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 اشیای 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

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

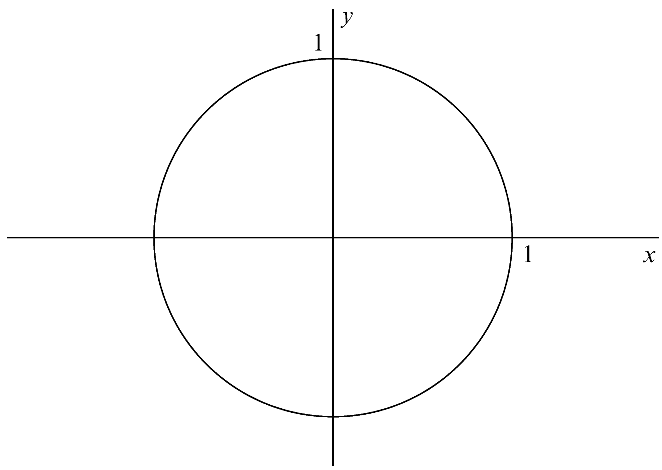
$\mathbf{V}(f_1, \ldots, f_s)$ را **چندگونای آفین** تعریف شده توسط $f_1, \ldots, f_s$ می‌نامیم.

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

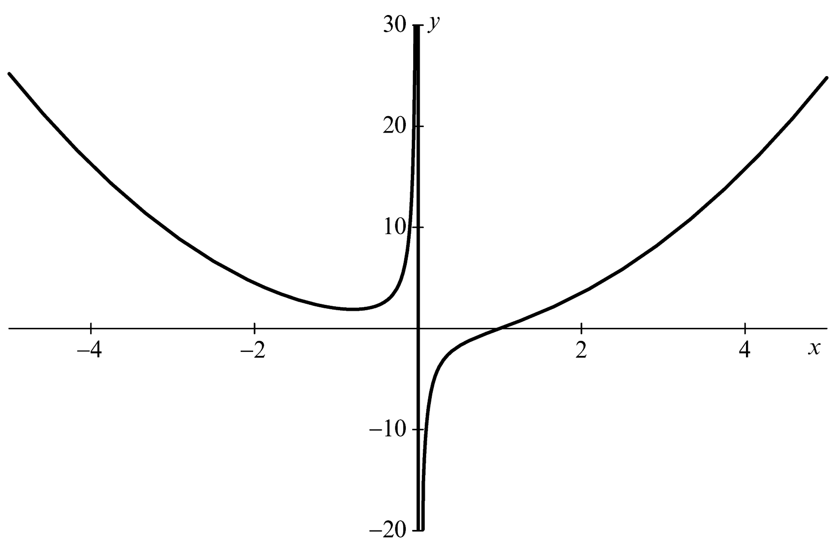
[1] Lagrange

آفین به‌کار می‌بریم. هدف اصلی این بخش، معرفی تعداد *قابل‌توجهی* مثال به خواننده است که بعضی جدید و بعضی آشنایند. از میدان $k = \mathbb{R}$ استفاده خواهیم کرد تا بتوانیم شکل‌ها را رسم کنیم.

بحث را با چندگونای $\mathbf{V}(x^2 + y^2 - 1)$ در صفحهٔ $\mathbb{R}^2$ آغاز می‌کنیم که دایره‌ای به شعاع 1 و به مرکز مبداء است:

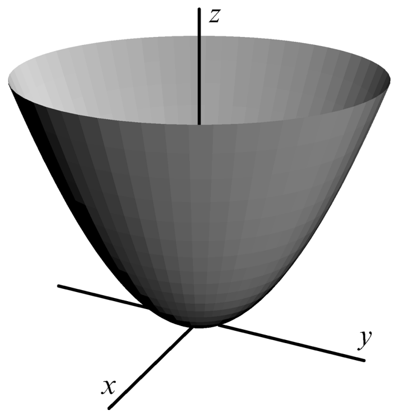


مقاطع مخروطی مطالعه شده در دبیرستان (دایره‌ها، بیضی‌ها، سهمی‌ها و هذلولی‌ها) چندگوناهای آفین‌اند. نمودارهای توابع چندجمله‌ای نیز چندگوناهای آفین‌اند. [نمودار $y = f(x)$ عبارت است از $\mathbf{V}(y - f(x))$]. اگرچه چندان واضح نیست، نمودارهای توابع گویا نیز چندگوناهای آفین‌اند. برای مثال، نمودار $y = \frac{x^3-1}{x}$ را درنظر می‌گیریم:

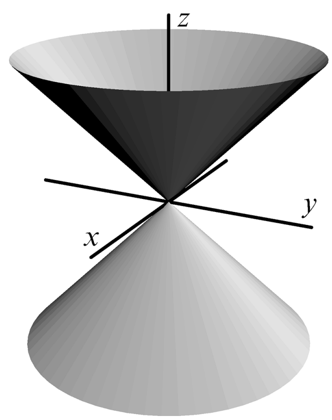


به‌سادگی می‌توان بررسی کرد که این نمودار، چندگونای آفین $\mathbf{V}(xy - x^3 + 1)$ است.

