پایه گربنر
و کاربردهای آن

گردآوری و تدوین

امیر هاشمی

دانشیار دانشکده علوم ریاضی
دانشگاه صنعتی اصفهان

انتشارات دانشگاه صنعتی اصفهان

شماره کتاب ۱۸۴ گروه علوم ۴۶

پایه گربنر و کاربردهای آن

گردآوری و تدوین:	دکتر امیر هاشمی
صفحه آرا:	فرزاد میرزاوند
طراح جلد:	مرضیه خردمند
ناشر:	انتشارات دانشگاه صنعتی اصفهان
لیتوگرافی، چاپ و صحافی:	چاپخانه دانشگاه صنعتی اصفهان
چاپ اول:	بهار ۱۴۰۲
شمارگان:	۲۰۰ جلد
شابک:	۹۷۸-۶۰۰-۸۲۵۷-۶۱-۵
قیمت:	۱۳۰۰۰۰۰ ریال

سرشناسه	: هاشمی، امیر، ۱۳۵۴، گردآورنده
عنوان و نام پدیدآور	: پایه گربنر و کاربردهای آن/ گردآوری و تدوین امیر هاشمی.
مشخصات نشر	: اصفهان: دانشگاه صنعتی اصفهان، انتشارات، ۱۴۰۱.
مشخصات ظاهری	: ۲۹۳ ص.
فروست	: انتشارات دانشگاه صنعتی اصفهان؛ ۱۸۴. گروه علوم؛ ۴۶.
شابک	: ۹۷۸-۶۰۰-۸۲۵۷-۶۱-۵
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: ص. ع. به انگلیسی: A.Hashemi.Gröbner basis and its applications.
یادداشت	: واژه‌نامه
یادداشت	: کتابنامه:ص.[۲۷۵]-۲۷۷.
موضوع	: پایه‌های گروبنر Gröbner bases
	جبر تعویض‌پذیر - داده‌پردازی Commutative algebra - Data processing
شناسه افزوده	: دانشگاه صنعتی اصفهان. انتشارات
رده‌بندی کنگره	: QA۲۵۱ /۳
رده‌بندی دیویی	: ۵۱۲/۲۴
شماره کتابشناسی ملی	: ۹۱۳۸۳۴۰

اصفهان: دانشگاه صنعتی اصفهان - انتشارات- کدپستی ۸۴۱۵۶-۸۳۱۱۱، تلفن: ۳۳۹۱۲۹۵۲ (۰۳۱) دورنگار: ۳۳۹۱۲۵۵۲ برای خرید اینترنتی کلیه کتاب‌های منتشره انتشارات می‌توانید به وبگاه http://publication.iut.ac.ir مراجعه و یا مستقیما از کتابفروشی انتشارات واقع در کتابخانه مرکزی دانشگاه صنعتی اصفهان (تلفن ۳۳۹۱۳۹۵۲) خریداری فرمائید.

پیشگفتار

در دنیای صنعتی امروز، ریاضیات نقش مهم و بسزایی دارد و با پیشرفت صنعت، نیاز به ریاضیات بیش از پیش احساس می‌شود. برخی از مسائل صنعتی، با استفاده از چندجمله‌ای‌ها مدل‌سازی می‌شوند و در نتیجه، حل و تحلیل دستگاه‌های معادلات چندجمله‌ای را می‌توان به عنوان هسته اصلی برخی از مسائل در مهندسی و محاسبات علمی دانست. ساده‌ترین نوع این دستگاه‌ها، دستگاه‌های معادلات خطی هستند که به دلیل اهمیت آن‌ها، ابزاری به نام جبرخطی برای حل این معادلات در ریاضیات پدید آمد که از پیشرفت قابل ملاحظه‌ای از دیدگاه نظری و عملی برخوردار بوده است. اگر بخواهیم یک قدم فراتر از دستگاه‌های معادلات خطی پیش برویم، به دستگاه‌های غیرخطی برمی‌خوریم که در بسیاری از زمینه‌های مهندسی و علوم مانند بیولوژی، شیمی، کدگشایی، رباتیک، برنامه‌ریزی خطی، معادلات دیفرانسیل با مشتقات جزئی و غیره کاربرد فراوان دارد. از طرفی، گاهی یافتن ریشه‌های دقیق یک دستگاه معادلات چندجمله‌ای مورد نظر است و در نتیجه به روش‌های نمادین برای یافتن ریشه‌های دقیق یک دستگاه معادلات نیاز داریم. این روش‌ها تا اواسط قرن نوزدهم مورد استقبال قرار نگرفت تا این که پیشرفت‌های چشمگیر در عرصه الکترونیک و علوم کامپیوتر باعث شد علایق جدیدی در زمینه ساختارهای محاسباتی در جبر مطرح شود. تلاش‌های ریاضی‌دانان در این زمینه منجر به ظهور شاخه جدیدی در ریاضیات به نام جبر محاسباتی [1] شد که ریشه‌های آن در ریاضیات و علوم کامپیوتر است. جبر محاسباتی یکی از شاخه‌های به نسبت نوین ریاضیات است که یکی از اهداف آن، حل و تحلیل دستگاه‌های معادلات چندجمله‌ای بر اساس ابزارهای جبری و با استفاده از روش‌های الگوریتمیک به منظور بهرمندی از کامپیوتر است. دو واژه کلیدی در این شاخه، جبر و الگوریتم است که ریشه آن به کتاب و نام ریاضی‌دان ایرانی خوارزمی [2]

