دانشگاه کاشان

دانشکده علوم

گروه ریاضی

پایان نامه

جهت اخذ درجه ی کارشناسی ارشد در رشته ی ریاضی-جبر

عنوان:

کلاسهای هم ارزی خمهای ابربیضوی با گونای ۲
و کاربردهای آن در رمزنگاری

استاد راهنما:

دکتر حسن دقیق

توسط:

امیرمهدی یزدانی

اسفند ماه ۱۳۸۷

تقدیم به

پدر و مادر عزیزم

که چراغ راه زندگانی‌ام هستند.

تقدیر و سپاس

سپاس خدای راست عزوجل که طاعتش موجب قربت است و به شکر اندرش مزید نعمت.

بر خود لازم می‌دانم از تمامی اساتید بزرگوار به ویژه اساتید دوره‌ی کارشناسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت و فضایل اخلاقی یاری نموده‌اند تقدیر و تشکر نمایم.

از استاد گرامی و بزرگوار جناب آقای **دکتر حسن دقیق** که راهنمایی اینجانب را در انجام تحقیق، پژوهش و نگارش این پایان‌نامه پذیرفتند نهایت تشکر و سپاسگزاری را دارم.

همچنین از جناب آقای **دکتر رضا جهانی نژاد** به عنوان استاد داور داخل دانشگاه و جناب آقای **دکتر مرتضی میرمحمدرضایی** به عنوان استاد مدعو خارج از دانشگاه که این پایان‌نامه را مورد مطالعه قرار داده و در جلسه‌ی دفاع شرکت نمودند تشکر می‌نمایم. در پایان از جناب آقای **دکتر علی اکبر عباسیان** که به عنوان نماینده‌ی تحصیلات تکمیلی دانشگاه قبول زحمت نموده‌اند سپاسگزاری می‌نمایم.

امیرمهدی یزدانی

اسفند ۱۳۸۷

چکیده

در این پایان‌نامه ابتدا به معرفی خم‌های جبری و گونای آن‌ها می‌پردازیم. سپس خم‌های ابربیضوی و ژاکوبین آن‌ها و مسئله‌ی لگاریتم گسسته روی ژاکوبین یک خم ابربیضوی را مورد بررسی قرار خواهیم داد. پس از آن یک معادله‌ی جایگزین برای خم‌های ابربیضوی از گونای ۲ روی میدان‌های متناهی با مشخصه‌ی مخالف ۲ و ۵ ارائه خواهیم داد.

در پایان به یافتن تعداد کلاس‌های ایزومورفیسم خم‌های ابربیضوی از گونای ۲ روی میدان متناهی با فرض دارابودن یک نقطه‌ی وایرشتراس پرداخته راهکار ارائه شده را برای گونای ۳ نیز به‌کار خواهیم گرفت.

کلمات کلیدی: خم ابربیضوی، ژاکوبین، رمزنگاری، مسئله‌ی لگاریتم گسسته، برآیند و مبیّن

فهرست مندرجات

مقدمه

رمزنگاری دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره‌ی اطلاعات به صورت امن حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره‌ی اطلاعات ناامن باشند می‌پردازد. رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد نتواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه‌ی مقدمات بسیاری از قبیل تئوری‌اطلاعات، نظریه‌اعداد و آمار بنا شده است و امروزه به‌طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد.

معادل رمزنگاری در زبان انگلیسی کلمه‌ی $cryptography$ است که برگرفته از لغات یونانی $kryptos$ به مفهوم ((محرمانه)) و $graphien$ به معنای ((نوشتن)) است.

