



دانشکده علوم ریاضی
گروه ریاضی محض

پروژه کارشناسی ریاضی گرایش هندسه جبری محاسباتی

عنوان

مقدمه‌ای بر انتگرال‌گیری نمادین

پژوهشگر

شکیب شریفی

استاد راهنما

دکتر امیر هاشمی

فهرست مطالب

۱	پیش‌گفتار
۳	فصل ۱: پیش‌نیازهای جبری
۳	۱.۱ گروه، حلقه و ایده‌آل
۸	۲.۱ حلقه چندجمله‌ای‌ها
۹	۳.۱ دامنه صحیح و میدان
۹	۱.۳.۱ دامنه صحیح
۱۲	۲.۳.۱ دامنه تجزیه یکتا
۱۳	۳.۳.۱ دامنه ایده‌آل اصلی
۱۴	۴.۳.۱ دامنه اقلیدسی
۱۵	۵.۳.۱ میدان
۱۶	۶.۳.۱ میدان کسرها
۱۷	۴.۱ الگوریتم‌هایی برای چندجمله‌ای‌ها
۱۸	۱.۴.۱ تقسیم چندجمله‌ای‌ها
۲۱	۲.۴.۱ شبه‌تقسیم
۲۵	۳.۴.۱ الگوریتم اقلیدسی
۲۹	۵.۱ منتج دو چندجمله‌ای
۳۴	فصل ۲: جبر دیفرانسیلی و انتگرال‌گیری توابع گویا
۳۴	۱.۲ گذار از آنالیز به جبر

۲.۲	مشتق جبری و حلقه‌های دیفرانسیلی	۳۵
۳.۲	تجزیه بدون مربع	۴۰
۴.۲	انتگرال جبری و ساختار انتگرال توابع گویا	۴۵
۵.۲	روش هرmit	۴۷
۶.۲	الگوریتم روتشتاین-تراگر	۵۲
۷.۲	الگوریتم جامع انتگرال‌گیری توابع گویا	۵۵
فصل ۳: توسیع‌های میدانی و قضیه لیوویل		
۱.۳	توسیع‌های میدانی	۵۸
۲.۳	توسیع‌های دیفرانسیلی	۵۹
۳.۳	توابع مقدماتی و قضیه لیوویل	۶۱
۴.۳	کاربردهای قضیه لیوویل	۶۴
۱.۴.۳	اثبات درستی روش روتشتاین-تراگر	۶۴
۲.۴.۳	بررسی فرم بسته مقدماتی برای انتگرال‌ها	۶۵
فصل ۴: آشنایی مختصر با انتگرال‌گیری توابع غیرگویا		
۶۹		
فهرست منابع		
۷۴		
واژه‌نامه فارسی به انگلیسی		
۷۵		
واژه‌نامه انگلیسی به فارسی		
۸۰		

پیش‌گفتار

«شایسته نیست که انسان‌های برجسته، ساعات عمر خود را مانند پرده‌ها صرف کار طاقت‌فرسای محاسبه کنند؛ کاری که اگر از ماشین‌ها استفاده می‌شد، به سادگی می‌شد آن را به هر کس دیگری سپرد.»

— گوتفرید ویلهلم لایبنیتس

ریاضیات همواره زبان مشترک علوم و پایه اصلی پیشرفت در مهندسی، محاسبات صنعتی و فناوری‌های نوینی مانند هوش مصنوعی بوده است. در دنیای امروز، مدل‌سازی پدیده‌های فیزیکی و طراحی سیستم‌های پیچیده بدون تکیه بر ابزارهای دقیق ریاضی غیرممکن است. برای حل مسائل ریاضی به کمک کامپیوتر، در رویکرد کلی وجود دارد: رویکرد عددی و رویکرد نمادین. در رویکرد عددی، پاسخ‌ها به صورت تقریبی محاسبه می‌شوند که در بسیاری از کاربردهای مهندسی کارگشا است. اما در رویکرد نمادین، هدف رسیدن به پاسخ دقیق و تحلیلی است، درست مانند کاری که یک ریاضی‌دان روی کاغذ انجام می‌دهد. این نیاز، به توسعه «سیستم‌های جبر کامپیوتری» انجامید. این سیستم‌ها امروزه کاربرد گسترده‌ای در پژوهش‌های علمی، طراحی الگوریتم‌ها و حل معادلات پیچیده دارند و امکان انجام محاسبات دقیق را در مقیاس وسیع فراهم می‌کنند. یکی از مسائل کلاسیک و مهم در ریاضیات، یافتن انتگرال یا همان پادمشتق توابع است. در رویکرد عددی، انتگرال معین یک تابع مانند f روی بازه $[a, b]$ با استفاده از تقریب مساحت زیر نمودار و به شکل $\int_a^b f(x) dx \approx \sum_{i=1}^n f(x_i) \Delta x$ محاسبه می‌شود. اما اگر به دنبال انتگرال نامعین و یافتن ساختار دقیق تابع پاسخ باشیم (یعنی یافتن تابع F به گونه‌ای که $F'(x) = f(x)$)، روش‌های عددی ناکارآمد خواهند بود. در این مرحله رویکرد نمادین وارد عمل می‌شود تا ساختار تحلیلی پاسخ را مشخص کند. پیاده‌سازی انتگرال‌گیری نمادین روی کامپیوتر، نیازمند تغییر نگاه ما به این مسئله است. مفاهیم حساب دیفرانسیل و انتگرال بر پایه حد و پیوستگی بنا شده‌اند که پیاده‌سازی این مفاهیم در منطق کامپیوتر دشوار است. برای حل این مشکل، از حوزه آنالیز ریاضی به جبر مجرد گذر می‌کنیم. در این مسیر،

رشته نوظهور «جبر دیفرانسیلی» چارچوبی فراهم می‌کند تا عملگرهای مشتق و انتگرال را به عنوان نگاشت‌هایی جبری روی یک دامنه مشخص بازتعریف کنیم. به بیان دقیق‌تر، مسئله انتگرال‌گیری به یافتن وارون یک مشتق در یک ساختار جبری مانند میدان دیفرانسیلی تقلیل می‌یابد. این تغییر رویکرد، پایه اصلی کارهای ما در این پروژه است. در این نوشتار، مسیر انتگرال‌گیری نمادین را در چهار فصل طی می‌کنیم. در فصل اول، پیش‌نیازهای جبری شامل مفاهیم حلقه، ایده‌آل و نظریه حلقه چندجمله‌ای‌ها را مرور کرده و ابزارهای محاسباتی مانند الگوریتم اقلیدسی و مفهومی به نام منتج دو چندجمله‌ای را معرفی می‌کنیم. در فصل دوم، با ورود به حلقه‌های دیفرانسیلی، الگوریتم‌های انتگرال‌گیری توابع گویا را بررسی می‌کنیم و روش کاهشی هرمیت و الگوریتم روتشتاین-تراگر را برای استخراج بخش‌های گویا و لگاریتمی پاسخ شرح می‌دهیم. فصل سوم به بررسی توسیع‌های میدانی و توسیع‌های دیفرانسیلی اختصاص دارد تا ساختار توابع مقدماتی را فرمول‌بندی کرده و قضیه مهم لیوویل را اثبات کنیم. در نهایت، در فصل چهارم با عبور از توابع گویا، نمایی کلی از چالش‌های توابع متعالی ارائه داده و الگوریتم ابتکاری ریش-نورمن را معرفی می‌کنیم. باید یادآور شویم که مبحث محاسبات نمادین و جبر دیفرانسیلی بسیار گسترده‌تر و پیچیده‌تر از مطالب این نوشتار است. آنچه در این نوشتار گردآوری شده، بسیار مختصر و ساده بوده و تنها به عنوان یک معرفی اولیه برای ورود به این حوزه تدوین شده است. مطالب این پروژه، بر پایه منابع معتبر این شاخه از ریاضیات تنظیم شده است [۱، ۳، ۲، ۶، ۴، ۵، ۷، ۸].

در پایان، وظیفه خود می‌دانم که از استاد راهنمای بزرگوام، جناب دکتر امیر هاشمی، که با نهایت حوصله و توجه و کمک‌های ارزنده خود، مسیر تدوین این نوشتار را آسان کردند، کمال سپاسگزاری را داشته باشم.

شکیب شریفی

شهریور ۱۴۰۵

فصل ۱

پیش نیازهای جبری

در این فصل، مسیر خود را با مروری بر ساختارهای پایه‌ای مانند گروه، حلقه و ایده‌آل آغاز کرده و سپس با تمرکز بر حلقه چندجمله‌ای‌ها، به معرفی و بررسی ویژگی‌های ساختارهای جبری پیشرفته‌تر مانند دامنه صحیح، دامنه تجزیه یکتا، دامنه ایده‌آل اصلی، دامنه اقلیدسی، میدان و میدان کسرها می‌پردازیم. در نهایت، با ارائه روش‌های محاسباتی مانند الگوریتم تقسیم، الگوریتم شبه‌تقسیم، الگوریتم اقلیدسی و معرفی مفهوم کلیدی منتج دو چندجمله‌ای، زمینه مورد نیاز برای ورود بحث انتگرال‌گیری در فصل‌های آینده را فراهم می‌کنیم. عمده مطالب این فصل، از منابع [۱، ۲، ۳، ۴، ۶] گردآوری شده است.

۱.۱ گروه، حلقه و ایده‌آل

جبر مجرد بر پایه مطالعه ساختارهایی انتزاعی مانند «گروه‌ها» و «حلقه‌ها» استوار است. در این بخش، مروری بر این دو ساختار جبری خواهیم داشت و در ادامه «ایده‌آل‌ها» را که زیرمجموعه‌های مهم و مفیدی از حلقه‌ها هستند، معرفی می‌کنیم.

تعریف ۱.۱.۱. یک گروه $(G, *)$ ، مجموعه ناتهی G با عمل دوتایی $G \times G \rightarrow G : *$ است که در شرایط زیر صدق می‌کند:

$$1. \text{ (شرکت‌پذیری) برای هر } a, b, c \in G \text{ داشته باشیم } a * (b * c) = (a * b) * c.$$

۲. (وجود عضو همانی) عنصری مانند $e \in G$ وجود داشته باشد، به طوری که برای هر $a \in G$ داشته باشیم $a * e = e * a = a$.

۳. (وارون‌پذیری) برای هر $a \in G$ ، عنصر $b \in G$ وجود داشته باشد، به طوری که $a * b = b * a = e$.

گروه $(G, *)$ را آبدلی^۱ (یا جابجایی) می‌گوییم، هرگاه برای هر $a, b \in G$ ، تساوی $a * b = b * a$ برقرار باشد. به سادگی می‌توان اثبات کرد که عضو همانی و وارون هر عنصر در گروه، عناصری یکتا هستند.

تعریف ۲.۱.۱. یک حلقه $(R, +, \cdot)$ ، مجموعه ناتهی R با عمل‌های دوتایی $+: R \times R \rightarrow R$ (جمع) و $\cdot: R \times R \rightarrow R$ (ضرب) است که در شرایط زیر صدق می‌کند:

۱. $(R, +)$ یک گروه آبدلی باشد.

۲. (شرکت‌پذیری $\cdot$) برای هر $a, b, c \in R$ ، داشته باشیم $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

۳. (پخش‌پذیری چپ $\cdot$ نسبت به $+$) برای هر $a, b, c \in R$ ، داشته باشیم $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

۴. (پخش‌پذیری راست $\cdot$ نسبت به $+$) برای هر $a, b, c \in R$ ، داشته باشیم $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

تذکره ۱.۱.۱. جهت سهولت در نوشتن و انتقال مطلب، حلقه $(R, +, \cdot)$ و گروه $(G, *)$ را به ترتیب با مجموعه‌های زمینه آنها یعنی R و G نشان می‌دهیم؛ همچنین، $a \cdot b$ را ab می‌نویسیم. این مورد را برای هر ساختار جبری دیگری که در ادامه معرفی می‌کنیم، به کار خواهیم برد.

حلقه R را جابجایی می‌گوییم، هرگاه برای هر $a, b \in R$ ، رابطه $ab = ba$ برقرار باشد. همچنین R را یک‌دار می‌گوییم، هرگاه دارای عنصر همانی ضرب باشد. این عنصر، همانند عنصر همانی گروه، در صورت وجود، منحصر به فرد است. عنصر همانی عمل جمع حلقه را با نماد 0 و در صورت وجود، عنصر همانی عمل ضرب حلقه را با نماد 1 نشان می‌دهیم.

تعریف ۳.۱.۱. عنصری از حلقه R را که نسبت به عمل ضرب وارون دارد، یک حلقه می‌نامیم. مجموعه همه یک‌ه‌های حلقه R را با نماد R^* نشان می‌دهیم.

^۱نیلز هنریک آبل (Niels Henrik Abel) (۱۸۰۲-۱۸۲۹ میلادی)، ریاضی‌دان برجسته نروژی که کارهای بنیادینی در زمینه جبر و نظریه معادلات انجام داد.

مشابه گروه‌ها، وارون ضربی یک‌های حلقه نیز یکتا هستند. وارون جمعی و وارون ضربی (در صورت وجود) عنصر a از حلقه R را به ترتیب با نمادهای $-a$ و a^{-1} نمایش می‌دهیم.

گزاره ۱.۱.۱. فرض کنیم R یک حلقه و $a, b \in R$ عناصری دلخواه باشند. در این صورت

$$(-1)a = -a, \quad 0 \cdot a = a \cdot 0 = 0, \quad a(-b) = -ab, \quad (-a)(-b) = ab.$$

در این نوشتار همه حلقه‌ها را یک‌دار و جابجایی در نظر می‌گیریم، مگر این که در جایی خلاف آن ذکر شود. مثال ۱.۱.۱. مجموعه‌های اعداد طبیعی ($\mathbb{N}$)، صحیح ($\mathbb{Z}$)، گویا ($\mathbb{Q}$)، حقیقی ($\mathbb{R}$) و مختلط ($\mathbb{C}$) را در نظر می‌گیریم. مجموعه‌های $\mathbb{Z}$ ، $\mathbb{Q}$ ، $\mathbb{R}$ و $\mathbb{C}$ با اعمال معمول جمع و ضرب تشکیل حلقه می‌دهند، اما $\mathbb{N}$ به دلیل نداشتن وارون جمعی (برای مثال $-1 \notin \mathbb{N}$) حلقه نیست. مجموعه یک‌های این حلقه‌ها به صورت زیر است:

$$\mathbb{Z}^* = \{1, -1\}, \quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\}.$$

قرارداد ۱.۱.۱. در ادامه این نوشتار، فرض می‌کنیم که $0 \in \mathbb{N}$.

مثال ۲.۱.۱. برای عدد صحیح $n > 1$ ، مجموعه $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ را در نظر می‌گیریم که در آن نماد $[a]$ ، رده هم‌ارزی عدد a را به پیمانه n مشخص می‌کند. این مجموعه همراه با عمل‌های جمع و ضرب رده‌ها به صورت $[a] + [b] = [a+b]$ و $[a] \cdot [b] = [ab]$ ، تشکیل یک حلقه می‌دهد.

در بررسی حلقه‌ها، گاهی جمع کردن مکرر عنصر همانی ضرب با خودش به عنصر صفر منتهی می‌شود. این ویژگی ساختاری، سبب تعریف مفهومی به نام «مشخصه» می‌شود که نقش مهمی در طبقه‌بندی و رفتارهای محاسباتی حلقه‌ها ایفا می‌کند.

تعریف ۴.۱.۱. فرض کنیم R یک حلقه باشد. مشخصه حلقه R که با نماد $\text{char}(R)$ نمایش داده می‌شود، برابر با کوچکترین عدد طبیعی مثبت n است که در تساوی زیر صدق کند:

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ بار}} = n \cdot 1 = 0.$$

اگر هیچ عددی با این ویژگی وجود نداشته باشد، تعریف می‌کنیم $\text{char}(R) = 0$.

مثال ۳.۱.۱. در حلقه‌های $\mathbb{Z}$, $\mathbb{Q}$ و $\mathbb{R}$ جمع مکرر عدد ۱، هرگز صفر نمی‌شود، در نتیجه

$$\text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = 0.$$

در حلقه $\mathbb{Z}_n$ ، کمترین دفعات جمع رده $[1]$ برای رسیدن به عنصر صفر برابر با n است، بنابراین $\text{char}(\mathbb{Z}_n) = n$.

برای شناخت بهتر ساختار حلقه‌ها و درک مفاهیمی مانند بخش‌پذیری و تجزیه، نیازمند بررسی دسته ویژه‌ای از زیرمجموعه‌ها به نام «ایده‌آل» هستیم. در واقع، ایده‌آل‌ها خواصی مانند زوجیت و مضرب ۳ بودن در اعداد صحیح را به ساختارهای مجردتر تعمیم می‌دهند.

تعریف ۵.۱.۱. زیرمجموعه غیرتهی I از حلقه R را یک ایده‌آل می‌گوییم، هرگاه در شرایط زیر صدق کند:

$$1. \text{ به ازای هر } a, b \in I, a + b \in I.$$

$$2. \text{ برای هر } a \in I \text{ و } r \in R, ra \in I.$$

هر ایده‌آل I از حلقه R با عمل جمع و صفر حلقه، تشکیل یک گروه می‌دهد. برای بیان دقیق‌تر روابط بین عناصر یک حلقه و ایده‌آل‌هایی که توسط آن‌ها تولید می‌شوند، ابتدا نیازمند تعریف مفهوم «عاد کردن» در حلقه‌ها هستیم.

تعریف ۶.۱.۱. فرض کنیم R یک حلقه باشد و $a, b \in R$. اگر $k \in R$ وجود داشته باشد، به طوری که $ka = b$ می‌گوییم a را عاد می‌کند و این رابطه را به صورت $a \mid b$ نمایش می‌دهیم.

تعریف ۷.۱.۱. فرض کنیم $H \neq \emptyset$ یک زیرمجموعه حلقه R باشد. ایده‌آل تولید شده توسط H را اشتراک همه ایده‌آل‌های R که شامل H هستند تعریف می‌کنیم و با نماد $\langle H \rangle$ نمایش می‌دهیم. همچنین اگر داشته باشیم $H = \{h_1, h_2, \dots, h_n\}$ ، ایده‌آل تولید شده توسط H را با نماد $\langle h_1, h_2, \dots, h_n \rangle$ نمایش می‌دهیم.

تعریف ۸.۱.۱. ایده‌آل I از حلقه R را اصلی می‌گوییم، هرگاه توسط یک عنصر تولید شود. به عبارتی دیگر، برای یک $a \in R$ ، رابطه $I = \langle a \rangle$ برقرار باشد.

گزاره ۲.۱.۱. فرض کنیم R یک حلقه باشد و $\emptyset \neq H \subseteq R$. در این صورت

$$\langle H \rangle = \left\{ \sum_{k=1}^n r_k h_k \mid n \in \mathbb{N}, \quad \forall 1 \leq k \leq n \quad r_k \in R, \quad h_k \in H \right\}.$$

اثبات. مجموعه سمت راست تساوی بالا را با I نمایش می‌دهیم. ابتدا ثابت می‌کنیم که I یک ایده‌آل حلقه R است. به ازای $1 \in R$ و هر $h \in H$ ، داریم $1 \cdot h = h \in I$ ، بنابراین $1 \neq \emptyset$. فرض کنیم $a = \sum_{k=1}^n r_k h_k$ و $b = \sum_{k=1}^{n'} r'_k h'_k$ دو عنصر دلخواه I و r نیز یک عنصر دلخواه R باشند، در این صورت خواهیم داشت

$$a+b = \sum_{k=1}^n r_k h_k + \sum_{k=1}^{n'} r'_k h'_k = \sum_{k=1}^{n+n'} r''_k h''_k \quad \begin{cases} r_k = r''_k, h_k = h''_k & 1 \leq k \leq n \\ r'_{k-n} = r''_k, h'_{k-n} = h''_k & n+1 \leq k \leq n+n' \end{cases},$$

$$ra = \sum_{k=1}^n \overbrace{(r \cdot r_k)}^{\in R} h_k.$$

در نتیجه $a+b$ و ra نیز عضو I هستند، که نشان‌دهنده آن است که I یک ایده‌آل R است. حال نشان می‌دهیم $\langle H \rangle = I$.

$\subseteq$ واضح است که به ازای $1 \in R$ و هر $h \in H$ ، داریم $1 \cdot h = h \in I$ ، بنابراین $H \subseteq I$ و در نتیجه I یک ایده‌آل شامل H است. بنابراین $\langle H \rangle \subseteq I$.

$\supseteq$ فرض کنیم J یک ایده‌آل R ، که شامل H است، باشد. نشان می‌دهیم $I \subseteq J$. عنصر $a \in I$ را در نظر می‌گیریم:

$$a = \underbrace{r_1 h_1}_{\in J} + \underbrace{r_2 h_2}_{\in J} + \cdots + \underbrace{r_n h_n}_{\in J} \in I.$$

□

از آنجا که a به صورت جمع عناصری از J است، داریم $a \in J$.

مثال ۴.۱.۱. در حلقه $\mathbb{Z}$ ، طبق گزاره ۲.۱.۱، ایده‌آل $\langle 4, 6 \rangle$ شامل تمام ترکیب‌های خطی این دو عضو است که در نهایت ایده‌آل اصلی $\langle 2 \rangle$ را می‌سازد:

$$\langle 4, 6 \rangle = \{4r_1 + 6r_2 \mid r_1, r_2 \in \mathbb{Z}\} = \langle 2 \rangle = \{\dots, -4, -2, 0, 2, 4, \dots\}.$$

۲.۱ حلقه چندجمله‌ای‌ها

چندجمله‌ای‌ها از مفاهیم محوری و کلیدی محاسبات نمادین هستند. در این بخش، چندجمله‌ای‌ها را از دیدگاه جبری و به عنوان عناصر یک حلقه بررسی کرده و نمادگذاری‌های استاندارد آن‌ها را معرفی می‌کنیم. مجموعه $R[x]$ را شامل همه چندجمله‌ای‌های تک‌متغیره با ضرایب در R و متغیر x در نظر می‌گیریم. به بیان دیگر

$$R[x] = \left\{ \sum_{k=0}^n a_k x^k \mid n \in \mathbb{N}, \forall 0 \leq k \leq n \ a_k \in R \right\}.$$

به ازای هر $Q = \sum_{j=0}^n b_j x^j, P = \sum_{i=0}^m a_i x^i \in R[x]$ که $a_m, b_n \neq 0$ ، عملگرهای جمع و ضرب روی $R[x]$ را به این شکل تعریف می‌کنیم:

$$P + Q = \sum_{i=0}^m a_i x^i + \sum_{j=0}^n b_j x^j = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k,$$

$$P \cdot Q = \left(\sum_{i=0}^m a_i x^i \right) \cdot \left(\sum_{j=0}^n b_j x^j \right) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^k a_l b_{k-l} \right) x^k.$$

ذکر این نکته نیز لازم است که قرارداد می‌کنیم برای هر اندیس $k > m$ ، مقدار $a_k = 0$ و برای هر $k > n$ ، مقدار $b_k = 0$. همچنین برای حفظ جامعیت عملیات روی حلقه، قرارداد می‌کنیم که جمع هر چندجمله‌ای با چندجمله‌ای صفر برابر با خود آن چندجمله‌ای، و ضرب آن در چندجمله‌ای صفر برابر با صفر است.

گزاره ۱.۲.۱. مجموعه $R[x]$ با عمل جمع و ضرب تعریف شده، تشکیل یک حلقه می‌دهد.

اثبات. عنصر $0 \in R$ عضو همانی جمع و عنصر $1 \in R$ عضو همانی ضرب $R[x]$ هستند. وارون جمعی هر چندجمله‌ای P در $R[x]$ ، چندجمله‌ای $-P = \sum_{k=0}^n (-a_k) x^k$ است. جابجایی و شرکت‌پذیر بودن عمل جمع و ضرب و همچنین خاصیت پخش‌پذیری، به سادگی اثبات می‌شوند و به همین دلیل از آنها صرف‌نظر می‌کنیم. $\square$

تعریف ۱.۲.۱. فرض کنیم R یک حلقه و $0 \neq P = a_n x^n + \dots + a_0$ یک چندجمله‌ای دلخواه در $R[x]$ باشد، به طوری که $a_n \neq 0$. در این صورت درجه P ، که با $\deg(P)$ نشان می‌دهیم، برابر با n تعریف می‌شود. اگر $P = 0$ ، قرارداد می‌کنیم $\deg(0) = -\infty$.

