خم‌های بیضوی و فرم‌های مدولار

علی چراغی

استاد راهنما: دکتر امیر جعفری

دانشکده علوم ریاضی

دانشگاه صنعتی شریف

سال تحصیلی ۹۵-۹۶

فهرست مطالب

۱ مقدمه

در این پروژه سعی می‌کنیم با ارائه دادن پیشنیازهای مناسب به قضیه مدولاریتی[۱] و قضیه آخر فرما برسیم. برای این کار باید خم‌های بیضوی و فرم‌های مدولار و نمایش‌های گالوا و ارتباط بین این سه را بررسی کنیم. در بخش ۲، دلیل مهم بودن بررسی خم‌های بیضوی را با دسته‌بندی خم‌های جبری توسط گونه[۲] آن‌ها توضیح داده‌ایم و همچنین قضایای مربوط به خم‌ها با گونه‌های داده شده را بیان کرده‌ایم. سپس در بخش ۳، خم‌های بیضوی را به تفصیل توضیح داده‌ایم. مقداری نظریه میدان‌های رده‌ای[۳] و کوهمولوژی گالوا[۴] در بعضی اثبات‌ها و مطالب بخش ۳ فرض شده است. قضیه موردل-وی را برای خم‌های بیضوی روی هر میدان عددی ثابت کرده‌ایم. همچنین در انتهای بخش ۳، خم‌های بیضوی روی اعداد مختلط را در نظر گرفته‌ایم و مخصوصاً ضرب مختلط[۵] را مفصل‌تر توضیح داده‌ایم.

پس از آن در مورد فرم‌های مدولار توضیح داده‌ایم و عملگرهای هکه و همچنین خم‌های پیمانه‌ای را تعریف کرده‌ایم.

نمایش‌های گالوا روی خم‌های بیضوی و فرم‌های مدولار را نیز نوشته‌ایم و سپس L-توابع این اشیا را توضیح داده‌ایم. در انتها نیز ایده‌ی اثبات قضیه آخر فرما توسط وایلز را توضیح داده‌ایم.

[1] Modularity
[2] Genus
[3] Class Field Theory
[4] Galois Cohomology
[5] Complex Multiplication

۲ دسته‌بندی خم‌های جبری

منظور ما از یک خم جبری، همواره، یک واریته تصویری با بعد ۱ روی میدان کامل[۶] K است که با C/K نمایش می‌دهیم. خم‌های جبری را می‌توان با استفاده از گونه آن‌ها دسته‌بندی کرد. در بخش‌های بعدی سعی شده است همه خم‌ها با گونه داده شده را در حد ایزومورفیسم پیدا کنیم. قضیه ریمان-رخ از مهم‌ترین ابزارها برای این کار است. مقدمات قضیه ریمان-رخ را در ابتدا بیان می‌کنیم.

۱.۲ قضیه ریمان-رخ

قضیه ریمان-رخ از مهم‌ترین قضیه‌های ریاضیات است. یکی از مهم‌ترین اهداف هندسه جبری، دسته‌بندی واریته‌ها در حد ایزومورفیسم است. این کار در ابتدا با بعد یک واریته انجام می‌شود. سپس برای واریته‌های تصویری از بعد ۱ می‌توان دسته‌بندی را جلوتر برد و آن‌ها را با گونه‌شان طبقه‌بندی کرد. در واقع، گونه، یک ناوردای دوگویا[۷] است که مقادیر نامنفی می‌گیرد. همچنین برای هر $g > 0$ داده شده، یک واریته تحویل‌ناپذیر $\mathcal{M}_g$ به نام "واریته مدولی خم‌های گونه g" وجود دارد که همه‌ی خم‌های هموار را در حد تعادل دوگویا[۸] طبقه‌بندی می‌کند، به عبارت دیگر، هر نقطه از آن به یک خم گونه g تناظر داده می‌شود. پس در واقع همه‌ی خم‌های هموار با یک مولفه‌ی "گسسته" (گونه) و یک مولفه‌ی "پیوسته" (واریته مدولی) داده می‌شوند. خم‌های هموار با گونه‌ی ۱ با نقاط K-گویا، خم‌های بیضوی روی K نامیده می‌شوند. (البته در ابتدا آن‌ها با این روش تعریف نشده‌اند.)

"نامساوی ریمان" در سال ۱۸۵۷ توسط ریمان بدست آمد و سپس توسط رخ در سال ۱۸۶۵ به شکل قضیه‌ای در مورد رویه‌های ریمانی (خمینه‌های مختلط یک بعدی یا معادلاً خم‌های ۱ بعدی تعریف شده روی اعداد مختلط) درآمد. منظور از گونه‌ی ریمانی تعداد سوراخ‌های آن است و این تعریف گونه را می‌توان به همه‌ی خم‌های جبری تعمیم داد. این قضیه تعمیم‌های بسیاری داده شده است. ما قضیه ریمان-رخ را برای خم‌های جبری بیان می‌کنیم و در بخش‌های بعدی از آن استفاده می‌کنیم.

برای بیان کردن قضیه ریمان-رخ نیاز به تعریف مقسم[۹] و توضیحاتی در مورد آن است که در پایین گفته شده است:

تعریف. یک مقسم روی خم C/K ، جمعی صوری و متناهی از نقاط آن است. پس هر مقسم را می‌توان به شکل زیر نمایش داد:

$$D = \sum_{P \in C} n_P(P)$$

که $n_P = 0$ به جز تعدادی متناهی $p \in C$. به عدد $\sum_{P \in C} n_P$ درجه D می‌گوییم و با $\deg D$ نمایش می‌دهیم.

به هر $f \in K(C)$ می‌توان یک مقسم به شکل زیر نسبت داد:

$$div\ f = \sum_{P \in C} ord_P f\ (P)$$

که $ord_P f$ مرتبه صفر شدن f در P است.

حکم. برای هر $f \in K(C)$ داریم $\deg(div\ f) = 0$.

برهان. فرض کنید $f = G/H$ که G, H دو فرم همگن درجه m در $K[x, y, z]$ هستند. در این صورت طبق قضیه بزو درجه مقسم‌های G, H برابر mn است. پس چون $div(f) = div(G) - div(H)$، کار تمام است.

می‌گوییم مقسم $D = \sum_{P \in C} n_P(P)$ ، موثر[۱۰] است و با $D \geq 0$ نمایش می‌دهیم، هرگاه $n_P \geq 0$ برای هر $P \in C$.

[6] Perfect
[7] Birational
[8] Birational Equivalence
[9] Divisor
[10] Effective

تعریف. فرض کنید C/K یک خم جبری و D یک مقسم روی آن باشد. در این صورت $L(D)$ را برابر با فضای برداری زیر تعریف می‌کنیم:

$$L(D) = \{f \in \bar{K}(C) | div\ f + D \geq 0\}$$

به سادگی مشاهده می‌شود که این فضا متناهی‌بعد است. بعد این فضا را با $l(D)$ نمایش می‌دهیم و حکم زیر را داریم:

حکم. فرض کنید D یک مقسم باشد. در این صورت:

۱) اگر $\deg D < 0$ آن‌گاه $L(D) = \{0\}$

۲) اگر $\deg D \geq 0$ آن‌گاه $l(D) \leq \deg D + 1$

برهان. رجوع شود به بخش ۲.۸، حکم ۳ از [۱]

همچنین به هر فرم دیفرانسیلی ω روی خم جبری هموار C ، می‌توان یک مقسم به شکل مقابل نسبت داد. برای هر نقطه $P \in C$ یک یکسان‌ساز[11] مثل $t_P \in K(C)$ انتخاب کنید. در این صورت از آن‌جا که بعد فضای برداری فرم های دیفرانسیل روی $K(C)$ برابر ۱ است، پس برای هر $p \in C$ می‌توان $f_P \in K(C)$ پیدا کرد که:

$$\omega = f_P dt_P$$

در این صورت تعریف می‌کنیم:

$$div\ \omega := \sum_{P \in C} ord_P f_P\ (P)$$

همچنین هم‌ارزی خطی[12] دو مقسم را تعریف می‌کنیم:

تعریف. دو مقسم D و D' را هم ارز خطی می‌گوییم و با $D \sim D'$ نمایش می‌دهیم، هرگاه $f \in K(C)^*$ موجود باشد بطوری که:

$$D = D' + div\ f$$

از آن‌جا که بعد فضاهای دیفرانسیلی روی $K(E)$، ۱ است، پس هر دو مقسم که از فرم‌های دیفرانسیلی بدست آمده‌اند با یکدیگر هم‌ارز خطی هستند.

تعریف. منظور از مقسم کانونی[13] ، $div\ \omega$ است برای یک فرم دیفرانسیلی ناصفر ω .

پس مقسم کانونی W، در حد هم‌ارزی خطی تعریف می‌شود، ولی $l(W)$ به ω انتخاب شده بستگی ندارد. در واقع اگر $div\ \omega = div\ \omega' + div\ f$ ، آن‌گاه:

$$l(div\ \omega) = l(div\ \omega' + div\ f) = l(div \omega')$$

زیرا $L(div\ \omega' + div\ f) = L(div\ \omega')$

حال می‌توان قضیه ریمان-رخ را بیان کرد:

قضیه. (ریمان-رخ) فرض کنید C/K یک خم جبری هموار و D یک مقسم از آن و W یک مقسم کانونی روی آن باشد. در این صورت عدد صحیح نامنفی g به نام گونه وجود دارد بطوری که:

$$l(D) - l(W - D) = \deg D + 1 - g$$

[11] Uniformizer
[12] linear equivalence
[13] Canonical divisor

برهان. رجوع شود به بخش ۶.۸ از [۱]

در واقع این قضیه تقریبی برای محاسبه $l(D)$ بدست می‌دهد زیرا می‌گوید $l(D) \approx \deg D + 1 - g$ با جمله خطای $l(W - D)$.