در گذشته سازمان‌ها و شرکت‌هایی که نیاز به رمزگذاری یا سرویس‌های دیگر رمزنگاری داشتند، الگوریتم رمزنگاری منحصربه‌فردی را طراحی می‌نمودند. به مرور زمان مشخص گردید که گاهی ضعف‌های امنیتی بزرگی در این الگوریتم‌ها وجود دارد که موجب سهولت شکسته شدن رمز می‌شود. به همین دلیل امروزه رمزنگاری مبتنی بر

پنهان داشتن الگوریتم، رمزنگاری منسوخ شده است و در روش‌های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده است و آنچه پنهان است فقط کلید رمز است. بنابراین تمام امنیت حاصل شده از الگوریتم‌ها متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم‌ها برای عموم منتشر می‌شود.

یکی از مهمترین این الگوریتم‌ها، الگوریتم‌های مبتنی بر لگاریتم گسسته است و علم رمزنگاری همواره در حال پیچیده‌تر کردن مسئله‌ی لگاریتم گسسته و در عین حال ابداع راه‌هایی برای حل آن می‌باشد. در این میان خم‌های ابربیضوی از گونای ۲ و ۳ و کاربرد مسئله‌ی لگاریتم گسسته روی ژاکوبین آن‌ها دارای اهمیت خاصی هستند و شناخت هر چه بیشتر آن‌ها باعث بازشدن دریچه‌های جدیدی در علم رمزنگاری می‌شود.

در این پایان‌نامه در فصل اول به معرفی واریته‌ها و خم‌ها می‌پردازیم و در این میان خم‌های بیضوی را معرفی می‌کنیم. در پایان فصل اول به بیان قضیه‌ی ریمان راخ و مفهوم گونا می‌پردازیم. البته اثبات بیشتر قضایای فصل اول به دلیل این‌که نیاز به معرفی پیش‌نیازهای زیادی دارد و این کار باعث دور شدن از مسیر اصلی بحث می‌گردد به منابع ذکر شده ارجاع داده شده است و خواننده‌ی علاقه‌مند می‌تواند به کتاب‌هایی همچون ($Hartshorne$[۱۲]) و($Silverman$[۱۹]) مراجعه نماید.

فصل دوم از دو بخش تشکیل شده است. در بخش اول مفاهیم اساسی درباره‌ی خم ابربیضوی و فرم وایرشتراس و بخشیاب یک خم ابربیضوی را بیان می‌کنیم و مطالعه‌ی آن برای فهم مطالب بعدی ضروری است. در بخش دوم دو روش محاسباتی را بیان می‌کنیم که می‌توانند در رمزنگاری با استفاده از خم‌های ابربیضوی مفید واقع شوند.

در ابتدای فصل سوم اهمیت خم‌های ابربیضوی با گونای ۲ و ۳ و ۴ را در رمزنگاری بیان می‌کنیم. بنابراین یافتن تعداد این خمها اهمیت زیادی می‌یابد. پس از تعریف مفهوم هم‌ارزی دو خم، یک معادله‌ی جایگزین برای خم ابربیضوی از گونای ۲ روی میدان‌های متناهی با مشخصه‌ی مخالف ۲ و ۵ ارائه می‌دهیم. همچنین قضایای مربوط به یافتن تعداد کلاسهای ایزومورفیسم از گونای ۲ وقتی‌که مشخصه‌ی میدان متناهی مورد نظر ۲ و ۵ است را در این بخش بدون اثبات آورده‌ایم. در پایان این فصل به شمردن تعداد کلاس‌های ایزومورفیسم خم‌های ابربیضوی وقتی‌که مشخصه‌ی میدان متناهی مورد نظر مخالف ۲ و ۵ است پرداخته‌ایم.

در فصل چهارم به یافتن تعداد کلاس‌های ایزومورفیسم خم‌های ابربیضوی از گونای ۳ وقتی‌که مشخصه‌ی میدان متناهی مخالف ۲ و ۷ است با استفاده از روشی مشابه با فصل قبل پرداخته‌ایم. در حالاتی که مشخصه‌ی میدان متناهی برابر ۲ یا ۷ است تنها به آوردن قضایای مربوط بسنده کرده‌ایم.

