فصل ۱

هندسه، جبر و الگوریتم‌ها

در این فصل برخی از موضوعات اصلی این کتاب را معرفی خواهیم کرد. هندسه‌ای که به آن علاقه‌مندیم به *چندگوناهای آفین*، یعنی به خم‌ها و رویه‌ها (و اشیاء با بُعد بالاتر) تعریف شده توسط معادلات چندجمله‌ای، مربوط است. برای فهم چندگوناهای آفین، به مقداری جبر نیاز داریم و به‌ویژه، لازم است که *ایده‌آل‌های* در حلقهٔ چندجمله‌ای‌های $k[x_1, \ldots, x_n]$ را مطالعه کنیم. سرانجام، برای نشان دادن نقشی که توسط *الگوریتم‌ها* ایفا می‌شود، چندجمله‌ای‌های از یک متغیر را مورد بحث قرار خواهیم داد.

§۱ چندجمله‌ای‌ها و فضای آفین

برای پیوند دادن جبر و هندسه، چندجمله‌ای‌های روی یک میدان را مطالعه خواهیم کرد. همه می‌دانیم که چندجمله‌ای‌ها چه اشیایی هستند، امّا واژهٔ *میدان* ممکن است که ناآشنا باشد. شهود ابتدایی این است که یک میدان، مجموعه‌ای است که در آن می‌توانیم جمع، تفاضل، ضرب و تقسیم با خواص معمول را تعریف کنیم. مثال‌های متعارف عبارت‌اند از اعداد حقیقی $\mathbb{R}$، اعداد مختلط $\mathbb{C}$، درحالی‌که اعداد صحیح $\mathbb{Z}$ یک میدان نیست زیرا عمل تقسیم برقرار نیست (3 و 2 اعداد صحیح‌اند، ولی خارج‌قسمت آنها $3/2$ صحیح نیست). تعریف صوری میدان در پیوست (الف) ارائه شده است.

یک دلیل اهمیت میدان‌ها این است که جبرخطی روی هر میدان قابلِ اجراست. بنابراین حتی اگر در درس جبرخطی‌تان اسکالرها محدود به $\mathbb{R}$ یا $\mathbb{C}$ بوده‌اند، بیشتر قضایا و روش‌هایی که آموخته‌اید، روی هر میدان دلخواه k قابلِ اجرا هستند. در این کتاب، میدان‌های متفاوت را برای مقاصد متفاوت به‌کار خواهیم گرفت. متداول‌ترین میدان‌ها عبارت‌اند از:

- اعداد گویای $\mathbb{Q}$: میدانِ بیشتر مثال‌های رایانه‌ای.
- اعداد حقیقی $\mathbb{R}$: میدان ترسیم شکل‌های خم‌ها و رویه‌ها.
- اعداد مختلط $\mathbb{C}$: میدان اثبات بسیاری از قضایا.

بعضی مواقع، با میدان‌های دیگر، مانند میدان توابع گویا (که بعداً تعریف خواهد شد)، مواجه خواهیم شد. نظریهٔ خیلی جالبی نیز دربارهٔ میدان‌های متناهی وجود دارد ـــ برای مشاهدهٔ یکی از مثال‌های ساده‌تر، تمرین‌ها را ببینید.

اکنون می‌توانیم چندجمله‌ای‌ها را تعریف کنیم. خواننده مطمئناً با چندجمله‌ای‌های از یک و دو متغیر آشناست، امّا لازم است که چندجمله‌ای‌های از n متغیر $x_1, \ldots, x_n$ با ضرایب در یک میدان دلخواه k را مورد بحث قرار دهیم.

تعریف ۱. یک **یکجمله‌ای** از $x_1, \ldots, x_n$، حاصل‌ضربی به‌صورت

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

است که در آن همهٔ توان‌های $\alpha_1, \ldots, \alpha_n$ اعداد صحیح نامنفی‌اند. **درجهٔ کلی** این یکجمله‌ای عبارت است از مجموع $\alpha_1 + \cdots + \alpha_n$.

