K[X]$ главноидеалски домен, постоји полином $d_1 \in K[X]$ који је такав да $d_1 = \text{нзд}(f_1, g_1)$. Имамо да је

$$\begin{array}{rcl} f_1 & = & d_1 f_2 \\ g_1 & = & d_1 g_2 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} f_1 & = & \alpha d_1' \cdot \beta f_2' \\ g_1 & = & \alpha d_1' \cdot \gamma g_2', \end{array}$$

где су d_1', f_2', g_2' примитивни полиноми у $V[X]$ и $\alpha, \beta, \gamma \in K$. Према леми 27, производи $d_1'f_2'$ и $d_1'g_2'$ су примитивни, тако да су производи $\alpha\beta, \alpha\gamma$ заправо у $\mathrm{U}(V)$. Имаћемо овакве релације у $V[X]$:

$$\begin{aligned} f_1 &= d_1'f_2'', \qquad & f_2'' &= \alpha\beta f_2' \\ g_1 &= d_1'g_2'', \qquad & g_2'' &= \alpha\gamma g_2'. \end{aligned}$$

Нека је $\bar{d} \in V[X]$ заједнички делилац за f_1 и g_1. Да бисмо доказали да важи да $d_1' = \text{нзд}(f_1, g_1)$ у $V[X]$, довољно је показати да $\bar{d} \mid d_1'$. Елемент $\bar{d}$ је такође заједнички делилац за f_1 и g_1 у $K[X]$, па следи да $\bar{d} \mid d_1$. Пошто је $d_1 = \alpha d_1'$, имамо да $\bar{d} \mid d_1'$ у $K[X]$. Нека је $d_1' = \bar{d}h$, за $h \in K[X]$. Тада важи да

$$d_1' = \bar{d}\delta h_1, \qquad \delta \in K,$$

и $h_1 \in V[X]$ је примитиван. Полином $\bar{d}$ је примитиван, јер је делилац примитивних полинома f_1 и g_1. Дакле, како су $\bar{d}h_1$ и d_1' примитивни, следи да је δ инвертибилан у V, па $\bar{d}$ дели d_1' у $V[X]$.

Приметимо да у $V[X]$ важи следећа еквиваленција:

$$ap \mid bq \qquad \Leftrightarrow \qquad a \mid b, \ p \mid q,$$

за $a, b \in V$ и примитивне полиноме $p, q \in V[X]$. Једна импликација је очигледна. Што се тиче друге, нека је

$$bq = apct, \qquad \text{где } c \in V \text{ и где је } t \in V[X] \text{ примитиван.}$$

Пошто су pt и q примитивни, следи да се b и ac разликују до на производ са инвертибилним елементом. Закључујемо да $a \mid b$, а самим тим и $p \mid q$.

Докажимо коначно да

$$\text{нзд}(f, g) = \text{нзд}(a, b)\text{нзд}(f_1, g_1).$$

Нека је t заједнички делитељ за f и g. Тада је $t = ct_1$, где је t_1 примитиван. С обзиром на то да $ct_1 \mid af_1$ и $ct_1 \mid bg_1$, следи да c дели a и b, као и да t_1 дели f_1 и g_1, чиме завршавамо доказ. □

2.2 Гребнерова база

Докажимо да се у случају валуационих прстена, а самим тим и валуационих домена, појмови Гребнерове базе и јаке Гребнерове базе заправо подударају.

Тврђење 29. *Нека је $G = \{g_1, \ldots, g_r\}$ Гребнерова база за идеал I у $V[X]$, где је V валуациони прстен. Тада је G такође јака Гребнерова база за I.*

Доказ. Нека је $f \in I$. Како је G Гребнерова база, то постоје полиноми $p_1(X), \ldots, p_r(X)$ такви да

$$\mathrm{LT}(f) = p_1(X)\mathrm{LT}(g_1) + \cdots + p_r(X)\mathrm{LT}(g_r).$$

Нека су

$$p_i(X) = b_0^{(i)} + b_1^{(i)}X + \cdots + b_{s_i}^{(i)}X^{s_i}, \qquad i \in \{1, \ldots, r\},$$

као и $\mathrm{LT}(g_i) = a_i X^{n_i}$, за $i \in \{1, \ldots, r\}$ и $\mathrm{LT}(f) = aX^n$. Следи да је

$$aX^n = \sum_{i=1}^{r} \sum_{j=0}^{s_i} a_i X^{n_i} b_j^{(i)} X^j.$$

Према томе, за неки подскуп $K \subseteq \{1, \ldots, r\}$, важи да

$$aX^n = \sum_{k \in K} a_k X^{n_k} b_{n-n_k}^{(k)} X^{n-n_k} = \left(\sum_{k \in K} a_k b_{n-n_k}^{(k)} \right) X^n.$$

Можемо закључити да је

$$a = \sum_{k \in K} a_k b_{n-n_k}^{(k)}.$$

Пошто је V валуациони прстен, постоји $k_0 \in K$ тако да $a_{k_0} \mid a_k$ за све $k \in K$. Тада имамо да је $a_{k_0} X^{n_{k_0}} \mid aX^n$, чиме је тврђење доказано. $\square$

У [32] доказано је да за валуациони домен димензије 1 и коначно генерисани идеал $I \triangleleft V[X]$ важи да је идеал водећих чланова $\mathrm{LT}(I)$ коначно генерисан. У том раду користе се одређене методе, као и особине кохерентних и Безуових прстена. Са друге стране, закључивање коришћено за резултат теореме 35, где је доказано постојање минималне јаке Гребнерове базе за идеал I у $V[X]$, при чему је $\dim(V) = 1$, омогућава и одређивање Гребнерове базе за дати идеал. Кроз леме које претходе наведеној теореми и њихове доказе се могу увидети начини на који се та база може одредити, а процедура је илустрована и у примеру 36. Сви резултати представљени у наставку ове главе настали су у току целокупног процеса бављења тематиком коначне генерисаности за $\mathrm{LT}(I)$, где је I идеал у $R[X]$.

Наредна лема, иако једноставна, биће од изузетног значаја у тексту који следи. У њој започињемо разматрање коначне генерисаности асоцираних модула I_k за идеал $I \triangleleft R[X]$.

Лема 30. *Нека је R прстен и I идеал у $R[X]$. Ако је I генерисан полиномима $f, f_1, \ldots, f_s$, где је f моничан полином степена n, тада је асоцирани модул I_{n-1} коначно генерисан R-модул.*

Доказ. Ако је $I = \langle f \rangle$, то јест, ако је $s = 0$, тада је $I_{n-1} = \{0\}$. Ако није, докажимо да тада остаци при дељењу полинома $X^t f_i$ са f, заправо скуп елемената

$$\rho(X^t f_i, f), \qquad \text{где је} \qquad 0 \le t \le n-1, \qquad 1 \le i \le s,$$

генерише I_{n-1}.

Нека је $g \in I_{n-1}$. Пошто је $g \in I$, имамо да

$$g = hf + h_1 f_1 + \cdots + h_s f_s, \tag{2.1}$$

за неке $h, h_1, \ldots, h_s \in R[X]$. За $1 \le i \le s$ важи да је $h_i = q_i f + h_i'$, где је $\deg h_i' < n$. Према томе, важи да је

$$g = (h + q_1 f_1 + \cdots + q_s f_s) f + h_1' f_1 + \cdots + h_s' f_s.$$

Одавде следи да можемо претпоставити да $\deg h_1, \deg h_2, \ldots, \deg h_s < n$ у једнакости (2.1). Нека је сада

$$h_i = \sum_{t=0}^{k_i} \alpha_t^{(i)} X^t, \qquad k_i < n, \qquad 1 \le i \le s,$$

$$X^t f_i = f r_t^{(i)} + \rho(X^t f_i, f), \qquad 0 \le t \le k_i, \qquad 1 \le i \le s.$$

Заменом у једнакост (2.1) добијамо следеће:

$$g = f\left(h + \sum_{i=1}^{s}\sum_{t=0}^{k_i} \alpha_t^{(i)} r_t^{(i)}\right) + \sum_{i=1}^{s}\sum_{t=0}^{k_i} \alpha_t^{(i)} \rho(X^t f_i, f).$$

Имамо сада да је полином g облика $fp+q$, где је $p \in R[X]$ и q је R-линеарна комбинација полинома $\rho(X^t f_i, f)$, за $0 \le t \le k_i$. Пошто је $g \in I_{n-1}$, тада је $\deg(g) < n$. Како је полином f моничан, можемо закључити да је $p = 0$. Такође из

$$\rho(X^t f_i, f) = X^t f_i - f r_t^{(i)}$$

следи да $\rho(X^t f_i, f)$ припада идеалу I, па самим тим припада и I_{n-1}. Видимо сада да се полином g изражава као R-линеарна комбинација полинома $\rho(X^t f_i, f)$, за $0 \le t \le n-1$, $1 \le i \le s$, чиме смо доказали тврђење леме. $\square$

Наставимо испитивање коначне генерисаности асоцираних модула. У следећој леми, уместо произвољног прстена R, мораћемо да претпоставимо да је у питању валуациони домен.

Лема 31. *Нека је V валуациони домен и I идеал у $V[X]$ који је генерисан полиномима $f, f_1, \ldots, f_s$, при чему је f моничан полином степена n. Тада су $I_{n-2}, I_{n-3}, \ldots, I_0$ коначно генерисани V-модули.*

Доказ. Претпоставимо да је $I \neq \langle f \rangle$, тако да $I_{n-1} \neq \{0\}$. Нека су

$$\pi_k : V[X]_k \to V, \text{ за } 0 \le k \le n-1,$$

хомоморфизми V-модула такви да је $\pi_k(p)$ коефицијент у полиному p уз производ X^k. Према леми 30, V-модул I_{n-1} је коначно генерисан. Следи да је слика $\pi_{n-1}(I_{n-1})$ такође коначно генерисан подмодул од V, то јест, коначно генерисан идеал. Пошто је V валуациони домен, ова слика заправо мора бити главни идеал $\pi_{n-1}(I_{n-1}) = \langle c_{n-1} \rangle$. Приметимо да $c_{n-1} \neq 0$. Да бисмо доказали да су наведени модули I_k коначно генерисани, посматраћемо кратак тачан низ

$$0 \longrightarrow I_{n-2} \longrightarrow I_{n-1} \xrightarrow{\pi_{n-1}} \langle c_{n-1} \rangle \to 0.$$

Прво пресликавање је инклузија. Пошто је изоморфан са V, модул $\langle c_{n-1} \rangle$ је слободан, па се овај низ цепа. Следи да је

$$I_{n-1} \cong I_{n-2} \times \langle c_{n-1} \rangle.$$

Из цепања низа имамо и пројекцију $\pi : I_{n-1} \to I_{n-2}$. Одавде следи да је модул I_{n-2} коначно генерисан, јер је то и I_{n-1}. Ако је $I_{n-2} \neq \{0\}$, настављамо на исти начин, помоћу формирања кратког тачног низа. Тако да можемо закључити да су сви модули $I_{n-2}, I_{n-3}, \ldots, I_0$ (који су ненула) коначно генерисани, као и да за све $k \in \{0, \ldots, n-2\}$ важи да

$$I_k \cong \langle c_k \rangle \times \cdots \times \langle c_0 \rangle \cong V^l,$$

за неко $l \le k+1$ (ако је $c_t = 0$, тада је такође и $c_m = 0$ за $m < t$).

Можемо чак одредити и генераторе за V-модул I_k, на исти начин на који смо то урадили за I_{n-1} у леми 30. Пођимо од модула I_{n-2}. За $g \in I_{n-2} \subseteq I_{n-1}$, важи да се може представити као збир
$$g = \sum r_{ti}\rho(X^t f_i, f),$$
где су $r_{ti} \in V$ и $\rho(X^t f_i, f)$ као у доказу претходне леме. Пошто су сви остаци $\rho(X^t f_i, f)$ елементи у I_{n-1}, можемо их поделити са h_{n-1}, полиномом таквим да је водећи коефицијент од h_{n-1} управо генератор за $\pi_{n-1}(I_{n-1})$, то јест, таквим да $\mathrm{LT}(h_{n-1}) = c_{n-1}X^{n-1}$. Према томе, важи да је
$$\rho(X^t f_i, f) = a_{ti}h_{n-1} + f_{ti}, \qquad \text{за све } 0 \leq t \leq n-1,\ 1 \leq i \leq s.$$
Приметимо да се може десити да је $a_{ti} = 0$. Коначно, имамо да је
$$g = \sum r_{ti}(a_{ti}h_{n-1} + f_{ti}) = \left(\sum r_{ti}a_{ti}\right) h_{n-1} + \sum r_{ti}f_{ti}.$$
Како је V интегрални домен, $\deg(h_{n-1}) = n-1$ и $\deg(\sum r_{ti}f_{ti}) \leq n-2$, следи да $\sum r_{ti}a_{ti} = 0$ и $g = \sum r_{ti}f_{ti}$. Тако да сваки елемент у I_{n-2} може бити представљен као V-линеарна комбинација елемената
$$f_{ti} = \rho(\rho(X^t f_i, f), h_{n-1}), \qquad \text{где } 1 \leq i \leq s,\ 0 \leq t \leq n-1.$$
Поступак је исти за $I_{n-3}, \dots, I_0$. $\square$

Следећа лема ће нам бити значајна у будућем испитивању минималности јаке Гребнерове базе.

Лема 32. *Нека је V валуациони домен и I идеал у $V[X]$ који је генерисан полиномима $f_1, \dots, f_s$. Ако I садржи моничан полином, тада постоји коначни подскуп $B \subset \mathcal{LT}(I)$ тако да*

1. $(\forall g \in I)(\exists b \in B)\ b \mid \mathrm{LT}(g)$;
2. $(\forall b_1, b_2 \in B)(b_1 \neq b_2 \Rightarrow b_1 \nmid b_2)$.

Доказ. Нека је $f \in I$ моничан полином и претпоставимо да је $\deg(f) = n$. Можемо формирати скуп B на следећи начин: нека је $X^n \in B$. Из претходне леме имамо да
$$\pi_k(I_k) = \langle c_k \rangle, \qquad \text{за } 0 \leq k \leq n-1,$$
при чему су елементи c_k јединствени, до на производ са инвертибилним елементом. Ако је c_kX^k ненула, нека је тада $c_kX^k \in B$, за све $0 \leq k \leq n-1$. Такође, ако се деси да за неко $l > k$ важи да $c_k \mid c_l$, тада можемо искључити елемент c_lX^l из B.

Јасно је да B задовољава тражене услове. Наиме, ако је g полином из I такав да је $\deg(g) = m \geq n$, тада $X^n \mid \mathrm{LT}(g)$. Ако је $\deg(g) = m < n$, тада је $c_kX^k \mid \mathrm{LT}(g)$, за неко $k \leq m$. $\square$

Наредни резултат ће нам бити користан у леми 34.

Лема 33. *Нека је $A \subseteq B \subseteq C$ низ раширења интегралних домена и нека је I идеал у домену B. Ако за сваки елемент $c \in C$ постоји $a \in A \setminus \{0\}$ тако да $ac \in B$ и ако је $I^e \cap A \neq \{0\}$, тада је $I^c \neq \{0\}$.*

Доказ. Како је $I^e \cap A \neq \{0\}$, то постоје елементи $\bar{a} \in A \setminus \{0\}$, $c_1, \dots, c_s \in C$ и $f_1, \dots, f_s \in I$ за које је

$$c_1 f_1 + \cdots + c_s f_s = \bar{a}.$$

Нека је за свако $1 \leq i \leq s$ елемент $a_i \in A \setminus \{0\}$ такав да $a_i c_i \in B$. Тада, за елемент $a = a_1 \cdots a_s \in A \setminus \{0\}$ имамо да важи једнакост $a\bar{a} = ac_1 f_1 + \cdots + ac_s f_s$. Пошто је

$$ac_i = a_i c_i \cdot \frac{a}{a_i} \in B,$$

а $f_1, \dots, f_s \in I$, следи да $a\bar{a} \in I$. Како је и $a\bar{a} \in A$, следи да је $a\bar{a}$ ненула елемент у I^c. □

Видимо да је у лемама 30, 31 и 32 тражено да идеалу који се посматра припада моничан полином. Следећа лема се бави питањем постојања тог моничног полинома. Претпоставка леме ће бити и да је валуациони домен димензије 1.

Нека су $f_1, \dots, f_s \in V[X]$, где је V валуациони домен и нзд$(f_1, \dots, f_s)$ је једнак 1. Јасно је да тада бар један од полинома f_i има бар један инвертибилан коефицијент. У супротном, највећи заједнички делилац тих полинома не би био једнак 1. Ова чињеница нам је потребна за саму формулацију наредне леме.

Лема 34. *Нека је $I = \langle f_1, \dots, f_s \rangle$ идеал у $V[X]$, где је V валуациони домен димензије 1, такав да је $s \geq 2$ и нзд$(f_1, \dots, f_s) = 1$. Нека је $f_i = \sum_j a_{ij} X^j$ и нека је*

$$k = \min\{l \in \mathbb{N} \mid (\exists i \in \{1, \dots, s\})(a_{il} \in \mathrm{U}(V) \text{ и } (\forall j > l) a_{ij} \notin \mathrm{U}(V))\}.$$

Тада постоји моничан полином f у I степена k.

Доказ. Прво докажимо да је $I^c = I \cap V \neq \{0\}$. Без умањења општости, можемо претпоставити да је индекс i који се појављује у дефиницији броја k једнак 1, као и да је тај инвертибилни елемент $a_{ik} = a_{1k}$ заправо једнак 1. Ако је f_1 моничан, нема шта да се доказује. Претпоставимо да није моничан. Тада је f_1 збир моничног полинома и полинома чији су сви коефицијенти у максималном идеалу M (неинвертибилни елементи), и кога можемо видети као производ елемента из M и полинома чији један коефицијент је једнак 1. Следи да је

$$f_1(X) = bp(X) + q(X), \qquad b \in M,\ q \text{ моничан у } V[X] \text{ и степена } k.$$

Највећи заједнички делилац полинома $f_1, \dots, f_s$ је 1 у $V[X]$, па то важи и у $K[X]$, где је K поље разломака за V. Уочимо низ

$$V \subset V[X] \subset K[X],$$

за који очигледно важи први део претпоставке из леме 33. Такође, како је $K[X]$ главноидеалски домен и нзд$(f_1, \dots, f_s) = 1$, следи да је $I^e = K[X]$, то јест, $I^e \cap V \neq \{0\}$. Из леме 33 можемо сада закључити да је $I^c \neq \{0\}$. Нека је $d \in I^c$ ненула, тада је и Vd ненула идеал у V. Његов радикал је пресек простих идеала који садрже d, а како је V интегрални домен димензије 1, тај пресек је једнак M. Тако да је $b \in M = \sqrt{Vd}$. Одатле следи да постоји $m \in \mathbb{N}$ тако да

$$b^m \in Vd \subseteq I^c \subseteq I,$$

то јест, $b \in \sqrt{I}$. Такође је

$$q(X) = f_1(X) - bp(X) \in \sqrt{I},$$

тако да постоји моничан полином у I (наиме, јасно је да ако $b^m \in I$, тада је $q(X)^m \in I$).

Покажимо сада да постоји моничан полином степена k у I. Поделимо полином $X^t f_1$ овим моничним полиномом q^m, где је $t = (m-1)k - 1$. Сада је коефицијент уз производ $X^t X^k = X^{mk-1}$ у полиному $X^t f_1$ једнак 1 и делимо моничним полиномом q^m, који је степена mk. Сви коефицијенти у полиному $X^t f_1$ који су уз степен већи од $mk-1$ су у идеалу M, тако да је количник у овом дељењу такође умножак неког елемента који припада M. Водећи коефицијент остатка је онда облика $1-\mu$, где је $\mu \in M$, а самим тим је и инвертибилан. Тако да смо доказали да I садржи моничан полином степена $mk-1$. Можемо поновити овај поступак:

$$\begin{aligned}
X^t f_1 &= q^m q_1 + r_1 \\
X^{t-1} f_1 &= r_1 q_2 + r_2 \\
&\vdots \\
X^2 f_1 &= r_{t-2} q_{t-1} + r_{t-1} \\
X f_1 &= r_{t-1} q_t + r_t \\
f_1 &= r_t q_{t+1} + r_{t+1}.
\end{aligned}$$

Овде имамо да $r_i \in I$, $\deg(r_i) = mk - i$ и иако ови полиноми нису монични, њихови водећи коефицијенти су инвертибилни. Следи да је r_{t+1} полином у I степена k чији водећи коефицијент је инвертибилан. Ово значи да постоји моничан полином у I који је степена k, чиме завршавамо доказ. $\square$

Сада можемо прећи на доказ главне теореме која говори о постојању Гребнерове базе за коначно генерисани идеал у $V[X]$, где је V валуациони домен димензије 1.

