دانشکده مهندسی مکانیک

گروه سیالات

پایان نامه کارشناسی ارشد مهندسی مکانیک - گرایش تبدیل انرژی

مطالعه انتقال حرارت جابجایی اجباری در جریان تراکم پذیر از مجموع لوله ها به روش سلول برش خورده کارتزین

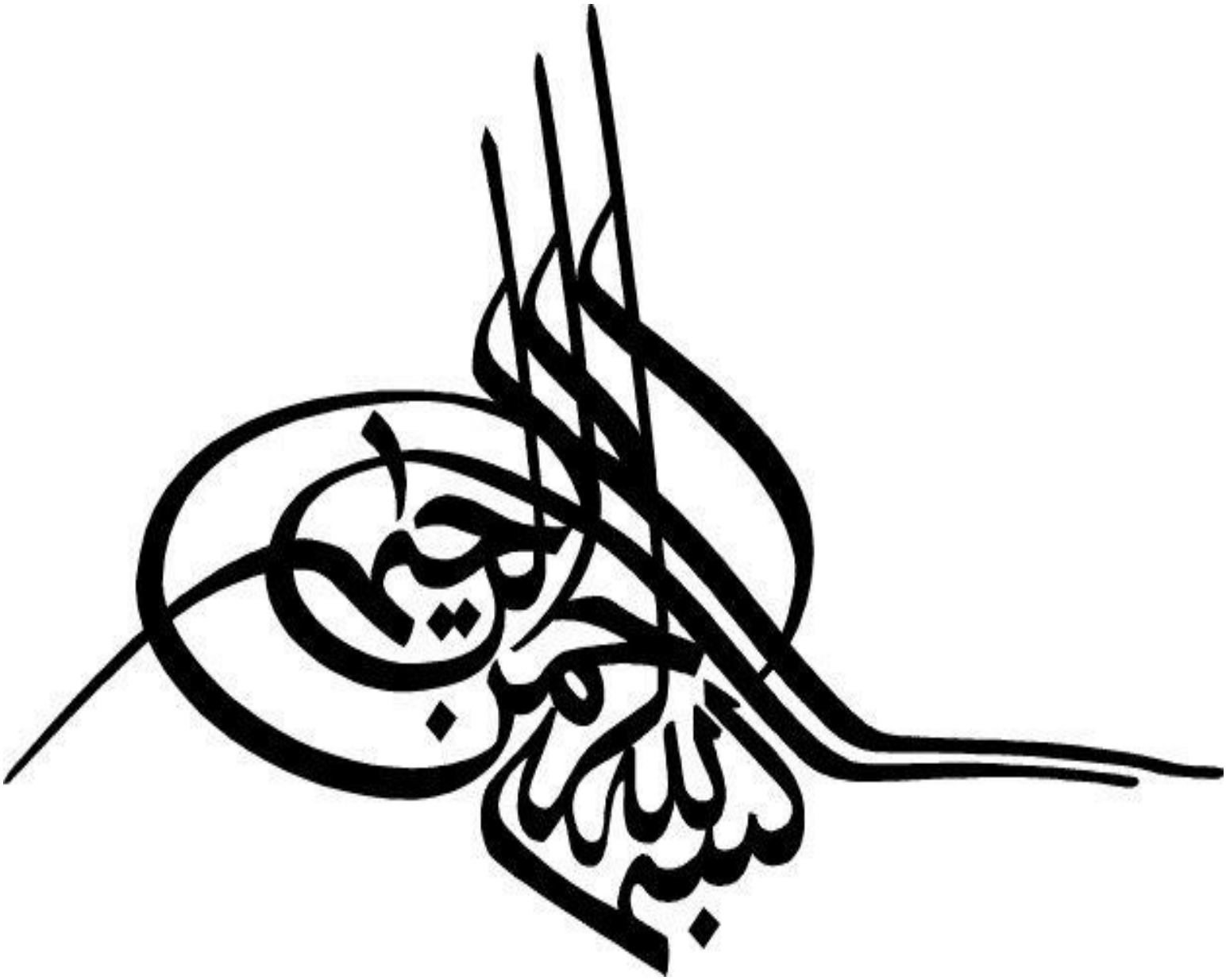
توسط:

رشید غیاثی

استاد راهنما:

دکتر محمد محسن شاه مردان

تیر ماه۱۳۸۸


بسم الله الرحمن الرحيم

سپاسگذاری

من لم یشکر خالق لم یشکر مخلوق
منزهی تو ای خدا، چقدر راهها تنگ و دشوار است بر کسی که تو راهنمایش نباشی و اگر تو هدایت کنی چقدر راه حق واضح و هویداست، خدایا ما را به راهی بر، که به درگاهت رسیم

از استاد راهنمای ارجمندم، آقای دکتر شاه مردان به خاطر راهنمایی ها، کمک های فکری و روحی و صبر و شکیبایی که در این مدت نسبت به من روا داشتند تا توانستم پروژه خود را به پایان برسانم عرض تشکر دارم.
از پدر و مادر عزیزم که در تمامی لحظات پشتیبان من بوده اند قدرانی فراوان دارم هر چند که هیچ گاه نخواهم توانست محبت هایشان را به کمال جبران کنم.
در پایان از همسر مهربانم که مرا کمک فکری و روحی نمودند تشکر فراوان دارم.

با آرزوی بهروزی
غیاثی
تیر ماه ۸۸

چکیده

در این پایان نامه روش سلول برش خورده کارتزین برای شبیه سازی انتقال حرارت جابجایی اجباری اطراف سیلندر با روش میانیابی دو بعدی به کار گرفته شده است.
برای انتقال حرارت جابجایی اجباری آرام بر روی سیلندر افقی همدما با طول بینهایت با میانیابی چند جمله ای غیر خطی استفاده شده تا شاری که از سطح برش خورده عبور می کند را طراحی کند
برای شارهای موجود در سطح جسم پروفیل چند جمله ای درجه دو فرض شده و معادلات مومنتوم ، انرژی و جرم با استفاده از روش حجم محدود با آرایش تلفیقی گسسته سازی شده است و ارتباط بین سرعت و فشار به وسیله ی یک روش کسری دو زمانه انجام می پذیرد
شرایط مرزی برای میدان سرعت میانی طبق مرحله دوم روش مذکور مطابقت پیدا کرده است.
نتایج برای انتقال حرارت جابجایی برای $10^2 < Ra < 2\times10^4$ بدست آمده و با کارهای عددی اخیر مقایسه شده است.

کلید واژه: جابجایی اجباری، انتقال حرارت، روش سلول برش خورده، اطراف سیلندر، لوله های هم دما

عنوان **صفحه**

فصل اول:پایه گروبنر

فصل دوم: حلقه های پایا

فصل سوم : پایه ساگبی وساگبی گروبنر در حلقه های پایا

فصل چهارم : الگوریتم F_5- پایا

فصل اول

پایه گروبنر

در این فصل ابتدا تعاریف و قضایای لازم برای بیان پایه گروبنر را شرح می‌دهیم و سپس الگوریتمی برای محاسبه پایه گروبنر[1] ارائه می دهیم .

۱-۱ : مقدمه

دراین بخش الگوریتم تقسیم چند جمله‌ایها را ارائه می دهیم، برای اینکار ابتدا مقدمات زیر را بیان می کنیم:

فرض کنید $\alpha_n, \dots, \alpha_2, \alpha_1$ اعدادی صحیح و نامنفی باشند، در این‌صورت هر حاصل‌ضرب به شکل $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ را یک تک جمله‌ای از متغیرهای $x_n, \dots, x_2, x_1$ می‌نامیم.

تک‌جمله‌ای فوق را با نماد X^α نشان می‌دهیم که در آن $\alpha = (\alpha_1, \dots, \alpha_n)$ می‌باشد، به عبارتی :

$$X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

اگر $\alpha = (0,0, \dots, 0)$ آنگاه $X^\alpha = 1$ می باشد.

[1] -Gröebner Basis

درجه X^{α} را با نماد $\deg X^{\alpha}$ یا $|\alpha|$ نمایش داده به صورت زیر تعریف می‌کنیم:

$$|\alpha| = \deg X^{\alpha} = \alpha_1 + \alpha_2 + \cdots + \alpha_n \qquad (۱-۱)$$

هر چند جمله‌ای f از n متغیر $x_1, x_2, \ldots, x_n$ با ضرائب در k ، ترکیب خطی تعداد متناهی از تک جمله‌ایها می‌باشد، یعنی :

$$f = \sum_{\alpha} a_{\alpha} X^{\alpha} \quad , \quad a_{\alpha} \in k \qquad (۱-۲)$$

که در آن حداکثر تعداد متناهی از a_{α}ها مخالف صفر می‌باشد. مجموعه ی تمام چند جمله ایها از n متغیر $x_1, x_2, \ldots, x_n$ با ضرائب در k را با نماد $k[x_1, x_2, \ldots, x_n]$ نمایش می دهیم که با جمع و ضرب معمول چند جمله ایها تشکیل یک حلقه می دهد، به عبارتی

$$k[x_1, x_2, \ldots, x_n] == \left\{ \sum_{\alpha} a_{\alpha} X^{\alpha} \mid \alpha \in \mathbb{Z}_{\geq 0}^{n} , a_{\alpha} \in k, \text{حداکثر تعدادی متناهی از} a_{\alpha} \text{ها مخالف صفر هستند} \right\} \qquad (۱-۳)$$

چند جمله‌ای $f = x^3 z + \frac{1}{2} y^2$ متعلق به $\mathbb{Q}[x, y, z]$ می‌باشد.

اگر $f = \sum_{\alpha} a_{\alpha} X^{\alpha}$ یک چند جمله‌ای در $k[x_1, x_2, \ldots, x_n]$ باشد، آنگاه:

۱- a_{α} را ضریب تک جمله‌ای X^{α} می نامیم.

۲- اگر $a_{\alpha} \neq 0$ باشد، آنگاه $a_{\alpha} X^{\alpha}$ را یک ترم می نامیم.

۳- درجه f را با نماد $deg\ (f)$ نمایش داده و به صورت زیر تعریف می‌کنیم:

$$deg(f) = max\ \{|\alpha| | a_{\alpha} \neq 0\} \qquad (۱-۴)$$

در چند جمله ای $f = x^3 yz + \frac{1}{2} y^2 z + 7xy$ ، ضرائب تک جمله‌ایهای $xy, y^2 z, x^3 yz$ می‌باشند $7, \frac{1}{2}, 1$ و f دارای سه ترم ودرجه f برابر ۵ می‌باشد.

فـرض کنیـد f عضوی از $k[x]$ باشد. در این صورت بـزرگترین تـوان x را درجه f می‌نـامیم و با $deg\ (f)$ نشان می‌دهیم.

تک جمله‌ای از f که بزرگترین توان را دارد تک جمله‌ای پیشروی f نام دارد وآن را با $Lm(f)$ نشان مـی‌دهیم و ضریب تک جمله‌ای پیشرو را ضریب پیشرو f نامیده و با $Lc(f)$ نمایش می‌دهیم. همچنین $Lc(f).Lm(f)$ را با $Lt(f)$ نمایش داده و ترم پیشروی f نامیم.

به عبارتی اگر $f = a_n x^n + \cdots + a_1 x^1 + a_0$ به طوری که $a_n, \dots, a_0$ متعلق بـه k هسـتند و $a_n \neq 0$ ، آنگـاه $deg(f) = n$، $Lm(f) = x^n$ و $Lc(f) = a_n$ و $Lt(f) = a_n x^n$ است.

اگر f, g دو چند جمله‌ای غیر صفر باشند در این صورت $deg(f) \leq deg(g)$ اگر وتنها اگـر $Lt(g)$ مضـربی از $Lt(f)$ باشد .یعنی :

$$Lt(f)|Lt(g) \qquad (۱-۵)$$

اگر k یک میدان باشد، آنگاه $k[x_1, x_2, \dots, x_n]$ یک حلقـه نـوتری اسـت یعنـی هـر ایـده آل $k[x_1, x_2, \dots, x_n]$ توسط تعداد متناهی عضو تولید می‌شود.

فرض کنیم f_1, f_2 دو چند جمله‌ای در $k[x_1, x_2, \dots, x_n]$ باشند که حداقل یکی از آنها مخالف صفر باشد. در این صورت m را بزرگترین مقسوم علیه مشترک f_1 و f_2 گوییم و می‌نویسیم $m = \gcd(f_1, f_2)$ هرگاه :

۱) چند جمله‌ای m، هم چند جمله‌ای f_1 و هم چند جمله‌ای f_2 را عاد کند.

۲) اگر $\acute{m} \in k[x_1, x_2, \dots, x_n]$ ای موجود باشد که $\acute{m}$، هم f_1 و هم f_2 را عاد کند، آنگاه $\acute{m}$، چند جمله‌ای m را نیز عاد کند.

اگر I زیر مجموعه‌ای از $k[x_1, x_2, \dots, x_n]$ باشد، آنگاه ایده‌آل تولید شده توسط I را با نماد $< I >$ نمایش می-دهیم. اگر $I = \{f_1, \dots, f_s\}$ آنگاه داریم:

$$< I >= \{g_1 f_1 + \cdots + g_s f_s | g_i \in k[x_1, x_2, \dots, x_n]\ \} \qquad (۱-۶)$$

۱-۲ : ترتیب روی تک جمله‌ایها

در این بخش رابطه ترتیبی روی حلقه ی چند جمله ایهای $k[x_1,\dots,x_n]$ را معرفی می کنیم.

نماد گذاری: مجموعه تک جمله‌ای‌های در$k[x_1,x_2,\dots,x_n]$ را با نماد $\mathbb{T}$ نمایش می‌دهیم، یعنی :

$$\mathbb{T}=\{{x_1}^{\alpha_1}\dots{x_n}^{\alpha_n}|(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}_{\geq 0}^n\}$$

رابطه ی $\leq$ یک ترتیب کلی روی مجموعه A است هرگاه دارای خواص زیر باشد:

۱) خاصیت انعکاسی: به ازای هر $a\in A$، $a\leq a$.

۲) خاصیت پادتقارنی : به ازای هر $a,b\in A$، اگر $a\leq b$ و $b\leq a$ آنگاه $a=b$.

۳) خاصیت تعددی : به ازای هر$a,b,c\in A$ ، اگر $a\leq b$ و $b\leq c$ آنگاه $a\leq c$.

۴) خاصیت تثلیث : یعنی به ازای هر $a,b\in A$ ، $a<b$ یا $b<a$ یا $a=b$.

حال چند نمونه از ترتیب‌هائی که کاربرد بیشتری دارند را معرفی می‌کنیم. برای تعریف یک ترتیب در$k[x_1,x_2,\dots,x_n]$ ، کافی است ترتیبی روی مجموعه تک جمله‌ای‌های آن یعنی $\mathbb{T}$ تعریف کنیم.

توجه کنید که تناظری یک به یک بین $\mathbb{T}$ و $\mathbb{Z}_{\geq 0}^n$ وجود دارد. لذا هر ترتیب در $\mathbb{Z}_{\geq 0}^n$ ، یک ترتیب در $\mathbb{T}$ است و بالعکس.

رابطه $\leq$ روی $\mathbb{Z}_{\geq 0}^n$ (به طور معادل روی $\mathbb{T}$) را یک رابطه ترتیبی تک جمله‌ای‌ها نامیم هرگاه:

الف :رابطه $\leq$ یک ترتیب کلی باشد.

ب: برای هر α,β,γ در $\mathbb{Z}_{\geq 0}^n$ رابطه $\alpha\leq\beta$ ایجاب کند: $\alpha+\gamma\leq\beta+\gamma$.

پ : $(\mathbb{Z}_{\geq 0}^n,\leq)$خوش‌ترتیب باشد، یعنی هر زیر مجموعه ی ناتهی آن عضو می‌نیمال داشته باشد.($\mathbb{T}$ خوش‌ترتیب باشد.)

$\mathbb{T}$ خوش‌ترتیب است اگر و تنها اگر هر زیر زنجیر نزولی از اعضای $\mathbb{T}$ ایستا باشد.

معمولاً با هر ترتیبی فرض می‌کنیم $x_1 > x_2 > \cdots > x_n$ ، مگر اینکه خلاف آن ذکر شود.

ترتیب قاموسی[۲] روی $k[x_1, \ldots, x_n]$ را با نماد $<_{lex}$ نمایش داده و به صورت زیر تعریف می‌کنیم:

$$x^{\alpha} <_{lex} x^{\beta} \Leftrightarrow \exists i \quad \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i \qquad (۱-۷)$$

به عبارتی $x^{\alpha} <_{lex} x^{\beta}$، اگر اولین درایه ناصفر سمت چپ $\beta - \alpha$ مثبت باشد.

با شرط $x > y > z$ داریم :

$$z^4 <_{lex} x^2y^2 \qquad (۱-۸)$$

ترتیب قاموسی درجه‌ای[۳] روی $k[x_1, \ldots, x_n]$ به این صورت تعریف می‌شود که $x^{\alpha} <_{grlex} x^{\beta}$ اگر درجه x^{β} از درجه x^{α} بیشتر باشد و در حالت تساوی درجه‌ها، x^{β} از x^{α} نسبت به رابطه ترتیبی قاموسی بزرگتر باشد .یعنی :

$$x^{\alpha} <_{grlex} x^{\beta} \Leftrightarrow |\alpha| < |\beta| \quad \text{یا} \quad |\alpha| = |\beta| \,, \alpha <_{lex} \beta$$

با شرط $x > y > z$ داریم :

$x^2yz <_{grlex} xyz^3$ زیرا $|(2,1,1)| < |(1,1,3)|$ و همچنین $xyz^2 <_{grlex} xy^2z$ زیرا $y <_{lex} y^2$.

ترتیب قاموسی معکوس درجه‌ای[۴] روی $k[x_1, \ldots, x_n]$ که آن را با نماد $<_{grevlex}$ نمایش می دهیم به صورت زیر تعریف می‌شود :

$$x^{\alpha} <_{grevlex} x^{\beta} \Leftrightarrow |\alpha| < |\beta| \quad \text{یا} \quad |\alpha| = |\beta| \,, \exists i;\ \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i > \beta_i \qquad (۱-۹)$$

۲-Lexicographic Order
۳ -Graded Lex Order
٤ -Graded Reverse Lex Order

یعنی اگر $|\alpha| = |\beta|$، آنگاه برای اینکه $x^{\alpha} <_{grevlex} x^{\beta}$ برقرار باشد باید اولین درایه غیر صفر سمت راست $\beta - \alpha$ منفی باشد.

با شرط $x > y > z$ داریم :

$x^4yz^3 <_{grevlex} xy^5z^2$ زیرا $|(1,5,2)| = |(4,1,3)|$ و $(1,5,2) <_{grevlex} (4,1,3)$ و $\beta - \alpha = (-3,4,-1)$.

در حالت دو متغییره ترتیب‌های $<_{grevlex}$ و $<_{grlex}$ یکی هستند، یعنی $x^{\alpha_1}y^{\beta_1} <_{grlex} x^{\alpha_2}y^{\beta_2}$ اگر وتنها اگر $x^{\alpha_1}y^{\beta_1} <_{grevlex} x^{\alpha_2}y^{\beta_2}$.

قرار دهید $a = (\alpha_1, \beta_1), b = (\alpha_2, \beta_2)$ و بدون اینکه به کلیت مسئله خللی وارد شود فرض کنید $\alpha_1 < \alpha_2$.

ابتدا فرض کنید $x^{\alpha_1}y^{\beta_1} <_{grlex} x^{\alpha_2}y^{\beta_2}$ ، در این صورت دو حالت داریم:

۱) $|a| < |b|$ ، در اینصورت با توجه به تعریف (۱-۲-۹) داریم: $x^{\alpha_1}y^{\beta_1} <_{grevlex} x^{\alpha_2}y^{\beta_2}$.

۲) $|a| = |b|$ ، با توجه به اینکه $\alpha_1 - \alpha_2$ منفی می‌باشد و لذا $\beta_1 - \beta_2$ مثبت و با بکارگیری تعریف داریم:

$$x^{\alpha_1}y^{\beta_1} <_{grevlex} x^{\alpha_2}y^{\beta_2} \qquad (۱-۱۰)$$

بالعکس : با توجه به آنچه در قبل ثابت شد به همین ترتیب اثبات می شود وحکم ثابت می شود.

فرض کنید f عضوی از $k[x_1, \dots, x_n]$ باشد و $\leq$ یک رابطه ترتیبی روی تک‌جمله‌ای‌ها باشد . در این صورت مجموعه تمام تک جمله‌ای‌های f را با نماد $M(f)$ نمایش می‌دهیم، به عبارتی اگرداشته باشیم :

$f = \sum_{\alpha \in A} a_{\alpha}x^{\alpha}$ که در آن $a_{\alpha} \neq 0$ آنگاه

$$M(f) = \{{x_1}^{\alpha_1} \dots {x_n}^{\alpha_n} | \alpha \in A\} \qquad (۱-۱۱)$$

با مفروضات تعریف بالا داریم :

$$multideg(f) = \max\{(\alpha_1, \dots, a_n) | {x_1}^{\alpha_1} \dots {x_n}^{\alpha_n} \in M(f)\} \qquad (۱-۱۲)$$

که در آن ماکسیمم نسبت به ترتیب $\leq$ گرفته می‌شود و به عبارت بهتر $multideg(f)$ برابر با بزرگترین توان تک جمله ایهای f با ترتیب مفروض می باشد .

$a_{multideg(f)}$ را ضریب پیشروی f[۵] و $x^{multideg(f)}$ را تک جمله ای پیشروی f[۶] و $a_{multideg(f)}.x^{multideg(f)}$ را ترم پیشروی f[۷] نامیم و به ترتیب با $Lc(f)$ و $Lm(f)$ و $Lt(f)$ نمایش می‌دهیم.

فرض کنید f عضوی از $k[x_1,\dots,x_n]$ باشد و $\leq$یک رابطه ترتیبی روی تک‌جمله‌ای‌ها باشد . در این صورت مجموعه تمام ترم های f را با نماد $T(f)$ نمایش می‌دهیم.

برای $f = y^2z + 8xz^2 - 6x^3y + 7x^2z^2$ با در نظر گرفتن ترتیب $<_{lex}$ با شرط $x > y > z$ داریم:

$$T(f) = \{y^2z, 8xz^2, -6x^3y, 7x^2z^2\}$$

$$multideg(f) = (3,1,0)$$

$$Lc(f) = -6$$

$$Lm(f) = x^3y$$

$$Lt(f) = -6x^3y$$

حال با توجه به مقدمات گفته شده به الگوریتم تقسیم می پردازیم :

۱-۳ : الگوریتم تقسیم در $k[x_1,\dots,x_n]$

فرض کنید $f, f_s, \dots, f_1$ اعضائی از $k[x_1,\dots,x_n]$ باشند، و $>$ یک رابطه ی ترتیبی روی $k[x_1,\dots,x_n]$ باشد، در این صورت منظور از تقسیم f بر $f_s,\dots,f_1$ عبارت است از یافتن چند جمله‌ای‌های $r, a_s, \dots, a_1$ که در رابطه زیر صدق کند:

$$f = a_1f_1 + \cdots + a_sf_s + r \qquad (۱-۱۳)$$

---

[۵] -Leading Coefficent
[۶] -Leading Monomial
[۷] -Leading Term

به قسمی که هیچ یک ازجملات پیشروی $f_1, \dots, f_s$، تک جمله‌ای‌های r را نشمارد و همین طـور اگـر $a_i f_i$ صـفر نباشد آنگاه

$$multideg(a_i f_i) \leq multideg(f) \qquad (۱-۱۴)$$

مـی‌خـواهیم $f = x^2y^2 + xy^2 + y^2$ را بـر $f_1 = xy - 1, f_2 = y^2 - 1$ بـا در نظـر گـرفتن رابطـه ترتیبـی $<_{grlex}$ با شرط $x > y$ تقسیم کنیم. بدین منظور فرض می‌کنیم:

a_1:

a_2:

$xy - 1$

$y^2 - 1$ $\qquad \sqrt{f = x^2y^2 + xy^2 + y^2}$ $\qquad (۱-۱۵)$

از تعاریف (۱-۲-۱۴) داریم $Lt(f_1) = xy, Lt(f_2) = y^2$، که هر دو می‌توانند $Lt(f) = x^2y$ را عاد کنند.

از f_1 شروع می‌کنیم. خارج‌قسمت تقسیم x^2y بر xy برابر x می باشد،در این صورت با تفریق f از f_1.x داریم:

a_1: x

a_2:

$xy - 1$

$y^2 - 1$

$$\sqrt{\begin{matrix} x^2y^2 + xy^2 + y^2 \\ \hline x^2y^2 - x \\ \hline xy^2 + x + y \end{matrix}} \qquad (۱-۱۶)$$

حال این روند را برای $xy^2 + x + y$ ادامه می‌دهیم. این بار هم باید از f_1 استفاده کنیم، زیرا $Lt(f_1) = xy$ می‌باشد که می‌تواند $Lt(xy^2 + x + y) = xy^2$ را بشمارد. پس داریم:

a_1: $x + y$

a_2:

$xy-1$

y^2-1

$$\sqrt{\begin{array}{c} x^2y^2+xy^2+y^2 \\ \hline x^2y^2-x \\ \hline xy^2+x+y^2 \\ \hline xy^2-y \\ \hline x+y^2+y \end{array}} \qquad (۱-۱۷)$$

با تکرار روند فوق برای $x+y^2+y$ داریم :

a_1: $x+y$

a_2: 1

$xy-1$

y^2-1

$$\sqrt{\begin{array}{c} x^2y^2+xy^2+y^2 \\ \hline x^2y^2-x \\ \hline xy^2+x+y^2 \\ \hline xy^2-y \\ \hline x+y^2+y \\ \hline y^2-1 \\ \hline x+y+1 \end{array}} \qquad (۱-۱۸)$$

از آنجا که $Lt(f_1), Lt(f_2)$ نمی‌توانند $Lt(x+y+1)=x$ را عاد کنند، لذا باقیمانده برابر $x+y+1$ است.

اکنون می‌توانیم f را به صورت زیر بنویسیم:

$$x^2y^2+xy^2+y^2=(x+y).(xy-1)+(1).(y^2-1)+x+y+1 \qquad (۱-۱۹)$$

اگـر مثـال قبـل را بـا همـان شـرایط در نظـر بگیـریم بـا ایـن تفـاوت کـه جـای f_1 ، f_2 را عـوض کنـیم، یعنـی باشند داریم: $f_1 = y^2 - 1$,$f_2 = xy - 1$

a_1: $x + 1$

a_2: x

$y^2 - 1$

$xy - 1$

$$\sqrt{\begin{array}{c} x^2y^2 + xy^2 + y^2 \\ \hline xy^2 - x \\ \hline x^2y + x + y^2 \\ \hline x^2y - x \\ \hline y^2 + 2x \\ \hline y^2 - 1 \\ \hline 2x + 1 \end{array}} \qquad (۱-۲۰)$$

لذا f را می توان به صورت زیر نوشت :

$$x^2y^2 + xy^2 + y^2 = (x + 1).(y^2 - 1) + (x).(xy - 1) + (2x + 1) \qquad (۱-۲۱)$$

با توجه به دو مثال قبل بنا به انتخاب $f_1, \dots, f_s$ می‌توانیم نمایش‌های مختلفی برای f در $\frac{k[x,y]}{<xy-1,y^2-1>}$ بنویسـیم. هدف یافتن نمایشی منحصربفرد برای f بـا اسـتفاده از $f_1, \dots, f_s$ اسـت. در زیـر الگـوریتمی بـرای تقسـیم f بـر $f_1, \dots, f_s$ ارائه می‌دهیم :.

INPUT: $f, f_1, \dots, f_s$

OUTPUT: $a_1, \dots, a_s, r$

$a_1 := 0; \dots; a_s := 0;$

$r := 0; p := f;$

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

$i := 1$

$divisionoccurred := false$

WHILE $i \leq s$ ***AND*** $divisionoccurred = false$ **DO**

IF $lt(f_i)$ *divides* $lt(p)$ ***THEN***

$$a_i := a_i + \frac{lt(p)}{lt(f_i)}$$

$$p := p - (\frac{lt(p)}{lt(f_i)})f_i$$

$$divisionoccurred := true$$

ELSE $i := i + 1$

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

$r := r + lt(p)$

$p := p - lt(p)$

RETURN$(a_1, \dots, a_s, r)$;

A-۱ الگوریتم تقسیم در$k[x_1, \dots, x_n]$

(درستی الگوریتم تقسیم چند متغیره):

فرض کنید $f, f_s, \dots, f_1$ عناصری از $k[x_1, \dots, x_n]$ باشد، در این صورت برای هر ترتیب دلخواه از تک جمله‌ای‌ها عناصر $a_s, \dots, a_1, r$ از $k[x_1, \dots, x_n]$ چنان موجودند که :

الف : $f = a_1 f_1 + \cdots + a_s f_s + r$

ب: برای هر γ متعلق به $M(r)$ وبرای هر $1 \leq i \leq s$ ، γ توسط جمله پیشروی f_i شمرده نمی شود .