تعریف ۲.۲.۱. فرض کنیم R یک حلقه و $0 \neq P = a_n x^n + \dots + a_0$ یک چندجمله‌ای دلخواه در $R[x]$ باشد، به طوری که $a_n \neq 0$. در این صورت $a_n x^n$ ، x^n و a_n را به ترتیب جمله پیشرو، تک جمله‌ای پیشرو و ضریب پیشرو P می‌نامیم و با نمادهای $LT(P)$ ، $LM(P)$ و $LC(P)$ نمایش می‌دهیم. همچنین اگر $LC(P) = 1$ ، چندجمله‌ای P را تکین می‌نامیم.

مثال ۱.۲.۱. چندجمله‌ای $P = -5x^4 + 2x^2 - 7$ را در حلقه $\mathbb{Z}[x]$ در نظر می‌گیریم. در این صورت مقادیر زیر حاصل می‌شوند:

$$\deg(P) = 4, \quad LC(P) = -5, \quad LM(P) = x^4, \quad LT(P) = -5x^4.$$

۳.۱ دامنه صحیح و میدان

در این بخش به بررسی شرایط انجام عمل تقسیم در حلقه می‌پردازیم و ساختارهای جبری دیگری همچون دامنه صحیح، دامنه تجزیه یکتا، دامنه ایده‌آل اصلی، دامنه اقلیدسی، میدان و میدان کسرها را معرفی می‌کنیم و روابط میان آنها را تشریح خواهیم کرد.

۱.۳.۱ دامنه صحیح

تعریف ۱.۳.۱. حلقه غیرصفر D را یک دامنه صحیح می‌گوییم، اگر برای هر $a, b \in D$ داشته باشیم

$$ab = 0 \implies a = 0 \quad \text{یا} \quad b = 0 \quad (\text{خاصیت حاصل ضرب صفر}).$$

مثال ۱.۳.۱. حلقه‌های $\mathbb{Z}$ ، $\mathbb{Q}$ و $\mathbb{R}$ دامنه صحیح هستند، اما حلقه $\mathbb{Z}_6$ یک دامنه صحیح نیست، زیرا عناصر غیرصفر $[2], [3] \in \mathbb{Z}_6$ وجود دارند که رابطه $[2] \cdot [3] = [0]$ را (به پیمانه ۶) نتیجه می‌دهند.

قضیه ۱.۳.۱. اگر D یک دامنه صحیح باشد، آنگاه $D[x]$ نیز یک دامنه صحیح است.

اثبات. فرض کنیم $P = \sum_{k=0}^m a_k x^k$ و $Q = \sum_{k=0}^n b_k x^k$ دو چندجمله‌ای غیرصفر از $D[x]$ باشند، به طوری که $a_m, b_n \neq 0$. اگر رابطه $P \cdot Q = 0$ برقرار باشد، آنگاه داریم $\text{LC}(P \cdot Q) = a_m b_n = 0$ ، که با دامنه صحیح بودن D در تناقض است، بنابراین $P \cdot Q \neq 0$. $\square$

نتیجه ۱.۳.۱. فرض کنیم D یک دامنه صحیح باشد. در این صورت به ازای هر $P, Q \in D[x]$ ، داریم

$$\deg(P \cdot Q) = \deg(P) + \deg(Q).$$

«بزرگترین مقسوم‌علیه مشترک» دو عدد صحیح جزو مفاهیم اولیه نظریه اعداد است و در جبر مجرد نیز تعریفی عمومی و کلی‌تر برای آن بیان می‌شود.

تعریف ۲.۳.۱. فرض کنیم D یک دامنه صحیح و $a, b \in D$ ، عناصری دلخواه باشند، به طوری که حداقل یکی از آنها مخالف صفر است. در این صورت، d را یک بزرگترین مقسوم‌علیه مشترک (ب.م.م.) a و b می‌گوییم، هرگاه

$$1. \quad d \mid b \text{ و } d \mid a.$$

$$2. \quad \text{اگر } c \in D \text{ وجود داشته باشد که } c \mid a \text{ و } c \mid b, \text{ آنگاه } c \mid d.$$

تذکر ۱.۳.۱. در تعریف ۲.۳.۱، اگر $a = b = 0$ ، ب.م.م. a و b تعریف نمی‌شود، زیرا هر عنصری در D صفر را عاد می‌کند. در ادامه این نوشتار، فرض می‌کنیم که a و b هر دو صفر نیستند.

گزاره ۱.۳.۱. در یک دامنه صحیح، یک ب.م.م. دو عنصر (در صورت وجود) در حد ضرب یک عنصر وارون‌پذیر یکتاست.

اثبات. فرض کنیم D یک دامنه صحیح باشد و $a, b \in D$. فرض کنیم d_1 و d_2 ب.م.م.هایی برای a و b باشند، در این صورت، داریم $d_2 \mid d_1$ و $d_1 \mid d_2$. بنابراین عناصری مانند $k_1, k_2 \in D$ وجود دارند، به طوری که $d_2 = k_1 d_1$ و $d_1 = k_2 d_2$. در نتیجه، $d_1 = k_2 k_1 d_1$ و بنابراین رابطه $d_1(1 - k_2 k_1) = 0$ حاصل می‌شود. از آنجا که D یک دامنه صحیح است، داریم $k_2 k_1 = 1$ که نشان‌دهنده این است که $k_1, k_2 \in D^*$. $\square$

همان‌طور که ملاحظه شد، به طور کلی الزامی بر وجود یا یکتایی ب.م.م. دو عنصر در یک دامنه صحیح نیست. بنابراین استفاده از یک نماد برای نمایش ب.م.م. خوش‌تعریف نیست. ما با تساهل، از نماد $\gcd(a, b)$ برای

نمایش یک ب.م.م. a و b از نماد معمول تساوی $(=)$ ، برای نشان دادن رابطه «برابر بودن در حد ضرب یک» استفاده خواهیم کرد.

مثال ۲.۳.۱. در حلقه $\mathbb{Z}$ ، برای دو عنصر ۱۲ و ۱۸، داریم $\gcd(12, 18) = 6$ یا $\gcd(12, 18) = -6$ ، از آنجا که این دو مقدار در حد ضرب در یک عنصر وارون‌پذیر $\mathbb{Z}$ (یعنی ۱ یا -۱) با هم برابرند. در حلقه چندجمله‌ای‌های $\mathbb{Q}[x]$ ، برای دو چندجمله‌ای $x^2 - 1$ و $x^2 - x$ ، هر عنصر در مجموعه $\{a(x-1) \mid a \in \mathbb{Q}^*\}$ یک ب.م.م. به شمار می‌رود.

در یک دامنه صحیح، همانند حلقه اعداد صحیح، بررسی اینکه چگونه یک عنصر به عناصر کوچکتر تجزیه می‌شود اهمیت بالایی دارد. برای بیان مفهوم تجزیه در حلقه‌ها و رسیدن به دامنه‌هایی که در آن‌ها تجزیه یکتاست، ابتدا باید معادل‌های تعمیم‌یافته اعداد اول را تعریف کنیم.

تعریف ۳.۳.۱. فرض کنیم D یک دامنه صحیح باشد. عنصر غیر صفر $p \in D \setminus D^*$ را یک عنصر اول می‌گوییم، هرگاه به ازای $a, b \in D$ داشته باشیم

$$p \mid ab \implies p \mid a \quad \text{یا} \quad p \mid b.$$

مثال ۳.۳.۱. عنصر ۵ در حلقه $\mathbb{Z}$ یک عنصر اول است اما همین عنصر در حلقه $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ که $i = \sqrt{-1}$ ، اول نیست، زیرا به صورت $5 = (1+2i)(1-2i)$ تجزیه می‌شود.

تعریف ۴.۳.۱. فرض کنیم D یک دامنه صحیح باشد. عنصر غیر صفر $a \in D \setminus D^*$ را یک عنصر تحویل‌ناپذیر می‌گوییم، هرگاه به ازای $b, c \in D$ داشته باشیم

$$a = bc \implies b \in D^* \quad \text{یا} \quad c \in D^*.$$

مثال ۴.۳.۱. چندجمله‌ای $x^2 + 1$ در حلقه $\mathbb{R}[x]$ یک عنصر تحویل‌ناپذیر است اما همین چندجمله‌ای در حلقه $\mathbb{C}[x]$ تحویل‌ناپذیر نیست، زیرا به صورت حاصل ضرب دو عنصر غیریکه $x^2 + 1 = (x-i)(x+i)$ تجزیه می‌شود.

قضیه ۱.۳.۱. در یک دامنه صحیح، هر عنصر اول، یک عنصر تحویل‌ناپذیر است.

اثبات. فرض کنیم D یک دامنه صحیح و $p \in D$ یک عنصر اول باشد. فرض کنیم برای عناصر دلخواه $a, b \in D$ داشته باشیم $p = ab$. از آنجا که p اول است، طبق تعریف داریم $p \mid ab$. بدون کاستن از کلیت، فرض می‌کنیم که $p \mid a$ ، بنابراین برای یک $k \in D$ داریم $a = kp$ و در این صورت

$$p = ab = (pk)b \implies p(1 - kb) = 0.$$

طبق خاصیت حاصل ضرب صفر D ، خواهیم داشت $kb = 1$ ، که نشان‌دهنده این است که b عنصری یکه است. $\square$

مثال ۵.۳.۱. عکس قضیه بالا به طور کلی برقرار نیست، یعنی در یک دامنه صحیح، هر عنصر تحویل‌ناپذیر، لزوماً اول نیست. برای مثال، در دامنه صحیح $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ، عنصر ۳ یک عنصر تحویل‌ناپذیر است، اما یک عنصر اول نیست. زیرا $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \mid 9$ ، در حالی که ۳ هیچ‌کدام از این دو عنصر را عاد نمی‌کند.

۲.۳.۱ دامنه تجزیه یکتا

همان‌طور که در مثال قبل دیدیم، در یک دامنه صحیح دلخواه، تجزیه یک عنصر به عوامل تحویل‌ناپذیر لزوماً منحصر به فرد نیست. این موضوع، انگیزه‌ای برای تعریف دسته مهمی از دامنه‌هاست که در آن‌ها عمل تجزیه همانند تجزیه اعداد صحیح به عوامل اول است.

تعریف ۵.۳.۱. دامنه صحیح D را یک دامنه تجزیه یکتا (UFD) می‌گوییم، هرگاه برای هر عنصر غیرصفر $a \in D \setminus D^*$ ، داشته باشیم

$$1. \quad a = p_1 p_2 \cdots p_n \quad \text{به طوری که } p_1, p_2, \dots, p_n \text{ عناصری تحویل‌ناپذیر در } D \text{ باشند.}$$

۲. اگر $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ ، دو تجزیه a به عناصر تحویل‌ناپذیر باشند، آنگاه $m = n$ و یک نگاشت دوسویی $\varphi : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ موجود باشد، به طوری که هر p_i با $q_{\varphi(i)}$ در حد ضرب یک‌ه، برابر باشد.

مثال ۶.۳.۱. طبق «قضیه اساسی حساب»^۱ در نظریه اعداد، حلقه اعداد صحیح $\mathbb{Z}$ یک دامنه تجزیه یکتا است. حلقه $\mathbb{Z}[\sqrt{-5}]$ ، یک دامنه تجزیه یکتا نیست. برای نمونه، در این حلقه عنصر ۹ دارای دو تجزیه متفاوت به عناصر تحویل‌ناپذیر است:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

قضیه ۲.۳.۱. در یک دامنه تجزیه یکتا، هر عنصر تحویل‌ناپذیر، یک عنصر اول است.

اثبات. فرض کنیم D یک دامنه تجزیه یکتا و p یک عنصر تحویل‌ناپذیر D باشد، به طوری که برای عناصر دلخواه $a, b \in D$ ، داشته باشیم $p \mid ab$. بنابراین یک $k \in D$ وجود دارد که $ab = kp$. حال عناصر a ، b و k را به حاصل ضرب عناصر تحویل‌ناپذیر در D تجزیه می‌کنیم:

$$a = p_1 p_2 \cdots p_l, \quad b = q_1 q_2 \cdots q_m, \quad k = r_1 r_2 \cdots r_n.$$

در نتیجه خواهیم داشت

$$ab = p_1 p_2 \cdots p_l q_1 q_2 \cdots q_m = kp = r_1 r_2 \cdots r_n p.$$

از سوی دیگر، از آنجا که در D تجزیه هر عنصری یکتاست، می‌توان نتیجه گرفت که $l + m = n + 1$ و به ازای یک i یا j ، عنصر p در حد ضرب یکه، با p_i یا q_j برابر است؛ بنابراین $p \mid a$ یا $p \mid b$. $\square$

قضیه ۲.۳.۱. در یک دامنه تجزیه یکتا، هر دو عنصر دلخواه، دارای بزرگترین مقسوم‌علیه مشترک هستند.

$\square$

اثبات. به [۲، گزاره ۱۳، صفحه ۲۸۷] مراجعه شود.

۳.۳.۱ دامنه ایده‌آل اصلی

تعریف ۶.۳.۱. دامنه صحیحی را که هر ایده‌آل آن اصلی باشد، دامنه ایده‌آل اصلی (PID) می‌گوییم.

^۱قضیه اساسی حساب (Fundamental Theorem of Arithmetic). این قضیه بیان می‌کند که هر عدد صحیح بزرگتر از ۱، یا اول است یا می‌توان آن را به صورت یکتا (صرف‌نظر از ترتیب عوامل) به حاصل ضرب اعداد اول تجزیه کرد.

مثال ۷.۳.۱. حلقه $\mathbb{Z}$ یک دامنه ایده‌آل اصلی است اما حلقه $\mathbb{Z}[x]$ چنین نیست. به عنوان مثال، ایده‌آل $\langle 2, x \rangle$ توسط هیچ عنصر واحدی تولید نمی‌شود.

۴.۳.۱ دامنه اقلیدسی

اکنون با گونه خاصی از دامنه‌های صحیح آشنا می‌شویم که تعمیم الگوریتم تقسیم در اعداد صحیح برای حلقه‌هاست.

تعریف ۷.۳.۱. دامنه صحیح D را یک دامنه اقلیدسی^۱ می‌گوییم، هرگاه تابع $g : D \setminus \{0\} \rightarrow \mathbb{N}$ موجود باشد، به طوری که

$$1. \text{ برای هر دو عنصر ناصفر } a, b \in D, \text{ داشته باشیم } g(a) \leq g(ab).$$

۲. برای $a, b \in D$ که شرط $b \neq 0$ برقرار است، عناصر $q, r \in D$ وجود داشته باشند، به طوری که $a = bq + r$ و $r = 0$ یا $g(r) < g(b)$.

در تعریف ۷.۳.۱، تابع g را یک تابع ارزیاب و q و r را به ترتیب خارج قسمت و باقیمانده می‌گوییم.

مثال ۸.۳.۱. حلقه‌های $\mathbb{Q}[x]$ ، $\mathbb{R}[x]$ و $\mathbb{C}[x]$ با تابع ارزیاب $\deg$ دامنه اقلیدسی هستند، اما $\mathbb{Z}[x]$ چنین نیست. به عنوان مثال، برای $2x, x^2 \in \mathbb{Z}[x]$ ، هیچ چندجمله‌ای‌های Q و R در $\mathbb{Z}[x]$ ، در رابطه زیر صدق نمی‌کنند:

$$x^2 = (2x)Q + R \quad (R = 0 \text{ یا } \deg(R) < \deg(2x)).$$

قضیه ۳.۳.۱. هر دامنه اقلیدسی، یک دامنه ایده‌آل اصلی است.

اثبات. فرض کنیم D یک دامنه اقلیدسی و I یک ایده‌آل از آن باشد، به طوری که $I \neq \{0\}$.

مجموعه $A = \{g(a) \mid 0 \neq a \in I\}$ را در نظر می‌گیریم، این مجموعه، یک زیرمجموعه غیرتهی از $\mathbb{N}$ است و طبق اصل خوش‌ترتیبی^۲، دارای کوچک‌ترین عضو است. فرض کنیم عنصر $b \in D$ به گونه‌ای باشد که رابطه $g(b) = \min(A)$ برقرار شود. ثابت می‌کنیم که $I = \langle b \rangle$. اگر $a \in I$ عنصری باشد که رابطه $a \nmid b$ را

^۱ اقلیدس (Euclid) (حدود ۳۲۵-۲۶۵ پیش از میلاد)، ریاضی‌دان برجسته یونان باستان که وی را پدر علم هندسه می‌نامند و نظام اصل موضوعی را در ریاضیات پایه‌گذاری کرد.

^۲ این اصل بیان می‌کند که برای هر زیرمجموعه ناتهی از اعداد طبیعی، حتماً یک عضو کوچکتر از دیگر اعضا یافت می‌شود.

نتیجه دهد، آنگاه به ازای $q, r \in D$ خواهیم داشت $a = bq + r$ ، به طوری که $g(r) < g(b)$. از سوی دیگر، عنصر r در $a - bq = r$ قرار دارد، اما این با کمینه بودن $g(b)$ در A در تناقض است، بنابراین به ازای هر $a \in I$ داریم $a \mid b$. $\square$

قضیه ۴.۳.۱. هر دامنه ایده‌آل اصلی، یک دامنه تجزیه یکتا است.

اثبات. به [۶، قضیه ۵.۲، صفحه ۱۱۲] مراجعه شود. $\square$

قضیه ۵.۳.۱. فرض کنیم D یک دامنه ایده‌آل اصلی باشد. در این صورت به ازای هر $a, b \in D$ داریم، $\langle a, b \rangle = \langle \gcd(a, b) \rangle$.

اثبات. از آنجا که D یک دامنه ایده‌آل اصلی است، به ازای یک $d \in D$ داریم $\langle a, b \rangle = \langle d \rangle$. طبق قضایای ۴.۳.۱ و ۲.۳.۱ می‌دانیم که $\gcd(a, b)$ وجود دارد. نشان می‌دهیم که $d = \gcd(a, b)$. از آنجا که $a, b \in \langle d \rangle$ مشخص است که $a \mid d$ و $b \mid d$. حال فرض کنیم $c \in D$ عنصری دلخواه باشد که $a \mid c$ و $b \mid c$ ؛ بنابراین به ازای $k_1, k_2 \in D$ داریم $a = k_1 c$ و $b = k_2 c$. از سوی دیگر، از آنجا که $d \in \langle a, b \rangle$ ، طبق گزاره ۲.۱.۱، به ازای $k'_1, k'_2 \in D$ خواهیم داشت $d = k'_1 a + k'_2 b$ ، که در کل نتیجه می‌گیریم $d = k'_1 k_1 c + k'_2 k_2 c$ و $c \mid d$. $\square$

۵.۳.۱ میدان

برای اینکه بتوانیم در حلقه چندجمله‌ای‌ها عمل تقسیم را بدون محدودیت‌هایی مانند مقسوم‌علیه‌های صفر یا عناصر وارون‌ناپذیر انجام دهیم، به ساختاری نیاز داریم که در آن عمل ضرب برای تمام عناصر غیرصفر، وارون‌پذیر باشد. «میدان» چنین ساختاری است و زمینه اصلی الگوریتم تقسیم چندجمله‌ای‌ها را فراهم می‌کند.

تعریف ۸.۳.۱. به حلقه‌ای که هر عنصر غیرصفر آن، نسبت به عمل ضرب وارون داشته باشد، یک میدان می‌گوییم.

مثال ۹.۳.۱. حلقه‌های $\mathbb{Q}$ ، $\mathbb{R}$ و $\mathbb{C}$ میدان هستند اما حلقه چندجمله‌ای‌های $\mathbb{Q}[x]$ میدان نیست، زیرا هر عنصر از آن که دارای درجه حداقل ۱ است، وارون‌پذیر نخواهد بود.

گزاره ۲.۳.۱. هر میدان، یک دامنه صحیح است.

اثبات. فرض کنیم K یک میدان و $a, b \in K$ دو عنصر دلخواه باشند، به طوری که $ab = 0$. بدون کاستن از کلیت، فرض می‌کنیم $a \neq 0$. در این صورت با ضرب با a^{-1} در دو طرف تساوی، خواهیم داشت $b = 0$. $\square$

گزاره ۳.۳.۱. هر میدان، یک دامنه اقلیدسی است.

اثبات. فرض کنیم K یک میدان باشد. تابع ارزیاب را تابع ثابت ۱ در نظر می‌گیریم و به ازای هر $a, b \in K$ که $b \neq 0$ ، قرار می‌دهیم $q = ab^{-1}$ و $r = 0$ ، بنابراین تساوی $a = bq + r$ حاصل می‌شود. $\square$

۶.۳.۱ میدان کسرها

همان‌طور که می‌دانیم حلقه $\mathbb{Z}$ میدان نیست اما زیرمجموعه میدان $\mathbb{Q}$ است و عناصر آن به صورت کسرهایی با صورت و مخرج صحیح هستند. این موضوع در جبر، الهام‌بخش چنین ایده‌ای است که بتوانیم یک حلقه (یا به طور دقیق‌تر یک دامنه صحیح) را به میدانی شامل آن گسترش داد.

تعریف ۹.۳.۱. فرض کنیم D یک دامنه صحیح باشد. مجموعه $\text{Frac}(D)$ را شامل رده‌های هم‌ارزی از زوج‌های مرتب (a, b) تعریف می‌کنیم که در آن $a, b \in D$ و $b \neq 0$. این رده‌های هم‌ارزی را با نماد کسر یعنی $\frac{a}{b}$ نمایش می‌دهیم، به طوری که دو کسر $\frac{a}{b}$ و $\frac{c}{d}$ با یکدیگر برابرند هرگاه $ad = bc$. عمل‌های جمع و ضرب روی این مجموعه به صورت زیر تعریف می‌شوند:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

گزاره ۴.۳.۱. مجموعه $\text{Frac}(D)$ همراه با عمل‌های جمع و ضرب تعریف‌شده، تشکیل یک میدان می‌دهد که آن را میدان کسرهاهای دامنه صحیح D می‌نامیم.

اثبات. خوش‌تعریف بودن عمل‌های جمع و ضرب، شرکت‌پذیری، جابجایی و خاصیت پخش‌پذیری مستقیماً از خواص دامنه صحیح D نتیجه می‌شوند. عناصر همانی جمع و ضرب در این ساختار به ترتیب به صورت $\frac{1}{1}$ و $\frac{0}{1}$ هستند. همچنین وارون جمعی کسر $\frac{a}{b}$ برابر با کسر $\frac{-a}{b}$ خواهد بود. حال فرض کنیم $\frac{a}{b}$ یک عنصر ناصفر دلخواه باشد، بنابراین $a \neq 0$ ؛ در این صورت زوج مرتب (b, a) خوش‌تعریف بوده و کسر $\frac{b}{a}$ در $\text{Frac}(D)$ موجود است که در رابطه زیر صدق می‌کند:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

بنابراین هر عنصر ناصفر دارای وارون ضربی است و مجموعه $\text{Frac}(D)$ تشکیل یک میدان می‌دهد. $\square$

با توجه به ساختار بالا، می‌توان هر عنصر دلخواه a از دامنه صحیح D را با کسر $\frac{a}{1}$ در میدان کسرها $\text{Frac}(D)$ هم‌ارز دانست. بر همین اساس، عناصر همانی جمع و ضرب در این میدان به ترتیب به صورت $\frac{0}{1}$ و $\frac{1}{1}$ هستند. همچنین وارون ضربی هر کسر ناصفر $\frac{a}{b}$ در این ساختار، برابر با کسر $\frac{b}{a}$ خواهد بود. به عنوان یک نتیجه، برای هر کسر ناصفر $\frac{b}{1}$ ، وارون ضربی به شکل $\frac{1}{b}$ به دست می‌آید.

تذکر ۲.۳.۱. باید توجه داشت که نماد کسر $\frac{a}{b}$ در میدان کسرها $\text{Frac}(D)$ نباید با تقسیم در دامنه صحیح D اشتباه گرفته شود. در یک دامنه صحیح، عمل تقسیم همواره امکان‌پذیر نیست. در واقع، نماد $\frac{a}{b}$ در اینجا نشان‌دهنده یک کلاس هم‌ارزی از زوج‌های مرتب (a, b) است و نه حاصل عمل تقسیم a بر b . با این وجود، پس از ساخت و گسترش میدان کسرها، این نماد با عملگر تقسیم در میدان جدید کاملاً سازگار عمل خواهد کرد.