Теорема 35. *Нека је V валуациони домен димензије 1. Ако је I ненула коначно генерисани идеал у $V[X]$, тада постоји минимална јака Гребнерова база за I.*

Доказ. Нека је $I = \langle f_1, \dots, f_s \rangle$. Према теореми 28, постоји полином $d = \text{нзд}(f_1, \dots, f_s)$ у прстену $V[X]$. Нека је $f_i = d a_i$, и тада је

$$I = d\langle a_1, \dots, a_s \rangle.$$

Сада се можемо сконцентрисати на идеал $J = \langle a_1, \dots, a_s \rangle$.

Пошто је $\text{нзд}(a_1, \dots, a_s) = 1$, према леми 34, идеал J садржи моничан полином. Нека је n степен тог полинома. На основу леме 32 следи да постоји скуп

$$B = \{b_1, \dots, b_r\} \subset \mathcal{LT}(J)$$

такав да за било које $a \in J$ постоји $k \in \{1, \dots, r\}$ такво да $b_k \mid \mathrm{LT}(a)$. Према томе, ако је $h_k \in J$ полином такав да $\mathrm{LT}(h_k) = b_k$ и ако означимо $g_k = d h_k$, можемо закључити да је $G = \{g_1, \dots, g_r\}$ минимална јака Гребнерова база за I.

Наиме, ако $f \in I$ тада је $f = da$ за неко $a \in J$. Ако $\mathrm{LT}(h_k) \mid \mathrm{LT}(a)$, тада је очигледно да $\mathrm{LT}(g_k) \mid \mathrm{LT}(f)$. $\square$

Представимо сада један пример валуационог домена Крулове димензије 1 који није Нетерин. Такође, на примеру једног идеала над овим прстеном можемо илустровати претходне леме и теореме, као и поступак одређивање Гребнерове базе за тај идеал.

Пример 36. Нека је прстен R задат на следећи начин:

$$R = \mathbb{Q}[X_1, X_2, X_3, \dots]/\langle X_2^2 - X_1, X_3^2 - X_2, \dots\rangle.$$

Посматрајмо локализацију R_M овог прстена у односу на максимални идеал

$$M = \langle x_1, x_2, \dots\rangle,$$

где је x_i ознака за класу елемента X_i у R.

Приметимо да је сваки елемент у R облика $f(x_m)$ за неки полином f са рационалним коефицијентима и за неко $m \in \mathbb{N}$. Наиме, за $r \in R$, видимо да је $r = g(x_1, \dots, x_m)$. Како у R важе релације

$$x_1 = x_2^2 = \dots = x_m^{2^{m-1}},$$

следи да је

$$r = g(x_m^{2^{m-1}}, \dots, x_m) = f(x_m).$$

Докажимо да су елементи x_m трансцендентни над $\mathbb{Q}$. Претпоставимо да је $f(x_m) = 0$, за полином $f \in \mathbb{Q}[X_m]$. Дакле, $f(X_m)$ припада $\langle X_2^2 - X_1, X_3^2 - X_2, \dots\rangle$ и тада имамо следећу једнакост:

$$f(X_m) = p_1(X_1, \dots, X_k)(X_1 - X_2^2) + \dots + p_s(X_1, \dots, X_k)(X_s - X_{s+1}^2),$$

за неке $k, s \geq 1$. Користећи замене

$$X_1 = X_2^2, \qquad X_2 = X_3^2, \qquad \dots \qquad X_s = X_{s+1}^2,$$

једну за другом, добијамо да $f(X_m) = 0$ за $s < m$, као и $f(X_{s+1}^{2^{s-m+1}}) = 0$ за $s \geq m$. У оба случаја, сви коефицијенти полинома f су нула.

Ако важи да је $r_1 r_2 = 0$, где су $r_1, r_2 \in R$, тада постоје полиноми f и g са рационалним коефицијентима, који су такви да $r_1 = f(x_m)$ и $r_2 = g(x_m)$, за неко m. Приметимо да овде можемо изабрати исто m јер је $x_i = x_{i+1}^2$ за све i. Према томе, важи да је $f(x_m)g(x_m) = 0$, па је заправо $fg = 0$ у $\mathbb{Q}[X_1, X_2, \dots]$. Одатле следи да је $f = 0$ или $g = 0$, тако да је $r_1 = 0$ или $r_2 = 0$. Следи да је R интегрални домен, па то онда важи и за R_M.

Што се тиче доказа да је R_M валуациони прстен, довољно је доказати да су елементи $f_1(x_m)$ и $f_2(x_m)$ упоредиви у односу на релацију дељења. Ови елементи могу се видети и на следећи начин:

$$f_1(x_m) = x_m^s u \qquad \text{и} \qquad f_2(x_m) = x_m^t v,$$

где су u и v инвертибилни елементи. На основу овога се упоређивање елемената f_1 и f_2 своди на упоређивање степена s и t.

Докажимо сада да је $\dim(R_M) = 1$. Претпоставимо да је P ненула прост идеал у прстену R_M. Тада важи да је $P \subseteq M$ (уместо $R_M M$, писаћемо кратко M) и треба показати да је $P = M$. Као што знамо, било који ненула елемент у R_M је облика $x_m^s u$, где је u инвертибилан. Према томе, из $x_m^s u \in P$ добијамо да $x_m^s \in P$, што значи да $x_m \in P$ јер је P прост идеал (и самим тим $s \neq 0$). Пошто је

$$x_k = x_m^{2^{m-k}} \text{ за } k < m \qquad \text{и} \qquad x_m = x_k^{2^{k-m}} \text{ за } k > m,$$

можемо закључити да $x_k \in P$ за све k, тако да је $P = M$.

За доказ да R_M није Нетерин прстен, претпоставимо да је ланац идеала

$$\langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \cdots$$

стационаран. Тада имамо да је $\langle x_{n-1} \rangle = \langle x_n \rangle$, за неко n. Следи да $x_n \in \langle x_n^2 \rangle$ и тада је $x_n = px_n^2$. Можемо закључити да је $x_n(1 - px_n) = 0$. Фактор $1 - px_n$ је инвертибилан будући да $px_n \in M$. Коначно имамо да је $x_n = 0$, што је контрадикција.

Нека је сада I идеал у прстену $R_M[X]$ који је генерисан полиномима

$$\begin{aligned} f_1(X) &= x_1X^4 - x_1x_2X^3 + X^2 + x_2x_3X + x_1 \\ f_2(X) &= x_2X^2 + (x_3 - x_1x_3)X - x_2x_3 \\ f_3(X) &= x_2X^2 - x_1x_3X. \end{aligned}$$

Ако искористимо релације које важе за x_1, x_2, x_3, можемо видети ове полиноме на следећи начин:

$$\begin{aligned} f_1(X) &= x_3^4X^4 - x_3^6X^3 + X^2 + x_3^3X + x_3^4 \\ f_2(X) &= x_3^2X^2 + (x_3 - x_3^5)X - x_3^3 \\ f_3(X) &= x_3^2X^2 - x_3^5X. \end{aligned}$$

Означимо, ради једноставности, x_3 са α. Ови полиноми су узајамно прости, чак су то f_2 и f_3. Уз помоћ елементарних трансформација, можемо наћи релацију која важи у $K[X]$, где је K поље разломака за R_M.

$$\left(\begin{array}{c|cc} \alpha^2X^2 + (\alpha - \alpha^5)X - \alpha^3 & 1 & 0 \\ \alpha^2X^2 - \alpha^5X & 0 & 1 \end{array}\right) \xrightarrow{V_1 \mapsto V_1 - V_2} \left(\begin{array}{c|cc} \alpha X - \alpha^3 & 1 & -1 \\ \alpha^2X^2 - \alpha^5X & 0 & 1 \end{array}\right)$$

$$\xrightarrow{V_2 \mapsto V_2 - \alpha X V_1} \left(\begin{array}{c|cc} \alpha X - \alpha^3 & 1 & -1 \\ \alpha^4(1-\alpha)X & -\alpha X & 1 + \alpha X \end{array}\right) \xrightarrow{V_1 \mapsto V_1 - \frac{1}{\alpha^3(1-\alpha)}V_2}$$

$$\left(\begin{array}{c|cc} -\alpha^3 & 1 + \frac{1}{\alpha^2(1-\alpha)X} & -1 - \frac{1+\alpha X}{\alpha^3(1-\alpha)X} \\ \alpha^4(1-\alpha)X & -\alpha X & 1 + \alpha X \end{array}\right)$$

Дакле, релација у $K[X]$ је следећа:

$$-\alpha^3 = \left(1 + \frac{1}{\alpha^2(1-\alpha)}X\right) f_2 - \left(\frac{\alpha^3 - \alpha^4 + 1}{\alpha^3(1-\alpha)} + \frac{1}{\alpha^2(1-\alpha)}X\right) f_3,$$

то јест,

$$\alpha^6(1-\alpha) = (-\alpha^3(1-\alpha) - \alpha X)f_2 + (\alpha^3 - \alpha^4 + 1 + \alpha X)f_3.$$

Следи да $\alpha^6 \in (I \cap R_M) \setminus \{0\}$, пошто је $1 - \alpha$ инвертибилан елемент. Као у доказу леме 34, видимо да је $b = \alpha^4$ и $b^2 \in I$, тако да полином q^2 припада I, где је $q = X^2 + \alpha^3X + \alpha^4$. Према наведеној леми, и моничан полином степена $k = 2$ припада I. Пошто важи да је $t = k(m-1) - 1 = 1$, поделићемо Xf_1 са q^2. После овог дељења, добијамо да моничан полином

$$r_1(X) = X^3 + \alpha^3u_1X^2 + \alpha^4u_2X + \alpha^{14}u_3$$

припада I, где су $u_1, u_2, u_3 \in \mathrm{U}(R_M)$. Настављамо поступак, делимо f_1 са r_1 и добијамо полином

$$r_2(X) = X^2 + \alpha^3u_4X + \alpha^4u_5, \qquad u_4, u_5 \in \mathrm{U}(R_M),$$

који припада идеалу I.

Моничан полином степена 2 смо могли добити и променом генератора идеала I уз помоћ следећих трансформација:

$$\begin{pmatrix} \alpha^4X^4-\alpha^6X^3+X^2+\alpha^3X+\alpha^4 \\ \alpha^2X^2+(\alpha-\alpha^5)X-\alpha^3 \\ \alpha^2X^2-\alpha^5X \end{pmatrix} \xrightarrow{V_2\mapsto V_2-V_3} \begin{pmatrix} \alpha^4X^4-\alpha^6X^3+X^2+\alpha^3X+\alpha^4 \\ \alpha X-\alpha^3 \\ \alpha^2X^2-\alpha^5X \end{pmatrix}$$

$$\xrightarrow{V_3\mapsto V_3-\alpha X V_2} \begin{pmatrix} \alpha^4X^4-\alpha^6X^3+X^2+\alpha^3X+\alpha^4 \\ \alpha X-\alpha^3 \\ \alpha^4(1-\alpha)X \end{pmatrix} \xrightarrow{V_3\mapsto V_3-\alpha^3(1-\alpha)V_2}$$

$$\begin{pmatrix} \alpha^4X^4-\alpha^6X^3+X^2+\alpha^3X+\alpha^4 \\ \alpha X-\alpha^3 \\ \alpha^6(1-\alpha) \end{pmatrix} \xrightarrow{V_1\mapsto V_1-\alpha^3X^3V_2} \begin{pmatrix} X^2+\alpha^3X+\alpha^4 \\ \alpha X-\alpha^3 \\ \alpha^6(1-\alpha) \end{pmatrix}$$

Дакле, I је генерисан са

$$h=X^2+\alpha^3X+\alpha^4, \qquad h_1=\alpha X-\alpha^3, \qquad h_2=\alpha^6.$$

Одредимо за почетак генераторе модула I_1:

$$\begin{aligned} \rho(Xh_1,h) &= -\alpha^3(1+\alpha)X-\alpha^5 \\ \rho(Xh_2,h) &= \alpha^6X \\ \rho(h_1,h) &= h_1=\alpha X-\alpha^3 \\ \rho(h_2,h) &= h_2=\alpha^6. \end{aligned}$$

Сада видимо да је $\pi_1(I_1)$ генерисан са α. Такође, h_1 је полином чији водећи коефицијент генерише $\pi_1(I_1)$. У следећем кораку тражимо генераторе за I_2:

$$\begin{aligned} \rho(\rho(Xh_1,h),h_1) &= -\alpha^5(2+\alpha) \\ \rho(\rho(Xh_2,h),h_1) &= \alpha^8 \\ \rho(h_2,h_1) &= \alpha^6. \end{aligned}$$

Следи да је $\pi_0(I_0)=I_0$ генерисан са α^5.

Коначно добијамо да је

$$\mathrm{LT}(I)=\langle X^2,\alpha X,\alpha^5\rangle=\langle X^2,x_3X,x_1x_3\rangle,$$

а минимална јака Гребнерова база за I је дата са

$$g_1=X^2+x_2x_3X+x_1, \qquad g_2=x_3X-x_1x_2, \qquad g_3=x_1x_3.$$

Глава 3

Валуациони прстени димензије 0

У литератури постоји више начина на који су спровођене генерализације појма валуационог домена на прстен са делитељима нуле. Споменимо два: Манисов валуациони прстен (видети [33]) и ланчасти прстен, прстен за који важи да је његов скуп идеала тотално уређен инклузијом (видети [22]). Овде ћемо користити дефиницију 24 дату у претходној глави, формулисану преко својства дељивости елемената, која такође постоји у литератури (видети, на пример, [42]).

Дакле, у овој глави бавићемо се валуационим прстенима, без претпоставке да је тај прстен и интегрални домен. У [31] аутори су доказали да је идеал водећих чланова $\mathrm{LT}(I)$ коначно генерисан, где је I коначно генерисан идеал у $V[X]$ и V валуациони прстен димензије 0. Уз губитак општости у односу на споменуто, то јест, уз додатни услов да је анулатор сваког елемента из V коначно генерисан идеал, резултат о коначној генерисаности $\mathrm{LT}(I)$ је приказан у теореми 39, која је заједно са осталим резултатима из [41] представљена у овој глави. Споменути резултат се може наћи и у [34], где је формулисан у терминима архимедског својства и кохерентности. Докази овде су представљени по аналогији са резултатима из претходне главе, и такође садрже методе за одређивање Гребнерове базе.

У глави 2 користили смо чињеницу да је сваки валуациони прстен V локални (M ће и овде бити ознака за његов максимални идеал). Такође смо имали лему 30, која важи за произвољни прстен R и на коју ћемо се и овде надовезати.

За следећу лему, биће нам потребна претпоставка да је прстен R валуациони, као и да је анулатор сваког елемента коначно генерисан. Доказ ћемо спровести слично леми 31, уз неопходне корекције због различитих услова.

Лема 37. *Нека је V валуациони ӣрсӯен у коме је анулаӯор свакоī елеменӯа коначно īенерисан. Нека је I идеал у $V[X]$ īенерисан ӣолиномима $f, f_1, \ldots, f_s$, īде је f моничан ӣолином сӯеӣена n. Тада су $I_{n-2}, I_{n-3}, \ldots, I_0$ коначно īенерисани V-модули.*

Доказ. Према леми 30, V-модул I_{n-1} је коначно генерисан. Нека су

$$\pi_k : V[X]_k \to V$$

хомоморфизми такви да је $\pi_k(p)$ коефицијент уз производ X^k у полиному p. Слика $\pi_{n-1}(I_{n-1})$ је коначно генерисан, то јест, главни идеал у V:

$$\pi_{n-1}(I_{n-1}) = \langle c_{n-1} \rangle.$$

Ако претпоставимо да бар један од елемената $f_1, \ldots, f_s$ није умножак од f, имамо да је $c_{n-1} \neq 0$. Нека је $h_{n-1} \in I_{n-1}$ полином такав да $\mathrm{LT}(h_{n-1}) = c_{n-1}X^{n-1}$ и тај полином је заправо један од остатака $\rho(X^t f_i, f)$, баш као и у доказу леме 30.

Докажимо да је I_{n-2} коначно генерисани V-модул тако што ћемо наћи експлицитно његов генераторни скуп. Пошто је $g \in I_{n-2} \subseteq I_{n-1}$, тада је очигледно

$$g = \sum r_{ij}\rho(X^i f_j, f), \qquad r_{ij} \in V,\ 1 \leq j \leq s,\ 0 \leq i \leq n-1.$$

Када поделимо остатке $\rho(X^i f_j, f)$ са h_{n-1}, добићемо релацију $\rho(X^i f_j, f) = a_{ij}h_{n-1} + f_{ij}$. Даље следи да је

$$g = \sum r_{ij}(a_{ij}h_{n-1} + f_{ij}) = \left(\sum r_{ij}a_{ij}\right) h_{n-1} + \sum r_{ij}f_{ij}.$$

С обзиром на то да $g \in I_{n-2}$, тада $\sum r_{ij}a_{ij}$ припада $\mathrm{Ann}(c_{n-1})$. Овај анулатор је коначно генерисан, то јест, главни. Нека је

$$\mathrm{Ann}(c_{n-1}) = \langle d_{n-1} \rangle.$$

Следи да је сваки елемент у I_{n-2} V-линеарна комбинација елемената

$$d_{n-1}h_{n-1} \text{ и } f_{ij} = \rho(\rho(X^i f_j, f), h_{n-1}), \text{ где је } 1 \leq j \leq s,\ 0 \leq i \leq n-1.$$

Можемо поновити овај поступак. Ако је $I_{n-2} = \{0\}$, тада је $I_0 = \cdots = I_{n-3} = \{0\}$. Ако $I_{n-2} \neq \{0\}$, тада је $\pi_{n-2}(I_{n-2})$ коначно генерисан подмодул у V, па постоји $c_{n-2} \in V$ тако да важи $\pi_{n-2}(I_{n-2}) = \langle c_{n-2} \rangle$. Нека је $h_{n-2} \in I_{n-2}$ полином такав да $\mathrm{LT}(h_{n-2}) = c_{n-2}X^{n-2}$. Генераторни скуп за I_{n-3} састоји се од остатака при дељењу генератора за I_{n-2} са h_{n-2} заједно са полиномом $d_{n-2}h_{n-2}$, где је $\mathrm{Ann}(\mathrm{LC}(h_{n-2})) = \langle d_{n-2} \rangle$. Можемо наставити на овај начин и доказати да су сви ови модули коначно генерисани. □

Посветимо се сада питању постојања моничног полинома у идеалу који разматрамо. Ако је $I = \langle f_1, \ldots, f_s \rangle \lhd V[X]$, тада постоји коефицијент $\alpha \in V$ неког од генератора који дели све остале коефицијенте свих полинома који генеришу I. Нека је $f_i = \alpha g_i$, за $i \in \{1, \ldots, s\}$. Тада је $I = \alpha\langle g_1, \ldots, g_s \rangle$ и бар један од коефицијената међу генераторима $g_1, \ldots, g_s$ је инвертибилан. Под претпоставком да је димензија валуационог прстена нула, у следећој леми доказаћемо да $\langle g_1, \ldots, g_s \rangle$ садржи моничан полином.