نتیجه. اگر W خم جبری هموار C و g گونه آن باشد، آن‌گاه $\deg W = 2g - 2$.

برهان. ابتدا در قضیه ریمان-رخ قرار دهید $D = 0$، در این صورت:

$$\begin{aligned} l(0) - l(W - 0) &= \deg 0 + 1 - g \Rightarrow \\ 1 - l(W) &= 1 - g \Rightarrow \\ l(W) &= g \end{aligned}$$

حال در قضیه ریمان-رخ قرار دهید $D = W$ و پس:

$$\begin{aligned} l(W) - l(0) &= \deg W + 1 - g \Rightarrow \\ g - 1 &= \deg W + 1 - g \Rightarrow \\ \deg W &= 2g - 2 \end{aligned}$$

این نتیجه روشی برای محاسبه g بدست می‌دهد که در مثال زیر آن را بیان می‌کنیم:

مثال. می‌خواهیم ثابت کنیم گونه‌ی $\mathbb{P}^1_K$ برابر ۰ است. در واقع اگر $\mathbb{P}^1_K$ را با $\{[t : 1] \mid t \in K\} \cup \{\infty\}$ مختصه‌بندی کنیم و فرم دیفرانسیلی dt را در نظر بگیریم داریم:

$$div\ dt = -2(\infty)$$

و پس

$$2g - 2 = \deg(div\ dt) = -2 \Rightarrow g = 0$$

همچنین قضیه‌ای برای محاسبه گونه خم‌های جبری صفحه‌ای (قابل نشاندن در $\mathbb{P}^2_K$) وجود دارد که در زیر بیان می‌کنیم:

قضیه. فرض کنید $C/\bar{K}$ یک خم جبری صفحه‌ای از درجه n باشد و فرض کنید که نقاط ناهمواری آن معمولی (با خطوط مماس مختلف) و روی P_iها باشند و با تکرر r_{P_i} باشد. در این صورت

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P_i} \frac{r_{P_i}(r_{P_i} - 1)}{2}$$

برهان. رجوع شود به بخش ۳.۸، نتیجه‌ی ۱ از [۱]

۲.۲ خم های با گونه ۰

در بخش پیش ثابت کردیم که $\mathbb{P}^1_K$ گونه ۰ دارد. در این بخش معکوسی برای این قضیه ثابت می‌کنیم. فرض کنید $\bar{K}$ یک بستار جبری ثابت از K باشد.

قضیه. فرض کنید $C/\bar{K}$ یک خم جبری هموار باشد. در این صورت اگر گونه C، ۰ باشد آن‌گاه C با $\mathbb{P}^1_{\bar{K}}$ ایزومورف است.

برهان. فرض کنید $p \in C$ و در قضیه ریمان-رخ قرار دهید $D = (p)$. پس

$$l((p)) - l(W - (p)) = \deg p + 1 - g = 2 - 0 = 2$$

پس $l((p)) \geq 2$. نتیجه می‌گیریم که به جز توابع ثابت، تابع دیگری مثل $\phi \in \bar{K}(C)$ در $l(p)$ هست. پس این تابع باید فقط یک قطب ساده در p داشته باشد و هیچ‌جای دیگر قطب نداشته باشد. پس $\phi : C \to \mathbb{P}^1_K$ یک تابع درجه ۱ می‌دهد، پس یک ایزومورفیسم است.

نکته. در اثبات بالا فقط از وجود $p \in C$ استفاده کردیم. پس اگر K یک میدان (نه لزوماً بسته جبری) باشد و p یک نقطه‌ی K-گویا روی آن، همین اثبات کار می‌کند و نتیجه می‌گیریم $E \cong \mathbb{P}^1_K$.

پس در واقع حساب روی خم‌های جبری با گونه ۰، برابر با حساب روی $\mathbb{P}^1_K$ است و این حساب روی خم جبری ساده است. در بخش‌های بعدی خم‌های با گونه بیشتر را بررسی می‌کنیم.

۳.۲ خم های با گونه ۱

حال به قسمتی اصلی از خم‌های بررسی شده در این مقاله می‌پردازیم. به یک خم جبری هموار با گونه ۱ و نقاط K-گویا، خم بیضوی گویند. پس باید سعی کنیم با مختصه‌هایی کار کردن و حساب روی آن را ساده‌تر کنیم و یک مدل کانونی برای آن پیدا کنیم. در این بخش سعی شده با قضیه‌ای مانند قضیه بخش پیش، این فرم را پیدا کنیم:

قضیه. فرض کنید E/K یک خم بیضوی باشد. در این صورت $a_i \in K$ها وجود دارند که E را می‌توان با فرم کانونی وایرشتراس زیر بیان کرد:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

برهان. فرض کنید نقطه‌ی K-گویای ∞ در E باشد. برای آن با قضیه ریمان-رخ داریم:

$$l(n(\infty)) - l(W - n(\infty)) = \deg n(\infty) + 1 - 1 = n$$

همچنین از آن‌جا که $\deg W = 2g - 2 = 0$ پس برای $n \geq 1$ داریم $l(W - n(\infty)) = 0$ پس:

$$l(n(\infty)) = n \quad (n \geq 1)$$

حال قرار دهید $n = 2$ و توابع $\{1, x\}$ را پایه‌ای برای $L(2(\infty))$ فرض کنید. همچنین برای $L(3(\infty))$ این پایه را گسترش دهید و مثلاً $\{1, x, y\}$ را پیدا کنید. حال داریم که

$$\{1, x, y, x^2, xy, y^2, x^3\} \subseteq L(6(\infty))$$

پس از آن‌جا که بعد $L(6(\infty))$، ۶ است، پس این ۷ تابع باید یک رابطه خطی داشته باشند:

$$c_1 + c_2x + c_3y + c_4x^2 + c_5xy + c_6y^2 + c_7x^3 = 0$$

همچنین به دلیل خواص x, y ، باید داشته باشیم که $c_6c_7 \neq 0$. (چون اگر یکی از این‌ها صفر بودند، همه بقیه مرتبه قطب‌هایشان در ∞ فرق می‌کرد و این ترکیب خطی نمی‌توانست صفر باشد.)

پس ما یک تابع $\phi : C \to \mathbb{P}^2_K$ به شکل زیر می‌گیریم :

$$\phi : \begin{cases} p \mapsto [x(p) : y(p) : 1] & p \neq \infty, \\ \infty \mapsto [0 : 1 : 0] \end{cases}$$

حال تابع $[x : 1]$، درجه‌ی ۲ دارد (زیرا x یک قطب مرتبه‌ی ۲ در ∞ دارد) و همچنین تابع $[y : 1]$ درجه‌ی ۳ دارد و پس داریم:

$$[K(E) : K(x, y)] \mid [K(E) : K(x)] = 2$$
$$[K(E) : K(x, y)] \mid [K(E) : K(y)] = 3$$

پس $K(E) = K(x, y)$ و پس ϕ از درجه ۱ است و پس ایزومورفیسم است. همچنین برای میدان‌های با $char\ K \neq 2, 3$ می‌توان این مختصات را بهتر کرد و تعدادی از جمله‌ها را با تغییر مختصات وارون‌پذیر از بین برد و آن را به فرم زیر درآورد:

$$y^2 = x^3 + Ax + B \quad (A, B \in K)$$

همچنین عکس قضیه بالا برای خم‌های با فرم کانونی وایرشتراس درست است:

قضیه. فرض کنید یک خم بیضوی روی میدان K با مختصات زیر داده شده باشد:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

در این صورت گونه‌ی E برابر ۱ است.

برهان. فرم دیفرانسیلی $\frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$ را در نظر بگیرید. به سادگی می‌توان چک کرد که این فرم هلومورف است و جایی صفر نمی‌شود. حال طبق قضیه ریمان-رخ درجه‌ی مقسم آن برابر با $2g - 2$ است و پس داریم:

$$2g - 2 = \deg(div\ w) = \deg(0) = 0$$

پس $g = 1$.

۴.۲ خم‌های با گونه‌ی بزرگتر از ۱

برای خم‌های با گونه‌ی بزرگتر از ۱ نیز می‌توان مدل‌هایی مانند مدل‌های بخش قبل پیدا کرد. مثلاً خم‌های هموار با گونه‌ی ۲ به همراه نقطه‌ی K-گویا روی میدان با مشخصه صفر K را می‌توان به شکل خم ابربیضوی زیر نوشت:

$$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

از آن‌جایی که نقاط $\mathbb{Q}$-گویا روی خم‌ها برای ما اهمیت بسیاری دارد، قضایا و حدس‌های این خم‌ها را بیان می‌کنیم که نشان می‌دهد بررسی نقاط $\mathbb{Q}$-گویا روی این خم‌ها نباید بسیار دشوار باشد.

موردل در سال ۱۹۲۲ حدسی را بیان می‌کند بدین مضمون که هر خم با گونه‌ی بزرگتر یا مساوی ۲ حداکثر متناهی نقطه تعریف شده روی اعداد گویا می‌تواند داشته باشد. این حدس ۶۰ سال بعد توسط فالتینگز به اثبات رسید.

قضیه. (فالتینگز) فرض کنید E یک خم با گونه‌ی بزرگتر مساوی ۲ روی اعداد گویا باشد. در این صورت E متناهی نقطه‌ی $\mathbb{Q}$-گویا دارد.

این قضیه اثبات‌های متعددی دارد. خود فالتینگز از یک کاستن به حدس تیت و ابزارها و ایده‌های هندسه جبری و مدل‌های نرون استفاده کرد. پس از او وجتا با استفاده از تقریب دیوفانتی و به شکلی کاملاً متفاوت آن‌را ثابت کرد. همچنین یک اثبات مقدماتی‌تر توسط بمبیری بدست آمد.