مثال ۱۰.۳.۱. آشناترین مثال برای این مفهوم، ساختن میدان اعداد گویا از حلقه اعداد صحیح است، به عبارت دیگر $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$. به عنوان یک نمونه پرکاربرد در محاسبات نمادین، دامنه صحیح $K[x]$ را به طوری که K یک میدان باشد، در نظر می‌گیریم. میدان کسرها $\text{Frac}(K[x])$ این دامنه صحیح را با نماد $K(x)$ نشان می‌دهیم که به آن **میدان توابع گویا** می‌گوییم و عناصر آن همان کسرها $\frac{P}{Q}$ هستند که $P, Q \in K[x]$ و $Q \neq 0$.

تذکر ۳.۳.۱. قائل شدن رابطه تساوی برای میدان کسرها $\text{Frac}(D)$ با یک میدان شناخته‌شده K به شکل $K = \text{Frac}(D)$ (مانند $\mathbb{Q} = \text{Frac}(\mathbb{Z})$ در مثال ۱۰.۳.۱)، از دیدگاه دقیق ریاضیاتی با کمی اغماض همراه است. در واقع، میدان کسرها $\text{Frac}(D)$ یک دامنه صحیح، مجموعه‌ای ساخته‌شده از رده‌های هم‌ارزی است و برای بیان دقیق ارتباط آن با میدان K ، نیازمند استفاده از مفاهیمی مانند «هم‌ریختی»، «نشاندن» و «یک‌ریختی» هستیم تا نشان دهیم این دو ساختار در اصل با یکدیگر یک‌ریخت هستند ($K \cong \text{Frac}(D)$). از آنجایی که در این نوشتار، رفتار و ساختار این میدان‌های یک‌ریخت را کاملاً یکسان در نظر گرفته‌ایم، از ورود به جزئیات این مفاهیم صرف‌نظر کرده و با تساهل از نماد تساوی استفاده می‌کنیم.

۴.۱ الگوریتم‌هایی برای چند جمله‌ای‌ها

در بخش‌های قبل، با قضایای جبری برای اثبات وجود مفاهیمی مانند خارج قسمت، باقیمانده و بزرگترین مقسوم‌علیه مشترک در دامنه‌های اقلیدسی آشنا شدیم اما در محاسبات نمادین، ما نیازمند روش‌هایی سازنده و اجرایی برای

یافتن این مقادیر هستیم. در این بخش، الگوریتم‌های کلیدی تقسیم، شبه‌تقسیم و الگوریتم اقلیدسی تعمیم‌یافته را برای چندجمله‌ای‌ها ارائه می‌کنیم.

۱.۴.۱ تقسیم چندجمله‌ای‌ها

قضیه زیر نشان می‌دهد که حلقه $K[x]$ ، به این شرط که K میدان باشد، با تابع $\deg$ ، یک دامنه اقلیدسی است.

قضیه ۱.۴.۱ (الگوریتم تقسیم برای چندجمله‌ای‌های تک‌متغیره). فرض کنیم K یک میدان باشد و A و B دو چندجمله‌ای دلخواه در $K[x]$ باشند، به شرطی که $B \neq 0$. در این صورت چندجمله‌ای‌های یکتای Q و R در $K[x]$ وجود دارند، به طوری که

$$A = BQ + R \quad (R = 0 \quad \text{یا} \quad \deg(R) < \deg(B)).$$

اثبات. ابتدا ثابت می‌کنیم چندجمله‌ای‌های Q و R با این ویژگی وجود دارند. اگر $A \mid B$ ، آنگاه $Q \in K[x]$ وجود دارد، به طوری که $A = BQ$. در این حالت مقدار باقیمانده برابر با صفر خواهد بود ($R = 0$). حال فرض کنیم که $A \nmid B$. مجموعه‌های S و M را به صورت زیر تعریف می‌کنیم:

$$S = \{A - BQ \mid Q \in K[x]\}, \quad M = \{\deg(P) \mid P \in S\}.$$

از آنجا که M تهی نیست، طبق اصل خوش‌ترتیبی، دارای کوچکترین عضو مانند m است، بنابراین $Q, R \in K[x]$ وجود دارند، به طوری که $\deg(R) = m$ و $A - BQ = R$. (فرض خلف) فرض می‌کنیم $\deg(R) \geq \deg(B)$. قرار می‌دهیم $\deg(B) = n$ و تعریف می‌کنیم $H = R - \text{LC}(B)^{-1} \text{LC}(R)x^{m-n}B$ ، در این صورت

$$\begin{aligned} H &= R - \text{LC}(B)^{-1} \text{LC}(R)x^{m-n}B \\ &= A - BQ - \text{LC}(B)^{-1} \text{LC}(R)x^{m-n}B \\ &= A - (Q + \text{LC}(B)^{-1} \text{LC}(R)x^{m-n})B \in S. \end{aligned}$$

همچنین از آنجایی که $\deg(H) < m$ داریم $\text{LT}(R) = \text{LT}[\text{LC}(B)^{-1}\text{LC}(R)x^{m-n}B]$ با انتخاب $R \in S$ با کمترین درجه است و در نتیجه $\deg(R) < \deg(B)$. حال یکتایی Q و R را ثابت می‌کنیم. فرض کنیم به ازای $Q', R' \in K[x]$ ، داشته باشیم

$$A = BQ + R = BQ' + R' \quad (\deg(R') < \deg(B)).$$

اگر $Q \neq Q'$ ، آنگاه داریم

$$\deg(B) \leq \deg(B(Q - Q')) = \deg(R' - R) \leq \max\{\deg(R), \deg(R')\} < \deg(B),$$

□

که یک تناقض است. بنابراین $Q = Q'$ که نتیجه می‌دهد $R = R'$.

اکنون با استفاده از قضیه‌ای که اثبات کردیم، می‌توانیم یک نتیجه مفید در مورد حلقه چندجمله‌ای‌ها با ضرایبی از یک میدان داشته باشیم.

لم ۲.۴.۱. فرض کنیم K یک میدان باشد. در این صورت، حلقه چندجمله‌ای‌های $K[x]$ یک دامنه تجزیه یکتا است.

اثبات. از قضیه ۱.۴.۱ داریم که حلقه $K[x]$ همراه با تابع درجه $\deg$ یک دامنه اقلیدسی است. از سوی دیگر، طبق قضایای ۳.۳.۱ و ۴.۳.۱، هر دامنه اقلیدسی یک دامنه ایده‌آل اصلی و هر دامنه ایده‌آل اصلی، یک دامنه تجزیه یکتا است؛ بنابراین حلقه $K[x]$ یک دامنه تجزیه یکتا خواهد بود.

□

قضیه ۱.۴.۱، تنها وجود چندجمله‌ای‌های Q و R (خارج‌قسمت و باقیمانده) را ثابت می‌کند و روشی برای محاسبه آنها ارائه نمی‌دهد. الگوریتمی که در ادامه معرفی می‌کنیم، این کار را ممکن می‌سازد.

الگوریتم ۱.۱ تقسیم برای چندجمله‌ای‌های تک‌متغیره $\text{PolyDivide}(A, B)$

Require: $A, B \in K[x]$ where K is a field and $B \neq 0$

Ensure: The quotient and remainder of the division of A by B

```

 $Q \leftarrow 0, R \leftarrow A$ 
while  $R \neq 0$  and  $\text{LT}(B) \mid \text{LT}(R)$  do
     $Q \leftarrow Q + \frac{\text{LT}(R)}{\text{LT}(B)}$ 
     $R \leftarrow R - \frac{\text{LT}(R)}{\text{LT}(B)} B$ 
end while
return  $(Q, R)$ 

```

قضیه ۳.۴.۱. الگوریتم ۱.۱ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

اثبات. ابتدا نشان می‌دهیم که الگوریتم پس از تعدادی متناهی مرحله، پایان می‌یابد. فرض کنیم Q_i و R_i به ترتیب نتایج به دست آمده در مرحله i -ام اجرای الگوریتم باشند، در این صورت $Q_0 = 0$ ، $R_0 = A$. (فرض خلف) فرض می‌کنیم الگوریتم پایان‌پذیر نباشد. دنباله $\{\deg(R_i)\}_{i=0}^{\infty}$ را در نظر می‌گیریم. این دنباله اکیدا نزولی است، چرا که اگر الگوریتم در i -امین مرحله پایان نیابد، خواهیم داشت

$$R_{i+1} = R_i - \frac{\text{LT}(R_i)}{\text{LT}(B)} B = [\text{LC}(R_i)x^{\deg(R_i)} + \dots] - [1 \cdot \text{LC}(R_i)x^{\deg(R_i)} + \dots],$$

و از آنجا که $\deg(R_i) \geq \deg(B)$ ، نتیجه می‌گیریم که $\deg(R_i) > \deg(R_{i+1})$. بنابراین دنباله $\{\deg(R_i)\}_{i=0}^{\infty}$ دارای کوچکترین عضو نخواهد بود و این با اصل خوش‌ترتیبی اعداد طبیعی در تناقض است. حال برای اثبات درستی الگوریتم، با استقرا نشان می‌دهیم که برای هر مرحله i ، داریم $A = BQ_i + R_i$. اگر $i = 0$ ، آنگاه حکم به وضوح برقرار است. فرض کنیم حکم برای مرحله i -ام درست باشد، یعنی $A = BQ_i + R_i$. در این صورت

$$BQ_{i+1} + R_{i+1} = B \cdot (Q_i + \frac{\text{LT}(R_i)}{\text{LT}(B)}) + (R_i - \frac{\text{LT}(R_i)}{\text{LT}(B)} B) = BQ_i + R_i = A.$$

فرض کنیم الگوریتم در مرحله n -ام به پایان برسد، در این صورت $R_n = 0$ یا $\deg(R_n) < \deg(B)$. $\square$

مثال ۱.۴.۱. مراحل اجرای الگوریتم $\text{PolyDivide}(A, B)$ برای $A = x^2 + 1$ و $B = 2x + 1$ در $\mathbb{Q}[x]$:

گام	Q	R	$T = \frac{\text{LT}(R)}{\text{LT}(B)}$
۰	۰	$x^2 + 1$	$\frac{1}{2}x$
۱	$\frac{1}{2}x$	$-\frac{1}{2}x + 1$	$-\frac{1}{2}$
۲	$\frac{1}{2}x - \frac{1}{2}$	$\frac{5}{2}$	

از آنجا که در مرحله آخر $\deg(R) < \deg(B)$ ، حلقه پایان می‌یابد؛ بنابراین داریم $A = B \left(\frac{1}{2}x - \frac{1}{2} \right) + \frac{5}{2}$.

۲.۴.۱ شبه‌تقسیم

نکته‌ای که باید به آن توجه کرد، شرط میدان بودن K در قضیه ۱.۴.۱ و الگوریتم ۱.۱ است؛ چرا که اگر حلقه زمینه یک دامنه صحیح D باشد، ضریب پیشرو $\text{LC}(B)$ لزوماً $\text{LC}(A)$ را عاد نمی‌کند، بنابراین استفاده از الگوریتم تقسیم همواره ممکن نیست. در ادامه رویکرد دیگری را برای پرداختن به این مسئله به کار می‌بریم.

قضیه ۲.۴.۱ (الگوریتم شبه‌تقسیم برای چندجمله‌ای‌های تک‌متغیره). فرض کنیم D یک دامنه صحیح و A و B دو چندجمله‌ای دلخواه در $D[x]$ باشند، به طوری که $B \neq 0$. قرار می‌دهیم

$$\delta = \max\{0, \deg(A) - \deg(B) + 1\}.$$

در این صورت، چندجمله‌ای‌های یکتای $Q, R \in D[x]$ وجود دارند، به طوری که

$$\text{LC}(B)^\delta A = BQ + R \quad (R = 0 \quad \text{یا} \quad \deg(R) < \deg(B)).$$

Q و R را به ترتیب شبه‌خارج‌قسمت و شبه‌باقیمانده می‌گوییم و با نمادهای $\text{Pquo}(A, B)$ و $\text{Prem}(A, B)$ نمایش می‌دهیم.

اثبات. با ارائه یک الگوریتم و اثبات پایان‌پذیری و درستی آن، نشان می‌دهیم که Q و R با ویژگی‌های بالا وجود دارند و یکتا هستند.

الگوریتم ۲.۱ شبه‌تقسیم برای چندجمله‌ای‌های تک‌متغیره $\text{PseudoPolyDivide}(A, B)$

Require: $A, B \in D[x]$ where D is an integral domain and $B \neq 0$

Ensure: The pseudo-quotient and pseudo-remainder of the pseudo-division of A by B

```

 $\delta \leftarrow \max\{0, \deg(A) - \deg(B) + 1\}$ 
 $Q \leftarrow 0, R \leftarrow A$ 
while  $R \neq 0$  and  $\deg(R) \geq \deg(B)$  do
     $d \leftarrow \deg(R) - \deg(B)$ ,  $T \leftarrow \text{LC}(R)x^d$ 
     $Q \leftarrow \text{LC}(B)Q + T$ ,  $R \leftarrow \text{LC}(B)R - TB$ 
     $\delta \leftarrow \delta - 1$ 
end while
 $Q \leftarrow \text{LC}(B)^\delta Q$ 
 $R \leftarrow \text{LC}(B)^\delta R$ 
return  $(Q, R)$ 

```

ابتدا پایان‌پذیری الگوریتم را نشان می‌دهیم. فرض کنیم Q_i, R_i و T_i به ترتیب مقادیر به دست آمده در گام i -ام از اجرای حلقه الگوریتم باشند، در این صورت $R_0 = A$ و $Q_0 = 0$. (فرض خلف) فرض می‌کنیم که الگوریتم پایان‌پذیر نباشد. دنباله درجات باقیمانده‌ها یعنی $\{\deg(R_i)\}_{i=0}^\infty$ را در نظر می‌گیریم. این دنباله اکیدا نزولی است؛ چرا که اگر الگوریتم در گام i -ام پایان نیابد، خواهیم داشت

$$\begin{aligned}
 R_{i+1} &= \text{LC}(B)R_i - T_i B \\
 &= \text{LC}(B)R_i - \text{LC}(R_i)x^{\deg(R_i)-\deg(B)} B \\
 &= [\text{LC}(B)\text{LC}(R_i)x^{\deg(R_i)} + \dots] - [\text{LC}(B)\text{LC}(R_i)x^{\deg(R_i)} + \dots],
 \end{aligned}$$

و از آنجا که جمله پیشرو با ضریب یکسان حذف می‌شود، نتیجه می‌گیریم $\deg(R_{i+1}) < \deg(R_i)$. از آنجا که درجه چندجمله‌ای‌های ناصفر عددی نامنفی در $\mathbb{N}$ است، وجود یک دنباله نامتناهی و اکیدا نزولی از این اعداد

با اصل خوش‌ترتیبی در تناقض است؛ بنابراین الگوریتم حتماً پس از تعداد متناهی گام پایان می‌پذیرد. حال برای اثبات درستی، فرض می‌کنیم δ_i مقدار متغیر δ در گام i -ام باشد و $\delta = \delta_0$. با استقرا نشان می‌دهیم که در هر گام i رابطه زیر برقرار است:

$$\mathbf{LC}(B)^\delta A = \mathbf{LC}(B)^{\delta_i} Q_i B + \mathbf{LC}(B)^{\delta_i} R_i.$$

اگر $i = 0$ ، آنگاه حکم به وضوح برقرار است. فرض می‌کنیم حکم برای گام i درست باشد. این یعنی

$$\begin{aligned} \mathbf{LC}(B)^{\delta_{i+1}} Q_{i+1} B + \mathbf{LC}(B)^{\delta_{i+1}} R_{i+1} &= \mathbf{LC}(B)^{\delta_i - 1} [\mathbf{LC}(B) Q_i + T_i] B \\ &\quad + \mathbf{LC}(B)^{\delta_i - 1} [\mathbf{LC}(B) R_i - T_i B] \\ &= \mathbf{LC}(B)^{\delta_i} Q_i B + \mathbf{LC}(B)^{\delta_i} R_i \\ &= \mathbf{LC}(B)^{\delta} A. \end{aligned}$$

فرض کنیم الگوریتم پس از n تکرار پایان یابد. در این صورت، $R = \mathbf{LC}(B)^{\delta_n} R_n$ و $Q = \mathbf{LC}(B)^{\delta_n} Q_n$ که طبق رابطه استقرا در تساوی $\mathbf{LC}(B)^{\delta} A = BQ + R$ صدق می‌کنند. همچنین داریم $R_n = 0$ یا $\deg(R_n) < \deg(B)$. از آنجا که D دامنه صحیح است و $\mathbf{LC}(B) \neq 0$ ، ضرب در توانی از $\mathbf{LC}(B)$ درجه را تغییر نمی‌دهد و بنابراین $R = 0$ یا $\deg(R) < \deg(B)$. اکنون یکتایی Q و R را ثابت می‌کنیم. فرض کنیم به ازای $Q', R' \in D[x]$ ، داشته باشیم:

$$\mathbf{LC}(B)^{\delta} A = BQ + R = BQ' + R' \quad (\deg(R), \deg(R') < \deg(B)).$$

از تساوی بالا نتیجه می‌گیریم که $B(Q - Q') = R' - R$. اگر $Q \neq Q'$ ، از آنجا که D یک دامنه صحیح است و $B \neq 0$ ، طبق نتیجه ۱.۳.۱ خواهیم داشت

$$\deg(B) \leq \deg(B(Q - Q')) = \deg(R' - R) \leq \max\{\deg(R), \deg(R')\} < \deg(B),$$

□

که تناقض است. بنابراین $Q = Q'$ که نتیجه می‌دهد $R = R'$.

تذکره ۱.۴.۱. در حالتی که $\deg(A) < \deg(B)$ ، الگوریتم شبه‌تقسیم دارای یک جواب بدیهی است. در این حالت طبق تعریف داریم $\delta = 0$ که نتیجه می‌دهد $\text{LC}(B)^0 = 1$. بنابراین رابطه شبه‌تقسیم به صورت $A = BQ + R$ تبدیل می‌شود که با انتخاب مقادیر بدیهی $Q = 0$ و $R = A$ برقرار است. علاوه بر این، تعریف δ به صورت $\max\{0, \deg(A) - \deg(B) + 1\}$ مانع از ایجاد توان‌های منفی برای ضریب پیشرو در حلقه شده و یکتایی شبه‌خارج‌قسمت و شبه‌باقیمانده را تضمین می‌کند. مثال زیر می‌تواند این نکته را به خوبی روشن سازد.

مثال ۲.۴.۱. دو چندجمله‌ای $A = 2x + 1$ و $B = 2x + 3$ را در حلقه $\mathbb{Z}[x]$ در نظر می‌گیریم. طبق الگوریتم ۲.۱ و با توجه به اینکه $\delta = 1$ ، داریم

$$\text{LC}(B)^1 A = 2(2x + 1) = (2x + 3)(2) - 4 \implies (Q, R) = (2, -4).$$

همچنین اگر توان $\text{LC}(B)$ را کمتر از δ (مثلاً ۰) در نظر بگیریم، خواهیم داشت

$$\text{LC}(B)^0 A = 1(2x + 1) = (2x + 3)(1) - 2 \implies (Q', R') = (1, -2).$$

از آنجایی که هر دو حالت در رابطه شبه‌تقسیم صدق می‌کنند، مقید نکردن توان $\text{LC}(B)$ به یک مقدار ثابت مانند δ ، باعث نقض یکتایی Q و R خواهد شد.

مثال ۳.۴.۱. مراحل اجرای الگوریتم $\text{PseudoPolyDivide}(A, B)$ برای $A = x^2 + 1$ و $B = 2x + 1$ در $\mathbb{Z}[x]$:

گام	δ	Q	R	$d = \deg(R) - \deg(B)$	$T = \text{LC}(R)x^d$
۰	۲	۰	$x^2 + 1$	۱	x
۱	۱	x	$-x + 2$	۰	-1
۲	۰	$2x - 1$	۵		

در پایان، از آنجا که $\delta = 0$ ، مقادیر نهایی بدون تغییر باقی مانده و خروجی الگوریتم برابر با $(2x - 1, 5)$ خواهد بود؛ بنابراین داریم $4A = B(2x - 1) + 5$.

۳.۴.۱ الگوریتم اقلیدسی

در مباحث قبلی، صرفاً مفهوم ب.م.م. و ویژگی‌هایش را مطالعه کردیم و روشی عملی برای محاسبه آن ارائه نشد. در ادامه، الگوریتم اقلیدسی را برای محاسبه ب.م.م. دو چندجمله‌ای تک‌متغیره معرفی می‌کنیم اما پیش از آن به دو لم زیر برای ورود به بحث اصلی نیازمندیم.

لم ۵.۴.۱. فرض کنیم D یک دامنه صحیح و $a \in D$ یک عنصر دلخواه باشد، به طوری که $a \neq 0$. در این صورت $\gcd(a, 0) = a$.

لم ۶.۴.۱. فرض کنیم D یک دامنه اقلیدسی و $a, b \in D$ عناصری دلخواه باشند، به طوری که $b \neq 0$. اگر $r \in D$ باقیمانده تقسیم a بر b باشد، آنگاه $\gcd(a, b) = \gcd(b, r)$.

اثبات. فرض کنیم $d_1 = \gcd(a, b)$ و $d_2 = \gcd(b, r)$. نشان می‌دهیم که $d_1 \mid d_2$ و $d_2 \mid d_1$ ، یا به عبارت دیگر، ثابت می‌کنیم که d_1 و d_2 در حد ضرب یک‌ه، برابر هستند. از آنجا که r باقیمانده تقسیم a بر b است، عنصر $q \in D$ وجود دارد، به طوری که $a = bq + r$. از آنجا که $d_1 \mid a$ و $d_1 \mid b$ ، نتیجه می‌گیریم $d_1 \mid a - bq = r$. بنابراین $d_1 \mid d_2$. از سوی دیگر، $d_2 \mid b$ و $d_2 \mid r$ ، بنابراین $d_2 \mid bq + r = a$ و در نتیجه $d_2 \mid d_1$. $\square$

الگوریتم ۳.۱ محاسبه ب.م.م. چندجمله‌ای‌های تک‌متغیره $\text{Euclidean}(A, B)$

Require: $A, B \in K[x]$ where K is a field and $(A, B) \neq (0, 0)$

Ensure: $\gcd(A, B)$

```

while  $B \neq 0$  do
     $(Q, R) \leftarrow \text{PolyDivide}(A, B)$ 
     $A \leftarrow B, B \leftarrow R$ 
end while
return  $A$ 

```

قضیه ۷.۴.۱. الگوریتم ۳.۱ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

اثبات. ابتدا پایان‌پذیری الگوریتم را نشان می‌دهیم. فرض کنیم A_i, B_i, R_i به ترتیب نتایج به دست آمده در مرحله i -ام اجرای الگوریتم باشند، در این صورت $A_0 = A$ و $B_0 = B$. همچنین فرض می‌کنیم

R برابر با باقیمانده تقسیم A بر B است. (فرض خلف) فرض می‌کنیم که الگوریتم پایان‌پذیر نباشد. دنباله $\{\deg(B_i)\}_{i=0}^{\infty}$ را در نظر می‌گیریم. این دنباله اکیدا نزولی است، چرا که اگر الگوریتم در i -امین مرحله پایان نیابد، B_{i+1} باقیمانده تقسیم A_i بر B_i است و بنابراین خواهیم داشت $\deg(B_i) > \deg(B_{i+1})$ که با اصل خوش‌ترتیبی اعداد طبیعی در تناقض است. برای اثبات درستی الگوریتم، با استقرا نشان می‌دهیم که در هر مرحله i داریم $\gcd(A, B) = \gcd(A_i, B_i)$. به وضوح حکم برای $i = 0$ برقرار است. فرض کنیم حکم برای مرحله i -ام درست باشد. در این صورت

$$\gcd(A_{i+1}, B_{i+1}) = \gcd(B_i, R_i) \stackrel{۴.۴.۱}{=} \gcd(A_i, B_i) = \gcd(A, B).$$

حال فرض کنیم الگوریتم در مرحله n -ام به پایان برسد، در این صورت

$$\gcd(A, B) = \gcd(A_n, B_n) = \gcd(A_n, 0) \stackrel{۵.۴.۱}{=} A_n. \quad \square$$

مثال ۴.۴.۱. مراحل اجرای الگوریتم $\text{Euclidean}(A, B)$ برای محاسبه ب.م.م. دو چندجمله‌ای

$$A = x^3 - 1 \text{ و } B = x^2 - 1 \text{ در } \mathbb{Q}[x]:$$

گام	A	B	Q	R
۰	$x^3 - 1$	$x^2 - 1$	x	$x - 1$
۱	$x^2 - 1$	$x - 1$	$x + 1$	۰
۲	$x - 1$	۰		

با صفر شدن متغیر B ، الگوریتم پایان یافته و مقدار A در سطر آخر بازگردانده می‌شود، بنابراین خواهیم داشت $\gcd(A, B) = x - 1$.

