بسم الله الرحمن الرحيم

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

خم‌های ماکزیمال روی میدان‌های متناهی از مشخصهٔ دو

پایان‌نامهٔ کارشناسی ارشد

زهرا خرقانی

استاد راهنما: دکتر سعید تفضلیان

مهر ۱۳۸۹

تقدیم به پدر و مادرم عزیزم
به پاس محبت‌های بی‌دریغشان

قدردانی و تشکر

تا چشم بر هم زدیم ۲ سال تمام شد. خداوند را شاکرم که انجام این کار را نصیب من نمود. بر خود لازم می‌دانم که از همهٔ عزیزانی که مرا در این راه همراهی نمودند قدردانی نمایم.

ابتدا از استاد عزیز و بزرگوار خود جناب دکتر سعید تفضلیان برای تمام درس‌هایی که به من آموختند و همراهی و مساعدت ایشان در طی تحقیق و تدوین پایان‌نامه کمال تشکر را دارم.

از اساتید محترم گروه ریاضی به‌خصوص دکتر ورسایی و دکتر میرزائی نیز خاضعانه سپاس‌گزارم.

از خانواده عزیزم به خاطر حمایت‌های عاشقانه‌شان در تمام دوران زندگی‌ام کمال تشکر را دارم. و همچنین از دوستان عزیزم، خانم‌ها سیما یوسفی، لاله ملازاده، بیان نامی، زهرا احمدی، بهناز قربانلو، رقیه رهبرفام، شیما شفقت، مهناز علوی نژاد، مینا پیری و آقایان مسعود عطائی، سجاد زارع و سایر دوستان عزیزم که با حمایت‌های بی‌دریغشان در طول دوران تحصیل برای من خاطراتی زیبا آفریدند، صمیمانه تشکر نموده و برایشان آرزوی سلامتی و پیروزی دارم.

چکیده

فرض می‌کنیم خم χ، یک خم ماکسیمال از گونای g روی میدان متناهی F_{q^2} باشد. گونای خم ماکسیمال روی میدان F_{q^2} برابر $g \leq g_1 := q(q-1)/2$ یا

$$g \leq g_2 := \begin{cases} (q-1)^2/4 & \text{اگر} q \text{ فرد باشد} \\ q(q-2)/4 & \text{اگر} q \text{زوج باشد} \end{cases}$$

است. خم ماکسیمال با گونای g_1، خم هرمیتی با رابطهٔ $y^q + y = x^{q+1}$ است. تنها خم ماکسیمال با گونای g_2 و q فرد، با $y^q + y = x^{q+1/2}$ داده می‌شود. در این پایان نامه نشان داده می شودکه یک خم F_{q^2}—ماکسیمال با گونای g_2 و q زوج، F_{q^2}—یکریخت با خم مسطح ناتکین $\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$ است، مشروط بر اینکه $q/2$ یک غیرنقصان وایرشتراس در بعضی از نقاط خم باشد.

فهرست

۲ نیم گروه‌های وایرشتراس و مرتبه‌های فروبنیوس

۳ تابع زتا و قضیهٔ هسه—ویل

۴ خم های ماکسیمال

مقدمه

در این پایان نامه مرجع اصلی، [۲] است.

خم χ را یک خم تصویری، تحویل ناپذیر و ناتکین روی میدان متناهی F_ℓ با ℓ عنصر در نظر می‌گیریم. فرض می‌کنیم $\chi(F_\ell)$ مجموعهٔ نقاط گویای خم χ روی F_ℓ باشد. هسه[۱] برای خم‌های بیضوی [۲] ثابت کرد تعداد نقاط گویای خم χ با گونای g، در رابطهٔ

$$\#\chi(F_\ell) \leq \ell + 1 + 2g\sqrt{\ell}$$

صدق می‌کند. و ویل آن را برای همهٔ خم‌ها ثابت کرد. بنابراین رابطهٔ بالا، رابطهٔ هسه—ویل نام گرفت. اگر تعداد نقاط گویای خم χ، برابر کران بالای رابطهٔ هسه—ویل باشد، آنگاه خم χ ماکسیمال گفته می‌شود. البته توجه می‌کنیم که در این حالت ℓ باید مربع کامل باشد. پس فرض می‌کنیم $\ell = q^2$. بنابراین اگر χ ماکسیمال باشد، آنگاه

$$\#\chi(F_{q^2}) = q^2 + 1 + 2qg.$$

علاقه به مطالعهٔ خم‌ها روی میدان‌های متناهی، از زمانی که گوپا [۳] کاربردهای این خم‌ها به‌ویژه خم‌های ماکسیمال را در نظریهٔ کد[۴] بیان کرد، افزایش یافت و بعد از آن به‌طور جدی مورد توجه قرار گرفت.