این قضیه نتایج بسیاری دارد. مثال زیر نشان‌دهنده‌ی قدرت این قضیه است.

مثال. فرض کنید $n \geq 4$ ثابت است. در این صورت $x^n + y^n = z^n$ متناهی جواب صحیح دارد. در واقع، خم تصویری هموار $x^n + y^n = z^n$ را در $\mathbb{P}^2_{\mathbb{Q}}$ در نظر بگیرید. در این صورت از قضیه‌ی آخر بخش ۲.۱ داریم که گونه‌ی آن برابر با $\frac{(n-1)(n-2)}{2} \leq 2$ است. پس از قضیه فالتینگز حکم نتیجه می‌شود.

۳ خم‌های بیضوی

همان طور که گفته شد، خم بیضوی روی میدان K یک خم جبری هموار روی K با نقطه‌ای K-گویا است. در این‌جا تلاش می‌کنیم خم‌های بیضوی را به عنوان یک حوزه‌ی مجرد و نه فقط یک ابزار، بررسی کنیم. در ابتدا عمل گروه روی آن را بررسی می‌کنیم و سپس ساختار گروه آن روی میدان‌های عددی را بررسی می‌کنیم. قضیه موردل-وی روی میدان‌های عددی را با استفاده از کوهمولوژی گالوا ثابت می‌کنیم و در بررسی آن گروه‌های سلمر و شفرویچ-تیت را معرفی می‌کنیم. سپس در مورد نقاط صحیح روی خم‌های بیضوی صحبت می‌کنیم و نحوه‌ی بدست آوردن آن‌ها را با گفتن قضایای ناگل-لوتز و روش کاستن به پیمانه اعداد اول بیان می‌کنیم. پس از آن ضرب مختلط را به تفصیل بیشتری بررسی می‌کنیم. همچنین قسمت‌های تحلیلی تر آن مانند توابع زتا و L-توابع آن‌ها را در بخش‌های بعدی بررسی می‌کنیم.

۱.۳ تعاریف مقدماتی

در بخش ۲.۳ ثابت کردیم که هر خم بیضوی E روی میدان K را می‌توان به شکل زیر نمایش داد:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

با $a_1, a_2, a_3, a_4, a_6 \in K$ که البته در حالت $char\ K \neq 2, 3$ با یک تغییر مختصات ساده می‌توان آن‌را به شکل ساده‌تر زیر درآورد:

$$E : y^2 = x^3 + Ax + B \quad (A, B \in K)$$

برای این که همواری این خم را در هنگام "کاستن" بررسی کنیم، می‌توانیم عددی به نام تفکیک‌کننده را تعریف کنیم که صفر نشدن آن به منزله‌ی همواری خم است.

تعریف. تفکیک‌کننده خم E با مختصات بالا را به شکل زیر تعریف می کنیم. قرار دهید:

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$

در این صورت تفکیک‌کننده برابر است با

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

در حالت $char\ K \neq 2, 3$ این عبارت به حالت ساده‌تر $\Delta_E = -16(4A^3 + 27B^2)$ در می‌آید. می‌توان به سادگی بررسی کرد که $\Delta_E = 0$ اگر و تنها اگر E ناهموار باشد.

همچنین "ناوردایی" وجود دارد به نام j-ناوردا که خم بیضوی را در حد ایزومورفیسم مشخص می کند و به صورت زیر تعریف می شود:

تعریف. با نمادگذاری‌های تعریف بالا، j-ناوردا را برابر مقدار زیر تعریف می‌کنیم:

$$j_E = \frac{(b_2^2 - 24b_4)^3}{\Delta_E}$$

که در حالت $char\ K \neq 2, 3$ داریم:

$$j_E = -1728\frac{(4A)^3}{\Delta_E}$$

همان‌گونه که گفته شد در مورد j-ناوردا قضیه مهم زیر را داریم:

قضیه. ۱) دو خم بیضوی ایزومورف روی بستار جبری $\bar{K}$ هستند، اگر و تنها اگر j-ناوردای آنها با هم یکسان باشند.

۲) فرض کنید $j_0 \in \bar{K}$، در این صورت خم بیضوی E تعریف شده روی $K(j_0)$ وجود دارد بطوری که $j_E = j_0$

برهان. ۱) فرض می‌کنیم $char\ K \neq 2,3$ (در حالت‌های کنار گذاشته شده نیز می‌توان به سادگی این کارها را انجام داد)، در این صورت فرض کنید برای $E : y^2 = x^3 + Ax + B$ و $E' : y^2 = x^3 + A'x + B'$ داشته باشیم $j_E = j_{E'}$. در این صورت:

$$j_E = j_{E'} \Leftrightarrow -1728\frac{(4A)^3}{\Delta_E} = -1728\frac{(4A')^3}{\Delta'_E} \Leftrightarrow \frac{A^3}{4A^3 + 27B^2} = \frac{A'^3}{4A'^3 + 27B'^2} \Leftrightarrow$$
$$A^3B'^2 = A'^3B^2 \Leftrightarrow (\frac{A}{A'})^3 = (\frac{B}{B'})^2$$

(حالت‌های $A' = 0$ یا $B' = 0$ را نیز می‌توان به همین شکل بررسی کرد)

حال $\lambda \in \bar{K}$ را طوری انتخاب کنید که $\lambda^6 = \frac{B}{B'}$ (از آن‌جایی که $\bar{K}$ بسته جبری است چنین λ یافت می‌شود). در این صورت روی E، تغییر مختصات زیر را انجام بدهید:

$$x \mapsto \lambda^2 xy \mapsto \lambda^3 y$$

در این صورت داریم:

$$E \cong \hat{E} : \lambda^6 y^2 = \lambda^6 x^3 + A\lambda^2 x + B \Leftrightarrow y^2 = x^3 + \frac{Ax}{\lambda^4} + \frac{B}{\lambda^6}$$

پس از رابطه‌ی بالا:

$$\lambda^{12} = (\frac{B}{B'})^2 = (\frac{A}{A'})^3 \Rightarrow' \lambda^4 = \frac{A}{A'}$$

که علامت پریم بالای $\Rightarrow$ به این معنی است که ممکن است مجبور باشیم λ را با $\lambda\omega$ که ω یک ریشه‌ی سوم واحد است عوض کنیم. حال داریم:

$$\hat{E} : y^2 = x^3 + \frac{Ax}{\lambda^4} + \frac{B}{\lambda^6} \Leftrightarrow y^2 = x^3 + A'x + B' : E'$$

و پس E و E' ایزومورف روی $\bar{K}$ هستند. همچنین اگر ایزومورف باشند، به سادگی می‌توان دید که هر ایزومورفیسم بین آن‌ها که فرم وایرشتراس E را به فرم وایرشتراس E' ببرد، باید به فرم زیر باشد:

$$x \mapsto u^2x + r, \quad y \mapsto u^3y + u^2sx + t$$

با $u, r, s, t \in \bar{K}$ و $u \neq 0$، پس از اعمال تغییر مختصات و چک کردن j-ناوردای بدست آمده می‌توان بررسی کرد که آنها با یکدیگر برابرند.

۲) فرض کنید $j_0 \neq 0, 1728$، برای این قسمت کافی است خمی را پیدا کنیم که خواص بالا را داشته باشد. قرار دهید: $E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$ در این صورت $j_E = j_0$ و این خم هموار است چون

$$\Delta_E = \frac{j_0^3}{(j_0 - 1728)^3}$$

همچنین برای حالات دیگر داریم:

$$E_1 : y^2 + y = x^3, \quad j_E = 0 E_2 : y^2 = x^3 + x, \quad j_E = 1728$$

و قضیه ثابت می‌شود.

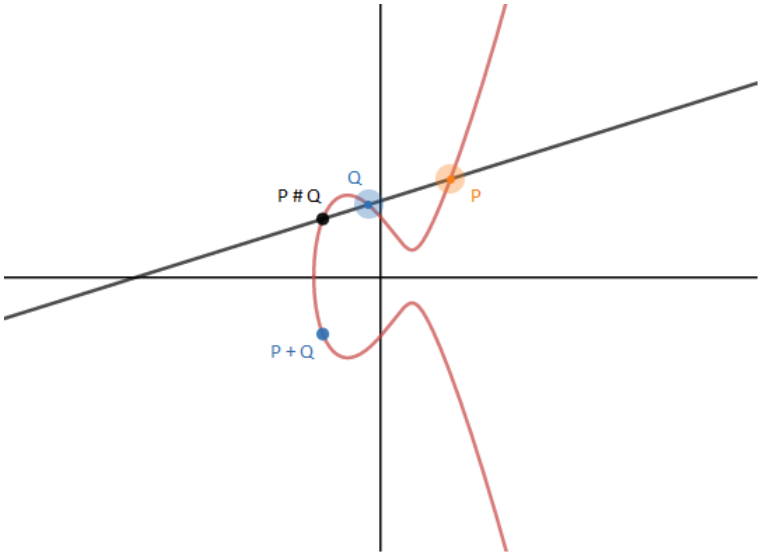
برای یک خم بیضوی، فرم‌های دیفرانسیل هلومورف یک فضای برداری ۱ بعدی روی K تشکیل می‌دهند. برای خم‌های بیضوی داده شده با فرم وایرشتراس، می‌توان فرم دیفرانسیل هلومورف زیر را در نظر گرفت:

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

به این فرم دیفرانسیلی، دیفرانسیل ناوردا گویند به آن دلیل که تحت انتقال با "عمل گروه" ثابت می‌ماند.

قضیه. برای این فرم دیفرانسیلی داریم $div\ \omega = 0$.

برهان. رجوع شود به حکم ۵.۱ از [۸].