---

[1] با توجه به این که ریاضیاتی که در جبر کامپیوتری مورد استفاده قرار می‌گیرد متفاوت از کارهای معمول در جبر مجرد است، متأسفانه این بخش جذاب و کاربردی ریاضیات هنوز جایگاه مناسب خود را در دنیای ریاضیات پیدا نکرده است. به ویژه در ایران، در حال حاضر تعداد معدودی از محققین در این زمینه فعال هستند و هنوز هم برخی از مراکز پژوهشی و دانشگاهی، توجه درخوری به این رشته نشان نداده‌اند. یکی از دلایل نگارش کتاب حاضر، معرفی یکی از ابزارهای مهم این رشته در سطح کارشناسی و کارشناسی ارشد است تا شاید بتوان با رشد و توسعه تدریجی این رشته در آینده، امید داشت تا پژوهشگران جوان، بیش از پیش جذب این رشته شوند.

[2] ابو جعفر محمد بن موسی الخوارزمی معروف به خوارزمی، ریاضی‌دان شهیر ایرانی است که حدود سال ۷۸۰ میلادی در خوارزم (که در حال حاضر شهری از ازبکستان کنونی است ولی در آن زمان بخشی از امپراطوری ایران بود) متولد شد. کتاب «المختصر فی حساب الجبر و المقابله» او را بسیاری از مترجمان مشهور قرون وسطی ترجمه کرده‌اند. در این کتاب، خوارزمی برای اولین بار، روشی الگوریتمیک را برای حل معادلات خطی و درجه دوم بر حسب یک متغیر ارائه کرد و به همین خاطر، او را می‌توان پدر جبر محاسباتی دانست. خوارزمی پس از این کتاب، رساله‌ای مقدماتی در حساب به نام «الجمع و التفریق بحساب الهند» نوشت که در آن، روش‌هایی الگوریتمیک برای انجام جمع، تفریق، ضرب، تقسیم و جذر اعداد در دستگاه هندی (یا به غلط عربی) بیان کرد و ترجمه این کتاب (در قرن دوازدهم میلادی) به لاتین تحت عنوان *Algirithmi de numero Indorum* باعث شد تا (در قرن شانزدهم میلادی) دستگاه عددی در اروپا، از عددنویسی رومی به عددنویسی هندی (یعنی سیستم دهدهی که امروزه استفاده می‌شود) تغییر یابد.

برمی‌گردد. کلمه جبر را اروپایی‌ها از کتاب «المختصر فی حساب الجبر و المقابله» گرفته‌اند و کلمه «الگوریتم» نیز غربی‌سازی واژه الخوارزمی است.