مهمترین ویژگی خم‌های ماکسیمال، وجود سری خطی مستقل از پایهٔ $\mathcal{D}_\chi := |(q+1)P_0|$ که $P_0 \in \chi(F_{q^2})$، با ویژگی‌های زیر است:

(الف) $qP + Fr_\chi(P) \in \mathcal{D}_\chi$

(ب) $\mathcal{D}_\chi$ ساده است

(پ) $\dim(\mathcal{D}_\chi) \geq 2$.

که Fr_χ، نگاشت فروبنیوس [۵] خم χ روی میدان F_{q^2} است.

---

[۱] Hasse

[۲] elliptic

[۳] Goppa

[۴] Coding Theory

[۵] Frobenius

در این پایان‌نامه به موارد زیر می‌پردازیم:

در فصل اول مفاهیم پایه‌ای مانند میدان تابع و حلقه‌های ارزیاب، خم‌های جبری، بخشیاب‌ها، سری‌های خطی روی خم‌ها، رابطهٔ بین سری‌های خطی و ریخت‌ها، فرمول گونای هورویتس[۶] و همچنین ناورداهای هرمیتی و مشتق‌های هسه را مطرح می‌کنیم.

سپس در فصل دوم، با دنبالهٔ مرتبه‌ها، بخشیاب انشعاب و $\mathcal{D}$–فضاهای اشتراک آشنا می‌شویم. در ادامه مفاهیم اساسی نیم‌گروه‌های وایرشتراس را معرفی می‌کنیم و بعد از آن مرتبه‌های فروبنیوس را مطرح می‌کنیم.

در فصل سوم تابع زتای یک میدان را معرفی می‌کنیم و از طریق آن فرض ریمان را نشان می‌دهیم. در ادامهٔ فصل سوم نشان می‌دهیم خم هرمیتی با رابطهٔ $y^q + y = x^{q+1}$، تنها خم ماکسیمال با گونای $q(q-1)/2$ است و برخی از خواص این خم را مطالعه می‌کنیم. گارسیا[۷] و تورس[۸] در مرجع [۶] نشان دادند، تنها خم ماکسیمال با گونای $(q-1)^2/4$، q فرد، خم $y^q + y = x^{q+1/2}$ است.

در فصل چهارم که هدف اصلی پایان‌نامه است ثابت می‌کنیم خم ماکسیمال با گونای $q(q-2)/4$، q زوج، همریخت با خم ناتکین زیر است:

$$\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$$

که $q = 2^t$ و $q/2$ یک غیرنقصان وایرشتراس در هر نقطهٔ دلخواه از خم است.

در اثبات این قضیه، سری خطی متناظر با خم χ و مرتبه‌ها نقش اساسی دارند.

---

[۶] Riemann-Hurwitz-Formula

[۷] Garcia

[۸] Torres

فصل اول

مقدمات

در این فصل مفاهیم اساسی میدان تابع و حلقه‌های ارزیاب، خم‌های جبری، بخشیاب‌ها، سری‌های خطی روی خم، رابطهٔ بین سری‌های خطی و ریخت‌ها، فرمول گونای ریمن—هورویتس، ناورداهای هرمیتی و مشتق‌های هسه را مطرح می‌کنیم. برای دیدن اثباتی از گزاره‌ها و قضایای این بخش می‌توانید به مراجع ([۱۳]و[۱۱]و[۲۴]) رجوع کنید.

۱.۱ میدان تابع و حلقه‌های ارزیاب

منظور از n− فضای آفین[۱] روی میدان K، مجموعهٔ n−تایی‌های

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \bar{K}\}$$

است. فضای تصویری [۲] را به‌صورت مجموعه خطوط فضای آفین یک بعد بالاتر تعریف می‌کنیم. یک نقطه $(x_0 : \ldots : x_n)$ در $\mathbb{P}^n$ یک خط در $\mathbb{A}^{n+1}$ است که از مبدأ و $(x_0, \ldots, x_n)$ می‌گذرد. بنابراین برای $(x_0 : \ldots : x_n), (y_0 : \ldots : y_n) \in \mathbb{P}^n$، $(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n)$، اگروتنهااگر $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$، طوری‌که $\lambda \in K^*$.