پ : برای هر i با شرط $a_i f_i \neq 0$، داشته باشیم: $\deg(a_i f_i) \leq \deg(f)$

نشان می‌دهیم الگوریتم (A-۱) شرایط را برآورده می‌کند و پایان‌پذیر است.

الف: ابتدا نشان می‌دهیم در هر گام از الگوریتم داریم:

$$f = a_1 f_1 + \cdots + a_s f_s + r + p \qquad (1)$$

(۱-۲۲)

به وضوح در شروع کار رابطه **(۱-۲۲)** برقرار است. برای ادامه فرض می‌کنیم (🗁) تا گام بخصوصی درست باشد، گام بعدی آن را اثبات می‌کنیم.

کافی است درستی **(۱-۲۲)** را در شرط‌های IF الگوریتم بررسی کنیم.

ابتدا اولین شرط IF: در گام جدید برای $a_i f_i, p$ داریم:

$$a_i f_i := (a_i + \frac{Lt(p)}{Lt(f_i)}) f_i$$

$$p := p - (\frac{Lt(p)}{Lt(f_i)}) f_i \qquad \textbf{(۱-۲۳)}$$

اما از گام قبلی داریم :

$$f = a_1 f_1 + \cdots + a_i f_i + \cdots + a_s f_s + r + p \qquad \textbf{(۱-۲۴)}$$

لذا از روابط بالا داریم :

$$f = a_1 f_1 + \cdots + \left(a_i + \frac{Lt(p)}{lt(f_i)}\right) f_i + \cdots + a_s f_s + r + p - (\frac{lt(p)}{lt(f_i)}) f_i \qquad \textbf{(۱-۲۵)}$$

که درستی رابطه **(۱-۲۲)** را نشان می‌دهد.

برای دومین شرط IF نیز از گام قبلی داریم: $p + r$، لذا در گام جدید خواهیم داشت:

$$\big(p - Lt(p)\big) + \big(r + Lt(p)\big) \qquad \textbf{(۱-۲۶)}$$

با توجه به اینکه در پایان الگوریتم $p = 0$ است، لذا از (🗁) شرط ا لف برقرار است.

ب: یک جمله وقتی به r اضافه می‌شود که مضرب هیچ یک از $Lt(f_i)$ نباشد. لذا ب نیز برقرار است.

پ: توجه کنید که تنها جملاتی به شکل $\frac{Lt(p)}{Lt(f_i)}$ به a_i اضافه می‌شوندو همین‌طور $Lt(p) \leq Lt(f)$ (زیرا در شرط-های IF جمله پیشروی p از آن کم می‌شود)، پس

$$Lt(a_i f_i) = Lt(a_i).Lt(f_i) = \left(\frac{Lt(p)}{Lt(f_i)}\right).Lt(f_i) = Lt(p) \leq Lt(f) \qquad (۱-۲۷)$$

از خوش‌ترتیبی رابطه ترتیبی تک جمله‌ای‌ها، می‌توان نتیجه گرفت که پس از تعداد متناهی بار، $p = 0$ می‌شود.

نتیجه:فرض کنید چند جمله‌ای‌های $f, f_s, \dots f_1$ متعلق به $k[x_1, \dots, x_n]$ باشند و r باقیمانده f بر $f_s, \dots f_1$ باشد بطوری که $r = 0$ ، در این صورت f متعلق به $< f_1, \dots, f_s >$ می باشد .

توجه کنید که با در نظر گرفتن ایده‌آل $I =< xy + 1, x + 1, y + 1 >$ وبا استفاده از الگـوریتم A-۱ ملاحظـه می‌شود که $f = xy^2 + 1$ به I تعلق دارد ولی باقیمانده f نسبت به I صفر نیست .

ایده‌آل I از $k[x_1, \dots, x_n]$ را یک ایده‌آل تک جمله‌ای نامیم هرگاه زیر مجموعه S از $\mathbb{Z}_{\geq 0}^n$ چنان موجود باشد که

$$I =< x^\alpha | \alpha \in S > \qquad (۱-۲۸)$$

$I =< x^4y^2, x^2y^5 >= \{\alpha.x^4y^2 + \beta.x^2y^5 | \alpha, \beta \in k[x_1, \dots, x_n]\}$ یک ایده‌آل تک جمله‌ای است.

فرض کنید $I =< x^\alpha | \alpha \in A >$ یک ایده‌آل تک جمله‌ای باشد، در این صورت $x^\beta \in I$ اگـر و تنهـا اگـر α_0 ای متعلق به A چنان موجود باشد که x^β مضربی از x^{α_0} باشد .($x^{\alpha_0} | x^\beta$).

ابتدا فرض کنیم $\alpha_0 \in A$ چنان موجود باشد که $x^{\alpha_0} | x^\beta$، لذا γ ی در $\mathbb{Z}_{\geq 0}^n$ موجـود اسـت کـه $x^\beta = x^{\alpha_0}x^\gamma$، در نتیجه $x^\beta \in I$

بالعکس: فرض کنیم $x^{\beta} \in I$، لذا $\alpha(1), \dots, \alpha(s)$ متعلق به A و همین‌طور چند جمله‌ای های $h_s, \dots, h_1$ در $k[x_1, \dots, x_n]$ موجودند که $x^{\beta} = \sum_{i=1}^{s} h_i x^{\alpha(i)}$

حال اگر h_i را بسط دهیم هر جمله سمت راست مضربی از $x^{\alpha(i)}$ ها است. (دو چند جمله‌ای وقتی با هم برابرند که جملات نظیر به نظیر با هم برابر باشند.) لذا x^{β} مضرب یکی از $x^{\alpha(i)}$ است.

فرض کنید I یک ایده‌آل تک جمله‌ای باشد و fعضوی از $k[x_1, \dots, x_n]$باشد ،در این‌صورت احکام زیر معادلند:

الف :f متعلق به I است.

ب: برای هر t در مجموعه ترم‌های f ، t متعلق به I می باشد .

پ: عناصر $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ متعلق به ایده‌آل I و همین‌طور$\lambda_s, \dots, \lambda_1$ در k چنان موجودند که $f = \sum_{i=1}^{s} \lambda_i x^{\alpha(i)}$.

ابتدا فرض کنیم برای هر t در مجموعه ترم‌های f، ترم t متعلق به I باشد. می‌خواهیم ثابت کنیم $f \in I$ که با توجه به فرض چیزی برای اثبات نداریم.

حال فرض کنیم چند جمله‌ای f متعلق به I باشد، نشان می دهیم عناصر $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ متعلق به ایده‌آل I و $\lambda_s, \dots, \lambda_1$ در k چنان موجودند که $f = \sum_{i=1}^{s} \lambda_i x^{\alpha(i)}$ می‌باشد .

و اگر فرض کنیم $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ در I و $\lambda_s, \dots, \lambda_1$ در k چنان موجود باشند که $f = \sum_{i=1}^{s} \lambda_i x^{\alpha(i)}$ که برای هر t در مجموعه ترم‌های f، ترم t متعلق به I است با توجه به اینکه ترم‌ها از I انتخاب می‌شود .

فرض کنید $I =< x^4y^2, x^3y^4, x^2y^5 >$ و $f = xy^4 + 5x^3y^2 + x^5y^3$ در این صورت f متعلق به I نیست، زیرا xy^4 مضرب هیچ یک از تک جمله ایهای x^4y^2, x^3y^4, x^2y^5 نیست داریم $f \ xy^4 \notin I$ متعلق به I نیست .

فرض کنید I, J دو ایده‌آل تک جمله‌ای باشند، در اینصورت $I = J$ اگر وتنها اگر مجموعه ی تک جمله ای های ایده آل I که آن را با $M(I)$نمایش می دهیم با مجموعه ی تک جمله ای های ایده آل J برابر است، به عبارتی:$M(I) = M(J)$.

ابتدا فرض کنید $I = J$ که در این صورت با توجه به فرض چیزی برای اثبات باقی نمی‌ماند.

حال فرض کنید $M(I) = M(J)$، می‌دانیم I, J به ترتیب توسط $M(I), M(J)$ تولید می‌شوند، لذا $I = J$.

(لم دیکسون[۸]):

فرض کنید $I =< x^{\alpha} | \alpha \in A \subseteq \mathbb{Z}_{\geq 0}^{n} >$، در این صورت $\alpha(s), \dots, \alpha(1)$ در A چنان موجودند که

$$I =< x^{\alpha(1)}, \dots, x^{\alpha(s)} > \qquad (۱-۲۹)$$

ابتدا با استقرا روی n نشان می‌دهیم I با مولد متناهی است.

برای $n = 1$ داریم :عضو α از زیر مجموعه A در $\mathbb{Z}_{\geq 0}$ موجود است به‌طوریکه ایده‌آل I در $k[x_1]$ توسط ${x_1}^{\alpha}$ تولید می‌شود. کوچکترین عضو مجموعه A را β می‌نامیم لذا ${x_1}^{\beta}$ تمامی مولدهای I را می‌شمارد، لذا داریم: $I =< {x_1}^{\beta} >$.

فرض هر ایده‌آل تک جمله‌ای در در شرط صدق کند و فرض کنیم y متغیری جدید و I ایده‌آلی تک جمله‌ای از $k[x_1, \dots, x_{n-1}, y]$ که آن رابرای سادگی با $k[x, y]$ نمایش می‌دهیم. قرار می‌دهیم:

$$M(k[x,y]) = \{x^{\alpha} y^{m} | \alpha \in \mathbb{Z}_{>0}^{n-1}, m \in \mathbb{Z}_{>0}\} \qquad (۱-۳۰)$$

ایده‌آل تک جمله‌ای J از $k[x_1, \dots, x_n]$ را به صورت زیر تعریف می‌کنیم:

$$J =< \{x^{\alpha} | \exists m \in \mathbb{Z}_{\geq 0} \ ; \ x^{\alpha} y^{m} \in I\} > \qquad (۱-۳۱)$$

که برای ایده‌آل داریم: $A = \{\alpha \in \mathbb{Z}_{>0}^{n-1} | \exists m \in \mathbb{Z}_{>0} \ ; \ x^{\alpha} y^{m} \in I\}$

اما از فرض استقرا مقادیر $\alpha(s), \dots, \alpha(1)$ از $\mathbb{Z}_{>0}^{n-1}$ موجود است که $J =< x^{\alpha(1)}, \dots, x^{\alpha(s)} >$. لذا از ساختار J مشاهده می‌شود که برای هر $1 \leq i \leq s$ ، مقدار m_i در $\mathbb{Z}_{\geq 0}$ موجود است که $x^{\alpha(i)} y^{m_i} \in I$

قرار می‌دهیم: $m := max\{m_1, \dots, m_s\}$.

حال برای هر $0 \leq l \leq m - 1$ ، ایده‌آل تک جمله‌ای I_l از $k[x_1, \dots, x_n]$را به صورت زیر تعریف می کنیم :

---

[۸] -Dickson

$$J_l := < x^\beta \,|\, x^\beta y^l \in I > \qquad (۱-۳۲)$$

بنابر فرض استقرا برای هر $0 \le l \le m-1$ عناصر $\alpha_l(s_l), \dots, \alpha_l(1)$ در $\mathbb{Z}_{>0}^{n-1}$ موجودند که $J_l := < x^{\alpha_l(1)}, \dots, x^{\alpha_l(s_l)} >$. ادعا می‌کنیم که I توسط مجموعه تک جمله‌ای‌های زیر تولید می‌شود:

$$x^{\alpha(1)}y^m, \dots, x^{\alpha(s)}y^m$$
$$x^{\alpha_0(1)}, \dots, x^{\alpha_0(s_0)}$$
$$x^{\alpha_1(1)}y, \dots, x^{\alpha_1(s_1)}y$$
$$\vdots$$
$$x^{\alpha_{m-1}(1)}y^{m-1}, \dots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1} \qquad (۱-۳۳)$$

(مشاهده می‌شود که سطر ۱ از J ، سطر ۲ از J_0 ، سطر ۳ از J_1 ،... سطر آخر از J_{m-1} می‌باشند. مجموعه فوق را B می‌نامیم) یعنی $I =< B >$. ابتدا ثابت می‌کنیم $I \supseteq < B >$.

اما داریم: $x^{\alpha(i)}y^m = x^{\alpha(1)}y^{m_i}y^{m-m_i}$ که عضوی از I است، لذا سطر اول در I قرار دارد. برای سطرهای بعدی هم $0 \le l \le m-1$ موجود است که هر عضوش به صورت $x^{\alpha_l(j)}y^l$ است که به J_l تعلق دارد. لذا از تعریف J_l بدست می‌آید $x^{\alpha_l(j)}y^l \in I$، لذا $B \subseteq I$ ، پس $< B > \subseteq I$. هر تک جمله‌ای ایده‌آل I ، مضرب یکی از اعضای B است. فرض کنید $x^\alpha y^u \in I$ (1)

در این‌صورت دو حالت در نظر می‌گیریم:

۱) فرض کنید $u \ge m$ ، در این‌صورت از تعریف ایده‌آل J داریم $x^\alpha \in J$، $\alpha(i)$ ای موجود است که $x^{\alpha(i)}$ بتواند x^α را عاد کند و همین طور γ متعلق به $\mathbb{Z}_{>0}^{n-1}$ موجود است که $x^\alpha = x^{\alpha(i)}x^\gamma$. پس $x^\alpha y^u = x^{\alpha(i)}y^m x^\gamma y^{u-m}$ که $x^{\alpha(i)}y^m$ به B متعلق است، لذا رابطه اخیر به $< B >$ تعلق دارد.

۲) فرض کنید $u < m-1$، از (۱-۲۲) داریم $x^\alpha \in J_u$ ، از تعریف ایده‌آل J_l داریم: مقادیر $1 \le j \le s$ در $\mathbb{Z}_{>0}^{n-1}$ موجودند که $x^\alpha = x^{\alpha_u(j)}x^\gamma$. لذا داریم: $x^\alpha y^u = x^{\alpha_u(j)}y^u x^\gamma$ که $x^{\alpha_u(j)}y^u$ به B تعلق دارد، پس $x^\alpha y^u$ در

$< B >$ قرار دارد. لذا در هر دو حالت رابطه $x^{\alpha}y^{u} \in < B >$ برقـرار اسـت، لـذا $I \subseteq < B >$ ، در نتیجـه داریـم: $I =< B >$.

برای تکمیل اثبات نشان می‌دهیم که عناصر $\gamma_s, \dots, \gamma_1$ در A چنان موجودند که:

$$I =< x^{\gamma_1}, \dots, x^{\gamma_s} > \qquad (۱-۳۴)$$

اما در قسمت قبـل دیـدیم کـه مقـادیر $\theta(1), \dots, \theta(z)$ در $\mathbb{Z}_{\geq 0}^{n}$ موجودنـد کـه $I =< x^{\theta(1)}, \dots, x^{\theta(z)} >$. امـا $x^{\theta(i)} \in I$ و از طرفی داریم $I =< x^{\alpha} | \alpha \in A >$ ، بـرای هـر $1 \leq i \leq z$ ، مقـادیر $\gamma(i) \in A$ و λ از $\mathbb{Z}_{\geq 0}^{n}$ چنـان موجودند که $x^{\theta(i)} = x^{\gamma(i)}x^{\lambda}$. اما از آنجا که $\gamma(i)|\theta(i)$ لذا

$$< x^{\gamma(1)}, \dots, x^{\gamma(s)} > \subseteq < x^{\theta(1)}, \dots, x^{\theta(z)} >$$

از طرفی سمت راست برابر I است و سمت چپ ابر مجموعه ایده‌آل I است، لذا عکس رابطـه بـالا برقراراسـت. در نتیجه داریم: $I =< x^{\gamma_1}, \dots, x^{\gamma_s} >$ و اثبات تمام است.

فرض کنید $\leq$ یک رابطه ترتیبی روی مجموعه $\mathbb{Z}_{\geq 0}^{n}$ باشد بطوریکه:

الف : $\leq$یک رابطه ترتیب کلی است.

ب: اگر $\beta \leq \alpha$، آنگاه برای γ در $\mathbb{Z}_{\geq 0}^{n}$ داشته باشیم: $\beta + \gamma \leq \alpha + \gamma$

در این صورت $(\mathbb{Z}_{\geq 0}^{n}, \leq)$ خوش‌ترتیب است اگر و تنها اگر برای هر α در $\mathbb{Z}_{\geq 0}^{n}$ بتوان نتیجه گرفت: $\alpha \geq 0$.

ابتدا فرض کنید برای هر α در $\mathbb{Z}_{\geq 0}^{n}$ داشته باشیم $\alpha \geq 0$. نشان می‌دهیم هر زیر مجموعه ناتهی مانند A از $\mathbb{Z}_{\geq 0}^{n}$ دارای می‌نیمم است. فرض کنید $I =< x^{\alpha} | \alpha \in A >$ ایده آلـی از $k[x_1, \dots, x_n]$باشـد، از لـم دیکسـون عناصـر $\alpha(s), \dots, \alpha(1)$ در A چنان موجودند که :

$$I =< x^{\alpha(1)}, \dots, x^{\alpha(s)} >$$

بدون کاستن از کلیت می‌توان فرض کرد: $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$. ادعا می‌کنیم

$$\alpha(1) = minA \qquad (۱-۳۵)$$

فرض $\alpha \in A$، لذا $1 \leq i \leq s \; x^{\alpha} \in I$ وجود دارد به گونه‌ای که x^{α} مضـربی از $x^{\alpha(i)}$ مـی باشـد ، لـذا γ در $\mathbb{Z}_{\geq 0}^{n}$ چنان موجود است که $x^{\alpha} = x^{\alpha(i)}x^{\gamma}$. چون $\gamma \geq 0$ و از شرط ب داریم :

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1) \qquad (۱-۳۶)$$

لذا خواهیم داشت: $\alpha \geq \alpha(1)$

حال فرض کنید $(\mathbb{Z}_{\geq 0}^{n}, \leq)$ خوش‌ترتیب باشد وهمین طور $\beta = min\mathbb{Z}_{>0}^{n}$، نشان می‌دهیم $\beta \geq 0$.

فرض کنید $\beta < 0$، در اینصورت از شرط ب داریم: $\beta + \beta < 0 + \beta$ ، لذا:

$$\beta + \beta < \beta = min\mathbb{Z}_{\geq 0}^{n} \qquad (۱-۳۷)$$

که این یک تناقض است، بنا براین $\beta \geq 0$، لذا برای هر عنصر $\mathbb{Z}_{\geq 0}^{n}$ مانند α داریم $\alpha \geq \beta \geq 0$ در نتیجه $\alpha \geq 0$و بدین ترتیب حکم ثابت می شود.

۱-۴ : پایه گروبنر

فرض کنید I ایده آلی از $k[x_1, \dots, x_n]$باشد ،در این صورت تعریف می‌کنیم:

$$LT(I) = \{c_{\alpha}x^{\alpha} | \alpha \in \mathbb{Z}_{\geq 0}^{n}, c_{\alpha} \in k, \exists f \in I \;\; ; \;\; Lt(f) = c_{\alpha}x^{\alpha}\} \qquad (۱-۳۸)$$

هرگاه $I =< f_1, \dots, f_s >$ ایده آلی از $k[x_1, \dots, x_n]$ باشد، در این صورت در حالت کلی داریم:

$$< LT(I) > \neq < Lt(f_1), \dots, Lt(f_s) > \qquad (۱-۳۹)$$

ولی همواره داریم:

$$< LT(I) > \supseteq < Lt(f_1), \dots, Lt(f_s) > \qquad (۱-۴۰)$$

$G = \{g_1, \dots, g_s\}$ را یک پایه گروبنر برای ایده‌آل I (نسبت به رابطه ترتیبی تک جمله‌ای دلخواه) نامیم هرگاه :

$$< LT(I) > = < Lt(g_1), \dots, Lt(g_s) > \qquad (۱-۴۱)$$

به عبارتی G یک پایه گروبنر برای I است اگر برای هر f در I ، چند جمله‌ای g_i متعلق به G چنان موجود باشد که $Lt(g_i)$، بتواند $Lt(f)$ را بشمارد.

فرض کنید I ایده آلی از $k[x_1,\dots,x_n]$ باشد، در این صورت:

الف : $< LT(I) >$یک ایده‌آل تک جمله‌ای است.

ب: عناصر $g_s,\dots,g_1$ از I چنان موجودند که $< LT(I) >=< Lt(g_1),\dots,Lt(g_s) >$

الف: داریم که $< LM(I) >=< LT(I) >$ و $< LM(I) >$ ایده‌آل تک جمله‌ای است.

هر ایده‌آل غیر صفر در $k[x_1,\dots,x_n]$، یک پایه گروبنر دارد.

فرض کنید I ایده آلی از $k[x_1,\dots,x_n]$ داریم $< LT(I) >$ ایده‌آل تک جمله‌ای است، بنابراین چند جمله‌ای‌های $f_s,\dots,f_1$ از I چنان موجودند که:

$$< LT(I) >=< lt(f_1),\dots,lt(f_s) > \qquad (۱-۴۱)$$

نتیجه هر پایه گروبنر برای یک ایده‌آل، مولدی برای آن ایده‌آل است

با توجه به نتیجه (۱-۴-۵) می‌دانیم که هر ایده‌آل غیر صفر در $k[x_1,\dots,x_n]$ پایه‌ای گروبنر دارد. فرض کنید عناصر $f_s,\dots,f_1$ از I چنان موجودند که $< LT(I) >=< lt(f_1),\dots,lt(f_s) >$. ادعا می‌کنیم :

$$I =< f_1,\dots,f_s > \qquad (۱-۴۲)$$

با توجه به فرض $< f_1,\dots,f_s >$ زیر مجموعه ای از I است . برای اثبات جزئیت عکس فرض کنید f عضوی از I باشد، نشان می دهیم fمتعلق به $< f_1,\dots,f_s >$است ، بنا بر الگوریتم تقسیم چندجمله‌ای‌های $g_s,\dots,g_1,r$ در $k[x_1,\dots,x_n]$ چنان موجودند که $(1)\ f = f_1g_1+\dots+f_sg_s+r$، که در آن $r=0$ یا هیچ ترمی از r مضربی از $Lt(f_i)$ نیست. ادعا می‌کنیم $r=0$. فرض کنیدچنین نباشددر این صورت از رابطه **(۱-۴۲)** داریم:

$$r = f - (f_1 g_1 + \cdots + f_s g_s) \qquad (۱-۴۳)$$

که از آن نتیجه می‌شود: $Lt(r) \in < LT(I) > = < Lt(f_1), \ldots, Lt(f_s) >$. لذا $Lt(r)$ مضرب یکی از $Lt(f_i)$ است که این تناقض است، بنا براین $r = 0$ و در نتیجه f متعلق به $< f_1, \ldots, f_s >$ است.

پایه هیلبرت:

هر ایده‌آل در $k[x_1, \ldots, x_n]$ با تولید متناهی است.

فرض کنید I ایده آلی از $k[x_1, \ldots, x_n]$ باشد در این صورت بنا به نتیجه دارای یک پایه گروبنر می باشد و بنا به هر پایه گروبنر برای یک ایده‌آل، مولدی برای آن ایده‌آل است.

فرض کنید $G = \{g_1, \ldots, g_s\}$ پایه گروبنری برای ایده‌آل I باشد. در این صورت برای هر $f \in I$، عنصر منحصربفرد r متعلق به $k[x_1, \ldots, x_n]$ چنان موجود است که

۱) هیچ ترمی از r، مضربی از $Lt(g_i)$ها نیست.

۲) چند جمله‌ای g در I موجود است که $f = g + r$.

بعلاوه r باقیمانده تقسیم f بر G است و این باقیمانده مستقل از ترتیب قرار گرفتن $g_1, \ldots, g_s$ است.

بنا به الگوریتم تقسیم چند جمله‌ای‌های $f_1, \ldots, f_s$ از I و r در $k[x_1, \ldots, x_n]$ چنان موجودند که

$$f = g_1 f_1 + \cdots + g_s f_s + r \qquad (۱-۴۴)$$

که r و g در شرایط ۱ و ۲ صدق می کند .

اثبات منحصربفردی : فرض کنید r^* نیز در شرایط ۱ و ۲ صدق کند، بنابراین g^* در I چنان موجود است که $f = g^* + r^* = g + r$، پس داریم: $r - r^* = g^* - g \in I$.

حال اگر $r - r^* \neq 0$ آنگاه:

$$Lt(r - r^*) = Lt(g^* - g) \in < LT(I) > = < Lt(g_1), \ldots, Lt(g_s) > \quad \text{یکی از ترم‌های } r \text{ یا } r^* \qquad (۱-۴۵)$$

که تناقض است،پس $r - r^* = 0$ و $r = r^*$ لذا r منحصربفرد است.

اگر f چند جمله‌ای در $k[x_1, \dots, x_n]$ و $\{g_1, \dots, g_s\}$ پایه گروبنر باشد، آنگاه باقیمانده f بر $\{g_1, \dots, g_s\}$ را فرم نرمال [۹] f نسبت به $\{g_1, \dots, g_s\}$ می‌نامیم و به صورت $NormalForm(f, [g_1, \dots, g_s])$ نمایش می‌دهیم .

نماد گذاری : قرار می دهیم $G = \{g_1, \dots, g_s\}$ در این صورت فرم نرمال f نسبت به G را به صورت زیر نمایش می دهیم :

$$\bar{f}^G := NormalForm(f, G). \qquad (۱-۴۶)$$

اگر $G = \{g_1, \dots, g_s\}$ یک پایه گروبنر برای I باشد، چند جمله‌ای f عضو ایده‌آل I است اگر وتنها اگر $NormalForm(f, G) = 0$.

فرض کنیم فرم نرمال f نسبت به G صفر باشد، در این‌صورت با توجه به نتیجه حکم برقرار است. حال فرض کنید $f \in I$ ، در این‌صورت با استفاده از و با فرض $f = g$ خواهیم داشت: $f = f + 0$. با توجه به منحصر بفرد بودن r و تعریف داریم: $r = 0$.

حال به دنبال الگوریتمی برای تشخیص این که یک مجموعه از چند جمله‌ای‌ها یک پایه گروبنر برای یک ایده‌آل است یا نه هستیم ، بدین منظور ابتدا به معرفی چند مفهوم خاص از جمله، کوچکترین مضرب مشترک و $s-$ چند جمله‌ایها می پردازیم.

فرض کنید p, q اعضای $\mathbb{Z}_{\geq 0}^n$ باشند، در این‌صورت کوچکترین مضرب مشترک p و q برابر است با :

$$\gamma = (\max(p_1, q_1), \max(p_2, q_2), \dots, \max(p_n, q_n)) \qquad (۱-۴۷)$$

به همین ترتیب می توان کوچکترین مضرب مشترک دو تک جمله ای را تعریف کرد .

---

[۹] -NormalForm

به عنوان مثال کوچکترین مضرب مشترک دو تک جمله‌ای x^2y^2z و yz^4 برابر است با $x^2y^2z^4$.

فرض کنید f,g دو چند جمله‌ای در $k[x_1,\dots,x_n]$ باشند، در این‌صورت s - چند جمله‌ای f,g را با نماد $S(f,g)$ نمایش داده و به صورت زیر نمایش می‌دهیم:

$$S(f,g) \coloneqq \frac{x^\gamma}{Lt(f)}f - \frac{x^\gamma}{Lt(g)}g \qquad (۱-۴۸)$$

که در آن x^γ کوچکترین مضرب مشترک جملات پیشروی f,g است.

فرض کنید $f = y - x^2, g = z - x^3$ دو چند جمله‌ای در $k[x,y]$ و ترتیب $<_{lex}$ با $x > y > z$ در نظر بگیرید. در این صورت داریم :

$$Lt(f) = -x^2$$

$$Lt(g) = -x^3$$

$$x^\gamma = x^3$$

$$S(f,g) = \frac{x^3}{-x^2}f - \frac{x^3}{-x^3}g = -xf + g = -xy + z \qquad (۱-۴۹)$$

اگر ترم پیشروی ترکیبی از چند جمله‌ای‌ها با جمله پیشروی یکسان حذف شود، آنگاه ترکیب فوق را می‌توان به صورت مجموعی از s - چند جمله‌ای‌ها نوشت.

