دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

مقدمه‌ای بر تجزیه جبری استوانه‌ای و کاربردهای آن

پایان‌نامه کارشناسی

کسرا کاکاوند

استاد راهنما

دکتر امیر هاشمی

۱۴۰۴

تقدیم به:

کلمه راستین، تنها نامی که پایدار است

Soli Deo Gloria.

فهرست مطالب

چکیده:

این رساله مقدمه‌ای جامع بر تجزیه استوانه‌ای جبری (CAD) ارائه می‌دهد که یک الگوریتم پایه‌ای در هندسه جبری حقیقی محاسباتی و محاسبات نمادین است و کاربردهای اصلی آن را بررسی می‌کند. ساختار این اثر به گونه‌ای طراحی شده است که پیش‌زمینه نظری لازم را پیش از ارائه مکانیسم و سودمندی CAD بنا می‌کند.

کار را با مروری بر چارچوب نظریه مدل آغاز می‌کنیم که تمرکز آن بر منطق مرتبه اول، ساختارها و نظریه میدان‌های حقیقی بسته است؛ این مبانی منطقی حذف سور را تشکیل می‌دهند. فصل دوم با پیوند هندسه جبری و منطق، مسئله حذف سور را به تفصیل شرح می‌دهد و در نتیجه چالش محوری که CAD حل می‌کند را مستقر می‌سازد. فصل سوم به پایه‌های گربنر و محاسبه آنها می‌پردازد و یک تکنیک جبری جایگزین برای مسئله عضویت در ایده‌آل و حل دستگاه معادلات ارائه می‌کند که زمینه‌ای برای مقایسه با رویکرد هندسی متمایز CAD فراهم می‌آورد.

اوج این رساله، شرح مفصلی از خود تجزیه استوانه‌ای جبری است. ما تجزیه‌های استوانه‌ای فضای اقلیدسی را تعریف می‌کنیم، الگوریتم کلاسیک تصویر کردن و توسیع دادن را ارائه داده و پیچیدگی آن را بحث می‌کنیم. در نهایت، قدرت CAD را از طریق کاربردهای کلیدی آن شامل حذف سور حقیقی، مسائل تصمیم‌گیری برای مجموعه‌های نیمه‌جبری و مثالی از اثبات قضایای خودکار نشان می‌دهیم. این اثر در نظر دارد تا درکی مستحکم از مبانی نظری ،CAD ساختار الگوریتمی آن و تأثیر عملی‌اش در حل مسائل ریاضی و مهندسی را در اختیار خواننده قرار دهد.

پیشگفتار

در آغاز، سپاس و ستایش را ویژه پروردگار یکتا می‌دانم که توفیق انجام این پژوهش و هر گام در مسیر دانش را از الطاف بی‌پایان او می‌دانم.

این رساله را با کمال عشق و احترام به پدر و مادر عزیزم تقدیم می‌کنم که پشتیبانی و فداکاری بی‌دریغ ایشان پشتوانه همیشگی من بوده است.

بر خود فرض می‌دانم از استاد راهنمای گران‌قدرم، دکتر امیر هاشمی، که با صبر و حوصله مثال‌زدنی و راهنمایی‌های ارزنده خویش مسیر این پژوهش را هموار ساختند، صمیمانه سپاسگزاری نمایم. از ایشان بسیار آموختم.

فصل ۱

نظریه مدل

نظریه مدل یکی از شاخه‌های اصلی و بنیادین منطق ریاضی است که به مطالعه ساختارهای ریاضی از طریق زبان‌های صوری و تفسیرهای آن‌ها می‌پردازد. این نظریه به بررسی ویژگی‌های مدل‌ها و ارتباط آن‌ها با نظریه‌های صوری می‌پردازد و ابزارهای قدرتمندی را برای تحلیل و اثبات قضایا در اختیار محققان قرار می‌دهد. در واقع، نظریه مدل به ما امکان می‌دهد تا به جای کار با اشیاء ریاضی خاص، با کلاس‌های گسترده‌تری از ساختارها کار کنیم و از این طریق به درک بهتری از مفاهیم ریاضی برسیم.

تاریخچه نظریه مدل به اوایل قرن بیستم باز می‌گردد و با کارهای اولیهٔ افرادی چون لودویگ ویتگنشتاین و آلفرد تارسکی پایه‌ریزی شده است. تارسکی به‌ویژه نقش مهمی در توسعهٔ این نظریه داشته و مفهوم «حقیقت در یک مدل» را معرفی کرده است. این مفهوم به عنوان یکی از پایه‌های اساسی نظریه مدل محسوب می‌شود و به تحلیل دقیق‌تر و سیستماتیک‌تر ساختارهای ریاضی کمک کرده است.

یکی از جنبه‌های مهم نظریه مدل، توانایی آن در اثبات نتایج بنیادی مانند قضیه‌های تمامیت و ناتمامیت گودل است. این قضایا نشان می‌دهند که در هر سیستم منطقی قدرتمندی، جملاتی وجود دارند که نمی‌توانند در چارچوب آن سیستم اثبات یا رد شوند. این نتایج نه تنها در ریاضیات بلکه در فلسفه و علوم کامپیوتر نیز تاثیرات عمیقی داشته‌اند.

نظریه مدل به ویژه در دهه‌های اخیر توانسته است تأثیرات قابل توجهی در زمینه‌های مختلف ریاضیات و علوم کامپیوتر داشته باشد. از کاربردهای این نظریه می‌توان به اثبات قضایای مهم در ریاضیات محض، تحلیل پیچیدگی الگوریتم‌ها، و حتی مدل‌سازی سیستم‌های بیولوژیکی اشاره کرد. به عنوان مثال، در نظریه مجموعه‌ها و نظریه اعداد، نظریه مدل به ما کمک می‌کند تا ساختارهای مختلف را مقایسه و تفاوت‌ها و شباهت‌های آن‌ها را تحلیل کنیم.

در این فصل، ابتدا به معرفی مفاهیم پایه‌ای نظریه مدل پرداخته و سپس به بررسی برخی از نتایج و قضایای مهم در این

زمینه خواهیم پرداخت. همچنین کاربردهای عملی این نظریه در شاخه‌های مختلف علمی مورد بحث قرار خواهد گرفت. هدف از این فصل، فراهم کردن یک دیدگاه جامع و منسجم از نظریه مدل و نشان دادن اهمیت و کاربردهای گسترده آن در حوزه‌های مختلف تحقیقاتی است.

در بخش‌های بعدی، به تفصیل به موضوعاتی مانند زبان‌های صوری، ساختارها، مدل‌ها و تفسیرها خواهیم پرداخت. همچنین، مفاهیم اساسی مانند هم‌ارزی مدل‌ها، نظریه‌های دستوری، و جملات عمومی را مورد بررسی قرار می‌دهیم. در نهایت، با مرور برخی از نتایج پیشرفته‌تر و کاربردهای عملی، نشان خواهیم داد که چگونه نظریه مدل می‌تواند ابزار قدرتمندی برای تحلیل و درک ساختارهای پیچیده باشد.

۱.۱ زبان و ساختار

در منطق ریاضی، برای شناخت انواع ساختارها، از منطق مرتبه اول استفاده می‌کنیم. منظور از یک ساختار، مجموعه‌ای است که در موضوع خاصی مورد بررسی واقع شده و مجهز به گردایه‌ای از توابع، روابط و عناصر متمایز است. سپس، یک زبان را انتخاب می‌کنیم که در آن می‌توانیم از این گردایه سخن بگوییم و نه بیشتر. برای مثال، زمانی که میدان مرتب اعداد حقیقی را با توابع نمایی مطالعه می‌کنیم، ساختار $(\mathbb{R}, +, \cdot, \exp, <, ۰, ۱)$ مد نظر است.

تعریف ۱-۱. به سه تایی $(\mathcal{R}, \mathcal{C}, \mathcal{F})$ یک زبان گفته می‌شود هرگاه

(۱) $\mathcal{F}$ یک مجموعه از نمادهای تابعی،

(۲) $\mathcal{R}$ یک مجموعه از نمادهای رابطه‌ای و

(۳) $\mathcal{C}$ یک مجموعه از ثوابت باشد.

از این به بعد، منظور از n_f و n_R این است که f یک تابع n_f متغیره، و R یک رابطه n_R تایی است و معمولاً می‌نویسیم

$$\mathcal{L} = (\mathcal{R}, \mathcal{C}, \mathcal{F})$$

برای مثال، $\mathcal{L}_r = \{+, -, ۰, ۱, \cdot\}$ زبان حلقه‌هاست که در آن $+$، $-$ و $\cdot$ نمادهای تابعی و ۰ و ۱ نمادهای ثوابت هستند.

تعریف ۲-۱. به $\mathcal{M}$ یک $\mathcal{L}$ـ ساختار گفته می‌شود هرگاه شامل موارد زیر باشد:

(۱) یک مجموعه ناتهی M که به آن جهان، دامنه یا مجموعه زیرین از $\mathcal{M}$ گفته می‌شود،

(۲) یک تابع $f^{\mathcal{M}} : M^{n_f} \longrightarrow M$ برای هر $f \in \mathcal{F}$،

(۳) یک مجموعه $R^{\mathcal{M}} \subseteq M^{n_R}$ برای هر $R \in \mathcal{R}$،

(۴) یک عنصر $c^{\mathcal{M}} \in M$ برای هر $c \in \mathcal{C}$.

معمولا ساختار را با $\mathcal{M} = (M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C})$ نمایش می‌دهیم و $f^{\mathcal{M}}$، $R^{\mathcal{M}}$ و $c^{\mathcal{M}}$ را تفسیرهای نمادهای f، R و c می‌نامیم.

برای مثال، فرض کنید در حال مطالعه گروه‌ها هستیم. در این صورت، از زبان $\mathcal{L}_g = \{e, \cdot\}$ استفاده می‌کنیم که در آن $\cdot$ نماد دوتایی تابع و e نماد ثابت است. یک $\mathcal{L}_g$-ساختار $\mathcal{G} = (G, \cdot^{\mathcal{G}}, e^{\mathcal{G}})$، شامل یک مجموعه G با رابطه دوتایی $\cdot^{\mathcal{G}}$ و عنصر متمایز $e^{\mathcal{G}}$ است. به عنوان مثال، $\mathcal{G} = (\mathbb{R}, \cdot, ۱)$ یک $\mathcal{L}_g$-ساختار است که در آن $\cdot$ را به عنوان ضرب و e را به عنوان ۱ در نظر می‌گیریم.

تعریف ۳-۱. فرض کنید $\mathcal{M}$ و $\mathcal{N}$ به ترتیب دو ساختار با جهان‌های M و N باشند. یک $\mathcal{L}$-نشاندن $\eta : \mathcal{M} \longrightarrow \mathcal{N}$، یک نگاشت یک‌به‌یک $\eta : \mathcal{M} \longrightarrow \mathcal{N}$ است که خواص مجموعه $\mathcal{M}$ را برای نمادهای $\mathcal{L}$ حفظ می کند. به طور دقیق‌تر:
(۱) $f^{\mathcal{N}}(\eta(a_۱), \ldots, \eta(a_{n_f})) = \eta(f^{\mathcal{M}}(a_۱, \ldots, a_{n_f}))$ برای هر $f \in \mathcal{F}$ و $a_۱, \ldots, a_n \in M$ ؛
(۲) $(a_۱, \ldots, a_{m_R}) \in R^{\mathcal{M}}$ اگر و تنها اگر $(\eta(a_۱), \ldots, \eta(a_{M_R})) \in R^{\mathcal{N}}$ برای هر $R \in \mathcal{R}$ و $a_۱, \ldots, a_{m_j} \in M$؛
(۳) $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$ برای هر $c \in \mathcal{C}$.

به یک $\mathcal{L}$-نشاندن دوسویی، یک $\mathcal{L}$-یکریختی می‌گویند. اگر $M \subseteq N$ و نگاشت شمول یک $\mathcal{L}$-نشاندن باشد، می‌گوییم $\mathcal{M}$ یک زیرساختار از $\mathcal{N}$، یا $\mathcal{N}$ یک توسیع از $\mathcal{M}$ است.

مثال ۴-۱. $(\mathbb{Z}, +, ۰)$ یک زیرساختار از $(\mathbb{R}, +, ۰)$ است.

مثال ۵-۱. اگر $\eta : \mathbb{Z} \to \mathbb{R}$ یک تابع باشد که $\eta(x) = e^x$، آنگاه η یک $\mathcal{L}_g$-نشاندن از $(\mathbb{Z}, +, ۰)$ به $(\mathbb{R}, \cdot, ۱)$ است.

تعریف ۶-۱. مجموعه $\mathcal{L}$-ترم‌ها، کوچکترین مجموعه $\mathcal{T}$ است که شامل موارد زیر می‌شود:
(۱) $c \in \mathcal{T}$ برای هر نماد ثابت $c \in \mathcal{C}$.
(۲) هر نماد متغیر $v_i \in \mathcal{T}$ برای $i = ۱, ۲, \ldots, n$ و
(۳) اگر $t_۱, \ldots, t_{n_f} \in \mathcal{T}$ و $f \in \mathcal{F}$، آنگاه $f(t_۱, \ldots, t_{n_f}) \in \mathcal{T}$.
.

برای مثال، $\cdot((v_۱), -(v_۳, ۱)), \cdot(+(v_۱, v_۲), +(v_۳, ۱))$ و $+(۱, +(۱, +(۱, ۱)))$، $\mathcal{L}_r$-ترم هستند.
برای سادگی، یک $\mathcal{L}$-ترم را ترم یا کلمه می‌نامیم.

تعریف ۷-۱. می‌گوییم ϕ یک $\mathcal{L}$-فرمول اتمی است هرگاه یکی از شرایط زیر برای ϕ برقرار باشد:
(۱) $t_۱ = t_۲$، که $t_۱$ و $t_۲$ هردو ترم باشند، یا
(۲) $R(t_۱, \ldots, t_{n_R})$، به طوری که $R \in \mathcal{R}$ و $t_۱, \ldots, t_{n_R}$ ترم باشند.

تعریف ۸-۱. مجموعه $\mathcal{L}$-فرمول‌ها کوچکترین مجموعه $\mathcal{W}$ است که شامل فرمول‌های اتمی است به طوری که:
(۱) اگر $\phi \in \mathcal{W}$ آنگاه $\neg\phi \in \mathcal{W}$،
(۲) اگر ϕ و ψ در $\mathcal{W}$ آنگاه $(\phi \wedge \psi)$ و $(\phi \vee \psi)$ در $\mathcal{W}$ باشند،
(۳) اگر $\phi \in \mathcal{W}$ آنگاه $\exists v_i \phi$ و $\forall v_i \phi$ در $\mathcal{W}$ باشند.

می‌گوییم یک متغیر v، در فرمول ϕ آزادانه اتفاق می‌افتد هرگاه درون یک سور $\exists v$ یا $\forall v$ نباشد. در غیر این صورت، آن را یک کران می‌نامیم.
فرمولی را که متغیر آزاد نداشته باشد، جمله می‌نامیم.

عبارات زیر، چند مثال از جمله‌ها در $\mathcal{L}_{or}$ (زبان حلقه‌های مرتب) هستند:

- $v_۱ = ۰ \vee v_۱ > ۰$.
- $\exists v_۱ \ v_۲ \cdot v_۲ = v_۱$.
- $\forall v_۱ \ (v_۱ = ۰ \vee \exists v_۲ \ v_۲ \cdot v_۱ = ۱)$.

از این به بعد برای سادگی نوشتار، قرار می‌دهیم $\overline{a} = (a_{i_۱}, \dots, a_{i_m})$.

تعریف ۹-۱. فرض کنید ϕ یک فرمول با متغیرهای آزاد $\overline{v} = (v_{i_۱}, \dots, v_{i_m})$ باشد و $\overline{a} = (a_{i_۱}, \dots, a_{i_m}) \in M^n$.
عبارت $\mathcal{M} \models \phi(\overline{a})$ را به صورت زیر تعریف می‌کنیم:
(۱) اگر $\phi \equiv t_۱ = t_۲$ و $t_۱^{\mathcal{M}}\phi(\overline{a}) = t_۲^{\mathcal{M}}\phi(\overline{a})$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۲) اگر $\phi \equiv R(t_۱, \dots, t_{n_R})$ و $(t_۱^{\mathcal{M}}(\overline{a}), \dots, t_۲^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}}$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۳) اگر $\phi \equiv \neg\psi$ و $\mathcal{M} \not\models \psi(\overline{a})$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۴) اگر $\phi \equiv (\psi \wedge \theta)$، $\mathcal{M} \models \psi(\overline{a})$ و $\mathcal{M} \models \theta(\overline{a})$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۵) اگر $\phi \equiv (\psi \vee \theta)$، $\mathcal{M} \models \psi(\overline{a})$ یا $\mathcal{M} \models \theta(\overline{a})$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۶) اگر $\phi \equiv \exists v_j \psi(\overline{v}, v_j)$ و $b \in M$ وجود داشته باشد به طوری که $\mathcal{M} \models \psi(\overline{a}, b)$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.
(۷) اگر $\phi \equiv \forall v_j \psi(\overline{v}, v_j)$ و $b \in M$ وجود داشته باشد به طوری که $\mathcal{M} \models \psi(\overline{a}, b)$، آنگاه $\mathcal{M} \models \phi(\overline{a})$.

اگر $\mathcal{M} \models \phi(\overline{a})$، می‌گوییم $\mathcal{M}$ مستلزم $\phi(\overline{a})$، یا $\phi(\overline{a})$ در $\mathcal{M}$ درست است. برای $\psi_۱ \wedge \cdots \wedge \psi_n$ و $\psi_۱ \vee \cdots \vee \psi_n$ به ترتیب می‌نویسیم $\bigwedge \psi_i$ و $\bigvee \psi_i$، برای $i = ۱, \dots, n$.

در واقع سورهای $\forall$ و $\exists$ فقط روی عناصر یک مدل قرار داده می‌شوند. برای مثال، این جمله که "هر زیرمجموعه کران‌دار، حداقل یک کوچکترین کران بالا دارد" را نمی‌توان توسط یک فرمول بیان کرد چون نمی‌توانیم از سورها روی زیرمجموعه‌ها استفاده کنیم. از آن‌جا که به قرار دادن سور روی عناصر یک ساختار محدود می‌شویم، سبب می‌شود آن را "منطق مرتبه اول" بنامیم.
گزاره زیر نشان می‌دهد اگر یک فرمول بدون سور در یک ساختار درست باشد، آنگاه در هر توسیعی درست است؛ این را با استقرا روی فرمول‌های بدون سور اثبات می‌کنیم.

گزاره ۱۰-۱. فرض کنید $\mathcal{M}$ یک زیرساختار از $\mathcal{N}$، $\overline{a} \in M$ و $\phi(\overline{v})$ یک فرمول بدون سور باشد. در این صورت، $\mathcal{M} \models \phi(\overline{a})$ اگر و تنها اگر $\mathcal{N} \models \phi(\overline{a})$.

اثبات. ادعا: اگر $t(\overline{v})$ یک ترم باشد و $b \in M$، آنگاه $t^{\mathcal{M}}(\bar{b}) = t^{\mathcal{N}}(\bar{b})$. این را با استقرا روی ترم‌ها اثبات می‌کنیم. اگر t نماد ثابت c باشد، آنگاه $c^{\mathcal{M}} = c^{\mathcal{N}}$. اگر t متغیر v_i باشد، آنگاه $t^{\mathcal{M}}(\bar{b}) = b_i = t^{\mathcal{N}}(\bar{b})$.

فرض کنید $t = f(t_1, \ldots, t_n)$، به طوری که f یک نماد تابعی n تایی، $t_1, \ldots, t_n$ ترم باشند و $t_i^{\mathcal{M}}(\bar{b}) = t_i^{\mathcal{N}}(\bar{b})$ برای $i = 1, \ldots, n$. از آنجایی که $\mathcal{M} \subseteq \mathcal{N}$، داریم $f^{\mathcal{M}} = |f^{\mathcal{N}}|_{M^n}$. بنابراین

$$\begin{aligned} t^{\mathcal{M}}(\bar{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\bar{b}), \ldots, t_n^{\mathcal{N}}(\bar{b})) \\ &= t^{\mathcal{N}}(\bar{b}). \end{aligned}$$

حال، گزاره را با استقرا روی فرمول‌های ثابت می‌کنیم. اگر ϕ، $t_1 = t_2$ باشد، آنگاه

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \Leftrightarrow t_1^{\mathcal{N}}(\overline{a}) = t_2^{\mathcal{N}}(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a})$$

اگر ϕ، $R(t_1, \ldots, t_n)$ باشد به طوری که R یک نماد رابطه‌ای n تایی است، آنگاه

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow (t_1^{\mathcal{N}}(\overline{a}), \ldots, t_n^{\mathcal{N}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow \mathcal{N} \models \phi(\overline{a}) \end{aligned}$$

بنابراین، گزاره برای همه فرمول‌های اتمی درست است.

فرض کنید گزاره برای ψ درست و ϕ، $\neg\psi$ باشد. در این صورت،

$$\mathcal{M} \models \neg\phi(\overline{a}) \Leftrightarrow \mathcal{M} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a}).$$

اکنون فرض کنید گزاره برای ψ_0 و ψ_1 درست و ϕ، $\psi_0 \wedge \psi_1$ باشد. در این صورت

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow \mathcal{M} \models \psi_0(\overline{a}) \text{ و } \mathcal{M} \models \psi_1(\overline{a}) \\ &\Leftrightarrow \mathcal{N} \models \psi_0(\overline{a}) \text{ و } \mathcal{N} \models \psi_1(\overline{a}) \\ &\Leftrightarrow \mathcal{N} \models \phi(\overline{a}) \end{aligned}$$

در نتیجه، نشان دادیم گزاره برای همه فرمول‌های اتمی برقرار و اگر برای ϕ و ψ برقرار باشد، آنگاه برای $\neg\phi$ و $\phi \wedge \psi$ نیز برقرار است. از آنجایی که مجموعه فرمول‌های بدون، کوچک‌ترین مجموعه از فرمول‌های شامل فرمول‌های اتمی است و همچنین تحت نقیض و ترکیب‌های عطفی بسته است، گزاره برای همه فرمول‌های بدون سور درست است. □

تعریف ۱-۱۱. می‌گوییم دو $\mathcal{L}$-ساختار $\mathcal{M}$ و $\mathcal{N}$، هم‌ارز مقدماتی‌اند و می‌نویسیم $\mathcal{M} \equiv \mathcal{N}$ اگر:

$$\mathcal{M} \models \phi \Longleftrightarrow \mathcal{N} \models \phi$$

برای هر $\mathcal{L}$-جمله ϕ.
به مجموعه $\mathrm{Th}(\mathcal{M}) = \{\phi \mid \mathcal{M} \models \phi\}$، تئوری کامل گفته می‌شود که شامل همه $\mathcal{L}$-جمله‌های ϕ است به طوری که $\mathcal{M} \models \phi$. واضح است که $\mathcal{M} \equiv \mathcal{N}$ اگر و تنها اگر $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$. در ادامه خواهیم دید که $\mathrm{Th}(\mathcal{M})$ یک یکریختی پایا از $\mathcal{M}$ است.

قضیه ۱-۱۲. فرض کنید که $\mathcal{N} \longrightarrow \mathcal{M} : j$ یک یکریختی باشد. آنگاه، $\mathcal{M} \equiv \mathcal{N}$.

اثبات. با استقرا روی فرمول ها نشان می‌دهیم که $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ اگر و تنها اگر $\mathcal{N} \models \phi(j(a_1), \ldots, j(a_n))$، برای هر فرمول ϕ. ابتدا نشان می‌دهیم که همه ترم‌ها خوش رفتارند.
ادعا: فرض کنید t یک ترم و متغیرهای آزاد در t به فرم $\overline{v} = (v_1, \ldots, v_n)$ باشند. برای $\overline{a} \in M$، قرار می‌دهیم $j(\overline{a})$ برای $(j(a_1), \ldots, j(a_n))$. آنگاه $j(t^{\mathcal{M}}(\overline{a}) = t^{\mathcal{N}}(j(\overline{a}))$. این را با استقرا روی ترم‌ها اثبات می‌کنیم.
(۱) اگر $t = c$، آنگاه $j(t^{\mathcal{M}}(\overline{a})) = j(c^{\mathcal{M}}) = c^{\mathcal{M}} = t^{\mathcal{N}}(j(\overline{a}))$.
(۲) اگر $t = v_i$، آنگاه $j(t^{\mathcal{M}}(\overline{a})) = j(a_i) = t^{\mathcal{N}}(j(a_i))$.
(۳) اگر $t = f(t_1, \ldots, t_m)$، آنگاه :

$$\begin{aligned} j(t^{\mathcal{M}}(\overline{a})) &= j(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_m^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(j(t_1^{\mathcal{M}}(\overline{a}), \ldots, j(t_m^{\mathcal{M}}(\overline{a})))) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(j(\overline{a})), \ldots, t_m^{\mathcal{N}}(j(\overline{a}))) \\ &= t^{\mathcal{N}}(j(\overline{a})) \end{aligned}$$

با استقرا روی فرمول‌ها ادامه می‌دهیم.
(۱) اگر $\phi(\overline{v}) \equiv t_1 = t_2$، آنگاه

$$\mathcal{M} \models \phi(\overline{a}) \quad \Leftrightarrow t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \quad \Leftrightarrow j(t_1^{\mathcal{M}}(\overline{a})) = j(t_2^{\mathcal{M}}(\overline{a})) \Leftrightarrow t_1^{\mathcal{N}}(j(\overline{a})) = t_2^{\mathcal{N}}(j(\overline{a})) \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a}))$$

(۲) اگر $\phi(\overline{v}) \equiv R(t_1, \ldots, t_n)$، آنگاه

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) \Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \Leftrightarrow (j(t_1^{\mathcal{M}}(\overline{a})), \ldots, j(t_n^{\mathcal{M}}(\overline{a}))) \in R^{\mathcal{N}} \\ \Leftrightarrow (t_1^{\mathcal{N}}(j(\overline{a})), \ldots, t_n^{\mathcal{N}}(j(\overline{a}))) \in R^{\mathcal{N}} \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

(۳) اگر $\phi \equiv \neg\psi$، آنگاه با استقرا داریم

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \nvDash \psi(\overline{a}) \Leftrightarrow \mathcal{N} \nvDash \psi(j(\overline{a})) \Leftrightarrow \mathcal{N}\phi j(\overline{a}).$$

(۴) اگر $\phi \equiv \psi \wedge \theta$، آنگاه

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \models \psi(\overline{a}) \quad ; \quad \mathcal{M} \models \theta(\overline{a}) \Leftrightarrow \mathcal{N} \models \psi(j(\overline{a})) \quad ; \quad \mathcal{N} \models \theta(j(\overline{a})) \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})).$$

(۵) اگر $\phi(\overline{v}) \equiv \exists w \psi(\overline{v}, w)$، آنگاه

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \models \psi(\overline{a}, b) \Leftrightarrow \mathcal{N} \models \psi(j(\overline{a}), c) \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})).$$

برای $b, c \in M$. □

۲.۱ تئوری‌ها

در چارچوب نظریه مدل، یک تئوری به صورت یک مجموعه بسته از جملات در یک زبان مرتبه اول تعریف می‌شود؛ یعنی مجموعه‌ای از فرمول‌ها که تحت نتیجه‌گیری منطقی بسته است: اگر جمله‌ای نتیجه منطقی مجموعه باشد، در خود تئوری نیز موجود است. تئوری‌ها نمایانگر توصیفات صوری از کلاس‌هایی از ساختارها هستند که در آن‌ها تمامی جملات تئوری برقرارند. از این‌رو، تئوری‌ها ابزار قدرتمندی برای انتزاع و تحلیل خواص ساختاری در ریاضیات به شمار می‌آیند.

به طور مشخص، یک تئوری در زبان $\mathcal{L}$ را می‌توان مجموعه‌ای از جملات $\mathcal{L}$ دانست که به لحاظ نحوی سازگار و تحت استنتاج بسته باشد. در این بخش، پس از ارائه تعریف رسمی تئوری، به بررسی چند نمونه‌ی مهم از تئوری‌های مرتبه اول می‌پردازیم که در ریاضیات نقش کلیدی دارند، از جمله: تئوری گروه‌ها، حلقه‌ها و میدان‌ها، گراف‌ها، R–مدول‌ها و سایر ساختارهای مشابه. در هر مورد، زبان مناسب انتخاب می‌شود و مجموعه‌ای از اصول موضوعه ارائه می‌گردد که تئوری مربوطه را تشکیل می‌دهند.

هدف این بخش، فراهم آوردن بستری مفهومی و فنی برای بررسی دقیق‌تر مفاهیم مدل‌پذیری، کامل بودن، قطعیت، و سایر ویژگی‌های منطقی تئوری‌ها در ادامه‌ی فصل است.

تعریف ۱-۱۳. فرض کنید $\mathcal{L}$ یک زبان باشد. یک $\mathcal{L}$–تئوری T در واقع یک مجموعه از جمله‌هاست . اگر $\mathcal{M} \models \phi$ برای هر جمله $\phi \in T$، می‌گوییم $\mathcal{M}$ یک مدل برای T است و می‌نویسیم $\mathcal{M} \models T$.
مجموعه $T = \{\forall x\, x = 0, \exists x\, x \neq 0\}$ یک تئوری است و چون دو جمله آن باهم در تناقض‌اند، مدلی برای T وجود ندارد. اگر مدلی برای T وجود داشته باشد، می‌گوییم T تعریف‌پذیر است .

تعریف ۱-۱۴. یک کلاس از $\mathcal{L}$–ساختار ها مانند $\mathcal{K}$ در نظر بگیرید. اگر یک $\mathcal{L}$–تئوری T وجود داشته باشد به طوری که $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \models T\}$، می‌گوییم $\mathcal{K}$ یک کلاس مقدماتی است.

مثال ۱-۱۵. گراف‌ها
فرض کنید $\mathcal{L} = \{R\}$، به طوری که R یک رابطه دوتایی است. گراف‌های بدون بازتاب توسط دو جمله اصل‌بندی می‌شوند:

$\forall x \neg R(x,x),$

$\forall x \forall y\ (R(x,y) \to R(y,x)).$

مثال ۱۶-۱. گروه‌ها

فرض کنید $\mathcal{L} = \{\cdot, e\}$. کلاس گروه‌ها به صورت زیر اصل‌بندی می‌شود:

$\forall x\ x \cdot e = x$،

$\forall x \forall y \forall z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$،

$\forall x \exists y\ x \cdot y = y \cdot x = e$.

همچنین می‌توانیم با اضافه کردن اصل زیر به اصول بالا، کلاس گروه‌های مرتب آبلی را اصل بندی کرد:

$\forall x \forall y\ x \cdot y = y \cdot x.$

مثال ۱۷-۱. گروه‌های آبلی مرتب

فرض کنید $\mathcal{L} = \{+, <, \circ\}$ که $+$ یک نماد تابعی دو موضعی، $<$ یک نماد رابطه‌ای دو موضعی و $\circ$ یک نماد ثابت است. اصول گروه‌های مرتب عبارتند از

(i) اصول گروهای جمعی،

(ii) اصول ترتیب‌های خطی و

(iii) $\forall x \forall y \forall z (x < y \to x + z < y + z)$.

مثال ۱۸-۱. R-مدول‌های چپ

فرض کنید R یک حلقه با عضو خنثی ضربی ۱ باشد و $\mathcal{L} = \{+, \circ\} \cup \{r : r \in R\}$ که $+$ یک نماد دو موضعی تابعی، $\circ$ یک ثابت و r یک نماد تابعی تک موضعی برای هر $r \in R$ باشد. در یک R-مدول، r را به عنوان ضرب اسکالر توسط R در نظر می‌گیریم. اصول R-مدول‌های چپ عبارتند از

(i) اصول گروه‌های جابجایی،

(ii) $\forall x r(x+y) = r(x) + r(y)$، برای هر $r \in R$،

(iii) $\forall x (r+s)(x) = r(x) + s(x)$، برای هر $r, s \in R$،

(iv) $\forall x r(s(x)) = rs(x)$، برای $r, s \in R$،

(v) $\forall x \mathbf{1}(x) = x.$

مثال ۱۹-۱. حلقه‌ها و میدان‌ها

زبان حلقه‌ها $\mathcal{L}_r$ را در نظر بگیرید. اصول حلقه‌ها به صورت زیر هستند:

$\forall x \forall y \forall z\ (x - y = z \leftrightarrow x = y + z)$،

$\forall x\ x \cdot \circ = \circ$،

$\forall x \forall y \forall z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z),$

$\forall x\ x \cdot \mathbf{1} = x,$

$$\forall x \forall y \forall z \; x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$
$$\forall x \forall y \forall z \; (x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

کلاس میدان‌ها با اضافه کردن موارد زیر به اصول بالا، اصل‌بندی می‌شوند:

$$\forall x \forall y \; x \cdot y = y \cdot x،$$
$$\forall x \; (x \neq ۰ \to \exists y \; x \cdot y = ۱).$$

مثال ۱-۲۰. میدان‌های دیفرانسیلی

فرض کنید $\mathcal{L} = \mathcal{L}_r \cup \{\delta\}$ به طوری که δ نماد تابعی است. کلاس میدان‌های مشتق توسط اصول میدان‌ها اصل‌بندی می‌شوند:

$$\forall x \forall y \; \delta(x + y) = \delta(x) + \delta(y),$$
$$\forall x \forall y \; \delta(x \cdot y) = \delta(x) \cdot \delta(y).$$

مثال ۱-۲۱. میدان‌های مرتب

فرض کنید $\mathcal{L}_{or} = \mathcal{L} \cup \{<\}$. کلاس میدان‌های مرتب توسط اصول میدان‌ها اصل‌بندی می‌شوند:

$$\forall x \forall y \forall z \; (x < y \to x + z < y + z),$$
$$\forall x \forall y \forall z \; ((x < y \wedge y > ۰) \to x \cdot z < y \cdot z).$$

تعریف ۱-۲۲. فرض کنید T یک تئوری و ϕ یک جمله باشد. اگر $\mathcal{M} \models \phi$ هرگاه $\mathcal{M} \models T$، می‌گوییم ϕ نتیجه منطقی T است و می‌نویسیم $T \models \phi$.

مثال ۱-۲۳. فرض کنید $\mathcal{L} = \{+, <, ۰\}$ و T تئوری گروه‌های مرتب آبلی باشد. در این صورت،

$$\forall x \; (x \neq ۰ \to x + x \neq ۰)$$

یک نتیجه منطقی T است.

۳.۱ مجموعه‌های تعریف‌پذیر و تفسیرپذیری

یکی از مباحث کلیدی در نظریه مدل، مفهوم تعریف‌پذیری (Definability) و تفسیرپذیری (Interpretability) ساختارها و مجموعه‌هاست. این مفاهیم ابزارهای ظریفی را برای تحلیل روابط بین ساختارهای مختلف فراهم می‌آورند و نقش اساسی در درک محتوای منطقی و قدرت بیانی زبان‌ها و نظریه‌ها ایفا می‌کنند.

در این بخش، ابتدا به تعریف دقیق مجموعه‌های تعریف‌پذیر در یک ساختار مرتبه اول می‌پردازیم. این مجموعه‌ها، به‌طور شهودی، زیرمجموعه‌هایی از توان‌های مختلف دامنه که توسط فرمول‌های بدون پارامتر یا با پارامتر در زبان ساختار توصیف‌پذیرند، هستند. در ادامه، مفهوم تفسیرپذیری یک ساختار در ساختاری دیگر معرفی می‌شود؛ مفهومی که امکان کدگذاری یک ساختار ریاضی درون ساختاری دیگر را با حفظ روابط و خواص اساسی فراهم می‌آورد.

در طول این بخش، علاوه بر ارائه تعاریف دقیق و نتایج مقدماتی، به بررسی چند نمونه مهم و غیربدیهی از مجموعه‌ها و ساختارهای تعریف‌پذیر می‌پردازیم. از جمله این مثال‌ها می‌توان به ماشین تورینگ، اعداد صحیح p–ادیک، و خم‌های بیضوی اشاره کرد. این مثال‌ها نشان می‌دهند که چگونه مفاهیم تعریف‌پذیری و تفسیرپذیری می‌توانند در تحلیل ساختارهای پیچیده با منشأ متفاوت – از منطق محاسباتی تا هندسه جبری – به کار گرفته شوند.

این بخش زیربنای بسیاری از بحث‌های پیشرفته در نظریه مدل است، از جمله تحلیل پیچیدگی‌های توصیفی، تفسیر تئوری‌ها در یکدیگر، و انتقال ویژگی‌های منطقی از ساختاری به ساختار دیگر.

۱.۳.۱ مجموعه‌های تعریف‌پذیر

تعریف ۱-۲۴. فرض کنید $\mathcal{M} = (M, \dots)$ یک $\mathcal{L}$–ساختار باشد. می‌گوییم $X \subseteq M^n$ تعریف‌پذیر است اگر و تنها اگر یک فرمول $\phi(v_1, \dots, v_n, w_1, \dots, w_m)$ و $\overline{b} \in M^m$ وجود داشته باشد به طوری که

$$X = \{\overline{a} \in M^n : \mathcal{M} \models \phi(\overline{a}, \overline{b})\}.$$

می‌گوییم X، $\phi(\overline{v}, \overline{b})$ را تعریف می‌کند. همچنین می‌گوییم X، A–تعریف‌پذیر یا روی A تعریف‌پذیر است هرگاه یک فرمول $\psi(\overline{v}, w_1, \dots, w_l)$ و $\overline{b} \in A^l$ وجود داشته باشند به طوری که X، $\psi(\overline{v}, \overline{b})$ را تعریف کند.

مثال ۱-۲۵. زبان $\mathcal{L}_r$ را در نظر بگیرید. فرض کنید $\mathcal{M} = (R, +, -, \cdot, 0, 1)$ یک حلقه و $p(X) \in R[X]$ باشد. در این صورت، $Y = \{x \in R : p(x) = 0\}$ تعریف‌پذیر است.

مثال ۱-۲۶. در زبان $\mathcal{L}_r$، حلقه اعداد صحیح $\mathcal{M} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ را در نظر بگیرید. فرض کنید

$$X = \{(m, n) \in \mathbb{Z}^2 : m < n\}.$$

آنگاه X تعریف‌پذیر *(درواقع $\varnothing$–تعریف‌پذیر)* است. طبق قضیه لاگرانژ، هر عدد صحیح نامنفی حاصل جمع چهار عدد مربع است. بنابراین، اگر فرمول $\phi(x, y)$ را به صورت

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2)$$

تعریف کنیم، آنگاه $X = \{(m, n) \in \mathbb{Z}^2 : \mathcal{M} \models \phi(m, n)\}$.

مثال ۱-۲۷. فرض کنید F یک میدان و $\mathcal{M} = (F[X], +, -, \cdot, 0, 1)$ حلقه چندجمله‌ای‌ها روی F باشد. در این صورت، F در $\mathcal{M}$ تعریف‌پذیر است. در واقع، F مجموعه عناصر یکه $F[X]$ است و توسط فرمول $x = 0 \vee \exists y\ xy = 1$ تعریف می‌شود.

خم‌های بیضوی که به‌صورت معادلاتی از نوع $y^2 = x^3 + ax + b$ تعریف می‌شوند، ساختارهایی مهم در هندسه جبری و نظریه اعداد هستند. از منظر نظریه مدل، می‌توان آن‌ها را به‌عنوان زیرمجموعه‌های تعریف‌پذیر از $\mathbb{A}^2$ یا حتی $\mathbb{P}^2$ در

یک میدان مناسب در نظر گرفت. افزون بر این، گروه نقاط روی یک خم بیضوی (با عمل جمع تعریف‌شده هندسی) خود می‌تواند به‌عنوان یک ساختار تعریف‌پذیر بررسی شود. این تحلیل امکان بررسی ویژگی‌های منطقی این گروه‌ها – همچون وجود انواع خاصی از هم‌ریختی‌ها یا ویژگی‌های مدل‌پذیر – را فراهم می‌کند و پیوندی میان مدل تئوری و هندسه دیوفانتینی برقرار می‌سازد.

مثال ۲۸-۱. فرض کنید $\mathcal{M} = (\mathbb{C}(X), +, -, \cdot, ۰, ۱)$ میدان توابع گویا با ضرایب مختلط تک متغیره باشد. ادعا می‌کنیم $\mathbb{C}$ در $\mathbb{C}(X)$ با فرمول

$$\exists x\, \exists y \quad y^۲ = v \wedge x^۳ + ۱ = v$$

تعریف می‌شود. برای هر $z \in \mathbb{C}$ می‌توانیم x و y را پیدا کنیم به طوری که $y^۲ = x^۳ + ۱ = z$. فرض کنید h یک تابع غیرثابت با ضرایب گویا و توابع غیرثابت با ضرایب گویا f و g وجود داشته باشند به طوری که $h = g^۲ = f^۳ + ۱$. در این صورت $t \mapsto (f(t), g(t))$ یک تابع غیرثابت گویا از یک زیرمجموعه باز در $\mathbb{C}$ به خم E با معادله $y^۲ = x^۳ + ۱$ است. اما E یک خم بیضوی است و می‌دانیم که چنین توابعی وجود ندارند. به طور مشابه می‌توان نشان داد که $\mathbb{C}$ مجموعه توابع گویای f است به طوری که f و $f + ۱$ هر دو توان‌های چهارم هستند. این ایده‌ها نشان می‌دهند که $\mathbb{C}$ در هر توسیع جبری متناهی از $\mathbb{C}(X)$ تعریف‌پذیر است.

ساختار اعداد صحیح p–ادیک $\mathbb{Z}_p$، که از نظریه اعداد و توپولوژی غیر گسسته نشأت می‌گیرد، نمونه‌ای غنی از ساختاری است که تعریف‌پذیری در آن نقش کلیدی دارد. در مدل تئوری، می‌توان نشان داد که $\mathbb{Z}_p$ در برخی از زبان‌های گسترش‌یافته نظریه میدان‌ها، مانند زبان $Presburger$ یا زبان میدان ارزیاب، ساختاری تعریف‌پذیر است. از سوی دیگر، بسیاری از خواص جبری و عددی این ساختار از طریق مجموعه‌های تعریف‌پذیر در آن قابل بیان و بررسی هستند، که زمینه را برای تحلیل‌های مدل‌نظری عمیق‌تر فراهم می‌آورد.

مثال ۲۹-۱. فرض کنید $\mathcal{M} = (\mathbb{Q}_p, +, -, \cdot, ۰, ۱)$ میدان اعداد پی‌ادیک باشد. در این صورت، $\mathbb{Z}_p$، حلقه اعداد صحیح پی‌ادیک تعریف‌پذیر است. فرض کنید $p \neq ۲$ و $\phi(x)$ یک فرمول به صورت $\exists y\, y^۲ = px^۲ + ۱$. ادعا می‌کنیم $\phi(x)$، $\mathbb{Z}_p$ را تعریف می‌کند.

ابتدا، فرض کنید $y^۲ = pa^۲ + ۱$ و v ارزیاب پی‌ادیک باشد. از آن‌جایی که $v(pa^۲) = ۲v(a) + ۱$، اگر $v(a) < ۰$، آنگاه $v(pa^۲)$ یک عدد صحیح فرد منفی است و $v(y^۲) = v(pa^۲ + ۱) = v(pa^۲)$. از طرفی، $v(y^۲) = ۲v(y)$، یک عدد صحیح زوج است. بنابراین، اگر $\mathcal{M} \models \phi(a)$، آنگاه $v(a) \geq ۰$؛ پس $a \in \mathbb{Z}_p$. حال از طرفی دیگر، فرض کنید $a \in \mathbb{Z}_p$ و $F(X) = X^۲ - (pa^۲ + ۱)$. همچنین فرض کنید $\overline{F}$ کاهش F به پیمانه p باشد. از آن‌جایی که $v(a) \geq ۰$، $v(pa) > ۰$ و $\overline{F}(X) = X^۲ - ۱$ و $\overline{F}' = ۲X$. بنابراین، $\overline{F}(۱) = ۰$ و $\overline{F}'(۱) \neq ۰$؛ پس طبق لم هنسل یک $b \in \mathbb{Z}_p$ وجود دارد که $F(b) = ۰$. بنابراین $\mathcal{M} \models \phi(a)$.

مثال ۳۰-۱. میدان اعداد گویا $\mathcal{M} = (\mathbb{Q}, +, -, \cdot, ۰, ۱)$ را در نظر بگیرید. فرض کنید $\phi(x, y, z)$ فرمول

$$\exists a \exists b \exists c \quad xyz^۲ + ۲ = a^۲ + xy^۲ - yc^۲$$

و $\psi(x)$ فرمول

$$\forall y \forall z \quad ([\phi(y,z,\circ) \wedge (\forall w(\phi(y,z,w) \to \phi(y,z,w+۱)))] \to \phi(y,z,x))$$

باشد. یک نتیجه بسیار جالب از جولیا رابینسون[۱] نشان می‌دهد که $\psi(x)$، اعداد صحیح در $\mathbb{Q}$ را تعریف می‌کند.

ماشین‌های تورینگ به عنوان مدلی پایه برای محاسبه، نقشی محوری در نظریه محاسبات ایفا می‌کنند. از دید نظریه مدل، می‌توان رفتار ماشین‌های تورینگ را در قالب ساختارهایی تعریف کرد که نوار، وضعیت، تابع انتقال و ورودی را در زبان مرتبه اول مدلسازی می‌کنند. به‌طور خاص، مجموعه پیکربندی‌های قابل دستیابی توسط یک ماشین تورینگ خاص را می‌توان به صورت یک مجموعه تعریف‌پذیر در ساختاری مناسب بازسازی کرد. این بازسازی امکان تحلیل منطقی ویژگی‌های محاسباتی همچون توقف یا بازگشت‌پذیری را فراهم می‌آورد و پلی میان منطق ریاضی و نظریه محاسبه برقرار می‌سازد.

مثال ۳۱-۱. اعداد طبیعی $\mathbb{N}$ را با ساختار $\mathcal{L} = \{+, \cdot, \circ, ۱\}$ در نظر بگیرید. در این حالت، مجموعه‌های تعریف‌پذیر بسیار پیچیده هستند. برای مثال، یک $\mathcal{L}$–فرمول $T(e,x,s)$ وجود دارد به طوری که $\mathbb{N} \models T(e,x,s)$ اگر و تنها اگر ماشین تورینگ که توسط e کدگذاری شده باشد، در حداکثر s مرحله با ورودی x چاپ کند. بنابراین، ماشین تورینگ با برنامه e و با ورودی x چاپ می‌کند اگر و تنها اگر $\mathbb{N} \models \exists s T(e,x,s)$. پس مجموعه محاسبات پرینت کننده، تعریف‌پذیر است که می‌دانیم این مجموعه قابل محاسبه نیست. این منجر به یک نتیجه جالب می‌شود.

گزاره ۳۲-۱. تئوری کامل اعداد طبیعی در زبان $\mathcal{L}$ تصمیم‌پذیر نیست؛ یعنی الگوریتمی وجود ندارد که اگر یک $\mathcal{L}$–جمله ψ به عنوان ورودی به آن داده شد، همیشه اگر $\mathbb{N} \models \psi$ عبارت 'بله' و اگر $\mathbb{N} \models \neg\psi$ عبارت 'خیر' را چاپ کند.

اثبات. برای هر e و x، فرض کنید $\phi_{e,x}$، $\mathcal{L}$–فرمول به صورت

$$\exists s \quad T(\underbrace{۱+\cdots+۱}_{e-\text{times}}, \underbrace{۱+\cdots+۱}_{x-\text{times}}, s)$$

باشد. اگر چنین الگوریتمی وجود داشته باشد می‌توانیم تصمیم بگیریم آیا با پرسیدن $\mathbb{N} \models \phi_{e,x}$ برنامه کدگذاری شده با e و با ورودی x، پرینت می‌کند یا خیر؟ □

یک مجموعه را شمارش پذیر بازگشتی می‌نامیم هرگاه یک تابع بازگشتی وجود داشته باشد که تمام عناصر آن مجموعه را تولید کند. بنابر پاسخ ماتیجاسویچ–رابینسون–دیوس–پانتوم[۲] به مسئله دهم هیلبرت، برای هر مجموعه شمارش‌پذیر بازگشتی $A \subseteq \mathbb{N}^n$ چندجمله‌ای $p(x_۱, \cdots, x_n, y_۱, \cdots, y_n) \in \mathbb{Z}[\overline{x}, \overline{y}]$ وجود دارد به طوری که

$$A = \{\overline{x} \in \mathbb{N}^n \ : \ \mathbb{N} \models \exists y_۱ \cdots \exists y_m \, p(\overline{x}, \overline{y}) = \circ\}.$$

لم زیر در ادامه مفید خواهد بود.

---

۱ Julia Robinson ۲ Matijasevic–Robinson–Davis–Putnam

لم ۳۳-۱. فرض کنید $\mathcal{L}_r$ زبان حلقه‌های مرتب و $\mathcal{M} = (\mathbb{R}, +, -, \cdot, <, ۰, ۱)$ میدان مرتب اعداد حقیقی باشد. فرض کنید $X \subseteq \mathbb{R}^n$، Aـ تعریف‌پذیر باشد. در این صورت بستار توپولوژیک X هم Aـ تعریف‌پذیر است.

اثبات. فرض کنید $\phi(v_۱, \ldots, v_n, \overline{a})$، X را تعریف کند و $\psi(v_۱, \ldots, v_n, \overline{w})$ فرمول

$$\forall \epsilon [\epsilon > ۰ \to \exists y_۱, \cdots y_n \, (\phi(\overline{y}, \overline{w}) \wedge \sum_{i=۱}^{n} (x_i - y_i)^۲ < \epsilon)]$$

باشد. در این صورت $\overline{b}$ در بستار X وجود دارد اگر و تنها اگر $\mathcal{M} \models \psi(\overline{b}, \overline{a})$. □

در گزاره زیر، دسته‌بندی بهتری از مجموعه‌های تعریف‌پذیر ارائه می‌کنیم.

گزاره ۳۴-۱. فرض کنید $\mathcal{M}$ یک $\mathcal{L}$ـ ساختار باشد. همچنین فرض کنید D_n گردایه تمام زیرمجموعه‌های M^n برای $n \geq ۱$ و $\mathcal{D} = (D_n : n \geq ۱)$ کوچکترین گردایه‌ای باشد به طوری که:

(i) $M^n \in D_n$؛

(ii) برای همه نمادهای توابع n تایی f از $\mathcal{L}$، گراف (نمودار) $f^{\mathcal{M}}$ هم در $D_{n+۱}$ باشد؛

(iii) برای همه نمادهای رابطه n تایی R از $\mathcal{L}$، $R^{\mathcal{M}} \in D_n$؛

(iv) به ازای هر $i, j \leq n$، $\{(x_۱, \ldots, x_n) \in M^n : x_i = x_j\} \in D_n$؛

(v) اگر $X \in D_n$، آنگاه $M \times X \in D_{n+۱}$؛

(vi) هر D_n تحت مکمل، اجتماع و اشتراک بسته باشد؛

(vii) اگر $X \in D_{n+۱}$ و $\pi : M^{n+۱} \to M^n$ نگاشت تصویر باشد که $(x_۱, \ldots, x_{n+۱}) \mapsto (x_۱, \ldots, x_n)$، آنگاه $\pi(X) \in D_n$؛

$(viii)$ اگر $X \in D_{n+m}$ و $b \in M^m$، آنگاه $\{a \in M^n : (a, b) \in X\} \in D_n$.

در این صورت، $X \subseteq M^n$ تعریف‌پذیر است اگر و تنها اگر $X \in D_n$.

اثبات. ابتدا نشان می‌دهیم مجموعه‌های تعریف‌پذیر در موارد بستار $(viii) - (i)$ صدق می‌کنند. از آنجایی که $\mathcal{D}$ کوچک‌ترین گردایه شامل این ویژگی‌های بستار است، هر $X \in D_n$ تعریف‌پذیر می‌شود.

(i) M^n توسط $v_۱ = v_۱$ تعریف‌پذیر است.

(ii) گراف $f^{\mathcal{M}}$ توسط $f(x_۱, \ldots, x_{n_f}) = y$ تعریف‌پذیر است.

(iii) رابطه $R^{\mathcal{M}}$ توسط R تعریف‌پذیر است.

(iv) مجموعه $\{x \in M^n : x_i = x_j\}$ با $v_i = v_j$ تعریف می‌شود.

(v) اگر $X \subseteq M^n$ با $\phi(v_۱, \ldots, v_n, \overline{a})$ تعریف شود، آنگاه $M \times X$ توسط $\phi(v_۲, \ldots, v_{n+۱}, \overline{a})$ تعریف می‌شود.

(vi) اگر $X \subseteq M^n$ با $\phi(\overline{v}, \overline{a})$ و $Y \subseteq M^n$ با $\psi(\overline{v}, \overline{b})$ تعریف شود، آنگاه $M \setminus X$ با $\neg\phi(\overline{v}, \overline{a})$، $X \cap Y$ با $\phi(\overline{v}, \overline{a}) \wedge \psi(\overline{v}, \overline{b})$ و $X \cup Y$ توسط $\phi(\overline{v}, \overline{a}) \vee \psi(\overline{v}, \overline{b})$ تعریف می‌شود.

(vii) اگر $X \subseteq M^{n+۱}$ با $\phi(v_۱, \ldots, v_{n+۱}, \overline{a})$ تعریف شود، آنگاه $\pi(X)$ توسط $\exists v_{n+۱} \, \phi(\overline{v}, \overline{a})$ تعریف می‌شود.

$(viii)$ اگر $X \subset M^{n+m}$ با $\phi(v_۱, \ldots, v_{n+m}, \overline{c})$ تعریف شده باشد و $\overline{b} \in M^m$، آنگاه $\{\overline{a} \in M^n : (\overline{a}, \overline{b}) \in X\}$ با

$\phi(v_1, \ldots, v_n, \overline{b}, \overline{c})$ تعریف می‌شود.

بنابراین، اگر $X \in D_n$، آنگاه X تعریف‌پذیر است.

حال، نشان می‌دهیم اگر $X \subseteq M^n$ تعریف‌پذیر باشد، آنگاه $X \in D_n$. ابتدا، با استقرا نشان می‌دهیم اگر $t(v_1, \ldots, v_n)$ یک ترم باشد، آنگاه $\{(\overline{x}, y) \in M^{n+1} : t^{\mathcal{M}}(\overline{x}) = y\} \in D_{n+1}$.

اگر t ترم ثابت c باشد، باید نشان دهیم $\{(\overline{x}, c^{\mathcal{M}}) : \overline{x} \in M^n\} \in D_{n+1}$. بنابر (iv) و $(viii)$، $\{c^{\mathcal{M}}\} \in D_1$. در نتیجه، با n بار استفاده از (v)، $\{(\overline{x}, c^{\mathcal{M}}) : \overline{x} \in M^n\} \in D_{n+1}$. اگر t، v_i باشد، آنگاه باید نشان دهیم $\{(\overline{x}, x_i) : \overline{x} \in M^n\} \in D_{n+1}$ که از (i) و (iv) به راحتی نتیجه می‌شود.

فرض کنید $t = f(t_1, \ldots, t_m)$. با استقرا فرض می‌کنیم $G_i \in D_{n_i}$ که در آن G_i گراف $t_i^{\mathcal{M}} : M^n \to M$ است. فرض کنید $G \in D_{m+1}$ گراف $f^{\mathcal{M}}$ باشد. در این صورت، گراف $t^{\mathcal{M}}$ برابر است با:

$$\{(\overline{x}, y) : \exists z_1, \ldots, \exists z_m (\bigwedge_{i=1}^{m} (\overline{x}, z_i) \in G_i \wedge (\overline{z}, y) \in G)\}.$$

با ویژگی‌های بستار $\mathcal{D}$، به سادگی مشاهده می‌شود که این در D_{n+1} قرار می‌گیرد.

حال با استقرا روی فرمول‌ها نشان می‌دهیم هر $\emptyset$–تعریف‌پذیر $X \subseteq M^n$ در D_{n+1} قرار دارد. فرض کنید $\phi \equiv t_1 = t_2$ باشد. در این صورت

$$\{\overline{x} \in M^n : t_1^{\mathcal{M}}(\overline{x}) = t_2^{\mathcal{M}}(\overline{x})\} = \{\overline{x} \in M^n : \exists y \exists z (t_1^{\mathcal{M}} = y \wedge t_2^{\mathcal{M}} = z \wedge y = z)\} \in D_n.$$

فرض کنید ϕ، $R(t_1, \cdots, t_m)$ باشد. در این صورت

$$\{\overline{x} \in M^n : \mathcal{M} \models \phi(\overline{x})\} = \{\overline{x} \in M^n : \exists z_1, \ldots, \exists z_m \bigwedge_{i=1}^{m} t_i^{\mathcal{M}}(\overline{x}) = z_i \wedge \overline{z} \in R^{\mathcal{M}}\}.$$

بنابراین، تمام مجموعه‌های تعریف شده با فرمول‌های اتمی روی $\emptyset$ در $\mathcal{D}$ قرار دارند. از آنجایی که $\mathcal{D}$ نسبت به ترکیب‌های بولی و تصویرها بسته است، همه مجموعه‌های $\emptyset$–تعریف‌پذیر در $\mathcal{D}$ قرار دارند. طبق مورد $(viii)$، تمام مجموعه‌های تعریف‌پذیر در $\mathcal{D}$ هستند. □

گزاره ۳۵-۱. فرض کنید $\mathcal{M}$ یک $\mathcal{L}$–ساختار باشد. اگر $X \subset M^n$، A–تعریف‌پذیر باشد، آنگاه همه $\mathcal{L}$–اتومرفیسم‌های $\mathcal{M}$ که A را به صورت نقطه‌ای ثابت می‌کنند، X را هم به صورت مجموعه‌ای ثابت می‌کنند؛ یعنی σ یک اتومرفیسم از $\mathcal{M}$ باشد به طوری که $\sigma(a) = a$ برای هر $a \in A$، آنگاه $\sigma(X) = X$.

اثبات. فرض کنید $\psi(\overline{v}, \overline{a})$ فرمول تعریف کننده X در $\mathcal{L}$ باشد به طوری که $\overline{a} \in A$. همچنین، فرض کنید σ یک اتومرفیسم از $\mathcal{M}$ با $\sigma(\overline{a}) = \overline{a}$ باشد و $\overline{b} \in M^n$.

در اثبات قضیه ۱۲-۱، نشان دادیم اگر $j : \mathcal{M} \to \mathcal{N}$ یک یکریختی باشد، آنگاه $\mathcal{M} \models \phi(\overline{a})$ اگر و تنها اگر $\mathcal{N} \models \phi(j(\overline{a}))$. بنابراین

$$\mathcal{M} \models \psi(\overline{b}, \overline{a}) \leftrightarrow \mathcal{M} \models (\sigma(\overline{b}), \sigma(\overline{a})) \Leftrightarrow \mathcal{M} \models (\sigma(\overline{b}), \overline{a})$$

به عبارت دیگر، $\overline{b} \in X$ اگر و تنها اگر $\sigma(\overline{b}) \in X$. □

نتیجه ۳۶-۱. مجموعه اعداد حقیقی در میدان اعداد مختلط تعریف‌پذیر نیست.

اثبات. اگر $\mathbb{R}$ تعریف‌پذیر بود، آنگاه باید روی یک زیرمجموعه متناهی $A \subset \mathbb{C}$ تعریف‌پذیر باشد. فرض کنید $r, s \in \mathbb{C}$ روی A مستقل جبری باشند به طوری که $r \in \mathbb{R}$ و $s \notin \mathbb{R}$. در این صورت یک اتومرفیسم σ از $\mathbb{C}$ وجود دارد که تحدید آن به A، همانی می شود و $\sigma(r) = s$. بنابراین، $\sigma(\mathbb{R}) \neq \mathbb{R}$ و $\mathbb{R}$ روی A تعریف‌پذیر نیست. □

۴.۱ تفسیرپذیری

معمولا، مطالعه کردن ساختارهایی که در یک ساختار داده شده تعریف شده‌اند، مفید است. برای مثال، فرض کنید K یک میدان و $G = GL_۲(K)$ گروه ماتریس‌های وارون‌پذیر ۲×۲ روی K باشد. همچنین فرض کنید $X = \{(a, b, c, d) \in K^۴ \ : \ ad - bc \neq ۰\}$ و $f : X^۲ \to X$ که

$$f((a_۱, b_۱, c_۱, d_۱), (a_۲, b_۲, c_۲, d_۲)) = (a_۱a_۲ + b_۱c_۲, a_۱b_۲ + b_۱d_۲, c_۱a_۲ + d_۱c_۲, c_۱b_۲ + d_۱d_۲).$$

به طور واضح، X و f در $(K, +, \cdot)$ تعریف‌پذیر هستند و مجموعه X با عمل f با $GL_۲(K)$ یکریخت است به طوری که عنصر خنثی مجموعه X، $(۱, ۰, ۰, ۱)$ است. $\mathcal{L}_۰$-ساختار $\mathcal{N}$ را در $\mathcal{L}$-ساختار $\mathcal{M}$ به طور تعریف‌پذیر تفسیر شده می‌نامیم اگر و تنها اگر بتوانیم یک مجموعه تعریف‌پذیر $X \subseteq M^n$ پیدا کنیم و نمادهای $\mathcal{L}_۰$ را به عنوان زیرمجموعه‌های تعریف‌پذیر و توابع روی X تفسیر کنیم که $\mathcal{L}_۰$-ساختار حاصل، با $\mathcal{N}$ یکریخت باشد. مثال بالا نشان می‌دهد $(GL_n(K), \cdot, e)$ در $(K, +, \cdot, ۰, ۱)$ به طور تعریف‌پذیر تفسیر شده است. منظور از یک گروه جبری خطی روی K، یک زیرگروه از $GL_n(K)$ تعریف شده توسط معادلات چندجمله‌ای روی K است. به سادگی قابل مشاهده است که هر گروه جبری خطی روی K، به طور تعریف پذیر تفسیر شده روی K است.

برای مثال، فرض کنید $\mathcal{L} = \emptyset$، $\mathcal{M}$ یک $\mathcal{L}$-ساختار باشد که $|M| = \aleph_۰$ و $\mathcal{L}_۰ = \{E\}$ به طوری که E یک رابطه دوتایی است. همچنین فرض کنید $\mathcal{N} = (N, E)$، $\mathcal{L}_۰$-ساختاری باشد که E یک رابطه هم‌ارزی با تعداد $\aleph_۰$ کلاس، هر کدام از سایز $\aleph_۰$، است. قرار دهید

$$R = \{((x_۱, x_۲), (y_۱, y_۲)) \in M^۲ \times M^۲ \ : \ x_۱ = y_۱\}.$$

در این صورت، $\mathcal{N} \cong (M^۲, R)$؛ پس $\mathcal{N}$ به طور تعریف‌پذیر در M تفسیر شده است.

۵.۱ تفسیر کردن یک میدان در گروه آفین

مثال جالب‌تری را در نظر می‌گیریم. فرض کنید F یک میدان نامتناهی و G گروهی از ماتریس‌هایی به شکل

$$\begin{pmatrix} a & b \\ ۰ & ۱ \end{pmatrix}$$

باشد، که در آن $a, b \in F$ و $a \neq ۰$. این گروه با گروه تبدیل‌های آفین از نوع $x \mapsto ax + b$ که در آن $a, b \in F$ و $a \neq ۰$، یکریخت است.

نشان خواهیم داد که F در گروه G به‌طور تعریف‌پذیر، تفسیر می‌شود.

فرض کنید

$$\alpha = \begin{pmatrix} ۱ & ۱ \\ ۰ & ۱ \end{pmatrix} \quad \text{و} \quad \beta = \begin{pmatrix} \tau & ۰ \\ ۰ & ۱ \end{pmatrix},$$

که در آن $\tau \neq ۰, ۱$. مجموعه A را به‌صورت زیر تعریف می‌کنیم

$$A = \{g \in G : g\alpha = \alpha g\} = \left\{ \begin{pmatrix} ۱ & x \\ ۰ & ۱ \end{pmatrix} : x \in F \right\}$$

و

$$B = \{g \in G : g\beta = \beta g\} = \left\{ \begin{pmatrix} x & ۰ \\ ۰ & ۱ \end{pmatrix} : x \neq ۰ \right\}.$$

به وضوح، A و B با استفاده از پارامترهای α و β قابل تعریف هستند. گروه B بر روی A با مزدوج عمل می‌کند:

$$\begin{pmatrix} x & ۰ \\ ۰ & ۱ \end{pmatrix}^{-۱} \begin{pmatrix} ۱ & y \\ ۰ & ۱ \end{pmatrix} \begin{pmatrix} x & ۰ \\ ۰ & ۱ \end{pmatrix} = \begin{pmatrix} ۱ & \frac{y}{x} \\ ۰ & ۱ \end{pmatrix}.$$

عمل $(a, b) \mapsto b^{-۱}ab$ تعریف‌پذیر است. می‌توان نگاشت $i : A \setminus \{۱\} \to B$ را به صورت $i(a) = b$ تعریف کرد اگر و تنها اگر $b^{-۱}ab = \alpha$، یعنی

$$i \begin{pmatrix} ۱ & x \\ ۰ & ۱ \end{pmatrix} = \begin{pmatrix} x & ۰ \\ ۰ & ۱ \end{pmatrix}.$$

یک عملگر $*$ را بر روی A به‌صورت زیر تعریف می‌کنیم

$$a * b = \begin{cases} i(b)a(i(b))^{-۱} & b \neq I \text{ if} \\ ۱ & b = I \text{ if} \end{cases},$$

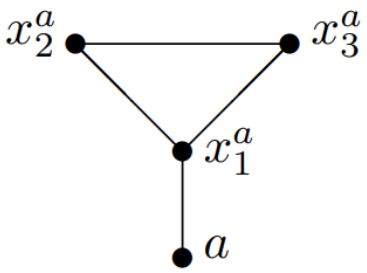
که در آن I ماتریس همانی است. اکنون به سادگی می‌توان دید که $(F, +, \cdot, ۰, ۱)$ با $(A, \cdot, *, ۱, \alpha)$ یکریخت است.

۶.۱ تفسیر کردن ترتیب‌ها در گراف‌ها

گراف‌ها به عنوان ساختارهایی شامل مجموعه‌ای از رأس‌ها به‌همراه رابطه‌ی یالی متقارن و بدون طوقه، در نگاه نخست فاقد هرگونه ساختار ترتیبی هستند. با این حال، در برخی شرایط می‌توان یک ترتیب خطی یا ترتیب جزئی را درون یک گراف تفسیر کرد. به‌طور مشخص، اگر گراف دارای ویژگی‌هایی نظیر وجود زیرگراف‌هایی با ساختارهای سلسله‌مراتبی خاص باشد (مانند زنجیره‌ها یا مسیرهای جهت‌دار در گراف‌های جهت‌دار مناسب)، می‌توان مجموعه‌ای از فرمول‌ها در زبان گراف‌ها تعریف کرد که رابطه‌ی ترتیبی را بر روی زیرمجموعه‌ای از رأس‌ها مدل‌سازی کنند. این تفسیرها نقش مهمی در تحلیل پیچیدگی مدل‌نظری کلاس گراف‌ها دارند؛ به‌ویژه در بررسی عدم پایایی، ω–پایایی یا قابلیت تعریف نظریه‌های قدرتمندتر (مانند حساب پئانو) در دل نظریه گراف‌ها. از این‌رو، تفسیر ترتیب‌ها در گراف‌ها مثالی کلیدی از عمق مفهومی تفسیرپذیری است که مرزهای میان ساختارهای ”ساده“ و ”پیچیده“ را بازتعریف می‌کند.

ساختارهای بسیار پیچیده اغلب می‌توانند در ساختارهایی که به‌ظاهر ساده‌تر هستند، تفسیر شوند. برای مثال، هر ساختاری در یک زبان شمارا می‌تواند در یک گراف تفسیر شود. یک مثال ساده از این ساختار را ارائه می‌دهیم که در آن ترتیب‌های خطی را در گراف‌ها تفسیر می‌کنیم.

فرض کنید $(A, <)$ یک ترتیب خطی باشد. گراف G_A را به‌صورت زیر می‌سازیم. برای هر $a \in A$، گراف G_A شامل رأس‌های $a, x^a_۱, x^a_۲, x^a_۳$ خواهد بود و زیرگراف زیر را شامل می‌شود:



هیچ یالی به‌جز یال‌های ذکر شده در بالا، هیچ یک از x^a_iها را به‌عنوان رأس نخواهد داشت. اگر $a < b$، گراف G_A دارای رأس‌های $y^{a,b}_۱, y^{a,b}_۲$ و $y^{a,b}_۳$ خواهد بود و زیرگراف زیر را شامل می‌شود:

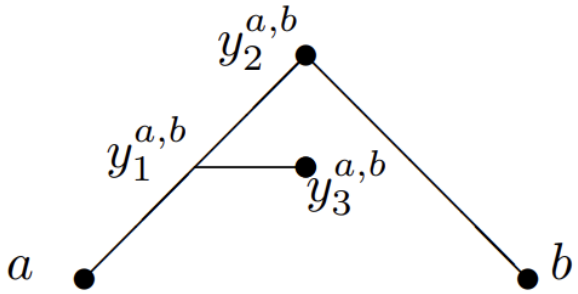
هیچ یالی به‌جز یال‌های نشان داده شده شامل هیچ یک از رأس‌های $y^{a,b}_i$ نخواهد بود و گراف G_A هیچ یالی به جز آن‌هایی که توصیف کرده‌ایم نخواهد داشت.

فرض کنید

$$V_A = A \cup \{x^a_۱, x^a_۲, x^a_۳ : a \in A\} \cup \{y^{a,b}_۱, y^{a,b}_۲, y^{a,b}_۳ : a, b \in A \text{ و } a < b\}$$

و R_A کوچک‌ترین رابطه‌ی متقارن شامل تمامی یال‌های زیر باشد:

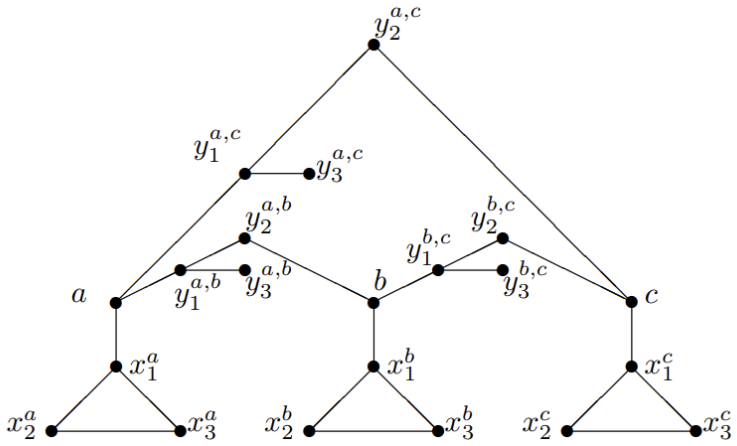
$$(a, x^a_۱), \quad (x^a_۱, x^a_۲), \quad (x^a_۱, x^a_۳), \quad (x^a_۲, x^a_۳),$$



برای $a \in A$ و

$$(a, y_1^{a,b}), \quad (y_1^{a,b}, y_2^{a,b}), \quad (y_1^{a,b}, y_3^{a,b}), \quad (y_2^{a,b}, b)$$

برای $a < b$. به عنوان مثال، اگر A یک ترتیب خطی شامل سه عنصر $a < b < c$ باشد، در این صورت گراف G_A به‌صورت زیر است:



فرض کنید $\mathcal{L} = \{R\}$ که در آن R یک رابطه دودویی است. یک $\mathcal{L}$–تئوری T را برای گراف‌هایی توصیف خواهیم کرد که در آن هر مدل از T گراف G_A برای یک ترتیب خطی یکتا A است.

ابتدا دو فرمول در زبان گراف‌ها معرفی می‌کنیم که دو نمودار اول را توصیف می‌کنند.

فرمول $\phi(x, u, v, w)$ را در نظر بگیرید که بیان می‌کند x, u, v, w متمایز هستند و یال‌های $(x, u), (u, v), (u, w)$ و (v, w) وجود دارند و این‌ها تنها یال‌های دربرگیرنده‌ی رأس‌های u, v, w هستند. توجه کنید که:

$$G_A \models \phi(a, x_1^a, x_2^a, x_3^a)$$

برای هر $a \in A$. فرمول $\psi(x,y,u,v,w)$ را در نظر بگیرید که بیان می‌کند x,y,u,v,w متمایز هستند و یال‌های $(x,u),(u,w),(u,w)$ و (v,y) وجود دارند و این‌ها تنها یال‌های دربرگیرنده رأس‌های u,v,w هستند. توجه کنید که:

$$G_A \models \psi(a,b,y_1^{a,b},y_2^{a,b},y_3^{a,b})$$

هرگاه در A داشته باشیم $a<b$.

فرمول‌های $\theta_0(z),\ldots,\theta_5(z)$ را به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned}
\theta_0(z) &\equiv \exists u \exists v \exists w\, \phi(z,u,v,w),\\
\theta_1(z) &\equiv \exists x \exists u \exists w\, \phi(x,z,u,w),\\
\theta_2(z) &\equiv \exists x \exists u \exists w\, \phi(x,x,z,w),\\
\theta_3(z) &\equiv \exists x \exists y \exists w\, \psi(x,y,z,v,w),\\
\theta_4(z) &\equiv \exists x \exists y \exists u \exists w\, \psi(x,y,u,z,w),\\
\theta_5(z) &\equiv \exists x \exists y \exists u \exists v\, \psi(x,y,u,v,z).
\end{aligned}$$

اگر $a,b \in A$ و $a<b$، آنگاه:

$$G_A \models \theta_0(a) \wedge \theta_1(x_1^a) \wedge \theta_2(x_2^a) \wedge \theta_2(x_3^a),$$

و

$$G_A \models \theta_3(y_1^{a,b}) \wedge \theta_4(y_2^{a,b}) \wedge \theta_5(y_3^{a,b}).$$

بنابراین، برای هر رأس x در G_A، داریم:

$$G_A \models \theta_i(x), \quad i = 0,1,\ldots,5.$$

لم ۳۷-۱. اگر $(A,<)$ یک ترتیب خطی باشد، آنگاه برای تمام رأس‌های x در G_A، یک مقدار یکتا $i \leq 5$ وجود دارد به‌طوری که $G_A \models \theta_i(x)$.

اثبات. فرض کنید x یک رأس در G_A باشد. اگر x بخشی از یک ۳-چرخه باشد، آنگاه $x = x_i^a$ برای مقداری از $a \in A$. درجه یک رأس تعداد یال‌هایی است که آن رأس را در بر می‌گیرند. اگر درجه x برابر ۳ باشد، آنگاه $\theta_1(x)$ یگانه فرمولی است که برقرار است. اگر درجه x برابر ۲ باشد، آنگاه $\theta_2(x)$ یگانه فرمولی است که برقرار است.

حال فرض کنید که x بخشی از یک ۳-چرخه نیست. در این حالت، یا x در A است یا $x = y_i^{a,b}$ که در آن $a,b \in A$ و $a<b$ و $i \leq 3$ است. اگر یک یال (x,v) وجود داشته باشد که v در یک ۳-چرخه باشد، آنگاه $\theta_0(x)$ یگانه فرمولی است که برقرار است. اگر x درجه ۱ داشته باشد، آنگاه $\theta_5(x)$ یگانه فرمولی است که برقرار است. اگر یک یال (x,v)

وجود داشته باشد که v درجه ۱ داشته باشد، آنگاه $\theta_3(x)$ یگانه فرمولی است که برقرار است. در غیر این صورت، $\theta_4(x)$ یگانه فرمولی است که برقرار است.

فرض کنید T تئوری $\mathcal{L}$ با اصول موضوعه زیر باشد:

(i) R متقارن و نامنعکس است؛

(ii) برای هر x، دقیقاً یکی از θ_i برقرار است؛

(iii) اگر $\theta_0(x)$ و $\theta_0(y)$ برقرار باشند، آنگاه $\neg R(x,y)$؛

(iv) اگر $\exists u \exists v \exists w\, \psi(x,y,u,v,w)$ برقرار باشد، آنگاه $\forall u_1 \forall v_1 \forall w_1 \neg\psi(y,x,u_1,v_1,w_1)$؛

(v) اگر $\exists u \exists v \exists w\, \psi(x,y,u,v,w)$ و $\exists u_1 \exists v_1 \exists w_1\, \psi(y,x,u_1,v_1,w_1)$ برقرار باشند، آنگاه

$$\exists u_2 \exists v_2 \exists w_2\, \psi(x,z,w_2,v_2,w_2)$$

(vi) اگر $\theta_0(x)$ و $\theta_0(y)$ برقرار باشند، آنگاه یا $x=y$ یا $\exists x \exists y \exists u \exists w\, \psi(x,y,u,v,w)$ برقرار است؛

(vii) اگر $\phi(x,u,v,w) \wedge \phi(x,u',v',w')$ برقرار باشد، آنگاه $u=u'$، $v=v'$ و $w=w'$؛

(viii) اگر $\psi(x,y,u,v,w) \wedge \psi(x,y,u',v',w')$ برقرار باشد، آنگاه $u=u'$، $v=v'$ و $w=w'$.

اگر $(A,<)$ یک ترتیب خطی باشد، آنگاه $G_A \models T$. بنابراین، هر ترتیب خطی می‌تواند در یک مدل از T تفسیر شود.

فرض کنید که $G \models T$. مجموعه $X_G = \{x \in G : G \models \theta_0(x)\}$ را در نظر بگیرید. از آن‌جا که $G \models T$ و اصول موضوعه (i)-(vi) تضمین می‌کنند که می‌توانیم X_G را خطی مرتب کنیم، بنابراین ترتیب‌های خطی را در هر مدل از T تفسیر می‌کنیم. □

لم بعدی بیان می‌کند که در واقع $(A,<) \mapsto G_A$ یک تناظر یک‌به‌یک بین ترتیب‌های خطی و مدل‌های T است. اثبات این مورد را به عهده خواننده باقی می‌گذاریم.

لم ۳۸-۱. اگر $(A,<)$ یک ترتیب خطی باشد، آنگاه

$$(X_{G_A}, <_{G_A}) \cong (A,<).$$

علاوه بر این، برای هر $G \models T$، داریم:

$$G_{X_G} \cong G.$$

۱.۶.۱ خارج قسمت‌ها

اغلب مطلوب است ساختارهای عمومی‌تری را در نظر بگیریم. برای مثال، فرض کنید که یک گروه تعریف‌پذیر G و یک زیرگروه نرمال تعریف‌پذیر H داشته باشیم. ممکن است بخواهیم گروه G/H را بررسی کنیم. امکان دارد که G/H در ساختار ما متناظر با یک گروه قابل تعریف نباشد. اما متناظر با کلاس‌های هم‌ارزی یک رابطه هم‌ارزی تعریف‌پذیر است.

تعریف ۳۹-۱. می‌گوییم که یک ساختار $\mathcal{L}_\circ$، تحت عنوان $\mathcal{N}$، در یک ساختار $\mathcal{L}$ به نام M قابل تفسیر یا تفسیرپذیر است اگر مجموعه‌ای تعریف‌پذیر $X \subseteq M^n$ و یک رابطه هم‌ارزی تعریف‌پذیر E روی X وجود داشته باشد و برای هر نماد از $\mathcal{L}_\circ$ بتوانیم مجموعه‌های ناوردا تحت E که در $\mathcal{L}$ تعریف‌پذیر هستند را در X بیابیم، به طوری که خارج‌قسمت X/E با ساختار القایی خود با $\mathcal{N}$ یکریخت باشد.

فرض کنید K یک میدان باشد. مجموعه X را به‌صورت زیر تعریف می‌کنیم:

$$X = \left\{ (a_\circ, \dots, a_n) \in K^{n+1} : \bigvee_{i=\circ}^{n} a_i \neq \circ \right\}.$$

رابطه هم‌ارزی $\sim$ را روی X به‌صورت $\bar{a} \sim \bar{b}$ تعریف می‌کنیم اگر و تنها اگر عدد ناصفر $\lambda \in K$ وجود داشته باشد که $\lambda\bar{a} = \bar{b}$. به‌وضوح، X و $\sim$ تعریف‌پذیر هستند و خارج‌قسمت $X/\sim$ برابر $\mathbb{P}^n(K)$، یعنی فضای تصویری n-بعدی روی K است.

فرض کنید $f(X_\circ, \dots, X_n)$ یک چندجمله‌ای همگن روی K باشد (یعنی عددی d وجود داشته باشد که برای هر λ و $\bar{x}$ داشته باشیم $f(\lambda\bar{x}) = \lambda^d f(\bar{x})$). مجموعه V را به‌صورت زیر تعریف می‌کنیم:

$$V = \{\bar{x} \in X : f(\bar{x}) = \circ\}.$$

چون f همگن است، مجموعه V نسبت به $\sim$ ناوردا‌ست. بنابراین، می‌توانیم $(\mathbb{P}^n(K), V/\sim)$ را در $(K, +, \cdot, \circ, ۱)$ تفسیر کنیم.

حال نشان می‌دهیم که چگونه می‌توانیم گروه جمعی مرتب اعداد صحیح را در میدان $\mathbb{Q}_p$ تفسیر کنیم. دیدیم که Z_p یک زیرمجموعه تعریف‌پذیر از $\mathbb{Q}_p$ است. مجموعه U را به‌صورت زیر تعریف می‌کنیم:

$$U = \{x \in \mathbb{Z}_p : \exists y \in \mathbb{Z}_p \text{ که } xy = ۱\}$$

که مجموعه عناصر یکه در $\mathbb{Z}_p$ است. در این حالت، $(\mathbb{Z}, +)$ با گروه ضربی $\mathbb{Q}_p^\times/U$ هم‌ریخت است. می‌توانیم ترتیب را روی $\mathbb{Q}_p^\times/U$ به‌صورت $x/U \geq y/U \iff \frac{x}{y} \in \mathbb{Z}_p$ تعریف کنیم.

۷.۱ قضیه فشردگی

فرض کنید T یک تئوری و ϕ یک جمله در زبان $\mathcal{L}$ باشد. برای اینکه $T \models \phi$ باید نشان بدهیم ϕ در همه مدل‌های T برقرار است، که این کار به نظر طاقت فرسا به نظر می‌رسد. بنابراین با یک روند بی‌قاعده ریاضی نشان می‌دهیم که ϕ در همه مدل‌های T "درست" است. یک اثبات برای ϕ از T یک دنباله متناهی از $\mathcal{L}$–فرمول‌های $\psi_1, ..., \psi_n$ است که $\psi_n = \phi$ و $\psi_i \in T$ یا ψ_i از $\psi_1, ..., \psi_{n-1}$ توسط یک روند منطقی ساده نتیجه می‌شود. اگر برای ϕ یک اثبات از T وجود داشته باشد، می‌نویسیم $T \vdash \phi$. برای مثال: ϕ و ψ نتیجه می‌دهند $\phi \wedge \psi$، یا $\phi \wedge \psi$ نتیجه می‌دهد ϕ.
در ابتدا، نیاز به اشاره به چند نکته داریم :
(۱) اثبات ها متناهی‌اند.
(۲) اگر $T \vdash \phi$، آنگاه $T \models \phi$.
(۳) اگر T یک مجموعه متناهی از جمله‌ها باشد، آنگاه الگوریتمی وجود دارد که، زمانی که به آن یک دنباله از فرمول‌های σ و یک دنباله از جمله‌های ϕ به عنوان ورودی داده شود، نشان می‌دهد که σ یک اثبات برای ϕ از T هست یا خیر.

تعریف ۴۰-۱. فرض کنید $\mathcal{L}$ یک زبان و T یک تئوری باشد. اگر الگوریتمی وجود داشته باشد که نشان دهد دنباله‌ای از نمادها، یک $\mathcal{L}$–فرمول است، آنگاه زبان $\mathcal{L}$ را یک زبان بازگشتی می‌نامیم. حال تئوری T را بازگشتی می‌نامیم اگر الگوریتمی وجود داشته باشد که هر زمان یک دنباله‌ی $\mathcal{L}$–فرمول ϕ به عنوان ورودی به آن داده شود، نشان دهد که $\phi \in T$ یا $\phi \notin T$.

گزاره ۴۱-۱. اگر L یک زبان بازگشتی و T یک تئوری بازگشتی L باشد، آنگاه مجموعه $\{\phi : T \vdash \phi\}$ به‌طور بازگشتی قابل شمارش است؛ یعنی یک الگوریتم وجود دارد که هنگامی که ϕ به‌عنوان ورودی داده می‌شود، در صورتی که $T \vdash \phi$، چاپ می‌کند و در صورتی که $T \nvdash \phi$، متوقف می‌شود.