[۱] Affine Space

[۲] Projective Space

تعریف ۱.۱.۱ فرض کنیم $K[X] := K[X_\circ, \dots, X_n]$ حلقهٔ چندجمله‌ای‌های $n+1$−متغیره و $I \subseteq K[X]$ یک ایده‌آل باشد. به هر چنین ایده‌آلی، زیر مجموعه‌ای از $\mathbb{A}^n$ را به‌صورت

$$V_I := \{P \in \mathbb{A}^n \mid f(P) = \circ \text{ ،} f \in I \text{ به ازای هر}\}.$$

متناظر می‌کنیم. به V_I مجموعه جبری آفین در $\mathbb{A}^n$ می‌گوییم. منظور از ابر صفحهٔ H، مجموعهٔ ریشه‌های $\sum_{i=1}^{n} a_i x^i = \circ$ است.

تعریف ۲.۱.۱ اگر V یک مجموعهٔ جبری آفین باشد، ایده‌آل متناظر با V به‌صورت

$$I(V) := \{f \in \bar{K}[X] \mid f(P) = \circ \text{ ،} P \in V \text{ برای هر}\}$$

تعریف می‌شود.

چندجمله‌ای $f \in \bar{K}[X] = \bar{K}[X_\circ, \dots, X_n]$ را همگن[۳] از درجه d می‌گوییم هرگاه برای هر $\lambda \in \bar{K}$ داشته باشیم:

$$f(\lambda X_\circ, \dots, \lambda X_n) = \lambda^d f(X_\circ, \dots, X_n)$$

ایده‌آل $I \subseteq \bar{K}[X]$ را همگن گوییم هرگاه توسط چندجمله‌ای‌های همگن تولید شود.

تعریف ۳.۱.۱ مجموعه جبری آفین V را یک چندگونای[۴] آفین گوییم، هرگاه $I(V)$ یک ایده‌آل اول در $\bar{K}[X]$ باشد.

تعریف ۴.۱.۱ به هر ایده‌آل همگن $I \subset K[X_\circ, \dots, X_n]$، زیرمجموعه‌ای از $\mathbb{P}^n$ را به‌صورت زیر متناظر می‌کنیم.

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = \circ \text{ ،} f \in I \text{ برای هر چندجمله‌ای همگن}\}.$$

یک مجموعهٔ جبری تصویری، مجموعه‌ای به‌شکل V_I است. اگر V یک مجموعهٔ جبری تصویری باشد، ایده‌آل همگن متناظر با V_I، ایده‌آلی در $\bar{K}[X]$ به صورت

$$I(V) = \langle f \in \bar{K}[X_\circ, \dots, X_n] \mid f(P) = \circ \text{ ،} P \in V \text{ همگن و برای هر } f \rangle$$

---

[۳] Homogenouse

[۴] Variety

است. یک مجموعهٔ جبری تصویری را چندگونای تصویری می‌گوییم اگر ایده‌آل همگن متناظر با آن، یک ایده‌آل اول در $\bar{K}[X_0, \ldots, X_n]$ باشد.

تعریف ۵.۱.۱ میدان تابع جبری F/K با یک متغیر روی میدان K، میدان توسیع $F \supseteq K$ است طوری‌که عنصر متعالی $x \in F$ روی K وجود داشته باشد، طوری‌که F توسیع جبری متناهی روی $K(x)$ باشد.

نکته. عنصر $z \in F$ متعالی است اگروفقط‌اگر توسیع $F/K(z)$ از درجهٔ متناهی باشد.

برهان. اگر $z \in F$ متعالی باشد، طبق تعریف میدان تابع $F/K(z)$ از درجهٔ متناهی است. حال فرض کنیم توسیع $F/K(z)$ از درجهٔ متناهی باشد. اگر $z \in F$ جبری باشد آنگاه $[K(z):K]$ از درجهٔ متناهی، در نتیجه F/K از درجهٔ متناهی است. بنابراین z یک عنصر متعالی است. □

لم ۶.۱.۱ فرض کنیم F/K یک میدان تابع جبری باشد. در این‌صورت مجموعهٔ

$$\tilde{K} = \{z \in F \mid \text{جبری است } K \text{ روی } z\}$$

زیر یک زیر میدان از F است. $\tilde{K}$ را میدان ثابت F/K گوییم و داریم $K \subseteq \tilde{K} \subsetneqq F$. اگر $K = \tilde{K}$، گوییم K در F بستهٔ جبری است.

