وزارت علوم، تحقیقات و فناوری
دانشگاه تحصیلات تکمیلی علوم پایه
گاوازنگ - زنجان

کاربردهایی از پایه‌های گروبنر در رمزنگاری

پایان‌نامهٔ کارشناسی ارشد

محمدباقر صفری

استاد راهنما: **دکتر رشید زارع نهندی**

استاد مشاور: **دکتر علی طاهرخانی**

شهریور ۱۳۹۱


بسم الله الرحمن الرحیم

تقدیم به:

مادرم
پدرم
همسرم

و همه کسانی که ریاضی را برای ریاضت نفس خود می‌خوانند و پیش می‌برند.

چکیده

امروزه پایه‌های گروبنر کاربرد وسیعی در حل دستگاه‌های غیر خطی روی میدان‌های متناهی پیدا کرده است. از طرفی تلاش دانشمندان برای ساخت و طراحی سیستم‌های رمز امن، آنها را وادار به حل دستگاه‌هایی از درجه ۲ روی میدان‌های متناهی با تعداد متغیر زیاد واداشته است. در این نوشتار قصد داریم چند سیستم رمز و ارتباط آنها با پایه‌های گروبنر را بررسی کنیم.

واژه‌های کلیدی: *پایه‌های گروبنر، سیستم‌های رمز کلید عمومی چند متغیره*

فهرست

لیست تصاویر

پیش‌گفتار

در این پایان‌نامه سعی شده است با بیانی ساده و در عین حال جامع رمزنگاری و کاربرد پایه‌های گروبنر در آن معرفی شود.

فصل اول به سه بخش تقسیم شده است، در بخش اول بنا را بر آن گذاشته‌ایم که خواننده با مفاهیم جبری آشنایی دارد و فقط برای یادآوری، تعدادی از قضیه‌ها و گزاره‌هایی که در ضمن فصل‌های بعدی به کار خواهند آمد، آورده‌ایم. در زیربخش اول تعریف‌ها و نمادهای پرکاربرد جبری را معرفی نموده‌ایم. در زیربخش دوم به بیان گزاره‌هایی در مورد میدان‌های متناهی پرداخته‌ایم و در نهایت در زیربخش سوم مقدمه‌ای کوتاه از هندسه جبری ارائه داده‌ایم. بسیاری از گزاره‌های این فصل به آسانی قابل اثبات هستند و حتی بعضی از آنها مایه اثبات بقیه هستند. البته ممکن است از نگاه خواننده آوردن تمام این گزاره‌ها ضروری نباشد. در بخش دوم و سوم به طور بسیار مختصر با رمزنگاری و پیچیدگی محاسباتی آشنا می‌شویم. خوانندگانی که با پیچیدگی محاسبه آشنایی دارند می‌توانند از خواندن این بخش صرف نظر کنند.

در فصل دوم نمونه‌هایی از سیستم‌های رمزنگاری از نوع متقارن را شرح داده‌ایم. خواندن این فصل برای فصل‌های بعدی ضروری به نظر می‌رسد، زیرا نمادهایی که برای تعریف این سیستم‌ها استفاده شده است در تمام منابع یکسان نیست و ما در فصل چهارم از نمادهای استفاده شده در این فصل استفاده نموده‌ایم.

در فصل سوم طرح کلی سیستم‌های رمز کلید عمومی چندمتغیره را آورده‌ایم. این سیستم‌ها که می‌توان آنها را از جدیدترین و پرکاربردترین سیستم‌های رمز امروزی دانست، می‌توانند آینده درخشانی در رمزنگاری کلید عمومی داشته باشند. در انتهای این فصل یک نمونه قدیمی و اولیه (که پایه‌ای برای بسیاری از سیستم‌های از این نوع است) معرفی نموده‌ایم. این سیستم گونه‌های مختلفی دارد که حتی

بعضی از آنها امروزه در کارت‌های هوشمند استفاده می‌شوند.

فصل آخر، پایه‌های گروبنر را معرفی می‌کند. پایه‌های گروبنر در حلقه چندجمله‌ای‌ها یک مولد خاص برای یک ایده‌آل داده شده است. در انتهای این فصل به بیان کاربردهایی از پایه‌های گروبنر در تحلیل و طراحی سیستم‌های رمز می‌پردازیم.