فرض کنید $f = \sum_{i=1}^{s} c_i f_i$ که در آن $c_i \in k$, $f_i \in k[x_1,\dots,x_n]$ ، و همین طور برای هر $1 \le i \le s$ داشته باشیم: $multideg(f_i) = \gamma$.

حال اگر داشته باشیم $multideg(f) < \gamma$، آنگاه c_{i_j} هائی متعلق به k چنان موجودند که $f = \sum_{i=1}^{s}\sum_{j=1}^{s} c_{i_j} S(f_i,f_j)$ و بعلاوه برای هر $1 \le i \le s$ داریم: $multideg\left(S(f_i,f_j)\right) < \gamma$.

فرض کنید $d_i = lc(f_i)$، نشان می‌دهیم :

$$f = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s) \quad (1) \quad (۱-۵۰)$$

بدین منظور قرار می‌دهیم: $p_i = \frac{f_i}{d_i}$

توجه کنید که $Lt(f_i) = d_i x^\gamma$. فرض کنید کوچکترین مضرب مشترک $lm(f_i), lm(f_j)$ برابر x^γ باشد، در این‌صورت داریم:

$$S(f_i, f_j) = \frac{x^\gamma}{lt(f_i)} f_i - \frac{x^\gamma}{lt(f_j)} f_j = \frac{x^\gamma}{d_i x^\gamma} f_i - \frac{x^\gamma}{d_j x^\gamma} f_j = p_i - p_j \quad (۱-۵۱)$$

با بسط سمت راست رابطه (۱-۵۰)داریم:

$$c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \quad (۱-۵۲)$$

اما از فرض داریم: $multideg(f) < \gamma$ ، لذا $c_1 d_1 + \cdots + c_s d_s = 0$ ، بنا براین رابطه فوق را می توان به صورت زیر نوشت :

$$\begin{aligned} c_1 d_1 p_1 + (-c_1 d_1 + c_1 d_1) p_2 + c_2 d_2 p_2 + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) p_{s-1} + \\ \ldots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) p_s + (c_1 d_1 + \cdots + c_s d_s) p_s = c_1 d_1 p_1 + c_2 d_2 p_2 + \cdots + c_s d_s p_s \\ = c_1 f_1 + \cdots + c_s f_s \\ = f \end{aligned} \quad (۱-۵۳)$$

برای قسمت آخر از آنجا که $S(f_i, f_j) = p_i - p_j$ ، و از طرفی

$$multideg(p_i) = \gamma, multideg(p_j) = \gamma \quad (۱-۵۴)$$

لذا

$$multideg\left(S(f_i, f_j)\right) = multideg(p_i - p_j) < \gamma \quad (۱-۵۵)$$

s – چند جمله‌ای محک بوخبرگر[۱۰] را برای تشخیص اینکه یک مولد برای یک ایده آل یک پایه گروبنر هست یا نه ارائه می دهیم .

محک بوخبرگر

فرض کنید $G = \{g_1, \dots, g_s\}$ مولدی برای ایده‌آل I باشد، در این‌صورت G یک پایه گروبنر برای I است اگر وتنها اگر برای هر i,j باقیمانده تقسیم $S(g_i, g_j)$ نسبت به G برابر صفر باشد.

ابتدا فرض کنید G یک پایه گروبنر برای ایده‌آل I باشد، در این‌صورت برای هر i,j با توجه به اینکه $S(g_i, g_j)$ عضوی از I است داریم: $NormalForm(S(g_i, g_j), G) = 0$ یعنی باقیمانده $S(g_i, g_j)$ نسبت به G برابر صفر است.

بالعکس، فرض کنید برای هر i,j باقیمانده $S(g_i, g_j)$ نسبت به G برابر صفر باشد، نشان می دهیم G یک پایه گروبنر برای I است. بدین منظور فرض می‌کنیم f عضوی از ایده آل $I =< g_1, \dots, g_s >$ باشد، نشان می‌دهیم ترم پیشروی f متعلق به ایده‌آل $< lt(g_1), \dots lt(g_s) >$ می باشد.

ترکیبی از f مانند $f = \sum_{i=1}^{s} h_i g_i$ را انتخاب می‌کنیم که اگر برای آن داشته باشیم $f = \sum_{i=1}^{s} \acute{h}_i g_i$ ، آنگاه بتوان نتیجه گرفت:

$$\max\{multideg(g_i h_i)\} \leq \max\{multideg(g_i \acute{h}_i)\} \qquad (۱-۵۶)$$

همچنین برای هر i تعریف می‌کنیم: $m(i) = multideg(g_i h_i)$ و $\gamma = \max\{multideg(g_i h_i)\}$. از طرفی $multideg(f) \leq \max\{multideg(g_i h_i)\}$، حال اگر ثابت کنیم $multideg(f) = \gamma$ آنگاه حکم ثابت است، زیرا در این‌صورت عنصر j ای موجود است که $multideg(g_j h_j) = \gamma$، لذا حاصل ضرب جمله پیشروی g_j و جمله پیشروی h_j برابر جمله پیشروی f می‌شود، لذا :

$$Lt(f) \in < Lt(g_1), \dots Lt(g_s) >$$

---

[۱۰] -Buchberger

فرض کنید $multideg(f) < \gamma$، لذا داریم:

$$f = \sum_{m(i)=\gamma} g_i h_i + \sum_{m(i)<\gamma} g_i h_i$$
$$= \sum_{m(i)=\gamma} Lt(h_i) g_i + \sum_{m(i)=\gamma} (h_i - Lt(h_i)) g_i + \sum_{m(i)<\gamma} g_i h_i \qquad (1) \qquad (۱-۵۷)$$

در آخرین تساوی رابطه فوق ، جملات مجموع دوم و سوم دارای مالتی درجه کمتر از γ هستند(در جملات مجموع دوم هر h_i از ترم پیشروی خود کم شده است) لذا ، مالتی درجه مجموع دوم و سوم از γ کمتر است.اما مالتی درجه f نیز از γ کمتر است، بنا براین باید مالتی درجه مجموع اول نیز از γ کمتر باشد. از طرفی در مجموع اول مالتی درجه هر جمله برابر γ است، لذا شرایط برای مجموع اول برقرار است. داریم:

$$\sum_{m(i)=\gamma} Lt(h_i) g_i = \sum_{i,j} c_{i_j} S(Lt(h_i) g_i, Lt(h_j) g_j) \quad (2)$$

(۱-۵۸)

که در آن

$$multideg\left(S(Lt(h_i) g_i, Lt(h_j) g_j)\right) < \gamma \quad (3) \qquad (۱-۵۹)$$

اما با فرض $Lt(h_i) = d_i x^{\alpha(i)}$ داریم:

$$S(Lt(h_i) g_i, Lt(h_j) g_j) = \frac{x^\gamma}{Lt(g_i) d_i x^{\alpha(i)}} Lt(h_i) g_i - \frac{x^\gamma}{Lt(g_j) d_i x^{\alpha(i)}} Lt(h_j) g_j$$
$$= \frac{x^\gamma}{Lt(g_i)} g_i - \frac{x^\gamma}{Lt(g_j)} g_j \frac{x^\gamma}{x^{\delta_{i_j}}} S(g_i, g_j) \qquad (۱-۶۰)$$

(دقت کنید که $multideg(lt(h_i) g_i) = multideg(g_i h_i)$ و همین‌طور $x^{\delta_{i_j}}$ کوچکترین مضرب مشترک $lm(g_i), lm(g_j)$ می‌باشد.) با توجه به اینکه باقیمانده $S(g_i, g_j)$ نسبت به G برابر صفر است بنا بر الگوریتم تقسیم چند متغیره (A-۱) عناصر ω_{i_j} از $k[x_1, \dots, x_n]$ چنان موجودند که

$$S(g_i, g_j) = \sum_{l=1}^{s} \omega_{i_j} g_l + 0 \quad ; \quad multideg\left(\omega_{i_j} g_l\right) \le multideg(S(g_i, g_j))$$

(۱-۶۱)

با ضرب $x^{\gamma-\delta_{i_j}}$ در دو طرف رابطه اخیر داریم:

$$x^{\gamma-\delta_{i_j}} S(g_i, g_j) = \sum_{l=1}^{s} x^{\gamma-\delta_{i_j}} \omega_{i_j} g_l \qquad (5)$$

(۱-۶۲)

با استفاده از تساوی‌های **(۱-۵۸)** و **(۱-۶۰)** داریم:

$$\sum_{m(i)=\gamma} lt(h_i) g_i = \sum_{l} \sum_{i,j} c_{i_j} x^{\gamma-\delta_{i_j}} \omega_{i_j} g_l$$

(۱-۶۳)

و بنا به نامساوی **(۱-۵۹)** و تساوی‌های **(۱-۶۰)** و **(۱-۶۱)** خواهیم داشت:

$$multideg\left(c_{i_j} x^{\gamma-\delta_{i_j}} \omega_{i_j} g_l\right) < \gamma$$

که با قرار دادن رابطه بالا در **(۱-۵۹)** به تناقض می‌رسیم. لذا فرض خلف باطل بوده و مالتی درجه f برابر γ است، پس حکم برقرار است.

اگر $G = \{g_1, \dots, g_s\}$ مولدی برای ایده‌آل I در $k[x_1, \dots, x_n]$ باشد آنگاه شرایط زیر معادل می باشند:

الف :مجموعه G پایه گروبنر برای I می‌باشد.

ب: برای هر ترم t در مجموعه ترم‌های پیشروی I ، ترم s در مجموعه ترم‌های پیشروی G موجود باشد که t مضربی از s باشد.

۱-۵ : الگوریتم بوخبرگر

در ابتدای این بخش به بیان الگوریتم بوخبرگر برای محاسبه پایه گروبنر پرداخته و سپس با بیان تعاریف جدید، پایه گروبنر منحصر بفردی برای ایده‌آل بدست می‌آوریم ودر انتها روشی برای بهینه کردن الگورتیم بوخبرگر را ارائه می‌کنیم.

الگوریتم بوخبرگر

فرض کنید $I =< f_1, \dots, f_s >$ یک ایده‌آل از چند جمله‌ای‌ها در $k[x_1, \dots, x_n]$ باشد، در این‌صورت با استفاده از الگوریتم زیر پایه گروبنری برای ایده‌آل I در تعداد متناهی گام بدست می‌آید.

INPUT: $F = (f_1, \dots, f_s)$
OUTPUT: *a Groebner basis* $G = (g_1, \dots, g_t)$ *for* I *, with* $F \subset G$
$G := F$
REPEAT
$G' := G$
    FOR *each pair* $\{p, q\}$ *,* $p \neq q$ *in* G' **DO**
        $S := \overline{S(p,q)}^{G}$
        IF $S \neq 0$ **THEN** $G := G \cup \{S\}$
UNTIL $G = G'$

A-۲- الگوریتم بوخبرگر

نشان می‌دهیم:

الف) در هر گام از الگوریتم G زیر مجموعه‌ای ازایده‌آل I است.

ب) در پایان کار، G یک پایه گروبنر است.

ج) الگوریتم پایان پذیر است.

الف) ابتدا در شروع کار داریم: $G = F \subset I$ و در ادامه طبق الگوریتم اعضای G وقتی افزایش می‌یابند که چند جمله‌ای غیر صفر $g = \overline{S(p,q)}^{G}$ به آن اضافه شود. پس برای هر p, q در G' که $G' \subseteq G$ است داریم $s-$ چند جمله‌ای p, q متعلق به I است. لذا داریم $\overline{S(p,q)}^{G} \in I$ ، پس g به I تعلق دارد. پس (الف) همواره برقرار است.

ب) در پایان الگوریتم برای هر p, q ، مشاهده می‌شود که $s-$ چند جمله‌ای p, q نسبت به G برابر صفر است، می‌دانیم که G یک پایه گروبنر است که F را شامل می‌شود.

ج) در هر گام از الگوریتم G' زیر مجموعه‌ای از G است، لذا $< Lt(G') >$ نیز زیر مجموعه‌ای از $< Lt(G) >$ می‌باشد. قبل از پایان حلقه اصلی نشان می‌دهیم: $Lt(G') \neq Lt(G)$.

فرض کنید در گام مفروضی عنصر غیر صفر $g = \overline{S(p,q)}^{G'}$ به G اضافه شده باشد، پس G باقیمانده تقسیم $S(p,q)$ نسبت به مجموعه G' است و بنابراین ترم پیشروی g مضرب هیچ یک از ترم‌های پیشروی اعضای G' نمی‌باشد. لذا $Lt(g) \notin < Lt(G') >$ ولی ترم پیشروی g عضوی از $< Lt(G) >$ است. حال اگر G', G را در گام i-ام الگوریتم به ترتیب G'_i, G_i بنامیم زنجیر صعودی اکید زیر را داریم:

$$< Lt(G'_1) > \subsetneq < Lt(G'_2) > \subsetneq \cdots \subsetneq < Lt(G'_i) > \subsetneq \cdots$$

که بنا به شرط زنجیر صعودی در حلقه نوتری $k[x_1, \ldots, x_n]$ ، لذا الگوریتم پس از چند گام متناهی متوقف می‌شود.

فرض کنید $I = < f_1, f_2 >$ که در آن $f_1 = x^3 - 2xy\,, f_2 = x^2y - 2y^2 + x$ باشند و رابطه ترتیبی $<_{lex}$ با $x > y$ را در نظر گرفته شده باشد. به دنبال پایه گروبنری برای I هستیم. ملاحظه می‌کنید از آنجا که $Lt(S(f_1,f_2)) = x^2$ و x^2 عضوی از $< Lt(f_1), Lt(f_2) >$ نمی‌باشد پس $\{f_1, f_2\}$ پایه گروبنری برای I نیست. داریم $S(f_1,f_2) = x^2$، که باقیمانده x^2 نسبت به $\{f_1, f_2\}$ صفر نمی‌شود. لذا با قرار دادن $f_3 = S(f_1,f_2)$ داریم $F = (f_1, f_2, f_3)$. داریم: $\overline{S(f_1,f_2)}^F = \overline{f_3}^F = 0$ ولی $\overline{S(f_1,f_3)}^F = \overline{-2xy}^F \neq 0$. پس باید $f_4 = -2xy$ به F اضافه شود. با بکار بردن دوباره الگوریتم بوخبرگر خواهیم داشت: $\overline{S(f_1,f_2)}^F = \overline{S(f_1,f_3)}^F = 0$ و $\overline{S(f_1,f_4)}^F = \overline{-2xy^2}^F = 0$ است، اما $\overline{S(f_2,f_3)}^F = \overline{-2y^2 + x}^F \neq 0$

با تکرار روند بالا و در نظر گرفتن $f_5 = -2y^2 + x$ و $F = (f_1, f_2, f_3, f_4, f_5)$ برای هر $1 \leq i < j \leq 5$ داریم: $\overline{S(f_i,f_j)}^F = 0$. پس بنا به محک بوخبرگر $G = \{f_1, f_2, f_3, f_4, f_5\}$ یک پایه گروبنر برای I است.

فرض کنید $G = \{g_1, \ldots, g_s\}$ پایه گروبنری برای I باشد. اگر p در G چنان موجود باشد که جمله پیشروی p متعلق به $< Lt(G - \{p\}) >$ باشد، آنگاه $G - \{p\}$ نیز یک پایه گروبنر است.

چون G پایه گربنر برای I است لذا $< Lt(I) >=< Lt(G) >$. با استفاده از تعریف پایه گروبنر کافی است نشان دهیم: $< Lt(G) >=< Lt(G - \{p\}) >$.

توجه کنید که $G - \{p\} \subseteq G$ لذا ترم پیشروی $(G - \{p\})$ زیر مجموعه ترم پیشروی G است و در نتیجه داریم:

$< Lt(G - \{p\}) > \subseteq < Lt(G) >$.

بـرای اثبـات جزئیـت عکـس، فـرض کنیـد α متعلـق بـه $< Lt(G) >$ باشـد ، نشـان مـی دهـیم α متعلـق بـه $< Lt(G - \{p\}) >$ است. بنا بر فرض i ای موجوداست که ترم پیشروی g_i بتواند α را بشمارد. دو حالت در نظـر می‌گیریم:

الف : اگر $g_i \neq p$ ، آنگاه حکم برقرار است.

ب : اگر $g_i = p$ ،آنگاه از فرض j ای موجود است که $i \neq j$ وترم پیشروی p مضربی از ترم پیشروی g_i می باشد و همین طور $Lt(p)$ عنصر α را عاد می‌کند . لذا حکم برقرار است.

پایه گروبنر G برای ایده‌آل I را یک پایه گروبنر می‌نیمال نامیم هر گاه:

الف :برای هر p در G، ضریب پیشروی p برابر ۱ باشد.

ب : برای هر p در G ، ترم پیشروی p در ایده‌آل $< lt(G - \{p\}) >$ نباشد.

فـرض کنیـد مجموعـه ی G تعریـف شـده بـه صـورت زیـر یـک پایـه گروبنـر بـرای ایـده آل $I =< x^3 - 2xy\,, x^2y - 2y^2 + x >$ باشد.

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

ترتیب $<_{lex}$ با شرط $x > y$ را در نظر بگیرید ، از آنجا که $Lt(f_1) = x^3 = -x.Lt(f_3)$ لذا با استفاده از (۱-۵-۳) f_1 در پایه گروبنر می‌نیمال نیست.

همین طور $Lt(f_2) = x^2y = -\left(\frac{1}{2}\right)x.Lt(f_4)$، لذا f_2 را نیز می‌توان حذف کرد.

پایه گروبنر می‌نیمال برای I به صورت زیر بدست می‌آید:

$$G = \{g_1 = x^2, g_2 = xy, g_3 = y^2 - \frac{1}{2}x\} \qquad (۱-۶۴)$$

اکنون به دنبال پایه گروبنری منحصر بفرد برای ایده‌آل دلخواه I نسبت به ترتیب مفروض هستیم.

چند جمله‌ای g از G را نسبت به G تقلیل یافته نامیم هر گاه هیچ یک از جملات g مضربی از هیچ یـک از تـرم-های پیشروی $G - \{g\}$ نباشد.

به طور مثال باقیمانده f نسبت به $G = \{g_1, \dots, g_s\}$ ، عنصری تقلیل یافته نسبت به G است.

پایه گروبنر G برای ایده‌آل I را یک پایه گروبنر تقلیل یافته برای I نامیم هر گاه:

الف: برای هر عنصر p از G، ضریب پیشروی p برابر یک باشد.

ب : برای هر ترم دلخواه t از مجموعه ترم‌های p در G ،رابطه زیر برقرار باشد:

$t \notin < Lt(G - \{p\}) >$، یعنی p نسبت به G تقلیل یافته باشد.

هر ایده‌آل غیر صفر در $k[x_1, \dots, x_n]$ نسبت به یک ترتیب مفروض دارای پایه گروبنر تقلیل یافته منحصر بفردی است.

می‌دانیم برای ایده‌آل غیر صفر I ، پایه گروبنر G موجود است که مـی‌تـوان G را بـا اسـتفاده از (۱-۶۴)بـه پایـه گروبنر می‌نیمال تبدیل کرد. فرض کنید g عضوی دلخواه در G باشد. قرار می‌دهیم $g' = \bar{g}^{G-\{g\}}$ و همـین طـور $G' = (G - \{g\}) \cup \{g'\}$ ، در اینصورت با توجه به اینکه g' باقیمانده نسبت به G' است لذا g' نسبت به G' تقلیل یافته است. اما G' زیر مجموعه I است و چون تنها اختلاف G, G' در g, g' است و داریم $Lt(g) = Lt(g')$ ، لذا

$$< Lt(I) > = < Lt(G) > = < Lt(G') > \qquad (1) \qquad (۱-۶۵)$$

(دقت کنید G می‌نیمال است پس ترم پیشروی g مضرب هیچ یک از ترم‌های پیشروی $G - \{g\}$ نیست و لذا در باقیمانده یعنی g' می‌ماند) از (۱-۶۵) نتیجه می‌شود G' یک پایه گروبنر می‌نیمال است. با تکرار فرایند فوق برای همه عناصر G ، پایه گروبنر بدست آمده تقلیل یافته است. حال فرض کنید G, G' دو پایـه گروبنـر تقلیـل یافتـه

برای ایده‌آل I باشند. نشان می‌دهیم: $G = \acute{G}$. از اینکه $G, \acute{G}$ دو پایه گروبنر می‌نیمال هستند داریم: $Lt(G) = Lt(\acute{G})$.

فرض $g \in G$ باشد، نشان می‌دهیم g به $\acute{G}$ تعلق دارد. از این که g عضو G است نتیجه می‌گیریم که ترم پیشروی g به $Lt(\acute{G}), Lt(G)$ تعلق دارد، لذا $\acute{g}$ در $\acute{G}$ وجود دارد که $Lt(g) = Lt(\acute{g})$.

نشان می دهیم: $g = \acute{g}$. اما از این که $Lt(g) = Lt(\acute{g})$ لذا ترم پیشروی $g - \acute{g}$ حذف می‌شود و ترم‌های $g - \acute{g}$ مضرب هیچ یک از جملات پیشروی G (که با جملات پیشروی $\acute{G}$ یکی هستند) نیستند، پس داریم: $\overline{g - \acute{g}}^{G} = g - \acute{g}$. از طرفی $g - \acute{g}$ به ایده‌آل I تعلق دارد، پس داریم $\overline{g - \acute{g}}^{G} = 0$. از طرفی چون G پایه گروبنر و بنابر باقیمانده $g - \acute{g}$ نسبت به G منحصر بفرد است پس باید $g - \acute{g} = 0$ و لذا $g = \acute{g}$ باشد. پس G زیر مجموعه $\acute{G}$ است و به طریق مشابه $\acute{G}$ زیر مجموعه G است،

در نتیجه داریم: $G = \acute{G}$و لذا پایه گروبنر تقلیل یافته برای ایده‌آل I منحصر بفرد است.

می‌دانیم که $G = \{g_1 = x^2, g_2 = xy, g_3 = y^2 - \frac{1}{2}x\}$ یک پایه گروبنر می‌نیمال برای ایده‌آل $I =< x^3 - 2xy\ , x^2y - 2y^2 + x >$ است. با استفاده از تعاریف $H = \{x^2, xy, y^2 - \frac{1}{2}x\}$ یک پایه گروبنر تقلیل یافته برای I است.

در حالتی که $F = \{f_1, \dots, f_s\}$ به عنوان زیر مجموعه ای از $k[x_1, \dots, x_n]$ شامل چند جمله ایهای خطی باشد ، دراین صورت ماتریس تحویل شده سطری پلکانی معادل با ماتریس ضرا ئب F یک پایه گروبنر تقلیل یافته می باشد .

ترتیب $<_{lex}$ با شرط $x > y > z > w$ را در نظر بگیرید برای ایده آل $I =< 3x - 6y - 2z\ , 2x - 4y + 4w, x - 2y - z - w >$ داریم :

$$\begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & -4 \\ 1 & -2 & -1 & -1 \end{pmatrix}$$

باانجام اعمال سطری پلکانی تحویل شده ماتریس فوق به ماتریس زیر تبدیل می شود:

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

لذا داریم:

$$I =< 3x - 6y - 2z\,, 2x - 4y + 4w, x - 2y - z - w >=< x - 2y + 2w, z + 3w > \qquad (۱-۶۶)$$

دو ایده آل I و J برابرند اگر وتنها اگر پایه گروبنر تقلیل یافته ی آنها نسبت به یک ترتیب خاص برابر باشند.

چند جمله‌ای f و مجموعه $G = \{g_1, \dots, g_s\}$ در $k[x_1, \dots, x_n]$ و رابطه ترتیبی $<$ را در نظر بگیرید.اگر چند جمله‌ای‌های $a_s, \dots, a_1$ در $k[x_1, \dots, x_n]$ موجود باشد که بتوان f را به صورت $f = a_1g_1 + \cdots + a_sg_s$ نمایش داد که در آن برای هر $a_ig_i \neq 0$ داشته باشیم:

$$multideg\,(f) \geq multideg\,(a_ig_i) \qquad (۱-۶۷)$$

آنگاه گوییم f نسبت به G به صفر تقلیل می‌یابد و به صورت زیر نمایش می‌دهیم : $f \to_G 0$.

چند جمله‌ای f و مجموعه مرتب $G = \{g_1, \dots, g_s\}$ در $k[x_1, \dots, x_n]$را در نظر بگیرید.اگر فرم نرمال f نسبت به G صفر باشد آنگاه f نسبت به G تقلیل می‌یابد .

اگر فرم نرمال f نسبت به G صفر باشد از الگوریتم A-🗁 چند جمله‌ای‌های $a_1, \dots, a_s$ موجودند که

$$f = a_1g_1 + \cdots + a_sg_s + 0 \qquad (۱-۶۸)$$

و برای هر a_ig_i که مخالف صفر باشد داریم: $multideg\,(f) \geq multideg\,(a_ig_i)$

این نشان می‌دهد که f نسبت به G تقلیل می‌یابد.

فصل دوم

حلقه های پایا

۲-۱: چند جمله ایهای پایا

در این بخش خواص اساسی حلقه های پایا از گروههای ماتریسی متناهی شرح داده می شود.

فرض کنید k یک میدان با مشخصه صفر باشد و $R = k[x_1, x_2, \dots, x_n]$ حلقه چند جمله ای ها روی متغیرهای $x_n, \dots x_2, x_1$ باشد .

چندجمله ای $f(x_1, x_2, \dots, x_n)$ متعلق به $R = k[x_1, x_2, \dots, x_n]$ را یک چند جمله ای متقارن نامیم هرگاه :

$$f(x_1, x_2, \dots, x_n) = f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) \qquad (۲-۱)$$

برای هر جایگشتی که در آن $\{i_1, \dots, i_n\} = \{1, \dots, n\}$.

بویژه چندجمله ایهای

$$\delta_1 = x_1 + x_2 + \cdots + x_n$$
$$\vdots$$

$$\delta_r = \sum_{1 \le i_1 < \cdots < i_r \le n} x_{i_1} \cdots x_{i_r}$$

$$\vdots$$

$$\delta_n = x_1 . x_2 . \ldots . x_n$$

چند جمله ایهای متقارن مقدماتی می باشند .

قضیه اساسی چند جمله ایهای متقارن

هر چند جمله ای متقارن در $R = k[x_1, x_2, \ldots, x_n]$ را می توان به صورت منحصربفردی به عنوان چند جمله ای از δ_1 و ... و δ_n نوشت .

نشان می دهیم برای هر چندجمله ای متقارن f از $R = k[x_1, x_2, \ldots, x_n]$ چندجمله ای g متعلق به $k[y_1, y_2, \ldots, y_n]$ چنان موجود است که $f = g(\delta_1, \ldots, \delta_n)$. ترتیب Lex را در $k[x_1, x_2, \ldots, x_n]$ با شرط $x_1 > x_2 > \cdots > x_n$ در نظر می گیریم . فرض کنید

$$Lt(f) = \gamma X^{\alpha} = \gamma x_1^{\alpha_1} \cdots x_n^{\alpha_n} \qquad (۲-۲)$$

ادعا می کنیم $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_n$.

فرض کنید $1 \le j \le n$ ای موجود باشد که $\alpha_j < \alpha_{j+1}$ ، قرار می دهیم :

$$\beta = (\alpha_1, \ldots, \alpha_{j+1}, \alpha_j, \ldots, \alpha_n) \qquad (۲-۳)$$

توجه کنید که در واقع β جایگشتی از α می باشد . از آنجا که f متقارن است ، داریم :

$$f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{j+1}, x_j \ldots, x_n) \qquad (۲-۴)$$

بنابراین $\acute{\gamma}$ ای متعلق به K چنان موجود است که $\acute{\gamma} X^{\beta}$ متعلق به $T(f)$ می باشد لذا داریم :

(۲-۵)

$$\acute{\gamma} X^{\beta} \le \gamma X^{\alpha} = Lt(f)$$

بنابراین $X^{\beta} <_{lex} X^{\alpha}$ که این یک تناقض است، زیرا با توجه به تعریف β و ترتیب در نظر گرفته شده داریم $X^{\alpha} <_{lex} X^{\beta}$. لذا فرض خلف باطل است و داریم $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_n$.