در پایان بر خود لازم می‌دانم از استاد عزیز و بزرگوار جناب آقای **دکتر دقیق** به خاطر تمامی راهنمایی‌های ایشان تشکر کنم. به‌راستی که اگر راهنمایی‌های ایشان نبود نمی‌توانستم برای برخی از سوالاتی که در روند این پایان‌نامه برایم پیش می آمد جوابی پیدا کنم. برای ایشان آرزوی سرفرازی و موفقیت دارم.

امیر مهدی یزدانی

زمستان ۸۷

فصل ۱

مقدمات و پیش‌نیازها

این فصل از دو بخش تشکیل شده است. دربخش اول این فصل به معرفی واریته‌ها پرداخته و نگاشت‌های میان واریته‌ها را مورد بررسی قرار می‌دهیم. در بخش دوم به معرفی خم‌های جبری و نگاشت‌های میان آن‌هاپرداخته، نوع خاصی از این خم‌ها بنام خم‌های بیضوی را مورد بحث قرار می‌دهیم. همچنین بخشیاب‌های یک خم و فضای فرم‌های دیفرانسیل و قضیه‌ی ریمان‌راخ مفاهیمی هستند که در این بخش آورده شده‌اند و مطالعه‌ی آن‌ها برای فهم مطالب بعدی ضروری است. خواننده‌ی علاقه‌مند برای بررسی بیشتر درباره‌ی مباحثی که در این فصل بیان شده می‌تواند به کتاب‌های هندسه‌ی‌جبری مراجعه نماید.

۱.۱ واریته‌ها

این بخش را با معرفی واریته‌های آفین آغاز می‌کنیم. پس از آن به واریته‌های تصویری که از اضافه نمودن نقاط در بینهایت به واریته‌های آفین به‌دست می‌آیند پرداخته و در پایان این بخش نگاشت‌های میان واریته‌ها در فضاهای تصویری را بررسی می‌کنیم.

۱.۱.۱ واریته‌های آفین

تعریف ۱.۱ فرض کنیم K یک میدان کامل است یعنی هر توسیع جبری K تفکیک‌پذیر می‌باشد و $\bar{K}$ بستار جبری K است. منظور از $n-$ **فضای آفین** روی K مجموعه‌ی n تایی‌های

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \left\{p = (x_1, \ldots, x_n) : x_i \in \bar{K}\right\}$$

می‌باشد. به‌طور مشابه **نقاط** K **گویا** در $\mathbb{A}^n$ به صورت

$$\mathbb{A}^n(K) = \{p = (x_1, \ldots, x_n) : x_i \in K\}$$

تعریف می‌شود.

تعریف ۲.۱ فرض کنیم $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$ حلقه‌ی چندجمله‌ای‌های n متغیره باشد. فرض کنیم $I \subseteq \bar{K}[X]$ یک ایده‌آل باشد. برای هر چنین I ای زیرمجموعه‌ی زیر

از $\mathbb{A}^n$ را تعریف می‌کنیم:

$$V_I = \{p \in \mathbb{A}^n : f(p) = 0; \forall f \in I\}$$

منظور از **مجموعه‌ی جبری آفین** هرمجموعه به شکل V_I است.

مثال ۳.۱ مجموعه صفر یک چندجمله‌ای خطی درجه یک در $K[X_1, \dots, X_n]$، یک مجموعه‌ی جبری آفین است که یک ابرصفحه‌ی آفین خوانده می‌شود. به‌ویژه اگر $f(x,y) = ax + by + c \in K[x,y]$ و I ایده‌آل پدیدآمده توسط f باشد آن‌گاه V_I یک خط در صفحه‌ی $\mathbb{A}^2$ است.