فصل اول

مقدّمات و پیشنیازها

در این فصل ابتدا کمی از جبر صحبت خواهیم نمود و بخشی از نمادها، تعاریف و قضایای مورد نیاز را ارائه می‌کنیم. بعد از آن رمزنگاری را با شروع از تاریخچه‌ای کوچک معرفی خواهیم کرد و برخی مفاهیم مورد نیاز در فصل‌های بعدی را مطرح می‌نماییم و در نهایت کمی از پیچیدگی محاسبات بحث می‌کنیم و تا حدّی با طبقه‌بندی مسائل NP و NP-Complete آشنا می‌شویم.

۱.۱ پیشنیازهای جبری

۱.۱.۱ حلقه‌ها و ایده‌آل‌ها

در سراسر این نوشتار منظور از حلقه، حلقه‌ای یکدار و جابه‌جایی است و معمولاً با R نمایش داده می‌شود. ایده‌آل‌ها را معمولاً با I و J نشان می‌دهیم. $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$و $\mathbb{C}$ به ترتیب نماینده اعداد طبیعی، صحیح، گویا، حقیقی و مختلط هستند.

اگر $\underline{X} = x_1, x_2, x_3, \ldots, x_n$ دنباله‌ای از متغیرها باشد، $R[\underline{X}]$ همان حلقه چندجمله‌ای‌ها با ضرایب در R و متغیرهای $x_1, x_2, \ldots, x_n$ خواهد بود، همچنین اگر $F = \{f_1, f_2, \ldots, f_n\} \subseteq R[\underline{X}]$ باشد ایده‌آل تولید شده توسط F را با $< F >=< f_1, f_2, \ldots, f_n >$ نشان می‌دهیم.

عضو $a \neq 0$ از حلقه R را یکه می‌گویند هر گاه عضوی مانند $b \neq 0$ در R موجود باشد که $ab = 1$. عضو ناصفر و غیر یکه $a \in R$ را تحویلناپذیر می‌گوییم هرگاه از هر تجزیه $a = bc; b, c \in R$ نتیجه شود یا b یکه است یا c. حوزه صحیح R را یک حوزه تجزیه یکتا (UFD) می‌گویند هرگاه بتوان هر عضو آن را تا حد ترتیب عوامل و یکه‌ها به صورت یکتا به عناصر تحویلناپذیر تجزیه نمود. می‌دانیم اگر R یک UFD باشد آنگاه $R[x]$ و در نتیجه به استقرا $R[\underline{X}]$نیز UFD خواهد بود.

هر همریختی حلقه‌ای عضو همانی حلقه دامنه را به عضو همانی حلقه برد می‌نگارد. اگر $\varphi : R \mapsto S$ یک همریختی حلقه‌ای باشد، آنگاه هسته φ را با $\varphi^{-1}(0)$ تعریف می‌کنیم و با $\ker(\varphi)$ نشان می‌دهیم. اگر $\psi : \mathbb{Z} \mapsto R$ یکتا همریختی از $\mathbb{Z}$ به R باشد، آنگاه $\ker(\psi)$ ایده‌آلی از $\mathbb{Z}$ خواهد بود و از آنجا که $\mathbb{Z}$ یک حوزه ایده‌آل اصلی (PID) است، $\ker(\psi) = m\mathbb{Z}$ است؛ مشخصه R را با $\mathrm{char}(R) := m$ تعریف می‌کنیم.

حلقه R را نوتری می‌گویند هرگاه هر دنباله صعودی (با رابطه شمول) از ایده‌آل‌ها پایا باشد، به عبارت دیگر اگر

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

دنباله‌ای از ایده‌آل‌های R باشد، $n \in \mathbb{N}$ وجود داشته باشد که $I_n = I_{n+1} = I_{n+2} = \ldots$.

قضیه ۱.۱.۱. (***قضیه پایه هیلبرت***) *اگر R حلقه‌ای نوتری باشد آنگاه $R[x]$ نیز نوتری است.*

اثبات. برای اثبات میتوانید به اکثر کتب جبر جابجایی یا هندسه جبری مانند [۱۲] صفحه ۷ مراجعه نمایید. □

ایده‌آل سره J از حلقه R را ماکسیمال گویند هرگاه اگر I ایده‌آلی از R باشد که $J \subseteq I$ آنگاه یا

$I = R$ یا $I = J$. همچنین ایده‌آل P از R را اول می‌گویند هرگاه اگر $a, b \in R; ab \in P$ آنگاه $a \in P$ یا $b \in P$.