یکی از ابزارهای قوی در هندسه جبری و جبر محاسباتی برای حل و تحلیل دستگاه‌های معادلات چندجمله‌ای، پایه گربنر است. این مفهوم را بوخبرگر [۱] در سال ۱۹۶۵ در رساله دکترایش معرفی کرد و بعدها به احترام استاد راهنمایش، آن را پایه گربنر [۲] نامید [۷]. او همچنین الگوریتمی برای محاسبه این پایه ارائه کرد. با توجه به جنبه‌های نظری و محاسباتی پایه گربنر، این مفهوم به یکی از ابزارهای مهم در علوم و مهندسی تبدیل شده است. تاکنون حدود ۶ کتاب و بالغ بر ۳۰۰۰ مقاله (بر اساس پایگاه داده‌های $Mathscinet$) در زمینه پایه گربنر و کاربردهای آن، نگاشته شده است که نشان از اهمیت و کاربردی بودن این مفهوم دارد. برای توضیح ایده اصلی نظریه پایه گربنر، به مثال زیر توجه کنید. فرض کنیم I یک ایده‌آل باشد که توسط تعدادی چندجمله‌ای تک‌متغیره تولید شده باشد. برای بررسی تعلق f به I، باید بزرگترین مقسوم‌علیه مشترک مولدهای I را بدست آوریم و سپس f را به این چندجمله‌ای تقسیم کنیم. اگر باقیمانده صفر شد، $f \in I$ و در غیر این صورت $f \notin I$. نظریه پایه گربنر، یک تلاش موفق در انجام این روند برای چندجمله‌ای‌های چندمتغیره است. اگر I ایده‌آلی باشد که توسط تعدادی چندجمله‌ای چندمتغیره تولید شود و f یک چندجمله‌ای دلخواه باشد، برای بررسی تعلق f به I، یک پایه گربنر I را محاسبه می‌کنیم و اگر باقیمانده تقسیم f بر این پایه صفر شد، $f \in I$ و در غیر این صورت $f \notin I$.

با توجه به اجراهای متنوع و مؤثر الگوریتم‌های محاسبه پایه گربنر در نرم‌افزارهای مختلف، زمینه‌های کاربردهای آن در علوم (مانند حل دستگاه‌های معادلات چندجمله‌ای، کدگذاری، برنامه‌ریزی خطی و جبرخطی) و مهندسی (مانند پردازش تصویر، دیدکامپیوتری و نظریه کنترل) فراهم شده است. از طرفی برای برخی مثال‌های عملی از محاسبه پایه گربنر، به دلیل بالا بودن حجم محاسبات، الگوریتم‌های ارائه شده قادر به محاسبه پایه گربنر مورد نظر نیستند. بنابراین یکی از چالش‌هایی که پژوهشگران این رشته مشغول تحقیق و پژوهش روی آن هستند این است که چگونه می‌توان از دیدگاه ریاضی و کامپیوتری الگوریتم‌های محاسبه پایه گربنر را ارتقا داد طوری که بتوان پایه گربنر مورد نظر را سریعتر محاسبه کرد. در این زمینه تلاش‌های زیادی صورت گرفته است و الگوریتم‌های متعددی برای این منظور طراحی شده است که در فصل سوم به برخی از آن‌ها اشاره خواهیم کرد.

پایه گربنر، به بسیاری از مسائل الگوریتمیک که مرتبط با چندجمله‌ای‌های چندمتغیره هستند پاسخ می‌دهد. یکی از مهم‌ترین این مسائل، همان‌طور که پیشتر اشاره شد، حل دستگاه‌های معادلات چندجمله‌ایست. با ارائه یک مثال ساده، نشان می‌دهیم چگونه با استفاده از این پایه می‌توان یک دستگاه معادلات غیرخطی را حل کرد. دستگاه زیر را در نظر می‌گیریم

$$\begin{cases} x^۲+y+z &= ۱ \\ x+y^۲+z &= ۱ \\ x+y+z^۲ &= ۱. \end{cases}$$

حال ایده‌آل تولید شده توسط چندجمله‌ای‌های $x^۲+y+z-۱$، $x+y^۲+z-۱$ و $x+y+z^۲-۱$

---

[۱] برونو بوخبرگر (Bruno Buchberger) ریاضی‌دان اتریشی است که در سال ۱۹۴۲ متولد شد و شهرتش به خاطر خلق نظریه پایه گربنر و توسعه جبر کامپیوتریست.

[۲] ولفگانگ گربنر (Wolfgang Groebner) ریاضی‌دان اتریشی (۱۹۸۰ – ۱۸۹۹) و استاد دانشگاه اینسبروگ بود. او مدتی در دانشگاه گوتینگن در آلمان با امی نوتر ریاضی‌دان برجسته آلمانی در زمینه جبر جابجایی تحقیق و پژوهش کرد و حاصل تحقیقات او چاپ چندین کتاب و مقاله در زمینه هندسه جبری (بویژه به زبان آلمانی) است که مورد توجه ریاضی‌دانان حوزه جبر کامپیوتری قرار گرفته است.