تعریف ۴.۱ اگر V یک مجموعه‌ی جبری باشد ایده‌آل $I(V)$ را به‌صورت زیر تعریف می‌کنیم:

$$I(V) = \left\{f \in \bar{K}[X] : f(p) = 0 : \forall p \in V\right\}$$

$\bar{K}$ میدان و بنابراین حلقه‌ای نوتری است. لذا بنا به قضیه‌ی پایه‌ای هیلبرت $\bar{K}[X]$ نیز نوتری است و چون $I(V)$ ایده‌آلی از $\bar{K}[X]$ می‌باشد بنابراین متناهی مولد است. می‌گوییم مجموعه‌ی جبری V روی K تعریف می‌شود اگر ایده‌آل $I(V)$ توسط چندجمله‌ای‌هایی از $K[X]$ تولید شود و آن را با V/K نمایش می‌دهیم.

تعریف ۵.۱ مجموعه‌ی جبری آفین V را **واریته‌ی آفین** می‌نامیم اگر $I(V)$ ایده‌آلی اول در $\bar{K}[X]$ باشد.

تذکر ۶.۱ اگر V روی K تعریف شده باشد بررسی اول بودن $I(V/K)$ کافی نیست. به‌عنوان مثال ایده‌آل $\langle X_1^2 - 2X_2^2 \rangle$ را در $\mathbb{Q}[X_1, X_2]$ در نظر می‌گیریم. چون $\mathbb{Q}[X_1, X_2]$ یک دامنه‌ی تجزیه‌ی یکتاست و چندجمله‌ای $X_1^2 - 2X_2^2$ در $\mathbb{Q}[X_1, X_2]$ تحویلناپذیر است ایده‌آل $\langle X_1^2 - 2X_2^2 \rangle$ ایده‌آلی اول در $\mathbb{Q}[X_1, X_2]$ است. ولی مشاهده می‌کنیم که چندجمله‌ای $X_1^2 - 2X_2^2$ در $\bar{\mathbb{Q}}[X_1, X_2]$ تحویل‌پذیر است.

$$X_1^2 - 2X_2^2 = (X_1 - \sqrt{2}X_2)(X_1 - \sqrt{2}X_2)$$

تعریف ۷.۱ فرض کنید V/K یک واریته باشد. در این صورت **حلقه‌ی مختصات آفین** V/K که به صورت زیر تعریف می‌شود دامنه‌ی صحیح است.

$$K[V] = K[X]/I(V/K)$$

و میدان خارج قسمتی آن که با $K(V)$ نمایش داده می‌شود را **میدان تابعی** V/K گوییم.

تعریف ۸.۱ فرض کنیم V یک واریته باشد. منظور از **بعد** V که با $dim(V)$ نمایش داده می‌شود درجه‌ی تعالی $\bar{K}(V)$ روی $\bar{K}$ است.

تعریف ۹.۱ فرض کنیم V یک واریته و $p \in V$ باشد. ایده‌آل M_p از $\bar{K}[V]$ را به صورت زیر تعریف می‌کنیم:

$$M_p = \left\{ f \in \bar{K}[V] : f(p) = 0 \right\}$$

همریختی

$$\phi : \bar{K}[V] \longrightarrow \bar{K}$$
$$\phi(f) = f(p)$$

یک همریختی پوشاست و $Ker\phi = M_p$. لذا بنابه قضیه‌ی اول یکریختی $\bar{K}[V]/M_p \simeq \bar{K}$ و بنابراین M_p یک ایده‌آل ماکسیمال از $\bar{K}[V]$ می‌باشد. همچنین توجه می‌کنیم که خارج قسمت $M_p/M_p^{۲}$ فضای برداری متناهی بعد روی $\bar{K}$ است. زیرا $\bar{K}$ یک میدان و لذا نوتری است. بنابراین $\bar{K}[V] = \bar{K}[X]/I(V/K)$ نیز نوتری است و لذا M_p به‌عنوان ایده‌آلی از $\bar{K}[V]$ متناهی مولد است.