می‌توانیم نمادگذاری یکجمله‌ای‌ها را به‌صورت زیر ساده کنیم: فرض کنیم $\alpha = (\alpha_1, \ldots, \alpha_n)$ یک nـتایی از اعداد صحیح نامنفی باشد. دراین‌صورت قرار می‌دهیم

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

توجه شود که $x^\alpha = 1$ وقتی $\alpha = (0, \ldots, 0)$. همچنین فرض می‌کنیم $|\alpha| = \alpha_1 + \cdots + \alpha_n$ درجهٔ کلی یکجمله‌ای x^α را نمایش دهد.

تعریف ۲. یک **چندجمله‌ای** f از $x_1, \ldots, x_n$ با ضرایب در یک میدان k، یک ترکیب خطی متناهی (با ضرایب در k) از یکجمله‌ای‌ها است. یک چندجمله‌ای f را به‌صورت

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k$$

می‌نویسیم که در آن مجموع روی تعدادی متناهی nـتایی $\alpha = (\alpha_1, \ldots, \alpha_n)$ است. مجموعهٔ همهٔ چندجمله‌ای‌های از $x_1, \ldots, x_n$ با ضرایب در k را با $k[x_1, \ldots, x_n]$ نمایش می‌دهیم.

وقتی با چندجمله‌ای‌های از تعدادی کم متغیر سروکار داریم، معمولاً از اندیس‌ها صرف‌نظر می‌کنیم. بنابراین چندجمله‌ای‌های از یک، دو و سه متغیر را به‌ترتیب در $k[x]$، $k[x, y]$ و $k[x, y, z]$ درنظر می‌گیریم. برای مثال،

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

یک چندجمله‌ای در $\mathbb{Q}[x, y, z]$ است. معمولاً از حروف f، g، h، p، q، r را برای نمایش چندجمله‌ای‌ها استفاده می‌کنیم.

اصطلاحات زیر را در بحث با چندجمله‌ای‌ها به‌کار خواهیم برد.

تعریف ۳. فرض کنیم $f = \sum_\alpha a_\alpha x^\alpha$ یک چندجمله‌ای در $k[x_1, \dots, x_n]$ باشد.

(i) a_α را **ضریب** یکجمله‌ای x^α می‌نامیم.

(ii) اگر $a_\alpha \neq 0$، $a_\alpha x^\alpha$ را یک **جملهٔ** f می‌نامیم.

(iii) **درجهٔ کلی** $f \neq 0$، که با $\deg(f)$ نمایش داده می‌شود، ماکزیمم $|\alpha|$ است به‌طوری‌که ضریب a_α ناصفر است. درجهٔ کلی چندجمله‌ای صفر تعریف نشده است.

به‌عنوان یک مثال، چندجمله‌ای $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ که در بالا ارائه شد، دارای چهار جمله و درجهٔ کلی شش است. توجه شود که دو جمله با درجهٔ کلی ماکزیمال وجود دارد و این اتفاقی است که برای چندجمله‌ای‌های از یک متغیر، نمی‌تواند رخ دهد. در فصل ۲، نحوهٔ *مرتب کردن* جملات یک چندجمله‌ای را مطالعه خواهیم کرد.

مجموع و حاصل‌ضرب دو چندجمله‌ای، دوباره یک چندجمله‌ای است. گوییم یک چندجمله‌ای f، یک چندجمله‌ای g را *می‌شمارد* هرگاه برای یک چندجمله‌ای $h \in k[x_1, \dots, x_n]$، $g = fh$.