لم ۲.۱.۱. *فرض کنید R یک حلقه و J ایده‌آلی از آن است آنگاه:*

i) J ماکسیمال است اگر و فقط اگر $\frac{R}{J}$ میدان باشد.

ii) J اول است اگر و فقط اگر $\frac{R}{J}$ حوزه صحیح باشد.

قضیه ۳.۱.۱. *فرض کنید R یک حلقه است، شرایط زیر معادلند:*

i) R نوتری است.

ii) هر ایده‌آل R متناهی مولد است.

iii) هر زیرمجموعه از ایده‌آل‌های R دارای عضو ماکسیمال است.

رادیکال ایده‌آل I از حلقه R به صورت

$$\sqrt{I} := \{r \in R;\ \exists n \in \mathbb{N} \quad s.t. \quad r^n \in I\}$$

تعریف می‌شود. اگر $\sqrt{I} = I$ باشد می‌گوییم I یک ایده‌آل رادیکال است.

۲.۱.۱ میدان‌ها

در این زیربخش چند قضیه از میدان‌های متناهی مطرح می‌شود که خواننده می‌تواند برای اثبات آنها به کتاب‌های جبر مرجع مانند [۱۷] یا نظریه میدان مانند [۲۱] مراجعه کند. به هر حال اثبات این قضایا هدف این نوشتار نیست.

حوزه صحیح R را یک میدان گویند هرگاه هر عضو آن یکه باشد. میدان‌ها را معمولا با $\mathbb{F}$، k یا K نمایش می‌دهیم. مشخصه یک میدان همان مشخصه آن به عنوان یک حلقه است. اگر $F \subseteq K$ هر دو میدان باشند، می‌گوییم K یک توسیع (میدانی) F است، همچنین با ضرب اسکالر $\alpha.a = \alpha a$،

K ساختار F-فضای برداری خواهد داشت؛ اگر بُعد K به عنوان F-فضای برداری متناهی باشد، می‌گوییم K یک توسیع متناهی F و در غیر این صورت یک توسیع نامتناهی F است. این بعد را درجه توسیع نیز می‌نامند. فرض کنید $k \subseteq K$ میدان باشند، عضو $a \in K$ را روی k جبری می‌گوییم هرگاه چندجمله‌ای ناصفر $f \in k[x]$ وجود داشته باشد به طوری که $f(a) = ۰$. اگر هر عضو میدان K روی k جبری باشد می‌گویند K یک توسیع جبری k است. اگر k غیر از خودش هیچ توسیع جبری دیگری نداشته باشد، یک میدان بسته جبری خوانده می‌شود.

تعریف ۴.۱.۱. میدان متناهی: میدان k را متناهی می‌گوییم هرگاه $|k| < \infty$.

نکته ۵.۱.۱. میدان‌های متناهی را معمولا با $\mathrm{GF}(q)$ نمایش می‌دهیم، که در آن q همان اندازه میدان است.

لم ۶.۱.۱. *اگر k میدان و $\mathrm{char}(k) = p$ آنگاه یا $p = ۰$ یا p عددی اول خواهد بود.*

قضیه ۷.۱.۱. *فرض کنید k یک میدان متناهی و $\mathrm{char}(k) = p$ است. در این صورت $p \neq ۰$ و $m \in \mathbb{N}$ وجود دارد که $|k| = p^m$.*

قضیه ۸.۱.۱. *اگر k یک میدان متناهی با $|k| = q$ باشد، آنگاه گروه ضربی $k \setminus \{۰\}$ یک گروه دوری از مرتبه $q - ۱$ است.*

تعریف ۹.۱.۱. فرض کنید k یک میدان متناهی است، عضو ناصفر g از k را عضو اولیه (میدانی) k می‌گویند هرگاه مولد گروه دوری $k^* = k \setminus \{۰\}$ باشد.

تعریف ۱۰.۱.۱. فرض کنید k و k' دو میدان هستند. همریختی حلقه‌ای $\iota : k \mapsto k'$ را یک یکریختی میدانی می‌گویند هرگاه یک به یک و پوشا باشد. هرگاه چنین یکریختی‌ای وجود داشته باشد می‌گویند k و k' یکریختند و می‌نویسند $k \cong k'$. اگر $k = k'$ آنگاه ι را یک خودریختی می‌نامند.