Лема 38. *Нека је $I = \langle f_1, \ldots, f_s \rangle$ идеал у $V[X]$, где је V валуациони прстен димензије нула и нека је бар један коефицијент међу свим коефицијентима генератора од I инвертибилан. Ако означимо са $f_i = \sum_j a_{ij}X^j$ и*

$$k = \min\{l \in \mathbb{N} \mid (\exists i \in \{1, \ldots, s\})(a_{il} \in \mathrm{U}(V) \text{ и } (\forall j > l)a_{ij} \notin \mathrm{U}(V))\},$$

тада постоји моничан полином f у I степена k.

Доказ. Без губитка општости, можемо претпоставити да f_1 има бар један инвертибилни коефицијент, као и да је тај инвертибилни коефицијент једнак 1. Ако је $\mathrm{LC}(f_1) = 1$, имамо тврђење леме. У супротном, f_1 је збир моничног полинома и полинома чији су сви коефицијенти у M (неинвертибилни елементи). Овај последњи може се видети као производ елемента у M и полинома чији један коефицијент је једнак 1. Тако да је

$$f_1(X) = bp(X) + q(X), \qquad b \in M, \qquad q \text{ моничан у } V[X].$$

Како је V локални прстен димензије нула, важи да

$$\mathrm{Nil}(V) = \bigcap_{P \text{ прост}} P = \bigcap_{M \text{ максималан}} M = \mathrm{J}(V) = M.$$

Следи да је сваки елемент у V или нилпотентан или инвертибилан, тако да постоји $m \in \mathbb{N}$ за које важи да $b^m = 0$. Према формули

$$(y+q)^m - y^m = (y+q)q_1 + (-1)^{m+1}q^m,$$

за неке полиноме y, q, q_1 и $m \geq 1$, имамо да је

$$\begin{aligned} I \ni f_1(X)^m &= (bp(X) + q(X))^m = (bp(X) + q(X))^m - (bp(X))^m \\ &= (bp(X) + q(X))q_1(X) + (-1)^{m+1}q(X)^m \\ &= f_1(X)q_1(X) + (-1)^{m+1}q(X)^m. \end{aligned}$$

Према томе, моничан полином q^m припада I. Даље настављамо као у леми 34, јер чињеница да је у тој леми у питању интегрални домен никако не утиче на наставак доказа, свакако вршимо дељење моничним полиномима. Нека је $t = (m-1)k - 1$ и пређимо на сукцесивно дељење полиномима чији водећи коефицијенти су инвертибилни:

$$\begin{aligned} X^t f_1 &= q^m q_1 + r_1 \\ X^{t-1} f_1 &= r_1 q_2 + r_2 \\ &\dots \\ X^2 f_1 &= r_{t-2} q_{t-1} + r_{t-1} \\ X f_1 &= r_{t-1} q_t + r_t \\ f_1 &= r_t q_{t+1} + r_{t+1}. \end{aligned}$$

Последњи остатак у овом дељењу је r_{t+1}, полином у I степена k чији водећи коефицијент је инвертибилан, чиме завршавамо доказ. □

Сада можемо доказати главну теорему.

Теорема 39. *Нека је V валуациони прстен димензије нула у коме је анулатор сваког елемента коначно генерисан. Ако је I коначно генерисан идеал у $V[X]$, тада постоји минимална јака Гребнерова база за I.*

Доказ. Нека је $I = \langle f_1, \dots, f_s \rangle$ и $\alpha \in V$ је коефицијент неког од генератора који дели све остале коефицијенте свих полинома који генеришу идеал I. Нека је $f_i = \alpha g_i$, за $i \in \{1, \dots, s\}$. Тада је

$$I = \alpha \langle g_1, \dots, g_s \rangle.$$

Довољно је доказати да $J = \langle g_1, \dots, g_s \rangle$ има Гребнерову базу.

Можемо претпоставити да је бар један од коефицијената међу свим коефицијентима полинома $g_1, \dots, g_s$ једнак 1 и нека је индекс k као у леми 38. Према тој леми, постоји моничан полином f степена k у J. Тада су према леми 37, V-модули $J_{k-1}, \dots, J_0$ коначно генерисани. Као у доказу леме 37, нека су пресликавања $\pi_l : V[X]_l \to V$ хомоморфизми тако да је $\pi_l(p)$ коефицијент уз производ X^l у полиному p. Следи да су слике $\pi_l(J_l)$

главни идеали у V. Нека је $\pi_l(J_l) = \langle c_l \rangle$ и нека су $h_l \in J_l$ такви да $\mathrm{LT}(h_l) = c_l X^l$. Ако означимо са $\mathcal{S}$ скуп индекса $i \in \{1, \dots, k-1\}$ таквих да $c_i \neq 0$ и

$$c_j \nmid c_i, \qquad \text{за све } j < i,$$

тада је скуп

$$B = \{X^k, \mathrm{LT}(h_i) \,|\, i \in \mathcal{S}\}$$

такав да $\langle B \rangle = \mathrm{LT}(I)$. Наиме, минимална јака Гребнерова база за J дата је са

$$G = \{f, h_i \mid i \in \mathcal{S}\}.$$

Нека је $p \in J \setminus \{0\}$. Ако $\deg(p) \geq k$, тада $X^k \mid \mathrm{LT}(p)$. Ако је $\deg(p) = l < k$, тада $p \in J_l$; следи да $c_i X^i \mid \mathrm{LT}(p)$ за неко $i \leq l$ и $i \in \mathcal{S}$. Означимо са

$$G' = \{\alpha g \mid g \in G\},$$

што представља минималну јаку Гребнерову базу за полазни идеал I. $\square$

Можемо направити малу промену у примеру 36 и добити прстен за који важи да је валуациони прстен Крулове димензије 0 и није Нетерин.

Пример 40. Нека је

$$R = \mathbb{Q}[X_1, X_2, X_3, \dots]/\langle X_1^2, X_2^2 - X_1, X_3^2 - X_2, \dots \rangle.$$

Уочимо локализацију R_M овог прстена у односу на максимални идеал $M = \langle x_1, x_2, \dots \rangle$, где је x_i ознака за класу елемента X_i у R.

Слично као у споменутом примеру се може доказати да овај прстен није Нетерин, као и да је сваки елемент у R_M облика $f(x_m) = x_m^s u$, за неко x_m, $s \geq 0$ и инвертибилан елемент u, а самим тим је R_M и валуациони прстен.

Нека је M ознака и за максимални идеал у R_M. Како је

$$0 = x_1^2 = x_2^4 = x_3^8 = \cdots$$

следи да је сваки елемент у R_M нилпотентан или инвертибилан. Како је R_M локални прстен, следи да је

$$M = \mathrm{J}(R_M) = \mathrm{Nil}(R_M) = \bigcap_{P \text{ прост}} P.$$

Ово значи да је $M \subseteq P$, за сваки прост идеал P у R_M, па следи да је R_M димензије 0.

Докажимо сада да је анулатор сваког елемента из R_M коначно генерисан. Нека је $f(x_m) = x_m^l u$ елемент у R_M, где је $m \geq 1$ најмање могуће и $u \in \mathrm{U}(R_M)$. Јасно је да важи $\mathrm{Ann}(f) = \mathrm{Ann}(x_m^l)$. Докажимо да је

$$\mathrm{Ann}(x_m^l) = \langle x_m^{2^m - l} \rangle.$$

Јасно је да $x_m^{2^m-l} \in \mathrm{Ann}(x_m^l)$. Са друге стране, нека је $p(x_n) = x_n^k v \in \mathrm{Ann}(x_m^l)$. Ако је $n \leq m$, онда се $p(x_n)$ може написати као $x_m^s v$. Следи да је

$$p(x_n) \cdot x_m^l = x_m^s v \cdot x_m^l = 0 = x_m^{2^m},$$

тако да је $s + l \geq 2^m$. Одавде следи да је $s \geq 2^m - l$, па је

$$p(x_m) = x_m^s v \in \langle x_m^{2^m - l} \rangle.$$

За случај када је $n > m$, узмимо $s = n - m$. Тада је

$$x_m^l = (x_{m+s}^{2^s})^l = (x_n^{2^s})^l = x_n^{2^s l}.$$

Из

$$p(x_n) \cdot x_m^l = x_n^k v \cdot x_n^{2^s l} = 0 = x_n^{2^n}$$

следи да $2^s l + k \geq 2^n$. Према томе, важи да је

$$k \geq 2^n - 2^s l = 2^{m+s} - 2^s l = 2^s(2^m - l).$$

Дакле, x_n^k је дељив са

$$x_n^{2^s(2^m - l)} = (x_n^{2^s})^{2^m - l} = x_m^{2^m - l},$$

што је и требало показати.

Нека је I идеал генерисан истим полиномима као у примеру 36. После одговарајућих замена, имамо да су ти елементи једнаки

$$\begin{aligned} f_1(X) &= x_3^4 X^4 - x_3^6 X^3 + X^2 + x_3^3 X + x_3^4 \\ f_2(X) &= x_3^2 X^2 + (x_3 - x_3^5) X - x_3^3 \\ f_3(X) &= x_3^2 X^2 - x_3^5 X. \end{aligned}$$

Означимо са $x_3 = \alpha$. Како је

$$f_1(X) = \alpha^4 (X^4 - \alpha^2 X^3) + X^2 + \alpha^3 X + \alpha^4$$

и $(\alpha^4)^2 = 0$, према леми 38 следи да полином

$$q(X)^2 = (X^2 + \alpha^3 X + \alpha^4)^2 \in I.$$

Можемо наћи и моничан полином мањег степена: поделимо $X f_1$ са q^2. Моничан полином

$$r_1(X) = X^3 + \alpha^3 X^2 + \alpha^4 X$$

припада I. Поделимо затим f_1 са r_1. Следи да је

$$r_2(X) = X^2 + \alpha^3 X + \alpha^4 \in I.$$

Уведимо ознаку $r_2 = h$. Како је

$$\begin{aligned} \rho(f_1, h) &= 0 \\ \rho(f_2, h) &= \alpha(1 - 2\alpha^4) X - \alpha^3 (1 + \alpha^3) \\ \rho(f_3, h) &= -2\alpha^5 X - \alpha^6, \end{aligned}$$

имамо да је I генерисан са

$$h = X^2 + \alpha^3 X + \alpha^4, \qquad h_1 = \alpha X - \alpha^3 (1 + \alpha^3 + 2\alpha^4), \qquad h_2 = \alpha^5 X + \alpha^6.$$

Израчунајмо остатке потребне за одређивање генератора за I_1. *Важи да*

$$\begin{aligned}
\rho(Xh_1, h) &= -\alpha^3(1+\alpha+\alpha^3+2\alpha^4)X+\alpha^5\\
\rho(Xh_2, h) &= \alpha^6 X\\
\rho(h_1, h) &= \alpha X-\alpha^3(1+\alpha^3+2\alpha^4)\\
\rho(h_2, h) &= \alpha^5 X+\alpha^6,
\end{aligned}$$

што значи да је $\pi_1(I_1)$ генерисан са α и да је h_1 полином чији је то водећи коефицијент. Одредимо још

$$\begin{aligned}
\rho(\rho(Xh_1, h), h_1) &= -\alpha^6(1+2\alpha^2+4\alpha^3+2\alpha^4+\alpha^5+4\alpha^6)\\
\rho(\rho(Xh_2, h), h_1) &= \alpha^5\\
\rho(h_2, h_1) &= \alpha^6(1-2\alpha).
\end{aligned}$$

Како је и $\mathrm{Ann}(\alpha)=\langle\alpha^7\rangle$ и пошто је $\alpha^7 h_1=0$, следи да је $\pi_0(I_0)=I_0$ генерисан са α^5.

Коначно имамо да је $\mathrm{LT}(I)=\langle X^2, \alpha X, \alpha^5\rangle=\langle X^2, x_3X, x_1x_3\rangle$, док је минимална јака Гребнерова база за I дата са

$$g_1=X^2+x_2x_3X+x_1, \qquad g_2=x_3X-x_2x_3-x_1x_2-2x_1x_2x_3, \qquad g_3=x_1x_3.$$

Глава 4

Приферови домени

4.1 Уводна тврђења

Појам Приферовог домена уведен је у [39], а сада га многи сматрају једним од централних појмова у теорији комутативних интегралних домена. О његовом значају говори и чињеница да се у теорији дефинише на преко 40 еквивалентних начина, при чему те дефиниције залазе у разне гране алгебре, највише у теорију идеала. Наведимо бар неке од тих дефиниција (видети [19], [17], [10]).

Нека је R интегрални домен у коме важи неки од следећих услова:

- За сваки прост (респективно, максималан) идеал P (респективно, M) у R локализација R_P (респективно, R_M) је валуациони домен.
- Сваки ненула коначно генерисани идеал у R је инвертибилан.
- Сваки торзионо слободни коначно генерисани модул над R је пројективан.
- Сваки подмодул равног R-модула је раван.
- Ако су M и N торзионо слободни R-модули, тада је и $M \otimes_R N$ торзионо слободан.
- Сваки натпрстен од R садржан у његовом пољу разломака је интегрално затворен.
- R је интегрално затворен и постоји природан број $n > 1$ тако да за све $a, b \in R$ важи да
$$(a,b)^n = (a^n, b^n).$$
- За све ненула идеале I, J, K у R важи да $I \cap (J+K) = (I \cap J) + (I \cap K)$.
- За све ненула идеале I, J, K у R важи да $I(J \cap K) = IJ \cap IK$.
- За све ненула идеале I, J у R важи да $(I+J)(I \cap J) = IJ$.
- За све ненула идеале I, J, K у R, где је J коначно генерисан, важи да
$$(I+J) : K = I : K + J : K.$$
- За све ненула идеале I, J, K у R, где је J коначно генерисан, важи да
$$K : (I \cap J) = K : I + K : J.$$

- За све коначно генерисане идеале I, J, K у R важи: ако је $IJ = IK$ и I је ненула, тада је $J = K$.

Дефиниција 41. *Ако за интегрални домен R важи бар један од горе наведених услова, кажемо да је R Приферов домен.*

Сваки Приферов домен је интегрално затворен. Такође, Приферов и Нетерин домен је Дедекиндов домен и Крулове је димензије један. Често се на Приферов домен гледа као на ненетерин аналогон Дедекиндовог домена. Подсетимо се да се Дедекиндов домен може дефинисати као интегрално затворен Нетерин домен Крулове димензије један.

Важи да је комутативни полунаследни интегрални домен исто што и Приферов домен. Тако да се понекад у литератури могу наћи резултати о Приферовим доменима под овим називом, као и под називом аритметички домен. Уведимо и дефиницију овог појма, који ће нам бити потребан у следећој глави.

Дефиниција 42. *Аритметички прстен је комутативни прстен у коме за све ненула идеале I, J, K важи да*

$$I \cap (J + K) = (I \cap J) + (I \cap K).$$

Приметимо да за произвољне идеале I, J, K увек важи да

$$I \cap J \subseteq I \cap (J + K), \qquad I \cap K \subseteq I \cap (J + K),$$

па и

$$(I \cap J) + (I \cap K) \subseteq I \cap (J + K).$$

Из наведених еквиваленција за Приферов домен видимо да је аритметички прстен који је интегрални домен исто што и Приферов домен.

Историјски је прво уведен појам Приферовог домена, а тек касније је тај појам генерализован до појма Приферовог прстена. Наиме, прстен је Приферов ако је сваки његов коначно генерисани регуларни идеал инвертибилан, где је идеал регуларан ако садржи регуларан елемент. За еквивалентне услове Приферовог прстена видети [8], а у даљем тексту ће нам бити битна чињеница да је сваки аритметички прстен и Приферов прстен.

Један од важних примера Приферовог домена је прстен свих алгебарских целих (видети теорему 101 у [24]):

$$\bar{\mathbb{Z}} = \{z \in \mathbb{C} \mid p(z) = 0 \text{ за моничан полином } p \in \mathbb{Z}[X]\}.$$

Такође, прстен целовредносних полинома са рационалним коефицијентима

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$$

је Приферов домен (теорема 17 у [14]).

Уведимо још појам кохерентног прстена који ће бити потребан за доказ теореме 52.

Дефиниција 43. *Модул M над прстеном R је коначно представљив ако постоји тачан низ*

$$F_1 \to F_0 \to M \to 0,$$

где су F_0 и F_1 коначно генерисани слободни R-модули.

Дакле, ако је модул коначно представљив, онда је коначно генерисан са коначно генерисаним релацијама.

Дефиниција 44. *Модул M над прстеном R је кохерентан ако је коначно генерисан и ако је сваки његов коначно генерисани подмодул коначно представљив.*

Дефиниција 45. *Прстен R је кохерентан ако је кохерентан као R-модул, то јест, ако је сваки коначно генерисан идеал у R коначно представљив.*

Како је у Приферовом домену сваки коначно генерисани идеал инвертибилан (то јест, пројективан као R-модул), на основу леме 8(iii) (стр. 20) у [10] следи да је и коначно представљив. Тако да је сваки Приферов домен и кохерентан.

Представићемо неке дефиниције које ће бити потребне у наредном тексту. За више детаља, видети [17].

Дефиниција 46. *Нека је I идеал у $R[X]$, где је R интегрални домен и нека су*

$$I_{(n)} \subseteq R, \ n \geq 0,$$

идеали водећих коефицијената полинома степена мањег или једнаког са n у I. Такође, нека је

$$I_\infty = \bigcup_{n=0}^{\infty} I_{(n)}.$$

Идеали $I_{(n)}$ и I_∞ се називају асоцираним идеалима идеала I.

Очито имамо да $I_{(0)} \subseteq I_{(1)} \subseteq \cdots \subseteq I_{(n)} \subseteq \cdots \subseteq I_\infty$.

Дефиниција 47. *Интегрални домен R задовољава својство KP ако су за сваки коначно генерисани идеал I у $R[X]$ асоцирани идеали $I_{(n)}, n \geq 0$ и $I_\infty = \cup_{n=0}^{\infty} I_{(n)}$ коначно генерисани. Такође, R задовољава својство K_0P ако је за сваки коначно генерисани идеал I у $R[X]$ асоцирани идеал $I_{(0)} = I \cap R$ коначно генерисан.*

Назив за својство KP из претходне дефиниције потиче од „Kaplanski property”. Следећи резултат је дат као теорема 6.2.10 у [17] и биће нам од суштинског значаја у доказу о постојању Гребнерове базе за коначно генерисани идеал у прстену полинома са једном неодређеном над Приферовим доменом димензије 1.

Теорема 48. *Нека је R Приферов домен. Следећа тврђења су еквивалентна:*

1. *R задовољава KP;*
2. *R задовољава K_0P;*
3. $\dim(R) \leq 1$.

Представимо сада доказ о постојању Гребнерове базе. Резултати следеће теореме, као и теорема 52, 55 и леме 54, могу се наћи у [38].

Теорема 49. *Нека је R Приферов домен Крулове димензије 1. Ако је I коначно генерисан идеал у $R[X]$, тада постоји Гребнерова база G за I.*

Доказ. Означимо са $I_{(n)}$ и I_∞ асоциране идеала идеала I. Према теореми 48, сви ти идеали су коначно генерисани. Нека је

$$I_\infty = \langle c_1, \dots, c_s \rangle.$$

Тада постоје $f_1, \dots, f_s \in I$ тако да

$$\mathrm{LT}(f_i) = c_i X^{k_i}, \qquad \text{за } 1 \le i \le s.$$

Нека је $j \in \{1, \dots, s\}$ такав да

$$k_j \ge k_i, \qquad \text{за све } i \in \{1, \dots, s\}.$$

Ако означимо са n број k_j, и означимо са $g_{i,n}$ полиноме $f_i X^{n-k_i}$ степена n, тада видимо да је $I_\infty = I_{(n)}$.

Наиме, ако је $c \in I_\infty$ водећи коефицијент полинома у I степена l, и $l > n$, тада је

$$c = a_1 c_1 + \dots + a_s c_s, \qquad \text{за } a_1, \dots, a_s \in R.$$

Следи да је полином $a_1 g_{1,n} + \dots + a_s g_{s,n}$ степена n чији водећи коефицијент је c, па је $c \in I_{(n)}$.