شکل ۱: عمل گروه روی خم بیضوی

۲.۳ عمل گروه

بچت با استفاده از روش وتر-مماس[14]، روی یک خم هموار در صفحه از درجه ۳ که روی اعداد گویا تعریف شده است، توانست تعداد زیادی نقطه گویا پیدا کند. این روش بدین شکل است که فرض کنید نقطه‌ای گویا روی خم هموار درجه ۳ مثل x داریم. در این صورت خط مماس بر آن خم در نقطه x را در نظر بگیرید، از آن‌جایی که این خم از درجه ۳ است، این خط در جایی دیگر (با احتساب تکرر) این خم را قطع می کند. در این صورت آن نقطه جدید بدست آمده نیز، یک نقطه‌ی گویا روی این خم خواهد بود. برای این که این موضوع را ببینیم، می‌دانیم که خم از درجه ۳ است و ما به دنبال نقاط گویا روی یک خط هستیم، پس با جای‌گذاری معادله خط در خم درجه ۳، یک چندجمله‌ای درجه ۳ از یک متغیر پیدا می‌کنیم که ریشه‌های آن مختصه‌ی x یا y از تقاطع خط و خم هستند. ضرایب این چندجمله‌ای گویا هستند، زیرا خم ما روی اعداد گویا تعریف شده بود و پس مماس‌های آن در نقاط گویا، با ضرایب گویا داده شده‌اند. اما این چندجمله‌ای دو ریشه (مکرر) در x (که گویا است) دارد و پس ریشه دیگر آن نیز باید گویا باشد و پس آن نقطه روی خم نیز دارای مختصات گویا است.

در این بخش فرمول‌بندی بهتری برای این روش روی خم بیان می‌کنیم و یک عمل گروه روی خم بیضوی با استفاده از این روش می‌سازیم.

برای این کار یک خم بیضوی E با نقطه‌ی گویای $O = [0 : 1 : 0]$ فیکس کنید. می‌خواهیم روی $E(K)$ یک عمل گروه تعریف کنیم. پس دو نقطه $P, Q \in E(K)$ را در نظر می‌گیریم و جمع آن‌ها را به شکل هندسی نشان داده شده در شکل ۱ تعریف می‌کنیم. همچنین اگر بخواهیم نقطه‌ای را با خودش جمع کنیم، خط گذرنده از آن نقطه و خودش (خط مماس بر خم در آن نقطه) را در نظر می‌گیریم. این عمل خوش‌تعریف است، زیرا می‌توان مانند بالا استدلال کرد و نتیجه گرفت $P + Q \in E(K)$.

با استفاده از فرم وایرشتراس، می‌توان دید که یک خم بیضوی همواره دقیقاً یک نقطه در بی‌نهایت دارد که با مختصه‌های همگن $O = [0 : 1 : 0] \in E(K)$ داده می‌شود. این نقطه را همواره به عنوان نقطه گویای خم در نظر می‌گیریم و پس در عمل گروه پس از به دست آوردن $P \sharp Q$ باید آن را نسبت به محور x تقارن بدهیم تا $P + Q$ را بدست آوریم (در حالت کلی باید $P \sharp Q$ را به O وصل کنیم و نقطه‌ی سوم را بدست آوریم. اصول یک گروه را می‌توان به سادگی برای این عمل چک کرد (اثبات شرکت‌پذیری آن کمی سخت‌تر از بقیه است که این کار می‌توان با قضیه بزو انجام داد. رجوع شود به بخش ۲.۱ از [۷]). همچنین با روش بچت، می‌توان مختصه‌های نقطه $P + Q$ را محاسبه کرد.

در اینجا بهتر است روش دیگری را که با استفاده از آن می‌توان روی نقاط یک خم بیضوی عمل گروه قرار داد را نیز توضیح دهیم. این روش با استفاده از

[14] Chord-tangent

مقسم‌ها انجام می‌شود. ابتدا گروه $Pic^0(C)$ را برای یک خم جبری C تعریف می‌کنیم:

تعریف. فرض کنید C یک خم جبری روی میدان K باشد. در این صورت گروه $Pic(C)$ را برابر با خارج‌قسمت زیر تعریف می‌کنیم:

$$Pic(C) = \frac{Div(C)}{PDiv(C)} = \frac{Div(C)}{\{div\, f | f \in K(C)\}}$$

و گروه $Piv^0(C)$ را برابر با زیرگروه مقسم‌های درجه ۰ از $Pic(C)$ است:

$$Pic^0(C) = \frac{Div^0(C)}{PDiv(C)} = \frac{\{D | \deg D = 0\}}{\{div\, f | f \in K(C)\}}$$

حال قضیه‌ای بیان می‌کنیم که نشان می‌دهد گروه $Pic^0(E)$ برای هم خم بیضوی E، در واقع گروهی روی نقاط خم تعریف می‌کند که با گروه هندسی بیان شده یکی است.

قضیه. فرض کنید E یک خم بیضوی و P, Q نقاطی روی آن (در $E(\bar{K})$) باشند. در این صورت:

۱) $(P) \sim (Q)$ (P هم‌ارز خطی با Q است) $\Leftrightarrow P = Q$.

۲) تابع زیر یک ایزومورفیسم گروهی می‌دهد:

$$\sigma : E \to Pic^0(E)$$
$$P \mapsto (P) - (O)$$

برهان. رجوع شود به لم ۳.۳ و حکم ۴.۳ از [۸]

پس ما دو روش، یکی جبری و دیگری هندسی، برای این عمل گروهی تعریف کرده‌ایم که عملاً هر دو، همان روش بچت را می‌دهند.

در اینجا سوالی پیش می‌آید که آیا روی خم‌های دیگر نیز می‌توان چنین عمل گروهی روی نقاط یافت؟ در واقع اگر بخواهیم که اعمال گروه ما به اندازه کافی با ساختار جبری سازگار باشند، جواب "تقریباً" خیر است و قضیه زیر را داریم:

قضیه. فرض کنید C یک خم تصویری روی میدان بسته جبری $\bar{K}$ باشد بطوری که یک گروه جبری است (جمع و وارونی دارد که با توابع گویا داده شده‌اند) در این صورت گونه‌ی C برابر ۱ است.

تذکر. طبق این قضیه هر خم تصویری هموار که گروه جبری باشد، باید یک خم بیضوی باشد (روی فضای بسته جبری).

برهان. فرض کنید ω یک فرم دیفرانسیلی هلومورف روی خم باشد، در این صورت اگر برای نقطه‌ی P، تابع انتقال τ_P را برابر با $\tau_P(.) = P + .$ تعریف کنیم، $\tau_P^*\omega$ یک فرم دیفرانسیلی روی آن است که برای هر $Q \in C$ داریم:

$$ord_Q(\tau_P^*\omega) = ord_Q(\omega) \Rightarrow ord_P(\omega) = ord_Q(\omega)$$

پس روی نامتناهی نقطه، مرتبه ω باید ثابت باشد ولی درجه‌ی آن متناهی است، پس باید مرتبه آن روی همه نقاط صفر باشد و پس:

$$div\, \omega = 0 \Rightarrow \deg div\, \omega = 0$$

اما از طرفی از قضیه ریمان-رخ:

$$2g - 2 = \deg div\, \omega = 0 \Rightarrow g = 1$$

۳.۳ نقاط تابی

از آن‌جا عمل گروه خم بیضوی روی میدان K، یک گروه آبلی بدست می‌دهد، پس بررسی نقاط تابی آن اهمیت دارد. همچنین این زیرگروه تحت عمل گالوا ثابت می‌ماند که اهمیت آن را افزایش می‌دهد.

در تعریف زیر، از نماد $[n]P = \overbrace{P + P + \cdots + P}^{n \text{ بار}}$ و $[-n]P = \overbrace{(-P) + (-P) + \cdots + (-P)}^{n \text{ بار}}$ استفاده می‌کنیم:

تعریف. فرض کنید E یک خم بیضوی و O نقطه در بی‌نهایت آن (عضو خنثی جمع) باشد. منظور از نقاط n-تابی خم بیضوی، گروه مجرد زیر است:

$$E[n] := \{P \in E \mid [n]P = O\}$$

و گروه همه‌ی نقاط تابی را با E_{tors} نمایش می‌دهیم. پس

$$E_{tors} = \bigcup_{n=1}^{\infty} E[n]$$

همچنین نقاط $E(K)[n]$ و $E_{tors}(K)$ را برابر نقاط تابی که روی K تعریف شده‌اند، قرار می‌دهیم.

شناختن ساختار این زیرگروه‌ها، به شناخت ساختار گروهی خم‌های بیضوی بسیار کمک می‌کند. ابتدا این را برای خم‌های بیضوی روی اعداد گویا بررسی می‌کنیم.

فرض کنید E یک خم بیضوی روی اعداد مختلط باشد. پس می‌توان نقاط مختلط این خم بیضوی را در نظر گرفت $(E(\mathbb{C}))$ و در این صورت با استفاده از عمل گروه می‌توان یک گروه لی مختلط همبند فشرده یک بعدی آبلی پیدا کرد (فشرده بودن آن از تصویری بودن این خم بدست می‌آید). در این صورت با استفاده از یک قضیه معروف در نظریه گروه‌های لی داریم:

قضیه. یک گروه لی آبلی یک بعدی مختلط و همبند و فشرده، چنبره است.

طرح برهان. فرض کنید G این گروه لی باشد و T_eG فضای مماس در عضو خنثی باشد. در این صورت تابع

$$\exp : T_eG \to G$$

به طور موضعی یک دیفیومورفیسم می‌دهد و تصویر آن باز و بسته است (چون $\exp$ در این‌جا هوموفیسم است و تصویر آن یک همسایگی از عضو خنثی را دارد)، پس باید پوشا باشد و همچنین هسته‌ی آن یک زیرگروه گسسته از T_eG است. پس یک ایزومورفیسم به شکل زیر می‌دهد:

$$\exp : T_eG \to \frac{T_eG}{ker(\exp)} \xrightarrow{\sim} G$$

و پس از آن‌جا که G فشرده است، باید $ker(\exp)$ یک شبکه در $T_eG \cong \mathbb{C}$ باشد و پس $G \cong \frac{\mathbb{C}}{\mathbb{Z}^2} \cong S^1 \times S^1$. حال با استفاده از این قضیه، می‌توان ساختار $E(K)[n]$ را تا حدودی تعیین کرد.