الگوریتم اقلیدسی تنها مقدار ب.م.م. را محاسبه می‌کند اما در بسیاری از کاربردهای محاسباتی که در فصل‌های بعد مشاهده می‌کنیم، نیازمند یافتن ضرایبی هستیم که ب.م.م. را به صورت ترکیب خطی از دو چندجمله‌ای اولیه تولید کنند. قضیه مهم زیر می‌تواند ما را به این هدف برساند.

قضیه ۸.۴.۱ (اتحاد بزو)^۱. فرض کنیم D یک دامنه ایده‌آل اصلی باشد. در این صورت برای هر $a, b \in D$

^۱اتین بزو (Étienne Bézout) (۱۷۳۰-۱۷۸۳ میلادی)، ریاضی‌دان فرانسوی که برای نخستین بار صورتی از این قضیه را در نظریه

عناصر $k_1, k_2 \in D$ وجود دارند، به طوری که $k_1 a + k_2 b = \gcd(a, b)$ و k_1 و k_2 را ضرایب بزو می‌نامیم).

□

اثبات. از قضیه ۵.۳.۱ و گزاره ۲.۱.۱ نتیجه می‌شود.

تذکره ۲.۴.۱. مفاهیم ب.م.م. و اتحاد بزو برای n عنصر نیز قابل تعمیم هستند. ب.م.م. چند عنصر به صورت بازگشتی با رابطه $\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$ محاسبه می‌شود. همچنین در یک دامنه ایده‌آل اصلی، اتحاد بزو به صورت ترکیب خطی تعمیم یافته و عناصری مانند $k_1, \dots, k_n \in D$ وجود دارند که $\sum_{i=1}^n k_i a_i = \gcd(a_1, \dots, a_n)$.

الگوریتم ۴.۱ محاسبه ب.م.م. و ضرایب بزو چند جمله‌ای‌های تک‌متغیره $\text{ExtEuclidean}(A, B)$

Require: $A, B \in K[x]$ where K is a field and $(A, B) \neq (0, 0)$

Ensure: $\gcd(A, B), K_1, K_2$ such that $K_1 A + K_2 B = \gcd(A, B)$

$K_1 \leftarrow 1, K_2 \leftarrow 0, K'_1 \leftarrow 0, K'_2 \leftarrow 1$

while $B \neq 0$ **do**

$(Q, R) \leftarrow \text{PolyDivide}(A, B)$

$A \leftarrow B, B \leftarrow R$

$R_1 \leftarrow K_1 - K'_1 Q, R_2 \leftarrow K_2 - K'_2 Q$

$K_1 \leftarrow K'_1, K_2 \leftarrow K'_2, K'_1 \leftarrow R_1, K'_2 \leftarrow R_2$

end while

return (A, K_1, K_2)

قضیه ۹.۴.۱. الگوریتم ۴.۱ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

اثبات. اثبات پایان‌پذیری و خروجی درست ب.م.م. الگوریتم، مشابه الگوریتم ۳.۱ است.

فرض کنیم $(K_1)_i, (K_2)_i, (K'_1)_i, (K'_2)_i$ به ترتیب نتایج به دست آمده در مرحله i -ام اجرای الگوریتم باشند. با استقرا ثابت می‌کنیم که برای هر i داریم

$$A_i = (K_1)_i A + (K_2)_i B, \quad B_i = (K'_1)_i A + (K'_2)_i B.$$

اعداد اثبات کرد.

به وضوح حکم برای $i = 0$ درست است. فرض کنیم حکم برای i درست باشد، در این صورت داریم

$$(K_1)_{i+1} = (K'_1)_i, \quad (K_2)_{i+1} = (K'_2)_i, \quad A_{i+1} = B_i,$$

و در نتیجه $A_{i+1} = (K_1)_{i+1}A + (K_2)_{i+1}B$ برای اثبات رابطه دوم داریم

$$\begin{aligned} (K'_1)_{i+1}A + (K'_2)_{i+1}B &= [(K_1)_i - (K'_1)_i Q_i]A + [(K_2)_i - (K'_2)_i Q_i]B \\ &= [(K_1)_i A + (K_2)_i B] - [(K'_1)_i A + (K'_2)_i B] Q_i \\ &= A_i - B_i Q_i = B_{i+1}. \end{aligned}$$

فرض کنیم الگوریتم در مرحله n -ام به پایان برسد، در این صورت

$$\gcd(A, B) = A_n = (K_1)_n A + (K_2)_n B. \quad \square$$

مثال ۵.۴.۱. مراحل اجرای الگوریتم **ExtEuclidean**(A, B) برای $A = x^3 - 1$ و $B = x^2 - 1$ در $\mathbb{Q}[x]$:

گام	A	B	Q	R	K_1	K_2	K'_1	K'_2
۰	$x^3 - 1$	$x^2 - 1$	x	$x - 1$	۱	۰	۰	۱
۱	$x^2 - 1$	$x - 1$	$x + 1$	۰	۰	۱	۱	$-x$
۲	$x - 1$	۰			۱	$-x$	$-x - 1$	$x^2 + x + 1$

خروجی الگوریتم نشان می‌دهد که $\gcd(A, B) = x - 1$ و ضرایب بزو برابر با $K_1 = 1$ و $K_2 = -x$ هستند. درستی این نتیجه با برقراری رابطه زیر مشخص می‌شود:

$$1 \cdot (x^3 - 1) + (-x) \cdot (x^2 - 1) = x - 1.$$

۵.۱ منتج دو چندجمله‌ای

در بحث محاسبات نمادین، اغلب نیاز داریم بدون محاسبه صریح و کامل ریشه‌های دو چندجمله‌ای، متوجه شویم که آیا آن‌ها ریشه مشترکی دارند یا خیر. با تعریف «منتج» دو چندجمله‌ای و ارائه قضیه‌ای مرتبط با آن در این بخش، می‌توانیم به چنین هدفی برسیم.

تعریف ۱.۵.۱. فرض کنیم D یک دامنه صحیح و $A, B \in D[x]$ دو چندجمله‌ای به صورت زیر باشند:

$$A = \sum_{i=0}^m a_i x^i \quad (a_m \neq 0), \quad B = \sum_{j=0}^n b_j x^j \quad (b_n \neq 0),$$

به طوری که $m = \deg(A)$ و $n = \deg(B)$. ماتریس سیلوستر^۱ دو چندجمله‌ای A و B ، که آن را با $\text{Syl}(A, B)$ نشان می‌دهیم، یک ماتریس مربعی از مرتبه $(m+n) \times (m+n)$ است که درآیه‌های آن از ضرایب A و B تشکیل شده و به شکل زیر ساخته می‌شود:

• n سطر اول ماتریس، شامل ضرایب A است که در هر سطر، یک واحد به سمت راست انتقال پیدا کرده‌اند.

• m سطر بعدی ماتریس، شامل ضرایب B است که به همین ترتیب انتقال پیدا کرده‌اند.

• سایر درآیه‌های ماتریس صفر هستند.

^۱جیمز جوزف سیلوستر (James Joseph Sylvester) (۱۸۱۴-۱۸۹۷ میلادی)، ریاضی‌دان انگلیسی که سهم بسزایی در توسعه نظریه ماتریس‌ها، نظریه ناوردها و ترکیبیات داشت.

به بیان دقیق‌تر، این ماتریس به شکل زیر است:

$$\text{Syl}(A, B) = \left(\begin{array}{cccccc} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & b_n & b_{n-1} & \cdots & b_0 \end{array} \right) \left. \begin{array}{l} \\ \\ \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} \text{سطر } n \\ \\ \\ \\ \text{سطر } m \end{array}.$$

تعریف ۲.۵.۱. فرض کنیم D یک دامنه صحیح و $A, B \in D[x]$ دو چندجمله‌ای دلخواه باشند. **منتج** این دو چندجمله‌ای، که با $\text{Res}(A, B)$ نشان می‌دهیم، برابر است با دترمینان ماتریس سیلوستر A و B ، یا به بیان دیگر

$$\text{Res}(A, B) = \det(\text{Syl}(A, B)).$$

مثال ۱.۵.۱. دو چندجمله‌ای $A = x^2 - 3x + 2$ و $B = x^2 - 1$ را در حلقه $\mathbb{Z}[x]$ در نظر می‌گیریم. از آنجایی که $\deg(A) = 2$ و $\deg(B) = 2$ ، ماتریس سیلوستر آن‌ها یک ماتریس 4×4 خواهد بود:

$$\text{Syl}(A, B) = \begin{pmatrix} 1 & -3 & 2 & 0 \\ 0 & 1 & -3 & 2 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

با محاسبه دترمینان این ماتریس، داریم $\text{Res}(A, B) = 0$.

بدیهی است که منتج دو چندجمله‌ای از $D[x]$ ، همواره یک عنصر در دامنه صحیح D است. برای مثال اگر حلقه زمینه D ، خود یک حلقه چندجمله‌ای مانند $K[t]$ باشد، آنگاه برای دو چندجمله‌ای دلخواه $A, B \in K[t][x]$ ،

ماتریس سیلواستر آن‌ها نسبت به متغیر x تشکیل می‌شود. در این حالت، دترمینان این ماتریس (یعنی منتج) متغیر x را به طور کامل حذف کرده و خروجی آن، یک چندجمله‌ای تنها بر حسب متغیر t در حلقه $K[t]$ خواهد بود. برای تأکید بر اینکه ماتریس سیلواستر و منتج نسبت به کدام متغیر محاسبه شده است، از نمادهای $\text{Syl}_x(A, B)$ و $\text{Res}_x(A, B)$ استفاده می‌کنیم. مثالی که در ادامه ارائه می‌دهیم، این مسئله را روشن‌تر می‌سازد.

مثال ۲.۵.۱. دو چندجمله‌ای $A = x^2 - 1$ و $B = -2tx + 1$ را در حلقه $\mathbb{Q}[t][x]$ در نظر می‌گیریم. می‌خواهیم $\text{Res}_x(A, B)$ را محاسبه کنیم. در اینجا درجه A نسبت به x برابر با ۲ ($m = 2$) و درجه B نسبت به x برابر با ۱ ($n = 1$) است. بنابراین ماتریس سیلواستر آن‌ها یک ماتریس 3×3 خواهد بود که درآیه‌های آن چندجمله‌ای‌هایی بر حسب t هستند:

$$\text{Syl}_x(A, B) = \begin{pmatrix} 1 & 0 & -1 \\ -2t & 1 & 0 \\ 0 & -2t & 1 \end{pmatrix}.$$

با محاسبه دترمینان این ماتریس با بسط سطر اول، خواهیم داشت

$$\text{Res}_x(A, B) = 1(1 - 0) - 0 + (-1)(4t^2 - 0) = 1 - 4t^2.$$

همان‌طور که مشاهده می‌شود، متغیر x حذف شده و حاصل یک چندجمله‌ای در $\mathbb{Q}[t]$ است.

قضیه زیر، کاربرد منتج را به عنوان محکی برای تشخیص وجود ریشه‌های مشترک دو چندجمله‌ای نشان می‌دهد.

قضیه ۱.۵.۱. فرض کنیم K یک میدان و $A, B \in K[x]$ دو چندجمله‌ای غیرصفر باشند. دو چندجمله‌ای A و B دارای عامل مشترک غیربدیهی (به عبارت دیگر $\deg(\gcd(A, B)) > 0$) هستند، اگر و تنها اگر $\text{Res}(A, B) = 0$.

اثبات. ($\Rightarrow$) ابتدا فرض می‌کنیم A و B دارای عامل مشترک غیربدیهی باشند، یعنی $\deg(\gcd(A, B)) > 0$. قرار می‌دهیم $D = \gcd(A, B)$ و فرض می‌کنیم $d = \deg(D) \geq 1$. در این صورت چندجمله‌ای‌های $A_1, B_1 \in K[x]$ وجود دارند، به طوری که $A = A_1 D$ و $B = B_1 D$. با توجه به درجات، خواهیم داشت

$\deg(A_1) = m - d < m$ و $\deg(B_1) = n - d < n$ از سوی دیگر، با ضرب کردن داریم

$$A_1 B = A_1 B_1 D = A B_1,$$

که نتیجه می‌دهد $B_1 A + (-A_1) B = 0$. این رابطه نشان می‌دهد که یک ترکیب خطی غیربدیهی از A و B با ضرایب چندجمله‌ای از درجه کمتر از n و m برابر با صفر شده است. در ساختار ماتریس سیلویستر، این دقیقاً معادل با آن است که سطرهای ماتریس سیلویستر از لحاظ خطی وابسته‌اند. در نتیجه دترمینان ماتریس برابر با صفر خواهد بود که یعنی $\text{Res}(A, B) = 0$.

($\Leftarrow$) اکنون فرض می‌کنیم $\text{Res}(A, B) = 0$. بنابراین دترمینان ماتریس سیلویستر صفر است که نشان می‌دهد سطرهای آن وابستگی خطی دارند. این وابستگی خطی تضمین می‌کند که چندجمله‌ای‌هایی مانند $U, V \in K[x]$ وجود دارند (که هر دو همزمان صفر نیستند)، به طوری که $\deg(U) < n$ و $\deg(V) < m$ و همچنین

$$UA + VB = 0.$$

(فرض خلف) فرض می‌کنیم $\deg(\gcd(A, B)) = 0$. طبق لم ۲.۴.۱، حلقه چندجمله‌ای‌های $K[x]$ یک دامنه تجزیه یکتا است و از قضیه ۲.۳.۱ و گزاره ۱.۳.۱ داریم که بزرگترین مقسوم‌علیه مشترک موجود و تنها در حد ضرب یک عنصر یکه منحصر به فرد است، پس می‌توانیم فرض کنیم $\gcd(A, B) = 1$. از رابطه $UA = -VB$ نتیجه می‌گیریم $A \mid VB$. از آنجا که A و B نسبت به هم اول هستند، باید داشته باشیم $A \mid V$ ، اما از آنجا که $\deg(V) < m = \deg(A)$ داریم $V = 0$. با جایگذاری $V = 0$ در معادله، خواهیم داشت $UA = 0$. از آنجا که $A \neq 0$ ، نتیجه می‌گیریم $U = 0$. اینکه $U = V = 0$ ، با فرض غیربدیهی بودن آن‌ها (وابستگی خطی) در تناقض است، بنابراین $\deg(\gcd(A, B)) > 0$. $\square$

مثال ۳.۵.۱. دو چندجمله‌ای $A = x^2 - 4$ و $B = x^2 + x - 6$ را در حلقه $\mathbb{Q}[x]$ در نظر می‌گیریم. با تجزیه این دو چندجمله‌ای مشاهده می‌شود که ریشه $x = 2$ بین آن‌ها مشترک است، بنابراین $\gcd(A, B) = x - 2$ و درجه آن بزرگتر از صفر خواهد بود. ماتریس سیلویستر این دو چندجمله‌ای یک ماتریس 4×4 به شکل زیر

است:

$$\text{Syl}(A, B) = \begin{pmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & -4 \\ 1 & 1 & -6 & 0 \\ 0 & 1 & 1 & -6 \end{pmatrix}.$$

با محاسبه دترمینان این ماتریس، خواهیم دید که $\text{Res}(A, B) = 0$. حال اگر چندجمله‌ای $C = x - 1$ را در نظر بگیریم، بدیهی است که A و C هیچ عامل مشترکی جز ۱ ندارند که نشان‌دهنده این است که $\deg(\gcd(A, C)) = 0$. از آنجا که $\deg(A) = 2$ و $\deg(C) = 1$ ، ماتریس سیلواستر آن‌ها 3×3 خواهد بود:

$$\text{Syl}(A, C) = \begin{pmatrix} 1 & 0 & -4 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}.$$

با محاسبه دترمینان، نتیجه می‌گیریم $\text{Res}(A, C) = -3 \neq 0$.

فصل ۲

جبر دیفرانسیلی و انتگرال گیری توابع گویا

در این فصل، با استفاده از پیش نیازهایی که در فصل گذشته مطرح کردیم، مفاهیم مقدماتی «جبر دیفرانسیلی»^۱ را تعریف کرده و به بررسی مسئله انتگرال گیری نمادین برای توابع گویا می پردازیم. ابتدا مفاهیم مشتق و انتگرال جبری را برای حلقه های دیفرانسیلی معرفی کرده و ساختار انتگرال توابع گویا را بیان می کنیم. سپس با استفاده از الگوریتم تجزیه بدون مربع، روش هرمیت برای استخراج بخش گویای انتگرال و الگوریتم روتشتاین-تراگر را برای محاسبه بخش لگاریتمی آن تشریح خواهیم کرد. در نهایت، با ترکیب این روش ها، الگوریتم جامع انتگرال گیری توابع گویا را ارائه خواهیم داد. در این فصل، از منابع [۱، ۳، ۵، ۷، ۸] بهره برده ایم.

۱.۲ گذار از آنالیز به جبر

«جبر، پیشنهادی است که شیطان به ریاضی دان می دهد. شیطان می گوید: من به تو این ماشین قدرتمند را می دهم که به هر سوالی که بخواهی پاسخ می دهد. تنها کاری که باید بکنی این است که روح را به من بدهی؛ از هندسه دست بکش تا این ماشین شگفت انگیز از آن تو شود.»

— سر مایکل عطیه^۲

^۱ جبر دیفرانسیلی، شاخه ای از ریاضیات است که با افزودن عملگر مشتق به ساختارهای جبر مجرد (مانند حلقه ها و میدان ها)، به مطالعه معادلات دیفرانسیل از دیدگاه جبری می پردازد. بنیان های این شاخه در نیمه نخست قرن بیستم توسط ریاضی دانانی چون جوزف ریت (Joseph Ritt) و ایس کولچین (Ellis Kolchin) پایه گذاری شد و امروزه پایه اصلی الگوریتم های انتگرال گیری و محاسبات نمادین محسوب می شود.

^۲ سر مایکل عطیه (Sir Michael Atiyah) (۱۹۲۹-۲۰۱۹ میلادی)، ریاضی دان برجسته بریتانیایی و برنده مدال فیلدز و جایزه آبل که کارهای بنیادینی در زمینه هندسه، توپولوژی و فیزیک نظری انجام داد.

در حساب دیفرانسیل و انتگرال کلاسیک، عملگرهای مشتق و انتگرال بر پایه مفاهیمی آنالیزی مانند همگرایی، حد و پیوستگی شکل گرفته‌اند. به بیان دقیق‌تر، برای تابع دلخواه $f(x)$ که روی یک بازه مانند $[a, b]$ تعریف شده است، مشتق و انتگرال معین آن به صورت زیر تعریف می‌شوند:

$$f'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}, \quad \int_a^b f(x) dx = \lim_{n \rightarrow \infty} \sum_{i=1}^n f(x_i^*) \Delta x.$$

همچنین طبق «قضیه اساسی حسابان» می‌دانیم که انتگرال نامعین (پادمشتق) و مشتق، در واقع عمل وارون یکدیگر هستند؛ به بیان دقیق‌تر داریم

$$\int f'(x) dx = f(x) + C.$$

با کمی دقت، پی می‌بریم که تعاریف بالا با شهود و درک هندسی نیز سازگارند؛ اما در رویکرد محاسبات نمادین و سیستم‌های جبری کامپیوتری، این مفاهیم از حوزه آنالیز ریاضی جدا شده و در قالب ساختارهای جبری و به صورت انتزاعی بازتعریف می‌شوند. در این گذار، توابع به عنوان عناصری از یک میدان در نظر گرفته می‌شوند. عملگر مشتق صرفاً یک نگاشت خطی است که در قاعده ضرب صدق می‌کند و هیچ نیازی به محاسبه حد ندارد. در همین راستا، عملگر انتگرال نیز مفهوم هندسی و آنالیزی خود را از دست داده و صرفاً نقش وارون مشتق را ایفا می‌کند.

۲.۲ مشتق جبری و حلقه‌های دیفرانسیلی

برای فرمول‌بندی مسئله انتگرال‌گیری در جبر، ابتدا باید ساختارهایی تعریف کنیم که در آن عملگر مشتق به شکلی خوش‌تعریف روی عناصر آن عمل کند.

تعریف ۱.۲.۲. فرض کنیم R یک حلقه باشد. نگاشت $\delta : R \rightarrow R$ را یک مشتق روی R می‌گوییم، هرگاه در شرایط زیر صدق کند:

$$1. \quad (\text{خطی بودن نسبت به جمع}) \quad \text{برای هر } a, b \in R, \text{ داشته باشیم } \delta(a+b) = \delta(a) + \delta(b).$$

$$2. \quad (\text{قاعده ضرب یا لایب‌نیتس}^1) \quad \text{برای هر } a, b \in R, \text{ داشته باشیم } \delta(ab) = \delta(a)b + a\delta(b).$$

^۱گوتفرید ویلهلم لایب‌نیتس (Gottfried Wilhelm Leibniz) (۱۶۴۶-۱۷۱۶ میلادی)، ریاضی‌دان برجسته آلمانی که یکی از

مثال ۱.۲.۲. به عنوان یک مثال بدیهی، فرض کنیم R یک حلقه دلخواه باشد. نگاشت $\delta : R \rightarrow R$ با ضابطه $\delta(r) = 0$ برای هر $r \in R$ ، در شرایط خطی بودن و قاعده لایب‌نیتس صدق می‌کند و بنابراین یک مشتق روی R است، همچنین به عنوان یک نتیجه از قاعده لایب‌نیتس، برای عنصر ۱ حلقه داریم

$$\delta(1) = \delta(1 \cdot 1) = \delta(1) \cdot 1 + 1 \cdot \delta(1) = \delta(1) + \delta(1),$$

که با ساده کردن آن، همواره رابطه $\delta(1) = 0$ برقرار خواهد بود.

تعریف ۲.۲.۲. زوج (R, δ) شامل یک حلقه R و یک مشتق δ روی آن را یک حلقه دیفرانسیلی می‌نامیم. همچنین در صورتی که R یک میدان باشد، آن را یک میدان دیفرانسیلی می‌گوییم.

مثال ۲.۲.۲. حلقه چندجمله‌ای‌های $R = \mathbb{Q}[x]$ همراه با عملگر مشتق‌گیری استاندارد $\delta = \frac{d}{dx}$ ، تشکیل یک حلقه دیفرانسیلی می‌دهد. همچنین اگر میدان کسرها $K = \mathbb{Q}(x)$ را در نظر بگیریم، ساختار $(\mathbb{Q}(x), \frac{d}{dx})$ نمونه‌ای از یک میدان دیفرانسیلی است.

در حسابان کلاسیک، می‌دانیم که مشتق مقادیر ثابت همواره صفر است یا به اصطلاح، مقادیر ثابت تحت مشتق بی‌اثر هستند؛ از این رو، قصد داریم با الگو گرفتن از مفهوم «ثابت بودن» و تعمیم آن به حلقه‌های دیفرانسیلی، آن دسته از عناصر که مقدارشان تحت عملگر مشتق حلقه صفر می‌شود را بیشتر مورد بررسی قرار دهیم.

تعریف ۳.۲.۲. فرض کنیم (R, δ) یک حلقه دیفرانسیلی باشد. مجموعه

$$\text{Const}(R) = \{c \in R \mid \delta(c) = 0\}$$

را مجموعه ثابت‌ها می‌نامیم.

می‌توان نشان داد که مجموعه ثابت‌ها یک زیرحلقه از حلقه دیفرانسیلی است، علاوه بر آن، عملگر مشتق نسبت به عناصر مجموعه ثابت‌ها بی‌اثر عمل می‌کند. این نکات را در ادامه ثابت خواهیم کرد.

گزاره ۱.۲.۲. اگر (R, δ) یک حلقه دیفرانسیلی باشد، آنگاه $\text{Const}(R)$ یک زیرحلقه از R است، همچنین اگر R یک میدان باشد، $\text{Const}(R)$ نیز یک زیرمیدان از R خواهد بود که آن را میدان ثابت‌ها می‌نامیم.

پایه‌گذاران اصلی حساب دیفرانسیل و انتگرال به شمار می‌رود.