را در نظر می‌گیریم. یک پایه گربنر این ایده‌آل به صورت زیر است

$$\{-z^2 - 4z^4 + 4z^3 + z^6, -z^2 + z^4 + 2yz^2, -z^2 - y + z + y^2, x + y + z^2 - 1\}.$$

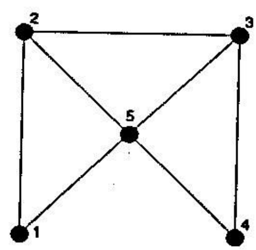
در فصل سوم ثابت خواهیم کرد که دستگاه بالا و دستگاه متناظر این پایه یعنی

$$\begin{cases} -z^2 - 4z^4 + 4z^3 + z^6 & = 0 \\ -z^2 + z^4 + 2yz^2 & = 0 \\ -z^2 - y + z + y^2 & = 0 \\ x + y + z^2 & = 1 \end{cases}$$

دارای ریشه‌های یکسانی هستند. از طرفی حل دستگاه دوم به راحتی انجام‌پذیر است. معادله اول آن را می‌توان به $z^2(z-1)^2(z^2+2z-1)$ تجزیه کرد که ریشه‌های آن $0, 1, -1+\sqrt{2}, -1-\sqrt{2}$ هستند. با جایگذاری هر کدام از این مقادیر در معادلات دوم و سوم (که تنها بر حسب y و z هستند)، می‌توان مقادیر y را بدست آورد. در نهایت با جایگذاری هر مقدار y و z در معادله $x + y + z^2 = 1$، می‌توان مقدار متناظر x را نیز محاسبه کرد. با انجام این مراحل برای همه مقدارهای z، ریشه‌های دستگاه به صورت زیر بدست می‌آیند

$$\begin{gathered} (1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1), \\ (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), \\ (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}). \end{gathered}$$

در پایان، به عنوان مثالی از کاربردهای پایه گربنر نشان می‌دهیم که چگونه می‌توان با استفاده از این پایه، مسأله رنگ‌آمیزی گراف را بررسی کرد. گراف زیر را در نظر می‌گیریم می‌خواهیم ۳-رنگ‌پذیر بودن این گراف را بررسی



کنیم. برای این منظور فرض کنیم $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ یک ریشه مکعب ۱ باشد، یعنی $\xi^3 = 1$. حال می‌خواهیم گراف مورد نظر را با سه رنگ قرمز، سبز و آبی رنگ‌آمیزی کنیم. این رنگ‌ها را به ترتیب با ۱، ξ و ξ^2 که سه ریشه متمایز $x^3 = 1$ در $\mathbb{C}$ هستند، نمایش می‌دهیم. همچنین فرض می‌کنیم $x_1, \dots, x_5$ نمایش رنگ‌های رئوس این گراف باشند. بنابراین $x_i^3 = 1$ برای هر i. در نتیجه $x_i^3 = x_j^3$ و $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$ برای هر i و j. از طرفی، برای مثال، برای رئوس مجاور ۱ و ۲ داریم $x_1 \neq x_2$ و $x_1^2 + x_1 x_2 + x_2^2 = 0$. برای رئوس مجاور، این معادلات را تشکیل می‌دهیم و در نهایت، ۳-رنگ‌پذیری این گراف معادل ریشه داشتن

دستگاه معادلات زیر است

$$
\begin{cases}
x_1^3 & = & 0 \\
 & \vdots & \\
x_5^3 & = & 0 \\
x_1^2 + x_1x_2 + x_2^2 & = & 0 \\
 & \vdots & \\
x_4^2 + x_4x_5 + x_5^2 & = & 0.
\end{cases}
$$

در فصل سوم ثابت خواهیم کرد که این دستگاه دارای جواب است اگر پایه گربنر ایده‌آل متناظر آن شامل عدد ثابت نباشد. با محاسبه پایه گربنر مورد نظر، می‌توان دید که این گراف ۳-رنگ‌پذیر است و با حل دستگاه متناظر با این پایه گربنر (مشابه روش بالا)، جواب‌های زیر را بدست می‌آوریم که شش روش رنگ‌آمیزی گراف را ارائه می‌کند

$$
\begin{array}{c}
(\xi \quad \xi^2 \quad \xi \quad \xi^2 \quad 1) \\
(\xi^2 \quad \xi \quad \xi^2 \quad \xi \quad 1) \\
(\xi \quad 1 \quad \xi \quad 1 \quad \xi^2) \\
(1 \quad \xi \quad 1 \quad \xi \quad \xi^2) \\
(\xi^2 \quad 1 \quad \xi^2 \quad 1 \quad \xi) \\
(1 \quad \xi^2 \quad 1 \quad \xi^2 \quad \xi).
\end{array}
$$