Нека је сада

$$I_{(m)} = \langle \mathrm{LC}(g_{1,m}), \dots, \mathrm{LC}(g_{s_m,m}) \rangle, \qquad \text{за } 0 \le m \le n-1,$$

где су $g_{1,m}, \dots, g_{s_m,m}$ полиноми степена m који припадају I. Нека је

$$G = \{g_{j,m} \mid 1 \le j \le s_m,\ 0 \le m \le n-1\} \cup \{g_{1,n}, \dots, g_{s,n}\}.$$

Докажимо да је G Гребнерова база за I. Нека је $f \in I$ полином степена m. Ако је $m \ge n$, тада $\mathrm{LC}(f) \in I_\infty$ и

$$\mathrm{LC}(f) = \alpha_1 c_1 + \dots + \alpha_s c_s, \qquad \text{за } \alpha_i \in R.$$

Према томе, важи да

$$\mathrm{LT}(f) = (\alpha_1 c_1 + \dots + \alpha_s c_s) X^m = \alpha_1 X^{m-n} \mathrm{LT}(g_{1,n}) + \dots + \alpha_s X^{m-n} \mathrm{LT}(g_{s,n}).$$

Ако је $m < n$, тада је $\mathrm{LC}(f) \in I_{(m)}$ и

$$\mathrm{LC}(f) = \beta_1 \mathrm{LC}(g_{1,m}) + \dots + \beta_{s_m} \mathrm{LC}(g_{s_m,m}), \qquad \beta_i \in R.$$

Дакле, имамо да

$$\mathrm{LT}(f) = \beta_1 \mathrm{LT}(g_{1,m}) + \dots + \beta_{s_m} \mathrm{LT}(g_{s_m,m}).$$

Следи да у сваком случају $\mathrm{LT}(f) \in \langle \mathrm{LT}(g) \mid g \in G \rangle$. □

Напомена 50. *Сваки валуациони домен је и Приферов домен. Према томе, из претходне теореме следи да у случају валуационог домена димензије 1, коначно генерисани идеал I у $V[X]$ има Гребнерову базу. Из тврђења 29 следи да постоји и јака база, тако да смо резултат теореме 35 могли добити и на овај начин, уз додатно остваривање минималности те базе. Разлика је наравно у томе што у овом случају немамо алгоритам за одређивање Гребнерове базе, као што имамо у случају валуационих домена.*

4.2 Подмодули коначно генерисаних слободних $R[X]$-модула

Кратко ћемо представити потребне појмове и дефиниције, и то само за случај једне неодређене (видети [1]). Нека је R прстен и M коначно генерисан $R[X]$-подмодул у $R[X]^m$, $m \geq 1$. Сваки елемент у M може да се представи преко стандардне базе

$$e_1 = (1, 0, \ldots, 0), \ \ldots \ , e_m = (0, \ldots, 0, 1).$$

Елементе модула $R[X]^m$ који су облика $X^r e_i$, $r \geq 0$, називамо производима. Такође, кажемо да производ $X^r e_i$ дели производ $X^s e_j$ ако је $i = j$ и $r \leq s$, и тада пишемо $X^r e_i \,|\, X^s e_j$. У овом случају, количник у дељењу је X^{s-r}. Елементе облика $\alpha X^r e_i$, за $\alpha \in R$, називамо мономима или члановима. Слично, моном $\alpha X^r e_i$ дели $\beta X^s e_j$ ако $\alpha \,|\, \beta$ и $X^r e_i \,|\, X^s e_j$.

Даље, под мономним поретком на $R[X]^m$ подразумевамо линеарно уређење $\leq$ на производима, које задовољава следеће услове:

1. $X^r e_i < X^s X^r e_i$, за сваки производ $X^r e_i$ и свако $s \geq 1$;
2. Ако је $X^r e_i < X^s e_j$ за производе $X^r e_i, X^s e_j$, тада важи $X^t X^r e_i < X^t X^s e_j$ за све $t \geq 0$.

Постоје различити примери мономних поредака, али онај који је овде од интереса је „position over term” или краће POT и дефинише се на следећи начин:

$$X^r e_i < X^s e_j \Leftrightarrow i > j \quad \text{или} \quad i = j, \, r < s.$$

Лако се може проверити да ово јесте један мономни поредак на $R[X]^m$.

Када фиксирамо мономни поредак $<$ на $R[X]^m$, тада сваки елемент $f \in R[X]^m$ може да се представи као

$$f = \alpha_1 X^{s_1} e_{k_1} + \alpha_2 X^{s_2} e_{k_2} + \cdots + \alpha_l X^{s_l} e_{k_l},$$

где су $\alpha_i \in R$ и $X^{s_i} e_{k_i}$ су производи, такви да важи

$$X^{s_1} e_{k_1} > X^{s_2} e_{k_2} > \cdots > X^{s_l} e_{k_l}.$$

Тада се водећи члан и водећи коефицијент за f означавају са

$$\mathrm{LT}(f) = \alpha_1 X^{s_1} e_{k_1}, \qquad \mathrm{LC}(f) = \alpha_1.$$

Ако је M подмодул од $R[X]^m$, тада је

$$\mathcal{LT}(M) = \{\mathrm{LT}(f) \,|\, f \in M\} \qquad \text{и} \qquad \mathrm{LT}(M) = \langle \mathcal{LT}(M) \rangle.$$

Дефиниција 51. *Нека је M коначно генерисани подмодул у $R[X]^m$, где је R прстен. Подскуп $G = \{g_1, \ldots, g_r\}$ у M је Гребнерова база за M ако $\mathrm{LT}(M) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle$.*

Сада ћемо представити главну теорему која се односи на егзистенцију Гребнерове базе за коначно генерисане подмодуле, где је базни прстен Приферов домен Крулове димензије 1.

Теорема 52. *Нека је M коначно генерисани подмодул у $R[X]^m$, где је R Приферов домен Крулове димензије један и нека је фиксиран мономни поредак POT на $R[X]^m$. Тада постоји Гребнерова база G за M.*

Доказ. Нека је $M = \langle (f_{11}, f_{12}, \dots, f_{1m}), \dots, (f_{s1}, f_{s2}, \dots, f_{sm}) \rangle$. Ако дефинишемо

$$I = \{ f \in R[X] \mid (f(X), f_2(X), \dots, f_m(X)) \in M, \text{ за неке } f_2, \dots, f_m \in R[X] \},$$

тада је I идеал у $R[X]$ који је коначно генерисан. Заправо, $I = \langle f_{11}, \dots, f_{s1} \rangle$. Према теореми 49, постоји Гребнерова база за I. Нека је то $\{g_{11}, \dots, g_{k1}\}$. Пошто ови полиноми припадају I, постоје $(m-1)$-торке $(g_{12}, \dots, g_{1m}), \dots, (g_{k2}, \dots, g_{km})$ тако да

$$(g_{11}, g_{12}, \dots, g_{1m}), \dots, (g_{k1}, g_{k2}, \dots, g_{km}) \in M.$$

Нека је сада

$$M_1 = \{ (f_2(X), \dots, f_m(X)) \in R[X]^{m-1} \mid (0, f_2(X), \dots, f_m(X)) \in M \}.$$

Да бисмо доказали да је M_1 коначно генерисан $R[X]$-модул, приметимо прво да је, према последици 7.3.4 у [20], прстен $R[X]$ кохерентан домен, то јест, кохерентан $R[X]$-модул. Тада је $R[X]^m$ такође кохерентан модул. Пошто је $\{0\} \times M_1$ пресек модула M и подмодула $\langle e_2, \dots, e_m \rangle$ од $R[X]^m$, а и један и други су коначно генерисани, следи да је $\{0\} \times M_1$ такође коначно генерисан, то јест, M_1 је коначно генерисан (за више резултата о кохерентности видети [20]).

Настављамо користећи математичку индукцију. Како је M_1 коначно генерисан подмодул у $R[X]^{m-1}$, следи да постоји Гребнерова база G_1 за M_1. Гребнерова база G за M је дата са

$$\{ (0, h_2, \dots, h_m) \mid (h_2, \dots, h_m) \in G_1 \} \cup \{ (g_{11}, g_{12}, \dots, g_{1m}), \dots, (g_{k1}, g_{k2}, \dots, g_{km}) \}.$$

Случај $m = 1$ је садржан у теореми 49.

Наиме, нека је $f = (f_1, \dots, f_m) \in M$. Ако је $f_1 \neq 0$, тада важи да је $\mathrm{LT}(f) = \mathrm{LT}(f_1)e_1$. Пошто је

$$\mathrm{LT}(f_1) = p_1 \mathrm{LT}(g_{11}) + \cdots + p_k \mathrm{LT}(g_{k1}), \text{ за } p_i \in R[X],$$

када помножимо са e_1 добијемо да је

$$\mathrm{LT}(f) = p_1 \mathrm{LT}((g_{11}, g_{12}, \dots, g_{1m})) + \cdots + p_k \mathrm{LT}((g_{k1}, g_{k2}, \dots, g_{km})).$$

Тако да следи да $\mathrm{LT}(f) \in \langle \mathrm{LT}(g) \mid g \in G \rangle$.

Ако је $f_1 = 0$, тада $(f_2, \dots, f_m) \in M_1$ и потом имамо да

$$\mathrm{LT}((f_2, \dots, f_m)) \in \langle \mathrm{LT}(h) \mid h \in G_1 \rangle.$$

Следи да је

$$\mathrm{LT}(f) = \mathrm{LT}((0, f_2, \dots, f_m)) \in \langle \mathrm{LT}((0, h_2, \dots, h_m)) \mid (h_2, \dots, h_m) \in G_1 \rangle,$$

чиме завршавамо доказ. □

Уведимо дефиницију јаке Гребнерове базе за M.

Дефиниција 53. *Нека је M коначно генерисани подмодул од $R[X]^m$, где је R прстен. Подскуп $G = \{g_1, \ldots, g_r\}$ у M је јака Гребнерова база за M ако за било који $f \in M$ постоји $g_i \in G$ тако да $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.*

Као и у случају идеала у $V[X]$ за валуациони домен V, појмови Гребнерове базе и јаке Гребнерове базе су еквивалентни.

Лема 54. *Нека је $G = \{h_1, \ldots, h_r\}$ Гребнерова база за коначно генерисани подмодул M у $V[X]^m$, где је V валуациони домен. Тада је G јака Гребнерова база за M.*

Доказ. Нека је $f = (f_1, \ldots, f_m) \in M$ и нека је

$$i = \min\{1 \leq j \leq m \mid f_j \neq 0\}.$$

Како је G Гребнерова база, имамо да је

$$\mathrm{LT}(f) = p_1 \mathrm{LT}((g_{11}, \ldots, g_{1m})) + \cdots + p_r \mathrm{LT}((g_{r1}, \ldots, g_{rm})),$$

где је $h_j = (g_{j1}, \ldots, g_{jm})$ и $p_j \in V[X]$, за $1 \leq j \leq r$. Очигледно је да неки од p_j може бити нула, као и да неки од сабирака могу да се пониште. У сваком случају, $\mathrm{LT}(f) = \mathrm{LT}(f_i)e_i$ и постоје индекси $s_1, \ldots, s_t \in \{1, \ldots, r\}$ такви да

$$\mathrm{LT}(f_i) = p_{s_1} \mathrm{LT}(g_{s_1 i}) + \cdots + p_{s_t} \mathrm{LT}(g_{s_t i}).$$

Сада смо у истој ситуацији као у тврђењу 29. Следи да постоји $l \in \{s_1, \ldots, s_t\}$ тако да $\mathrm{LT}(g_{li}) \mid \mathrm{LT}(f_i)$. Пошто је $\mathrm{LT}(h_l) = \mathrm{LT}(g_{li})e_i$, важи да је $\mathrm{LT}(h_l) \mid \mathrm{LT}(f)$. □

Сада можемо закључити да важи следећа теорема.

Теорема 55. *Нека је M коначно генерисан подмодул од $V[X]^m$, где је V валуациони домен димензије један и нека је фиксиран мономни поредак POT на $V[X]^m$. Тада постоји јака Гребнерова база G за M.* □

Напомена 56. *Лако се можемо уверити да је сваки Безуов домен и Приферов домен. Наиме, домен је Безуов ако је сваки коначно генерисан идеал главни. Пошто је сваки главни идеал инвертибилан, следи да је у том домену сваки коначно генерисани идеал инвертибилан, што је једна од дефиниција Приферовог домена. Према томе, претходна теорија се може применити и на ову врсту прстена.*

Глава 5

Фон Нојман регуларни комутативни прстени

5.1 Дефиниција и основне особине

Фон Нојман регуларни прстен првобитно је уведен у [36] и изучаван је у контексту функционалне анализе и алгебра оператора. Наравно, ови прстени су проучавани и сами за себе, а како се овде бавимо само комутативним прстенима, више информација о комутативним фон Нојман регуларним прстенима може се наћи у [6]. Ово поглавље започећемо основним особинама ових прстена.

Дефиниција 57. *Прстен R је фон Нојман регуларни прстен ако за сваки елемент $a \in R$ постоји $b \in R$ тако да*

$$a = aba.$$

Неки од примера фон Нојман регуларних прстена су прстен ендоморфизама $\mathrm{End}_K(V)$ векторског простора V (не нужно коначно димензионог) над пољем K, као и прстен $\mathrm{M}_n(R)$ матрица реда n над фон Нојман регуларним прстеном R (видети [25]).

Наведимо неке занимљиве чињенице везано за ове прстене. У [21] можемо наћи следећи резултат: комутативни прстен је фон Нојман регуларан ако и само ако је редукован и димензије нула (теорема 1.16). Затим, сваки леви R-модул је раван ако и само ако је R фон Нојман регуларан (пропозиција 4 у [30]). Локализација у било ком максималном идеалу R_M је поље.

У наставку ове главе бавимо се само комутативним прстенима. У том случају, услов да је прстен фон Нојман регуларан је еквивалентан са постојањем елемента $b \in R$ тако да

$$a = a^2b,$$

то јест, $a(1 - ab) = 0$. Одавде је очигледно да је комутативни фон Нојман регуларни прстен без делитеља нуле заправо једно поље.

Следећа лема нам даје једну корисну репрезентацију неког елемента фон Нојман регуларног прстена. У питању је позната чињеница о комутативним фон Нојман регуларним прстенима, али ће овде бити дат директан доказ. Резултат се може наћи у [6] (видети теорему 2.2).

Лема 58. *Нека је R прстен. Тада је R фон Нојман регуларни прстен ако и само ако за сваки елемент $a \in R$ постоји инвертибилан елемент $u \in R$ и идемпотент $e \in R$ тако да је $a = ue$.*

Доказ. Нека је $b \in R$ такав да је $a = aba$. Важи да је

$$(a + 1 - ab)ab = a^2b + ab - a^2b^2 = a + ab - ab = a.$$

Нека је $u = a + 1 - ab$ и $e = ab$. Како је

$$e^2 = a^2b^2 = ab = e,$$

следи да је e идемпотент. Такође,

$$(a + 1 - ab)(ab^2 + 1 - ab) = 1,$$

па је u инвертибилан.

За другу импликацију, нека је $a = ue \in R$, где је u инвертибилан елемент, а e идемпотент. Важи да је

$$a = ue = uu^{-1} \cdot ue = u^2eu^{-1} = u^2e^2 \cdot u^{-1} = (ue)^2u^{-1} = a^2u^{-1}.$$

Ако ставимо да је $b = u^{-1}$, добијамо тражени облик за елемент a. □

Следећа чињеница је такође врло корисна у разматрању фон Нојман регуларних прстена.

Лема 59. *Нека је R прстен и $e \in R$ идемпотент. За $a \in R$ важи да $e \,|\, a$ ако и само ако је $a = ea$.*

Доказ. Ако $e \,|\, a$, тада је $a = eb$, за $b \in R$. Следи да је $a = eb = eeb = ea$. Доказ у обрнутом смеру је тривијалан. □

Очигледно је да се у фон Нојман регуларним прстенима највише бавимо идемпотентима. На основу леме 59, можемо утврдити да је тачна следећа важна чињеница. Ако су e и s идемпотенти, тада је

$$1 - (1 - e)(1 - s)$$

идемпотент који дели и e и s. Јасно је да су $1 - e$ и $1 - s$ такође идемпотенти, па је због комутативности прстена R то и њихов производ $(1-e)(1-s)$. Следи да је и $1-(1-e)(1-s)$ идемпотент. Приметимо да важи

$$\begin{aligned}(1 - (1 - e)(1 - s))e &= e\\ (1 - (1 - e)(1 - s))s &= s.\end{aligned}$$

Ова чињеница је у основи следеће теореме, као и лема 63 и 65 (видети теорему 4.23 у [29], или лему на 68. стр. у [30]).

Теорема 60. *Нека је J коначно генерисани идеал у R, где је R фон Нојман регуларни прстен. Тада је J генерисан идемпотентним елементом.*

Доказ. Нека је $J = \langle a_1, \ldots, a_n \rangle$. Према леми 58, постоје инвертибилни елементи $u_1, \ldots, u_n$ прстена R и идемпотенти $e_1, \ldots, e_n$ у R тако да је

$$a_i = u_i e_i, \qquad \text{за } 1 \leq i \leq n.$$

Јасно је да $J = \langle e_1, \ldots, e_n \rangle$. Докажимо да је тада и

$$J = \langle 1 - \prod_{i=1}^{n} (1 - e_i) \rangle.$$

Наиме,

$$e_j \cdot (1 - \prod_{i=1}^{n} (1 - e_i)) = e_j - e_j(1 - e_j) \prod_{i \neq j} (1 - e_i) = e_j,$$

за све $j \in \{1, \ldots, n\}$. Према леми 59, елемент $1 - \prod_{i=1}^{n}(1 - e_i)$ дели сваки генератор идеала J, тако да је

$$\langle e_1, \ldots, e_n \rangle \subseteq \langle 1 - \prod_{i=1}^{n} (1 - e_i) \rangle.$$

Такође имамо да

$$1 - \prod_{i=1}^{n} (1 - e_i) = \sum_{i=1}^{n} e_i - \sum_{i \neq j} e_i e_j + \cdots + (-1)^{n-1} \prod_{i=1}^{n} e_i,$$

па је

$$1 - \prod_{i=1}^{n} (1 - e_i) \in \langle e_1, \ldots, e_n \rangle.$$

Производ $\prod_{i=1}^{n}(1 - e_i)$ је идемпотентни елемент, јер су то и елементи $1 - e_1, \ldots, 1 - e_n$. Следи да је $1 - \prod_{i=1}^{n}(1 - e_i)$ такође идемпотент. □

Ова теорема се може доказати и коришћењем математичке индукције. Наиме, ако је $1 - \prod_{i=1}^{k}(1 - e_i)$ идемпотент који дели $e_1, \ldots, e_k$ и e_{k+1} је нови идемпотент, тада је

$$1 - (1 - (1 - \prod_{i=1}^{k} (1 - e_i)))(1 - e_{k+1}) = 1 - \prod_{i=1}^{k} (1 - e_i) \cdot (1 - e_{k+1}) = 1 - \prod_{i=1}^{k+1} (1 - e_i)$$

идемпотент који дели $e_1, \ldots, e_{k+1}$.

Следећа лема се бави питањем анулатора елемента који је идемпотент у комутативном прстену.

Лема 61. *Нека је $e \in R$ идемпотент. Тада је* $\mathrm{Ann}(e) = \langle 1 - e \rangle$.