می‌توان نشان داد که تحت جمع و ضرب، $k[x_1, \dots, x_n]$ در تمام اصول موضوعه میدان‌ها به‌جز وجود وارون ضربی صدق می‌کند (زیرا برای مثال، $1/x_1$ یک چندجمله‌ای نیست). یک چنین ساختار ریاضی، یک حلقهٔ جابه‌جایی نامیده می‌شود (پیوست (الف) را برای تعریف کامل ببینید) و به همین دلیل به $k[x_1, \dots, x_n]$ به‌عنوان یک *حلقهٔ چندجمله‌ای‌ها* مراجعه خواهیم کرد.

موضوع بعدی که باید درنظر بگیریم، فضای آفین است.

تعریف ۴. برای یک میدان k و یک عدد صحیح مثبت n، **فضای آفین** n-بُعدی روی k را مجموعهٔ

$$k^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in k\}$$

تعریف می‌کنیم.

برای یک مثال از فضای آفین، حالت $k = \mathbb{R}$ را درنظر می‌گیریم. در اینجا فضای آشنای $\mathbb{R}^n$ از حسابان و جبرخطی را به‌دست می‌آوریم. در حالت کلی، $k^1 = k$ را *خط آفین* و k^2 را *صفحهٔ آفین* می‌نامیم.

در ادامه، می‌خواهیم ببینیم که چگونه چندجمله‌ای‌ها به فضای آفین مربوط می‌شوند. ایدهٔ کلیدی این است که یک چندجمله‌ای $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \dots, x_n]$، یک تابع

$$f : k^n \longrightarrow k$$

را به‌دست می‌دهد که به‌صورت زیر تعریف می‌شود: برای $(a_1, \dots, a_n) \in k^n$، هر x_i را در عبارت f با a_i جایگزین می‌کنیم. ازآنجاکه همهٔ ضرایب نیز در k قرار دارند، این عمل یک عنصر $f(a_1, \dots, a_n) \in k$ را به‌دست می‌دهد. توانایی درنظر گرفتن یک چندجمله‌ای به‌عنوان یک تابع همان چیزی است که پیوند جبر و هندسه را ممکن می‌سازد.

ماهیت دوگانهٔ چندجمله‌ای‌ها نتایج غیرمنتظره‌ای به همراه خواهد داشت. برای مثال، این پرسش که «آیا

$f = 0$؟» دو معنی بالقوه دارد: آیا f چندجمله‌ای صفر است؟ که بدین معنی است که همهٔ ضرایب a_α صفرند یا اینکه آیا f تابع صفر است؟ که بدین معنی است که برای هر $(a_1, \ldots, a_n) \in k^n$، $f(a_1, \ldots, a_n) = 0$. واقعیت تعجب‌آور آن است که این دو عبارت در حالت کلی معادل نیستند. برای مثالی از چگونگی تفاوت آنها، مجموعهٔ مرکب از دو عنصر 0 و 1 را درنظر می‌گیریم. در تمرین‌ها مشاهده خواهید کرد که این مجموعه را می‌توان به یک میدان تبدیل کرد که در آن $1 + 1 = 0$. این میدان را معمولاً $\mathbb{F}_2$ می‌نامند. اکنون چندجمله‌ای $x^2 - x = x(x-1) \in \mathbb{F}_2[x]$ را درنظر می‌گیریم. ازآنجاکه این چندجمله‌ای در 0 و 1 صفر می‌شود، چندجمله‌ای ناصفری به‌دست آورده‌ایم که روی فضای آفین $\mathbb{F}_2^1$ تابع صفر است. مثال‌های دیگری در تمرین‌ها مورد بحث قرار خواهند گرفت.

اگرچه، وقتی k یک میدان نامتناهی است، مشکلی وجود ندارد.