اثبات. برای اثبات زیرحلقه بودن، ابتدا نشان می‌دهیم که عنصر همانی جمع $\circ$ و عنصر همانی ضرب $\cdot$ حلقه R در آن قرار دارند. طبق خواص مشتق و مشابه مثال ۱.۲.۲، داریم $\delta(\circ) = \circ$ و $\delta(1) = \circ$. بنابراین، عناصر $\circ$ و 1 حلقه نیز در $\text{Const}(R)$ موجود هستند. حال فرض کنیم $a, b \in \text{Const}(R)$ دو عنصر دلخواه باشند که نشان‌دهنده این است که $\delta(a) = \circ$ و $\delta(b) = \circ$. با استفاده از خواص خطی بودن و قاعده لایب‌نیتس مشتق داریم

$$\delta(a + b) = \delta(a) + \delta(b) = \circ + \circ = \circ,$$

$$\delta(ab) = \delta(a)b + a\delta(b) = \circ \cdot b + a \cdot \circ = \circ.$$

از آنجا که این مجموعه شامل عنصر همانی جمع و ضرب است و نسبت به این اعمال نیز بسته است^۱، نتیجه می‌گیریم که $\text{Const}(R)$ یک زیرحلقه از R است. حال فرض کنیم R یک میدان و $a \in \text{Const}(R)$ یک عنصر دلخواه ناصفر باشد. می‌خواهیم نشان دهیم $a^{-1} \in \text{Const}(R)$ یا به عبارت دیگر $\delta(a^{-1}) = \circ$. با مشتق‌گیری از تساوی $aa^{-1} = 1$ و قاعده لایب‌نیتس خواهیم داشت

$$\delta(aa^{-1}) = \delta(1) = \circ \implies \delta(a)a^{-1} + a\delta(a^{-1}) = \circ.$$

از آنجایی که $\delta(a) = \circ$ ، نتیجه می‌گیریم $a\delta(a^{-1}) = \circ$. از آنجا که R یک میدان است و $a \neq \circ$ ، داریم $\delta(a^{-1}) = \circ$. بنابراین $a^{-1} \in \text{Const}(R)$ و این نشان می‌دهد که مجموعه ثابت‌ها در صورت میدان بودن R ، تشکیل یک میدان می‌دهد. $\square$

لم ۱.۲.۲. فرض کنیم (R, δ) یک حلقه دیفرانسیلی باشد. برای هر عنصر دلخواه $a \in R$ و هر عنصر ثابت $c \in \text{Const}(R)$ داریم $\delta(ca) = c\delta(a)$.

اثبات. با استفاده از قاعده لایب‌نیتس به آسانی اثبات می‌شود. $\square$

مثال ۳.۲.۲. در حلقه دیفرانسیلی $(\mathbb{R}[x], \frac{d}{dx})$ ، از برقراری شرط $\delta(P) = \frac{d}{dx}P = \circ$ نتیجه می‌شود که چندجمله‌ای P باید یک مقدار ثابت حقیقی باشد؛ بنابراین $\text{Const}(\mathbb{R}[x]) = \mathbb{R}$.

^۱در اینجا منظور از بسته بودن این است که عملگرهای دوتایی جمع و ضرب حلقه R ، در صورت تحدید به این زیرمجموعه، همچنان نگاشت‌هایی خوش‌تعریف به شکل $\text{Const}(R) \times \text{Const}(R) \rightarrow \text{Const}(R)$ ، $+, \cdot$ تشکیل دهند.

فرض کنیم (R, δ) یک حلقه دیفرانسیلی باشد. عملگر مشتق δ به طور متعارف می‌تواند از حلقه زمینه R به حلقه چندجمله‌ای‌های $R[x]$ گسترش یابد، به طوری که برای هر چندجمله‌ای $P = \sum_{i=0}^n a_i x^i$ ، مشتق کلی آن با استفاده از قاعده لایب‌نیتس به صورت زیر تعریف می‌شود:

$$\delta(P) = \sum_{i=0}^n (\delta(a_i)x^i + ia_i x^{i-1} \delta(x)).$$

در بیشتر موارد، حلقه زمینه به گونه‌ای است که $\delta(a_i) = 0$ و $\delta(x) = 1$. تحت این شرایط، رابطه بالا به شکل زیر ساده می‌شود:

$$P' = \sum_{i=1}^n ia_i x^{i-1}$$

چنین نتیجه‌ای سبب می‌شود این دسته از مشتق‌ها اهمیت بیشتری در بحث ما داشته باشند.

تعریف ۴.۲.۲. فرض کنیم R یک حلقه و $P = \sum_{i=0}^n a_i x^i$ یک چندجمله‌ای دلخواه در حلقه چندجمله‌ای‌های $R[x]$ باشد. **مشتق صوری** P نسبت به متغیر x ، که آن را با نماد P' یا $\frac{d}{dx}P$ نشان می‌دهیم، به صورت زیر تعریف می‌شود:

$$P' = \sum_{i=1}^n ia_i x^{i-1}.$$

بدیهی است که تعریف بالا باید ویژگی‌های یک مشتق را در تعریف ۱.۲.۲ داشته باشد.

گزاره ۲.۲.۲. مشتق صوری تعریف شده در بالا، یک عملگر مشتق معتبر روی حلقه $R[x]$ است. به بیان دیگر، برای هر $P, Q \in R[x]$ و عنصر ثابت $c \in R$ داریم

$$1. (P + Q)' = P' + Q'$$

$$2. (PQ)' = P'Q + PQ'$$

$$3. (cP)' = cP'$$

اثبات. با استفاده از تعریف مشتق صوری و خواص جمع و ضرب چندجمله‌ای‌ها به آسانی اثبات می‌شود. $\square$

مثال ۴.۲.۲. فرض کنیم $R = \mathbb{Z}[t]$. برای چندجمله‌ای $P = t^2 x^3 + 2tx \in \mathbb{Z}[t][x]$ ، با استفاده از تعریف مشتق صوری نسبت به متغیر x داریم $P' = t^2 \cdot (3x^2) + 2t \cdot (1) = 3t^2 x^2 + 2t$. در این مثال، عناصر

حلقه زمینه $R = \mathbb{Z}[t]$ (شامل ضرایب صحیح و متغیر t) در مشتق‌گیری نسبت به x به عنوان یک عنصر ثابت عمل می‌کنند.

همان‌طور که در فصل گذشته دیدیم، هر دامنه صحیح را می‌توان به میدان کسرهای آن گسترش داد. اکنون این پرسش مطرح می‌شود که اگر یک دامنه صحیح دارای یک عملگر مشتق باشد، می‌توان این مشتق را نیز به میدان کسرهای آن تعمیم داد؟ قضیه زیر نشان می‌دهد که این تعمیم ممکن و ضابطه آن نیز به صورت یکتاست. در واقع، این قضیه همان قاعده آشنای مشتق‌گیری از خارج‌قسمت در آنالیز است که ما از دیدگاه جبری به آن می‌پردازیم.

قضیه ۲.۲.۲. فرض کنیم D یک دامنه صحیح و δ یک عملگر مشتق روی آن باشد. در این صورت، مشتق δ به طور یکتا به میدان کسرهای $K = \text{Frac}(D)$ تعمیم می‌یابد؛ به طوری که برای هر عنصر $\frac{a}{b} \in K$ ، مشتق آن به صورت زیر تعریف می‌شود:

$$\delta\left(\frac{a}{b}\right) = \frac{\delta(a)b - a\delta(b)}{b^2}.$$

اثبات. ابتدا نشان می‌دهیم ضابطه ارائه‌شده خوش‌تعریف است. فرض کنیم $\frac{a}{b} = \frac{c}{d}$ ، بنابراین $ad = bc$. با مشتق‌گیری از طرفین دامنه صحیح D داریم

$$\delta(a)d + a\delta(d) = \delta(b)c + b\delta(c).$$

با ضرب طرفین این رابطه در bd و استفاده از جایگذاری $ad = bc$ برای بازآرایی جملات، پس از فاکتورگیری به تساوی زیر در دامنه صحیح D می‌رسیم:

$$(\delta(a)b - a\delta(b))d^2 = (\delta(c)d - c\delta(d))b^2.$$

این تساوی طبق تعریف میدان کسرها، برابری زیر را در میدان K نتیجه می‌دهد:

$$\frac{\delta(a)b - a\delta(b)}{b^2} = \frac{\delta(c)d - c\delta(d)}{d^2}.$$

خطی بودن و قاعده لایب‌نیتس نیز با روندی مشابه نتیجه می‌شوند. اکنون یکتایی این تعمیم را نشان می‌دهیم. فرض کنیم مشتق δ به میدان کسرها تعمیم یافته باشد. در میدان K ، داریم $b \cdot \frac{a}{b} = a$. با اعمال عملگر δ بر دو

طرف و استفاده از قاعده لایب‌نیتس، خواهیم داشت

$$\delta(b) \frac{a}{b} + b \delta\left(\frac{a}{b}\right) = \delta(a).$$

با انتقال جمله اول به سمت راست و ضرب طرفین در $\frac{1}{b}$ داریم

$$\delta\left(\frac{a}{b}\right) = \frac{\delta(a) - \delta(b) \frac{a}{b}}{b} = \frac{\delta(a)b - a\delta(b)}{b^2}. \quad \square$$

۳.۲ تجزیه بدون مربع

در محاسبات نمادین و الگوریتم‌های انتگرال‌گیری، تجزیه کامل یک چندجمله‌ای به عوامل تحویل‌ناپذیر، عملیاتی به‌شدت پرهزینه و زمان‌بر است. در عوض، از رویکردی کارآمدتر به نام «تجزیه بدون مربع» بهره می‌بریم که تنها با محاسبه مشتق صوری و ب.م.م، یک چندجمله‌ای را به حاصل ضرب توان‌هایی از عوامل فاقد ریشه تکراری تجزیه می‌کند.

تذکر ۱.۳.۲. از این به بعد، قرارداد می‌کنیم که میدان K همواره یک میدان با مشخصه صفر (مانند $\mathbb{Q}$ ، $\mathbb{R}$ یا $\mathbb{C}$) است، مگر این که در جایی خلاف آن ذکر شود. ضرورت این فرض به خاطر رفتار عملگر مشتق صوری است؛ در میدانی با مشخصه $p > 0$ ، برای چندجمله‌ای غیرثابتی مانند x^p ، داریم $(x^p)' = px^{p-1} = 0$. این پدیده سبب می‌شود رابطه میان ریشه‌های تکراری یک چندجمله‌ای و مشتق آن از بین برود و در نتیجه، الگوریتم‌هایی مبتنی بر چنین ایده‌ای، کارایی خود را از دست بدهند.

تعریف ۱.۳.۲. چندجمله‌ای $A \in K[x]$ را بدون مربع می‌نامیم، هرگاه هیچ چندجمله‌ای $B \in K[x] \setminus K$ وجود نداشته باشد که $B^2 \mid A$.

با استفاده از مشتق صوری که در بخش قبل معرفی کردیم، می‌توانیم محکی برای تشخیص بدون مربع بودن یک چندجمله‌ای ارائه دهیم.

قضیه ۱.۳.۲. چندجمله‌ای $A \in K[x] \setminus K$ بدون مربع است اگر و تنها اگر $\gcd(A, A') = 1$.

اثبات. $(\Rightarrow)$ فرض کنیم $\deg(\gcd(A, A')) > 0$. در این صورت یک عامل تحویل‌ناپذیر مانند $P \in K[x]$ وجود دارد که $P \mid A$ و $P \mid A'$. از آنجا که $P \mid A$ ، یک چندجمله‌ای $Q \in K[x]$ وجود دارد که $A = PQ$. با مشتق‌گیری خواهیم داشت $A' = P'Q + PQ'$. از آنجا که $P \mid A'$ و $P \mid PQ'$ ، نتیجه می‌گیریم $P \mid P'Q$. از آنجا که $\deg(P') < \deg(P)$ و P تحویل‌ناپذیر است، داریم $\gcd(P, P') = 1$. بنابراین $P \mid Q$. در نهایت داریم $P^2 \mid A$ که با بدون مربع بودن A در تناقض است.

$(\Leftarrow)$ فرض کنیم A بدون مربع نباشد. در نتیجه، برای چندجمله‌ای‌های $B, C \in K[x]$ که $\deg(B) > 0$ ، داریم $A = B^2 C$. با مشتق‌گیری خواهیم داشت

$$A' = 2BB'C + B^2 C' = B(2B'C + BC').$$

در نتیجه $B \mid A$ و $B \mid A'$. بنابراین $B \mid \gcd(A, A') \neq 1$. $\square$

تعریف ۲.۳.۲. تجزیه بدون مربع برای یک چندجمله‌ای $A \in K[x]$ ، تجزیه‌ای به شکل زیر است:

$$A = \prod_{i=1}^k A_i^i = A_1 A_2^2 \cdots A_k^k,$$

به طوری که هر A_i یک چندجمله‌ای بدون مربع است و برای هر $i \neq j$ ، داریم $\gcd(A_i, A_j) = 1$.

از آنجایی که بحثمان در مورد «تجزیه» است، طرح مفهومی مانند «یکتایی تجزیه» که در فصل قبلی به آن اشاره کردیم، دور از انتظار نیست. در ادامه، با ارائه و اثبات یک لم، یکتایی تجزیه بدون مربع را ثابت می‌کنیم.

لم ۲.۳.۲. فرض کنیم K یک میدان باشد. چندجمله‌ای $A \in K[x] \setminus K$ را در نظر می‌گیریم. اگر دو تجزیه A به صورت

$$A = c \prod_{i=1}^k A_i^i = d \prod_{j=1}^m B_j^j$$

وجود داشته باشند، به طوری که $c, d \in K^*$ و چندجمله‌ای‌های $A_i, B_j \in K[x]$ همگی تکین و بدون مربع باشند، آنگاه $c = d$ و $k = m$ و با یک بازآرایش و تطابق مناسب اندیس‌ها، برای هر $1 \leq i \leq k$ داریم $A_i = B_i$.

اثبات. طبق لم ۲.۴.۱، حلقه چندجمله‌ای‌های $K[x]$ یک دامنه تجزیه یکتا است؛ بنابراین هر چندجمله‌ای ناصفر تجزیه‌ای یکتا به حاصل ضرب عوامل اول تحویل‌ناپذیر دارد. با دسته‌بندی عوامل تحویل‌ناپذیر بر حسب توان‌های متناظر در تجزیه یکتای A ، هر مولفه A_i حاصل ضرب عواملی خواهد بود که با توان دقیق i در تجزیه ظاهر شده‌اند. از یکتایی تجزیه به عوامل اول و تطابق توان‌ها نتیجه می‌گیریم $k = m$ و برابری ضرایب پیشرو و شرط تکین بودن، تساوی مولفه‌ها را ثابت می‌کند. $\square$

الگوریتم زیر، روشی استاندارد برای استخراج مولفه‌های تجزیه بدون مربع یک چندجمله‌ای در میدان‌هایی با مشخصه صفر فراهم می‌کند.

الگوریتم ۱.۲ تجزیه بدون مربع چندجمله‌ای‌های تک‌متغیره $\text{SquareFree}(A)$

Require: $A \in K[x]$ where $\deg(A) > 0$

Ensure: Square-free factors $A_1, A_2, \dots, A_k$

```

 $C \leftarrow \text{Euclidean}(A, A')$ 
 $(W, -) \leftarrow \text{PolyDivide}(A, C)$ 
 $(Y, -) \leftarrow \text{PolyDivide}(A', C)$ 
 $Z \leftarrow Y - W'$ 
 $i \leftarrow 1$ 
while  $W \neq 1$  do
     $A_i \leftarrow \text{Euclidean}(W, Z)$ 
     $(W, -) \leftarrow \text{PolyDivide}(W, A_i)$ 
     $(Q, -) \leftarrow \text{PolyDivide}(Z, A_i)$ 
     $Z \leftarrow Q - W'$ 
     $i \leftarrow i + 1$ 
end while
return  $(A_1, A_2, \dots, A_{i-1})$ 

```

قضیه ۳.۳.۲. الگوریتم ۱.۲ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

□

اثبات. به [۸] مراجعه شود.

مثال ۱.۳.۲. چندجمله‌ای $A = x^3 - 3x + 2$ را در حلقه $\mathbb{Q}[x]$ در نظر می‌گیریم. با مشتق‌گیری صوری A ، داریم $A' = 3x^2 - 3$. همچنین در گام آغازین $\text{SquareFree}(A)$ داریم

$$\begin{cases} C = \text{Euclidean}(A, A') = x - 1, \\ (W, R) = \text{PolyDivide}(A, C) \implies W = x^2 + x - 2, \\ (Y, R) = \text{PolyDivide}(A', C) \implies Y = 3x + 3, \\ Z = Y - W' = (3x + 3) - (2x + 1) = x + 2. \end{cases}$$

مراحل اجرای حلقه به صورت زیر است:

گام	W	Z	A_i	Q	$\frac{W}{A_i}$	$Q - W'$
۱	$x^2 + x - 2$	$x + 2$	$x + 2$	۱	$x - 1$	۰
۲	$x - 1$	۰	$x - 1$	۰	۱	۰

در پایان تکرار دوم از آنجا که $W = 1$ ، حلقه پایان می‌یابد و الگوریتم عوامل $A_1 = x + 2$ و $A_2 = x - 1$ را به عنوان خروجی برمی‌گرداند؛ بنابراین $A = A_1 A_2 = (x + 2)(x - 1)^2$.

کاربرد اصلی تجزیه بدون مربع در مسئله انتگرال‌گیری، شکستن مخرج کسر به عواملی با توان‌های تفکیک‌شده است. قضیه زیر نشان می‌دهد که چگونه هر تابع گویا را می‌توان به کسرهای جزئی بر حسب عوامل بدون مربع تجزیه کرد.

قضیه ۴.۳.۲. فرض کنیم K یک میدان باشد. کسر گویای $\frac{A}{D} \in K(x)$ را با شرط $\gcd(A, D) = 1$ و $\deg(A) < \deg(D)$ در نظر می‌گیریم. اگر تجزیه بدون مربع مخرج به صورت

$$D = \prod_{i=1}^k D_i^{e_i} = D_1 D_2 \cdots D_k^k$$

باشد، آنگاه چندجمله‌ای‌های یکتای $A_{i,j} \in K[x]$ وجود دارند، به طوری که برای هر $1 \leq i \leq k$ و $1 \leq j \leq e_i$

i ، داریم $\deg(A_{i,j}) < \deg(D_i)$ و همچنین

$$\frac{A}{D} = \sum_{i=1}^k \sum_{j=1}^i \frac{A_{i,j}}{D_i^j}.$$

اثبات. ابتدا برای هر $1 \leq i \leq k$ ، چندجمله‌ای $U_i = \frac{D}{D_i^i}$ را تعریف می‌کنیم. از آنجا که عوامل D_i^i دو به دو نسبت به هم اول هستند، داریم $\gcd(U_1, \dots, U_k) = 1$. طبق اتحاد بزو، چندجمله‌ای‌هایی مانند $S_1, \dots, S_k$ وجود دارند که

$$\sum_{i=1}^k S_i U_i = 1.$$

با ضرب این تساوی در کسر $\frac{A}{D}$ و با توجه به اینکه $D = U_i D_i^i$ ، داریم

$$\frac{A}{D} = \sum_{i=1}^k \frac{A S_i U_i}{D} = \sum_{i=1}^k \frac{A S_i}{D_i^i}.$$

اگر هر $A S_i$ را بر D_i^i تقسیم کنیم، باقیمانده‌ای مانند B_i با شرط $\deg(B_i) < \deg(D_i^i)$ حاصل می‌شود. از آنجایی که $\deg(A) < \deg(D)$ ، مجموع خارج‌قسمت‌های این تقسیم‌ها صفر خواهد بود و رابطه به شکل $\frac{A}{D} = \sum_{i=1}^k \frac{B_i}{D_i^i}$ تبدیل می‌شود. در مرحله بعد، برای تفکیک هر کسر $\frac{B_i}{D_i^i}$ ، صورت B_i را به طور متوالی بر D_i تقسیم می‌کنیم:

$$B_i = Q_1 D_i + A_{i,i},$$

$$Q_1 = Q_2 D_i + A_{i,i-1},$$

$$\vdots$$

$$Q_{i-1} = 0 \cdot D_i + A_{i,1}.$$

با جایگذاری متوالی این روابط، بسط B_i به صورت $B_i = \sum_{j=1}^i A_{i,j} D_i^{i-j}$ حاصل می‌شود، به طوری که $\deg(A_{i,j}) < \deg(D_i)$. در نهایت با تقسیم این بسط بر D_i^i کسرهای جزئی به صورت $\frac{A_{i,j}}{D_i^j}$ تولید می‌شوند. یکتایی این تجزیه مستقیماً از یکتایی خارج‌قسمت و باقیمانده در الگوریتم تقسیم حلقه چندجمله‌ای‌ها نتیجه

□

می‌شود.

مثال ۲.۳.۲. کسر گویای $\frac{A}{D} = \frac{3x^2+3x+3}{x^3-3x+2}$ را در $\mathbb{Q}(x)$ در نظر می‌گیریم. طبق مثال ۱.۳.۲، تجزیه بدون مربع مخرج به صورت $D = D_1 D_2^2 = (x+2)(x-1)^2$ است. با اعمال الگوریتم $\text{ExtEuclidean}(D_1, D_2^2)$ ، رابطه بزو به شکل زیر حاصل می‌شود:

$$\frac{1}{9}(x-1)^2 + \frac{-x+4}{9}(x+2) = 1.$$

با ضرب این تساوی در صورت کسر (A) و استخراج باقیمانده‌ها بر اساس روند اثبات قضیه ۴.۳.۲، تفکیک اولیه به دست می‌آید:

$$\frac{A}{D} = \frac{1}{x+2} + \frac{2x+1}{(x-1)^2}.$$

اکنون با اجرای $\text{PolyDivide}(2x+1, x-1)$ ، داریم $2x+1 = 2(x-1) + 3$. در نهایت با جایگذاری در کسر دوم، نمایش کسرهای جزئی بدون مربع به دست می‌آید:

$$\frac{3x^2+3x+3}{x^3-3x+2} = \frac{1}{x+2} + \frac{2}{x-1} + \frac{3}{(x-1)^2}.$$

۴.۲ انتگرال جبری و ساختار انتگرال توابع گویا

همان‌طور که عملگر مشتق را از مفهوم حد جدا کرده و در قالب حلقه‌های دیفرانسیلی بازتعریف کردیم، عملگر انتگرال نیز در این ساختار، ماهیتی جبری به خود می‌گیرد. در واقع، انتگرال صرفاً به عنوان عملگر وارون مشتق در یک میدان دیفرانسیلی شناخته می‌شود.

تعریف ۱.۴.۲. فرض کنیم (K, δ) یک میدان دیفرانسیلی و $a \in K$ یک عنصر دلخواه باشد. اگر عنصری مانند b (در K یا در یک توسیع دیفرانسیلی^۱ از K) وجود داشته باشد که $\delta(b) = a$ ، در این صورت b را یک **انتگرال** a می‌نامیم و آن را با نماد $\int a$ نمایش می‌دهیم.

^۱توسیع دیفرانسیلی یک میدان دیفرانسیلی مانند K ، میدان دیفرانسیلی بزرگتری است که K را به عنوان یک زیرمیدان در بر گرفته و عملگر مشتق آن در صورت اعمال بر عناصر K ، دقیقاً همان عملگر مشتق اولیه را نتیجه می‌دهد. مفاهیم و ساختار دقیق توسیع‌های دیفرانسیلی را در فصل آینده به تفصیل بررسی خواهیم کرد.

اکنون با چند ویژگی مقدماتی انتگرال جبری آشنا می‌شویم.

گزاره ۱.۴.۲. فرض کنیم (K, δ) یک میدان دیفرانسیلی با میدان ثابت‌های $C = \text{Const}(K)$ باشد. عملگر انتگرال در ویژگی‌های زیر صدق می‌کند:

۱. (یکتایی در حد ثابت) اگر b_1 و b_2 هر دو انتگرال عنصر $a \in K$ باشند، آنگاه $b_1 - b_2 = c \in C$.

۲. (خطی بودن) برای هر $a, b \in K$ و ثابت $c \in C$ داریم $\int (ca + b) = c \int a + \int b$.

۳. (انتگرال‌گیری جزء به جزء) برای هر $a, b \in K$ داریم $\int a \delta(b) = ab - \int b \delta(a)$.

اثبات. برای اثبات ویژگی اول، فرض می‌کنیم $\delta(b_1) = a$ و $\delta(b_2) = a$. با کم کردن این دو رابطه و استفاده از خطی بودن عملگر δ داریم

$$\delta(b_1 - b_2) = 0.$$

طبق تعریف، $b_1 - b_2$ عنصری ثابت در C است. ویژگی دوم نتیجه مستقیم خطی بودن عملگر مشتق است. برای ویژگی سوم، با اعمال عملگر انتگرال بر دو طرف قاعده لایب‌نیتس $\delta(ab) = \delta(a)b + a\delta(b)$ خواهیم داشت

$$ab = \int b \delta(a) + \int a \delta(b).$$

□

با بازآرایی جملات، فرمول جزء به جزء به صورت جبری ثابت می‌شود.