قضیه ۱۱.۱.۱. *اگر k و k' دو میدان متناهی باشند که $|k| = |k'|$ آنگاه $k \cong k'$.*

قضیه ۱۲.۱.۱. *اگر k یک میدان متناهی از اندازه q، $m \in \mathbb{N}$ و $y \in k$ باشد، آنگاه معادله $x^m = y$ حداکثر $\gcd(m, q - ۱)$ جواب در k دارد.*

حالا فرض کنید p یک عدد اول است و یک میدان متناهی مانند $\mathbb{F}_p$ داریم. قضایای بعدی طریقه ساخت توسیع‌های میدانی از درجه n را روی $\mathbb{F}_p$ توضیح می‌دهند.

تعریف ۱.۱.۱۳. فرض کنید k یک میدان است. $f \in k[x]$ را یک چندجمله‌ای تحویلناپذیر می‌گویند هرگاه به عنوان عضوی از حلقه $k[x]$ تحویلناپذیر باشد.

چون یکه‌های حلقه $k[x]$ همان یکه‌های k است، چندجمله‌ای $f \in k[x]$ تحویلناپذیر است هرگاه اگر برای $f = gh$، $g, h \in k[x]$ باشد آنگاه یا g عضو k باشد یا h.

قضیه ۱.۱.۱۴. *فرض کنید k یک میدان متناهی است، آنگاه برای هر $n \in \mathbb{N}$ چندجمله‌ای تحویلناپذیر $f \in k[x]$ از درجه n وجود دارد.*

لم ۱.۱.۱۵. *اگر k یک میدان باشد و $f \in k[x]$ یک چندجمله‌ای تحویلناپذیر باشد آنگاه $< f >$ یک ایده‌آل ماکسیمال $k[x]$ است.*

قضیه ۱.۱.۱۶. *فرض کنید k یک میدان متناهی و $p = |k|$ است. همچنین فرض کنید $f \in k[x]$ یک چندجمله‌ای تحویلناپذیر از درجه n باشد. در این صورت $K := \frac{k[x]}{< f >}$ میدانی متناهی از اندازه p^n است و $\mathrm{char}(K) = p$.*

در قضیه فوق K توسیعی از k از درجه n خواهد بود؛ به این معنا که اگر k را با تصویر ثابت‌ها در K معادل در نظر بگیریم، داریم $k \subseteq K$، همچنین از آنجا که f یک چندجمله‌ای از درجه n فرض شده است، هر عضو K به صورت:

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n-1} x^{n-1} + < f >$$

است که در آن α_iها عضو k هستند. بنابراین $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}\}$ یک پایه برای k-فضای برداری K است و در نتیجه K یک توسیع درجه n از k است.

تعریف ۱.۱.۱۷. فرض کنید k یک میدان و $f \in k[x]$ یک چندجمله‌ای تحویلناپذیر از درجه n و $K = \frac{k[x]}{< f >}$ همان توسیع درجه n از k است. نگاشت $\phi : K \mapsto k^n$ را با ضابطه:

$$\phi(\alpha_0 \bar{1} + \alpha_1 \bar{x} + \alpha_2 \bar{x}^2 + \ldots \alpha_{n-1} \bar{x}^{n-1}) = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

یکریختی k-خطی استاندارد بین K و k^n می‌نامند. به وضوح ϕ یک k-فضای برداری یکریختی بین K و k^n است.

مثال ۱.۱.۱۸. می‌خواهیم میدان $\mathrm{GF}(۲^۲)$ را بسازیم. فرض کنید $f = x^۲ + x + ۱ \in \mathbb{F}_۲[x]$ باشد. به وضوح f هیچ ریشه‌ای در $\mathbb{F}_۲$ ندارد و از آنجا که از درجه ۲ است، روی $\mathbb{F}_۲[x]$ تحویلناپذیر است. بنابراین داریم:

$$\mathrm{GF}(۲^۲) = \frac{\mathbb{F}_۲[x]}{< f >} = \{\bar{۰}, \bar{۱}, \bar{x}, \bar{x}^۲\}$$

که دارای جداول جمع و ضرب زیر است:

$+$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{x}^2$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{x}^2$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{x}^2$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\bar{x}^2$	$\bar{0}$	$\bar{1}$
$\bar{x}^2$	$\bar{x}^2$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$*$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{x}^2$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{x}^2$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{x}^2$	$\bar{1}$
$\bar{x}^2$	$\bar{0}$	$\bar{x}^2$	$\bar{1}$	$\bar{x}$

البته محاسبه جدول‌های بالا کار ساده‌ای است و از اینکه $\bar{f} = \bar{x}^۲ + \bar{x} + \bar{۱} = \bar{۰}$ به راحتی نتیجه می‌شود، به عنوان مثال $\bar{x} + \bar{x}^۲ = \bar{۱}$ یا مثلا $\bar{x} * \bar{x}^۲ = \bar{x} * (\bar{۱} + \bar{x}) = \bar{x}^۲ + \bar{x} = \bar{۱}$.