اثبات. یک لیست محاسبه‌پذیر از تمام دنباله‌های متناهی $\mathcal{L}$–فرمول‌ها به‌صورت $\sigma_0, \sigma_1, \sigma_2, \ldots$ وجود دارد. در مرحله iام از الگوریتم، بررسی می‌کنیم که آیا σ_i اثباتی برای ψ از T است. پس بررسی می‌کنیم که هر فرمول یا در T است (که می‌توانیم بررسی کنیم زیرا T بازگشتی است) یا از طریق یک قاعده منطقی از فرمول‌های قبلی در دنباله σ_i بدست می‌آید و فرمول آخر، ϕ است. اگر σ_i اثباتی از ϕ از T باشد، سپس پذیرش می‌کنیم؛ در غیر این صورت، به مرحله $i+1$ می‌رویم. □

قضیه ۴۲-۱ (تمامیت گودل). فرض کنید T یک $\mathcal{L}$–تئوری و ϕ یک $\mathcal{L}$–جمله باشد، در این صورت

$$T \models \phi \text{ اگر و تنها اگر } T \vdash \phi.$$

درواقع، قضیه تمامیت یک محک برای مشخص کردن تعریف‌پذیری یک تئوری است. تئوری T را ناسازگار می‌نامیم هرگاه برای جمله ϕ داشته باشیم $T \vdash (\phi \wedge \neg\phi)$؛ در غیر این صورت آن را سازگار می‌نامیم.

نتیجه ۴۳-۱. تئوری T سازگار است اگر و تنها اگر T تعریف‌پذیر باشد.

اثبات. فرض کنید T سازگار نباشد. چون هیچ مدلی از T وجود ندارد، همه مدل‌های T یک مدل از $(\phi \wedge \neg\phi)$ هستند. بنابراین، $T \models (\phi \wedge \neg\phi)$ و طبق قضیه تمامیت گودل، $T \vdash (\phi \wedge \neg\phi)$. □

قضیه ۴۴-۱ (فشردگی). تئوری T تعریف‌پذیر است اگر و تنها اگر هر زیر مجموعه‌ای از T تعریف‌پذیر باشد.

اثبات. به سادگی مشاهده می‌شود که اگر T تعریف‌پذیر باشد، آنگاه هر زیر مجموعه T تعریف‌پذیر است. از طرفی دیگر اگر T تعریف‌پذیر نباشد، آنگاه T ناسازگار است. فرض کنید σ اثبات یک تناقض در تئوری T باشد. چون σ متناهی است، تعداد فرضیات استفاده شده در اثبات از T باید متناهی باشد. بنابراین یک $T_0 \subseteq T$ متناهی وجود دارد که σ یک اثبات از یک تناقض در T_0 است. اما T_0 یک زیر مجموعه متناهی تعریف‌ناپذیر در T می‌باشد. □

اگرچه این یک پیامد ساده از نظریه کمال و طبیعت محدود اثبات است، اما نظریه فشردگی اساس نظریه مدل است. زیرا برای ما مفید نخواهد بود که ماهیت دقیق سیستم اثبات خود را درک کنیم، بنابراین ما نظریه کمال را اثبات نخواهیم کرد. در عوض، اثبات دومی از نظریه فشردگی ارائه خواهیم داد که مستقیماً به نظریه کمال استناد نمی‌کند. این اثبات همچنین می‌تواند برای اثبات نظریه کمال استفاده شود.

۱.۷.۱ ساختارهای هنکینی

می‌گوییم تئوری T به‌طور متناهی قابل‌رضایت است اگر هر زیرمجموعه متناهی از T قابل‌رضایت باشد. نشان می‌دهیم که هر تئوری به طور متناهی قابل‌رضایت T، قابل‌رضایت است. برای این کار، باید مدلی از T بسازیم. ایده اصلی در ساخت این مدل این است که به زبان، تعداد کافی ثابت اضافه خواهیم کرد به طوری که هر عنصر از مدل با یک نماد ثابت نامگذاری شود. تعریف زیر شرایط کافی برای ساخت مدل از ثابت‌ها را به ما خواهد داد.

تعریف ۴۵-۱. می‌گوییم که یک $\mathcal{L}$-تئوری T دارای خاصیت شاهد است، اگر $\phi(v)$ یک $\mathcal{L}$-فرمول با یک متغیر آزاد v باشد، آنگاه یک نماد ثابت $c \in L$ وجود دارد به طوری که $T \models (\exists v\, \phi(v)) \to \phi(c)$.

تعریف ۴۶-۱. یک $\mathcal{L}$-تئوری T را ماکسیمال می‌نامیم هرگاه برای هر ϕ، $\phi \in T$ یا $\neg\phi \in T$.

در ادامه، از لم زیر استفاده خواهیم کرد.

لم ۴۷-۱. فرض کنید T یک $\mathcal{L}$-تئوری ماکسیمال و به طور متناهی قابل‌رضایت باشد. اگر $\Delta \subseteq T$ متناهی باشد و $\Delta \models \psi$، آنگاه $\psi \in T$.

اثبات. اگر $\psi \notin T$، آنگاه چون T ماکسیمال است، $\neg\psi \in T$. اما در این صورت، $\Delta \cup \{\neg\psi\}$ یک زیرمجموعه متناهی غیرقابل‌رضایت از T خواهد بود که یک تناقض است. □

لم ۴۸-۱. فرض کنید که T یک $\mathcal{L}$-تئوری ماکسیمال و به طور متناهی قابل‌رضایت با خاصیت شاهد باشد. در این صورت، T یک مدل دارد. در حقیقت، اگر κ یک عدد کاردینال باشد و $\mathcal{L}$ حداکثر به تعداد κ نماد ثابت داشته باشد، آنگاه $\mathcal{M} \models T$ وجود دارد که $|\mathcal{M}| \leq \kappa$.

اثبات. فرض کنید $\mathcal{C}$ مجموعه نمادهای ثابت از $\mathcal{L}$ باشد. برای $c, d \in C$، می‌گوییم $c \sim d$ اگر $T \models c = d$.

ادعا ۱: $\sim$ یک رابطه هم‌ارزی است.

به وضوح، $c = c$ در T است. فرض کنید که $c = d$ و $d = e$ در T باشد. طبق لم ۴۸-۱، $d = c$ و $c = e$ در T خواهند بود.

جهان این مدل $\mathcal{M} = \mathcal{C}/\sim$ با کلاس‌های هم‌ارزی $\mathcal{C}$ به پیمانه $\sim$ است. به‌وضوح، $|M| \leq \kappa$. فرض می‌کنیم c^* کلاس هم‌ارزی c باشد و c را به عنوان کلاس هم‌ارزی c تفسیر کنیم؛ یعنی $c^{\mathcal{M}} = c^*$. در ادامه، نشان خواهیم داد که چگونه نمادهای رابطه و تابع $\mathcal{L}$ را تفسیر کنیم.

فرض کنید R یک نماد رابطه‌ای n موضعی از $\mathcal{L}$ باشد.

ادعا ۲: فرض کنید که $c_1, \ldots, c_n, d_1, \ldots, d_n \in \mathcal{C}$ و $c_i \sim d_i$ برای $i = 1, \ldots, n$، در این صورت $R(\bar{c}) \in T$ اگر و تنها اگر $R(\bar{d}) \in T$.

از آن‌جایی که $c_i = d_i \in T$ برای $i = 1, \ldots, n$، طبق لم ۴۸-۱، اگر یکی از $R(\bar{c})$ و $R(\bar{d})$ در T باشند، آنگاه هر دو در T خواهند بود.

R را به‌صورت زیر تفسیر می‌کنیم:

$$R^{\mathcal{M}} = \{(c_1^*, \ldots, c_n^*) : R(c_1, \ldots, c_n) \in T\}.$$

طبق ادعا ۲، $R^{\mathcal{M}}$ خوش‌تعریف است.

فرض کنید f یک نماد تابعی n موضعی از L باشد و $c_1, \ldots, c_n \in \mathcal{C}$. چون $\emptyset \models \exists v f(c_1, \ldots, c_n) = v$ و T خاصیت شاهد را دارد، طبق لم ۴۸-۱، یک $c_{n+1} \in C$ وجود دارد به طوری که $f(c_1, \ldots, c_n) = c_{n+1} \in T$. مانند بالا، اگر $d_i \sim c_i$ برای $i = 1, \ldots, n+1$، آنگاه $f(d_1, \ldots, d_n) = d_{n+1} \in T$. علاوه بر این، چون f یک نماد تابعی است، اگر $e_i \sim c_i$ برای $i = 1, \ldots, n$ و $f(e_1, \ldots, e_n) = e_{n+1} \in T$، آنگاه $e_{n+1} \sim c_{n+1}$. بنابراین، یک تابع به‌طور دقیق تعریف شده داریم

$$f^{\mathcal{M}} : M^{\mathcal{M}} \to M^{\mathcal{M}}$$

به طوری که

$$f^{\mathcal{M}}(c_1^*, \ldots, c_n^*) = d^* \text{ اگر و تنها اگر } f(c_1, \ldots, c_n) = d \in T.$$

این، توضیحات ساختار $\mathcal{M}$ را کامل می‌کند. پیش از نشان دادن اینکه $\mathcal{M} \models T$، باید نشان دهیم که عبارات به‌درستی رفتار می‌کنند.

ادعا ۳ فرض کنید که t یک ترم با متغیرهای آزاد از $v_1, \ldots, v_n$ است. اگر $c_1, \ldots, c_n, d \in C$، آنگاه $t(c_1, \ldots, c_n) = d \in T$ اگر و تنها اگر $t^{\mathcal{M}}(c_1^*, \ldots, c_n^*) = d^*$.

($\Rightarrow$) ابتدا نشان می‌دهیم، با استقرا روی ترم‌ها، که اگر $t(c_1,\dots,c_n)=d\in T$، آنگاه $t^{\mathcal{M}}(c_1^*,\dots,c_n^*)=d^*$.
اگر t یک نماد ثابت c، آنگاه $c=d\in T$ و $c^{\mathcal{M}}=d^*$.
اگر t متغیر v_i باشد، آنگاه $c_i=d\in T$ و $t(c_1,\dots,c_n)=c_i=d^*$.
فرض کنید که ادعا برای $t_1,\dots,t_m$ درست باشد و t برابر با $f(t_1,\dots,t_m)$ باشد. با استفاده از خاصیت شاهد و لم ۴۸-۱، می‌توانیم $d,d_1,\dots,d_n\in C$ پیدا کنیم به طوری که $t_i(c_1,\dots,c_n)=d_i\in T$ برای $i\le m$ و $f(d_1,\dots,d_m)=d\in T$. طبق فرض استقرا، $t^{\mathcal{M}}(c_1^*,\dots,c_n^*)=d_i^*$ و $f^{\mathcal{M}}(d_1^*,\dots,d_m^*)=d^*$. بنابراین، $t^{\mathcal{M}}(c_1^*,\dots,c_n^*)=d^*$.

($\Leftarrow$) حالا فرض کنید که $t^{\mathcal{M}}(c_1^*,\dots,c_n^*)=d^*$. با استفاده از خاصیت شاهد و لم ۴۸-۱، یک $e\in C$ وجود دارد به‌طوری که $t(c_1,\dots,c_n)=e\in T$. با استفاده از جهت ($\Rightarrow$) اثبات، $t^{\mathcal{M}}(c_1^*,\dots,c_n^*)=e^*$. بنابراین، $e^*=d^*$ و $e=d\in T$. طبق لم ۴۸-۱، $t(c_1,\dots,c_n)=d\in T$.

ادعا ۴ برای تمام فرمول‌های L به‌صورت $\phi(v_1,\dots,v_n)$ و $c_1,\dots,c_n\in C$، $\mathcal{M}\models\phi(c_1^*,\dots,c_n^*)$ اگر و تنها اگر $\phi(c_1,\dots,c_n)\in T$.

این ادعا را با استفاده از استقرا بر روی فرمول‌ها اثبات می‌کنیم.

فرض کنید که ϕ برابر با $t_1=t_2$ باشد. با استفاده از لم ۴۸-۱ و خاصیت شاهد، می‌توانیم d_1 و d_2 را پیدا کنیم به‌طوری که $t_1(c)=d_1$ و $t_2(c)=d_2$ در T باشند. طبق ادعا ۳، $\mathcal{M}(c)=d^*$ برای $i=1,2$. سپس فرض کنید که ϕ برابر با $R(t_1,\dots,t_m)$ باشد. چون T خاصیت شاهد دارد، طبق لم ۴۸-۱، مقادیر $d_1,\dots,d_m\in C$ وجود دارد به طوری که $t_i(c)=d_i\in T$ و طبق ادعا ۴، $t_1(c)=t_2(c)\in T$ طبق لم ۴۸-۱.
بنابراین،

$$\mathcal{M}\models\phi(c^*)\iff\vec{d^*}\in R^{\mathcal{M}}\iff R(\vec{d})\in T\iff\phi(c)\in T$$. طبق لم ۴۸-۱

فرض کنید که ادعا برای ϕ درست باشد. اگر $\mathcal{M}\models\neg\phi(c^*)$، آنگاه $\mathcal{M}\models\phi(c^*)$. طبق فرض استقرا، $\phi(c)\notin T$. بنابراین، طبق حداکثر بودن، $\neg\phi(c)\in T$. از طرف دیگر، اگر $\neg\phi(c)\in T$، آنگاه چون T به طور محدود قابل‌رضایت است، $\phi(c)\notin T$. بنابراین، طبق استقرا، $\mathcal{M}\models\neg\phi(c^*)$ و $\mathcal{M}\models\neg\phi(c)$.
فرض کنید که ادعا برای ϕ و ψ درست باشد. در این صورت

$$\mathcal{M}\models(\phi\wedge\psi)(c^*)\iff\varphi(c)\in T\text{ و }\psi(c)\in T\iff(\phi\wedge\psi)(c)\in T$$. طبق لم ۴۸-۱

فرض کنید که ϕ برابر با $\exists v\,\psi(v,c)$ و ادعا برای ψ درست باشد. اگر $\mathcal{M}\models\exists v\,\psi(d^*,c^*)$، آنگاه طبق فرض استقرا، $\psi(d,c)\in T$ و $\exists v\,\psi(v,c)\in T$، طبق لم ۴۸-۱. از طرف دیگر، اگر $\exists v\,\psi(v,c)\in T$، آنگاه طبق خاصیت شاهد و لم ۴۸-۱، $\psi(d,c)\in T$ برای برخی c. طبق استقرا، $\mathcal{M}\models\psi(d^*,c^*)$ و $\mathcal{M}\models\exists v\,\psi(d^*,c^*)$.
این استقرا را کامل می‌کند. در نتیجه داریم $\mathcal{M}\models T$. □

این ترم‌ها نشان می‌دهند که هر تئوری به طور متناهی قابل‌رضایت می‌تواند به یک تئوری ماکسیمال به طور محدود قابل‌رضایت با خاصیت شاهد گسترش یابد.

لم ۴۹-۱. فرض کنید T یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت باشد. در این صورت، زبان $\mathcal{L}^* \supset \mathcal{L}$ و یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت $T^* \supset T$ وجود دارد به طوری که T^* $\mathcal{L}^*$–تئوری دارای خاصیت شاهد است.

اثبات. ابتدا نشان می‌دهیم که یک زبان $\mathcal{L}_1 \supset \mathcal{L}$ و یک تئوری $T_1 \supset T$ $\mathcal{L}_1$–که به طور متناهی قابل‌رضایت است، وجود دارد به طوری که برای هر فرمول $\mathcal{L}$–که $\phi(v)$، یک نماد ثابت $\mathcal{L}_1$ وجود دارد به طوری که $T_1 \models (\exists v\, \phi(v)) \to \phi(c)$. برای هر فرمول $\mathcal{L}$–که $\phi(v)$، بگذارید c_ϕ یک نماد ثابت جدید باشد و بگذارید $\mathcal{L}_1 = \mathcal{L} \cup \{c_\phi : \phi(v)$ {$\mathcal{L}$ یک فرمول $\}$. برای هر فرمول $\mathcal{L}$–که $\phi(v)$، قرار دهید Θ_ϕ جمله $\mathcal{L}_1$–که $(\exists v\, \phi(v)) \to \phi(c_\phi)$ باشد. قرار دهید $T_1 = T \cup \{\Theta_\phi :$ {$\mathcal{L}$ یک فرمول $\phi(v)\}$.

ادعا: T_1 به طور متناهی قابل‌رضایت است.

فرض کنید که Δ یک زیرمجموعه متناهی از T_1 باشد. سپس، $\Delta = \Delta_0 \cup \{\Theta_{\phi_1}, \ldots, \Theta_{\phi_n}\}$، که در آن Δ_0 یک زیرمجموعه متناهی از T است. چون T به طور متناهی قابل‌رضایت است، $\mathcal{M} \models \Delta_0$. حال، $\mathcal{M}$ را به یک $\mathcal{L} \cup \{c_{\phi_1}, \ldots, c_{\phi_n}\}$–ساختار $\mathcal{M}'$ تبدیل می‌کنیم. از آنجایی که تفسیر نمادها را در $\mathcal{L}$ تغییر نخواهیم داد، داریم $\mathcal{M}' \models \Delta_0$. برای این کار، باید نشان دهیم که چگونه می‌توان نمادهای c_{ϕ_i} را در $\mathcal{M}'$ تفسیر کرد. اگر $\mathcal{M} \models \exists v\ \phi(v)$، عناصر a_i از M را طوری انتخاب می‌کنیم که $\mathcal{M} \models \phi(a_i)$ و فرض کنید $c_{\phi_i}^{\mathcal{M}'}$. در غیر این صورت، فرض کنید $c_{\phi_i}^{\mathcal{M}'}$ هر عنصر دلخواهی از M باشد. به وضوح، برای $i \leq n$، $\mathcal{M}' \models \Theta_{\phi_i}$. بنابراین، T_1 به طور متناهی قابل رضایت است.

روند بالا را تکرار می‌کنیم تا یک دنباله از زبان‌های $\mathcal{L} \subseteq \mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \ldots$ و یک دنباله از $\mathcal{L}_i$–تئوری‌های به طور متناهی قابل رضایت $T \subseteq T_1 \subseteq T_2 \subseteq \ldots$ بسازیم به طوری که اگر $\phi(v)$ یک $\mathcal{L}_i$–فرمول باشد، آنگاه یک نماد ثابت $c \in \mathcal{L}_{i+1}$ وجود دارد به طوری که $T_{i+1} \models (\exists v \phi(v)) \to \phi(c)$. فرض کنید $\mathcal{L}^* = \bigcup \mathcal{L}_i$ و $T^* = \bigcup T_i$. بنابر ساختار، T^* دارای خاصیت شاهد است. اگر Δ یک زیرمجموعه متناهی از T^* باشد، آنگاه $\Delta \subseteq T_i$. درنتیجه، Δ قابل رضایت و T^* به طور متناهی قابل رضایت است. اگر $|\mathcal{L}_i|$ بیانگر تعداد نمادهای تابعی، رابطه‌ای و ثابت در $\mathcal{L}_i$ باشد، آنگاه حداکثر $|\mathcal{L}_i| + \aleph_0$ فرمول در $\mathcal{L}_i$ وجود دارد. بنابراین، با استقرا، $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$.

□

لم ۵۰-۱. فرض کنید T یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت و ϕ یک $\mathcal{L}$–جمله باشد. در این صورت $T \cup \{\phi\}$ یا $T \cup \{\neg\phi\}$ به طور متناهی قابل رضایت است.

اثبات. فرض کنید $T \cup \{\phi\}$ به طور متناهی قابل رضایت نباشد. در این صورت یک زیرمجموعه متناهی $\Delta \subseteq T$ وجود دارد به طوری که $\Delta \models \neg\phi$. نشان می‌دهیم که $T \cup \{\neg\phi\}$ به طور متناهی قابل رضایت است. فرض کنید Σ یک زیرمجموعه متناهی از T باشد. از آنجایی که $\Delta \cup \Sigma$ قابل رضایت است و $\Delta \cup \Sigma \models \neg\phi$، پس $\Sigma \cup \{\neg\phi\}$ قابل رضایت است. بنابراین، $T \cup \{\neg\phi\}$ به طور متناهی قابل رضایت است. □

نتیجه ۵۱-۱. اگر T یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت باشد، آنگاه یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت ماکسیمال $T' \supseteq T$ وجود دارد.

اثبات. فرض کنید I مجموعه تمام $\mathcal{L}$–تئوری‌های به طور متناهی قابل رضایت شامل T باشد. روی I، با استقرا، به طور جزئی ترتیب می‌گذاریم. اگر $C \subseteq I$ یک زنجیر باشد، فرض کنید $T_C = \bigcup\{\Sigma : \Sigma \in C\}$. اگر Δ یک زیرمجموعه متناهی از T_C باشد، آنگاه $\Sigma \in C$ وجود دارد به طوری که $\Delta \subseteq \Sigma$. پس T_C به طور متناهی قابل رضایت است و $T_C \supseteq \Sigma$ برای هر $\Sigma \in C$. در نتیجه، هر زنجیر در I یک کران بالا دارد و با استفاده از لم زرن، می‌توانیم یک $T' \in I$ پیدا کنیم که نسبت به ترتیب جزئی ماکسیمال است. بنابر لم ۱-۵۰، $T' \cup \{\phi\}$ یا $T' \cup \{\neg\phi\}$ به طور متناهی قابل رضایت است. با توجه به ماکسیمال بودن T'، یکی از ϕ یا $\neg\phi$ در T' قرار دارد. بنابراین، T' یک تئوری ماکسیمال است. □

قضیه ۱-۵۲. اگر T یک $\mathcal{L}$–تئوری به طور متناهی قابل رضایت و κ یک کاردینال نامتناهی باشد که $\kappa \geq |\mathcal{L}|$، آنگاه مدلی از T با حداکثر کاردینال κ وجود دارد.

اثبات. طبق لم ۱-۴۹، می‌توانیم $\mathcal{L} \subseteq \mathcal{L}^*$ و یک $\mathcal{L}^*$–تئوری به طور متناهی قابل رضایت $T^* \supseteq T$ پیدا کنیم به طوری که هر $\mathcal{L}^*$–تئوری با گسترش T^* دارای خاصیت شاهد و کاردینال $\mathcal{L}^*$ حداکثر κ است. طبق نتیجه ۱-۵۱، می‌توانیم یک $\mathcal{L}^*$–تئوری به طور متناهی قابل رضایت ماکسیمال $T' \supseteq T$ پیدا کنیم. از آنجایی که T' خاصیت شاهد دارد، لم ۱-۴۸ تضمین می‌کند که $\mathcal{M} \models T$ وجود دارد که $|M| \leq \kappa$. □

این اثبات قضیه فشردگی بر اساس اثبات هنکین برای قضیه کامل بودن است. روش ساخت مدلی که جهان آن از نمادهای ثابت ساخته شده است، به عنوان «ساختار هنکین» شناخته می‌شود و نظریه‌هایی که دارای ویژگی شاهد هستند، گاهی «هنکین‌شده» نامیده می‌شوند.

این بخش را با چند کاربرد استاندارد قضیه فشردگی به پایان می‌رسانیم.

گزاره ۱-۵۳. فرض کنید $\mathcal{L}$ زبانی شامل $\{\cdot, e\}$، یعنی زبان گروه‌ها، باشد، T یک $\mathcal{L}$–تئوری گسترش‌دهنده نظریه گروه‌ها باشد، و $\phi(v)$ یک $\mathcal{L}$–فرمول باشد. اگر برای هر n، $G_n \models T$ و $g_n \in G_n$ وجود داشته باشند که مرتبه‌ای متناهی بزرگتر از n دارد و $G_n \models \phi(g_n)$، آنگاه $G \models T$ و $g \in G$ وجود دارد که $G \models \phi(g)$ و g دارای مرتبه نامتناهی است. به ویژه، هیچ فرمولی وجود ندارد که نقاط تاب را در تمام مدل‌های T تعریف کند.

اثبات. فرض کنید $\mathcal{L}^* = \mathcal{L} \cup \{c\}$، که در آن c یک نماد ثابت جدید است. T^* را به عنوان $\mathcal{L}$–تئوری زیر در نظر بگیرید:

$$T \cup \{\phi(c)\} \cup \{\underbrace{c \cdot c \cdots c}_{n\text{بار}} \neq e : n = 1, 2, \ldots\}.$$

اگر G مدلی از T^* باشد و g تفسیر c در G باشد، آنگاه $G \models \phi(g)$ و g دارای مرتبه نامتناهی است. بنابراین، کافی است نشان دهیم که T^* قابل رضایت است.

فرض کنید $\Delta \subseteq T^*$ متناهی باشد. در این صورت:

$$\Delta \subseteq T \cup \{\phi(c)\} \cup \{\underbrace{c \cdot c \cdots c}_{n\text{بار}} \neq e : n = 1, 2, \ldots, m\}$$

برای مقداری m. G_m را به عنوان یک ساختار $\mathcal{L}^*$ در نظر بگیرید که در آن c به عنوان g_m تفسیر شده است. چون $G_m \models T \cup \{\phi(g_m)\}$ و g_m دارای مرتبه‌ای بزرگتر از m است، $G_m \models \Delta$. بنابراین، T^* به طور متناهی قابل رضایت است و در نتیجه، طبق قضیه فشردگی، قابل رضایت است. □

گزاره ۵۴-۱. فرض کنید $\mathcal{L} = \{\cdot, +, <, \circ, ۱\}$ و $\mathrm{Th}(\mathbb{N})$ تئوری کامل $\mathcal{L}$-اعداد طبیعی باشد. در این صورت، $\mathcal{M} \models \mathrm{Th}(\mathbb{N})$ و $a \in M$ وجود دارد که a از هر عدد طبیعی بزرگتر است.

اثبات. فرض کنید $\mathcal{L}^* = \mathcal{L} \cup \{c\}$، که در آن c یک نماد ثابت جدید است، و

$$T = \mathrm{Th}(\mathbb{N}) \cup \{\underbrace{۱ + ۱ + \ldots + ۱}_{n\text{بار}} < c : n = ۱, ۲, \ldots\text{برای }\}.$$

اگر Δ یک زیرمجموعه متناهی از T باشد، می‌توانیم $\mathbb{N}$ را به مدلی از Δ تبدیل کنیم به طوری که c را به عنوان یک عدد طبیعی به اندازه کافی بزرگ تفسیر کنیم. بنابراین، T به طور متناهی قابل رضایت است و $\mathcal{M} \models T$ وجود دارد. اگر $a \in M$ تفسیر c باشد، آنگاه a از هر عدد طبیعی بزرگتر است. □

لم بعدی نتیجه آسانی از قضیه کامل‌بودن است، اما می‌توان آن را از قضیه فشردگی نیز نتیجه گرفت.

لم ۵۵-۱. اگر $T \models \phi$، آنگاه $\Delta \models T$ برای زیرمجموعه متناهی $\Delta \subseteq T$.

اثبات. فرض کنید چنین نباشد. اگر $\Delta \subseteq T$ متناهی باشد و از آن‌جایی که $\Delta \not\models \phi$، نتیجه می‌گیریم که $\Delta \cup \{\neg\phi\}$ قابل رضایت است. بنابراین $T \cup \{\neg\phi\}$ به طور متناهی قابل رضایت است و طبق قضیه فشردگی، $T \not\models \phi$. □

۸.۱ تئوری‌های کامل

تعریف ۵۶-۱. یک $\mathcal{L}$-تئوری T را کامل می‌نامیم اگر برای هر $\mathcal{L}$-جمله ϕ، $T \models \phi$ یا $T \models \neg\phi$ برقرار باشد.

برای یک $\mathcal{L}$-ساختار $\mathcal{M}$، تئوری

$$\mathrm{Th}(\mathcal{M}) = \{\phi : \mathcal{M} \models \phi\}$$

که ϕ یک $\mathcal{L}$-جمله است. یک تئوری کامل است. تعیین دقیق اینکه چه جملاتی در $\mathrm{Th}(\mathcal{M})$ قرار دارند، دشوار است. در بسیاری از موارد، کلید شناخت $\mathrm{Th}(\mathcal{M})$ یافتن یک $\mathcal{L}$-تئوری ساده‌تر T است به طوری که $\mathcal{M} \models T$ و T کامل باشد. در این صورت، $\mathcal{M} \models \phi$ اگر و فقط اگر $T \models \phi$، زیرا اگر $T \not\models \phi$، آنگاه $T \models \neg\phi$ و $\mathcal{M} \models \neg\phi$.

قضیه فشردگی یک آزمون کامل بودن کارآمد ارائه می‌دهد که در این بخش از آن استفاده خواهیم کرد تا نشان دهیم چندین تئوری، کامل هستند. این نتایج پیامدهای چشمگیری برای میدان‌های بسته جبری خواهند داشت.

گزاره ۵۷-۱. فرض کنید T یک $\mathcal{L}$-تئوری با مدل‌های نامتناهی باشد. اگر κ یک عدد کاردینال نامتناهی باشد و $|\mathcal{L}| \leq \kappa$، آنگاه مدلی از T با کاردینال κ وجود دارد.

اثبات. فرض کنید $\mathcal{L}^* = \mathcal{L} \cup \{c_\alpha : \alpha < \kappa\}$، که در آن هر c_α یک نماد ثابت جدید است. را $\mathcal{L}^*$–تئوری T^* را به صورت زیر در نظر بگیرید:

$$T \cup \{c_\alpha \neq c_\beta : \alpha, \beta < \kappa, \alpha \neq \beta\}.$$

واضح است که اگر $\mathcal{M} \models T^*$، آنگاه $\mathcal{M}$ مدلی از T با کاردینال حداقل κ است. بنابراین، طبق قضیه ۵۲-۱، کافی است نشان دهیم که T^* به طور متناهی قابل رضایت است. اما اگر $\Delta \subset T^*$ متناهی باشد، آنگاه

$$\Delta \subseteq T \cup \{c_\alpha \neq c_\beta : \alpha \neq \beta, \alpha, \beta \in I\},$$

که در آن I یک زیرمجموعه متناهی از κ است. فرض کنید $\mathcal{M}$ یک مدل نامتناهی از T باشد. می‌توانیم نمادهای $\{c_\alpha : \alpha \in I\}$ را به عنوان $|I|$ عنصر متمایز از M تفسیر کنیم. چون $\mathcal{M} \models \Delta$، T^* به طور متناهی قابل رضایت است. □

تعریف ۵۸-۱. فرض کنید κ یک عدد کاردینال نامتناهی باشد و T یک تئوری با مدل‌هایی به اندازه κ. می‌گوییم T κ– جازم است هرگاه هر دو مدل از T با کاردینال κ یکریخت باشند.

فرض کنید $\mathcal{L} = \{+, \circ\}$ زبان گروه‌های جمعی و T، $\mathcal{L}$–تئوری گروه‌های آبلی بدون تاب و بخش‌پذیر. اصول T شامل اصول گروه‌های آبلی به همراه اصول زیر است:

$$\forall x \left(x \neq \circ \to \underbrace{x + \ldots + x}_{n-\text{بار}} \neq \circ \right).$$

و

$$\forall y \exists x \underbrace{x + \ldots + x}_{n-\text{بار}} = y$$

برای $n = ۱, ۲, \ldots$.

گزاره ۵۹-۱. تئوری گروه‌های آبلی بدون تاب و بخش‌پذیر برای همه $\kappa > \aleph_\circ$، κ– جازم است.

اثبات. ابتدا استدلال می‌کنیم که مدل‌های T همان فضاهای برداری روی میدان اعداد گویا هستند. واضح است که اگر V یک فضای برداری روی $\mathbb{Q}$ باشد، آنگاه گروه جمعی متناظر با V یک مدل از T است. از طرف دیگر، اگر $G \models T$، $g \in G$، و $n \in \mathbb{N}$ با $n > \circ$، می‌توانیم $h \in G$ را پیدا کنیم به طوری که $nh = g$. اگر $nk = g$، آنگاه $n(h - k) = \circ$. چون G بدون تاب است، تنها یک $h \in G$ وجود دارد به طوری که $nh = g$. این عنصر را g/n می‌نامیم. می‌توانیم G را به عنوان یک $\mathbb{Q}$–فضای برداری تحت عمل $\frac{m}{n} g = m(g/n)$ در نظر بگیریم.

دو $\mathbb{Q}$–فضای برداری یکریخت هستند اگر و فقط اگر ابعاد یکسانی داشته باشند. بنابراین، مدل‌های T تا یکریختی توسط بعدشان مشخص می‌شوند. اگر G بعد λ داشته باشد، آنگاه $|G| = \lambda + \aleph_\circ$. اگر κ ناشمارا باشد و G کاردینال κ داشته باشد، آنگاه G بعد κ دارد. بنابراین، برای $\kappa > \aleph_\circ$، هر دو مدل از T با کاردینال κ یکریخت هستند. □

توجه کنید که T $\aleph_0$–جازم نیست. در واقع، $\aleph_0$ مدل غیر یکریخت متناظر با فضاهای برداری با ابعاد $1, 2, 3, \ldots$ و $\aleph_0$ وجود دارد.

استدلال مشابهی برای تئوری میدان‌های بسته جبری نیز اعمال می‌شود. فرض کنید ACF_p تئوری میدان‌های بسته جبری با مشخصه p باشد، که در آن p یا 0 یا یک عدد اول است.

گزاره ۶۰–۱. ACF_p برای همه اعداد کاردینال ناشمارا κ، κ–جازم است.

اثبات. دو میدان بسته جبری یکریخت هستند اگر و فقط اگر مشخصه یکسان و درجه متعالی یکسانی داشته باشند. یک میدان بسته جبری با درجه متعالی λ کاردینال $\aleph_0 + \lambda$ دارد. اگر $\kappa > \aleph_0$، یک میدان بسته جبری با کاردینال κ نیز درجه متعالی κ دارد. بنابراین، هر دو میدان بسته جبری با مشخصه یکسان و کاردینال ناشمارای یکسان، یکریخت هستند. □

دو مثال ساده‌تر ارائه می‌دهیم.

– فرض کنید $\mathcal{L}$ زبان تهی باشد. آنگاه تئوری یک مجموعه نامتناهی برای همه اعداد کاردینال κ، κ–جازم است.

– فرض کنید $\mathcal{L} = \{E\}$، که در آن E یک رابطه دوتایی است، و T تئوری یک رابطه هم‌ارزی با دقیقاً دو کلاس باشد که هر دو نامتناهی هستند. به راحتی می‌توان دید که هر دو مدل شمارا از T یکریخت هستند. از طرف دیگر، T برای $\kappa > \aleph_0$، κ–جازم نیست. برای مشاهده این، فرض کنید $\mathcal{M}_0$ مدلی باشد که هر دو کلاس کاردینال κ دارند، و $\mathcal{M}_1$ مدلی باشد که یک کلاس کاردینال κ و کلاس دیگر کاردینال $\aleph_0$ دارد. واضح است که $\mathcal{M}_0$ و $\mathcal{M}_1$ یکریخت نیستند.

قضیه ۶۱–۱ (آزمون وات[۳]). فرض کنید T یک تئوری قابل رضایت بدون مدل‌های متناهی باشد که برای یک عدد کاردینال نامتناهی $\kappa \geq |\mathcal{L}|$، κ–جازم است. آنگاه T کامل است.

اثبات. فرض کنید T کامل نباشد. در این صورت، جمله‌ای مانند ϕ وجود دارد به طوری که $T \not\models \phi$ و $T \not\models \neg\phi$. از آن‌جا که $T \not\models \psi$ اگر و فقط اگر $T \cup \{\neg\psi\}$ قابل رضایت باشد، تئوری‌های $T_0 = T \cup \{\phi\}$ و $T_1 = T \cup \{\neg\phi\}$ قابل رضایت هستند. چون T مدل متناهی ندارد، هر دو T_0 و T_1 مدل‌های نامتناهی دارند. طبق گزاره ۵۷–۱ می‌توان مدل‌های $\mathcal{M}_0$ و $\mathcal{M}_1$ با کاردینال κ یافت به طوری که $\mathcal{M}_i \models T_i$. از آنجا که $\mathcal{M}_0$ و $\mathcal{M}_1$ درباره ϕ اختلاف نظر دارند، این مدل‌ها معادل اولیه نیستند و در نتیجه یکریخت نیستند. این با κ–جازم بودن T در تناقض است. □

شرط نداشتن مدل‌های متناهی برای T ضروری است. فرض کنید T، $\{+, 0\}$–تئوری گروه‌ها باشد که در آن هر عنصر مرتبه ۲ دارد. T برای هر $\kappa \geq \aleph_0$، κ–جازم است. اما T کامل نیست. جمله $\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge z \neq x)$ در گروه دو عنصری نادرست اما در سایر مدل‌های T درست است.

آزمون وات نشان می‌دهد که همه تئوری‌های جازم مورد بحث کامل هستند. به ویژه، میدان‌های بسته جبری کامل هستند. این نتیجه تارسکی چندین پیامد جالب دارد.

تعریف ۶۲–۱. یک $\mathcal{L}$–تئوری T را **تصمیم‌پذیر** می‌نامیم اگر الگوریتمی وجود داشته باشد که با دریافت یک $\mathcal{L}$–جمله ϕ به عنوان ورودی، تصمیم بگیرد آیا $T \models \phi$ یا خیر.

[۳] Vaught's Test

لم ۶۳-۱. فرض کنید T یک تئوری بازگشتی کامل و قابل رضایت در یک زبان بازگشتی $\mathcal{L}$ باشد. آنگاه T تصمیم‌پذیر است.

اثبات. از آنجا که T قابل رضایت است، مجموعه‌های $A = \{\phi : T \models \phi\}$ و $B = \{\phi : T \models \neg\phi\}$ جدا از هم هستند. چون T سازگار است، $A \cup B$ مجموعه همه $\mathcal{L}$–جملات است. طبق قضیه کامل‌بودن، $A = \{\phi : T \vdash \phi\}$ و $B = \{\phi : T \vdash \neg\phi\}$. پس، A و B شمارای بازگشتی هستند. اما هر مجموعه شمارای بازگشتی با متمم شمارای بازگشتی، بازگشتی است. □

به طور غیررسمی، برای تصمیم‌گیری درباره اینکه آیا ϕ یک نتیجه منطقی از یک تئوری بازگشتی کامل و قابل رضایت T است، جستجو در میان اثبات‌های ممکن از T را آغاز می‌کنیم تا زمانی که یا اثباتی برای ϕ یا اثباتی برای $\neg\phi$ بیابیم. از آن‌جا که T قابل رضایت است، هرگز اثباتی برای هر دو پیدا نخواهیم کرد و چون T کامل است، در نهایت اثبات یکی از آن‌ها را خواهیم یافت.

نتیجه ۶۴-۱. برای $p = 0$ یا p اول، ACF_p تصمیم‌پذیر است. به ویژه، $\mathrm{Th}(\mathbb{C})$، تئوری مرتبه اول میدان اعداد مختلط، تصمیم‌پذیر است.

نتیجه ۶۵-۱. فرض کنید ϕ یک جمله در زبان حلقه‌ها باشد. موارد زیر معادل هستند:
(i) ϕ در اعداد مختلط درست است،
(ii) ϕ در هر میدان بسته جبری با مشخصه صفر درست باشد،
(iii) ϕ در برخی میدان‌های بسته جبری با مشخصه صفر درست باشد،
(iv) اعداد اول به بزرگی دلخواه p وجود داشته باشند که ϕ در برخی میدان‌های بسته جبری با مشخصه p درست باشد،
(v) عددی مانند m وجود داشته باشد که برای همه $p > m$، ϕ در تمام میدان‌های بسته جبری با مشخصه p درست باشد.

اثبات. معادل بودن $(i) - (iii)$ از کامل بودن ACF_0 نتیجه می‌شود و $(v) \Rightarrow (iv)$ واضح است.

برای $(ii) \Rightarrow (v)$، فرض کنید $\mathrm{ACF}_0 \models \phi$. طبق لم ۵۵-۱، زیرمجموعه متناهی $\Delta \subset \mathrm{ACF}_0$ وجود دارد که $\Delta \models \phi$. بنابراین اگر p را به اندازه کافی بزرگ انتخاب کنیم، $\mathrm{ACF}_p \models \Delta$ خواهد بود. در نتیجه $\mathrm{ACF}_p \models \phi$ برای همه اعداد اول به اندازه کافی بزرگ p برقرار است.

برای $(iv) \Rightarrow (ii)$، فرض کنید $\mathrm{ACF}_0 \not\models \phi$. از آنجا که ACF_0 کامل است، $\mathrm{ACF}_0 \models \neg\phi$. با استدلال مشابه بالا، $\mathrm{ACF}_p \models \neg\phi$ برای pهای به اندازه کافی بزرگ. بنابراین (iv) نقض می‌شود. □

قضیه ۶۶-۱. هر نگاشت چندجمله‌ای یک‌به‌یک از $\mathbb{C}^n$ به $\mathbb{C}^n$، پوشاست.

اثبات. نکته کلیدی این اثبات مشاهده ساده‌ای است که اگر k یک میدان متناهی باشد، هر تابع یک‌به‌یک $f : k^n \to k^n$ پوشاست. از این مشاهده به راحتی می‌توان نشان داد که همین امر برای $\mathbb{F}_p^{\mathrm{alg}}$ (بستار جبری میدان p عنصری) نیز صادق است.

ادعا: هر نگاشت چندجمله‌ای یک‌به‌یک $f : (\mathbb{F}_p^{\mathrm{alg}})^n \to (\mathbb{F}_p^{\mathrm{alg}})^n$ پوشاست.

(برهان خلف) فرض کنید $\bar{a} \in \mathbb{F}_p^{\text{alg}}$ ضرایب f و $\bar{b} \in (\mathbb{F}_p^{\text{alg}})^n$ نقطه‌ای خارج از برد f باشد. اگر k زیرمیدان $\mathbb{F}_p^{\text{alg}}$ تولید شده توسط $\bar{a}, \bar{b}$ باشد، آنگاه $f|_{k^n}$ یک نگاشت چندجمله‌ای یک‌به‌یک و غیرپوشا از k^n به خودش خواهد بود. اما $\mathbb{F}_p^{\text{alg}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ یک میدان موضعاً متناهی است، بنابراین k متناهی خواهد بود که تناقض ایجاد می‌کند.

حال فرض کنید قضیه نادرست باشد. فرض کنید $X = (X_1, \ldots, X_n)$ و $f(X) = (f_1(X), \ldots, f_n(X))$ یک مثال نقض باشد که هر $f_i \in \mathbb{C}[X]$ حداکثر درجه d دارد. جمله $\Phi_{n,d}$ در زبان $\mathcal{L}$ وجود دارد به طوری که برای یک میدان K، $K \models \Phi_{n,d}$ اگر و فقط اگر هر نگاشت چندجمله‌ای یک‌به‌یک از K^n به K^n که هر مؤلفه آن حداکثر درجه d دارد، پوشا باشد.

به عنوان مثال، $\Phi_{2,2}$ جمله‌ای است که به صورت زیر بیان می‌شود:

$$\forall a_{0,0} \forall a_{0,1} \forall a_{0,2} \forall a_{1,0} \forall a_{1,1} \forall a_{2,0} \forall b_{0,0} \forall b_{0,1} \forall b_{0,2} \forall b_{1,0} \forall b_{1,1} \forall b_{2,0}$$

$$\Big(\forall x_1 \forall y_1 \forall x_2 \forall y_2 \Big(\Big(\sum a_{i,j} x_1^i y_1^j = \sum a_{i,j} x_2^i y_2^j \wedge \sum b_{i,j} x_1^i y_1^j = \sum b_{i,j} x_2^i y_2^j\Big)$$

$$\rightarrow (x_1 = x_2 \wedge y_1 = y_2)$$
$$\rightarrow \forall u \forall v \exists x \exists y \left(\sum a_{i,j} x^i y^j = u \wedge \sum b_{i,j} x^i y^j = v\right).$$

طبق ادعا، $\mathbb{F}_p^{\text{alg}} \models \Phi_{n,d}$ برای همه اعداد اول p برقرار است و طبق نتیجه ۶۵-۱، $\mathbb{C} \models \Phi_{n,d}$ که تناقض ایجاد می‌کند. □

۹.۱ بالا و پایین

در بخش‌های قبل، به بررسی دسته‌ی ساختارهای $\mathcal{L}$ و مفهوم $\mathcal{L}$-نشاندن‌های بین ساختارها پرداختیم. این توابع، روابط، ثوابت و توابع $\mathcal{L}$ را حفظ می‌کنند. اغلب می‌خواهیم کلاس محدودتری از توابع را در نظر بگیریم که همه‌ی ویژگی‌های مرتبه اول را حفظ می‌کنند.

تعریف ۶۷-۱. اگر $\mathcal{M}$ و $\mathcal{N}$ ساختارهای $\mathcal{L}$ باشند، یک $\mathcal{L}$-نشاندن به نام $j : \mathcal{M} \to \mathcal{N}$ را نشاندن اولیه می‌نامیم هرگاه برای همه فرمول‌های $\mathcal{L}$ مانند $\phi(v_1, \ldots, v_n)$ و همه‌ی $a_1, \ldots, a_n \in M$ داشته باشیم

$$\mathcal{M} \models \phi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{N} \models \phi(j(a_1), \ldots, j(a_n))$$

اگر $\mathcal{M}$ زیرساختاری از $\mathcal{N}$ باشد، می‌گوییم $\mathcal{M}$ یک زیرساختار اولیه است و می‌نویسیم $\mathcal{M} \prec \mathcal{N}$ هرگاه تابع شمول یک نگاشت اولیه باشد. همچنین می‌گوییم $\mathcal{N}$ یک گسترش اولیه از $\mathcal{M}$ است. یکریختی‌ها، نشاندن‌های اولیه هستند.

تعریف ۶۸-۱. فرض کنید $\mathcal{M}$ یک ساختار $\mathcal{L}$ باشد. $\mathcal{L}_M$ را زبانی در نظر بگیرید که به $\mathcal{L}$، نمادهای ثابت m را برای هر عنصر M اضافه کرده‌ایم. نمودار اتمی $\mathcal{M}$ مجموعه‌ای است از فرمول‌های $\phi(m_1, \ldots, m_n)$ به طوری که ϕ یا یک

فرمول اتمی $\mathcal{L}$ است یا نقیض یک فرمول اتمی $\mathcal{L}$ و $\mathcal{M} \models \phi(m_1, \ldots, m_n)$. نمودار اولیه $\mathcal{M}$ مجموعه‌ای است از تمام فرمول‌های $\phi(m_1, \ldots, m_n)$ که $\mathcal{M} \models \phi(m_1, \ldots, m_n)$ برای هر فرمول $\mathcal{L}$ برقرار است. نمودار اتمی و اولیه $\mathcal{M}$ را به ترتیب با $\mathrm{Diag}(\mathcal{M})$ و $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ نشان می‌دهیم.

لم ۶۹-۱.

(i) فرض کنید $\mathcal{N}$ یک $\mathcal{L}_M$-ساختار باشد و $\mathcal{N} \models \mathrm{Diag}(\mathcal{M})$. در این صورت، اگر $\mathcal{N}$ را به عنوان یک $\mathcal{L}$-ساختار در نظر بگیریم، یک $\mathcal{L}$-نشاندن از $\mathcal{M}$ به $\mathcal{N}$ وجود دارد.

(ii) اگر $\mathcal{N} \models \mathrm{Diag}_{el}(\mathcal{M})$، آنگاه یک نشاندن مقدماتی از $\mathcal{M}$ به $\mathcal{N}$ وجود دارد.

اثبات.

(i) تابع $j : M \to N$ را به صورت $j(m) = m^{\mathcal{N}}$ تعریف می‌کنیم؛ یعنی $j(m)$ تفسیر نماد ثابت m در $\mathcal{N}$ است. اگر m_1, m_2 عناصر متمایزی از M باشند، آنگاه $m_1 \neq m_2 \in \mathrm{Diag}(\mathcal{M})$؛ بنابراین $j(m_1) \neq j(m_2)$ و در نتیجه j یک نشاندن است. اگر f یک نماد تابع در $\mathcal{L}$ باشد و $f^{\mathcal{M}}(m_1, \ldots, m_n) = m_{n+1}$، آنگاه فرمول $f(m_1, \ldots, m_n) = m_{n+1}$ در $\mathrm{Diag}(\mathcal{M})$ وجود دارد و $f^{\mathcal{N}}(j(m_1), \ldots, j(m_n)) = j(m_{n+1})$. اگر R یک نماد رابطه باشد و $\overline{m} \in R^{\mathcal{M}}$، آنگاه $R(m_1, \ldots, m_n) \in \mathrm{Diag}(\mathcal{M})$ و $(j(m_1), \ldots, j(m_n)) \in R^{\mathcal{N}}$). بنابراین j یک نشاندن $\mathcal{L}$ است.

(ii) اگر $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$، آنگاه تابع j تعریف شده در بالا یک نشاندن اولیه است. □

ترکیب این مشاهدات با قضیه‌ی فشردگی به ما امکان می‌دهد گسترش‌های اولیه بسازیم.

قضیه ۷۰-۱ (لوونهایم-اسکولم رو به بالا)**.** فرض کنید $\mathcal{M}$ یک ساختار $\mathcal{L}$-بی‌نهایت و κ یک عدد کاردینال نامتناهی با $\kappa \geq |\mathcal{M}| + |\mathcal{L}|$ باشد. در این صورت، ساختار $\mathcal{L}$-ای مانند $\mathcal{N}$ با کاردینال κ و یک نشاندن اولیه $j : \mathcal{M} \to \mathcal{N}$ وجود دارد.

اثبات. از آنجا که $\mathcal{M} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$، تئوری $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ قابل رضایت است. طبق قضیه ۵۲-۱، ساختار $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ با کاردینال κ وجود دارد. طبق لم ۶۹-۱، یک نشاندن اولیه $j : \mathcal{M} \to \mathcal{N}$ وجود دارد. □

قضیه لوونهایم-اسکولم رو به پایین روشی برای ساخت زیرمدل‌های اولیه کوچک ارائه می‌دهد. اثبات آن از آزمون تارسکی-وات برای گسترش‌های اولیه استفاده می‌کند.

گزاره ۷۱-۱. فرض کنید $\mathcal{M}$ یک زیرساختار از $\mathcal{N}$ باشد. در این صورت، $\mathcal{M}$ یک زیرساختار اولیه است اگر و فقط اگر برای هر فرمول $\phi(v, \overline{w})$ و $\overline{a} \in M$، اگر $b \in N$ وجود داشته باشد به طوری که $\mathcal{N} \models \phi(b, \overline{a})$، آنگاه $c \in M$ وجود دارد که $\mathcal{N} \models \phi(c, \overline{a})$.

اثبات. اگر $\mathcal{N}$ یک گسترش اولیه از $\mathcal{M}$ باشد، شرط به وضوح برقرار است. برای اثبات عکس، باید نشان دهیم که برای همه $\overline{a} \in M$ و همه فرمول‌های $\mathcal{L}$-ای $\psi(\overline{v})$:

$$\mathcal{M} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \psi(\overline{a}).$$

این را با استقرا روی فرمول‌ها اثبات می‌کنیم.

می‌دانیم که اگر $\phi(\overline{v})$ بدون سور باشد، آنگاه $\mathcal{M} \models \phi(\overline{a})$ اگر و فقط اگر $\mathcal{N} \models \phi(\overline{a})$. بنابراین، ادعا برای همه فرمول‌های اتمی درست است.

اگر ادعا برای ψ درست باشد، آنگاه

$$\mathcal{M} \models \neg\psi(\overline{a}) \Leftrightarrow \mathcal{M} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \neg\psi(\overline{a}).$$

به طور مشابه، اگر ادعا برای ψ و θ درست باشد، آنگاه

$$\mathcal{M} \models (\psi \wedge \theta)(\overline{a}) \Leftrightarrow \mathcal{M} \models \psi(\overline{a}) \text{ و } \mathcal{M} \models \theta(\overline{a}) \Leftrightarrow \mathcal{N} \models \psi(\overline{a}) \text{ و } \mathcal{N} \models \theta(\overline{a}) \Leftrightarrow \mathcal{N} \models (\psi \wedge \theta)(\overline{a})..$$

فرض کنید ادعا برای $\psi(v, \overline{w})$ درست باشد. اگر $\mathcal{M} \models \exists v\psi(v, \overline{a})$، آنگاه $b \in M$ وجود دارد که $\mathcal{M} \models \psi(b, \overline{a})$. با فرض استقرا، $\mathcal{N} \models \psi(b, \overline{a})$ و در نتیجه $\mathcal{N} \models \exists v\psi(v, \overline{a})$.

از طرف دیگر، اگر $\mathcal{N} \models \exists v\psi(v, \overline{a})$، با فرض مسأله، $c \in \mathcal{M}$ وجود دارد که $\mathcal{N} \models \psi(c, \overline{a})$. با استقرا، $\mathcal{M} \models \psi(c, \overline{a})$ و در نتیجه $\mathcal{M} \models \exists v\psi(v, \overline{a})$. □

می‌گوییم یک $\mathcal{L}$–تئوری T دارای توابع اسکولم داخلی است اگر برای هر فرمول $\mathcal{L}$–ای $\phi(v, w_1, \ldots, w_n)$، یک نماد تابع f وجود داشته باشد به طوری که:

$$T \models \forall\overline{w}((\exists v\phi(v, \overline{w})) \to \phi(f(\overline{w}), \overline{w})).$$

به عبارت دیگر، به اندازه کافی نماد تابع در زبان وجود دارد تا همه گزاره‌های وجودی را شاهد بگیرد.

لم ۷۲-۱. فرض کنید T یک $\mathcal{L}$–تئوری باشد. زبان $\mathcal{L}^* \supseteq \mathcal{L}$ و $\mathcal{L}^*$–تئوری $T^* \supseteq T$ وجود دارد به طوری که T^* دارای توابع اسکولم داخلی است و اگر $\mathcal{M} \models T$، آنگاه می‌توانیم $\mathcal{M}$ را به $\mathcal{M}^* \models T^*$ گسترش دهیم. می‌توانیم $\mathcal{L}^*$ را طوری انتخاب کنیم که $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$.

از این پس، T^* را اسکولمیزه T می‌نامیم.

اثبات. دنباله‌ای از زبان‌ها $\mathcal{L} = \mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \ldots$ و $\mathcal{L}_i$–تئوری‌های T_i می‌سازیم به طوری که $T = T_0 \subseteq T_1 \subseteq \ldots$.

برای هر $\mathcal{L}_i$، تعریف می‌کنیم:

$$\mathcal{L}_{i+1} = \mathcal{L} \cup \{f_\phi : \phi(v, w_1, \ldots, w_n) \text{ یک } \mathcal{L}_i\text{–فرمول است}, n = 1, 2, \ldots\}$$

که در آن f_ϕ یک نماد تابع n–تایی است. برای هر $\mathcal{L}_i$–فرمول $\phi(v, \overline{w})$، جمله Ψ_ϕ را به صورت زیر تعریف می‌کنیم:

$$\forall\overline{w}((\exists v\phi(v, \overline{w})) \to \phi(f_\phi(\overline{w}), \overline{w}))$$

و $T_{i+1} = T_i \cup \{\Psi_\phi : \phi\text{-formula} \mathcal{L}_i \text{ a is}\}$.

ادعا: اگر $\mathcal{M} \models T_i$، می‌توان نمادهای تابع در $\mathcal{L}_{i+1} \setminus \mathcal{L}_i$ را طوری تفسیر کرد که $\mathcal{M} \models T_{i+1}$.

یک عنصر ثابت $c \in M$ انتخاب می‌کنیم. برای هر $\mathcal{L}_i$–فرمول $\phi(v, w_1, \ldots, w_n)$، تابع $g : M^n \to M$ را طوری تعریف می‌کنیم که اگر $\overline{a} \in M^n$ و $X_{\overline{a}} = \{b \in M : \mathcal{M} \models \phi(b, \overline{a})\} \neq \emptyset$، آنگاه $g(\overline{a}) \in X_{\overline{a}}$، و در غیر این صورت $g(\overline{a}) = c$. بنابراین اگر $\mathcal{M} \models \exists v \phi(v, \overline{a})$، آنگاه $\mathcal{M} \models \phi(g(\overline{a}), \overline{a})$. اگر f_ϕ را به عنوان g تفسیر کنیم، $\mathcal{M} \models \Psi_\phi$.

حال $\mathcal{L}^* = \bigcup \mathcal{L}_i$ و $T^* = \bigcup T_i$ را تعریف می‌کنیم. برای هر $\mathcal{L}^*$–فرمول $\phi(v, \overline{w})$، $\phi \in \mathcal{L}_i$ برای برخی i و $\Psi_\phi \in T_{i+1} \subseteq T^*$، بنابراین T^* دارای توابع اسکولم داخلی است. □

قضیه ۷۳–۱ (لوونهایم–اسکولم). فرض کنید $\mathcal{M}$ یک $\mathcal{L}$–ساختار و $X \subseteq M$ باشد. در این صورت یک زیرمدل اولیه $\mathcal{N}$ از $\mathcal{M}$ وجود دارد به طوری که:

- $X \subseteq N$
- $|\mathcal{N}| \leq |X| + |\mathcal{L}| + \aleph_0$

اثبات. طبق لم ۷۲–۱ می‌توان فرض کرد که $\mathrm{Th}(\mathcal{M})$ دارای توابع اسکولم داخلی است. $X_0 = X$ را تعریف می‌کنیم. برای هر X_i، X_{i+1} را به صورت زیر تعریف می‌کنیم:

$$X_{i+1} = X_i \cup \{f^{\mathcal{M}}(\overline{a}) : f \text{ is an } n\text{-ary function symbol }, \overline{a} \in X_i^n, n = 1, 2, \ldots\}$$

$N = \bigcup X_i$ را در نظر می‌گیریم. در این صورت $|N| \leq |X| + |\mathcal{L}| + \aleph_0$.

اگر f یک نماد تابع n–تایی از $\mathcal{L}$ و $\overline{a} \in N^n$ باشد، آنگاه $\overline{a} \in X_i^n$ برای برخی i و $f^{\mathcal{M}}(\overline{a}) \in X_{i+1} \subseteq N$. بنابراین می‌توان $f^{\mathcal{N}} = f^{\mathcal{M}}|_{N^n}$ را تعریف کرد. به طور مشابه برای نمادهای رابطه و ثابت عمل می‌کنیم.

اگر $\phi(v, \overline{w})$ یک $\mathcal{L}$–فرمول باشد، $\overline{a}, b \in M$ و $\mathcal{M} \models \phi(b, \overline{a})$، آنگاه $\mathcal{M} \models \phi(f(\overline{a}), \overline{a})$ برای نماد تابعی f از $\mathcal{L}$. طبق ساختار، $f^{\mathcal{M}}(\overline{a}) \in N$. بنابراین، طبق گزاره ۷۲–۱، $\mathcal{N} \prec \mathcal{M}$. □

تعریف ۷۴–۱. یک جمله جهانی به شکل $\forall \overline{v} \phi(\overline{v})$ است که ϕ سور ندارد. می‌گوییم یک $\mathcal{L}$–تئوری T بدیهی‌سازی جهانی دارد اگر مجموعه‌ای از جملات جهانی $\mathcal{L}$ مانند Γ وجود داشته باشد به طوری که برای هر $\mathcal{L}$–ساختار $\mathcal{M}$ داشته باشیم:

$$\mathcal{M} \models T \text{ اگر و فقط اگر } \mathcal{M} \models \Gamma$$

قضیه ۷۵–۱. یک $\mathcal{L}$–تئوری T بدیهی‌سازی جهانی دارد اگر و فقط اگر هرگاه $\mathcal{M} \models T$ و $\mathcal{N}$ زیرساختاری از $\mathcal{M}$ باشد، آنگاه $\mathcal{N} \models T$. به عبارت دیگر، یک تئوری تحت زیرساختار حفظ می‌شود اگر و فقط اگر بدیهی‌سازی جهانی داشته باشد.

اثبات. فرض کنید $\mathcal{N} \subseteq \mathcal{M}$. می‌دانیم که اگر $\phi(\overline{v})$ یک فرمول بدون سور باشد و $\overline{a} \in N$، آنگاه

$$\mathcal{N} \models \phi(\overline{a}) \text{ اگر و فقط اگر } \mathcal{M} \models \phi(\overline{a})$$

بنابراین اگر $\mathcal{M} \models \forall \overline{v} \phi(\overline{v})$، آنگاه $\mathcal{N}$ نیز همین طور است.

حال فرض کنید T تحت زیرساختارها حفظ شود. تعریف می‌کنیم

$$\Gamma = \{\phi : \phi \text{ is universal}, T \models \phi\}.$$

واضح است که اگر $\mathcal{N} \models T$، آنگاه $\mathcal{N} \models \Gamma$. برای جهت معکوس، فرض کنید $\mathcal{N} \models \Gamma$. ادعا می‌کنیم $\mathcal{N} \models T$.

ادعا: $T \cup \mathrm{Diag}(\mathcal{N})$ قابل رضایت است.

اگر نباشد، طبق قضیه فشردگی، زیرمجموعه متناهی $\Delta \subseteq \mathrm{Diag}(\mathcal{N})$ وجود دارد به طوری که $T \cup \Delta$ قابل رضایت نباشد. فرض کنید

$$\Delta = \{\psi_1, \dots, \psi_n\}.$$

نمادهای ثابت جدید از N مورد استفاده در $\psi_1, \dots, \psi_n$ را $\overline{c}$ می‌نامیم و می‌گوییم $\psi_i = \phi_i(\overline{c})$ که ϕ_i یک $\mathcal{L}$–فرمول بدون سور است.

اگر مدلی برای $T \cup \{\exists \overline{v} \bigwedge \phi_i(\overline{v})\}$ وجود داشته باشد، با تفسیر $\overline{c}$ به عنوان شاهدی برای فرمول وجودی، $T \cup \Delta$ قابل رضایت خواهد بود. بنابراین

$$T \models \forall \overline{v} \bigvee \neg \phi_i(\overline{v}).$$

از آنجا که این فرمول جهانی است، $\forall \overline{v} \bigvee \neg \phi_i(\overline{v}) \in \Gamma$ که با $\mathcal{N} \models \Gamma$ در تناقض است.

طبق لم ۶۹-۱، $\mathcal{M} \models T$ وجود دارد با $\mathcal{M} \supseteq \mathcal{N}$. چون T تحت زیرساختار حفظ می‌شود، $\mathcal{N} \models T$ و Γ یک بدیهی‌سازی جهانی برای T است. □

تعریف ۷۶-۱. فرض کنید $(I, <)$ یک ترتیب خطی باشد. اگر $\mathcal{M}_i$ یک $\mathcal{L}$–ساختار برای هر $i \in I$ باشد، می‌گوییم $(\mathcal{M}_i : i \in I)$ یک زنجیره از $\mathcal{L}$–ساختارهاست اگر $\mathcal{M}_i \subseteq \mathcal{M}_j$ برای $i < j$. اگر $\mathcal{M}_i \prec \mathcal{M}_j$ برای $i < j$، آن را زنجیره اولیه می‌نامیم.

اگر $(\mathcal{M}_i : i \in I)$ یک زنجیره ناتهی از ساختارها باشد، می‌توان $\mathcal{M} = \bigcup_{i \in I} \mathcal{M}_i$ را به صورت زیر تعریف کرد:

- دامنه $\mathcal{M}$ برابر است با $M = \bigcup_{i \in I} M_i$،
- اگر c یک ثابت در زبان باشد، آنگاه $c^{\mathcal{M}_i} = c^{\mathcal{M}_j}$ برای هر $i, j \in I$ و $c^{\mathcal{M}} = c^{\mathcal{M}_i}$.

فرض کنید $\overline{a} \in M$. چون I به صورت خطی مرتب شده است، می‌توان $i \in I$ را یافت به طوری که $\overline{a} \in M_i$. اگر f یک نماد تابع در $\mathcal{L}$ باشد و $i < j$، آنگاه $f^{\mathcal{M}_i}(\overline{a}) = f^{\mathcal{M}_j}(\overline{a})$. بنابراین $f^{\mathcal{M}} = \bigcup_{i \in I} f^{\mathcal{M}_i}$ یک تابع خوش‌تعریف است. به طور مشابه، اگر R یک نماد رابطه در $\mathcal{L}$ باشد و $i < j$، آنگاه $\overline{a} \in R^{\mathcal{M}_i}$ اگر و فقط اگر $\overline{a} \in R^{\mathcal{M}_j}$. در این صورت $R^{\mathcal{M}} = \bigcup_{i \in I} R^{\mathcal{M}_i}$ را تعریف می‌کنیم. اکنون به راحتی می‌توان دید که $\mathcal{M}_i \subseteq \mathcal{M}$، برای هر $i \in I$.

گزاره ۷۷-۱. فرض کنید $(I, <)$ یک ترتیب خطی و $(\mathcal{M}_i : i \in I)$ یک زنجیره اولیه باشد. در این صورت $\mathcal{M} = \bigcup_{i \in I} M_i$ یک گسترش اولیه برای هر $\mathcal{M}_i$ است.

اثبات. با استقرا روی فرمول‌ها نشان می‌دهیم که برای همه $i \in I$، همه فرمول‌های $\phi(\overline{v})$ و همه $\overline{a} \in M_i^n$:

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M}_i \models \phi(\overline{a})$$

از آنجا که $\mathcal{M}_i$ یک زیرساختار از $\mathcal{M}$ است، می‌دانیم این امر برای همه ϕهای اتمی برقرار است. به راحتی می‌توان دید که اگر این گزاره برای ϕ و ψ برقرار باشد، برای $\neg\phi$ و $\phi \wedge \psi$ نیز برقرار خواهد بود.

فرض کنید ϕ به صورت $\exists v\psi(v, \overline{w})$ باشد و ادعا برای ψ برقرار باشد. اگر $\mathcal{M}_i \models \psi(b, \overline{a})$، آنگاه $\mathcal{M}$ نیز همین طور است. بنابراین اگر $\mathcal{M}_i \models \phi(\overline{a})$، آنگاه $\mathcal{M}$ نیز همین طور است. از طرف دیگر، اگر $\mathcal{M} \models \psi(b, \overline{a})$، آنگاه $j \geq i$ وجود دارد به طوری که $b \in M_j$. با استقرا، $\mathcal{M}_j \models \psi(b, \overline{a})$، بنابراین $\mathcal{M}_j \models \phi(\overline{a})$. چون $\mathcal{M}_i \prec \mathcal{M}_j$، در نتیجه $\mathcal{M}_i \models \phi(\overline{a})$ که همان نتیجه مطلوب است. □

فصل ۲

هندسه جبری و حذف سور

۱.۲ حذف سور

مطالعه مجموعه‌های تعریف‌پذیر به علت وجود سورها اغلب مشکل و طاقت فرسا است. برای مثال در ساختار $(\mathbb{N}, +, \cdot, <)$ مجموعه‌های تعریف‌پذیر بدون سور توسط معادلات و نامعادلات چندجمله‌ای تعریف می‌شوند. بنابر جوابی که توسط $Matijavic, Robinson, Davis$ و $Putnam$ به مسئله دهم هیلبرت داده شد، هر زیرمجموعه شمارش‌پذیر بازگشتی از $\mathbb{N}$ برای $p \in \mathbb{N}[X, Y_1, \ldots, Y_n]$، توسط فرمول زیر تعریف می‌شود

$$\exists v_1 \ldots \exists v_n p(x, v_1, \ldots, v_n) = 0$$

هرچقدر سورها را متناوب کنیم، با مجموعه‌های تعریف‌پذیر پیچیده‌تری برخورد می‌کنیم. واضح است که مطالعه مجموعه‌های تعریف‌پذیری که توسط فرمول‌های بدون سور تعریف شده‌اند ساده‌تر است.

تعریف ۱-۲. می‌گوییم تئوری T حذف سور دارد هرگاه برای هر فرمول ϕ، یک فرمول بدون سور ψ وجود داشته باشد به طوری که $T \models \phi \leftrightarrow \psi$.

برای مثال، فرض کنید $\phi(a, b, c)$ فرمولی به صورت

$$\exists x \ \ ax^2 + bx + c = 0$$

باشد. بنابر فرمول معادله درجه دو، داریم

$$\mathbb{R} \models \phi(a, b, c) \longleftrightarrow [(a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (b \neq 0 \vee c = 0))],$$

که در میدان اعداد مختلط خواهیم داشت

$$\mathbb{C} \models \phi(a,b,c) \longleftrightarrow (a \neq ۰ \vee b \neq ۰ \vee c = ۰).$$

در هر حالت، ϕ با یک فرمول بدون سور معادل است. برای مثالی دیگر، فرض کنید $\phi(a,b,c,d)$ فرمول

$$\exists x \exists y \exists u \exists v \ \ (xa + yc = ۱ \wedge xb + yd = ۰ \wedge ua + vc = ۰ \wedge ub + vd = ۱)$$

باشد. فرمول $\phi(a,b,c,d)$ بیان می‌کند که ماتریس

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

واورن‌پذیر است. پس برای هر میدان F داریم

$$F \models \phi(a,b,c,d) \longleftrightarrow ad - bc \neq ۰$$

در ابتدا، نشان می‌دهیم DLO (تئوری ترتیب‌های خطی چگال بدون نقاط انتهایی) در زبان $\mathcal{L} = \{<\}$ حذف سور دارد. این تئوری، با اصول ترتیب‌های خطی و

$$\forall x \forall y \quad (x < y \longrightarrow \exists z \ x < z < y),$$
$$\exists x \exists y \exists z \quad y < x < z$$

اصل‌بندی می‌شود. قبل از آن که نشان دهیم تئوری DLO حذف سور دارد، قضیه زیر را اثبات می‌کنیم:

قضیه ۲-۲. تئوری DLO، کامل و $\aleph_۰$-جازم است.

اثبات. فرض کنید $(A,<)$ و $(B,<)$ دو مدل شمارش‌پذیر از DLO و $a_۰, a_۱, a_۲, \ldots$ و $b_۰, b_۱, b_۲, \ldots$ به ترتیب شمارش یک‌به‌یک از A و B باشند. یک دنباله از نگاشت‌های دوسویی جزئی $f_i : A_i \to B_i$ خواهیم ساخت که $A_i \subset A$ و $B_i \subset B$ متناهی هستند و $f_۰ \subseteq f_۱ \subseteq \ldots$ و اگر $x, y \in A_i$ و $x < y$، آنگاه $f_i(x) < f_i(y)$. این دنباله را طوری می‌سازیم که $A = \bigcup A_i$ و $B = \bigcup B_i$. در این حالت، $f = \bigcup f_i$ ایزومرفیسم موردنظر از $(A,<)$ به $(B,<)$ است. f_i را یک نشاندن جزئی می‌نامیم. در مراحل فرد، شرط $A = \bigcup A_i$ و در مراحل زوج، شرط $B = \bigcup B_i$ را تشکیل می‌دهیم.

مرحله ۱: $A_۰ = B_۰ = f_۰ = \emptyset$ قرار می‌دهیم.

مرحله $n+۱ = ۲m+۱$: مطمئن می‌شویم که $a_m \in A_{n+۱}$.

اگر $a_m \in A_n$، آنگاه $A_{n+۱} = A_n$، $B_{n+۱} = B_n$ و $f_{n+۱} = f_n$. اگر $a_m \notin A_n$ باشد، برای افزودن a_m به دامنه نشاندن جزئی، باید $b \in B \setminus B_n$ را طوری پیدا کنیم که برای هر $\alpha \in A_n$

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

به عبارت دیگر، باید $b \in B$ پیدا کنیم که در تصویر برش a_m در A_n تحت f_n قرار گیرد. دقیقاً یکی از موارد زیر برقرار است:

۱) a_m از هر عنصر A_n بزرگتر است،

۲) a_m از هر عنصر A_n کوچکتر است،

۳) α و $\beta \in A_n$ وجود دارند به طوری که $\alpha < \beta$ و برای همه $\gamma \in A_n$، $\gamma \leq \alpha$ یا $\gamma \geq \beta$ و $\alpha < a_m < \beta$.

در حالت ۱)، چون B_n متناهی است و $B \models \mathrm{DLO}$، می‌توان $b \in B$ یافت که از هر عنصر B_n بزرگتر باشد. به طور مشابه در حالت ۲) می‌توان $b \in B$ یافت که از هر عنصر B_n کوچکتر باشد. در حالت ۳)، چون f_n یک نشاندن جزئی است، $f_n(\alpha) < f_n(\beta)$ و می‌توان $b \in B \setminus B_n$ انتخاب کرد به طوری که $f_n(\alpha) < b < f_n(\beta)$. توجه کنید که

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

برای هر $\alpha \in A_n$.

در هر صورت، قرار می‌دهیم $A_{n+1} = A_n \cup \{a_m\}$، $B_{n+1} = B_n \cup \{b\}$ و f_n را به $f_{n+1} : A_{n+1} \to B_{n+1}$ با فرستادن a_m به b گسترش می‌دهیم. این، مرحله n را به پایان می‌رساند.

مرحله ۲ $n+1 = 2m+2$: مطمئن می‌شویم که $b_m \in B_{n+1}$.

اگر b_m از قبل در B_n باشد، تغییری ایجاد نمی‌کنیم و فرض می‌کنیم $A_{n+1} = A_n$، $B_{n+1} = B_n$ و $f_{n+1} = f_n$. در غیر این صورت، باید $a \in A$ را طوری پیدا کنیم که تصویر برش a در A_n، برش b_m در B_n باشد. این کار مشابه حالت فرد انجام می‌شود.

به وضوح، در مراحل فرد نشان دادیم که $\bigcup A_n = A$ و در مراحل زوج $\bigcup B_n = B$ برقرار است. چون هر f_n یک نشاندن جزئی است، $f = \bigcup f_n$ یک یکریختی از A به B است.

از آنجا که ترتیب‌های خطی چگال متناهی وجود ندارند، بنابر آزمون وات، تئوری DLO کامل است. □

لم ۳-۲. فرض کنید $(A, <)$ و $(B, <)$ دو ترتیب خطی چگال شمارش‌پذیر باشند که $a_1, \ldots, a_n \in A$ و $b_1, \ldots, b_n \in B$ به طوری که $a_1 < \ldots < a_n$ و $b_1 < \ldots < b_n$. در این صورت، یکریختی $f : A \to B$ وجود دارد به طوری که $f(a_i) = b_i$ برای $i = 1, 2, \ldots, n$.

اثبات. از اثبات قضیه ۲-۲ استفاده می‌کنیم به طوری که با $A_0 = \{a_1, \ldots, a_n\}$، $B_0 = \{b_1, \ldots, b_n\}$ و $f_0 : A_0 \to B_0$ شروع می‌کنیم به طوری که $f_0(a_i) = b_i$. بقیه اثبات مشابه اثبات قضیه ۲-۲ است. □

قضیه ۴-۲. تئوری DLO حذف سور دارد.

اثبات. فرض کنید ϕ یک جمله باشد. اگر $\mathbb{Q} \models \phi$، آنگاه از آن‌جایی که DLO کامل است، $\mathrm{DLO} \models \phi$ و

$$\mathrm{DLO} \models \phi \longleftrightarrow x_1 = x_1$$

در حالی که اگر $\mathbb{Q} \models \neg\phi$، آنگاه

$$\mathrm{DLO} \models \phi \longleftrightarrow x_1 \neq x_1.$$

حال فرض کنید ϕ یک فرمول با متغیرهای آزاد $x_1, \ldots, x_n$ باشد که $n \geq 1$. اکنون نشان می‌دهیم که فرمول بدون سور ψ با متغیرهای آزاد $x_1, \ldots, x_n$ وجود دارد که

$$\mathbb{Q} \models \forall \overline{x} \ \ (\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$$

از آنجا که DLO کامل است،

$$\mathrm{DLO} \models \forall \overline{x}\, (\phi(\overline{x}) \leftrightarrow \psi(\overline{x})).$$

برای $\sigma : \{(i,j) : 1 \leq i < j \leq n\} \to 3$ ، فرمول $\chi_\sigma(x_1, \ldots, x_n)$ را به صورت زیر تعریف می‌کنیم

$$\bigwedge_{\sigma(i,j)=0} x_i = x_j \wedge \bigwedge_{\sigma(i,j)=1} x_i < x_j \wedge \bigwedge_{\sigma(i,j)=2} x_i > x_j.$$

به χ_σ یک شرط علامت می‌گوییم. هر شرط علامت، یک چیدمان از n عنصر در یک مجموعه‌ی مرتب را توصیف می‌کند.

فرض کنید $\mathcal{L}$ زبان تئوری ترتیب‌های خطی و ϕ یک $\mathcal{L}$–فرمول $n \geq 1$ متغیر آزاد باشد. Λ_ϕ را مجموعه تمام شرایط علامت $\sigma : \{(i,j) : 1 \leq i < j \leq n\} \to 3$ در نظر بگیرید به طوری که برای برخی $\overline{a} \in \mathbb{Q}$ داشته باشیم $\mathbb{Q} \models \chi_\sigma(\overline{a}) \wedge \phi(\overline{a})$. دو حالت را بررسی می‌کنیم.

حالت اول: $\Lambda_\phi = \emptyset$.

در این صورت، $\mathbb{Q} \models \forall \overline{x} \ \neg\phi(\overline{x})$ و $\mathbb{Q} \models \phi(\overline{x}) \leftrightarrow x_1 \neq x_1$.

حالت دوم: $\Lambda_\phi \neq \emptyset$.

فرض کنید

$$\psi_\phi(\overline{x}) = \bigvee_{\sigma \in \Lambda_\phi} \chi_\sigma(\overline{x}).$$

با توجه به انتخاب Λ_ϕ، داریم

$$\mathbb{Q} \models \phi(\overline{x}) \to \psi_\phi(\overline{x}).$$

از طرف دیگر، فرض کنید $\bar{b} \in \mathbb{Q}$ و $\mathbb{Q} \models \psi_\phi(\bar{b})$. همچنین فرض کنید $\sigma \in \Lambda_\phi$ به طوری که $\mathbb{Q} \models \chi_\sigma(\bar{b})$. در این صورت $\overline{a} \in \mathbb{Q}$ وجود دارد که $\mathbb{Q} \models \phi(\overline{a}) \wedge \chi_\sigma(\overline{a})$. می‌دانیم یک اتومرفیسم f از $(\mathbb{Q}, <)$ وجود دارد که $f(\overline{a}) = \bar{b}$. پس $\mathbb{Q} \models \phi(\bar{b})$. بنابراین، $\phi(\bar{b}) \leftrightarrow \psi_\phi(\bar{b})$.

□

قضیه ۵-۲. فرض کنید $\mathcal{L}$ یک زبان با نماد ثابت c، T یک تئوری و $\phi(\overline{v})$ یک فرمول در $\mathcal{L}$ باشد. در این صورت، موارد زیر باهم معادل هستند:

(۱) یک فرمول بدون سور $\psi(\overline{v})$ وجود دارد به طوری که $T \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$،
(۲) اگر $\mathcal{M}$ و $\mathcal{N}$ دو مدل از T و $\mathcal{A}$ یک $\mathcal{L}$-ساختار و $\mathcal{A} \subseteq \mathcal{M}$ و $\mathcal{A} \subseteq \mathcal{N}$، آنگاه $\mathcal{M} \models \phi(\overline{a})$ اگر و تنها اگر $\mathcal{N} \models \phi(\overline{a})$، برای هر $\overline{a} \in \mathcal{A}$.

اثبات. $(i) \Rightarrow (ii)$ فرض کنید $T \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$، که در آن ψ بدون سور است. همچنین فرض کنید $\overline{a} \in \mathcal{A}$، که $\mathcal{A}$ یک زیرساختار مشترک از $\mathcal{M}$ و $\mathcal{N}$ است و هر دو ساختار مدل‌هایی از T هستند. می‌دانیم که فرمول‌های بدون سور تحت زیرساختار و گسترش حفظ می‌شوند. بنابراین

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\iff \mathcal{M} \models \psi(\overline{a}) \\
&\iff \mathcal{A} \models \psi(\overline{a}) \quad (\text{since } \mathcal{A} \subseteq \mathcal{M}) \\
&\iff \mathcal{N} \models \psi(\overline{a}) \quad (\text{since } \mathcal{A} \subseteq \mathcal{N}) \\
&\iff \mathcal{N} \models \phi(\overline{a}).
\end{aligned}$$

$(ii) \Rightarrow (i)$ در ابتدا، اگر $T \models \forall \overline{v} \phi(\overline{v})$، آنگاه $T \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow c = c)$. حال اگر $T \models \forall \overline{v} \neg\phi(\overline{v})$، آنگاه $T \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow c \neq c)$.

بنابراین می‌توان فرض کرد که هر دو $T \cup \{\phi(\overline{v})\}$ و $T \cup \{\neg\phi(\overline{v})\}$ قابل‌رضایت هستند.
فرض کنید

$$\Gamma(\overline{v}) = \{\psi(\overline{v}) \ : \ \psi \text{ is quantifier-free and } T \models \forall \overline{v} \ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))\}$$

و $T \models \forall \overline{v}(\phi(\overline{v}) \rightarrow \psi(\overline{v}))\}$. نمادهای ثابت جدید $d_1, \ldots, d_m$ را در نظر بگیرید. نشان می‌دهیم که $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$.
طبق قضیه فشردگی، فرمول‌های $\psi_1, \ldots, \psi_n \in \Gamma$ وجود دارند به طوری که

$$T \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \rightarrow \phi(\overline{v}) \right).$$

در نتیجه

$$T \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \leftrightarrow \phi(\overline{v}) \right),$$

و $\bigwedge_{i=1}^{n} \psi_i(\overline{v})$ بدون سور است. کافیست ادعای زیر را اثبات کنیم:
ادعا: $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$.

فرض کنید چنین نباشد. پس فرض کنید $\mathcal{M} \models T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}$ و $\mathcal{A}$ زیرساختار تولید شده توسط $\overline{d}$ در $\mathcal{M}$ باشد.

فرض کنید $\Sigma = T \cup \mathrm{Diag}(\mathcal{A}) \cup \phi(\overline{d})$. اگر Σ قابل‌رضایت نباشد، آنگاه فرمول‌های بدون سور $\psi_1(\overline{d}), \ldots, \psi_n(\overline{d}) \in \mathrm{Diag}(\mathcal{A})$ وجود دارند به طوری که

$$T \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \rightarrow \neg\phi(\overline{v}) \right).$$

اما در این صورت

$$T \models \forall \overline{v} \left(\phi(\overline{v}) \to \bigvee_{i=1}^{n} \neg \psi_i(\overline{v}) \right),$$

بنابراین $\bigvee_{i=1}^{n} \neg \psi_i(\overline{d}) \in \Gamma$ و $\mathcal{A} \models \bigvee_{i=1}^{n} \neg \psi_i(\overline{d})$ که تناقض ایجاد می‌کند. در نتیجه، Σ قابل‌رضایت است.

فرض کنید $\mathcal{N} \models \Sigma$. در این صورت $\mathcal{N} \models \phi(\overline{d})$. از آن‌جایی که $\mathcal{A} \subseteq \mathcal{N}$، $\Sigma \supseteq \mathrm{Diag}(\mathcal{A})$. اما $\mathcal{M} \models \neg\phi(\overline{d})$؛ بنابراین $\mathcal{N} \models \neg\phi(\overline{d})$ که یک تناقض است. □

این اثبات را می‌توان به حالتی که $\mathcal{L}$ فاقد نمادهای ثابت است نیز تعمیم داد. در این حالت، هیچ جمله بدون سوری وجود ندارد، اما برای هر جمله می‌توان فرمول بدون سور $\psi(v_1)$ یافت به طوری که $T \models \phi \leftrightarrow \psi(v_1)$.

لم ۶-۲. فرض کنید T یک تئوری در زبان $\mathcal{L}$ باشد. اگر برای هر فرمول بدون سور $\theta(\overline{v}, w)$، فرمول بدون سور $\psi(\overline{v})$ وجود داشته باشد به طوری که

$$T \models \exists w\, \theta(\overline{v}, w) \leftrightarrow \psi(\overline{v}),$$

آنگاه T حذف سور دارد.

اثبات. فرض کنید $\phi(\overline{v})$ یک $\mathcal{L}$–فرمول باشد. می‌خواهیم نشان دهیم که

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$$

برای برخی فرمول‌های بدون سور $\psi(\overline{v})$. این را با استقرا روی ساختار $\phi(\overline{v})$ اثبات می‌کنیم.

اگر ϕ بدون سور باشد، چیزی برای اثبات باقی نمی‌ماند. حال فرض کنید برای $i = 0, 1$،

$$T \models \forall \overline{v}\ (\theta_i(\overline{v}) \leftrightarrow \psi_i(\overline{v}))$$

که در آن ψ_i بدون سور است. اگر $\phi(\overline{v}) = \neg\theta_0(\overline{v})$، آنگاه

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \neg\psi_0(\overline{v})).$$

اگر $\phi(\overline{v}) = \theta_0(\overline{v}) \wedge \theta_1(\overline{v})$، آنگاه

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow (\psi_0(\overline{v}) \wedge \psi_1(\overline{v}))).$$

در هر دو حالت، ϕ معادل یک فرمول بدون سور است. حال فرض کنید

$$T \models \forall \overline{v} (\theta(\overline{v}, w) \leftrightarrow \psi_0(\overline{v}, w)),$$

که در آن ψ_0 بدون سور است و

$$\phi(\overline{v}) = \exists w\, \theta(\overline{v}, w).$$

در این صورت،

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \exists w\ \psi_{\circ}(\overline{v}, w)).$$

با توجه به فرض لم، فرمول بدون سور $\psi(\overline{v})$ وجود دارد به طوری که

$$T \models \forall \overline{v}\ (\exists w\ \psi_{\circ}(\overline{v}, w) \leftrightarrow \psi(\overline{v})).$$

اما در این صورت

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v})).$$

□

نتیجه ۷-۲. فرض کنید T یک $\mathcal{L}$-تئوری باشد و برای هر فرمول بدون سور $\phi(\overline{v}, w)$، اگر $\mathcal{M}, \mathcal{N} \models T$، $\mathcal{A}$ زیرساختار مشترک $\mathcal{M}$ و $\mathcal{N}$ باشد، $\overline{a} \in A$ و $b \in M$ وجود داشته باشد به طوری که $\mathcal{M} \models \phi(\overline{a}, b)$، آنگاه یک $c \in N$ وجود داشته باشد به طوری که $\mathcal{N} \models \phi(\overline{a}, c)$. در این صورت، T دارای حذف سور است.