گزاره ۵. *فرض کنیم k یک میدان نامتناهی باشد و $f \in k[x_1, \ldots, x_n]$. دراین‌صورت در $k[x_1, \ldots, x_n]$، $f = 0$ اگروفقط‌اگر $f : k^n \to k$ تابع صفر باشد.*

برهان. یک جهت اثبات، بدیهی است زیرا چندجمله‌ای صفر به‌وضوح تابع صفر را به‌دست می‌دهد. برای اثبات درجهت عکس، باید نشان دهیم که اگر برای هر $(a_1, \ldots, a_n) \in k^n$، $f(a_1, \ldots, a_n) = 0$، دراین‌صورت f چندجمله‌ای صفر است. با استقراء روی n، تعداد متغیرها، عمل می‌کنیم. برای $n = 1$، می‌دانیم که یک چندجمله‌ای ناصفر در $k[x]$ با درجه m دارای حداکثر m ریشه متمایز است (این حقیقت را درنتیجه ۳ از §۵ ثابت خواهیم کرد) و برای $f \in k[x]$ در این حالت، فرض ما بر این است که برای هر $a \in k$، $f(a) = 0$. ازآنجاکه k نامتناهی است، این بدین معنی است که f دارای بی‌نهایت ریشه است و درنتیجه باید چندجمله‌ای صفر باشد.

اکنون فرض کنیم عکس قضیه برای $n - 1$ برقرار باشد و $f \in k[x_1, \ldots, x_n]$ یک چندجمله‌ای باشد که در تمام نقاط k^n صفر می‌شود. با دسته‌بندی توان‌های مختلف x_n، می‌توانیم f را به‌صورت

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i$$

بنویسیم که در آن $g_i \in k[x_1, \ldots, x_{n-1}]$. نشان می‌دهیم که هر g_i چندجمله‌ای صفر از $n - 1$ متغیر است که ایجاب می‌کند f چندجمله‌ای صفر در $k[x_1, \ldots, x_n]$ است.

اگر $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ را ثابت بگیریم، دراین‌صورت چندجمله‌ای $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ را به‌دست می‌آوریم. باتوجه به فرضِ دربارهٔ f، این چندجمله‌ای برای هر $a_n \in k$، صفر می‌شود. از حالت $n = 1$، نتیجه می‌شود که $f(a_1, \ldots, a_{n-1}, x_n)$ چندجمله‌ای صفر در $k[x_n]$ است. با استفاده از فرمول فوق، می‌بینیم که ضرایب $f(a_1, \ldots, a_{n-1}, x_n)$ عبارت‌اند از $g_i(a_1, \ldots, a_{n-1})$ و درنتیجه برای هر i، $g_i(a_1, \ldots, a_{n-1}) = 0$. ازآنجاکه انتخاب $(a_1, \ldots, a_{n-1})$ در k^{n-1} دلخواه است، نتیجه می‌شود که هر $g_i \in k[x_1, \ldots, x_{n-1}]$ تابع صفر روی k^{n-1} را به‌دست می‌دهد. دراین‌صورت فرض استقراء ایجاب می‌کند که g_i در $k[x_1, \ldots, x_{n-1}]$ چندجمله‌ای صفر است. این سبب می‌شود که f در $k[x_1, \ldots, x_n]$ چندجمله‌ای صفر باشد و بدین ترتیب برهان گزاره کامل

می‌شود. □

توجه شود که در حکم گزارهٔ ۵، ادعای «در $k[x_1,\ldots,x_n]$، $f=0$» بدین معنی است که f چندجمله‌ای صفر است، یعنی هر ضریب f صفر است. بنابراین از نماد «0» هم برای نمایش عنصر صفر k و هم برای چندجمله‌ای صفر در $k[x_1,\ldots,x_n]$ استفاده می‌کنیم. اینکه این نماد را برای کدام منظور استفاده می‌کنیم، از روی متن مشخص خواهد شد.

نتیجه ۶. فرض کنیم k یک میدان نامتناهی باشد و $f,g\in k[x_1,\ldots,x_n]$. دراین‌صورت در $k[x_1,\ldots,x_n]$، $f=g$ اگروفقط‌اگر $f:k^n\to k$ و $g:k^n\to k$ توابعی یکسان باشند.