تعریف ۱.۱.۱۹. فرض کنید α روی k جبری است. چندجمله‌ای مونیک (یعنی با ضریب پیشرو ۱) $f \in k[x]$ با کمترین درجه را چندجمله‌ای مینیمال α روی k می‌گویند. این چندجمله‌ای را معمولا با $\min(k, \alpha)$ نمایش می‌دهند.

تعریف ۱.۱.۲۰. فرض کنید K یک توسیع میدانی k و X زیرمجموعه‌ای از آن است. حلقه تولید شده توسط k و X را اشتراک تمام زیرحلقه‌هایی از K که شامل k و X هستند تعریف می‌کنیم و با نماد $k[X]$ نمایش می‌دهیم. به همین ترتیب میدان تولید شده توسط k و X را اشتراک تمام زیرمیدان‌هایی از K که شامل k و X هستند تعریف می‌کنیم و با نماد $k(X)$ نمایش می‌دهیم. اگر $X = \{\alpha\}$ تک عضوی باشد از نماد $k[\alpha]$ یا $k(\alpha)$ استفاده می‌نماییم.

گزاره ۱.۱.۲۱. *فرض کنید K یک توسیع میدانی میدان k و $\alpha \in K$ روی k جبری است، داریم:*

i) چندجمله‌ای $\min(k,\alpha)$ به عنوان عضوی از $k[x]$ تحویل‌ناپذیر است.

ii) اگر $g(x) \in k[x]$ باشد، آنگاه $g(\alpha) = ۰$ اگر و تنها اگر $\min(k,\alpha)$، $g(x)$ را عاد کند.

iii) اگر n درجه $\min(k,\alpha)$ باشد آنگاه $\{۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}\}$ یک پایه برای k-فضای برداری $k(\alpha)$ است. همچنین $k(\alpha) = k[\alpha]$.

تعریف ۲۲.۱.۱. فرض کنید p یک عدد اول است. چندجمله‌ای $f \in \mathrm{GF}(p)[x]$ را یک چندجمله‌ای اولیه می‌نامند هرگاه چندجمله‌ای مینیمال یک عضو اولیه از $\mathrm{GF}(p^m)$ باشد.

نتیجه ۲۳.۱.۱. *فرض کنید $f(x) \in \mathbb{Z}_p[x]$ یک چندجمله‌ای تحویل‌ناپذیر از درجه m است. اگر $\bar{x}$ یک عضو اولیه $\frac{\mathbb{Z}_p[x]}{<f(x)>}$ باشد، آنگاه f یک چندجمله‌ای اولیه است.*

قضیه ۲۴.۱.۱. *فرض کنید k یک میدان متناهی و $|k| = q$ است. اگر $f : k \mapsto k$ تابعی دلخواه باشد، آنگاه $\bar{f} \in k[x]$ از درجه $m < q$ وجود دارد که برای هر $\alpha \in k$ داریم $f(\alpha) = \bar{f}(\alpha)$.*

قضیه بالا به راحتی با استفاده از چندجمله‌ای‌های درونیاب لاگرانژ اثبات می‌شود (می‌توانید به [۱۵] صفحه ۱۲۴ مراجعه کنید.)

تعریف ۲۵.۱.۱. اگر k یک میدان و $\mathrm{char}(k) = ۰$ یا $\mathrm{char}(k) = p$ باشد و هر عضو k ریشه p-ام داشته باشد، آن را یک میدان کامل می‌گویند.