تعریف ۸-۲. فرض کنید $(G, +)$ یک گروه آبلی باشد. اگر برای هر عدد صحیح مثبت n داشته باشیم $nG = G$، آنگاه G را یک گروه بخش‌پذیر می‌نامیم.

لم ۹-۲. فرض کنید G و H گروه‌های آبلی بدون تاب و بخش‌پذیر نابدیهی باشند به طوری که $G \subseteq H$. همچنین فرض کنید $\psi(\overline{v}, w)$ یک فرمول بدون سور باشد، $\overline{a} \in G$، $b \in H$ و $H \models \psi(\overline{a}, b)$. در این صورت عضوی مانند $c \in G$ وجود دارد به طوری که $G \models \psi(\overline{a}, c)$.

اثبات. ابتدا توجه می‌کنیم که ψ را می‌توان به فرم نرمال جداگانی نوشت، یعنی اتمی یا نقیض اتمی وجود دارند مانند $\theta_{i,j}(\overline{v}, w)$ به طوری که

$$\psi(\overline{v}, w) \leftrightarrow \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \theta_{i,j}(\overline{v}, w).$$

از آنجا که $H \models \psi(\overline{a}, b)$، برای یک i داریم $H \models \bigwedge_{j=1}^{m} \theta_{i,j}(\overline{a}, b)$. بنابراین، بدون کاستن از کلیت مسئله، می‌توان فرض کرد که ψ ترکیب فصلی از فرمول‌های اتمی و نقیض اتمی است. از طرفی، فرمول‌های بدون سور در گروه‌های آبلی، ترکیب‌های بولی از معادلات و نامعادلات خطی و فرمول‌های اتمی معادلات خطی هستند. برای مثال،

$$\theta(\overline{v}, w) \equiv n_1 v_1 + \cdots + n_m v_m + kw = 0,$$

که $n_i, k \in \mathbb{Z}$. نقیض فرمول‌های اتمی نامعادله‌ها هستند:

$$\neg\theta(\overline{v}, w) \equiv n_1 v_1 + \cdots + n_m v_m + kw \neq 0.$$

بنابراین، $\psi(\overline{a}, w)$ را می‌توان به صورت

$$\bigwedge_{i=1}^{s}(g_i + m_i w = 0) \wedge \bigwedge_{i=1}^{t}(h_i + m_i' w \neq 0),$$

نوشت به طوری که $g_i, h_i \in G$ (چون $\overline{a} \in G$ و G تحت ترکیبات $\mathbb{Z}$-خطی بسته است). اگر هر یک از $m_i \neq 0$، آنگاه معادله $g_i + m_i w = 0$ دارای جواب منحصر به فرد $w = -\frac{g_i}{m_i} \in G$ است. پس $-\frac{g_i}{m_i}$، چون G بخش‌پذیر است. بنابراین، $b = -fracg_i m_i \in G$ و $G \models \psi(\overline{a}, b)$.

اگر $m_i = 0$، فرمول به $\bigwedge_{i=1}^{t}(h_i + m_i' w \neq 0)$ کاهش پیدا می‌کند و این یعنی $w \neq -\frac{h_i}{m_i}$. از آن‌جایی که G نامتناهی و بدون تاب است، تعداد نامتناهی $c \in G$ وجود دارند که در این تعداد متناهی شرط صدق می‌کنند. بنابراین چنین $c \in G$ وجود دارد. □

لم ۱۰-۲. فرض کنید G یک گروه آبلی بدون تاب باشد. در این صورت، یک گروه آبلی بخش‌پذیر و بدون تاب H وجود دارد که به آن پوسته بخش‌پذیر G می‌گویند، و یک نشاندن $i : G \to H$ به طوری که اگر $j : G \to H'$ یک نشاندن از G به یک گروه آبلی بخش‌پذیر و بدون تاب باشد، آنگاه $h : H \to H'$ وجود دارد که $j = h \circ i$.

اثبات. اگر G گروه بدیهی باشد، می‌توان $H = \mathbb{Q}$ را انتخاب کرد. بنابراین فرض می‌کنیم G نابدیهی است. فرض کنید $X = \{(g, n) : g \in G, n \in \mathbb{N}, n > 0\}$. هر زوج (g, n) را به عنوان g/n در نظر می‌گیریم. یک رابطه‌ی هم‌ارزی $\sim$ روی X تعریف می‌کنیم: $(g, n) \sim (h, m)$ اگر و فقط اگر $mg = nh$. حال فرض کنید $H = X/\sim$. برای هر $(g, n) \in X$، کلاس هم‌ارزی آن را با $[(g, n)]$ نشان می‌دهیم. برای هر (g, n)، کلاس هم‌ارزی آن را با $[(g, n)]$ نشان می‌دهیم. عملگر $+$ را روی H به صورت زیر تعریف می‌کنیم:

$$[(g, n)] + [(h, m)] = [(mg + nh, mn)].$$

باید نشان دهیم که این عملگر خوش‌تعریف است. فرض کنید $(g_0, n_0) \sim (g, n)$. ادعا می‌کنیم که

$$(mg_0 + n_0 h, mn_0) \sim (mg + nh, mn).$$

باید بررسی کنیم که $mn_0(mg + nh) = mn(mg_0 + n_0 h)$. از آنجا که G آبلی است، داریم

$$mn_0(mg + nh) = m^2 n_0 g + mn_0 nh.$$

اما $ng_0 = n_0 g$، بنابراین $mn_0(mg+nh) = m^2 ng_0 + mn_0 nh = mn(mg_0 + n_0 h)$. پس عملگر $+$ خوش‌تعریف است. به طور مشابه، می‌توان عملگر $-$ را به صورت زیر تعریف کرد:

$$[(g, n)] - [(h, m)] = [(mg - nh, mn)].$$

این عملگر نیز خوش‌تعریف است. به سادگی می‌توان نشان داد که $(H, +)$ یک گروه آبلی است که در آن $[(0, 1)]$ عنصر خنثی و $[(-g, n)]$ واورن $[(g, n)]$ است. اگر $[(g, m)] \in H$ و $n > 0$، آنگاه $n[(g, m)] = [(ng, m)]$. اگر

$(ng, m) \sim (0, k)$، آنگاه $kng = 0$. از آنجا که $k > 0$، $n > 0$ و G بدون تاب است، نتیجه می‌گیریم $g = 0$. بنابراین $[(g, m)] = [(0, 1)]$. این نشان می‌دهد که H بدون تاب است.

حال فرض کنید $[(g, m)] \in H$ و $n > 0$. در این صورت $n[(g, mn)] = [(ng, mn)] = [(g, m)]$. پس H بخش‌پذیر است. می‌توان G را با نگاشت $i(g) = [(g, 1)]$ در H نشاند. به وضوح از $g_0 \neq g_1$ می‌توانیم نتیجه بگیریم $[(g_0, 1)] \neq [(g_1, 1)]$. همچنین $[(g, 1)] + [(h, 1)] = [(g + h, 1)]$.

حال فرض کنید H' یک گروه آبلی بخش‌پذیر و بدون تاب باشد و $j : G \to H'$ یک نشاندن باشد. نگاشت $h : H \to H'$ را تعریف می‌کنیم به طوری که

$$h([g, n]) = j(g)/n.$$

خواننده می‌تواند بررسی کند که h یک نشاندن خوش‌تعریف است و $j = h \circ i$. □

قضیه ۱۱-۲. تئوری گروه‌های آبلی بخش‌پذیر (به اختصار DAG)، حذف سور دارد.

اثبات. فرض کنید G_0 و G_1 دو گروه بدون تاب آبلی بخش‌پذیر باشند به طوری که G زیرگروه مشترکی از G_0 و G_1 است، $\overline{g} \in G$، $h \in G_0$ و $G_0 \models \phi(\overline{a}, h)$ که ϕ یک فرمول بدون سور است. نشان می‌دهیم یک $h' \in G_1$ وجود دارد به طوری که $G_1 \models \phi(\overline{g}, h')$. فرض کنید H پوسته بخش‌پذیر G با نشاندن‌های $i_0 : H \hookrightarrow G_0$ و $i_1 : H \hookrightarrow G_1$ باشد. از آن‌جایی که $h \in G_0$ در $\phi(\overline{g}, h)$ صدق می‌کند (در G_0) و $\overline{g} \in G \subseteq H$، می‌توانیم این جواب را به H منتقل کنیم. لم ۹-۲ بیان می‌کند که اگر یک فرمول بدون سور $\psi(\overline{v}, w)$ در یک گروه بزرگتر G_0 جواب داشته باشد، آنگاه در پوسته بخش‌پذیر H هم جواب دارد. پس از آن‌جایی که $\phi(\overline{g}, h)$ در G_0 جواب دارد، داریم $H \models \exists w\, \phi(\overline{g}, w)$. بنابراین، یک $c \in H$ وجود دارد به طوری که $H \models \phi(\overline{g}, c)$. حال، H را در G_1 با i_1 می‌نشانیم که $c \in H$ را به $h' = i_1(c) \in G_1$ می‌برد. چون ϕ بدون سور است و $H \models \phi(\overline{g}, c)$، داریم $G_1 \models \phi(\overline{g}, h')$. بنابراین، طبق نتیجه ۷-۲، تئوری DAG، حذف سور دارد. □

مثال ۱۲-۲. فرض کنید $\phi(x, y) \equiv 2y = x$. در $G_0 = \mathbb{R}$ برای $x = 1$، $y = 0.5$ یک جواب است. پوسته بخش‌پذیر $\mathbb{Z}$، $\mathbb{Q}$ است که $y \in \mathbb{Q}$. در $G_1 = \mathbb{Q}$، این جواب نیز برقرار است. حذف سور تضمین می‌کند که این انتقال همیشه امکان‌پذیر است.

حذف سور تصویر روشنی از مجموعه‌های تعریف‌پذیر در یک مدل از DAG به ما می‌دهد. فرض کنید که

$$\phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$$

یک فرمول اتمی باشد. در این صورت، اعداد صحیحی مانند $k_1, \ldots, k_n$ و $l_1, \ldots, l_m$ وجود دارند به طوری که

$$\phi(\overline{v}, \overline{w}) \leftrightarrow \sum k_i x_i + \sum l_i y_i = 0.$$

اگر $G \models \text{DAG}$ و $a_1, \ldots, a_m \in G$، آنگاه $\phi(\overline{v}, \overline{a})$ مجموعه زیر را تعریف می‌کند:

$$\{\overline{g} \in G^n : \sum k_i g_i + \sum l_i a_i = 0\},$$

که یک ابرصفحه در G^n است. از آنجا که هر فرمول $\mathcal{L}$–ای $\phi(\overline{v},\overline{w})$ در DAG معادل ترکیب بولی از فرمول‌های اتمی $\mathcal{L}$ است، هر زیرمجموعه تعریف‌پذیر از G^n یک ترکیب بولی از ابرصفحه‌ها خواهد بود.

به طور خاص، فرض کنید $\overline{a} \in G^m$ و $\phi(v,\overline{a})$ زیرمجموعه‌ای از G را تعریف کند. در این حالت، «ابرصفحه‌ها» در G صرفاً نقاط تنها هستند. بنابراین:

$$\{g \in G : G \models \phi(g,\overline{a})\}$$

یا متناهی است یا هم‌متناهی. در نتیجه، هر زیرمجموعه تعریف‌پذیر از G در واقع در زبان تساوی نیز از قبل تعریف‌پذیر بوده است. این نمونه‌ای از یک پدیده بسیار مهم است.

تعریف ۱۳-۲. می‌گوییم تئوری T، به شدت کمینه است اگر برای هر $\mathcal{M} \models T$، هر زیرمجموعه تعریف‌پذیر از M ، یا متناهی و یا هم‌متناهی باشد.

نتیجه ۱۴-۲. تئوری گروه‌های آبلی بخش‌پذیر، به شدت کمینه است.

تعریف ۱۵-۲. تئوری T را مدل کامل می‌نامیم هرگاه برای هر دو مدل $\mathcal{A} \subseteq \mathcal{B}$ از T داشته باشیم $\mathcal{A} \prec \mathcal{B}$.

گزاره ۱۶-۲. اگر T حذف سور داشته باشد، آنگاه T یک مدل کامل است.

اثبات. فرض کنید $\mathcal{M} \subseteq \mathcal{N}$ دو مدل از T باشند. باید نشان دهیم که $\mathcal{M}$ یک زیرمدل مقدماتی است. فرض کنید $\phi(\overline{v})$ یک فرمول و $\overline{a} \in M$ باشد. آنگاه یک فرمول بدون سور $\psi(\overline{v})$ وجود دارد که $\mathcal{M} \models \forall\overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. چون فرمول‌های حذف سور تحت زیرساختارها و توسیع‌ها حفظ می شود، $\mathcal{M} \models \psi(\overline{a})$ اگر و تنها اگر $\mathcal{N} \models \psi(\overline{a})$. بنابراین

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a})$$

□

گزاره ۱۷-۲. فرض کنید T یک تئوری مدل کامل باشد. فرض کنید یک $\mathcal{M}_0$ وجود دارد به طوری که $\mathcal{M}_0 \models T$ و در همه‌ی مدل‌های T نشانده می‌شود. در این صورت T کامل است.

اثبات. اگر $\mathcal{M}_0 \models T$، آنگاه هر نشاندن $\mathcal{M}_0$ در $\mathcal{M}$ مقدماتی است. به عبارتی دیگر $\mathcal{M}_0 \equiv \mathcal{M}$. بنابراین هر دو مدل از T، باهم هم‌ارز مقدماتی‌اند. □

تعریف ۱۸-۲. ساختار مرتب $(M,<,\ldots)$ را o–مینیمال گوییم هرگاه برای هر مجموعه تعریف‌پذیر $X \subseteq M$ تعداد متناهی بازه $I_1,\ldots,I_m$ وجود داشته باشند، با نقاط انتهایی در $M \cup \{\pm\infty\}$، و یک مجموعه متناهی X_0 داشته باشیم به طوری که $X = X_0 \cup I_1 \cup \ldots \cup I_m$.

۲.۲ حذف سور در میدان‌های بسته جبری

یکی از مفاهیم بنیادی در جبر و نظریه میدان، میدان‌های بسته جبری است؛ میدان‌هایی که در آن‌ها هر چندجمله‌ای غیرصفر با ضریب‌هایی از آن میدان، دست‌کم یک ریشه در همان میدان دارد. این ویژگی، میدان‌های بسته جبری را به بستری ایده‌آل برای مطالعهٔ معادلات چندجمله‌ای و رفتار ریشه‌ها تبدیل می‌کند.

نقش میدان‌های بسته جبری در جبر کلاسیک و مدرن، به‌ویژه در زمینه‌هایی مانند هندسه جبری، نظریه گالوا، و نظریه نمایش، برجسته و بنیادین است. میدان اعداد مختلط $\mathbb{C}$ مهم‌ترین نمونه میدان بسته جبری است که در بسیاری از مباحث تحلیلی و جبری نقش محوری دارد.

در این بخش، ابتدا به تعریف دقیق میدان‌های بسته جبری پرداخته، سپس ویژگی‌های مهم آن‌ها را بررسی می‌کنیم. همچنین به برخی قضایای اساسی مانند قضیه بنیادی جبر اشاره خواهیم کرد که اهمیت و جایگاه این میدان‌ها را در ساختار کلی ریاضیات نشان می‌دهد.

تعریف ۱۹-۲. میدان K را یک میدان بسته جبری می‌نامیم هرگاه هر چندجمله‌ای $f(x) \in K[x] \backslash K$، حداقل یک ریشه داشته باشد.

مثال ۲۰-۲. میدان اعداد مختلط؛ یعنی $\mathbb{C}$، یک میدان بسته جبری است در حالی که میدان اعداد حقیقی $\mathbb{R}$ یک میدان بسته جبری نیست.

تعریف ۲۱-۲. می‌گوییم یک فرمول $\varphi(X_1, \ldots, X_n)$ به فرم نرمال پیش‌سور[1] است هرگاه به شکل زیر باشد:

$$(Q_1 Y_1) \cdots (Q_m Y_m) \psi(X_1, \ldots, X_n, Y_1, \ldots, Y_m),$$

که در آن هر Q_i یکی از سورهای $\exists$ یا $\forall$ و $\psi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ یک فرمول بدون سور است.

دو فرمول φ و φ' از یک زبان را معادل منطقی می‌نامیم هرگاه $\varphi \leftrightarrow \varphi'$ یک فرمول برقرار باشد.

لم ۲۲-۲. هر فرمول $\varphi(X_1, \ldots, X_n)$ از یک زبان $\mathcal{L}$ معادل منطقی با یک فرمول $\varphi^*(X_1, \ldots, X_n)$ به فرم نرمال پیش‌سور است.

اثبات. لم را با استقرا روی ساختار فرمول‌ها اثبات می‌کنیم. فرمول‌های اتمی متغیر ندارند، پس از قبل به فرم نرمال پیش‌سور هستند. فرض کنید φ به این فرم باشد. در این صورت $\neg\varphi$ به شکل $(Q'_1 Y_1) \ldots (Q'_m Y_m) \neg\psi(X, Y)$ خواهد بود به طوری که اگر $Q_i = \forall$، داریم $Q'_i = \exists$ و اگر $Q_i = \exists$، داریم $Q'_i = \forall$. قرار دهید $\mathbf{X} = (X_1, \ldots, X_n)$ و $\mathbf{Y} = (Y_1, \ldots, Y_m)$. اگر φ به فرم نرمال پیش‌سور و φ' به فرم $(Q'_1 Y'_1) \cdots (Q'_{m'} Y'_{m'}) \psi'(\mathbf{X}, \mathbf{Y}')$ باشد، آنگاه جایگزین کردن متغیرهای Y'_i، در صورت نیاز، با متغیرهای جدید متفاوت از Y_iها و X_iها، فرمول $\varphi \vee \varphi'$ معادل منطقی با

$$(Q_1 Y_1) \cdots (Q_m Y_m)(Q'_1 Y'_1) \cdots (Q'_{m'} Y'_{m'})[\psi(\mathbf{X}, \mathbf{Y}) \vee \psi'(\mathbf{X}, \mathbf{Y}')]$$

است. □

[1] prenex normal form

اثبات لم ۳۲-۲ به طور مؤثری φ^* را از φ تولید می‌کند. تعداد حروف در φ یک کران برای تعداد مراحل این روش است. بنابراین در هر روش تصمیم‌گیری، فرض می‌کنیم که جملات (یا در صورت نیاز، فرمول‌ها) به فرم نرمال پیش‌سور هستند.

یک روند حذف سور برای یک تئوری T از زبان $\mathcal{L}$، روندی است که از یک فرمول داده شده $\psi(X, Z_1, \ldots, Z_n)$، فرمول $\psi'(Z_1, \ldots, Z_n)$ را می‌سازد به طوری که

$$T \models (\exists X)[\psi(X, \mathbf{Z})] \leftrightarrow \psi'(\mathbf{Z}).$$

این یعنی برای هر مدل $\mathcal{A}$ از T با جهان سخن A و هر n–تایی $(a_1, \ldots, a_n)$ از A، $\mathcal{A} \models (\exists X)\psi(X, \mathbf{a})$ اگر و تنها اگر $\mathcal{A} \models \psi'(\mathbf{a})$؛ یعنی سور $\exists$ حذف شده است. اگر $T \models (\exists X)[\neg\psi(X\mathbf{Z})] \leftrightarrow \psi''(\mathbf{Z})$، آنگاه

$$T \models (\forall X)[\psi(X, \mathbf{Z})] \leftrightarrow \neg\psi''(\mathbf{Z}).$$

پس حذف $\exists$ منجر به حذف $\forall$ نیز می‌شود. با شروع از یک فرمول $\varphi(X_1, \ldots, X_n)$ به فرم نرمال پیش‌سور، می‌توان فرمول $\psi_1(\mathbf{X}, Y_1, \ldots, Y_{m-1})$ را پیدا کرد به طوری که

$$T \models (Q_m Y_m)[\psi(\mathbf{X}, Y_1, \ldots, Y_m)] \leftrightarrow \psi_1(\mathbf{X}, Y_1, \ldots, Y_{m-1}).$$

سپس،

$$T \models (Q_1 Y_1) \cdots (Q_m Y_m)[\psi(\mathbf{X}, Y_1, \cdots, Y_m)] \leftrightarrow (Q_1 Y_1) \cdots (Q_{m-1} Y_{m-1})[\psi_1(\mathbf{X}, Y_1, \ldots, Y_{m-1})].$$

با استقرا، این روش سورهای $Q_m, Q_{m-1}, \ldots, Q_1$ را یک به یک حذف می‌کند تا به فرمول بدون سور $\psi_m(\mathbf{X})$ برسد که با $\varphi(\mathbf{X})$ به پیمانه T معادل است. اگر $\mathcal{A} \subseteq \mathcal{B}$ دو مدل از T و $a_1, \ldots, a_n$ عناصری از A باشند، آنگاه $\mathcal{A} \models \psi_m(\mathbf{a})$ اگر و تنها اگر $\mathcal{B} \models \psi_m(\mathbf{a})$. بنابراین $\mathcal{A} \models \varphi(\mathbf{a})$ اگر و تنها اگر $\mathcal{B} \models \varphi(\mathbf{a})$. از آنجایی که φ دلخواه بود، $\mathcal{A} \prec \mathcal{B}$.

اعمال روند حذف سور بر یک جمله θ، جمله بدون سور θ' را تولید می‌کند به طوری که $T \models \theta \leftrightarrow \theta'$. اگر علاوه بر این بتوانیم تصمیم بگیریم که آیا یک جمله بدون سور θ' متعلق به T است و T از نظر استنتاجی بسته باشد، آنگاه T تصمیم‌پذیر است.

یک فرمول بدون سور $\psi(X_1, \ldots, X_n)$ از چندجمله‌ای‌های بولی $P(Z_1, \ldots, Z_m)$ با جایگزین کردن یک فرمول اتمی $\tau_i(X_1, \ldots, X_n)$ به جای Z_i برای $i = 1, \ldots, m$ به دست می‌آید. برای ساده‌سازی ψ، $P(Z_1, \ldots, Z_m)$ را به فرم

$$P'(Z_1, \ldots, Z_m) = \bigvee_{i \in I} \Big(\bigwedge_{j \in J} Z_{ij} \ \wedge \ \bigwedge_{j \in J'} \neg Z_{ij} \Big)$$

تبدیل می‌کنیم به طوری که هر Z_{ij} در $\{Z_1, \ldots, Z_m\}$ قرار دارد. بنابراین، $P(Z_1, \ldots, Z_m)$ و $P'(Z_1, \ldots, Z_m)$ برای هر تابع $f : \{Z_1, \ldots, Z_m\} \to \{\text{درست، نادرست}\}$ مقدار درستی یکسانی دارد. با اعمال قوانین دمورگان[۲] (مثلاً

[۲] de Morgan's laws

$(\neg(X \vee Y) \equiv (\neg X) \wedge (\neg Y)$ یا $X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$) از P به P' می‌رسیم. واضح است که ψ از نظر منطقی با فرمول $P'(\tau_1, \ldots, \tau_m)$ معادل است.

برای ساده‌سازی بیشتر، از معادل‌های منطقی $(\exists X)[\psi \vee \psi'] \equiv (\exists X)[\psi] \vee (\exists X)[\psi']$ استفاده می‌کنیم. بنابراین، مسئله به بررسی فرمولی از شکل $(\exists Y)[\bigwedge_{j \in J} \tau_j(Y, X_1, \ldots, X_n)]$ تقلیل می‌یابد، که در آن $\tau_j(Y, \mathbf{X})$ یا یک فرمول اتمی یا نقیض یک فرمول اتمی است. تنها نیاز است فرمول $\psi'(X_1, \ldots, X_n)$ را پیدا کنیم که معادل این فرمول به پیمانه T باشد.

۳.۲ یک روند حذف سور

کلید این روش، یک الگوریتم تقسیم برای چندجمله‌ای‌ها است.

تعریف ۲-۲۳. فرض کنید R یک حلقه باشد. تئوری میدان‌ها را با نماد $\Pi(R)$ در زبان $\mathcal{L}_r$ نمایش می‌دهیم.

تعریف ۲-۲۴. فرض کنید ϕ و ψ دو فرمول در زبان حلقه‌ها باشند. می‌گوییم ψ به پیمانه $\Pi(R)$ با ϕ معادل است هرگاه $\Pi(R) \models \phi \leftrightarrow \psi$.

یک دامنه صحیح R را در نظر می‌گیریم و از زبان $\mathcal{L}_r$ استفاده می‌کنیم. مدل‌های اصول $\Pi(R)$ دقیقاً همان میدان‌هایی هستند که شامل یک تصویر همریخت از R هستند. $\Pi(R)$ را به مجموعه جدیدی از اصول با نماد $\tilde{\Pi}(R)$ با اضافه کردن جملات زیر گسترش می‌دهیم:

$$(\forall Z_0) \cdots (\forall Z_{n-1})(\exists X)[X^n + Z_{n-1}X^{n-1} + \cdots + Z_0 = 0], \quad n = 1, 2, \ldots .$$

یک مدل F از $\Pi(R)$، مدلی از $\tilde{\Pi}(R)$ نیز هست اگر و فقط اگر F بسته جبری باشد. هدف نهایی ما در ادامه، معرفی یک روش حذف سور برای $\tilde{\Pi}(R)$ است. هر عبارت در زبان $\mathcal{L}_r$ به پیمانه $\Pi(R)$ معادل با یک چندجمله‌ای $f(X_1, \ldots, X_n)$ با ضرایب در R است. بنابراین، هر فرمول اتمی به پیمانه $\Pi(R)$ با یک معادله $f(X_1, \ldots, X_n) = 0$ معادل است. یک ترکیب عطفی $g_1(\mathbf{X}) \cdots g_m(\mathbf{X}) \neq 0$ از نامعادله‌ها معادل با نامعادله $\bigwedge_{i=1}^{m} g_i(\mathbf{X}) \neq 0$ است. بنابراین، برای یک روش حذف سور برای $\tilde{\Pi}(R)$، فقط نیاز داریم که Y را از فرمول‌هایی به شکل زیر حذف کنیم:

$$(\exists Y)[f_1(\mathbf{X}, Y) = 0 \ \wedge \ \cdots \ \wedge \ f_m(\mathbf{X}, Y) = 0 \ \wedge \ g(\mathbf{X}, Y) \neq 0] \qquad (1)$$

که در آن $f_1, \ldots, f_m, g \in R[X_1, \ldots, X_n, Y]$.

قضیه ۲-۲۵. فرض کنید R یک دامنه صحیح و $\varphi(X_1, \ldots, X_n)$ یک فرمول در $\mathcal{L}_r$ باشد. بنابراین $\varphi(X_1, \ldots, X_n)$ به پیمانه $\tilde{\Pi}(R)$ با یک فرمول بدون سور $\psi(X_1, \ldots, X_r)$ معادل است. اگر φ یک جمله باشد، آنگاه یک عنصر ناصفر $c \in R$ وجود دارد به طوری که یا φ در هر مدل از $\tilde{\Pi}(R) \cup \{c \neq 0\}$ درست، یا φ در هر مدل از $\tilde{\Pi}(R) \cup \{c \neq 0\}$ نادرست است.

اثبات. می‌توان فرض کرد که φ توسط (۱) داده شده است. اثبات شامل سه بخش است:

بخش الف: کاهش به حالتی که تنها یکی از $f_1, \ldots, f_m$ شامل Y باشد.

هر یک از عطف‌هایی که در (۱) ظاهر می‌شوند و شامل Y نیستند را با استفاده از قاعده

$$(\exists Y)[\varphi \wedge \psi] \equiv \varphi \wedge (\exists Y)[\psi] \quad \text{اگر } Y \text{ در } \phi \text{ ظاهر نشود}$$

به سمت چپ $(\exists Y)$ منتقل می‌کنیم. بنابراین فرض می‌کنیم که $\deg_Y(f_i(\mathbf{X}, Y)) \geq 1$ برای $i = 1, \ldots, m$ و $m \geq 2$. حال استقرا را روی $\sum \deg_Y(f_i(\mathbf{X}, Y))$ انجام می‌دهیم. فرض کنید $p(\mathbf{X}, Y)$ و $q(\mathbf{X}, Y)$ چندجمله‌ای‌هایی با ضرایب در R باشند به طوری که $0 \leq \deg_Y(p(\mathbf{X}, Y)) \leq \deg_Y(q(\mathbf{X}, Y)) = d$. $p(\mathbf{X}, Y)$ را به شکل زیر می‌نویسیم:

$$p(\mathbf{X}, Y) = a_k(\mathbf{X})Y^k + a_{k-1}(\mathbf{X})Y^{k-1} + \cdots + a_0(\mathbf{X}) \qquad (۲)$$

که در آن $a_j \in R[\mathbf{X}]$. برای هر j با $0 \leq j \leq k$ قرار می‌دهیم

$$p_j(\mathbf{X}, Y) = a_j(\mathbf{X})Y^j + a_{j-1}(\mathbf{X})Y^{j-1} + \cdots + a_0(\mathbf{X}).$$

اگر $a_j(\mathbf{X})$ صفر نباشد، تقسیم $q(\mathbf{X}, Y)$ بر $p_j(\mathbf{X}, Y)$، $q_j(\mathbf{X}, Y)$ و $r_j(\mathbf{X}, Y)$ را در $R[\mathbf{X}, Y]$ تولید می‌کند به طوری که

$$a_j(\mathbf{X})^d q(\mathbf{X}, Y) = q_j(\mathbf{X}, Y)p_j(\mathbf{X}, Y) + r_j(\mathbf{X}, Y), \qquad (۳)$$

و $\deg_Y(r_j) < \deg_Y(p_j) \leq d$. فرض کنید F مدلی از $\Pi(R)$ باشد. اگر $x_1, \ldots, x_n, y$ عناصری از F باشند به طوری که $a_k(\mathbf{x}) = \cdots = a_{j+1}(\mathbf{x}) = 0$ و $a_j(\mathbf{x}) \neq 0$، آنگاه $[p(\mathbf{x}, y) = 0 \ \wedge \ q(\mathbf{x}, y) = 0]$ در F با $[p_j(\mathbf{x}, y) = 0 \wedge r_j(\mathbf{x}, y) = 0]$ معادل است. بنابراین، فرمول $[p(\mathbf{X}, Y) = 0 \wedge q(\mathbf{X}, Y) = 0]$ به پیمانه $\Pi(R)$ با فرمول

$$\bigvee_{j=0}^{k} \big[a_k(\mathbf{X}) = 0 \wedge \cdots \wedge a_{j+1}(\mathbf{X}) = 0 \qquad (۴)$$

$$\wedge\, a_j(\mathbf{X}) \neq 0 \ \wedge \ p_j(\mathbf{X}, Y) = 0 \ \wedge \ r_j(\mathbf{X}, Y) = 0]$$

$$\vee\, [a_k(\mathbf{X}) = 0 \ \wedge \cdots \wedge \ a_0(\mathbf{X}) = 0 \ \wedge \ q(\mathbf{X}, Y) = 0]$$

معادل است. همچنین برای هر j بین 0 و k داریم

$$\deg_Y(p_j(\mathbf{X}, Y)) \leq \deg_Y(p(\mathbf{X}, Y)) \quad \text{و}$$

$$\deg_Y(r_j(\mathbf{X}, Y)) < \deg_Y(p(\mathbf{X}, Y)),$$

و آخرین عطف فقط شامل یک چندجمله‌ای $q(\mathbf{X},Y)$ است که Y در آن ظاهر می‌شود. نتیجه (۴) را بر $f_1(\mathbf{X},Y)$ و $f_m(\mathbf{X},Y)$ (از (۱)) اعمال می‌کنیم. با اعمال قاعده

$$(\exists Y)[\varphi \vee \psi] \equiv (\exists Y)[\varphi] \vee (\exists Y)[\psi]$$

بر (۴)، (۱) را با عطف‌هایی از فرم (۱) جایگزین می‌کنیم که در هر یک از آنها مجموع $\sum \deg_Y(f_i(\mathbf{X},Y))$ کوچکتر است. با استفاده از فرض استقرا نتیجه می‌گیریم که می‌توان m را حداکثر ۱ در نظر گرفت.

بخش ب: کاهش به حالتی که $m = 0$

با ادامه نمادگذاری بخش الف، به نقطه‌ای رسیدیم که باید Y را از $p(\mathbf{X},Y)$ در عبارت زیر حذف کنیم

$$(\exists Y)[p(\mathbf{X},Y) = 0 \ \wedge \ g(\mathbf{X},Y) \neq 0]. \qquad (۵)$$

مدل $\tilde{F}$ از $\tilde{\Pi}(R)$ و عناصر $x_1,\ldots,x_n$ در $\tilde{F}$ را در نظر بگیرید. اگر $p(\mathbf{x},Y)$ صفر نباشد، آنگاه (از آنجا که $\tilde{F}$ بسته جبری است) تقسیم با باقی‌مانده نشان می‌دهد که گزاره

$$\tilde{F} \models (\exists Y)[p(\mathbf{x},Y) = 0 \ \wedge \ g(\mathbf{x},Y) \neq 0]$$

معادل است با گزاره "$p(\mathbf{x},Y)$، $g(\mathbf{x},Y)^k$ را در $\tilde{F}[Y]$ نمی‌شمارد".

بنابراین، با قرار دادن $q(\mathbf{X},Y) = g(\mathbf{X},Y)^k$ و با نمادگذاری (۲) و (۳)، فرمول (۵) به پیمانه $\hat{\Pi}(R)$ معادل است با فرمول

$$\bigvee_{j=0}^{k} \left[a_k(\mathbf{X}) = 0 \ \wedge \ \cdots \ \wedge \ a_{j+1}(\mathbf{X}) = 0 \ \wedge \ a_j(\mathbf{X}) \neq 0 \ \wedge \ (\exists Y)[r_j(\mathbf{X},Y) \neq 0]\right]$$

$$\vee \left[a_k(\mathbf{X}) = 0 \ \wedge \ \cdots \ \wedge \ a_0(\mathbf{X}) = 0 \ \wedge \ (\exists Y)[g(\mathbf{X},Y) \neq 0]\right]$$

که عطفی از گزاره‌های به فرم (۱) با $m = 0$ است.

بخش پ: تکمیل اثبات

با توجه به بخش ب، به نقطه‌ای رسیده‌ایم که باید Y را از گزاره‌ای به شکل زیر حذف کنیم:

$$(\exists Y)[a_l(\mathbf{X})Y^l + a_{l-1}(\mathbf{X})Y^{l-1} + \cdots + a_0(\mathbf{X}) \neq 0].$$

از آنجا که مدل‌های $\hat{\Pi}(R)$ میدان‌های نامتناهی هستند، این فرمول به پیمانه $\hat{\Pi}(R)$ با

$$a_l(\mathbf{X}) \neq 0 \ \vee \ a_{l-1}(\mathbf{X}) \neq 0 \ \vee \ \cdots \ \vee \ a_0(\mathbf{X}) \neq 0$$

معادل است. اکنون روش تبدیل یک فرمول داده شده $\varphi(X_1,\ldots,X_n)$ از $\mathcal{L}_r$ به یک فرمول بدون سور $\psi(X_1,\ldots,X_n)$ به پیمانه $\hat{\Pi}(R)$ را کامل کرده‌ایم. به طور خاص، اگر φ یک جمله باشد، ψ را می‌توان به شکل

$$\bigvee_{i\in I} \bigwedge_{j\in J} [a_{ij} = 0 \ \wedge \ c_i \neq 0] \qquad (۶)$$

در نظر گرفت که در آن $a_{ij}, c_i \in R$. اگر c حاصلضرب تمام c_iهای ناصفر و تمام a_{ij}های ناصفر باشد (یا $c = ۱$ اگر چنین عبارتی وجود نداشته باشد)، و اگر $\tilde{F}$ مدلی از $\hat{\Pi}(R) \cup \{c \neq ۰\}$ باشد، آنگاه (۶) در $\tilde{F}$ درست است اگر و تنها اگر در R درست باشد. □

نتیجه ۲-۲۶. فرض کنید R یک دامنه صحیح با $K = \mathrm{Quot}(R)$ باشد و θ یک جمله در $\mathcal{L}_r$. در این صورت، یک عنصر ناصفر c در R با ویژگی‌های زیر وجود دارد:

(الف) اگر $\tilde{K} \models \theta$، آنگاه $\tilde{F} \models \theta$ برای هر میدان بسته جبری $\tilde{F}$ که شامل یک تصویر همریخت $\tilde{R}$ از R باشد و در آن تصویر $\tilde{c}$ از c ناصفر باشد.

(ب) اگر میدان بسته جبری $\tilde{F}$ وجود داشته باشد که شامل یک تصویر همریخت $\tilde{R}$ از R باشد به طوری که $\tilde{c} \neq ۰$ و $\tilde{F} \models \theta$، آنگاه $\tilde{K} \models \theta$.

قضیه ۲-۲۷. تئوری میدان‌های بسته جبری حذف سور دارد.

اثبات. فرض کنید D یک دامنه صحیح باشد. آنگاه بستار جبری میدان تقسیم D در هر میدان بسته جبری که شامل D باشد، نشانده می‌شود. بنابراین، تئوری میدان‌های بسته جبری، مدل کامل دارد. برای اثبات داشتن حذف سور این تئوری فقط باید نشان دهیم که اگر F و K میدان بسته جبری باشند به طوری که $F \subseteq X$، $\phi(x, \overline{y})$ بدون سور است و اگر $K \models \phi(b, \overline{a})$ برای $\overline{a} \in F$ و $b \in K$، آنگاه $F \models \exists v \phi(v, \overline{a})$. فرض کنید $\phi(x, \overline{y})$ اجتماعی از فرمول‌های اتمی و نقیض آن‌ها باشد. در زبان حلقه‌ها، فرمول‌های اتمی $\theta(v_۱, \ldots, v_n)$ به صورت $p(\overline{v}) = ۰$ هستند به طوری که $p \in \mathbb{Z}[X_۱, \ldots, X_n]$. اگر $p(X, \overline{Y}) \in \mathbb{Z}[X, \overline{Y}]$، می‌توانیم $p(X, \overline{a})$ را یک چندجمله‌ای در $F[X]$ در نظر بگیریم. پس چندجمله‌هایی $p_۱, \ldots, p_n, q_۱, \ldots, q_m \in F[X]$ وجود دارند که $\phi(v, \overline{a})$ با

$$\bigwedge_{i=۱}^{n} p_i(v) = ۰ \wedge \bigwedge_{i=۱}^{m} q_i(v) \neq ۰$$

هم‌ارز است. اگر هر چندجمله‌ای p_i ناصفر بود، آنگاه b روی F جبری است. در این مورد چون F بستار جبری است، $b \in F$. بنابراین فرض می‌کنیم که $\phi(v, \overline{a})$ با

$$\bigwedge_{i=۱}^{m} q_i(v) \neq ۰$$

هم‌ارز است. اما $q_i(X) = ۰$ برای $i \leq m$ فقط تعداد متناهی جواب دارد. پس فقط تعداد متناهی عنصر در F هستند که در F صدق نمی‌کنند. چون میدان‌های بسته جبری نامتناهی‌اند، $c \in F$ وجود دارد که $F \models \phi(c, \overline{a})$. □

نتیجه ۲-۲۸. تئوری میدان‌های بسته جبری، مدل کامل است.

اثبات. مدل کامل بودن، نتیجه مستقیم حذف سور است. □

۱.۳.۲ کاربردها

مدل کامل بودن تئوری میدان‌های بسته جبری، اثبات‌های جایگزینی برای برخی نتایج پایه‌ای هندسه جبری ارائه می‌دهد. یکی از آنها قضیه ضعیف صفرهای هیلبرت[۳] است.

قضیه ۲-۲۹. فرض کنید K یک میدان، $f_1(\mathbf{X}),\dots,f_m(\mathbf{X})\in K[X_1,\dots,X_n]$ و I ایده‌آل تولید شده توسط f_iها باشد. اگر $I\neq K[\mathbf{X}]$، آنگاه نقاط $x_1,\dots,x_n$ در $\tilde{K}$ وجود دارند به طوری که $f_i(\mathbf{x})=0$ برای $i=1,\dots,m$.

اثبات. با استفاده از لم زرن، ایده‌ال ماکسیمال $\mathfrak{m}$ از $K[\mathbf{X}]$ وجود دارد که شامل I است. حلقه $F=K[\mathbf{X}]/\mathfrak{m}$ را در نظر بگیرید. F شامل یک میدان K است و n-تایی $(X_1+\mathfrak{m},\dots,X_n+\mathfrak{m})$ هر چندجمله‌ای در $\mathfrak{m}$ را صفر می‌کند. بنابراین، جمله

$$(\exists X_1)\dots(\exists X_n)\,[\bigwedge_{i=1}^{m} f_i(X_1,\dots,X_n)=0] \tag{۷}$$

در زبان $\mathcal{L}_r$ در $\tilde{F}$ درست است. با توجه به نتیجه ۲-۲۸، $\bar{K}\prec\bar{F}$. بنابراین، (۷) در $\bar{K}$ نیز درست است. □

قضیه قوی صفرهای هیلبرت از قضیه ضعیف نتیجه می‌شود:

قضیه ۲-۳۰. فرض کنید $f_1,\dots,f_m,g$ چندجمله‌ای‌هایی در $K[X_1,\dots,X_n]$ باشند. اگر g در هر نقطه صفر مشترک $f_1,\dots,f_m$ در $\bar{K}^n$ صفر شود، آنگاه توانی از g به ایده‌آل I تولید شده توسط $f_1,\dots,f_m$ در $K[\mathbf{X}]$ تعلق دارد.

اثبات. فرض کنید Y یک متغیر اضافی باشد و بدون کاستن از کلیت مسئله، $g\neq 0$. چندجمله‌ای $1-Yg(\mathbf{X})$ را در نظر بگیرید. در این صورت، $m+1$ چندجمله‌ای

$$f_1(\mathbf{X}),\dots,f_m(\mathbf{X}),\ \ 1-Yg(\mathbf{X})$$

در $K[\mathbf{X},Y]$ هیچ نقطه صفر مشترکی در $\bar{K}^{n+1}$ ندارند. با توجه به قضیه ۲-۲۹، این چندجمله‌ای‌ها کل حلقه را تولید می‌کنند. به طور خاص، چندجمله‌ای‌هایی $a_1,\dots,a_m,b$ در $K[\mathbf{X},Y]$ وجود دارند به طوری که

$$1=\sum_{i=1}^{m} a_i(\mathbf{X},Y)f_i(\mathbf{X})+b(\mathbf{X},Y)(1-Yg(\mathbf{X})). \tag{۸}$$

با جایگزینی $Y=g(\mathbf{X})^{-1}$ در (۸)، داریم $\sum_{i=1}^{m} a_i(\mathbf{X},g(\mathbf{X})^{-1})f_i(\mathbf{X})=1$. با انتخاب

$$r\geq \max_{1\leq i\leq m} \deg_Y a_i(\mathbf{X},Y)$$

داریم $g(\mathbf{X})^r=\sum_{i=1}^{m} g(\mathbf{X})^r a_i(\mathbf{X},g(\mathbf{X})^{-1})f_i(\mathbf{X})$ که به I تعلق دارد. □

[۳] Hilbert's Nullstellensatz

۴.۲ موضعی‌سازی

در این بخش، فرآیند گسترش یک حلقه A را با استفاده از کسرهایی با درایه‌هایی در A معرفی می‌کنیم. اگر A یک دامنه صحیح باشد، کار ساده‌تر است، اما به حالت کلی‌تر نیاز داریم. به دلایلی که در بافت هندسی آشکار خواهند شد، این فرآیند موضعی‌سازی نامیده می‌شود.

تعریف ۳۱-۲. فرض کنید A یک حلقه و $S \subset A$ یک زیرمجموعه باشد. می‌گوییم S یک مجموعه ضربی است اگر $1 \in S$ و برای هر $s, t \in S$ داشته باشیم $st \in S$.

مثال ۳۲-۲. *(الف)* برای هر $a \in A$ ناصفر، مجموعه

$$S = \{1, a, a^2, \ldots\}$$

یک مجموعه ضربی است.

(ب) اگر $P \subset A$ یک ایده‌آل اول باشد، آنگاه $S = A \setminus P$ یک مجموعه ضربی است. به طور کلی‌تر اگر $\{P_i\}$ یک خانواده از ایده‌آل‌های اول A باشد، مجموعه ضربی $S = A \setminus \bigcup_i P_i$ را داریم.

(پ) مجموعه مقسوم‌علیه‌های صفر A یک مجموعه ضربی است. همچنین مجموعه عناصر وارون‌پذیر نیز مجموعه ضربی است.

(ت) اگر $I \subset A$ یک ایده‌آل باشد، $S = 1 + I$ یک مجموعه ضربی است.

(ث) فرض کنید $A = k[x_1, \ldots, x_n]$ *(که k یک میدان است)* و $V \subset k^n$ یک زیرمجموعه دلخواه باشد. آنگاه

$$S = \{f \in k[x_1, \ldots, x_n] \mid f(x) \neq 0 \text{ برای همه } x \in V\}$$

یک مجموعه ضربی است.

(ج) فرض کنید k یک میدان و $A = k[x]$ باشد؛ آنگاه

$$S = \{f \in k[x] \mid f \text{ در } k \text{ هیچ ریشه‌ای ندارد}\}$$

یک مجموعه ضربی است.

تعریف ۳۳-۲. فرض کنید A یک حلقه با یک مجموعه ضربی S باشد. در این صورت موضعی‌سازی A در S را به عنوان حلقه $S^{-1}A$ که به صورت زیر به دست می‌آید تعریف می‌کنیم.

عناصر $S^{-1}A$ زوج‌های $(a,s) \in A \times S$ به پیمانه رابطه هم‌ارزی زیر هستند.
دو زوج (a,s) و (b,t) هم‌ارز هستند اگر $u \in S$ وجود داشته باشد به طوری که

$$atu = bsu.$$

نمی‌توانیم از u صرف‌نظر کنیم مگر اینکه A یک دامنه صحیح باشد. کلاس هم‌ارزی (a,s) را با a/s نشان می‌دهیم. جمع و ضرب را در $S^{-1}A$ با قواعد زیر تعریف می‌کنیم:

$$a/s + b/t = (at+bs)/(st), \quad a/s \cdot b/t = (ab)/(st).$$

بررسی این که عمل‌ها خوش‌تعریف‌اند ساده است، بنابراین $S^{-1}A$ به یک حلقه جابجایی، با یک ۱/۱، تبدیل می‌شود.
به واسطه ساختار، یک هم‌ریختی طبیعی

$$\iota : A \to S^{-1}A$$

داریم که a را به $a/1$ می‌فرستد. به طور کلی این هم‌ریختی یک‌به‌یک نیست: در واقع

$$\ker \iota = \{a \in A \mid \exists u \in S \quad au = 0\}.$$

بنابراین ι زمانی یک‌به‌یک است که S شامل هیچ مقسوم‌علیه صفری نباشد. در این حالت به خودمان اجازه می‌دهیم که $\iota(a) = a/1$ را با a نشان دهیم. وقتی می‌خواهیم S را در نمادگذاری یادآوری کنیم، می‌نویسیم $\iota = \iota_S$، یا حتی $\iota = \iota_P$ اگر $S = A \setminus P$.

یک نمادگذاری برای $S^{-1}A$ داریم. وقتی $S = \{a^n, n \geq 0\}$، می‌نویسیم $S^{-1}A = A_a$.

وقتی $S = A \setminus P$، که P یک ایده‌آل اول است، قرار می‌دهیم $S^{-1}A = A_P$. این مهم‌ترین حالت موضعی‌سازی است.

در نهایت وقتی S مجموعه مقسوم‌علیه‌های صفر باشد، قرار می‌دهیم $S^{-1}A = \mathcal{F}(A)$ و آن را حلقه کسرهای کلی A می‌نامیم. اگر A یک دامنه صحیح باشد، آنگاه $S = A \setminus \{0\}$ و $\mathcal{F}(A)$ یک میدان است که آن را میدان کسرهای A می‌نامیم.

تبصره ۲-۳۴. هر موضعی‌سازی از یک دامنه صحیح A در میدان $\mathcal{F}(A)$ قرار دارد، بنابراین خودش نیز یک دامنه صحیح است.

ویژگی جهانی زیر از تعریف به دست می‌آید:

گزاره ۲-۳۵. فرض کنید $f : A \to B$ یک هم‌ریختی از حلقه‌ها و $S \subset A$ یک مجموعه ضربی باشد به طوری که $f(S) \subset B^*$. در این صورت یک هم‌ریختی یکتا $\hat{f} : S^{-1}A \to B$ وجود دارد به طوری که $f = \hat{f} \circ \iota$.

پس $S^{-1}A$ به همراه نگاشت ι برای چنین هم‌ریختی‌هایی جهانی است. ایده‌آل‌ها تحت موضعی‌سازی رفتار خوبی دارند.

تعریف ۳۶-۲. حلقه A را موضعی می‌نامیم هرگاه فقط یک ایده‌آل ماکسیمال داشته باشد. A را نیمه‌موضعی می‌نامیم هرگاه تعداد متناهی ایده‌آل ماکسیمال داشته باشد. یک حلقه موضعی A با ایده‌آل ماکسیمال M را گاهی با زوج (A, M) نشان می‌دهیم.

گزاره ۳۷-۲. فرض کنید A یک حلقه و $S \subset A$ یک مجموعه ضربی باشد. در این صورت

(i) برای هر ایده‌آل $I \subset S^{-1}A$، I توسط $\iota(\iota^{-1}(I))$ تولید می‌شود؛ به ویژه هر ایده‌آل $S^{-1}A$ توسیع یک ایده‌آل از A است.

(ii) برای هر ایده‌آل $I \subset A$ داریم
$$\iota^{-1}(I \cdot S^{-1}A) = \bigcup_{s \in S} (I : s).$$

(iii) ایده‌آل $I \cdot S^{-1}A$ کل $S^{-1}A$ است اگر و تنها اگر $I \cap S \neq \emptyset$.

اثبات. (i) قرار دهید
$$J := \iota^{-1}(I) \cdot S^{-1}A.$$
شمول $J \subset I$ بدیهی است. برعکس، فرض کنید $a/s \in I$. در این صورت $a \in \iota^{-1}(I)$، پس $a/s \in J$.

(ii) قرار دهید
$$J := \iota^{-1}(I \cdot S^{-1}A)$$
ابتدا ثابت می‌کنیم که $(I : s) \subset J$ برای هر $s \in S$. در واقع فرض کنید $a \in (I : s)$، پس $as \in I$. در این صورت
$$a \in \iota^{-1}\left(\frac{as}{s}\right) \subset J.$$
حال فرض کنید $a \in J$؛ یعنی $a/1 = b/s$ برای برخی $b \in I$، $s \in S$. بنابراین $u \in S$ وجود دارد به طوری که
$$asu = bu \in I.$$
این نشان می‌دهد که $a \in (I : su)$.

(iii) ایده‌آل $I \cdot S^{-1}A$ بدیهی است اگر و تنها اگر 1 را شامل باشد. این معادل است با $i/s = 1$ برای برخی $i \in I$ و $s \in S$، که به معنای $iu = su$ برای برخی $u \in S$ است. در نهایت، این به معنای $iu = su \in I \cap S$ است.
□

مثال ۳۸-۲. در حلقه $\mathbb{Z}_{(2)}$، ایده‌آل‌های $\langle 2 \rangle$ و $\langle 6 \rangle$ از $\mathbb{Z}$ به یک ایده‌آل واحد توسیع می‌یابند؛ زیرا 3 پس از موضعی‌سازی وارون‌پذیر می‌شود.

نتیجه ۳۹-۲. فرض کنید A یک حلقه و $S \subset A$ یک مجموعه ضربی باشد. یک تناظر دوسویی بین ایده‌آل‌های اول $S^{-1}A$ و ایده‌آل‌های اول A که با S اشتراک ندارند وجود دارد.

اثبات. نشان می‌دهیم که اگر $P \subset A$ اول باشد، آنگاه $P = \iota^{-1}(P \cdot S^{-1}A)$. داریم

$$\iota^{-1}(P \cdot S^{-1}A) = \bigcup_{s \in S} (P : s)$$

و $(P : s) = P$ برای هر $s \in S$؛ زیرا P اول است و $s \notin P$. □

یادآور می‌شویم که $N(A)$ ایده‌آل تشکیل شده از عناصر پوچ‌توان A است.

گزاره ۴۰-۲. رادیکال پوچ $N(A)$ از A، اشتراک همه ایده‌آل‌های اول A است.

اثبات. فرض کنید P یک ایده‌آل اول باشد و $a \in N(A)$. در این صورت توانی $a^n = 0 \in P$، بنابراین $a \in P$. این یک طرف شمول را اثبات می‌کند.

برای طرف دیگر، فرض کنید a در یک ایده‌آل اول قرار دارد. در این صورت A_a حلقه‌ای بدون ایده‌آل اول است؛ یعنی A_a باید حلقه صفر باشد. سپس $\iota(1) = 0$ به معنای $1 \cdot a^n = 0$ برای برخی n. بنابراین a پوچ‌توان است. □

نتیجه ۴۱-۲. فرض کنید I یک ایده‌آل از A باشد. در این صورت $\sqrt{I}$ اشتراک همه ایده‌آل‌های اولی است که I را شامل می‌شوند.

گزاره ۴۲-۲. فرض کنید S یک مجموعه ضربی و $I \subset A$ یک ایده‌آل باشد به طوری که $I \cap S = \emptyset$. در این صورت یک‌ریختی طبیعی بین $S^{-1}A/S^{-1}I$ و $T^{-1}(A/I)$ وجود دارد، که در آن T تصویر S درون A/I است.

اثبات. واضح است که T یک مجموعه ضربی است. هسته ترکیب نگاشت‌های طبیعی

$$A \to S^{-1}A \to S^{-1}A/S^{-1}I$$

برابر است با $\iota^{-1}(S^{-1}I) = I$. بنابراین یک هم‌ریختی یک‌به‌یک

$$A/I \to S^{-1}A/S^{-1}I$$

داریم. از آن‌جا که این T را به عناصر وارون‌پذیر می‌فرستد، ویژگی جهانی موضعی‌سازی یک هم‌ریختی

$$\phi : T^{-1}(A/I) \to S^{-1}A/S^{-1}I$$

را نتیجه می‌دهد. برعکس، ترکیب

$$A \to A/I \to T^{-1}(A/I)$$

را در نظر بگیرید. این S را به عناصر وارون‌پذیر می‌فرستد، بنابراین یک هم‌ریختی

$$S^{-1}A \to T^{-1}(A/I)$$

به دست می‌آوریم، که هسته آن $S^{-1}I$ را شامل می‌شود. بنابراین یک نگاشت در جهت دیگر

$$\psi : S^{-1}A/S^{-1}I \to T^{-1}(A/I)$$

داریم.

بررسی این که ϕ و ψ وارون یکدیگر هستند واضح است. □

نتیجه ۴۳-۲. فرض کنید $P \subset A$ یک ایده‌آل اول باشد. در این صورت میدان کسرهای دامنه صحیح A/P به طور کانونی با A_P/PA_P (یعنی خارج‌قسمت حلقه موضعی A_P توسط ایده‌آل ماکسیمال آن)، یک‌ریخت است.

تعریف ۴۴-۲. فرض کنید $P \subset A$ یک ایده‌آل اول باشد. میدان

$$k(P) = \mathcal{F}(A/P) = A_P/PA_P$$

میدان مانده[۴] A در P نامیده می‌شود.

تعریف ۴۵-۲. فرض کنید A یک حلقه، S یک مجموعه ضربی و M یک Aـ مدول باشد. در این صورت $S^{-1}A$ـ مدول $S^{-1}M$ را به صورت زیر تعریف می‌کنیم. عناصر $S^{-1}M$ زوج‌های $(m,s) \in M \times S$ هستند. زوج‌های (m,s) و (n,t) هم‌ارز هستند وقتی $u \in S$ وجود داشته باشد به طوری که

$$mtu = nsu.$$

کلاس هم‌ارزی (m,s) با m/s نشان داده می‌شود. همانند حالت حلقه‌ها، یک هم‌ریختی از Aـ مدول‌ها

$$\iota_M : M \to S^{-1}M$$

داریم که با $\iota_M(m) = m/1$ داده می‌شود.

گزاره ۴۶-۲. فرض کنید M یک Aـ مدول باشد.

(i) برای هر زیرمدول $N \subset S^{-1}M$، N توسط $\iota(\iota^{-1}(N))$ تولید می‌شود؛ به ویژه هر زیرمدول $S^{-1}M$ توسیع یک زیرمدول از M است.

(ii) برای هر زیرمدول $N \subset M$ داریم

$$\iota^{-1}(S^{-1}N) = \bigcup_{s \in S} (N : s).$$

[۴] Residue Field

در اینجا $S^{-1}N$ توسیع N در $S^{-1}M$ را نشان می‌دهد؛ یعنی $S^{-1}A$ـزیرمدول تولید شده توسط N. زیرمدول $(N : s)$ با

$$(N : s) := \{m \in M \mid ms \in N\}$$

تعریف می‌شود.

گزاره ۴۷-۲. موضعی‌سازی مدول‌ها دنباله‌های دقیق را حفظ می‌کند.

اثبات. فرض کنید

$$\cdots \to M_{n-1} \xrightarrow{\alpha_{n-1}} M_n \xrightarrow{\alpha_n} M_{n+1} \to \cdots$$

یک دنباله دقیق از Aـمدول‌ها باشد. در این صورت یک دنباله القا شده از $S^{-1}A$ـمدول‌ها داریم:

$$\cdots \to S^{-1}M_{n-1} \xrightarrow{\alpha_{n-1}} S^{-1}M_n \xrightarrow{\alpha_n} S^{-1}M_{n+1} \to \cdots .$$

درستی در M_n را بررسی می‌کنیم. ابتدا برای هر $m/s \in M_{n-1}$ داریم

$$\alpha_n(\alpha_{n-1}(m/s)) = \alpha_n(\alpha_{n-1}(m))/s = 0.$$

برعکس، فرض کنید $m/s \in M_n$ و $\alpha_n(m/s) = \alpha_n(m)/s = 0$. در این صورت $u \in S$ وجود دارد به طوری که

$$\alpha_n(um) = u\alpha_n(m) = 0.$$

پس $um = \alpha_{n-1}(m')$ برای برخی $m' \in M_{n-1}$ داریم و در نهایت $m/s = \alpha_{n-1}(m'/(su))$. □

گزاره ۴۸-۲. فرض کنید M یک Aـمدول باشد و $m \in M$. در این صورت $m = 0$ اگر و تنها اگر $\iota_P(m) = 0 \in M_P$ برای هر ایده‌آل ماکسیمال $P \subset A$.

اثبات. یک سوی اثبات بدیهی است. برای سوی دیگر فرض کنید $\iota_P(m) = 0$ برای هر ایده‌آل‌های ماکسیمال $P \subset A$؛ یعنی برای هر چنین P، $s \notin P$ پیدا می‌کنیم به طوری که $sm = 0$. به عبارت دیگر، ایده‌آل $\mathrm{Ann}(m)$ در هیچ ایده‌آل ماکسیمالی قرار ندارد، بنابراین باید کل A باشد. □

نتیجه ۴۹-۲. فرض کنید M یک Aـمدول باشد. در این صورت $M = 0$ اگر و تنها اگر $M_P = 0$ برای هر ایده‌آل ماکسیمال $P \subset A$.

نتیجه ۵۰-۲. فرض کنید $f : M \to N$ یک هم‌ریختی Aـمدول باشد. در این صورت f یک‌به‌یک است اگر و تنها اگر هم‌ریختی القا شده $f_P : M_P \to N_P$ یک‌به‌یک باشد برای هر ایده‌آل ماکسیمال $P \subset A$.

۵.۲ حلقه‌های نوتری

یکی از پرکاربردترین مفاهیم در جبر جابجایی، مفهوم «شرایط زنجیره‌ای» است که در قالب حلقه‌های نوتری تجلی می‌یابد. این حلقه‌ها، که نام خود را از ریاضیدان برجسته آلمانی، امی نوتر، گرفته‌اند، ساختارهایی هستند که از یک «خوبی» جبری بنیادین برخوردارند؛ به این معنا که هر زنجیره صعودی از ایده‌آل‌هایشان، پس از مراحل متناهی، ثابت می‌ماند.

این شرط به ظاهر ساده، که به «شرایط زنجیره‌ای صعودی[۵]» معروف است، پیامدهای ساختاری مهمی به همراه دارد. در حقیقت، می‌توان نشان داد که این شرط با این ویژگی هم‌ارز است که هر ایده‌آل در این حلقه‌ها، متناهی‌تولید است. این ویژگی، امکان استقرای ریاضی و استدلال‌های ترکیباتی را روی ایده‌آل‌ها فراهم می‌سازد و حلقه‌های نوتری را به ابزاری قدرتمند برای مطالعه مسائل پیچیده جبری بدل می‌کند.

اهمیت حلقه‌های نوتری تنها به تعریف زیبای آن محدود نمی‌شود. بسیاری از مهم‌ترین حلقه‌ها در ریاضیات، مانند حلقه اعداد صحیح، حلقه‌های چندجمله‌ای و حلقه‌های موضعی به‌دست‌آمده از هندسه جبری، همگی در رده حلقه‌های نوتری قرار می‌گیرند. این امر، دامنه نفوذ و کاربرد این مفهوم را از نظریه اعداد تا هندسه جبری گسترده می‌سازد.

در این بخش، به بررسی نظام‌مند حلقه‌های نوتری خواهیم پرداخت. ابتدا تعاریف پایه و چندین شرط هم‌ارز را ارائه کرده، سپس به مطالعه رفتار این حلقه‌ها تحت عملیات جبری مختلف مانند تقسیم حلقه‌ها و توسعه‌های متناهی می‌پردازیم. در نهایت، با معرفی و اثبات قضیه بنیادی هیلبرت، که تضمین می‌کند حلقه چندجمله‌ای بر روی یک حلقه نوتری، خود نوتری است، این بخش را به پایان خواهیم برد. هدف از این بخش، تجهیز خواننده به ابزارهای ضروری برای درک ساختار حلقه‌های نوتری و کاربردهای گسترده آن در شاخه‌های مختلف ریاضیات است.

تعریف ۵۱-۲. حلقه R را نوتری گوییم هرگاه هر زنجیر صعودی $I_1 \subset I_2 \subset \dots$ از ایده‌آل‌های R ایستا باشد؛ یعنی $I_N = I_{N+1} = \dots$ برای یک $N \in \mathbb{N}$. به عبارت دیگر اگر هر ایده‌آل در حلقه R متناهی تولید باشد، R را نوتری می‌نامیم.

تعریف ۵۲-۲. فرض کنید R یک حلقه باشد و $f = a_n x^n + \dots + a_0$ یک چندجمله‌ای 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 f می نامیم و با نمادهای $\mathrm{LT}(f)$، $\mathrm{LM}(f)$ و $\mathrm{LC}(f)$ نمایش می‌دهیم.

قضیه ۵۳-۲ (پایه‌ای هیلبرت)**.** اگر R یک حلقه نوتری باشد، آنگاه $R[x]$ هم نوتری است.

اثبات. فرض کنید I یک ایده‌آل در $R[x]$ باشد. برای هر $n \geq 0$، قرار دهید :

$$I_n = \{\mathrm{LC}(f) \mid f \in I, \mathrm{LM}(f) = x^n\} \cup \{0\}$$

با توجه به اینکه I یک ایده‌آل است، به سادگی مشاهده می‌شود که برای هر n، I_n یک ایده‌آل است و $I_1 \subset I_2 \subset \dots$. با توجه به اینکه R نوتری است، یک عدد طبیعی مانند N وجود دارد که $I_N = I_{N+1} = \dots$. از طرفی برای هر $0 \geq i \geq N$، هر ایده‌آل I_i مولدی متناهی مانند B_i دارد. توجه کنید که برای هر $a \in B_i$، چند جمله‌ای $f_a \in I$ موجود

[۵] ACC

است که $\mathrm{LT}(f_a) = ax^i$. قرار دهید $B = B_0 \cup \ldots \cup B_N$. ادعا می‌کنیم که $I = \langle f_a \mid a \in B \rangle$. کافیست ثابت کنیم هر $f \in I$ توسط چندجمله‌های متناظر B ساخته می‌شود.این رابطه را با استقرا روی درجه f ثابت می‌کنیم. اگر $\deg(f) = 0$، آنگاه $f \in I_0$. چون I_0 توسط B_0 تولید می‌شود، پس $f \in \langle f_a \mid a \in B \rangle$. حال فرض کنید $\deg(f) = i$ و حکم برای هر $j < i$ برقرار باشد و همچنین فرض کنید $\mathrm{LT}(f) = bx^i$. ابتدا فرض کنید $0 \leq i \leq N$. بنابراین $b \in I_i$. طبق فرض، b توسط عناصر B_i تولید می‌شود و در نتیجه $b = \sum_{a \in B_i} r_a a$ که $r_a \in R$. حال چندجمله‌ای $f - \sum_{a \in B_i} r_a f_a$ را در نظر بگیرید. با توجه به اینکه $\mathrm{LT}(f) = bx^i$ و $\mathrm{LT}(f - \sum_{a \in B_i} r_a f_a) = bx^i$. بنابراین درجه $f - \sum_{a \in B_i} r_a f_a$ کمتر از i است. بنابراین طبق فرض استقرا داریم :

$$f - \sum_{a \in B_i} r_a f_a \in \langle f_a \mid a \in B \rangle .$$

با توجه به اینکه $B_i \subset B$، پس حکم موردنظر برای هر $0 \leq i \leq N$ برقرار است. حال فرض کنید $i > N$ و $LT(f) = bx^i$. با توجه به اینکه $b \in B_N$ و $I_i = I_N$، بنابراین $b = \sum_{a \in B_N} r_a a$. حال چندجمله‌ای $f - \sum_{a \in B_N} r_a x^{i-N} f_a$ را درنظر بگیرید. با تکرار روند بالا، به راحتی مشاهده می‌شود که درجه این چندجمله‌ای کمتر از i است و در نتیجه با استفاده از فرض استقرا، $f \in \langle f_a \mid a \in B \rangle$. □

نتیجه ۵۴-۲. اگر R یک حلقه نوتری باشد، آنگاه $R[x_1, \ldots, x_n]$ هم نوتری است.

اثبات. اگر K یک میدان باشد، تنها ایده‌آل‌های آن $\{0\}$ و K هستند. پس K یک حلقه نوتری است. □

نتیجه ۵۵-۲. اگر K یک میدان باشد، آنگاه $K[x_1, \ldots, x_n]$ نوتری است.

لم ۵۶-۲. فرض کنید R یک حلقه نوتری باشد. در این صورت هر مجموعه مولد یک ایده‌آل، شامل یک مجموعه مولد متناهی برای ایده‌آل است.

اثبات. فرض کنید $S \subset R$ و $I = \langle S \rangle$. نشان می‌دهیم زیرمجموعه‌ای متناهی از S موجود است که I را تولید می‌کند. $a_0 \in S$ را در نظر بگیرید. اگر $I = \langle a_0 \rangle$ آنگاه حکم مورد نظر برقرار است. در غیر این صورت $a_1 \in S \setminus \langle a_0 \rangle$ وجود دارد. اگر $I = \langle a_0, a_0 \rangle$ حکم ثابت می‌شود. در غیر این صورت $a_2 \in S \setminus \langle a, a_0 \rangle$ وجود دارد. اگر این روند ادامه پیدا کند، زنجیر صعودی $\ldots \subsetneq \langle a_0, a_1, a_2 \rangle \subsetneq \langle a_0, a_1 \rangle \subsetneq \langle a_0 \rangle$ را خواهیم داشت که ایستا نیست که در تناقض با نوتری بودن R است. در نتیجه این روند متوقف می‌شود و یک زیرمجموعه متناهی از S، I را تولید می‌کند. □

۶.۲ حلقه‌های اقلیدسی

در جستجو برای تعمیم و انتزاع مفاهیم بنیادی، ریاضیات اغلب ساختارهای آشنا را در قالب‌های عمومی‌تر بازمی‌یابد. یکی از درخشان‌ترین این تعمیم‌ها، مفهوم حلقه‌های اقلیدسی است. این حلقه‌ها، که نام خود را از الگوریتم مشهور اقلیدس برای یافتن بزرگ‌ترین مقسوم‌علیه‌مشترک گرفته‌اند، تعمیمی طبیعی از ساختار اعداد صحیح به دنیای گسترده‌تر جبر مجرد هستند. در این بخش، به مطالعه دقیق این حلقه‌های مهم خواهیم پرداخت. ابتدا تعریف رسمی و چندین مثال کلیدی، از

جمله حلقه اعداد صحیح و حلقه چندجمله‌ای‌ها بر روی یک میدان را بررسی می‌کنیم. سپس به رابطه سلسله‌مراتبی بین حلقه‌های اقلیدسی، دامنه‌های ایده‌آل اصلی و دامنه‌های تجزیه یکتا خواهیم پرداخت و نشان خواهیم داد که چگونه الگوریتم اقلیدسی منجر به ایجاد این ساختارهای غنی می‌گردد. هدف نهایی، درک عمیق‌تر این کلاس از حلقه‌ها و ابزار قدرتمندی است که برای تحلیل ساختاری آن‌ها در اختیار ما قرار می‌دهند.

تعریف ۵۷-۲. فرض کنید A یک دامنه صحیح باشد. می‌گوییم A یک دامنه اقلیدسی است هرگاه تابعی

$$N\colon A \setminus \{0\} \to \mathbb{N},$$

وجود داشته باشد، که یک نُرم نامیده می‌شود، به طوری که:

(۱) برای هر a, b ناصفر در A،

$$N(a) \leq N(ab);$$

(۲) برای هر $a, b \in A$ که $b \neq 0$، $q, r \in A$ وجود دارند به طوری که

$$a = qb + r$$

و یا $r = 0$ یا $N(r) < N(b)$.

به طور خلاصه حلقه‌های اقلیدسی، حلقه‌هایی هستند که در آن‌ها می‌توانیم تقسیم با باقی‌مانده انجام دهیم، به گونه‌ای که باقی‌مانده «کوچک‌تر» از مقسوم‌علیه باشد. بر خلاف الگوریتم اقلیدسی برای اعداد صحیح، منحصر به فرد بودن تجزیه $a = qb + r$ را، حتی در حد عناصر وارون‌پذیر، همیشه در دست نداریم. عناصر وارون‌پذیر A دقیقاً همان‌هایی هستند که نُرم کمینه را دارند. در واقع، شرط اول بیان می‌کند $N(1) \leq N(b)$ برای هر b ناصفر در A. بنابراین $m = N(1)$ کمینه نُرم ممکن است. اگر $a \in A$ یکه باشد، آنگاه $N(a) \leq N(aa^{-1}) = m$، بنابراین $N(a) = m$.

برعکس، فرض کنید $N(a) = m$. در این صورت بنابر خاصیت تقسیم $q, r \in A$ وجود دارند به طوری که

$$1 = qa + r;$$

از آن‌جایی که نمی‌توانیم داشته باشیم $N(r) < N(a)$، باید $r = 0$؛ یعنی a وارون‌پذیر است.

مثال ۵۸-۲. حلقه $\mathbb{Z}$ با نُرم همان قدر مطلق، یک دامنه اقلیدسی است:

$$N(n) = |n|.$$

مثال ۵۹-۲. برای هر میدان k، حلقه $k[x]$ یک دامنه اقلیدسی است. برای نُرم می‌توانیم $N(f) = \deg(f)$ را در نظر بگیریم؛ تقسیم در این حلقه، همان تقسیم معمول بین چندجمله‌ای‌ها است.

مثال ۶۰-۲. حلقه $\mathbb{Z}[i]$ یک دامنه اقلیدسی است. در اینجا نُرم، مربع اندازه برای اعداد مختلط است؛ یعنی

$$N(a+ib) = a^۲ + b^۲.$$

فرض کنید $z, w \in \mathbb{Z}[i]$ و خارج قسمت $u = z/w \in \mathbb{C}$ را در نظر بگیرید. اگر $u \in \mathbb{Z}[i]$، آنگاه به سادگی می‌توان تقسیم در این حلقه را مشاهده کرد. در غیر این صورت u در درون یک مربع ۱×۱ با مختصات صحیح قرار دارد. فرض کنید q نزدیک‌ترین رأس این مربع باشد و r را به صورت

$$r = z - qw$$

تعریف کنید. در این صورت $N(r) = N((u-q)w) < N(w)$ زیرا اندازه $u-q$ کمتر از ۱ است.

توجه کنید که در این مثال ممکن است رأس‌های دیگری نیز کارساز باشند، بنابراین هیچ نوع منحصر به فردی نداریم.

مثال ۶۱-۲. حلقه $k[[x]]$ نیز یک دامنه اقلیدسی است. برای یک سری توانی $a(x)$، $N(a)$ را درجه اولین تک جمله‌ای ناصفر قرار می‌دهیم؛ یعنی اگر

$$a(x) = x^t a_۱(x)$$

که $a_۱(۰) \neq ۰$، آنگاه $N(a) = t$. شرط اول به وضوح برقرار است. برای وجود تقسیم، هر دو سری توانی $a(x), b(x)$ با $b \neq ۰$ را در نظر بگیرید. اگر $N(a) \geq N(b)$، قرار می‌دهیم

$$a(x) = x^{N(a)} a_۱(x),$$
$$b(x) = x^{N(b)} b_۱(x),$$

پس می‌توانیم a را بر b تقسیم کنیم به طوری که

$$q(x) = x^{N(a)-N(b)} a_۱(x) b_۱(x)^{-۱}, \qquad r(x) = ۰.$$

اگر $N(a) < N(b)$، فقط $q = ۰$ و $r = a$ را در نظر بگیرید.

اگر A یک دامنه اقلیدسی باشد، می‌توانیم الگوریتم اقلیدسی را انجام دهیم. با داشتن $a, b \in A$، تقسیم‌های متوالی زیر را انجام می‌دهیم:

$$a = q_۱ b + r_۱,$$
$$b = q_۲ r_۱ + r_۲,$$
$$r_۱ = q_۳ r_۲ + r_۳,$$
$$\vdots$$

تا جایی که $r_n = ۰$. این باید در تعداد متناهی مرحله رخ دهد؛ زیرا

$$N(b) > N(r_۱) > N(r_۲) > \cdots$$

یک دنباله نزولی از اعداد طبیعی است. بنابراین یک مرحله آخر داریم

$$r_{n-۲} = q_n r_{n-۱}.$$

با استقرا می‌بینیم که $r_{n-۱}$ هر دو a و b را عاد می‌کند. با معکوس کردن مراحل، مشاهده می‌کنیم که

$$\begin{aligned} r_{n-۱} &= r_{n-۳} - q_{n-۱} r_{n-۲} \\ &= r_{n-۳} - q_{n-۱}(r_{n-۴} - q_{n-۲} r_{n-۳}) = \cdots = xa + yb \end{aligned}$$

برای $x, y \in A$. بنابراین اگر c هر دو a و b را عاد کند، باید $r_{n-۱}$ را نیز عاد کند. در این حالت می‌گوییم $r_{n-۱}$ یک بزرگ‌ترین مقسوم‌علیه مشترک بین a و b است. $r_{n-۱} = xa + yb$، رابطه بزو نامیده می‌شود.

گزاره ۶۲-۲. فرض کنید A یک دامنه اقلیدسی باشد. در این صورت هر ایده‌آل در A اصلی است.

اثبات. فرض کنید $I \subset A$ یک ایده‌آل و $a \in I$ ناصفر با نُرم کمینه باشد؛ برای مثال $m = N(a)$. اگر $b \in I$، قرار دهید

$$b = qa + r;$$

از آنجا که نمی‌توانیم داشته باشیم $N(r) < m$، باید $r = ۰$، یعنی $b \in (a)$. □

۷.۲ الگوریتم تقسیم

هر دانشجوی ریاضی از نخستین روزهای آشنایی با حساب، با مفهوم ساده اما عمیق «تقسیم» آشنا می‌شود: فرآیندی که به ما می‌آموزد چگونه هر عدد صحیح را می‌توان به صورت $a = bq + r$ نوشت، به طوری که باقیمانده r عددی نامنفی و کوچک‌تر از b باشد. این فرآیند که در هسته آموزش‌های ابتدایی ریاضی قرار دارد، در واقع تجلی یک اصل ساختاری بسیار قدرتمند است که در شاخه‌های مختلف جبر مجرد تعمیم می‌یابد. این اصل، الگوریتم تقسیم نامیده می‌شود.

اهمیت الگوریتم تقسیم فراتر از یک روش محاسباتی ساده است؛ این الگوریتم سنگ بنای بسیاری از مفاهیم پیشرفته‌تر در جبر است. وجود این الگوریتم در یک ساختار جبری (مانند حلقه‌های اقلیدسی)، تضمین‌کنندهٔ خواص ساختاری بسیار مطلوبی است. برای نمونه، حلقهٔ اعداد صحیح و حلقهٔ چندجمله‌ای‌ها بر روی یک میدان، که از مهم‌ترین حلقه‌ها در ریاضیات محض و کاربردی هستند، هر دو از الگوریتم تقسیم بهره می‌برند.

قضیه ۶۳-۲ (الگوریتم تقسیم در اعداد صحیح). فرض کنید m و n دو عدد صحیح باشند به طوری که $n \neq ۰$. در این صورت اعداد صحیح و یکتای q و r موجودند که $m = nq + r$ و $۰ \leq r < |n|$. q را خارج‌قسمت و r را باقیمانده تقسیم m بر n گوییم.

اثبات. قرار دهید $S = \{m - tn \geq ۰ \mid t \in \mathbb{Z}\}$. اگر $m \geq ۰$، آنگاه با قرار دادن $t = ۰$ داریم $m \in S$ و اگر $m < ۰$ آنگاه با قرار دادن $t = mn$ و با توجه به اینکه $۰ \leq n^۲ - ۱$ داریم :

$$m - tn = m - mn^۲ = m(۱ - n^۲) \geq ۰$$

و $m - tn \in S$. پس S زیرمجموعه‌ای ناتهی از مجموعه اعداد طبیعی است و بنابر اصل خوش‌ترتیبی اعداد طبیعی، دارای کوچکترین عضو مانند r است. بنابراین عدد صحیح q وجود دارد که $m = nq + r$. کافیست ثابت کنیم $r < |n|$. فرض کنید $r \leq |n|$ (برهان خلف). پس $r - |n| \leq ۰$ و

$$r - |n| = m - nq - (\pm n) = m - (q + (\pm ۱))n \in S \text{ ،} r - |n| < r$$

که در تناقض با انتخاب r به عنوان کوچکترین عضو S است. برای اثبات یکتایی q و r فرض کنید

$$m = nq_۱ + r_۱ = nq_۲ + r_۲ \quad \text{،} ۰ \leq r_۱ \text{ ،} r_۲ < |n|.$$

پس $|n| > r_۱ \geq ۰$ و $۰ \geq -r_۲ > -|n|$. در نتیجه $|n| > r_۱ - r_۲ > -|n|$ و $|n| > |r_۱ - r_۲|$. از طرفی داریم $r_۱ - r_۲ = n(q_۲ - q_۱)$. حال اگر $q_۱ \neq q_۲$، آنگاه $|r_۱ - r_۲| \geq |n|$ که یک تناقض است. پس $q_۱ = q_۲$ و $r_۱ = r_۲$. □

حال الگوریتم زیر را برای محاسبه خارج‌قسمت و باقیمانده تقسیم در $\mathbb{Z}$ بیان می‌کنیم که در آن منظور از $[x]$ جزء صحیح x است.

قضیه ۶۴-۲. الگوریتم ۱ پایان‌پذیر است و خروجی آن، شرایط مورد نظر را برآورده می‌کند.

اثبات. ابتدا پایان‌پذیری الگوریتم را بررسی می‌کنیم. برای هر عدد صحیح x داریم $|[\frac{x}{۲}]| \leq |x| - ۱$، بنابراین بعد از حداکثر $|x|$ بار فراخوانی الگوریتم، به صفر خواهیم رسید و در نتیجه الگوریتم پایان‌پذیر خواهد بود. برای اثبات درستی الگوریتم، x را نامنفی در نظر می‌گیریم و در حالتی که x منفی باشد، اثبات مشابه خواهد شد. اگر $x = ۰$، آنگاه واضح است که $q = r = ۰$. در غیر این صورت، فرض کنیم q و r به ترتیب خارج‌قسمت و باقیمانده تقسیم $[\frac{x}{۲}] = qy + r$. دو حالت زیر را در نظر بگیرید :
(۱) اگر x زوج باشد، آنگاه $\frac{x}{۲} = qy + r$. در نتیجه $x = ۲qy + ۲r$. در این صورت قرار می‌دهیم $q' = ۲q$ و $r' = ۲r$.
(۲) اگر x فرد باشد، آنگاه $\frac{x-۱}{۲} = qy + r$. پس $x = ۲qy + ۲r + ۱$. در این حالت قرار می‌دهیم $q' = ۲q$ و $r' = ۲r + ۱$.
بنابراین می‌توان نوشت $x = q'y + r'$. حال اگر $r' < y$، آنگاه q' و r' به ترتیب خارج‌قسمت و باقیمانده تقسیم x بر y است. در غیر این صورت داریم

$$x = q'y + r' - y + y = (q' + ۱) + (r' - y) = q'y + r'.$$

از طرفی می‌دانیم $۰ \leq r < y$. پس $۰ \leq ۲r < ۲y$ و $۰ \leq ۲r + ۱ < ۲y$. بنابراین $y \leq r' \leq ۲y$ و $۰ \leq r' - y < y$. در نتیجه خارج‌قسمت و باقیمانده تقسیم x بر y به ترتیب $q' + ۱$ و $r' - y$ است و اثبات درستی الگوریتم به پایان می‌رسد. □

Procedure ۱ Division in $\mathbb{Z}$

Input: Two integers x and y, $y \geq 1$

Output: The quotient and the remainder of the division of x by y

if $x = 0$ **then**
  return $(0, 0)$;
end if;
$(q, r) :=$ Division $\mathbb{Z}([\frac{x}{2}], y)$
$q := 2q$
if $2 \nmid x$ **then**
  $r := 2r + 1$
else
  $r := 2r$
end if;
if $r \geq y$ **then**
  $r := r - y$
  $q := q + 1$
end if;
return (q, R);
end;

قضیه ۶۵-۲ (الگوریتم تقسیم برای چندجمله‌ای‌های تک متغیره). فرض کنید K یک میدان باشد، f و g دو چندجمله‌ای در $K[x]$ باشند و $g \neq 0$. در این صورت چندجمله‌ای‌های یکتای $q, r \in K[x]$ وجود دارند به طوری که $f = qg + r$ و $r = 0$ یا $\deg(r) < \deg(g)$.

اثبات. ابتدا ثابت می‌کنیم چندجمله‌ای‌های q و r با این ویژگی وجود دارند. قرار می‌دهیم $S = \{f - qg \mid q \in K[x]\}$. اگر $0 \in S$، آنگاه $q \in K[x]$ وجود دارد که $f = qg$. در این صورت قرار می‌دهیم $r = 0$ و حکم مورد نظر ثابت می‌شود. در غیر این صورت، قرار می‌دهیم $A = \{\deg(p) \mid p \in S\}$. مجموعه A زیرمجموعه‌ای از اعداد طبیعی است و بنا بر اصل خوش ترتیبی، A دارای کوچکترین عضو مانند m است. بنابراین چندجمله‌ای $r \in S$ وجود دارد که $\deg(r) = m$. پس چندجمله‌ای $q \in K[x]$ وجود دارد که $r = f - qg$ یا به طور معادل $f = qg + r$. حال کافیست ثابت کنیم

$\deg(r) < \deg(g)$. (فرض خلف) فرض کنید $\deg(r) \geq \deg(g)$ و

$$r = a_m x^m + \ldots + a_1 x + a_0, \quad a_m \neq 0$$
$$g = b_n x^n + \ldots + b_1 x + b_0, \quad b_n \neq 0$$

که m بزرگتر یا مساوی n است. چون K یک میدان است و $b_n \neq 0$، پس وارون b_n یعنی b_n^{-1} در K وجود دارد. تعریف کنید $h = r - b_n^{-1} a_m x^{m-n} g$. حال داریم

$$h = r - b_n^{-1} a_m x^{m-n} g = f - qg - b_n^{-1} a_m x^{m-n} g = f - (q + b_n^{-1} a_m x^{m-n}) g \in S.$$

همچنین

$$\begin{aligned} h = r - b_n^{-1} a_m x^{m-n} g &= a_m x^m + \ldots + a_0 - b_n^{-1} a_m x^{m-n} (b_n x^n + \ldots + b_0) \\ &= a_m x^m + \ldots + a_0 - (a_m x^m + B) \end{aligned}$$

که B شامل جملاتی با درجه کمتر از m است. پس $\deg(h) < m$ که در تناقض با انتخاب $r \in S$ با کمترین درجه است و $\deg(r) < \deg(g)$. برای اثبات یکتایی q و r، فرض کنید $f = qg + r = q'g + r'$ که $\deg(r') < \deg(g)$. پس $(q - q')g = r' - r$. اگر $q \neq q'$، آنگاه $q - q' \neq 0$ و در نتیجه $\deg((q - q')g) \geq \deg(g)$. به طور معادل $\deg(r' - r) \geq \deg(g)$ که یک تناقض است، زیرا

$$\deg(r' - r) \leq max\{\deg(r'), \deg(r)\} < \deg(g).$$

بنابراین $q = q'$ و در نتیجه $r = r'$. □

حال الگوریتم زیر را برای محاسبه خارج‌قسمت و باقیمانده تقسیم در $K[x]$ بیان می‌کنیم.