برهان. برای اثبات جهت نابدیهی، فرض کنیم $f,g\in k[x_1,\ldots,x_n]$ توابعی یکسان روی k^n تعریف کنند. طبق فرض، چندجمله‌ای $f-g$ روی همهٔ نقاط k^n صفر می‌شود. دراین‌صورت گزارهٔ ۵ ایجاب می‌کند که $f-g$ چندجمله‌ای صفر باشد. این ثابت می‌کند که در $k[x_1,\ldots,x_n]$، $f=g$. □

سرانجام، لازم است که خاصیتی خاص از چندجمله‌ای‌های روی میدان اعداد مختلط $\mathbb{C}$ را به‌خاطر بسپاریم.

قضیه ۷. *هر چندجمله‌ای غیرثابت $f\in\mathbb{C}[x]$ دارای ریشه‌ای در $\mathbb{C}$ است.*

برهان. این قضیهٔ اساسی جبر است و اثبات‌هایی را برای آن می‌توان در بسیاری از کتاب‌های مقدماتی دربارهٔ آنالیز مختلط یافت (اگرچه اثبات‌های دیگری نیز برای آن وجود دارند). □

یک میدان k را *جبری‌بسته* گوییم هرگاه هرچندجمله‌ای غیرثابت در $k[x]$ دارای ریشه‌ای در k باشد. بنابراین $\mathbb{R}$ جبری‌بسته نیست (ریشه‌های x^2+1 چیست؟)، ولی طبق قضیهٔ فوق $\mathbb{C}$ جبری‌بسته است. در فصل ۴، یک تعمیم قوی از قضیهٔ ۷ به‌نام قضیهٔ صفرهای هیلبرت را ثابت خواهیم کرد.

تمرین‌های ۱§

۱. فرض کنیم $\mathbb{F}_2=\{0,1\}$ و جمع و ضرب را توسط $0+0=1+1=0$، $0+1=1+0=1$، $0\cdot 0=0\cdot 1=1\cdot 0=0$ و $1\cdot 1=1$ تعریف می‌کنیم. توضیح دهید که چرا $\mathbb{F}_2$ یک میدان است. (لزومی ندارد خواص شرکت‌پذیری و توزیع‌پذیری را بررسی کنید، امّا وجود عناصر همانی و وارون‌ها را برای هردوی جمع و ضرب باید بررسی کنید.)

۲. فرض کنیم $\mathbb{F}_2$ میدان در تمرین ۱ باشد.

الف) چندجمله‌ای $g(x,y)=x^2y+y^2x\in\mathbb{F}_2[x,y]$ را درنظر می‌گیریم. نشان دهید که برای هر $(x,y)\in\mathbb{F}_2^2$، $g(x,y)=0$ و توضیح دهید چرا این گزارهٔ ۵ را نقض نمی‌کند.

ب) یک چندجمله‌ای ناصفر در $\mathbb{F}_2[x,y,z]$ بیابید که در هر نقطهٔ $\mathbb{F}_2^3$ صفر شود. سعی کنید نمونه‌ای بیابید که هر سه متغیر در آن ظاهر شوند.

پ) یک چندجمله‌ای ناصفر در $\mathbb{F}_2[x_1,\ldots,x_n]$ بیابید که هر نقطهٔ $\mathbb{F}_2^n$ صفر شود. آیا می‌توانید نمونه‌ای بیابید که تمام متغیرها در آن ظاهر شوند.

۳. (با پیش‌نیاز جبر مجرد) فرض کنیم p یک عدد اوّل باشد. حلقهٔ اعداد صحیح به پیمانهٔ p یک میدان با p عضو است که با $\mathbb{F}_p$ نمایش داده می‌شود.