مثال ۱.۴.۲. میدان دیفرانسیلی $(\mathbb{Q}(x), \frac{d}{dx})$ را در نظر می‌گیریم. برای عنصر $a = \frac{-2x}{(x^2+1)^2} \in \mathbb{Q}(x)$ ، از آنجا که $\frac{d}{dx} \left(\frac{1}{x^2+1} \right) = a$ ، عنصر $b = \frac{1}{x^2+1}$ یک انتگرال a است که در خود میدان $\mathbb{Q}(x)$ قرار دارد. اما برای عنصر $c = \frac{1}{x} \in \mathbb{Q}(x)$ هیچ عنصری در $\mathbb{Q}(x)$ یافت نمی‌شود که مشتق آن برابر با c باشد. از این رو، انتگرال این عنصر (یعنی $\ln(x)$) در میدان پایه موجود نبوده و تعیین آن نیازمند یک توسیع دیفرانسیلی از $\mathbb{Q}(x)$ است.

تذکر ۱.۴.۲. از آنجا که متغیر مشتق‌گیری در حلقه دیفرانسیلی $(K(x), \frac{d}{dx})$ از پیش مشخص است، برای سادگی نمادگذاری و تأکید بر ماهیت جبری عملگر، از نوشتن جزء دیفرانسیلی dx در کنار نماد انتگرال صرف‌نظر می‌کنیم.

پیش از ورود به الگوریتم‌های محاسبه انتگرال، لازم است بدانیم خروجی انتگرال یک تابع گویا دقیقا به چه صورت است. طبق «قضیه لیوویل^۱»، که مفاهیم پیش‌نیاز و اثبات دقیق آن را در فصل آینده بررسی خواهیم کرد، انتگرال هر تابع $f \in K(x)$ به دو بخش مجزا تفکیک می‌شود:

$$\int f = v + \sum_{i=1}^k c_i \ln(u_i).$$

در این رابطه، $v \in K(x)$ یک تابع گویا است و بخش گویای انتگرال نامیده می‌شود. عبارت دوم که شامل مجموعی از توابع لگاریتمی است (که در آن $u_i \in K[x]$ و c_i ها مقادیری ثابت هستند که لزوما در میدان K قرار ندارند)، بخش لگاریتمی انتگرال نام دارد. هدف اصلی در انتگرال‌گیری نمادین توابع گویا، ارائه الگوریتم‌هایی است که این دو بخش را به صورت مجزا و طی فرآیندی متناهی استخراج کنند.

مثال ۲.۴.۲. تابع گویای $f = \frac{2x^2 - x + 1}{x^2 - x - 1}$ را در $\mathbb{Q}(x)$ در نظر می‌گیریم. انتگرال این تابع به شکل زیر تفکیک می‌شود:

$$\int f = \frac{1}{x} + 2 \ln(x - 1).$$

در اینجا، کسر $\frac{1}{x}$ بخش گویای انتگرال و عنصری در $\mathbb{Q}(x)$ است و عبارت $2 \ln(x - 1)$ بخش لگاریتمی آن را تشکیل می‌دهد.

۵.۲ روش هرمیت

در اواخر قرن نوزدهم میلادی، «شارل هرمیت^۲» روشی جبری برای محاسبه انتگرال توابع گویا ارائه داد که نیاز به یافتن ریشه‌های مخرج (تجزیه کامل به عوامل تحویل‌ناپذیر) را به طور کامل برطرف می‌کرد. این روش مبتنی بر تجزیه بدون مربع مخرج و محاسبه ضرایب بزو است و بخش گویای انتگرال را با فرآیندی کاهشی از بخش لگاریتمی آن تفکیک می‌کند. طبق قضیه ۴.۳.۲، هر تابع گویای سره $\frac{A}{D} \in K(x)$ را می‌توان به صورت مجموع

^۱ ژوزف لیوویل (Joseph Liouville) (۱۸۸۲-۱۸۰۹ میلادی)، ریاضی‌دان برجسته فرانسوی که با پایه‌گذاری نظریه انتگرال‌گیری در فرم‌های متناهی، گام بزرگی در مسیر پیوند زدن حسابان به جبر برداشت.
^۲ شارل هرمیت (Charles Hermite) (۱۹۰۱-۱۸۲۲ میلادی)، ریاضی‌دان برجسته فرانسوی که دستاوردهای مهمی در نظریه اعداد، جبر خطی و توابع بیضوی داشت.

کسرهایی به صورت $\frac{B}{V^m}$ تجزیه کرد، به طوری که V یک چندجمله‌ای بدون مربع، $m \geq 1$ و $\deg(B) < m$ باشد. برای محاسبه انتگرال این تابع، عباراتی که در آن‌ها $m = 1$ ، به عنوان بخش لگاریتمی در نظر گرفته می‌شوند و عبارات با $m > 1$ طی یک فرآیند جبری به کسرهایی با توان مخرج کمتر تبدیل خواهند شد.

تذکر ۱.۵.۲. در الگوریتم‌های انتگرال‌گیری توابع گویا، پیش فرض محاسبات بر این است که با یک تابع گویای $\frac{A}{D}$ مواجه هستیم؛ یعنی تابعی مانند $\frac{A}{D}$ که درجه صورت آن اکیدا کمتر از مخرج باشد. اگر تابع گویای مفروض ناسره باشد، پیش از اعمال الگوریتم، با استفاده از الگوریتم تقسیم چندجمله‌ای‌ها صورت را بر مخرج تقسیم می‌کنیم ($A = DQ + R$). با این کار، انتگرال به شکل زیر تفکیک می‌شود:

$$\int \frac{A}{D} = \int Q + \int \frac{R}{D}.$$

انتگرال چندجمله‌ای Q با قواعد پایه جبری محاسبه شده و کسر باقیمانده $\frac{R}{D}$ که اکنون یک کسر سره است، به عنوان ورودی به فرآیند کاهش هر میت تحویل داده می‌شود.

فرض کنیم انتگرال $\int \frac{B}{V^m}$ با شرایط $m > 1$ و بدون مربع بودن V مفروض باشد. از آنجا که V فاقد ریشه تکراری است ($\gcd(V, V') = 1$)، با استفاده از الگوریتم اقلیدسی تعمیم‌یافته چندجمله‌ای‌های $S, T \in K[x]$ وجود دارند که در معادله زیر صدق کنند:

$$SV + TV' = B, \quad (*)$$

به طوری که $\deg(T) < \deg(V)$. با تقسیم طرفین این معادله بر V^m داریم:

$$\frac{B}{V^m} = \frac{S}{V^{m-1}} + \frac{TV'}{V^m}.$$

حال با اعمال عملگر انتگرال بر طرفین و استفاده از قاعده انتگرال‌گیری جزء به جزء برای کسر دوم، به دست می‌آوریم:

$$\int \frac{TV'}{V^m} = \frac{-T}{(m-1)V^{m-1}} + \int \frac{T'}{(m-1)V^{m-1}}.$$

با جایگذاری این نتیجه در انتگرال رابطه (*)، کاهش توان مخرج به صورت زیر انجام می‌شود:

$$\int \frac{B}{V^m} = \frac{-T}{(m-1)V^{m-1}} + \int \frac{S + \frac{1}{m-1}T'}{V^{m-1}}.$$

این فرآیند تا رسیدن به مخرجی با توان یک ($m = 1$) تکرار می‌شود و در هر گام، بخشی از عبارت گویای نهایی تولید خواهد شد. در نهایت، ساختار کسر اولیه به دو چندجمله‌ای $G, H \in K[x]$ و چندجمله‌ای بدون مربع $U \in K[x]$ کاهش می‌یابد:

$$\int \frac{A}{D} = \frac{G}{U^*} + \int \frac{H}{U}.$$

در این نمایش، $\frac{G}{U^*}$ نماینده بخش گویای انتگرال و $\int \frac{H}{U}$ بخش لگاریتمی آن است که مخرج آن (U) بدون ریشه تکراری است. ساختار دقیق الگوریتم، در ادامه ارائه شده است.

الگوریتم ۲.۲ کاهش هرمیت (استخراج بخش گویا) $\text{HermiteReduce}(A, D)$

Require: $A, D \in K[x]$ where $\gcd(A, D) = 1$ and $\deg(A) < \deg(D)$

Ensure: Rational part and logarithmic part integrand

$G \leftarrow 0, H \leftarrow 0, U \leftarrow 1$

$(D_1, \dots, D_k) \leftarrow \text{SquareFree}(D)$

Find $A_{i,j} \in K[x]$ such that $\frac{A}{D} = \sum_{i=1}^k \sum_{j=1}^i \frac{A_{i,j}}{D_i^j}$ {Based on Theorem 2.3.4}

for $i = 1$ **to** k **do**

$U \leftarrow U \cdot D_i$

$H \leftarrow H + A_{i,1} \cdot \frac{U}{D_i}$

for $j = i$ **downto** 2 **do**

$B \leftarrow A_{i,j}$

Find $S, T \in K[x]$ such that $SD_i + TD'_i = B$ and $\deg(T) < \deg(D_i)$

$G \leftarrow G + \frac{-T}{(j-1)D_i^{j-1}}$

$A_{i,j-1} \leftarrow A_{i,j-1} + S + \frac{T'}{j-1}$

end for

end for

return $(G, \frac{H}{U})$

قضیه ۱.۵.۲. الگوریتم ۲.۲ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

اثبات. ابتدا پایان‌پذیری الگوریتم را بررسی می‌کنیم. الگوریتم از دو حلقه متناهی **for** تشکیل شده است که کران‌های آن‌ها بر اساس درجات و توان‌های مقسوم‌علیه‌های چندجمله‌ای مخرج (D) تعیین شده‌اند. تنها مرحله‌ای که ممکن است باعث توقف نشدن اجرای الگوریتم شود، محاسبه ضرایب S و T است. از آنجا که هر D_i خروجی الگوریتم تجزیه بدون مربع است، فاقد ریشه تکراری بوده و $\gcd(D_i, D'_i) = 1$. در نتیجه، الگوریتم اقلیدسی تعمیم‌یافته همواره در زمان متناهی معادله مربوط به ضرایب بزو را حل می‌کند. بنابراین کل الگوریتم پایان‌پذیر است.

برای اثبات درستی محاسبات، در نظر می‌گیریم که روند با تجزیه کسر اولیه به کسرهای جزئی آغاز می‌شود:

$$\int \frac{A}{D} = \sum_{i=1}^k \sum_{j=1}^i \int \frac{A_{i,j}}{D_i^j}.$$

در حلقه داخلی، برای هر چندجمله‌ای بدون مربع D_i و به ازای هر توان $j \geq 2$ ، قرار می‌دهیم $B = A_{i,j}$. از آنجا که $\gcd(D_i, D'_i) = 1$ ، چندجمله‌ای‌های S و T وجود دارند که $SD_i + TD'_i = B$ و $\deg(T) < \deg(D_i)$. با تقسیم طرفین بر D_i^j و انتگرال‌گیری جزء به جزء، دقیقاً همانند روند تشریح شده در رابطه (*)، به دست می‌آوریم:

$$\int \frac{B}{D_i^j} = \frac{-T}{(j-1)D_i^{j-1}} + \int \frac{S + \frac{1}{j-1}T'}{D_i^{j-1}}.$$

بر اساس این رابطه، الگوریتم در هر گام کسر خارج از انتگرال را به بخش گویای پاسخ (متغیر G) اضافه می‌کند. هم‌زمان، صورت کسر درون انتگرال را به عنوان صورت جدید $(A_{i,j-1})$ برای مخرجی با یک توان کمتر $(j-1)$ جایگذاری می‌کند تا در تکرار بعدی حلقه محاسبه شود. از آنجا که $\deg(B) < \deg(D_i)$ و $\deg(T) < \deg(D_i)$ ، از رابطه $SD_i = B - TD'_i$ نتیجه می‌شود که $\deg(S) < \deg(D_i) - 1$. بنابراین صورت کسر باقیمانده یعنی $S + \frac{1}{j-1}T'$ همچنان درجه‌ای اکیدا کمتر از D_i خواهد داشت. پس از پایان حلقه داخلی ($j=2$)، تمامی عبارات با توان مخرج بزرگتر از یک تجزیه شده‌اند و تنها کسرهایی به صورت $\frac{A_{i,1}}{D_i}$ باقی می‌مانند. متغیر $U = \prod_{i=1}^k D_i$ محاسبه شده و متغیر H مجموع این کسرهای باقیمانده را با مخرج مشترک U تشکیل می‌دهد:

$$\frac{H}{U} = \sum_{i=1}^k \frac{A_{i,1}}{D_i} = \sum_{i=1}^k A_{i,1} \frac{U}{D_i}.$$

با توجه به حفظ شدن کران درجات در تمام مراحل، درجه صورت نهایی (H) نیز اکیدا کمتر از مخرج (U) خواهد بود. $\square$

مثال ۱.۵.۲. تابع گویای $\frac{A}{D} = \frac{3x^2+3x+3}{x^3-3x+2}$ را در $\mathbb{Q}(x)$ در نظر می‌گیریم. در مثال پایانی بخش قبل، تجزیه کسرهای جزئی بدون مربع این تابع را به صورت زیر محاسبه کردیم:

$$\frac{A}{D} = \frac{1}{x+2} + \frac{2}{x-1} + \frac{3}{(x-1)^2}.$$

دو کسر اول مخرج‌هایی با توان یک دارند و بخش لگاریتمی را تشکیل می‌دهند. با اعمال الگوریتم هرمیت روی کسر سوم، داریم $D_i = x - 1$ ، $j = 2$ و $B = 3$. با محاسبه مشتق $D'_i = 1$ ، باید معادله $SD_i + TD'_i = B$ را با شرط $\deg(T) < \deg(D_i)$ حل کنیم:

$$S(x - 1) + T(1) = 3.$$

از آنجا که $\deg(T) < 1$ ، نتیجه می‌گیریم T یک مقدار ثابت است. با ارزیابی معادله در ریشه مخرج (یعنی $x = 1$)، به دست می‌آوریم $T = 3$ ، که با جایگذاری آن نتیجه می‌شود $S = 0$. با جایگذاری این مقادیر در رابطه کاهشی هرمیت داریم:

$$\int \frac{3}{(x-1)^2} = \frac{-T}{(2-1)(x-1)^{2-1}} + \int \frac{S + \frac{T'}{2-1}}{(x-1)^{2-1}} = \frac{-3}{x-1} + \int 0.$$

در نهایت، انتگرال تابع اصلی به شکل زیر تفکیک می‌شود:

$$\int \frac{A}{D} = \int \frac{3x^2 + 3x + 3}{x^2 - 3x + 2} = \frac{-3}{x-1} + \int \left(\frac{1}{x+2} + \frac{2}{x-1} \right).$$

به این ترتیب، بخش گویا استخراج شده و مخرج کسر باقیمانده برای انتگرال‌گیری، چندجمله‌ای بدون مربع $U = (x+2)(x-1) = x^2 + x - 2$ خواهد بود.

۶.۲ الگوریتم روتشتاین-تراگر

پس از اعمال روش هرمیت، انتگرال تابع گویای اولیه به یک بخش گویا و یک انتگرال باقیمانده به صورت $\int \frac{H}{U}$ کاهش می‌یابد، به طوری که $\deg(H) < \deg(U)$ و مخرج U یک چندجمله‌ای بدون مربع است ($\gcd(U, U') = 1$). هدف الگوریتم روتشتاین-تراگر^۱، محاسبه دقیق بخش لگاریتمی این انتگرال بدون نیاز به تجزیه پرهزینه مخرج به عوامل خطی است. این الگوریتم بر پایه ویژگی‌های منتج دو چندجمله‌ای بنا شده است.

^۱مایکل روتشتاین (Michael Rothstein) و بری تراگر (Barry Trager)، دو پژوهشگر علوم کامپیوتر که در سال ۱۹۷۶ میلادی به صورت مستقل از یکدیگر، این الگوریتم کاملاً جبری را برای محاسبه بخش لگاریتمی انتگرال توابع گویا ارائه دادند.

$$R = \mathbf{Res}_x(H - tU', U) = \circ.$$
$$v_i = \gcd(H - c_i U', U).$$

۳.۲ روتشتاین-تراگر (استخراج بخش لگاریتمی) $\text{RothsteinTrager}(H, U)$

$$R \leftarrow \mathbf{Res}_x(H - tU', U)$$

Find distinct roots $c_1, \dots, c_k$ of $R = 0$ in an algebraic extension of K

$$L \leftarrow 0$$
for $i = 1$ **to** k **do**
$$v_i \leftarrow \mathbf{Euclidean}(H - c_i U', U) \text{ \{Computed in } K(c_i)[x]\}$$
$$L \leftarrow L + c_i \ln(v_i)$$

end for

return L

۱.۶.۲. قضیه ۳.۲ پایان پذیر است و نتیجه را به درستی برمی گرداند.

۵۳

□

اثبات. به [۷] مراجعه شود.

مثال ۱.۶.۲. محاسبه انتگرال $\int \frac{1}{x^2-2}$ را در $\mathbb{Q}(x)$ در نظر می‌گیریم. در اینجا $H = 1$ و $U = x^2 - 2$. از آنجا که $U' = 2x$ و مخرج فاقد ریشه تکراری است، مستقیماً الگوریتم روتشتاین-تراگر را اعمال می‌کنیم. ابتدا معادله منتج را نسبت به متغیر x تشکیل می‌دهیم:

$$R = \text{Res}_x(H - tU', U) = \text{Res}_x(1 - 2tx, x^2 - 2).$$

با محاسبه دترمینان ماتریس سیلویستر متناظر با این دو چندجمله‌ای، داریم

$$R = 1 - 4t^2.$$

ریشه‌های معادله $R = 0$ در توسیع جبری $\mathbb{Q}(\sqrt{2})$ ^۱ برابرند با $c_1 = \frac{\sqrt{2}}{2}$ و $c_2 = -\frac{\sqrt{2}}{2}$. این مقادیر، همان ضرایب لگاریتم‌ها در پاسخ نهایی هستند. حال برای هر ریشه، چندجمله‌ای‌های درون لگاریتم (ب.م.م.) را استخراج می‌کنیم:

$$\begin{aligned} v_1 &= \gcd\left(1 - \frac{\sqrt{2}}{2}(2x), x^2 - 2\right) = \gcd\left(1 - \frac{\sqrt{2}}{2}x, x^2 - 2\right) = x - \sqrt{2}, \\ v_2 &= \gcd\left(1 - \left(-\frac{\sqrt{2}}{2}\right)(2x), x^2 - 2\right) = \gcd\left(1 + \frac{\sqrt{2}}{2}x, x^2 - 2\right) = x + \sqrt{2}. \end{aligned}$$

با جایگذاری در رابطه قضیه، خروجی نهایی به دست می‌آید:

$$\int \frac{1}{x^2-2} = \frac{\sqrt{2}}{4} \ln(x - \sqrt{2}) - \frac{\sqrt{2}}{4} \ln(x + \sqrt{2}).$$

^۱نماد $\mathbb{Q}(\sqrt{2})$ نشان‌دهنده یک توسیع جبری از میدان اعداد گویا ($\mathbb{Q}$) است که با افزودن ریشه معادله (یعنی $\sqrt{2}$) به آن ساخته می‌شود. در واقع، این میدان توسیع‌یافته شامل تمامی اعدادی به صورت $a + b\sqrt{2}$ است که در آن $a, b \in \mathbb{Q}$. مفاهیم بنیادین توسیع‌های میدانی و نقش آن‌ها در ساختار خروجی انتگرال‌ها را در فصل آینده به تفصیل بررسی خواهیم کرد.

۷.۲ الگوریتم جامع انتگرال‌گیری توابع گویا

اکنون پس از آشنایی با الگوریتم‌های هر میت و روتشتاین-تراگر، می‌توانیم فرآیند یکپارچه‌ای برای محاسبه نمادین انتگرال هر تابع گویای دلخواه ارائه دهیم.

IntegrateRational(A, D)	الگوریتم ۴.۲ انتگرال‌گیری توابع گویا
Require: $A, D \in K[x]$ with $D \neq 0$	
Ensure: $\int \frac{A}{D}$	
$(Q, R) \leftarrow \text{PolyDivide}(A, D)$	
$P \leftarrow \int Q$ {Polynomial Integration}	
if $R = 0$ then	
return P	
end if	
$(G, \frac{H}{U}) \leftarrow \text{HermiteReduce}(R, D)$	
$L \leftarrow \text{RothsteinTrager}(H, U)$	
return $P + G + L$	

قضیه ۱.۷.۲. الگوریتم ۴.۲ پایان‌پذیر است و نتیجه را به درستی برمی‌گرداند.

اثبات. ابتدا پایان‌پذیری الگوریتم را بررسی می‌کنیم. این الگوریتم از چند عملیات پایه‌ای تشکیل شده است و حلقه تکرار در ساختار خود ندارد. از آنجا که پایان‌پذیری الگوریتم‌های **HermiteReduce**، **PolyDivide** و **RothsteinTrager** در مباحث پیشین ثابت شده است و محاسبه انتگرال یک چندجمله‌ای ($P = \int Q$) نیز در زمان متناهی انجام می‌شود، کل الگوریتم همواره پس از طی مراحل متناهی پایان می‌یابد. برای اثبات درستی، بر اساس قضیه الگوریتم تقسیم داریم $A = DQ + R$ که در آن $R = 0$ یا $\deg(R) < \deg(D)$. با تقسیم طرفین این تساوی بر D و اعمال عملگر انتگرال، داریم

$$\int \frac{A}{D} = \int Q + \int \frac{R}{D}.$$

بخش اول این عبارت نشان‌دهنده انتگرال یک چندجمله‌ای است که نتیجه آن در متغیر P ذخیره می‌شود. اگر $R = 0$ ، انتگرال تابع اولیه تنها همان بخش چندجمله‌ای P خواهد بود که الگوریتم در همین گام آن را بازمی‌گرداند؛ اما اگر $R \neq 0$ ، کسر $\frac{R}{D}$ یک تابع گویای سره است. با ارسال این کسر به الگوریتم کاهش هرمیت، بر اساس درستی اثبات‌شده برای این الگوریتم، بخش گویای انتگرال (G) و کسر باقیمانده برای بخش لگاریتمی $(\frac{H}{U})$ با حفظ کران درجات استخراج می‌شوند، به طوری که

$$\int \frac{R}{D} = G + \int \frac{H}{U}.$$

در نهایت، انتگرال کسر سره $\frac{H}{U}$ (که مخرج آن فاقد ریشه تکراری است) توسط الگوریتم روتشتاین-تراگر محاسبه می‌شود و خروجی آن، بخش لگاریتمی انتگرال (L) خواهد بود. با جمع کردن این مقادیر، در نهایت خواهیم داشت

$$\int \frac{A}{D} = P + G + L.$$

□

مثال ۱.۷.۲. تابع گویای زیر را در میدان $\mathbb{Q}(x)$ در نظر می‌گیریم:

$$f = \frac{x^4 - x^3 + x^2 + 2x - 1}{x^3 - x^2}.$$

با اجرای الگوریتم PolyDivide، صورت بر مخرج تقسیم می‌شود. خارج‌قسمت و باقیمانده این تقسیم عبارت‌اند از $Q = x$ و $R = x^2 + 2x - 1$. بنابراین، انتگرال بخش چندجمله‌ای برابر است با $P = \frac{1}{4}x^2$. برای حالت $R \neq 0$ ، کسر باقیمانده به الگوریتم کاهش هرمیت ارجاع داده می‌شود. در این مرحله، تجزیه بدون مربع مخرج عبارت است از $D = x^2(x - 1)$. با اعمال رابطه بزو و انتگرال‌گیری جزء به جزء، بخش گویای انتگرال و کسر سره باقیمانده برای بخش لگاریتمی استخراج می‌شوند؛ به طوری که داریم $\frac{H}{U} = \frac{x+1}{x^2-x}$ و $G = -\frac{1}{x}$. اکنون الگوریتم روتشتاین-تراگر روی این کسر اعمال می‌شود. با تشکیل معادله منتج، تساوی زیر را داریم:

$$\text{Res}_x((x+1) - t(2x-1), x^2-x) = -(t+1)(t-2) = 0.$$

ریشه‌های این معادله عبارت‌اند از $c_1 = 2$ و $c_2 = -1$. از آنجا که این مقادیر در خود میدان $\mathbb{Q}$ قرار دارند، نیازی به توسیع میدانی نخواهد بود. با محاسبه ب.م.م. متناظر با هر ریشه برای استخراج چندجمله‌ای‌های درون لگاریتم، خروجی بخش لگاریتمی برابر است با $L = 2 \ln(x - 1) - \ln(x)$. در نهایت، با جمع کردن این مقادیر، خروجی الگوریتم جامع برای تابع اولیه به صورت زیر بازگردانده می‌شود:

$$\int \frac{x^4 - x^3 + x^2 + 2x - 1}{x^3 - x^2} = \frac{1}{2}x^2 - \frac{1}{x} + 2 \ln(x - 1) - \ln(x).$$

فصل ۳

توسیع‌های میدانی و قضیه لیوویل

در این فصل، با تکیه بر مفاهیم جبری و الگوریتم‌های انتگرال‌گیری ارائه‌شده در فصل‌های پیشین، به بررسی دقیق ساختارهایی می‌پردازیم که زمینه نظری این الگوریتم‌ها را فراهم می‌کنند. ابتدا مفهوم توسیع میدانی و عناصر جبری و متعالی را معرفی کرده و سپس این مفاهیم را به حلقه‌ها و میدان‌های دیفرانسیلی گسترش می‌دهیم. با تعریف توسیع‌های لگاریتمی و نمایی، ساختار توابع مقدماتی را از دیدگاه جبر مجرد فرمول‌بندی خواهیم کرد. در نهایت، با بیان قضیه لیوویل، پایه‌های نظری انتگرال‌گیری نمادین را استوار ساخته و درستی روش روتشتاین-تراگر را از طریق مفاهیم منتج و توسیع‌های میدانی به اثبات می‌رسانیم. علاوه بر آن، چند کاربرد مفید این قضیه را نیز بیان می‌کنیم. بیشتر مطالب این فصل از منابع [۱، ۵، ۷] استخراج شده است.