---

۲ Procedure Division in $K[x]$

Input: $f, g \in K[x]$ where $g \neq 0$

Output: The quotient and the remainder of the division of f by g

$q := 0;\ r := f$

while $r \neq 0$ and $\mathrm{LT}(g) \mid \mathrm{LT}(r)$ **do**

$q := q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}$

$r := r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)} . g$

end while;

return (q, r);

end;

قضیه ۶۶-۲. الگوریتم ۲ پایان‌پذیر است و خروجی آن، شرایط مورد نظر را برآورده می‌کند.

اثبات. ابتدا نشان می‌دهیم که الگوریتم پایان‌پذیر است. فرض کنید q_i و r_i به ترتیب نتایج بدست آمده برای q و r در مرحله i–ام اجرای الگوریتم باشند. پس $q_۰ = ۰$ و $r_۰ = f$. (فرض خلف) فرض کنید الگوریتم پایان‌پذیر نباشد. در این صورت در مرحله i–ام اجرای الگوریتم داریم

$$r_i = a_m x^m + \ldots + a_۰, \quad g = b_n x^n + \ldots + b_۰$$

که $r_i \neq ۰$ و $m \geq n$. در نتیجه

$$r_{i+۱} = r_i - \frac{\mathrm{LT}(r_i)}{\mathrm{LT}(g)}.g = a_m x^m + \ldots + a_۰ - \frac{a_m x^m}{b_n x^n}.(b_n x^n + \ldots + b_۰)$$

به راحتی مشاهده می‌شود $\deg(r_i) > \deg(r_{i+۱})$ و دنباله $\deg(r_۰) > \deg(r_۱) > \ldots$ از اعداد طبیعی بدست می‌آید که با اصل خوش‌ترتیبی اعداد طبیعی در تناقض است. پس الگوریتم پایان‌پذیر است. برای اثبات درستی الگوریتم، با استقرا نشان می‌دهیم که برای هر i داریم $f = q_i g + r_i$. برای $i = ۰$ به وضوح حکم برقرار است. فرض کنید حکم برای مرحله i–ام درست باشد، یعنی $f = q_i g + r_i$. در این صورت

$$q_{i+۱} g + r_{i+۱} = (q_i + \frac{\mathrm{LT}(r_i)}{\mathrm{LT}(g)}).g + (r_i - \frac{\mathrm{LT}(r_i)}{\mathrm{LT}(g)}.g) = q_i g + r_i = f.$$

در پایان، با توجه به پایان‌پذیر بودن الگوریتم، $i_۰$ وجود دارد که برای آن $r_{i_۰}$ یا $\deg(r_{i_۰}) < \deg(g)$. بنابراین، $r_{i_۰}, q_{i_۰}$ به ترتیب خارج‌قسمت و باقیمانده تقسیم f بر g هستند. □

مثال ۶۷-۲. مراحل اجرای الگوریتم بالا برای چندجمله‌ای‌های $f = x^۳ + ۲x^۲ + x + ۱$ و $g = ۲x + ۱$ به صورت زیر است:

$$\longrightarrow q_۰ = ۰, \quad r_۰ = f$$
$$\longrightarrow q_۱ = \tfrac{۱}{۲}x^۲ + \tfrac{۳}{۴}x, \quad r_۲ = \tfrac{۱}{۴}x + ۱$$
$$\longrightarrow q_۲ = \tfrac{۱}{۲}x^۲ + \tfrac{۳}{۴}x + \tfrac{۱}{۸}, \quad r_۳ = \tfrac{۷}{۸}$$

بنابراین $\frac{۱}{۸} + \frac{۳}{۴}x + \frac{۱}{۲}x^۲$ و $\frac{۷}{۸}$ به ترتیب خارج‌قسمت و باقیمانده تقسیم f بر g است.

۸.۲ بزرگترین مقسوم علیه مشترک

بزرگترین مقسوم‌علیه مشترک دو عدد صحیح بزرگترین عدد صحیحی است که آن دو عدد را عاد کند. مشابه این مفهوم را برای چندجمله‌ای‌ها تعریف می‌کنیم. در این بخش، این مفهوم را در یک دامنه صحیح یادآوری و الگوریتم‌هایی را برای محاسبه آن معرفی می‌کنیم. در این بخش، R به عنوان یک دامنه صحیح در نظر گرفته شده است.

تعریف ۶۸-۲. فرض کنید $a_1, \ldots, a_n \in R$. در این صورت $d \in R$ را بزرگترین مقسوم‌علیه مشترک *(ب.م.م.)* $a_1, \ldots, a_n$ می‌نامیم هرگاه:
(۱) $d \mid a_1, \ldots, d \mid a_n$.
(۲) برای هر $r \in R$ اگر $r \mid a_1, \ldots, r \mid a_n$، آنگاه $r \mid d$.

لازم به ذکر است که در حالتی که $a_1 = \ldots = a_n = 0$ با استفاده از تعریف بالا نمی‌توان ب.م.م $a_1, \ldots, a_n$ را بدست آورد، زیرا هر عضو R صفر را عاد می‌کند. در برخی مراجع این ب.م.م. صفر تعریف می‌شود. بنابراین در ادامه این بخش، همه a_iها ناصفر در نظر گرفته شده‌اند.

گزاره ۶۹-۲. ب.م.م $a_1, \ldots, a_n \in R$ *(که آن را با نماد* $\gcd(a_1, \ldots, a_n)$ نشان می‌دهیم*)* در حد ضرب در یک عنصر وارون‌پذیر R یکتاست.

اثبات. اگر d_1 و d_2 دو ب.م.م برای a_iها باشند، آنگاه $d_2 \mid d_1$ و $d_1 \mid d_2$. پس $u, v \in R$ وجود دارند که $d_1 = ud_2$ و $d_2 = vd_1$. بنابراین $d_1 = uvd_1$ و در نتیجه $d_1(1 - uv) = 0$. با استفاده از دامنه بودن R، داریم $uv = 1$ و حکم ثابت می‌شود. □

نتیجه ۷۰-۲. اگر $d = \gcd(a_1, \ldots, a_n)$ و $u \in R$ وارون‌پذیر باشد، آنگاه ud نیز یک ب.م.م $a_1, \ldots, a_n$ است.

لازم به ذکر است که برخلاف این که برای $a_1, \ldots, a_n \in R$ ممکن است بیش از یک ب.م.م وجود داشته باشد، برای هر ب.م.م مانند d برای این عناصر از تساوی $d = \gcd(a_1, \ldots, a_n)$ استفاده می‌کنیم.

مثال ۷۱-۲. در $\mathbb{Q}(\sqrt{2})[x]$ داریم $\gcd(x, x^2) = (\sqrt{2} - 1)x$ و $\gcd(x, x^2) = x$. دقت کنید $1 + \sqrt{2}$ وارون $1 - \sqrt{2}$ در $\mathbb{Q}(\sqrt{2})$ است.

برای ارائه الگوریتم محاسبه ب.م.م دو عدد صحیح، به دو لم زیر نیاز داریم.

لم ۷۲-۲. اگر $a, b \in \mathbb{Z}$ و r باقیمانده تقسیم a بر b باشد، آنگاه $\gcd(a, b) = \gcd(b, r)$.

اثبات. بنابر الگوریتم تقسیم در $\mathbb{Z}$، عددهای صحیح q, r وجود دارند که $a = bq + r$. در ادامه، فرض کنید $d_1 = \gcd(a, b)$ و $d_2 = \gcd(b, r)$. در این صورت $d_1 \mid a$ و $d_1 \mid b$. پس $d_1 \mid r$ و بنابراین $d_1 \mid d_2$. از طرفی $d_2 \mid b$ و $d_2 \mid r$. بنابراین $d_2 \mid a = bq + r$ و در نتیجه $d_2 \mid d_1$. پس $d_1 = d_2$. □

لم ۷۳-۲. برای هر عدد صحیح a داریم $\gcd(a, 0) = a$.

اثبات. واضح است. □

الگوریتم اقلیدس برای محاسبه ب.م.م دو عدد صحیح به صورت زیر بیان می‌شود که در آن منظور از $\text{rem}(a, b)$، باقیمانده تقسیم a بر b است.

Procedure 3 Euclid in $\mathbb{Z}$

Input: $a, b \in \mathbb{Z}$ where $a \geq b \geq 0$

Output: $\gcd(a, b)$

$h := a;\ s := b$

while $s \neq 0$ **do**

$r := \mathrm{rem}(h, s)$

$h := s$

$s := r$

end while;

return (h)

end;

قضیه ۷۴-۲. الگوریتم ۳ پایان‌پذیر است و شرایط مورد نظر را برآورده می‌کند.

اثبات. ابتدا نشان می‌دهیم که الگوریتم پایان‌پذیر است. فرض کنید h_i و s_i نتایج مرحله i–ام الگوریتم باشند. در این صورت $h_۰ = a$ و $s_۰ = b$. (فرض خلف) فرض کنید الگوریتم پایان‌پذیر نباشد. می‌توان نوشت $s_{i+۱} = \mathrm{rem}(h_i, s_i)$ و برای هر i داریم $s_{i+۱} < s_i$. بنابراین دنباله نزولی $\ldots < s_۲ < s_۱ < s_۰$ اط اعداد طبیعی بدست می‌آید که با اصل خوش‌ترتیبی اعداد طبیعی در تناقض است. پس الگوریتم پایان‌پذیر است. برای اثبات درستی الگوریتم، با استقرا ثابت می‌کنیم برای هر i رابطه $\gcd(a, b) = \gcd(h_i, s_i)$ برقرار است. برای $i = ۰$ به وضوح حکم برقرار است. حال فرض کنید $\gcd(a, b) = \gcd(h_i, s_i)$. در این صورت بنابر لم ۳-۵۳ داریم $\gcd(h_i, s_i) = \gcd(s_i, \mathrm{rem}(h_i, s_i))$. بنابراین

$$\gcd(h_{i+۱}, s_{i+۱}) = \gcd(s_i, \mathrm{rem}(h_i, s_i)) = \gcd(h_i, s_i) = \gcd(a, b).$$

از طرفی، پایان‌پذیری الگوریتم نتیجه می‌دهد که $i_۰$ وجود دارد که $s_{i_۰} = ۰$ و

$$\gcd(a, b) = \gcd(h_{i_۰}, s_{i_۰}) = \gcd(h_{i_۰}, ۰) = h_i.$$

□

مثال ۷۵-۲. مراحل اجرای الگوریتم بالا برای محاسبه ب.م.م $a = ۳$ و $b = ۲$ به صورت زیر است:

$\longrightarrow h_۰ = ۳,\ s_۰ = ۲$

$\longrightarrow r = \mathrm{rem}(۳, ۲) = ۱,\ h_۱ = ۲,\ s_۱ = ۱$

$\longrightarrow r = \mathrm{rem}(۲, ۱) = ۰,\ h_۲ = ۱,\ s_۲ = ۰$

$\longrightarrow h_۲ = \gcd(۳, ۲) = ۱$

Procedure 4 RecEuclid in $\mathbb{Z}$

Input: $a, b \in \mathbb{Z}$ where $a \geq b \geq 0$

Output: $\gcd(a, b)$

if $b \neq 0$ **then**

return (a)

else

return $(\text{RecEuclid}(b, \text{rem}(a, b)))$

end if;

end;

در ادامه، یک الگوریتم بازگشتی برای محاسبه ب.م.م ارائه می‌کنیم.

لازم به ذکر است که اثبات پایان‌پذیری و درستی این الگوریتم، مشابه الگوریتم ۳ است. حال الگوریتم اقلیدس را در حلقه $K[x]$ بیان می‌کنیم که K یک میدان است.

Procedure 5 Euclid in $K[x]$

Input: $f, g \in K[x]$

Output: $\gcd(f, g)$

$h := f;\ s := g$

while $S \neq 0$ **do**

$r := \text{rem}(h, s)$

$h := s$

$s := r$

end while;

return (h)

end;

قضیه ۷۶-۲. الگوریتم ۵ پایان‌پذیر است و شرایط مورد نظر را برآورده می‌کند.

اثبات. ابتدا نشان می‌دهیم که الگوریتم پایان‌پذیر است. فرض کنید h_i و s_i نتایج اجرای مرحله i–ام الگوریتم باشند. در این صورت $h_۰ = f$ و $s_۰ = g$. همچنین $s_{i+۱} = \text{rem}(h_i, s_i)$. پس $\deg(s_{i+۱}) < \deg(s_i)$. (فرض خلف) اگر الگوریتم پایان‌پذیر نباشد، دنباله نزولی $\deg(s_۰) > \deg(s_۱) > \deg(s_۲) > \dots$ از اعداد طبیعی بدست می‌آید که با اصل خوش‌ترتیبی اعداد طبیعی در تناقض است. پس الگوریتم است. اثبات درستی، الگوریتم مشابه اثبات درستی الگوریتم ۳ است. □

مثال ۷۷-۲. مراحل اجرای الگوریتم بالا برای محاسبه ب.م.م $f = x^3 - 1$ و $g = x^2 - 1$ به صورت زیر است:

$\longrightarrow h_0 = x^3 - 1,\ s_0 = x^2 - 1$

$\longrightarrow r = \mathrm{rem}(x^3 - 1, x^2 - 1) = x - 1,\ h_1 = x^2 - 1,\ s_1 = x - 1$

$\longrightarrow r = \mathrm{rem}(x^2 - 1, x - 1) = 0,\ h_2 = x - 1,\ s_2 = 0$

$\longrightarrow h_2 = \gcd(x^3 - 1, x^2 - 1) = x - 1$

گزاره ۷۸-۲. برای $\gcd(f_1, \ldots, f_k) = \gcd(f_1, \gcd(f_2, \ldots, f_k)), f_1, \ldots, f_k \in K[x]$. با استفاده از الگوریتم ۶ زیر می‌توان ب.م.م چندجمله‌ای‌های $f_1, \ldots, f_k \in K[x]$ را محاسبه کرد.

Procedure 6 GCD in $K[x]$

Input: $f_1, \ldots, f_k \in K[x]$

Output: $\gcd(f_1, \ldots, f_k)$

$A := \mathrm{Euclid}K[x](f_1, f_2)$

for i from 3 to k **do**

$A := \mathrm{Euclid}K[x](A, f_i)$

end for;

return (A)

end;

Procedure 7 RecGCD in $K[x]$

Input: $f_1, \ldots, f_k \in K[x]$

Output: $\gcd(f_1, \ldots, f_k)$

if $k = 2$ **then**

return $(\mathrm{Euclid}K[x](f_1, f_2))$

else

return $(\mathrm{Euclid}K[x](f_1, \mathrm{RecGCD}K[x](f_2, \ldots, f_k)))$

end if;

end;

گزاره ۷۹-۲ (اتحاد بزو). فرض کنید R یک دامنه ایده‌آل اصلی باشد. برای هر $a, b \in R$، $\gcd(a, b)$ وجود دارد و همچنین $A, B \in R$ وجود دارند که $Aa + Bb = \gcd(a, b)$ (این تساوی را اتحاد بزو و A و B را ضرایب بزو می‌نامیم).

اثبات. چون R یک دامنه ایده‌آل اصلی است، پس $h \in R$ وجود دارد که $\langle a,b\rangle = \langle h\rangle$. کافیست ثابت کنیم $h = \gcd(a,b)$. با توجه به این که $a,b \in \langle h\rangle$، پس $h \mid a$ و $h \mid b$. حال فرض کنید $d \mid a$ و $d \mid b$. پس $a,b \in \langle d\rangle$ و در نتیجه $\langle h\rangle = \langle a,b\rangle \subset \langle d\rangle$. بنابراین $d \mid h$ و حکم ثابت می‌شود. □

الگوریتم ۷ با استفاده از روش بازگشتی، ب.م.م تعدادی چندجمله‌ای را محاسبه می‌کند.

در ادامه نشان می‌دهیم دامنه‌های $\mathbb{Z}$ و $K[x]$ اصلی هستند و سپس با ارائه یک الگوریتم روش محاسبه ضرایب پیشرو بزو را شرح می‌دهیم.

قضیه ۸۰-۲. $\mathbb{Z}$ یک دامنه ایده‌آل اصلی است و هر ایده‌آل $\mathbb{Z}$ به شکل $n\mathbb{Z}$ است که $n \in \mathbb{Z}$.

اثبات. فرض کنید I یک ایده‌آل $\mathbb{Z}$ باشد. اگر $I = \{0\}$، در این صورت $I = 0\mathbb{Z}$. در غیر این صورت مجموعه $A = \{|m| \mid m \in I,\ m \neq 0\}$ را در نظر بگیرید. به وضوح $\emptyset \neq A \subset \mathbb{N}$. بنابر اصل خوش‌ترتیبی اعداد طبیعی، A دارای کوچکترین عضو مانند n است. نشان می‌دهیم $I = n\mathbb{Z}$. واضح است که $n\mathbb{Z} \subset I$. برای اثبات عکس این رابطه، فرض کنید $m \in I$. پس با تقسیم m بر n می‌توان نوشت $m = nq + r$ که $q \in \mathbb{Z}$ و $0 \leq r \leq n$. اگر $r = 0$، آنگاه $m \in n\mathbb{Z}$. در غیر این صورت $r \in A$ و $0 < r < n$ که با انتخاب n در تناقض است. □

قضیه ۸۱-۲. $K[x]$ یک دامنه ایده‌آل اصلی است. علاوه بر این، اگر f یک مولد برای یک ایده‌آل مانند $I \subset K[x]$ باشد، f در حد ضرب یک عنصر وارون‌پذیر، یکتاست.

اثبات. ایده‌آل $I \subset K[x]$ را در نظر بگیرید. اگر $I = \{0\}$، آنگاه $I = \langle 0\rangle$. در غیر این صورت، قرار می‌دهیم $A = \{\deg(f) \mid f \in I,\ f \neq 0\}$. چون $I \neq 0$، بنابراین $A \neq \emptyset$ و $A \subset \mathbb{N}$. پس بنابر اصل خوش‌ترتیبی اعداد طبیعی، A دارای کوچکترین عضو است. بنابراین پمدجمله‌ای غیرصفر $f \in I$ با کمترین درجه وجود دارد. ثابت می‌کنیم $I = \langle f\rangle$. چون $f \in I$، در نتیجه $\langle f\rangle \subset I$. برعکس، فرض کنید $g \in I$. با تقسیم g بر f طبق الگوریتم تقسیم خواهیم داشت $g = qf + r$ که $r = 0$ یا $\deg(r) < \deg(f)$. اگر $r \neq 0$، آنگاه

$$r = g - qf \in I, \quad \deg(r) < \deg(f)$$

که در تناقض با انتخاب f است و $r = 0$. در نتیجه $g = qf \in \langle f\rangle$ و $I = \langle f\rangle$. برای اثبات یکتایی f، فرض کنید $f, g \in I$ وجود داشته باشند که $I = \langle f\rangle = \langle g\rangle$. در این صورت تک‌جمله‌ای مخالف صفر h وجود دارد که $f = hg$ و $\deg(f) = \deg(h) + \deg(h)$. بنابراین $\deg(f) \geq \deg(g)$. به طور مشابه $\deg(f) \leq \deg(g)$. بنابراین $\deg(h) = 0$ و $h \in K$ یک عدد ثابت ناصفر است. □

نتیجه ۸۲-۲. برای $f_1, \ldots, f_k \in K[x]$ داریم $\langle f_1, \ldots, f_k\rangle = \langle \gcd(f_1, \ldots, f_k)\rangle$.

مثال ۸۳-۲. قضیه بالا معادل این است که $K[x]$ یک دامنه اتده‌آل اصلی است. از طرفی $K[x,y]$ یک دامنه ایده‌آل اصلی نیست، زیرا برای مثال $f \in K[x,y]$ وجود ندارد که $\langle f\rangle = \langle x,y\rangle$.

فرض کنید $f, g \in K[x]$. در این صورت، به عنوان یک نتیجه از گزاره ۶۰-۲، $A, B \in K[x]$ وجود دارند که $\gcd(f,g) = Af + Bg$. با استفاده از الگوریتم زیر، ضرایب A, B را محاسبه می‌کنیم. لازم به ذکر است که منظور از دستور $\mathrm{quot}(f,g)$ در این الگوریتم، خارج قسمت تقسیم f بر g است.

Procedure 8 ExtEuclid in $K[x]$

Input: $f, g \in K[x]$ where $g \neq 0$

Output: $\gcd(f,g), A, B$ such that $\gcd(f,g) = Af + Bg$

$A := 1;\ B := 0;\ C := 0;\ D := 1$

$h := Af + Bg$

$s := Cf + Dg$

while $s \neq 0$ **do**

$A' := A;\ B' := B;\ A := C;\ B := D$

$r := \mathrm{rem}(h,s);\ q := \mathrm{quot}(h,s)$

$C := A' - qC;\ D := B' - qD$

$h := s;\ s := r$

end while;

return (h, A, B)

end;

قضیه ۸۴-۲. الگوریتم ۸ پایان‌پذیر است و شرایط مورد نظر را برآورده می‌کند.

اثبات. اثبات پایان‌پذیری الگوریتم مشابه الگوریتم Euclid$K[x]$ است. برای اثبات درستی، کافیست نشان دهیم $h = \gcd(f,g) = Af + Bg$. فرض کنید A_i, B_i, C_i, h_i, s_i نتایج مرحله i-ام الگوریتم باشند. می‌دانیم $h = \gcd(f,g)$. با استفاده از استقرا ثابت می‌کنیم برای هر i داریم $h_i = A_i f + B_i g$ و $s_i = C_i f + D_i g$. به وضوح این رابطه برای $i = 0$ برقرار است. فرض کنید این رابطه برای i برقرار باشد، آن را برای $i+1$ ثابت می‌کنیم. از طرفی، چون قرار می‌دهیم $A_{i+1} = C_i$، $B_{i+1} = D_i$ و $h_{i+1} = s_i$ پس داریم $h_{i+1} = A_{i+1} f + B_{i+1} g$. حال $s_{i+1} = \mathrm{rem}(h_i, s_i)$ پس $s_{i+1} = h_i - q s_i$ که q خارج‌قسمت تقسیم h_i بر s_i است. بنابراین، با استفاده از استقرا s_{i+1} را می‌توان به صورت زیر نوشت

$$A_i f + B_i g - q(C_i f + D_i g) = (A_i - qC_i) f + (B_i - qD_i) g = C_{i+1} f + D_{i+1} g.$$

در نتیجه، اگر i_0 اندیسی باشد که با آن الگوریتم پایان می‌پذیرد، داریم $h_{i_0} = A_{i_0} f + B_{i_0} g$ و درستی الگوریتم اثبات می‌شود. □

مثال ۸۵-۲. مراحل اجرای الگوریتم بالا برای $f = x^۳ - ۱$ و $g = x^۲ - ۱$ به صورت زیر است:

$\longrightarrow A_۰ = D_۰ = ۱,\ B_۰ = C_۰ = ۰,\ h_۰ = x^۳ - ۱,\ s_۰ = x^۲ - ۱$
$\longrightarrow r = x - ۱,\ q = x,\ A_۱ = ۰,\ B_۱ = C_۱ = ۱,\ D_۱ = -x,\ h = x^۲ - ۱,\ s = x - ۱$
$\longrightarrow r = ۰,\ q = x + ۱,\ A = ۱,\ B = -x,\ C = -x - ۱,\ D = x^۲ + x + ۱,\ h = x - ۱,\ s = ۰$
$\longrightarrow h = Af + Bg = (x^۳ - ۱) + (-x)(x^۲ - ۱) = x - ۱.$

۹.۲ منتج دو چندجمله‌ای

منتج دو چندجمله‌ای، یک چندجمله‌ای بر حسب ضرایب دوچندجمله‌ای است که با استفاده از آن می‌توان تشخیص داد آی دو چندجمله‌ای ریشه مشترک دارند یا خیر. منتج سابقه طولانی و ۲۵۰ ساله در ریاضیات دارد. این مبحث برای اولین توسط بزو در سال ۱۷۶۴ تحت عنوان منتج دو چندجمله‌ای تک‌متغیره معرفی شد و بعدها سیلوستر، ریاضی‌دان انگلیسی در سال ۱۸۴۰ با یافتن ارتباط منتج و نظریه ماتریس‌ها توانست منتج را به ابزاری توانمند در جبر تبدیل کند. در واقع منتج را می‌توان به عنوان روشی برای حذف یک متغیر در یک دستگاه و یافتن یک چندجمله‌ای با تعداد متغیر کمتر دانست. در این بخش منتج دو چندجمله‌ای تک‌متغیره را بررسی می‌کنیم ولی در حالت کلی می‌توان منتج n چندجمله‌ای n متغیره را تعریف کرد و از آن به عنوان ابزاری در حل دستگاه‌های معادلات بهره برد. در این بخش، منتج دو چندجمله‌ای تک متغیره را به طور خلاصه مرور می‌کنیم و از آن برای تشخیص عامل مشترک غیربدیهی داشتن دو چندجمله‌ای استفاده می‌کنیم. فرض می‌کنیم K یک میدان است.

لم ۸۶-۲. فرض کنید $f, g \in K[x]$، $\deg(f) = l > ۰$ و $\deg(g) = m > ۰$. در این صورت f و g یک عامل مشترک در $K[x] \setminus K$ دارند اگر و تنها اگر $A, B \in K[x]$ وجود داشته باشند به طوری که:
(۱) حداقل یکی از دو چندجمله‌ای A و B مخالف صفر است.
(۲) درجه A حداکثر $m - ۱$ و درجه B حداکثر $l - ۱$ است.
(۳) $Af + Bg = ۰$.

اثبات. ($\Leftarrow$) فرض کنید $h \in K[x] \setminus K$ یک عامل مشترک f و g باشد. پس $f_۱$ و $g_۱$ در $K[x]$ وجود دارند که $f = hf_۱$ و $g = hg_۱$. از آنجایی که $h \in K[x] \setminus K$، درجه $f_۱$ حداکثر $l - ۱$ و درجه $g_۱$ حداکثر $m - ۱$ است. از طرفی $g_۱.f + (-f_۱).g = g_۱.hf_۱ - f_۱.hg_۱ = ۰$. با انتخاب $A = g_۱$ و $B = -f_۱$ حکم برقرار نخواهد بود.
($\Rightarrow$) فرض کنید A و B سه ویژگی بالا را داشته باشند. بنابر قسمت (۱) حداقل یکی از دو چندجمله‌ای A و B مخالف صفر است. فرض کنید $B \neq ۰$. (فرض حلف) اگر f و g عامل مشترک در $K[x] \setminus K$ نداشته باشند، بزرگترین مقسوم‌علیه مشترک آن‌ها برابر ۱ خواهد بود. بنابر گزاره ۶۰-۲، چمدجمله‌ای‌های $A', B' \in K[x]$ وجود دارند به قسمی که $A'f + B'g = ۱$. حال با ضرب طرفین در B و استفاده از رابطه (۳) خواهیم داشت

$$B = (A'f + B'g)B = A'Bf + B'Bg = A'Bf - B'Af = (A'B - B'A)f.$$

از آن‌جایی که $B \neq 0$، تساوی بالا نشان می‌دهد که درجه B حداقل l است که با (۲) در تناقض است. بنابراین f و g یک عامل مشترک با درجه مثبت دارند. □

اکنون می‌خواهیم با استفاده از ابزار جبرخطی A و B را محاسبه کنیم. فرض کنید

$$A = c_{m-1}x^{m-1} + \ldots + c_0, \quad B = d_{l-1}x^{l-1} + \ldots + d_0$$

که $c_{m-1}, \ldots, c_0, d_{l-1}, \ldots, d$ مجهول هستند. هدف اصلی ما یافتن مقادیر این مجهول‌هاست طوری‌که $Af+Bg = 0$. برای این کار f و g را نیز به صورت زیر می‌نویسیم

$$f = a_l x^l + \ldots + a_0, \quad g = b_m x^m + \ldots + b_0$$

به طوری‌که $a_l \neq 0$ ، $b_m \neq 0$ و a_iها و b_iها عناصری از میدان K هستند. با جایگذاری f،g،A و B در $Af+Bg = 0$ و با صفر قرار دادن ضرایب آن، به یک دستگاه معادلات خطی به صورت زیر می‌رسیم

$$\begin{aligned}
a_l c_{m-1} + b_m d_{l-1} &= 0 \\
a_{l-1}c_{m-1} + a_l c_{m-2} + b_{m-1}d_{l-1} + b_m d_{l-2} &= 0 \\
&\vdots \\
a_0 c_0 + b_0 d_0 &= 0.
\end{aligned}$$

از آن‌جایی که $l+m$ معادله با $l+m$ مجهول داریم، این دستگاه جواب غیربدیهی (مخالف صفر) دارد اگر و تنها اگر دترمینان ماتریس ضرایب آن صفر باشد. این بحث ما را به تعریف مفهومی به نام منتج راهنمایی می‌کند.

تعریف ۸۷-۲. دو چندجمله‌ای $f, g \in K[x]$ با درجه‌های m, l را که حداقل یکی از l و m مخالف صفر است به صورت زیر در نظر می‌گیریم :

$$\begin{aligned}
f &= a_l x^l + a_{l-1}x^{l-1} + \ldots + a_0, \quad a_l \neq 0 \\
g &= b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0, \quad b_m \neq 0.
\end{aligned}$$

در این صورت ماتریس سیلوستر چندجمله‌های f و g برابر است با ماتریس ضرایب دستگاه معادلات بالا که آن را با $\mathrm{Syl}(f,g)$ نمایش می‌دهیم. $\mathrm{Syl}(f,g)$ یک ماتریس $(l+m)\times(l+m)$ است که به صورت زیر نمایش داده می‌شود که

درآیه‌های خالی آن صفر هستند.

$$\mathrm{Syl}(f,g)=\begin{bmatrix} a_l & & & & b_m & & & \\ a_{l-1} & a_l & & & b_{m-1} & b_m & & \\ a_{l-2} & a_{l-1} & \ddots & & b_{m-2} & b_{m-1} & \ddots & \\ \vdots & a_{l-2} & \ddots & a_l & \vdots & b_{m-2} & \ddots & b_m \\ a_0 & \vdots & \ddots & a_{l-1} & b_0 & \vdots & \ddots & b_{m-1} \\ & a_0 & & a_{l-2} & & b_0 & & b_{m-2} \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{bmatrix}$$

تعریف ۸۸-۲. منتج $f,g\in K[x]$ برابر است با دترمینان ماتریس سیلوستر f و g که آن را با $\mathrm{Res}(f,g)$ نمایش می‌دهیم. هرگاه بخواهیم به وابسته بودن منتج f و g به x اشاره کنیم می‌نویسیم $\mathrm{Res}(f,g,x)$.

مثال ۸۹-۲. به عنوان مثال می‌توان نوشت

$$\mathrm{Res}(x^3+x-1,2x^2+3x+7)=\det\begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 1 & 0 & 7 & 3 & 2 \\ -1 & 1 & 0 & 7 & 3 \\ 0 & -1 & 0 & 0 & 7 \end{bmatrix}=159$$

تعریف ۹۰-۲. یک چندجمله‌ای را چندجمله‌ای صحیح گوییم هرگاه همه ضرایب آن اعدادی صحیح باشند.

گزاره ۹۱-۲. دو چندجمله‌ای $f,g\in K[x]$ از درجه مثبت را در نظر بگیرید. در این صورت:
(۱) *(چندجمله‌ای صحیح)* منتج f و g، یک جندجمله‌ای صحیح بر حسب ضرایب f و g است.
(۲) *(عامل مشترک)* f و g یک عامل مشترک در $K[x]\setminus K$ دارند اگر و تنها اگر $\mathrm{Res}(f,g)=0$.

اثبات. قسمت (۱) با توجه به تعریف دترمینان واضح است. برای اثبات قسمت (۲)، منتج f و g صفر است اگر و تنها اگر ماتریس ضرایب دستگاه معادلات ذکر شده در بالا دارای دترمینان صفر باشد که این معادل با این است که این دستگاه جواب غیرصفر داشته باشد. از طرفی وجود جواب غیرصفر برای دستگاه، هم‌ارز با وجود A و B معرفی شده در لم ۶۷-۲ است. پس بنابر لم ۶۷-۲ حکم برقرار است. □

برای مثال، با توجه به اینکه منتج x^3+x-1 و $2x^2+3x+7$ برابر ۱۵۹ است، پس هیچ ریشه مشترکی در $\mathbb{C}$ ندارند. گزاره زیر یک گزاره معروف در جبرخطی است که اثبات آن در هر کتاب جبرخطی قابل دسترس است.

گزاره ۹۲-۲ (روش کرامر). فرض کنید A یک ماتریس $n \times n$ و وارون‌پذیر باشد. در این صورت دستگاه معادلات خطی $AX = B$ دارای جواب یکتای $X = A^{-1}B$ است که مؤلفه i–ام X به صورت $\det(M_i)/\det(A)$ است که در آن M_i نمایش ماتریس $n \times n$ حاصل از جایگزینی B به جای i–امین ستون ماتریس A است.

قضیه ۹۳-۲ (ویژگی حذف). فرض کنید $f, g \in K[x]$ دو چندجمله‌ای از درجه مثبت باشند. در این صورت چندجمله‌ای‌های $A, B \in K[x]$ وجود دارند که $\mathrm{Res}(f,g) = Af + Bg$. علاوه بر این، ضرایب A و B چندجمله‌ای‌هایی صحیح بر حسب ضرایب f و g هستند.

اثبات. اگر منتج f و g صفر باشد، با انتخاب $A = B = ۰$ نتیجه حاصل می‌شود. فرض منتج مخالف صفر باشد. در این صورت بزرگترین مقسوم‌علیه مشترک f و g برابر ۱ خواهد بود (گزاره ۷۲-۲). پس بنابر گزاره ۶۰-۲، چندجمله‌ای‌های $A', B' \in K[x]$ وجود دارند که $A'f + B'g = ۱$. قرار دهید

$$f = a_l x^l + \ldots + a_۰, \quad a_l \neq ۰, \quad g = b_m x^m + \ldots + b_۰, \quad b_m \neq ۰$$
$$A' = c_{m-۱} x^{m-۱} + \ldots + c_۰, \quad B' = d_{l-۱} x^{l-۱} + \ldots + d_۰$$

که $c_۰, \ldots, c_{m-۱}, d_۰, \ldots, d_{l-۱}$ مجهول‌هایی در K هستند. از طرفی، با جایگذاری f،g،A' و B' در $A'f + B'g = ۱$، به دستگاه معادلات خطی زیر می‌رسیم که c_iها و d_iها مجهول و a_iها و b_iها ضرایب معادلات و همگی عضو K هستند

$$a_l c_{m-۱} + b_m d_{l-۱} = ۰$$
$$a_{l-۱} c_{m-۱} + a_l c_{m-۲} + b_{m-۱} d_{l-۱} + b_m d_{l-۲} = ۰$$
$$\vdots$$
$$a_۰ c_۰ + b_۰ d_۰ = ۱.$$

این معدلات همان معادلاتی هستند که پیش‌تر ذکر شد، با این تفاوت که مقدار ثابت آخرین معادله برابر ۱ است. پس ماتریس ضرایب همان ماتریس سیلوستر است. از آن‌جایی که $l + m$ معادله با $l + m$ مجهول داریم و منتج f و g نیز مخالف صفر است، دستگاه معادلات بالا یک جواب یکتا دارد. حال با استفاده از روش کرامر می‌توانیم c_iها و d_iها را بدست آوریم. برای مثال

$$c_۰ = \frac{۱}{\mathrm{Res}(f,g,x)} \det \begin{bmatrix} ۰ & & & & b_m & & & \\ ۰ & a_l & & & b_{m-۱} & b_m & & \\ ۰ & a_{l-۱} & \ddots & & b_{m-۲} & b_{m-۱} & \ddots & \\ \vdots & a_{l-۲} & \ddots & a_l & \vdots & b_{m-۲} & \ddots & b_m \\ ۰ & \vdots & \ddots & a_{l-۱} & b_۰ & \vdots & \ddots & b_{m-۱} \\ \vdots & a_۰ & & a_{l-۲} & & b_۰ & & b_{m-۲} \\ ۰ & & \ddots & \vdots & & & \ddots & \vdots \\ ۱ & & & a_۰ & & & & b_۰ \end{bmatrix}$$

می‌دانیم دترمینان هر ماتریس یک چندجمله‌ای صحیح بر حسب درآیه‌های آن است. پس $c_0 = h_0 / \operatorname{Res}(f,g,x)$ که h_0 یک چندجمله‌ای با ضرایب صحیح بر حسب a_iها و b_iهاست. به طور مشابه می‌توان سایر c_iها و d_iها را محاسبه کرد. چون $A' = c_{m-1}x^{m-1} + \ldots + c_0$، با جایگذاری c_iها در A' و فاکتورگیری از $1/\operatorname{Res}(f,g,x)$، می‌توان A' را به صورت $A' = A/\operatorname{Res}(f,g,x)$ نوشت که A شک چندجمله‌ای در $K[x]$ با ضرایب صحیح بر حسب a_iها و b_iهاست. حال به طور مشابه می‌توان نوشت $B' = B/\operatorname{Res}(f,g,x)$، که $B \in K[x]$ یک چندجمله‌ای با ضرایب صحیح بر حسب a_iها و b_iهاست. از طرفی $A'f + B'g = 1$، که با ضرب طرفین در $\operatorname{Res}(f,g,x)$ خواهیم داشت $\operatorname{Res}(f,g,x) = Af + Bg$ و حکم مورد نظر اثبات می‌شود. □

۱۰.۲ لم گاوس

از موضوعات مهم در جبر، تحویل‌پذیری یک چندجمله‌ای با ضرایب در یک دامنه است و این که این موضوع چه ارتباطی به تحویل‌پذیری چندجمله‌ای روی میدان کسرهای آن دامنه دارد. برای مطالعه این ارتباط نیاز به بیان لم گاوس داریم که در این به بخش به آن و برخی کاربردهای آن می‌پردازیم. در این بخش، فرض می‌کنیم R یک دامنه تجزیه صحیح یکتا باشد. فرض می‌کنیم $f = a_m x^m + \ldots + a_0$ یک چندجمله‌ای متعلق به $R[x]$ باشد که $a_m \neq 0$. در این صورت محتوای f به صورت $\operatorname{cont}(f) = \gcd(a_0, \ldots, a_m)$ تعریف می‌شود. واضح است که برای هر چندجمله‌ای f می‌توان نوشت $f = c \cdot f_1$ که $c = \operatorname{cont}(f)$ و محتوای f_1 برابر ۱ است. هر چندجمله‌ای با محتوای ۱ را چندجمله‌ای اولیه می‌نامیم.

قضیه ۹۴-۲ (لم گاوس). اگر $f, g \in R[x]$، آنگاه $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.

اثبات. فرض کنید $f = c \cdot f_1$ و $g = d \cdot g_1$ که $c = \operatorname{cont}(f)$ و $d = \operatorname{cont}(g)$. بنابراین، کافیست ثابت کنیم $f_1 \cdot g_1$ اولیه است. فرض کنید

$$f_1 = a_m x^m + \ldots + a_0, \quad a_m \neq 0$$
$$g_1 = b_n x^n + \ldots + b_0, \quad b_n \neq 0$$

دو چندجمله‌ای اولیه باشند. عضو تحویل‌ناپذیر $p \in R$ را در نظر می‌گیریم و ادعا می‌کنیم همه ضرایب $f_1 \cdot g_1$ توسط p عاد نمی‌شوند. فرض کنید r و s به ترتیب بزرگترین اندیس‌هایی باشند که p ضرایب a_r و b_s را عاد نکند. حال ضریب x^{r+s} را می‌توان به صورت

$$e = \ldots + a_{r-1}b_{s+1} + a_r b_s + a_{r+1}b_{s-1} + \ldots$$

نوشت. به وضوح، $p \nmid a_r b_s$ و p هر جمله دیگری در e را عاد می‌کند. در نتیجه p ضریب e را عاد نمی‌کند و این ادعا را اثبات می‌کند. □

در ادامه این بخش، فرض می‌کنیم K میدان کسرهای R باشد.

قضیه ۹۵-۲. (۱) فرض کنید $f,g \in K[x]$ و $f_۰, g_۰ \in R[x]$ چندجمله‌ای‌های اولیه نظیر f,g باشند. اگر در $K[x]$، f چندجمله‌ای g را عاد کند، آنگاه در $R[x]$، $f_۰$ نیز $g_۰$ را عاد می‌کند.
(۲) فرض کنید $f,g \in K[x]$ دو چندجمله‌ای باشند به طوری که f اولیه باشد. اگر در $K[x]$، f چندجمله‌ای g را عاد کند، آنگاه در $R[x]$، f نیز چندجمله‌ای g را عاد می‌کند.
(۳) اگر $f,g \in K[x]$ یک عامل مشترک غیر ثابت در $K[x]$ داشته باشند، آنگاه این دو چندجمله‌ای یک عامل مشترک غیر ثابت در $R[x]$ دارند.

اثبات. ادعای اول نتیجه ادعای دوم است، زیرا اگر در $K[x]$، f چندجمله‌ای g را عاد کند، آنگاه به وضوح در $K[x]$، $f_۰$ نیز $g_۰$ را عاد می‌کند. بنابراین، طبق ادعای دوم، در $R[x]$، $f_۰$ نیز $g_۰$ را عاد می‌کند. حال به اثبات ادعای دوم می‌پردازیم. طبق فرض، $q \in K[x]$ موجود است که $g = q \cdot f$. فرض کنید $q = cq_۰$ که $c \in R$ و $q_۰ \in R[x]$ اولیه باشد. بنابراین، $g = cfq_۰$ و طبق لم گاوس $fq_۰$ اولیه است. با توجه به اینکه g و $fq_۰$ متعلق به $R[x]$ هستند پس $fq_۰$ چندجمله‌ای اولیه g است و $c \in R$ که اثبات را تمام می‌کند. برای اثبات ادعای سوم، فرض کنید $h \in K[x]$ یک عامل مشترک غیر ثابت f,g باشد. بدون از دست دادن کلیت مسأله، می‌توان فرض کرد $h \in R[x]$ و h در $R[x]$ اولیه است. بنابراین طبق ادعای دوم، h، f و g را در $R[x]$ عاد می‌کند. □

۱۱.۲ بسته زاریسکی و چندگوناهای آفین

حذف سور یک وجه هندسی نیز دارد. برای واضح‌تر شدن این امر باید برخی از تعاریف و قضایای هندسه جبری را بازگو کنیم. چندگونای آفین را می‌توان پل ارتباطی بین جبر و هندسه دانست. به بیان ساده یک چندگونای آفین مجموعه جواب‌های یک دستگاه معادلات چندجمله‌ای روی یک میدان داده شده است. درواقع، یک چندگونای آفین را می‌توان به عنوان یک شئ هندسی در نظر گرفت. البته با توجه به اینکه ممکن است یک چندگونای آفین شامل یک نقطه تکین باشد، در حالت کلی یک چندگونای آفین، منیفلد نیست. هدف اصلی در هندسه جبری توسعه ابزارهای جبری مورد نیاز برای حل و تحلیل یک چندگونای آفین است. در این بخش، مفهوم چندگونای آفین و برخی ویژگی‌های آن را مطالعه می‌کنیم. در این بخش فرض می‌کنیم K یک میدان باشد و $R = K[x_۱, \ldots, x_n]$.

تعریف ۹۶-۲. برای عدد صحیح مثبت n، $K^n = \{(a_۱, \ldots, a_n) \mid a_۱, \ldots, a_n \in K\}$ را فضای آفین n-بعدی روی K گوییم.

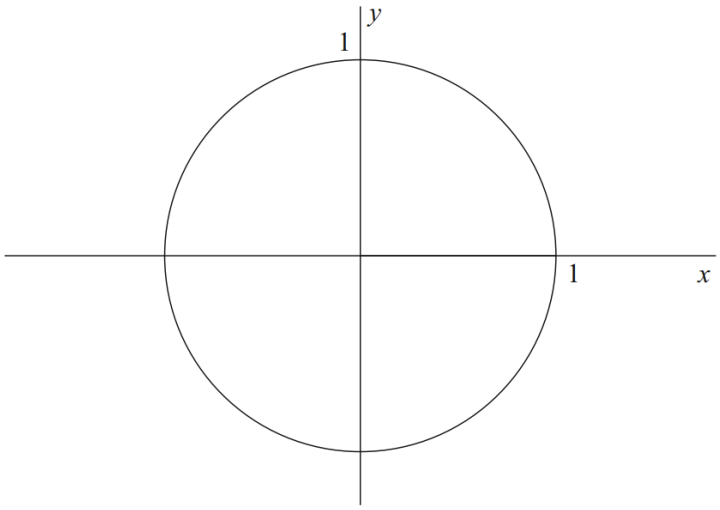
تعریف ۹۷-۲. فرض کنید K یک میدان و $f_۱, \ldots, f_s$ چندجمله‌ای‌هایی در $K[x_۱, \ldots, x_n]$ باشند. در این صورت چندگونای آفین $V(f_۱, \ldots, f_s)$ را به صورت

$$\boldsymbol{V}(f_۱, \ldots, f_s) = \{(a_۱, \ldots, a_n) \in K^n \mid f_i(a_۱, \ldots, a_n) = ۰ \ \forall \ \ ۱ \le i \le s\}$$

تعریف می‌کنیم.

بنابراین چندگونای آفین $\mathbf{V}(f_1, \ldots, f_s) \subseteq k^n$ درواقع مجموعه همه جواب‌های یک دستگاه معادلات به صورت $f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0$ است. معمولا چندگوناهای آفین را با حروف V, W نشان می‌دهیم. برای ساده بودن ترسیم اشکال، $k = \mathbb{R}$ در نظر می‌گیریم. در ادامه، مثال‌های متعددی از انواع چندگوناهای آفین خواهیم دید.

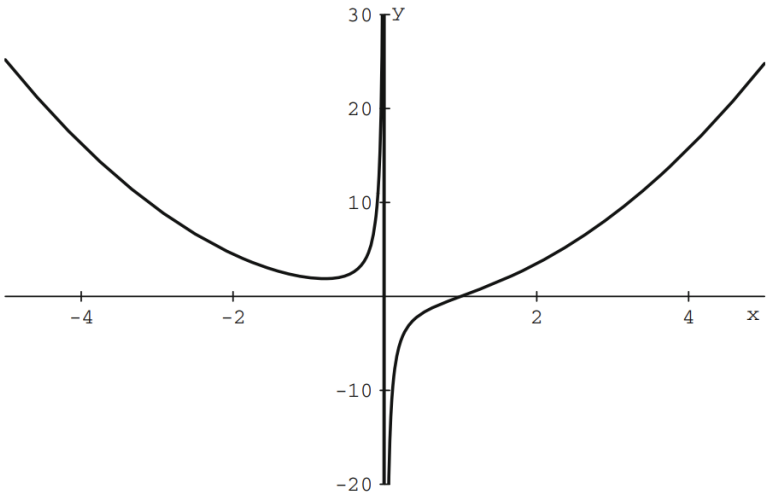
مثال ۹۸-۲. مانند زیر، چندگونای آفین $\boldsymbol{V}(x^2 + y^2 - 1)$ در $\mathbb{R}^2$ یک دایره با شعاع ۱ در مرکز است:



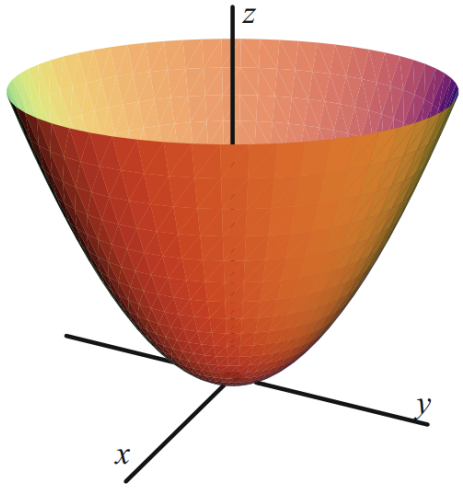
همه اشکال مانند دایره، بیضی، سهمی و ... چندگونای آفین هستند. همچنین نمودار توابع هم چندگونا هستند؛ برای مثال، چندگونای آفین $y = f(x)$، $\boldsymbol{V}(y - f(x))$ است.

مثال ۹۹-۲. همچنین نمودار توابع گویا هم چندگونای آفین است. برای مثال نمودار $y = \frac{x^3 - 1}{x}$ را در نظر بگیرید:

مثال ۱۰۰-۲. حال به مثال‌های سه بعدی در $\mathbb{R}^3$ می‌پردازیم.

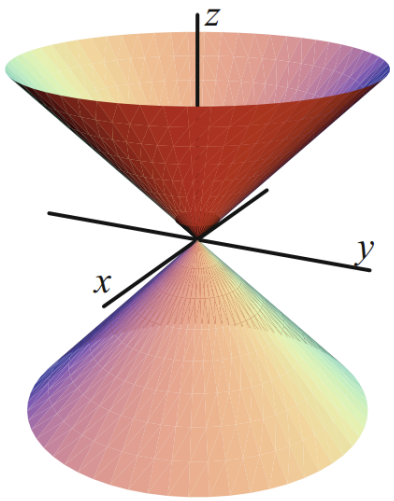


شکل ۱-۲: $\mathbf{V}(xy - x^3 + 1)$

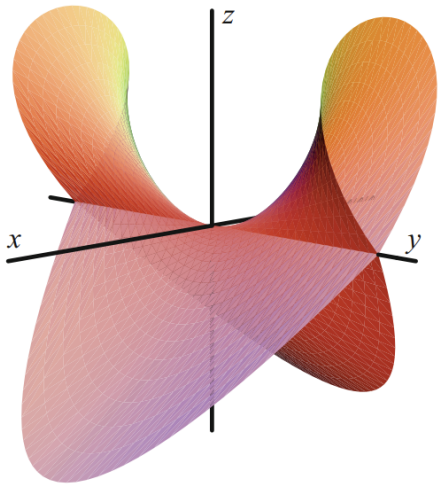


به سادگی می‌توان مشاهده کرد که $\boldsymbol{V}(z - x^2 - y^2)$ چندگونای آفین سهمی‌گون $z = x^2$ است که نسبت به محور z دوران داده شده.

مثال ۱۰۱-۲. برای $\boldsymbol{V}(z^2 - x^2 - y^2)$ داریم:



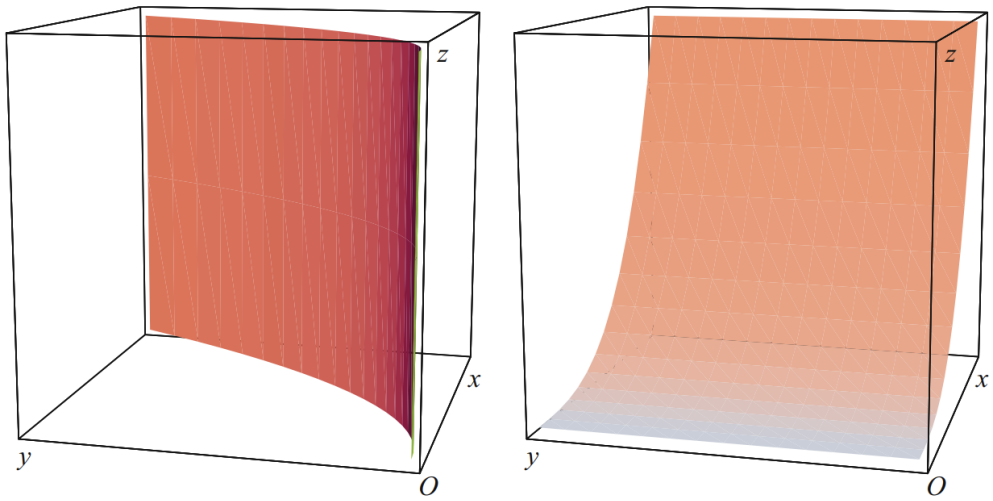
مثال ۱۰۲-۲. رویه چندگونای آفین $\boldsymbol{V}(x^۲ - y^۲z^۲ + z^۳)$ به صورت زیر است:



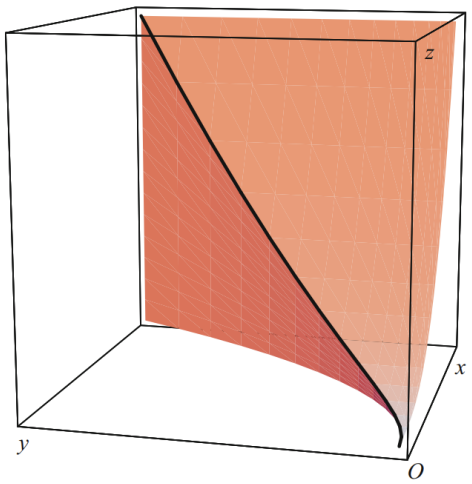
رویه‌های دو مثال آخر همه جا هموار نبودند. مثال مخروط در مرکز خود شکل تیزی داشته و مثال آخر خود را در محور y قطع می‌کند. این‌ها مثالی از نقاط تکین بودند که در آینده به آن‌ها می‌پردازیم.

مثال ۱۰۳-۲. یک مثال جالب از یک خم در $\mathbb{R}^۳$، مکعب پیچ‌خورده[۶] نام دارد. برای شروع، ابتدا دو رویه $y = x^۲$ و $z = x^۲$ را رسم می‌کنیم:

[۶] Twisted Cube



حاصل اشتراک این دو مکعب پیچ‌خورده است:



لازم به ذکر است که با یک معادله در $\mathbb{R}$ یک خم بدست آوردیم که شئ یک بعدی است. مشابها این اتفاق در $\mathbb{R}^۳$ نیز خواهد افتاد که یک معادله در $\mathbb{R}^۳$ معمولا منجر به یک رویه می‌شود.

گزاره ۱۰۴-۲. فرض کنید $V, W \subset K^n$ دو چندگونا باشند. در این صورت $V \cap W$ و $V \cap W$ نیز چندگونا هستند.

اثبات. با استفاده از تعریف، فرض کنید $V = \mathbf{V}(f_۱, \ldots, f_k)$ و $W = \mathbf{V}(g_۱, \ldots, g_t)$ که $f_۱, \ldots, f_k, g_۱, \ldots, g_t \in R$. ابتدا ثابت می‌کنیم $V \cap W$ چندگوناست. برای این منظور ثابت می‌کنیم

$$V \cap W = \mathbf{V}(f_۱, \ldots, f_k, g_۱, \ldots, g_t).$$

فرض کنید $(a_۱,\dots,a_n) \in R$. پس برای هر $i \in \{۱,\dots,k\}$ و $j \in \{۱,\dots,t\}$ داریم $f_i(a_۱,\dots,a_n) = ۰ = g_j(a_۱,\dots,a_n)$. از طرفی، اگر $(a_۱,\dots,a_n)$ ریشه مشترک f_iها و g_iها باشد، آنگاه $(a_۱,\dots,a_n) \in V \cap W$. بنابراین تساوی مورد نظر ثابت می‌شود و $V \cap W$ چندگوناست. حال ثابت می‌کنیم مجموعه $V \cup W$، جبری است. به همین منظور نشان می‌دهیم

$$V \cup W = \mathbf{V}(f_i g_i \mid ۱ \le i \le k,\ ۱ \le j \le t).$$

اگر $(a_۱,\dots,a_n) \in V$، آنگاه مقدار f_i و در نتیجه مقدار $f_i g_i$ در $(a_۱,\dots,a_n)$ برابر صفر است. پس $V \subset \mathbf{V}(f_i g_i)$. به طور مشابه $W \subset \mathbf{V}(f_i g_i)$ و $V \cup W \subset \mathbf{V}(f_i g_i)$. برای اثبات عکس رابطه شمول، فرض کنید $(a_۱,\dots,a_n) \in \mathbf{V}(f_i g_i)$. اگر $(a_۱,\dots,a_n) \in V$، آنگاه حکم ثابت است. در غیر این صورت $۱ \le i_۰ \le k$ وجود دارد که $f_{i_۰}(a_۱,\dots,a_n) \neq ۰$. از آن‌جایی که برای هر j، مقدار $f_{i_۰} g_j$ در $(a_۱,\dots,a_n)$ برابر صفر است، پس مقدار g_j در $(a_۱,\dots,a_n)$ باید برابر صفر باشد. بنابراین $(a_۱,\dots,a_n) \in W$ و $\mathbf{V}(f_i g_i) \subset V \cup W$. □

با استفاده از استقرا و گزاره قبل، به راحتی می‌توان نتیجه زیر را اثبات کرد.

نتیجه ۱۰۵-۲. اگر $V_۱,\dots,V_m$، m چندگونا در K^n باشند، آنگاه $V_۱ \cup \dots \cup V_m$ و $V_۱ \cap \dots \cap V_m$ چندگونا در K^n هستند.

مثال ۱۰۶-۲. فرض کنید $V = \boldsymbol{V}(x-۱, y-۲)$ و $W = \boldsymbol{V}(x-۳, y-۴)$ دو چندگونا باشند. در این صورت $V = \{(۱,۲)\}$، $W = \{(۳,۴)\}$ و $V \cup W = \{(۱,۲),(۳,۴)\}$. همچنین می‌توان نوشت

$$V \cap W = \boldsymbol{V}(x-۱, y-۲, x-۳, y-۴) = \emptyset,$$
$$V \cup W = \boldsymbol{V}((x-۱)(x-۳), (x-۱)(y-۴), (y-۲)(x-۳), (y-۲)(y-۴)).$$

مثال ۱۰۷-۲. هر زیرمجموعه نامتناهی از $\mathbb{R}$ یک چندگوناست. به عنوان مثال

$$\{۱,۲,۳,۴,۵,۶,۷\} = \boldsymbol{V}((x-۱)(x-۲)\dots(x-۷)).$$

گزاره ۱۰۸-۲. اگر $f_۱,\dots,f_k, g_۱,\dots,g_t$ متعلق به R باشند و $\langle f_۱,\dots,f_k\rangle = \langle g_۱,\dots,g_t\rangle$، آنگاه

$$\boldsymbol{V}(f_۱,\dots,f_k) = \boldsymbol{V}(g_۱,\dots,g_t).$$

اثبات. فرض کنید $(a_۱,\dots,a_n) \in \mathbf{V}(f_۱,\dots,f_k)$. در این صورت برای هر $i = ۱,\dots,k$ داریم $f_i(a_۱,\dots,a_n) = ۰$. از طرفی برای هر $j = ۱,\dots,t$، $g_j \in \langle f_۱,\dots,f_k\rangle$. بنابراین چندجمله‌ای‌های $h_{j۱},\dots,h_{jk} \in R$ وجود دارند که $g_j = h_{j۱}f_۱ + \dots + h_{jk}f_k$. در نتیجه $g_j(a_۱,\dots,a_n) = ۰$ و $(a_۱,\dots,a_n) \in \mathbf{V}(g_۱,\dots,g_t)$. عکس رابطه شمول به طور مشابه ثابت می‌شود. □

گزاره ۱۰۹-۲. فرض کنید K یک میدان نامتناهی باشد و $f \in R$. اگر برای هر $(a_۱,\dots,a_n) \in K^n$ داشته باشیم $f(a_۱,\dots,a_n) = ۰$، آنگاه f چندجمله‌ای صفر است.

اثبات. اثبات را با استقرا روی تعداد متغیرها انجام می‌دهیم. فرض کنید $n = ۱$. برای هر $a \in K$، $f(a) = ۰$. چون هر چندجمله‌ای از درجه m، حداکثر m ریشه دارد و K نامتناهی است، پس f باید چندجمله‌ای صفر باشد. حال فرض کنید حکم برای $n - ۱$ درست و $f \in R$ در هر نقطه از K^n صفر باشد. بنابراین f را می‌توان به صورت

$$f = \sum_{i=۰}^{N} g_i(x_۱, \ldots, x_{n-۱}) x_n^i$$

نوشت که $g_i \in K[x_۱, \ldots, x_{n-۱}]$. نشان می‌دهیم هر g_i چندجمله‌ای صفر بر حسب $n - ۱$ متغیر است. برای نقطه ثابت $(a_۱, \ldots, a_{n-۱})$، چندجمله‌ای $f(a_۱, \ldots, a_{n-۱}, x_n)$ را در نظر می‌گیریم که بنابر فرض، برای هر $a_n \in K$ برابر صفر است. بنابراین $f(a_۱, \ldots, a_{n-۱}, x_n)$ باید چندجمله‌ای صفر باشد و برای هر i باید داشته باشیم $g_i(a_۱, \ldots, a_{n-۱}) = ۰$. از آن‌جایی که $(a_۱, \ldots, a_{n-۱})$ دلخواه بود، پس طبق فرض استقرا هر g_i در $K[x_۱, \ldots, x_{n-۱}]$ چندجمله‌ای صفر است. بنابراین f در R چندجمله‌ای صفر است. □

این بخش را با مطالعه چندگونای دو چندجمله‌ای بر حسب دو متغیر به پایان می‌بریم.

گزاره ۱۱۰-۲. فرض کنید K یک میدان باشد و $f, g \in K[x, y]$. اگر f, g عامل مشترک داشته نداشته باشند، در این صورت $\boldsymbol{V}(f, g)$ متناهی است.

اثبات. چون $f, g \in K[x][y]$ عامل مشترک ندارند بنابراین در $K(x)[y]$ هم عامل مشترک ندارند. از طرفی چون $K(x)[y]$ یک دامنه ایده‌آل اصلی است پس $\gcd(f, g) = ۱$ و در نتیجه قبل قضیه بزو، $p, q \in K(x)[y]$ موجود است که $pf + qg = ۱$. بنابراین، $A, B \in K[x, y]$ و $D \in K[x]$ وجود دارند که $Af + Bg = D$. حال فرض کنید $(a, b) \in \mathbf{V}(f, g)$. در نتیجه $D(a) = ۰$ و تعداد انتخاب a متناهی است. با استدلال مشابه، تعداد انتخاب b هم متناهی خواهد شد و این حکم را اثبات می‌کند. □

۱۲.۲ ایده‌آل یک چندگونا

ایده‌آل نظیر یک چندگونا، یک ساختار جبری است که امکان استفاده از ابزارهای مختلف جبری برای تحلیل بهتر چندگونا را فرآهم می‌کند. در این بخش، با معرفی این مفهوم، برخی ویژگی‌های آن را بررسی می‌کنیم. در این بخش K یک میدان است و $R = K[x_۱, \ldots, x_n]$.

تعریف ۱۱۱-۲. فرض کنید $V \subset K^n$ یک چندگونا باشد. ایده‌آل چندگونای آفین V را به صورت

$$\mathbf{I}(V) = \{f \in R \mid \forall (a_۱, \ldots, a_n) \in V \quad f(a_۱, \ldots, a_n) = ۰\}$$

تعریف می‌کنیم.

به راحتی می‌توان مشاهده کرد $\mathbf{I}(V)$ یک ایده‌آل در R است. لازم به ذکر است که می‌توان ایده‌آل یک زیرمجموعه دلخواه از K^n را نیز تعریف کرد.

مثال ۱۱۲-۲. به عنوان مثال، داریم $\mathbf{I}(\emptyset) = \langle ۱ \rangle$ و $\mathbf{I}(\mathbb{R}) = \langle ۰ \rangle$.

مثال ۱۱۳-۲. فرض کنید $V = \{(۰,۰)\}$. در این صورت $\mathbf{I}(V) = \langle x, y \rangle$؛ زیرا اگر $f \in \langle x, y \rangle$، آنگاه $f_۱, f_۲ \in K[x, y]$ وجود دارند که $f = xf_۱ + yf_۲$. بنابراین $f(۰,۰) = ۰$ و $f \in \mathbf{I}(V)$. همچنین اگر $f \in \mathbf{I}(V)$، آنگاه $f_۱, f_۲ \in K[x, y]$ و $c \in K$ وجود دارند به طوری که

$$f = xf_۱ + yf_۲ + c.$$

از طرفی $f(۰,۰) = ۰$. در نتیجه $c = ۰$ و $f \in \langle x, y \rangle$.

لم ۱۱۴-۲. اگر $f_۱, \ldots, f_k \in R$، آنگاه $\langle f_۱, \ldots, f_k \rangle \subset \mathbf{V}(\mathbf{f_۱}, \ldots, \mathbf{f_k})$.

اثبات. فرض کنید $f \in \langle f_۱, \ldots, f_k \rangle$. در این صورت چندجمله‌ای‌های $h_۱, \ldots, h_k \in R$ وجود دارند که $f = \sum_{i=۱}^{k} h_i f_i$. از آن‌جایی که مقدار $f_۱, \ldots, f_k$ روی $\mathbf{V}(f_۱, \ldots, f_k)$ صفر است، پس f روی $\mathbf{V}(f_۱, \ldots, f_k)$ برابر صفر است؛ یعنی $f \in \mathbf{I}(\mathbf{V}(f_۱, \ldots, f_k))$. □

مثال ۱۱۵-۲. فرض کنید $V = (y - x^۲, z - x^۳) \subset \mathbb{R}^۳$. پس $\langle y - x^۲, z - x^۳ \rangle \subset \mathbf{I}(V)$. حال فرض کنید $f \in \mathbf{I}(V)$. چون f یک چندجمله‌ای در $\mathbb{R}[x, y, z]$ است، می‌توان نوشت

$$f = f_۱(y - x^۲) + f_۲(z - x^۳) + f_۳$$

که $f_۱, f_۲ \in \mathbb{R}[x, y, z]$ و $f_۳ \in \mathbb{R}[x]$. از طرفی $V = \{(t, t^۲, t^۳) \mid t \in \mathbb{R}\}$. پس برای هر $t \in \mathbb{R}$ داریم $f(t, t^۲, t^۳) = f_۳(t) = ۰$. بنابراین $f_۳ = ۰$ و در نتیجه $f \in \langle y - x^۲, z - x^۳ \rangle$.

مثال ۱۱۶-۲. با توجه به اینکه

$$\langle x^۲, y^۲ \rangle \subsetneq \mathbf{I}(\mathbf{V}(x^۲, y^۲)) = \mathbf{I}(\{(۰,۰)\}) = \langle x, y \rangle,$$

در لم قبل در حالت کلی، رابطه تساوی برقرار نیست.

نتیجه ۱۱۷-۲. اگر K یک میدان نامتناهی باشد، برای هر عدد صحیح مثبت n داریم $\mathbf{I}(K^n) = \{۰\}$.

گزاره ۱۱۸-۲. فرض کنید V و W دو چندگونا در K^n باشند. در این صورت:

(۱) $V \subset W$ اگر و تنها اگر $\mathbf{I}(W) \subset \mathbf{I}(V)$.

(۲) $V = W$ اگر و تنها اگر $\mathbf{I}(W) = \mathbf{I}(V)$.

اثبات. (۱) ابتدا فرض کنید $V \subset W$ و $f \in \mathbf{I}(W)$. در این صورت خواهیم داشت $f(W) = ۰$. پس $f(V) = ۰$ و $f \in \mathbf{I}(V)$. برعکس، فرض کنید $\mathbf{I}(W) \subset \mathbf{I}(V)$. می‌توان نوشت $V = \mathbf{V}(f_۱, \ldots, f_k)$ و $W = \mathbf{V}(g_۱, \ldots, g_t)$ که $f_۱, \ldots, f_k, g_۱, \ldots, g_t \in R$. بنابراین $f_۱, \ldots, f_k \in \mathbf{I}(V)$ و $g_۱, \ldots, g_t \in \mathbf{I}(W)$. حال فرض کنید $(a_۱, \ldots, a_n) \in V$. در نتیجه برای هر $f \in \mathbf{I}(V)$ داریم $f(a_۱, \ldots, a_n) = ۰$. از آن‌جایی که $\mathbf{I}(W) \subset \mathbf{I}(V)$، برای هر i، $g_i \in \mathbf{I}(W)$ و $g_i(a_۱, \ldots, a_n) = ۰$ که نتیجه می‌دهد $(a_۱, \ldots, a_n) \in W$. به راحتی می‌توان مشاهده کرد که (۲) نتیجه (۱) است. □

۱۳.۲ قضیه ریشه‌های هیلبرت

در این زیربخش، ابتدا مفهوم بسته زاریسکی را تعریف کرده و سپس به قضیه ریشه‌های هیلبرت می‌پردازیم و آن را با استفاده از ابزارهای منطقی، اثبات می‌کنیم.

تعریف ۱۱۹-۲. فرض کنید $I \subseteq k[x_1, \ldots, x_n]$. $X \subseteq k^n$ را بسته زاریسکی گوییم هرگاه $X = \boldsymbol{V}(I)$.

لم ۱۲۰-۲ (تجزیه اولیه). فرض کنید F یک میدان باشد. در این صورت:
(۱) اگر $X \subseteq k^n$، آنگاه $\mathbf{I}(X)$ یک ایده‌آل رادیکال است،
(۲) اگر X بسته زاریسکی باشد، آنگاه $X = \boldsymbol{V}(\mathbf{I}(X))$،
(۳) اگر X و Y بسته زاریسکی باشند و $X \subseteq Y \subseteq k^n$، آنگاه $\mathbf{I}(Y) \subseteq \mathbf{I}(X)$،
(۴) اگر $X, Y \subseteq k^n$ بسته زاریسکی باشند، آنگاه $X \cup Y = \boldsymbol{V}(\mathbf{I}((X) \cap \mathbf{I}(Y)))$ و $X \cap Y = \boldsymbol{V}(\mathbf{I}(X) + \mathbf{I}(Y))$.

اثبات. (۱) فرض کنید $p, q \in \mathbf{I}(X)$ و $f \in k[x_1, \ldots, x_n]$. اگر $a \in X$ آنگاه $p(a) + q(a) = f(a)p(a) = 0$. پس $p + q, fp \in I(X)$ و $I(X)$ یک ایده‌آل است. اگر $f^n \in \mathbf{I}(X)$ و $a \in X$ آنگاه $f^n(a) = 0$، پس $f(a) = 0$. بنابراین $f \in \mathbf{I}(X)$ و $\mathbf{I}(X)$ یک ایده‌آل رادیکال است.
(۲) اگر $a \in X$ و $p \in I(X)$ آنگاه $p(a) = 0$. پس $X \subseteq \mathbf{V}(\mathbf{I}(X))$. اگر $a \in \mathbf{V}(\mathbf{I}(X)) \backslash X$، آنگاه یک $p \in \mathbf{I}(X)$ وجود دارد که $p(a) \neq 0$، که تناقض است. بنابراین $X = \mathbf{V}(\mathbf{I}(X))$.
(۳) اگر $p \in \mathbf{I}(Y)$ و $a \in X$، آنگاه $p(a) = 0$ چون $a \in Y$. بنابراین $\mathbf{I}(Y) \subseteq \mathbf{I}(X)$. طبق قسمت (۲) اگر $\mathbf{I}(X) = \mathbf{I}(Y)$، آنگاه $X = Y$.
(۴) اگر $p \in \mathbf{I}(X) \cap \mathbf{I}(Y)$، آنگاه برای $a \in X$ یا $a \in Y$ داریم $p(a) = 0$. پس $X \cup Y \subseteq \mathbf{V}(\mathbf{I}(X) \cap \mathbf{I}(Y))$. از طرفی اگر $a \notin X \cup Y$، آنگاه $p \in \mathbf{I}(x)$ و $q \in \mathbf{I}(Y)$ وجود دارند که $p(a) \neq 0$ و $q(a) \neq 0$. اما $p(a)q(a) \neq 0$. چون $pq \in \mathbf{I}(X) \cap \mathbf{I}(Y)$، $a \notin \mathbf{V}(\mathbf{I}(X) \cap \mathbf{I}(Y))$. اگر $a \in X \cup Y$، $p \in \mathbf{I}(X)$ و $q \in \mathbf{I}(Y)$، آنگاه $p(a) + q(a) = 0$. پس $X \cup Y \subseteq \mathbf{V}(\mathbf{I}(X) + \mathbf{I}(Y))$. اگر $a \notin X$، آنگاه یک $p \in \mathbf{I}(X) \subseteq \mathbf{I}(X) + \mathbf{I}(Y)$ وجود دارد که $p(a) \neq 0$. بنابراین $a \notin \mathbf{V}(\mathbf{I}(X) + \mathbf{I}(Y))$. به طور مشابه، اگر $a \notin Y$، آنگاه $a \notin \mathbf{V}(\mathbf{I}(X) + \mathbf{I}(Y))$. □

قضیه ۱۲۱-۲ (ریشه‌های هیلبرت). فرض کنید K یک میدان بسته جبری و I و J دو ایده‌آل رادیکال در $K[X_1, \ldots, X_n]$ باشند به طوری که $I \subset J$. در این صورت، $\boldsymbol{V}(J) \subset \boldsymbol{V}(I)$. بنابراین $X \mapsto \mathbf{I}(X)$ یک تناظر دوسویی بین مجموعه‌های بسته زاریسکی و ایده‌آل‌های رادیکال است.

اثبات. فرض کنید $p \in J \backslash I$. بنابر لم تجزیه اولیه، یک ایده‌آل اول P شامل I وجود دارد که $p \notin P$. نشان می‌دهیم که $x \in \mathbf{V}(P) \subseteq \mathbf{V}(I)$ وجود دارد که $p(x) \neq 0$. پس $\mathbf{V}(J) \neq \mathbf{V}(I)$. چون P اول و $K[\overline{X}]/P$ یک دامنه است، می‌توانیم F را بستار جبری میدان کسرهای نظیر آن در نظر بگیریم. فرض کنید $q_1, \ldots, q_m \in K[X_1, \ldots, X_n]$ مولد J باشند. همچنین فرض کنید a_i یک عنصر از X_i/P در F باشد. چون $q_i \in P$ و $p \notin P$:

$$F \models \bigwedge_{i=1}^{m} q_i(\overline{a}) = 0 \wedge p(\overline{a}) \neq 0$$

بنابراین،

$$F \models \exists \overline{w} \bigwedge_{i=1}^{m} q_i(\overline{w}) = 0 \wedge p(\overline{w}) \neq 0$$

و بنابر مدل کامل بودن،

$$K \models \exists \overline{w} \bigwedge_{i=1}^{m} q_i(\overline{w}) = 0 \wedge p(\overline{w}) \neq 0.$$

پس $\bar{b} \in K^n$ وجود دارد که $q_1(\bar{b}) = \ldots = q_m(\bar{b}) = 0$ و $p(\overline{w}) \neq 0$. اما $\bar{b} \in V(P) \backslash V(J)$. □

نتیجه ۱۲۲-۲. اگر $J \subseteq K[\overline{X}]$ یک ایده‌آل رادیکال باشد، آنگاه $J = \mathbf{I}(\mathbf{V}(J))$.

اثبات. به سادگی مشاهده می‌شود که $\mathbf{V}(J) \subseteq \mathbf{I}(\mathbf{V}(J))$. می‌دانیم که $\mathbf{V}(J) = \mathbf{V}(\mathbf{I}(\mathbf{V}(J)))$. پس بنابر قضیه ریشه‌های هیلبرت $J = \mathbf{I}(\mathbf{V}(J))$. □

می‌دانیم که یک چندگونای $V \subseteq k^n$ را می‌توان با ایده‌آل

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid \forall a \in V \quad f(a) = 0\}$$

از همه چندجمله‌ای‌هایی که روی V صفر می‌شوند، مطالعه کرد. بنابراین نگاشت زیر را داریم:

$$\begin{array}{ccc} \text{ایده‌آل‌ها} & \longrightarrow & \text{چندگوناهای آفین} \\ V & \longrightarrow & \mathbf{I}(V) \end{array}$$

برعکس، برای ایده‌آل $I \subseteq k[x_1, \ldots, x_n]$، می‌توانیم مجموعه

$$\mathbf{V}(I) = \{a \in k^n \mid \forall f \in I \quad f(a) = 0\}.$$

بنابر قضیه پایه‌ای هیلبرت، $\mathbf{V}(I)$ در واقع یک چندگونا است؛ زیرا یک مجموعه متناهی از چندجمله‌ای‌های $f_1, \ldots, f_s \in I$ وجود دارد به طوری که $I = \langle f_1, \ldots, f_s \rangle$ و می‌دانیم که $\mathbf{V}(I)$ مجموعه ریشه‌های مشترک این چندجمله‌ای‌ها است. بنابراین داریم:

$$\begin{array}{ccc} \text{چندگوناهای آفین} & & \text{ایده‌آل‌ها} \\ I & \longrightarrow & \mathbf{V}(I). \end{array}$$

این دو نگاشت به ما یک تناظر بین ایده‌آل‌ها و چندگوناها می‌دهند. در ادامه، به بررسی ماهیت این تناظر خواهیم پرداخت.

اولین نکته‌ای که باید به آن توجه کرد این است که این تناظر (به طور دقیق‌تر، نگاشت $\mathbf{V}$) یک به یک نیست: ایده‌آل‌های مختلف می‌توانند یک چندگونای یکسان تولید کنند. برای مثال، $\langle x \rangle$ و $\langle x^2 \rangle$ ایده‌آل‌های متفاوتی در $k[x]$ هستند که چندگونای یکسانی دارند $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. اگر میدان k بسته جبری نباشد، مشکلات جدی‌تری

می‌توانند رخ دهند. برای مثال، چندجمله‌ای‌های ۱، $۱+x^۲$ و $۱+x^۲+x^۴$ را در $\mathbb{R}[x]$ در نظر بگیرید که ایده‌آل‌های متفاوتی تولید می‌کنند:

$$I_۱ = \langle ۱ \rangle = \mathbb{R}[x], \quad I_۲ = \langle ۱ + x^۲ \rangle, \quad I_۳ = \langle ۱ + x^۲ + x^۴ \rangle,$$

اما هیچ‌کدام از این چندجمله‌ای‌ها ریشه حقیقی ندارند. بنابراین چندگوناهای متناظر با آن‌ها، همگی تهی هستند:

$$\mathbf{V}(I_۱) = \mathbf{V}(I_۲) = \mathbf{V}(I_۳) = \emptyset.$$

نمونه‌هایی از چندجمله‌ای‌های دو متغیره بدون ریشه حقیقی شامل $۱+x^۲+y^۲$ و $۱+x^۲+y^۴$ می‌شوند. این‌ها ایده‌آل‌های متفاوتی در $\mathbb{R}[x,y]$ تشکیل می‌دهند که با چندگونای تهی در تناظر هستند.

آیا این مشکل داشتن ایده‌آل‌های مختلف که بیانگر چندگونای تهی هستند، اگر میدان k بسته جبری باشد، از بین می‌رود؟ در حالت تک متغیره $k[x]$، این اتفاق می‌افتد؛ چون هر ایده‌آل I در $k[x]$ می‌تواند توسط یک چندجمله‌ای تولید شود ($k[x]$ یک دامنه ایده‌ال اصلی است). بنابراین می‌توانیم بنویسیم $I = \langle f \rangle$ برای چندجمله‌ای‌های $f \in k[x]$. در این صورت $\mathbf{V}(I)$ مجموعه ریشه‌های f است؛ یعنی مجموعه $a \in k$ به طوری که $f(a) = ۰$. اما از آنجا که k بسته جبری است، هر چندجمله‌ای غیرثابت در $k[x]$ یک ریشه دارد. بنابراین، برای اینکه $\mathbf{V}(I) = \emptyset$ باید f یک ثابت ناصفر باشد. در این حالت، $۱/f \in k$. بنابراین، $I \ni (۱/f) \cdot f = ۱$، که یعنی $g = g \cdot ۱ \in I$ برای هر $g \in k[x]$. این نشان می‌دهد که $I = k[x]$ تنها ایده‌آل $k[x]$ است که وقتی k بسته جبری باشد، بیانگر چندگونای تهی است.

در هر حلقه چندجمله‌ای، بسته جبری بودن کافی است تا تضمین کند که تنها ایده‌آلی که متناظر چندگونای تهی است، خود حلقه چندجمله‌ای است. اکنون قضیه ریشه‌های ضعیف هیلبرت را بیان و اثبات می‌کنیم.

قضیه ۱۲۳-۲ (ریشه‌های ضعیف هیلبرت). فرض کنید k یک میدان بسته جبری و $I \subseteq k[x_۱, \ldots, x_n]$ یک ایده‌آل باشد به طوری که $\mathbf{V}(I) = \emptyset$. در این صورت $I = k[x_۱, \ldots, x_n]$.

اثبات. عکس نقیض قضیه را اثبات می‌کنیم؛ یعنی

$$I \subsetneq k[x_۱, \ldots, x_n] \Longrightarrow \mathbf{V}(I) \neq \emptyset.$$

می‌دانیم $I = k[x_۱, \ldots, x_n] \Leftrightarrow ۱ \in I$. برای $a \in k$ و $f \in k[x_۱, \ldots, x_n]$، فرض کنید $\bar{f} = f(x_۱, \ldots, x_{n-۱}, a) \in k[x_۱, \ldots, x_{n-۱}]$. مجموعه

$$I_{x_n = a} = \{\bar{f} \mid f \in I\}$$

یک ایده‌آل از $k[x_۱, \ldots, x_{n-۱}]$ است.

ادعا: اگر k بسته جبری و $I \subseteq k[x_۱, \ldots, x_n]$ یک ایده‌آل سره باشد، آنگاه $a \in k$ وجود دارد به طوری که $I_{x_n = a} \subseteq k[x_۱, \ldots, x_{n-۱}]$ سره است.

هنگامی که ادعا را ثابت کنیم، با استقرا عناصر $a_۱, \ldots, a_n \in k$ را پیدا می‌کنیم که $I_{x_n = a_n, \ldots, x_۱ = a_۱} \subseteq k$. اما تنها ایده‌آل‌های k، $\{۰\}$ و k هستند، بنابراین $I_{x_n = a_n, \ldots, x_۱ = a_۱} = \{۰\}$. بنابراین $(a_۱, \ldots, a_n) \in \mathbf{V}(I)$. نتیجه می‌گیریم که $\mathbf{V}(I) \neq \emptyset$ و قضیه ثابت خواهد شد.

برای اثبات ادعا، دو حالت برای $I \cap k[x_n]$ وجود دارد.

حالت ۱: $I \cap k[x_n] \neq \{0\}$. فرض کنید $f \in I \cap k[x_n]$ ناصفر باشد و توجه کنید که f غیرثابت است؛ زیرا در غیر این صورت $1 \in I \cap k[x_n] \subseteq I$، که با $I \neq k[x_1, \ldots, x_n]$ در تناقض است.

چون k بسته جبری است، $f = c\prod_{i=1}^{r}(x_n - b_i)^{m_i}$ که در آن $c, b_1, \ldots, b_r \in k$ و $c \neq 0$. فرض کنید که $I_{x_n=b_i} = k[x_1, \ldots, x_{n-1}]$ برای هر i. در این صورت، $B_i \in I$ وجود دارد به طوری که $B_i(x_1, \ldots, x_{n-1}, b_i) = 1$. پس

$$1 = B_i(x_1, \ldots, x_{n-1}, b_i) = B_i(x_1, \ldots, x_{n-1}, x_n - (x_n - b_i)) = B_i + A_i(x_n - b_i)$$

برای $A_i \in k[x_1, \ldots, x_n]$. از آن‌جایی که این برای $i = 1, \ldots, r$ برقرار است، داریم:

$$1 = \prod_{i=1}^{r}(A_i(x_n - b_i) + B_i)^{m_i} = A\prod_{i=1}^{r}(x_n - b_i)^{m_i} + B,$$

که در آن $A = \prod_{i=1}^{r} A_i^{m_i}$ و $B \in I$. سپس از $\prod_{i=1}^{r}(x_n - b_i)^{m_i} = c^{-1}f \in I$ نتیجه می‌گیریم $1 \in I$، که با $I \neq k[x_1, \ldots, x_n]$ در تناقض است. بنابراین $I_{x_n=b_i} \neq k[x_1, \ldots, x_{n-1}]$. این b_i همان a مورد نظر است.

حالت ۲: $I \cap k[x_n] = \{0\}$. فرض کنید $G = \{g_1, \ldots, g_t\}$ یک پایه گربنر برای I نسبت به ترتیب الفبایی با $x_1 > \cdots > x_n$ باشد و قرار دهید:

$$g_i = c_i(x_n)x^{\alpha_i} + (\text{جمله‌های} < x^{\alpha_i}), \qquad (۹)$$

که در آن $c_i(x_n) \in k[x_n]$ ناصفر است و x^{α_i} یک تک‌جمله‌ای در $x_1, \ldots, x_{n-1}$ است.