الف) توضیح دهید که چرا $\mathbb{F}_p \setminus \{0\}$ تحت ضرب یک گروه است.
ب) با استفاده از قضیهٔ لاگرانژ[1] نشان دهید که برای هر $a \in \mathbb{F}_p \setminus \{0\}$، $a^{p-1} = 1$.
پ) ثابت کنید که برای هر $a \in \mathbb{F}_p$، $a^p = a$. راهنمایی: حالت‌های $a = 0$ و $a \neq 0$ را جداگانه درنظر بگیرید.
ت) یک چندجمله‌ای ناصفر در $\mathbb{F}_p[x]$ بیابید که در تمام نقاط $\mathbb{F}_p$ صفر شود. راهنمایی: قسمت (پ) را به‌کار ببرید.

۴. (با پیش‌نیاز جبرمجرد) فرض کنیم F یک میدان متناهی با q عضو باشد. با اقتباس از استدلال تمرین ۳ ثابت کنید که $x^q - x$ یک چندجمله‌ای ناصفر در $F[x]$ است که در هر نقطهٔ F صفر می‌شود و این نشان می‌دهد که گزارهٔ ۵ برای *تمام* میدان‌های متناهی برقرار نیست.

۵. در برهان گزارهٔ ۵، $f \in k[x_1, \ldots, x_n]$ را درنظر گرفتیم و آن را به‌صورت یک چندجمله‌ای از x_n با ضرایب در $k[x_1, \ldots, x_{n-1}]$ نوشتیم. برای اینکه ببینیم این کار در یک حالت خاص به چه صورتی است، چندجمله‌ای

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3$$

را درنظر می‌گیریم.
الف) f را به‌صورت یک چندجمله‌ای از x با ضرایب در $k[y, z]$ بنویسید.
ب) f را به‌صورت یک چندجمله‌ای از y با ضرایب در $k[x, z]$ بنویسید.
پ) f را به‌صورت یک چندجمله‌ای از z با ضرایب در $k[x, y]$ بنویسید.

۶. در درون $\mathbb{C}^n$، زیرمجموعهٔ $\mathbb{Z}^n$ قرار دارد که مرکب از نقاط با مختصات صحیح است.
الف) ثابت کنید که اگر $f \in \mathbb{C}[x_1, \ldots, x_n]$ در هر نقطهٔ $\mathbb{Z}^n$ صفر شود، f چندجمله‌ای صفر است. راهنمایی: برهان گزارهٔ ۵ را وفق دهید.
ب) فرض کنیم $f \in \mathbb{C}[x_1, \ldots, x_n]$ و M بزرگترین توان هر متغیری باشد که در f ظاهر می‌شود. فرض کنیم $\mathbb{Z}^n_{M+1}$ مجموعه نقاط $\mathbb{Z}^n$ باشد که تمام مختصاتشان بین 1 و $M + 1$ شامل خود این دو عدد هستند. نشان دهید که اگر f در تمام نقاط $\mathbb{Z}^n_{M+1}$ صفر شود، دراین‌صورت f چندجمله‌ای صفر است.

§۲ چندگوناهای آفین

اکنون می‌توانیم اشیاء هندسی اصلی مورد مطالعه در این کتاب را معرفی کنیم.

تعریف ۱. فرض کنیم k یک میدان باشد و $f_1, \ldots, f_s$ چندجمله‌ای‌هایی در $k[x_1, \ldots, x_n]$ باشند. دراین‌صورت قرار می‌دهیم

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ ،} 1 \leq i \leq s \text{ برای هر } \}.$$

$\mathbf{V}(f_1, \ldots, f_s)$ را **چندگونای آفین** تعریف شده توسط $f_1, \ldots, f_s$ می‌نامیم.

بنابراین یک چندگونای آفین $\mathbf{V}(f_1, \ldots, f_s) \subseteq k^n$، مجموعهٔ تمام جواب‌های دستگاه معادلات چندجمله‌ای $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$ است. حروف V, W و مانند اینها را برای نمایش چندگوناهای

[1] Lagrange