تعریف ۷.۱.۱ حلقهٔ ارزیاب[۵] میدان تابع F/K، یک زیر حلقهٔ $\mathcal{O} \subseteq F$ با خواص زیر است:

(الف) $K \subsetneqq \mathcal{O} \subsetneqq F$،

(ب) برای هرعنصر $z \in F$، $z \in \mathcal{O}$ یا $z^{-1} \in \mathcal{O}$.

نکته. حلقه‌های ارزیاب، موضعی هستند. یعنی دارای تنها یک ایده‌آل ماکسیمال منحصربه‌فرد $P = \mathcal{O} \setminus \mathcal{O}^{\times}$ هستند که در آن مجموعهٔ

$$\mathcal{O}^{\times} = \{z \in \mathcal{O} \mid zw = 1 \text{ طوری وجود داشته باشد که } w \in \mathcal{O}\}$$

گروه یکال‌های $\mathcal{O}$ است.

---

[۵] Valuation Ring

لم ۸.۱.۱ فرض کنیم $\mathcal{O}$ حلقهٔ ارزیاب میدان تابع F/K و P ایده‌آل ماکسیمال متناظر با آن باشد آنگاه شرایط زیر هم‌ارزند:

(الف) P یک ایده‌ال اصلی است،

(ب) اگر $P = t\mathcal{O}$، آنگاه هر عنصر $z \in F$ ، $z \neq 0$، نمایش منحصر به‌فردی به شکل $z = t^n u$ دارد که در آن $n \in \mathbb{Z}$ و $u \in \mathcal{O}^\times$،

(پ) $\mathcal{O}$ یک حوزهٔ ایده‌آل اصلی است. به بیان دقیق‌تر اگر $P = t\mathcal{O}$ و $\{0\} \neq I \subseteq \mathcal{O}$ یک ایده‌آل باشد، دراین‌صورت به ازای یک n داریم $I = t^n\mathcal{O}$.

حلقه‌ای که یکی از شرایط فوق را داشته باشد حلقهٔ ارزیاب گسسته [۶] و عضو t را پارامتر موضعی [۷] آن گویند.

تعریف ۹.۱.۱ (الف) منظور از مکان[۸] P در میدان تابع F/K، ایده‌آل ماکسیمال حلقهٔ ارزیاب در F/K است. اگر به‌ازای عنصر $t \in P$ بتوان P را به‌صورت $P = t\mathcal{O}$ نوشت که در آن $\mathcal{O}$ حلقهٔ ارزیاب آن در F/K است، آنگاه t را یک عنصر اول در P نامیم.

(ب) مجموعهٔ $\mathbb{P}_F$ را به‌صورت زیر تعریف می‌کنیم،

$$\mathbb{P}_F := \{P | \text{است } F/K \text{ یک مکان در } P\}$$

و آن را مجموعهٔ مکان‌های میدان تابع F/K نامیم.

تعریف ۱۰.۱.۱ یک ارزیاب گسسته[۹] از میدان تابع F/K، یک تابع $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$، با خواص زیر است:

(الف) $v(x) = \infty$ اگروفقط‌اگر $x = 0$؛

(ب) برای هر x و $y \in F$، $v(xy) = v(x) + v(y)$؛

(پ) برای هر x و $y \in F$، $v(x+y) \geq \min\{v(x), v(y)\}$؛

۶ Discrete Valuation Ring

۷ Local Parameter

۸ Place

۹ Discrete Valuation

(ت) برای یک عنصر $z \in F$ داریم $v(z) = ۱$؛

(ث) برای هرعنصر ناصفر $a \in K$، $v(a) = ۰$.

تعریف ۱۱.۱.۱ به هر مکان $P \in \mathbb{P}_F$، ارزیاب گسستهٔ $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ را به‌صورت زیر متناظر می‌کنیم:

هر عنصر ناصفر $z \in F$، به ازای پارامتر موضعی t برای P، نمایش منحصربه‌فردی به‌صورت $z = t^n u$ دارد که در آن $n \in \mathbb{Z}$ و $u \in \mathcal{O}^\times$. تعریف می‌کنیم $v_P(z) := n$ و $v_P(۰) := \infty$.