قضیه. داریم: $E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

برهان. از قضیه قبل، $E(\mathbb{C}) \cong S^1 \times S^1$ و پس $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

همچنین می‌توان روی اعداد حقیقی نیز چنین کارهایی انجام داد و قضیه زیر را نتیجه گرفت.

قضیه. فرض کنید $E : y^2 = f(x)$ یک خم بیضوی روی $\mathbb{R}$ باشد. در این صورت داریم:

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times S^1 & f(x) \text{ سه جواب حقیقی دارد} \\ S^1 & f(x) \text{ یک جواب حقیقی دارد} \end{cases}$$

شکل ۲: دو حالت مختلف نقاط خم‌های بیضوی روی اعداد حقیقی

و پس به همین شکل نقاط تابی روی اعداد حقیقی آن نیز بدست می‌آید.

حال نقاط تابی را روی اعداد گویا و میدان‌های عددی بررسی می کنیم. پس فرض کنید E یک خم بیضوی روی یک میدان عددی K باشد. در این زمینه مقدار زیادی کار انجام شده و روی اعداد گویا و میدان‌های عددی با درجه کم روی اعداد گویا، انواع آن‌ها کاملاً شناسایی شده‌اند. پیدا کردن نقاط تابی روی خم‌های بیضوی با ضرایب صحیح با استفاده از قضیه زیر به سادگی انجام می‌شود:

قضیه. (ناگل-لوتز) خم بیضوی $y^2 = x^3 + Ax + B$ با $A, B \in \mathbb{Z}$ در نظر بگیرید. در این صورت اگر $P = (x, y)$ نقطه‌ای تابی باشد، آن‌گاه $x, y \in \mathbb{Z}$ و داریم: $y = 0$ یا $y^2 \mid \Delta_E$.

یک قضیه معروف و عمیق از میزر است که همه حالات نقاط تابی روی اعداد گویا را می‌دهد:

قضیه. (میزر) فرض کنید E یک خم بیضوی روی اعداد گویا باشد. در این صورت داریم: $E_{tors}(\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$ برای $1 \leq n \leq 10$ یا $n = 12$ و یا $E_{tors}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ برای $1 \leq n \leq 4$.

همچنین روی میدان‌های عددی دیگر نیز نتایجی بدست آمده که از مهم‌ترین آن‌ها قضیه‌ای بود که مرل[15] در سال ۱۹۹۴ اثبات کرد:

قضیه. (مرل) برای هر عدد صحیح مثبت d یک ثابت $B(d)$ وجود دارد که برای هر خم بیضوی روی میدان عددی K با $[K : \mathbb{Q}] = d$ داریم:

$$|E(K)_{tors}| \leq B(d)$$

۴.۳ کاستن به پیمانه $\mathfrak{p}$

در این بخش در مورد کاستن یک خم بیضوی تعریف شده روی یک میدان عددی، به پیمانه‌ی یک ایدآل اول $\mathfrak{p}$ را توضیح می‌دهیم. پس فرض کنید K یک میدان عددی و E/K یک خم بیضوی باشد که مثلاً با $E : y^2 = x^3 + Ax + B$ داده شده است. در این صورت خم بیضوی $\bar{E}/\mathbb{F}_\mathfrak{p} : y^2 = x^3 + \bar{A}x + \bar{B}$ که $\bar{A}, \bar{B}$ تصویر A, B در $\mathbb{F}_\mathfrak{p}$ هستند را کاستن خم بیضوی به پیمانه $\mathfrak{p}$ می‌نامیم. اگر $\mathfrak{p} \nmid \Delta_E$ در این صورت $\bar{E}$ نیز یک خم بیضوی خواهد بود. در این حالت آن ایدآل را اول خوب می‌نامیم. اگر به پیمانه آن ایدآل اول، هموار نباشد، دو حالت داریم:

۱)به پیمانه آن اول، یک گره[16] داشته باشیم، که به آن یک کاستن ضربی می‌گوییم.

۲)به پیمانه آن ایدآل اول، یک نوک هلال[17] داشته باشیم که به آن کاستن جمعی گوییم.

[15] Merel
[16] Node
[17] Cusp

به یک ایدآل اول نیمه پایدار گوییم هرگاه آن اول یک اول خوب یا به پیمانه آن یک کاستن ضربی داشته باشیم.

تذکر. این واژه‌گذاری به دلیل آن است که در حالات ناهموار، خم بیضوی بجز آن نقطه‌ی هموار یک ساختار گروهی دارد که در حالت کاستن ضربی با $\mathbb{F}_{\mathfrak{p}}^*$ و در حالت کاستن جمعی با $\mathbb{F}_{\mathfrak{p}}^+$ ایزومورف می‌شود.

یکی از کاربردهایی که کاستن به پیمانه یک ایدآل اول دارد، قضیه زیر است:

قضیه. فرض کنید E خم بیضوی روی اعداد گویا باشد و p یک عدد اول باشد که $p \nmid 2\Delta_E$. در این صورت هomomورفیسم طبیعی $E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$ یک‌به‌یک است.

در قسمت مثال‌ها، نحوه استفاده از این قضیه را برای بدست آوردن نقاط مرتبه متناهی توضیح می‌دهیم.

۵.۳ یک‌جنسی

از این به بعد یک خم بیضوی E با نقطه K-گویای O را با (E, O) نمایش می‌دهیم. حال مورفیسم‌های بین خم‌های بیضوی را بررسی می‌کنیم. تاکنون دیدیم که یک خم بیضوی به همراه ساختار گروهی‌اش، تشکیل یک گروه جبری می‌دهد، پس منطقی است مورفیسم‌های بین آن‌ها را برابر با مورفیسم‌های گروه جبری‌ای بین آن‌ها قرار دهیم. در واقع قضیه زیر یک شرط کافی برای بررسی مورفیسم بودن یک تابع بین دو خم بیضوی می‌دهد.

قضیه. فرض کنید (E_1, O_1) و (E_2, O_2) دو خم بیضوی باشند. اگر $\phi : E_1 \to E_2$ مورفیسمی جبری (به عنوان دو خم جبری) باشد که $\phi(O_1) = O_2$، آن‌گاه ϕ یک مورفیسم از آن‌ها به عنوان دو گروه جبری نیز هست.

برهان. در اینجا از معادل بودن دو تعریف معادل برای عمل گروه یک خم بیضوی استفاده می کنیم. در واقع نمودار زیر را در نظر بگیرید:

$$\begin{array}{ccc} E_1(\bar{K}) & \xrightarrow{\sim} & Pic^0(E_1) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ E_2(\bar{K}) & \xrightarrow{\sim} & Pic^0(E_2) \end{array}$$

می‌خواهیم g را طوری تعریف کنیم که نمودار بالا جابجا شود. پس قرار دهید:

$$g([\sum n_P(P)]) = [\sum n_P(g(P))]$$

برای هر مقسم. می توان به سادگی چک کرد که g خوش‌تعریف و هomomورفیسم است و با نمودار بالا جابجا می شود. پس از آن‌جا که هomomورفیسم‌های افقی ایزومورفیسم هستند، f نیز باید هomomورفیسم و پس مورفیسمی از گروه‌های جبری باشد.

تعریف. یک‌جنسی $f : (E_1, O_1) \to (E_2, O_2)$ یک مورفیسم از این دو خم بیضوی به عنوان گروه‌های جبری است. به دو خم (E_1, O_1) و (E_2, O_2) یک‌جنس گویند هر گاه یک یک‌جنسی $f : (E_1, O_1) \to (E_2, O_2)$ وجود داشته باشد. یک‌جنس بودن یک رابطه‌ی هم‌ارزی است (البته این حکم بدیهی نیست).

پس یک کتگوری از خم‌های بیضوی روی میدان K با نقاط K-گویا تشکیل می‌دهیم به همراه یک‌جنسی‌ها به عنوان مورفیسم‌ها.

پس $Hom(E_1, E_2)$ را برابر با همه‌ی یک‌جنسی‌ها از (E_1, O_1) به (E_2, O_2) قرار می‌دهیم. همچنین، $End(E) = Hom(E, E)$. مجموعه‌ی یک‌جنسی‌های وارون‌پذیر در $End(E)$ را با $Aut(E)$ نمایش می‌دهیم. همچنین $Hom_L(E_1, E_2)$ و $End_L(E)$ و $Aut_L(E)$ را برابر با یک‌جنسی‌های مربوط و تعریف شده روی میدان L قرار می‌دهیم.

حال درجه یک یک‌جنسی را تعریف می‌کنیم:

تعریف. فرض کنید $f : E_1 \to E_2$ یک یک‌جنسی غیر ثابت باشد. در این صورت خواهیم داشت $f^*(\bar{K}(E_2)) \subseteq \bar{K}(E_1)$ یک توسیع متناهی از میدان‌ها خواهد بود و درجه f را برابر با $[\bar{K}(E_1) : f^*(\bar{K}(E_2))]$ تعریف می‌کنیم و با $\deg(f)$ نمایش می‌دهیم. همچنین درجه‌ی یک جنسی ثابت $[0]$ را برابر با 0 تعریف می‌کنیم.