اکنون $a \in k$ را طوری انتخاب کنید که $c_i(a) \neq 0$ (میدان‌های بسته جبری، نامتناهی هستند). به راحتی می‌توان دید که چندجمله‌ای‌های

$$\bar{g}_i = g_i(x_1, \ldots, x_{n-1}, a)$$

یک پایه برای $I_{x_n=a}$ تشکیل می‌دهند. با جایگذاری $x_n = a$ در معادله (۱۶)، به راحتی دیده می‌شود که $\mathrm{LT}(\bar{g}_i) = c_i(a)x^{\alpha_i}$ زیرا $c_i(a) \neq 0$. همچنین توجه کنید که $x^{\alpha_i} \neq 1$، زیرا در غیر این صورت $g_i = c_i \in I \cap k[x_n] = \{0\}$، در حالی که $c_i \neq 0$. این نشان می‌دهد که $\mathrm{LT}(\bar{g}_i)$ برای هر i غیرثابت است.

ادعا می‌کنیم که $\bar{g}_i$ها یک پایه گربنر برای $I_{x_n=a}$ تشکیل می‌دهند. با فرض ادعا، نتیجه می‌شود که $1 \notin I_{x_n=a}$؛ زیرا هیچ $\mathrm{LT}(\bar{g}_i)$ نمی‌تواند 1 را عاد کند. بنابراین $I_{x_n=a} \neq k[x_1, \ldots, x_{n-1}]$ که همان نتیجه مطلوب است.

برای اثبات ادعا، $g_i, g_j \in G$ و چندجمله‌ای زیر را در نظر بگیرید:

$$S = c_j(x_n)\frac{x^\gamma}{x^{\alpha_i}}g_i - c_i(x_n)\frac{x^\gamma}{x^{\alpha_j}}g_j,$$

که $x^\gamma = \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_j})$. بنابر ساختار، $x^\gamma > \mathrm{LT}(S)$. از آن‌جایی که $S \in I$، یک نمایش استاندارد $S = \sum_{l=1}^{t} A_l g_l$ دارد. پس با محاسبه در $x_n = a$ داریم

$$c_j(a)\frac{x^\gamma}{x^{\alpha_i}}\bar{g}_i - c_i(a)\frac{x^\gamma}{x^{\alpha_j}}\bar{g}_j = \overline{S} = \sum_{l=1}^{t}\bar{A}_l\bar{g}_l.$$

چون $\mathrm{LT}(\bar{g}_i) = c_i(a)x^{\alpha_i}$، مشاهده می‌شود $\overline{S}$، S–چندجمله‌ای $S(\bar{g}_i, \bar{g}_j)$ در حد یک ثابت ناصفر $c_i(a)c_j(a)$ است. پس

$$x^\gamma > \mathrm{LT}(S) \geq \mathrm{LT}(A_l g_l), \quad A_l g_l \neq 0$$

نتیجه می‌دهد

$$x^\gamma > \mathrm{LT}(\bar{A}_l \bar{g}_l), \quad \bar{A}_l \bar{g}_l \neq 0.$$

از آن‌جایی که $x^\gamma = \mathrm{lcm}(\mathrm{LM}(\bar{g}_i), \mathrm{LM}(\bar{g}_j))$، $S(\bar{g}_i, \bar{g}_j)$ برای هر i, j یک نمایش ک.م.م دارد و در نتیجه یک پایه گربنر است. این ادعا را ثابت می‌کند. □

در حالت خاص وقتی $k = \mathbb{C}$، قضیه ریشه‌های ضعیف ممکن است به عنوان «قضیه اساسی جبر برای چندجمله‌ای‌های چندمتغیره» در نظر گرفته شود: هر دستگاه از چندجمله‌ای‌ها که ایده‌آلی به طور اکید کوچک‌تر از $\mathbb{C}[x_1, \ldots, x_n]$ تولید کند، یک ریشه مشترک در $\mathbb{C}^n$ دارد.

قضیه ریشه‌های ضعیف همچنین به ما اجازه می‌دهد مسئله سازگاری[۷] را حل کنیم. آیا یک دستگاه

$$\begin{cases} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{cases}$$

از معادلات چندجمله‌ای یک جواب مشترک در $\mathbb{C}^n$ دارد یا خیر. چندجمله‌ای‌ها جواب مشترک ندارند اگر و تنها اگر $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$. توسط قضیه ریشه‌های ضعیف، حالت اخیر برقرار است اگر و تنها اگر $1 \in \langle f_1, \ldots, f_s \rangle$. بنابراین، برای حل مسئله سازگاری، نیاز داریم تعیین کنیم که آیا ۱ به یک ایده‌آل تعلق دارد یا خیر. این با مشاهده اینکه برای هر ترتیب تک‌جمله‌ای، $\{1\}$ تنها پایه گربنر کاهش‌یافته ایده‌آل $\langle 1 \rangle = k[x_1, \ldots, x_n]$ است، آسان می‌شود.

برای توجیح کردن این گزاره، فرض کنید $\{g_1, \ldots, g_t\}$ یک پایه گربنر برای $I = \langle 1 \rangle$ باشد. بنابراین

$$1 \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$$

و در نتیجه ۱ توسط برخی $\mathrm{LT}(g_i)$، برای مثال $\mathrm{LT}(g_1)$ عاد می‌شود. پس $\mathrm{LT}(g_1)$ لزوماً ثابت است. سپس هر $\mathrm{LT}(g_i)$ دیگر مضربی از آن ثابت است، بنابراین $g_2, \ldots, g_t$ می‌توانند از پایه گربنر حذف شوند. در نهایت، از آن‌جایی که $\mathrm{LT}(g_1)$ ثابت است، خود g_1 ثابت است. بنابراین پایه گربنر کاهش‌یافته موردنظر، $\{1\}$ است.

با داشتن چندجمله‌ای‌های $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$، یک پایه گربنر کاهش‌یافته از ایده‌آلی که تولید می‌کنند را نسبت به هر ترتیب تک‌جمله‌ای محاسبه می‌کنیم. اگر این پایه $\{1\}$ باشد، چندجمله‌ای‌ها هیچ ریشه مشترکی در $\mathbb{C}^n$ ندارند؛ اگر پایه $\{1\}$ نباشد، باید یک صفر مشترک داشته باشند. توجه کنید که این الگوریتم روی هر میدان بسته جبری کار می‌کند.

[۷] Consistency

اگر روی میدان k کار می‌کنیم که بسته جبری نیست، آنگاه الگوریتم سازگاری هنوز در یک جهت کار می‌کند. اگر $\{۱\}$ یک پایه گربنر کاهش‌یافته از $\langle f_۱, \dots, f_s \rangle$ باشد، آنگاه معادلات $f_۱ = \cdots = f_s = ۰$ هیچ جواب مشترکی ندارند. عکس این مطلب درست نیست.

با الهام از قضیه ریشه‌های ضعیف، ممکن است امیدوار باشیم که تناظر بین ایده‌آل‌ها و چندگوناها یک به یک باشد، به شرطی که فقط به میدان‌های بسته جبری محدود شویم. متأسفانه، مثال قبلی $\mathbf{V}(x) = \mathbf{V}(x^۲) = \{۰\}$ روی هر میدانی کار می‌کند. به طور مشابه، ایده‌آل‌های $\langle x^۲, y \rangle$ و $\langle x, y \rangle$ (و به همین ترتیب، $\langle x^n, y^m \rangle$ که در آن n و m اعداد صحیح بزرگ‌تر از یک هستند) متفاوت هستند اما یک چندگونای یکسان را تعریف می‌کنند: یعنی نقطه $\{(۰,۰)\} \subseteq k^۲$. این مثال‌ها یک دلیل اساسی را نشان می‌دهند که چرا ایده‌آل‌های مختلف می‌توانند یک چندگونای یکسان را تعریف کنند. یک توان از یک چندجمله‌ای روی همان مجموعه‌ای که چندجمله‌ای اصلی صفر می‌شود، صفر می‌شود. قضیه ریشه‌های ضعیف هیلبرت بیان می‌کند که روی یک میدان بسته جبری، این تنها دلیلی است که ایده‌آل‌های مختلف می‌توانند یک چندگونای یکسان را بدهند: اگر یک چندجمله‌ای f در همه نقاط یک چندگونای $\mathbf{V}(I)$ صفر شود، آنگاه توانی از f باید به I تعلق داشته باشد.

قضیه ۱۲۴-۲ (ریشه‌های هیلبرت)**.** فرض کنید k یک میدان بسته جبری باشد. اگر $f, f_۱, \dots, f_s \in k[x_۱, \dots, x_n]$، آنگاه $f \in \mathbf{I}(\mathbf{V}(f_۱, \dots, f_s))$ است اگر و تنها اگر

$$f^m \in \langle f_۱, \dots, f_s \rangle$$

برای عدد صحیح $m \geq ۱$.

اثبات. با داشتن یک چندجمله‌ای ناصفر f که در هر ریشه مشترک چندجمله‌ای‌های $f_۱, \dots, f_s$ صفر می‌شود، باید نشان دهیم که عدد صحیح $m \geq ۱$ و چندجمله‌ای‌های $A_۱, \dots, A_s$ وجود دارند به طوری که

$$f^m = \sum_{i=۱}^{s} A_i f_i.$$

ایده‌آل زیر را در نظر بگیرید:

$$\bar{I} = \langle f_۱, \dots, f_s, ۱ - yf \rangle \subseteq k[x_۱, \dots, x_n, y].$$

ادعا می‌کنیم $\mathbf{V}(\bar{I}) = \emptyset$. برای اثبات این ادعا، $(a_۱, \dots, a_n, a_{n+۱}) \in k^{n+۱}$ را در نظر بگیرید. یا $(a_۱, \dots, a_n)$ یک ریشه مشترک از $f_۱, \dots, f_s$ است، یا $(a_۱, \dots, a_n)$ یک ریشه مشترک از $f_۱, \dots, f_s$ نیست.

در حالت اول $f(a_۱, \dots, a_n) = ۰$؛ زیرا f در هر صفر مشترک $f_۱, \dots, f_s$ صفر می‌شود. بنابراین، چندجمله‌ای $۱ - yf$ مقدار $۱ - a_{n+۱} f(a_۱, \dots, a_n) = ۱ \neq ۰$ را در نقطه $(a_۱, \dots, a_n, a_{n+۱})$ می‌گیرد و $(a_۱, \dots, a_n, a_{n+۱}) \notin \mathbf{V}(\bar{I})$. در حالت دوم، برای برخی i که $۱ \leq i \leq s$، باید داشته باشیم $f_i(a_۱, \dots, a_n) \neq ۰$. با در نظر گرفتن f_i به عنوان تابعی از $n+۱$ متغیر که به آخرین متغیر وابسته نیست، داریم $f_i(a_۱, \dots, a_n, a_{n+۱}) \neq ۰$. به ویژه، دوباره نتیجه

می‌گیریم که $(a_1,\dots,a_n,a_{n+1}) \notin \mathbf{V}(\bar{I})$. از آن‌جایی که $(a_1,\dots,a_n,a_{n+1}) \in k^{n+1}$ دلخواه بود، داریم $\mathbf{V}(\bar{I}) = \emptyset$، همانطور که ادعا شد.

اکنون قضیه ریشه‌های ضعیف را اعمال می‌کنیم تا نتیجه بگیریم که $1 \in \bar{I}$. بنابراین

$$1 = \sum_{i=1}^{s} p_i(x_1,\dots,x_n,y)f_i + q(x_1,\dots,x_n,y)(1-yf) \tag{۱۰}$$

برای چندجمله‌ای‌های $p_i, q \in k[x_1,\dots,x_n,y]$. اکنون قرار دهید $y = 1/f(x_1,\dots,x_n)$. سپس رابطه (۱۰) نتیجه می‌دهد

$$1 = \sum_{i=1}^{s} p_i(x_1,\dots,x_n,1/f)f_i. \tag{۱۱}$$

هر دو طرف این معادله را در یک توان f^m ضرب می‌کنیم، که در آن m به اندازه کافی بزرگ انتخاب شده است تا همه مخرج‌ها را حذف کند. داریم:

$$f^m = \sum_{i=1}^{s} A_i f_i, \tag{۱۲}$$

برای چندجمله‌ای‌های $A_i \in k[x_1,\dots,x_n]$، که همان چیزی است که باید نشان می‌دادیم. □

۱.۱۳.۲ تناظر ایده‌آل‌ها و چندگوناها

برای کاوش بیشتر در رابطه بین ایده‌آل‌ها و چندگوناها، طبیعی است که قضیه ریشه‌های هیلبرت را بر حسب ایده‌آل‌ها بازسازی کنیم. آیا می‌توانیم انواع ایده‌آل‌هایی را که به عنوان ایده‌آل یک چندگونا ظاهر می‌شوند، مشخص کنیم؟ به عبارت دیگر، آیا می‌توانیم آن ایده‌آل‌هایی را که شامل همه چندجمله‌ای‌هایی هستند که روی یک چندگونای V صفر می‌شوند، شناسایی کنیم؟ این مشاهده کلیدی در لم ساده زیر نهفته است.

لم ۱۲۵-۲. فرض کنید V یک چندگونا باشد. اگر $f^m \in \mathbf{I}(V)$، آنگاه $f \in \mathbf{I}(V)$.

اثبات. فرض کنید $a \in V$. اگر $f^m \in \mathbf{I}(V)$، آنگاه $(f(a))^m = 0$. اما این تنها زمانی می‌تواند رخ دهد که $f(a) = 0$. از آنجا که $a \in V$ دلخواه بود، باید داشته باشیم $f \in \mathbf{I}(V)$. □

نتیجه ۱۲۶-۲. ایده‌آل $\mathbf{I}(V)$ یک ایده‌آل رادیکال است.

قضیه ۱۲۷-۲ (ریشه‌های قوی هیلبرت)**.** فرض کنید k یک میدان بسته جبری باشد. اگر I یک ایده‌آل در $k[x_1,\dots,x_n]$ باشد، آنگاه

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

اثبات. می‌دانیم $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$؛ زیرا اگر $f \in \sqrt{I}$، آنگاه $f^m \in I$ برای عدد صحیح m است. در نتیجه، f^m روی $\mathbf{V}(I)$ صفر می‌شود که مستلزم آن است f نیز روی $\mathbf{V}(I)$ صفر شود. بنابراین، $f \in \mathbf{I}(\mathbf{V}(I))$.

برعکس، فرض کنید $f \in \mathbf{I}(\mathbf{V}(I))$. در این صورت، طبق تعریف، f روی $\mathbf{V}(I)$ صفر می‌شود. طبق قضیه ریشه‌های هیلبرت، عدد صحیح $m \geq ۱$ وجود دارد به طوری که $f^m \in I$. اما این یعنی $f \in \sqrt{I}$. از آن‌جایی که f دلخواه بود، نتیجه می‌گیریم $\mathbf{I}(\mathbf{V}(I)) \subseteq \sqrt{I}$ و اثبات تمام می‌شود. □

مهم‌ترین نتیجه قضیه ریشه‌های هیلبرت این است که به ما اجازه می‌دهد یک «فرهنگ واژه» بین هندسه و جبر برقرار کنیم. اساس این فرهنگ واژه در قضیه زیر نهفته است.

قضیه ۱۲۸-۲ (تناظر ایده‌آل‌ها و چندگوناها). *(۱)* نگاشت‌های

$$\text{ایده‌آل‌ها} \xrightarrow{\mathbf{I}} \text{چندگوناهای آفین}$$

و

$$\text{چندگوناهای آفین} \xrightarrow{\mathbf{V}} \text{ایده‌آل‌ها}$$

شمول را حفظ می‌کنند؛ یعنی اگر $I_۱ \subseteq I_۲$ ایده‌آل باشند، آنگاه $\mathbf{V}(I_۱) \supseteq \mathbf{V}(I_۲)$ و به طور مشابه، اگر $V_۱ \subseteq V_۲$ چندگونا باشند، آنگاه $\mathbf{I}(V_۱) \supseteq \mathbf{I}(V_۲)$.

(۲) برای هر چندگونای V،

$$\mathbf{V}(\mathbf{I}(V)) = V,$$

در نتیجه $\mathbf{I}$ همواره یک‌به‌یک است. از طرف دیگر، هر ایده‌آل I در رابطه زیر صدق می‌کند:

$$\mathbf{V}(\sqrt{I}) = \mathbf{V}(I).$$

(۳) اگر k بسته جبری باشد و خود را به ایده‌آل‌های رادیکال محدود کنیم، آنگاه نگاشت‌های

$$\text{ایده‌آل‌های رادیکال} \xrightarrow{\mathbf{I}} \text{چندگونای آفین}$$

و

$$\text{چندگونای آفین} \xrightarrow{\mathbf{V}} \text{ایده‌آل‌های رادیکال}$$

دوسویی هستند که رابطه شمول را حفظ کرده و وارون یکدیگرند.

اثبات. (۱) واضح است.

(۲) فرض کنید $V = \mathbf{V}(f_۱, \ldots, f_s)$ یک چندگونا در k^n باشد. از آن‌جایی که هر $f \in \mathbf{I}(V)$ روی V صفر می‌شود، شمول $V \subseteq \mathbf{V}(\mathbf{I}(V))$ به طور مستقیم از تعریف $\mathbf{V}$ نتیجه می‌شود. توجه کنید که طبق تعریف $\mathbf{I}$، داریم $f_۱, \ldots, f_s \in \mathbf{I}(V)$ و در نتیجه $\langle f_۱, \ldots, f_s \rangle \subseteq \mathbf{I}(V)$. از آن‌جایی که $\mathbf{V}$ شمول را وارون می‌کند،

$$\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_۱, \ldots, f_s \rangle) = V.$$

پس $\mathbf{V}(\mathbf{I}(V)) = V$ و در نتیجه $\mathbf{I}$ یک‌به‌یک است؛ زیرا یک وارون چپ دارد. گزاره نهایی بخش (۲) به راحتی قابل مشاهده است.

(۳) از آن‌جایی که $\mathbf{I}(V)$ یک ایده‌آل رادیکال است، می‌توانیم $\mathbf{I}$ را به عنوان تابعی در نظر بگیریم که چندگوناها را به ایده‌آل‌های رادیکال می‌برد. علاوه بر این، می‌دانیم $\mathbf{V}(\mathbf{I}(V)) = V$. پس باید ثابت کنیم $\mathbf{I}(\mathbf{V}(I)) = I$ هرگاه I یک ایده‌آل رادیکال باشد. بنابر قضیه ریشه‌های هیلبرت، $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ و رادیکال بودن I مستلزم $\sqrt{I} = I$ است. این تساوی مطلوب را به دست می‌دهد. در نتیجه، $\mathbf{V}$ و $\mathbf{I}$ معکوس یکدیگر هستند و بنابراین، دوسویی‌هایی بین مجموعه ایده‌آل‌های رادیکال و چندگوناهای آفین تعریف می‌کنند. □

به عنوان نتیجه این قضیه، هر پرسشی درباره چندگوناها را می‌توان به صورت یک پرسش جبری درباره ایده‌آل‌های رادیکال بازگو کرد (و برعکس)، به شرطی که روی یک میدان بسته جبری کار کنیم. این توانایی گذار بین جبر و هندسه به ما توانایی قابل توجهی خواهد داد.

با توجه به قضیه ریشه‌های هیلبرت و اهمیتی که به ایده‌آل‌های رادیکال می‌دهد، طبیعی است که بپرسیم آیا می‌توان مولدهایی برای رادیکال از روی مولدهای ایده‌آل اولیه محاسبه کرد. در واقع، سه پرسش درباره یک ایده‌آل $I = \langle f_1, \dots, f_s \rangle$ مطرح است:

- **(مولدهای رادیکال)** آیا الگوریتمی وجود دارد که مجموعه‌ای از چندجمله‌ای‌ها مانند $\{g_1, \dots, g_m\}$ را چنان تولید کند که $\sqrt{I} = \langle g_1, \dots, g_m \rangle$؟
- **(ایده‌آل رادیکال)** آیا الگوریتمی وجود دارد که تعیین کند آیا I رادیکال است یا خیر؟
- **(عضویت در رادیکال)** به ازای $f \in k[x_1, \dots, x_n]$، آیا الگوریتمی وجود دارد که تعیین کند آیا $f \in \sqrt{I}$ است یا خیر؟

وجود این الگوریتم‌ها از کار هرمان (۱۹۲۶) نتیجه می‌شود. الگوریتم‌های عملی‌تر برای یافتن رادیکال‌ها از کار جیانی، تراگر و زکریاس (۱۹۸۸)، کریک و لوگان (۱۹۹۱)، و آیزنباد، هونکه و واسکونسلوس (۱۹۹۲) نتیجه می‌شوند. در حال حاضر، به حل مسئله متواضع‌تر عضویت در رادیکال بسنده می‌کنیم. برای آزمودن اینکه آیا $f \in \sqrt{I}$، می‌توانستیم از الگوریتم عضویت ایده‌آل استفاده کنیم تا بررسی کنیم آیا $f^m \in I$ برای هر عدد صحیح $m > 0$. این راه‌حل بهینه نیست؛ زیرا ممکن است مجبور شویم تا توان‌های بسیار بزرگی از m پیش برویم و هرگز نتوانیم تعیین کنیم $f \notin \sqrt{I}$ (مگر اینکه کران‌های قبلی بر m در دسترس باشد). خوشبختانه، می‌توانیم اثبات قضیه ریشه‌های هیلبرت را برای ارائه یک الگوریتم جهت تعیین اینکه آیا $f \in \sqrt{\langle f_1, \dots, f_s \rangle}$، تطبیق دهیم.

گزاره ۱۲۹-۲ (عضویت در رادیکال). فرض کنید k یک میدان دلخواه و $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$ یک ایده‌آل باشد. در این صورت $f \in \sqrt{I}$ اگر و تنها اگر چندجمله‌ای ثابت ۱ متعلق به ایده‌آل $\bar{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k[x_1, \dots, x_n, y]$ باشد، که در این حالت، $\bar{I} = k[x_1, \dots, x_n, y]$.

اثبات. در اثبات قضیه ریشه‌های هیلبرت، معادلات (۲)، (۳) و (۴) نشان می‌دهند که $1 \in \bar{I}$ مستلزم $f^m \in I$ برای عدد صحیح m است و در نتیجه $f \in \sqrt{I}$. فرض کنید $f \in \sqrt{I}$. در این صورت $f^m \in I \subseteq \bar{I}$. اما می‌دانیم $1 - yf \in \bar{I}$

و در نتیجه،

$$۱ = y^m f^m + (۱ - y^m f^m) = y^m \cdot f^m + (۱ - yf) \cdot (۱ + yf + \cdots + y^{m-۱} f^{m-۱}) \in \bar{I},$$

و گزاره اثبات می‌شود. □

برای تعیین اینکه آیا $f \in \sqrt{\langle f_۱, \ldots, f_s \rangle} \subseteq k[x_۱, \ldots, x_n]$، یک پایه گربنر کاهش‌یافته از ایده‌آل $\langle f_۱, \ldots, f_s, ۱ - yf \rangle \subseteq k[x_۱, \ldots, x_n, y]$ را نسبت به یک ترتیب تک‌جمله‌ای محاسبه می‌کنیم. اگر نتیجه $\{۱\}$ باشد، آنگاه $f \in \sqrt{I}$. در غیر این صورت، $f \notin \sqrt{I}$.

به عنوان مثال، ایده‌آل $I = \langle xy^۲ + ۲y^۲, x^۴ - ۲x^۲ + ۱ \rangle$ در $k[x, y]$ را در نظر بگیرید. بررسی می‌کنیم که آیا $f = y - x^۲ + ۱$ در $\sqrt{I}$ قرار دارد یا خیر. با استفاده از ترتیب الفبایی روی $k[x, y, z]$، بررسی می‌شود که پایه گربنر کاهش‌یافته ایده‌آل

$$\bar{I} = \langle xy^۲ + ۲y^۲, x^۴ - ۲x^۲ + ۱, ۱ - z(y - x^۲ + ۱) \rangle \subseteq k[x, y, z]$$

برابر است با $\{۱\}$. بنابراین $y - x^۲ + ۱ \in \sqrt{I}$. با استفاده از الگوریتم تقسیم، می‌توانیم بررسی کنیم که چه توانی از $y - x^۲ + ۱$ در I قرار می‌گیرد:

$$\overline{y - x^۲ + ۱}^G = y - x^۲ + ۱, \overline{(y - x^۲ + ۱)^۲}^G = -۲x^۲ y + ۲y, \overline{(y - x^۲ + ۱)^۳}^G = ۰,$$

که در آن $G = \{x^۴ - ۲x^۲ + ۱, y^۲\}$ یک پایه گربنر برای I نسبت به ترتیب الفبایی و $\overline{p}^G$ باقی‌مانده تقسیم p بر G است. در نتیجه، می‌بینیم که $(y - x^۲ + ۱)^۳ \in I$، اما هیچ توان پایین‌تری از $y - x^۲ + ۱$ در I نیست (به طور خاص، $y - x^۲ + ۱ \notin I$).

همچنین می‌توان مشاهده کرد که در این مثال از نظر هندسی چه اتفاقی در حال رخ دادن است. به عنوان یک مجموعه، $\mathbf{V}(I) = \{(\pm ۱, ۰)\}$، اما (با بیان کمی نادقیق) هر چندجمله‌ای در I در هر یک از دو نقطه در $\mathbf{V}(I)$ حداقل تا مرتبه ۲ صفر می‌شود. این از مولدهای I قابل مشاهده است:

$$xy^۲ + ۲y^۲ = y^۲(x + ۲) \quad \text{و} \quad x^۴ - ۲x^۲ + ۱ = (x^۲ - ۱)^۲.$$

حتی با این که $f = y - x^۲ + ۱$ نیز در $(\pm ۱, ۰)$ صفر می‌شود، اما f فقط تا مرتبه ۱ در آن نقاط صفر می‌شود.

این بخش را با بحثی درباره تنها حالتی که می‌توانیم رادیکال یک ایده‌آل را محاسبه کنیم به پایان می‌بریم، یعنی وقتی با یک ایده‌آل اصلی $I = \langle f \rangle$ سروکار داریم. می‌دانیم هر چندجمله‌ای غیرثابت f را می‌توان به صورت حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر نوشت. با جمع‌آوری چندجمله‌ای‌های تحویل‌ناپذیری که فقط در مضرب‌های ثابتی از یکدیگر تفاوت دارند، می‌توان f را به صورت

$$f = c f_۱^{a_۱} \cdots f_r^{a_r}, \quad c \in k,$$

نوشت که در آن f_iها، برای $۱ \le i \le r$، چندجمله‌ای‌های تحویل‌ناپذیر متمایز هستند؛ یعنی f_i و f_j هرگاه $i \neq j$، مضرب ثابتی از یکدیگر نیستند.

گزاره ۱۳۰-۲. فرض کنید $f \in k[x_1, \ldots, x_n]$ و $I = \langle f \rangle$ ایده‌آل اصلی تولید شده توسط f باشد. اگر $f = cf_1^{a_1} \cdots f_r^{a_r}$ یک تجزیه برای f به حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر متمایز باشد، آنگاه

$$\sqrt{I} = \sqrt{\langle f \rangle} = \langle f_1 f_2 \cdots f_r \rangle.$$

اثبات. ابتدا نشان می‌دهیم که $f_1 f_2 \cdots f_r$ متعلق به $\sqrt{I}$ است. فرض کنید N ماکسیمم $a_1, \ldots, a_r$ باشد. در این صورت

$$c(f_1 f_2 \cdots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} \left(cf_1^{a_1} \cdots f_r^{a_r}\right) = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} f$$

یک مضرب چندجمله‌ای از f است. این نشان می‌دهد که $(f_1 f_2 \cdots f_r)^N \in I$، پس $f_1 f_2 \cdots f_r \in \sqrt{I}$. بنابراین $\langle f_1 f_2 \cdots f_r \rangle \subseteq \sqrt{I}$.

برعکس، فرض کنید $g \in \sqrt{I}$. در این صورت یک عدد صحیح مثبت M وجود دارد به طوری که $g^M \in I = \langle f \rangle$، بنابراین g^M مضربی از f و در نتیجه مضربی از هر عامل تحویل‌ناپذیر f_i در f است. بنابراین، f_i یک عامل تحویل‌ناپذیر از g^M است. با این حال، تجزیه یکتای g^M به چندجمله‌ای‌های تحویل‌ناپذیر متمایز، برابر با توان Mام تجزیه g است. نتیجه می‌شود که هر f_i یک عامل تحویل‌ناپذیر از g است. بنابراین، g یک مضرب چندجمله‌ای از $f_1 f_2 \cdots f_r$ است و در نتیجه، g در ایده‌آل $\langle f_1 f_2 \cdots f_r \rangle$ قرار می‌گیرد. □

تعریف ۱۳۱-۲. اگر $f \in k[x_1, \ldots, x_n]$ یک چندجمله‌ای باشد، قسمت کاهش‌یافته *(یا* **بدون مربع***)* f را که با f_{red} نشان داده می‌شود، به صورت چندجمله‌ای تعریف می‌کنیم که در $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$ صدق کند. یک چندجمله‌ای را کاهش‌یافته *(یا* **بدون مربع***)* گویند اگر $f = f_{red}$.

بنابراین، f_{red} چندجمله‌ای f است که عوامل تکراری از آن «حذف شده‌اند». برای مثال، اگر $f = (x+y^2)^3(x-y)$، آنگاه $f_{\text{red}} = (x + y^2)(x - y)$. توجه کنید که f_{red} فقط در حد یک عامل ثابت در k یکتا است.

گزاره ۱۳۲-۲. فرض کنید k یک میدان شامل اعداد گویا $\mathbb{Q}$ و $I = \langle f \rangle$ یک ایده‌آل اصلی در $k[x_1, \ldots, x_n]$ باشد. در این صورت $\sqrt{I} = \langle f_{\text{red}} \rangle$، که در آن

$$f_{\text{red}} = \frac{f}{\gcd\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\right)}.$$

اثبات. با نوشتن f به صورت مورد نظر در گزاره قبل، می‌دانیم که $\sqrt{I} = \langle f_1 f_2 \cdots f_r \rangle$. بنابراین، کافی است نشان دهیم

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}. \tag{۱۳}$$

ابتدا از قاعده ضرب استفاده می‌کنیم:

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1} \left(a_1 \frac{\partial f_1}{\partial x_j} f_2 \cdots f_r + \cdots + a_r f_1 \cdots f_{r-1} \frac{\partial f_r}{\partial x_j}\right).$$

این ثابت می‌کند که $f_۱^{a_۱-۱}f_۲^{a_۲-۱}\cdots f_r^{a_r-۱}$ ب.م.م مورد نظر را عاد می‌کند. باید نشان دهیم برای هر i، مقدار $\frac{\partial f}{\partial x_j}$ وجود دارد که بر $f_i^{a_i}$ بخش‌پذیر نیست. چندجمله‌ای f را به صورت $f = f_i^{a_i}h_i$ بنویسید، که در آن h_i بر f_i بخش‌پذیر نیست. از آن‌جایی که f_i غیرثابت است، باید متغیر x_j مشخصی در f_i ظاهر شود. بنابر قاعده ضرب داریم:

$$\frac{\partial f}{\partial x_j} = f_i^{a_i-۱}\Big(a_i\frac{\partial f_i}{\partial x_j}h_i + f_i\frac{\partial h_i}{\partial x_j}\Big).$$

اگر این عبارت بر $f_i^{a_i}$ بخش‌پذیر باشد، آنگاه $\frac{\partial f_i}{\partial x_j}h_i$ باید بر f_i بخش‌پذیر باشد. از آن‌جایی که f_i تحویل‌ناپذیر است و h_i را عاد نمی‌کند، این سبب می‌شود که f_i، $\frac{\partial f_i}{\partial x_j}$ را عاد کند. $\frac{\partial f_i}{\partial x_j}$ ناصفر است؛ زیرا $\mathbb{Q} \subseteq k$ و x_j در f_i ظاهر می‌شود. از آن‌جایی که درجه کلی $\frac{\partial f_i}{\partial x_j}$ از f_i کمتر است، f_i نمی‌تواند $\frac{\partial f_i}{\partial x_j}$ را عاد کند. بنابراین، $\frac{\partial f_i}{\partial x_j}$ نمی‌تواند $f_i^{a_i}$ را عاد کند و در نتیجه اثبات تمام می‌شود. □

۱۴.۲ جمع، ضرب و اشتراک ایده‌آل‌ها

ایده‌آل‌ها اشیاء جبری هستند و در نتیجه، می‌توانیم عملیات جبری طبیعی‌ای روی آن‌ها تعریف کنیم. در این بخش، سه عمل را در نظر می‌گیریم: جمع، ضرب و اشتراک. این‌ها عملیات دوتایی هستند: به هر جفت ایده‌آل، یک ایده‌آل جدید مرتبط می‌کنند. به ویژه به دو پرسش کلی که در ارتباط با هر یک از این عملیات مطرح می‌شوند، علاقه‌مند خواهیم بود. اولی می‌پرسد که چگونه، با داشتن مولدهای یک جفت ایده‌آل، می‌توان مولدهای ایده‌آل‌های جدید حاصل از اعمال این عملیات را محاسبه کرد. دومی در پی معنای هندسی این عملیات جبری است.

۱.۱۴.۲ جمع ایده‌آل‌ها

تعریف ۱۳۳-۲. اگر I و J ایده‌آل‌های حلقه $k[x_۱,\ldots,x_n]$ باشند، آنگاه جمع I و J، که با $I+J$ نشان داده می‌شود، مجموعه زیر است:

$$I + J = \{f + g \mid f \in I \text{ و } g \in J\}.$$

گزاره ۱۳۴-۲. اگر I و J ایده‌آل‌هایی در $k[x_۱,\ldots,x_n]$ باشند، آنگاه $I+J$ نیز یک ایده‌آل در $k[x_۱,\ldots,x_n]$ است. در حقیقت، $I+J$ کوچک‌ترین ایده‌آل شامل I و J است. علاوه بر این، اگر $I = \langle f_۱,\ldots,f_r\rangle$ و $J = \langle g_۱,\ldots,g_s\rangle$، آنگاه $I + J = \langle f_۱,\ldots,f_r,g_۱,\ldots,g_s\rangle$.

اثبات. ابتدا توجه کنید که $۰ = ۰ + ۰ \in I + J$. فرض کنید $h_۱, h_۲ \in I + J$. طبق تعریف $I+J$، چندجمله‌ای‌های $f_۱, f_۲ \in I$ و $g_۱, g_۲ \in J$ وجود دارند به طوری که $h_۱ = f_۱ + g_۱$ و $h_۲ = f_۲ + g_۲$. در این صورت، از مرتب‌سازی جمله‌ها، $h_۱ + h_۲ = (f_۱ + f_۲) + (g_۱ + g_۲)$. اما $f_۱ + f_۲ \in I$؛ زیرا I یک ایده‌آل است و به طور مشابه، $g_۱ + g_۲ \in J$. در نتیجه $h_۱ + h_۲ \in I + J$. برای بررسی بسته بودن تحت ضرب، فرض کنید $h \in I + J$ و $p \in k[x_۱,\ldots,x_n]$ یک چندجمله‌ای دلخواه باشد. در این صورت، $f \in I$ و $g \in J$ وجود دارند به طوری که $h = f + g$.

اما $p \cdot h = p \cdot (f+g) = p \cdot f + p \cdot g$. سپس $p \cdot f \in I$ و $p \cdot g \in J$؛ زیرا I و J ایده‌آل هستند. در نتیجه، $p \cdot h \in I + J$. این نشان می‌دهد که $I + J$ یک ایده‌آل است.

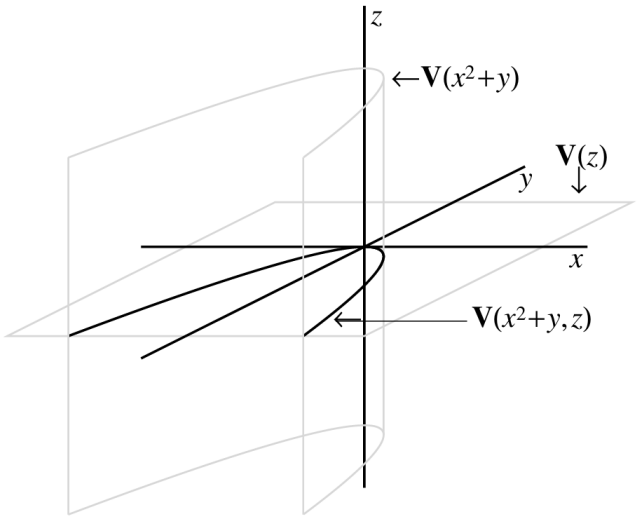
اگر H یک ایده‌آل باشد که شامل I و J باشد، آنگاه H باید تمام عناصر $f \in I$ و $g \in J$ را شامل شود. از آنجایی که H یک ایده‌آل است، H باید تمام $f+g$ها را که در آن $f \in I$ و $g \in J$ است، شامل شود. به طور خاص، $H \supseteq I + J$. بنابراین، هر ایده‌آلی که I و J را شامل شود، $I + J$ را نیز شامل می‌شود و در نتیجه، $I + J$ باید کوچک‌ترین چنین ایده‌آلی باشد.

در نهایت، اگر $I = \langle f_1, \ldots, f_r \rangle$ و $J = \langle g_1, \ldots, g_s \rangle$، آنگاه $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ یک ایده‌آل شامل I و J است. بنابراین $I + J \subseteq \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. عکس این رابطه آشکار است، پس $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

نتیجه ۱۳۵-۲. اگر $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$، آنگاه

$$\langle f_1, \ldots, f_r \rangle = \langle f_1 \rangle + \cdots + \langle f_r \rangle.$$

برای دیدن آنچه از نظر هندسی رخ می‌دهد، فرض کنید $I = \langle x^2 + y \rangle$ و $J = \langle z \rangle$ ایده‌آل‌هایی در $R[x, y, z]$ باشند. تتصویر $\mathbf{V}(I)$ و $\mathbf{V}(J)$ را در زیر ترسیم کرده‌ایم. در این صورت $I + J = \langle x^2 + y, z \rangle$ هر دو $x^2 + y$ و z را شامل می‌شود. بنابراین، چندگونای $\mathbf{V}(I + J)$ باید متشکل از آن نقاطی باشد که در آن هم $x^2 + y$ و هم z صفر می‌شوند؛ یعنی باید اشتراک $\mathbf{V}(I)$ و $\mathbf{V}(J)$ باشد.



قضیه ۱۳۶-۲. اگر I و J ایده‌آل‌هایی در $k[x_1, \ldots, x_n]$ باشند، آنگاه

$$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J).$$

اثبات. اگر $a \in \mathbf{V}(I+J)$، آنگاه $a \in \mathbf{V}(I)$؛ چون $I \subseteq I+J$. به طور مشابه، $a \in \mathbf{V}(J)$. بنابراین، $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$ و نتیجه می‌گیریم

$$\mathbf{V}(I+J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J).$$

برای به دست آوردن عکس این شمول، فرض کنید $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$ و h یک چندجمله‌ای در $I+J$ باشد. در این صورت $f \in I$ و $g \in J$ وجود دارند به طوری که $h = f+g$. داریم $f(a) = ۰$؛ زیرا $a \in \mathbf{V}(I)$ و $g(a) = ۰$؛ چون $a \in \mathbf{V}(J)$. بنابراین، $h(a) = f(a)+g(a) = ۰+۰ = ۰$. از آن‌جایی که h دلخواه بود، نتیجه می‌گیریم $a \in \mathbf{V}(I+J)$. از این رو، $\mathbf{V}(I+J) \supseteq \mathbf{V}(I) \cap \mathbf{V}(J)$. □

۲.۱۴.۲ ضرب ایده‌آل‌ها

در بخش‌های پیش، با این واقعیت مواجه شدیم که یک ایده‌آل تولید شده توسط حاصل‌ضرب‌های مولدهای دو ایده‌آل دیگر، متناظر با اجتماع چندگوناهاست:

$$\mathbf{V}(f_۱, \ldots, f_r) \cup \mathbf{V}(g_۱, \ldots, g_s) = \mathbf{V}(f_i g_j \mid ۱ \leq i \leq r, ۱ \leq j \leq s).$$

بنابراین، برای مثال، چندگونای $\mathbf{V}(xz, yz)$ که متناظر با یک ایده‌آل تولید شده توسط حاصل‌ضرب مولدهای ایده‌آل‌های $\langle x, y\rangle$ و $\langle z\rangle$ در $k[x, y, z]$ است، اجتماع $\mathbf{V}(x, y)$ (محور z) و $\mathbf{V}(z)$ (صفحه (x, y)) می‌باشد. این امر سبب می‌شود تعریف زیر را داشته باشیم.

تعریف ۱۳۷-۲. اگر I و J دو ایده‌آل در $k[x_۱, \ldots, x_n]$ باشند، آنگاه ضرب آن‌ها، که با $I \cdot J$ نشان داده می‌شود، به عنوان ایده‌آل تولید شده توسط تمام چندجمله‌ای‌های $f \cdot g$ که $f \in I$ و $g \in J$ هستند، تعریف می‌شود.

بنابراین، ضرب $I \cdot J$ از I و J، مجموعه زیر است:

$$I \cdot J = \{f_۱ g_۱ + \cdots + f_r g_r \mid f_۱, \ldots, f_r \in I, g_۱, \ldots, g_r \in J, r \in \mathbb{Z}^+\}.$$

برای دیدن این که این یک ایده‌آل است، توجه کنید که $۰ = ۰ \cdot ۰ \in I \cdot J$. علاوه بر این، واضح است که از $h_۱, h_۲ \in I \cdot J$ نتیجه می‌گیریم $h_۱ + h_۲ \in I \cdot J$. در نهایت، اگر $h = f_۱ g_۱ + \cdots + f_r g_r \in I \cdot J$ و p یک چندجمله‌ای باشد، آنگاه

$$ph = (pf_۱) g_۱ + \cdots + (pf_r) g_r \in I \cdot J$$

چون $pf_i \in I$ برای هر i، $۱ \leq i \leq r$. توجه کنید که مجموعه حاصل‌ضرب‌ها به خودی خود یک ایده‌آل نخواهد بود زیرا تحت جمع بسته نخواهد بود. گزاره ساده زیر نشان می‌دهد که محاسبه مجموعه‌ای از مولدها برای $I \cdot J$ با داشتن مجموعه‌ای از مولدها برای I و J، سرراست است.

گزاره ۱۳۸-۲. فرض کنید $I = \langle f_۱, \ldots, f_r\rangle$ و $J = \langle g_۱, \ldots, g_s\rangle$. در این صورت $I \cdot J$ توسط مجموعه تمام حاصل‌ضرب‌های مولدهای I و J تولید می‌شود:

$$I \cdot J = \langle f_i g_j \mid ۱ \leq i \leq r, ۱ \leq j \leq s\rangle.$$

اثبات. واضح است که ایده‌آل تولید شده توسط حاصل‌ضرب‌های f_ig_j از مولدها، در $I \cdot J$ موجود است. برای برقراری عکس رابطه شمول، توجه کنید که هر چندجمله‌ای در $I \cdot J$، مجموعی از چندجمله‌ای‌های به شکل fg است که در آن $f \in I$ و $g \in J$. اما می‌توانیم f و g را به ترتیب بر حسب مولدهای $f_1, \ldots, f_r$ و $g_1, \ldots, g_s$ به صورت

$$f = a_1 f_1 + \cdots + a_r f_r, \quad g = b_1 g_1 + \cdots + b_s g_s$$

برای چندجمله‌ای‌های مناسب $a_1, \ldots, a_r, b_1, \ldots, b_s$ نوشت. بنابراین، fg و در نتیجه هر مجموعی از چندجمله‌ای‌های به این شکل را می‌توان به صورت یک مجموع $\sum_{ij} c_{ij} f_i g_j$ نوشت، که در آن $c_{ij} \in k[x_1, \ldots, x_n]$. □

قضیه ۱۳۹-۲. اگر I و J ایده‌آل‌هایی در $k[x_1, \ldots, x_n]$ باشند، آنگاه $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

اثبات. فرض کنید $a \in \mathbf{V}(I \cdot J)$. در این صورت برای هر $g \in I$ و $h \in J$، داریم $g(a)h(a) = 0$. اگر برای هر $g \in I$ $g(a) = 0$، آنگاه $a \in \mathbf{V}(I)$. اگر $g(a) \neq 0$ برای $g \in I$، آنگاه $h(a) = 0$ برای هر $h \in J$. در هر صورت، $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$.

برعکس، فرض کنید $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. یا $g(a) = 0$ برای هر $g \in I$ یا $h(a) = 0$ برای هر $h \in J$. بنابراین، $g(a)h(a) = 0$ برای هر $g \in I$ و $h \in J$. بنابراین، $f(a) = 0$ برای هر $f \in I \cdot J$ و در نتیجه، $a \in \mathbf{V}(I \cdot J)$. □

در ادامه، اغلب ضرب ایده‌آل‌ها را به صورت IJ می‌نویسیم.

۳.۱۴.۲ اشتراک ایده‌آل‌ها

عمل تشکیل اشتراک دو ایده‌آل، از برخی جنبه‌ها، حتی ابتدایی‌تر از عملیات جمع و ضرب است.

تعریف ۱۴۰-۲. اشتراک $I \cap J$ دو ایده‌آل I و J در $k[x_1, \ldots, x_n]$، مجموعه چندجمله‌ای‌هایی است که به هر دو I و J تعلق دارند.

همانند مورد جمع‌ها، مجموعه ایده‌آل‌ها تحت اشتراک بسته است.

گزاره ۱۴۱-۲. اگر I و J ایده‌آل‌هایی در $k[x_1, \ldots, x_n]$ باشند، آنگاه $I \cap J$ نیز یک ایده‌آل است.

اثبات. توجه کنید که $0 \in I \cap J$؛ زیرا $0 \in I$ و $0 \in J$. اگر $f, g \in I \cap J$، آنگاه $f + g \in I$؛ زیرا $f, g \in I$. به طور مشابه، $f + g \in J$ و در نتیجه، $f + g \in I \cap J$. در نهایت، برای بررسی بسته بودن تحت ضرب، فرض کنید $f \in I \cap J$ و h هر چندجمله‌ای در $k[x_1, \ldots, x_n]$ باشد. از آن‌جایی که $f \in I$ و I یک ایده‌آل است، داریم $h \cdot f \in I$. به طور مشابه، $h \cdot f \in J$ و در نتیجه، $h \cdot f \in I \cap J$. □

توجه کنید که همواره $IJ \subseteq I \cap J$؛ زیرا عناصر IJ مجموع‌هایی از چندجمله‌ای‌های به شکل fg با $f \in I$ و $g \in J$ هستند. اما دومی به هر دو I (زیرا $f \in I$) و J (زیرا $g \in J$) تعلق دارد. با این حال، IJ می‌تواند به طور سره در $I \cap J$

موجود باشد. برای مثال، اگر $I = J = \langle x, y\rangle$، آنگاه $IJ = \langle x^۲, xy, y^۲\rangle$ به طور سره در $I \cap J = I = \langle x, y\rangle$ وجود دارد ($x \in I \cap J$، اما $x \notin IJ$).

با داشتن دو ایده‌آل و یک مجموعه مولد برای هر یک، مطلوب است که بتوانیم یک مجموعه مولد برای اشتراک محاسبه کنیم. این امر بسیار ظریف‌تر از مسائل مشابه برای جمع و ضرب ایده‌آل‌ها است، که به طور کامل سرراست بودند. فرض کنید I ایده‌آل در $\mathbb{Q}[x, y]$ توسط چندجمله‌ای $f = (x + y)^۴(x^۲ + y)^۲(x - ۵y)$ و J ایده‌آل توسط چندجمله‌ای $g = (x + y)(x^۲ + y)^۳(x + ۳y)$ تولید شده باشد. بررسی این که

$$I \cap J = \langle (x + y)^۴(x^۲ + y)^۳(x - ۵y)(x + ۳y)\rangle$$

از آن‌جایی که تجزیه‌های f و g را به عوامل تحویل‌ناپذیر در اختیار داریم، این محاسبه واضح است. به طور کلی، چنین تجزیه‌هایی ممکن است در دسترس نباشند. بنابراین هر الگوریتمی که اشتراک‌ها را محاسبه می‌کند، باید به اندازه کافی قدرتمند باشد تا از این مشکل دوری کند.

با این وجود، یک ترفند خوب وجود دارد که محاسبه اشتراک‌ها را به محاسبه اشتراک یک ایده‌آل با یک زیرحلقه (یعنی حذف متغیرها) کاهش می‌دهد، مسئله‌ای که ما از قبل حل کرده‌ایم. برای بیان قضیه، به کمی نمادگذاری نیاز داریم: اگر I یک ایده‌آل در $k[x_۱, \ldots, x_n]$ و $f(t) \in k[t]$ یک چندجمله‌ای بر حسب t باشد، آنگاه $f(t)I$ نشان‌دهنده ایده‌آل در $k[x_۱, \ldots, x_n, t]$ است که توسط مجموعه چندجمله‌ای‌های $\{f(t) \cdot h \mid h \in I\}$ تولید می‌شود. این با مفهوم عادی ما از ضرب متفاوت است؛ زیرا ایده‌آل I و ایده‌آل تولید شده توسط $f(t)$ در $k[t]$ در حلقه‌های متفاوتی قرار دارند. در واقع، ایده‌آل $I \subseteq k[x_۱, \ldots, x_n]$ یک ایده‌آل در $k[x_۱, \ldots, x_n, t]$ نیست؛ زیرا تحت ضرب در t بسته نیست. برای تأکید کردن بر این که یک چندجمله‌ای $h \in k[x_۱, \ldots, x_n]$ فقط شامل متغیرهای $x_۱, \ldots, x_n$ است، می‌نویسیم $h = h(x)$. در همان راستا، اگر یک چندجمله‌ای g در $k[x_۱, \ldots, x_n, t]$ را در نظر می‌گیریم و می‌خواهیم تأکید کنیم که می‌تواند شامل متغیرهای $x_۱, \ldots, x_n$ و همچنین t باشد، می‌نویسیم $g = g(x, t)$. بر حسب این نمادگذاری، $f(t)I = \langle f(t)h(x) \mid h(x) \in I\rangle$. بنابراین، برای مثال، اگر $f(t) = t^۲ - t$ و $I = \langle x, y\rangle$، آنگاه ایدئال $f(t)I$ در $k[x, y, t]$ شامل $(t^۲ - t)x$ و $(t^۲ - t)y$ است. در واقع $f(t)I$ به عنوان یک ایدئال توسط $(t^۲ - t)x$ و $(t^۲ - t)y$ تولید می‌شود. این یک مورد خاص از لم زیر است.

لم ۱۴.۲-۲. *(i)* اگر I به عنوان یک ایده‌آل در $k[x_۱, \ldots, x_n]$ توسط $p_۱(x), \ldots, p_r(x)$ تولید شود، آنگاه $f(t)I$ به عنوان یک ایده‌آل در $k[x_۱, \ldots, x_n, t]$ توسط $f(t) \cdot p_۱(x), \ldots, f(t) \cdot p_r(x)$ تولید می‌شود.

(ii) اگر $g(x, t) \in f(t)I$ و a هر عنصری از میدان k باشد، آنگاه $g(x, a) \in I$.

اثبات. برای اثبات گزاره اول، توجه کنید که هر چندجمله‌ای $g(x, t) \in f(t)I$ را می‌توان به صورت مجموعی از جمله‌های به شکل $h(x, t) \cdot f(t) \cdot p(x)$ برای $h \in k[x_۱, \ldots, x_n, t]$ و $p \in I$ بیان کرد. اما از آن‌جایی که I توسط $p_۱, \ldots, p_r$ تولید می‌شود، چندجمله‌ای $p(x)$ را می‌توان به صورت مجموعی از جمله‌های به شکل $q_i(x)p_i(x)$، $۱ \le i \le r$، بیان کرد. به عبارت دیگر،

$$p(x) = \sum_{i=۱}^{r} q_i(x)p_i(x).$$

از این رو،

$$h(x,t)\cdot f(t)\cdot p(x)=\sum_{i=1}^{r}h(x,t)q_i(x)f(t)p_i(x).$$

حال، برای هر i، $1\le i\le r$، $h(x,t)\cdot q_i(x)\in k[x_1,\dots,x_n,t]$. بنابراین، $h(x,t)\cdot f(t)\cdot p(x)$ به ایده‌آل در $k[x_1,\dots,x_n,t]$ تولید شده توسط $f(t)\cdot p_1(x),\dots,f(t)\cdot p_r(x)$ تعلق دارد. از آن‌جایی که $g(x,t)$ مجموعی از چنین جمله‌هایی است،

$$g(x,t)\in\langle f(t)\cdot p_1(x),\dots,f(t)\cdot p_r(x)\rangle,$$

که (i) را ثابت می‌کند. گزاره دوم با جایگزینی $a\in k$ به جای t نتیجه می‌شود. □

قضیه ۱۴۳-۲. فرض کنید I، J دو ایده‌آل در $k[x_1,\dots,x_n]$ باشند. در این صورت

$$I\cap J=(tI+(1-t)J)\cap k[x_1,\dots,x_n].$$

اثبات. توجه کنید که $tI+(1-t)J$ یک ایده‌آل در $k[x_1,\dots,x_n,t]$ است. فرض کنید $f\in I\cap J$. از آن‌جایی که $f\in I$، داریم $t\cdot f\in tI$. به طور مشابه، $f\in J$ نتیجه می‌دهد $(1-t)\cdot f\in(1-t)J$. بنابراین، $f=t\cdot f+(1-t)\cdot f\in tI+(1-t)J$. از آن‌جایی که $I,J\subseteq k[x_1,\dots,x_n]$، داریم $f\in(tI+(1-t)J)\cap k[x_1,\dots,x_n]$. بنابراین که $I\cap J\subseteq(tI+(1-t)J)\cap k[x_1,\dots,x_n]$.

برای برقراری عکس این شمول، فرض کنید $f\in(tI+(1-t)J)\cap k[x_1,\dots,x_n]$. در این صورت $f(x)=g(x,t)+h(x,t)$، که $g(x,t)\in tI$ و $h(x,t)\in(1-t)J$. ابتدا قرار دهید $t=0$. از آن‌جایی که هر عنصر از tI مضربی از t است، داریم $g(x,0)=0$. بنابراین، $f(x)=h(x,0)$ و در نتیجه، $f(x)\in J$. از طرف دیگر، $t=1$ را در رابطه $f(x)=g(x,t)+h(x,t)$ قرار دهید. از آن‌جایی که هر عنصر از $(1-t)J$ مضربی از $1-t$ است، داریم $h(x,1)=0$. بنابراین، $f(x)=g(x,1)$ و در نتیجه، $f(x)\in I$. از آن‌جایی که f به هر دو I و J تعلق دارد، داریم $f\in I\cap J$. بنابراین، $I\cap J\supseteq(tI+(1-t)J)\cap k[x_1,\dots,x_n]$ و این اثبات را کامل می‌کند. □

اگر $I=\langle f_1,\dots,f_r\rangle$ و $J=\langle g_1,\dots,g_s\rangle$ دو ایده‌آل در $k[x_1,\dots,x_n]$ باشند، ایده‌آل

$$\langle tf_1,\dots,tf_r,(1-t)g_1,\dots,(1-t)g_s\rangle\subseteq k[x_1,\dots,x_n,t]$$

را در نظر می‌گیریم و یک پایه گربنر نسبت به ترتیب الفبایی که $t\prec_{lex}x_i$ محاسبه می‌کنیم. عناصر این پایه که متغیر t را شامل نمی‌شوند، یک پایه (در واقع، یک پایه گربنر) برای $I\cap J$ تشکیل خواهند داد.

به عنوان یک مثال ساده، فرض کنید می‌خواهیم اشتراک ایده‌آل‌های $I=\langle x^2y\rangle$ و $J=\langle xy^2\rangle$ را در $\mathbb{Q}[x,y]$ محاسبه کنیم. ایده‌آل

$$tI+(1-t)J=\langle tx^2y,(1-t)xy^2\rangle=\langle tx^2y,txy^2-xy^2\rangle$$

را در $\mathbb{Q}[t,x,y]$ در نظر می‌گیریم. با محاسبه S-چندجمله‌ای مولدها، به $tx^۲y^۲ - (tx^۲y^۲ - x^۲y^۲) = x^۲y^۲$ می‌رسیم. به راحتی می‌توان بررسی کرد که $\{tx^۲y, txy^۲ - xy^۲, x^۲y^۲\}$ یک پایه گربنر برای $tI + (۱-t)J$ نسبت به ترتیب الفبایی با $t > x > y$ است. طبق قضیه حذف، $\{x^۲y^۲\}$ یک پایه (گربنر) برای $(tI + (۱-t)J) \cap \mathbb{Q}[x,y]$ است. بنابراین،

$$I \cap J = \langle x^۲y^۲ \rangle.$$

تعریف ۱۴۴-۲. یک چندجمله‌ای $h \in k[x_۱, \ldots, x_n]$ را یک ک.م.م *(کوچک‌ترین مضرب مشترک)* از $f, g \in k[x_۱, \ldots, x_n]$ می‌نامیم و آن را با $h = \operatorname{lcm}(f,g)$ نشان می‌دهیم هرگاه

(i) f، h را بشمارد و g، h را بشمارد.

(ii) اگر f و g هر دو چندجمله‌ای p را بشمارند، آنگاه h، p را بشمارد.

برای مثال،

$$\operatorname{lcm}(x^۲y, xy^۲) = x^۲y^۲$$

و

$$\operatorname{lcm}\Big((x+y)^۴(x^۲+y)^۲(x-۵y), (x+y)(x^۲+y)^۳(x+۳y)\Big) = (x+y)^۴(x^۲+y)^۳(x-۵y)(x+۳y).$$

به طور کلی‌تر، فرض کنید $f, g \in k[x_۱, \ldots, x_n]$ و $f = cf_۱^{a_۱} \cdots f_r^{a_r}$ و $g = c' g_۱^{b_۱} \cdots g_s^{b_s}$ تجزیه‌های آن‌ها به چندجمله‌ای‌های تحویل‌ناپذیر متمایز باشند. ممکن است برخی از عوامل تحویل‌ناپذیر f مضرب‌های ثابتی از عوامل g باشند. در این حالت، فرض کنید ترتیب چندجمله‌ای‌های تحویل‌ناپذیر در عبارات f و g را بازآرایی کرده‌ایم به طوری که برای l، $۱ \le l \le \min(r,s)$، f_i یک ثابت (ناصفر) مضرب g_i برای $۱ \le i \le l$ باشد و برای هر $i,j > l$، f_i مضرب ثابتی از g_j نباشد. سپس از تجزیه یکتا نتیجه می‌شود

$$\operatorname{lcm}(f,g) = f_۱^{\max(a_۱,b_۱)} \cdots f_l^{\max(a_l,b_l)} \cdot g_{l+۱}^{b_{l+۱}} \cdots g_s^{b_s} \cdot f_{l+۱}^{a_{l+۱}} \cdots f_r^{a_r}. \qquad (۱۴)$$

(در حالتی که f و g هیچ عامل مشترکی ندارند، داریم $\operatorname{lcm}(f,g) = f \cdot g$).

گزاره ۱۴۵-۲. *(i)* اشتراک $I \cap J$ دو ایده‌آل اصلی $I, J \subseteq k[x_۱, \ldots, x_n]$، یک ایده‌آل اصلی است.

(ii) اگر $I = \langle f \rangle$، $J = \langle g \rangle$ و $I \cap J = \langle h \rangle$، آنگاه

$$h = \operatorname{lcm}(f,g).$$

اثبات. واضح است. □

این نتیجه، به همراه الگوریتم برای محاسبه اشتراک دو ایده‌آل، یک الگوریتم برای محاسبه کوچک‌ترین مضرب مشترک دو چندجمله‌ای به دست می‌دهد. برای محاسبه کوچک‌ترین مضرب مشترک دو چندجمله‌ای $f, g \in k[x_1, \ldots, x_n]$، اشتراک $\langle f \rangle \cap \langle g \rangle$ را با استفاده از الگوریتم محاسبه اشتراک ایده‌آل‌ها محاسبه می‌کنیم. گزاره پیش تضمین می‌کند که این اشتراک یک ایده‌آل اصلی است و هر مولد آن یک کوچک‌ترین مضرب مشترک از f و g است.

گزاره ۱۴۶-۲. فرض کنید $f, g \in k[x_1, \ldots, x_n]$. در این صورت

$$\operatorname{lcm}(f, g) \cdot \gcd(f, g) = fg.$$

اثبات. این با بیان f و g به عنوان حاصل‌ضرب‌هایی از عوامل تحلیل‌ناپذیر متمایز و سپس استفاده از توضیحات قبل از گزاره ۱۳، به ویژه معادله (۲۱)، نتیجه می‌شود. شما جزئیات را در تمرین ۵ ارائه خواهید داد. □

از گزاره قبل نتیجه می‌شود

$$\gcd(f, g) = \frac{f \cdot g}{\operatorname{lcm}(f, g)}. \tag{۱۵}$$

قضیه ۱۴۷-۲. اگر I و J دو ایده‌آل در $k[x_1, \ldots, x_n]$ باشند، آنگاه $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

اثبات. فرض کنید $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. در این صورت $a \in \mathbf{V}(I)$ یا $a \in \mathbf{V}(J)$؛ یعنی $f(a) = 0$ برای هر $f \in I$، یا $f(a) = 0$ برای هر $f \in J$. بنابراین، $f(a) = 0$ برای هر $f \in I \cap J$. از این رو، $a \in \mathbf{V}(I \cap J)$. بنابراین، $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$.

از طرف دیگر، توجه کنید که از آن‌جایی که $IJ \subseteq I \cap J$، داریم $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ)$. اما $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ و ناتساوی مطلوب نتیجه می‌شود. □

گزاره ۱۴۸-۲. اگر I، J دو ایده‌آل‌های دلخواه باشند، آنگاه

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

اثبات. اگر $f \in \sqrt{I \cap J}$، آنگاه $f^m \in I \cap J$ برای عدد صحیح $m > 0$. از آن‌جایی که $f^m \in I$، داریم $f \in \sqrt{I}$. به طور مشابه، $f \in \sqrt{J}$. بنابراین، $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.

برعکس، فرض کنید $f \in \sqrt{I} \cap \sqrt{J}$. در این صورت اعداد صحیح $m, p > 0$ وجود دارند به طوری که $f^m \in I$ و $f^p \in J$. بنابراین $f^{m+p} = f^m f^p \in I \cap J$، پس $f \in \sqrt{I \cap J}$. □

فصل ۳

پایه گربنر و محاسبه آن

در قلب جبر جابجایی و هندسه جبری، مسئله حل دستگاه معادلات چندجمله‌ای، جایگاهی محوری دارد. برای قرن‌ها، ریاضیدانان به دنبال الگوریتم‌ها و روش‌های نظام‌مندی بودند که بتواند مجموعه جواب‌های چنین دستگاه‌هایی را به طور موثر توصیف و محاسبه کند. ایده اساسی، تعمیم مفهوم حذف متغیرها در دستگاه‌های خطی به دنیای غیرخطی معادلات چندجمله‌ای است.

در دهه ۱۹۶۰، یک دانشجوی دکترای اتریشی به نام «برونو بوخبرگر»، در رساله دکترای خود تحت راهنمایی ولفگانگ گربنر، پاسخی نوآورانه به این چالش ارائه داد. او مفهومی را معرفی کرد که امروزه به احترام استادش، «پایه گربنر» نامیده می‌شود. یک پایه گربنر، برای یک ایده‌آل در یک حلقه چندجمله‌ای، یک مجموعه مولد خاص است که ویژگی‌های محاسباتی مطلوبی دارد. در حقیقت، این مفهوم، تعمیمی از پایه‌های استاندارد برای فضای برداری و الگوریتم تقسیم در چندجمله‌ای‌های تک‌متغیره به دنیای چندمتغیره است.

دستاورد بزرگ بوخبرگر، نه تنها معرفی این مفهوم، بلکه ارائه یک الگوریتم برای محاسبه آن بود. این الگوریتم که به الگوریتم بوخبرگر مشهور است، با تعمیم مفهوم «S-چندجمله‌ای» از الگوریتم تقسیم چندجمله‌ای‌ها، امکان محاسبه سیستماتیک یک پایه گربنر را فراهم می‌کند. این الگوریتم، اگرچه در بدترین حالت از پیچیدگی نمایی برخوردار است، اما به دلیل پیاده‌سازی در سامانه‌های جبر کامپیوتری، به یک ابزار قدرتمند و کاربردی در ریاضیات محاسباتی تبدیل شده است. در این فصل، به بررسی سیستماتیک این مفهوم کلیدی می‌پردازیم. ابتدا با یادآوری مقدمات لازم از جبر جابجایی و تعریف ترتیب‌های تک‌جمله‌ای آغاز می‌کنیم. سپس به طور دقیق مفهوم پایه گربنر و الگوریتم بوخبرگر برای محاسبه آن را ارائه خواهیم داد. در ادامه، به کاربردهای عملی آن در حل دستگاه معادلات و مسئله عضویت در ایده‌آل می‌پردازیم و در نهایت، برخی تعمیم‌ها و کاربردهای پیشرفته‌تر را به اختصار مورد بحث قرار می‌دهیم. هدف این فصل، تجهیز خواننده به

ابزارهای نظری و عملی لازم برای به کارگیری این تکنیک قدرتمند در مسائل ریاضی است.

۱.۳ ترتیب روی تک‌جمله‌ای‌ها در $K[x_1,\dots,x_n]$

تعریف ۱-۳. منظور از یک ترتیب تک‌جمله‌ای $>$ روی $K[x_1,\dots,x_n]$، یک رابطه $>$ روی $\mathbb{Z}^n$ برای اعداد نامنفی است. به عبارت دیگر، یک ترتیب تک‌جمله‌ای یک رابطه روی مجموعه تک‌جمله‌ای ها به صورت x^α برای $\alpha \in \mathbb{Z}^n$ است به طوری که:

(۱) $>$ یک ترتیب خطی روی $\mathbb{Z}^n$ است،

(۲) اگر $\alpha > \beta$ و $\gamma \in \mathbb{Z}^n$، آنگاه $\alpha+\gamma > \beta+\gamma$.

(۳) رابطه $>$ روی $\mathbb{Z}^n$ خوش‌ترتیب است. یعنی اگر $A \subseteq \mathbb{Z}^n$ ناتهی باشد، آنگاه $\alpha \in A$ وجود دارد که برای $\alpha \neq \beta$، $\beta > \alpha$.

تعریف ۲-۳ (ترتیب الفبایی). فرض کنید $\alpha = (\alpha_1,\dots,\alpha_n)$ و $\beta = (\beta_1,\dots,\beta_n)$ به طوری که $\alpha,\beta \in \mathbb{Z}^n$. می‌گوییم $\alpha >_{lex} \beta$ اگر چپ‌ترین ورودی ناصفر بردار حاصل از تفاضل $\alpha-\beta \in \mathbb{Z}^n$، مثبت باشد. اگر $\alpha >_{lex} \beta$، می‌نویسیم $x^\alpha >_{lex} x^\beta$.

مثال ۳-۳. $(0,3,4) >_{lex} (1,2,0)$، چون $\alpha-\beta = (1,-1,-4)$.

مثال ۴-۳. $(3,2,1) >_{lex} (3,2,4)$، چون $\alpha-\beta = (0,0,3)$

مثال ۵-۳. برای متغیرهای $x_1,\dots,x_n$ داریم:

$$(1,0,\dots,0) >_{lex} (0,1,\dots,0) >_{lex} \dots >_{lex} (0,\dots,0,1).$$

بنابراین $x_1 >_{lex} x_2 >_{lex} \dots >_{lex} x_n$.

از این به بعد در برخی از موارد، ترتیب الفبایی را با نماد $\prec_{lex}$ نشان می‌دهیم.

گزاره ۶-۳. ترتیب الفبایی روی $\mathbb{N}^n$ یک ترتیب تک‌جمله‌ای است.

اثبات. ابتدا نشان می‌دهیم ترتیب الفبایی یک ترتیب کلی روی $\mathbb{N}^n$ است. به وضوح برای هر $\alpha \in \mathbb{N}^n$ داریم $\alpha \preceq_{lex} \alpha$. حال فرض کنید $\alpha \preceq_{lex} \beta$ و $\beta \preceq_{lex} \alpha$. اگر $\alpha \neq \beta$، آنگاه $1 \leq i \leq b$ وجود دارد که برای هر $1 \leq j < i$ داریم $\alpha_j = \beta_j$ و برای مثال $\alpha_i < \beta_i$ که در تناقض با $\beta \preceq_{lex} \alpha$ است. اکنون فرض کنید $\alpha \prec_{lex} \beta$ و $\beta \prec_{lex} \gamma$. همچنین فرض کنید i و j کوچکترین اندیس‌هایی باشند که $\alpha_i < \beta_i$ و $\beta_j < \gamma_j$. اگر $j < i$، آنگاه

$$\alpha_1 = \beta_1 = \gamma_1, \dots, \alpha_{j-1} = \beta_{j-1} = \gamma_{j-1}, \quad \alpha_j = \beta_j < \gamma_j.$$

در نتیجه $\alpha \prec_{lex} \gamma$. حال اگر $i \leq j$، آنگاه

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

و بنابراین $\alpha\prec_{lex}\gamma$. همچنین واضح است که برای هر $\alpha,\beta\in\mathbb{N}^n$، $\alpha\preceq_{lex}\beta$ یا $\beta\preceq_{lex}\alpha$. بنابراین ترتیب الفبایی یک ترتیب کلی است. حال فرض کنید $\alpha\prec_{lex}\beta$ و $\gamma\in\mathbb{N}^n$. پس اولین مؤلفه ناصفر $\beta-\alpha$ مثبت است. از آن‌جایی که $(\beta+\gamma)-(\alpha+\gamma)=\beta-\alpha$، داریم $\alpha+\gamma\prec_{lex}\beta+\gamma$. در پایان واضح است که برای هر $\alpha\in\mathbb{N}^n$، $\alpha=(0,\dots,0)$ و یا اولین مؤلفه ناصفر $\alpha=\alpha-(0,\dots,0)$ مثبت است. بنابراین ترتیب الفبایی یک ترتیب تک‌جمله‌ای است.
□

تعریف ۳-۷ (ترتیب الفبایی مدرج). فرض کنید $\alpha,\beta\in\mathbb{N}^n$. گوییم $\alpha\prec_{dlex}\beta$ هرگاه

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

یا اگر $|\alpha|=|\beta|$، آنگاه $\alpha\prec_{lex}\beta$.

مثال ۳-۸. $(0,2,5,0)\prec_{dlex}(1,2,3,0)$ و $(1,2,5,2)\prec_{dlex}(1,2,3,4)$. پس برای مثال در حلقه $K[x,y,z,w]$ داریم $xy^2z^3\prec_{dlex}y^2z^5$ و $xy^2z^5w^2\prec_{dlex}xy^2z^3w^4$.

مثال ۳-۹. از آن‌جایی که $\boldsymbol{e}_1\prec_{dlex}\dots\prec_{dlex}\boldsymbol{e}_n$، بنابراین در $K[x_1,\dots,x_n]$ داریم $x_1\prec_{dlex}\dots\prec_{dlex}x_n$.

تعریف ۳-۱۰ (ترتیب الفبایی معکوس مدرج). فرض کنید $\alpha,\beta\in\mathbb{N}^n$. گوییم $\alpha\prec_{drl}\beta$ هرگاه $|\alpha|<|\beta|$ یا $|\alpha|=|\beta|$ و سمت راست‌ترین مؤلفه ناصفر $\beta-\alpha$ منفی باشد.

مثال ۳-۱۱. اگر $\alpha=(2,3,5)$ و $\beta=(3,2,5)$، آنگاه $\beta-\alpha=(1,-1,0)$. بنابراین $\alpha\prec_{drl}\beta$. پس در $K[x,y,z]$ داریم $x^3y^2z^5\prec_{drl}x^2y^3z^5$.

مثال ۳-۱۲. در $K[x_1,\dots,x_n]$ می‌توان نوشت $x_1\prec_{drl}\dots\prec_{drl}x_n$.

تعریف ۳-۱۳ (ترتیب ضربی). فرض کنید $\prec_x$ یک ترتیب تک‌جمله‌ای روی حلقه $K[x_1,\dots,x_n]$ و $\prec_y$ یک ترتیب تک‌جمله‌ای روی حلقه $K[y_1,\dots,y_m]$ باشند. در این صورت، ترتیب ضربی $\prec_x$ و $\prec_y$ که یک ترتیب تک‌جمله‌ای روی $K[x_1,\dots,x_n,y_1,\dots,y_m]$ است را با نماد $\prec_{x,y}$ نمایش می‌دهیم و به صورت زیر تعریف می‌کنیم:

$$x^\alpha y^\eta\prec_{x,y}x^\beta y^\gamma \text{ اگر } x^\alpha\prec_x x^\beta \text{ یا } x^\alpha=x^\beta \text{ و } y^\eta\prec_y y^\gamma.$$

مشابه گزاره ۳-۶ می‌توان نشان داد که $\prec_{dlex}$، $\prec_{drl}$ و ضرب دو ترتیب تک‌جمله‌ای، ترتیب‌های تک‌جمله‌ای هستند.

تبصره ۳-۱۴. در تعریف‌های بالا، متناظر تک‌جمله‌ای $x_1^{\alpha_1}\dots x_n^{\alpha_n}$، n-تایی مرتب $(\alpha_1,\dots,\alpha_n)$ را در نظر گرفتیم و بر اساس آن، یک ترتیب تک‌جمله‌ای را تعریف کردیم. لازم به ذکر است که در عمل، نیاز به تثبیت موقعیت متغیرها نیست و موقعیت متغیرها را با استفاده از ترتیب تک‌جمله‌ای معرفی می‌کنیم. برای مثال وقتی می‌نویسیم $x\prec_{lex}y\prec_{lex}z$، یعنی متناظر $x^2y^3z^5$، ۳-تایی $(5,3,2)$ را در نظر می‌گیریم و از این نمایش در مقایسه تک‌جمله‌ای‌ها استفاده می‌کنیم.

۲.۳ الگوریتم تقسیم در حلقه چندجمله‌ای‌های چندمتغیره

الگوریتم تقسیم در حلقه چندجمله‌ای‌های چندمتغیره سابقه طولانی در ریاضیات ندارد و می‌توان آن را به عنوان یک تعمیم طبیعی الگوریتم تقسیم در حالت تک‌متغیره در نظر گرفت. این الگوریتم یکی از ابزارهای اصلی در محاسبه پایه گربنر است و روند آن بستگی زیادی به انتخاب ترتیب تک‌جمله‌ای روی حلقه دارد. در این بخش، الگوریتم تقسیم را معرفی می‌کنیم و پس از اثبات پایان‌پذیری و درستی آن، با ارائه یک مثال، روند آن را توضیح می‌دهیم. در پایان، نسخه ساده‌تری از این الگوریتم را ارائه می‌کنیم ولی اثبات پایان‌پذیری و درستی آن، به مراتب مشکل‌تر از الگوریتم اصلی تقسیم است. در این بخش $R = K[x_1, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی R در نظر گرفته شده است.

قضیه ۱۵-۳ (الگوریتم تقسیم در حلقه چندجمله‌ای‌ها). فرض کنید $f_1, \ldots, f_k \in R$. در این صورت هر چندجمله‌ای $f \in R$ را می‌توان به صورت $f = q_1 f_1 + \ldots + q_k f_k + r$ نوشت که $q_1, \ldots, q_k, r \in R$ و $r = 0$ یا هیچ جمله‌ای از r توسط $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k)$ عاد نمی‌شود. در این حالت، $q_1, \ldots, q_k$ را خارج‌قسمت‌ها و r را یک باقیمانده تقسیم f بر $f_1, \ldots, f_k$ می‌نامیم.

اثبات. با ارائه یک الگوریتم و اثبات پایان‌پذیری و درستی آن، نشان می‌دهیم که $q_1, \ldots, q_k, r$ با ویژگی‌های بالا وجود دارند.

ابتدا نشان می‌دهیم الگوریتم پایان‌پذیر است. برای این منظور فرض کنید $q_{1i}, \ldots, q_{ki}, r_i, p_i$ نتایج بدست آمده برای $q_1, \ldots, q_k, r, p$ به ترتیب در مرحله i-ام اجرای الگوریتم باشند. پس $q_{1\circ} = \ldots = q_{k\circ} = 0$، $r_\circ = 0$ و $p_\circ = f$. در هر بار اجرای حلقه **while** دوم، یکی از حالات زیر اتفاق می‌افتد:

حالت اول: فرض کنید i وجود داشته باشد که $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$. در نتیجه $p_{j+1} = p_j - \frac{\mathrm{LT}(p_j)}{\mathrm{LT}(f_i)} f_i$. از طرفی

$$\mathrm{LT}(\tfrac{\mathrm{LT}(p_j)}{\mathrm{LT}(f_i)} f_i) = \tfrac{\mathrm{LT}(p_j)}{\mathrm{LT}(f_i)} \mathrm{LT}(f_i) = \mathrm{LT}(p_j).$$

حالت دوم: فرض کنید به ازای هر i، $\mathrm{LT}(f_i) \nmid \mathrm{LT}(p)$. پس $p_{j+1} = p_j - \mathrm{LT}(p_j)$.

بنابراین به ازای هر j داریم $\mathrm{LT}(p_{j+1}) \prec \mathrm{LT}(p_j)$. اگر الگوریتم پایان‌ناپذیر باشد، یک دنباله اکیداً نزولی نامتناهی به صورت $\mathrm{LT}(p_\circ) \prec \mathrm{LT}(p_1) \prec \ldots$ خواهیم داشت که با فرض خوش‌ترتیب بودن $\prec$ در تناقض است. بنابراین پس از متناهی‌بار اجرای الگوریتم، $p = 0$ و الگوریتم پایان می‌پذیرد.

برای اثبات درستی الگوریتم با استفاده از استقرا نشان می‌دهیم در مرحله j-ام الگوریتم

$$f = q_{1j} f_1 + \ldots + q_{kj} f_k + \ldots + p_j + r_j. \qquad (1)$$

به وضوح برای $j = 0$، حکم برقرار است. فرض کنید این تساوی در مرحله j-ام برقرار باشد و حکم را برای مرحله $(j+1)$-ام ثابت می‌کنیم. اگر در مرحله $(j+1)$-ام در حلقه **while** دوم تغییری رخ دهد، آنگاه $1 \leq i \leq k$ وجود دارد

Procedure 9 Division

Input: $f_1, \ldots, f_k \in R$ and a minimal ordering $\prec$

Output: $q_1, \ldots, q_k, r \in R$ such that $f = q_1 f_1 + \ldots + q_k f_k = r$

$p := f;\ r := 0;\ q_1 := 0; \ldots; q_k := 0$

while $p \neq 0$ **do**

$i := 1$

$flag := false$

while $i \leq k$ and $flag = false$ **do**

if $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$ **then**

$q_i := q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$

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

$flag := true$

else

$i := i + 1$

end if;

end while;

if $flag = flase$ **then**

$r := r + \mathrm{LT}(p)$

$p := p - \mathrm{LT}(p)$

end if;

end while;

return $(q_1, \ldots, q_k, r)$

end;

که $\mathrm{LT}(f_i) \mid \mathrm{LT}(p_{j+1})$. در نتیجه

$$
\begin{aligned}
& q_{1(j+1)} f_1 + \ldots + q_{i(j+1)} f_i + \ldots + q_{k(j+1)} f_k + p_{j+1} + r_{j+1} \\
&= q_{1j} f_1 + \ldots + (q_{ij} + \frac{\mathrm{LT}(p_j)}{\mathrm{LT}(f_i)}) f_i + \ldots + q_{kj} f_k + (p_j - \frac{\mathrm{LT}(p_j)}{\mathrm{LT}(f_i)} f_i) + r_j \\
&= q_{1j} f_1 + \ldots + q_{kj} f_k + p_j + r_j = f.
\end{aligned}
$$

در غیر این صورت $r_{j+1} = r_j - \mathrm{LT}(p_j)$ و $p_{j+1} = p_j - \mathrm{LT}(p_j)$. در نتیجه می‌توان نوشت

$$\begin{aligned} &q_{(j+1)}f_1 + \ldots + q_{k(j+1)}f_k + p_{j+1} + r_{j+1} \\ &= q_{1j}f_1 + \ldots + q_{kj}f_k + p_j - \mathrm{LT}(p_j) + r_j + \mathrm{LT}(p_j) = f. \end{aligned}$$

بنابراین تساوی (۱) برای هر j برقرار است. اما چون الگوریتم پایان‌پذیر است، j_0 وجود دارد که $p_{j_0} = 0$. پس $f = q_{1j_0}f_1 + \ldots + q_{kj_0}f_k + r_{j_0}$. با قرار دادن $q_i = q_{ij_0}$ و $r = r_{j_0}$، قسمت اول حکم مورد نظر ثابت می‌شود. با توجه به ساختار الگوریتم، یا هیچ جمله‌ای به r اضافه نمی‌شود که در این صورت $r = 0$ یا جملاتی به r اضافه می‌شوند که توسط $\mathrm{LT}(f_i)$ها عاد نمی‌شوند؛ یعنی هیچ جمله‌ای از r توسط $\mathrm{LT}(f_i)$ها عاد نمی‌شوند. □

مثال ۱۶-۳. در این مثال، مراحل اجرای الگوریتم بالا را برای محاسبه خارج‌قسمت‌ها و باقیمانده تقسیم $f = xy^2 + 1$ بر $f_1 = xy + 1$ و $f_2 = y + 1$ با استفاده از ترتیب $y \prec_{lex} x$ بیان می‌کنیم. ابتدا قرار می‌دهیم $p = xy^2 + 1$. چون $\mathrm{LT}(f_1) = xy \mid xy^2 = \mathrm{LT}(p)$، پس با تقسیم xy^2 بر xy داریم $q_1 = y$ و $p = -y_1$. حال چون $\mathrm{LT}(f_1) = xy \nmid -y = \mathrm{LT}(p)$ و $\mathrm{LT}(f_2) = y \mid -y$، پس با تقسیم $-y$ بر y داریم $q_2 = -1$ و $p = 2$. از آن‌جایی که $\mathrm{LT}(f_1)$ و $\mathrm{LT}(f_2)$، هیچ‌کدام ۲ را عاد نمی‌کنند، بنابراین $r = 2$ و در نتیجه $xy^2 + 1 = y(xy + 1) + (-1)(y + 1) + 2$.

مثال ۱۷-۳. باقیمانده تقسیم یک چندجمله‌ای بر یک دنباله از چندجمله‌ای‌ها در حالت کلی یکتا نیست. فرض کنید $f = x^2y + xy^2 + y^2$، $f_1 = y^2 - 1$ و $f_2 = xy - 1$ چندجمله‌ای‌هایی در $K[x, y]$ باشند و $y \prec_{lex} x$. با تقسیم f به (f_1, f_2) داریم

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

در حالی که با تقسیمf به (f_1, f_2) خواهیم داشت $f = (x + y)(xy - 1) + (y^2 - 1)(x + y + 1)$.

تبصره ۱۸-۳. فرض کنید $f, f_1, \ldots, f_k$ چندجمله‌ای‌هایی در R باشند. اگر باقیمانده تقسیم f بر $f_1, \ldots, f_k$ صفر باشد، آنگاه $f \in \langle f_1, \ldots, f_k \rangle$.

مثال ۱۹-۳. صفر نبودن باقیمانده تقسیم، شرط لازم برای عضویت f در ایده‌آل $I = \langle f_1, \ldots, f_k \rangle$ نیست. برای مثال، فرض کنید $f = xy^2 - x$، $f_1 = xy + 1$ و $f_2 = y^2 - 1$ چندجمله‌ای‌هایی در $K[x, y]$ باشند و $y \prec_{lex} x$. با تقسیم f به (f_1, f_2) داریم

$$f = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

از طرفی، با تقسیم f به (f_1, f_2) خواهیم داشت $f = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0 \in \langle f_1, f_2 \rangle$. در نتیجه تنها با تقسیم یک چندجمله‌ای f بر $f_1, \ldots, f_k$، نمی‌توان تعیین کرد f متعلق به I است یا خیر. همچنین چندجمله‌ای $yf_2 - f_1 = x + y$ متعلق به I است در حالی که باقیمانده تقسیم این چندجمله‌ای بر f_1, f_2 تحت هر ترتیب تک‌جمله‌ای و هر ترتیب f_1, f_2 برابر با $x + y$ است.

در بخش بعد، خواهیم دید که تحت چه شرایطی روی f_iها، صفر شدن باقیمانده شرط لازم و کافی برای عضویت f در $\langle f_1, \ldots, f_k \rangle$ است. در ادامه، الگوریتم ساده‌تری نسبت به الگوریتم قبل برای محاسبه باقیمانده و خارج‌قسمت تقسیم یک چندجمله‌ای بر تعدادی چندجمله‌ای معرفی می‌کنیم.

قضیه ۲۰-۳. الگوریتم ۱۰ در تعداد متناهی گام پایان می‌پذیرد و خارج‌قسمت‌ها و یک باقیمانده تقسیم f بر $f_1, \ldots, f_k$ را محاسبه کند.