تعریف ۱۲.۱.۱ فرض کنیم $z \in F$ و $P \in \mathbb{P}_F$، اگر $v_P(z) = m > ۰$، می‌گوییم P یک صفر مرتبه m برای z و اگر $v_P(z) = -m < ۰$، یک قطب مرتبه m از z است.

۲.۱ خم‌های جبری

تعریف ۱.۲.۱ فرض کنیم $K = F_q$ یک میدان متناهی، F بستار جبری F_q و $F(\chi)$ میدان تابع (منظور میدان خارج قسمتی حلقهٔ $\frac{K[X_۰,\ldots,X_n]}{I}$) باشد. فرض کنیم $f_۱(x_۰,\ldots,x_n)$ ، $f_۲(x_۰,\ldots,x_n)$ ، ...، $f_{n-۱}(x_۰,\ldots,x_n)$، $(n-۱)$ چندجمله‌ای در حلقهٔ چندجمله‌ای $F_q[x_۰,\ldots,x_n]$ باشند در این‌صورت خم جبری آفین χ را به‌صورت زیر تعریف می‌کنیم:

$$\chi := \{\ (a_۰,\ldots,a_n) \in F^n \mid f_j(a_۰,\ldots,a_n) = ۰ \ \text{،}\ j = ۱,\ldots,n-۱ \ \text{،برای هر}\}$$

و مجموعه نقاط گویای خم χ را به‌صورت

$$\chi(F_q) = \{(a_۰,\ldots,a_n) \in \chi \mid a_۰,\ldots,a_n \in F_q\}$$

تعریف می‌کنیم. اگر $f(x,y) \in F_q[x,y]$ یک چندجمله‌ای تحویل‌ناپذیر روی $\bar{F}_q$ باشد، آنگاه مجموعهٔ زیر را خم جبری مسطح آفین می‌نامیم

$$\chi_f = \{(\alpha,\beta) \in \bar{F}_q \times \bar{F}_q \mid f(\alpha,\beta) = ۰\}$$

که در آن به نقاط $(\alpha,\beta) \in F_q$، نقاط گویا روی F_q گفته می‌شود.

تعریف ۲.۲.۱ چندگوناهای تصویری یک بعدی را خم جبری می‌نامند. خم جبری χ را تحویل‌ناپذیر[۱۰] گوییم، هرگاه نتوان آن را به‌صورت اجتماع دو چندگونای تصویری مجزا نوشت.

خم تصویری مسطح، چندگونای $V \subseteq \mathbb{P}^{2}$ است که ایده‌آل همگن $I(V) \in F_q[x_0, x_1, x_2]$ توسط یک چندجمله‌ای تحویل‌ناپذیر $h \in F_q[x_0, x_1, x_2]$ تولید می‌شود.

تعریف ۳.۲.۱ یک خم χ را در نقطهٔ P ناتکین[۱۱] گوییم هرگاه برای هر نقطهٔ $P = (a, b) \in \bar{F}_q \times \bar{F}_q$ از خم مسطح وابسته به چندجمله‌ای $f(x, y) \in \bar{F}_q[x, y]$ (یعنی $f(a, b) = 0$)، داشته باشیم $f_x(a, b) \neq 0$ یا $f_y(a, b) \neq 0$ (f_y, f_x، مشتقات جزئی هستند). در غیراین‌صورت P تکین است.

خم χ را ناتکین گوییم هرگاه در هر نقطهٔ $P \in \chi$ ناتکین باشد.

۱.۲.۱ بخشیاب‌ها و قضیهٔ ریمان—رخ

تعریف ۴.۲.۱ گروه بخشیاب‌های خم χ، گروه آبلی آزاد تولید شده توسط نقاط خم χ است و با $\mathrm{div}(\chi)$ نمایش داده می شود. بخشیاب $D \in \mathrm{div}(\chi)$، یک جمع صوری به شکل

$$\sum_{P \in \chi} v_P(D)P$$

است که در آن $v_P(D)$ ضریب P در D است و برای همه مگر تعداد متناهی $P \in \chi$، $v_P(D) = 0$. بخشیاب $\mathrm{div}(f) := \sum_{P \in \mathbb{P}_F} v_P(f)P$ را تعریف می‌کنیم که در آن $v_P(f)$ چندگانگی f در P است. درجه و محمل بخشیاب D، به ترتیب به‌صورت $\deg(D) = \sum_{P \in \chi} v_p(D)$ و $\mathrm{Supp}(D) = \{P \in \chi \mid v_P(D) \neq 0\}$ تعریف می‌شود. برای هر $P \in \chi$ ترتیب جزئی $\preceq$ برای هر P روی $\mathrm{div}(\chi)$ به‌صورت زیر تعریف می‌شود:

$$D_1 \preceq D_2 \text{ اگروتنهااگر } v_P(D_1) \leq v_P(D_2)$$

بخشیاب $D \succeq 0$ را بخشیاب موثر[۱۲] می گویند.