مثال ۱۰.۱ بعد $\mathbb{A}^n$، n است. زیرا $\bar{K}(\mathbb{A}^n) = \bar{K}(X_۱, \ldots, X_n)$. به‌طور مشابه اگر $V \subseteq \mathbb{A}^n$ با معادله‌ی یک چندجمله‌ای ناثابت $f(X_۱, \ldots, X_n) = ۰$ داده شده باشد، $dim(V) = n - ۱$. عکس این مطلب نیز درست است. برای بررسی به گزاره‌ی ۷.۱ از فصل اول [۱۲] مراجعه کنید.

تعریف ۱۱.۱ فرض کنیم V یک واریته و $p \in V$ و $f_۱, \ldots, f_m \in \bar{K}[X]$ مجموعه‌ی مولدهای $I(V)$ باشند. در این صورت V را در p **غیرمنفرد** گوییم اگر ماتریس $(\frac{\partial f_i}{\partial x_j}(p))_{۱\leq i\leq m, ۱\leq j\leq n}$ دارای رتبه‌ی $n - dim(V)$ باشد.

قضیه ۱۲.۱ فرض کنیم V یک واریته باشد. نقطه‌ی $p \in V$ غیرمنفرد است اگر و تنها اگر

$$dim M_p/M_p^{۲} = dim V$$

اثبات. به قضیه‌ی ۵.۱ از فصل اول [۱۲] مراجعه کنید. □

مثال ۱۳.۱ فرض کنید V با معادله‌ی چندجمله‌ای ناثابت $f(X_1, \ldots, X_n) = 0$ داده شده باشد. در این صورت $dim(V) = n - 1$ و لذا $p \in V$ تکین است اگر و تنها اگر

$$\frac{\partial f}{\partial X_1}(p) = \cdots = \frac{\partial f}{\partial X_n}(p) = 0$$

چون $f(p) = 0$ است، $n + 1$ معادله برای n مختصات نقطه تکین به‌دست می‌آید. بنابراین با انتخاب تصادفی f می‌توان انتظار داشت که V ناتکین باشد.

مثال ۱۴.۱ دو واریته زیر را درنظر بگیرید:

$$V_1 : Y^2 = X^3 + X$$
$$V_2 : Y^2 = X^3 + X^2$$

ابتدا نقطه‌ی $p = (0, 0)$ را روی واریته‌ی V_1 در نظرمی‌گیریم. لذا M_p ایده‌آلی از $\bar{K}[V_1] = \frac{\bar{K}[X, Y]}{\langle Y^2 - X^3 - X \rangle}$ تولید شده توسط X و Y است و M_p^2 ایده‌آل تولید شده توسط X^2، XY و Y^2 است. داریم:

$$X = Y^2 - X^3 \overset{M_p^2}{\equiv} 0$$

لذا M_p/M_p^2 تنها با Y تولید می‌شود. با توجه به این که V_1 دارای بعد یک می‌باشد از قضیه‌ی ۱۲.۱ نتیجه می‌شود که V_1 در p غیرمنفرد است.

اکنون همین نقطه را روی واریته‌ی V_2 در نظر می‌گیریم. به‌طور مشابه M_p ایده‌آلی از $\bar{K}[V_2] = \frac{\bar{K}[X, Y]}{\langle Y^2 - X^3 - X^2 \rangle}$ تولیدشده توسط X و Y است و M_p^2 ایده‌آل تولیدشده توسط X^2، XY و Y^2 است. ولی برای V_2 رابطه‌ای نابدیهی میان X و Y به پیمانه‌ی M_p^2 موجود نیست و لذا M_p/M_p^2 هم به X و هم به Y به عنوان مولد نیاز دارد. از آنجا که V_2 نیز دارای بعد یک می‌باشد بنا به قضیه‌ی ۱۲.۱ V_2 در p منفرد است.

البته آنچه که گفتیم را می‌توان به راحتی به کمک تعریف ۱۱.۱ نیز بررسی کرد.