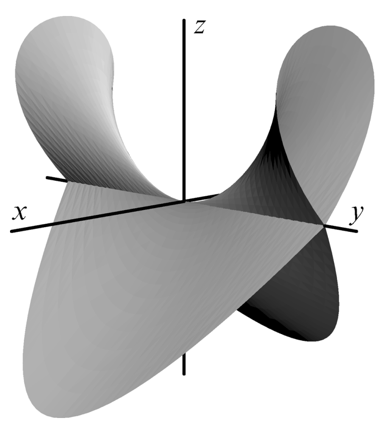
در ادامه، فضای 3ـبُعدی $\mathbb{R}^3$ را درنظر می‌گیریم. سهمی‌وار دوّار $\mathbf{V}(z - x^2 - y^2)$، مثالی خوب برای چندگوناهای آفین است که از دوران سهمی $z = x^2$ حول zـمحور به‌دست می‌آید (با استفاده از مختصات قطبی، این مطلب را می‌توان بررسی کرد). شکل حاصل به‌صورت زیر است:



یک مثال آشنای دیگر، مخروط $\mathbf{V}(z^2 - x^2 - y^2)$ است:

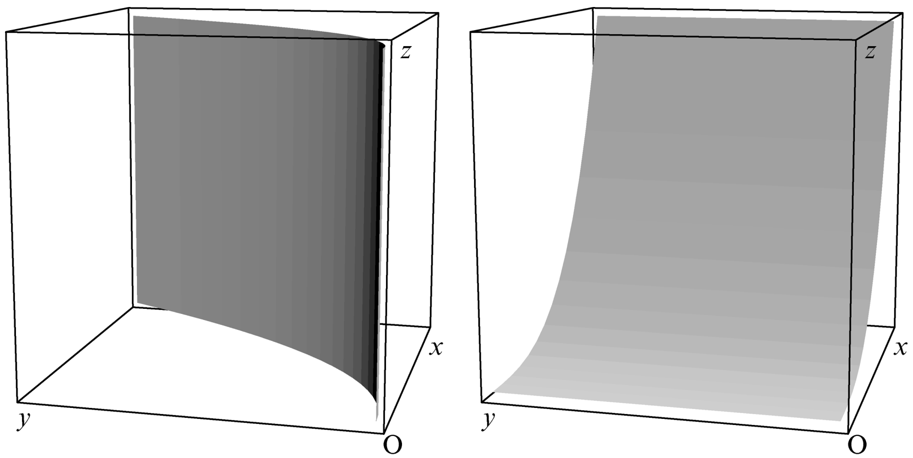


یک رویهٔ به‌مراتب پیچیده‌تر، چندگونای $\mathbf{V}(x^2 - y^2z^2 + z^3)$ است:

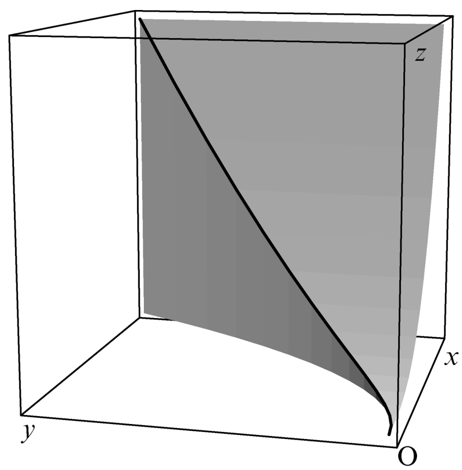


در دو مثال اخیر، رویه‌ها در همه‌جا هموار نیستند: مخروط دارای نقطه‌ای تیز در مبداء است و در مثال اخیر، رویه خودش را در امتداد کل y-محور قطع می‌کند. اینها مثال‌هایی برای *نقاط تکین* هستند که بعداً در این کتاب مطالعه خواهیم کرد.

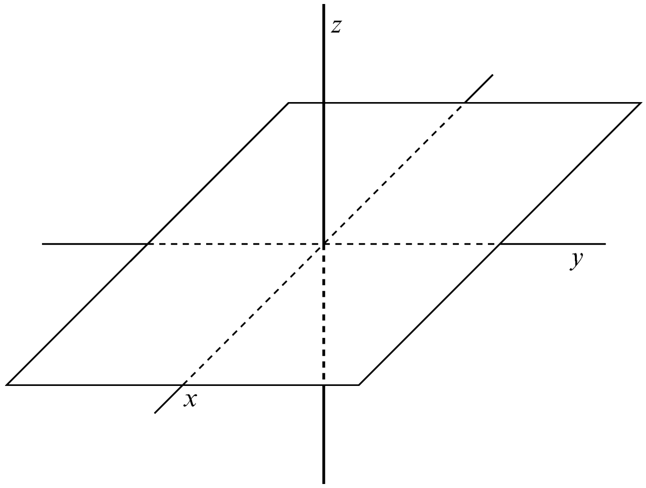
مثالی جالب برای یک خم در $\mathbb{R}^3$، خم درجهٔ *سهٔ تابدار*، یعنی چندگونای $\mathbf{V}(y-x^2, z-x^3)$ است. برای سادگی، خود را به بخش واقع در یک هشتم نخست دستگاه مختصات محدود می‌کنیم. ابتدا رویه‌های $y=x^2$ و $z=x^3$ را به‌طور مجزا رسم می‌کنیم:



دراین‌صورت اشتراکشان خم درجهٔ سهٔ تابدار را به‌دست می‌دهد:



توجه شود که وقتی یک معادله در $\mathbb{R}^2$ داریم، یک خم به‌دست می‌آوریم که یک شیء 1ـبُعدی است. وضعیتی مشابه در $\mathbb{R}^3$ رخ می‌دهد: یک معادله در $\mathbb{R}^3$، معمولاً یک رویه به‌دست می‌دهد که دارای بُعد 2 است. دوباره، بُعد یک واحد کم می‌شود. اکنون خم درجهٔ سهٔ تابدار را درنظر می‌گیریم: در اینجا، دو معادله در $\mathbb{R}^3$ یک خم به‌دست می‌دهند و بُعد دو واحد کم می‌شود. ازآنجاکه هر معادله یک محدودیت اضافی را تحمیل می‌کند، شهودمان می‌گوید هر معادله یک واحد از بُعد می‌کاهد. بنابراین اگر در $\mathbb{R}^4$ باشیم، می‌توان این انتظار را داشت که یک چندگونای آفین که توسط دو معادله تعریف می‌شود، یک رویه باشد. متاسفانه، مفهوم بُعد ظریف‌تر از آن چیزی است که توسط مثال‌های فوق نشان داده می‌شود. برای مشاهدهٔ این مطلب، چندگونای $\mathbf{V}(xz, yz)$ را درنظر می‌گیریم. به‌سادگی می‌توان بررسی کرد که معادلات $xz = yz = 0$ اجتماع (x,y)ـصفحه با zـمحور را تعریف می‌کنند:



بنابراین این چندگونا مرکب از دو قطعه است که بُعدهای متفاوتی دارند و یکی از قطعه‌ها (صفحه)، برطبق شهود فوق دارای بُعد «نادرست» است.

در ادامه، می‌خواهیم مثال‌هایی از چندگوناهای با بُعدهای بالاتر ارائه دهیم. یک حالت آشنا از جبرخطی نشأت می‌گیرد. یعنی، یک میدان k را ثابت می‌گیریم و یک دستگاه m معادلهٔ خطی از n مجهول $x_1, \ldots, x_n$ با ضریب در k را درنظر می‌گیریم:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{۱}$$

جواب‌های این معادلات تشکیل یک چندگونای آفین در k^n می‌دهند که آن را یک *چندگونای خطی* می‌نامیم. بنابراین خط‌ها و صفحه‌ها چندگوناهای خطی‌اند و مثال‌هایی با بُعد به دلخواه بزرگ وجود دارند. از جبرخطی با روش تحویل سطری (که روش حذف گاوسی[1] هم نامیده می‌شود) آشنایی داریم که الگوریتمی برای یافتن تمام جواب‌های یک چنین دستگاه معادلاتی به‌دست می‌دهد. در فصل ۲، تعمیمی از این روش را مطالعه خواهیم کرد که برای دستگاه‌های معادلات چندجمله‌ای به‌کار می‌رود.

چندگوناهای خطی به خوبی به بحث‌مان راجع به بُعد مربوط می‌شوند. یعنی، اگر $V \subseteq k^n$ چندگونایی خطی باشد که توسط (۱) تعریف می‌شود، دراین‌صورت V لزوماً دارای بُعد $n - m$ نیست با اینکه V توسط m معادله تعریف می‌شود. درحقیقت، وقتی V ناتهی است، برطبق نتایج جبرخطی V دارای بُعد $n - r$ است که در آن r رتبه ماتریس (a_{ij}) است. بنابراین برای چندگوناهای خطی، بُعد توسط تعداد معادلات *مستقل* تعیین می‌شود. این شهود برای چندگوناهای آفین کلی‌تر قابلِ اجراست، به‌جز آنکه مفهوم «مستقل» ظریف‌تر است.

برخی از مثال‌های پیچیده در بُعدهای بالاتر، از حسابان نشأت می‌گیرند. برای مثال، فرض کنیم می‌خواهیم مینیمم و ماکزیمم مقادیر $f(x, y, z) = x^3 + 2xyz - z^2$ را مشروط به قید $g(x, y, z) = x^2 + y^2 + z^2 = 1$ بیابیم. طبق روش ضرایب لاگرانژ در یک مینیمم یا ماکزیمم موضعی داریم $\nabla f = \lambda \nabla g$ [یادآوری می‌کنیم که

[1] Gaussian elimination