عنصر ناصفر $x \in F$ را در نظر می گیریم. فرض کنیم Z مجموعهٔ صفرها و N مجموعهٔ قطب‌های $x \in F$ باشد،

[۱۰] Irreducible
[۱۱] Non-Singular
[۱۲] Effective

بخشیاب‌های صفر[۱۳]، قطب [۱۴] و اصلی [۱۵] را به صورت زیر تعریف می‌کنیم:

$$(x)_\circ := \sum_{P\in Z} v_P(x)P \qquad \text{بخشیاب صفر } x$$

$$(x)_\infty := \sum_{P\in N} (-v_P(x))P \qquad \text{بخشیاب قطب } x$$

و

$$(x) := (x)_\circ - (x)_\infty \qquad \text{بخشیاب اصلی } x$$

بخشیاب اصلی x، یعنی (x) را با $\mathrm{div(x)}$ نیز نمایش می‌دهیم.

تعریف ۵.۲.۱ فرض کنیم $D \in \mathrm{div}(\chi)$. فضای ریمان—رخ [۱۶] متناظر با D به صورت زیر تعریف می‌شود:

$$L(D) := \{f \in K(\chi)^* \mid D + div(f) \geq \circ\} \cup \{\circ\}$$

بعد $L(D)$ به عنوان $K-$ فضای برداری با $\ell(D) = \dim_K L(D)$ نمایش می‌دهند.

تعریف ۶.۲.۱ دو بخشیاب D, E را هم ارز خطی گویند و با $D \sim E$ نمایش می‌دهند، اگر و تنها اگر $f \in K(\chi)$ موجود باشد که $D + \mathrm{div}(f) = E$. مجموعه $\mid E \mid$ را به صورت زیر تعریف می‌کنیم:

$$\mid E \mid := \{D \in div(\chi) \mid D \geq \circ,\ D \sim E\}$$

و یا معادلاً

$$\mid E \mid := \{E + div(f) \mid f \in L(E) \setminus \{\circ\}\}$$

[۱۳] Zero divisor

[۱۴] Pole divisor

[۱۵] Principal divisor

[۱۶] Riemann-Roch

و می‌توانیم $\mid E \mid$ را به یک ساختار از فضای تصویری از بعد $\ell(E) - ۱$ به‌صورت زیر مجهز کنیم:

$$\mid E \mid \longrightarrow \mathbb{P}(L(E))$$

$$div(f) + E \longmapsto [f]$$

یعنی $\mid E \mid \cong \mathbb{P}(L(E))$. این رابطه خوشتعریف است. زیرا برای هر $f, g \in F(\chi)^*$ ، $\mathrm{div}(f) = \mathrm{div(g)}$، اگر و تنها اگر عنصر $a \in K^*$ وجود داشته باشد که $af = g$.

قضیه ۷.۲.۱ ریمان—رخ[۱۷]: فرض کنیم χ یک خم هموار و C بخشیاب کانونیک χ باشد (یک بخشیاب از درجه $۲g - ۲$ و بعد g). عدد صحیح $g \geq ۰$، که گونای خم χ است طوری وجود دارد که برای هر $D \in \mathrm{div}(\chi)$ داریم

$$\ell(D) - \ell(C - D) = \deg(D) - g + ۱$$

برهان. اثبات در مرجع [۲۳]. □

تعریف ۸.۲.۱ فرض کنیم χ یک خم هموار تصویری روی F_q باشد. گونای خم χ را با $g = \ell(C)$ نمایش می‌دهیم.

گزاره ۹.۲.۱ اگر $\chi \subseteq \mathbb{P}^۲$ یک خم هموار مسطح از درجه d باشد، آنگاه گونای خم χ از رابطهٔ
$$g = \frac{۱}{۲}(d - ۱)(d - ۲)$$
به‌دست می آید.