درجه خاصیت ضربی دارد. به عبارت دیگر، اگر یک‌جنسی‌های زیر را داشته باشیم:

$$\phi : E_1 \to E_2, \quad \psi : E_2 \to E_3$$

در این صورت:

$$\deg(\psi \circ \phi) = \deg(\phi)\deg(\psi)$$

مثال. مهم‌ترین مثال از یک‌جنسی‌ها، درون‌ریختی‌های $[m] : E \to E$ برای $m \in \mathbb{Z}$ هستند. در این صورت $[m]$ روی K تعریف شده است و به سادگی می‌توان چک کرد که این یک‌جنسی به جز در حالت $m = 0$ ثابت نیست.

قضیه. ۱) $Hom(E_1, E_2)$ یک گروه آبلی بدون عضو تابی است.

۲) فرض کنید E یک خم بیضوی باشد. در این صورت $End(E)$ یک حلقه با مشخصه ۰ و بدون مقسوم‌علیه صفر است.

برهان. ۱) فرض کنید برای $f \neq [0]$ داشتیم $[n]f = 0$. در این صورت داریم:

$$0 = \deg([n]f) = \deg([n])\deg(f) \neq 0$$

چون هیچ‌کدام از f و $[n]$ها یک‌جنسی ثابت نیستند.

۲) از قسمت اول داریم که این حلقه مشخصه صفر دارد. اگر $\phi \circ \psi = [0]$ برای دو یک‌جنسی غیرثابت ϕ و ψ. آن‌گاه:

$$0 = \deg([0]) = \deg(\phi \circ \psi) = \deg(\phi)\deg(\psi) \neq 0$$

که تناقض است.

۶.۳ قضیه موردل-وی

قضیه موردل-وی در مورد ساختار گروهی نقاط یک خم بیضوی روی میدان‌های عددی صحبت می‌کند. به‌طور دقیق‌تر این قضیه می‌گوید:

قضیه. (موردل-وی) فرض کنید E یک خم بیضوی و K یک میدان عددی باشد. در این صورت $E(K)$ یک گروه آبلی متناهی‌تولید است.

برای اثبات این قضیه ابتدا باید قضیه ضعیف موردل-وی را مطرح و اثبات کنیم و سپس با استفاده از روشی مانند نزول نامتناهی فرما می‌توانیم آن را ثابت کنیم.

قضیه. (ضعیف موردل-وی) اگر E یک خم بیضوی و K یک میدان عددی باشد، در این صورت $E(K)/mE(K)$ برای هر m طبیعی متناهی است.

برای اثبات این قضیه، $E(K)/mE(K)$ را در گروهی متناهی به نام گروه m-ام سلمر می نشانیم. برای این کار دنباله دقیق زیر را در نظر بگیرید:

$$0 \to E(\bar{K})[m] \xrightarrow{[m]} E(\bar{K}) \to E(\bar{K}) \to 0$$

در این صورت $G_K = Gal(\bar{K}/K)$ روی آن عمل می‌کند و با استفاده از دنباله دقیق بلند کوهمولوژی گالوا داریم:

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K) \to H^1(G_K, E(\bar{K})[m]) \to H^1(G_K, E(\bar{K})) \xrightarrow{m} H^1(G_K, E(\bar{K})) \to \cdots$$

و پس از این می‌توان دنباله دقیق کوتاه زیر را ساخت:

$$0 \to E(K)/mE(K) \to H^1(G_K, E(\bar{K})[m]) \to H^1(G_K, E(\bar{K}))[m] \to 0$$

اما متأسفانه گروه $H^1(G_K, E(\bar{K})[m])$ متناهی نیست و باید آن را کوچک‌تر کنیم. پس دیاگرام زیر را در نظر بگیرید:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E(\bar{K})[m]) & \longrightarrow & H^1(G_K, E(\bar{K}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in M_K} E(K_v)/mE(K_v) & \longrightarrow & \prod_{v\in M_K} H^1(G_{K_v}, E(\bar{K_v})[m]) & \longrightarrow & \prod_{v\in M_K} H^1(G_{K_v}, E(\bar{K_v}))[m] & \longrightarrow & 0 \end{array}$$

که M_K مجموعه‌ی همه‌ی اول‌ها (ارشمیدسی و غیرارشمیدسی) K است.

حال گروه m-ام سلمر را تعریف می‌کنیم:

$$Sel_m(E/K) = \ker\{H^1(G_K, E(\bar{K})[m]) \to \prod_v H^1(G_{K_v}, E(\bar{K_v}))\}$$

حال قضیه زیر را داریم.

قضیه. گروه $Sel_m(E/K)$ متناهی است.

طرح برهان. فرض کنید $\mathfrak{p}$ ایدآلی اول در K باشد که m را عاد نمی‌کند و خم بیضوی در آن کاستن بد ندارد. . در این صورت به سادگی دیده می شود که $E(K)[m] \to E(\mathbb{F}_{N\mathfrak{p}})$ یک‌به‌یک است. پس اگر یک هم‌دور σ در $Sel_m(E)$ داشته باشیم، این هم‌دور باید در $\mathfrak{p}$ غیرشاخه‌ای باشد. حال از آن‌جا که $E(\bar{K})[m]$ متناهی است، این هم‌دور از یک توسیع متناهی مثل L/K فاکتور گرفته می‌شود:

$$Gal(\bar{K}/K) \to Gal(L/K) \to E(\bar{K})[m]$$

و پس اگر قرار دهیم S را مجموعه‌ی متناهی همه ایدآل‌های اول قرار دهیم که خم در آن‌ها کاستن بد (غیرخوب!) دارد یا m را عاد می‌کنند، آن‌گاه L باید بیرون S غیرشاخه‌ای باشد. همچنین از آن‌جا که $E[m]$ آبلی است، $Gal(L/K)$ باید آبلی باشد. حال طبق قضیه‌ی هرمیت-مینکوفسکی می‌دانیم که متناهی توسیع S-غیرشاخه‌ای از درجه کراندار یک میدان عددی وجود دارد. پس برای همه‌ی هم‌دورها متناهی‌تا توسیع L/K یافت می‌شود. پس همه‌ی توابع $Gal(L/K) \to E[m]$ برای همه‌ی چنین توسیع‌هایی متناهی است و پس همچنین تعداد هم‌دور ها متناهی است.

پس اثبات قضیه ضعیف موردل-وی انجام می‌شود. حال برای این‌که قضیه موردل-وی را اثبات کنیم، نیاز به یک تابع "ارتفاع" روی نقاط خم بیضوی داریم:

قضیه. تابع $h : E(K) \to [0, \infty)$ وجود دارد که خواص زیر را دارد:

۱) برای همه $P \in E(K)$ داریم $h(mP) = m^2h(P) + O(1)$

۲) برای همه $P, Q \in E(K)$ داریم $h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1)$

۳) برای هر $H \geq 0$، $\{P \in E(K) \mid h(P) \leq H\}$

به این تابع تابع ارتفاع گفته می‌شود.

ایده برهان. تابع $h : \mathbb{P}^2(K) \to [0, \infty)$ را برابر با مقدار زیر تعریف کنید:

$$h([x : y : z]) = \sum_{v\in M_K} \log \max(|x|_v, |y|_v, |z|_v)$$

که M_K مجموعه‌ی همه‌ی اول‌ها (ارشمیدسی و غیرارشمیدسی) K است. می‌توان چک کرد که تحدید این تابع به خم بیضوی در خواص بالا صدق می‌کند. برای رهایی از $O(1)$ها نیز می‌توان ازتفاع کانونی (نرون-تیت) را تعریف کرد: $\hat{h} : P \mapsto \lim_{n\to\infty} \frac{h(2^n P)}{4^n}$ و این ارتفاع کانونی این خاصیت مهم را دارد که یک فرم درجه ۲ روی $E(K)$ می‌دهد.

حال اثبات قضیه موردل-وی را کامل می‌کنیم. قضیه ضعیف موردل-وی می‌گوید که $E(K)/2E(K)$ متناهی است. فرض کنید $P_1, P_2, \cdots, P_n$ یک مجموعه کامل از نمایشگرهای هم‌مجموعه‌های $E(K)/2E(K)$ باشد. حال قرار دهید $S = \{P \in E(K) \mid h(P) \leq \max_i(h(P_i))\}$ ادعا می‌کنیم که این مجموعه‌ی متناهی، $E(K)$ را می‌سازد. فرض کنید نسازد و Q نقطه‌ای با ارتفاع کانونی مینیمال در بیرون S باشد. در این صورت از آن‌جا که $\{P_1, P_2, \cdots, P_n\}$ مجموعه کاملی به پیمانه $2E(K)$ هستند، پس برای i و Rی داریم: $P = P_i + 2R$

حال به دلیل خاصیت مینیمال Q داریم:

$$\hat{h}(Q) \leq \hat{h}(R) = \frac{1}{4}\hat{h}(2R) \leq \frac{1}{4}\hat{h}(Q - P_i) \leq \frac{2}{4}(\hat{h}(Q) + \hat{h}(P_i)) \leq \frac{1}{2}(\hat{h}(Q) + \max_i(\hat{h}(P_i))$$

و پس

$$\hat{h}(Q) \leq \max_i(\hat{h}(P_i))$$

که تناقض است و اثبات قضیه موردل-وی به پایان می‌رسد.

پس از قضیه موردل-وی نتیجه می‌شود که $E(K)$ را به عنوان گروه‌های مجرد می‌توان به شکل زیر نمایش داد:

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^{r_E}$$

همچنین قضایایی که قبلاً بیان کردم باعث می‌شوند که شناسایی $E(K)_{tors}$ برای میدان‌های عددی با درجه کم، نسبتاً راحت باشد. ولی در مورد r_E (حتی برای $K = \mathbb{Q}$) به همین سادگی نیست و قضیه‌ها و حکم‌های کمی در مورد آن وجود دارد. (البته با فرض حدس بیرچ سوینرتون-دیر محاسبه آن روی اعداد گویا ساده‌تر می‌شود).