Доказ. Како је $(1 - e)e = 0$, следи да $\langle 1 - e \rangle \subseteq \mathrm{Ann}(e)$. Са друге стране, нека $a \in \mathrm{Ann}(e)$, то јест, $ae = 0$. Можемо закључити да је

$$a = a \cdot 1 = a(e + 1 - e) = ae + a(1 - e) = a(1 - e) \in \langle 1 - e \rangle,$$

што је и требало доказати. □

На основу до сада изнетих особина које важе за фон Нојман регуларне комутативне прстене, можемо закључити да је фон Нојман регуларни прстен и кохерентан. Наиме, важи да је прстен R кохерентан ако и само ако је пресек два коначно генерисана идеала у R такође коначно генерисан као и да је $\mathrm{Ann}(a)$ коначно генерисан за сваки $a \in R$ (теорема 2.3.2 у [20]). Нека су I и J коначно генерисани идеали у R. На основу претходног, можемо претпоставити да $I = \langle e_1 \rangle$ и $J = \langle e_2 \rangle$, где су e_1 и e_2 идемпотенти. Лако се можемо уверити да је $\langle e_1 \rangle \cap \langle e_2 \rangle = \langle e_1 e_2 \rangle$. Ако је

$$a \in \langle e_1 \rangle \cap \langle e_2 \rangle, \quad \text{тада је } a = e_1 a_1 = e_2 a_2, \quad \text{за } a_1, a_2 \in R,$$

што повлачи да

$$a = e_1 a_1 = e_1 e_1 a_1 = e_1 e_2 a_2, \quad \text{па је } a \in \langle e_1 e_2 \rangle.$$

На основу леме 61, следи и да је $\mathrm{Ann}(a)$ коначно генерисан, одакле закључујемо да за прстен R важи услов кохерентности.

Уведимо сада појам садржаја полинома.

Дефиниција 62. *Нека је $f \in R[X]$ такав да $f(X) = a_n X^n + \cdots + a_1 X + a_0$. Тада се садржај полинома f дефинише као идеал*

$$c(f) = \langle a_n, \ldots, a_0 \rangle \subseteq R.$$

У наставку овог и следећег одељка биће приказани оригинални резултати, који су представљени у [37].

Прво ћемо представити пар резултата који ће нам омогућити да докажемо да у коначно генерисаном идеалу прстена полинома над фон Нојман регуларним прстеном постоји полином чији водећи коефицијент дели све коефицијенте свих полинома тог идеала. Почнимо следећом лемом.

Лема 63. *Нека је $p(X) \in R[X]$, где је R фон Нојман регуларни прстен, такав да је $\deg(p) = n$. Тада постоји полином $r \in \langle p(X) \rangle$ такав да $\deg(r) = n$ и $\langle \mathrm{LC}(r) \rangle = c(p)$.*

Доказ. Без умањења општости, можемо претпоставити да је водећи коефицијент полинома p идемпотент. Наиме, водећи коефицијент је производ једног инвертибилног и једног идемпотентног елемента. Можемо помножити цео полином p са одговарајућим инвертибилним елементом, што неће утицати на идеале $\langle p(X) \rangle$ и $c(p)$.

Нека је

$$p(X) = e_n X^n + u_{n-1} e_{n-1} X^{n-1} + u_{n-2} e_{n-2} X^{n-2} + \cdots + u_1 e_1 X + u_0 e_0,$$

где су $u_{n-1}, \ldots, u_0$ инвертибилни елементи и $e_n, \ldots, e_0$ идемпотенти. Дефинишимо прво низ елемената $e^{(k)}$ рекурзивно:

$$\begin{aligned} e^{(0)} &= e_n \\ e^{(k)} &= e^{(k-1)} + (1 - e^{(k-1)}) e_{n-k}, \ \text{за } 1 \leq k \leq n. \end{aligned}$$

Као и у дискусији после теореме 60, важи да је за свако $0 \leq k \leq n$ елемент $e^{(k)}$ идемпотент, као и да је

$$e^{(k)} = 1 - (1 - e_n)(1 - e_{n-1}) \cdots (1 - e_{n-k}),$$

одакле се лако може видети да $e^{(k)}$ дели елементе $e_n, \dots, e_{n-k}$. Такође је, према теореми 60, $c(p) = \langle e^{(n)} \rangle$.

Дефинишимо сада полином $r^* \in R[X]$ тако да

$$r^*(X) = 1 + u_{n-1}^{-1}(1 - e^{(0)})X + u_{n-2}^{-1}(1 - e^{(1)})X^2 + \cdots + u_0^{-1}(1 - e^{(n-1)})X^n.$$

Пошто је

$$e_s(1 - e^{(k)}) = 0, \qquad \text{за свако } s \geq n - k,$$

важи да је $\deg(p \cdot r^*) = n$. Осим тога,

$$\begin{aligned}
\mathrm{LC}(pr^*) &= e_n + (1 - e^{(0)})e_{n-1} + (1 - e^{(1)})e_{n-2} + \cdots + (1 - e^{(n-2)})e_1 + (1 - e^{(n-1)})e_0 \\
&= e^{(1)} + (1 - e^{(1)})e_{n-2} + \cdots + (1 - e^{(n-2)})e_1 + (1 - e^{(n-1)})e_0 \\
&= \cdots \\
&= e^{(n-1)} + (1 - e^{(n-1)})e_0 \\
&= e^{(n)}.
\end{aligned}$$

За крај доказа, дефинишимо тражени полином са $r = pr^*$. □

Напомена 64. *У леми 63, ако је један од коефицијената полинома p инвертибилан елемент, то јест, ако је неки идемпотент e_k једнак 1, представљена конструкција даје моничан полином r. У низу елемената $e^{(s)}$, сви елементи $e^{(n-k)}, \dots, e^{(n)}$ ће бити једнаки 1.*

На сличан начин, можемо конструисати полином такав да његов водећи коефицијент дели све коефицијенте два дата полинома p и q и чији степен је једнак $\max\{\deg(p), \deg(q)\}$.

Лема 65. *Нека су $p(X), q(X) \in R[X]$, где је R фон Нојман регуларни прстен, такви да $\deg(p) = n$ и $\deg(q) = m \leq n$. Тада постоји полином $r \in \langle p(X), q(X) \rangle$ такав да је $\deg(r) = n$ и $\langle \mathrm{LC}(r) \rangle = c(p) + c(q)$.*

Доказ. Према леми 63, постоји полином

$$r_1 \in \langle p(X) \rangle \text{ такав да } \deg(r_1) = n \text{ и } \langle \mathrm{LC}(r_1) \rangle = c(p).$$

Можемо претпоставити да је $\mathrm{LC}(r_1) = e$, где је e идемпотент. Нека је

$$q(X) = e_m X^m + u_{m-1}e_{m-1}X^{m-1} + u_{m-2}e_{m-2}X^{m-2} + \cdots + u_1 e_1 X + u_0 e_0,$$

где су $u_{m-1}, \dots, u_0$ инвертибилни елементи и $e_m, \dots, e_0$ су идемпотенти. Овде такође можемо претпоставити, без умањења општости, да је водећи коефицијент полинома q идемпотент. Као и у претходној леми, дефинишемо низ елемената $e^{(k)}$:

$$\begin{aligned}
e^{(0)} &= e \\
e^{(1)} &= e^{(0)} + (1 - e^{(0)})e_m \\
e^{(k)} &= e^{(k-1)} + (1 - e^{(k-1)})e_{m-k+1}, \text{ за } 2 \leq k \leq m + 1.
\end{aligned}$$

Ови елементи су идемпотенти и $e^{(k)}$ дели елементе $e, e_m, \dots, e_{m-k+1}$ за $1 \leq k \leq m + 1$, што се лако може видети из једнакости

$$e^{(k)} = 1 - (1 - e)(1 - e_m)(1 - e_{m-1}) \cdots (1 - e_{m-k+1}).$$

Очигледно је $e^{(m+1)}$ елемент који дели e (то јест, све коефицијенте полинома p) и такође дели све коефицијенте полинома q. Тако да је

$$\langle e^{(m+1)} \rangle = c(p) + c(q).$$

Нека је $r^* \in R[X]$ такав да

$$\begin{aligned} r^*(X) = (1-e^{(0)})X^{n-m} &+ u_{m-1}^{-1}(1-e^{(1)})X^{n-m+1} + u_{m-2}^{-1}(1-e^{(2)})X^{n-m+2} + \\ &\cdots + u_1^{-1}(1-e^{(m-1)})X^{n-1} + u_0^{-1}(1-e^{(m)})X^n. \end{aligned}$$

Уочимо полином $r_1 + qr^*$. Знамо да је

$$e_s(1-e^{(k)}) = 0, \qquad \text{за све } s \geq m-k+1,$$

одакле можемо закључити да

$$\begin{aligned} \mathrm{LC}(r_1 + qr^*) &= e + (1-e^{(0)})e_m + (1-e^{(1)})e_{m-1} + \cdots + (1-e^{(m-1)})e_1 + (1-e^{(m)})e_0 \\ &= e^{(1)} + (1-e^{(1)})e_{m-1} + \cdots + (1-e^{(m-1)})e_1 + (1-e^{(m)})e_0 \\ &= \cdots \\ &= e^{(m)} + (1-e^{(m)})e_0 \\ &= e^{(m+1)}. \end{aligned}$$

Нека је $r = r_1 + qr^*$. Тада

$$r \in \langle p(X) \rangle + \langle q(X) \rangle = \langle p(X), q(X) \rangle.$$

С обзиром на то да $\deg(r) = n$ и $\mathrm{LC}(r) = e^{(m+1)}$, следи да је $\langle \mathrm{LC}(r) \rangle = c(p) + c(q)$. □

Докажимо сада главни резултат овог одељка.

Теорема 66. *Нека је R фон Нојман регуларни прстен и $I = \langle f_1, \ldots, f_m \rangle$ идеал у $R[X]$. Тада постоји полином $f \in I$ такав да је*

$$\deg(f) = \max\{\deg(f_1), \ldots, \deg(f_m)\} \text{ и } \langle \mathrm{LC}(f) \rangle = c(f_1) + \cdots + c(f_m).$$

Доказ. Можемо почети од генератора идеала I који је највећег степена. Тада ћемо узастопном применом претходне леме добити елемент у I такав да његов водећи коефицијент дели све коефицијенте свих генератора у I. □

5.2 Гребнерова база

У овом одељку ћемо показати да сваки коначно генерисани идеал I у $R[X]$, где је R фон Нојман регуларни прстен, има Гребнерову базу.

Почнимо са једном лемом, где ћемо испитивати коначну генерисаност асоцираних R-модула $I_0, I_1, \ldots, I_{n-1}$, где је I идеал у $R[X]$.

Лема 67. *Нека је $I = \langle f_1, \ldots, f_m \rangle$ коначно генерисани идеал у прстену $R[X]$, где је R фон Нојман регуларни прстен. Тада су R-модули $I_0, I_1, \ldots, I_{n-1}$ коначно генерисани, при чему је $n = \max\{\deg(f_1), \ldots, \deg(f_m)\}$.*

Доказ. Према теореми 66, постоји полином $f \in I$ тако да $\mathrm{LC}(f)$ дели све коефицијенте свих полинома у I и такав да је $\deg(f) = n$. Тада је и $I = \langle f, f_1, \ldots, f_m \rangle$.

Претпоставимо да је $\mathrm{LC}(f) = e$, за идемпотент e. Прво ћемо показати да је I_{n-1} коначно генерисани R-модул. Наиме, као и у главама 2 и 3, елементи

$$\rho(X^i f_j, f), \qquad 0 \le i \le n-1, \qquad 1 \le j \le m,$$

чине скуп генератора овог R-модула. За почетак приметимо да су ови остаци добро дефинисани, јер су сви коефицијенти полинома $f_1, \ldots, f_m$ дељиви са e.

Нека је $h \in I_{n-1}$. Како је $h \in I$, следи да је

$$h = rf + r_1 f_1 + \cdots + r_m f_m,$$

за неке $r, r_1, \ldots, r_m \in R[X]$. Можемо претпоставити да $\deg(r_1), \ldots, \deg(r_m) < n$. У супротном, било би $f_j = e p_j$, за $1 \le j \le m$, и тада би важило

$$h = rf + r_1 f_1 + \cdots + r_m f_m = rf + e r_1 p_1 + \cdots + e r_m p_m.$$

Следи да се $er_1, \ldots, er_m$ могу поделити са f. Нека је

$$e r_j = q_j f + t_j, \qquad \deg(t_j) < n,\ 1 \le j \le m.$$

Коефицијенти полинома t_j такође су дељиви са e. Ако је $t_j = e s_j$, за $1 \le j \le m$, тада је

$$\begin{aligned} h &= rf + (q_1 f + t_1)p_1 + \cdots + (q_m f + t_m)p_m \\ &= rf + (q_1 f + e s_1)p_1 + \cdots + (q_m f + e s_m)p_m \\ &= (r + q_1 p_1 + \cdots + q_m p_m)f + s_1 e p_1 + \cdots + s_m e p_m \\ &= (r + q_1 p_1 + \cdots + q_m p_m)f + s_1 f_1 + \cdots + s_m f_m. \end{aligned}$$

Очигледно, $\deg(s_j)(= \deg(t_j))$ је мањи од n.

Дакле, нека је

$$r_j = \sum_{i=0}^{k_j} \alpha_i^{(j)} X^i, \qquad k_j < n, \qquad 1 \le j \le m,$$

$$X^i f_j = f s_i^{(j)} + \rho(X^i f_j, f), \qquad 0 \le i \le k_j, \qquad 1 \le j \le m.$$

Следи да је

$$h = f\left(r + \sum_{j=1}^{m}\sum_{i=0}^{k_j} \alpha_i^{(j)} s_i^{(j)}\right) + \sum_{j=1}^{m}\sum_{i=0}^{k_j} \alpha_i^{(j)} \rho(X^i f_j, f).$$

Према томе, полином h је облика $fp + q$, за $p \in R[X]$ и где је q једна R-линеарна комбинација полинома $\rho(X^i f_j, f)$, $0 \le i \le k_j$, $1 \le j \le m$. Пошто је $h \in I_{n-1}$, следи да је $\deg(h) < n$.

Ако је $p = 0$, тада је h једна R-линеарна комбинација остатака $\rho(X^i f_j, f)$. Претпоставимо да p није нула. Нека је

$$p = \beta_l X^l + \cdots + \beta_0, \text{ где је } \beta_l \neq 0.$$

Производ fp можемо видети као

$$fp = f \cdot \beta_l X^l + f \cdot \beta_{l-1} X^{l-1} + \cdots + f \cdot \beta_0.$$

Коефицијент у fp уз моном X^{n+l} мора бити једнак нули. Следи да је $e\beta_l = 0$. На основу леме 61, $\mathrm{Ann}(e) = \langle 1 - e \rangle$. Сада следи да је $\beta_l = a(1-e)$, за $a \in R$. С обзиром на то да је сваки коефицијент полинома f дељив са e, имамо да је

$$f \cdot \beta_l X^l = 0.$$

На сличан начин, како $e\beta_{l-1}$ мора бити нула, следи да је β_{l-1} дељиво са $1-e$ и тада је $f \cdot \beta_{l-1} X^{l-1} = 0$. Понављајући овај поступак добијамо да је $f \cdot p = 0$.

Следи да је у сваком случају полином h једна R-линеарна комбинација остатака $\rho(X^i f_j, f)$. Из чињенице да $\rho(X^i f_j, f) = X^i f_j - f s_i^{(j)}$ следи да сви остаци $\rho(X^i f_j, f)$, за $0 \leq i \leq k_j$ и $1 \leq j \leq m$, припадају идеалу I, а самим тим припадају и I_{n-1}. Можемо закључити да ови полиноми представљају генераторни скуп за R-модул I_{n-1}.

Докажимо сада да су и остали R-модули $I_{n-2}, \ldots, I_0$ коначно генерисани. Нека су $\pi_k : R[X]_k \to R$ хомоморфизми такви да је $\pi_k(p)$ коефицијент производа X^k у полиному p. Ако је $I_{n-1} = \{0\}$, тада је $I_0 = \cdots = I_{n-2} = \{0\}$.

Ако је $I_{n-1} \neq \{0\}$, тада је слика $\pi_{n-1}(I_{n-1})$ такође коначно генерисани идеал у R. Према теореми 60, ова слика је главни идеал $\pi_{n-1}(I_{n-1}) = \langle c_{n-1} \rangle$ и c_{n-1} је ненула идемпотент. Нека је $g_{n-1} \in I_{n-1}$ полином такав да $\mathrm{LT}(g_{n-1}) = c_{n-1} X^{n-1}$.

Ако је $h \in I_{n-2}$, тада $h \in I_{n-1}$ и

$$h = \sum r_{ij} \rho(X^i f_j, f), \qquad r_{ij} \in R,\ 1 \leq j \leq m,\ 0 \leq i \leq n-1.$$

Пошто су сви остаци $\rho(X^i f_j, f)$ у I_{n-1}, можемо их поделити са g_{n-1}. Тако да важи једнакост $\rho(X^i f_j, f) = a_{ij} g_{n-1} + f_{ij}$. Сада имамо да је

$$h = \sum r_{ij}(a_{ij} g_{n-1} + f_{ij}) = \left(\sum r_{ij} a_{ij} \right) g_{n-1} + \sum r_{ij} f_{ij}.$$

Како $h \in I_{n-2}$, следи да $\sum r_{ij} a_{ij}$ мора припадати $\mathrm{Ann}(c_{n-1})$. На основу леме 61, важи да $\mathrm{Ann}(c_{n-1}) = \langle 1 - c_{n-1} \rangle$. Следи да је сваки елемент у I_{n-2} једнак R-линеарној комбинацији полинома

$$(1 - c_{n-1}) g_{n-1} \text{ и } f_{ij} = \rho(\rho(X^i f_j, f), g_{n-1}), \text{ где је } 1 \leq j \leq m,\ 0 \leq i \leq n-1.$$

Овај поступак може се редом примењивати и на остале модуле, одакле следи тврђење леме. □

Захваљујући представљеној леми, сада можемо доказати главну теорему.

Теорема 68. *Нека је R фон Нојман регуларни прстен и I коначно генерисани идеал у прстену $R[X]$. Тада постоји јака Гребнерова база за I.*

Доказ. Нека је $I = \langle f_1, \ldots, f_m \rangle$. На основу теореме 66, постоји полином $f \in I$ такав да је

$$\deg(f) = \max\{\deg(f_1), \ldots, \deg(f_m)\} (= n)$$

и $\mathrm{LC}(f)$ дели све коефицијенте свих полинома у I. Даље, према леми 67, R-модули $I_{n-1}, \ldots, I_0$ су коначно генерисани. Као и у доказу ове леме, нека су $\pi_k : R[X]_k \to R$ хомоморфизми такви да је $\pi_k(p)$ коефицијент производа X^k у полиному p. Нека је $\pi_k(I_k) = \langle c_k \rangle$ и нека је $g_k \in I_k$ полином такав да $\mathrm{LT}(g_k) = c_k X^k$. Тада је јака Гребнерова база G за I дата са

$$G = \{f, g_i \,|\, i \in \{0, \ldots, n-1\}, g_i \neq 0\}.$$

Наиме, претпоставимо да је $p \in I \setminus \{0\}$. Ако је $\deg(p) \geq n$, тада $\mathrm{LT}(f) \mid \mathrm{LT}(p)$. Ако је $\deg(p) = k < n$, тада $p \in I_k$. Следи да је $c_k X^k \mid \mathrm{LT}(p)$, чиме смо и доказали тврђење теореме. □

Напомена 69. *Сетимо се да је Булов прстен B онај у коме је сваки елемент идемпотент. Дакле, за свако $e \in B$ важи да*

$$e = e^2 = e \cdot 1 \cdot e,$$

што значи да је B и фон Нојман регуларни прстен. Сваки Булов прстен је и комутативан, на основу чега можемо закључити да резултати изложени у овом поглављу важе и за Булове прстене.

Можемо се уверити да је сваки фон Нојман регуларни прстен R и аритметички. На основу дефиниције 42 и коментара после, следи да је довољно доказати да

$$I \cap (J + K) \subseteq (I \cap J) + (I \cap K),$$

за све ненула идеале I, J, K у R. Нека је $a \in I \cap (J + K)$. Тада је $a \in I$, као и $a = b + c$, за $b \in J$ и $c \in K$. Важи и да

$$a = u_1 e_1 = u_2 e_2 + u_3 e_3, \text{ за идемпотенте } e_1 \in I, e_2 \in J, e_3 \in K \text{ и } u_1, u_2, u_3 \in \mathrm{U}(R).$$

Следи да је

$$a = u_1 e_1 = u_1 e_1 e_1 = u_2 e_2 e_1 + u_3 e_3 e_1.$$

Како је

$$u_2 e_2 e_1 \in I \cap J \text{ и } u_3 e_3 e_1 \in I \cap K,$$

следи да $a \in (I \cap J) + (I \cap K)$.