قضیه ۲۶.۱.۱. *فرض کنید k یک میدان متناهی از اندازه $|k| = q$ و K یک توسیع درجه n از آن است. داریم:*

i) برای هر $\alpha \in k$:

$$\alpha^q = \alpha$$

و برای هر $\alpha \in k \setminus \{۰\}$:

$$\alpha^{q-۱} = ۱.$$

ii) *برای هر* $X, Y \in K$

$$(X+Y)^q = X^q + Y^q.$$

iii) *اگر* ι *یک خودریختی روی* K *باشد که برای هر* $\alpha \in k$، $\iota(\alpha) = \alpha$ *آنگاه* $0 < i < n$ *وجود دارد که*

$$\forall X \in K; \qquad \iota(X) = X^{q^i}.$$

حالا فرض کنید k یک میدان متناهی با $\mathrm{char}(k) = p$ است. همریختی $\varphi : k \mapsto k$ با ضابطه $\varphi(\alpha) = \alpha^p$ را در نظر بگیرید. از آنجا که این همریختی ناصفر است به وضوح یک به یک است و از آنجا که k متناهی است، پوشاست، پس φ یک یکریختی است، پس $k = k^p$ بنابراین هر میدان متناهی میدانی کامل است.

۳.۱.۱ هندسه جبری

در این زیربخش نیز مانند قبل با هدف اثبات قضایا جلو نخواهیم رفت و قضایای مطرح شده صرفا برای یادآوری و آشنایی مطرح می‌شوند. برای دیدن اثبات این گزاره‌ها می‌توانید به کتاب‌های مرجع هندسه جبری مانند [۱۲] مراجعه نمایید.

فرض کنید k یک میدان است، n-فضای آفین روی k به صورت

$$\mathbb{A}^n_k := \{(a_1, a_2, a_3, \ldots, a_n);\ a_1, a_2, \ldots, a_n \in k\}$$

تعریف می‌شود. در حالت خاص $n = 1$ آن را خط آفین و در حالت $n = 2$ صفحه آفین می‌نامند. عناصر $\mathbb{A}^n_k$ را نقاط می‌نامند. اگر $\underline{X} = x_1, x_2, x_3, \ldots, x_n$، $f \in k[\underline{X}]$ و $p = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n_k$ باشد به طوری که $f(p) = f(a_1, a_2, \ldots, a_n) = 0$ باشد، می‌گوییم p یک صفر f است. تمام صفرهای f را با $\mathrm{V}(f)$ نمایش می‌دهیم و به آن ابرسطح یا ابررویه می‌گوییم. در حالت کلی‌تر اگر $S \subseteq k[\underline{X}]$ باشد

$\mathrm{V}(S) := \cap_{f\in S}\mathrm{V}(f)$ تعریف می‌شود. اگر S متناهی و برابر $\{f_1, f_2, \ldots, f_m\}$ باشد معمولا به جای $\mathrm{V}(S)$ از $\mathrm{V}(f_1, f_2, \ldots, f_m)$ استفاده می‌نماییم. $X \subseteq \mathbb{A}^n_k$ را یک مجموعه جبری (آفین) می‌خوانند هرگاه $S \subseteq k[\underline{X}]$ موجود باشد که $X = \mathrm{V}(S)$.

ویژگی‌های زیر به راحتی قابل بررسی هستند:

۱) اگر I ایده‌آلی از $k[\underline{X}]$ باشد که توسط S تولید شده باشد آنگاه $\mathrm{V}(S) = \mathrm{V}(I)$ و بنابراین هر مجموعه جبری برابر $\mathrm{V}(I)$ای است.

۲) اگر $\{I_\alpha\}_\alpha$ خانواده‌ای از ایده‌آل‌ها باشد، آنگاه $\mathrm{V}(\cup_\alpha I_\alpha) = \cap_\alpha \mathrm{V}(I_\alpha)$. بنابراین اشتراک هر خانواده‌ای از مجموعه‌های جبری مجموعه‌ای جبری است.

۳) اگر $I \subset J$ آنگاه $\mathrm{V}(J) \subseteq \mathrm{V}(I)$.

۴) اگر $f, g \in k[\underline{X}]$ دو چندجمله‌ای باشند، آنگاه $\mathrm{V}(fg) = \mathrm{V}(f) \cup \mathrm{V}(g)$ پس $= \mathrm{V}(I) \cup \mathrm{V}(J)$ $\mathrm{V}(\{fg; f \in I, g \in J\})$ بنابراین اجتماع هر تعداد متناهی از مجموعه‌های جبری مجموعه‌ای جبری است.