۷.۳ ضرب مختلط

در این بخش خم‌های بیضوی با ضرب مختلط را توضیح می‌دهیم و نشان می‌دهیم که خواص شگفت‌انگیزی دارند. مرجع اصلی این بخش [۹] و [۱۰] بوده است.

روی یک خم بیضوی همواره درون‌ریختی‌های $[n]$ برای $n \in \mathbb{Z}$ وجود دارد. این که آیا درون‌ریختی‌های دیگر روی یک خم بیضوی وجود دارد، ما را به مفهوم ضرب مختلط می‌رساند. پس خم بیضوی با ضرب مختلط را به شکل زیر تعریف می‌کنیم:

تعریف. به خم بیضوی E تعریف شده روی اعداد مختلط، خم بیضوی با ضرب مختلط گویند هرگاه یک درون‌ریختی دیگر به جز $[n]$ها وجود داشته باشد.

قضیه زیر استفاده از این واژه برای این تعریف را معین می‌کند:

قضیه. فرض کنید E خمی بیضوی روی اعداد مختلط باشد. در این صورت $End(E)$ یکی از حالت‌های زیر را دارد:

۱) $End(E) \cong \mathbb{Z}$.

۲) $End(E)$ با یک دسته در میدان عددی درجه دو و مختلط ایزومورف است.

تذکر. یک دسته در یک میدان عددی K، یک زیرحلقه R است بطوری که به عنوان گروه آبلی متناهی تولید باشد و داشته باشیم: $R \otimes \mathbb{Q} = K$.

حال خم‌های بیضوی روی اعداد مختلط را می‌توان با استفاده از تابع پی وایرشتراس به شکل ساده‌تری نگاه کرد (گفته شد که با چنبره ایزومورف هستند). در واقع قضیه زیر را داریم:

قضیه. فرض کنید Λ شبکه‌ای در اعداد مختلط (دو بعدی روی اعداد حقیقی) باشد و قرار دهید:

$$g_2(\Lambda) = 60 \sum_{0\neq\omega\in\Lambda} \frac{1}{\omega^4}, \quad g_3(\Lambda) = 140 \sum_{0\neq\omega\in\Lambda} \frac{1}{\omega^6}$$

و همچنین قرار دهید

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{0\neq\omega\in\Lambda} (\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$$

در این صورت قرار دهید:

$$E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

این خم، یک خم بیضوی خواهد بود و داریم که تابع

$$\wp : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad z \mapsto [\wp(z) : \wp'(z) : 1]$$

یک ایزومورفیسم تحلیلی از گروه‌های لی مختلط است.

ایده برهان. برهان این چیزی به جز بسط دادن $\wp$ و مشتق گرفتن و چک کردن این رابطه نیست. همچنین ایزومورفیسم بودن روی ساختار گروه از چک کردن آن روی مقسم‌ها نتیجه می‌شود.

پس به هر خم بیضوی E به این شکل یک شبکه در اعداد مختلط مانند Λ نسبت داده می‌شود بطوری که $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. پس مجموعه‌ی $End(E)$ برابر با همه‌ی $\alpha \in \mathbb{C}$هایی خواهد بود بطوری که $\alpha\Lambda \subseteq \Lambda$. در واقع برای این‌که این تابع یک تابع جمعی تحلیلی از $\mathbb{C}/\Lambda$ به خودش شود، باید بتوان آن‌را به‌طور پیوسته روی پوشش جهانی آن، که برابر $\mathbb{C}$ است، گسترش داد. در این صورت تابعی خواهیم داشت از $\mathbb{C}$ به $\mathbb{C}$ بطوری که جمعی است، و در این صورت طبق قضیه‌ای ساده، باید برابر با $z \mapsto \alpha z$ برای $\alpha \in \mathbb{C}$ای باشد و به‌وضوح این تابع باید Λ را به داخل خودش ببرد. پس کلمه‌ی "ضرب مختلط" به این شکل توجیه می‌شود.

واضح است که برای هر n صحیح، تابع $z \mapsto nz$ شبکه را به خودش می‌برد - این توابع همان $[n]$ها هستند که در حالت جبری بررسی کردیم - همچنین اگر $\alpha \in \mathbb{R}$، آن‌گاه از آن‌جا باید شبکه به خودش نگاشته شود، باید داشته باشیم: $\alpha \in \mathbb{Z}$.

برهان قضیه. فرض کنید خم بیضوی E ضرب مختلط داشته باشد. در این صورت شبکه وابسته به خم بیضوی را Λ بنامید. پس داریم:

$$End(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$$

ادعا می‌کنم همه‌ی αها در یک میدان درجه ۲ و مختلط قرار دارند. درواقع فرض کنید Λ با دو عضو ω_1, ω_2 ساخته شود. در این صورت از رابطه‌ی $\alpha\Lambda \subseteq \Lambda$ داریم که باید ماتریس $A \in M_2(\mathbb{Z})$ باشد که $\alpha \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ پس $(\alpha I - A) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = 0$ و پس دترمینان ماتریس سمت چپ باید صفر باشد که نشان می‌دهد α در یک معادله‌ی درجه ۲ روی اعداد صحیح (که ضریب پیشروی آن ۱ است) صدق می‌کند. پس همه‌ی اعضای میدان $End(E) \otimes \mathbb{Q}$ در یک معادله‌ی درجه ۲ روی اعداد گویا صدق می‌کنند، پس میدان باید روی اعداد گویا درجه ۲ باشد. همچنین گفتیم که اگر $\alpha \in \mathbb{R}$ آنگاه باید $\alpha \in \mathbb{Z}$ پس میدان باید درجه ۲ و مختلط باشد. همچنین همه‌ی αها باید عدد صحیح جبری باشند، پس باید دسته باشد. (همچنین این استدلال نشان می‌دهد که دسته‌ی ماکسیمال باید مجموعه‌ی اعداد صحیح جبری باشد، در واقع هر دسته به عنوان حلقه‌ی درون‌ریختی‌های یک خم بیضوی می‌آید (اعداد مختلط تقسیم بر آن دسته)).

حال قضیه‌ی زیر را داریم:

قضیه. فرض کنید R یک دسته در یک میدان درجه ۲ مختلط باشد. در این صورت مجموعه‌ی خم‌های بیضوی با حلقه‌ی درون‌ریختی‌های R در حد ایزومورفیسم، تناظر یک‌به‌یکی با $Cl(R)$ دارد.

ایده‌ی برهان. یک عمل متعدی ساده از $Cl(R)$ روی خم‌های بیضوی با درون‌ریختی‌های R وجود دارد (E_Λ خمی بیضوی است که به شبکه Λ نسبت داده شده است.):

$$\mathfrak{a} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

حال قضیه‌ای غافلگیرانه در مورد این خم‌ها وجود دارد که بیان می‌کنیم:

قضیه. فرض کنید K یک میدان مربعی مختلط باشد و E یک خم بیضوی با حلقه‌ی درون‌ریختی‌های ماکسیمال O_K. در این صورت:

۱) j_E یک عدد صحیح جبری است.

۲) $K(j_E)$ میدان رده‌ای هیلبرت K است.

۳) $Gal(K(j_E)/K)$ روی مجموعه‌ی $\{j_E \mid End(E) = O_K\}$ به شکل متعدی عمل می‌کند.

همچنین هسه قضیه زیر را اثبات کرد که عمل گالوا را روی j-ناورداها مشخص می‌کند.

قضیه. با فرضیات قضیه بالا، فرض کنید $\mathfrak{p}$ یک ایدآل اول خوب از K برای E باشد. در این صورت با نمادگذاری بالا داریم:

$$Frob_\mathfrak{p}(j_{E_\Lambda}) = j_{E_{\Lambda\mathfrak{p}^{-1}}}$$

از آنجا که عمل عناصر فروبنیوس عملاً از گروه $Cl(O_K)$ فاکتور گرفته می‌شود، پس قضیه بالا می‌گوید که عمل $Cl(O_K)$ روی خم‌های بیضوی با حلقه‌ی درون‌ریختی‌های O_K یک انتقال است.

برای برهان این قضایا به [۱۰] رجوع شود. همچنین قضیه زیر نیز در آن اثبات شده که از تکنیک‌های نظریه میدان‌های رده‌ای و قضایای بالا برای اثبات آن استفاده می‌کند:

قضیه. فرض کنید E یک خم بیضوی با حلقه‌ی درون‌ریختی‌های O_K باشد. در این صورت مختصات نقاط تابی (برای هر مختصه‌بندی‌ای) را به K اضافه کنید و میدان بدست آمده را L بنامید. در این صورت L توسیع آبلی ماکسیمال K است.

۴ فرم‌های مدولار

در این بخش فرم‌های مدولار را بررسی می‌کنیم و در مورد مفهوم‌هایی کلی و مخصوصاً مفهوم‌هایی از فرم‌های مدولار که در اثبات وایلز از قضیه آخر فرما کاربرد دارند صحبت می‌کنیم. در ابتدا تعریف فرم‌های مدولار روی زیرگروه‌های هم‌نهشتی را بیان می‌کنیم. سپس در مورد خواص تحلیلی فرم‌های مدولار صحبت می‌کنیم و پس از آن عملگرهای هکه را تعریف می‌کنیم و در مورد ضرب داخلی پترسون و سازگاری آن با عملگرهای هکه صحبت می‌کنیم. پس از آن در مورد خم‌های پیمانه‌ای کمی توضیح می‌دهیم.