قرار دهید $g_1 = {\delta_1}^{\alpha_1-\alpha_2} \dots {\delta_{n-1}}^{\alpha_{n-1}-\alpha_n} {\delta_n}^{\alpha_n}$. با توجه به آنچه در فوق گفته شد توانها نامنفی هستند و داریم $g_1 \in T^n$. لذا :

$$Ltg_1 = Lt(\delta_1)^{\alpha_1-\alpha_2} \dots Lt(\delta_{n-1})^{\alpha_{n-1}-\alpha_n} Lt(\delta_n)^{\alpha_n} \qquad (۲-۶)$$

بنابراین

(۲-۷)

$$Ltg_1 = {x_1}^{\alpha_1-\alpha_2} \dots (x_1 x_2 \dots x_{n-1})^{\alpha_{n-1}-\alpha_n} {x_n}^{\alpha_n} = X^{\alpha}$$

قرار می دهیم : $f_2 = f - \gamma g_1$ که در آن f_2 چند جمله ای متقارن است. (f و g_1 متقارن هستند) .

اگر $f_2 = 0$ باشد که حکم ثابت می شود. ($f = \gamma g_1$ و g_1 چند جمله ای از چند جمله ایهای متقارن مقدماتی می باشد) در غیر اینصورت داریم $Lt(f_2) < Lt(f)$. با تکرار فرآیند روی f_2 تک جمله ای g_2 از چند جمله ایهای متقارن مقدماتی و γ_2 ای متعلق به K مو جودند که :

$$Lt(f_2) = \gamma_2 Lt(g_2) \qquad (۲-۸)$$

قرار می دهیم :

$$f_3 = f_2 - \gamma_2 g_2 = f - \gamma g_1 - \gamma_2 g_2 \qquad (۲-۹)$$

$Lt(f_3) < Lt(f_2)$. که در این صورت حکم ثابت می شود و یا $f_3 = 0$ داریم یا

از خوش ترتیبی ترتیب گفته شده نتیجه می شود بعد از حداکثر s بار تک جمله ایهای $g_s, \dots, g_1$ از چند جمله ایهای متقارن مقدماتی δ_1 و ... و δ_n و ضرائب γ_1 و ... و γ_s از K موجودند که :

$$f = \gamma_1 g_1 + \dots + \gamma_s g_s \qquad (۲-۱۰)$$

اثبات منحصربفردی قضیه اساسی چند جمله ایهای متقارن :

فرض کنید g_2, g_1 متعلق به $k[y_1, y_2, \dots, y_n]$ موجود باشند که:

$$g_1(\delta_1,\dots,\delta_n) = g_2(\delta_1,\dots,\delta_n) \in k[x_1,x_2,\dots,x_n] \qquad (۲-۱۱)$$

نشان می دهیم $g_1 = g_2$. قرار می دهیم $g = g_1 - g_2$. اگر $g \neq 0$ ، قرار می دهیم :

$$Lt(g) = \gamma {y_1}^{\beta_1} \dots {y_n}^{\beta_n} \qquad (۲-۱۲)$$

در این صورت داریم :

$$Lt\big(g(\delta_1,\dots,\delta_n)\big) = Lt\big({\delta_1}^{\beta_1},\dots,{\delta_n}^{\beta_n}\big) = {x_1}^{\beta_1}\dots(x_1\cdots x_n)^{\beta_n}$$
$$= {x_1}^{\beta_1+\cdots+\beta_n}\dots{x_n}^{\beta_n} \qquad (۲-۱۳)$$

اما برای هر $(\beta_1,\dots,\beta_n)(\gamma_1,\dots,\gamma_n) = \gamma \neq \beta = (\beta_1$, … , داریم :

$${x_1}^{\beta_1+\cdots+\beta_n}\dots{x_n}^{\beta_n} \neq {x_1}^{\gamma_1+\cdots+\gamma_n}\dots{x_n}^{\gamma_n} \quad (1) \qquad (۲-۱۴)$$

اما $g = g_1 - g_2$ بنابراین $g(\delta_1,\dots,\delta_n) = 0$ ، لذا بایستی $\gamma{\delta_1}^{\beta_1},\dots,{\delta_n}^{\beta_n}$ با ترم دیگری از g حذف شود .که این با توجه به (۲-۱۴) شدنی نیست و لذا $g = 0$ در نتیجه $g_1 = g_2$ و بدین ترتیب حکم ثابت می شود .

چند جمله ای $f = x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3$ متعلق به $k[x,y,z]$ یک چند جمله ای متقارن می باشد، می خواهیم آن را به صورت یک چند جمله ای از چند جمله ایهای متقارن مقدماتی بنویسیم. بدین منظور ترتیب قاموسی با شرط $z < y < x$ را در نظر می گیریم. داریم :

$$g_1 = {\delta_1}^{3-1}\,{\delta_2}^{1-0}{\delta_3}^{0} = {\delta_1}^{2}\delta_2 \qquad (۲-۱۵)$$

که در آن

$$\delta_1 = x + y + z$$
$$\delta_2 = xy + yz + xz$$
$$\delta_3 = xyz$$

(۲-۱۶)

بنا براین داریم :

$$g_1 = (x^2 + y^2 + z^2 + 2xy + 2xz + 2yz)(xy + yz + xz)$$

$$g_1 = x^3y + x^3z + xy^3 + y^3z + xz^3 + yz^3 + 5x^2yz + 5xy^2z + 5xyz^2$$
$$+2x^2y^2 + 2x^2z^2 + 2y^2z^2$$
$$f_1 = f - g_1 = -5(x^2yz + xy^2z + xyz^2) - 2(x^2y^2 + x^2z^2 + y^2 \qquad (۲-۱۷))$$

$$g_2 = -2{\delta_1}^{2-2}\,{\delta_2}^{2-0}{\delta_3}^0 = -2{\delta_2}^2$$

$$f_2 = f_1 - g_2 = -(x^2yz + xy^2z + xyz^2) \qquad (۲-۱۸)$$

$$g_3 = -{\delta_1}^{2-1}\,{\delta_2}^{1-1}{\delta_3}^1 = -2\delta_1\delta_3$$

$$g_3 = -(x^2yz + xy^2z + xyz^2)$$

$$f_2 - g_3 = 0 \qquad (۲-۱۹)$$

از روابط (۲-۱۷) و(۲-۱۸)و(۲-۱۹) داریم :

$$f_2 - g_3 = f - g_1 - g_2 - g_3 = {\delta_1}^2\delta_2 + 2{\delta_2}^2 + \delta_1\delta_3 = 0$$

$$f = {\delta_1}^2\delta_2 + 2{\delta_2}^2 + \delta_1\delta_3 \qquad (۲-۲۰)$$

لذا با قرار دادن $g = {y_1}^2y_2 + 2{y_2}^2 + y_1y_3$ داریم :

$$f = g(\delta_1, \delta_2, \delta_3) \qquad (۲-۲۱)$$

الگوریتمی برای تبدیل یک چند جمله ای متقارن به چندجمله ایهای متقارن مقدماتی در [3] ارائه شده است .

چند جمله ای f متعلق به $k[x_1, x_2, \ldots, x_n]$ را یک چند جمله ای همگن از درجه ی d نامیم، هرگاه برای هـر t متعلق به مجموعه ترمهای f داشته باشیم :

$$\deg(t) = d \qquad (۲-۲۲)$$

فرض کنید f متعلق به $k[x_1, x_2, \ldots, x_n]$ و f_i ها مو لفه ها ی همگن f باشند و $f = \sum_{i=1}^{s} f_i$ در این صورت f متقارن است اگر وتنها اگر برای هر $1 \le i \le s$، f_i ها متقارن باشند .

فرض کنید برای هر $1 \le i \le s$، f_i ها متقارن باشند، در این صورت $\sum_{i=1}^{s} f_i$ نیز متقارن خواهد بـود، بنـابراین f متقارن است. با لعکس فرض کنید f متقارن است، نشان می- دهیم برای هر $1 \le i \le s$ ، f_i ها متقارن هسـتند .

بدین منظور فرض کنید i ثابت باشد و $(x_{j_1}, \dots, x_{j_n})$ جایگشتی از $(x_1, \dots, x_n)$ باشد نشان می دهیم برای هـر $1 \leq i \leq s$ داریم :

$$f_i(x_{j_1}, \dots, x_{j_n}) = f_i(x_1, \dots, x_n) \qquad (۲-۲۳)$$

اما از آنجا که f متقارن است ، داریم :

$$f(x_{j_1}, \dots, x_{j_n}) = f(x_1, \dots, x_n) \qquad (۲-۲۴)$$

لذا :

$$\sum_{t=1}^{s} f_t \quad (x_{j_1}, \dots, x_{j_n}) = \sum_{t=1}^{s} f_t\,(x_1, \dots, x_n) \qquad (۲-۲۵)$$

از تساوی فوق نتیجه می گیریم که بایستی مولفه های نظیر به نظیر باهم برابر باشند، بنابراین برای هـر $1 \leq i \leq s$ داریم : $f_i(x_{j_1}, \dots, x_{j_n}) = f_i(x_1, \dots, x_n)$ و بدین ترتیب حکم ثابت می شود.

نمادگذاری: در $k[x_1, x_2, \dots, x_n]$ برای هر t متعلق به مجموعه ی اعداد طبیعی تعریف می کنیم :

$$s_t = x_1^t + \cdots + x_n^t \qquad (۲-۲۶)$$

فرض کنید K میدانی با مشخصه ی صفر باشد و $f \in k[x_1, x_2, \dots, x_n]$ متقارن باشد، دراین صـورت چندجملـه ای g متعلق به $k[y_1, y_2, \dots, y_n]$ موجوداست بطوری که

$$f = g(s_1 \text{ و } \dots \text{ و } s_n) \qquad (۲-۲۷)$$

بدون کاستن از کلیت مسئله می توان فرض کرد f یک چند جمله ای متقارن مقـدماتی اسـت.اما بنـا بـه اتحـاد نیوتن می توان نشان داد برای هر $1 \leq k \leq n$ داریم:

$$s_k - \delta_1 s_{k-1} + \cdots + (-1)^i \delta_i s_{k-1} + \cdots + (-1)^{k-1} \delta_{k-1} s_1 + (-1)^k \delta_k k = 0 \qquad (۲-۲۸)$$

اثبات را با استقرا ء روی k ادامه می دهیم. برای $k = 1$ داریم :

$$s_1 = x_1 + \cdots + x_n = \delta_1 \qquad (۲-۲۹)$$

بنابراین با قرار دادن $g\left(y_1 \text{ و } \dots \text{ و } y_n\right) = y_1$ حکم ثابت می شود .

فرض استقراء : فرض کنید برای هر $1 \leq i \leq k-1$ ، g_i ای متعلق به $k[y_1, y_2, \dots, y_n]$ چنان موجود است که :

$$\delta_i = g_i(s_1 \text{ و } \dots \text{ و } s_n)$$

در این صورت با توجه رابطه ی (۲-۲۸) داریم :

$$\delta_k = \frac{(-1)^{k+1}}{k}(s_k - \cdots + (-1)^i \delta_i s_{k-1} + \cdots + (-1)^{k-1}\delta_{k-1}s_1) \qquad (۲-۳۰)$$

بنا براین با توجه به فرض استقرا ء حکم ثابت می شود

مجموعه تمام ماتریس های معکوس پذیر $n \times n$ با درایه های در میدان k را با نماد $GL(n,k)$ نمایش می دهیم.

$GL(n,k)$ یک گروه غیرآبلی است .

هر زیر مجموعه ی ناتهی متناهی از $GL(n,k)$ که تحت عمل ضرب بسته باشد، یک گروه ماتریسی متناهی نامیده می شود .

اگر A عضوی از $GL(n,k)$ و برای عضوی مانند m متعلق به مجموعه ی اعداد طبیعی داشته باشیم $A^m = I$ و m کوچکترین عدد با این خاصیت باشد، آنگاه :

$$c_m = \{I_n, A, A^2, \dots, A^{m-1}\} \qquad (۲-۳۱)$$

یک گروه ماتریسی متناهی است .

فرض کنید $G = \{M_\delta \in GL(n,k) \mid \text{ستون } \delta(i) \text{ ام } M \text{ برابر با ستون } i \text{ ام } I_n \text{ باشد}\}$ در این صورت G یک گروه ماتریسی متناهی می باشد .

قرار می دهیم :

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \qquad (۲-۳۲)$$

فرض کنید H زیر مجموعه ای ازگروه ماتریسی $G \subseteq GL(n,k)$ باشد، چند جمله ای f متعلق به R را یک چندجمله ای پایا تحت H نامیم هرگاه برای هر A متعلق به H داشته باشیم:

$$f(AX) = f(X) \qquad (۲-۳۳)$$

مجموعه ی تمام چندجمله ایهای پایا تحت G را با نماد R^G نمایش می دهیم .

R^G یک K- جبر است.

K یک میدان است بنابراین R^G یک K– مدول یکانی می باشد و برای هر a, b متعلق به R^G وهر $k \in K$ داریم

$$k(ab) = (ka)(b) = a(kb) \qquad (۲-۳۴)$$

لذا R^G یک K- جبر است و در نتیجه یک حلقه است.

فرض کنید H مولدی برای گروه ماتریسی $G \subseteq GL(n,k)$ و f چند جمله ای متعلق به $k[x_1, x_2, \dots, x_n]$ باشند، در اینصورت f تحت G پایا ست اگر و تنها اگر f تحت H پایا باشد.

نشان می دهیم هرگاه $A_1, \dots, A_n$ متعلق به G چنان موجود باشند که $G = \{B_1 \dots B_s | B_i \in \{A_1, \dots, A_n\}, 1 \le i \le s\}$ در اینصورت f تحت G پایا ست اگرو تنها اگر

$$f(X) = f(A_1X) = \cdots = f(A_nX) \qquad (۲-۳۵)$$

ابتدا فرض می کنیم f تحت G پایا ست، در اینصورت از آنجا که $A_1, \dots, A_n$ متعلق به G هستند داریم:

$$\forall\, 1 \le i \le s \;;\; f(A_iX) = f(X) \qquad (۲-۳۶)$$

بالعکس به استقراء روی s نشان می دهیم هرگاه $f(X) = f(B_1X) = \cdots = f(B_sX)$ در اینصورت :

$$f(B_1B_2 \dots B_sX) = f(X) \qquad (۲-۳۷)$$

برای $s = 1$ حکم برقرار است زیرا داریم :

$$f(X) = f(B_1X) \qquad (۲-۳۸)$$

فرض می کنیم حکم برای هر حاصل ضرب کمتر از $s \le 2$برقرار باشد، داریم:

(۲-۳۹)

$$f(B_1B_2.\dots.B_sX) = f(B_1B_2.\dots.B_{s-1}B_sX)$$

بنا به فرض استقراء f تحت $B_1B_2.\dots.B_{s-1}$ پایا ست، لذا تساوی فوق را بصورت زیر داریم:

$$f(B_1B_2.\dots.B_sX) = f(B_1B_2.\dots.B_{s-1}B_sX) = f(X) \qquad (۲-۴۰)$$

حال فرض کنید $A \in G$، لذا $B_1B_2.\dots.B_s$ هائی در $\{A_1, \dots, A_n\}$ چنان موجودند که :

$$A = B_1B_2.\dots.B_s \qquad (۲-۴۱)$$

اما f تحت هر یک از B_i ها پایا ست، لذا بنا بر آنچه اثبات شد f تحت حاصل ضرب B_i ها پایا است، بنابراین f تحت هر $A \in G$ پایا ست لذا f تحت G پایا ست و حکم ثابت می شود.

فرض کنید G یک گروه ماتریسی تولید شده توسط $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ باشد، دراینصورت :

الف :اگر $f = x_1^2 + x_2^2$ عضوی در حلقه $\mathbb{Q}[x_1, x_2]$ باشد ، آنگاه f تحت G پایاست، کافی است نشان دهیم :

$$f(AX) = f(X) \qquad (۲-۴۱)$$

داریم:

$$f\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = f(x_2, -x_1) = x_2^2 + x_1^2 = f(X) \qquad (۲-۴۲)$$

ب: برای $g = x_1x_2$ داریم:

$$g\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = g(x_2, -x_1) = -x_1x_2 \neq g(X) \qquad (۲-۴۳)$$

بنابراین g یک چند جمله ای پایا تحت G نمی باشد .

۲-۲: عملگر رینولد

فرض کنید $G \subseteq GL(n,k)$ یک گروه ماتریسی متناهی و f یک چند جمله ای در $R = k[x_1, x_2, \dots, x_n]$ باشد. عملگر رینولد[۱۱] f تحت G را بصورت زیر تعریف می کنیم:

(۲-۴۴)

$$R_G(f) = \frac{1}{|G|}\sum_{A\in G} f(AX)$$

عملگر رینولد تحت گروه ماتریسی $G \subseteq GL(n,k)$ ، یک تابع به صورت

$$\begin{aligned} \boldsymbol{R}&: \mathrm{R} \to \mathrm{R}^{\mathrm{G}} \\ & f \to R_G(f) \end{aligned}$$

با خواص زیر تعریف می کند:

الف: عملگر $\boldsymbol{R}$ ، k - خطی است.

ب:اگر f متعلق به R^{G} باشد، آنگاه $R_G(f) = f$.

ابتدا نشان می دهیم $\boldsymbol{R}$ یک تابع است، یعنی اگر f متعلق به R باشد آنگاه $R_G(f)$ متعلق به R^{G} می باشد.

بدین منظور نشان می دهیم به ازای هر C متعلق به G ، $R_G(f)(X) = R_G(f)(CX)$ داریم:

(۲-۴۵)

$$R_G(f)(CX) = \frac{1}{|G|}\sum_{A\in G} f(A.CX)$$

قرار می دهیم $B = A.C$ و از آنجا که G یک گروه ماتریسی متناهی است داریم $B \in G$ ، بنابراین:

(۲-۴۶)

$$R_G(f)(CX) = \frac{1}{|G|}\sum_{A\in G} f(A.CX) = \frac{1}{|G|}\sum_{B\in G} f(BX) = R_G(f)(X)$$

لذا $R_G(f)$ متعلق به R^{G} می باشد.

۱-Reynold

الف: فرض کنید f و g متعلق به R باشد و عضوی از K باشد، در اینصورت داریم :

$$\boldsymbol{R}(f+\alpha g)=\frac{1}{|G|}\sum_{A\in G}(f+\alpha g)(AX)=\frac{1}{|G|}\sum_{A\in G}f(AX)+\frac{\alpha}{|G|}\sum_{A\in G}g(AX) \qquad (۲-۴۷)$$

بنابراین با توجه به تساوی بالا داریم :

$$\boldsymbol{R}(f+\alpha g)=\boldsymbol{R}(f)+\alpha\boldsymbol{R}(g) \qquad (۲-۴۸)$$

لذا عملگر $\boldsymbol{R}$، $\mathbf{k}$ - خطی است.

ب : فرض کنید f متعلق به R^{G} باشد، نشان می دهیم :

$$R_G(f)(X)=f(X) \qquad (۲-۴۹)$$

داریم :

$$R_G(f)(X)=\frac{1}{|G|}\sum_{A\in G}f(AX) \qquad (۲-۵۰)$$

از آنجا که f متعلق به R^{G} می باشد، بنابراین f تحت G پایا ست و لذا برای هر A متعلق به G داریم :

$$f(AX)=f(X) \qquad (۲-۵۱)$$

$$R_G(f)(X)=\frac{1}{|G|}\sum_{A\in G}f(AX)=\frac{1}{|G|}\sum_{A\in G}f(X)=f(X) \qquad (۲-۵۲)$$

بدین ترتیب حکم ثابت می شود.

فرض کنید $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ و $c_4=<A>$ یک گروه ماتریسی متناهی از $GL(2,k)$ باشد. در این صورت داریم :

$$c_4=\{I,A,A^2,A^3\} \qquad (۲-۵۳)$$

داریم :

$$k[x,y]^{c_4} = \{ f \in k[x,y] | f(X) = f(AX) \} = \{ f \in k[x,y] | f(x,y) = f(-y,x) \} \qquad (۲-۵۴)$$

اما

$$R_G\big(f(x,y)\big) = \frac{1}{|c_4|}\sum_{B \in c_4} f(BX) = \frac{1}{4}\big(f(x,y) + f(-x,y) + f(-x,-y) + f(y,-x)\big)$$

$$(۲-۵۵)$$

در این صورت داریم :

$$R_G(x^2)(x,y) = \frac{1}{4}(x^2 + (-y)^2 + (-x)^2 + y^2) = \frac{1}{2}\,(x^2 + y^2) \qquad (۲-۵۶)$$

به همین ترتیب نشان می دهیم که :

$$R_G(xy)(x,y) = \frac{1}{4}(xy + (-yx) + xy + (-yx)) = 0$$
$$R_G(x^3y)(x,y) = \frac{1}{4}(x^3y + (-y^3x) + x^3y + (-y^3x)) = \frac{1}{2}(x^3y + (-y^3x))$$
$$R_G(x^2y^2)(x,y) = \frac{1}{4}(x^2y^2 + (y^2x^2) + x^2y^2 + y^2x^2) = x^2y^2$$

$$(۲-۵۷)$$

با توجه به مطالب گفته شده به دنبال پیدا کردن راهی برای محاسبه ی $k[x,y]^{c_4}$ هستیم..

فرض کنید $X^\alpha = x_1^{\alpha_1}.\ \dots\ .x_n^{\alpha_n}$ و G یک گروه ماتریسی متناهی در $GL(n,k)$ باشد، در این صورت :

$\mathrm{R}(\mathrm{X}^\alpha)$ یک چند جمله ای همگن از درجه ی $|\alpha|$ در $k[x_1, x_2, \dots, x_n]^G$ می باشد.

اولاً توجه کنید که برای هر $A \in G$ داریم :

$$AX = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} A_1X \\ \vdots \\ A_nX \end{bmatrix} \qquad (۲-۵۸)$$

که در آن A_i ها سطر های ماتریس A می باشند .

ثانیاً داریم :

$$(2)R_G(\mathrm{X}^\alpha) = \frac{1}{|G|}\sum_{A \in G}(AX)^\alpha = \frac{1}{|G|}\sum (A_1X)^{\alpha_1}\ \dots.\ (A_nX)^{\alpha_n} \qquad (۲-۵۹)$$

با توجه به روابط(۲-۵۸)و(۲-۵۹)داریم :

$$R_G(\mathrm{X}^\alpha) = \frac{1}{|G|}\sum_{A\in G}(a_{11}x_1 + \cdots + a_{1n}x_n)^{\alpha_1}.\ldots.(a_{n1}x_1 + \cdots + a_{nn}x_n)^{\alpha_n} \qquad (۲-۶۰)$$

با توجه به تساوی بالا $(a_{11}x_1 + \cdots + a_{1n}x_n)^{\alpha_1}$ و ... و $(a_{n1}x_1 + \cdots + a_{nn}x_n)^{\alpha_n}$ چند جمله ای های همگن از درجه ی به ترتیب α_1 و . . . و α_n می باشند، بنابراین $R_G(\mathrm{X}^\alpha)$ یک چند جمله ای همگن از درجه ی $|\alpha| = \alpha_1 + \cdots + \alpha_n$ می باشد و بنا به قسمت ب $R_G(\mathrm{X}^\alpha)$ متعلق به $k[x_1, x_2, \ldots, x_n]^G$ می باشد.

قضیه نوتر

فرض کنید $G \subseteq GL(n,k)$، یک گروه ماتریسی متناهی باشد . در این صورت $k[x_1, x_2, \ldots, x_n]^G$ **توسط تعدادی** متناهی چند جمله ای همگن پایا تحت G تولید می شود. به عبارتی دقیق تر

$$k[x_1, x_2, \ldots, x_n]^G = k[\ R_G(\mathrm{X}^\alpha)\ \mid\ |\alpha| \leq |G\ |\ \ ]$$

(۲-۶۱)

فرض کنید f عضوی از $k[x_1, x_2, \ldots, x_n]$ باشد، در این صورت :

$$f = \sum_{\alpha\in\beta} \mathrm{a}_\alpha\, \mathrm{X}^\alpha$$

(۲-۶۲)

که در آن β زیر مجموعه ای متناهی از $\mathbb{Z}^n_{\geq 0}$ است. لذا :

$$R_G(f) = R_G\left(\sum_{\alpha\in\beta} \mathrm{a}_\alpha\, \mathrm{X}^\alpha\right) = \sum_{\alpha\in\beta} \mathrm{a}_\alpha\ R_G(\mathrm{X}^\alpha)$$

(۲-۶۳)

نشان می دهیم سمت راست تساوی بالا چند جمله ای از $R_G(\mathrm{X}^\alpha)$ برای $|\alpha| \leq |G\ |$ می باشد ، بدین منظور ابتدا ملاحظه می شود که :

$$(z_1 + \cdots + z_n)^k = \sum_{|\alpha|=k} \lambda_\alpha\ z^\alpha$$

(۲-۶۴)

حال n متغیر جدید u_1 و ... و u_n را در نظر بگیرید و برای $A \in G$ و $k \in \mathbb{N}$ دلخواه با توجه به رابطه ی بالا داریم

$$u_A^k = (u_1A_1X + \cdots + u_nA_nX)^k = \sum_{|\alpha|=k} \lambda_\alpha (u_1A_1X)^{\alpha_1} \cdots (u_nA_nX)^{\alpha_n} = \sum_{|\alpha|=k} \lambda_\alpha \, u^\alpha (AX)^\alpha$$

(۲-۶۵)

که در آن $|\alpha| = \alpha_1 + \cdots + \alpha_n$ و A_i سطر های ماتریس A می باشند . با ثابت گرفتن k و تغییر A در G قرار می دهیم:

$$S_k = \sum_{A\in G}(u_1A_1X + \cdots + u_nA_nX)^k = \sum_{A\in G}\sum_{|\alpha|=k} \lambda_\alpha \, u^\alpha (AX)^\alpha = \sum_{|\alpha|=k}(\frac{1}{|G|}\sum_{A\in G} (AX)^\alpha)|G|\lambda_\alpha u^\alpha$$

(۲-۶۶)

با در نظر گرفتن اینکه S_k ، برحسب A های مختلف اندیس گذاری می شود، S_k را می توان به صورت یک چند جمله ای از S_i ها نوشت که تعداد شان متناهی وبرابر $|G|$ می باشد . به عبارت دقیق تر h ای متعلق به $k[y_1, y_2, \ldots, y_{|G|}]$ چنان موجود است که :

$$s_k = h(s_1, \ldots, s_{|G|}) \qquad \textbf{(۲-۶۷)}$$

با توجه به روابط **(۲-۶۶)** و **(۲-۶۷)** داریم :

$$s_k = h(\sum_{|\alpha|=1}|G|\,\lambda_\alpha u^\alpha R_G(X^\alpha), \ldots, \sum_{|\alpha|=|G|}|G|\,\lambda_\alpha u^\alpha R_G(X^\alpha)) \qquad \textbf{(۲-۶۸)}$$

اما با توجه به روابط **(۲-۶۶)** و**(۲-۶۸)**ضرائب دو طرف برحسب u^α با هم برابرند، یعنی برای α داریم:

$|G|\lambda_\alpha u^\alpha R_G(X^\alpha)$ = چند جمله ای برحسب $\{R_G(X^\alpha) \mid |\alpha| \le |G|\}$

بنابراین θ ای متعلق به $k[y_1, y_2, \ldots, y_n]$ چنان موجود است که :

$$|G|\lambda_\alpha u^\alpha R_G(X^\alpha) = \theta(R_G(X), \ldots, R_G(X^{|G|})) \qquad \textbf{(۲-۶۹)}$$

با قرار دادن $b_\alpha = |G|\lambda_\alpha$ ، $(b_\alpha \ge 0)$، داریم :

$$R_G(X^\alpha) = \frac{1}{b_\alpha}\ \theta(R_G(X), \dots, R_G(X^{|G|})) \qquad (۲-۷۰)$$

که در آن $|\alpha| \leq |G|$. بدین ترتیب حکم ثابت می شود .

اکنون با توجه به قضایای گفته شده می توان $k[x_1, x_2, \dots, x_n]^G$ را محاسبه کرد. با توجه به قضیه نوتر داریم :

$$k[x,y]^{c_4} = k[\ R_G(x^i y^j)|\ \ i+j \leq 4\ ] \qquad (۲-۷۱)$$

بنا براین :

$$k[x,y]^{c_4} = k[R_G(X), R_G(y), R_G(x^2), R_G(x^3), R_G(x^4), R_G(xy), R_G(x^2y),$$
$$R_G(xy^2), R_G(x^2y^2), R_G(y^2), R_G(y^3), R_G(x^3y)] \qquad (۲-۷۲)$$

$$k[x,y]^{c_4} = k[x^2+y^2, x^2y^2, x^3y - y^3x, x^4+y^4] \qquad (۲-۷۳)$$

با توجه به اینکه $x^4 + y^4 = (x^2+y^2)^2 - \frac{1}{2}x^2y^2$ داریم :

$$k[x,y]^{c_4} = k[x^2+y^2, x^2y^2, x^3y - y^3x] \qquad (۲-۷۴)$$

از این پس برای ساده نویسی از نماد $R(f)$ به جای $R_G(f)$ استفاده می کنیم .