Procedure 10 Division 2

Input: $f_1, \ldots, f_k \in R$ and a monomial ordering $\prec$

Output: $q_1, \ldots, q_k, r \in R$ such that $f = q_1 f_1 + \ldots + q_k f_k = r$

$p := f;\ q_1 := 0; \ldots; q_k := 0$

while $(p \neq 0)$ and $(\exists f_i,\ \mathrm{LT}(f_i) \mid am$ where am is a term in $p)$ **do**

$q_i := q_i + \frac{am}{\mathrm{LT}(f_i)}$

$p := p - \frac{am}{\mathrm{LT}(f_i)} \cdot f_i$

end while;

return $(q_1, \ldots, q_k, p)$

end;

اثبات. فرض کنید $q_{1i}, \ldots, q_{ki}, p_i$ نتایج اجرای الگوریتم در مرحله i–ام باشند. (برهان خلف) فرض کنید این الگوریتم پایان‌پذیر نباشد. در این صورت دنباله $p_0, p_1, p_2, \ldots$ وجود دارد که ایستا نیست. برای هر i چندجمله‌ای p_i را به صورت دنباله $(a_{i1}m_{i1}, \ldots, a_{ik_i}m_{ik_i})$ نمایش می‌دهیم که $p_i = a_{i1}m_{i1} + \ldots + a_{ik_i}m_{ik_i}$، $m_{ik_i} \prec \ldots \prec m_{i1}$، $a_{ij} \in K \neq 0$ و m_{ij} یک تک‌جمله‌ای است. بنابراین می‌توان ماتریسی نامتناهی در نظر گرفت که درآیه‌های ابتدایی سطر i–ام، تک جمله‌ای‌های p_i و بقیه درآیه‌های آن صفر هستند

$$\begin{aligned} p_1 &\longrightarrow m_{11}, \ldots, m_{1k_1}, 0, 0, \ldots \\ p_2 &\longrightarrow m_{21}, \ldots, m_{2k_2}, 0, 0, \ldots \\ &\vdots \end{aligned}$$

با توجه به ساختار الگوریتم، می‌دانیم $m_{11} \preceq m_{21} \preceq \ldots$. بنابراین با توجه به این که $\prec$ یک ترتیب تک‌جمله‌ای است، این دنباله ایستا و i_1 موجود است که $m_{i_11} = m_{(i_1+1)1} = \ldots$. حال ستون دوم را در نظر می‌گیریم. می‌دانیم $m_{i_12} \prec m_{i_11}$ و همچنین در ستون دوم $m_{i_12} \preceq m_{(i_1+1)2} \preceq \ldots$. در نتیجه اندیس i_2 وجود دارد که $m_{i_22} = m_{(i_j+1)j} = \ldots$. به همین ترتیب برای ستون j–ام، اندیس i_j موجود است که $m_{i_jj} = m_{(i_j+1)j}$. از طرفی چون طبق فرض الگوریتم

پایان‌ناپذیر است، پس در ماتریس مورد نظر، هیچ ستونی وجود ندارد که همه ستون‌های بعد از آن صفر باشند (در غیر این صورت، اگر آخرین ستون غیرصفر ستون j–ام باشد، با توجه به این که ستون j–ام از اندیس i_j به بعد پایاست، پس از سطر i_j–ام به بعد، چندجمله‌ای‌ها برابر هستند). بنابراین دنباله

$$\ldots \prec m_{i_3 3} \prec m_{i_2 2} \prec m_{i_1 1}$$

را خواهیم داشت که اکیداً نزولی است و این در تناقض با خوش‌ترتیبی $\prec$ است. پس الگوریتم پایان‌پذیر است. برای اثبات درستی، مشابه قضیه قبل، می‌توان برای هر i نشان داد $f = q_{1i}f_1 + \ldots + q_{ki}f_k + p_i$. با توجه به پایان‌پذیری الگوریتم، اندیس i_0 وجود دارد که $f = q_1 f_1 + \ldots + q_k f_k + p_{i_0}$ و $p_{i_0} = 0$ یا هیچ جمله‌ای از p_{i_0} توسط $LT(f_1), \ldots, LT(f_k)$ عاد نمی‌شود. □

با توجه به روند الگوریتم ۱۰ نمادگذاری زیر را معرفی می‌کنیم.

تذکر ۲۱-۳. فرض کنید $f, f_1, \ldots, f_k \in R$ و $F = \{f_1, \ldots, f_k\}$. گوییم h نتیجه یک مرحله تقسیم f بر F است و می‌نویسیم $f \longrightarrow_F h$ اگر جمله‌ای مانند X در f و عدد $1 \leq i \leq k$ وجود داشته باشد طوری که $\mathrm{LT}(f_i)$ جمله X را عاد کند و $h = f - \frac{X}{\mathrm{LT}(f_i)} f_i$. همچنین گوییم r یک باقیمانده تقسیم f بر F است و می‌نویسیم $f \longrightarrow_F^* r$ (همچنین برای نمایش این خاصیت گاهی از $r = \mathrm{rem}(f, F)$ نیز استفاده می‌کنیم) هرگاه عدد طبیعی m و دنباله $f \longrightarrow_F h_1 \longrightarrow_F \ldots \longrightarrow_F h_m = r$ موجود باشد که $\mathrm{LT}(f_i)$ برای هر i هیچ جمله‌ای از r را عاد نکند.

تعریف ۲۲-۳. ایده‌آل $I \subset R$ را یک ایده‌آل تک‌جمله‌ای می‌نامیم هرگاه توسط مجموعه‌ای از تک‌جمله‌ای‌ها تولید شود. بنابراین اگر I یک ایده‌آل تک‌جمله‌ای باشد، آنگاه $A \in \mathbb{N}^n$ وجود دارد که $I = \langle x^\alpha \mid \alpha \in A \rangle$.

مثال ۲۳-۳. برای مثال $I = \langle xy^2, y^3 \rangle \subset K[x, y]$ یک ایده‌آل تک‌جمله‌ای است و خواهیم داشت $A = \{(1, 2), (0, 3)\}$.

لم ۲۴-۳. فرض کنید $A \subset \mathbb{N}^n$، $I = \langle x^\alpha \mid \alpha \in A \rangle$ یک ایده‌آل تک‌جمله‌ای و $x^\beta \in R$ یک تک‌جمله‌ای باشد. در این صورت $x^\beta \in I$ اگر و تنها اگر $\alpha \in A$ وجود داشته باشد که $x^\alpha \mid x^\beta$.

اثبات. اگر برای $\alpha_0 \in A$ داشته باشیم $x^{\alpha_0} \mid x^\beta$، آنگاه طبق تعریف $x^\beta \in I$. برعکس، فرض کنید $x^\beta \in I$. در این صورت $h_\alpha \in R$ وجود دارند که $x^\beta = \sum_{\alpha \in A} h_\alpha x^\alpha$. برای هر $\alpha \in A$ فرض کنید $h_\alpha = \sum_{\gamma \in A_\alpha} a_{\alpha,\gamma} x^\gamma$. پس با جایگذاری h_α می‌توان x^β را به صورت

$$x^\beta = \sum_{\alpha \in A, \gamma \in A_\alpha} a_{\alpha,\gamma} x^\gamma x^\alpha$$

نوشت. بنابراین x^β باید در سمت راست این تساوی ظاهر شود و $\alpha \in A$ و $\gamma \in A_\alpha$ وجود دارد که $x^\beta = x^\gamma x^\alpha$. □

لم ۲۵-۳. فرض کنید I یک ایده‌آل تک‌جمله‌ای باشد و $f \in R$. در این صورت موارد زیر باهم معادل‌اند:

(۱) $f \in I$.

(۲) هرجمله از f متعلق به I است.

(۳) f به صورت ترکیب خطی از جملات متعلق به I نوشته می‌شود.

اثبات. (۳) ⇐ (۲) ⇐ (۱) واضح است. برای اثبات (۱) ⇐ (۳) ایده‌آل I را به صورت $\langle x^\alpha \mid \alpha \in A\rangle$ در نظر بگیرید که $A \subset \mathbb{N}^n$. اگر $f \in I$، آنگاه می‌توان نوشت $f = \sum_{\alpha\in A} h_\alpha x^\alpha$ که $h_\alpha \in R$. با بسط سمت راست این عبارت و ضرب هر جمله h_α در x^α، عضوی از I بدست می‌آید و در نتیجه f به صورت ترکیب خطی از جملات متعلق به I نوشته می‌شود. □

قضیه ۲۶-۳ (لم دیکسون). فرض کنید $A \subset \mathbb{N}^n$ و $I = \langle x^\alpha \mid \alpha \in A\rangle$ یک تک جمله‌ای در R باشد. در این صورت I را می‌توان به صورت $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(k)}\rangle$ نوشت که $\alpha(1), \ldots, \alpha(k) \in A$. یعنی I دارای یک مجموعه مولد متناهی از تک جمله‌ای‌هاست.

اثبات. اثبات را با استقرا روی n انجام می‌دهیم. اگر $n = 1$، که $I = \langle x_1^\alpha \mid \alpha \in A\rangle$ $A \subset \mathbb{N}$. فرض کنید β کوچکترین عضو A باشد. پس برای هر $\alpha \in A$، $\beta \le \alpha$. بنابراین $x_1^\alpha \mid x_1^\beta$ و $I = \langle x_1^\beta\rangle$. حال فرض کنید حکم برای $n-1$ درست باشد و همچنین $I = \langle x^\alpha \mid \alpha \in A\rangle$ در $K[x_1, \ldots, x_n]$ یک ایده‌آل تک‌جمله‌ای باشد. حال ایده‌آل تک‌جمله‌ای $J = I|_{x_n=1}$ را در حلقه $K[x_1, \ldots, x_{n-1}]$ در نظر بگیرید. طبق فرض استقرا می‌توان نوشت $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(k)}\rangle$ که $\alpha(i) = (\alpha_{i,1}, \ldots, \alpha_{i,n-1})$. با توجه به تعریف J، برای هر i، عدد طبیعی m_i موجود است که $(\alpha_{i,1}, \ldots, \alpha_{i,n-1}, m_i) \in A$. قرار می‌دهیم $m = max\{m_1, \ldots, m_k\}$ و برای هر عدد طبیعی l که $0 \le l \le m$ تعریف کنید :

$$J_l = \langle x^\beta \in K[x_1, \ldots, x_{n-1}] \mid (\beta_1, \ldots, \beta_{n-1}, l) \in A\rangle \subset K[x_1, \ldots, x_{n-1}].$$

در ادامه، با استفاده دوباره از فرض استقرا، برای هر l، می‌توان نوشت $J_l = \langle x^{\alpha_l(1)}, \ldots, x^{\alpha_l(k_l)}\rangle$ که در آن $\alpha_l(j) = (\alpha_1^{j,l}, \ldots, \alpha_{n-1}^{j,l})$ و $(\alpha_1^{j,l}, \ldots, \alpha_{n-1}^{j,l}, l) \in A$). ادعا می‌کنیم I توسط عناصر

$$\begin{aligned}
&x^{\alpha(1)}x_n^{m_1}, \ldots, x^{\alpha(k)}x_n^{m_k}\\
&x^{\alpha_0(1)}, \ldots, x^{\alpha_0(k_0)}\\
&x^{\alpha_1(1)}x_n, \ldots, x^{\alpha_1(k_1)}x_n\\
&\vdots\\
&x^{\alpha_{m-1}(1)}x_n^{m-1}, \ldots, x^{\alpha_{m-1}(k_{m-1})}x_n^{m-1}.
\end{aligned}$$

تولید می‌شود. لازم به ذکر است که این تک‌جمله‌ای‌ها، زیرمجموعه $\{x^\alpha \mid \alpha \in A\}$ هستند. برای اثبات ادعا، فرض کنید $x^\alpha x_n^p \in I$ یک تکجمله‌ای باشد که $x^\alpha \in K[x_1, \ldots, x_{n-1}]$ و $p \in \mathbb{N}$. دو حالت امکان‌پذیر است :

حالت اول: اگر $p \ge m$، آنگاه $x^\alpha \in J$. بنابراین طبق لم ۸-۳، $1 \le i \le k$ وجود دارد که $x^\alpha \mid x^{\alpha(i)}$ و $x^\alpha x_n^p \mid x^{\alpha(i)}x_n^p$.

حالت دوم: اگر $p < m$، آنگاه $x^\alpha \in J_p$. بنابراین طبق لم ۸-۳، $1 \le i \le k_p$ وجود دارد که $x^\alpha \mid x^{\alpha_p(i)}$ و $x^\alpha x_n^p \mid x^{\alpha_p(i)}x_n^p$.

بنابراین حکم مورد نظر ثابت می‌شود. □

۳.۳ پایه گربنر

پس از معرفی مقدمات مورد نیاز در بخش‌های قبل، در این بخش مفهوم پایه گربنر را معرفی می‌کنیم. یکی از ابزارهای قوی در هندسه جبری و جبر محاسباتی برای حل و تحلیل دستگاه‌های معادلات چندجمله‌ای، پایه گربنر است. این مفهوم را بوخبرگر در سال ۱۹۶۵ در رساله دکترایش معرفی کرد و بعدها آن را به افتخار استاد راهنمایش پایه گربنر نامید. او در رساله خود اولین الگوریتم محاسبه یک پایه گربنر، این پایه به یکی از ابزارهای جذاب در علوم و مهندسی تبدیل شد و مورد توجه بسیاری از مهندسین و ریاضیدانان قرار گرفت. در این بخش، فرض می‌کنیم $I \subset R = K[x_1, \ldots, x_n]$ یک ایده‌آل ناصفر و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد.

تعریف ۲۷-۳. ایده‌آل جمله پیشروی I را به صورت $\mathrm{LT}(I) = \langle \mathrm{LT}(f) \mid f \in I \rangle$ تعریف می‌کنیم.

تذکر ۲۸-۳. فرض کنید $f_1, \ldots, f_k$ چندجمله‌ای‌هایی در R باشند و $I = \langle f_1, \ldots, f_k \rangle$. در این صورت طبق تعریف $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k) \rangle \subset \mathrm{LT}(I)$، اما عکس این رابطه در حالت کلی برقرار نیست. برای مثال فرض کنید $f_1 = x^3 - 2xy$، $f_2 = x^2y - 2y^2 + x$، $I = \langle f_1, f_2 \rangle$ و $x \prec_{dlex} y$. در این صورت

$$x^2 = x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) \in I.$$

بنابراین $x^2 = \mathrm{LT}(x^2) \in \mathrm{LT}(I)$. در حالی که $\mathrm{LT}(f_1) = x^3$ و $\mathrm{LT}(f_2) = x^2y$، x^2 را عاد نمی‌کنند. پس داریم $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.

گزاره ۲۹-۳. فرض کنید I ایده‌آلی در R باشد. در این صورت:
(۱) $\mathrm{LT}(I)$ یک ایده‌آل تک‌جمله‌ای است.
(۲) چندجمله‌ای‌های $g_1, \ldots, g_t \in I$ وجود دارند که $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

اثبات. (۱) از تعریف واضح است. (۲) چون $\mathrm{LT}(I) = \langle \mathrm{LT}(f) \mid f \in I \rangle$، پس طبق لم دیکسون، چندجمله‌ای‌های $g_1, \ldots, g_t \in I$ وجود دارند که $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ و حکم برقرار است. □

قضیه ۳۰-۳ (پایه‌ای هیلبرت). هر ایده‌آل $I \subset R$ دارای یک مجموعه مولد متناهی است.

اثبات. اگر $I = \{0\}$، آنگاه $\{0\}$ مجموعه مولد متناهی مورد نظراست. بدون از دست دادن کلیت مسأله، فرض کنید $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد. حال اگر $I \neq \{0\}$ بنابر گزاره قبل چندجمله‌ای‌های $g_1, \ldots, g_t \in I$ وجود دارند به طوری که $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. ادعا می‌کنیم I برابر با $\langle g_1, \ldots, g_t \rangle$ است. به وضوح $\langle g_1, \ldots, g_t \rangle \subset I$، زیرا $g_1, \ldots, g_t \in I$. برعکس، فرض کنید $f \in I$. بنابر الگوریتم تقسیم، چندجمله‌ای‌های $q_1, \ldots, q_t, r \in R$ وجود دارند که $f = q_1g_1 + \ldots + q_tg_t + r$ که $r = 0$ یا هیچ جمله از r توسط $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ عاد نمی‌شود. از طرفی، توجه کنید که $r = f - q_1g_1 - \ldots - q_tg_t \in I$. اگر $r \neq 0$، $\mathrm{LT}(r)$ متعلق به $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ است. بنابراین، $\mathrm{LT}(r)$ باید توسط یکی از $\mathrm{LT}(g_i)$ها عاد شود که در تناقض با باقیمانده بودن r است. در نتیجه $r = 0$ و در پایان $f = q_1g_1 + \ldots + q_tg_t \in \langle g_1, \ldots, g_t \rangle$. □

تعریف ۳-۳۱. زیرمجموعه متناهی $G = \{g_1, \ldots, g_t\}$ از I را یک پایه گربنر برای I نسبت به $\prec$ گوییم هرگاه $\langle \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

مفهوم پایه گربنر برای اولین بار توسط برونو بوخبرگر در سال ۱۹۶۵ در رساله دکترایش معرفی شد. لازم به ذکر است که قبل از بوخبرگر، شیرشف در سال ۱۹۶۲ در پایه شیرشف(ـگربنر) را برای رده‌بندی و محاسبه در نظریه گروه‌ها و نظریه جبر لی معرفی کرد و دو سال بعد، هیروناکا مفهوم پایه استاندارد را برای مطالعه یک ایده‌آل در یک حلقه سری‌های توانی معرفی کرد. شیوه تعریف این دو پایه، محاسبه و کاربرد آن‌ها بسیار شبیه به پایه گربنر است.

نتیجه ۳-۳۲. عبارات زیر برقرارند:
(۱) I دارای یک پایه گربنر نسبت به $\prec$ است.
(۲) اگر $\{g_1, \ldots, g_t\}$ یک پایه گربنر برای I باشد، آنگاه $I = \langle g_1, \ldots, g_t \rangle$.

مثال ۳-۳۳. فرض کنید $I = \langle g_1 := x + z, g_2 := y - z \rangle$ ایده‌آلی در $\mathbb{R}[x, y, z]$ باشد. نشان می‌دهیم $G = \{g_1, g_2\}$ یک پایه گربنر برای I نسبت به ترتیب $z \prec_{lex} y \prec_{lex} x$ است. برای این کار، توجه کنید که $G \subset I$. نشان می‌دهیم جمله پیشروی هر عضو غیرصفر I، در ایده‌آل $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2) \rangle = \langle x, y \rangle$ قرار می‌گیرد یا به طور معادل، توسط x یا y عاد می‌شود. اگر f یک چندجمله‌ای غیرصفر در I باشد و $\mathrm{LT}(f)$ توسط x و y عاد نشود، آنگاه f باید یک چندجمله‌ای بر حسب تنها z باشد. از طرفی، f روی مجموعه زیر صفر است

$$\mathbf{V}(x + z, y - z) = \{(-t, t, t) \mid t \in \mathbb{R}\} \subset \mathbb{R}^3$$

و تنها چندجمله‌ای بر حسب z که روی این مجموعه صفر است، چندجمله‌ای صفر است که این یک تناقض است.

مثال ۳-۳۴. پایه گربنر برای یک ایده‌آل نسبت به یک ترتیب داده شده یکتا نیست. ایده‌آل مثال قبل را در نظر بگیرید. واضح است که $I = \langle x + y, y - z \rangle$. از طرفی در مثال قبل ثابت کردیم $\{x + z, y - z\}$ یک پایه گربنر برای I است و در نتیجه $\mathrm{LT}(I) = \langle x, y \rangle$. بنابراین مجموعه $\{x + y, y - z\}$ نیز یک پایه گربنر دیگر برای I است.

۴.۳ برخی ویژگی‌های پایه گربنر

در این بخش، برخی ویژگی‌های مهم پایه گربنر را بررسی می‌کنیم و در فصل بعد، به تفصیل به کاربردهای پایه گربنر خواهیم پرداخت. به عنوان مهمترین ویژگی، ثابت می‌کنیم که باقیمانده تقسیم یک چندجمله‌ای بر یک پایه گربنر یکتاست. در این بخش فرض می‌کنیم $R = K[x_1, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد.

تعریف ۳-۳۵. مجموعه متناهی $G \subset R$ را یک پایه گربنر گوییم هرگاه G یک پایه گربنر برای $\langle G \rangle$ باشد.

گزاره ۳-۳۶. فرض کنید $f \in R$ و $G = \{g_1, \ldots, g_t\} \subset R$ یک پایه گربنر باشد. در این صورت باقیمانده تقسیم f بر G یکتاست.

اثبات. با استفاده از الگوریتم تقسیم، چندجمله‌ای‌های $r, q_1, \ldots, q_t$ متعلق به R وجود دارند به طوری که $f = q_1 g_1 + \ldots + q_t g_t + r$ که $r = 0$ یا هیچ جمله آن توسط $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ عاد نمی‌شود. فرض کنید r یکتا نباشد. بنابراین عناصر $r', q'_1, \ldots, q'_t \in R$ موجود هستند که می‌توان f را به شکل $f = q'_1 g_1 + \ldots + q'_t g_t + r'$ نوشت که r' در شرایط باقیمانده بودن صدق می‌کند. به وضوح $r - r' \in I$. اگر $r - r' \neq 0$، آنگاه

$$\mathrm{LT}(r - r') \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle .$$

در نتیجه برای یک $1 \leq i \leq t$ داریم $\mathrm{LT}(g_i) \mid \mathrm{LT}(r - r')$. از آن‌جا که $\mathrm{LM}(r - r')$ جمله‌ای از r یا r' است، پس $\mathrm{LT}(g_i)$ یکی از جملات r یا r' را عاد می‌کند که غیرممکن است و $r = r'$. □

با نمادگذاری اثبات قبل و با توجه به $q_1 g_1 + \ldots + q_t g_t \in \langle G \rangle$، می‌توان نتیجه زیر را بیان کرد.

نتیجه ۳۷-۳. فرض کنید $f \in R$ و G یک پایه گربنر برای I باشد. در این صورت چندجمله‌ای یکتای $r \in R$ و $g \in I$ موجود است که $f = g + r$ و $r = 0$ یا هیچ جمله r توسط $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ عاد نمی‌شود.

حال با استفاده از نتیجه ۳۷-۳ میتوانیم تعریف زیر را ارائه کنیم.

تعریف ۳۸-۳. فرض کنید $f \in R$ و G یک پایه گربنر باشد. باقیمانده تقسیم f بر G را شکل متعارف f می‌نامیم و با نماد $\mathrm{NF}_G(f)$ نمایش می‌دهیم.

با استفاده از این نتایج، می‌توانیم به مسأله تعلق به ایده‌آل پاسخ می‌دهیم. این مسأله به بررسی تعلق یک چندجمله‌ای به یک ایده‌آل می‌پردازد که با استفاده از آن می‌توان تعیین کرد آیا یک دستگاه معادلات ریشه دارد یا خیر.

نتیجه ۳۹-۳. فرض کنید G یک پایه گربنر برای ایده‌آل $I \subset R$ باشد. در این صورت $f \in I$ اگر و تنها اگر $\mathrm{NF}_G(f) = 0$.

مثال ۴۰-۳. فرض کنید $R = K[x, y]$ و $x \prec_{dlex} y$. همچنین فرض کنید I ایده‌آل تولید شده توسط $f_1 = x^2 - y$ و $f_2 = xy - x$ باشد. قرار دهید $f = y^2 - y$. برای بررسی تعلق f به I، باید یک پایه گربنر برای I بدست آوریم. در بخش بعد خواهیم دید که $G = \{f_1, f_2, f_3\}$ یک پایه گربنر برای I است که $f_3 = y^2 - x^2$. با تقسیم f بر G داریم

$$f \longrightarrow_{f_2} f - f_3 = x^2 - y \longrightarrow_{f_1} 0$$

و در نتیجه $f \in I$، در حالی که با تقسیم f بر f_1 و f_2، نمی‌توان این تعلق را اثبات کرد.

تذکر ۴۱-۳. اگر $G \subset R$ یک مجموعه متناهی باشد، مجموعه $\{\mathrm{LT}(g) \mid g \in G\}$ را با نماد $\mathrm{LT}(G)$ نمایش می‌دهیم.

قضیه ۴۲-۳. فرض کنید $I \subset R$ یک ایده‌آل باشد و $G = \{g_1, \ldots, g_t\} \subset I$. دراین صورت عبارات زیر معادل‌اند:
(۱) G یک پایه گربنر برای I است.
(۲) برای هر $f \in I$، باقیمانده تقسیم f بر G صفر است.
(۳) $f \in I$ اگر و تنها اگر $h_1, \ldots, h_t \in R$ وجود داشته باشند طوری که $f = \sum_{i=1}^{t} h_i g_i$ و همچنین

$$\mathrm{LM}(f) = \max_{\prec}\{\mathrm{LM}(h_i)\mathrm{LM}(g_i) \mid ۱ \le i \le t\}.$$

اثبات. (۱) $\Leftarrow$ (۲) همان نتیجه ۳۹-۳ است. (۲) $\Leftarrow$ (۳) اگر $f \in I$، طبق فرض $\mathrm{rem}(f, G) = ۰$. بر اساس الگوریتم تقسیم، $h_۱, \ldots, h_t \in R$ وجود دارند که $f = \sum_{i=۱}^{t} h_i g_i$. با توجه به روند الگوریتم $\mathrm{LM}(f) = \max_{\prec}\{\mathrm{LM}(h_i)\mathrm{LM}(g_i) | ۱ \le i \le t\}$. (۳) $\Leftarrow$ (۱) با توجه به تعریف پایه گربنر، باید ثابت کنیم $\langle \mathrm{LT}(G)\rangle = \mathrm{LT}(I)$. کافیست ثابت کنیم برای هر $f \in I$، $\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$. طبق فرض

$$f = \sum_{i=۱}^{t} h_i g_i, \quad \mathrm{LM}(f) = \max_{\prec}\{\mathrm{LM}(h_i)\mathrm{LM}(g_i) \mid ۱ \le i \le t\}.$$

حال اگر برای هر i داشته باشیم $\mathrm{LM}(f) \neq \mathrm{LM}(h_i)\mathrm{LM}(g_i)$، پس $\mathrm{LM}(f) \prec \mathrm{LM}(h_i)\mathrm{LM}(g_i)$ و $\mathrm{LM}(f) \prec \mathrm{LM}(f)$ که یک تناقض است. بنابراین $۱ \le i \le t$ وجود دارد که $\mathrm{LM}(f)$ برابر با $\mathrm{LM}(h_i)\mathrm{LM}(g_i)$ است و $\mathrm{LM}(g_i) \mid \mathrm{LM}(f)$. □

در مثال زیر، مجموعه مولدی برای یک ایده‌آل معرفی می‌کنیم که رابطه (۳) برای آن برقرار نیست و نشان می‌دهیم که این مجموعه، یک پایه گربنر نیست.

مثال ۴۳-۳. فرض کنید $R = K[x, y]$، $f_۱ = x^۲ - y$، $f_۲ = xy - x$ و $I = \langle f_۱, f_۲\rangle$. ترتیب تک‌جمله‌ای $x \prec_{dlex} y$ را روی R در نظر بگیرید. بنابراین چندجمله‌ای

$$f := yf_۱ - xf_۲ = -y^۲ + x^۲$$

متعلق به I است. با توجه به اینکه $\mathrm{LT}(f) = -y^۲ \notin \langle \mathrm{LT}(f_۱), \mathrm{LT}(f_۲)\rangle = \langle x^۲, xy\rangle$، بنابراین $\{f_۱, f_۲\}$ یک پایه گربنر برای I نیست. از طرفی باقیمانده تقسیم f بر $\{f_۱, f_۲\}$ صفر نیست و f به صورت $yf_۱ - xf_۲$ نوشته می‌شود که در آن $\mathrm{LM}(f) = y^۲ \prec_{dlex} \mathrm{LM}(yf_۱) = \mathrm{LM}(xf_۲) = x^۲y$.

تذکر ۴۴-۳. یک نکته قابل توجه این است که فرض $G \subset I$ در قضیه ۴۲-۳ ضروری است. برای مثال اگر $I = \langle x^۲, y^۲\rangle$، $G = \{x, y\}$ و $y \prec_{lex} x$، آنگاه G یک پایه گربنر است و $I \subset \langle G\rangle$. پس باقیمانده تقسیم هر $f \in I$ بر G برابر صفر است، در حالی که G یک پایه گربنر برای I نیست زیرا $G \nsubseteq I$.

مثال ۴۵-۳. فرض کنید $R = K[x, y, z]$، $f_۱ = y - x$، $f_۲ = y - x$ و $I = \langle f_۱, f_۲\rangle$. ترتیب تک‌جمله‌ای $x \prec_{lex} y \prec_{lex} z$ را روی R در نظر بگیرید. نشان می‌دهیم $G = \{f_۱, f_۲\}$ یک پایه گربنر برای I است. با استفاده از قضیه ۴۲-۳ فرض کنید $f \in I$ یک چندجمله‌ای دلخواه باشد. اگر جمله پیشروی f شامل y یا z باشد حکم ثابت است. در غیر این صورت، $f \in K[x]$. از طرفی چون $f \in I$ پس $h_۱, h_۲ \in R$ موجود است که $f = (y-x)h_۱ + (z+x)h_۲$. چون y در f ظاهر نمی‌شود پس اگر در سمت راست این تساوی قرار دهیم $y = x$، آنگاه $f = (z + x)h_۲(x, x, z)$. بنابراین $z + x$ چندجمله‌ای f را عاد می‌کند که در تناقض با فرض $f \in K[x]$ است و G یک پایه گربنر برای I است.

در ادامه، برای معرفی یک رده‌بندی جدید برای پایه‌های گربنر به لم زیر نیاز داریم.

لم ۴۶-۳. فرض کنید برای هر $f \in R$، باقیمانده تقسیم f بر $G = \{g_1, \ldots, g_t\}$ یکتا باشد، $g \in R$، $c \in K$ مخالف صفر و $cX \in R$ یک جمله باشد. اگر $g \longrightarrow^*_G r$، آنگاه برای هر $1 \leq i \leq t$ داریم $g - cXg_i \longrightarrow^*_G r$.

اثبات. سه حالت را در نظر بگیرید :
حالت اول: $\mathrm{LT}(cXg_i) = \mathrm{LT}(g)$. در این صورت $g \longrightarrow_{g_i} g - cXg_i$ را می‌توان یک مرحله از تقسیم g بر G در نظر گرفت. چون باقیمانده تقسیم g بر G یکتاست، پس با ادامه تقسیم، باقیمانده r خواهد بود و در نتیجه $g - cXg_i \longrightarrow^*_G r$.
حالت دوم: $\mathrm{LM}(cXg_i) = \mathrm{LM}(g)$ و $\mathrm{LT}(cXg_i) \neq \mathrm{LT}(g)$. در این حالت تک‌جمله‌ای $X\mathrm{LM}(g_i)$ در چندجمله‌ای $g - cXg_i$ وجود دارد و در نتیجه می‌توان نوشت

$$g - cXg_i \longrightarrow_{g_i} g \longrightarrow^*_G r.$$

حالت سوم: $\mathrm{LM}(cXg_i) \neq \mathrm{LM}(g)$. مشابه حالت دوم، جمله $cX\mathrm{LT}(g_i)$ در $g - cXg_i$ وجود دارد و بنابراین $g - cXg_i \longrightarrow_{g_i} g \longrightarrow^*_G r$. □

قضیه ۴۷-۳. فرض کنید $G \subset R$ یک مجموعه متناهی و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد. در این صورت G یک پایه گربنر است اگر و تنها اگر برای هر $f \in R$، باقیمانده تقسیم f بر G یکتا باشد.

اثبات. در گزاره ۳۶-۳ ثابت کردیم باقیمانده تقسیم هر چندجمله‌ای $f \in R$ بر G یکتاست. برای اثبات رابطه عکس، با توجه قضیه ۴۲-۳، کافیست ثابت کنیم اگر $f \in \langle G \rangle$، آنگاه $f \longrightarrow^*_G 0$. از آن‌جایی که $f \in \langle G \rangle$، می‌توان نوشت $f = h_1 g_1 + \ldots + h_t g_t$ که $h_i \in R$. فرض کنید باقیمانده تقسیم f بر G برابر r باشد و $h_1 = c_1 X_1 + \ldots + c_s X_s$. با استفاده لم ۴۶-۳ داریم $f - c_1 X_1 g_1 \longrightarrow^*_G r$. با استقرا می‌توان نشان داد که $f - c_1 X_1 g_1 - \ldots - c_s X_s g_1 \longrightarrow^*_G r$. بنابراین $f - h_1 g_1$. به همین ترتیب می‌توان ثابت کرد $f - h_1 g_1 - \ldots - h_t g_t \longrightarrow^*_G r$. با توجه به این که $f - h_1 g_1 - \ldots - h_t g_t = 0$ و باقیمانده تقسیم صفر بر G برابر صفر است، پس $r = 0$ و حکم مورد نظر اثبات می‌شود. □

۵.۳ محاسبه پایه گربنر

محاسبه پایه گربنر یکی از چالش‌های جدی در جبر محاسباتی است و در حوزه نظریه پیچیدگی به عنوان یک مسأله خیلی دشوار محسوب می‌شود. بنابراین یافتن یک الگوریتم بهتر همواره مورد توجه ریاضی‌دانان بوده است. در این بخش، پس از بیان مقدمات مورد نیاز، قضیه محک بوخبرگر را بیان و با استفاده از آن، الگوریتم بوخبرگر را برای محاسبه پایه گربنر ارائه می‌کنیم. در پایان با ارائه یک مثال، روند این الگوریتم را شرح خواهیم داد. در این بخش، فرض می‌کنیم $R = K[x_1, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد.

تعریف ۴۸-۳. اگر $f, g \in R$ دو چندجمله‌ای ناصفر باشند و $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$، آنگاه Sـ چندجمله‌ای f و g را به صورت زیر تعریف می‌کنیم

$$\mathrm{Spoly}(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

تذکر ۳-۴۹. با توجه به اینکه جملات $\mathrm{LT}(\frac{x^\gamma}{\mathrm{LT}(f)} \cdot f)$ و $\mathrm{LT}(\frac{x^\gamma}{\mathrm{LT}(g)} \cdot g)$ با هم برابر هستند. بنابراین در $\mathrm{Spoly}(f,g)$ حذف خواهند شد و $\mathrm{LT}(\mathrm{Spoly}(f,g)) \prec x^\gamma$.

در ادامه، محک بوخبرگر که مهمترین قضیه این بخش است را بیان و اثبات می‌کنیم.

قضیه ۳-۵۰ (محک بوخبرگر). مجموعه متناهی $G \subset R$ یک پایه گربنر است اگر و تنها اگر برای هر $g_i, g_j \in G$ داشته باشیم $\mathrm{Spoly}(g_i,g_j) \longrightarrow^*_G 0$.

اثبات. فرض کنید G یک پایه گربنر باشد. در این صورت برای هر i و j، تک‌جمله‌ای‌های $m_i, m_j \in R$ و $a_i, a_j \in K$ وجود دارند که $\mathrm{Spoly}(g_i,g_j) = a_i m_j g_j - a_j m_j g_j$. بنابراین $\mathrm{Spoly}(g_i,g_j) \in I$ که $I = \langle G \rangle$ و طبق قضیه ۳-۴۲، باقیمانده تقسیم آن بر G برابر صفر است. برای اثبات رابطه عکس، با توجه به همین قضیه کافیست ثابت کنیم برای هر $f \in I$، نمایش $f = \sum_{g\in G} h_g g$ وجود دارد که برای هر g، $\mathrm{LM}(h_g g) \preceq \mathrm{LM}(f)$. از تعلق $f \in I$، چندجمله‌ای $q_g \in R$ وجود دارند که $f = \sum_{g\in G} q_g g$. برای سهولت، q_gها را به صورت جمع تعدادی جمله متعلق به R می‌نویسیم و بنابراین $f = \sum_{i=1}^{l} a_i m_i g_i$ که m_iها تک‌جمله‌ای هستند، $a_i \in K$ و g_iها لزوما متمایز نیستند. قرار می‌دهیم $s = \max_\prec\{\mathrm{LM}(m_i g_i) \mid i = 1,\dots,l\}$ و فرض کنید s کوچکترین تک‌جمله‌ای برای همه نمایش‌های ممکن برای f باشد. اگر $s = \mathrm{LM}(f)$، آنگاه نمایش $f = \sum_{i=1}^{l} a_i m_i g_i$ موجود است که $\mathrm{LM}(m_i g_i) \preceq LM(f)$ برای هر i و حکم مورد نظر اثبات می‌شود. در غیر این صورت $\mathrm{LM}(f) \prec s$. نشان می‌دهیم یک نمایش $f = \sum_{i=1}^{l'} a'_i m'_i g_i$ برای f وجود دارد که $\mathrm{LM}(m'_i, g_i) \prec s$ برای هر i. قرار می‌دهیم $n_s = |\{i \mid \mathrm{LM}(m_i g_i) = s\}|$. واضح است که $n_s > 1$. فرض کنید $n_s = 2$. برای سادگی، فرض کنید $s = \mathrm{LM}(m_1 g_1) = \mathrm{LM}(m_2 g_2)$. اما $s = m_1 \mathrm{LM}(g_1) = m_2 \mathrm{LM}(g_2)$. بنابراین داریم $s \mid \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$ و در نتیجه تک‌جمله‌ای $u \in R$ چنان موجود است که تساوی $s = u \cdot \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$ برقرار باشد. از طرفی از $n_s = 2$ و $\mathrm{LM}(f) \prec s$ داریم $a_1 m_1 \mathrm{LT}(g_1) = -a_2 m_2 \mathrm{LT}(g_2)$ و در نتیجه $a_1 \mathrm{LC}(g_1) = -a_2 \mathrm{LC}(g_2)$. اگر قرار دهیم $a = a_1 \mathrm{LC}(g_1) = -a_2 \mathrm{LC}(g_2)$، آنگاه می‌توان نوشت

$$\begin{aligned}
au \cdot \mathrm{Spoly}(g_1,g_2) &= au\Big(\frac{\mathrm{lcm}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))}{\mathrm{LT}(g_1)} \cdot g_1 - \frac{\mathrm{lcm}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))}{\mathrm{LT}(g_2)} \cdot g_2\Big) \\
&= \frac{as}{\mathrm{LT}(g_1)} \cdot g_1 - \frac{as}{\mathrm{LT}(g_2)} \cdot g_2 \\
&= \frac{am_1 \mathrm{LM}(g_1)}{\mathrm{LT}(g_1)} \cdot g_1 - \frac{am_2 \mathrm{LM}(g_2)}{\mathrm{LT}(g_2)} \cdot g_2 \\
&= a_1 m_1 g_1 + a_2 m_2 g_2.
\end{aligned}$$

با استفاده از فرض قضیه، $\mathrm{Spoly}(f_1,f_2)$ دارای نمایشی به صورت $\sum_{g\in G} p_g g$ است به طوری که داشته باشیم $LM(p_g q) \prec \mathrm{lcm}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))$. بنابراین $\sum_{g\in G} up_g g$ یک نمایش برای چندجمله‌ای $a_1 m_1 g_1 + a_2 m_2 g_2$ است که $s = u\,\mathrm{lcm}(\mathrm{LM}(g_1),\mathrm{LM}(g_2)) \succ u\mathrm{LM}(p_g g)$. در نتیجه با جایگزینی $\sum_{g\in G} up_g g$ به جای $a_1 m_1 g_1 +$

$a_۲m_۲g_۲$ در نمایش f، می‌توان یک نمایش به صورت $\sum_{g\in G} up_g g + \sum_{i=۳}^{l} a_i m_i g_i$ برای f معرفی کرد که بیشترین جمله آن از s کوچکتر است و این در تناقض با کمینه بودن s است. حال فرض کنید $n_s > ۲$ و بدون از دست دادن کلیت مسأله فرض کنید $\mathrm{LM}(m_i g_i) = s$ برای $i = ۱, \ldots, n_s$. فرض کنید $\sum_{i=۱}^{l} a_i m_i g_i$ نمایشی برای f باشد که n_s کمینه باشد. در این صورت $f = \sum_{i=۱}^{l} a_i m_i g_i$ را می‌توان به شکل

$$a_۱ m_۱ g_۱ - \tfrac{a_۱ \mathrm{LC}(g_۱)}{\mathrm{LC}(g_۲)} m_۲ g_۲ + (a_۲ + \tfrac{a_۱ \mathrm{LC}(g_۱)}{\mathrm{LC}(g_۲)}) m_۲ g_۲ + \textstyle\sum_{i=۳}^{l} a_i m_i g_i$$

نوشت. بنابراین $\mathrm{LT}(\frac{a_۱ \mathrm{LC}(g_۱)}{\mathrm{LC}(g_۲)} m_۲ g_۲) = \mathrm{LT}(a_۱ m_۱ g_۱)$ و در نتیجه با استفاده از استدلال قسمت اول می‌توان $a_۱ m_۱ g_۱ - \frac{a_۱ \mathrm{LC}(g_۱)}{\mathrm{LC}(g_۲)} m_۲ g_۲$ را با نمایشی مانند $\sum_{g\in G} p_g g$ جایگزین کرد که $\mathrm{LM}(p_g g) \prec s$ برای هر g. بنابراین نمایش جدید f به صورت

$$\textstyle\sum_{g\in G} p_g g + (a_۲ + \frac{a_۱ \mathrm{LC}(g_۱)}{\mathrm{LC}(g_۲)}) m_۲ g_۲ + \sum_{i=۳}^{l} a_i m_i g_i$$

است که تعداد مؤلفه‌های آن با تک‌جمله‌ای پیشروی s، برابر با $n_s - ۱$ است. این موضوع با کمینه بودن n_s در تناقض است. در نتیجه s نمی‌تواند بزرگتر از $\mathrm{LM}(f)$ باشد و حکم اثبات می‌شود. □

تذکر ۵۱-۳. فرض کنید I یک ایده‌آل R، $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد و $G \subset I$. در این صورت اگر برای هر $g_i, g_j \in G$ داشته باشیم $\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G ۰$، نمی‌توان در حالت کلی ادعا کرد که G یک پایه گربنر برای I است. برای مثال اگر $I = \langle x, y\rangle$، $x \prec_{lex} y$ و $G = \{x\}$، آنگاه G دارای شرط بالاست، در حالی که G یک پایه گربنر برای I نیست، زیرا یک مجموعه مولد I نیست.

نتیجه ۵۲-۳. فرض کنید I یک ایده‌آل R، $\prec$ یک ترتیب چندجمله‌ای روی R باشد و $G \subset I$ یک مجموعه مولد I باشد. در این صورت G یک پایه گربنر برای I است اگر و تنها اگر برای هر $g_i, g_j \in G$ داشته باشیم $\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G ۰$.

اثبات. با استفاده از قضیه ۵۰-۳، G یک پایه گربنر برای $\langle G\rangle$ است اگر و تنها اگر برای هر $g_i, g_j \in G$ داشته باشیم $\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G ۰$. با توجه به اینکه $I = \langle G\rangle$، حکم مورد نظر اثبات می‌شود. □

نتیجه ۵۳-۳. فرض کنید $G \subset R$ و $\prec$ یک ترتیب چندجمله‌ای روی R باشد. در این صورت:
(۱) اگر $|G| = ۱$، آنگاه G یک پایه گربنر است.
(۲) اگر G مجموعه‌ای از جملات باشد، آنگاه G یک پایه گربنر است.

اثبات. (۱) با توجه به اینکه به ازای $f \in G$ داریم $\mathrm{Spoly}(f, f) = ۰$، G یک پایه گربنر است (قضیه ۵۰-۳).
(۲) فرض کنید $g_i, g_j \in G$. چون g_i و g_j جمله هستند، پس می‌توان نوشت $g_i = c_i m_i$ و $g_j = c_j m_j$ که $c_i, c_j \in K$ و m_i و m_j تک‌جمله‌ای هستند. بنابراین اگر $x^\gamma = \mathrm{lcm}(m_i, m_j)$، آنگاه با توجه به تعریف داریم

$$\mathrm{Spoly}(g_i, g_j) = \tfrac{x^\gamma}{c_i m_i} \cdot -\tfrac{x^\gamma}{c_j m_j} \cdot c_j m_j = ۰.$$

در نتیجه طبق قضیه ۵۰-۳، G یک پایه گربنر است. □

مثال ۵۴-۳. فرض کنید $I = \langle x^۲, xy\rangle \subset K[x,y]$. بنابراین $G = \{x^۲, xy\}$ یک پایه گربنر برای I نسبت به هر ترتیب تک‌جمله‌ای است.

مثال ۵۵-۳. با استفاده از محک بوخبرگر نشان می‌دهیم مجموعه معرفی شده در قضیه ۲ – ۵ – ۶ یک پایه گربنر است. قرار می‌دهیم $G = \{f_۱, f_۲, f_۳\}$ که $f_۱ = x^۲ - y$، $f_۲ = xy - x$ و $f_۳ = y^۲ - x^۲$. ترتیب تک‌جمله‌ای را $x \prec_{dlex} y$ در نظر می‌گیریم. به راحتی مشاهده می‌شود

$$\mathrm{Spoly}(f_۲, f_۳) = y(xy - x) - x(y^۲ - x^۲) = x^۳ - xy \longrightarrow_{f_۱} ۰.$$

به طور مشابه باقیمانده $\mathrm{Spoly}(f_۱, f_۲)$ و $\mathrm{Spoly}(f_۱, f_۲)$ بر G برابر صفر است و در نتیجه طبق محک بوخبرگر، G یک پایه گربنر است

در پایان این بخش، بر اساس قضیه ۵۰-۳، الگوریتم بوخبرگر را برای محاسبه پایه گربنر بیان و اثبات می‌کنیم. این الگوریتم توسط برونو بوخبرگر در سال ۱۹۶۵ در رساله دکترایش ارائه شد.

Procedure 11 Buchberger

Input: $F = \{f_1, \ldots, f_k\}$ a monomial ordering $\prec$

Output: A Groebner basis G for $\langle F\rangle$ w.r.t $\prec$

$G := F$

$P := \{\{g_i, g_j\} \mid g_i, g_j \in G,\ g_i \neq g_j\}$

while $p \neq \emptyset$ **do**

Select $\{g_i, g_j\} \in P$

$p := p \setminus \{\{g_i, g_j\}\}$

$\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G h$

if $h \neq 0$ **then**

$P := P \cup \{\{g_i, g_j\}\}$

$G := G \cup \{h\}$

end if;

end while;

return (G)

end;

قضیه ۵۶-۳ (الگوریتم بوخبرگر). فرض کنید $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد و همچنین $F = \{f_۱, \ldots, f_k\}$ مجموعه‌ای از چندجمله‌ای از چندجمله‌ای‌های غیرصفر در R باشد. در این صورت الگوریتم ۱۱ پایان‌پذیر است و خروجی آن، یک پایه گربنر برای $\langle F\rangle$ است.

اثبات. ابتدا با استفاده از برهان خلف نشان می‌دهیم الگوریتم پایان‌پذیر است. فرض کنید G_i نتیجه اجرای الگوریتم و h_i چندجمله‌ای بدست آمده در مرحله i–ام باشد. منظور از مرحله i–ام، مرحله‌ای است که i–امین چندجمله‌ای ناصفر تولید می‌شود. بنابراین زنجیر نامتناهی صعودی زیر را خواهیم داشت

$$F = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \dots.$$

لازم به ذکر است که برای هر i، $G_i = G_{i-1} \bigcup \{h_i\}$ و با توجه به اینکه برای هر i داریم $F \subset G_i$ و $h_i \in \langle F \rangle$، بنابراین $\dots = \langle G_0 \rangle = \langle G_1 \rangle$ و در نتیجه با استفاده از این زنجیر و نوتری بودن R، نمی‌توانیم پایان‌پذیری الگوریتم را ثابت کنیم. از طرفی چون h_i باقیمانده تقسیم یک چندجمله‌ای بر G_i است، پس $\mathrm{LT}(h_i) \notin \langle \mathrm{LT}(G_i) \rangle$. بنابراین زنجیر اکیداً صعودی

$$\langle \mathrm{LT}(G_0) \rangle \subsetneq \langle \mathrm{LT}(G_1) \rangle \subsetneq \langle \mathrm{LT}(G_2) \rangle \subsetneq \dots$$

بدست می‌آید که در تناقض با نوتری بودن R است. برای اثبات درستی الگوریتم، فرض کنید G خروجی الگوریتم بوخبرگر باشد. دقت کنید $F \subset G \subset \langle F \rangle$. بنابراین G یک مجموعه مولد برای $\langle F \rangle$ است. حال چون الگوریتم پایان‌پذیر است، با توجه به ساختار الگوریتم، برای هر $g_i, g_j \in G$، باقیمانده تقسیم $\mathrm{Spoly}(g_i, g_j)$ بر G به G اضافه می‌شود و $\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G 0$، پس طبق نتیجه ۵۲-۳، G یک پایه گربنر است. □

در ادامه این بخش، هر عضو P را یک زوج بحرانی می‌نامیم.

مثال ۵۷-۳. فرض کنید $I = \langle f_1 := x^3 - 2xy,\ f_2 := x^2y - 2y^2 + x \rangle \subset K[x,y]$ و $y \prec_{dlex} x$. با استفاده از الگوریتم بوخبرگر یک پایه گربنر برای I محاسبه می‌کنیم. با توجه به ساختار الگوریتم قرار می‌دهیم $P = \{\{f_1, f_2\}\}$. با ورود به حلقه ***while*** و انتخاب تنها زوج متعلق به P می‌توان نوشت $f_3 := \mathrm{Spoly}(f_1, f_2) = -x^2$. چون f_3 قابل تقسیم بر G نیست، f_3 را به G اضافه می‌کنیم $G = \{f_1, f_2, f_3\}$. بنابراین $P = \{\{f_1, f_3\}, \{f_2, f_3\}\}$. با انتخاب عضو دیگری از P داریم

$$\mathrm{Spoly}(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy.$$

اما $\mathrm{rem}(-2xy, G) \neq 0$. بنابراین $f_4 := -2xy$ را به G اضافه می‌کنیم. همچنین

$$\mathrm{Spoly}(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x.$$

که $-2y^2+x$ بر G قابل تقسیم نیست. پس $f_5 := -2y^2+x$ را به G اضافه می‌کنیم. بنابراین $G = \{f_1, f_2, f_3, f_4, f_5\}$ و $P = \{f_i, f_j | j = 4, 5 i < j\}$. به سادگی می‌توان نشان داد برای هر $j \leq 5$، $1 \leq i$، $\mathrm{rem}(\mathrm{Spoly}(f_i, f_j), G) = 0$. در نتیجه $P = \emptyset$ و با پایان‌یافتن حلقه ***while***، مجموعه G یک پایه گربنر برای I است.

۶.۳ پایه گربنر کمینه

در این بخش، با مفهوم پایه گربنر کمینه و برخی ویژگی‌های آن تلاش می‌کنیم عناصر اضافی یک پایه گربنر را حذف کنیم. در این بخش، فرض کنید I یک ایده‌آل حلقه $R = K[x_۱, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد. به عنوان اولین گام، به کمک لم زیر می‌توانیم با حذف اعضای غیرضروری یک پایه گربنر، یک پایه گربنر کوچکتر معرفی کنیم.

لم ۵۸-۳. فرض کنید G یک پایه گربنر برای $I \subseteq k[x_۱, \ldots, x_n]$ و $p \in G$ یک چندجمله‌ای باشد به طوری که $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$. در این صورت $G \setminus \{p\}$ هم یک پایه گربنر برای I است.

بر اساس این لم می‌توانیم تعریف زیر را بیان کنیم.

تعریف ۵۹-۳. یک پایه گربنر G برای ایده‌آل $I \subset R$ را یک پایه گربنر کمینه گوییم هرگاه برای $g \in G$ شرایط زیر برقرار باشند:

(۱) $\mathrm{LC}(g) = ۱$.

(۲) $\mathrm{LT}(g) \notin \langle \mathrm{LT}(G \setminus \{g\}) \rangle$.

مثال ۶۰-۳. ایده‌آل I در مثال ۵۷-۳ را در نظر بگیرید. دیدیم که مجموعه

$$\{f_۱ = x^۳ - ۲xy,\ f_۲ = x^۲y - ۲y^۲ + x,\ f_۳ = -x^۲,\ f_۴ = -۲xy,\ f_۵ = -۲y^۲ + x\}$$

یک پایه گربنر برای I نسبت به ترتیب $x \prec_{dlex} y$ است. چون $\mathrm{LT}(f_۱) \mid \mathrm{LT}(f_۳)$ و $\mathrm{LT}(f_۲) \mid \mathrm{LT}(f_۴)$، در نتیجه با حذف $f_۱$ و $f_۲$، مجموعه $G' = \{x^۲, xy, y^۲ - \frac{۱}{۲}x\}$ یک پایه گربنر کمینه برای I است. همچنین برای هر $a \in K$، مجموعه $G" = \{x^۲ + axy, xy, y^۲ - \frac{۱}{۲}x\}$ نیز یک پایه گربنر کمینه برای I است. بنابراین پایه گربنر کمینه، در حالت کلی یکتا نیست.

با استفاده از الگوریتم زیر می‌توان یک پایه گربنر را کمینه کرد.

قضیه ۶۱-۳.

قضیه ۶۲-۳. الگوریتم ۹ پایان‌پذیر است و خروجی آن، شرایط مورد نظر را برآورده می‌کند.

اثبات. ابتدا نشان می‌دهیم الگوریتم پایان‌پذیر است. چون هر حلقه **for** در یک مجموعه متناهی عمل می‌کند، پس الگوریتم پایان‌پذیر است. حال به اثبات درستی آن می‌پردازیم. در ابتدای الگوریتم، $G' = G$ برای I یک پایه گربنر است. اولین حلقه **for** ضرایب پیشرو را برابر ۱ می‌کند ولی تاثیری روی تک‌جمله‌ای‌های پیشرو ندارد. بنابراین در انتهای حلقه **for**، G' یک پایه گربنر است. همچنین طبق لم می‌دانیم که در حلقه‌ی **for** دوم، هر بار که عنصر p را از G' حذف کنیم، هنوز یک پایه گربنر است. در نتیجه G' یک پایه گربنر برای I است. حال باید نشان بدهیم که G' در شرط $\mathrm{LT}(p_۰) \notin \langle \mathrm{LT}(G' \setminus \{p_۰\}) \rangle$ برای هر $p_۰ \in G'$ صدق می‌کند. فرض کنید این اتفاق در حلقه دوم **for** هنگامی که به

Procedure 12 Minimal Gröbner Basis
Input: G, a Groebner basis for $I = \langle G \rangle$
Output: G', a minimal Groebner basis for I

```
G' := G
for each p ∈ G' do
  p := p/LC(p)
end for;
for each p ∈ G' do
  if exists p' ∈ G' \{p} with LT(p') divides LT(p) then
    G' := G' \{p}
  end if;
end for;
return G'
end;
```

$p_۰$ می‌رسد، رخ دهد. در این لحظه از الگوریتم، فرض کنید $G'_۰$ مقدار نظیر G' باشد. چون فقط در حلقه دوم **for** عناصر حذف می‌شوند، $G'_۰$ شامل G' است. اما $p_۰$ در G' نهایی وجود دارد؛ یعنی شرط **if** برای $p_۰$ برقرار نبوده. به عبارت دیگر، $\mathrm{LT}(p')$، $\mathrm{LT}(p_۰)$ را برای هر $p' \in G'_۰ \setminus \{p\}$ عاد نمی‌کند. پس همین روند برای هر $p' \in G'_۰ \setminus \{p_۰\}$ نیز برقرار است. در نتیجه برای هر $p_۰ \in G'$ داریم $\mathrm{LT}(p_۰) \notin \langle \mathrm{LT}(G' \setminus \{p_۰\}) \rangle$. □

گزاره ۶۳-۳. فرض کنید $G = \{g_۱, \ldots, g_t\}$ و $G' = \{g'_۱, \ldots, g'_s\}$ دو پایه گربنر کمینه برای I نسبت به ترتیب تک‌جمله‌ای $\prec$ باشند. در این صورت $s = t$ و $\mathrm{LT}(G) = \mathrm{LT}(G')$.

اثبات. ابتدا ادعا می‌کنیم نگاشت $\phi : G \to \mathrm{LT}(G)$ با ضابطه $\phi(g) = \mathrm{LT}(g)$، یک نگاشت یک به یک و پوشاست. پوشایی ϕ واضح و یک به یک بودن آن هم نتیجه ساده‌ای از کمینه بودن G است. پس $|G| = |\mathrm{LT}(G)|$. حال ادعا می‌کنیم $\mathrm{LT}(G) = \mathrm{LT}(G')$. چندجمله‌ای $g'_۱ \in G$ را در نظر می‌گیریم. چون G یک پایه گربنر برای I است، پس $g_i \in G$ وجود دارد که $\mathrm{LT}(g'_۱) \mid \mathrm{LT}(g_i)$. بدون کاستن از کلیت مسأله، می‌توانیم فرض کنیم $i = ۱$. از طرفی $g_۱ \in I$ و G' یک پایه گربنر برای I است. بنابراین $۱ \leq j \leq s$ وجود دارد که $\mathrm{LT}(g_۱) \mid \mathrm{LT}(g'_j)$. با توجه به این رابطه، $\mathrm{LT}(g'_۱) \mid \mathrm{LT}(g'_j)$ و چون G' یک پایه گربنر کمینه است، پس $j = ۱$ و در نتیجه $\mathrm{LT}(g_۱) = \mathrm{LT}(g'_۱)$ (توجه کنید که ضریب پیشروی $g_۱$ و $g'_۱$ برابر یک است). بنابراین $\mathrm{LT}(G') \subset \mathrm{LT}(G)$. به همین ترتیب می‌توان عکس این رابطه را نیز اثبات کرد و در نتیجه $\mathrm{LT}(G) = \mathrm{LT}(G')$. با توجه به ادعای ثابت شده $|\mathrm{LT}(G)| = |\mathrm{LT}(G')| = |G| = |G'|$ و $s = t$. □

در پایان این بخش، با انجام تغییرات جزئی در الگوریتم بوخبرگر، الگوریتمی ارائه می‌کنیم که در حین محاسبه پایه

گربنر، آن را کمینه کند. این روند منجر به تولید تعداد کمتری زوج در مجموعه P و در نتیجه باعث بهبود الگوریتم بوخبرگر خواهد شد.

Procedure 13 Minimal Groebner Basis

Input: $F = \{f_1, \ldots, f_k\}$ and a monomial ordernig $\prec$

Output: A minimal Groebner basis G for $\langle F \rangle$ w.r.t $\prec$

$G := F$
$P := \{\{g_i, g_j\} \mid g_i, g_j \in G,\ g_i \neq g_j\}$
while $P \neq \emptyset$ **do**
  Select $\{g_i, g_j\} \in P$
  $P := P \setminus \{\{g_i, g_j\}\}$
  $h := \mathrm{Spoly}(g_i, g_j)$
  $h := \mathrm{rem}(h, G)$
  if $h \neq 0$ **then**
    $h := h/\mathrm{LC}(h)$
    $P := P \cup \{\{g_i, g_j\} \mid g \in G\}$
    for $g \in G$ **do**
      if $\mathrm{LT}(h) \mid \mathrm{LT}(g)$ **then**
        $G := G \setminus \{g\}$
      end if;
    end for;
  end if;
end while;
return (G)
end;

قضیه ۶۴-۳. الگوریتم ۱۳ پایان‌پذیر است و خروجی آن، یک پایه گربنر کمینه برای $\langle F \rangle$ است.

اثبات. پایان‌پذیری این الگوریتم مشابه الگوریتم بوخبرگر است. اثبات درستی این الگوریتم نیز مشابه الگوریتم بوخبرگر است با این تفاوت که باید نشان دهیم $\langle G \rangle = \langle F \rangle$ و S-چندجمله‌ای هر دو عضو G در تقسیم بر G به صفر کاهش می‌یابد. برای اثبات ادعای اول فرض کنید $F = \{f_1, \ldots, f_k\}$ و G خروجی این الگوریتم باشد. A را مجموعه همه چندجمله‌ای‌های مخالف صفر f که $\mathrm{LT}(f)$ توسط $\mathrm{LT}(g)$ عاد می‌شود در نظر بگیرید که f, g چندجمله‌ای‌های محاسبه شده

در حین محاسبه پایه گربنر باشند. ابتدا نشان می‌دهیم هر عضو $f \in A$ را می‌توان به صورت ترکیبی از عناصر G نوشت که جمله پیشروی هر جمله در این ترکیب از $\mathrm{LT}(f)$ بیشتر نیست. اگر $A = \emptyset$ حکم ثابت است. در غیر این صورت، فرض کنید f کوچکترین عضو A نسبت به $\prec$ باشد (در صورت وجود چندجمله‌ای‌های با جمله پیشروی یکسان، چندجمله‌ای که زودتر محاسبه شده باشد را انتخاب می‌کنیم). بنابراین در حین محاسبه پایه گربنر، چندجمله‌ای g محاسبه می‌شود که $\mathrm{LT}(g) \mid \mathrm{LT}(f)$. توجه کنید که زوج $\{f, g\}$ به P اضافه می‌شود. از طرفی با توجه به اینکه $\mathrm{LT}(g) \mid \mathrm{LT}(f)$، داریم

$$\mathrm{Spoly}(f,g) = \frac{\mathrm{LM}(f)}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{LM}(f)}{\mathrm{LT}(g)} \cdot g = \frac{f}{\mathrm{LC}(f)} - \frac{\mathrm{LM}(f)}{\mathrm{LT}(g)} \cdot g.$$

با توجه به انجام فرآیند تکین‌سازی در این الگوریتم، $\mathrm{LC}(f) = ۱$. با تقسیم $\mathrm{Spoly}(f,g)$ بر مجموعه $\{g_۱, \ldots, g_t\}$ شامل چندجمله‌ای‌های ساخته‌شده در هنگام مطالعه این زوج، می‌توان نوشت

$$f - \frac{\mathrm{LM}(f)}{\mathrm{LT}(g)} \cdot g = \sum_{i=۱}^{t} h_i g_i + r$$

که $r, h_i \in R$. با توجه به فرض، r را می‌توان به صورت ترکیبی از عناصر G نوشت. بنابراین، می‌توان ثابت کرد برای هر i داریم $f_i \in \langle G \rangle$ و ادعای اول اثبات می‌شود. ادعای دوم هم نتیجه مستقیمی از اثبات ادعای اول است. در واقع، با استفاده از ادعای اول و درستی الگوریتم بوخبرگر، باقیمانده تقسیم S-چندجمله‌ای هر دو عضو G بر G صفر است. □

تذکر ۶۵-۳. الگوریتم بوخبرگر $F \subset G$، در حالی که این رابطه لزوماً در الگوریتم بالا برقرار نیست.

۷.۳ پایه گربنر کاهش‌یافته

در این بخش، مفهوم پایه گربنر کاهش‌یافته را معرفی می‌کنیم و نشان می‌دهیم که هر ایده‌آل نسبت به یک ترتیب تک‌جمله‌ای داده شده، یک پایه گربنر کاهش‌یافته یکتا دارد. با استفاده از این ویژگی، قادر خواهیم بود تساوی دو ایده‌آل را به راحتی بررسی کنیم. در این بخش فرض کنید I یک ایده‌آل حلقه $R = K[x_۱, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله ای روی R باشد.

تعریف ۶۶-۳. یک پایه گربنر G برای ایده‌آل $I \subset R$ را یک پایه گربنر کاهش‌یافته گوییم هرگاه برای هر $g \in G$ شرایط زیر برقرار باشند:

(۱) $\mathrm{LC}(g) = ۱$.

(۲) هیچ جمله‌ای از g متعلق به $\langle \mathrm{LT}(G \setminus \{g\}) \rangle$ نباشد.

گزاره ۶۷-۳. ایده‌آل I دارای یک پایه گربنر کاهش‌یافته یکتا نسبت به $\prec$ است.

اثبات. فرض کنید $G = \{g_۱, \ldots, g_t\}$ یک پایه گربنر کمینه برای I نسبت به $\prec$ باشد. قرار می‌دهیم $h_۱ = \mathrm{rem}(g_۱, G \setminus \{g_۱\})$ و برای هر $۲ \leq i \leq t$ تعریف می‌کنیم $h_i = \mathrm{rem}(g_i, H_i)$ که H_i برابر با $\{h_۱, \ldots, h_{i-۱}, g_{i+۱}, \ldots, g_t\}$ است. قرار دهید $H = \{h_۱, \ldots, h_t\}$. از آن‌جایی که G یک پایه گربنر کمینه است، با استفاده از استقرا می‌توان برای هر i ثابت کرد $h_i \neq ۰$، $h_i \in I$ و $\mathrm{LT}(h_i) = \mathrm{LT}(g_i)$. بنابراین

$$\langle \mathrm{LT}(h_1), \mathrm{LT}(h_t)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \mathrm{LT}(I).$$

با توجه به این تساوی و اینکه $h_1, \ldots, h_t \in I$، نتیجه می‌گیریم که H یک پایه گربنر برای I است. از طرفی، چون برای هر i، هیچ جمله‌ای از h_i توسط اعضای مجموعه

$$\{\mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_{i-1}), \mathrm{LT}(h_{i+1}), \ldots, \mathrm{LT}(g_t)\}$$

عاد نمی‌شود، مجموعه H کاهش‌یافته است. برای اثبات یکتایی، فرض کنید $H = \{h_1, \ldots, h_2\}$ و $H' = \{h'_1, \ldots, h'_t\}$ دو پایه گربنر کاهش‌یافته I نسبت به $\prec$ باشند. برای هر i می‌توان فرض کرد $\mathrm{LT}(h_i) = \mathrm{LT}(h'_i)$. نشان می‌دهیم $h_i = h'_i$. (فرض خلف) فرض کنید $h_i \neq h'_i$. پس $h_i - h'_i$ عضو غیرصفری از I است. از آن‌جایی که $\mathrm{LT}(h_i - h'_i) \prec \mathrm{LT}(h_i)$، بدون کاستن از کلیت مسأله، فرض می‌کنیم $\mathrm{LM}(h_i - h'_i)$ جمله‌ای از h_i باشد. در نتیجه j وجود دارد که $\mathrm{LT}(h_j) \mid \mathrm{LT}(h_i - h'_i)$. پس $j \neq i$ و $\mathrm{LT}(h_j)$ جمله‌ای از h_i را عاد می‌کند که در تناقض با کاهش‌یافته بودن H است. پس $h_i = h'_i$ برای هر i و حکم مورد نظر اثبات می‌شود. □

در ادامه الگوریتمی برای تبدیل یک پایه گربنر کمینه به یک پایه گربنر کاهش یافته ارائه می‌کنیم :

Procedure 14 Reduced Gröbner Basis
Input: G, a minimal Groebner basis for $I = \langle G\rangle$
Output: G', a reduced Groebner basis for I

```
G' := G
for each p ∈ G' do
    p := p̄^{G' \ {p}}
end for;
return G'
end;
```

قضیه ۶۸-۳. الگوریتم ۱۰ پایان‌پذیر است و خروجی آن، شرایط مورد نظر را برآورده می‌کند.

اثبات. الگوریتم به علت عمل کردن روی یک مجموعه متناهی، پایان‌پذیر است. درستی این الگوریتم نتیجه‌ی مستقیم اثبات قضیه است. □

مثال ۶۹-۳. در این مثال، ارتباط پایه گربنر کاهش‌یافته و شکل کاهش‌یافته سطری پلکانی یک ماتریس را بررسی می‌کنیم. برای این منظور، دستگاه معادلات خطی زیر را در نظر بگیرید

$$\begin{cases} 3x - 6y - 2z = 0 \\ 2x - 4y + 4w = 0 \\ x - 2y - z - w = 0. \end{cases}$$

فرض کنید $f_۱$، $f_۲$ و $f_۳$ به ترتیب چندجمله‌ای‌های متناظر با دستگاه بالا باشند و $I = \langle f_۱, f_۲, f_۳\rangle$. همچنین ترتیب تک‌جمله‌ای $w \prec_{lex} z \prec_{lex} y \prec_{lex} x$ را در نظر بگیرید. قرار دهید $G = \{f_۱, f_۲, f_۳\}$. در این صورت

$$\mathrm{Spoly}(f_۱, f_۲) = ۲f_۱ - ۳f_۲ = -۴z - ۱۲w.$$

اگر قرار دهیم $f_۴ = -۴z - ۱۲w$، آنگاه باقیمانده تقسیم $f_۴$ بر G برابر خودش است. پس $f_۴$ را به G اضافه می‌کنیم. با توجه به اینکه برای هر $f, g \in G$، داریم $\mathrm{Spoly}(f,g) \longrightarrow^*_G ۰$، پس G یک پایه گربنر برای I است. به وضوح، مجموعه $\{\frac{f_۴}{-۴}, \frac{f_۱}{۳}\}$ یک پایه گربنر کمینه برای I است و مجموعه $\{\frac{f_۱}{۳} + \frac{f_۴}{-۶} = x - ۲y + ۲w, \frac{f_۴}{-۴} = z + ۳w\}$، پایه گربنر کاهش‌یافته برای I است. حال ماتریس متناظر با دستگاه بالا را به صورت زیر در نظر بگیرید

$$A = \begin{bmatrix} ۳ & -۶ & -۲ & ۰ \\ ۲ & -۴ & ۰ & ۴ \\ ۱ & -۴ & ۰ & ۴ \end{bmatrix}.$$

لازم به ذکر است که انتخاب ضرایب x به عنوان ستون اول ماتریس A معادل ای است که x از بقیه متغیرها بزرگتر است. بنابراین ترتیب ستون‌های این ماتریس معادل انتخاب ترتیب تک‌جمله‌ای برای محاسبه پایه گربنر است. برای محاسبه شکل بالامثلثی ماتریس A، از عملیات سطری پلکانی استفاده می‌کنیم. برای این منظور با استفاده از سطر اول، اولین درآیه‌های سطرهای دوم و سوم را صفر خواهیم کرد. در واقع کاهش سطر دوم با استفاده از سطر اول معادل محاسبه S–چندجمله‌ای بین $f_۱$ و $f_۲$ است. با انجام این عملیات، ماتریس بالامثلثی

$$\begin{bmatrix} ۳ & -۶ & -۲ & ۰ \\ ۰ & ۰ & \frac{۴}{۳} & ۴ \\ ۰ & ۰ & ۰ & ۰ \end{bmatrix}$$

بدست می‌آید. مجموعه چندجمله‌ای‌های متناظر با سطرهای غیرصفر این ماتریس، یک پایه گربنر برای I است که با استفاده از الگوریتم بوخبرگر قابل محاسبه است. از طرفی، این ماتریس بالامثلثی را می‌توان به یک ماتریس سطری پلکانی تبدیل کرد که در آن، اولین درآیه غیرصفر هر سطر *(درآیه مؤثر)* برابر یک است. در این صورت ماتریس سطری پلکانی

$$\begin{bmatrix} ۱ & -۲ & \frac{-۲}{۳} & ۰ \\ ۰ & ۰ & ۱ & ۳ \\ ۰ & ۰ & ۰ & ۰ \end{bmatrix}$$

بدست می‌آید که مجموعه چندجمله‌ای‌های متناظر با سطری‌های غیرصفر آن، یک پایه گربنر کمینه برای I است. در پایان با استفاده از عملیات گاوس– جردن، می‌توان این ماتریس را به شکل کاهش‌یافته سطری پلکانی تبدیل کرد که در آن، همه درآیه‌های مؤثر برابر یک و بقیه درآیه‌های ستون شامل یک درآیه مؤثر برابر صفر هستند. با انجام این عملیات، ماتریس

$$\begin{bmatrix} ۱ & -۲ & ۰ & ۲ \\ ۰ & ۰ & ۱ & ۳ \\ ۰ & ۰ & ۰ & ۰ \end{bmatrix}$$

بدست می‌آید که مجموعه چندجمله‌ای‌های متناظر با سطرهای غیرصفر آن، همان پایه گربنر کاهش‌یافته برای I است.

۸.۳ الگوریتم بوخبرگر بهبودیافته

همان طور که در مثال‌های محاسبه پایه گربنر مشاهده شد بخش مهمی از زمان اجرای الگوریتم بوخبرگر، صرف محاسبه باقیمانده‌های منجر به صفر می‌شود و در واقع این زمان از دست می‌رود. یکی از چالش‌های مهم در جبر محاسباتی یافتن الگوریتمی سریع برای محاسبه پایه گربنر است. در این راستا بوخبرگر در سال ۱۹۷۹ دو محک ارائه نمود که با نصب آن‌ها روی الگوریتم خود، توانست تا حد خوبی از محاسبه کاهش‌های به صفر جلوگیری کند. در سال ۱۹۸۳، لازارد محاسبه پایه گربنر را با استفاده از ابزارهای جبرخطی انجام داد و با این کار، ارتباط مؤثری بین پایه گربنر و جبرخطی برقرار کرد. برقراری این ارتباط، به طراحی الگوریتم‌های جدیدی برای محاسبه پایه گربنر منجر شد که به دلیل استفاده از ابزارهای جبرخطی، دارای پیچیدگی کمتر و سرعت بالاتری هستند. بعد از آن، گوبر و مولر در سال ۱۹۸۸ توانستند دو محک بوخبرگر را به نحو مؤثری در الگوریتم بوخبرگر به کار برند و نسخه بهبودیافته الگوریتم بوخبرگر را معرفی نمایند. سپس در سال ۱۹۹۲ مولر، مورا و تراورسو با استفاده بهینه از کاهش‌های به صفر، سرعت این الگوریتم را تا حدودی بهبود بخشیدند. فوژر در سال ۱۹۹۹ با استفاده از ایده‌های لازارد، مولر، مورا و تراورسو، الگوریتم $F_۴$ را طراحی کرد. در طراحی و اجرای این الگوریتم، از ابزارهای پیشرفته جبرخطی استفاده می‌شود و بر همین اساس، در عمل، محاسبات را با سرعت بالایی انجام می‌دهد. فوژر در سال ۲۰۰۲، الگوریتم کامل‌تر و سریع‌تری نسبت به $F_۴$ به نام $F_۵$ را طراحی نمود. ویژگی بارز این الگوریتم این است که در اکثر موارد، هیچ کاهش به صفری را محاسبه نمی‌کند. به همین دلیل، الگوریتم $F_۵$ تاکنون به عنوان سریع‌ترین و مؤثرترین الگوریتم محاسبه پایه گربنر شناخته شده است. پس از آن گائو و همکارانش در سال‌های ۲۰۱۰ و ۲۰۱۶ با استفاده از ایده الگوریتم $F_۵$، الگوریتم‌های $G^۲V$ و GVW را به عنوان نسخه‌های تغییریافته‌ای از $F_۵$ طراحی نمودند که ساده‌تر و در عمل سریع‌تر از $F_۵$ هستند. در سال ۲۰۱۵ برکش و شرایر الگوریتمی ساده و مؤثر برای نصب محک‌های بوخبرگر روی الگوریتم بوخبرگر توصیف کردند که ما در این بخش به معرفی آن خواهیم پرداخت.

در این بخش، پس از معرفی مفهوم نمایش استاندارد یک چندجمله‌ای نسبت به یک مجموعه از چندجمله‌ای‌ها، رده‌بندی دیگری برای پایه‌های گربنر را ارائه و با استفاده از آن، محک‌های اول و دوم بوخبرگر را معرفی می‌کنیم. در ادامه، مدیریت انتخاب زوج‌های بحرانی در الگوریتم بوخبرگر را مطرح و دو محک بوخبرگر را با استفاده از روش برکش–شرایر، روی

الگوریتم بوخبرگر نصب می‌کنیم. در این بخش، فرض کنید $R = K[x_1, \ldots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد.

تعریف ۷۰-۳. فرض کنید $f \in R$ یک چندجمله‌ای ناصفر، F مجموعه‌ای متناهی از چندجمله‌ای‌ها در R و m یک تک‌جمله‌ای باشد. نمایش $f = \sum_{i=1}^{k} h_i f_i$ را یک m-نمایش برای f نسبت به F گوییم هرگاه برای هر i، $\mathrm{LM}(h_i f_i) \preceq m$ که در آن $f_i \in F$ و $h_i \in R$. اگر $m = \mathrm{LM}(f)$، آنگاه این نمایش را یک نمایش استاندارد برای f نسبت به F می‌نامیم.

مثال ۷۱-۳. فرض کنید $F = \{f_1 = xy + 1,\ f_2 = yz + 1\} \subset \mathbb{Q}[x, y]$ و همچنین $z \prec_{lex} y \prec_{lex} x$. چندجمله‌ای $f = xy^2 + x + y - z$ را در نظر بگیرید. می‌توان نوشت $f = (y - z)f_1 + xf_2$ و

$$\max_{\prec}\{\mathrm{LM}((y - z)f_1), \mathrm{LM}(xf_2)\} = xy^2 = \mathrm{LM}(f).$$

بنابراین f دارای یک نمایش استاندارد نسبت به F است.

توجه کنید که اگر یک چندجمله‌ای دارای یک نمایش استاندارد نسبت به یک مجموعه باشد، لزومی ندارد که شکل متعارف این چندجمله‌ای نسبت به آن مجموعه، برابر صفر باشد. در مثال بالا دیدیم که چندجمله‌ای f نسبت به مجموعه F دارای یک نمایش استاندارد نسبت به G باشد.

لم ۷۲-۳. مجموعه متناهی G یک پایه گربنر نسبت به $\prec$ است اگر و تنها اگر هر چندجمله‌ای ناصفر $f \in \langle G \rangle$ دارای یک نمایش استاندارد نسبت به G باشد.

اثبات. فرض کنید $f \in \langle G \rangle$ دارای یک نمایش استاندارد به صورت $f = \sum_{i=1}^{t} h_i g_i$ نسبت به مجموعه $G = \{g_1, \ldots, g_t\}$ باشد. طبق تعریف، اندیس $1 \leq i \leq t$ وجود دارد که $\mathrm{LM}(f) = \mathrm{LM}(h_i g_i)$ و در نتیجه $\mathrm{LM}(g_i) \mid \mathrm{LM}(f)$. بنابراین G یک پایه گربنر است. برعکس، فرض کنید G یک پایه گربنر باشد. در این صورت باقیمانده تقسیم هر چندجمله‌ای عضو $\langle G \rangle$ بر G برابر صفر است و دارای یک نمایش استاندارد نسبت به G است. □

قضیه ۷۳-۳. فرض کنید $G \subset R$ مجموعه‌ای از چندجمله‌ای‌های غیرصفر باشد. در این صورت G یک پایه گربنر نسبت به $\prec$ است اگر و تنها اگر برای هر $g_i, g_j \in G$، $\mathrm{Spoly}(g_i, g_j)$ برابر صفر یا دارای یک m-نمایش نسبت به G باشد که $m \prec \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$.

اثبات. نتیجه مستقیم اثبات محک بوخبرگر است. □

نتیجه ۷۴-۳. فرض کنید $G \subset R$ مجموعه‌ای متناهی از چندجمله‌ای‌های غیرصفر باشد. در این صورت G یک پایه گربنر نسبت به $\prec$ است اگر و تنها اگر برای هر $g_i, g_j \in G$، $\mathrm{Spoly}(g_i, g_j)$ برابر صفر یا دارای یک نمایش استاندارد نسبت به G باشد.

اکنون با توجه به مطالب بالا، به بیان محک‌های اول و دم بوخبرگر می‌پردازیم. این دو محک، شرایطی را برای حذف زوج‌های بحرانی بی‌فایده فراهم می‌کنند. دو تک‌جمله‌ای $m_۱$ و $m_۲$ را مجزا گوییم هرگاه $\gcd(m_۱, m_۲) = ۱$ یا به عبارت دیگر $\operatorname{lcm}(m_۱, m_۲) = m_۱ m_۲$.

گزاره ۷۵-۳ (محک اول بوخبرگر). اگر $\{f, g\} \subset R$ و تکجمله‌ای پیشروی f و g مجزا باشند، آنگاه

$$\operatorname{Spoly}(f, g) \longrightarrow^*_{\{f,g\}} ۰.$$

اثبات. فرض کنید $f = \sum_{i=۱}^{k} a_i s_i$ و $g = \sum_{j=۱}^{l} b_j t_j$ که $a_i, b_j \in K \setminus \{۰\}$، $s_k \prec \ldots \prec s_۱$ و $t_l \prec \ldots \prec t_۱$. بنابراین $\operatorname{LT}(f) = a_۱ s_۱$ و $\operatorname{LT}(g) = b_۱ t_۱$. اما از آن‌جا که $\operatorname{lcm}(s_۱, t_۱) = s_۱ t_۱$،

$$\operatorname{Spoly}(f, g) = b_۱ t_۱ f - a_۱ s_۱ g = b_۱ t_۱ \textstyle\sum_{i=۲}^{k} a_i s_i - a_۱ s_۱ \sum_{j=۲}^{l} b_j t_j.$$

نشان می‌دهیم $b_۱ t_۱ \sum_{i=۲}^{k} a_i s_i$ و $a_۱ s_۱ \sum_{j=۲}^{l} b_j t_j$ هیچ جمله مشترکی ندارند. (فرض خلف) فرض کنید $۲ \le i \le k$ و $۲ \le j \le l$ وجود داشته باشند که $t_۱ s_i = s_۱ t_j$. در این صورت $t_۱ \mid t_۱ s_i$ و $s_۱ \mid t_۱ s_i$. بنابراین

$$s_۱ t_۱ = \operatorname{lcm}(s_۱, t_۱) \mid t_۱ s_i$$

و در نتیجه $s_۱ t_۱ \preceq t_۱ s_i$، یعنی $s_۱ \preceq s_i$ که یک تناقض است. بنابراین دو چندجمله‌ای بالا، هیچ جمله مشترکی ندارند. حال برای کاهش $\operatorname{Spoly}(f, g)$ نسبت به $\{f, g\}$، $b_۲ t_۲ f, \ldots, b_l t_l f$ را به $\operatorname{Spoly}(f, g)$ اضافه می‌کنیم. در نتیجه

$$\begin{aligned}
\operatorname{Spoly}(f, g) + f \sum_{j=۲}^{l} b_j t_j &= b_۱ t_۱ \sum_{i=۲}^{k} a_i s_i + (f - a_۱ s_۱) \sum_{j=۲}^{l} b_j t_j \\
&= b_۱ t_۱ \sum_{i=۲}^{k} a_i s_i + \sum_{i=۲}^{k} a_i s_i \sum_{j=۲}^{l} b_j t_j \\
&= g \sum_{i=۲}^{k} a_i s_i \longrightarrow^*_{\{g\}} ۰.
\end{aligned}$$

□

نتیجه ۷۶-۳. فرض کنید $\{g_i, g_j\}$ یک زوج بحرانی پدید آمده در اجرای الگوریتم بوخبرگر باشد. اگر $\operatorname{LM}(g_i)$ و $\operatorname{LM}(g_j)$ مجزا باشند، آنگاه می‌توان این زوج را از الگوریتم حذف کرد.

مثال ۷۷-۳. فرض کنید $G = \{x - yz + ۱,\ y^۲ - z,\ z^۳ - z^۲ + ۱\} \subset \mathbb{Q}[x, y, z]$ و همچنین $z \prec_{lex} y \prec_{lex} x$. از آنجا که تک‌جمله‌ای پیشروی اعضای G دوبه‌دو مجزا هستند، طبق محک اول بوخبرگر، مجموعه G یک پایه گربنر است.

گزاره ۷۸-۳ (محک دوم بوخبرگر). فرض کنید F زیرمجموعه‌ای متناهی از R، $p, g_1, g_2 \in R$ و برای $i = 1, 2$ داشته باشیم:

(۱) $\mathrm{LM}(p) \mid \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$.

(۲) $\mathrm{Spoly}(g_i, p)$ دارای یک نمایش t_i–نمایش نسبت به F باشد که $t_i \prec \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(p))$.