У претходној глави споменули смо да је аритметички прстен и Приферов прстен, тако да сада можемо закључити да ако је R фон Нојман регуларни комутативни прстен, тада је R и Приферов прстен. Дакле, у овој глави смо доказали да постоји јака Гребнерова база за коначно генерисане идеале над једним типом Приферових прстена.

Директни производ поља представља један од примера комутативних фон Нојман регуларних прстена. Можемо демонстрирати претходне резултате на следећем примеру.

Пример 70. Нека је $R = \prod_{k=1}^{\infty} \mathbb{F}_3$, где је $\mathbb{F}_3$ коначно поље реда 3. Нека су

$$f_1 = \alpha_2 X^2 + \alpha_1 X + \alpha_0 \qquad \text{и} \qquad f_2 = \beta_2 X^2 + \beta_0,$$

два полинома над прстеном R, где је

$$\begin{aligned}
\alpha_2 &= (2,1,1,0,0,0,0,0,\dots) \\
\alpha_1 &= (1,1,2,2,0,0,0,0,\dots) \\
\alpha_0 &= (0,0,0,0,1,0,0,0,\dots) \\
\\
\beta_2 &= (0,0,1,0,0,1,0,0,1,\dots) \\
\beta_0 &= (0,2,2,0,2,2,0,2,2,\dots).
\end{aligned}$$

Одредимо Гребнерову базу за идеал $I = \langle f_1, f_2\rangle$ користећи резултате из претходних теорема и њихових доказа. Како α_2 није идемпотент, можемо помножити f_1 инвертибилним елементом $(2,1,1,1,1,\dots)$ и тиме добијамо полином

$$\tilde{f}_1 = (1,1,1,0,0,0,\dots)X^2 + (2,1,2,2,0,0,\dots)X + (0,0,0,0,1,0,\dots).$$

Имамо да је $I = \langle \tilde{f}_1, f_2\rangle$. Можемо применити кораке из леме 63 да добијемо полином

$$r^* = (0,0,0,0,1,1,1,\dots)X^2 + (0,0,0,2,1,1,1,\dots)X + (1,1,1,1,1,1,\dots),$$

а потом и полином

$$r_1 = \tilde{f}_1 \cdot r^* = (1,1,1,1,1,0,0,\dots)X^2 + (2,1,2,2,1,0,0,\dots)X + (0,0,0,0,1,0,0,\dots),$$

који је такав да

$$\mathrm{LC}(r_1) = e = (1,1,1,1,1,0,0,\dots)$$

дели све коефицијенте полинома $\tilde{f}_1$.

Наставимо са применом леме 65 и формирајмо полином

$$r^{**} = (0,0,0,0,0,0,1,2,0,1,2,0,1,2,0,\dots)X^2 + (0,0,0,0,0,1,1,1,1,1,\dots),$$

као и

$$\begin{aligned}
r_1 + f_2 r^{**} \;=\;& (1,1,1,1,1,1,0,1,1,0,1,1,\dots)X^2 + (2,1,2,2,1,0,0,\dots)X + \\
&+ (0,0,0,0,1,2,0,2,2,0,2,2,\dots).
\end{aligned}$$

Полином $f = r_1 + f_2 r^{**}$ је такав да његов водећи коефицијент дели све коефицијенте полинома $\tilde{f}_1$ и f_2. Нека је $f = r_1 + f_2 r^{**}$.

Сада је $I = \langle f, \tilde{f}_1, f_2\rangle$. На исти начин као и у теореми 68, наћи ћемо генераторе за R-модуле I_1 и I_0. Важи да је

$$\begin{aligned}
\rho(\tilde{f}_1, f) &= (0,0,0,2,0,\dots)X + (0,0,0,0,1,0,\dots) \\
\rho(X\tilde{f}_1, f) &= (0,0,0,1,1,0,\dots)X \\
\rho(f_2, f) &= (0,0,1,0,0,\dots)X + (0,2,2,0,2,0,0,2,0,0,2,0,\dots) \\
\rho(Xf_2, f) &= (0,2,0,0,2,0,0,2,0,0,2,0,\dots)X.
\end{aligned}$$

Приметимо да је

$$\pi_1(I_1) = \langle (0,1,1,1,1,0,0,1,0,0,1,0,0,1,\dots)\rangle.$$

Нека је

$$\begin{aligned} g_1 &= (1,1,1,2,1,1,\dots)\rho(\tilde{f}_1, f) + \rho(X\tilde{f}_1, f) + \rho(f_2, f) + (1,2,1,1,2,1,1,2,1,\dots)\rho(Xf_2, f) \\ &= (0,1,1,2,2,0,0,1,0,0,1,\dots)X + (0,2,2,0,0,0,0,2,0,0,2,0,\dots). \end{aligned}$$

Помножимо овај полином инвертибилним елементом $(1,1,1,2,2,1,1,1,\dots)$, чиме добијамо полином

$$g_1^* = (0,1,1,1,1,0,0,1,0,0,1,\dots)X + (0,2,2,0,0,0,0,2,0,0,2,0,\dots).$$

Даље је

$$\mathrm{Ann}((0,1,1,1,1,0,0,1,0,0,1,\dots)) = \langle (1,0,0,0,0,1,1,0,1,1,0,1,1,\dots)\rangle,$$

и видимо да је $(1,0,0,0,0,1,1,0,1,1,0,1,1,\dots) \cdot g_1^* = 0$.

Настављамо са рачуном:

$$\begin{aligned} \rho(\rho(\tilde{f}_1, f), g_1^*) &= (0,0,0,0,1,0,\dots) \\ \rho(\rho(X\tilde{f}_1, f), g_1^*) &= 0 \\ \rho(\rho(f_2, f), g_1^*) &= (0,0,0,0,2,0,0,2,0,0,2,0,\dots) \\ \rho(\rho(Xf_2, f), g_1^*) &= (0,2,0,0,0,0,0,2,0,0,2,0,0,2,\dots). \end{aligned}$$

Сада се можемо уверити да је

$$I_0 = \pi(I_0) = \langle (0,1,0,0,0,0,0,1,0,0,1,0,0,\dots)\rangle.$$

Нека је $g_0 = (0,1,0,0,0,0,0,1,0,0,1,0,0,\dots)$. Према теореми 68, скуп $\{f, g_1^*, g_0\}$ чини Гребнерову базу за I.

Глава 6

Радикалски идеали у $(p-1)$-нил-чистим комутативним прстенима

6.1 О проблему припадности идеалу

У претходној глави значајну улогу су имали идемпотентни елементи и видели смо које закључке можемо добити захваљујући чињеници да је сваки елемент фон Нојман регуларног и комутативног прстена облика ue, за инвертибилни елемент u и идемпотентни елемент e. У $(p-1)$-нил-чистим прстенима идемпотентни елементи такође играју важну улогу. Представимо прво дефиницију.

Дефиниција 71. *Елемент прстена R је s-нил-чист ако је облика*

$$e_1 + \cdots + e_s + b,$$

где су $e_1, \ldots, e_s$ идемпотентни елементи, за $s \geq 1$, а b нилпотентан. Прстен у коме сваки елемент има ову особину се назива s-нил-чист прстен.

Почевши од увођења појма чистог прстена, у коме је сваки елемент збир једног идемпотента и једног инвертибилног елемента, уведене су и друге класе прстена са сличним условима. То су класе јако чистих прстена, нил-чистих, јако нил-чистих, 2-нил-чистих и тако даље. Постоји богата литература о свим наведеним класама, мада су овде од значаја нарочито нил-чисти прстени, у којима је сваки елемент сума једног идемпотентног и једног нилпотентног елемента, као и јако нил-чисти прстени, у којима имамо још додатни услов комутативности дата два елемента (видети, на пример, [15] и [11]). Појам s-нил-чистог прстена, као генерализације ових последњих, уведен је у [26].

Према [26], анализа s-нил-чистих се може свести на случај када је $s = p-1$, за прост број p, тако да ћемо се и овде бавити само овим случајем. Елемент прстена R је јако $(p-1)$-нил-чист ако је $(p-1)$-нил-чист и притом важи да сви елементи у датој суми међусобно комутирају. Како је прстен R по претпоставци комутативан, овде заправо разматрамо јако $(p-1)$-нил-чисте прстене.

Представимо сада преформулацију пропозиције 2.3 из [27] која ће нам бити корисна за сврху овог поглавља. Све пропозиције и последице које се цитирају у наредном доказу су из [26]. Споменимо још да ћемо користити ознаку:

$$(a)_s = a(a-1)\cdots(a-(s-1)),$$

где је $a \in R$ и $s > 1$.

Лема 72. *Нека је R један $(p-1)$-нил-чисӣ ӣрсӣен. Тада је $R/\mathrm{Nil}(R)$ фон Нојман реīуларни ӣрсӣен.*

Доказ. Да је $\mathrm{Nil}(R) = \mathrm{J}(R)$, као и да је $R/\mathrm{J}(R)$ прстен који је $(p-1)$-нил-чист може се наћи у последици 5, а из других резултата истог рада следи и да прстен R можемо видети као

$$R_1 \times \cdots \times R_l,$$

при чему је $\mathrm{char}(R_i) = p_i^{\alpha_i}$, где је p_i прост број и нилпотентан елемент у R_i за свако $i \in \{1, \ldots, l\}$. Важи да је

$$\mathrm{Nil}\left(\prod_{i=1}^{l} R_i\right) = \prod_{i=1}^{l} \mathrm{Nil}(R_i).$$

Докажимо да за произвољни елемент $a \in R/\mathrm{Nil}(R)$ важи да постоји елемент b истог прстена тако да је $a = a^2 b$. Нека је

$$a = (a_1, \ldots, a_l) \in R/\mathrm{Nil}(R) = \left(\prod_{i=1}^{l} R_i\right) \Big/ \mathrm{Nil}\left(\prod_{i=1}^{l} R_i\right) \cong \prod_{i=1}^{l} R_i/\mathrm{Nil}(R_i).$$

Пошто је елемент a $(p-1)$-нил-чист, то важи и за сваки од елемената a_i. Следи да је $(a_i)_p$ нилпотентан (пропозиција 6), а потом и да је $(a_i)_{p_i}$ нилпотентан (последица 2). Тада је $a_i^{p_i} - a_i$ нилпотентан у $R_i/\mathrm{Nil}(R_i)$, $1 \leq i \leq l$ (пропозиција 8). У сваком од наведених прстена $R_i/\mathrm{Nil}(R_i)$ нема нилпотентних ненула елемената, тако да следи да је $a_i^{p_i} = a_i$, за све $i \in \{1, \ldots, l\}$. Како је у сваком случају $p_i \geq 2$, следи да се може написати

$$a_i^2 \cdot a_i^{p_i - 2} = a_i, \qquad \text{за } 1 \leq i \leq l.$$

Ако ставимо да

$$b = (a_1^{p_1 - 2}, \ldots, a_l^{p_l - 2}),$$

тада важи да је $a = a^2 b$. □

Из ове леме можемо једноставно увидети познату чињеницу да је за нил-чисти комутативни прстен R количник $R/\mathrm{J}(R)$ Булов прстен ($p = p_1 = \cdots = p_l = 2$, па је $a_i^2 = a_i$ за све $1 \leq i \leq l$).

Сетимо се да је радикалски идеал I у прстену A онај за који важи да је $I = r(I)$, где је

$$r(I) = \{a \in A \,|\, a^n \in I, \text{ за неко } n \in \mathbb{N}\}$$

радикал идеала I. Једноставно је доказати чињеницу да сваки радикалски идеал у неком прстену садржи све нилпотентне елементе тог прстена. Наиме, ако је $a \in A$ нилпотентан, тада постоји $n \in \mathbb{N}$ тако да $a^n = 0$. Даље важи да

$$a^n = 0 \in I,$$

што повлачи да

$$a \in r(I) = I,$$

за било који радикалски идеал I у R.

Ако је у питању прстен полинома, важи да

$$\mathrm{Nil}(R[X]) = \mathrm{Nil}(R)[X],$$

где десна страна означава скуп полинома чији коефицијенти су нилпотентни (видети [7] на пример).

Следећа лема описује облик коначно генерисаних радикалских идеала у $R[X]$, за $(p-1)$-нил-чисти прстен R.

Лема 73. *Нека је I коначно генерисан радикалски идеал у прстену $R[X]$, где је R један $(p-1)$-нил-чист прстен. Тада је I облика $J + \mathrm{Nil}(R)[X]$, где је J коначно генерисан идеал и коефицијенти свих његових генератора су збирови идемпотената.*

Доказ. Нека је f било који елемент прстена $R[X]$. Тада је

$$f = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_s + b_s)X^s,$$

где су $a_0, \ldots, a_s$ збирови највише $p-1$ идемпотентних елемената, а $b_0, \ldots, b_s$ су нилпотентни. Нека су

$$p = a_0 + a_1X + \cdots + a_sX^s, \qquad q = b_0 + b_1X + \cdots + b_sX^s.$$

Следи да за сваки елемент прстена $R[X]$ важи да се може написати као збир $p+q$, где су коефицијенти од p збирови идемпотената, а коефицијенти од q нилпотенти.

Овако можемо представити сваки од генератора идеала I. Наиме, нека важи да је $I = \langle f_1, \ldots, f_k \rangle$ и нека је

$$f_i = p_i + q_i, \qquad 1 \leq i \leq k.$$

Сви коефицијенти од q_i су нилпотенти, па постоје довољно велики $m_i \in \mathbb{N}$ тако да је

$$(q_i(X))^{m_i} = 0, \qquad 1 \leq i \leq k.$$

Следи да за свако $i \in \{1, \ldots, k\}$ важи да

$$q_i \in \mathrm{Nil}(R[X]) \subseteq I.$$

Такође важи да

$$p_i = f_i - q_i \in I, \text{ за свако } i \in \{1, \ldots, k\}.$$

Посматрајмо идеал

$$J + \mathrm{Nil}(R)[X],$$

где је $J = \langle p_1, \ldots, p_k \rangle$ идеал у коме су коефицијенти свих његових генератора збирови идемпотената. Јасно је да је наведени збир идеала садржан у I.

Са друге стране, за елемент $f \in I$ важи да је облика

$$f = g_1f_1 + \cdots + g_kf_k = g_1p_1 + \cdots + g_kp_k + g_1q_1 + \cdots + g_kq_k,$$

за неке $g_1, \ldots, g_k \in R[X]$. Пошто одатле следи да је и $I \subseteq J + \mathrm{Nil}(R)[X]$, имамо да је $I = J + \mathrm{Nil}(R)[X]$, чиме смо доказали тврђење леме. □

У претходним главама били смо у могућности да експлицитно одредимо Гребнерову базу идеала. Уместо овога, у случају $(p-1)$-нил-чистих прстена, можемо да решимо проблем припадности идеалу.

Теорема 74. *Нека је I коначно генерисан радикалски идеал у прстену $R[X]$, за $(p-1)$-нил-чисти прстен R. Тада је могуће решити проблем припадности идеалу I, за сваки полином $f \in R[X]$.*

Доказ. Нека је f било који елемент прстена $R[X]$. Слично као у доказу леме 73, полином f се може написати као збир $p+q$, где су коефицијенти од p збирови идемпотената, а коефицијенти од q нилпотенти. Постоји довољно велико $m \in \mathbb{N}$ тако да је $q(X)^m = 0$, па пошто је I радикалски идеал, следи да

$$q \in \mathrm{Nil}(R[X]) \subseteq I.$$

На основу претходне леме, можемо написати I у облику $J + \mathrm{Nil}(R)[X]$, при чему је $J = \langle p_1, \dots, p_k \rangle$ за полиноме $p_1, \dots, p_k$ чији коефицијенти су збирови идемпотената. Посматрајмо количник

$$R[X]/\mathrm{Nil}(R)[X] \cong (R/\mathrm{Nil}(R))[X].$$

Према леми 72, последњи прстен полинома је над фон Нојман регуларним прстеном, тако да ћемо у том циљу користити теорему 68. Пројекција идеала I на количник $R[X]/\mathrm{Nil}(R)[X]$ је идеал $\bar{I} = \langle \bar{p}_1, \dots, \bar{p}_k \rangle$, при чему су $\bar{p}_i$ класе одговарајућих полинома у $R[X]/\mathrm{Nil}(R)[X]$.

Следи да

$$f \in I \qquad \Longleftrightarrow \qquad \bar{f} \in \bar{I},$$

где важи да је $\bar{f} = \bar{p}$. За коначно генерисани идеал $\bar{I}$ над фон Нојман регуларним прстеном $R/\mathrm{Nil}(R)$ можемо одредити јаку Гребнерову базу: нека је то $\{g_1, \dots, g_s\}$. Према томе, полином $f \in I$ ако и само ако $\mathrm{LT}(g_i) \mid \mathrm{LT}(\bar{p})$ за неко $i \in \{1, \dots, s\}$. $\square$

6.2 Примери

Поставља се питање постојања $(p-1)$-нил-чистог комутативног прстена који није Нетерин. Један пример био би следећи. Нека је G Абелова група са бесконачним скупом генератора $\{g_1, g_2, \dots\}$ и R прстен. Посматрајмо групни прстен $R[G]$ и низ идеала

$$\langle g_1 - 1 \rangle \subseteq \langle g_1 - 1, g_2 - 1 \rangle \subseteq \langle g_1 - 1, g_2 - 1, g_3 - 1 \rangle \subseteq \cdots$$

где је 1 јединица овог групног прстена и једнака је $1_R 1_G$, при чему је 1_R јединица прстена R, а 1_G неутрал групе G. Докажимо да је овај низ идеала строго растући, чиме ћемо доказати да $R[G]$ није Нетерин.

Нека су G_k подгрупе групе G тако да

$$G_k = \langle g_1, \dots, g_k \rangle.$$

Посматрајмо хомоморфизме

$$\Phi_k : R[G] \to R[G/G_k],$$

који су дефинисани на следећи начин. Нека је

$$\alpha = r_{i_1}g_{i_1} + r_{i_2}g_{i_2} + \cdots + r_{i_s}g_{i_s} \in R[G]$$

тако да $i_1 < i_2 < \cdots < i_s$. Ако је $k < i_1$, тада је $\Phi_k(\alpha) = \alpha$. Ако је $i_l \leq k < i_{l+1}$, тада је

$$\Phi_k(\alpha) = r_{i_1}1 + \cdots + r_{i_l}1 + r_{i_{l+1}}g_{i_{l+1}} + \cdots + r_{i_s}g_{i_s}.$$

Наиме, све елементе g_i где је $i < k$ сликамо у 1, а остале елементе у саме себе, то јест, у одговарајуће класе елемената.

Приметимо да је

$$\mathrm{Ker}(\Phi_k) = \langle g_1 - 1, \ldots, g_k - 1 \rangle.$$

Једна инклузија је очигледна. Ако је

$$r_{i_1}1 + \cdots + r_{i_l}1 + r_{i_{l+1}}g_{i_{l+1}} + \cdots + r_{i_s}g_{i_s} = 0,$$

тада је

$$r_{i_{l+1}}g_{i_{l+1}} + \cdots + r_{i_s}g_{i_s} = -r_{i_1}1 - \cdots - r_{i_l}1,$$

а потом и

$$\begin{aligned} r_{i_1}g_{i_1} + \cdots + r_{i_s}g_{i_s} &= r_{i_1}g_{i_1} + \cdots + r_{i_l}g_{i_l} - r_{i_1}1 - \cdots - r_{i_l}1 \\ &= r_{i_1}(g_{i_1} - 1) + \cdots + r_{i_l}(g_{i_l} - 1) \in \langle g_1 - 1, \ldots, g_k - 1 \rangle. \end{aligned}$$

Како је $\Phi_k(g_{k+1} - 1) = g_{k+1} - 1 \neq 0$, следи да

$$g_{k+1} - 1 \notin \langle g_1 - 1, \ldots, g_k - 1 \rangle,$$

па је полазни низ идеала строго растући.