فصل سوم

پایه ساگبی و ساگبی گروبنردرحلقه های پایا

دراین فصل ابتدا به تعریف چند مفهوم خاص از حلقه های پایا می پردازیم و سپس با یاد آوری تعـاریفی از پایـه ساگبی[۱۲] وطرح قضایای مربوط به آن، پایه ی ساگبی گروبنر[۱۳] را معرفی کرده و به بیان و اثبات قضایای مرتبط با آن خواهیم پرداخت .

۳-۱: تک جمله ایهای ابتدائی

برای هر مجموعه ی B از چند جمله ایها، مجموعه ی تمام جملات پیشروی B را بـا $LM(B)$ ومجموعـه ی تمـام تـرم هـای پیشـروی B را بـا نمـاد $LT(B)$ نمـایش مـی دهـیم، بـه عبـارتی $LM(B) = \{Lm(p)|p \in B\}$ و $LT(B) = \{Lt(p)|p \in B\}$.

۱-Initial
۲-SubAlgebra Analog Of Gröebner Basis For Ideals
۳-Sugbi Gröebner Basis

هر عضو $LM(\mathrm{R}^{\mathrm{G}})$ را یک تک جمله ای ابتدائی[۱۴] نامیم. به عبارتی تک جمله ای m را یک تک جمله ای ابتـدائی نامیم هرگاه چند جمله ای مانند f از R^{G}، چنان موجود باشد که جمله پیشروی f برابر m است .

اگر $G = S_3$ که روی سه متغیر $x_3 < x_2 < x_1$ عمل می کند با در نظر گرفتن ترتیب لغـت نامـه ای تـک جمله ای های x_1 , x_1x_2 ,$x_1x_2x_3$، تک جمله ای های ابتدائی هستند زیرا

$$f_1 = x_1 + x_2 + x_3 \in R^{S_3} \qquad lm(f_1) = x_1$$
$$f_2 = x_1x_2 + x_1x_3 + x_2x_3 \in R^{S_3} \qquad lm(f_2) = x_1x_2$$
$$f_3 = x_1x_2x_3 \in R^{S_3} \qquad lm(f_3) = x_1x_2x_3$$

مجموعه تمام تک جمله ایهای ابتدائی همراه عمل ضرب تشکیل یک تکواره می دهد.

برای هر f و g از $R = k[x_1, x_2, \dots, x_n]$ داریم:

$$Lt(fg) = Lt(f)Lt(g) \qquad (۳-۱)$$

بنابراین مجموعه گفته شده نسبت به ضرب بسته است وهمچنین شرکت پذیر است لذا یک نیم گروه است. علاوه بر این دارای عضو همانی می باشد ودر نتیجه یک تکواره است.

فـرض کنیـد $G \subseteq GL(n,k)$ یـک گـروه ماتریسـی و $R = k[x_1, x_2, \dots, x_n]$ در اینصـورت مجموعـه ی $B = \{R(m_\alpha^*) \mid m_\alpha^* \epsilon LM(R^G)\}$ یک مولد برای K- فضای برداری R^{G} می باشد، به عبارتی

$$\mathrm{R}^{\mathrm{G}} = \{ \sum C_\alpha R(m_\alpha^*) \mid m_\alpha^* \epsilon LM(R^G), C_\alpha \epsilon K \} \qquad (۳-۲)$$

فرض کنید f عضوی از R^{G} باشد ، در این صورت عناصری مانند α_1 و . . . وα_s از K و تـرم هـای f_1 و . . . وf_s از $k[x_1, x_2, \dots, x_n]$ چنان موجودند که :

$$f = \alpha_1 f_1 + \cdots + \alpha_s f_s \qquad (۳-۳)$$

فرض کنید A_1 و . . . و A_m متعلق به G باشند، تعریف می کنیم :

$$B_1 = \{f_1(A_1X), \dots, f_1(A_mX)\} \subseteq \{f_1, \dots, f_s\}$$

$$\vdots$$

$$B_s = \{f_s(A_1X), \dots, f_s(A_mX)\} \subseteq \{f_1, \dots, f_s\}$$

داریم :

$$B_1 \cup \dots \cup B_s = \{f_1, \dots, f_s\} \qquad (۳-۴)$$

ادعا می کنیم برای هر $1 \leq i,j \leq s$، اگر $B_i \cap B_j \neq \emptyset$ آنگاه $B_i = B_j$

فرض می کنیم s ای متعلق به $B_i \cap B_j$ موجود باشند در این صورت از آنجا که s هم متعلق به B_i و هم متعلق به B_j می باشد، k و l ای موجودند که

$$s = f_i(A_kX)$$

$$s = f_j(A_lX) \qquad (۳-۵)$$

بنابراین :

$$f_i(A_kX) = f_j(A_lX) \qquad (۳-۶)$$

که در این صورت :

$$f_i = f_j(A_k{}^{-1}A_lX) \qquad (۳-۷)$$

در نتیجه $B_i \subseteq B_j$ و به همین ترتیب می توان ثابت کرد که $B_j \subseteq B_i$. بنابراین $B_i = B_j$ و لذا $\{B_1, \dots, B_s\}$ افرازی برای $\{f_1, \dots, f_s\}$ می باشد. حال نشان می دهیم برای هر θ_1 و θ_2 متعلق به B_j داریم :

$$coeff(f, \theta_1) = coeff(f, \theta_2) \qquad (۳-۸)$$

از آنجا که θ_1 و θ_2 متعلق به B_j هستند بنابراین k_1 و k_2 ای موجودند که

$$\theta_1 = f_j(A_{k_1}X)$$

$$\theta_2 = f_j(A_{k_2}X) \qquad (۳-۹)$$

می دانیم f پایا ست در نتیجه $f(A_{k_1}X) = f(X) = f(A_{k_2}X)$ و داریم :

$$f = \alpha_1 f_1 + \cdots + \alpha_s f_s$$

$$f(X) = f(A_{k_1}X) = \alpha_1 f_1(A_{k_1}X) + \cdots + \alpha_s f_s(A_{k_1}X)$$

$$f(X) = f(A_{k_2}X) = \alpha_1 f_1(A_{k_2}X) + \cdots + \alpha_s f_s(A_{k_2}X) \qquad (۳-۱۰)$$

از تساوی رابطه های بالابرای هر $1 \le j \le s$ داریم:

$$coeff\left(f, f_j(A_{k_1}X)\right) = coeff\left(f, f_j(A_{k_2}X)\right) \qquad (۳-۱۱)$$

$f_j(A_{k_1}X)$ و $f_j(A_{k_2}X)$ متعلق به B_j هستند بنابراین

$$coeff(f, \theta_1) = coeff(f, \theta_2) \qquad (۳-۱۲)$$

از آنچه در بالا گفته شد ، می توان f را به صورت زیر نوشت:

$$f = \alpha_{11}m_{11} + \cdots + \alpha_{1t_1}m_{1t_1} + \cdots + \alpha_{p1}m_{p1} + \cdots + \alpha_{pt_p}m_{pt_p} \qquad (۳-۱۳)$$

که در آن α_{i1} و . . . و α_{it_i} ها با هم برابرند، با تجدید اندیس گذاری f به صورت زیر نوشته می شود :

$$f = \alpha_1 R(m_{11}) + \cdots + \alpha_p R(m_{p1}) \qquad (۳-۱۴)$$

و بدین ترتیب حکم ثابت می شود.

فرض کنید $G \subseteq GL(n,k)$ یک گروه ماتریسی، $A = (a_{ij})$ متعلق به R^G و f عضوی از $R = k[x_1, x_2, \ldots, x_n]$ باشند، قراردهید:

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

در اینصورت $f(AX) = f(X)$ اگر وتنها اگر

$$f(a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, a_{n1}x_1 + \cdots + a_{nn}x_n) = f(x_1, \ldots, x_n) \qquad (۳-۱۵)$$

بنابراین گاهی اوقات برای سادگی در بیان، ماتریس A را به عنوان یک تبدیل خطی از K^n به K^n در نظر می گیریم ، یعنی:

$$A: K^n \to K^n$$
$$X \to AX \qquad (۳-۱۶)$$

فرض کنید $S_n \subseteq GL(n,k)$ و $\rho \in S_n$ ، قرار می دهیم:

$$A_\rho = \begin{bmatrix} \vdots & 0 & \vdots \\ & \vdots & \\ \vdots & \vdots & \vdots \\ & 1 & \\ \vdots & 0 & \vdots \\ \vdots & \vdots & \vdots \end{bmatrix} \quad \begin{matrix} \\ \\ \\ \\ \\ \rho(i) \end{matrix} \qquad (۳-۱۷)$$

A_ρ ماتریسی $n \times n$ می باشد که ستون $\rho(i)$- ام آن ستون i - ام ماتریس همانی است، در اینصورت داریم:

$$A_\rho X = \begin{bmatrix} x_{\rho(1)} \\ \vdots \\ x_{\rho(n)} \end{bmatrix} \qquad (۳-۱۸)$$

و لذا برای $f \in R = k[x_1, x_2, \ldots, x_n]$ داریم:

$$f(A_\rho X) = f\left(\begin{bmatrix} x_{\rho(1)} \\ \vdots \\ x_{\rho(n)} \end{bmatrix}\right) = f([\rho(X)]^t) \qquad (۳-۱۹)$$

گاهی اوقات برای سادگی در نوشتار $f(A_\rho X)$ و $f(\rho X)$ را یکسان در نظر می گیریم.

فرض کنید $G = S_3 \subseteq GL(3,R)$ و $R = k[x_1,x_2,x_3]$ ، ترتیب LeX را با شرط $x_1 \succ x_2 \succ x_3$ در R در نظر بگیرید ، فرض کنید $f = x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3$ ، در اینصورت f تحت G پایا ست زیرا با توجه به تـذکر۳-۱-۷ برای $G = S_3$ داریم :

$$S_3 = \{\rho_0 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \rho_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \rho_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \mu_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \mu_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \mu_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\}$$

(۳-۲۰)

همچنین $f(\rho_0X) = f(X)$ و $f(\rho_1X) = f(X)$و . . . و $f(\mu_3X) = f(X)$.

از آنجا که f پایا ست،

$$f = R(f) \qquad \textbf{(۳-۲۰)}$$

اما بنا به قسمت (الف) که گفته شد داریم :

$$R(f) = R(x_1^2 + x_2^2 + x_3^2 + x_1x_2x_3) = R(x_1^2) + R(x_2^2) + R(x_3^2) + R(x_1x_2x_3) \qquad \textbf{(۳-۲۱)}$$

از طرفی با توجه به تعریف عملگر رینولد داریم:

$$R(f) = \frac{1}{6}(f(x_1,x_2,x_3) + f(x_3,x_1,x_2) + f(x_2,x_3,x_1) + f(x_1,x_3,x_2) + f(x_3,x_2,x_1) + f(x_2,x_1,x_3))$$

(۳-۲۲)

همچنین:

$$R(x_1^2) = \frac{1}{6}(x_1^2 + x_2^2 + x_3^2 + x_1^2 + x_2^2 + x_3^2) = \frac{1}{3}(x_1^2 + x_2^2 + x_3^2) \qquad \textbf{(۳-۲۳)}$$

و به همین ترتیب ملاحظه می شود که :

$$f = R(f) = 3R(x_1^2) + R(x_1x_2x_3) \qquad \textbf{(۳-۲۴)}$$

x_1^2 و $x_1x_2x_3$ متعلق به $LM(R^G)$ هستند لذا تک جمله ایهای ا بتدا ئی می باشند، بنا بـراین f بصـورت ترکیـب خطی از رینولد تک جمله ایهای ابتدائی نوشته شده است .

۳-۲: پایه ساگبی در R^G

در این بخش تعاریف و خواص مهم پایه ساگبی را یاد آوری می کنیم :

زیر مجموعه ی F از R^G یک پایه ساگبی نامیده می شود، هرگاه ترمهای پیشرو F، تکـواره ضـربی تولیـد شـده توسط ترمهای پیشروی R^G را تولید کند، به عبارتی تکواره تولید شده توسط $LT(F)$ با تکواره تولید شده توسط $Lt(R^G)$ برابر باشد. قابل ذکر است که تکواره تولید شده توسط $Lt(R^G)$ با $Lt(R^G)$ برابر است

اگر F یک پایه ساگبی برای R^G باشد آنگاه F، R^G را به عنوان یک K- جبر تولید می کند .

اولاً زیر جبر تولید شده توسط F مشمول در R^G است.($F \subseteq R^G$ و R^G یک جبراست).

ثانیاً نشان می دهیم همه ی عناصر R^G توسط F تولید می شوند :

فـرض کنیـد f متعلـق بـه R^G و $<$ یـک رابطـه ترتیـب روی تکـواره تولیـد شـده توسـط $X = \{x_1, \dots, x_n\}$ باشد، در اینصورت از آنجا که F یک پایه ساگبی برای R^G است لذا تکواره تولید شده توسط ترم های پیشرو F برابر ترم های پیشروی R^G می باشد، یعنی :

$$< LT(F) > = LT(R^G) \qquad (۳-۲۵)$$

در اینصورت $g_1, \dots, g_s$ ی در F چنان موجودند که :

$$Lm(f) = Lm(g_1. \dots . g_s) \qquad (۳-۲۶)$$

قرار می دهیم :

$$f_1 = f - \mathrm{Lc}(f).g_1. \dots . g_s$$

از آنجاکه f و $g_1, \dots, g_s$ در R^G هستند، لذا f_1 نیز متعلق به R^G می باشد. اما بنا به رابطه ی (۳-۲۶)داریم :

$$Lm(f_1) < Lm(f) \qquad (۳-۲۷)$$

این روش را ادامه می دهیم، داریم :

$$f_2 = f_1 - \mathrm{Lc}(f_1).p_1.\dots.p_s = f - \mathrm{Lc}(f).g_1.\dots.g_s - \mathrm{Lc}(f_1).p_1.\dots.p_s \qquad (۳-۲۸)$$

که در آن $p_1, \dots, p_s$ متعلق به ترم های پیشرو F هستند ودر نتیجه داریم :

$$Lm(f_2) < Lm(f_1) \qquad (۳-۲۹)$$

باتکرار روند فوق داریم:

$$Lm(f) > Lm(f_1) > Lm(f_2) > \cdots \qquad (۳-۳۰)$$

دنباله فوق یک دنباله نزولی است که بنا به خوش ترتیبی رابطه ی ترتیب داده شده متوقف می شود، یعنـی k ی موجود است که :

$$f_k = f - \mathrm{Lc}(f).g_1.\dots.g_s - \mathrm{Lc}(f_1).p_1.\dots.p_s - \dots - \mathrm{Lc}(f_k).z_1.\dots.z_s \qquad (۳-۳۱)$$

نشان می دهیم $f_k = 0$ ، اگر فرض می کنیم چنین نباشد یعنی $f_k \neq 0$، از آنجا که f_k متعلق به R^G است، لـذا جمله پیشرو f_k متعلق به جملات پیشرو R^G می باشد، یعنی:

$$Lm(f_k) \in LM(R^G) \qquad (۳-۳۲)$$

بنا به روندی که گفته شد، داریم :

$$f_{k+1} = f_k - \mathrm{Lc}(f_{k+1}).y_1.\dots.y_l \qquad (۳-۳۳)$$

که درآن y_1 و . . . و y_l متعلق به ترم های پیشروی F هستند. از طرفی

$$Lm(f_{k+1}) < Lm(f_k) \qquad (۳-۳۴)$$

و این با آنچه در مورد توقف زنجیر نزولی گفتیم در تناقض است، لذا فرض خلف باطل است و حکم ثابت می شود.

بنابراین $f_k = 0$ ودر نتیجه داریم :

$$f = \mathrm{Lc}(f).g_1.\dots.g_s - \mathrm{Lc}(f_1).p_1.\dots.p_s - \dots - \mathrm{Lc}(f_k).z_1.\dots.z_s \qquad (۳-۳۵)$$

که در آن g_i ها و p_i ها و . . . و z_i ها متعلق به F هستند ولذا f متعلق به زیر جبر تولید شده توسط F می باشد، بنابراین حکم ثابت می شود

اگر $G = S_3$ که روی سه متغیر $x_3 < x_2 < x_1$ عمل می کند با در نظر گرفتن ترتیب قاموسی مجموعه زیر یک پایه ساگبی برای R^G است.

$$B = \{x_1 + x_2 + x_3 , x_1x_2 + x_1x_3 + x_2x_3 , x_1x_2x_3\} \qquad (۳-۳۶)$$

با فرض $\delta_1 = x_1 + x_2 + x_3$ و $\delta_2 = x_1x_2 + x_1x_3 + x_2x_3$ و $\delta_3 = x_1x_2x_3$ داریم :

$$K[\delta_1 , \delta_2 , \delta_3] = R^{S_3} \qquad (۳-۳۷)$$

حال فرض می کنیم $m \in LM(R^{S_3})$، لذا f ای متعلق به R^{S_3}چنان موجود است که:

$$lm(f) = m \qquad (۳-۸۳)$$

اما چند جمله ای g متعلق به $K[y_1 , y_2 , y_3]$ چنان موجود است که :

$$f = g(\delta_1 , \delta_2 , \delta_3) = \sum_{(\alpha_1,\alpha_2,\alpha_3)\in A} \lambda_{\alpha_1,\alpha_2,\alpha_3} \delta_1^{\alpha_1}\delta_2^{\alpha_2}\delta_3^{\alpha_3} \qquad (۳-۳۹)$$

که در آن $A \subseteq \mathbb{Z}^3_{>0}$.

لذا عضوی مانند $(\alpha_1, \alpha_2, \alpha_3)$ از $\mathbb{Z}^3_{>0}$ چنان موجود است که :

$$m = lm(f) = lm\left(\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\sigma_3^{\alpha_3}\right) = lm(\sigma_1)^{\alpha_1} lm(\sigma_2)^{\alpha_2} lm(\sigma_3)^{\alpha_3} \qquad (۳-۴۰)$$

بنابراین B یک پایه ساگبی برای R^{S_3} است .

تک جمله ای m متعلق به $LM(R^G)$ تحویل نا پذیر است ، هرگاه نتوان آن را به صورت حاصل ضرب دو تک جمله ای غیر بدیهی ابتدائی نوشت .

هر عضو $Lt(R^G)$ را می توان به صورت حاصل ضرب متناهی از تک جمله ایهای ابتدائی تحویل ناپذیر نوشت .

فرض کنید X^{α} عضوی از $Lt(R^{G})$ باشد ، اگر X^{α} تحویل ناپـذیر باشـد کـه چیـزی بـرای اثبـات نـداریم در غیـر اینصورت f_1 و f_2 ای متعلق به R^{G} موجودند که :

$$X^{\alpha} = lt(f_1).lt(f_2) \qquad (۳-۴۱)$$

داریم:

$$\deg(lt(f_1)), \deg(lt(f_1)) < |\alpha| \qquad (۳-۴۲)$$

اگر ترم های پیشروی f_1 و f_2 تحویل ناپذیر باشند که حکم ثابت است در غیر این صورت روند گفته شده را برای ترم های پیشروی f_1 و f_2 ادامه می دهیم. با توجه به اینکه درجه ها نا منفی هستند و بنا به خوش ترتیبی رابطه ی ترتیب گفته شده، پس از تعداد متناهی بار روند فوق متوقف می شود و به یک عامل تحویل ناپـذیر θ_1 بـرای X^{α} می رسیم، یعنی g_1 ی موجود است که :

$$X^{\alpha} = lt(\theta_1).lt(g_1) \quad \text{و} \quad |\alpha| > \deg(lt(g_1)) \qquad (۳-۴۳)$$

با تکرار روند فوق برای ترم پیشروی g_1 به یک عامل تحویل ناپذیر θ_2 از ترم پیشروی g_1 می رسـیم ، بطـوری که g_2 ی موجود است که :

$$lt(g_1) = lt(\theta_2).lt(g_2) \quad \text{و} \quad \deg(lt(g_1)) > \deg(lt(g_2)) \qquad (۳-۴۴)$$

با تکرار روند به همین ترتیب داریم :

$$|\alpha| > \deg(lt(g_1)) > \deg(lt(g_2)) > \cdots \geq 0 \qquad (۳-۴۵)$$

همانطور که گفته شد درجه ها نامنفی هستند و روند فوق متوقف می شود . بنابراین در نهایت X^{α} را مـی تـوان به صورت حاصل ضرب متناهی از تک جمله ایهای ابتدائی تحویل ناپذیر نوشت و بدین ترتیب حکم ثابت می شود

پایه ساگبی F را تقلیل یافته نامیم هرگاه برای هر دو عضو f و g از F هیچ یـک از تـرم هـای g مضـربی از تـک جمله ای پیشروی f نباشد، یعنی :

$$\forall\, t\epsilon\, \mathrm{T(g)} \quad \mathrm{Lt}(f) \nmid t \tag{۳-۴۶}$$

اگر m یک تک جمله ای ابتدا ئی باشد، آنگاه هیچ یک از ترم های $R(m)$ به جز m ابتدائی نیستند.

فرض کنید m_1 یک تک جمله ای ابتدائی در $R(m)$ باشد، بنابراین f ای متعلق بـه R^G چنـان موجـود اسـت کـه $Lm(f) = m_1$، در این صورت از پایا بودن $R(m)$ تحت G نتیجه می شود :

$$T\big(R(m)\big) = T(R(m_1)) \tag{۳-۴۷}$$

لذا $lm\big(R(m)\big) = lm(R(m_1))$ در نتیجه $m = m_1$

زیر مجموعه ی F از R^G یک پایه ساگبی برای R^G است اگر و تنها اگر مجموعه ی ترم های پیشـروی F شـامل همه ی تک جمله ایهای تحویل ناپذیر $LM(R^G)$ باشد.

مجموعه ی همه ی رینولدهای تک جمله ایهای ابتدائی تحویل ناپذیر R^G، یک پایه ساگبی تقلیل یافتـه مینیمـال یکتا برای R^G می باشد .

نشان می دهیم زیر مجموعه ی F از R^G یک پایه ساگبی برای R^G است اگر و تنها اگر به ازای هر X^α تحویـل ناپذیر متعلق به $LM(R^G)$، X^α متعلق به ترم های پیشروی F است .

ابتدا فرض کنید F یک پایه ساگبی برای R^G باشد، بنا به تعریف پایه ساگبی، ترم های پیشروی F، ترم های پیشروی R^G را به عنوان یک تکواره تولید می کند و داریم :

$$X^\alpha \in LM(\ R^G) =< Lt(F) > \tag{۳-۴۸}$$

بنابراین f ی متعلق به R^G چنان موجود است که :

$$X^\alpha = Lm(\ f) \tag{۳-۴۹}$$

لذا f_1 و. . . و f_s هائی متعلق به F چنان موجودند که :

$$X^\alpha = Lm(\ f_1). \ldots . Lm(\ f_s) \tag{۳-۵۰}$$

اما از آنجا که X^{α} تحویل ناپذیر است، لذا باید $s = 1$ و حکم ثابت می شود .

بالعکس : فرض کنید ترم های پیشروی F شامل همه ی تک جمله ایهای تحویل ناپذیر $LM(R^G)$ باشد، نشان می دهیم زیر مجموعه ی F از R^G یک پایه ساگبی برای R^G است :

از آنجا که F زیر مجموعه ی R^G است لذا $Lt(F)$ زیر مجموعه ی $LT(R^G)$ می باشد. بنابراین

$$< Lt(F) > \subseteq LT(R^G) \qquad (۳-۵۱)$$

نشان می دهیم :

$$LT(R^G) \subseteq < Lt(F) > \qquad (۳-۵۲)$$

بدین منظور فرض می کنیم X^{α} متعلق به $LT(R^G)$ باشد، دو حالت در نظر می گیریم:

حالت اول : X^{α} تحویل ناپذیر باشد که در این صورت بنا به فرض ترم های پیشروی F شامل همه ی تک جمله ایهای تحویل ناپذیر $LM(R^G)$ می باشد و لذا X^{α} متعلق به $LT(F)$ است و حکم ثابت می شود .

حالت دوم : X^{α} تحویل ناپذیر نباشد، f_1 و. . . و f_n هائی از R^G چنان موجودند که :

$$X^{\alpha} = Lt(f_1). \dots . Lt(f_s) \qquad (۳-۵۳)$$

که هر یک از $Lt(f_i)$ ها تحویل ناپذیر است. از تساوی فوق داریم :

$$X^{\alpha} < Lt(F) > \qquad (۳-۵۴)$$

بنابراین

$$LT(R^G) \subseteq < Lt(F) > \qquad (۳-۵۵)$$

از رابطه ی (۳-۵۳) و(۳-۵۵)داریم :

$$< Lt(F) > = LT(R^G) \qquad (۳-۵۶)$$

که بنا بر تعریف پایه ساگبی، F یک پایه ساگبی برای R^G است و بدین ترتیب حکم ثابت می شود.

نشان می دهیم $B = \{R(m) \mid \exists\ f \in R^G ; Lm(f) = m, m \text{ تحویلناپذیر}\}$ یک پایه ساگبی مینیمال تقلیل یافته منحصر بفرد می باشد. ابتدا ادعا می کنیم :

$$Lm(R(m)) = m \qquad (۳-۵۷)$$

برای اثبات داریم :

$$\exists\ f \in R^G \quad ; \quad Lm(f) = m \qquad (۳-۵۸)$$

فرض می کنیم s ی متعلق به $LM(R^G)$ موجود باشد بطوری که s تحویل ناپذیر است و

$$Lm(R(m)) = s \qquad (۳-۵۹)$$

از رابطه ی (۳-۵۸) ، با ترتیب دلخواه داریم :

$$T(R(m)) \subseteq T(f) \qquad (۳-۵۹)$$

همچنین :

$$s = Lm(R(m)) \leq Lm(f) = m \qquad (۳-۶۰)$$

از طرفی می دانیم که m متعلق به مجموعه $T(R(m))$ می باشد (m تک جمله ای تحویل ناپذیر است)، بنابراین داریم :

$$m \leq Lm(R(m)) = s \qquad (۳-۶۱)$$

از رابطه های (۳-۶۰) و(۳-۶۱) داریم :

$$m = s$$

بنابراین $Lm(R(m)) = m$

بنابر ادعا مجموعه ی B شامل همه ی تک جمله ایهای تحویل ناپذیر $LM(R^G)$ می باشد، لذا طبق قسمت ا لف B یک پایه ساگبی برای R^G است. حال نشان می دهیم B مینیمال است .

فرض می کنیم B مینیمال نباشد لذا m ای متعلق به $LM(R^G)$ چنان موجود است که$\{R(m)\} - B = B'$ نیـز یک پایه ساگبی برای باشد. اما $R(m) \in R^G$ و لذا بایسـتی چنـد جملـه ای هـای f_1 وf_2 و ... وf_s در B' چنـان موجود باشند که:

$$m = lm(R(m)) = lm(f_1) \dots lm(f_s) \qquad (۳-۶۲)$$

که این متناقض با فرض تحویل ناپذیر بودن $m = lm(R(m))$ است. بنابراین B یک پایه ساگبی مینیمال است . حال در ادامه ی نشان می دهیم که B تقلیل یافته است . فرض می کنیم که اعضای f و g از B چنان موجودند که :

$$f = R(m_1)$$
$$g = R(m_2) \qquad (۳-۶۳)$$

و t ای متعلق به مجموعه ی جملات g چنان موجود است که مضـربی از $Lm(f)$ باشـد، دراین صـورت h ای متعلق به R^G موجود است که $a = Lm(h)$ و $t = am_1$ ، ملاحظه می شود که a و m_1 هر دو ابتـدائی هسـتند بنابراین t نیز ابتدا ئی است بنا بر ادعا ئی که اثبات شد هیچ یـک از تـرم هـای دیگـر $R(m_2)$ ابتـدائی نیسـتند بنابراین $t = m_2$ ، لذا داریم :

$$m_2 = am_1 \qquad (۳-۶۴)$$

از تحویل ناپذیری m_1 و m_2 داریم :

$$m_2 = m_1$$

در نتیجه $f = g$ خواهد بود ، لذا B تقلیل یافته است .