۱.۳ توسیع‌های میدانی

در بسیاری از معادلات ریاضی، ریشه مطلوب در میدان اعدادی که مسئله در آن مطرح شده است، قرار ندارد. برای نمونه، معادله $x^2 - 2 = 0$ در میدان اعداد گویا هیچ ریشه‌ای ندارد و حل آن نیازمند گذار به میدان بزرگتری است. این مفهوم در جبر تحت عنوان «توسیع میدانی» بیان می‌شود.

تعریف ۱.۱.۳. دو میدان E و F را به گونه‌ای در نظر می‌گیریم که F زیرمیدانی از E باشد. در این صورت، E را یک توسیع میدانی برای F می‌گوییم و آن را با نماد E/F نمایش می‌دهیم.

تعریف ۲.۱.۳. توسیع میدانی E/F و عنصر دلخواه $\alpha \in E$ را در نظر می‌گیریم. عنصر α را روی F جبری می‌گوییم، هرگاه چندجمله‌ای ناصفر $P \in F[x]$ وجود داشته باشد، به طوری که $P(\alpha) = 0$. در غیر این صورت، α را روی F متعالی می‌نامیم.

مثال ۱.۱.۳. توسیع میدانی $\mathbb{R}/\mathbb{Q}$ را در نظر می‌گیریم. عنصر $\sqrt{2} \in \mathbb{R}$ روی $\mathbb{Q}$ جبری است، زیرا برای چندجمله‌ای $P = x^2 - 2 \in \mathbb{Q}[x]$ رابطه $P(\sqrt{2}) = 0$ صدق می‌کند. در مقابل، اعدادی مانند π و e ریشه هیچ چندجمله‌ای با ضرایب گویا نیستند و روی میدان $\mathbb{Q}$ متعالی محسوب می‌شوند.

تعریف ۳.۱.۳. برای عنصر جبری α روی میدان F ، چندجمله‌ای تکین $P \in F[x]$ با کمترین درجه ممکن که دارای ریشه α است را چندجمله‌ای کمینه α روی F می‌نامیم.

مثال ۲.۱.۳. عنصر $\alpha = \sqrt[3]{2}$ را در توسیع میدانی $\mathbb{R}/\mathbb{Q}$ در نظر می‌گیریم. چندجمله‌ای تکین $P = x^3 - 2$ در حلقه $\mathbb{Q}[x]$ دارای ریشه α است. از آنجا که این چندجمله‌ای روی میدان $\mathbb{Q}$ تحویل‌ناپذیر است، هیچ چندجمله‌ای ناصفر دیگری با درجه کمتر از سه در $\mathbb{Q}[x]$ یافت نمی‌شود که دارای چنین ریشه‌ای باشد. در نتیجه، برای عنصر α ، چندجمله‌ای کمینه روی میدان $\mathbb{Q}$ ، $P = x^3 - 2$ است.

۲.۳ توسیع‌های دیفرانسیلی

در این بخش، با بهره‌گیری از مفاهیم توسیع میدانی و مشتق جبری که در فصل دوم بررسی شد، ساختار جدیدی برای تحلیل جواب انتگرال‌ها ارائه می‌کنیم. انگیزه اصلی از این رویکرد، رفع محدودیت میدان‌های پایه است؛ زیرا جواب بسیاری از انتگرال‌ها در میدان اولیه تابع موجود نیست. برای حل این مشکل، میدان پایه را گسترش داده و میدان‌های دیفرانسیلی وسیع‌تری را معرفی می‌کنیم.

تعریف ۱.۲.۳. میدان‌های دیفرانسیلی (E, δ_E) و (F, δ_F) را در نظر می‌گیریم. میدان E را یک توسیع دیفرانسیلی برای F می‌گوییم، هرگاه E/F یک توسیع میدانی بوده و عملگر δ_E در صورت اعمال بر عناصر F ، دقیقاً همان مقدار مشتق δ_F را داشته باشد. به بیان دیگر، برای هر عنصر $a \in F$ ، داشته باشیم

$$\delta_E(a) = \delta_F(a).$$

مثال ۱.۲.۳. ساختار (F, δ_F) شامل میدان پایه $F = \mathbb{Q}(x)$ و عملگر $\delta_F = \frac{d}{dx}$ را در نظر می‌گیریم. در این ساختار، انتگرال جبری برای کسر $\frac{1}{x}$ ، هیچ جوابی در میدان پایه ندارد. برای رفع این محدودیت، متغیر متعالی t را به آن افزوده و میدان توسیع‌یافته $E = \mathbb{Q}(x, t)$ را به عنوان دامنه جدید در نظر می‌گیریم. سپس عملگر δ_E روی این میدان به گونه‌ای تعریف می‌شود که ضمن حفظ قواعد اصلی مشتق، رابطه $\delta_E(t) = \frac{1}{x}$ برای عنصر t برقرار باشد. از آنجا که دامنه δ_E کل میدان پایه $\mathbb{Q}(x)$ را در بر گرفته و برای هر عنصر آن رابطه $\delta_E(a) = \delta_F(a)$ برقرار است، مجموعه E یک توسیع دیفرانسیلی برای F محسوب می‌شود. در نتیجه، متغیر t نقش جواب ناموجود انتگرال، یعنی تابع $\ln(x)$ را ایفا خواهد کرد.

تذکر ۱.۲.۳. در ادامه این نوشتار، به منظور جلوگیری از پیچیدگی نمادگذاری، عملگر مشتق را در میدان پایه و توسیع آن با یک نماد مشترک مانند δ نمایش می‌دهیم.

قضیه ۱.۲.۳. فرض کنیم E/F یک توسیع دیفرانسیلی باشد و عنصر $\alpha \in E$ روی F جبری باشد. در این صورت، عملگر مشتق δ از میدان F ، به صورت یکتا به توسیع میدانی $F(\alpha)$ تعمیم می‌یابد.

اثبات. برای اثبات این موضوع، کافی است نشان دهیم که مقدار $\delta(\alpha)$ به صورت یکتا تعیین می‌شود؛ زیرا هر عنصر در $F(\alpha)$ ترکیبی جبری از عناصر F و متغیر α است و یکتایی $\delta(\alpha)$ ، به دلیل خطی بودن و قاعده لایب‌نیتس، یکتایی مشتق را برای کل میدان $F(\alpha)$ تضمین می‌کند. عنصر جبری $\alpha \in E$ و چندجمله‌ای کمینه آن به شکل $P = \sum_{i=0}^n a_i x^i$ در $F[x]$ را در نظر می‌گیریم. طبق تعریف داریم $P(\alpha) = \sum_{i=0}^n a_i \alpha^i = 0$. با اعمال عملگر مشتق بر آن و استفاده از قاعده لایب‌نیتس، رابطه زیر نتیجه می‌شود:

$$\sum_{i=0}^n (\delta(a_i) \alpha^i + a_i \delta(\alpha^i)) = 0.$$

با جایگذاری رابطه $\delta(\alpha^i) = i\alpha^{i-1}\delta(\alpha)$ برای مشتق توان‌ها و فاکتورگیری از $\delta(\alpha)$ ، داریم

$$\sum_{i=0}^n \delta(a_i) \alpha^i + \left(\sum_{i=1}^n i a_i \alpha^{i-1} \right) \delta(\alpha) = 0.$$

در این رابطه، عبارت درون پرانتز نشان‌دهنده مشتق صوری نسبت به متغیر x است که به ازای عنصر α ، مقدار δ در این نوشتار، نماد $\mathbb{Q}(x, t)$ هم‌ارز با ساختار $\mathbb{Q}(x)(t)$ در نظر گرفته می‌شود؛ به این معنا که میدان دیفرانسیلی پایه به صورت $\mathbb{Q}(x)$ فرض شده و توسیع آن از طریق افزودن متغیر t صورت می‌گیرد.

$P'(\alpha)$ را تولید می‌کند. از آنجا که P نقش چندجمله‌ای کمینه را برای عنصر α ایفا می‌کند، شرط $\deg(P') < \deg(P)$ برقرار بوده و در نتیجه $P'(\alpha) \neq 0$. بنابراین مقدار $\delta(\alpha)$ به صورت یکتا و به شکل زیر تعیین می‌شود:

$$\delta(\alpha) = -\frac{\sum_{i=0}^n \delta(a_i) \alpha^i}{P'(\alpha)}. \quad \square$$

مثال ۲.۲.۳. توسیع میدانی $E = F(\alpha)$ را در میدان دیفرانسیلی $F = \mathbb{Q}(x)$ با عملگر $\delta = \frac{d}{dx}$ و برای عنصر جبری $\alpha = \sqrt{x}$ در نظر می‌گیریم. با تشکیل چندجمله‌ای کمینه $P(y) = y^2 - x$ در حلقه $F[y]$ ، مقادیر $\delta(-x) = -1$ و $\delta(1) = 0$ به عنوان مشتق ضرایب در میدان پایه به دست می‌آیند. از سوی دیگر، با محاسبه مشتق صوری و محاسبه مقدار آن به ازای ریشه α ، داریم $P'(\alpha) = 2\alpha$. در نهایت، با جایگذاری این اجزا در رابطه قضیه ۱.۲.۳، مشتق عنصر جبری در میدان توسیع یافته E ، به صورت زیر به دست می‌آید:

$$\delta(\alpha) = -\frac{\delta(-x) + \delta(1)\alpha^2}{P'(\alpha)} = -\frac{-1}{2\alpha} = \frac{1}{2\alpha}.$$

۳.۳ توابع مقدماتی و قضیه لیوویل

در حسابان کلاسیک، توابعی مانند لگاریتم و تابع نمایی بر پایه مفاهیم آنالیزی شکل گرفته‌اند. برای نمونه، تابع لگاریتم طبیعی برای متغیر مثبت x از طریق انتگرال معین تعریف می‌شود:

$$\ln(x) = \int_1^x \frac{1}{t} dt.$$

همچنین تابع نمایی، به عنوان وارون تابع لگاریتم طبیعی نیز می‌تواند از طریق سری‌های نامتناهی توانی محاسبه شود:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

با این وجود، به پیروی از رویکرد محاسبات نمادین که در فصل پیش با آن آشنا شدیم، وابستگی به مفاهیم و تعاریف آنالیزی را کنار گذاشته و چنین توابعی را با استفاده از قوانین مشتق‌گیری در توسیع‌های دیفرانسیلی بازتعریف می‌کنیم.

تعریف ۱.۳.۳. توسیع دیفرانسیلی E/F و عنصر $\theta \in E$ را در نظر می‌گیریم. عنصر θ را روی F لگاریتمی می‌گوییم، هرگاه عنصری مانند $u \in F^*$ وجود داشته باشد، به طوری که مشتق θ به صورت زیر محاسبه شود:

$$\delta(\theta) = \frac{\delta(u)}{u}.$$

در این حالت، با استفاده از نمادگذاری کلاسیک می‌نویسیم $\theta = \ln(u)$. همچنین عنصر θ را روی F نمایی می‌گوییم، هرگاه عنصری مانند $v \in F$ موجود باشد، به طوری که رابطه زیر برای مشتق θ صدق کند:

$$\delta(\theta) = \delta(v)\theta.$$

در این شرایط نیز از نمادگذاری $\theta = \exp(v)$ استفاده می‌کنیم.

مثال ۱.۳.۳. در میدان دیفرانسیلی $F = \mathbb{Q}(x)$ با عملگر $\delta = \frac{d}{dx}$ ، عنصر لگاریتمی θ_1 متناظر با متغیر $u = x$ را در نظر می‌گیریم. بر اساس تعریف، مشتق این عنصر به شکل زیر محاسبه می‌شود:

$$\delta(\theta_1) = \frac{\delta(x)}{x} = \frac{1}{x}.$$

به این ترتیب، متغیر θ_1 نقش تابع $\ln(x)$ را ایفا می‌کند. به صورت مشابه، با معرفی عنصر نمایی θ_2 متناظر با متغیر $x^2 = v$ ، رابطه مشتق زیر نتیجه می‌شود:

$$\delta(\theta_2) = \delta(x^2)\theta_2 = 2x\theta_2.$$

در نتیجه، متغیر θ_2 نیز مشابه تابع نمایی e^{x^2} را در ساختار توسیع یافته رفتار می‌کند.

تعریف ۲.۳.۳. توسیع دیفرانسیلی E/F را یک **توسیع مقدماتی** می‌گوییم، هرگاه دنباله‌ای (زنجیره) متناهی از میدان‌ها به صورت زیر وجود داشته باشد:

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E,$$

به طوری که برای هر $1 \leq i \leq n$ ، میدان $E_i = E_{i-1}(\theta_i)$ یک توسیع ساده^۱ برای میدان پیشین خود محسوب شود و عنصر θ_i روی E_{i-1} جبری، لگاریتمی یا نمایی باشد. عناصر قرار گرفته در یک توسیع مقدماتی از میدان توابع گویا، توابع مقدماتی نامیده می‌شوند.

مثال ۲.۳.۳. میدان دیفرانسیلی $F_* = \mathbb{Q}(x)$ با عملگر $\delta = \frac{d}{dx}$ را به عنوان میدان پایه در نظر می‌گیریم. برای نمایش تابع مقدماتی $f = e^{\sqrt{x}} + \ln(x)$ ، یک زنجیره از توسیع‌های میدانی را تشکیل می‌دهیم. در گام نخست، عنصر جبری θ_1 با معادله کمینه $\theta_1^2 - x = 0$ را به ساختار پایه افزوده و میدان $F_1 = F_*(\theta_1)$ را می‌سازیم. در گام بعد، برای عنصر نمایی θ_2 متناظر با متغیر θ_1 ، رابطه مشتق $\delta(\theta_2) = \delta(\theta_1)\theta_2$ را مبنا قرار داده و توسیع $F_2 = F_1(\theta_2)$ را تشکیل می‌دهیم. در مرحله پایانی، عنصر لگاریتمی θ_3 متناظر با متغیر x و با ضابطه مشتق $\delta(\theta_3) = \frac{1}{x}$ را به ساختار افزوده و میدان نهایی $F_3 = F_2(\theta_3)$ را به دست می‌آوریم. زنجیره میدانی $F_* \subseteq F_1 \subseteq F_2 \subseteq F_3$ یک توسیع مقدماتی را نشان می‌دهد. در این ساختار، متغیر $w = \theta_2 + \theta_3$ نقش تابع f را ایفا می‌کند.

اکنون پس از آشنایی با این تعاریف جبری، می‌توانیم قضیه لیوویل را که پیش‌تر در فصل دوم به عنوان اساس تعیین ساختار انتگرال توابع گویا به آن اشاره کردیم، به صورت رسمی بیان کنیم.

قضیه ۱.۳.۳ (قضیه لیوویل). میدان دیفرانسیلی F و تابع $f \in F$ را در نظر می‌گیریم. فرض می‌کنیم این تابع دارای انتگرالی باشد که در یک توسیع مقدماتی از F قرار دارد. در این صورت، عنصری مانند $v \in F$ ، ثابت‌های $c_1, \dots, c_k \in \text{Const}(F)$ و توابع ناصفر $u_1, \dots, u_k \in F^*$ وجود دارند به طوری که برای تابع f داریم

$$f = \delta(v) + \sum_{i=1}^k c_i \frac{\delta(u_i)}{u_i}.$$

□

اثبات. به [۱، قضیه ۱.۵.۵، صفحه ۱۳۹] مراجعه شود.

در بخش بعدی، با چند کاربرد و نتیجه مهم از این قضیه آشنا می‌شویم.

^۱توسیع ساده به میدانی گفته می‌شود که تنها با افزودن یک عنصر مشخص به میدان پایه ساخته شود. در این تعریف، نماد $E_{i-1}(\theta_i)$ نشان‌دهنده آن است که میدان جدید از الحاق عنصر θ_i به ساختار میدان پیشین، یعنی E_{i-1} ، به دست آمده است.

۴.۳ کاربردهای قضیه لیوویل

در فصل گذشته، به نقش قضیه لیوویل در درستی معادله منتج در الگوریتم روتشتاین-تراگر اشاره کردیم. اکنون به اثبات دقیق آن می‌پردازیم و پس از آن، مفهوم «فرم بسته مقدماتی» را برای یک انتگرال معرفی کرده و با استفاده از قضیه لیوویل، محکی در رابطه با این مفهوم ارائه می‌کنیم.

۱.۴.۳ اثبات درستی روش روتشتاین-تراگر

با بهره‌گیری از ساختار مشخص شده در قضیه لیوویل و ویژگی‌های منتج دو چندجمله‌ای، می‌توان درستی الگوریتم روتشتاین-تراگر را به صورت دقیق ثابت کرد. این اثبات نشان می‌دهد که چرا ریشه‌های معادله منتج، همان ثابت‌های بخش لگاریتمی را استخراج می‌کنند.

قضیه ۱.۴.۳. کسر گویای سره $\frac{H}{U} \in K(x)$ با شرط بدون مربع بودن U و $\gcd(H, U) = 1$ را در نظر می‌گیریم. فرض می‌کنیم انتگرال این تابع به صورت زیر تفکیک شده باشد:

$$\int \frac{H}{U} = \sum_{i=1}^k c_i \ln(v_i),$$

به طوری که c_i ریشه‌های متمایز در توسیع جبری میدان پایه و چندجمله‌ای‌های v_i عناصری تکی‌ن در حلقه $K(c_1, \dots, c_k)[x]$ باشند. در این صورت، ثابت‌های c_i ریشه‌های معادله منتج $\text{Res}_x(H - tU', U) = 0$ نسبت به متغیر t محسوب می‌شوند.

اثبات. با مشتق‌گیری از رابطه انتگرال، داریم

$$\frac{H}{U} = \sum_{i=1}^k c_i \frac{v'_i}{v_i}. \quad (*)$$

از آنجا که مخرج U فاقد ریشه تکراری است و کسر در ساده‌ترین حالت خود قرار دارد، مجموع کسرهای سمت راست نیز باید مخرجی برابر با چندجمله‌ای U تولید کند. بر اساس ویژگی تجزیه کسرهای جزئی، می‌توان نتیجه گرفت که مخرج تابع اصلی برابر با حاصل ضرب چندجمله‌ای‌های درون لگاریتم است، به بیان دیگر،

$U = \prod_{i=1}^k v_i$. با مشتق‌گیری از این حاصل ضرب، رابطه زیر برای مشتق مخرج حاصل می‌شود:

$$U' = \sum_{i=1}^k v'_i \prod_{j \neq i} v_j.$$

اکنون از اتحاد $U/v_i = \prod_{j \neq i} v_j$ استفاده کرده و رابطه (*) را با ضرب طرفین در متغیر U بازنویسی می‌کنیم:

$$H = \sum_{i=1}^k c_i v'_i \prod_{j \neq i} v_j.$$

برای بررسی ریشه‌های منتج، یک ثابت مشخص مانند c_m را در نظر می‌گیریم و عبارت $H - c_m U'$ را تشکیل می‌دهیم:

$$H - c_m U' = \sum_{i=1}^k (c_i - c_m) v'_i \prod_{j \neq i} v_j.$$

از آنجا که برای جمله $i = m$ تفاضل $(c_m - c_m)$ برابر با صفر می‌شود، عبارت متناظر با متغیر v'_m از مجموع حذف خواهد شد. بنابراین تمام جملات باقی‌مانده در این مجموع حاوی عامل مشترک v_m خواهند بود. این آرایش از جملات، تضمین می‌کند که چندجمله‌ای v_m مقسوم‌علیه مشترک عبارات $H - c_m U'$ و U است. وجود عامل مشترک غیربدیهی میان دو چندجمله‌ای، معادل با صفر شدن مقدار منتج آنهاست. بنابراین برای هر متغیر $t = c_i$ ، خواهیم داشت

$$\text{Res}_x(H - tU', U) = 0. \quad \square$$

۲.۴.۳ بررسی فرم بسته مقدماتی برای انتگرال‌ها

در ریاضیات، هنگامی که گفته می‌شود جواب یک مسئله دارای «فرم بسته» است، منظور این است که آن جواب با استفاده از تعداد متناهی از عملگرهای حسابی و ترکیب توابع پایه، قابل نمایش است. در مبحث انتگرال‌گیری آنالیزی، یک انتگرال دارای فرم بسته مقدماتی است، هرگاه پاسخ آن تنها با ترکیبی متناهی از توابع گویا، نمایی، لگاریتمی، رادیکالی و مثلثاتی (و وارون آن‌ها) بیان شود. از دیدگاه جبر دیفرانسیلی، برخورداری از فرم بسته به این

معناست که انتگرال تابع مورد نظر در یک توسیع مقدماتی از میدان پایه وجود داشته باشد. برای درک بهتر، انتگرال تابع xe^x را در نظر می‌گیریم. پاسخ این انتگرال به صورت تابع مقدماتی $e^x(x-1)$ به دست می‌آید؛ بنابراین دارای فرم بسته است. در مقابل، توابعی مانند e^{x^2} یا $\frac{\sin x}{x}$ با وجود پیوسته بودن و داشتن انتگرال مساحت‌دار در آنالیز، پاسخ آن‌ها با هیچ ترکیب متناهی از توابع یادشده قابل بیان نیست و فاقد فرم بسته مقدماتی هستند. یکی از مهم‌ترین کاربردهای قضیه لیوویل، ارائه یک معیار جبری برای اثبات عدم وجود پاسخ مقدماتی برای دسته وسیعی از این انتگرال‌های معروف است. پیش از توسعه جبر دیفرانسیلی، اثبات این که تابعی مانند e^{x^2} فاقد انتگرال در فرم بسته است، چالشی بزرگ در ریاضیات محسوب می‌شد. قضیه لیوویل نشان می‌دهد که اگر یک تابع دارای انتگرالی در یک توسیع مقدماتی باشد، ساختار آن انتگرال باید از فرم بسیار محدودی پیروی کند. به عنوان یک نتیجه از این قضیه، می‌توان محک زیر را برای توابع نمایی بیان و اثبات کرد.

قضیه ۳.۴.۲. فرض می‌کنیم توابع گویای $f, w \in K(x)$ به گونه‌ای باشند که تابع f ناصفر و تابع w غیرثابت باشد. انتگرال تابع fe^w دارای فرم بسته مقدماتی است، اگر و تنها اگر تابع گویایی مانند $g \in K(x)$ وجود داشته باشد که در معادله دیفرانسیل جبری زیر صدق کند:

$$g' + w'g = f.$$

اثبات. $\Leftarrow$ فرض می‌کنیم تابع گویای $g \in K(x)$ وجود داشته باشد که در معادله $g' + w'g = f$ صدق کند. تابع ge^w را در نظر می‌گیریم. با اعمال عملگر مشتق بر این تابع و استفاده از قاعده لایب‌نیتس، رابطه زیر حاصل می‌شود:

$$(ge^w)' = g'e^w + g(e^w)' = g'e^w + gw'e^w = (g' + gw')e^w.$$

با جایگذاری فرض اولیه در این رابطه، تساوی $(ge^w)' = fe^w$ نتیجه می‌شود. با اعمال عملگر انتگرال بر دو طرف این تساوی، پاسخ انتگرال تابع اصلی به صورت زیر خواهد بود:

$$\int fe^w = ge^w.$$

از آنجا که تابع g یک کسر گویا در میدان پایه و تابع e^w یک عنصر نمایی است، حاصل ضرب آن‌ها یک تابع مقدماتی به شمار می‌رود. بنابراین، انتگرال تابع مفروض دارای فرم بسته مقدماتی است.