در این صورت $\mathrm{Spoly}(g_1, g_2)$ دارای یک t–نمایش نسبت به F است که t یک تک‌جمله‌ای است و

$$t \prec \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)).$$

اثبات. طبق فرض (۱)، تک‌جمله‌ای‌های s_1 و s_2 وجود دارند که برای $i = 1, 2$

$$s_i \cdot \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(p)) = \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)).$$

به راحتی دیده می‌شود

$$\mathrm{Spoly}(g_1, g_2) = s_1 \cdot \mathrm{Spoly}(g_1, p) + s_2 \cdot \mathrm{Spoly}(p, g_2). \qquad (2)$$

از طرفی طبق فرض (۲)، نمایش‌های $\mathrm{Spoly}(g_1, p) = \sum_{i=1}^{k} p_i f_i$ و $\mathrm{Spoly}(p, g_2) = \sum_{i=1}^{k} q_i f_i$ وجود دارند که $F = \{f_1, \ldots, f_k\}$، $p_i, q_i \in F$ و

$$\max\nolimits_{\prec}\{\mathrm{LM}(p_i, f_i) \mid 1 \le i \le k\} \prec \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(p))$$
$$\max\nolimits_{\prec}\{\mathrm{LM}(p_i, f_i) \mid 1 \le i \le k\} \prec \mathrm{lcm}(\mathrm{LM}(p), \mathrm{LM}(g_2)).$$

با جایگذاری این نمایش‌ها در رابطه (۲) داریم

$$\mathrm{Spoly}(g_1, g_2) = s_1 \sum_{i=1}^{k} p_i f_i + s_2 \sum_{i=1}^{k} q_i f_i. \qquad (3)$$

همچنین برای هر $1 \le i \le k$ داریم

$$s_1 \cdot \mathrm{LM}(p_i f_i) \prec s_1 \cdot \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(p)) = \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$$
$$s_2 \cdot \mathrm{LM}(q_i f_i) \prec s_2 \cdot \mathrm{lcm}(\mathrm{LM}(p), \mathrm{LM}(g_2)) = \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)).$$

اگر قرار دهیم $t = \max_{\prec}\{s_1 \cdot \mathrm{LM}(p_i f_i), s_2 \cdot \mathrm{LM}(q_i f_i) \mid 1 \le i \le k\}$، آنگاه خواهیم داشت

$$t \prec \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$$

و در نتیجه (۳) یک t–نمایش برای $\mathrm{Spoly}(g_1, g_2)$ نسبت به G است. □

نتیجه ۷۹-۳. فرض کنید $\{g_۱, g_۲\}$ یک زوج بحرانی پدید آمده در اجرای الگوریتم بوخبرگر باشد. اگر چندجمله‌ای p در مجموعه چندجمله‌ای‌های ورودی الگوریتم یا چندجمله‌ای‌های بدست آمده در اجرای الگوریتم موجود باشد به طوری که $\mathrm{LM}(p) \mid \mathrm{lcm}(\mathrm{LM}(g_۱), \mathrm{LM}(g_۲))$ و باقیمانده زوج‌های $\{g_۱, p\}$ و $\{g_۲, p\}$ محاسبه شده باشند، آنگاه می‌توان $\{g_۱, g_۲\}$ را از الگوریتم حذف کرد.

حال با استفاده از روش برکش–شرایر چگونگی نصب این دو محک را روی الگوریتم بوخبرگر بیان می‌کنیم.

Procedure 15 Berkesch-Schreyer

Input: A finite set $F = \{f_1, \ldots, f_k\} \subset R$ and a monomial ordering $\prec$

Output: A Groebner basis G for $\langle F \rangle$ w.r.t $\prec$

$G := \{f_1\}$
$B := \emptyset$
for $i = 2, \ldots, k$ **do**
  $(G, B) :=$ Update(G, B, f_i)
end for;
while $B \neq 0$ **do**
  Select $\{g_i, g_j\} \in B$
  $B := B \setminus \{\{g_i, g_j\}\}$
  $\mathrm{Spoly}(g_i, g_j) \longrightarrow^*_G h$
  if $h \neq 0$ **then**
    $(G, B) :=$ Update(G, B, h)
  end if;
end while;
return (G)
end;

قضیه ۸۰-۳. فرض کنید $F \subset R$ مجموعه‌ای متناهی و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد. در این صورت الگوریتم ۱۵ یک پایه گربنر برای ایده‌آل $\langle F \rangle$ نسبت به $\prec$ محاسبه می‌کند.

اثبات. از آن‌جا که ساختار این الگوریتم مشابه ساختار الگوریتم بوخبرگر است، اثبات پایان‌پذیری این دو مشابه است. برای اثبات درستی این الگوریتم، کافیست نشان دهیم S–چندجمله‌ای نظیر هر زوج مرتبی که در زیرالگوریتم Update حذف می‌شود، دارای یک نمایش استاندارد نسبت به مجموعه خروجی الگوریتم است. لازم به ذکر است که حذف زوج‌های بحرانی ابتدا در ساخت مجموعه A رخ می‌دهد.

Procedure 16 Update

Input: Finite sets G, B and a polynomial $0 \neq h \in R$

Output: Update G_{new} of G and B_{new} of B

$A :=$ The minimal monomial generating set of $\langle \mathrm{LM}(g) \mid g \in G \rangle : \langle \mathrm{LM}(h) \rangle$

$B_{new} := B$ and $G_{new} := G \cup \{h\}$

for $\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h)) / \mathrm{LM}(h) \in A$ **do**

  if $\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h)) / \mathrm{LM}(h) \neq \mathrm{LM}(g)$ **then**

    $B_{new} := B_{new} \cup \{\{g, h\}\}$

  end if;

end for;

return (G_{new}, B_{new})

end;

می‌دانیم

$$\langle \mathrm{LM}(g) \mid g \in G \rangle : \langle \mathrm{LM}(h) \rangle = \langle \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h)) / \mathrm{LM}(h) \mid g \in G \rangle .$$

حال اگر $\mathrm{LM}(g_۱) \mid \mathrm{lcm}(\mathrm{LM}(g_۲), \mathrm{LM}(h)) / \mathrm{LM}(h)$، آنگاه $\mathrm{lcm}(\mathrm{LM}(g_۲), \mathrm{LM}(h)) / \mathrm{LM}(h)$ در مجموعه A حضور نخواهد داشت (فرض کنید زوج $\{g_۲, h\}$ زوجی با کمترین درجه $\mathrm{lcm}(\mathrm{LM}(g_۲), \mathrm{LM}(h))$ در اجرای الگوریتم باشد که حذف می‌شود). با توجه به ساختار الگوریتم زوج‌های $\{g_۱, h\}, \{g_۱, g_۲\}$ در B حضور خواهند داشت و مطالعه خواهند شد. بنابراین طبق محک دوم بوخبرگر، زوج $\{g_۲, h\}$ دارای یک نمایش استاندارد نسبت به مجموعه خروجی الگوریتم است. با تکرار این روش به راحتی می‌توان ثابت کرد هر زوجی که در محاسبه A حذف می‌شود غیرضروری است. حال در ادامه زیرالگوریتم Update، اگر $\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h)) / \mathrm{LM}(h) = \mathrm{LM}(g)$، آنگاه زوج نظیر آن یعنی $\{g, h\}$ حذف خواهد شد. در واقع، در صورتی که این تساوی برقرار باشد، $\mathrm{LM}(g)$ و $\mathrm{LM}(h)$ مجزا خواهند بود و زوج $\{g, h\}$ توسط محک اول بوخبرگر حذف می‌شود. □

با توجه به ساختار الگوریتم ۱۵ و اجرای آن، درمی‌یابیم که مدیریت انتخاب زوج‌های مرتب در این الگوریتم، امری مهم در بهره‌مندی از محک دوم بوخبرگر است. منظور از یک مدیریت انتخاب، مرتب کردن مجموعه زوج‌های مرتب در هر مرحله از الگوریتم است. از دیدگاه نظری، به کار بردن یک مدیریت انتخاب، در اثبات درستی یا پایان‌پذیری یک الگوریتم هیچ تأثیری ندارد؛ اما از دیدگاه محاسباتی، این امر می‌تواند در کاستن تعداد کاهش‌های به صفر مهم باشد. در ادامه، به دو نمونه از مهمترین روش‌های مدیریت انتخاب اشاره می‌کنیم.

- **مدیریت انتخاب طبیعی**: در این روش، زوج‌ها بر اساس ک.م.م. آن‌ها مرتب می‌شوند. به عبارت دقیق‌تر، فرض کنید $\{g_۱, g_۲\}$ و $\{g_۳, g_۴\}$ دو زوج مرتب باشند. اگر $\mathrm{lcm}(\mathrm{LM}(g_۱), \mathrm{LM}(g_۲))$ کوچکتر از $\mathrm{lcm}(\mathrm{LM}(g_۳), \mathrm{LM}(g_۴))$ باشد،

آنگاه زوج $\{g_۱, g_۲\}$ زودتر از $\{g_۳, g_۴\}$ انتخاب می‌شود.

• **مدیریت انتخاب پنهان:** در این روش در حین اجرای الگوریتم، به هر چندجمله‌ای، یک درجه پنهان اختصاص می‌یابد. درجه پنهان چندجمله‌ای f را با نماد $\deg_s(f)$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم:

(۱) اگر f عضو مجموعه ورودی باشد، آنگاه $\deg_s(f) = \deg(f)$.

(۲) اگر u یک تک‌جمله‌ای باشد، آنگاه $\deg_s(uf) = \deg(u) + \deg_s(f)$.

(۳) اگر f, g دو چندجمله‌ای باشند، آنگاه $\deg_s(f+g) = \max\{\deg_s(f), \deg_s(g)\}$.

در این مدیریت انتخاب، زوج‌ها براساس درجه پنهان S–چندجمله‌ای نظیر آن‌ها (از کوچک به بزرگ) مرتب می‌شوند. اگر درجه پنهان S–چندجمله‌ای دو زوج مرتب برابر باشد، آنگاه این دو زوج بر اساس مدیریت انتخاب طبیعی مرتب می‌شوند.

فصل ۴

هندسه جبری حقیقی و تجزیه جبری استوانه‌ای

۱.۴ هندسه جبری حقیقی

هندسه جبری حقیقی یکی از شاخه‌های مهم و پویای ریاضیات است که به مطالعه مجموعه‌های صفر چندجمله‌ای‌های با ضرایب حقیقی می‌پردازد. این شاخه از ریاضیات ترکیبی از مفاهیم هندسه جبری کلاسیک و تحلیل حقیقی را در بر می‌گیرد و به بررسی چندگوناهایی می‌پردازد که در فضای اقلیدسی قرار دارند و با معادلات چندجمله‌ای حقیقی تعریف می‌شوند. هندسه جبری حقیقی نقش مهمی در کاربردهای مختلف علمی و مهندسی ایفا می‌کند، از جمله در روباتیک، نظریه کنترل و بهینه‌سازی.

تاریخچه هندسه جبری حقیقی به اواخر قرن نوزدهم و اوایل قرن بیستم بازمی‌گردد و با کارهای افرادی چون دیوید هیلبرت و آلفرد تارسکی پایه‌ریزی شده است. هیلبرت به‌ویژه با مطرح کردن مسائل معروف خود در زمینه‌های مختلف ریاضیات، تأثیر بسزایی در توسعه این شاخه داشته است. یکی از مسائل مهم هیلبرت در این زمینه، مسئله هفدهم اوست که به بررسی نمایش چندجمله‌ای‌های غیرمنفی به صورت مجموع مربعات پرداخته است.

یکی از ویژگی‌های بارز هندسه جبری حقیقی، توانایی آن در بررسی خواص توپولوژیکی و هندسی چندگوناهای حقیقی است. این چندگوناها می‌توانند به صورت منحنی‌ها، سطوح و اشکال بالاتر در فضای اقلیدسی ظاهر شوند و رفتار پیچیده‌ای از خود نشان دهند. به عنوان مثال، می‌توان ویژگی‌هایی مانند تعداد نقاط حقیقی یک چندگونا، شکل و ساختار نقاط تکینگی و خواص توپولوژیکی کلی این چندگوناها را بررسی کرد.

در این فصل، ابتدا به معرفی مفاهیم پایه‌ای هندسه جبری حقیقی پرداخته و سپس به بررسی برخی از نتایج و قضایای مهم در این زمینه خواهیم پرداخت. این مفاهیم شامل واریته‌های حقیقی، نقاط حقیقی و مختلط، تجزیه نیمه‌جبری، و

نمودارهای نشان‌دار است.

هدف از این فصل، فراهم کردن یک دیدگاه جامع و منسجم از هندسه جبری حقیقی و نشان دادن اهمیت و کاربردهای گسترده آن در حوزه‌های مختلف تحقیقاتی است. با بررسی دقیق‌تر و جامع‌تر این مفاهیم، خواهیم دید که چگونه هندسه جبری حقیقی می‌تواند ابزار قدرتمندی برای تحلیل و درک ساختارهای پیچیده در فضای حقیقی باشد.

تعریف ۱-۴. فرض کنید M یک مجموعه و $\leq$ یک رابطه روی M به طوری که بازتابی، پادمتقارن و متعدی است. دوتایی $(M, \leq)$ را یک مجموعه مرتب جزئی می‌نامیم. اگر برای هر $x, y \in M$ داشته باشیم $x \leq y \vee y \leq x$، آنگاه رابطه $\leq$ را یک رابطه ترتیب کلی و $(M, \leq)$ را یک مجموعه مرتب کلی می‌نامیم.

مبحث ترتیب‌های یک میدان در ابتدا توسط آرتین[۱] و شرایر[۲] در سال ۱۹۲۷ مطرح شد.

تعریف ۲-۴. فرض کنید K یک میدان باشد.

(a) یک ترتیب روی K، رابطه ترتیب کلی $\leq$ روی مجموعه K با شرایط زیر است:

$$a \leq b \Rightarrow a + c \leq b + c \quad (۱)،$$

$$a \leq b,\ c \geq ۰ \Rightarrow ac \leq bc \quad (۲)$$

برای هر $a, b \in K$.

(b) دوتایی $(K, \leq)$ را یک میدان مرتب می‌نامیم که در آن K یک میدان و $\leq$ یک ترتیب روی K است.

(c) میدان K را حقیقی می‌نامیم هرگاه حداقل یک ترتیب برای آن وجود داشته باشد.

لم ۳-۴. فرض کنید $(K, \leq)$ یک میدان مرتب باشد و $a \in K$. در این صورت، $a \geq ۰$ معادل است با $-a \leq ۰$. همچنین اگر $a \neq ۰$، آنگاه با $\frac{۱}{a} \geq ۰$ هم معادل است. همیشه خواهیم داشت $a^۲ \geq ۰$.

اثبات. با اضافه کردن $-a$ به دو طرف عبارت $a \geq ۰$، نامساوی $-a \geq ۰$ حاصل می‌شود. از آن‌جایی که یکی از $a \geq ۰$ یا $-a \geq ۰$ برقرار است، داریم $a^۲ = (-a)^۲ \geq ۰$. اگر $a \neq ۰$، آنگاه $a = a^۲ \cdot \frac{۱}{a}$ و $\frac{۱}{a} = (\frac{۱}{a})^۲$. در نتیجه $a > ۰$ اگر و تنها اگر $\frac{۱}{a} > ۰$. □

گزاره ۴-۴. فرض کنید K یک میدان و $\leq$ یک ترتیب روی K باشد. در این صورت، مجموعه

$$P = P_{\leq} := \{a \in K \ : \ a \geq ۰\}$$

از عناصر ناصفر در شرایط زیر صدق می‌کند:

(a) $P + P \subseteq P$، $PP \subseteq P$،

(b) $P \cup (-P) = K$،

(c) $P \cap (-P) = \{۰\}$،

[۱] Artin

[۲] Schreier

$-۱ \notin P$ (c').

برعکس، اگر زیرمجموعه $P \subseteq K$ در (a) و (b) همزمان با (c) یا (c') صدق کند، آنگاه $a \leq_P b :\Rightarrow b - a \in P$ برای هر $a, b \in K$ یک ترتیب $\leq_P$ روی K تعریف می‌کند. هر زیرمجموعه P از K را که در (a)، (b) و (c) (یا (c')) صدق کند، یک مخروط مثبت از K می‌نامیم.

اثبات. در اینجا داریم $P + P := \{a + b : a, b \in P\}$ و $PP := \{ab : a, b \in P\}$. فرض کنید $\leq$ یک ترتیب روی K باشد. پس $P = \{a \in K : a \leq ۰\}$ به وضوح در (a) و (c) صدق می‌کند و شرط (b) از لم ۳-۵ نتیجه می‌شود. همچنین طبق لم قبل، $۰ < ۱^۲ = ۱$ و $۰ < -۱$.

برعکس، فرض کنید $P \subseteq K$ در شرایط (a) تا (c) صدق کرده و $\leq_P$ مانند بالا تعریف شده باشد. پس $\leq_P$ یک ترتیب کلی روی K است. اگر $a \leq_P b$ و $c \geq_P ۰$، آنگاه $b - a \in P$ و $c \in P$؛ پس $(b - a)c \in P$ و در نتیجه $ac \leq_P bc$. پس $\leq_P$ یک ترتیب روی K است. از طرفی دیگر، (c) از (a)، (b) و (c') نتیجه می‌شود. اگر عنصر ناصفر $a \in P \cap (-P)$ وجود داشته باشد، طبق (a) باید داشته باشیم $-a^۲ = a(-a) \in P$. اما از آن‌جایی که $\pm\frac{۱}{a} \in P$، داریم $\frac{۱}{a^۲} = (\pm\frac{۱}{a})^۲ \in P$. در نتیجه $-۱ = (-a^۲) \cdot \frac{۱}{a^۲} \in P$، که با (c') در تناقض است. □

تعریف ۴-۵. فرض کنید $(K, \leq)$ یک میدان مرتب باشد. علامت $a \in K$ نسبت به $\leq$، برابر است با ۱، ۰ یا -۱ هرگاه به ترتیب $a = ۰$ ،$a > ۰$ یا $a < ۰$. این علامت را با نماد $\operatorname{sign}_{\leq}(a)$ یا $\operatorname{sign}(a)$ نمایش می‌دهیم.

لازم به ذکر است که برای هر $a, b \in K$، داریم $\operatorname{sign}(ab) = \operatorname{sign}(a) \cdot \operatorname{sign}(b)$.

تعریف ۴-۶. فرض کنید $(K, \leq)$ یک میدان مرتب باشد. قدر مطلق $a \in K$ نسبت به $\leq$ برابر است با

$$|a|_{\leq} = |a| := \operatorname{sign}(a) \cdot a.$$

اگر $P \subseteq K$ یک مخروط ماکسیمال باشد، آنگاه از نمادهای $\operatorname{sign}_P(a)$ و $|a|_P$ استفاده می‌کنیم.

لم ۴-۷. قدر مطلق در روابط زیر، برای هر $a, b \in K$ صدق می‌کند:

(۱) $|a| = |-a| \geq ۰$،

(۲) $|ab| = |a| \cdot |b|$،

(۳) $|a + b| \leq |a| + |b|$ (نامساوی مثلث).

اثبات. واضح است. □

برای هر حلقه A (جابجایی و یکدار) مجموعه

$$\Sigma A^۲ := \{a_۱^۲ + \cdots + a_n^۲ : n \geq ۱, a_i \in A\}$$

را به عنوان مجموعه تمام مجموع مربعات[۳] (که اغلب به اختصار *sos* نامیده می‌شود) در A نشان می‌دهیم. امروزه بسیار رایج شده که از اصطلاح "sos" به عنوان صفت نیز استفاده می‌شود. بنابراین اغلب می‌گوییم که یک عنصر $a \in A$، *sos* است هرگاه $a \in \Sigma A^۲$.

[۳] Sums of Squares

نتیجه ۸-۴. فرض کنید K یک میدان باشد. برای هر مخروط مثبت P از K داریم $P \subseteq \Sigma K^۲$. به طور خاص، اگر K حقیقی باشد، آنگاه $-۱ \notin \Sigma K^۲$ و در نتیجه $\mathrm{char}(K) = ۰$.

اثبات. به طور مستقیم از لم ۳-۵ و گزاره ۴-۵ نتیجه می‌شود. □

فرض کنید $\mathbb{R}$ میدان اعداد حقیقی و $\leq$ رابطه ترتیب معمولی روی $\mathbb{R}$ باشد. در این صورت $(\mathbb{R}, \leq)$ یک میدان مرتب است. به ویژه، میدان اعداد حقیقی، حقیقی است. یک میدان بسته جبری مانند میدان $\mathbb{C}$ اعداد مختلط، هرگز حقیقی نیست، زیرا -۱ یک مربع است. برای p یک عدد اول، میدان $\mathbb{Q}_p$ اعداد p–ادیک حقیقی نیست زیرا -۱ مجموع مربع در $\mathbb{Q}_p$ است.

مثال ۹-۴. اگر $K_۰$ یک زیرمیدان از میدان K و P یک مخروط مثبت از K باشد، آنگاه $P_۰ := K_۰ \cap P$ یک مخروط مثبت از $K_۰$ است. می‌گوییم ترتیب $\leq_P$ روی K ترتیب $\leq_{P_۰}$ روی $K_۰$ را **توسعه** می‌دهد، یا $(K_۰, P_۰) \subseteq (K, P)$ یک گسترش میدان‌های مرتب است. این بدان معناست که رابطه ترتیب $\leq_{P_۰}$ روی $K_۰$، محدود شده رابطه ترتیب $\leq_P$ روی K است. به ویژه، هر زیرمیدان از یک میدان حقیقی خود حقیقی است، مانند $\mathbb{Q}$، $\mathbb{Q}(\sqrt{۲})$ و $\mathbb{Q}(\pi)$ که زیرمیدان‌های $\mathbb{R}$ هستند.

مثال ۱۰-۴. اگر برای دو مخروط مثبت P، Q از K داشته باشیم $P \subseteq Q$، آنگاه $P = Q$. بنابراین اگر $\Sigma K^۲$ یک ترتیب روی K باشد، تنها ترتیب ممکن روی K است. برای مثال، این برای $K = \mathbb{R}$ یا $K = \mathbb{Q}$ درست است.

به طور کلی، یک میدان حقیقی بیش از یک ترتیب دارد. برای مثال، میدان $K = \mathbb{Q}(\sqrt{۲}) = \mathbb{Q}(\alpha)$ را در نظر بگیرید که $\alpha^۲ = ۲$ است. در این صورت K دو نشاندن $\varphi_۱, \varphi_۲ : K \to \mathbb{R}$ را می‌پذیرد که با $\varphi_۱(\alpha) = \sqrt{۲} > ۰$ و $\varphi_۲(\alpha) = -\sqrt{۲} < ۰$ مشخص می‌شوند. با برگرداندن ترتیب $\mathbb{R}$ از طریق این نشاندن‌ها، دو ترتیب متفاوت $\leq_۱$، $\leq_۲$ روی K به دست می‌آید که $\alpha >_۱ ۰$ و $\alpha <_۲ ۰$ را برآورده می‌کنند.

برای مثالی جالب‌تر، به ترتیب‌های میدان توابع گویا $\mathbb{R}(t)$ در یک متغیر t اشاره می‌کنیم. با داشتن یک ترتیب $\leq$ روی $\mathbb{R}(t)$، عنصر t را نسبت به خط حقیقی $\mathbb{R}$ قرار می‌دهیم. بنابراین زیرمجموعه‌های زیر را در نظر می‌گیریم:

$$I := I_< := \{a \in \mathbb{R} \colon a < t\}, \quad J := J_< := \{a \in \mathbb{R} \colon a > t\}.$$

به وضوح $I \cap J = \varnothing$، $I \cup J = \mathbb{R}$ و $I < J$. بنابراین زوج (I, J) یک برش ددکیند از $\mathbb{R}$ است، مطابق تعریف زیر:

تعریف ۱۱-۴. فرض کنید $(M, \leq)$ یک مجموعه کاملاً مرتب باشد. یک برش ددکیند[۴] از $(M, \leq)$ زوجی (I, J) از زیرمجموعه‌های M است به طوری که $I \cup J = M$ و $I < J$ (یعنی $a < b$ برای هر $a \in I$، $b \in J$).

به بیان ساده، یک برش ددکیند از $(M, \leq)$ یک تجزیه ناسازگار از M به یک مجموعه پایین‌تر و بالاتر است.
فرض کنید $(M, \leq)$ یک مجموعه کاملاً مرتب باشد. برای هر $\xi \in M$،

[۴] Dedekind Cut

$$\xi_- := (\,]-\infty,\xi[\,,\ [\xi,\infty[\,) \text{ و } \xi_+ := (\,]-\infty,\xi]\,,\ ]\xi,\infty[\,)$$

برش‌های ددکیند از $(M,\leq)$ هستند، یکی "مستقیماً زیر" ξ و دیگری "مستقیماً بالای" ξ قرار دارد. به همراه

$$-\infty := (\varnothing, M),\ +\infty := (M,\varnothing),$$

$\xi_\pm$ شامل برش‌های بدیهی ددکیند از $(M,\leq)$ هستند. هر برش ددکیند از $(M,\leq)$ که بدیهی نباشد، آزاد نامیده می‌شود. به عبارت دیگر، یک برش ددکیند (I,J) آزاد است اگر و فقط اگر هر دو I و J ناتهی باشند، I بزرگترین عضو نداشته باشد و J کوچکترین عضو نداشته باشد. از حسابان سال اول می‌دانیم که میدان اعداد حقیقی $\mathbb{R}$ (کوشی) کامل است. این دقیقاً به این معنی است که $(\mathbb{R},\leq)$ هیچ برش ددکیند آزادی ندارد. هر میدان مرتبی غیر از $\mathbb{R}$ دارای یک برش ددکیند آزاد است. برای مثال اگر α یک عدد گنگ باشد، زوج

$$(\,]-\infty,\alpha[\cap\mathbb{Q},\ ]\alpha,\infty[\cap\mathbb{Q})$$

یک برش ددکیند آزاد از $\mathbb{Q}$ است. با داشتن هر برش ددکیند $\xi=(I,J)$ از $\mathbb{R}$ (که لزوماً غیرآزاد است)، می‌خواهیم یک ترتیب $\leq_\xi$ روی $\mathbb{R}(t)$ بسازیم که برش ξ را با توجه به مثال $\mathbb{R}(t)$ که پیش‌تر بیان شد، القا کند؛ یعنی $I<t<J$ را برآورده کند.

ابتدا این کار را برای $\xi=0_+$ انجام می‌دهیم. بنابراین می‌خواهیم یک ترتیب $\leq$ روی $\mathbb{R}(t)$ بسازیم به طوری که برای هر عدد حقیقی $\varepsilon>0$، $0<t<\varepsilon$ برقرار باشد. فرض کنید چنین ترتیبی یافت شده است. آنگاه برای هر $n\geq 1$ و هر عدد حقیقی $\varepsilon>0$، $0<t^n<\varepsilon$ برقرار است. فرض کنید $f\in\mathbb{R}[t]$ یک چندجمله‌ای ناصفر باشد، برای مثال $f=t^k g$ که در آن $k\geq 0$ و $g\in\mathbb{R}[t]$، $g(0)\neq 0$. در این صورت $\operatorname{sign}_\leq(f)=\operatorname{sign}_\leq(g)$؛ چون $t>0$. برای تعیین علامت g، می‌نویسیم:

$$g=\sum_{i=0}^{r} a_i t^i = a_0 + th$$

با $a_i\in\mathbb{R}$، $a_0\neq 0$ و $h=a_1+a_2t+\cdots+a_r t^{r-1}$. فرض کنید $|\cdot|$ قدر مطلق نسبت به ترتیب $\leq$ باشد. از آنجا که $|t|<1$، داریم

$$|h|<1+\sum_{i=1}^{r}|a_i| =: c,$$

که نتیجه می‌دهد $|th|<tc<|a_0|$؛ چون $t<\frac{|a_0|}{c}$. در نتیجه $\operatorname{sign}_\leq(f)=\operatorname{sign}_\leq(g)=\operatorname{sign}(a_0)$.

این استدلال نشان می‌دهد که در یافتن یک ترتیب $\leq$، در مورد علامت چندجمله‌ای‌ها انتخابی نداریم. بنابراین، اگر $\leq$ وجود داشته باشد، منحصر به فرد خواهد بود: برای یک تابع گویای دلخواه $f=\frac{p}{q}\in\mathbb{R}(t)$ که $p,q\in\mathbb{R}[t]$ و $q\neq 0$، از $f=\frac{1}{q^2}\cdot pq$ نتیجه می‌گیریم که $\operatorname{sign}_\leq(f)=\operatorname{sign}_\leq(pq)$.

برعکس، ساختار فوق در واقع یک ترتیب $\leq$ روی $\mathbb{R}(t)$ تعریف می‌کند. مخروط مثبت متناظر $P = P_{\circ,+}$ به صورت

$$P_{\circ,+} = \{\circ\} \cup \left\{ t^n \cdot \frac{p}{q} : \ n \in \mathbb{Z},\ p,q \in \mathbb{R}[t] \text{ و } p(\circ)q(\circ) > \circ \right\},$$

است و $P + P \subseteq P$ از $\frac{p_1}{q_1} + t^n \frac{p_2}{q_2} = \frac{p_1 q_2 + t^p p_2 q_1}{q_1 q_2}$ نتیجه می‌شود.

به روشی مشابه می‌توانیم یک مخروط مثبت $P_{\circ,-}$ بسازیم که ترتیب متناظر آن $-\varepsilon < t < \circ$ را برای هر $\varepsilon > \circ$ برآورده کند. همچنین مخروط‌های مثبت $P_{\pm\infty}$ از $\mathbb{R}(t)$ را می‌یابیم که $t - a \in P_{+\infty}$ و $a - t \in P_{-\infty}$ را برای هر $a \in \mathbb{R}$ برآورده می‌کنند. توجه کنید که همه این مخروط‌های مثبت را می‌توان از $P_{\circ,+}$ از طریق عمل استاندارد گروه $\mathrm{PGL}_2(\mathbb{R})$ تبدیل‌های موبیوس روی $\mathbb{R}(t)$ به دست آورد.

در مجموع نشان داده‌ایم که هر برش ددکیند از $\mathbb{R}$ توسط دقیقاً یک ترتیب از $\mathbb{R}(t)$ تحقق می‌یابد.

گزاره ۱۲-۴. بین ترتیب‌های میدان $\mathbb{R}(t)$ با برش‌های ددکیند $\mathbb{R}$ یک تناظر یک‌به‌یک وجود دارد، که $a_\pm$ *($a \in \mathbb{R}$)* به همراه $\pm\infty$ هستند.

فرض کنید (K, P) یک میدان مرتب دلخواه باشد. به روشی کاملاً مشابه، می‌توانیم ترتیب‌های $P_{a,\pm}$ $(a \in K)$ و $P_{\pm\infty}$ از میدان تابع گویا $K(t)$ را بسازیم که ترتیب P روی K را گسترش می‌دهند. با این حال، به طور کلی ترتیب‌هایی از $K(t)$ وجود دارند که نمی‌توان آنها را به این روش به دست آورد.

تعریف ۱۳-۴. میدان مرتب $(K, \leq)$، یا ترتیب $\leq$ روی K ارشمیدسی[۵] نامیده می‌شود اگر اصل ارشیمدس برقرار باشد:

$$\forall\, a,\ b \in K\ (b > \circ \ \Rightarrow\ \exists n \in \mathbb{N}\ \ nb > a).$$

مثال ۱۴-۴. ترتیب $\leq$ روی K ارشیمدسی است اگر و فقط اگر برای هر $a \in K$ عدد صحیح مثبت n وجود داشته باشد که $a < n$. واضح است که ترتیب یکتا روی $\mathbb{R}$ ارشیمدسی است. بنابراین هر زیرمیدان از $\mathbb{R}$ نیز اگر با ترتیب القا شده از $\mathbb{R}$ مجهز شود، ارشیمدسی خواهد بود.

مثال ۱۵-۴. میدان $\mathbb{R}(t)$ فقط ترتیب‌های غیرارشیمدسی دارد. برای مثال، با توجه به $P_{a,+}$ داریم $\frac{1}{t-a} > n$ برای هر $n \in \mathbb{N}$.

مثال ۱۶-۴. میدان $\mathbb{Q}(t)$ هم ترتیب‌های ارشیمدسی و هم غیرارشیمدسی دارد.

تعریف ۱۷-۴. اگر (K, P) و (L, Q) میدان‌های مرتب باشند، یک همریختی $\varphi : K \to L$ حفظ‌کننده ترتیب نسبت به P و Q است، هرگاه $\varphi(P) \subseteq Q$ *(و در نتیجه $P = \varphi^{-1}(Q)$)* برقرار باشد. همچنین می‌توانیم بگوییم $\varphi : (K, P) \to (L, Q)$ یک نشاندن ترتیبی است.

نتیجه بعدی بیان می‌کند که، در حد یکریختی حفظ‌کننده ترتیب، میدان‌های مرتب ارشیمدسی دقیقاً همان زیرمیدان‌های $\mathbb{R}$ هستند (با ترتیب القا شده از $\mathbb{R}$):

[۵] Archimedan

قضیه ۱۸-۴ (هولدر). برای هر میدان مرتب ارشیمدسی $(K,\leq)$، یک همریختی حفظ‌کننده ترتیب $\varphi\colon K\to\mathbb{R}$ وجود دارد. علاوه بر این، φ به طور یکتا تعیین می‌شود.

اثبات. توجه کنید که $\mathbb{Q}$ یک زیرمیدان از K است. برای $a\in K$، زیرمجموعه‌های زیر را در نظر می‌گیریم:

$$I_a :=]-\infty,a]_K\cap\mathbb{Q},\quad J_a := [a,\infty]_K\cap\mathbb{Q}$$

از $\mathbb{Q}$. واضح است که $I_a\leq J_a$ و $I_a\cup J_a=\mathbb{Q}$. بنابراین به ناچار φ را به صورت زیر تعریف می‌کنیم:

$$\varphi(a) := \sup I_a = \inf J_a\in\mathbb{R}.$$

از آنجا که $\leq$ یک ترتیب ارشیمدسی است، هر دو I_a و J_a ناتهی هستند و بنابراین $\varphi(a)$ یک عدد حقیقی به خوبی تعریف شده است. به سادگی می‌توان دید که برای $a,b\in K$، $I_a+I_b\subseteq I_{a+b}$ و $J_a+J_b\subseteq J_{a+b}$. با سوپریمم گرفتن از هر دو طرف نامساوی اول، $\varphi(a)+\varphi(b)\leq\varphi(a+b)$ به دست می‌آید، و با اینفیمم گرفتن از نامساوی دوم، نامساوی مخالف نتیجه می‌شود. بنابراین φ یک نگاشت جمعی است. از طرف دیگر، برای عناصر مثبت $a,b\in K$ داریم $I_a^+\cdot I_b^+\subseteq I_{ab}^+$ و $J_a^+\cdot J_b^+\subseteq J_{ab}^+$، که در آن $I_c^+ := I_c\cap[۰,\infty[$ و $J_c^+ := J_c\cap[۰,\infty[$. مشابه قبل، این نتیجه می‌دهد که $\varphi(ab)=\varphi(a)\varphi(b)$. □

نتیجه ۱۹-۴. ترتیب‌های ارشیمدسی یک میدان K با مجموعه $\mathrm{Hom}(K,\mathbb{R})$ از نشاندن‌های میدانی $K\to\mathbb{R}$ در تناظر یک‌به‌یک هستند.

نتیجه ۲۰-۴. تنها اندومورفیسم حلقه‌ای میدان $\mathbb{R}$ نگاشت همانی است.

نتیجه ۲۱-۴. اگر K یک گسترش میدانی سره از $\mathbb{R}$ باشد، آنگاه K هیچ ترتیب ارشیمدسی ندارد.

اثبات. در غیر این صورت، با توجه به قضیه هولدر، یک نشاندن $\varphi\colon K\to\mathbb{R}$ وجود دارد. از آنجا که $\varphi|_{\mathbb{R}}=\mathrm{id}$ (بنابر نتیجه قبل)، نگاشت φ نمی‌تواند یک‌به‌یک باشد، که تناقض است. □

تعریف ۲۲-۴. یک پیش‌ترتیب[۶] روی یک میدان K زیرمجموعه‌ای $T\subseteq K$ است که شرایط $T+T\subseteq T$، $TT\subseteq T$ و $a^۲\in T$ برای هر $a\in K$ را برآورده کند. پیش‌ترتیب T را سره می‌نامیم هرگاه $-۱\notin T$.

هر مخروط مثبت یک پیش‌ترتیب سره است. پیش‌ترتیب T سره است اگر و تنها اگر $T\cap(-T)=\{۰\}$. اگر $\mathrm{char}(K)\neq ۲$ باشد، آنگاه تنها پیش‌ترتیب ناسره $T=K$ است؛ چون $-۱\in T$ با توجه به اتحاد

$$x=\Big(\frac{x+۱}{۲}\Big)^۲-\Big(\frac{x-۱}{۲}\Big)^۲.$$

نتیجه می‌دهد $T=K$. اگر $\mathcal{F}=(T_i)_{i\in I}$ یک خانواده از پیش‌ترتیب‌های K باشد، اشتراک $\bigcap_{i\in I}T_i$ نیز یک پیش‌ترتیب است. کوچکترین پیش‌ترتیب در K، $\Sigma K^۲$ است؛ یعنی مجموعه تمام مجموع مربعات در K. اگر $\mathcal{F}$ به سمت بالا فیلتر

[۶] Preordering

شود (یعنی برای هر $i \in I$، $i_1, i_2 \in I$ وجود داشته باشد به طوری که $T_{i_1} \cup T_{i_2} \subseteq T_i$)، آنگاه اجتماع $\bigcup_{i\in I} T_i$ نیز یک پیش‌ترتیب است (و اگر همه T_i سره باشند، سره خواهد بود).

برای هر زیرمجموعه S از K می‌توانیم پیش‌ترتیب $T = PO(S)$ تولید شده توسط S را در نظر بگیریم. طبق تعریف، این اشتراک تمام پیش‌ترتیب‌های T' با $S \subseteq T'$ است. به طور صریح، T شامل تمام عناصر K به شکل

$$\sum_{e\in\{0,1\}^r} s_e \cdot t_1^{e_1} \cdots t_r^{e_r}$$

با $r \in \mathbb{N}$، $t_1, \ldots, t_r \in S \cup \{1\}$ و $s_e \in \Sigma K^2$ برای هر e است.

برعکس، اکنون ثابت می‌کنیم که هر پیش‌ترتیب سره اشتراکی از ترتیب‌ها است. در ادامه، فرض می‌کنیم K یک میدان باشد.

لم ۲۳-۴. اگر T یک پیش‌ترتیب سره از K باشد و $a \in K$ که $a \notin T$، آنگاه $T - aT = \{s - at : s, t \in T\}$ نیز یک پیش‌ترتیب سره از K است.

اثبات. می‌دانیم که $T - aT$ یک پیش‌ترتیب است. اگر فرض کنیم $-1 \in T - aT$، آنگاه $-1 = s - at$ که $s, t \in T$. در اینجا $t \neq 0$؛ چون $-1 \notin T$. بنابراین $a = \frac{1+s}{t} = \frac{1}{t^2}(1 + s)t \in T$ که با فرض تناقض دارد. □

گزاره ۲۴-۴. هر پیش‌ترتیب سره از K در یک مخروط مثبت از K قرار دارد.

اثبات. فرض کنید T یک پیش‌ترتیب سره از K باشد و $\mathcal{T}$ مجموعه تمام پیش‌ترتیب‌های سره T' که شامل T هستند. با توجه به لم زرن، $\mathcal{T}$ دارای یک عضو ماکسیمال P است. نشان می‌دهیم که هر چنین P یک مخروط مثبت از K است. باید نشان دهیم $P \cup (-P) = K$، بنابراین فرض کنید $a \in K$. اگر $a \notin P$، آنگاه $P - aP$ یک پیش‌ترتیب سره است که شامل P می‌شود، بنابراین با ماکسیمال بودن P داریم $P - aP = P$. در نتیجه $-a \in P$. □

نتیجه ۲۵-۴. هر پیش‌ترتیب سره ماکسیمال از K یک مخروط مثبت از K است.

گزاره ۲۶-۴. هر پیش‌ترتیب سره از K اشتراکی از مخروط‌های مثبت K است.

اثبات. فرض کنید T یک پیش‌ترتیب سره باشد و $a \in K$ با $a \notin T$. در این صورت $T - aT$ یک پیش‌ترتیب سره است و بنابراین در یک مخروط مثبت P قرار دارد. در نتیجه $a \notin P$. □

اگر K هر میدان حقیقی باشد، آنگاه $-1 \notin \Sigma K^2$، همانطور که از تعریف ترتیب‌ها مشاهده شد. اکنون می‌توانیم عکس آن را ثابت کنیم.

نتیجه ۲۷-۴. برای هر میدان K، موارد زیر معادل هستند:

(i) K حقیقی است؛ یعنی K دارای یک ترتیب است.

(ii) K دارای یک پیش‌ترتیب سره است.

(iii) $-۱ \notin \Sigma K^۲$.

(iv) $a_۱^۲ + \cdots + a_n^۲ = ۰$ با $a_۱, \ldots, a_n \in K$ نتیجه می‌دهد $a_۱ = \cdots = a_n = ۰$.

اثبات. نتیجه‌گیری‌های (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) و (iii) $\Leftrightarrow$ (iv) واضح هستند. اگر (iii) برقرار باشد، آنگاه $\Sigma K^۲$ یک پیش‌ترتیب سره از K است. بنابراین K با توجه به قضیه ۲۴-۵ دارای یک ترتیب است. □

قضیه ۲۸-۴ (آرتین). فرض کنید K یک میدان با $\mathrm{char}(K) \neq ۲$ باشد. یک عنصر $a \in K$ نسبت به هر ترتیب K نامنفی است اگر و فقط اگر a مجموع مربعات در K باشد.

قسمت "فقط اگر" زمانی که K یک میدان با مشخصه دو باشد، برقرار نیست. به همین دلیل حالت $\mathrm{char}(K) = ۲$ در قضیه مستثنی شده است.

اثبات. اگر K حقیقی باشد، آنگاه $\Sigma K^۲$ یک پیش‌ترتیب صحیح است و بنابراین طبق گزاره ۲۶-۵ اشتراک تمام مخروط‌های مثبت خواهد بود. اگر K حقیقی نباشد، آنگاه $-۱ \in \Sigma K^۲$ و بنابراین $\Sigma K^۲ = K$. □

این قضیه‌ای قابل توجه است، هرچند اثبات آن چندان دشوار نبود. آرتین و شِرایر مفهوم ترتیب‌دهی میدان‌ها را معرفی کردند تا به مسئله زیر بپردازند.

مسئله هفدهم هیلبرت:

فرض کنید $f(x_۱, \ldots, x_n)$ چندجمله‌ای با ضرایب حقیقی باشد که روی تمام نقاط $\mathbb{R}^n$ مقادیر نامنفی می‌گیرد. آیا می‌توان f را به صورت مجموع مربع‌هایی از توابع گویا در $(x_۱, \ldots, x_n)$ نوشت؟

پس هیلبرت پرسیده بود که آیا عبارتی به شکل $fh^۲ = f_۱^۲ + \cdots + f_r^۲$ وجود دارد که در آن $f_۱, \ldots, f_r$ و h چندجمله‌ای‌های حقیقی باشند و $h \neq ۰$؟

حالت $n = ۱$ ابتدایی است و هیلبرت خودش حالت $n = ۲$ را پاسخ داد. اما برای مقادیر بزرگتر n، مسئله کاملاً باز باقی ماند. معرفی مفهوم «انتزاعی» ترتیب‌دهی میدان‌ها، همراه با قضیه آرتین، دیدگاه جدیدی برای پرداختن به مسئله ارائه داد. با استفاده از این مفهوم و به ویژه قضیه ۲۸-۵، آرتین (۱۹۲۷) ثابت کرد که پاسخ همیشه مثبت است. می‌توانیم استراتژی ممکنی برای چنین اثباتی را ببینیم: از فرض $f(\xi) \geq ۰$ برای تمام $\xi \in \mathbb{R}^n$، سعی می‌کنیم نتیجه بگیریم که f نسبت به هر ترتیب در میدان توابع گویا $\mathbb{R}(x_۱, \ldots, x_n)$ نامنفی است. اگر این را نشان دهیم، با استفاده از قضیه آرتین کار تمام است. در واقع، این روش جواب می‌دهد و جزئیات کامل آن را در ادامه خواهیم دید.

توجه کنید که اثبات قضیه آرتین کاملاً غیرساختنی بود. به طور کلی، از این که فقط بدانیم یک عنصر $a \in K$ در هر مخروط مثبت K قرار دارد، هیچ اطلاعاتی درباره چگونگی یافتن نمایشی از a به صورت مجموع مربع‌ها به دست نمی‌آید. در آینده در موقعیت مسئله هفدهم هیلبرت، به این پرسش بازخواهیم گشت.

۲.۴ توسیع ترتیب‌ها و میدان‌های بسته حقیقی

همواره فرض می‌کنیم K یک میدان است. اگر L/K یک توسیع میدان و P یک مخروط مثبت از K باشد، کوچک‌ترین پیش‌ترتیب L که شامل P باشد به صورت زیر است:

$$T_L(P) := \Big\{ \sum_{i=1}^{n} a_i y_i^2 : n \in \mathbb{N},\ a_i \in P,\ y_i \in L \Big\}.$$

پس $T_L(P)$ برابر است با اشتراک تمام مخروط‌های مثبت Q از L که P را گسترش می‌دهند، یعنی به طوری که $Q \cap K = P$. نتیجه می‌گیریم:

لم ۲۹-۴. یک مخروط مثبت P از K به یک مخروط مثبت از L گسترش می‌یابد اگر و تنها اگر $-1 \notin T_L(P)$.

حال چند مورد خاص را بررسی می‌کنیم.

قضیه ۳۰-۴. فرض کنید $L = K(\sqrt{a})$ که در آن $a \in K$. یک مخروط مثبت P از K به L گسترش می‌یابد اگر و تنها اگر $a \in P$.

اثبات. اگر Q یک گسترش از P به L باشد، آنگاه $a = (\sqrt{a})^2 \in Q \cap K = P$. برعکس، فرض کنید $a \in P$ و $L \neq K$، یعنی $\sqrt{a} \notin K$. با فرض $-1 \in T_L(P)$، داریم:

$$-1 = \sum_{i=1}^{n} a_i \left(x_i + y_i \sqrt{a}\right)^2 = \sum_{i=1}^{n} a_i \left(x_i^2 + a y_i^2 + 2 x_i y_i \sqrt{a}\right)$$

که در آن $a_i \in P$ و $x_i,\ y_i \in K$. این رابطه نتیجه می‌دهد که $-1 = \sum_{i=1}^{n} a_i(x_i^2 + a y_i^2) \in P$، که یک تناقض است. □

قضیه ۳۱-۴. فرض کنید L/K یک توسیع میدان با درجه فرد باشد. در این صورت، هر ترتیب‌دهی از K به L گسترش می‌یابد.

اثبات. فرض کنید این گزاره نادرست باشد و L/K یک مثال نقض با کوچک‌ترین درجه فرد n باشد. فرض کنید P یک مخروط مثبت از K باشد که به L گسترش نمی‌یابد. از آن‌جا که $\mathrm{char}(K) = 0$، عضوی مانند $\alpha \in L$ وجود دارد که $L = K(\alpha)$. اگر $f \in K[t]$ چندجمله‌ای مینیمال α باشد، آنگاه $\deg(f) = n$ و L به صورت $K[t]/\langle f \rangle$ K-همریخت است. داریم $-1 \in T_L(P)$، بنابراین در L،

$$1 + \sum_{i=1}^{r} a_i y_i^2 = 0$$

که در آن $a_i \in P \neq 0$ و $y_i \in L \neq 0$ برای $i = 1, \ldots, r$. چندجمله‌ای‌هایی مانند $g_i \in K[t]$ را انتخاب کنید که $y_i = g_i(\alpha)$ و $\deg(g_i) < n$ $(i = 1, \ldots, r)$. در این صورت، رابطه زیر در $K[t]$ برقرار است:

$$۱ + \sum_{i=۱}^{r} a_i g_i(t)^۲ = f(t)h(t) \quad (۱.۱)$$

برای برخی چندجمله‌ای‌های $h \in K[t]$.

فرض کنید $d := \max_i \deg(g_i)$. در این صورت $d < n$ و درجه سمت چپ رابطه (۱.۱) حداکثر $۲d$ است. ضریب $t^{۲d}$ به شکل $\sum_{i=۱}^{r} a_i b_i^۲$ است که در آن $b_i \in K$ و حداقل برای یک اندیس $b_i \neq ۰$، بنابراین این ضریب نسبت به P مثبت است. در نتیجه، درجه چندجمله‌ای (۱.۱) برابر $۲d$ است و بنابراین $\deg(h)$ فرد است. همچنین $\deg(h) < n$ زیرا $d < n$. حداقل یک عامل تقلیل‌ناپذیر $h_۱$ از h با درجه فرد وجود دارد، و بنابراین میدان $L_۱ := K[t]/\langle h_۱ \rangle$ روی K دارای درجه فرد $< n$ است. علاوه بر این، $-۱ \in T_{L_۱}(P)$. پس ترتیب P به $L_۱$ گسترش نمی‌یابد که با انتخاب مینیمال L در تناقض است. □

قضیه ۳۲-۴. هر ترتیب‌دهی از K را می‌توان به میدان توابع گویا $K(x_۱, \ldots, x_n)$ برای هر $n \in \mathbb{N}$ گسترش داد.

اثبات. با استقرا، کافی است یک مخروط مثبت داده شده P از K را به $K(x)$ (با یک متغیر) گسترش دهیم. اگر فرض کنیم که P به $K(x)$ گسترش نمی‌یابد، آنگاه $-۱ \in T_{K(x)}(P)$. این یعنی $۰ = f_۰^۲ + \sum_{i=۱}^{r} a_i f_i^۲$ در $K[x]$ است که در آن $r \geq ۱$ و $۰ \neq a_i \in P$ $(i = ۱, \ldots, r)$، $۰ \neq f_i \in K[x]$ $(i = ۰, \ldots, r)$. با استدلالی مشابه اثبات قبلی، سمت چپ این رابطه دارای درجه $۲d$ است که در آن $d = \max\{\deg(f_i) : ۰ \leq i \leq r\}$. این عبارت، غیرصفر و در نتیجه یک تناقض است. □

تعریف ۳۳-۴. یک میدان K را بسته حقیقی می‌نامیم اگر K حقیقی باشد، اما هر توسیع جبری صحیح از K غیرحقیقی باشد.

برای مثال، میدان اعداد حقیقی $\mathbb{R}$ بسته حقیقی است، زیرا $\mathbb{C}$ تنها توسیع جبری صحیح از $\mathbb{R}$ است.

قضیه ۳۴-۴. برای یک میدان K، ویژگی‌های زیر معادل هستند:

(i) K بسته حقیقی است؛

(ii) K دارای یک ترتیب‌دهی است که به هیچ توسیع جبری صحیحی از K گسترش نمی‌یابد؛

(iii) K حقیقی است، هیچ توسیع صحیحی با درجه فرد ندارد، و $K^* = K^{*۲} \cup (-K^{*۲})$.

در اینجا $K^{*۲} = \{a^۲ : a \in K^*\}$.

اثبات. (i) $\Rightarrow$ (ii) از تعاریف واضح است.

(ii) $\Rightarrow$ (iii) فرض کنید P یک مخروط مثبت از K باشد که به هیچ توسیع متناهی صحیحی از K گسترش نمی‌یابد. پس K هیچ توسیع صحیحی با درجه فرد ندارد. هر عضو $a \in P$ یک مربع در K است، زیرا در غیر این صورت

$K(\sqrt{a})$ یک میدان بزرگ‌تر خواهد بود که P می‌تواند به آن گسترش یابد. بنابراین $P = \{a^۲ : a \in K\}$ و (iii) از $P \cup (-P) = K$ نتیجه می‌شود.

حال فرض کنید (iii) برقرار است، بنابراین $\mathrm{char}(K) = ۰$. برای اثبات (i) از یک استدلال گالوا استفاده می‌کنیم. طبق ،(iii) تنها غیرمربع‌های K عناصر $-a^۲$ با $a \neq ۰$ هستند. بنابراین $K(\sqrt{-۱})$ تنها توسیع درجه دوم K است. نشان می‌دهیم که هر توسیع جبری صحیح از K شامل یک زیرمیدان درجه دوم است، که ویژگی (i) را نتیجه می‌دهد. فرض کنید L/K یک توسیع متناهی صحیح باشد، E پوشش گالوایی L روی K و G گروه گالوا E روی K باشد. همچنین فرض کنید S یک زیرگروه سیلو ۲ از G باشد. اگر F زیرمیدان عناصر ثابت تحت عمل S را نشان دهد، آنگاه درجه $[F : K] = [G : S]$ فرد است. بنابراین $F = K$ طبق فرض ،(iii) و در نتیجه G یک ۲–گروه است. بنابراین هر زیرگروه صحیحی از G در یک زیرگروه با اندیس ۲ قرار می‌گیرد، که نشان می‌دهد L شامل یک توسیع درجه دوم از K است، همان‌طور که ادعا شد. □

نتیجه ۳۵–۴. اگر K یک میدان بسته حقیقی باشد، آنگاه $P := \{a^۲ : a \in K\}$ تنها مخروط مثبت K است.

مرسوم است که یک میدان بسته حقیقی کلی را با حرف R نشان می‌دهند. اگر R یک میدان بسته حقیقی باشد، ترتیب یکتا روی R را با $\leq$ نشان می‌دهیم و اغلب مخروط مثبت یکتای R را با $R_+ = \{a^۲ : a \in R\}$ نمایش می‌دهیم.

قضیه ۳۶–۴ (قضیه اساسی جبر)**.** اگر R یک میدان بسته حقیقی باشد، آنگاه میدان $R(\sqrt{-۱})$ بسته جبری است.

اثبات. مطابق معمول، $i = \sqrt{-۱}$ را در نظر می‌گیریم. هر توسیع متناهی از $R(i)$ دارای درجه‌ای از توان ۲ است. بنابراین کافی است ثابت کنیم که $R(i)$ توسیع درجه دوم ندارد. این بخش ابتدایی است: اگر $w = u + iv$ که $u, v \in R$ و $v \neq ۰$، آنگاه $w = z^۲$ برای $z := x + \frac{iv}{۲x} \in R$ و $x := \sqrt{\frac{۱}{۲}(u + \sqrt{u^۲ + v^۲})}$، که در آن باید مقدار مثبت را برای ریشه مربع داخلی انتخاب کرد. □

قضیه اساسی جبر یک عکس قوی دارد: اگر K یک میدان با بستار جبری $\overline{K}$ باشد و $۱ < [\overline{K} : K] < \infty$، آنگاه K بسته حقیقی است (و در نتیجه $\overline{K} = K(\sqrt{-۱})$).

نتیجه ۳۷–۴. فرض کنید R یک میدان بسته حقیقی باشد. چندجمله‌ای‌های تکین تحویل‌ناپذیر در $R[t]$ به صورت زیر هستند:

(۱) $t - a$، برای $a \in R$؛

(۲) $t^۲ + at + b$، برای $a, b \in R$ به طوری که $a^۲ < ۴b$.

بنابراین هر چندجمله‌ای تکین در $R[t]$ حاصلضرب تعداد متناهی از عوامل نوع (۱) یا (۲) است.

اثبات. فرض کنید $f \in R[t]$ تکین و تحویل‌ناپذیر باشد. پس، $\deg(f) \leq ۲$. این ادعا را نتیجه می‌دهد؛ زیرا $t^۲ + at + b$ روی R تحویل‌ناپذیر است اگر و تنها اگر $۴b - a^۲$ یک مربع نباشد (یعنی منفی باشد). □

اگر $f(t) \in R[t]$ یک چندجمله‌ای تکین تحویل‌ناپذیر از درجه ۲ باشد، آنگاه $f(t) > ۰$ برای هر $t \in R$.

مثال ۳۸-۴. فرض کنید $(K, \leq)$ یک میدان مرتب باشد، $L = K(i)$ با $i = \sqrt{-۱}$، و $z \mapsto \overline{z}$ خودریختی نابدیهی L/K را نشان دهد. اگر $|z|^۲ := z\overline{z}$ برای $z \in L$، آنگاه نابرابری کوشی–شوارتز

$$\left|\sum_{j=۱}^{n} x_j \overline{y}_j\right|^۲ \leq \Big(\sum_{j=۱}^{n} |x_j|^۲\Big) \cdot \Big(\sum_{j=۱}^{n} |y_j|^۲\Big)$$

برای هر $x, y \in L^n$ برقرار است. علاوه بر این، تساوی برقرار است اگر و تنها اگر x و y روی L وابسته خطی باشند. اثبات این موضوع مشابه حالتی است که روی $\mathbb{R}$ یا $\mathbb{C}$ کار می‌کنیم.

مثال ۳۹-۴. اگر میدان R بسته حقیقی باشد و $C = R(\sqrt{-۱})$ و $z \in C^n$، آنگاه تعریف می‌کنیم:

$$|z| := \sqrt{|z_۱|^۲ + \cdots + |z_n|^۲}.$$

نامساوی مثلث $|z + z'| \leq |z| + |z'|$ برای هر $z, z' \in C^n$ برقرار است که نتیجه‌ای از نابرابری کوشی–شوارتز است.

هر مخروط مثبت P از یک میدان K یک توپولوژی $\mathcal{T}_P$ روی K تعریف می‌کند، با این تعریف که بازه‌های باز J_a, bI_P (برای $a, b \in K$) را به عنوان پایه‌ای از مجموعه‌های باز در K در نظر بگیریم. این توپولوژی مرتب‌سازی (K, P) است. تمام عملیات میدان (جمع، ضرب، تقسیم) نسبت به $\mathcal{T}_P$ پیوسته هستند، که به این معنی است که $(K, \mathcal{T}_P)$ یک میدان توپولوژیک است. برای هر $n \in \mathbb{N}$، توپولوژی مرتب‌سازی $\mathcal{T}_P$ توپولوژی حاصلضرب روی K^n را می‌دهد که گوی‌های باز

$$B_r(x) = \{y \in K^n : |y - x|^۲ <_P r^۲\}$$

($x \in K^n$، $r \in K$) را به عنوان پایه‌ای از مجموعه‌های باز دارد. از توپولوژی مرتب‌سازی بدون هیچ توضیح اضافی استفاده خواهیم کرد، عمدتاً در مواردی که K بسته حقیقی است.

۳.۴ صفرهای حقیقی چندجمله‌ای‌های چند متغیره

برای یک چندجمله‌ای f با ضرایب حقیقی، مایلیم تعداد ریشه‌های حقیقی آن را بشماریم یا حداقل تخمین بزنیم، بدون آنکه مجبور به محاسبه مستقیم آنها باشیم. در ادامه چندین روش برای دستیابی به این هدف و روش‌های دقیق‌تر را خواهیم دید. این روش‌ها عمدتاً به قرن نوزدهم یا حتی قبل از آن بازمی‌گردند و می‌توان آنها را از اولین تجلیات چیزی دانست که امروزه به آن «جبر حقیقی» می‌گوییم.

برای ادامه بحث، مهم است که نتایج ارائه شده در اینجا بر روی هر میدان بسته حقیقی دلخواه R برقرار باشند، نه فقط بر روی $\mathbb{R}$. برخی از نتایج پایه‌ای که در ادامه می‌آیند، در حالت $R = \mathbb{R}$ از حسابان سال اول شناخته شده هستند، اما ما

آنها را مجدداً و فقط با استفاده از استدلال‌های کاملاً جبری بررسی می‌کنیم. تأکید می‌کنیم که ابزارهای سنتی حسابان بر روی یک میدان بسته حقیقی کلی R در دسترس نیستند، زیرا R فاقد ویژگی‌های کامل‌بودن لازم است.

در سرتاسر این بخش، R نشان‌دهنده یک میدان بسته حقیقی است. کار را با یک کران اولیه ساده برای اندازه ریشه‌ها بر حسب ضرایب شروع می‌کنیم:

لم ۴-۴۰. فرض کنید $f = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$ یک چندجمله‌ای تکین با ضرایب در $R(\sqrt{-1})$ باشد. در این صورت برای هر ریشه α از f در $R(\sqrt{-1})$ داریم:

$$|\alpha| \ \leq \ \max\{1,\ |a_1| + \cdots + |a_n|\}$$

اثبات. فرض کنید $\alpha \in R(\sqrt{-1})$ با $f(\alpha) = 0$ و $|\alpha| \geq 1$. در این صورت:

$$\alpha \ = \ -\Big(a_1 + \frac{a_2}{\alpha} + \cdots + \frac{a_n}{\alpha^{n-1}}\Big),$$

بنابراین ادعا از نابرابری مثلث نتیجه می‌شود. □

در ادامه برخی نتایج برای توابع گویا را اثبات می‌کنیم. وقتی $R = \mathbb{R}$، این نتایج از حسابان مقدماتی شناخته شده هستند و به طور کلی‌تر برای توابع با مشتق‌پذیری مناسب برقرارند.

برخی مفاهیم پایه را یادآوری کنیم. فرض کنید k یک میدان و $f = f(t) \in k(t)$ یک تابع گویای ناصفر باشد. برای $a \in k$ می‌توانیم (به طور یکتا) بنویسیم $f = (t-a)^n \cdot \frac{g}{h}$ که در آن $n \in \mathbb{Z}$ و g، $h \in k[t]$ به طوری که $g(a)h(a) \neq 0$. مرتبه صفرشدن f در $a \in k$ برابر است با $\mathrm{ord}_a(f) = n$. اگر $n \geq 1$، a یک ریشه از f نامیده می‌شود و n مرتبه آن است. اگر $n < 0$، a یک قطب از f است با مرتبه قطبی $|n|$. هر تابع گویای ناصفر f فقط تعداد محدودی ریشه یا قطب دارد. اگر $a \in k$ قطب f نباشد، مقدار $f(a) \in k$ در $t = a$ به خوبی تعریف شده است.

حال فرض کنید میدان $k = R$ بسته حقیقی باشد. هر تابع گویای ناصفر $f \in R(t)$ یک تجزیه حاصلضربی به شکل زیر دارد:

$$f(t) \ = \ \pm g(t) \cdot \prod_{i=1}^{r} (t - a_i)^{e_i} \quad (1.2)$$

با $r \geq 0$، $a_i \in R$ و $e_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$، که در آن $g(t) \in R(t)$ به گونه‌ای است که g هیچ قطبی در R ندارد و $g(\xi) > 0$ برای هر $\xi \in R$. بنابراین نتیجه می‌گیریم:

گزاره ۴-۴۱ (قضیه مقدار میانی)**.** فرض کنید $f \in R(t)$، و $a < b$ در R به گونه‌ای باشند که f هیچ قطبی در $[a,b]$ نداشته باشد و $f(a)\,f(b) < 0$. در این صورت تعداد ریشه‌های f در $[a,b]$، با احتساب تکرار، فرد است. به ویژه، f حداقل یک ریشه در $[a,b]$ دارد.

اثبات. در رابطه (۲.۱) می‌توانیم $g(t)$ و همچنین هر عامل $t - a_i$ با $a_i \notin [a,b]$ را نادیده بگیریم. □

فرض کنید $f \in R(t)$ و $f \neq 0$. $a \in R$. عدد $\varepsilon > 0$ در R وجود دارد به طوری که $|b-a| \geq \varepsilon$ برای هر ریشه یا قطب $b \neq a$ از f. پس، f دارای علامت‌های ثابت s_- در $]a-\varepsilon, a[$ و s_+ در $]a, a+\varepsilon[$ است، که در آن s_-، $s_+ \in \{\pm 1\}$. می‌گوییم f در a تغییر علامت می‌دهد (از s_- به s_+، اگر بخواهیم مشخص کنیم) اگر $s_- \neq s_+$. اگر $s_- = s_+$ باشد، f در a تغییر علامت نمی‌دهد.

لم ۴-۴۲. یک تابع گویای ناصفر $f \in R(t)$ در $a \in R$ تغییر علامت می‌دهد اگر و تنها اگر $\mathrm{ord}_a(f)$ فرد باشد.

اثبات. این نتیجه مستقیماً از $f = (t-a)^n \cdot g$ به دست می‌آید، که $n = \mathrm{ord}_a(f)$ و $g(a) \neq 0$. □

مشتق توابع گویا به صورت کاملاً صوری تعریف می‌شود. اگر $f = \sum_{i \geq 0} a_i t^i$ یک چندجمله‌ای با $a_i \in R$ باشد، آنگاه $f' = \sum_{i \geq 1} i a_i t^{i-1}$. به طور کلی‌تر، اگر $f = \frac{p}{q}$ یک تابع گویا با چندجمله‌ای‌های p، $q \in R[t]$ و $q \neq 0$ باشد، آنگاه $f' = \frac{p'q - pq'}{q^2}$ که مجدداً یک تابع گویا است. به جای f' از نماد $\frac{df}{dt}$ نیز استفاده می‌کنیم. مشتق‌های مراتب بالاتر f''، f'''، ... به صورت تکرار مشتق اول تعریف می‌شوند: $f^{(k)} = \frac{d^k f}{dt^k} := \frac{d}{dt}(f^{(k-1)})$ برای $k \geq 1$.

لم ۴-۴۳. فرض کنید $f \in R(t)$. $0 \neq f$. اگر $a \in R$ یک ریشه (یا قطب) از f باشد، «مشتق لگاریتمی» f'/f از f تغییر علامت از منفی به مثبت (یا از مثبت به منفی) می‌دهد.

اثبات. فرض کنید $a \in R$ با $n = \mathrm{ord}_a(f) \neq 0$. با نوشتن $f = (t-a)^n \cdot g$ و $g(a) \neq 0$، داریم:

$$\frac{f'(t)}{f(t)} = \frac{n}{t-a} + \frac{g'(t)}{g(t)}$$

که از آن می‌توان ادعا را نتیجه گرفت. □

قضیه ۴-۴۴. فرض کنید $f \in R(t)$، و $a < b$ در R با $f(a) = f(b) = 0$. اگر f هیچ ریشه یا قطبی در بازه باز $]a, b[$ نداشته باشد، تعداد ریشه‌های f' در $]a, b[$، با احتساب تکرار، فرد است.

اثبات. اعداد b $a < a_1 < b_1 < b$ را در R انتخاب کنید به طوری که f' در $]a, a_1] \cup [b_1, b[$ صفر نباشد. می‌دانیم $\frac{f'}{f}$ در $a + \varepsilon$ مثبت و در $b - \varepsilon$ منفی است، برای $\varepsilon > 0$ به اندازه کافی کوچک. بنابراین $\frac{f'}{f}$ در a_1 مثبت و در b_1 منفی است. در نتیجه، طبق قضیه مقدار میانی، تعداد ریشه‌های $\frac{f'}{f}$ در $[a_1, b_1]$، با احتساب تکرار، فرد است. این عدد برابر است با تعداد ریشه‌های f' در $]a, b[$. □

نتیجه ۴-۴۵ (قضیه رول). فرض کنید $f \in R(t)$. اگر $a < b$ در R به گونه‌ای باشند که $f(a) = f(b)$ و اگر f هیچ قطبی در $]a, b[$ نداشته باشد، آنگاه ξ وجود دارد که $a < \xi < b$ که $f'(\xi) = 0$.

اثبات. با جایگزینی f با $f - f(a)$ می‌توانیم فرض کنیم $f(a) = f(b) = 0$. همچنین می‌توانیم فرض کنیم $f \neq 0$ و b را با کوچک‌ترین ریشه c از f که بزرگ‌تر از a است جایگزین کنیم. □

نتایج زیر که از حسابان شناخته شده هستند، به دست می‌آیند:

نتیجه ۴-۴۶. فرض کنید $f \in R(t)$، و $a < b$ در R به گونه‌ای باشند که f هیچ قطبی در $[a,b]$ نداشته باشد.

(الف) (قضیه مقدار میانگین) ξی وجود دارد با $a < \xi < b$ که $f'(\xi) = \frac{f(b)-f(a)}{b-a}$.

(ب) اگر $f'(x) \geq ۰$ برای تمام $x \in]a,b[$، آنگاه f روی $[a,b]$ صعودی است.

اثبات. برای اثبات (الف)، قضیه رول را روی تابع زیر اعمال کنید:

$$g(t) = f(t) - \frac{t-a}{b-a}\left(f(b) - f(a)\right).$$

در واقع داریم $g(a) = g(b) = f(a)$ و هر ξ با $a < \xi < b$ که $g'(\xi) = ۰$، ادعا را برآورده می‌کند. گزاره (ب) نتیجه‌ای از (الف) است. □

اکنون به بحث اصلی این بخش می‌پردازیم، که شمارش تعداد ریشه‌های حقیقی یک چندجمله‌ای است، چه به صورت کلی و چه در یک بازه مشخص. برای روشن‌سازی، اگر R یک میدان بسته حقیقی و $f \in R[t]$ باشد، منظور از ریشه حقیقی f، عنصر $\alpha \in R$ است که $f(\alpha) = ۰$ (در مقابل ریشه‌های غیرحقیقی f که $\alpha \in R(\sqrt{-۱}) \setminus R$ با $f(\alpha) = ۰$ هستند). چندجمله‌ای ناصفر $f \in R[t]$ را حقیقی‌ـریشه‌ای می‌گوییم اگر تمام ریشه‌های آن حقیقی باشند. کار را با ارائه یک کران بالا برای تعداد ریشه‌های حقیقی شروع می‌کنیم.

تعریف ۴-۴۷. برای یک دنباله متناهی $c = (c_۱, \ldots, c_n)$ در R *(با $n \geq ۱$)*، تعریف می‌کنیم:

$$\mathrm{Var}(c) = \mathrm{Var}(c_۱, \ldots, c_n)$$

به عنوان تعداد تغییرات علامت در c پس از حذف تمام صفرها. بنابراین این تعداد جفت‌های (i,j) با $۱ \leq i < j \leq n$ است که $c_i c_j < ۰$ و $c_k = ۰$ برای تمام $i < k < j$.

قضیه ۴-۴۸ (قاعده علامت‌های دکارت). فرض کنید $f = \sum_{i=۰}^{n} a_i t^i$ یک چندجمله‌ای ناصفر در $R[t]$ باشد. تعداد ریشه‌های حقیقی مثبت f، با احتساب تکرار، حداکثر برابر $\mathrm{Var}(a_۰, \ldots, a_n)$ است.

اثبات. برای $n \leq ۱$ این موضوع واضح است. بنابراین فرض کنید $n = \deg(f) > ۱$، و قضیه برای تمام درجات کوچک‌تر اثبات شده باشد. واضح است که می‌توانیم فرض کنیم $a_۰ = f(۰) \neq ۰$. تمام شمارش ریشه‌ها با احتساب تکرار انجام می‌شود. $N_+(f)$ را برای تعداد ریشه‌های مثبت f بنویسید و $r \geq ۱$ را حداقل اندیسی در نظر بگیرید که $a_r \neq ۰$. از آن‌جا که $\mathrm{ord}_\xi(f') = \mathrm{ord}_\xi(f) - ۱$ برای هر ریشه ξ از f، قضیه رول نتیجه می‌دهد که $N_+(f') \geq N_+(f) - ۱$. از آن‌جا که $N_+(f') \leq \mathrm{Var}(a_r, \ldots, a_n) \leq \mathrm{Var}(a_۰, \ldots, a_n)$ با فرض استقرا برقرار است، اگر $N_+(f) \leq N_+(f')$، کار تمام است. این بدان معناست که می‌توانیم فرض کنیم $N_+(f) = ۱ + N_+(f')$. اگر ξ کوچک‌ترین ریشه مثبت f را نشان دهد، این فرض نتیجه می‌دهد که $f'(\eta) \neq ۰$ برای $۰ < \eta < \xi$. برای $۰ < \eta$ به اندازه کافی کوچک، علامت $f'(\eta)$ برابر با علامت a_r است، بنابراین نتیجه می‌گیریم که $\mathrm{sign}\, f'(\eta) = \mathrm{sign}(a_r)$ برای تمام $۰ < \eta < \xi$. در نتیجه

f روی $[\circ,\xi]$ یکنوا است. اگر $a_r > \circ$، f روی $[\circ,\xi]$ صعودی است و بنابراین $a_\circ = f(\circ) < f(\xi) = \circ$. اگر $a_r < \circ$، f روی $[\circ,\xi]$ نزولی است و بنابراین $a_\circ = f(\circ) > f(\xi) = \circ$. در هر دو حالت، $a_\circ a_r < \circ$، که به معنای $\mathrm{Var}(a_\circ,\dots,a_n) = \mathrm{Var}(a_r,\dots,a_n) + 1$ است. بنابراین $\mathrm{Var}(a_\circ,\dots,a_n) \geq 1 + N_+(f') = N_+(f)$ که گام استقرا را کامل می‌کند. □

می‌توان استدلال در اثبات قبلی را اصلاح کرد تا نشان دهیم که تفاوت $\mathrm{Var}(a_\circ,\dots,a_n) - N_+(f)$ همیشه زوج است. به ویژه، این نتیجه می‌دهد که اگر $\mathrm{Var}(a_\circ,\dots,a_n)$ فرد باشد، آنگاه f حداقل یک ریشه مثبت دارد.

به طور کلی، کران بالا قابل بهبود نیست، همان‌طور که توسط هر چندجمله‌ای با ریشه‌های فقط حقیقی و مثبت نشان داده می‌شود. از سوی دیگر، تعداد واقعی ریشه‌های مثبت ممکن است کمتر از تعداد تغییرات علامت باشد. برای مثال، $f = t^2 - t + 1$ هیچ ریشه حقیقی ندارد.

نتیجه ۴-۴۹. فرض کنید $f \in R[t]$ یک چندجمله‌ای ناصفر با دقیقاً m تک‌جمله‌ای باشد. در این صورت f حداکثر $2m-2$ ریشه ناصفر در R دارد، با احتساب تکرار.

این کران نیز توسط $f(t^2)$ به دست می‌آید، اگر f یک چندجمله‌ای با ریشه‌های فقط حقیقی و مثبت باشد.

اثبات. هر دو $f(t)$ و $f(-t)$ حداکثر $m-1$ ریشه مثبت دارند (طبق قضیه دکارت). بنابراین f حداکثر $2m-2$ ریشه ناصفر دارد. □

برای چندجمله‌ای‌های حقیقی–ریشه‌ای f، حتی می‌توان تعداد دقیق ریشه‌های مثبت و منفی را مستقیماً از دنباله ضرایب بدست آورد:

نتیجه ۴-۵۰. فرض کنید $f = \sum_{i=\circ}^{n} a_i t^i \in R[t]$ یک چندجمله‌ای حقیقی–ریشه‌ای ناصفر باشد. در این صورت تعداد ریشه‌های مثبت (به ترتیب منفی) f برابر است با $\mathrm{Var}(a_\circ, a_1, \dots, a_n)$ (به ترتیب $\mathrm{Var}(a_\circ, -a_1, \dots, (-1)^n a_n)$)، باز هم با احتساب تکرار.

اثبات. می‌توانیم فرض کنیم $\deg(f) = n \geq 1$ و $f(\circ) \neq \circ$. فرض کنید p (به ترتیب p') تعداد ریشه‌های مثبت (به ترتیب منفی) f باشد، و تعریف کنید:

$$W(x) := \mathrm{Var}(a_\circ + x,\, a_1 + x,\, \dots,\, a_n + x),$$

$$W'(x) := \mathrm{Var}(a_\circ + x,\, -(a_1 + x),\, \dots,\, (-1)^n (a_n + x))$$

برای $x \in R$. طبق دکارت داریم $p \leq W(\circ)$، و به طور مشابه $p' \leq W'(\circ)$ (با جایگزینی x با $-x$). $x > \circ$ را در R به اندازه‌ای کوچک انتخاب کنید که $x < |a_i|$ برای هر اندیس i با $a_i \neq \circ$. در این صورت $W(x) + W'(x) = n$ زیرا $a_i + x \neq \circ$ برای هر اندیس i، و چون در هر موقعیت دقیقاً یکی از دو دنباله تغییر علامت می‌دهد. از سوی دیگر، $\mathrm{Var}(a, \circ, \dots, \circ, b) \leq \mathrm{Var}(a + c, c, \dots, c, b + c)$ هرگاه $a,\, b,\, c \in R$ و $\circ < c < 1$ باشد. با توجه به $W(x) \geq$

$W(\circ)$ و $W'(x) \geq W'(\circ)$، و با توجه به اینکه $p + p' = n$ طبق فرض برقرار است، رابطه $W(x) + W'(x) = n$ همراه با نامساوی‌های

$$p \leq W(\circ) \leq W(x), \quad p' \leq W'(\circ) \leq W'(x)$$

نتیجه می‌دهد که $p = W(\circ)$ و $p' = W'(\circ)$. □

اکنون به بررسی دو روش می‌پردازیم که به ما امکان می‌دهند تعداد دقیق ریشه‌های حقیقی یک چندجمله‌ای دلخواه $f \in R[t]$ را بدون محاسبه هیچ یک از آن‌ها تعیین کنیم. در مقابل بحث قبلی، اکنون تمام تکرارها را نادیده می‌گیریم.

تعریف ۴-۵۱. فرض کنید $f \in R[t]$ یک چندجمله‌ای نابدیهی باشد. دنباله اشتورم برای f دنباله‌ای $(f_\circ, f_1, \ldots, f_r)$ از چندجمله‌ای‌ها در $R[t]$ است که به صورت بازگشتی به صورت زیر تعریف می‌شود: $f_\circ = f$، $f_1 = f'$ و

$$\begin{aligned} f_\circ &= q_1 f_1 - f_2\,, \\ f_1 &= q_2 f_2 - f_3\,, \\ &\vdots \\ f_{r-2} &= q_{r-1} f_{r-1} - f_r\,, \\ f_{r-1} &= q_r f_r \end{aligned} \tag{۳.۱}$$

که در آن $q_1, \ldots, q_r \in R[t]$ به گونه‌ای هستند که $f_1, \ldots, f_r$ ناصفر بوده و $\deg(f_i) < \deg(f_{i-1})$ $(i = 1, \ldots, r)$. توجه کنید که این تعریف $r \in \mathbb{N}$ و همچنین f_iها و q_iها را به طور یکتا مشخص می‌کند. برای $x \in R$ تعریف می‌کنیم:

$$v_f(x) := \mathrm{Var}(f_\circ(x), f_1(x), \ldots, f_r(x)).$$

اگر علامت منفی در سمت راست (۳.۱) را به مثبت تغییر دهیم، به شکل معمول الگوریتم اقلیدسی برای زوج (f, f') می‌رسیم. یادآوری می‌کنیم که الگوریتم اقلیدسی بزرگ‌ترین مقسوم‌علیه مشترک دو چندجمله‌ای را محاسبه می‌کند. علامت‌های منفی برای الگوریتم اشتورم جهت ارائه نتایج صحیح حیاتی هستند (در ادامه مشاهده خواهید کرد)، اما برای تقسیم اقلیدسی ضروری نیستند.

قضیه ۴-۵۲. برای $a < b$ در R با $f(a)f(b) \neq \circ$، تعداد ریشه‌های متمایز f در بازه $[a, b]$ برابر است با $v_f(a) - v_f(b)$.

اثبات. $v_f(x)$ را به عنوان تابعی از $x \in R$ در نظر بگیرید. در بازه‌های بین ریشه‌های حقیقی متناهی $f_\circ f_1 \cdots f_r$، این تابع ثابت است. $v_f(x)$ هنگام عبور از یک ریشه $f_\circ f_1 \cdots f_r$ چگونه تغییر می‌کند؟

ابتدا فرض کنید f و f' نسبت به هم اول باشند، بنابراین f ریشه‌های ساده دارد. در این صورت دنباله $(f_\circ, f_1, \ldots, f_r)$ شرایط زیر را برآورده می‌کند:

(۱) $\gcd(f_۰, f_۱) = ۱$،

(۲) در هر ریشه حقیقی $f_۰$، حاصلضرب $f_۰f_۱$ علامت را از منفی به مثبت تغییر می‌دهد،

(۳) برای $۱ \le i < r$ و هر $c \in R$ با $f_i(c) = ۰$، داریم $f_{i-۱}(c)f_{i+۱}(c) < ۰$.

در واقع، (۳) از $f_{i-۱} = q_i f_i - f_{i+۱}$ و $\gcd(f_{i-۱}, f_i) = ۱$ نتیجه می‌شود.

فرض کنید $c \in R$. با $x = c_\pm$ مقادیری از x را نشان می‌دهیم که $\operatorname{sign}(x-c) = \pm ۱$ و $|x-c|$ به اندازه کافی کوچک است. فرض کنید $۰ \le i < r$ با $f_i(c) = ۰$. در این صورت $f_{i+۱}(c) \neq ۰$ طبق (۳)، و $\varepsilon := \operatorname{sign} f_{i+۱}(c)$ را تعریف می‌کنیم. فقط از (۱)-(۳) استفاده خواهیم کرد:

- اگر $i = ۰$، (۲) طرح علامت‌های زیر را نتیجه می‌دهد:

	$x = c_-$	$x = c$	$x = c_+$
$f_۰(x)$	$-\varepsilon$	۰	ε
$f_۱(x)$	ε	ε	ε
$v_f(x)$	۱	۰	۰

- اگر $۱ \le i < r$، (۳) نتیجه می‌دهد:

	$x = c_-$	$x = c$	$x = c_+$
$f_{i-۱}(x)$	$-\varepsilon$	$-\varepsilon$	$-\varepsilon$
$f_i(x)$	?	۰	?
$f_{i+۱}(x)$	ε	ε	ε
$v_f(x)$	۱	۱	۱

می‌بینیم که برای هر ریشه حقیقی c از f، تابع $v_f(x)$ در c به اندازه ۱ کاهش می‌یابد، هنگام گذر از $x = c_-$ به $x = c_+$. خارج از ریشه‌های حقیقی f، تابع $v_f(x)$ در همه جا به صورت موضعی ثابت است. بنابراین، اگر $a < b$ در R با $f(a)f(b) \neq ۰$، آنگاه $v_f(a) - v_f(b)$ برابر است با تعداد ریشه‌های متمایز f در بازه $[a, b]$.

حال فرض کنید f دلخواه باشد و $g_i := f_i/f_r$ را برای $i = ۰, \dots, r$ تعریف کنید. دنباله $(g_۰, g_۱, \dots, g_r)$ از چندجمله‌ای‌ها شرایط مشابه (۱)-(۳) بالا را برآورده می‌کند، اگرچه ممکن است دنباله اشتورم برای علاوه بر این، اگر $x \in R$ شرط $f_r(x) \neq ۰$ را برآورده کند، آنگاه دنباله‌های $(g_۰(x), \dots, g_r(x))$ و $(f_۰(x), \dots, f_r(x))$ تعداد تغییرات علامت یکسانی دارند، زیرا دنباله دوم برابر است با $f_r(x)$ ضربدر دنباله اول. همچنین، $f_۰ = f$ و $g_۰$ ریشه‌های یکسانی دارند. بنابراین استدلال قبلی حکم قضیه را در حالت کلی نتیجه می‌دهد. □

با داشتن دنباله اشتورم $(f_0, f_1, \dots, f_r)$ برای f، فرض کنید $d_i := \deg(f_i)$ و c_i ضریب پیشرو (بزرگترین) f_i باشد، برای $i = 0, \dots, r$. در این صورت برای $x \ll 0$ داریم:

$$v_f(x) = \mathrm{Var}((-1)^{d_0} c_0,\ (-1)^{d_1} c_1, \dots, (-1)^{d_r} c_r) =: v_f(-\infty),$$

در حالی که برای $x \gg 0$:

$$v_f(x) = \mathrm{Var}(c_0, c_1, \dots, c_r) =: v_f(+\infty).$$

نتیجه ۴-۵۳. تعداد کل ریشه‌های حقیقی متمایز چندجمله‌ای نابدیهی $f \in R[t]$ برابر است با $v_f(-\infty) - v_f(+\infty)$.

روش اشتورم را می‌توان بیشتر توسعه داد. فرض کنید چندجمله‌ای‌های f، $g \in R[t]$ داده شده‌اند که f نابدیهی و $g \neq 0$ است. می‌خواهیم ریشه‌های حقیقی متمایز ξ از f را که $g(\xi) > 0$ را برآورده می‌کنند، بشماریم. برای این منظور، دنباله اشتورم تعمیم یافته برای زوج (f, g) را به صورت زیر تعریف می‌کنیم: فرض کنید $f_0 = f$، $f_1 = f'g$، و $f_2, \dots, f_r$ همانطور که در (۳.۱) با $f_{i-1} = q_i f_i - f_{i+1}$ و $\deg(f_{i+1}) < \deg(f_i)$ $(i = 1, \dots, r-1)$ تعریف می‌شوند، به همراه $f_i \neq 0$ و $f_{r-1} = q_r f_r$. برای $x \in R$ تعریف می‌کنیم:

$$v_{f,g}(x) := \mathrm{Var}(f_0(x),\ f_1(x), \dots,\ f_r(x)).$$

قضیه ۴-۵۴ (الگوریتم اشتورم تعمیم یافته)**.** اگر $a < b$ در R شرط $f(a)f(b) \neq 0$ را برآورده کنند، آنگاه:

$$v_{f,g}(a) - v_{f,g}(b) = \sum_{\substack{a<c<b \\ f(c)=0}} \operatorname{sign} g(c).$$

یعنی این عبارت برابر است با تعداد *(متمایز)* ریشه‌های c از f با $g(c) > 0$، منهای تعداد ریشه‌های c از f با $g(c) < 0$، هر دو در بازه $[a, b]$.

اثبات. ابتدا فرض می‌کنیم $\gcd(f, f'g) = 1$. دنباله $(f_0, \dots, f_r)$ شرایط (۱)، (۳) و زیر را برآورده می‌کند:

(۲′) برای هر $c \in R$ با $f_0(c) = 0$، حاصلضرب $f_0 f_1$ علامت را از $\operatorname{sign} g(c)$ به $-\operatorname{sign} g(c)$ تغییر می‌دهد. (توجه کنید که $g(c) \neq 0$ است.)