اثبات منحصربفردی:

فرض کنید که B_1 پایه ساگبی تقلیل یا فته دیگری با ضریب پیشروی ۱، برای R^G باشد و عضوی از B_1 مانند f را در نظر بگیرید بطوری که $m = Lm(f)$

از آنجا که $Lm\big(R(m)\big) = m = Lm(f)$ (بنا بر ادعا) لذا

$$T\big(R(m)\big) \subseteq T(f) \qquad (۳-۶۵)$$

بنابراین عناصر f_1 ازR^G و $\alpha \in K$ موجودند که :

$$f = \alpha R(m) + f_1 \qquad (۳-۶۶)$$

حال از آنجا که f_1 عضوی ازR^G است و همچنین B_1 پایه ساگبی تقلیل یا فته برای R^G می باشد لذا عناصر g_1 و. . . و g_n ای از $B_1 - \{f\}$ مو جودند بطوری که :

$$Lm(f_1) = Lm(g_1). \ldots . Lm(g_n) \qquad (۳-۶۷)$$

همچنین داریم:

$$Lm(f_1) = Lm(R(m_1)). \ldots . Lm(R(m_t)) = m_1. \ldots . m_t \qquad (۳-۶۸)$$

m_1 عضوی از ترم های پیشروی R^G است لذا توسط ترم های پیشروی B_1 تولید می شود و از آنجا که m_1 تحویل ناپذیر لذا دقیقاً با یکی از آنها برابر می شود. به عبارت دیگر g_1 ای عضو $B_1 - \{f\}$ موجود است که $m_1 = Lm(g_1)$ بنابراین بنا به آنچه گفته شد از رابطه **(۳-۶۸)**داریم :

$$Lm(f_1) = Lm(g_1). \ldots . m_t \qquad (۳-۶۹)$$

حال از آنجا که

$$Lm(f_1) \in T(f_1) \subseteq T(f) \qquad (۳-۷۰)$$

داریم : ترمی از f_1 و لذا ترمی از f مضربی از یکی از ترم های پیشروی $B_1 - \{f\}$ است که این با تقلیل یافته بودن B_1 در تناقض است. لذا $f_1 = 0$ در نتیجه $f = \alpha R(m)$، بنابراین :

$$B_1 \subseteq B \qquad (۳-۷۱)$$

نشان می دهیم $B \subseteq B_1$ ، عضوی از B مانند $R(m)$ درنظر می گیریم، از آنجا که

$$LT(B) \subseteq LT(B_1) \qquad (۳-۷۲)$$

لذا $m \in LT(B_1)$ ، در نتیجه g_1 ای متعلق به B_1 موجود است که

$$Lm(g_1) = m = Lm(R(m)) \qquad (۳-۷۳)$$

لذا عناصر h_1 از R^G و $\beta \in K$ موجودند که می توان g_1 را به صورت زیر نوشت :

$$g_1 = \beta R(m) + h_1 \qquad (۳-۷۴)$$

همانند آنچه در قسمت قبل اثبات شد می توان ثابت کرد که $h_1 = 0$ و $\beta = 1$ لذا $R(m) \in B_1$ ، بنابراین :

$$B \subseteq B_1 \qquad (۳-۷۵)$$

از روابط (۳-۷۱) و (۳-۷۵) نتیجه می گیریم:

$$B_1 = B$$

بنابراین B منحصر بفرد است .

در گروه بدیهی G، مجموعه عناصر تحویل ناپذیر ابتدائی عبارت است از $B = \{x_1, x_2, \dots, x_n\}$. مجموعه ی B یک پایه ساگبی مینیمال تقلیل یافته منحصر بفرد برای R^G می باشد. زیرا داریم :

$$R(x_1) = x_1 \text{ و } \dots \text{ و } R(x_n) = x_n \qquad (۳-۷۶)$$

x_1 و x_n همه ی تک جمله ایهای تحویل ناپذیر R^G می باشند .

فرض می کنیم $G = S_n$ و ترتیب قاموسی روی تک جمله ای ها باشد. ادعا می کنیم n تک جمله ای $x_1 x_2 \dots x_t$ که $1 \leq t \leq n$ تحویل ناپذیر است .

فرض کنیم $x_1 x_2 \dots x_t$ تحویل پذیر باشد در این صورت افرازی از $\{1,2,\dots,t\}$ مانند $\{i_1, \dots i_m\}$ و $\{j_1, \dots, j_s\}$ موجود است که $x_1 x_2 \dots x_t = x_{i_1} \dots x_{i_m} x_{j_1} \dots x_{j_s}$ واعضای f و g از R^G چنان موجود است که :

$$x_{j_1} \dots x_{j_s} = lm(g) \text{ و } x_{i_1} \dots x_{i_m} = lm(f) \quad (۳-۷۷)$$

بدون کاستن از کلیت می توان فرض کرد $1 \in \{i_1, \dots i_m\}$.اما عضوی از $G = S_n$ مانند σ چنان موجود است که:

$\sigma(x_{j_1} \dots x_{j_s}) = x_1 x_{l_1} \dots x_{l_{s-1}}$ که در آن $\{l_1, \dots, l_{s-1}\}$ زیر مجموعه ای از $\{1,2, \dots, t\}$ می باشد .

حال با توجه به ترتیب قاموسی در نظر گرفته شده داریم :

$$x_{j_1} \dots x_{j_s} < x_1 x_{l_1} \dots x_{l_{s-1}} \quad (۳-۷۸)$$

از طرفی

$$x_{l_1} \dots x_{l_{s-1}} \in T(g) \quad (۳-۷۹)$$

بنابراین از روابط (۳-۷۷)و(۳-۷۸)و(۳-۷۹)تناقض مورد نظر به دست می آید .

همچنین برای هر $1 \le t \le n$ ، تک جمله ای $x_1 x_2 \dots x_t$ یک تک جمله ای ابتدایی است زیرا می توان عناصری مانند δ_1و ... وδ_n از R^G را بصورت زیر معرفی کرد :

$$\delta_1 = x_1 + x_2 + \cdots + x_n = R(x_1)$$
$$\vdots$$
$$\delta_t = \sum_{1 \le i_1 < i_2 < \cdots < i_t \le n} x_{i_1} x_{i_2} \dots x_{i_t} = R(x_1 x_2 \dots x_t)$$
$$\vdots$$
$$\delta_n = x_1 x_2 \dots x_n = R(x_1 x_2 \dots x_n) \quad (۳-۸۰)$$

لذا برای هر $1 \le t \le n$ تک جمله ای $x_1 x_2 \dots x_t$ ابتدایی است بنابراین مجموعه $B = \{\sigma_1, \sigma_t, \dots, \sigma_n\}$ (مجموعه ی چند جمله ای های متقارن مقدماتی) پایه ساگبی مینیمال تقلیل یافته منحصر بفرد برای R^G می باشد .

فرض کنید $G = A_3$ گروه جایگشتی با سه متغیر z, y, x باشد، ادعا می کنیم هر تک جمله ای ابتدائی به شکل $x^s z^{s-1}$ که $s \geq 1$ تحویل ناپذیر است.

فرض کنید که بتوان $x^s z^{s-1}$ را بصورت حاصل ضرب دوتک جمله ای ابتدائی p و q بادرجات کمتر نوشت که در آن با فرض $p = x^h z^{h'}$ داریم $q = x^{s-h} z^{s-1-h'}$.

برای اینکه p و q ابتدائی باشند باید توان x بزرگتر از توان z باشد، یعنی :

$$h > h' \quad \text{و} \quad s - h > s - 1 - h' \qquad (۳-۸۱)$$

لذا $h' + 1 > h > h'$ و این یک تناقض است زیرا h و h' اعداد طبیعی هستند. بنابراین عناصر تحویل ناپذیر $LM(R^{A_3})$ نامتناهی اند و R^{A_3} پایه ساگبی متناهی ندارد.

ملاحظه می شود که علیرغم اینکه مسئله هیلبرت بیان می کند برای هر گروه متناهی G R^G به عنوان یک K - جبر باتولید متناهی است ولی R^G ممکن است پایه ساگبی متناهی نداشته باشد، لذا لزوما هر مولد K - جبر پایه ساگبی نیست .

۳-۳: پایه ساگبی گروبنر در R^G

هدف اولیه ی ما در این بخش تعریف پایه ساگبی گروبنر برای ایده آلهای R^G می باشد، سپس الگوریتمی شبیه الگوریتم بوخبرگر برای حلقه ی R^G ارائه می دهیم، در ادامه فرض می کنیم I ایده آلی همگن از R^G باشد .

زیر مجموعه ی F از ایده آل I یک پایه ساگبی گروبنر برای I نامیده می شود هرگاه مجموعه ی ترم های پیشروی F ، مولدی برای ایده آل $< LT(I) >$ از جبر $< LTR^G >$ باشد .

F را یک پایه ساگبی گروبنر جزئی از درجه حداکثر d نامیم اگر ترم هـای پیشـروی F، مولـدی بـرای ایـده آل $< LT(I_d) >$ باشد که در آن :

$$Lt(I_d) = \{\theta \in LT(I) |\ \deg\theta \leq d\}$$

مجموعه ی $F = \{f_1 , \dots , f_k\}$ را یک پایه ساگبی گروبنر نامیم، هرگاه یک پایه گروبنر برای ایده ال تولید شده توسط F باشد .

یاد آوری می کنیم هر ایده آل از یک حلقه ی چند جمله ایها دارای مولدی متناهی است و از قضایای بـوخبرگر نتیجه می شود که هر ایده آل نسبت به یک ترتیب مفروض دارای یک پایه گروبنر متناهی اسـت . ایـن خاصـیت برای پایه های ساگبی گروبنر در حالت کلی برقرار نیست . بدین دلیل برای محاسبه ی پایه ساگبی گروبنر معمولاً یک درجه ی ماکسیمم مانند D در نظر گرفته وعناصر پایه را تا درجه ی حداکثر D محاسبه می کنیم .

به منظور ارائه الگوریتمی برای محاسبه ی پایه ساگبی گروبنر ابتدا تعاریف مشابه ی آنچه برای محاسـبه ی پایـه گروبنر نیاز داریم مانند تعریف تقلیل یافتن نسبت به یک چند جمله ای و . . . را بیان می کنیم .

فرض کنید p و f و g متعلق به R^G چنان موجود باشند که f و p مخالف صفر هستند وهمچنین فرض کنید P زیرمجموعه ای از R^G باشد .در این صورت :

الف: f را $SG-$ تقلیل یافته به g به پیمانه ی p گوئیم هرگاه t ای متعلق به مجموعـه ی تـرم هـای f و s ای متعلق به LMR^G چنان موجود باشند که :

$$s.LT(p) = t$$

$$g = f - \left(\frac{a}{Lc(p).Lc(R(s))}\right).R(s).p \qquad (۳-۸۲)$$

بطوری که در آن a ضریب t در f و R عملگر رینولد G می باشند .

تعریف فوق را بصورت $f \underset{SG}{\overset{p}{\rightarrow}} g$ نمایش می دهیم.

ب: f را SG – تقلیل یافته به g به پیمانه ی P گوئیم هرگاه f ، SG – تقلیل یافته به g بـه پیمانـه ی p ای متعلق به P باشد. یعنی برای هر p متعلق به P داشته باشیم $f \underset{SG}{\overset{p}{\rightarrow}} g$.با توجه به تعاریف فـوق ، دو تعریـف زیـر را ارائه می دهیم:

f را SG – تقلیل پذیر به پیمانه ی P گوئیم هرگاه g ای متعلق به R^G چنان موجود باشد که f، SG – تقلیـل یافته به g به پیمانه ی P باشد .

g را SG – فرم نرمال f به پیمانه ی P گوئیم هرگاه P پایه ساگبی گروبنر باشد و f ، SG – تقلیل یافته بـه g به پیمانه ی P باشد .

در این قسمت تعریف معادلی برای تقلیل یافتن نسبت به یک پایه ساگبی گروبنر بیـان واثبـات مـی کنـیم .ایـن تعریف در حالتی که مشخصه ی میدان صفر نباشد و امکان تقسیم بر صفر در محاسبه ی عملگـر رینولـد داشـته باشیم مفید است .

تعریف معادل به صورت زیر است :

f را SG – تقلیل یافته به g به پیمانه ی p گوئیم هرگاه m ای متعلق به LMR^G چنان موجود باشند که :

$$g = f - \left(\frac{Lc(f)}{Lc(p)}\right).m^*.p \qquad (۳-۸۳)$$

بطوری که :

$$m^* = \sum_{M\in\{A.m|A\in G\}} M \qquad (۳-۸۴)$$

داریم :

$$m^* = \sum_{A\in G} m(A.X) = \sum_{A\in G} A.m \qquad (۳-۸۵)$$

تساوی فوق از تک جمله ای بودن m نتیجه می شود و همچنین بنا به عملگر رینولد G داریم :

$$\sum_{A\in G} m(A.X) = |G|.R(m) \qquad (۳-۸۶)$$

بنابراین داریم:

$$R(m) = \frac{1}{|G|}\sum_{A\in G} A.m \qquad (۳-۸۷)$$

در نتیجه $Lc\big(R(m)\big) = \frac{1}{|G|}$ خواهد بود.

حال با توجه به تعریف (قسمت ا لف) و آنچه در بالا گفته شد داریم:

$$g = f - \left(\frac{Lc(f)}{Lc(p).\frac{1}{|G|}}\right).R(m).p = f - \left(\frac{Lc(f)}{Lc(p)}\right).|G|R(m).p \qquad (۳-۸۸)$$

و این همان تعریف معادل $g = f - \left(\frac{Lc(f)}{Lc(p)}\right).m^*.p$ را نتیجه می دهد که در آن داریم :

$$m^* = |G|.R(m)$$

فرض کنید I ایده آلی از حلقه ی R^G و F زیر مجموعه ای از I باشد ، در این صورت گزاره های زیر معادل هستند .

ا لف : F پایه ساگبی گروبنر برای I است .

ب : برای هر h متعلق به I ، هر $SG-$فرم نرمال h به پیمانه ی F برابر صفر باشد.

ابتدا فرض می کنیم F پایه ساگبی گروبنر برای I و h عضوی از I باشند،نشان می دهیم هر $SG-$فرم نرمال h به پیمانه ی F برابر صفر است .

فرض کنیدچنین نباشد یعنی g ای مخالف صفر موجود باشد که $SG-$فرم نرمال h به پیمانه ی F برابر g باشد، در این صورت p_1 و . . . و p_l هائی متعلق به F چنان موجودند که :

$$g = h - \left(\frac{a_1}{Lc(p_1).Lc(R(s_1))}\right).R(s_1).p_1 - \cdots - \left(\frac{a_l}{Lc(p_l).Lc(R(s_l))}\right).R(s_l).p_l \qquad (۳-۸۹)$$

که به ازای هر i ، $t_i \in T(h)$ چنان موجود است که $s_i = \frac{t_i}{LT(p_i)}$.

بنا براین $g \in I$، لذا داریم : $Lt(g) \in LT(I)$

از آنجا که F یک پایه ساگبی گروبنر برای I است، لذا ایده آل تولید شده توسط $LT(F)$ در k - جبر $< LT(R^G) >$ می باشد، لذا چند جمله ای مانند p_1 در F و تک جمله ای ابتدائی مانند β در $LT(R^G)$ چنان موجودند که :

$$Lt(g) = Lt(p_1).\beta$$

این نشان می دهد که g نسبت به p_1، $SG-$ تقلیل پذیر است و این با فرض (تعریف $SG-$فرم نرمال) در تناقض است . لذا $g = 0$.

بالعکس : فرض می کنیم برای هر h متعلق به I ، هر $SG-$ فرم نرمال h به پیمانه ی F برابر صفر باشد نشان می دهیم F یک پایه ساگبی گروبنر برای I است، یعنی $LT(F)$ مولدی برای ایده آل تولید شده توسط $LT(I)$ در k - جبر $< LT(R^G) >$ می باشد .

ابتدا نشان می دهیم $LT(I) \subseteq < LT(F) >$ بدین منظور فرض می کنیم h عضوی از I باشد بنا به فرض هر $SG-$ فرم نرمال به پیمانه ی F برابر صفر است لذا f_1 و . . . و f_t هائی متعلق به F و s_1 و . . . و s_t های متعلق به $LM(R^G)$ چنان موجودند که :

$$0 = h - \left(\frac{a_1}{Lc(f_1).Lc(R(s_1))}\right).R(s_1).f_1 - \cdots - \left(\frac{a_t}{Lc(f_t).Lc(R(s_t))}\right).R(s_t).f_t \qquad (۳-۹۰)$$

که در آن به ازای هر i ، t_i ای متعلق به$T(h)$ چنان موجود است که $s_i = \frac{t_i}{LT(f_i)}$ و a_i ضریب t_i در f_i می باشد . داریم :

$$h = \left(\frac{a_1}{Lc(f_1).Lc(R(s_1))}\right).R(s_1).f_1 - \cdots - \left(\frac{a_t}{Lc(f_t).Lc(R(s_t))}\right).R(s_t).f_t \qquad (۳-۹۱)$$

لذا $Lt(h) \subseteq < LT(F) >$ بنابراین داریم :

$$< LT(I) > \subseteq < LT(F) > \qquad (۳-۹۲)$$

ازطرفی $F \subseteq I$، لذا:

$$< LT(F) > \subseteq < LT(I) > \qquad (۳-۹۳)$$

بنا براین از رابطه های (۳-۹۲) و (۳-۹۳) داریم :

$$< LT(I) > = < LT(F) >$$

لذا F یک پایه ساگبی گروبنر برای I است.

نتیجه: هر پایه ساگبی گروبنر برای I، I را به عنوان یک ایده آل از R^G تولید می کند .

فرض کنید F یک پایه ساگبی گروبنر برای I باشد، نشان می دهیم ایده آل تولید شده توسط F، I را تولید می کند، یعنی $I = < F >$.

از آنجا که F یک پایه ساگبی گروبنر برای I است لذا :

$< LTR^G >$ در جبر $LT(I)$ ایده آل تولید شده توسط $= < LT(I) > = < LT(F) >$

نشان می دهیم که اگر f عضوی از I باشد ، آنگاه g_1 و . . . و g_s هائی متعلق به R^G وf_1 و . . . و f_s هائی متعلق به F چنان موجودند که :

$$f = f_1 g_1 + \cdots + f_s g_s \qquad (۳-۹۴)$$

از آنجا که F پایه ساگبی گروبنر برای I است و f عضوی از I می باشد. هر $SG-$فرم نرمال به پیمانه ی F برابر صفر است، لذا f_1 و . . . و f_t هائی متعلق به F و s_1 و . . . و s_t های متعلق به $LM(R^G)$ چنان موجودند که :

$$0 = f - \left(\frac{a_1}{Lc(f_1).Lc(R(s_1))}\right).R(s_1).f_1 - \cdots - \left(\frac{a_t}{Lc(f_t).Lc(R(s_t))}\right).R(s_t).f_t \qquad (۳-۹۵)$$

که در آن به ازای هر i ، t_i ای متعلق به$T(h)$ چنان موجود است که $s_i = \frac{t_i}{LT(f_i)}$ و a_i ضریب t_i در f_i می باشد. از آنجا که $R(s_1)$ متعلق به R^G می باشد با قرار دادن

$$g_i = \left(\frac{a_i}{Lc(f_i).Lc(R(s_i))}\right).R(s_i).f_i \qquad (۳-۹۶)$$

و اینکه g_i ها متعلق به R^G می باشند .

نتیجه: فرض کنید I ایده آلی از R^G و F یک پایه ساگبی گروبنر برای I و f عضوی از R^G باشد، در اینصورت f متعلق به I است اگر وتنها اگر هر $SG-$فرم نرمال f به پیمانه ی F برابر صفر باشد .

فرض می کنیم هر $SG-$فرم نرمال f به پیمانه ی F برابر صفر باشد. نشان می دهیم f متعلق به I است. از آنجا که $f \underset{SG}{\overset{F}{\rightarrow}} 0$ لذا f_1 و . . . و f_t هائی متعلق به F و s_1 و . . . و s_t های متعلق به $LM(R^G)$ چنان موجودند که:

$$0 = f - \left(\frac{a_1}{Lc(f_1).Lc(R(s_1))}\right).R(s_1).f_1 - \cdots - \left(\frac{a_t}{Lc(f_t).Lc(R(s_t))}\right).R(s_t).f_t \qquad (۳-۹۷)$$

که در آن به ازای هر i، t_i ای متعلق به$T(h)$ چنان موجود است که $s_i = \frac{t_i}{LT(f_i)}$ و a_i ضریب t_i در f_i می باشد . بنابراین :

$$f = \left(\frac{a_1}{Lc(f_1).Lc(R(s_1))}\right).R(s_1).f_1 - \cdots - \left(\frac{a_t}{Lc(f_t).Lc(R(s_t))}\right).R(s_t).f_t$$

(۳-۹۸)

از آنجا که f_i ها متعلق به F و F زیر مجموعه ی I است لذا f_i ها متعلق به I هستند ودرنتیجه f متعلق به I است .

بالعکس : فرض کنید f متعلق به I باشد، از آنجا که F یک پایه ساگبی گروبنر برای I است ، هر $SG-$فرم نرمال f به پیمانه ی F برابر صفر می باشد .

۳-۴ الگوریتم بوخبرگر در حلقه های پایا

در این بخش الگوریتمی برای محاسبه ی پایه ساگبی گروبنر در حلقه ی R^G، که الگوریتم بوخبرگر پایا نام دارد ارائه می دهیم .

قبل از بیان الگوریتم ترتیب جدیدی را معرفی می کنیم سپس ابزارهای مهم استفاده شده در الگوریتم بوخبرگر پایا را با توجه به ترتیب گفته شده تعریف کرده و در نهایت به ارائه ی الگوریتم می پردازیم .

فرض کنید R یک مجموعه و $\prec$ یک رابطه ترتیبی جزئی در R باشد. در این صورت زوج $(R,\prec)$ را یک مجموعه مرتب جزئی می نا میم .

رابطه $\prec$ در $LM(R^G)$ را بصورت زیر تعریف می کنیم :

فرض کنید p و q دوتک جمله ای ابتدائی باشند.گوییم p ، q را عاد می کند یا q مضربی از p است و می نویسیم $p \prec q$ هرگاه یک تک جمله ای ابتدائی مانند r موجود باشد بطوریکه $q = pr$.

$(LM(R^G),\prec)$ یک مجموعه مرتب جزئی است .

فرض کنید m و n و p اعضایی از $< LM(R^G) >$ باشند، در این صورت :

الف – رابطه $\prec$ دارای خاصیت انعکاسی می باشد.

زیرا یک متعلق به $< LM(R^G) >$ می باشد و $m \prec m$.

ب – رابطه $\prec$ دارای خاصیت تعدی است .

زیرا اگر $n \prec p$ و $m \prec n$ آن گاه عناصر n_1 و m_1 از $< LM(R^G) >$ چنان موجودند که $n = mm_1$ و $p = nn_1$

لذا $p = mm_1n_1$ لذا $m \prec p$.

ج – رابطه $\prec$ پاد متقارن است .

زیرا اگر $n \prec m$ و $m \prec n$ آنگاه عناصر n_1 و m_1 از $< LM(R^G) >$ چنان موجودند که $m = nn_1$ و $n = mm_1$

، لذا $n = nn_1m_1$ ، بنابراین $n_1 = m_1 = 1$ و $n = m$

ابزار مهم استفاده شده در الگوریتم بوخبرگر S – چندجمله ایها هستند، در این قسمت برای بیان الگـوریتم ابتـدا سعی می کنیم S – چندجمله ایها را در R^G تعریف کنیم .

فرض کنید p و q دوتک جمله ای ابتدائی باشند، تک جمله ای ابتدائی r رایک کوچکترین مضرب مشـترک p و q می نامیم و با $r = LCM(p, q)$ نمایش می دهیم هرگاه p_1 و q_1 متعلق به $LM(R^G)$ چنان موجود باشند که :

$$r = pp_1 \text{ و } r = qq_1 \qquad (۳-۹۹)$$

و همچنین r با این خاصیت مینیمال باشد. به عبارتی اگر تک جمله ایهای اولیه $\acute{r}$ و $\acute{p_1}$ و $\acute{q_1}$ چنان موجود باشند که اگر $\acute{r} = p\acute{p_1}$ و $\acute{r} = q\acute{q_1}$ ، آنگاه تک جمله ای اولیه ی t چنان موجود است که $\acute{r} = rt$.

فرض کنید f_1 و f_2 دو چند جمله ای پایا باشند و r یک کوچکترین مضرب مشـترک $LM(f_1)$ و $LM(f_2)$ باشـد، در اینصورت قرار دهید :

$$p = \frac{r}{LM(f_1)} \quad \text{و} \quad q = \frac{r}{LM(f_2)} \qquad (۳-۱۰۱)$$

S – چندجمله ای f_1 و f_2 را به صورت زیر تعریف می کنیم :

$$S(f_1, f_2, r) = Lc(f_2).R(p_1).f_1 - Lc(f_1).R(p_2).f_2 \qquad (۳-۱۰۲)$$

ابتدا توجه کنید که تجزیه عناصر $LM(R^G)$ به حاصلضرب تک جمله ای های ابتدائی لزوما یکتـا نیسـت. بعنـوان مثال اگر $G = A_3$ که روی متغیرهای x و y و z عمل می کند و با در نظر گرفتن ترتیب قاموسی روی تـک جملـه

ای ها تک جمله ای $m = x^3yz$ را می توان بـه دو صـورت $m = (x^2z)(xy)$ و $m = (xyz)(x)(x)$ تجزیـه کرد که در آن داریم :

$$xyz = lm(xyz) \text{ و } xy = lm(xy + xz + yz) \text{ و } x^2z = lm(x^2z + z^2y + y^2x)$$

$$x = lm(x + y + z). \qquad (۳-۱۰۳)$$

فرض کنید $G = A_3$ گروه تناوبی روی سه متغیر z, y, x باشد. فرض کنید $p = xyz$ و $q = xy$، دراین صـورت x^3yz یک کوچکترین مضرب مشترک برای p و q اسـت. همچنـین x^4yz^2 و x^5yz^3 نیـز کـوچکترین مضـرب مشترک برای p و q می باشند.

نشان می دهیم بطور کلی برای هر $s \in \mathbb{N}$ ، $r = x^{s+2}yz^s$ یک $LCM(p,q)$ است زیرا با ضرب تک جملـه ای های ابتدائی $p' = x.x^sz^{s-1}$ و $q' = x^{s+1}z^s$ در p و q داریم :

$$pp' = qq' = x^{s+2}yz^s = r \qquad (۳-۱۰۴)$$

لذا r یک مضرب مشترکp وq می باشد .

حال ثابت می کنیم کهr مینیمال است ، بدین منظور نشان می دهیم هر تـک جملـه ای ابتـدائی کـوچکتر از r ،کوچکترین مضرب مشترک برای p و q نیست که این تک جمله ای ها را بطریق زیر بدست می آوریم :

الف : خارج قسمت تقسیم r بر تک جمله ای ابتدائی x^u برابر $r' = x^{s+2-u}yz^s$ است اما r' کوچکترین مضرب مشترک برای p و q نیست، زیرا $\frac{x^{s+2-u}yz^s}{xy} = x^{s+1-u}z^s$ و $x^{s+1-u}z^s$ تک جمله ای ابتدائی نیست .

ب : خارج قسمت تقسیم r بر تک جملـه ای ابتـدائی x^uy برابراسـت بـا $r' = x^{s+2-u}z^s$ امـا r' کـوچکترین مضرب مشترک برای p و q نیست، زیرا بر p بخش پذیر نیست .

ج : خارج قسمت تقسیم r بر تک جمله ای ابتدائی x^uz^t $(t+1 \leq u)$ برابراست با: $r' = x^{s+2-u}yz^{s-t}$.

اما r' کوچکترین مضرب مشترک بـرای p و q نیسـت، زیـرا $\frac{x^{s+2-u}yz^{s-t}}{xy} = x^{s+1-u}z^{s-t}$ و $x^{s+1-u}z^{s-t}$ تـک جمله ای ابتدائی نیست .

د : خارج قسمت تقسیم r بر تک جملـه ای ابتـدائی $(u \geq t)\ x^u yz^t$ برابراسـت بـا $r' = x^{s+2-u}z^{s-t}$ امـا r' کوچکترین مضرب مشترک برای p و q نیست ، زیرا بر p بخش پذیر نیست .

با توجه به مثال فوق نکته ی زیر را بیان می کنیم :

کوچکترین مضرب مشترک دو تک جمله ای ابتدائی منحصر بفرد نیست، بلکه ممکن است تعداد نا متناهی از آنها موجود باشد، در نتیجه برای دو چند جمله ای p و q از R^G

تعداد نا متناهی S – چند جمله ای موجود است .