($\Rightarrow$) فرض می‌کنیم انتگرال تابع $f e^w$ دارای فرم بسته مقدماتی باشد. میدان دیفرانسیلی پایه را به صورت $E = F(\theta)$ در نظر می‌گیریم و متغیر نمایی $\theta = e^w$ را به آن اضافه می‌کنیم تا توسیع دیفرانسیلی $E = F(\theta)$ شکل بگیرد. در این ساختار، ضابطه مشتق برای متغیر نمایی به صورت $\theta' = w'\theta$ تعریف می‌شود. بر اساس قضیه لیوویل و تحلیل رفتار عملگر مشتق در توسیع‌های متعالی نمایی^۱، اگر انتگرال عبارتی به فرم $f\theta$ (که در واقع چندجمله‌ای از درجه یک بر حسب متغیر θ است) دارای فرم بسته باشد، پاسخ آن باید یک ساختار جبری محدود به شکل $g\theta$ تولید کند، به گونه‌ای که تابع $g \in F$ یک تابع گویا بر حسب متغیر مستقل x باشد. بنابراین، تساوی زیر برای انتگرال تابع برقرار خواهد بود:

$$\int f e^w = g e^w.$$

اکنون با مشتق‌گیری از دو طرف این رابطه، داریم

$$f e^w = (g' + g w') e^w.$$

از آنجا که تابع نمایی e^w یک عنصر ناصفر است، با حذف آن از دو طرف تساوی، نتیجه می‌شود که تابع گویای g در معادله دیفرانسیل زیر صدق می‌کند:

$$g' + w'g = f. \quad \square$$

یکی دیگر از نتایج مهم قضیه لیوویل، تحلیل فرم بسته برای انتگرال توابع مثلثاتی است. در چارچوب جبری، توابع مثلثاتی به صورت ساختارهای مستقل بررسی نمی‌شوند، بلکه با بهره‌گیری از اتحاد اوایلر^{۲،۳} و ورود به میدان اعداد مختلط، به توابع نمایی تبدیل می‌شوند. این رویکرد و نتیجه آن برای یک تابع معروف، در قالب قضیه^۱ در توسیع‌های نمایی، عملگر مشتق درجه چندجمله‌ای‌ها را نسبت به متغیر متعالی تغییر نمی‌دهد و مشتق‌گیری از بخش‌های لگاریتمی نیز نمی‌تواند عبارات خطی تولید کند. به همین دلیل، بخش لگاریتمی پاسخ حذف شده و ساختار انتگرال مقید می‌شود. جهت مطالعه اثبات دقیق این رفتار جبری به [۱، بخش ۸.۵] مراجعه شود.

^۲ لئونهارد اوایلر (Leonhard Euler) (۱۷۰۷-۱۷۸۳ میلادی)، ریاضی‌دان و فیزیک‌دان برجسته سوئسی که یکی از پرکارترین دانشمندان تاریخ ریاضیات به شمار می‌رود. کارهای بنیادین او در حسابان، آنالیز مختلط و نظریه اعداد، همراه با معرفی بسیاری از نمادهای استاندارد ریاضی نظیر e و i ، نقش بسزایی در توسعه ریاضیات مدرن داشته است.

^۳ اتحاد اوایلر بیان می‌کند که برای هر متغیر حقیقی مانند x ، رابطه $e^{ix} = \cos x + i \sin x$ برقرار است. این اتحاد ساختار توابع مثلثاتی را به توابع نمایی در میدان اعداد مختلط پیوند می‌دهد.

زیر بیان می‌شود.

قضیه ۳.۴.۳. انتگرال تابع $\frac{\sin x}{x}$ فاقد پاسخ به صورت فرم بسته مقدماتی است.

اثبات. بر اساس اتحاد اوایلر، تابع سینوس با استفاده از یک‌ه موهومی $i = \sqrt{-1}$ در میدان اعداد مختلط به صورت بسط‌نمایی زیر بیان می‌شود:

$$\frac{\sin x}{x} = \frac{e^{ix} - e^{-ix}}{2ix} = \frac{1}{2i} \frac{e^{ix}}{x} - \frac{1}{2i} \frac{e^{-ix}}{x}.$$

ارزیابی انتگرال‌پذیری این عبارت به بررسی توابع‌نمایی مجزا شامل عبارات $\frac{e^{ix}}{x}$ و $\frac{e^{-ix}}{x}$ بر روی توسیع دیفرانسیلی $\mathbb{C}(x)$ تقلیل می‌یابد. با در نظر گرفتن توابع $f = \frac{1}{x}$ و $w = ix$ ، مشتق تابع دوم برابر با عنصر $w' = i$ به دست می‌آید. طبق قضیه ۲.۴.۳، عبارت $\frac{e^{ix}}{x}$ تنها در صورتی دارای پاسخ مقدماتی است که تابع گویایی مانند $g \in \mathbb{C}(x)$ یافت شود که در معادله دیفرانسیل زیر صدق کند:

$$g' + ig = \frac{1}{x}.$$

برای بررسی وجود تابع g ، فرض می‌کنیم این تابع به صورت کسر $\frac{A}{B}$ باشد که در آن چندجمله‌ای‌های A و B از حلقه $\mathbb{C}[x]$ ، نسبت به هم اول هستند. با جایگذاری این کسر در معادله و تحلیل درجات چندجمله‌ای‌های صورت و مخرج، مشخص می‌شود که هیچ ترکیب گویایی نمی‌تواند فرم $\frac{1}{x}$ را به عنوان حاصل جمع یک تابع گویا و مشتق آن تولید کند. $\square$

فصل ۴

آشنایی مختصر با انتگرال گیری توابع غیرگویا

در فصل‌های گذشته، مبانی جبری و الگوریتم‌های دقیق برای محاسبه انتگرال توابع گویا را بررسی کردیم. با این وجود، بسیاری از توابع کاربردی در ریاضیات شامل ساختارهای متعالی مانند توابع نمایی، لگاریتمی و مثلثاتی هستند. از آنجا که نظریه انتگرال‌گیری توابع متعالی گستردگی فراوانی دارد و ورود به آن نیازمند بررسی عمیق ساختارهای هندسی و حل معادلات دیفرانسیل در زنجیره میدان‌هاست، در این فصل قصد ورود جدی و اثبات قضایای این حوزه را نداریم. هدف ما در این بخش، تنها توصیف رویکردها و ارائه نمایی کلی از «الگوریتم ریش-نورمن»^۱ به عنوان یک روش ابتکاری^۱ و کارآمد در سیستم‌های محاسبات نمادین است. مطالب این فصل، برگرفته از منابع [۱، ۳] هستند.

الگوریتم کلاسیک ریش^۲، که بر پایه قضیه لیوویل بنا شده است، یک روش تصمیم‌گیری قطعی برای بررسی وجود فرم بسته انتگرال به شمار می‌رود. در این الگوریتم، توابع متعالی به صورت یک زنجیره متوالی از توسیع‌های دیفرانسیلی در قالب ساختار $K(x, \theta_1, \dots, \theta_n)$ در نظر گرفته می‌شوند، به گونه‌ای که هر متغیر θ_i روی میدان پیشین خود یک عنصر نمایی یا لگاریتمی باشد. با وجود دقت بالای این روش، ساختار بازگشتی آن یک چالش محاسباتی بزرگ ایجاد می‌کند. برای حل یک انتگرال در دامنه $K(x, \theta_1, \dots, \theta_n)$ ، الگوریتم کلاسیک نیازمند حل معادلات دیفرانسیل در میدان پیشین، یعنی ساختار $K(x, \theta_1, \dots, \theta_{n-1})$ ، است و این روند کاهش بُعد تا

^۱ الگوریتم ابتکاری، در علوم کامپیوتر به روشی گفته می‌شود که با هدف یافتن پاسخی قابل قبول در زمانی کوتاه طراحی شده است. این دسته از الگوریتم‌ها، برخلاف روش‌های قطعی، تضمینی برای رسیدن به پاسخ در تمامی حالت‌ها ارائه نمی‌دهند و کاربرد اصلی آن‌ها تسریع فرایند محاسبات برای مسائل رایج و روزمره است.

^۲ رابرت ریش (Robert Risch)، ریاضی‌دان آمریکایی که در سال ۱۹۶۹ میلادی الگوریتمی قطعی برای تعیین وجود یا عدم وجود فرم بسته انتگرال‌ها بر پایه قضیه لیوویل ارائه داد.

رسیدن به ساختار پایه، یعنی میدان $K(x)$ ، ادامه پیدا می‌کند. این فرآیند متوالی، به ویژه زمانی که تعداد توابع متعالی در صورت مسئله زیاد باشد، هزینه محاسباتی و زمان اجرای بسیار بالایی دارد. به منظور رفع مشکل کندی در الگوریتم بازگشتی ریش، آرتور نورمن^۱ رویکردی متفاوت و موازی را پیشنهاد کرد. در روش نورمن، به جای ساختن یک زنجیره متوالی از میدان‌ها و حل پله به پله معادلات، تمام توابع متعالی موجود در عبارت زیر انتگرال به صورت هم‌زمان به عنوان متغیرهای مستقل جبری در نظر گرفته می‌شوند. به بیان دیگر، اگر تابع اصلی در بر دارنده توابعی مانند e^x و $\ln(x)$ در ساختار خود باشد، این توابع به متغیرهای مستقلی مانند θ_1 و θ_2 در یک حلقه چندجمله‌ای چندمتغیره تبدیل می‌شوند. الگوریتم ریش-نورمن یک روش ابتکاری محسوب می‌شود؛ به این معنا که در حالت معمول بسیار سریع و کارآمد عمل می‌کند و پاسخ بسیاری از مسائل کاربردی را می‌یابد، اما برخلاف الگوریتم کلاسیک ریش، هیچ‌گونه تضمین قطعی برای یافتن فرم بسته (در صورت وجود) یا اثبات عدم وجود آن ارائه نمی‌دهد.

اساس کار الگوریتم ریش-نورمن بر پایه تشکیل یک جواب حدسی^۲ و تقلیل مسئله دیفرانسیلی به یک دستگاه معادلات خطی استوار است. شبه‌کد زیر، ساختار کلی این روش ابتکاری را به خوبی نشان می‌دهد.

^۱ آرتور نورمن (Arthur Norman)، پژوهشگر علوم کامپیوتر که در سال ۱۹۷۶ میلادی روشی موازی و مبتنی بر حدس جواب برای انتگرال‌گیری توابع متعالی ارائه داد تا بر محدودیت‌های الگوریتم ریش غلبه کند.

^۲ این ترکیب معادل اصطلاح Ansatz با ریشه آلمانی است و در متون ریاضی و فیزیک، به یک فرض اولیه سنجیده یا ساختار پیشنهادی برای پاسخ یک معادله گفته می‌شود که پیش از محاسبه دقیق اجزای آن، در نظر گرفته می‌شود.

الگوریتم ۱.۴ انتگرال‌گیری ابتکاری ریش-نورمن $\text{RischNorman}(f)$

Require: $f \in K(x, \theta_1, \dots, \theta_n)$

Ensure: $\int f$ or **Fail**

Determine the denominator B from the normal part of the denominator of f

Determine degree bounds d_i for the numerator A w.r.t each θ_i

Construct the ansatz $V \leftarrow \frac{A}{B} + \sum_{i=1}^k c_i \ln(v_i)$ with unknown coefficients q_j (for A) and c_i

Compute formal derivative V'

Form a linear system of equations by equating coefficients in $V' = f$

if the linear system has a solution for $q_j, c_i \in K$ **then**

 Substitute the solutions into V

return V

else

return **Fail**

end if

این الگوریتم در چند گام مشخص اجرا می‌شود که به ترتیب عبارتند از تشکیل جواب حدسی، تعیین کران درجات و تقلیل به دستگاه معادلات خطی:

- **تشکیل جواب حدسی:** فرض می‌کنیم تابع f به میدان دیفرانسیلی $K(x, \theta_1, \dots, \theta_n)$ تعلق دارد. بر اساس قضیه لیوویل، الگوریتم یک فرم کلی برای پاسخ انتگرال پیشنهاد می‌دهد. این فرم حدسی به شکل زیر در نظر گرفته می‌شود:

$$V = \frac{A}{B} + \sum_{i=1}^k c_i \ln(v_i).$$

در این ساختار، مخرج B با استفاده از ویژگی‌های جبری مخرج تابع f و مقسوم‌علیه‌های آن پیش‌بینی می‌شود و مقادیر c_i ثابت‌هایی نامشخص هستند. صورت کسر (یعنی چندجمله‌ای A) نیز به صورت یک چندجمله‌ای با ضرایب مجهول بر حسب متغیرهای θ_i در نظر گرفته می‌شود.

• **تعیین کران درجات:** برای این که جستجوی چندجمله‌ای A متناهی باشد، الگوریتم باید کران بالایی برای درجه این چندجمله‌ای نسبت به هر متغیر θ_i تعیین کند. این کران‌ها با تحلیل درجات صورت و مخرج تابع f و بررسی رفتار عملگر مشتق روی متغیرهای نمایی و لگاریتمی به دست می‌آیند. با محدود شدن درجات، چندجمله‌ای A به صورت یک ترکیب خطی از تک‌جمله‌ای‌ها با ضرایب مجهولی مانند پارامتر q_j بازنویسی می‌شود.

• **تقلیل به دستگاه معادلات خطی:** پس از تشکیل جواب حدسی V با ضرایب مجهول، عملگر مشتق صوری بر آن اعمال می‌شود. از آنجا که انتگرال و مشتق وارون یکدیگر هستند، باید رابطه دیفرانسیلی زیر برقرار باشد:

$$V' = f.$$

با مشتق‌گیری از جواب حدسی و برابر قرار دادن آن با تابع زیر انتگرال، و در ادامه هم‌مخرج کردن دو طرف تساوی، صورت کسرها در دو سوی معادله باید با یکدیگر برابر باشند. این برابری چندجمله‌ای‌ها، به معنای برابر بودن ضرایب تک‌جمله‌ای‌های هم‌درجه در دو طرف معادله است. با استخراج این ضرایب، یک دستگاه معادلات خطی بر حسب مجهولات q_j (ضرایب چندجمله‌ای صورت) و c_i (ثابت‌های بخش لگاریتمی) استخراج می‌شود. اگر این دستگاه دارای پاسخ سازگار در میدان پایه باشد، ضرایب مجهول مشخص شده و فرم بسته انتگرال بازگردانده می‌شود. در صورتی که دستگاه فاقد پاسخ باشد، الگوریتم ریش-نورمن با پیام شکست (Fail) متوقف می‌شود و نمی‌تواند درباره وجود یا عدم وجود فرم بسته جوابی ارائه دهد.

توسعه روش‌های ابتکاری مانند الگوریتم ریش-نورمن، تحول بزرگی در طراحی نرم‌افزارهای محاسبات ریاضی ایجاد کرد. در معماری این سیستم‌ها، به دلیل سرعت بالای روش موازی و تشکیل مستقیم دستگاه خطی، در گام نخست مسئله انتگرال‌گیری به تابع ریش-نورمن سپرده می‌شود. بررسی‌ها نشان می‌دهد که این الگوریتم می‌تواند پاسخ بخش عظیمی از انتگرال‌های مطرح‌شده در مهندسی و فیزیک را در کسری از ثانیه محاسبه کند. تنها در مواردی که این الگوریتم با شکست روبرو شود (یعنی دستگاه معادلات خطی به دست آمده ناسازگار باشد)، سیستم محاسباتی به عنوان آخرین راهکار به سراغ الگوریتم سنگین و بازگشتی کلاسیک ریش می‌رود تا وضعیت وجود یا عدم وجود پاسخ مقدماتی را به صورت قطعی مشخص سازد. این ترکیب هوشمندانه، کارایی و سرعت سیستم‌های محاسبات نمادین را به بالاترین سطح ممکن رسانده است. برای نمونه، کتابخانه محاسبات

نمادین زبان پایتون، یعنی SymPy^۱، از این معماری دوگانه بهره می‌برد. در این نرم‌افزار، پردازشگر انتگرال در گام نخست از روش‌های ابتکاری و سریع مانند رویکرد ریش-نورمن برای یافتن فرم بسته استفاده می‌کند. در بیشتر مسائل کاربردی، این روش با موفقیت عمل کرده و خروجی را در کمترین زمان ممکن تولید می‌کند. تنها در صورت توقف این الگوریتم و دریافت پیام شکست، سیستم برای تعیین تکلیف نهایی مسئله به سراغ اجرای الگوریتم قطعی ریش یا سایر روش‌های تحلیلی می‌رود. این راهکار باعث می‌شود سیستم‌های جبری مدرن به تعادلی کارآمد میان سرعت پردازش و جامعیت محاسبات ریاضی دست یابند.

^۱کتابخانه SymPy یک سیستم محاسبات جبری منبع‌باز در زبان برنامه‌نویسی پایتون است که با هدف انجام محاسبات نمادین ریاضی طراحی شده و به صورت گسترده در پژوهش‌های علمی مورد استفاده قرار می‌گیرد.

فهرست منابع

- [1] Manuel Bronstein. *Symbolic Integration I: Transcendental Functions*. Springer-Verlag, Berlin Heidelberg, 1997.
- [2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Hoboken, NJ, 3rd edition, 2004.
- [3] Keith O. Geddes, Stephen R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Springer Science & Business Media, 1992.
- [4] Amir Hashemi. *Gröbner basis and its applications*. Isfahan University of Technology Press (in Persian), 2023.
- [5] Amir Hashemi. Differential algebra (lecture notes). (in Persian), 2026.
- [6] Serge Lang. *Algebra*. Springer-Verlag, New York, revised third edition, 2002.
- [7] Barry M. Trager. Algebraic approach to rational function integration. In *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, SYMSAC '76, pages 219–226, New York, NY, USA, 1976. Association for Computing Machinery.
- [8] David Y. Y. Yun. On square-free decomposition algorithms. In *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, SYMSAC '76, pages 26–35, New York, NY, USA, 1976. Association for Computing Machinery.

واژه‌نامه فارسی به انگلیسی

الف

Bézout's Identity	اتحاد بزو
Heuristic Algorithm	الگوریتم ابتکاری
Euclidean Algorithm	الگوریتم اقلیدسی
Extended Euclidean Algorithm	الگوریتم اقلیدسی تعمیم یافته
Division Algorithm	الگوریتم تقسیم
Rothstein-Trager Algorithm	الگوریتم روتشتاین-تراگر
Risch-Norman Algorithm	الگوریتم ریش-نورمن
Classical Risch Algorithm	الگوریتم کلاسیک ریش
Algebraic Integral	انتگرال جبری
Ideal	ایده‌آل
Principal Ideal	ایده‌آل اصلی

ب

Remainder	باقیمانده
Rational Part	بخش گویا
Logarithmic Part	بخش لگاریتمی
Greatest Common Divisor	بزرگترین مقسوم علیه مشترک

ت

Square-free Factorization	تجزیه بدون مربع
Elementary Functions	توابع مقدماتی
Differential Extension	توسیع دیفرانسیلی
Simple Extension	توسیع ساده
Elementary Extension	توسیع مقدماتی
Field Extension	توسیع میدانی

ج

Differential Algebra	جبر دیفرانسیلی
Ansatz	جواب حدسی
Leading Term	جمله پیشرو

چ

Polynomial	چندجمله‌ای
Monic Polynomial	چندجمله‌ای تکین
Minimal Polynomial	چندجمله‌ای کمینه

ح

Ring	حلقه
Commutative Ring	حلقه جابجایی
Differential Ring	حلقه دیفرانسیلی

خ

Quotient خارج قسمت

د

Euclidean Domain دامنه اقلیدسی

Principal Ideal Domain دامنه ایده‌آل اصلی

Unique Factorization Domain دامنه تجزیه یکتا

Integral Domain دامنه صحیح

Degree درجه

System of Linear Equations دستگاه معادلات خطی

ش

Pseudo-remainder شبه باقیمانده

Pseudo-division شبه تقسیم

Pseudo-quotient شبه خارج قسمت

ض

Leading Coefficient ضریب پیشرو

ع

Prime Element عنصر اول

Irreducible Element عنصر تحویل ناپذیر

Algebraic Element عنصر جبری

Logarithmic Element	عنصر لگاریتمی
Transcendental Element	عنصر متعالی
Exponential Element	عنصر نمایی
Identity Element	عنصر همانی
Unit Element	عنصر یکه

ف

Elementary Closed Form	فرم بسته مقدماتی
------------------------	------------------

ک

Hermite Reduction	کاهش هر میت
Partial Fractions	کسرهای جزئی

گ

Group	گروه
Abelian Group	گروه آبدلی

م

Sylvester Matrix	ماتریس سیلوستر
Symbolic Computation	محاسبات نمادین
Characteristic	مشخصه
Formal Derivative	مشتق صوری
Resultant	منتج
Field	میدان

Field of Constants	 میدان ثابت‌ها
Differential Field	 میدان دیفرانسیلی
Field of Fractions	 میدان کسرها

واژه‌نامه انگلیسی به فارسی

A

Abelian Group	گروه آبلی
Algebraic Element	عنصر جبری
Algebraic Integral	انتگرال جبری
Ansatz	جواب حدسی

B

Bézout's Identity	اتحاد بزو
-------------------	-----------

C

Characteristic	مشخصه
Classical Risch Algorithm	الگوریتم کلاسیک ریش
Commutative Ring	حلقه جابجایی

D

Degree	درجه
Differential Algebra	جبر دیفرانسیلی
Differential Extension	توسیع دیفرانسیلی
Differential Field	میدان دیفرانسیلی
Differential Ring	حلقه دیفرانسیلی
Division Algorithm	الگوریتم تقسیم

E

Elementary Closed Form	فرم بسته مقدماتی
Elementary Extension	توسیع مقدماتی
Elementary Functions	توابع مقدماتی
Euclidean Algorithm	الگوریتم اقلیدسی
Euclidean Domain	دامنه اقلیدسی
Exponential Element	عنصر نمایی
Extended Euclidean Algorithm	الگوریتم اقلیدسی تعمیم‌یافته

F

Field	میدان
Field Extension	توسیع میدانی
Field of Constants	میدان ثابت‌ها
Field of Fractions	میدان کسرها
Formal Derivative	مشتق صوری

G

Greatest Common Divisor	بزرگترین مقسوم‌علیه مشترک
Group	گروه

H

Hermite Reduction	کاهش هر میت
Heuristic Algorithm	الگوریتم ابتکاری

I

Ideal	ایده‌آل
Identity Element	عنصر همانی
Integral Domain	دامنه صحیح
Irreducible Element	عنصر تحویل‌ناپذیر

L

Leading Coefficient	ضریب پیشرو
Leading Term	جمله پیشرو
Logarithmic Element	عنصر لگاریتمی
Logarithmic Part	بخش لگاریتمی

M

Minimal Polynomial	چندجمله‌ای کمینه
Monic Polynomial	چندجمله‌ای تکین

P

Partial Fractions	کسرهای جزئی
Polynomial	چندجمله‌ای
Prime Element	عنصر اول
Principal Ideal	ایده‌آل اصلی
Principal Ideal Domain	دامنه ایده‌آل اصلی
Pseudo-division	شبه تقسیم
Pseudo-quotient	شبه خارج قسمت
Pseudo-remainder	شبه باقیمانده

Q

Quotient	خارج قسمت
----------	-----------

R

Rational Part	بخش گویا
Remainder	باقیمانده
Resultant	منتج
Ring	حلقه
Risch-Norman Algorithm	الگوریتم ریش-نورمن
Rothstein-Trager Algorithm	الگوریتم روتشتاین-تراگر

S

Simple Extension	توسیع ساده
Square-free Factorization	تجزیه بدون مربع
Sylvester Matrix	ماتریس سیلوستر
Symbolic Computation	محاسبات نمادین
System of Linear Equations	دستگاه معادلات خطی

T

Transcendental Element	عنصر متعالی
------------------------	-------------

U

Unique Factorization Domain	دامنه تجزیه یکتا
Unit Element	عنصر یکه