این نتیجه نیز از لم ۷.۳.۱ به دست می‌آید. مانند قبل بررسی می‌کنیم که $v_{f,g}(x)$ هنگام عبور از یک ریشه حقیقی c از f_i چگونه تغییر می‌کند. اگر $i \geq 1$ باشد، استدلال قبلی همچنان معتبر است و نشان می‌دهد که $v_{f,g}(x)$ تغییر نمی‌کند. $\varepsilon := \operatorname{sign} f_1(c)$ را بنویسید و توجه کنید که $\varepsilon \neq 0$. اگر $i = 0$، با استفاده از (۲′) طرح علامت‌های اصلاح شده زیر را به دست می‌آوریم:

بنابراین $\nu_{f,g}(c_-) - \nu_{f,g}(c_+) = \operatorname{sign} g(c)$. در حالت کلی، دنباله $(f_0, \ldots, f_r)$ را با $(f_0/f_r, \ldots, f_r/f_r)$ جایگزین می‌کنیم و مشاهده می‌کنیم که (۱)، (۲') و (۳) برای دنباله جدید نیز معتبر باقی می‌مانند. هر دو دنباله در $x = a$ و $x = b$ تعداد تغییرات علامت یکسانی دارند، و بنابراین همانند قبل به نتیجه مطلوب می‌رسیم. □

مثال ۴-۵۵. دنباله اشتورم را برای چندجمله‌ای درجه سوم $f = t^3 + at + b$ با $a, b \in R$ محاسبه می‌کنیم. با فرض $a \neq 0$ داریم:

$$\begin{aligned} f_0 &= f, \\ f_1 &= f' = 3t^2 + a, \\ f_2 &= -\left(\frac{2a}{3}t + b\right), \\ f_3 &= -\frac{1}{4a^2}(4a^3 + 27b^2) = \frac{D}{4a^2} \end{aligned}$$

که در آن $D = -(4a^3 + 27b^2)$ دلتای f است. وقتی $a = 0$، دنباله کوتاه‌تر می‌شود؛ اگر $b \neq 0$ به $f_2 = -b$ و اگر $a = b = 0$ به $f_1 = f'$ ختم می‌شود. اگرچه این یک مثال ساده است، اما ویژگی مشخصه الگوریتم اشتورم را نشان می‌دهد: تکرار به صورت درختی از زیرحالت‌ها منشعب می‌شود که بستگی به ضرایب مشخص چندجمله‌ای دارد.

اکنون روش دوم برای شمارش دقیق ریشه‌های حقیقی را بررسی می‌کنیم. این روش متعلق به هرمیت و سیلوستر است و از ویژگی انشعاب الگوریتم اشتورم اجتناب می‌کند. ابتدا فرض کنید K یک میدان دلخواه و $f = t^n + a_1 t^{n-1} + \cdots + a_n$ یک چندجمله‌ای مونیک نابدیهی روی K باشد. فرض کنید $\alpha_1, \ldots, \alpha_n$ ریشه‌های f در بستار جبری $\overline{K}$ از K باشند، بنابراین $f = \prod_{j=1}^{n}(t - \alpha_j)$. برای $k = 0, 1, 2, \ldots$ تعریف می‌کنیم:

$$p_k = p_k(f) := \alpha_1^k + \cdots + \alpha_n^k,$$

که k-امین مجموع نیوتن f نامیده می‌شود. توجه کنید که $p_k \in K$ زیرا p_k نسبت به α_iها متقارن است. به طور صریح داریم $p_0 = n$، $p_1 = -a_1$، $p_2 = a_1^2 - 2a_2$، $p_3 = -a_1^3 + 3a_1a_2 - 3a_3$ و غیره. مجموع‌های نیوتن را می‌توان به صورت بازگشتی از رابطه زیر محاسبه کرد:

$$p_k + p_{k-1}a_1 + p_{k-2}a_2 + \cdots + p_1 a_{k-1} + k a_k = 0$$

برای $k \geq 0$، که در آن $a_j := 0$ برای $j > n$.

تعریف ۴-۵۶. ماتریس متقارن $n \times n$

$$H(f) := (p_{j+k}(f))_{0\le j,k\le n-1} = \begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{pmatrix}$$

(با درایه‌هایی در K) را ماتریس هرمیت f می‌نامیم.
درایه (j,k) ماتریس $H(f)$ فقط به $j+k$ بستگی دارد. ماتریس‌هایی با این ویژگی را ماتریس‌های هنکل می‌نامند.

برای $n \in \mathbb{N}$ و هر حلقه A، مجموعه (یا A–مدول) تمام ماتریس‌های متقارن $n \times n$ روی A را با $\mathrm{Sym}_n(A)$ نشان می‌دهیم. قضیه اینرسی سیلوستر برای ماتریس‌های متقارن روی $\mathbb{R}$ در جبر خطی شناخته شده است. اثبات استاندارد (با استقرا روی n) مستقیماً به این نتیجه تعمیم می‌یابد: اگر K یک میدان مرتب با مخروط مثبت P و $M \in \mathrm{Sym}_n(K)$ یک ماتریس متقارن دلخواه باشد، ماتریس معکوس‌پذیر $S \in \mathrm{GL}_n(K)$ وجود دارد به طوری که $S^\top MS = \mathrm{diag}(a_1, \ldots, a_n)$ یک ماتریس قطری است. عدد صحیح

$$\mathrm{sign}_P(M) := \sum_{i=1}^{n} \mathrm{sign}_P(a_i)$$

به M و P بستگی دارد اما به S بستگی ندارد، و به آن علامت (سیلوستر) M نسبت به P می‌گویند. ماتریس M نسبت به P معین مثبت است، که با $M >_P 0$ نشان داده می‌شود، اگر $\mathrm{sign}_P(M) = n$، یعنی اگر $a_i >_P 0$ برای $i = 1, \ldots, n$. اگر فقط نامساوی‌های $a_i \ge_P 0$ برای $i = 1, \ldots, n$ برقرار باشند، می‌گوییم M نسبت به P نیمه معین مثبت است، یا به اختصار *psd*، و با $M \ge_P 0$ نشان داده می‌شود.
اگر R یک میدان بسته حقیقی باشد و $M \in \mathrm{Sym}_n(R)$، هر مقدار ویژه M حقیقی است، یعنی در R قرار دارد. در واقع، اثبات معمول روی $\mathbb{R}$ برای R نیز کار می‌کند. پس

$$\mathrm{sign}(M) = \mathrm{Var}(1, a_1, a_2, \ldots, a_n) - \mathrm{Var}(1, -a_1, a_2, \ldots, (-1)^n a_n).$$

به ویژه، ماتریس M معین مثبت است اگر و تنها اگر $(-1)^j a_i > 0$، و نیمه معین مثبت است اگر و تنها اگر $(-1)^j a_i \ge 0$ برای $i = 1, \ldots, n$.

قضیه ۴-۵۷. فرض کنید K یک میدان با $\mathrm{char}(K) = 0$ و $f \in K[t]$ یک چندجمله‌ای تکین نابدیهی باشد.

(الف) رتبه $H(f)$ برابر است با تعداد ریشه‌های متمایز f در یک بستار جبری $\overline{K}$ از K.

(ب) اگر $K = R$ بسته حقیقی باشد، علامت $H(f)$ برابر است با تعداد ریشه‌های متمایز f در R.

به ویژه، برای $K = R$ بسته حقیقی، علامت سیلوستر $H(f)$ همیشه نامنفی است.

اثبات. (الف) فرض کنید $\alpha_1, \dots, \alpha_n \in \overline{K}$ به طوری که $f = \prod_{j=1}^{n}(t-\alpha_j)$. ماتریس هرمیت را می‌توان به صورت $H(f) = V^\top \cdot V$ تجزیه کرد، که در آن

$$V := \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

ماتریس وندرموند است. این یک قطری‌سازی (روی $\overline{K}$) از فرم درجه دوم نمایش داده شده توسط $H(f)$ ارائه می‌دهد: با نوشتن $x = (x_0, \dots, x_{n-1})^\top$ به عنوان بردار ستونی متغیرها، داریم

$$x^\top H(f) x = (Vx)^\top (Vx) = \sum_{j=1}^{n} L_{\alpha_j}(x)^2,$$

که در آن L_α فرم خطی $L_\alpha(x) = \sum_{k=0}^{n-1} \alpha^k x_k$ ($\alpha \in \overline{K}$) را نشان می‌دهد. اگر α_jها را به گونه‌ای برچسب بزنیم که $\alpha_1, \dots, \alpha_r$ ریشه‌های متمایز f باشند، فرم‌های خطی $L_{\alpha_1}, \dots, L_{\alpha_r}$ مستقل خطی هستند؛ زیرا مینور اصلی rام V ناصفر است. این موضوع رتبه $H(f) = r$ را اثبات می‌کند.

(ب) حال فرض کنید $K = R$ بسته حقیقی باشد. فرض کنید $i = \sqrt{-1}$، و $z \mapsto \overline{z}$ خودریختی نابدیهی $R(i)$ روی R (”مزدوج مختلط“) را نشان دهد. مطابق معمول، برای $z \in R(i)$ تعریف می‌کنیم $\mathrm{Re}(z) = \frac{1}{2}(z+\overline{z})$ و $\mathrm{Im}(z) = \frac{1}{2i}(z-\overline{z})$. برای $\alpha \in R(i)$ تعریف می‌کنیم $\mathrm{Re}(L_\alpha) := \frac{1}{2}(L_\alpha + L_{\overline{\alpha}})$ و $\mathrm{Im}(L_\alpha) := \frac{1}{2i}(L_\alpha - L_{\overline{\alpha}})$. این‌ها فرم‌های خطی با ضرایب در R هستند. با این نمادگذاری داریم $L_\alpha = \mathrm{Re}(L_\alpha) + i\,\mathrm{Im}(L_\alpha)$، $L_{\overline{\alpha}} = \mathrm{Re}(L_\alpha) - i\,\mathrm{Im}(L_\alpha)$ و بنابراین

$$L_\alpha^2 + L_{\overline{\alpha}}^2 = 2\mathrm{Re}(L_\alpha)^2 - 2\mathrm{Im}(L_\alpha)^2.$$

این نشان می‌دهد که هر جفت $\alpha_j \neq \overline{\alpha}_j$ از ریشه‌های مختلط مزدوج، تفاضل دو مربع از فرم‌های خطی حقیقی را ایجاد می‌کنند. از این مشاهده، گزاره (ب) واضح است. □

نتیجه ۴-۵۸. فرض کنید $K = R$ بسته حقیقی باشد. یک چندجمله‌ای $f \in R[t]$ حقیقی–ریشه‌ای است اگر و تنها اگر ماتریس هرمیت $H(f)$ آن نیمه معین مثبت باشد.

اثبات. یک ماتریس متقارن روی R نیمه معین مثبت است اگر و تنها اگر علامت آن برابر با رتبه آن باشد. □

نتیجه ۴-۵۹. دترمینان ماتریس هرمیت برابر است با $\det H(f) = D(f)$.

مثال ۴-۶۰. یک میدان بسته حقیقی R و یک چندجمله‌ای درجه سوم $f = t^3 + at + b$ با $a, b \in R$ را در نظر می‌گیریم. از جبر مجرد مشخص است که الگوی تجزیه f روی R فقط به علامت $D = D(f) = -(4a^3 + 27b^2)$ بستگی دارد. داریم

$$H(f) = \begin{pmatrix} ۳ & ۰ & -۲a \\ ۰ & -۲a & -۳b \\ -۲a & -۳b & ۲a^۲ \end{pmatrix}$$

با چندجمله‌ای مشخصه $p_{H(f)} = t^۳ + c_۱t^۲ + c_۲t + c_۳$ که در آن $c_۱ = -(۲a^۲ - ۲a + ۳)$، $c_۲ = -۴a^۳ + ۲a^۲ - ۶a - ۹b^۲$ و $c_۳ = -D$. توجه کنید که $c_۱ = -\frac{۱}{۲}((۲a-۱)^۲ + ۵) < ۰$ و $c_۲ = D + ۲a(a-۳) + ۱۸b^۲$. وقتی $D > ۰$، داریم $a < ۰$ و در نتیجه $c_۲ > ۰$، بنابراین در این حالت علامت $H(f)$ به صورت

$$\mathit{Var}(۱,\, c_۱ < ۰,\, c_۲ > ۰,\, -D < ۰) - \mathit{Var}(۱,\, -c_۱ > ۰,\, c_۲ > ۰,\, D > ۰) \;=\; ۳$$

است. برای $D = ۰$ و $(a,b) \neq (۰,۰)$ همچنان $c_۲ > ۰$ باقی می‌ماند و علامت $H(f) = ۲$ را به دست می‌آوریم. اگر $D < ۰$، داریم

$$\mathit{sign}\, H(f) \;=\; \mathit{Var}(۱,\, c_۱ < ۰,\, c_۲,\, -D > ۰) - \mathit{Var}(۱,\, -c_۱ > ۰,\, c_۲,\, D < ۰) \;=\; ۱$$

مستقل از علامت $c_۲$.

فرض کنید K یک میدان و $f = \prod_{j=۱}^{n}(t - \alpha_j)$ یک چندجمله‌ای تکین در $K[t]$ باشد، با $\alpha_۱, \ldots, \alpha_n$ در برخی بسطارهای جبری $\overline{K}$ از K. حلقه باقیمانده $A := K[t]/\langle f\rangle$ را به عنوان یک K–جبر در نظر بگیرید و $\overline{g} := g + \langle f\rangle \in A$ را برای $g \in K[t]$ بنویسید. در این صورت

$$\mathrm{tr}_{A/K}(\overline{g}) \;=\; \sum_{j=۱}^{n} g(\alpha_j).$$

بنابراین، با توجه به پایه $۱, \bar{t}, \ldots, \bar{t}^{n-۱}$ از A، ماتریس فرم دوسویه دقیقاً همان ماتریس هرمیت $H(f)$ است، زیرا

$$p_k \;=\; \sum_{j=۱}^{n} \alpha_j^k \;=\; \mathrm{tr}_{A/K}(\bar{t}^k)$$

برای تمام $k \geq ۰$.

را فراهم می‌کند. همانند قبل، فرض کنید $f \in K[t]$ یک چندجمله‌ای تکین از درجه $n \geq ۱$ با ریشه‌های $\alpha_۱, \ldots, \alpha_n$ در $\overline{K}$ باشد. برای هر $g \in K[t]$ دلخواه، مجموع‌های نیوتن نسبی را به صورت زیر تعریف می‌کنیم:

$$p_k(f,g) := \sum_{j=۱}^{n} \alpha_j^k\, g(\alpha_j) \quad (k \geq ۰).$$

ماتریس $n \times n$

$$H(f,g) := (p_{j+k}(f,g))_{0\le j,k\le n-1} = \begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{pmatrix}$$

(که در آن $p_\nu := p_\nu(f,g)$) را ماتریس هرمیت تعمیم یافته f و g می‌نامیم. اگر $g = \sum_l b_l t^l$ باشد، آنگاه

$$p_k(f,g) = \sum_j \alpha_j^k \sum_l b_l \alpha_j^l = \sum_{j,l} b_l \alpha_j^{k+l} = \sum_l b_l p_{k+l}(f) \quad (۱/۴)$$

برای هر k. بنابراین مجموع‌های نیوتن نسبی ترکیبات خطی از مجموع‌های نیوتن معمولی هستند.

لم ۴-۶۱. اگر $f, g \in K[t]$ و f تکین باشد، ضرایب $p_k(f,g)$ از $H(f,g)$ چندجمله‌ای‌های صحیحی در ضرایب f و g هستند.

می‌توانیم این گزاره را دقیق‌تر بیان کنیم: اگر $n \ge 1$, $m \ge 0$ ثابت باشند، آنگاه برای هر $k \ge 0$ یک چندجمله‌ای

$$P_k(a,b) = P_k(a_1, \dots, a_n, b_0, \dots, b_m)$$

در متغیرهای $a = (a_1, \dots, a_n)$ و $b = (b_0, \dots, b_m)$ وجود دارد، به طوری که برای تمام چندجمله‌ای‌های $f = t^n + \sum_{i=1}^n a_i t^{n-i}$ و $g = \sum_{j=0}^m b_j t^j$ داریم:

$$p_k(f,g) = P_k(a,b).$$

اثبات. واضح است. □

قضیه ۴-۶۲. فرض کنید K یک میدان با $\mathrm{char}(K) = 0$ و $f \in K[t]$ یک چندجمله‌ای تکین از درجه $n \ge 1$ باشد. برای هر چندجمله‌ای $g \in K[t]$ داریم:

$$\operatorname{rk} H(f,g) = \Big| \{\alpha \in \overline{K} \colon f(\alpha) = 0 \text{ و } g(\alpha) \ne 0\} \Big|.$$

اگر $K = R$ بسته حقیقی باشد، آنگاه:

$$\mathit{sign} H(f,g) = \sum_{\substack{\alpha \in K \\ f(\alpha)=0}} \mathit{sign} g(\alpha).$$

اثبات. مثل قبل $x = (x_0, \dots, x_{n-1})^T$ (بردار ستونی) را در نظر بگیرید، در این صورت:

$$x^T \cdot H(f,g) \cdot x = \sum_{j,k=0}^{n-1} \sum_{l=1}^{n} g(\alpha_l)\alpha_l^{j+k} x_j x_k = \sum_{l=1}^{n} g(\alpha_l) L_{\alpha_l}(x)^2,$$

با استفاده از:

$$\mathrm{Re}((a+ib)(u+iv)^2) = au^2 - 2buv - av^2$$

$(a,b,u,v \in R)$ برای $\alpha,\beta \in R(i)$ با $\alpha \neq \overline{\alpha}$ و $\beta \neq 0$ می‌بینیم که فرم درجه دوم:

$$\beta L_\alpha(x)^2 + \overline{\beta} L_{\overline{\alpha}}(x)^2$$

برابر است با $\lambda_1(x)^2 - \lambda_2(x)^2$ با فرم‌های خطی مستقل λ_1, λ_2 روی R. □

می‌توانیم ریشه‌های حقیقی را تحت تعداد دلخواهی از شرایط جانبی بشماریم، با استفاده از روش اشتورم یا هرمیت. برای توضیح این موضوع، فرض کنید چندجمله‌ای‌های $f, g_1, \ldots, g_r \in R[t]$ با $f \neq 0$ داده شده‌اند. برای هر چندتایی $e = (e_1, \ldots, e_r)$ از اعداد صحیح نامنفی، $g^e := g_1^{e_1} \cdots g_r^{e_r}$ را بنویسید و فرض کنید:

$$N_e := \sum_{c \in K : f(c)=0} \mathrm{sign} g^e(c).$$

همانطور که دیدیم، اعداد N_e را می‌توان به طور مؤثر از ضرایب f و g_iها با پیروی از روش اشتورم یا هرمیت به دست آورد. لم بعدی و نکته زیر نشان می‌دهند که چگونه از این اعداد N_e، تعداد ریشه‌های حقیقی c از f با علامت‌های مشخص شده برای $g_1(c), \ldots, g_r(c)$ را بازیابی کنیم:

گزاره ۴-۶۳. فرض کنید $f, g_1, \ldots, g_r \in R[t]$ با $f \neq 0$ و $r \geq 0$. آنگاه:

$$2^{-r} \sum_{e \in \{1,2\}^r} N_e = \Big|\{c \in R : f(c) = 0,\ g_1(c) > 0, \ldots, g_r(c) > 0\}\Big|.$$

اثبات. داریم

$$\sum_{e \in \{1,2\}^r} N_e = \sum_{\substack{c \in R \\ f(c)=0}} \sum_{e \in \{1,2\}^r} \mathrm{sign}(g_1(c)^{e_1} \cdots g_r(c)^{e_r}) = \sum_{\substack{c \in R \\ f(c)=0}} \prod_{i=1}^{r} \big(\mathrm{sign}\, g_i(c) + \mathrm{sign}\, g_i(c)^2\big)$$

که تساوی اول از تعریف N_e و دومی از بسط توزیعی حاصلضرب‌ها در جمع آخر ناشی می‌شود. از آن‌جا که برای $\varepsilon_1, \ldots, \varepsilon_r \in \{0, \pm 1\}$ داریم:

$$\prod_{i=۱}^{r}(\varepsilon_i+\varepsilon_i^{۲})=\begin{cases}۲^r & \text{اگر } \varepsilon_۱=\cdots=\varepsilon_r=۱,\\ ۰ & \text{در غیر این صورت},\end{cases}$$

اثبات کامل می‌شود. □

این گزاره به ما امکان می‌دهد تعداد

$$\left|\{c\in R\colon f(c)=۰,\ \operatorname{sign} g_j(c)=\varepsilon_j \text{ برای } j=۱,\dots,r\}\right|$$

را برای هر چندتایی مشخصی از علامت‌ها $\varepsilon=(\varepsilon_۱,\dots,\varepsilon_r)\in\{۰,۱,-۱\}^r$ تعیین کنیم.

۴.۴ تجزیه جبری استوانه‌ای

تجزیه جبری استوانه‌ای (CAD) یکی از ابزارهای قدرتمند در هندسه جبری حقیقی و جبر محاسباتی است که به تجزیه فضای اقلیدسی به سلول‌های هندسی ساده می‌پردازد. این سلول‌ها به گونه‌ای هستند که هر چندجمله‌ای در هر سلول دارای علامت ثابت است. CAD به‌ویژه در مسائل مربوط به تصمیم‌گیری در مورد خواص جبری و هندسی مجموعه‌های تعریف شده توسط چندجمله‌ای‌ها کاربرد دارد و نقش مهمی در تحلیل و حل مسائل پیچیده ریاضی ایفا می‌کند.

تاریخچه CAD به دهه ۱۹۷۰ بازمی‌گردد، زمانی که جورج کولینز این روش را برای اولین بار معرفی کرد. ابداع CAD باعث پیشرفت‌های قابل توجهی در جبر محاسباتی شد و به یکی از ابزارهای اصلی در تحلیل سیستم‌های چندجمله‌ای حقیقی تبدیل شد. یکی از کاربردهای مهم CAD، حل مسائل تصمیم‌گیری جبری حقیقی است، مانند تصمیم‌گیری در مورد تهی بودن یک مجموعه جبری یا تعیین علامت یک چندجمله‌ای در نقاط مختلف.

یکی از ویژگی‌های بارز CAD، توانایی آن در تبدیل مسائل پیچیده جبری به مسائل ساده‌تر و قابل حل است. این ویژگی باعث شده است که CAD در زمینه‌های مختلفی مانند بهینه‌سازی، کنترل رباتیک، و تحلیل سیستم‌های دینامیکی مورد استفاده قرار گیرد. به عنوان مثال، در بهینه‌سازی، CAD می‌تواند به تجزیه فضای جستجو به نواحی ساده‌تر کمک کند و امکان یافتن بهینه‌های محلی و جهانی را فراهم سازد.

در این فصل، ابتدا به معرفی مفاهیم پایه‌ای CAD پرداخته و سپس به بررسی برخی از نتایج و الگوریتم‌های مهم در این زمینه خواهیم پرداخت. این مفاهیم شامل تجزیه استوانه‌ای، سلول‌های جبری، و الگوریتم‌های تولید CAD است. همچنین به بررسی کاربردهای عملی CAD در زمینه‌های مختلف علمی و مهندسی خواهیم پرداخت.

هدف از این فصل، فراهم کردن یک دیدگاه جامع و منسجم از CAD و نشان دادن اهمیت و کاربردهای گسترده آن در حوزه‌های مختلف تحقیقاتی است. با بررسی دقیق‌تر و جامع‌تر این مفاهیم، خواهیم دید که چگونه CAD می‌تواند ابزار قدرتمندی برای تحلیل و حل مسائل پیچیده جبری و هندسی باشد. در بخش‌های بعدی، به تفصیل به موضوعاتی مانند بهبود الگوریتم‌های CAD، تحلیل پیچیدگی زمانی و مکانی، و کاربردهای عملی در مسائل علمی و مهندسی خواهیم پرداخت.

۵.۴ زیرمنتج دو چندجمله‌ای

مفهوم زیرمنتج درواقع تعمیم مفهوم منتج دو چندجمله‌ای است که در فصل ۲ به آن پرداخته شد. با استفاده از زیرمنتج دو چندجمله‌ای می‌توان درجه بزرگترین مقسوم علیه مشترک دو چندجمله‌ای را مشخص کرد. در این بخش، K را یک میدان و چندجمله‌ای‌های f و g را به صورت

$$f = a_n x^n + \ldots + a_1 x + a_0,$$
$$g = b_m x^m + \ldots + b_1 x + b_0$$

با درجه‌های n و m در $K[x]$ در نظر می‌گیریم.

تعریف ۴-۶۴. چندجمله‌ای‌های f و g را به صورت بالا در نظر بگیرید؛ اگر $m \neq n$، فرض می‌کنیم $0 \leq j \leq \min\{m, n\}$ و اگر $m = n$، فرض می‌کنیم $0 \leq j \leq n - 1$. j–امین ماتریس زیرمنتج $\mathrm{Sr}_j(f, g)$ از چندجمله‌ای‌های f و g ماتریس $(m + n - 2j) \times (m + n - j)$ به صورت زیر است:

$$\mathrm{Sr}_j(f,g) = \begin{bmatrix} a_n & a_{n-1} & \ldots & a_0 & & & \\ & a_n & a_{n-1} & \ldots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & \ldots & b_0 & & \\ & \ddots & \ddots & & & \ddots & \\ & & b_m & b_{m-1} & \ldots & \ldots & b_0 \end{bmatrix}$$

درواقع، ماتریس $\mathrm{Sr}_j(f, g)$ با حذف کردن j سطر اول نظیر f و حذف j سطر اول نظیر g از ماتریس سیلوستر بدست می‌آید. یادآور می‌شویم که ماتریس سیلوستر را به صورت زیر تعریف می‌کنیم:

$$\mathrm{Syl}(f,g) = \begin{bmatrix} a_n & a_{n-1} & \ldots & a_0 & & & \\ & a_n & a_{n-1} & \ldots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & \ldots & b_0 & & \\ & \ddots & \ddots & & & \ddots & \\ & & b_m & b_{m-1} & \ldots & \ldots & b_0 \end{bmatrix}$$

تعریف ۴-۶۵. چندجمله‌ای‌های f و g را به ترتیب با درجات n و m به صورت بالا در نظر بگیرید. j–امین زیرمنتج f

و g را به صورت ترکیب خطی زیر تعریف می‌کنیم:

$$\mathrm{SRC}_j(f,g) := x^{m-j-1}f, \ldots, xf, f, x^{n-j-1}g, \ldots, xg, g$$

حال اگر ضرایب r و s در میدان K وجود داشته باشند به طوری که ترکیب خطی $sf+rg=0$ وابسته خطی باشد، آنگاه $\mathrm{SRC}_j(f,g)=0$ قرار می‌دهیم و در غیر این صورت $\mathrm{SRC}_j(f,g)=1$.

می‌دانیم که چندجمله‌ای‌های f و g دارای بزرگترین مقسوم علیه مشترک است اگر و تنها اگر $\mathrm{Res}(f,g)=0$. حال قضیه مهمی را بیان و اثبات می‌کنیم که در ادامه از آن برای مشخص کردن درجه ب.م.م دو چندجمله‌ای استفاده می‌کنیم.

قضیه ۴-۶۶. منتج دو چندجمله‌ای $\mathrm{Res}(f,g)$ صفر می‌شود اگر و تنها اگر چندجمله‌ای‌های $r,s \in K[x]$ وجود داشته باشند که $s,r \neq 0$، $\deg(r) < \deg(f)$، $\deg(s) < \deg(g)$ و $sf+rg=0$.

اثبات. با استفاده از نمادهای چندجمله‌ای‌های f و g در بالا، سطرهای ماتریس سیلوستر را به صورت بردارهای

$$x^{m-1}f, \ldots, xf, f, x^{n-1}g, \ldots, xg, g$$

در K-فضای برداری با چندجمله‌ای‌های با درجه کمتر از $m+n$، با پایه $x^{m+n-1}, x^{m+n-2}, \ldots, x, 1$ در نظر می‌گیریم. منتج $\mathrm{Res}(f,g)$ صفر می‌شود اگر و تنها اگر این $m+n$ بردارها مستقل خطی باشند؛ یعنی اگر ضرایب $r_0, \ldots, r_{n-1}$ و $s_0, \ldots, s_{m-1}$ در K وجود داشته باشند که هم‌زمان صفر نمی‌شوند و

$$s_{m-1}x^{m-1}f + \ldots + s_1xf + s_0f + r_{n-1}x^{n-1}g + \ldots + r_1xg + r_0g = 0.$$

با قرار دادن $r := \sum_{i=0}^{n-1} r_i x^i$ و $s := \sum_{j=0}^{m-1} s_j x^j$، حکم مورد نظر برقرار می‌شود اگر و تنها اگر $(r,s) \neq (0,0)$. پس $\deg(r) < \deg(f)$، $\deg(s) < \deg(g)$ و $sf+rg=0$. □

لم ۴-۶۷. چندجمله‌ای‌های f و g را به صورت بالا در نظر بگیرید؛ اگر $m \neq n$، فرض می‌کنیم $0 \leq j \leq \min\{m,n\}$ و اگر $m=n$، فرض می‌کنیم $0 \leq j \leq n-1$. زیرمنتج $\mathrm{SRC}_j(f,g)$ صفر می‌شود اگر و تنها اگر چندجمله‌ای‌های $r,s \in K[x]\setminus\{0\}$ وجود داشته باشند که $\deg(r) < n-j$، $\deg(s) < m-j$ و $\deg(sf+rg) < j$.

اثبات. سطرهای ماتریس $\mathrm{SRC}_j(f,g)$ را می‌توان به صورت بردارهای

$$x^{m-j-1}f, \ldots, xf, f, x^{n-j-1}g, \ldots, xg, g$$

در K-فضای برداری با درجه کمتر از $m+n-j$ و با پایه $x^{m+n-j-1}, x^{m+n-j-2}, \ldots, x, 1$ در نظر گرفت. طبق تعریف زیرمنتج، $\mathrm{SRC}_j(f,g)$ صفر می‌شود اگر و تنها اگر این $m+n-2j$ بردارها به طور نابدیهی یک چندجمله‌ای با درجه کمتر از j تولید کنند. به طور معادل، ضرایب $r_0, \ldots, r_{n-j-1}$ و $s_0, \ldots, s_{m-j-1}$ در K وجود دارند که هم‌زمان صفر نمی‌شوند و

$$\deg(s_{m-j-1}x^{m-j-1}f + \ldots + s_1xf + s_0f + r_{n-j-1}x^{n-j-1}g + \ldots + r_1xg + r_0g) < j.$$

با قرار دادن $r = \sum_{i=۰}^{n-j-۱} r_i x^i$ و $s = \sum_{k=۰}^{m-j-۱} s_k x^k$ شرط مورد نظر برقرار می‌شود اگر و تنها اگر $(r,s) \neq (۰,۰)$، $\deg(r) < n-j$، $\deg(s) < m-j$ و $\deg(sf+rg) < j$. □

قضیه ۴-۶۸. چندجمله‌ای‌های f و g را به صورت بالا در نظر بگیرید؛ اگر $m \neq n$، فرض می‌کنیم $۰ \leq j \leq \min\{m,n\}$ و اگر $m = n$، فرض می‌کنیم $۰ \leq j \leq n-۱$. در این صورت f و g یک مقسوم علیه مشترک از درجه حداقل j دارند اگر و تنها اگر

$$\mathrm{SRC}_۰(f,g) = \ldots = \mathrm{SRC}_{j-۱}(f,g) = ۰.$$

اثبات. فرض کنید $h \in K[x]$ ب.م.م f و g با درجه j باشد. در این صورت چندجمله‌ای $f_۰$ با حداکثر درجه $n-j$ و چندجمله‌ای $g_۰$ با حداکثر درجه $m-j$ وجود دارد به طوری که

$$f = hf_۰, \qquad g = hg_۰.$$

قرار دهید $r := f_۰$ و $s := -g_۰$. در نتیجه $sf + rg = ۰$ و بنابر لم ۱-۶، $\mathrm{SRC}_i(f,g) = ۰$ برای $۰ \leq i < j$.
برعکس، فرض کنید $\mathrm{SRC}_i(f,g) = ۰$ برای $۰ \leq i < j$. حکم مورد نظر را با استقرا روی j اثبات می‌کنیم؛ در صورتی که $j = ۰$، حکم به طور بدیهی برقرار و هنگامی که $j = ۱$ بنابر قضیه‌ای که در بخش منتج دو چندجمله‌ای بیان شد، برقرار است. حال فرض کنید $j > ۱$ و $\mathrm{SRC}_۰(f,g) = \ldots = \mathrm{SRC}_{j-۱}(f,g) = ۰$. همچنین فرض کنید h ب.م.م f و g باشد. بنابر فرض استقرا، $\mathrm{SRC}_۰(f,g) = \ldots = \mathrm{SRC}_{j-۲}(f,g) = ۰$؛ یعنی h حداقل از درجه $j-۱$ است. چون $\mathrm{SRC}_{j-۱}(f,g) = ۰$ و بنابر لم ۱-۶، $r,s \in K[x]\setminus\{۰\}$ که $\deg(r) < n-(j-۱)$، $\deg(s) < m-(j-۱)$ و $\deg(sf+rg) < j-۱$، چون h، $sf+rg$ را عاد می‌کند و حداقل از درجه $j-۱$ است، داریم $sf+rg = ۰$؛ پس $sf = -rg$. در نتیجه $\mathrm{lcm}(f,g)$ حداکثر از درجه $n+m-j$ است. بنابراین h حداقل از درجه j است. □

نتیجه زیر بنابر لم ۱-۶ و قضیه ۲-۶ واضح است.

نتیجه ۴-۶۹. چندجمله‌ای‌های f و g را به صورت بالا در نظر بگیرید؛ اگر $m \neq n$، فرض می‌کنیم $۰ \leq j \leq \min\{m,n\}$ و اگر $m = n$، فرض می‌کنیم $۰ \leq j \leq n-۱$. در این صورت $\deg(\gcd(f,g)) = j$ اگر و تنها اگر

$$\mathrm{SRC}_۰(f,g) = \ldots = \mathrm{SRC}_{j-۱}(f,g) = ۰, \quad \mathrm{SRC}_j(f,g) \neq ۰.$$

مثال ۴-۷۰. چندجمله‌ای‌های $f = x^۳ - ۲x^۲ - x - ۶$ و $g = x^۴ + ۳x^۳ + ۷x^۲ + ۷x + ۶$ را در نظر بگیرید. در این صورت $\mathrm{SRC}_۰(f,g) = \mathrm{Res}(f,g) = ۰$ و

$$\mathrm{SRC}_۱(f,g) = \det \begin{pmatrix} ۱ & -۲ & -۱ & -۶ & ۰ \\ ۰ & ۱ & -۲ & -۱ & -۶ \\ ۰ & ۰ & ۱ & -۲ & -۱ \\ ۱ & ۳ & ۷ & ۷ & ۶ \\ ۰ & ۱ & ۳ & ۷ & ۷ \end{pmatrix} = ۰$$

و

$$\mathrm{SRC}_{۲}(f,g)=\det\begin{pmatrix}۱ & -۲ & -۱\\ ۰ & ۱ & -۲\\ ۱ & ۳ & ۷\end{pmatrix}=۱۸.$$

بنابراین $\deg(\gcd(f,g))=۲$.

اکنون به تعریف دقیق یک تجزیه جبری استوانه‌ای می‌پردازیم.

تعریف ۴-۷۱. یک تجزیه جبری استوانه‌ای $(C.A.D)$ از $\mathbb{R}^n$ عبارت است از دنباله $S_۱,\ldots,S_n$ که در آن S_i برای هر $۱\leq i\leq n$ یک افراز متناهی از $\mathbb{R}^i$ به زیرمجموعه‌های نیمه‌جبری است که سلول‌های در سطح i نامیده شده و در شرایط زیر صدق می‌کند

(۱) هر سلول $C\in S_۱$، یک نقطه یا یک بازه باز است.

(۲) برای هر $۱\leq i<n$ و هر $C\in S_i$، تعداد متناهی نگاشت نیمه‌جبری پیوسته $f_{C,۱}<\ldots<f_{C,l_C}:C\longrightarrow\mathbb{R}$ وجود دارد که استوانه $C\times\mathbb{R}\subset\mathbb{R}^{i+۱}$، اجتماع مجزای سلول‌های $S_{i+۱}$ به یکی از شکل‌های زیر است:

(i) نمودار یکی از توابع $f_{C,j}$، یعنی $\{(x',x_{j+۱})\in C\times\mathbb{R}\mid x_{j+۱}=f_{C,j}(x')\}$ برای $j=۱,\ldots,l_C$ است.

(ii) یک نوار استوانه‌ای کراندار شده توسط نمودار نگاشت‌های $f_{C,j}$ و $f_{C,j+۱}$ یعنی،

$$\{(x',x_{j+۱})\in C\times\mathbb{R}\mid f_{C,j}(x')<x_{j+۱}<f_{C,j+۱}(x')\}$$

برای $j=۰,\ldots,l_C$ است که در آن $f_{C,۰}=-\infty$ و $f_{C,l_C+۱}=+\infty$.

فرض کنید π_k نگاشت تصویر روی k مؤلفه اول باشد. در این صورت از تعریف بالا نتیجه می‌شود که برای هر سلول T از S_i که $k\leq i$، $C=\pi_k(T)$ یک سلول از S_k است. در این حالت گوییم سلول T بالای سلول C قرار گرفته است. اگر فرض کنیم که سلول $C\in S_i$ توسط سلول‌های $T_۱,\ldots,T_m\in S_{i+۱}$ تعریف شده باشد، آنگاه داریم $C\times\mathbb{R}=\bigcup_{j=۱}^{m}T_j$.

تعریف ۴-۷۲. خانواده متناهی از چندجمله‌ای‌های $P_۱,\ldots,P_r\in R[x_۱,\ldots,x_n]$ را در نظر بگیرید. زیرمجموعه C از $\mathbb{R}^n$ را $(P_۱,\ldots,P_r)$-پایا می‌نامیم هرگاه چندجمله‌ای P_i روی C علامت ثابت داشته باشد.

در حقیقت، در یک تجزیه جبری استوانه‌ای در پی افرازی از $\mathbb{R}^n$ هستیم که هر سلول در سطح n آن $(P_۱,\ldots,P_r)$-پایا باشد. چنین تجزیه‌ای را سازگار با $(P_۱,\ldots,P_r)$ می‌نامیم.

نمادگذاری ۴-۷۳ (دیسک)**.** منظور از یک دیسک باز با مرکز z و شعاع r، مجموعه $D(z,r)=\{w\in C\mid|z-w|<r\}$ است.

گزاره ۴-۷۴. فرض کنید $P=a_px^p+\ldots+a_۱x+a_۰\in C[x]$ و $a_p\neq۰$. اگر $x\in C$ یک ریشه برای P باشد، آنگاه

$$|x|\leq\max\left(p|\tfrac{a_{p-i}}{a_p}|\right)^{۱/i}=M,$$

برای $i=۱,\ldots,p$.

اثبات. اگر $z \in C$ به طوری باشد که $|z| > M$، آنگاه $|a_{p-i}| < |a_p||z|^i/p$، $i = ۱, \ldots, p$. بنابراین

$$|a_{p-۱}z^{p-۱} + \ldots + a_۰| \leq |a_{p-۱}||z|^{p-۱} + \ldots + |a_۰| < |a_p z^p|$$

و $P(z) \neq ۰$. □

چندجمله‌ای $x^q + b_{q-۱}x^{q-۱} + \ldots + b_۰ \in C[x]$ از درجه q را با نقطه $(b_{q-۱}, \ldots, b_۰) \in C^q$ شناسایی می‌کنیم.

لم ۴-۷۵. اگر $r > ۰$، یک همسایگی باز U حول $(x - z)^\mu$ در C^μ موجود است به طوری که ریشه‌های هر چندجمله‌ای تکین در U، در $D(z, r)$ قرار دارند.

اثبات. بدون کاستن از کلیت، می‌توانیم فرض کنیم $z = ۰$ و بنابر گزاره ۱۱-۶، حکم مورد نظر برقرار است. □

نگاشت

$$m : C^q \times C^r \longrightarrow C^{q+۱}$$
$$(Q, R) \mapsto QR$$

را تعریف شده توسط ضرب چندجمله‌ای‌های تکین، به ترتیب با درجات q و r، در نظر بگیرید.

لم ۴-۷۶. فرض کنید $P_۰ \in C^{q+۱}$ یک چندجمله‌ای تکین به صورت $P_۰ = Q_۰R_۰$ باشد که $Q_۰$ و $R_۰$ چندجمله‌ای‌های تکین هم‌اول *(ب.م.م آن‌ها ۱ است)* با درجات q و r هستند. همسایگی‌های باز U از $P_۰$ در $C^{q+۱}$، $U_۱$ از $Q_۰$ در C^q و $U_۲$ از $R_۰$ در C^r وجود دارند به طوری که هر $P \in U$ به طور منحصر به فردی، حاصل ضربی از چندجمله‌ای‌های تکین هم‌اول QR است که $Q \in U_۱$ و $R \in U_۲$.

اثبات. ماتریس ژاکوبی m، ماتریس سیلوستر نظیر

$$x^{q-۱}R_۰, \ldots, R_۰, x^{r-۱}Q_۰, \ldots, Q_۰$$

است. بنابراین ژاکوبی m، در حد علامت، با منتج $R_۰$ و $Q_۰$ برابر و در نتیجه ناصفر است؛ زیرا $R_۰$ و $Q_۰$ عامل مشترک ندارند. سپس، با استفاده از قضیه تابع ضمنی، حکم موردنظر برقرار می‌شود. □

قضیه ۴-۷۷ (پیوستگی ریشه‌ها). فرض کنید $P \in \mathbb{R}[x_۱, \ldots, x_n]$ و S زیرمجموعه نیمه‌جبری از $\mathbb{R}^{k-۱}$ باشد. همچنین فرض کنید $\deg(P(x', X_k))$ روی S ثابت و برای $a' \in S$، $z_۱, \ldots, z_j$ ریشه‌های مجزا $P(a', x_k)$ در $C = \mathbb{R}[i]$، با ضرایب $\mu_۱, \ldots, \mu_j$ باشند. اگر دیسک های باز $D(z_i, r) \subset C$ متمایز باشند، آنگاه یک همسایگی باز V حول a' وجود دارد به طوری که برای هر $x' \in V \cap S$، چندجمله‌ای $P(x', X_k)$ به طور دقیق μ_i ریشه *(با شمارش تکرار)* در $D(z_i, r)$ برای $i = ۱, \ldots, j$ دارد.

اثبات. فرض کنید $P_0 = (x-z_1)^{\mu_1}\dots(x-z_j)^{\mu_j}$. بنابر لم ۱۳-۶، همسایگی‌های باز U از P_0 در $C^{\mu_1+\dots+\mu_j}$، U_1 از $(x-z_1)^{\mu_1}$ در C^{μ_1} و به همین ترتیب U_j از $(x-z_j)^{\mu_j}$ وجود دارند به طوری که هر $P \in U$ را می‌توان به صورت $P = Q_1 \dots Q_j$ نوشت که Q_i، چندجمله‌ای‌هایی تکین در U_i هستند. با استفاده از لم ۱۲-۶، به سادگی قابل مشاهده است که یک همسایگی V حول a' در S وجود دارد به طوری که برای هر $x' \in V$، چندجمله‌ای $P(x', x_k)$ دقیقاً دارای μ_i ریشه (با شمارش تکرار) در $D(z_i, r)$ برای $i = 1, \dots, j$ است. □

در ادامه شرایطی را در نظر می‌گیریم که ریشه‌های دو چندجمله‌ای روی یک مجموعه نیمه‌جبری همبند، یک ساختار استوانه‌ای تشکیل بدهند.

گزاره ۷۸-۴. چندجمله‌ای‌های $P, Q \in \mathbb{R}[x_1, \dots, x_n]$ و زیرمجموعه نیمه‌جبری همبند S از $\mathbb{R}^{k-1}$ را در نظر بگیرید. فرض کنید P و Q روی S ناصفر، $(\deg(P(x', x_k))$، $\deg(Q(x', x_k))$، $\deg(\gcd(P(x', x_k), Q(x', x_k)))$، تعداد ریشه‌های متمایز $P(x', x_k)$ در C و تعداد ریشه‌های متمایز $Q(x', x_k)$ روی C ثابت باشند به طوری که $x' \in S$. در این صورت، توابع نیمه‌جبری $f_1 < \dots < f_l : S \longrightarrow R$ وجود دارند به طوری که، برای هر $x' \in S$، مجموعه ریشه‌های حقیقی $(PQ)(x', x_k)$ برابر است با $\{f_1(x'), \dots, f_l(x')\}$. همچنین، برای $i = 1, \dots, l$، تکرار ریشه‌های $f_i(x')$ از $P(x', x_k)$ ثابت است.

اثبات. فرض کنید $a' \in S$ و $z_1, \dots, z_j$ ریشه‌های متمایز ضرب $(PQ)(a', x_k)$ در C باشند. همچنین فرض کنید μ_i تعداد z_i به عنوان ریشه $P(a', x_k)$ و v_i تعداد z_i به عنوان ریشه $Q(a', x_k)$ باشد. درجه $\gcd(P(a', x_k), Q(a', x_k))$ برابر با $\sum_{i=1}^{j} \min(\mu_i, v_i)$ و هر z_i دارای تعداد $\min(\mu_i, v_i)$ به عنوان ریشه این ب.م.م است. $r > 0$ را به طوری انتخاب کنید که دیسک‌های $D(z_i, r)$ متمایز باشند. بنابر قضیه ۱۴-۶ و اینکه تعداد ریشه‌های مختلط متمایز بعد از S ثابت می‌مانند، نتیجه می‌گیریم که یک همسایگی V حول a' در S وجود دارد که برای هر $x' \in V$، هر دیسک $D(z_i, r)$ دارای حداقل یک ریشه از $P(x', x_k)$ با تعداد μ_i و یک ریشه از $Q(x', x_k)$ با تعداد v_i است. از آن‌جایی که درجه $\gcd(P(x', x_k), Q(x', x_k))$ برابر با $\sum_{i=1}^{j} \min(\mu_i, v_i)$ است، این ب.م.م باید یک ریشه ζ_i، با تعداد $\min(\mu_i, v_i)$، در هر دیسک $D(z_i, r)$ داشته باشد به طوری که $\min(\mu_i, v_i) > 0$. پس، برای هر $x' \in V$ و هر $i = 1, \dots, j$، به طور دقیق یک ریشه ζ_i از $(PQ)(x', x_k)$ در $D(z_i, r)$ وجود دارد به طوری که ریشه $P(x', x_k)$ و ریشه $Q(x', x_k)$ است. اگر z_i حقیقی باشد، آنگاه ζ_i هم حقیقی است. اگر z_i حقیقی نباشد، ζ_i هم حقیقی نیست (چون $D(z_i, r)$ با تصویرش (توسط مزدوج) متمایز است). بنابراین، اگر $x' \in V$، تعداد ریشه‌های حقیقی متمایز دو چندجمله‌ای $(PQ)(x', x_k)$ و $(PQ)(a', x_k)$ برابر است. از آن‌جایی که S نیمه‌جبری همبند است، برای هر $x' \in S$ تعداد ریشه‌های حقیقی متمایز $(PQ), (x', x_k)$ ثابت است؛ این عدد را با l نشان دهید. برای $1 \leq i \leq l$، فرض کنید $f_i : S \longrightarrow R$، $x' \in S$ را به i-امین ریشه حقیقی $(PQ)(x', x_k)$ بفرستد. با انتخاب r به اندازه کافی کوچک، قابل مشاهده است که f_iها پیوسته هستند. چون S نیمه‌جبری همبند است، هر $f_i(x')$ به عنوان یک ریشه از $P(x', x_k)$ و یک ریشه از $Q(x', x_k)$ تعداد

ثابتی دارد. اگر S توسط فرمول $\Theta(x')$ تعریف شده باشد، نمودار f_i توسط فرمول

$$\begin{aligned}&\Theta(x')\\&\wedge((\exists y_1)\dots(\exists y_l)(y_1<\dots<y_l\wedge(PQ)(x',y_1)=0\wedge\dots\wedge(PQ)(x',x_l)=0)\\&\wedge((\forall y)(PQ)(x',y)=0\Rightarrow(y=y_1\vee\dots\vee y=y_l))\wedge x_k=y_i),\end{aligned}$$

تعریف می‌شود که نشان می‌دهد f_i نیمه‌جبری است (طبق حذف سور). □

بنابراین نشان داده‌ایم:

نتیجه ۷۹-۴. فرض کنید $\mathcal{P}$ یک زیرمجموعه متناهی از $\mathbb{R}[x_1,\dots,x_n]$ و S یک زیرمجموعه نیمه‌جبری همبند از $\mathbb{R}^{k-1}$ باشد. همچنین فرض کنید برای هر $P\in\mathcal{P}$، $\deg(P(x',x_k))$ و تعداد ریشه‌های متمایز مختلط P روی S ثابت و برای هر جفت $P,Q\in\mathcal{P}$، $\deg(\gcd(P(x',x_k),Q(x',x_k)))$ روی S ثابت باشد. در این صورت، توابع نیمه‌جبری $f_1<\dots<f_l:S\longrightarrow R$ وجود دارند به طوری که برای هر $x'\in S$، مجموعه ریشه‌های حقیقی از $\prod_{P\in\mathcal{P}'}P(x',x_k)$، که $\mathcal{P}'$ شامل چندجمله‌ای‌های ناصفر روی S است، برابر است با $\{f_1(x'),\dots,f_l(x')\}$.

نمادگذاری ۸۰-۴ (کوتاه‌سازی). فرض کنید $Q=b_qx^q+\dots+b_0\in\mathbb{R}[x]$. برای $0\le i\le q$، کوتاه‌سازی Q در i را به صورت زیر تعریف می‌کنیم:

$$\mathrm{Tru}_i(Q)=b_ix^i+\dots+b_0$$

نمادگذاری ۸۱-۴ (حذف). با استفاده از نمادگذاری ۱۷-۶، با پارامترهای $x_1,\dots,x_{k-1}$ و متغیر اصلی x_k، فرض کنید

$$\mathrm{Tru}(\mathcal{P})=\{\mathrm{Tru}(P)\mid P\in\mathcal{P}\}.$$

حال، $\mathrm{Elim}_{x_k}(\mathcal{P})$ را مجموعه تمام چندجمله‌ای‌های در $\mathbb{R}[x_1,\dots,x_{k-1}]$ به شکل زیر تعریف می‌کنیم:

(۱) اگر $R\in\mathrm{Tru}(\mathcal{P})$، $\deg_{x_k}(R)\ge 2$، آنگاه $\mathrm{Elim}_{x_k}(\mathcal{P})$ شامل همه $\mathrm{SRC}_j(R,\partial R/\partial x_k)$ است که در R نیستند و $j=0,\dots,\deg_{x_k}(R)-2$.

(۲) اگر $R,S\in\mathrm{Tru}(\mathcal{P})$،

(i) اگر $\deg_{x_k}(R)>\deg_{x_k}(S)$، $\mathrm{Elim}_{x_k}(\mathcal{P})$ شامل همه $\mathrm{SRC}_j(R,S)$ است که در R وجود ندارند و $j=0,\dots,\deg_{x_k}(S)-1$،

(ii) اگر $\deg_{x_k}(R)<\deg_{x_k}(S)$، $\mathrm{Elim}_{x_k}(\mathcal{P})$ شامل همه $\mathrm{SRC}_j(S,R)$ است که در R وجود ندارند و $j=0,\dots,\deg_{x_k}(R)-1$،

(iii) اگر $\deg_{x_k}(R)=\deg_{x_k}(S)$، $\mathrm{Elim}_{x_k}(\mathcal{P})$ شامل همه $\mathrm{SRC}_j(S,\overline{R})$ است که $\overline{R}=\mathrm{LC}(S)R-\mathrm{LC}(R)S$ در R نیستند و $j=0,\dots,\deg_{x_k}(\overline{R})-1$.

(۳) اگر $R\in\mathrm{Tru}(\mathcal{P})$ و $\mathrm{LC}(R)$ در R نباشد، $\mathrm{Elim}_{x_k}(\mathcal{P})$ شامل $\mathrm{LC}(R)$ است.

قضیه ۴-۸۲. فرض کنید $\mathcal{P}$ یک زیرمجموعه از $\mathbb{R}[x_1,\ldots,x_n]$ و S یک زیرمجموعه نیمه‌جبری همبند از $\mathbb{R}^{k-1}$ باشد که $\mathrm{Elim}_{x_k}(\mathcal{P})$-پایا است. در این صورت، توابع نیمه‌جبری $f_1 < \ldots < f_l : S \longrightarrow R$ وجود دارند به طوری که برای هر $x' \in S$، $\{f_1(x'),\ldots,f_l(x')\}$ مجموعه تمام ریشه‌های حقیقی همه چندجمله‌ای‌های ناصفر $P(x',x_k)$ است که $P \in \mathcal{P}$. نمودار هر f_i یک مجموعه نیمه‌جبری همبند هم‌ریخت با S و در نتیجه $\mathcal{P}$-پایا است.

اثبات. برای $P \in \mathcal{P}$، $R \in \mathrm{Tru}(P)$، مجموعه ساختنی $A \subset \mathbb{R}^{k-1}$ تعریف شده توسط $\mathrm{LC}(R) \neq 0$ و $\deg(P) = \deg(R)$ را در نظر بگیرید. برای هر $a' \in A$، صفر شدن یا نشدن $\mathrm{SRC}_j(R, \partial R/\partial x_k)(a')$ تعیین کننده تعداد ریشه‌های متمایز $P(a',x_k)$ در C است؛ یعنی

$$\deg(R(a',x_k)) - \deg(\gcd(R(a',x_k), \partial R/\partial x_k(a',x_k))).$$

به طور مشابه، برای $R \in \mathrm{Tru}(P)$، $S \in \mathrm{Tru}(Q)$، مجموعه ساختنی B را تعریف شده توسط

$$\mathrm{LC}(R) \neq 0, \deg(P) = \deg(R), \mathrm{LC}(S) \neq 0, \deg(Q) = \deg(S)$$

در نظر بگیرید. به ازای هر $a' \in B$، که $\mathrm{SRC}_j(R,S)(a')$ صفر می‌شود، $\deg(\gcd(R(a',x_k), Q(a',x_k)))$ را می‌توان تعیین کرد. بنابراین، این فرض که یک زیرمجموعه نیمه‌جبری همبند از $\mathbb{R}^{k-1}$، $\mathrm{Elim}_{x_k}(\mathcal{P})$-پایا است، نتیجه می‌شود که فرض گزاره ۶-۱۶ برقرار و در نتیجه حکم مورد نظر اثبات می‌شود. □

حال قضیه بسیار مهم زیر را بیان و اثبات می‌کنیم که وجود یک تجزیه $(\mathcal{P})$-پایا را تضمین می‌کند.

قضیه ۴-۸۳ (تجزیه استوانه‌ای). برای هر خانواده متناهی از چندجمله‌ای‌های $P_1,\ldots,P_r$ در $\mathbb{R}[x_1,\ldots,x_n]$، یک تجزیه جبری استوانه‌ای از $\mathbb{R}^n$ سازگار با $(P_1,\ldots,P_r)$ وجود دارد.

اثبات. این قضیه را با استقرا با روی بُعد فضای محدود شده اثبات می‌کنیم. فرض کنید $\mathcal{Q} \subset \mathbb{R}[x_1]$ متناهی باشد. به سادگی قابل مشاهده است که یک تجزیه جبری استوانه‌ای از $\mathbb{R}$ سازگار با $\mathcal{Q}$ وجود ندارد؛ چون ریشه‌های حقیقی چندجمله‌ای‌های موجود در $\mathcal{Q}$ خط را به تعداد متناهی از نقاط و بازه‌ها تجزیه می‌کنند که باعث به وجود آمدن سلول‌های یک تجزیه جبری استوانه‌ای از $\mathbb{R}$ سازگار با $\mathcal{Q}$ می‌شود.
فرض کنید $\mathcal{Q} \subset \mathbb{R}[x_1,\ldots,x_i]$ متناهی باشد. یک تجزیه جبری استوانه‌ای از $\mathbb{R}^{i-1}$ سازگار با $\mathrm{Elim}_{x_i}(\mathcal{Q})$ را به سلول‌های تجزیه جبری استوانه‌ای قضیه ۶-۱۹ نظیر کنید. در نتیجه یک تجزیه استوانه‌ای از $\mathbb{R}^i$ سازگار با $\mathcal{Q}$ ساخته می‌شود. □

مثال ۴-۸۴. قضیه بالا را با یک تجزیه استوانه‌ای از $\mathbb{R}^3$ سازگار با چندجمله‌ای $P = x_1^2 + x_2^2 + x_3^2 - 1$. حال، 0-امین ماتریس سیلوستر P و $\partial P/\partial x_3$ برابر است با

$$\begin{pmatrix} 1 & 0 & x_1^2 + x_2^2 - 1 \\ 0 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}.$$

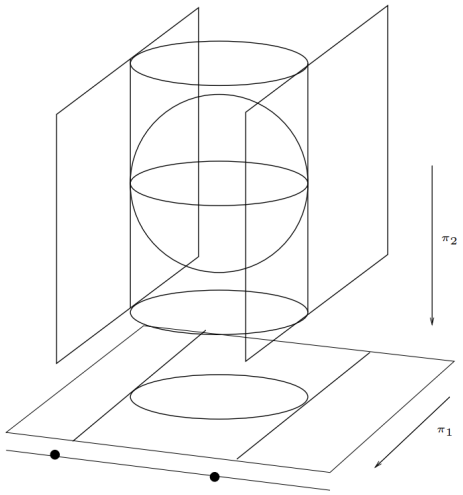
بنابراین، $\mathrm{SRC}_{\circ}(P, \partial P/\partial x_{۳}) = -۴(x_{۱}^{۲} + x_{۲}^{۲} - ۱)$ و $\mathrm{SRC}_{۱}(\partial P/\partial x_{۳}) = ۲$. با صرف نظر کردن از عامل‌های بی‌ربط داریم:

$$\mathrm{Elim}_{x_{۳}}(P) = \{x_{۱}^{۲} + x_{۲}^{۲} - ۱\}.$$

به طور مشابه،

$$\mathrm{Elim}_{x_{۲}}(\mathrm{Elim}_{x_{۳}}(P)) = \{x_{۱}^{۲} - ۱\}.$$

شکل ۱-۴: تجزیه جبری استوانه‌ای



فرض کنید S یک سلول در سطح i از یک تجزیه استوانه‌ای $\mathcal{S}$ باشد و $x \in S$. تصویر $\mathbb{R}^k$ به R^i را با نماد π_i نشان می‌دهیم. تفکیک متناهی از $\mathbb{R}^{k-i}$ که با اشتراک سلول‌های $\mathcal{S}_{i+j}$ بالای S همراه با $\pi_i^{-۱}(x)$ بدست می‌آید، یک تجزیه استوانه‌ای از $\mathbb{R}^{k-i}$ تشکیل می‌دهد.

$$\begin{cases} S_{۱} & = (-\infty, -۱) \\ S_{۲} & = \{-۱\} \\ S_{۳} & = (-۱, ۱) \\ S_{۴} & = \{۱\} \\ S_{۵} & = (۱, \infty) \end{cases}$$

بالای S_i برای $i = ۱, ۵$، هیچ توابع نیمه‌جبری وجود ندارند و فقط یک سلول $S_{i,۱} = S_i \times \mathbb{R}$ قرار دارد. بالای S_i برای

$i = ۲, ۴$ فقط یک تابع نیمه‌جبری نظیر -۱ و ۱ با مقدار ثابت ۰ وجود دارد و سه سلول قرار دارند:

$$\begin{cases} S_{i,۱} &= S_i \times (-\infty, ۰) \\ S_{i,۲} &= S_i \times ۰ \\ S_{i,۳} &= S_i \times (۰, \infty) \end{cases}$$

بالای $S_۳$ دو تابع نیمه‌جبری $f_{۳,۱}$ و $f_{۳,۲}$ نظیر $x \in S_۳$ با مقادیر $f_{۳,۱}(x) = -\sqrt{۱ - x^۲}$ و $f_{۳,۲}(x) = \sqrt{۱ - x^۲}$ وجود دارند. پنج سلول بالای $S_۳$ وجود دارند که نمودارهای $f_{۳,۱}$ و $f_{۳,۲}$ نوارهایشان به صورت

$$\begin{cases} S_{۳,۱} &= \{(x,y) \mid -۱ < x < ۱, y < f_{۳,۱}(x)\} \\ S_{۳,۲} &= \{(x,y) \mid -۱ < x < ۱, y = f_{۳,۱}(x)\} \\ S_{۳,۳} &= \{(x,y) \mid -۱ < x < ۱, f_{۳,۱}(x) < y < f_{۳,۲}(x)\} \\ S_{۳,۴} &= \{(x,y) \mid -۱ < x < ۱, y = f_{۳,۲}(x)\} \\ S_{۳,۵} &= \{(x,y) \mid -۱ < x < ۱, f_{۳,۲}(x) < y\}. \end{cases}$$

بالای $S_{i,j}$، $(i,j) \in \{(۱,۱), (۲,۱), (۲,۳), (۳,۱), (۳,۵), (۴,۱), (۴,۳), (۵,۱)\}$، هیچ تابع نیمه‌جبری وجود نداشته و فقط یک سلول وجود دارد:

$$S_{i,j,۱} = S_{i,j} \times \mathbb{R}$$

بالای $S_{i,j}$، $(i,j) \in \{(۲,۲), (۳,۲), (۳,۴), (۴,۲)\}$، فقط یک تابع نیمه‌جبری، تابع ثابت صفر و سه سلول

$$\begin{aligned} S_{i,j,۱} &= S_{i,j} \times (-\infty, ۰) \\ S_{i,j,۲} &= S_{i,j} \times \{۰\} \\ S_{i,j,۳} &= S_{i,j} \times (۰, \infty) \end{aligned}$$

وجود دارند. بالای $S_{۳,۳}$ فقط دو تابع نیمه‌جبری $f_{۳,۳,۱}$ و $f_{۳,۳,۲}$ نظیر $(x,y) \in S_{۳,۳}$ با مقادیر

$$\begin{aligned} f_{۳,۳,۱}(x,y) &= -\sqrt{۱ - x^۲ - y^۲} \\ f_{۳,۳,۲}(x,y) &= \sqrt{۱ - x^۲ - y^۲}, \end{aligned}$$

و پنج سلول

$$\begin{cases} S_{۳,۳,۱} &= \{(x,y,z) \mid (x,y) \in S_{۳,۳}, z < f_{۳,۳,۱}(x,y)\} \\ S_{۳,۳,۲} &= \{(x,y,z) \mid (x,y) \in S_{۳,۳}, z = f_{۳,۳,۱}(x,y)\} \\ S_{۳,۳,۳} &= \{(x,y,z) \mid (x,y) \in S_{۳,۳}, f_{۳,۳,۱}(x,y) < z < f_{۳,۳,۲}(x,y)\} \\ S_{۳,۳,۴} &= \{(x,y,z) \mid (x,y) \in S_{۳,۳}, z = f_{۳,۳,۲}(x,y)\} \\ S_{۳,۳,۵} &= \{(x,y,z) \mid (x,y) \in S_{۳,۳}, f_{۳,۳,۲}(x,y) < z\} \end{cases}$$

وجود دارند.

قضیه ۸۵-۴. هر زیرمجموعه نیمه‌جبری S از $\mathbb{R}^k$، اجتماعی متمایز از تعداد متناهی مجموعه‌های نیمه‌جبری است که هرکدام از آن‌ها، به طور نیمه‌جبری با یک iـ مکعب باز $(۰,۱)^i \subset \mathbb{R}^i$ یک‌ریخت توپولوژیک است *(برای $i \geq k$)*.

اثبات. می‌دانیم که یک تجزیه استوانه‌ای سازگار با S وجود دارد. از آن‌جایی که این سلول‌ها برای $i \geq k$ با یک iـ مکعب باز $(۰,۱)^i \subset \mathbb{R}^i$ یک‌ریخت توپولوژیک است، حکم مورد نظر برقرار می‌شود. □

گزاره زیر به راحتی از قضیه بالا نتیجه می‌شود.

گزاره ۸۶-۴. فرض کنید S یک مجموعه نیمه‌جبری و $f : S \longrightarrow \mathbb{R}^k$ یک تابع نیمه‌جبری باشد. در این صورت، یک تفکیک متناهی از S به مجموعه‌های نیمه‌جبری مانند $S_۱, \ldots, S_n$ وجود دارد به طوری که تحدید f به S_i، که آن را با f_i نمایش می‌دهیم، نیمه‌جبری و پیوسته است.

اثبات. بنابر قضیه ۲۲-۶، نمودار G از f اجتماع iـ مکعب‌هایی از بُعدهای متفاوت است، که به طور واضح نمودارهای توابع پیوسته نیمه‌جبری هستند. □

۶.۴ الگوریتم تجزیه جبری استوانه‌ای

در این بخش، با استفاده از مطالب بخش‌های قبل الگوریتم بازگشتی تجزیه استوانه‌ای را در سه مرحله بیان می‌کنیم.

تعریف ۸۷-۴. فرض کنید $P_۱, \ldots, P_r \in \mathbb{R}[x_۱, \ldots, x_n]$. مجموعه $\mathrm{Proj}(P_۱, \ldots, P_r)$ را کوچک‌ترین خانواده از چندجمله‌ای‌ها در $\mathbb{R}[x_۱, \ldots, x_{n-۱}]$ تعریف می‌کنیم که در شرایط زیر صدق کند:
(۱) اگر $\deg_{x_n}(P_i) = d > ۱$، آنگاه $\mathrm{Proj}(P_۱, \ldots, P_i, \ldots, P_r)$ شامل همه چندجمله‌ای‌های غیرثابت

$$\mathrm{SRC}_j(P_i, \partial P_i/\partial x_n)$$

برای $j = ۰, \ldots, d-۱$ است.

(۲) اگر $۱ \leq d = \min(\deg_{x_n}(P_i), \deg_{x_n}(P_k))$، آنگاه $\mathrm{Proj}(P_۱, \ldots, P_i, \ldots, P_k, \ldots, P_r)$ شامل همه غیرثابت‌های $\mathrm{SRC}_j(P_i, P_k)$ برای $j = ۰, \ldots, d-۱$ است.

(۳) اگر $\deg_{x_n}(P_i) \geq ۱$ و $\mathrm{LC}(P_i)$ غیرثابت باشد، آنگاه $\mathrm{Proj}(P_۱, \ldots, P_i, \ldots, P_r)$ شامل $\mathrm{LC}(P_i)$ و

$$\mathrm{Proj}(P_۱, \ldots, \mathrm{tail}(P_i), \ldots, P_r)$$

است.

(۴) اگر $\deg_{x_n}(P_i) = ۰$ و P_i غیرثابت باشد، آنگاه $\mathrm{Proj}(P_۱, \ldots, P_i, \ldots, P_r)$ شامل P_i است.

اگر یک تجزیه جبری استوانه‌ای از $\mathbb{R}^{n-۱}$، سازگار با $\mathrm{Proj}(P_۱, \ldots, P_r)$ داشته باشیم، قضیه ۱۹-۶ می‌تواند برای تعمیم این تجزیه به یک تجزیه جبری استوانه‌ای از $\mathbb{R}^n$، سازگار با $\mathrm{Proj}(P_۱, \ldots, P_r)$ استفاده شود. به عبارت دیگر، با $n-۱$ بار تکرار عملگر Proj، در نهایت به یک خانواده از چندجمله‌ای‌های تک‌متغیره نسبت به متغیر $x_۱$ می‌رسیم. ساختن یک تجزیه جبری استوانه‌ای از $\mathbb{R}$، سازگار با این خانواده ساده است؛ زیرا ریشه‌های حقیقی چندجمله‌ای‌های این خانواده، خط حقیقی را در تعداد متناهی نقطه و بازه باز قطع می‌کند.

نمادگذاری ۸۸-۴. فرض کنید $F = \{f_۱, \ldots, f_r\} \subset \mathbb{R}[x_۱, \ldots, x_n]$ یک خانواده از چندجمله‌ای‌ها باشد. در این صورت $\mathrm{Proj}^۰(F) = F$ و برای $۱ \leq i \leq n-۱$ داریم $\mathrm{Proj}^i(F) = \mathrm{Proj}(\mathrm{Proj}^{i-۱}(F))$.

منظور از نقاط نمونه در الگوریتم زیر، انتخاب یک نقطه دلخواه از هر سلول در هر سطح است. از آن‌جایی که رفتار چندجمله‌ای‌های مورد بررسی در هر سلول پایا است، پس با انتخاب یک نقطه نمونه از هر سلول می‌توان علامت هر یک از این چندجمله‌ای‌ها را در آن سلول مشخص کرد. برای تعیین نقطه نمونه سلول‌های در سطح یک، به صورت زیر عمل می‌کنیم. اگر سلول تک‌نقطه‌ای باشد، نقطه نمونه را همان سلول در نظر می‌گیریم و اگر سلول یک بازه باز باشد، معمولاً نقطه میانی را به عنوان نقطه نمونه انتخاب می‌کنیم.

اکنون، سه مراحل ذکر شده در الگوریتم را توصیف می‌کنیم.

مرحله تصویر: در این مرحله عملگر Proj را $n-۱$ بار به طور بازگشتی به کار می‌بریم و به n خانواده از چندجمله‌ای‌ها می‌رسیم. در هر زیرمرحله چندجمله‌ای‌های بدست آمده، یک متغیر کمتر نسبت به زیرمرحله قبل از خود دارند. به این ترتیب به خانواده‌ای از چندجمله‌ای‌های تک‌متغیره می‌رسیم که یافتن ریشه‌های آن با استفاده از روش‌های حل چندجمله‌ای‌های تک‌متغیره امکان پذیر است.

مرحله پایه: در این مرحله، ریشه‌های حقیقی خانواده چندجمله‌ای‌های تک‌متغیره $\mathrm{Proj}^{n-۱}(F)$ را محاسبه می‌کنیم. فرض کنید $a_۱ < \ldots < a_k$ ریشه‌های حقیقی این خانواده باشد. در این صورت سلول‌های تجزیه جبری استوانه‌ای از $\mathbb{R}$ عبارت است از $(-\infty, a_۱), a_۱, (a_۱, a_۲), a_۲, \ldots, (a_{k-۱}, a_k), a_k, (a_k, \infty)$. نقاط نمونه عبارتند از

$$b_۱ < a_۱ < b_۲ < a_۲ < \ldots < b_k < a_k < b_{k+۱}$$

Procedure 17 Cylindrical Algebraic Decomposition

Input: $F = \{f_1, \ldots, f_r\} \subset \mathbb{R}[x_1, \ldots, x_n]$

Output: An F-invariant C.A.D of $\mathbb{R}^n$

- **Projection**:

$$\begin{aligned} \mathrm{Proj}^0(F) &\subset \mathbb{R}[x_1, \ldots, x_n] \\ \mathrm{Proj}^1(F) &\subset \mathbb{R}[x_1, \ldots, x_{n-1}] \\ &\vdots \\ \mathrm{Proj}^{n-1}(F) &\subset \mathbb{R}[x_1] \end{aligned}$$

- **Base**: Compute the real roots of the polynomials of $\mathrm{Proj}^{n-1}(F) \subset \mathbb{R}[x_1]$ and then determine the cells of level 1 and the sample points in $\mathbb{R}$.
- **Extension**: Find the sample points of $\mathbb{R}^k$ and the cells of level $k = 2, \ldots, n$.

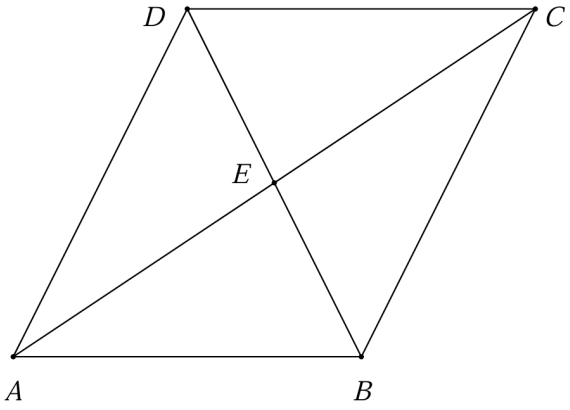
که برای $2 \leq i \leq k$، b_i به طور معمول نقاط میانی بازه (a_{i-1}, a_i) و $b_1 = a_1 - 1$ و $b_{k+1} = a_k + 1$ به عنوان نقاط نمونه انتخاب می‌شوند. توجه داشته باشید که هر نقطه دلخواه از یک سلول را می‌توان به عنوان یک نقطه نمونه انتخاب کرد.

مرحله توسیع: مرحله بازگشت در این مرحله صورت می‌گیرد. در مرحله‌های قبلی از یک خانواده از چندجمله‌ای‌های n متغیره شروع کردیم و به چندجمله‌ای‌های تک‌متغیره و سپس به تجزیه جبری استوانه‌ای از $\mathbb{R}$ و در نهایت به نقاط نمونه این تجزیه رسیدیم. در این مرحله از این نقاط شروع کرده و به تجزیه جبری استوانه‌ای از $\mathbb{R}^n$ می‌رسیم. به این ترتیب که ابتدا نقاط نمونه را در چندجمله‌ای‌های $\mathrm{Proj}^{n-2}(F)$ قرار می‌دهیم تا به یک خانواده از چندجمله‌ای‌های تک‌متغیره برحسب x_2 برسیم. مشابه مرحله پایه، این چندجمله‌ای‌ها را نسبت به x_2 حل کرده و بازه‌ها و نقاط نمونه محور x_2 را مشخص می‌کنیم. در نهایت، با استفاده از این بازه‌ها، سلول‌های تجزیه جبری استوانه‌ای از $\mathbb{R}^2$ که به صورت نقاط و گوی‌های باز هستند را تعیین و نقاط نمونه را انتخاب می‌کنیم. به همین ترتیب تجزیه جبری استوانه‌ای از $\mathbb{R}^i$ برای $i > 2$ را محاسبه کرده تا به تجزیه جبری استوانه‌ای از $\mathbb{R}^n$ برسیم که خروجی الگوریتم است.

۱.۶.۴ اثبات قضایای هندسی

در این زیربخش با استفاده از تجزیه جبری استوانه‌ای برای حذف سور حقیقی، یکی از قضایای هندسه اقلیدسی را به عنوان مثال، اثبات می‌کنیم.

مثال ۸۹-۴ (قطرهای متوازی‌الاضلاع). فرض کنید $ABCD$ یک متوازی‌الاضلاع و E نقطه برخورد قطرهای آن باشد. در این صورت، E وسط هر دو قطر است.



به زبان جبری، دو نوع متغیر را از هم متمایز می‌کنیم: از یک سو پارامترها را داریم که مختصاتی را توصیف می‌کنند که می‌توانند به طور دلخواه انتخاب شوند. از سوی دیگر متغیرهای وابسته را داریم که مختصاتی را توصیف می‌کنند که به طور یکتا توسط پارامترها تعیین می‌شوند.

پارامترها را با $u_1, \dots, u_m$ و متغیرهای وابسته را با $x_1, \dots, x_n$ نشان می‌دهیم. در این مثال، بدون کاسته شدن از کلیت، پارامترهای زیر را معرفی می‌کنیم:

$$A = (0, 0), \quad B = (u_1, 0), \quad C = (u_2, u_3).$$

برای هر انتخاب u_1, u_2, u_3، مختصات D و E اکنون به طور یکتا تعیین می‌شوند. از متغیرهای وابسته برای مختصات آن‌ها استفاده می‌کنیم:

$$D = (x_1, x_2), \quad E = (x_3, x_4).$$

با استفاده از این مختصات، اکنون می‌توانیم فرض را بازگو: برای اینکه $ABCD$ یک متوازی‌الاضلاع باشد، لازم است که $x_1 = u_2 - u_1$ و $x_2 = u_3$. نقطه E برخورد قطرهای AC و BD است اگر و تنها اگر روی هر دوی این قطرها قرار گرفته باشد. این به نوبه خود درست است اگر و تنها اگر خطوط AE و AC و خطوط BE و BD یکسان باشند. یکسانی خطوط با یک نقطه مشترک را می‌توان بر حسب شیب آن‌ها بیان کرد:

$$\frac{x_4}{x_3} = \frac{u_3}{u_2}, \quad \frac{x_4}{x_3 - u_1} = \frac{x_2}{x_1 - u_1}.$$

با ساده‌کردن مخرج‌ها، این به ترتیب معادل معادلات چندجمله‌ای $x_4 u_2 = u_3 x_3$ و $x_4(x_1 - u_1) = x_2(x_3 - u_1)$ است. نتیجه قضیه این است که E وسط هر دو قطر AC و BD است؛ یعنی

$$\sqrt{x_3^2 + x_4^2} = \frac{\sqrt{u_2^2 + u_3^2}}{2} \quad \text{و} \quad \sqrt{(x_3 - u_1)^2 + x_4^2} = \frac{\sqrt{(x_1 - u_1)^2 + x_2^2}}{2}.$$

این معادلات با چندجمله‌ای‌های به صورت زیر بازنویسی می‌شوند:

$$۴x_۳^۲ + ۴x_۴^۲ = u_۲^۲ + u_۳^۲ \quad و \quad ۴(x_۳ - u_۱)^۲ + ۴x_۴^۲ = (x_۱ - u_۱)^۲ + x_۲^۲.$$

در تمام معادلات چندجمله‌ای به دست آمده تا اینجا، طرف راست را از طرف چپ متناظر کم می‌کنیم و چندجمله‌ای‌های زیر را برای فرض‌ها و نتیجه‌ها به دست می‌آوریم:

$$\begin{aligned}
h_۱(\mathbf{u},\mathbf{x}) &= x_۱ + u_۱ - u_۲,\\
h_۲(\mathbf{u},\mathbf{x}) &= x_۲ - u_۳,\\
h_۳(\mathbf{u},\mathbf{x}) &= u_۲x_۴ - u_۳x_۳,\\
h_۴(\mathbf{u},\mathbf{x}) &= x_۴(x_۱ - u_۱) - x_۲(x_۳ - u_۱),\\
c_۱(\mathbf{u},\mathbf{x}) &= ۴x_۳^۲ + ۴x_۴^۲ - u_۲^۲ - u_۳^۲,\\
c_۲(\mathbf{u},\mathbf{x}) &= ۴(x_۳ - u_۱)^۲ + ۴x_۴^۲ - (x_۱ - u_۱)^۲ - x_۲^۲.
\end{aligned}$$

اثبات‌کننده‌های خودکار اکنون سعی می‌کنند اعتبار عمومی[۷] گزاره زیر را روی $\mathbb{R}$ یا $\mathbb{C}$ اثبات کنند:

$$\forall\mathbf{u}\forall\mathbf{x}\Big(\big(\bigwedge_{i=۱}^{۴} h_i(\mathbf{u},\mathbf{x}) = ۰\big) \longrightarrow \big(c_۱(\mathbf{u},\mathbf{x}) = ۰ \wedge c_۲(\mathbf{u},\mathbf{x}) = ۰\big)\Big).$$

اعتبار عمومی به معنای اعتبار تحت برخی شرایط فرعی است که باید توسط اثبات‌کننده خودکار کشف شوند. از مدل‌سازی ما باید روشن باشد که شرایط غیرانحطاطی به درستی بیان شده، پارامترهای $u_۱, \ldots, u_۳$ را درگیر می‌کنند و نه متغیرهای وابسته $x_۱, \ldots, x_۴$ را.

توجه کنید که در مرحله مدل‌سازی، مقدار معینی از دانش هندسی وارد می‌شود: برای مثال، فرمول‌بندی ما برای طول پاره‌خط‌های اقلیدسی نیازمند آگاهی از قضیه فیثاغورس است. تلاش برای اثبات قضیه فیثاغورس با چنین مدل‌سازی‌ای به یک فرمول‌بندی جبری بدیهی منجر خواهد شد. به طور کلی، باید در انجام بخش‌های مرتبط از اثبات در مرحله ترجمه بسیار دقت کرد. کوتزلر در رساله دکتری خود به این مسئله پرداخته است. به دنبال هیلبرت، او انواع مفاهیم پایه‌ای نقطه و خط را معرفی می‌کند و سپس مجموعه‌ای محدود از گزاره‌ها مانند موازی یا نقطه وسط را روی این انواع تعریف می‌کند. چاو[۸] از ترجمه جبری زیر برای این حدس استفاده می‌کند: نقاط دارای مختصات

$$A = (۰, ۰), \quad B = (u_۱, ۰), \quad C = (u_۲, u_۳), \quad D = (x_۲, x_۱), \quad E = (x_۴, x_۳)$$

[۷] Generic Validity

[۸] Chou

و فرض‌های $h_۱, \ldots, h_۴$ و نتیجه g به صورت زیر هستند:

$$\begin{aligned}
h_۱ &\equiv u_۱x_۱ - u_۱u_۳ = ۰ && AB \parallel DC\\
h_۲ &\equiv u_۳x_۲ - (u_۲ - u_۱)x_۱ = ۰ && DA \parallel CB\\
h_۳ &\equiv x_۱x_۴ - (x_۲ - u_۱)x_۳ - u_۱x_۱ = ۰ && E \in BD\\
h_۴ &\equiv u_۳x_۴ - u_۲x_۳ = ۰ && E \in AC\\
g &\equiv ۲u_۲x_۴ + ۲u_۳x_۳ - u_۳^۲ - u_۲^۲ = ۰ && AE \equiv CE.
\end{aligned}$$

با ورودی $\varphi \equiv \forall x_۱\forall x_۲\forall x_۳\forall x_۴(h_۱ \wedge h_۲ \wedge h_۳ \wedge h_۴ \longrightarrow g)$، پس از ۴۰ میلی‌ثانیه، با حذف سور عمومی نتیجه حذفی $\varphi' \equiv$ درست به همراه شرایط غیرانحطاط $\vartheta' \equiv u_۱ \neq ۰ \wedge u_۳ \neq ۰$ را به دست می‌آوریم که بیان می‌کند $ABCD$ یک متوازی‌الاضلاع است.

چاو علاوه بر این، یک شرط اضافی $u_۳x_۲ - u_۲x_۱ - u_۱u_۳ \neq ۰$ به دست می‌آورد. این شرط بیان می‌کند که قطرها شیب‌های متفاوتی دارند، که در هر متوازی‌الاضلاعی به طور بدیهی برقرار است. به طور دقیق‌تر، همیشه داریم $\nabla AC = -\nabla BD$.

نرم‌افزار REDLOG پس از ۲۰۰ میلی‌ثانیه برای حذف سور و سپس ساده‌سازی گربنر، فرمولی بدون سور معادل زیر را به دست می‌آورد:

$$\varphi' \equiv (u_۲ = ۰ \vee u_۳ \neq ۰) \wedge (u_۱ \neq ۰ \vee u_۳ = ۰).$$

کتاب‌نامه

[1] Atiyah, M. F.; Macdonald, I. G., ”Introduction to Commutative Algebra”. Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Company, Reading, Massachusetts, 1969.

[2] Basu, Saugata; Pollack, Richard; Roy, Marie-Françoise., ”Algorithms in Real Algebraic Geometry.” 2nd ed. Algorithms and Computation in Mathematics, vol. 10. Springer, Berlin, Heidelberg, 2006.

[3] Coste M., ”An Introduction to Semialgebraic Geometry”. Preprint, Institut de Recherche Mathématique de Rennes, 2002.

[4] Cox, David A.; Little, John; O'Shea, Donal., ”Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.” 2nd ed. Undergraduate Texts in Mathematics. Springer, New York, 1997..

[5] Cox, David A.; Little, John; O'Shea, Donal., ”Using Algebraic Geometry.” 2nd ed. Grad. Texts in Math., vol. 185. Springer, New York, 2005.

[6] Dolzmann, Andreas; Sturm, Thomas; Weispfenning, Volker., ”Real Quantifier Elimination in Practice” In: Algorithmic Algebra and Number Theory (Matzat, B. H., Greuel, G.-M., and Hiss, G., eds.). Springer, Berlin, Heidelberg, 1999, pp. 221–247.

[7] Ferretti, Andrea., ”Commutative Algebra.” Graduate Stud. Math., vol. 233. American Mathematical Society, Providence, RI, 2023.

[8] Fried, Michael D.; Jarden, Moshe., ”Field Arithmetic.” 4th ed. Ergeb. Math. Grenzgeb. (3), vol. 11. Springer, Cham, 2023.

[9] Marker, David., ”Model Theory: An Introduction”. Graduate Texts in Mathematics, vol. 217. Springer-Verlag, New York, 2006. Corrected second printing of the 2002 original.

[10] Marker, David., ”An Invitation to Mathematical Logic”. Graduate Texts in Mathematics, vol. 301. Springer, Cham, 2024.

[11] Scheiderer, Claus., ”A Course in Real Algebraic Geometry: Positivity and Sums of Squares.” Grad. Texts in Math., vol. 303. Springer, Cham, 2024.

[12] Sturm, Thomas., ”A Survey of Some Methods for Real Quantifier Elimination, Decision, and Satisfiability and Their Applications.” Math. Comput. Sci. 11, no. 3 (2017): 483–502.

[13] Tent, Katrin; Ziegler, Martin., ”A Course in Model Theory”. Lecture Notes in Logic, vol. 40. Cambridge University Press, Cambridge, 2012.

[14] Theobald, Thorsten., ”Real Algebraic Geometry and Optimization.” Graduate Stud. Math., vol. 241. American Mathematical Society, Providence, RI, 2024. MSC: Primary 14, 90, 68, 12, 52.