۵) $\mathrm{V}(\circ) = \mathbb{A}^n_k$، $\mathrm{V}(k[\underline{X}]) = \varnothing$ و $\mathrm{V}(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) = (a_1, a_2, \ldots, a_n)$. بنابراین هر زیرمجموعه متناهی از $\mathbb{A}^n_k$ یک مجموعه جبری است.

اگر $X \subseteq \mathbb{A}^n_k$ باشد تعریف می‌کنیم:

$$\mathrm{I}(X) = \{f \in k[\underline{X}];\ \forall p \in X, \quad f(p) = \circ\}$$

به آسانی می‌توان دید که این مجموعه یک ایده‌آل $k[\underline{X}]$ است. $\mathrm{I}(X)$ را ایده‌آل X می‌نامند. موارد زیر به راحتی از این تعریف نتیجه می‌شوند:

۱) اگر $X \subset Y$ آنگاه $\mathrm{I}(Y) \subset \mathrm{I}(X)$.

۲) $\mathrm{I}(\varnothing) = k[\underline{X}]$ و اگر k نامتناهی باشد $\mathrm{I}(\mathbb{A}^n_k) = \circ$. همچنین برای هر $(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n_k$

داریم: $\mathrm{I}(\{(a_1, a_2, \ldots, a_n)\}) =< x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n >$

۳) برای هر مجموعه S از چندجمله‌ای ها $S \subseteq \mathrm{I}(\mathrm{V}(S))$ و برای هر مجموعه X از نقاط $X \subseteq \mathrm{V}(\mathrm{I}(X))$.

۴) برای هر مجموعه از نقاط مانند X، $\sqrt{\mathrm{I}(X)} = \mathrm{I}(X)$ یعنی $\mathrm{I}(X)$ یک ایده‌آل رادیکال است.

با استفاده از روابط بالا و قضیه ۱.۱.۱ و ۳.۱.۱ به قضیه مهم زیر می‌رسیم:

قضیه ۲۷.۱.۱. *هر مجموعه جبری اشتراک تعداد متناهی ابررویه است.*

قضیه ۲۸.۱.۱. (***قضیه ضعیف صفرهای هیلبرت***) *اگر k یک میدان بسته جبری و I ایده‌آل سره ای از $k[\underline{X}]$ باشد، آنگاه $\mathrm{V}(I) \neq \varnothing$.*

قضیه ۲۹.۱.۱. (***قضیه صفرهای هیلبرت***[1]) *اگر k یک میدان بسته جبری و I ایده‌آل سره ای از $k[\underline{X}]$ باشد، آنگاه $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$.*

نتیجه ۳۰.۱.۱. *فرض کنید k یک میدان بسته جبری و $I \subseteq k[\underline{X}]$ ایده‌آلی رادیکال است. در این صورت $\mathrm{I}(\mathrm{V}(I)) = I$. بنابراین یک تناظر یک به یک بین ایده‌آل‌های رادیکال $k[\underline{X}]$ و مجموعه‌های جبری $\mathbb{A}^n_k$ وجود دارد. همچنین در این تناظر ایده‌آل‌های ماکسیمال با مجموعه‌های جبری تک نقطه‌ای در تناظرند.*

نتیجه ۳۱.۱.۱. *فرض کنید k یک میدان بسته جبری و $I \subseteq k[\underline{X}]$ یک ایده‌آل است. در این صورت $\mathrm{V}(I)$ متناهی است اگر و فقط اگر بعد k-فضای برداری $\frac{k[\underline{X}]}{I}$ متناهی باشد. اگر چنین باشد آنگاه اندازه $\mathrm{V}(I)$ حداکثر $\dim_k(\frac{k[\underline{X}]}{I})$ خواهد بود.*

اثبات. $\Rightarrow$: فرض کنید $p_1, p_2, \ldots, p_r \in \mathrm{V}(I)$ است. نشان می‌دهیم $r \leq \dim_k(\frac{k[\underline{X}]}{I})$. از آنجا که برای هر $j = 1, 2, \ldots, r$، $\mathrm{I}(\{p_1, \ldots, p_r\}) \neq \mathrm{I}(\{p_1, \ldots, p_r\} \setminus \{p_j\})$ (زیرا در غیر این صورت از جبری بودن مجموعه‌های متناهی و ویژگی سوم $\mathrm{I}()$ به تناقض می‌رسیم.) پس چندجمله‌ای f_j وجود

[1] Hilbert's Nullstellnsatz