تعریف ۱۵.۱ **حلقه‌ی موضعی** V در p که با $\bar{K}[V]_p$ نشان می‌دهیم موضعی‌سازی $\bar{K}[V]$ در M_p می‌باشد. به عبارت دیگر

$$\bar{K}[V]_p = \left\{F \in \bar{K}(V) : \exists f, g \in \bar{K}[V]; g(p) \neq 0, F = \frac{f}{g}\right\}$$

۲.۱.۱ واریته‌های تصویری

تعریف ۱۶.۱ بر $\mathbb{A}^{n+1} - \{0\}$ رابطه‌ی هم ارزی را این چنین تعریف می‌کنیم:
دو $n+1$ تایی $(x_0, \ldots, x_n)$ و $(y_0, \ldots, y_n)$ در $\mathbb{A}^{n+1} - \{0\}$ هم‌ارز نامیده می‌شوند اگر $\lambda \in \bar{K}$ موجود باشد به‌طوری‌که برای هر $0 \leq i \leq n$ داریم

$$x_i = \lambda y_i$$

کلاس هم‌ارزی شامل $(x_0, \ldots, x_n)$ را با $[x_0, \ldots, x_n]$ نمایش می‌دهیم.

نمادگذاری ۱۷.۱ مجموعه‌ی کلاس‌های هم‌ارزی رابطه‌ی تعریف‌شده در بالا را $n-$ **فضای تصویری** روی K می‌نامیم و با $\mathbb{P}^n(\bar{K})$ یا $\mathbb{P}^n$ نشان می‌دهیم.

تعریف ۱۸.۱ به‌طور مشابه $\mathbb{P}^n(K)$ این چنین تعریف می‌شود:

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \in K\}$$

توجه کنید اگر $p=[x_\circ,\dots,x_n]\in\mathbb{P}^n(K)$ نتیجه نمی‌شود که هر $x_i\in K$. بلکه این مطلب را نتیجه می‌دهد که $[y_\circ,\dots,y_n]\in\mathbb{P}^n(K)$ موجود است به‌طوری‌که $[x_\circ,\dots,x_n]=[y_\circ,\dots,y_n]$ و داریم:

$$\forall \circ\le i\le n \qquad y_i\in K$$

تعریف ۱۹.۱ چندجمله‌ای $f\in\bar{K}[X]=\bar{K}[X_\circ,\dots,X_n]$ را **همگن** از درجه‌ی d گوییم اگر برای هر $\lambda\in\bar{K}$

$$f(\lambda x_\circ,\dots,\lambda x_n)=\lambda^d f(x_\circ,\dots,x_n)$$

تعریف ۲۰.۱ ایده‌آل $I\subseteq\bar{K}[X]$ را **همگن** گوییم اگر دارای یک مجموعه‌ی مولد از چندجمله‌های همگن در $\bar{K}[X]$ باشد.

قضیه ۲۱.۱ فرض کنیم $f\in\bar{K}[X]$ یک چندجمله‌ای همگن و

$$(x_\circ,\dots,x_n)\sim(y_\circ,\dots,y_n)$$

و $f(x_\circ,\dots,x_n)=\circ$، آن‌گاه $f(y_\circ,\dots,y_n)=\circ$.

اثبات. چون $(x_\circ,\dots,x_n)=(y_\circ,\dots,y_n)$ بنابراین

$$\exists\lambda\in\bar{K}^* \qquad \text{به‌طوری‌که} \qquad (x_\circ,\dots,x_n)=(\lambda y_\circ,\dots,\lambda y_n)$$

لذا

$$\circ=f(x_\circ,\dots,x_n)=f(\lambda y_\circ,\dots,\lambda y_n)=\lambda^d f(y_\circ,\dots,y_n)$$

بنابراین

$$f(y_\circ,\dots,y_n)=\circ$$

□

تعریف ۲۲.۱ برای هر ایده‌آل همگن I زیرمجموعه‌ای از $\mathbb{P}^n$ را مربوط می‌کنیم:

$$V_I = \left\{p \in \mathbb{P}^n; f(p) = 0, f \in I \text{ برای هر چندجمله‌ای همگن} \right\}$$

هر مجموعه به شکل V_I را یک **مجموعه‌ی جبری تصویری** گوییم.