به منظور ارائه ی الگوریتمی برای یافتن مجموعه ای که اعضای آن کوچکترین مضرب مشترک دو تک جمله ای ابتدائی a و b از درجه d می باشند ، ابتدا الگوریتم زیر را ارائه می دهـیم بطـوری کـه الگـوریتم تشـخیص مـی دهدکه آیا تک جمله ای ابتدائی r مضرب مشترک a و b هست یا خیر؟

سپس الگوریتم نهائی را بیان می کنیم .الگوریتم به صورت زیر می باشد :

INPUT : *initial monomials* a, b, r .

" *true*" *if* r *is common multiple of* a *and* b *and* " *false* " *else*.***OUTPUT***:

IF $\frac{r}{a}$ is initial *and* $\frac{r}{b}$ is initial ***THEN***

RETURN (*true*);

ELSE

RETURN(*false*) ;

A-۳- الگوریتم تشخیص کوچکترین مضرب مشترک b و a

اکنون الگوریتم محاسبه مجموعه کوچکترین مضارب مشترک b و a ازدرجه d را ارائه می دهیم:

INPUT:*an integer* $d \geq 1$ *and two initial monomials* a, b.

OUTPUT : *lcms of* a, b *of degree* d .

$B := [\,];$

$M := \{initial\ monomials\ of\ degree\ d\ of\ I(G)\};$

FOR $all\ \ m \in M$ **DO**

IF $\text{isLcm}\left(a, b, \frac{m}{s}\right)$ **THEN**

$N := \{irreducibles\ initial\ monomial\ of\ degree\ \ s < d\};$

$sw := true;$

FOR $all\ \ s \in N$ **WHILE** sw **DO**

IF $\text{isinitial}\left(\frac{m}{s}\right)$ and $\text{isLcm}\left(a, b, \frac{m}{s}\right)$ **THEN**

$sw := false;$

END IF

END FOR

$B := B \cup \{m\};$

END IF

END FOR

RETURN(B**);**

A-۴- الگوریتم محاسبه مجموعه کوچکترین مضارب مشترک b_3a ازدرجه d

فرض کنید $G = S_2$ با دو متغیر x, y باشد، بنابراین R^{S_2} برابر مجموعه تمام چند جمله ای های متقارن برحسب x وy می باشد. ترتیب قاموسی با شرط $y < x$ را در نظر می گیریم. فرض کنید $f = x^2 + y^2$ و $F = x + y$ عضایی از R^{S_2} باشند، به کمک الگوریتم تقسیم f را بر F تقسیم می کنیم ، داریم: $lm(f) = x^2, lm(x + y) = x$, $m = \frac{x^2}{x} = x$.

لذا : $f = f - x(x+y) = y^2 - xy$. ملاحظه می کنیم که با قیمانده تقسیم f را بر F تحت G پایا نیست .باید راهکاری پیدا کنیم که با قیمانده تقسیم یک چندجمله ای پایا تحت G به یک مجموعه پایا از چندجمله ایها تحت G پایا باشد به کمک الگوریتم زیر که آنرا الگوریتم تقسیم پایا می نامیم خواسته ما برآورده می شود.

INPUT : *an invariant* f *and a family of invariants* $F = (f_1, \dots, f_t)$

OUTPUT : *an invariant remainder* $\overline{f}^F$ *of* f *on division by* F

WHILE $f \neq 0$ ***DO***

FOR $g \in F$ ***DO***

$m = \frac{lm(f)}{lm(g)}$;

IF m *is a monomial and* m *is a initial* ***THEN***

$f = f - \frac{lc(f)}{lc(g)} |G| R(m) g$

RESTART *main loop*

END IF

END FOR

EXIT *main loop;*

END WHILE

RETURN(f);

A

-۵- الگوریتم تقسیم پایا

حال به کمک الگوریتم گفته شده f را بر F تقسیم می کنیم. داریم :

f	g	$m = \frac{lm(f)}{lm(g)}$	m تک جمله ای ابتدائی است؟
$x^2 + y^2$	$x + y$	x	$x = lm(x + y)$
$-2xy$	$x + y$	y	y تک جمله ای ابتدائی نیست.

ازآنجا که y تک جمله ای ابتدائی نیست لذا تقسیم همین جا پایان می یابد. لذا باقیمانده $-2xy$ است.

باقیمانده تقسیم f را بر F ر ا با $\overline{f}^F$ نمایش می دهیم.

$\overline{f}^F$ تحت G پایاست زیرا درهر مرحله از f که عنصری تحت G پایا ست، یک چند جمله ای پایا را کم می کنیم در واقع $\overline{f}^F$ترکیبی از چند جمله ای های f و $R(m)$وg است که همگی تحت G پایا می باشند، لذا $\overline{f}^F$ تحت G پایاست. هما نند الگوریتم تقسیم معمولی تقسیم پایا نیز همواره نتیجه منحصر بفردی ندارد .به مثال زیر توجه کنید :

با مفروضات مثال قبل اگر $f = x^2 + y^2$ و$F = (x^2 + y^2, x + y)$

آنگاه $\overline{f}^F$ ممکن است 0 یا $-2xy$ باشد و این بستگی دارد به اینکه ابتدا تقسیم را بر کدام چند جمله ای انجام دهیم.

فرض می کنیم $I =< f_1, \dots, f_s >$ یک ایده آل از R^G باشد و B زیر مجموعه ای از I شامل $f_s, \dots, f_1$ در این صورت B یک پایه گروبنر پایا برای I است اگر وفقط اگر برای هر دو عضو $SG\ B$- فـرم نرمـال S - چنـد جمله ای آنهابه پیمانه ی B مساوی صفر باشد.

با تو جه به مقدمات گفته شده اکنون می توانیم الگوریتم بوخبرگر پایا را ارائه می دهیم :

INPUT: *a set of homogeneous polynomial invariants* $F = \{f_1, \dots, f_s\}$

and maximal degree D

OUTPUT: *a* $SG-$ *basis up to degree* D *of* $I =< F >$ *in* R^G

$B := F$;

REPEAT

$B' := B$;

FOR ALLs $-pair\ \ s := S(b_1, b_2, r) of$ *any two elements*

DO B' *such that degree* $r \leq D$

$s := SG - normal form\ s\ modulo\ \ B'$;

IF $s \neq 0$ ***THEN***

$B := B \cup \{s\};$

END IF

END FOR

UNTIL $B = B'$

A- ۶ الگوریتم پایه گروبنر پایا

نشان می‌دهیم:

الف) در هر گام از الگوریتم B زیر مجموعه‌ای ازایده‌آل I است.

ب) در پایان کار، B یک پایه گروبنر است.

الف) در شروع کار داریم: $B = F \subset I$ و در ادامه طبق الگوریتم اعضای B وقتی افزایش می‌یابند که $-SG$ فرم نرمال $s \coloneqq S(f_1, f_2, r)$ به پیمانه ی B' به آن اضافه شود. لذا برای هر b_1, b_2 در $B^{'}$ که $B^{'} \subseteq B$ است داریم $s-$ چند جمله‌ای b_1, b_2, r متعلق به I است. بنابراین $-SG$ فرم نرمال $S(b_1, b_2, r)$ به پیمانه ی B' متعلق به I است، لذا s به I تعلق دارد. بنابراین (الف) همواره برقرار است.

ب) در هر مرحله الگوریتم برای هر f_1, f_2، مشاهده می‌شود که فرم نرمال $s-$ چند جمله‌ای b_1, b_2, r نسبت به B برابر صفر است، لذا B یک پایه گروبنر است که F را شامل می‌شود

فصل چهارم

الگوریتم F_5-پایا

۴-۱: الگوریتم F_5- پایا

در این بخش فرم ماتریسی الگوریتم F_5 را برای محاسبه ی پایه ساگبی گروبنر حداکثر از درجه ی D برای ایـده آلهای حلقه های پایا از گروههای متناهی مورد بررسی قرار می دهیم.

برای ارائه ی ا لگوریتم ابتدا تعریف زیر از ماتریس مک کولی[۱۵] را بیان می کنیم :

(ماتریس مک کولی)

فرض کنید f_1 و . . . و f_m چند جمله ایهای همگن پایا از درجه ی d_1 و . . . و d_m باشند کـه $d_1 \leq \ldots \leq d_m$.

در این صورت ماتریس مک کولی پایای f_1 و . . . و f_m از درجه ی d را به صورت زیر تشکیل می دهیم :

[15] - **Macauly**

ابتدا برای هر $1 \le i \le s$ کلیه ی تک جمله ایهای ابتدائی از درجه ی $d - d_i$ را بدست مـی آوریـم. اگـر آنهـا را m_{i1} و . . . و m_{is_i} بنامیم ، آنگاه سطرهای ماتریس مک کولی از چند جمله ایهای زیر بدست می آیند .

و . . . و $R(m_{1s_2}).f_2$ و . . . و $R(m_{21}).f_2$ و . . . و $R(m_{1s_1}).f_1$و . . . و $R(m_{11}).f_1$

لذا ماتریس $s_1 + s_2 \cdots + s_m$ سطر خواهد داشت .که در آن s_i هـا تعـداد تـک جملـه ایهـای ابتـدائی از درجـه $d - d_i$ می باشد. ستونهای ماتریس متناظر با تک جمله ایهای ابتدائی از درجه ی d می باشند، به عبـارتی اگـر تمام تک جمله ایهای ابتدائی از درجه ی d را با $\tilde{m}_1$ و . . . و $\tilde{m}_k$ نمایش دهیم، آنگـاه مـاتریس دارای k سـتون خواهد بود و ستون j - ام ضریب $R(\tilde{m}_j)$ در چند جمله ایهای $R(m_{it}).f_i$ می باشد .

حال به ازای هر $1 \le i \le s$ و هر $1 \le j \le s_i$ ، $R(m_{ij}).f_i$ یک چند جمله ای است که می توان آن را به صورت ترکیبی از عملگر رینولد $\tilde{m}_1$ و . . . و $\tilde{m}_k$ نوشت. اما از آ نجا که کلیه ضرائب عملگر رینولد یک تک جملـه ای بـا هم برابرند، ستونها را می توان متناظر با خود تک جمله ایهای ابتدا ئی $\tilde{m}_1$ و . . . و $\tilde{m}_k$ در نظر گرفـت. مـاتریس ضرائب فوق ر ا با $M_{d,m}$ نمایش می دهیم، به عبارتی داریم :

$$M_{d,m} = \begin{array}{c} \\ R(m_{i1}).f_1 \\ \vdots \\ R(m_{is_1}).f_1 \\ \vdots \\ R(m_{it}).f_i \end{array} \begin{array}{c} \tilde{m}_k \quad\quad \tilde{m}_j \quad\quad \tilde{m}_1 \\ \begin{bmatrix} \cdots & & \cdots \\ \vdots & & \vdots \\ \vdots & \gamma & \vdots \\ \vdots & \gamma & \vdots \end{bmatrix} \end{array} \qquad (۴-۱)$$

می باشد. $R(m_{1t}).f_i$ در چند جمله ای $\tilde{m}_j$ ضریب γکه در آن

فرض کنید در مرحله ی i ، d از الگوریتم باشیم که d درجه ی ماتریس این مرحله و i تعداد چند جمله ای هـا می باشد .الگوریتم F_5– پایا ابتدا زیر ماتریس $M_{d,i}$ از ماتریس مک کولی را محاسبه می کند و سپس تقلیل یافته ی سطری آن را بدست می آوریم .

برای گذر از گام i-1 به i ، بایستی ضرا ئب سطرهای $R(m_{ij}).f_i$ به ماتریس افزوده می شوند ، که در آن m_{ij} ها تمام تک جمله ایهای ابتدا ئی از درجه ی $d-d_i$ می باشند که ترم پیشروی هیچ یـک از سـطرهای $\widetilde{M}_{d-d_i,i-1}$ نیستند. ($\widetilde{M}_{d-d_i,i-1}$ ماتریس سطری پلکانی $M_{d-d_i,i-1}$ می باشد .)

به منظور ذخیره سازی و بازیابی چندجمله ایهائی که منجر به ایجاد سطرهای جدید در مـاتریس مـی شـوند بـه هنگام ضرورت بهتر است ماتریس M را به عنوان یک نگاشت از $S \times T$ به میدان K در نظر بگیـریم کـه در آن S زیر مجموعه ای متناهی از $N \times \vartheta$ یک زیرمجموعه ی متناهی از ϑ می باشد که توسـط یـک ترتیـب درجـه ای مرتب شده است و در آن ϑ مجموعه

تمام تک جمله ایها و T مجموعه ی تک جمله ایهای ابتدائی از درجه ی d می باشد.

یک سطر در ماتریس M بوسیله ی اندیس $s=(i,m_{ij})$ که متناسب با مجموع حاصل ضـربهای $R(m_{ij})$ در f_i می باشد، مشخص می شود .

بردار $ROW(M,s)=[M_{s,t}|t\in T]$ و چندجمله ای $\sum_{t\in T} M_{s,t}.\mathrm{R(t)}$ را معرفی می کنیم . تـرم پیشـروی یـک سطر همان ترم پیشروی چند جمله ای متناظر با s می باشد . قرار داد می کنیم $ROWS(M)=S$ ، به عبارتی هر اندیس $s=(i,m_{ij})$ متناظر با سطر $R(m_{ij}).f_i$ از ماتریس $M_{\mathrm{d,m}}$ می باشد.

عمل سطری مقدماتی زیر را مورد توجه قرار می دهیم :

$$ROW(M,s)\rightarrow ROW(M,s)+\alpha.ROW(M,\acute{s}) \qquad (۴-۲)$$

که در آن α متعلق به میدان K و $\acute{s}$ متعلق به S می باشد و همچنین این عمل را وقتی بکار می بـریم کـه شـرط اضافه ی زیر برقرار باشد :

$$\acute{s}=(j\,,\acute{u}\,)<s=(j\,,u)\quad (j<j \quad \text{یا} \quad (j=j\,,\acute{u}<_{grlex}u)) \qquad (۴-۳)$$

(محک F_5- پایا)

فرض کنید m ترم پیشروی سطر $(\widetilde{M}_{d-d_i,i-1}, s)$ باشد که $s < (i,1)$. در این صورت سطر $R(m).f_i$، متعلق به فضای برداری تولید شده توسط سطرهای $M_{d,i}$ با اندیس کوچکتر می باشد .

می دا نیم m برابر ترم پیشروی یکی از سطرهای ماتریس $\widetilde{M}_{d-d_i,i-1}$ است که متناظر با انـدیس $s = (l,t)$ می باشد، که در آن $l < i$. (زیرا $s < (i,1)$).

بنابراین h ای موجود است که $m = Lt(h)$ و h ترکیب خطی از حاصل ضربهای $R(m_{rj}).f_r$ می باشد ، لذا

$$h = \sum_{j=1}^{r} \sum_{r=1}^{i-1} R(m_{rj}).f_r \qquad (۴-۴)$$

که در آن m_{rj} تک جمله ای از درجه ی $d - d_i - d_r$ می با شند و بنابراین h یک چند جمله ای از درجه ی $d - d_i$ می باشد . داریم :

$$R(m).f_i = (h + R(m) - h).f_i \qquad (۴-۵)$$

که از معادله ی (۴-۴) نتیجه می شود :

$$R(m).f_i = \sum_{j=1}^{r} \sum_{r=1}^{i-1} R(m_{rj}).f_r.f_i + (R(m) - h).f_i =$$

$$\sum_{j=1}^{r} (\sum_{r=1}^{i-1} R(m_{rj}).f_i).f_r + (R(m) - h).f_i \qquad (۴-۶)$$

توجه کنید که چند جمله ای $\sum_{r=1}^{i-1} R(m_{rj}).f_i$ یک چندجمله ای از درجه ی $d - d_r$ می باشد که مـی تـوان آن را به صورت ترکیب خطی از عملگر های رینولد تک جمله ایهائی از درجه ی $d - d_r$ نوشت، بنابراین عناصـر θ_1 و ... و θ_a متعلق به K و تک جمله ایهای m_1 و ... و m_a از درجه $d - d_r$ چنان موجودند که :

$$\sum_{j=1}^{r} \sum_{r=1}^{i-1} R(m_{rj}).f_i.f_r = \sum_{j=1}^{r} \sum_{r=1}^{i-1} \theta_j R(m_j).f_r$$

(۴-۷)

چند جمله ای $\theta_j R(m_j)$ یک چند جمله ای از درجه ی $d - d_r$ است (بنا به آنچه گفته شـد) و f_r از درجـه ی d_r می باشد، بنابراین $\theta_j R(m_j).f_r$ چند جمله ای از درجه ی d می باشد و در نتیجه چند جمله ای بدست آمده از تساوی فوق متعلق به $M_{d,i-1}$ می باشد .

بنابراین جمله ی اول رابطه ی (۴-۶) متعلق به فضای برداری تولید شده توسط سطر های $M_{d,i-1}$ و جمله دوم ترکیب خطی از سطرهای $M_{d,i}$ با اندیس کوچکتر می باشد و داریم :

$$Lt(R(m) - h) < Lt(h) = m \qquad (۴-۸)$$

اکنون الگوریتم F_5- پایا را با هر ترتیب دلخواه ارائه می دهیم .

INPUT: *homogeneous polynomial invariant* $(f_1, \dots, f_m)$ *with degree* $d_1 \leq \cdots \leq d_m$ *and a maximal degree D*
OTPUT : *The elements of degree at most D of reduced SG- bases of* $(f_1, \dots, f_i)$ *for* $i = 1, \dots, m$.
For j **from** 1 **to** m **do**
$G_j := \emptyset$
For d **from** d_1 **to** *D* **do**
$M_{d,0} := \emptyset$, $\widetilde{M}_{d,0} := \emptyset$
For *i* ***from*** 1 ***to*** *j* ***do***
IF $d < d_i$ **then**
$M_{d,i} := M_{d,i-1}$
E l se
IF $d = d_i$ **then**
$M_{d,i} :=$ *add new row* f_i *to* $\widetilde{M}_{d,i-1}$ with index (i, 1)
Else
$M_{d,i}$:=add new row
(R(m).f_i) for all monomials m of degree $d - d_i$ that do not appear as leading mpnomials in the $\widetilde{M}_{d-d_i,i-1}$ with index(i , m) in $\widetilde{M}_{d,i-1}$.
Compute $\widetilde{M}_{d,i}$ by Gaussian elimination from $M_{d,i}$ add to G_j all rows of $\widetilde{M}_{d,i}$ not reducible by LT(G_j) .
RETURN $[G_j | j = 1, \dots, m]$.

A-۷: الگوریتم F_5- پایا

درستی الگوریتم F_5- پایا

الگوریتم F_5 - پایا برای هر$1 \leq i \leq m$ تمام عناصر از درجه ی حداکثر D از پایه ساگبی گروبنر تقلیل یافته از $< f_1, \dots, f_i >$ را تولید می کند.

اثبات را با استقرا روی d وi انجام می دهیم. نخست فرض کنید $d = d_1$ و$i = 1$ دراین صورت تنها سطر ماتریس مک کولی از چند جمله ای $R(1).f_1 = f_1$ بدست می آید وستون های ماتریس، متناظر با تک جمله ایهای ابتدائی از درجه ی $d = d_1$ می باشند. در این حالت داریم $M_{d,1} = \tilde{M}_{d,1}$ و$G_1 = f_1$ و حکم برای شروع استقراء درست است. حال فرض می کنیم حکم برای $i = j - 1$ و $d_1 \leq \cdots \leq d_{j-1}$ برقرار باشد وقرار می دهیم $d = d_j$ ، بایستی ثابت کنیم سطر های $M_{d,j}$ ایده آل $< f_1, \dots, f_{d_j} >$ را تولید می کند، زیرا در این صورت نتیجه می شود $LT(\tilde{M}_{d,j})$ ، مولدی برای $LT(< f_1, \dots, f_j >_d)$ می باشد و در نتیجه جملات پیشروی G_j مولدی برای $LT(< f_1, \dots, f_j >_d)$ می باشد. بنابراین کافی است نشان دهیم برای هر تک جمله ای ابتدائی مانند θ از درجه ی $d - d_j$، چندجمله ای $R(\theta).f_j$ بوسیله ی سطر های $M_{d,j}$ تولید می شود. بدین منظور دو حالت در نظر می گیریم :

حالت اول : فرض کنید $\theta \in LT(\tilde{M}_{d-d_j,j-1})$ در این صورت بنا به گزاره ی(۴-۱-۲) $R(\theta).f_j$ به وسیله ی سطرهای ماتریسی که اندیس کوچکتر دارد تولید می شود و حکم بنا به فرض استقرا درست است .

حالت دوم : اگر حالت اول برقرار نباشد، آنگاه نتیجه می شود $R(\theta).f_j$ بوسیله ی الگوریتم به عنوان سطری از $M_{d,j}$ قرار گرفته و این اثبات را کامل می کند .

اکنون مثالی از الگوریتم F_5- پایا را ارائه می دهیم :

فرض کنید G گروه جایگشتی A_3 با سه متغییر x, y, z باشد، می توان نشان داد که :

$$R(f) = \frac{1}{3}(f(x,y,z) + f(z,x,y) + f(y,z,x)) \qquad (۴-۹)$$

ترتیب درجه ای با شرط $z < y < x$ را روی حلقه ی R^{A_3} در نظر می گیریم .

فرض کنید:

$$I =< f_1, f_2 >= < R(x), R(x^2y) - R(xyz) > \qquad (۴-۱۰)$$

با توجه به الگوریتم F_5- پایا ، یک پایه ساگبی گروبنر از درجه حداکثر ۵ برای I محاسبه می کنیم .

در مرحله اول برای درجه ی ۱ داریم $G_2 = \{f_1, f_2\}$ ، برای درجه ی ۲ ماتریس $M_{2,1}$ تولید می شود که سطرهای آن از ضرائب چند جمله ایهای زیر به دست می آید :

$$R(x).f_1 = \frac{1}{9}\mathrm{R}(x^2) + \frac{2}{9}\mathrm{R}(xy)$$

بنابراین :

$$M_{2,1} = \begin{matrix} \mathrm{R}(x^2) & \mathrm{R}(xy) \\ \left(\frac{1}{9} \right. & \left. \frac{2}{9}\right) \end{matrix}$$

(۴-۱۱)

با انجام عملیات سطری پلکانی روی $M_{2,1}$ داریم $M_{2,1} = \tilde{M}_{2,1}$ بنابراین چند جمله ای جدید بوجود نمی آید .

در درجه ی۳ ، ماتریس $M_{3,1}$ تولید می شود. سطرهای ماتریس $M_{3,1}$ از ضرا ئب چند جمله ایهای زیر بدست می آید .

$$R(x^2).f_1 = \frac{1}{9}\mathrm{R}(x^3) + \frac{1}{9}\mathrm{R}(x^2y) + \frac{1}{9}\mathrm{R}(x^2z)$$

$$R(xy).f_1 = \frac{1}{9}\mathrm{R}(x^2y) + \frac{1}{9}\mathrm{R}(x^2z) + \frac{1}{3}\mathrm{R}(xyz) \qquad (۴-۱۲)$$

بنابراین

$$M_{3,1} = \begin{matrix} \\ R(x^2).f_1 \\ R(xy).f_1 \end{matrix} \begin{matrix} \begin{matrix} R(x^3) & R(x^2y) & R(x^2z) & R(xyz) \end{matrix} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \end{pmatrix} \end{matrix}$$

توجه کنید که ماتریس سطری پلکانی $M_{3,1}$ یعنی $\widetilde{M}_{3,1}$ با خود آن برابر است ، لذا نتیجه ای حاصل نمی شود . اکنون ماتریس $M_{3,2}$ را محاسبه می کنیم . برای اینکار کافی است چند جمله ای f_2 را به $\widetilde{M}_{3,1}$ اضافه کنیم ، بنابراین داریم :

$$M_{3,1} = \begin{matrix} \\ R(x^2).f_1 \\ R(xy).f_1 \\ f_2 \end{matrix} \begin{matrix} \begin{matrix} R(x^3) & R(x^2y) & R(x^2z) & R(xyz) \end{matrix} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 & \frac{-1}{3} \end{pmatrix} \end{matrix}$$

بعداز اعمال سطری پلکانی روی $M_{3,1}$ داریم :

$$\widetilde{M}_{3,1} = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \\ 0 & 0 & \frac{-1}{3} & -2 \end{pmatrix}$$

بنابراین چند جمله ای $f_3 = -\frac{1}{3}R(x^2z) - 2R(xyz)$ حاصل می شود که آن را به G_2 اضافه می کنیم لذا داریم :

$$G_2 = \{f_1, f_2, f_3\}$$

در درجه ۴، سطرهای ماتریس $M_{4,1}$ توسط ضرا ئب چند جمله ایهای زیر به دست می آید:

$$R(x^3).f_1 = \frac{1}{9}\mathrm{R}(x^4) + \frac{1}{9}\mathrm{R}(x^3y) + \frac{1}{9}\mathrm{R}(x^3z)$$

$$R(x^2y).f_1 = \frac{1}{9}\mathrm{R}(x^3y) + \frac{1}{9}\mathrm{R}(x^2y^2) + \frac{1}{9}\mathrm{R}(x^2yz)$$

$$R(x^2z).f_1 = \frac{1}{9}\mathrm{R}(x^3z) + \frac{1}{9}\mathrm{R}(x^2y^2) + \frac{1}{9}\mathrm{R}(x^2yz)$$

$$R(xyz).f_1 = \frac{1}{3}\mathrm{R}(x^2yz)$$

بنابراین داریم :

$$M_{4,1} = \begin{array}{c} \\ R(x^3).f_1 \\ R(x^2y).f_1 \\ R(x^2z).f_1 \\ R(xyz).f_1 \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{R}(x^4) & \mathrm{R}(x^3y) & \mathrm{R}(x^3z) & \mathrm{R}(x^2y^2) & \mathrm{R}(x^2yz) \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & 0 & \frac{1}{3} \end{pmatrix} \end{array}$$

ماتریس سطری پلکانی $M_{4,1}$ ، یعنی $\tilde{M}_{4,1}$ با خود آن برابر است ، بنابراین چند جمله ای جدیدی حاصل نمی شود . برای $M_{4,2}$ نیز همین حالت پیش می آید و در نتیجه چند جمله ای جدیدی بوجود نمی آید . عملیات را برای درجه ی ۵ ادامه می دهیم .

سطرهای ماتریس $M_{5,1}$ توسط ضرا ئب چند جمله ایهای زیر بدست می آید :

$$R(x^4).f_1 = \frac{1}{9}\mathrm{R}(x^5) + \frac{1}{9}\mathrm{R}(x^4y) + \frac{1}{9}\mathrm{R}(x^4z)$$

$$R(x^3y).f_1 = \frac{1}{9}\mathrm{R}(x^4y) + \frac{1}{9}\mathrm{R}(x^3y^2) + \frac{1}{9}\mathrm{R}(x^3yz)$$

$$R(x^3z).f_1 = \frac{1}{9}\mathrm{R}(x^4z) + \frac{1}{9}\mathrm{R}(x^3z^2) + \frac{1}{9}\mathrm{R}(x^3yz)$$

$$R(x^2y^2).f_1 = \frac{1}{9}\mathrm{R}(x^3y^2) + \frac{1}{9}\mathrm{R}(x^3z^2) + \frac{1}{9}\mathrm{R}(x^2y^2z)$$

$$R(x^2yz).f_1 = \frac{1}{9}\mathrm{R}(x^3yz) + \frac{2}{9}\mathrm{R}(x^2y^2z)$$

لذا داریم :

$$M_{5,1} = \begin{array}{c} \\ R(x^4).f_1 \\ R(x^3y).f_1 \\ R(x^3z).f_1 \\ R(x^2y^2).f_1 \\ R(x^2yz).f_1 \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathrm{R}(x^5) & \mathrm{R}(x^4y) & \mathrm{R}(x^4z) & \mathrm{R}(x^3y^2) & \mathrm{R}(x^3yz) & \mathrm{R}(x^3z^2) & \mathrm{R}(x^2y^2z) \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & \frac{1}{9} & 0 & 1 & \frac{2}{9} \\ 0 & 0 & 0 & 0 & \frac{1}{9} & 0 & \end{pmatrix} \end{array}$$

با عملیات سطری پلکانی داریم : $M_{5,1} = \tilde{M}_{5,1}$

حال ماتریس $M_{5,2}$ با اضافه کردن سطرهای $R(x^2).f_2$ و $R(xy).f_2$ بدست مـی آیـد متعلـق بـه تـرم پیشـروی سطرهای $\tilde{M}_{2,1}$ $(i-1=1, d-d_i=2)$

می باشد، بنابراین $R(x^2).f_2$ از سطرهای ماتریس $M_{5,2}$ حذف می شود .