Ако је R било који $(p-1)$-нил-чисти прстен, а G елементарна абелова 2-група (која се некад назива и Буловом групом) која је и бесконачна, тада је на основу пропозиције 11 у [26] прстен $R[G]$ један $(p-1)$-нил-чисти ненетерин прстен.

Други пример био би следећи. У својој књизи Нагата уводи појам идеализације модула (видети [35]), а многе корисне особине овог појма можемо наћи у [4]. Нека је R комутативни прстен, а M модул над R. Идеализација модула M, у ознаци $R(+)M$, има за скуп носач $R \oplus M$. У односу на операције сабирања по координатама и множења датог са

$$(r_1, m_1)(r_2, m_2) = (r_1r_2, r_1m_2 + r_2m_1),$$

скуп $R(+)M$ чини комутативни прстен са јединицом. Прстен R се природно утапа у $R(+)M$ преко пресликавања $r \mapsto (r, 0)$. За сваки подмодул N од M, скуп $0(+)N$ чини један идеал у прстену $R(+)M$. Тако је и $0(+)M$ идеал овог прстена и отуд назив за целу конструкцију.

Идеализација је корисна на првом месту из разлога превођења резултата који се тичу модула на случај прстена, затим генерализације резултата са прстена на модуле, као и конструкције разних примера комутативних прстена који нису интегрални домени. Ненетерини нил-чисти прстени (заправо, 1-нил-чисти) са радикалским идеалима управо могу бити конструисани коришћењем идеализације модула.

Наиме, нека је B Булов прстен и N модул над B који није коначно генерисан. То може бити и $\bigoplus_{n\geq 1} B$. Посматрајмо идеализацију $B(+)N$. За сваки елемент $(b,n) \in B(+)N$ важи да

$$(b,n) = (b,0) + (0,n),$$

при чему је

$$(b,0)(b,0) = (b^2,0) = (b,0),$$

као и

$$(0,n)(0,n) = (0,0).$$

Дакле, сваки елемент је збир идемпотента и нилпотента. Приметимо и да је идеал $0(+)M$ у сваком случају нилпотентан. Такође, из теореме 4.8 у [4] следи да ако M није коначно генерисан, онда идеализација $R(+)M$ није Нетерин прстен. Радикалски идеали у $R(+)M$ су облика $I(+)M$ за радикалски идеал I у R (на основу теореме 3.2 у [4]), а такође важи и да је $(R(+)M)[X] \cong R[X](+)M[X]$ (последица 4.6). Следи да пример радикалског идеала у прстену полинома $(B(+)N)[X]$, где је очигледно $B(+)N$ ненетерин нил-чист прстен, јесте идеал $I(+)N[X]$, за било који радикалски идеал I у $B[X]$.

Глава 7

Резултати и коментари за прстен полинома са више неодређених

У претходним главама изложени су резултати који се односе на прстене полинома са једном неодређеном. Природно је питање да ли се ти резултати могу уопштити на прстене полинома са више неодређених.

Нека је D интегрални домен и нека је $D\langle X\rangle$ ознака за локализацију $D[X]_S$, где је S скуп свих моничних полинома прстена полинома $D[X]$. У [12] (теорема 1. (i)) представљен је следећи резултат. За интегрални домен D који није поље важи: $D\langle X\rangle$ је Приферов домен ако и само ако је D једнодимензиони Приферов домен. У том случају је $\dim(D\langle X\rangle) = 1$. Одавде видимо да за Приферов домен има индиција да се резултати могу уопштити.

Наиме, нека је R Приферов домен димензије 1. Пређимо на разматрање прстена полинома $R[X_1, \dots, X_n]$. Из споменуте теореме следи да је $R\langle X_1\rangle$ такође Приферов домен димензије 1. Применом индукције можемо закључити да је и $R\langle X_1, \dots, X_k\rangle$ Приферов домен димензије 1, где је $k \geq 1$, при чему се дефинише

$$R\langle X_1, \dots, X_k\rangle := R\langle X_1, \dots, X_{k-1}\rangle\langle X_k\rangle.$$

Заправо, елементи прстена $R\langle X_1, \dots, X_k\rangle$ су облика

$$\frac{p(X_1, \dots, X_k)}{q(X_1, \dots, X_k)},$$

где је q полином чији је водећи коефицијент, у односу на лексикографски мономни поредак где $X_k > X_{k-1} > \cdots > X_1$, једнак 1. Дакле, можемо га видети као локализацију прстена $R[X_1, \dots, X_k]$ у односу на скуп

$$S = \{p \in R[X_1, \dots, X_k] \,|\, \mathrm{LC}(p) = 1\}.$$

Нека је I коначно генерисани идеал у $R[X_1, \dots, X_n]$ и нека је задат лексикографски мономни поредак где $X_n > X_{n-1} > \cdots > X_1$. Користећи резултате из главе 4, можемо доказати да је

$$\mathrm{LC}(I) = \langle \mathrm{LC}(p) \,|\, p \in I\rangle,$$

коначно генерисан идеал у R.

Теорема 75. *Нека је* $I \triangleleft R[X_1, \ldots, X_n]$ *коначно генерисан идеал, где је* R *Приферов домен димензије 1. Тада је* $\mathrm{LC}(I)$ *коначно генерисан идеал у* R, *при чему је задати мономни поредак лексикографски и* $X_n > X_{n-1} > \cdots > X_1$.

Доказ. Докажимо ово тврђење индукцијом по броју неодређених. Случај $n = 1$ је садржан у теореми 48 (приметимо да је у овом случају $\mathrm{LC}(I) = I_\infty$ у претходним ознакама). Претпоставимо да је тврђење тачно за $n - 1$. На основу горње дискусије имамо да је $R\langle X_1, \ldots, X_{n-1}\rangle$ Приферов домен димензије 1. Према томе, следи да је

$$R[X_1, \ldots, X_n] \subset R\langle X_1, \ldots, X_{n-1}\rangle[X_n],$$

при чему можемо посматрати екстензију I^e идеала I. Дакле, у $R\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ су инвертовани сви полиноми по $X_1, \ldots, X_{n-1}$ чији водећи коефицијент је једнак 1. Ако применимо теорему 48 на овај прстен, можемо закључити да је идеал свих водећих коефицијената I^e_∞ коначно генерисан идеал у $R\langle X_1, \ldots, X_{n-1}\rangle$. Нека је

$$I^e_\infty = \langle f_1, \ldots, f_k\rangle, \quad \text{где су } f_1, \ldots, f_k \text{ елементи у } R\langle X_1, \ldots, X_{n-1}\rangle.$$

Елементи f_i су облика $\frac{a_i}{b_i}$, где су a_i, b_i полиноми по $X_1, \ldots, X_{n-1}$ и b_i је са водећим коефицијентом једнаким 1. С обзиром на то да су у прстену $R\langle X_1, \ldots, X_{n-1}\rangle$ полиноми b_i инвертибилни, можемо претпоставити и да су $f_1, \ldots, f_k \in R[X_1, \ldots, X_{n-1}]$.

Докажимо да је

$$\mathrm{LC}(I) = \mathrm{LC}(I_*),$$

где је

$$I_* = \langle f_1, \ldots, f_k\rangle_{R[X_1,\ldots,X_{n-1}]},$$

то јест, идеал генерисан са $f_1, \ldots, f_k$ у $R[X_1, \ldots, X_{n-1}]$. На основу индуктивне претпоставке, $\mathrm{LC}(I_*)$ је коначно генерисан идеал у R, тако да је довољно доказати наведену једнакост.

Нека је $a \in \mathrm{LC}(I)$, то јест, $a = \mathrm{LC}(p)$, где је $p \in I$. Тада је

$$\begin{aligned} p &= aX_1^{\alpha_{11}} \cdots X_n^{\alpha_{1n}} + a_2 X_1^{\alpha_{21}} \cdots X_n^{\alpha_{2n}} + \cdots + a_l X_1^{\alpha_{l1}} \cdots X_n^{\alpha_{ln}} \\ &= (aX_1^{\alpha_{11}} \cdots X_{n-1}^{\alpha_{1,n-1}} + a_{i_1} X_1^{\alpha_{i_1 1}} \cdots X_{n-1}^{\alpha_{i_1,n-1}} + \cdots + a_{i_s} X_1^{\alpha_{i_s 1}} \cdots X_{n-1}^{\alpha_{i_s,n-1}}) X_n^{\alpha_{1n}} + \cdots \\ &= q(X_1, \ldots, X_{n-1}) X_n^{\alpha_{1n}} + \cdots \end{aligned}$$

Сабирци у загради су заправо такви да је у одговарајућим члановима степен уз X_n једнак α_{1n}. То је овде највећи степен од X_n, а како имамо лексикографски поредак, то $q(X_1, \ldots, X_{n-1})$ припада I^e_∞. Наравно, важи и да је $a = \mathrm{LC}(q)$. Такође је $q(X_1, \ldots, X_{n-1}) \in R[X_1, \ldots, X_{n-1}]$.

Приметимо да је

$$I^e_\infty \cap R[X_1, \ldots, X_{n-1}] = I^e_* \cap R[X_1, \ldots, X_{n-1}] = I^{ec}_*.$$

Важи наравно да је $I_* \subseteq I^{ec}_*$, па је и $\mathrm{LC}(I_*) \subseteq \mathrm{LC}(I^{ec}_*)$. Такође је и $\mathrm{LC}(I^{ec}_*) \subseteq \mathrm{LC}(I_*)$. Наиме, нека $b \in \mathrm{LC}(I^{ec}_*)$. Тада је $b = \mathrm{LC}(r)$, за $r \in I^{ec}_*$. Овај полином (из $R[X_1, \ldots, X_{n-1}]$) је облика

$$r = \frac{t_1}{s_1} f_1 + \cdots + \frac{t_k}{s_k} f_k = \frac{t_1 s_2 \cdots s_k f_1 + t_2 s_1 s_3 \cdots s_k f_2 + \cdots + t_k s_1 \cdots s_{k-1} f_k}{s_1 \cdots s_k}.$$

С обзиром на то да је полином $s_1 \cdots s_k$ са водећим коефицијентом 1, важи да је водећи коефицијент за r једнак водећем коефицијенту за полином

$$t_1 s_2 \cdots s_k f_1 + t_2 s_1 s_3 \cdots s_k f_2 + \cdots + t_k s_1 \cdots s_{k-1} f_k.$$

Овај последњи полином припада I_*, тако да је

$$b = \mathrm{LC}(r) = \mathrm{LC}(t_1 s_2 \cdots s_k f_1 + t_2 s_1 s_3 \cdots s_k f_2 + \cdots + t_k s_1 \cdots s_{k-1} f_k) \in \mathrm{LC}(I_*).$$

Дакле, имамо да је

$$\mathrm{LC}(I_*) = \mathrm{LC}(I_*^{ec}).$$

Вратимо се на полином

$$q(X_1, \ldots, X_{n-1}) \in I_\infty^e \cap R[X_1, \ldots, X_{n-1}].$$

Из претходног видимо да $\mathrm{LC}(q) \in \mathrm{LC}(I_*)$. Дакле, $a \in \mathrm{LC}(I_*)$, па је $\mathrm{LC}(I) \subseteq \mathrm{LC}(I_*)$.

Нека је сада $a \in \mathrm{LC}(I_*)$. Тада постоји $q \in I_*$ тако да $a = \mathrm{LC}(q)$. Важи да је

$$q = t_1 f_1 + \cdots + t_k f_k, \text{ за } t_1, \ldots, t_k \in R[X_1, \ldots, X_{n-1}].$$

Како су f_i елементи који генеришу све водеће коефицијенте полинома по X_n у I, то постоје

$$F_1, \ldots, F_k \in I^e \subset R\langle X_1, \ldots, X_{n-1}\rangle[X_n]$$

такви да је водећи коефицијент полинома F_i по X_n једнак f_i, за $1 \leq i \leq k$. Без умањења општости можемо претпоставити да је

$$F_1, \ldots, F_k \in I \subset R[X_1, \ldots, X_n];$$

иначе бисмо помножили неким полиномима чији водећи коефицијенти су једнаки 1. Прецизније:

$$F_i = f_i X_n^{\beta_i} + \text{ чланови мањег степена по } X_n,$$

за $1 \leq i \leq k$. Нека је $\beta = \max\{\beta_1, \ldots, \beta_k\}$. Полином

$$F = t_1 F_1 X_n^{\beta - \beta_1} + \cdots + t_k F_k X_n^{\beta - \beta_k} \in R[X_1, \ldots, X_n]$$

је такав да припада I и да је његов водећи коефицијент по X_n једнак q. Због лексикографског поретка, водећи коефицијент полинома F је једнак водећем коефицијенту полинома q, а то је a. Дакле, $a \in \mathrm{LC}(I)$, чиме смо доказали и да $\mathrm{LC}(I_*) \subseteq \mathrm{LC}(I)$. $\square$

Можемо разматрати и водеће коефицијенте полинома који су одређеног степена по неодређеној X_n.

Дефиниција 76. *Нека је $I \lhd R[X_1, \ldots, X_n]$ идеал над прстеном R. Означимо са*

$$\mathrm{LC}_m(I), \text{ за } m \geq 0,$$

идеал генерисан водећим коефицијентима полинома из идеала I који су степена m по неодређеној X_n.

На врло сличан начин претходној теореми можемо доказати да је и $\mathrm{LC}_m(I)$ коначно генерисан идеал у R, за свако $m \geq 0$.

Теорема 77. *Нека је $I \triangleleft R[X_1, \ldots, X_n]$ коначно генерисан идеал, где је R Приферов домен димензије 1. Тада је $\mathrm{LC}_m(I)$, $m \geq 0$, коначно генерисан идеал у R, при чему је задати мономни поредак лексикографски и $X_n > X_{n-1} > \cdots > X_1$.*

Доказ. Уочимо екстензију I^e идеала I у $R\langle X_1, \ldots, X_{n-1}\rangle[X_n]$. За овај доказ не морамо користити математичку индукцију, већ ћемо користити резултат претходне теореме. На основу теореме 48 следи да је $I^e_{(m)}$, идеал водећих коефицијената полинома по X_n степена m, коначно генерисан идеал у $R\langle X_1, \ldots, X_{n-1}\rangle$. Нека је $I^e_{(m)} = \langle f_1, \ldots, f_k\rangle$, где можемо претпоставити да су $f_1, \ldots, f_k \in R[X_1, \ldots, X_{n-1}]$. Доказаћемо да је

$$\mathrm{LC}_m(I) = \mathrm{LC}(I_*),$$

где је

$$I_* = \langle f_1, \ldots, f_k\rangle_{R[X_1,\ldots,X_{n-1}]}.$$

Из претходне теореме следи да је $\mathrm{LC}(I_*)$ коначно генерисан идеал у R.

Нека је $a \in \mathrm{LC}_m(I)$. Тада је $a = \mathrm{LC}(p)$, где је $p \in I$ и $\mathrm{LT}(p)$ је степена m по X_n. Важи да је

$$p = q(X_1, \ldots, X_{n-1})X_n^m + \text{ чланови мањег степена по } X_n.$$

Такође је $a = \mathrm{LC}(q)$ и још важи да је

$$q(X_1, \ldots, X_{n-1}) \in I^e_{(m)} \cap R[X_1, \ldots, X_{n-1}].$$

Исто као и у доказу претходне теореме, можемо се уверити да је

$$I^e_{(m)} \cap R[X_1, \ldots, X_{n-1}] = I_*^{ec},$$

као и да је $\mathrm{LC}(I_*) = \mathrm{LC}(I_*^{ec})$.

Како је $a = \mathrm{LC}(q) \in \mathrm{LC}(I_*)$, следи да је $\mathrm{LC}_m(I) \subseteq \mathrm{LC}(I_*)$.

Обрнуто, за $a \in \mathrm{LC}(I_*)$, постоји $q \in I_*$ тако да $a = \mathrm{LC}(q)$. Важи да је

$$q = t_1 f_1 + \cdots + t_k f_k, \text{ за } t_1, \ldots, t_k \in R[X_1, \ldots, X_{n-1}].$$

Како су f_i елементи који генеришу све водеће коефицијенте полинома степена m по X_n у I, постоје

$$F_1, \ldots, F_k \in I \subseteq R[X_1, \ldots, X_n]$$

такви да је водећи члан полинома F_i по X_n једнак $f_i X_n^m$, за $1 \leq i \leq k$. Полином

$$F = t_1 F_1 + \cdots + t_k F_k \in R[X_1, \ldots, X_n]$$

припада I и његов водећи члан је једнак

$$\mathrm{LT}(q(X_1, \ldots, X_{n-1})X_n^m).$$

Због лексикографског поретка, водећи коефицијент полинома F је једнак водећем коефицијенту полинома q, што је a. Следи да је и $\mathrm{LC}(I_*) \subseteq \mathrm{LC}_m(I)$. □

Задржаћемо ознаке из претходне теореме и доказа у наредној дискусији. Означимо са

$$J = I_* = \langle f_1, \ldots, f_k\rangle_{R[X_1,\ldots,X_{n-1}]}.$$

На основу теореме 77 имамо да је $\mathrm{LC}_s(J)$ коначно генерисан идеал у R, за $s \geq 0$. Докажимо да је

$$\mathrm{LC}_{s,m}(I) = \mathrm{LC}_s(J),$$

где је

$$\mathrm{LC}_{s,m}(I) = \langle \mathrm{LC}(p) \mid \mathrm{LP}(p) = X_1^{k_1}\cdots X_{n-2}^{k_{n-2}}X_{n-1}^{s}X_n^{m} \text{ и } p \in I\rangle,$$

идеал у R генерисан водећим коефицијентима полинома из I који су степена s по X_{n-1} и степена m по X_n.

За елемент $a \in \mathrm{LC}_s(J)$ важи да постоји $f \in J$ тако да $a = \mathrm{LC}(f)$ и да је

$$\mathrm{LT}(f) = aX_1^{k_1}\cdots X_{n-2}^{k_{n-2}}X_{n-1}^{s}.$$

Како је $f \in J = I_*$, следи да постоје $t_1, \ldots, t_k \in R[X_1, \ldots, X_{n-1}]$ тако да $f = t_1f_1+\cdots+t_kf_k$. Полином

$$F = t_1F_1 + \cdots + t_kF_k = t_1f_1X_n^m + \cdots + t_kf_kX_n^m + \cdots$$

припада I и његов водећи члан је једнак

$$aX_1^{k_1}\cdots X_{n-2}^{k_{n-2}}X_{n-1}^{s}X_n^{m},$$

тако да следи да је $a = \mathrm{LC}(F) \in \mathrm{LC}_{s,m}(I)$.

Са друге стране, нека је $a \in \mathrm{LC}_{s,m}(I)$. Тада постоји полином у I:

$$F = aX_1^{k_1}\cdots X_{n-2}^{k_{n-2}}X_{n-1}^{s}X_n^{m} + \cdots$$

Приметимо да је

$$\begin{aligned} F &= (aX_1^{k_1}\cdots X_{n-2}^{k_{n-2}}X_{n-1}^{s} + a_{i_1}X_1^{k_{i_1 1}}\cdots X_{n-1}^{k_{i_1,n-1}} + \cdots + a_{i_l}X_1^{k_{i_l 1}}\cdots X_{n-1}^{k_{i_l,n-1}})X_n^m + \cdots \\ &= q(X_1,\ldots,X_{n-1})X_n^m + \cdots \end{aligned}$$

Јасно је да $q \in I_*$ и да $a = \mathrm{LC}(q)$. Због лексикографског поретка, важи да $a = \mathrm{LC}_s(q)$ и $q \in J$, па је $a \in \mathrm{LC}_s(J)$.

Овим смо доказали да су и идеали $\mathrm{LC}_{s,m}(I)$ коначно генерисани у R. На сличан начин бисмо могли да наставимо и доказивање коначне генерисаности идеала коефицијената где су фиксирани и степени уз $X_{n-2}, X_{n-3}, \ldots$.