برهان. به [۹، ص. ۲۰۱] مراجعه شود. □

تعریف ۱۰.۲.۱ یک خم ابربیضوی [۱۸] χ از گونای g ($g \geq ۱$) روی F_q، یک رابطه به‌صورت زیر

$$y^۲ + h(y)x = f(x)$$

[۱۷] Riemann-Roch Theorem

[۱۸] Hyperelliptic

در $F_q[x,y]$ است. طوری‌که $h(y)\in F_q[y]$ و $f(x)\in F_q[x]$ یک چندجمله‌ای از درجه $2g+1$ است.

اگر $char(F_q)\neq 2$، آنگاه خم χ به‌صورت $y^2=f(x)$ است، طوری‌که $\deg(f)=2g+1$.

مثال ۱۱.۲.۱ خم‌های بیضوی نمونه‌ای از خم‌های جبری هستند. خم بیضوی، یک خم جبری تصویری هموار با گونای یک است که دارای یک نقطهٔ مشخص، به‌نام نقطه در بی‌نهایت است. در مشخصه‌های $p\neq 2$ هر خم بیضوی را می‌توان به عنوان یک خم جبری مسطح ناتکین با معادلهٔ

$$y^2=x^3+ax+b$$

در نظر گرفت. معادلاً اگر $y^2=f(x)$، که در آن $f(x)$ یک چندجمله‌ای درجه ۳ از x بوده و ریشه تکراری ندارد، آنگاه یک خم مسطح ناتکین باگونای یک یا معادلاً یک خم بیضوی داریم.

در ادامه منظور از یک خم، خم جبری، تصویری و ناتکین روی میدان K است.

۳.۱ سری‌های خطی روی خم‌ها

تعریف ۱.۳.۱ یک سری خطی$\mathcal{D}$، یک زیرفضای $K-$خطی از $|E|$ به‌صورت زیر است:

$$\mathcal{D}:=\{E+\operatorname{div}(f)\mid f\in\mathcal{D}'\setminus\{0\}\}$$

طوری‌که $\mathcal{D}'$ یک زیرفضای $K-$خطی از $L(E)$ است.

اعداد $d=\deg(\mathcal{D}):=\deg(E)$ و $r=\dim(\mathcal{D}):=\dim(\mathcal{D}')-1$ را به‌ترتیب درجه و بعد سری خطی $\mathcal{D}$ می‌نامند و با g_d^r نمایش می‌دهند. سری خطی $\mathcal{D}$ را کامل گویند، هرگاه $\mathcal{D}=|E|$. با در نظر گرفتن یکریختی $\mathbb{P}(L(E))\cong|E|$، $\mathcal{D}$ متناظر با $\mathbb{P}(\mathcal{D}')$ است، یعنی $\mathcal{D}\cong\mathbb{P}(\mathcal{D}')\subseteq|E|$. سری خطی $\mathcal{D}_1\cong\mathbb{P}(\mathcal{D}'_1)\subseteq|E_1|$ زیر فضای $\mathcal{D}\cong\mathbb{P}(\mathcal{D}')\subseteq|E|$ است، هرگاه $L(E_1)\subseteq L(E)$ و $\mathcal{D}'_1\subseteq\mathcal{D}'$.

تعریف ۲.۳.۱ سری خطی $\mathcal{D}$ را مستقل از نقطه پایه[۱۹] گویند، اگر برای هر $P \in \chi$، یک بخشیاب $D \in \mathcal{D}$ موجود باشد که $P \notin \mathrm{Supp}(D)$.

تعریف ۳.۳.۱ یک ریخت $\phi : \chi \to \mathbb{P}^r(K)$ ناتباهیده[۲۰] است، اگروتنهااگر برای هر ابرصفحه H در $\mathbb{P}^r$، $\phi(\chi) \nsubseteq H$.

بعد از این منظور ما از سری خطی و ریخت، یک سری خطی مستقل از نقطه پایه و ریخت ناتباهیده است.

تعریف ۴.۳.۱ برای هر نقطه $P \in \chi$ و هر $i \in \mathbb{N}_{۰}$، $\mathcal{D}_i$ را به‌صورت

$$\mathcal{D}_i(P) = \{D \in \mathcal{D} \mid D \succeq iP\}.$$

تعریف می‌کنیم.

لم ۵.۳.۱ برای هر $P \in \chi$ احکام زیر برقرارند:

(الف) $\mathcal{D}_i(P)$ یک سری خطی است؛

(ب) $\mathcal{D}_i(P)$ زیرفضای $\mathcal{D}$ است؛

(پ) $\dim(\mathcal{D}_i(P)) \leq \dim(\mathcal{D}_{i+۱}(P)) + ۱$.