لذا داریم :

$$\begin{array}{ccccccc} \mathrm{R}(x^5) & \mathrm{R}(x^4y) & \mathrm{R}(x^4z) & \mathrm{R}(x^3y^2) & \mathrm{R}(x^3yz) & \mathrm{R}(x^3z^2) & \mathrm{R}(x^2y^2z) \end{array}$$

$$M_{5,2} = \begin{matrix} R(x^4).f_1 \\ R(x^3y).f_1 \\ R(x^3z).f_1 \\ R(x^2y^2).f_1 \\ R(x^2yz).f_1 \\ R(xy).f_2 \end{matrix} \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & 0 & \frac{1}{9} & 0 & 0 & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & 0 & 0 & \frac{1}{9} & 0 & \frac{-2}{9} \\ 0 & 0 & \frac{1}{9} & 0 & 0 & 0 & 0 \end{pmatrix}$$

با انجام عملیات سطری پلکانی داریم :

$$\widetilde{M}_{5,2} = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & 0 & \frac{1}{9} & 0 & 0 & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{2}{9} & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{9} & \frac{-5}{9} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

بنابراین یک چندجمله ای جدید $f_4 = \frac{-1}{9}R(x^3z^2) - \frac{5}{9}\,\mathrm{R}(x^2y^2z)$ حاصل می شود کـه آن را بـه G_2 اضـافه می کنیم . الگوریتم پایان می پذیرد و داریم :

$$G_2 = \{f_1, f_2, f_3, f_4\} \qquad (۴-۱۳)$$

که G_2 یک پایه ساگبی گروبنر تقلیل یافته است .

۴-۲: روشی برای پیدا کردن پایاهای ثانویه

در این بخش کاربردی از الگوریتم F_5- پایا برای محاسبه ی پایاهای ثانویه R^G ارائه می دهیم .

$$R^G = K[\ \ R(X^\alpha)\ \mid\ \ |\alpha| < |G|\ \ ] \qquad (۴-۱۴)$$

بنا براین R^G به عنوان یک K - جبر متناهیاً تولید شده است. مجموعه ی ایـن مولـدها را مجموعـه ی پایاهـای اساسی R^G نامیم. لذا زیر مجموعه ای متناهی از R^G مانند S چنان موجود است که R^G به عنوان یک مدول روی جبر $K[S]$ با تولید متناهی است .

زیر مجموعه ی S از R^G را یک مجموعه ی پایای اولیه R^G نامیم هرگاه R^G به عنوان یک مدول روی جبر $K[S]$ با تولید متناهی باشد و تعداد اعضای S با این خاصیت مینیمال باشد . در این صورت به هر مولد مینیمال R^G به عنوان یک مدول روی جبر $K[S]$ یک مجموعه ی پایای ثانویه گوئیم .

دراین بخش فرض می کنیم پایاهای اولیه داده شده اند، در الگوریتمی که ارائه می دهیم از درجه و تعداد پایاهای ثانویه استفاده می شود .

برای ارائه ی این الگوریتم گزاره ی زیر ازمقاله ی [6] را ارائه می دهیم .

فرض کنید $S = \{f_1, \dots, f_m\}$ یک مجموعه پایای اولیه R^G و برای $1 \le i \le m$

d_i درجه ی f_i باشند ، دراین صورت :

الف: تعداد پایاهای ثانویه برا بر است با :

$$t = \frac{d_1 \times \cdots \times d_m}{|G|} \qquad (۴-۱۵)$$

ب: اگر e_1 و . . . و e_t درجه ی پایاهای ثانویه باشند آنگاه سری هیلبرت R^G به صورت زیر تعریف می شود :

$$H(R^G, z) = \frac{z^{e_1} + \cdots + z^{e_t}}{(1-z^{d_1}) \cdots (1-z^{d_m})} \qquad (۴-۱۶)$$

فرض کنید I ایده آلی از R^G باشد .

الف : تک جمله ای ابتدائی m را نسبت به ایده آل I استاندارد نامیم هرگاه m متعلق به $< LT(I) >$ نباشد .

ب : چند جمله ای پایای $R(m)$ از تک جمله ای استاندارد m نسبت به I را یک چند جمله ای پایای استاندارد نسبت به ایده آل I نامیم .

فرض کنید I ایده آلی از R^G باشد، در این صورت مجموعه ی زیر یک پایه برای K- فضای برداری $\frac{R^G}{I}$ تشکیل می دهد

$A = \{R(m) \mid m$یک تک جمله ای استاندارد نسبت Iاست$\}$

فرض کنید $F = \{f_1, \dots, f_m\}$ یک پایه گروبنر برای ایده آل I و f عضوی از R^G باشند. با استفاده از الگوریتم تقسیم پایا f را به F تقسیم می کنیم . الگوریتم زمانی پایان می پذیرد که به ازای هر ترم از باقیمانده مانند t و به ازای هر $1 \le i \le m$ داشته باشیم $Lt(f_i) \nmid t$ ، به عبارتی t مضرب هیچ یک از جملات پیشروی اعضای F نباشد و یا اگر برای ترمی مانند t داشته باشیم $t = Lt(f_i).t$، آنگاه t ابتدائی نباشد. حال اگر باقیمانده را r بنامیم تک جمله ایهای ابتدائی m_1 و ... و m_s از $< LT(R^G) >$ و اسکالرهای $\lambda_1, \lambda_2 \dots \lambda_s$ چنان موجودند که :

$$r = \lambda_1 R(m_1) + \cdots + \lambda_s R(m_s) \qquad (۴-۱۷)$$

اما برای هر $1 \le i \le s$ داریم $m_i \notin < LT(I) >$ اگر برای $1 \le j \le s$ ای داشته باشیم $m_j \in < LT(I)$: ، از آنجا که F یک پایه ساگبی برای I است ، لذا

$$< LT(I) > = < LT(F) > \qquad (۴-۱۸)$$

f_i ای متعلق به F و h ای متعلق به R^G چنان موجودند که :

$$m_j = Lt(f_i).h \qquad (۴-۱۹)$$

لذا h بایستی یک تک جمله ای باشد، بنابراین $h = Lt(h) \in LT(R^G)$. اما این با اینکه m_j یکی از جملات باقیمانده است در تضاد است. بنابراین مجموعه ی A مولدی برای K- فضای برداری $\frac{R^G}{I}$ است . در ادامه اثبات می کنیم که عناصر A در K مستقل خطی هستند . بدین منظور فرض کنید داشته باشیم :

$$\lambda_1 R(m_1) + \cdots + \lambda_s R(m_s) = 0 \qquad (۴-۲۰)$$

از آنجا که $R(m_1)$ و ... و $R(m_s)$ هیچ جمله ی مشترکی ندارند لذا باید $\lambda_1 = \cdots = \lambda_s = 0$.

بنابراین عناصر A در K مستقل خطی هستند . بدین ترتیب حکم ثابت می شود

مجموعه ی عناصر همگن $B = \{g_1, \dots, g_m\}$ یک مجموعه ی پایای ثانویه نسبت به مجموعه ی پایای اولیه $\{f_1, \dots, f_s\}$ است اگروفقط اگرتصویر B در $\frac{R^G}{<f_1,\dots,f_s>}$ یک پایه برای $\frac{R^G}{<f_1,\dots,f_s>}$ به عنوان K- فضای برداری باشد

.

فرض کنید $I =< f_1, \dots, f_s >$ و $B = \{g_1, \dots, g_m\}$ پایای ثانویه نسبت به $\{f_1, \dots, f_s\}$ باشد و $A = K[f_1, \dots, f_s]$. در این صورت ابتدا نشان می دهیم $R^G = I$ و از آن نتیجه می شود تصویر B در $\frac{R^G}{I}$ یعنی $\{I\}$ مولدی برای $\frac{R^G}{I}$ است. با توجه به فرض داریم که R^G به عنوان یک A- مدول توسط B تولید می شود. عضوی مانند f از R^G در نظر می گیریم عناصر γ_1 و ... و γ_m از A چنان موجودند که:

$$f = \gamma_1 g_1 + \cdots + \gamma_m g_m \qquad (۴-۲۱)$$

ملاحظه می کنیم که: $f + I = \gamma_1 g_1 + \cdots + \gamma_m g_m + I = I$.

لذا $f \in I$ و $R^G = I$ و $\frac{R^G}{I}$ فضای برداری صفر است که توسط B تولید می شود .

بالعکس فرض می کنیم که $B = \{h_1, \dots, h_r\}$ پایه ای برای $\frac{R^G}{I}$ به عنوان K- فضای برداری باشد . می خواهیم ثابت کنیم که B یک پایای ثانویه نسبت به $f_s, \dots, f_1$ برای R^G است. عضوی مانند a از R^G در نظر می گیریم، بدون کاستن از کلیت مسئله می توان فرض کرد که a از درجه d باشد، داریم:

$$a + I \in \frac{R^G}{I} =< h_1 + I, \dots, h_r + I >$$

(۴-۲۲)

لذا عناصر λ_1 و ... و λ_r از K چنان موجودند که:

$$a + I = \sum_{i=1}^{r} \lambda_i h_i + I$$

(۴-۲۳)

لذا

$$a - \sum_{i=1}^{r} \lambda_i h_i \in I \qquad (۴-۲۴)$$

بنابراین عناصر α_1و ... وα_s از R^G چنان موجودند که :

$$a - \sum_{i=1}^{r} \lambda_i h_i = \sum_{i=1}^{s} \alpha_i f_i \qquad (۴-۲۵)$$

و لذا

$$a = \sum_{i=1}^{r} \lambda_i h_i + \sum_{i=1}^{s} \alpha_i f_i \qquad (۴-۲۶)$$

حال از آن جا که a همگن از درجه d است وبرای هر $1 \le i_1 \le s$ داریم $\deg(f_{i_1}) \ge 1$. لذا $\deg(\alpha_{i_1}) \le d-1$.

همچنین برای هر $1 \le i_1 \le s$ داریم $\alpha_{i_1} \in R^G$. همانند قبل برای هر $1 \le j \le r$ عناصر α_{j,i_1} از R^G و λ_{j,i_1} از K چنان موجودند که :

$$\alpha_{i_1} = \sum_{j=1}^{r} \lambda_{j,i_1} h_j + \sum_{j=1}^{s} \alpha_{j,i_1} f_j \qquad (۴-۲۷)$$

همانند قبل می توان نشان دادکه برای هر $1 \le j \le s$ و هر $1 \le i_1 \le s$ داریم :

$$\deg(\alpha_{j,i_1}) \le d-2 \qquad (۴-۲۸)$$

با ادامه این روند درجه این جملات مساوی یک خواهد شد. فرض می کنیم پس از m بار این اتفاق بیافتد لذا داریم :

$$\alpha_{i_1,\dots,i_m} = \sum_{j=1}^{r} \lambda_{j,i_1,\dots,i_m} h_j + \sum_{j=1}^{s} \alpha_{j,i_1,\dots,i_m} f_j \qquad (۴-۲۹)$$

که در آن $\deg(\alpha_{i_1,\dots,i_m}) = 1$.

بنابراین برای هر $1 \le j \le s$ داریم $\deg(\alpha_{j,i_1,\dots,i_m}) = 0$. لذا عناصر a_1 و ... و a_r و b_1 و ... و b_s از K چنان موجودند که :

$$\alpha_{i_1,\dots,i_m} = \sum_{i=1}^{r} a_i h_i + \sum_{i=1}^{s} b_i f_i$$

(۴-۳۰)

با جایگذاری روابط به دست آمده در رابطه **(۴-۳۲)**داریم :

$$a = \beta_1 h_1 + \cdots + \beta_r h_r \qquad \textbf{(۴-۳۱)}$$

که در آن برای هر $1 \le j \le r$ داریم : $\beta_j \in K[f_1, \dots, f_s]$.

لذا B یک پایای ثانویه نسبت به$f_s, \dots, f_1$ برای R^G است و بدین ترتیب حکم ثابت می شود.

اگر $I =< \theta_1, \dots, \theta_s >$ یک ایده آل ازR^G و $\{\theta_1, \dots, \theta_s\}$یک مجموعه پایای اولیه برای R^G باشد، آنگاه مجموعه عناصر پایای استاندارد نسبت به $< \theta_1, \dots, \theta_s >$ برابر است با یک مجموعه پایای ثانویه نسبت به $< \theta_1, \dots, \theta_s >$.

مجموعه عناصر پایای استاندارد نسبت به $< \theta_1, \dots, \theta_s >$ پایه ای برای فضای برداری $\frac{R^G}{<\theta_1,\dots,\theta_s>}$ می باشد قبل برابر است با یک مجموعه پایای ثانویه نسبت به $< \theta_1, \dots, \theta_s >$

با توجه به قضایای گفته شده، با داشتن پایای اولیه $F = (f_1, \dots, f_n)$ برای R^G مجموعه پایای ثانویه نسبت به $(f_1, \dots, f_n)$ برای ایده آل $I =< F >$ ر ا می توان محاسبه کرد .

اکنون می توانیم الگوریتم محاسبه ی پایاهای ثانویه را ارائه می دهیم . ا لگوریتم F_5 - پایا را برای f_1 و . . . و f_5 از درجه ی حداکثر e_t بکار می بریم . پایاهای استاندارد (پایاهای ثانویه) را محاسبه می کنیم . الگوریتم به صورت زیر است :

INPUT: A set of primary invariants(Homogeneous polynomials invariants $(f_1, \dots, f_n)$ with degree $d_1 \leq \cdots \leq d_n$)

OTPUT : The secondary invariant

Calculate the number and degree $e_1, \dots, e_t$

Standard :={}:

For i **from** 1 **to** t **do**

N_i = the set of initial monomial of degree e_i of R^G

Standard := Standard $\cup$ ($N_i \setminus LT(\tilde{M}_{e_i,n})$

RETURN Standard

A-۸- الگوریتم محاسبه ی پایاهای ثانویه

اکنون مثالی از ا لگوریتم گفته شده ارائه می دهیم :

فرض کنید G گروه ماتریسی تعریف شده به صورت زیر باشد :

$$G = \{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}\}$$

همچنین $\{f_1 = x^2 + y^2, f_2 = z^2, f_3 = x^4 + y^4\}$ مجموعه ای از پایاهای اولیه R^G باشند که $R = C[x,y,z]$

برای محاسبه ی پایاهای ثانویه ابتدا باید تعداد آنها برای ما مشخص باشد، بنا به گزاره ۴-۲-۱ داریم :

درجه ی $f_1 = d_1$ = ۲ و درجه ی $f_2 = d_2$ = ۲ و درجه ی $f_3 = d_3$ = ۴.

(ترتیب درجه ای با شرط $z < y < x$ را درنظر گرفته ایم) .

$$t = \frac{d_1 \times d_2 \times d_3}{|G|} = \frac{2 \times 2 \times 4}{4} = 4$$

بنابراین پایاهای ثانویه ی g_1 و g_2 و g_3 و g_4 ازدرجه ی e_1 و e_2 و e_3 و e_4 موجودند. بنا بـه گـزاره ی گفتـه شـده داریم :

$$(*) \qquad H(R^G,z)=\frac{z^{e1}+z^{e2}+z^{e3}+z^{e4}}{(1-z^2)(1-z^2)(1-z^3)} \qquad (۴-۳۲)$$

حال با توجه به فرمول فوق، باید درجه های e_1 و e_2 و e_3 و e_4 را محاسبه کنیم با توجه به تعریف مولین[۱۶] سـری هیلبرت حلقه های پایا از فرمول زیر به دست می آید :

$$H(R^G,z)=\frac{1}{|G|}\sum_{A\in G}\frac{1}{det(1-zA)} \qquad (۴-۳۳)$$

بنا براین برای گروه ماتریسی مفروض می توان محا سبه کرد که :

$$(**) \qquad H(R^G,z)=\frac{z^3+z^2-z+1}{(1+z)^2(1+z^2)(1-z)^3} \qquad (۴-۳۴)$$

با مقایسه ی دو سری هیلبرت بدست آمده یعنی روابط(۴-۳۲)و (۴-۳۴) داریم :

$$e_1=0\,,e_2=e_3=3\,,e_4=4 \qquad (۴-۳۵)$$

از طرفی عملگر رینولد f تحت گروه G را می توان به صورت زیر محاسبه کرد :

$$R(f)=\frac{1}{|G|}\sum_{A\in G}f(AX)$$

$$R(f)=\frac{1}{4}(f(x,y,z)+f(-y,x,-z)+f(-x\,,-y,z)+f(y,-x,-z)) \qquad (۴-۳۶)$$

۲- molien

حال با توجه به الگوریتم گفته شده در درجه ی ۳ داریم :

$N = \{x^2z, xyz\}$ و $Lt(\widetilde{M}_{3,3}) = \{\}$. بنـابراین مجموعـه ی چندجملـه ایهـای اسـتاندارد از درجـه ی ۳ برابـر $\{x^2z, xyz\}$ می باشد .

برای درجه ی ۴ داریم :$N = \{x^4, x^3y, x^2y^2, x^2z, z^4\}$ و $Lt(\widetilde{M}_{4,3}) = \{x^4, x^2y^2, x^2z, z^4\}$. بنـابراین چنـد جمله ای x^3y چندجمله ای استا ندارد از درجه ی ۴ است زیرا : $N - Lt(\widetilde{M}_{4,3}) = \{x^3y\}$

در نتیجه مجموعه ی $\{1, x^2z, xyz, x^3y\}$ مجموعه ی استانداردهای به دست آمده می باشد.

بنابراین پایاهای ثانویه g_1 و g_2 و g_3 و g_4 به صورت زیر به دست می آیند :

$g_1 = 1$ ، $g_2 = R(x^2z)$ ، $g_3 = R(xyz)$ ، $g_4 = R(x^3y)$

پیوست

الف) واژه نامه انگلیسی- فارسی

Coefficient	ضریب
Degree	درجه
Element	عنصر
Finite	تناهی
Fundamental	اساسی
Group	گروه
Homogeneous	همگن
Ideal	ایده آل
Infinit	نامتناهی
Initial	ابتدائی
Input	ورودی
Invariant	پایا
Irreducible	تحویل ناپذیر
Leading Coefficient	ضریب پیشرو
Leading Monomial	تک جمله ای پیشرو
Leading Term	ترم پیشرو
Lexicographical Oreder	ترتیب قاموسی
Monomial	تک جمله ای
Monoid	تکواره

Normal Form	فرم نرمال
Output	خروجی
Partial	جزئی
Polynomial	چند جمله ای
Primary	اولیه
Reduced	تقلیل یافته
Reduction	تقلیل
Relation	رابطه
Remainder	باقیمانده
Ring	حلقه
Secondary	ثانویه
Standard	استاندارد
Sub matrix	زیر ماتریس
Symmetric	متقارن
Unique	منحصر بفرد
Valid	صحیح
Variable	متغیر
Vector Space	فضای برداری

ب) واژه نامه فارسی - انگلیسی

Initial	ابتدائی
Standard	استاندارد
Fundamental	اساسی
Primary	اولیه
Ideal	ایده آل
Remainder	باقیمانده
Invariant	پایا
Irreducible	تحویل ناپذیر
Leading Term	ترم پیشرو
Leading Monomial	تک جمله ای پیشرو
Monomial	تک جمله ای
Monoid	تکواره
Reduction	تقلیل
Reduced	تقلیل یافته
Secondary	ثانویه
Solution	جواب
Partial	جزئی
Polynomial	چند جمله ای
Ring	حلقه
Degree	درجه

Relation	رابطه
Sub matrix	زیر ماتریس
Leading Coefficient	ضریب پیشرو
Coefficient	ضریب
Valid	صحیح
Element	عنصر
Normal Form	فرم نرمال
Vector Space	فضای برداری
Groulp	گروه
Finite	متناهی
Symmetric	متقارن
Variable	متغیر
Unique	منحصر بفرد
Infinit	نامتناهی
Input	ورودی
Homogeneous	همگن

مراجع

[1] J. Kim and P. Moin. Application of a Fractional-Step Method to Incompressible Navier-Stokes Equations. *Journal of Computational Physics*, vol. 59, pp. 308-323, 1985.

[2] M-H. Chung. Cartesian cut cell approach for simulating incompressible flows with rigid bodies of arbitrary shape. *Computers & Fluids*, vol. 35, pp. 607-623, 2006.

[3] T. Ye, R. Mittal, H.S. Udaykumar and W. Shyy. An Accurate Cartesian Grid Method for Viscous Incompressible Flows with Complex Immersed Boundaries. *Journal of Computational Physics*, vol. 156, pp. 209-240, 1999

[4] Yu-Heng Tseng, Joel H. Ferziger. A ghost-cell immersed boundary method for flow in complex geometry. *Journal of Computational Physics*, vol. 192, pp. 593-623, 2003.

[5] Donna Calhoun. A Cartesian Grid Method for Solving the Two-Dimensional Streamfunction-Vorticiy Equations in Irregular Regions. *Journal of Computational Physics*, vol. 176, pp.231-275, 2002.

[6] H. Johansen and P. Colella. A Cartesian Grid Embedded Boundary Method for Poisson's Equation on Irregular Domains. *Journal of Computational Physics*, vol. 147, pp. 60-85, 1998 .

[7] J. Kim, D. Kim and H. Choi. An Immersed-Boundary Finite-Volume Method for simulations of Flow in Complex Geometries. *Journal of Computational Physics*, vol. 171, pp.132-150, 2001.

[8] A Cartesian Grid Finite-Volume Method for the Advection-Diffusion Equaion in irregular Geometries. *Journal of Computational Physics*, vol. 14(7), pp.828-848, 2004.

[9] Rajat Mittal, Gianluca laccarino. Immersed Boundary Methods. *Annu. Rev, Fluid Mech.*, vol. 37, pp.237-261, 2005.

[10] J. R. Pacheco, A. Pacheco-Vega, T. Rodic and R. E. Perk. Numerical simulations of heat transfer and fluid flow problems using an immersed-boundary finite-volume method on non staggered grids.

[11] H.S. Udykumar, R. Mittal, P. Rampunggoon and A. Khanna. A Sharp Interface Cartesian Grid Method for Simulating Flows with Compelx Moving Boundarues. *Journal of Computational Physics*, vol. 174, pp. 345-380, 2001.

[12] H.S. Udykumar, Heng-Chuan Kan, Wei Shyy and Roger Tran-Son-Tay. Multiohase Gynamics in Arbitrary Geometries on Fixed Cartesian Grids. *Journal of Computational Physics*, vol. 137, pp. 366-405, 1997.

[13] D.M. Causon, D.M. Ingram, C.G. Mingham, G. Yang and R.V. Pearson. Calculation of Shallow water flows using a Cartesian cut cell approach. *Advances in Water Resources*, vol. 23, pp. 545-562, 2000.

[14] P.G. Tucker and Z. Pan. A Cartesian cut cell method for incompressible viscous flow. *Applied Mechanical Modeling*, vol. 24, pp.591-606, 2000.

[15] D.M. Ingham, D.M. Causon. C.G. Mingham. Developments in Cartesian cut cell methods. *Mathematics and Computers in Simulation*, vol. 61, pp.561-572, 2003.

[16] James J. Quirk. An alternative to unstructured grid for computing gas dynamic flows around arbitrary complex two-dimensional bodies. *Computers Fluids*, vol. 23(1), pp.125-142, 1994.

[17] S. Armfield and R. Street. Modified fractional-step methods for the Navier-Stokes equations. *ANZIAM J.*, vol. 45(E), pp.364-377, 2004.

[18] Alexandre Joel Chorin. Numerical Solution of the Navier-Stokes Equations. *Mathematics of Computation*, vol. 22(104), pp.745-762, 1968.

[19] Robert D. Guy and Aaron L. Fogelson. Stability of approximate projection methods on cell-centered grids. *Journal of Computational Physics*, vol. 203, pp.517-538, 2005.

Numerical Heat Transfer,Part B, vol. 48, pp.1-24, 2005.

[20] J.L. Guermond, P. Minev, Jie Shen. An overview of projection methods for incompressible flows. *Comput. Methods Appl. Mch. Engrg*, vol. 195, pp.6011-6045, 2006.

[21] Danesh Tafti. Alternate Formulations for the Pressure Equation Laplacian on a Collocated Grid for Solving the Unsteady Incompressible Navier-Stokes Equations. *Journal of Computational Physics*, vol. 116, pp. 143-153, 1995.

[22] A.W. Date. Fluid dynamical view of pressure checker boarding problem and smoothing pressure correction on meshes with collocated variables. *Int. J. of Heat and Mass Transfer*, vol. 46, pp. 4885-4898, 2003.

[23] C.M. Rhie and W.L. Chow. Numerical Study of the Turbulent Flow Past an Airfoil with Trailing Edge Separation. *AIAA Journal*, vol. 21(11), pp. 1525-1532, 1983.Bottom of Form

[24] A.W. Date. Solution of Transport equations on unstructured meshes with cell-centered collocated variables. Part I: Discretization. *Int. J. of Heat and Mass Transfer*, vol. 48, pp.1117-1127, 2005.

[25] Philip J. Davis. Interpolation and Approximation. *Brown University*, *First Edition*, 1963.

[26] Joe F. Thompson, Bharat K. Soni and Nigel P. Weather ill. Handbook of Grid Generation. *CRC*, 1998.

[27] A.W. Date. Introduction to Computational Fluid Dynamics. Indian Institute of Technology, Bombay. *Cambridge University Press*, 2005.

[28] B.E. Launder, and T.H. Massey. The Numerical Prediction of Viscous Flow and Heat Transfer in Tube Banks. *J. Heat Transfer*, vol 100, pp. 565–571, 1978

[29] Y. Zang, R.L. Street and J.R. Koseff. A Non-staggered Grid, Fractional Step Method for Time-Dependent Incompressible Navier-Stokes Equations in Curvilinear Coordinates. *Journal of Computational Physics*, vol. 114, pp. 18-33, 1994.

[30] T.H. Kuehn and R.J. Goldstein. Numerical Solution to the Navier-Stokes Equations for Laminar Natural Convection about a Horizontal Isothermal Circular Cylinder. *Int. J. Heat Mass Transfer*, vol. 23, pp.971-979, 1980.

[31] H.M. Badr. Heat Transfer in transient buoyancy driven flow adjacent to a horizontal rod. *Int. J. Heat Mass Transfer*, vol. 30(10) , pp. 1997-2012, 1987.

[32] T. Saitoh, T. Sajiki and K. Maruhara. Bench mark solutions to natural convection heat transfer problem around a horizontal circular cylinder. *Int. J. Heat Mass Transfer*, vol. 36(5) , pp. 1251–1259, 1993

١٢٣

[33] M. Corcione. Correlating equations for free convection heat transfer from horizontal isothermal cylinders set in a vertical array. *Int. J. Heat Mass Transfer*, vol. 48, pp. 3660–3673, 2005.

[34] L. Ma, J. van der Zanden, J. van der Kooi and Frans T.M. Nieuwstadt, Natural convection around a horizontal circular cylinder in infinite space and within confining plates: A finite element solution, *Numerical Heat Transfer, Part A*, vol. 25, pp. 441-446, 1994.

[35] R. Chouikh, A. Guizani, M. Maalej and A. Belghith, Numerical study of the natural convection flow around horizontal isothermal cylinder. Technical Note, *Renewable Energy*, vol. 13(1), pp. 77-88, 1998.

[36] B.A/K Abu-Hijleh, Natural Convection Heat Transfer and Entropy Generation From a Horizontal Cylinder with Baffles. *Journal of Heat Transfer*, vol. 122, pp. 679-692, 2000.

[37] J.H. Merkin. Free Convection Boundary Layers on Cylinders of Elliptic Cross Section. *Journal of Heat Transfer*, vol. 99, pp. 453-457, 1977.

[38] H.M. Badr and K. Shamsher. Free convection from an elliptic cylinder with major axis vertical. *Int. J. Heat and Mass Transfer*, vol. 36, pp.3593-3662, 1993

[39] H. Forrer and R. Jeltsch. A Highr-Order Boundary Treatment for Cartesian-Grid Methods. *Journal of Computational Physics*. vol. 140, pp.259-277, 1998

[40] B. Farouk and S. Guceri. Natural convection from horizontal cylinders in interacting flow folds. *Int. J. Heat and Mass Transfer*, vol. 26(2), pp.231-243, 1983.

[41] Adrian Bejan, Alex J. Fowler and George Stanescu. The optimal spacing between horizontal cylinders in a fixed volume cooled by natural convection. *Int. J. Heat and Mass Transfer*. vol. 38(11), pp.2047-2055, 1995.