Можемо се вратити на почетно питање постојања Гребнерове базе за идеал I и наставити разматрање за случај две неодређене: $R[X_1, X_2]$. Ако је задат лексикографски поредак тако да $X_2 > X_1$ и $I \lhd R[X_1, X_2]$ коначно генерисан идеал над Приферовим доменом димензије 1, тада су сви идеали $\mathrm{LC}(I)$ и $\mathrm{LC}_{s,m}(I)$, $s, m \geq 0$, коначно генерисани идеали у R. Нека је

$$\mathrm{LC}(I) = \langle a_1, \ldots, a_k\rangle,$$

и нека су $f_1, \ldots, f_k$ полиноми из I чији су ово водећи коефицијенти, то јест,

$$\begin{aligned} f_1 &= a_1X_1^{s_1}X_2^{m_1} + \cdots \\ &\cdots \\ f_k &= a_kX_1^{s_k}X_2^{m_k} + \cdots \end{aligned}$$

Нека су

$$n_1 = \max\{s_1, \ldots, s_k\} \qquad \text{и} \qquad n_2 = \max\{m_1, \ldots, m_k\}.$$

По аналогији са доказом теореме 49, битни су нам идеали

$$\mathrm{LC}_{p_1,p_2}(I), \qquad \text{за } p_1 \leq n_1 \text{ и } p_2 \leq n_2.$$

Али, са друге стране, сам лексикографски поредак овде доноси проблем. Наиме

$$X_1^{n_1+l} X_2^{n_2-1} < X_1^{p_1} X_2^{n_2}$$

за било које $l \geq 1$. Заправо имамо бесконачно много чланова мањих од $X_1^{n_1} X_2^{n_2}$, због чега не можемо на жељени начин формирати коначан скуп који би одређивао Гребнерову базу за I. Остаје питање да ли се и како овај приступ може прилагодити тако да добијемо жељени резултат.

Валуациони домени су као што знамо и Приферови домени, али са фином особином везано за дељивост елемената. Локализација $V\langle X_1, \ldots, X_n\rangle$ јесте Приферов домен димензије 1, а сем тога, и НЗД домен. У [44] (теорема 4) тврди се да у случају лексикографског поретка са n неодређених, за сваки коначно генерисани идеал I над једнодимензионим валуационим доменом важи да је и $\mathrm{LT}(I)$ коначно генерисан. Коришћена је индукција, као што се показало згодним и у горњој дискусији. Да би било могуће свођење на случај за $n-1$ неодређених, наговештава се коришћење одређене смене променљивих. Више објашњења о тој смени дато је у књизи [42], при чему можемо приметити да смена $X \mapsto X + Y^r$, $Y \mapsto Y$ омогућава свођење на претходни случај али не чува мономни поредак, док смена $X \mapsto X$, $Y \mapsto Y + X^r$ не ремети поредак али ни не омогућава коришћење индукције. Према томе, још много питања о Гребнеровим базама за идеале над прстенима полинома са више неодређених остаје отворено.

Проблеми са лексикографским поретком где за одређени члан постоји бесконачно много чланова мањих од њега, нестају у случају степенастог лексикографског поретка. У том случају се не могу примењивати претходни резултати, већ би био потребан другачији приступ.

Представимо прво пар дефиниција.

Дефиниција 78. *Нека је задат степенасти лексикографски мономни поредак на прстену $R[X_1, \ldots, X_n]$, где је R прстен. Сваки елемент $f \in R[X_1, \ldots, X_n]$ може се представити као збир*

$$f = f_0 + f_1 + \cdots + f_d,$$

где је f_i хомогена компонента полинома f степена i. Означимо са $\mathrm{LH}(f) = f_d$ највећу хомогену компоненту полинома f.

Подсетимо се да је хомогена компонента f_i полинома f једнака збиру свих чланова $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$ полинома f тако да је

$$\alpha_1 + \cdots + \alpha_n = i.$$

Полином који има само једну хомогену компоненту се назива хомоген полином и јасно је да је свака хомогена компонента неког полинома један хомоген полином. Такође, ако је $\mathrm{LP}(f) = X_1^{\beta_1} \cdots X_n^{\beta_n}$, тада кажемо да је тотални степен за полином f једнак збиру $d = \beta_1 + \cdots + \beta_n$.

Дефиниција 79. *Нека је I ненула идеал у $R[X_1, \ldots, X_n]$, где је R прстен и задати мономни поредак је степенасти лексикографски. Означимо са*

$$\mathcal{LH}(I) = \{\mathrm{LH}(f) \mid f \in I \setminus \{0\}\},$$

као и са $\mathrm{LH}(I) = \langle \mathcal{LH}(I) \rangle$ идеал у $R[X_1, \ldots, X_n]$ који је генерисан хомогеним компонентама највећег степена свих полинома из I.

Можемо уочити неке везе између коначне генерисаности за $\mathrm{LT}(I)$ и $\mathrm{LH}(I)$.

Теорема 80. *Нека је I идеал у $R[X_1, \ldots, X_n]$ и нека је задати мономни поредак степенасти лексикографски. Ако је $\mathrm{LT}(I)$ коначно генерисан идеал, тада је и $\mathrm{LH}(I)$ такође коначно генерисан идеал.*

Доказ. Нека је $\mathrm{LT}(I) = \langle t_1, \ldots, t_s \rangle$, где су t_i мономи. Постоје полиноми $q_i \in I$ такви да је $\mathrm{LT}(q_i) = t_i$. Докажимо да је

$$\mathrm{LH}(I) = \langle \mathrm{LH}(q_1), \ldots, \mathrm{LH}(q_s) \rangle.$$

Нека је $h \in \mathrm{LH}(I)$. Тада је $\mathrm{LT}(h) \in \mathrm{LT}(I)$, па следи да је

$$\mathrm{LT}(h) = p_1 t_1 + \cdots + p_s t_s, \text{ за неке } p_1, \ldots, p_s \in R[X_1, \ldots, X_n].$$

Без умањења општости, можемо претпоставити да су p_i мономи. Полином

$$h_1 = h - (p_1 \mathrm{LH}(q_1) + \cdots + p_s \mathrm{LH}(q_s))$$

је такав да $h_1 \in \mathrm{LH}(I)$, с обзиром на то да $h, \mathrm{LH}(q_1), \ldots, \mathrm{LH}(q_s) \in \mathrm{LH}(I)$. Такође, тотални степен за h_1 је или једнак тоталном степену за h или је $h_1 = 0$, јер у изражавању за $\mathrm{LT}(h)$ преостану само они који су истог мултистепена.

Ако је $h_1 \neq 0$, имамо да је $\mathrm{LP}(h_1) < \mathrm{LP}(h)$. Можемо применити овај поступак на h_1 и наставити на тај начин тако да добијамо низ елемената $h_1, h_2, \ldots$ За њих важи да

$$\mathrm{LP}(h_1) > \mathrm{LP}(h_2) > \cdots$$

Како постоји само коначно много монома који су мањи од $\mathrm{LP}(h)$, постоји $k \geq 1$ тако да је $h_k = 0$. Кад заменимо све добијено у полазну једнакост, добијамо да је h генерисан са $\mathrm{LH}(q_1), \ldots, \mathrm{LH}(q_s)$. □

Лако се може доказати и да важи следећа лема.

Лема 81. *Нека је I идеал у $R[X_1, \ldots, X_n]$ и нека је задати мономни поредак степенасти лексикографски. Тада је $\mathrm{LT}(I) \subseteq \mathrm{LT}(\mathrm{LH}(I))$.*

Доказ. За $f \in I$ и $t = \mathrm{LT}(f)$ важи да $t \in \mathrm{LT}(I)$. Нека је $f = f_0 + f_1 + \cdots + f_d$, где су f_i хомогене компоненте степена i. Тада имамо да је $\mathrm{LT}(f_d) = t$ и $f_d \in \mathrm{LH}(I)$, па следи да је $t \in \mathrm{LT}(\mathrm{LH}(I))$. Самим тим, $\langle \mathrm{LT}(f) \mid f \in I \rangle \subseteq \mathrm{LT}(\mathrm{LH}(I))$. □

Сада се можемо запитати да ли важи и тврђење обрнуто теореми 80. Наиме, ако је I идеал у $R[X_1, \ldots, X_n]$ са степенастим лексикографским поретком и идеал $\mathrm{LH}(I)$ коначно генерисан, питање је да ли је тада и $\mathrm{LT}(I)$ коначно генерисан.

Нека је $\mathrm{LH}(I) = \langle h_1, \ldots, h_s \rangle$, где су h_i хомогени полиноми. Претходна лема би нас могла упутити да је $\mathrm{LT}(I)$ генерисан водећим члановима елемената h_i, за $i \in \{1, \ldots, s\}$. Како су $h_i = \mathrm{LH}(q_i)$, за неке $q_i \in I$ и пошто је

$$\mathrm{LT}(h_i) = \mathrm{LT}(q_i),$$

следи да је $\langle \mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_s) \rangle \subseteq \mathrm{LT}(I)$. Са друге стране, нека је $t = \mathrm{LT}(f)$, за $f \in I$. Нека је $f = f_0 + f_1 + \cdots + f_d$, где су f_i хомогене компоненте степена i. Очигледно је t сабирак у f_d. Елемент f_d припада $\mathrm{LH}(I)$, па је према претпоставци

$$f_d = g_1 h_1 + g_2 h_2 + \cdots + g_s h_s,$$

за неке полиноме $g_1, \ldots, g_s \in R[X_1, \ldots, X_n]$. Али одавде не можемо закључити да се t изражава преко $\mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_s)$.

Приметимо да за ову последњу дискусију нисмо имали никакве претпоставке о прстену R. Такође видимо да је коришћена само чињеница да је поредак по тоталном степену, а не нужно степенасти лексикографски, као и да није дат ни поредак неодређених. Можемо се запитати под којим условима бисмо могли да довршимо претходну дискусију, као и које бисмо закључке могли да изведемо из коначне генерисаности идеала хомогених компонената. Можда би у том контексту било згодно разматрати хомогене идеале, то јест, идеале који су генерисани хомогеним полиномима.

Јасно је да је за овај важан проблем генерализације на случај више неодређених битан мономни поредак, а остаје и питање да ли се могу примењивати и друге методе сем индуктивних, то јест, да ли се може директно доказивати да је идеал водећих чланова коначно генерисан.

Уместо закључка, споменимо и друга питања која се могу поставити везано за ову тему. Једно од њих је и да ли се може наћи права Гребнерова база за $(p-1)$-нил-чисти прстен уместо решавања проблема припадности идеалу, као и да ли се могу проширити резултати и на неке сродне класе прстена, π-регуларне, на пример.

Који други ненетерини прстени се могу разматрати? Крулов домен R дефинише се тако да

$$R = \bigcap_{i \in \Lambda} V_i,$$

где су V_i дискретни валуациони домени и при чему важи да је сваки ненула елемент $a \in R$ инвертибилан у свим V_i, сем евентуално у коначно много тих домена (видети [18]). Један пример ненетериног Круловог домена је прстен полинома над пољем са бесконачно много неодређених. Резултати о валуационим доменима који су овде дати би могли да буду полазна тачка за изучавање питања Гребнерове базе над Круловим доменима. Кохерентни домени, који имају своје корене у алгебарској геометрији и који су већ споменути у глави 4, а представљају генерализацију Приферових домена, такође су важни за изучавање. Затим Матлисови домени, који се дефинишу као прстени R за које је пројективна димензија поља разломака K над R једнака 1, и тако даље. Постоји и пуно других класа прстена који су блиски онима споменутим у главама 2, 3 и 4, као што су рецимо, скоро валуациони, скоро Безуови, скоро Приферови домени. На пример, интегрални домен V је скоро валуациони ако важи да за све $a, b \in V \setminus \{0\}$ постоји природни број n тако да $a^n \mid b^n$ или $b^n \mid a^n$ (видети [5]).

На крају, надамо се да сви наведени резултати и разматрања доприносе бољем разумевању занимљиве теме Гребнерових база над прстенима који нису Нетерини, као и да могу упутити на разне правце у којима би даља истраживања ове теме могла да се развијају.

Литература

[1] W. W. Adams and P. Loustaunau. An Introduction to Gröbner Bases. Graduate Studies in Mathematics, Vol. 3, American Mathematical Society, Providence, 1994.

[2] W. W. Adams and P. Loustaunau. "Gröbner bases and primary decomposition in polynomial rings in one variable over Dedekind domains." J. Pure Appl. Algebra 121.1 (1997), pp. 1–15.

[3] D. D. Anderson. Non-Noetherian Commutative Ring Theory: GCD Domains, Gauss' Lemma, and Contents of Polynomials. Springer, 2009.

[4] D. D. Anderson and M. Winders. "Idealization of a module." J. Commut. Algebra 1 (2009), pp. 3–56.

[5] D. D. Anderson and M. Zafrullah. "Almoust Bezout domains." J. Algebra 142 (1991), pp. 285–309.

[6] D. F. Anderson and A. Badawi. "Von Neumann regular and related elements in commutative rings." Algebra Colloq. 19.Spec 1 (2012), pp. 1017–1040.

[7] M. F. Atiyah and I. G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, Reading, Massachusetts, 1969.

[8] S. Bazzoni and S. Glaz. Prüfer rings. Multiplicative Ideal Theory in Commutative Algebra: A tribute to the work of Robert Gilmer, Springer, New York, 2006.

[9] T. Becker and V. Weispfenning. Gröbner Bases: a Computational Approach to Commutative Algebra. Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

[10] N. Bourbaki. Commutative Algebra. Hermann, Paris, Addison-Wesley, Reading, Massachusetts, 1972.

[11] S. Breaz, P. Danchev, and Y. Zhou. "Rings in which every element is either a sum or a difference of a nilpotent and an idempotent." J. Algebra Appl. 15.8 (2016), p. 11.

[12] J. W. Brewer and D. L. Costa. "Projective modules over some non-Noetherian polynomial rings." J. Pure Appl. Algebra 13 (1978), pp. 157–163.

[13] B. Buchberger. "An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal (English translation), Ph. D. thesis, University of Innsbruck." J. Symb. Comput. 41.3-4 (2006), pp. 475–511.

[14] P.-J. Cahen and J.-L. Chabert. "What you should know about integer-valued polynomials." Amer. Math. Monthly 123 (2016), pp. 311–337.

[15] A. Diesl. "Nil clean rings." J. Algebra 383 (2013), pp. 197–211.

[16] D. S. Dummit and R. M. Foote. Abstract Algebra. 3rd ed. John Wiley and Sons, Inc., Hoboken, New York, 2004.

[17] M. Fontana, J. Huckaba, and I. Papick. Prüfer domains. Monographs, Textbooks in Pure, and Applied Mathematics, 203. Marcel Dekker Inc., New York, 1997.

[18] L. Fuchs and L. Salce. Modules over Non-Noetherian Domains. Mathematical Surveys and Monograph, Vol. 84, American Mathematical Society, Providence, 2001.

[19] R. Gilmer. Multiplicative Ideal Theory. Queen's Papers on Pure and Applied methematics, Vol. 90, Kingston, Canada, 1992.

[20] S. Glaz. Commutative Coherent Rings. Lecture Notes in Mathematics, 1371. Springer-Verlag, Berlin, 1989.

[21] K. R. Goodearl. Von Neumann regular rings. Monographs and Studies in Mathematics, No. 4, Pitman, London, San Francisco, Melbourne, 1979.

[22] J. A. Huckaba. Commutative Rings with Zero-divisors. Monographs, Textbooks in Pure, and Applied Mathematics, 117. Marcel Dekker Inc., New York, 1988.

[23] A. Hadj Kacem and I. Yengui. "Dynamical Gröbner bases over Dedekind rings." J. Algebra 324 (2010), pp. 12–24.

[24] I. Kaplansky. Commutative Rings. Revised edition, The University of Chicago Press, Chicago, London, 1974.

[25] I. Kaplansky. Fields and rings. Chicago Lectures in Mathematics, 2nd edition, The University of Chicago Press, Chicago, London, 1972.

[26] A. Kostić, Z. Z. Petrović Z. S. Pucanović, and M. Roslavcev. "A generalization of nil-clean rings." Miskolc Math. Notes 19:2 (2018), pp. 969–981.

[27] A. Kostić, Z. Z. Petrović Z. S. Pucanović, and M. Roslavcev. "On the generalized strongly nil clean property of matrix rings." Prihvaćen u Algebra Colloquium.

[28] W. Krull. "Allgemeine Bewertungstheorie." J. reine angew. Math. 167 (1932), pp. 160–196.

[29] T. Y. Lam. A first course in noncommutative rings. Springer-Verlag, New York, 1991.

[30] J. Lambek. Lectures on Rings and Modules. Blaisdell Publishing Co., Waltham, Massachusetts, 1966.

[31] D. Li, J. Liu, and L. Zheng. "A zero-dimensional valuation ring is 1-Gröbner." J. Algebra 484 (2017), pp. 334–343.

[32] H. Lombardi, P. Schuster, and I. Yengui. "The Gröbner ring conjecture in one variable." Math. Z. 270.3-4 (2012), pp. 1181–1185.

[33] M. E. Manis. "Extension of valuation theory." Bull. Amer. Math. Soc. 73 (1967), pp. 735–736.

[34] S. Monceur and I. Yengui. "On the leading terms ideals of polynomial ideals over a valuation ring." J. Algebra 351 (2012), pp. 382–389.

[35] M. Nagata. Local rings. Interscience Publishers, New York, 1962.

[36] J. von Neumann. Continuous geometry. Princeton Mathematical Series, No. 25, Princeton University Press, Princeton, N. J., 1960.

[37] Z. Z. Petrović and M. Roslavcev. "Commutative von Neumann regular rings are 1-Gröbner." Na recenziji.

[38] Z. Z. Petrović and M. Roslavcev. “Gröbner bases for modules over Prüfer domains.” Prihvaćen u Mathematical Reports.

[39] H. Prüfer. “Untersuchungen über Teilbarkeitseigenschaften in Körpern.” J. reine angew. Math. 168 (1932), pp. 1–36.

[40] М. Радовановић. *Гребнерове базе за многострукости застава и примене.* Докторска дисертација, Математички факултет у Београду, 2015.

[41] M. Roslavcev. “Gröbner bases for ideals in univariate polynomial rings over valuation rings.” Mat. Vesn. 73.3 (2021), pp. 183–190.

[42] I. Yengui. Constructive Commutative Algebra, Projective Modules Over Polinomial Rings and Dynamical Gröbner Bases. Lecture Notes in Mathematics, 2138. Springer, Cham, 2015.

[43] I. Yengui. “Dynamical Gröbner bases.” J. Algebra 301 (2006), pp. 447–458.

[44] I. Yengui. “The Gröbner ring conjecture in the lexicographical order case.” Math. Z. 276 (2014), pp. 261–265.

Биографија аутора

Маја Рославцев рођена је 6. маја 1987. у Београду. Дипломирала је на Математичком факултету 2010. године на смеру Теоријска математика и примене са просечном оценом 9,54. На истом факултету на смеру Теоријска математика и примене 2011. године одбранила је мастер рад под насловом „Градуисане слободне резолвенте” (ментор проф. др Александар Липковски) са оценом 10. Докторске студије уписала је 2011. године на Катедри за алгебру и математичку логику. Од 2010. запослена је на Математичком факултету, најпре као сарадник у настави, затим као асистент и асистент практичне наставе.

Прилог 1.

Изјава о ауторству

Потписана Маја Рославцев

број уписа 2009/2011.

Изјављујем

да је докторска дисертација под насловом

Гребнерове базе за коначно генерисане идеале над неким класама ненетериних прстена

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

Маја Рославцев

У Београду, 20.08.2021.

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Маја Рославцев

Број уписа 2009/2011

Студијски програм Математика

Наслов рада Гребнерове базе за коначно генерисане идеале над неким класама ненетериних прстена

Ментор др Зоран Петровић

Потписани Маја Рославцев

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 20.08.2021.

Маја Рославцев

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Гребнерове базе за коначно генерисане идеале над неким класама ненетериних прстена

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 20.08.2021.

Маја Роспавцев

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.