برهان. قرار می‌دهیم $\mathcal{D}_i := \mathcal{D}_i(P)$ و فرض می‌کنیم $f \in \mathcal{D}' \setminus \{۰\}$، آنگاه $E + \mathrm{div}(f) \in \mathcal{D}_i$، اگروفقط‌اگر $v_P(E) + v_P(f) \geq i$؛ یعنی $\mathcal{D}_i \cong \mathbb{P}(\mathcal{D}'_i)$، که در آن

$$\mathcal{D}'_i := \mathcal{D}' \cap L(E - iP)$$

که اثبات (الف) و(ب) را کامل می‌کند. حال $\frac{\mathcal{D}'_i}{\mathcal{D}'_{i+۱}}$، K−یکریخت با K−زیرفضای

$$\frac{L(E - iP)}{L(E - (i + ۱)P)}$$

است. چون

$$\dim_K \left(\frac{L(E - iP)}{L(E - (i + ۱)P)} \right) = \ell(E-iP)-\ell(E-(i+۱)P) \leq deg(E-iP)+۱-deg(E-(i+۱)P)-۱ = ۱.$$

---

[۱۹] Base-point-free

[۲۰] Non-degenerate

قسمت (پ) نیز به دست می‌آید. $\square$

تعریف ۶.۳.۱ چندگانگی $\mathcal{D}$ در $P \in \chi$ به‌صورت

$$b(P) := \min\{v_P(D) \mid D \in \mathcal{D}\}$$

تعریف می‌شود. $b(P) > 0$ اگروتنهااگر برای هر $D \in \mathcal{D}$، $P \in \operatorname{Supp}(D)$؛ بنابراین برای تعداد متناهی $P \in \chi$، $b(P) \neq 0$. لذا می‌توان بخشیاب مثبت $B = B^{\mathcal{D}}$ را روی χ با قرار دادن $v_P(B) := b(P)$ تعریف کرد.

تعریف ۷.۳.۱ بخشیاب B را مکان هندسی پایه[۲۱] $\mathcal{D}$ و نقطهٔ $P \in \operatorname{Supp}(B)$ را نقطهٔ پایه $\mathcal{D}$ می‌نامند. و بخشیاب $\mathcal{D}^B := \{D - B \mid D \in \mathcal{D}\}$ را تعریف می‌کنیم.

لم ۸.۳.۱ فرض کنید $\mathcal{D} \cong \mathbb{P}(\mathcal{D}') \subseteq |E|$ یک سری خطی باشد که در آن $\mathcal{D}' = \langle f_0, \ldots, f_s \rangle$ است، آنگاه E به‌وسیلهٔ $\mathcal{D}$ معین می‌شود، به عبارت دیگر

$$v_P(E) = b(P) - \min\{v_P(f_0), \ldots, v_P(f_s)\}.$$

برهان. چون $\mathcal{D}' \subseteq L(E - B)$، لذا برای هر i و هر $P \in \chi$، $v_P(E) - b(P) + v_P(f_i) \geq 0$، در نتیجه $v_P(E) \geq b(P) - \min\{v_P(f_0), \ldots, v_P(f_s)\}$. از طرفی از آنجا که $\mathcal{D}^B$ مستقل از پایه است، برای هر P، عنصر $(a_0 : \ldots : a_s) \in \mathbb{P}^s(F)$ وجود دارد طوری‌که $v_P(E - B + \operatorname{div}(\sum_i a_i f_i)) = 0$. بنابراین نتیجه به دست می‌آید. $\square$

لم ۹.۳.۱ فرض کنیم $\mathcal{D} \cong \mathbb{P}(\mathcal{D}')$ یک سری خطی مستقل از نقطه پایه از بعد r روی خم χ باشد. هر $K-$پایه $\{f_0, \ldots, f_r\}$ از $\mathcal{D}'$ یک ریخت ناتباهیده به صورت $\phi_{f_0,\ldots,f_r} = (f_0 : \ldots : f_r) \ : \chi \to \mathbb{P}^r$ تعریف می‌کند. اگر $g_0, \ldots, g_r$ پایه دیگری از $\mathcal{D}'$ باشد، آنگاه $T \in Aut(\mathbb{P}^r)$ طوری وجود دارد که $\phi_{g_0,\ldots,g_r} = T \circ \phi_{f_0,\ldots,f_r}$.

[۲۱] Base Locus