در ادامه، به بیان توضیحات کلی درباره کتاب و ساختار آن می‌پردازیم. این کتاب، حاصل تجربه تدریس چندین بار درس هندسه جبری در مقاطع کارشناسی و کارشناسی ارشد در دانشکده علوم ریاضی دانشگاه صنعتی اصفهان در طی سال‌های ۱۴۰۱-۱۳۸۶ است. مطالب این کتاب به نحوی تنظیم شده است که می‌تواند برای ارائه یک درس در مقطع کارشناسی (با حذف برخی مطالب پیشرفته) و یا یک درس در مقطع کارشناسی ارشد (با حذف برخی مطالب مقدماتی) قابل استفاده باشد. در فصل دوم، به بیان مقدمات جبری مورد نیاز می‌پردازیم. در فصل سوم، ترتیب چندجمله‌ای، الگوریتم تقسیم، پایه گربنر و ویژگی‌های مهم آن را بیان می‌کنیم. این فصل شامل روش‌های اصلی محاسبه پایه گربنر است. در فصل چهارم، به کاربردهای مهم پایه گربنر در جبر، جبرخطی، آنالیز، نظریه اعداد و برنامه‌ریزی خطی خواهیم پرداخت. لازم به ذکر است که بیشتر مطالب این کتاب از مراجع [۱، ۴، ۹، ۱۰، ۱۲، ۱۷، ۲۹، ۳۰، ۴۱] گردآوری شده است. در سرتاسر کتاب تلاش شده است شیوه استفاده از نرم‌افزار میپل برای انجام محاسبات مختلف توضیح داده شود. اصلاحات احتمالی و نکات تکمیلی از طریق وبگاه /https://amirhashemi.iut.ac.ir به استحضار خوانندگان گرامی خواهد رسید.

در پایان بر خود لازم می‌دانم از کلیه کسانی که مرا در تهیه این کتاب یاری کردند تشکر کنم. بدون شک، تدریس مطالب این کتاب در دانشگاه صنعتی اصفهان و ارتباط علمی دو طرفه‌ای که با دانشجویانم داشته‌ام، در ارتقای کیفیت و نوع ارائه مطالب کتاب، تأثیر قابل توجهی داشته است. بدین وسیله از همکارم آقای دکتر محسن خانی و همه دانشجویانم صمیمانه سپاس‌گزاری می‌کنم.

امیر هاشمی

اصفهان-پاییز ۱۴۰۱

فهرست نمادها

نماد	مفهوم	اولین صفحه مراجعه
$Z[i]$	حلقه اعداد صحیح گاوسی	۲
$\mathbb{Z}_n$	مجموعه کلاس‌های همنهشتی به پیمانه n	۲
$S[\Gamma]$	حلقه الحاقی	۵
$R[x_1, \ldots, x_n]$	حلقه چندجمله‌ای‌های بر حسب $x_1, \ldots, x_n$ با ضرایب در R	۵
$\deg(f)$	درجه چندجمله‌ای f	۶
R/I	حلقه خارج‌قسمتی R روی I	۸
$[a]$	هم‌دسته a	۸
$\langle H \rangle$	ایده‌آل تولید شده توسط H	۹
$I + J$	جمع دو ایده‌آل I و J	۱۰
$I.J$	ضرب دو ایده‌آل I و J	۱۰
$I : J$	خارج‌قسمت دو ایده‌آل I و J	۱۱
$\sqrt{I}$	رادیکال ایده‌آل I	۱۱
$Z(R)$	مجموعه مقسوم‌علیه‌های صفر R	۱۳
$\gcd(a_1, \ldots, a_n)$	ب.م.م. $a_1, \ldots, a_n$	۳۱
$\mathrm{Syl}(f, g)$	ماتریس سیلوستر f و g	۴۰
$\mathrm{Res}(f, g)$	منتج f و g	۴۰
$\mathrm{cont}(f)$	محتوی f	۴۲
$\mathbf{V}(f_1, \ldots, f_k)$	چندگونای $f_1, \ldots, f_k$	۴۵
$\mathbf{I}(V)$	ایده‌آل V	۵۲
$\mathrm{Ass}(I)$	مجموعه ایده‌آل‌های اول وابسته I	۶۴
$\prec$	ترتیب تک‌جمله‌ای	۷۱
$\prec_{lex}$	ترتیب الفبایی	۷۳
$\prec_{dlex}$	ترتیب الفبایی مدرج	۷۳
$\prec_{drl}$	ترتیب الفبایی معکوس مدرج	۷۴
$\mathrm{LC}(f)$	ضریب پیشروی f	۷۴

فهرست مطالب

فصل ۳ کاربردهای پایه گربنر ۱۵۱