اگر V مجموعه‌ی جبری تصویری باشد ایده‌آل همگن V که با $I(V)$ نشان می‌دهیم ایده‌آلی در $\bar{K}[X]$ است که توسط

$$\{f \in \bar{K}[X]; f(p) = 0 \quad \forall p \in V \text{ ، همگن است} f\}$$

تولید می‌شود. چنین V را تعریف شده روی K گوییم و با V/K نمایش می‌دهیم اگرایده‌آل $I(V)$ را بتوان توسط چندجمله‌ای‌های همگن در $K[X]$ تولید کرد.

مثال ۲۳.۱ یک خط در $\mathbb{P}^2$ یک مجموعه‌ی جبری با معادله‌ی خطی

$$aX + bY + cZ = 0$$

می‌باشد که $a, b, c \in \bar{K}$، همگی صفر نیستند. اگر $c \neq 0$ چنین خطی روی هر میدان شامل $\frac{a}{c}$ و $\frac{b}{c}$ تعریف شده است. به طور کلی‌تر یک ابرصفحه در $\mathbb{P}^n$ با معادله‌ی

$$a_0 X_0 + a_1 X_1 + \cdots + a_n X_n = 0$$

که a_i ها همگی صفر نیستند مشخص می‌شود.

تعریف ۲۴.۱ **میدان توابع واریته تصویری** V که با $\bar{K}(V)$ نشان می‌دهیم میدان توابع گویای V از توابع گویا به‌صورت $F(X) = \frac{f(x)}{g(x)}$ است به‌طوری‌که

۱) f و g همگن از درجه‌ی یکسانند.

۲) $g \notin I(V)$

۳) توابع $\frac{f}{g}$ و $\frac{f'}{g'}$ برابرند اگر $fg' - g'f \in I(V)$

۳.۱.۱ نگاشت‌های میان واریته‌ها

تعریف ۲۵.۱ فرض کنیم $V_1, V_2 \subseteq \mathbb{P}^n$ واریته‌های تصویری باشند. یک **نگاشت گویا** از V_1 به V_2 یک نگاشت به فرم

$$\begin{aligned} \phi &: V_1 \longrightarrow V_2 \\ \phi &= [f_0, \ldots, f_n] \end{aligned}$$

می‌باشد چنان‌که $f_0, \ldots, f_n \in \bar{K}(V_1)$ و برای هر $p \in V_1$ که در آن تعریف شده‌اند داریم:

$$\phi(p) = [f_0(p), \ldots, f_n(p)] \in V_2$$

اکنون اگر $\lambda \in \bar{K}^*$ موجود باشد چنان‌که

$$\lambda f_0, \ldots, \lambda f_n \in K(V_1)$$

گوییم ϕ روی K تعریف شده است. توجه کنید که در این صورت $[f_0, \ldots, f_n]$ و $[\lambda f_0, \ldots, \lambda f_n]$ نگاشت‌های یکسانی را روی نقاط مشخص می‌کنند.

تعریف ۲۶.۱ نگاشت گویای

$$\begin{aligned} \phi &: V_1 \longrightarrow V_2 \\ \phi &= [f_0, \ldots, f_n] \end{aligned}$$

را در $p \in V_1$ **منظم** گوییم اگرتابع $g \in \bar{K}(V_1)$ موجود باشد که

۱) هر gf_i در p تعریف شده باشد.

۲) i ای موجود باشد که $(gf_i)(p) \neq 0$