۱.۴ تعاریف

ابتدا باید یک تابع مدولار[۱۸] را تعریف کنیم. نیم‌صفحه‌ی بالای صفحه مختلط را در نظر بگیرید و آن را با $\mathbb{H}$ نمایش دهید. در این صورت گروه $SL_2(\mathbb{Z})$ روی آن با توابع موبیوس[۱۹] عمل می‌کند: فرض کنید $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ یک ماتریس در $SL_2(\mathbb{Z})$ باشد. در این صورت عمل آن را قرار دهید:

$$z \mapsto \frac{az+b}{cz+d}, \quad z \in \mathbb{H}$$

حال توابع مدولار را تعریف می‌کنیم:

تعریف. به تابع مرومورفیک[۲۰] $f : \mathbb{H} \to \mathbb{C}$ یک تابع مدولار از وزن k گویند هرگاه برای هر ماتریس $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ داشته باشیم:

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

در این صورت به سادگی می‌توان دید که برای kهای فرد فقط تابع 0 را داریم. حال علاقه‌مندیم که شروط بیشتری، مانند تحلیلی بودن و ... را برای آن قرار دهیم. برای این‌کار ابتدا ∞ را به فضای $\mathbb{H}$ اضافه می‌کنیم و آن را فشرده می‌کنیم. حال از آن‌جا که $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$، پس برای یک تابع مدولار، مثل f، داریم $f(z+1) = f(z)$ و پس تناوبی است و می‌توان بسط فوریه آن را نوشت:

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n z}, \quad a_n \in \mathbb{C}$$

حال می‌توان فرم مدولار[۲۱] را تعریف کرد.

تعریف. به یک تابع مدولار f، فرم مدولار می‌گوییم هرگاه روی $\mathbb{H}$ و ∞ تحلیلی باشد. شرط آخر به این معنی است که بسط فوریه‌ی f از $n = 0$ شروع شود و برای nهای منفی $a_n = 0$.

فضای همه‌ی فرم‌های مدولار از وزن k را با $M_k(SL_2(\mathbb{Z}))$ نمایش می‌دهیم. حال اگر یک فرم مدولار در کاسپ (∞) صفر باشد، به آن یک فرم کاسپ[۲۲] گوییم. (این بدان معنی است که علاوه بر nهای منفی، برای $n = 0$ نیز داشته باشیم: $a_0 = 0$.) همچنین فضای همه‌ی فرم‌های کاسپ را با $S_k(SL_2(\mathbb{Z}))$ نمایش می‌دهیم. این مجموعه‌ها، فضای برداری روی $\mathbb{C}$ تشکیل می‌دهند و می‌توان به سادگی اثبات کرد که بعد این فضاها متناهی است (در بخش‌های بعد این

[18] Modular function
[19] Mobius
[20] Meromorphic
[21] Modular form
[22] Cusp form

کار را انجام می‌دهیم). همچنین همان‌گونه که در مقدمه گفتیم، می توان به جای $SL_2(\mathbb{Z})$ از یک زیرگروه آن به نام زیرگروه‌های هم‌نهشتی استفاده کرد. ابتدا گروه‌های هم‌نهشتی اصلی را تعریف می‌کنیم:

فرض کنید N یک عدد نامنفی باشد.

$$\Gamma(N) := \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \}$$

از آنجا که این زیرگروه برابر با هسته‌ی تصویر زیر است:

$$SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$$

پس اندیس $\Gamma(N)$ در $SL_2(\mathbb{Z})$ متناهی است. حال به همه‌ی زیرگروه‌هایی از $SL_2(\mathbb{Z})$ بطوری که $\Gamma(N)$ را برای Nی داشته باشند، زیرگروه‌های هم‌نهشتی گوییم. یک زیرگروه هم‌نهشتی Γ فیکس کنید. در این صورت در تعریف تابع مدولار می‌توان به جای $SL_2(\mathbb{Z})$، Γ را قرار داد و تعریف تابع مدولار از وزن k روی Γ را پیدا کرد، اما برای یک فرم مدولار اول باید معنی نقاط بی‌نهایت این زیرگروه هم‌نهشتی را مشخص کنیم. اول به فضای $\mathbb{H}$، $\mathbb{P}^1_{\mathbb{Q}}$ را به طور مجزا اضافه می‌کنیم و با Γ روی آن عمل می‌کنیم بدین شکل که: بدین شکل که با $\frac{a}{b}$ مانند $\begin{bmatrix} a \\ b \end{bmatrix}$ رفتار می‌کنیم و با ∞ مانند $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ رفتار می‌کنیم. حال داریم که تعداد مدارهای این عمل روی $\mathbb{P}^1_{\mathbb{Q}}$ متناهی هستند (زیرا اندیس Γ در $SL_2(\mathbb{Z})$ متناهی است و $SL_2(\mathbb{Z})$ فقط یک مدار دارد). حال این مدارها را برابر با نقاط کاسپ این زیرگروه هم‌نهشتی تعریف می‌کنیم (در واقع این‌ها همان نقاطی‌اند که برای فشرده‌سازی $\mathbb{H}/\Gamma$ باید قرار دهیم). حال می‌توانیم فرم‌های مدولار و کاسپ روی Γ را تعریف کنیم.

تعریف. به یک تابع مدولار از وزن k روی Γ یک فرم مدولار روی Γ گوییم هرگاه روی $\mathbb{H}$ و کاسپ‌ها تحلیلی باشد. شرط آخر بدین معنی است که $\frac{1}{(cz+d)^k} f(\frac{az+b}{cz+d})$ برای همه‌ی $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ در بی‌نهایت تحلیلی باشد.

در واقع در این جا نیز (از آنجا که اندیس Γ متناهی است) برای $q \in \mathbb{Z}$ مینیمالی داریم $\begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$ و پس می‌توان بسط فوریه به شکل زیر برای f نوشت:

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n z/q}, \quad a_n \in \mathbb{C}$$

و پس این که f در بی‌نهایت تحلیلی باشد نیز برای این توابع معنی دارد. همچنین مانند بالا می‌توان فرم کاسپ را تعریف کرد که در همه‌ی تابع در همه‌ی کاسپ‌ها صفر شود. همچنین مانند بالا مجموعه‌ی همه‌ی فرم‌های مدولار و فرم‌های کاسپ از وزن k روی Γ را به ترتیب با $M_k(\Gamma)$ و $S_k(\Gamma)$ نمایش می‌دهیم. همچنین این‌ها نیز فضاهای برداری متناهی‌بعد روی $\mathbb{C}$ تشکیل می‌دهند.

۲.۴ مثال‌ها

اولاً قرار دهید $\Gamma = SL_2(\mathbb{Z})$. معروف‌ترین مثال‌های فرم‌های مدولار چنین فضایی سری‌های آیزنشتاین[۲۳] هستند. سری آیزنشتاین از وزن زوج $k > 2$ را به شکل زیر تعریف می‌کنیم:

$$G_k(z) = \sum_{(n,m)} \frac{1}{(nz+m)^k}, \quad z \in \mathbb{H}$$

[23] Eisenstein series

که مجموع روی همه‌ی n, mهای صحیح بجز $(0,0)$ انجام می‌شود. در این صورت این یک فرم مدولار از وزن k خواهد بود. در واقع، فرض کنید $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \gamma \in SL_2(\mathbb{Z})$. در این صورت:

$$G_k(\gamma(z)) = \sum_{(n,m)} \frac{1}{(n(\frac{az+b}{cz+d}) + m)^k} = (cz+d)^k \sum_{(n,m)} \frac{1}{((na+mc)z + (nb+md))^k} = (cz+d)^k G_k(z)$$

همچنین با استفاده از مشتق‌گیری‌های پی‌درپی از عبارت زیر می‌توان بسط فوریه سری‌های آیزنشتاین را بدست آورد:

$$\frac{1}{z} + \sum_{d \geq 1} (\frac{1}{z-d} + \frac{1}{z+d}) = \pi \cot \ \pi z = \pi i - 2\pi i \sum_{m=0}^{\infty} q^m, \quad q = e^{2\pi i z}$$

و خواهیم داشت:

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

که $\sigma_{k-1}(n)$ جمع توان‌های $k-1$ام مقسوم‌علیه‌های مثبت n است. پس این سری‌ها فرم‌های کاسپ نیستند، زیرا در بی‌نهایت برابر $2\zeta(k)$ می‌شوند.

در قسمت خم‌های بیضوی توابع g_2, g_3 را معرفی کردیم، می‌توان به سادگی رابطه‌ی بین آنها و سری‌های آیزنشتاین را پیدا کرد و پس داریم:

$$g_2(z) = 60G_4(\tau), \ g_3(\tau) = 140G_6(\tau)$$

همچنین خم بیضوی زیر را تشکیل دادیم:

$$E : y^2 = 4x^3 - g_2(z)x - g_3(z)$$

و پس می‌توان توابع تفکیک‌کننده و j-ناوردا را تعریف کرد:

$$\Delta : \mathbb{H} \to \mathbb{C}, \quad \Delta(z) = (g_2(z))^3 - 27(g_3(z))^2$$
$$j : \mathbb{H} \to \mathbb{C}, \quad j(z) = 1728\frac{(g_2(z))^3}{\Delta(z)}$$

با استفاده از وزن سری‌های آیزنشتاین داریم که Δ از وزن ۱۲ و j از وزن ۰ است (در واقع می‌بینیم که فرم مدولار نیست بلکه تابع مدولار است). در واقع، با استفاده از بسط فوریه‌ی سری‌های آیزنشتاین داریم که

$$\Delta(\infty) = (120\zeta(4))^3 - 27(280\zeta(6))^2 = 0$$

و پس تفکیک‌کننده یک فرم کاسپ در $S_{12}(SL_2(\mathbb{Z}))$ است. اما j-ناوردا یک فرم مدولار نیست، در واقع $g_2(\infty)$ صفر نیست ولی از بالا، $\Delta(\infty) = 0$، پس j در بینهایت تحلیلی نیست (در واقع یک قطب ساده با مانده ۱ دارد)، و فقط ییک تابع مدولار است (در واقع هر تابع مدولار دیگری از وزن ۰ یک چندجمله‌ای گویا از j خواهد بود. این را اثبات نمی‌کنم، اثبات آن در [۱۱] پیدا می‌شود).

همچنین در آخر گریزی به توابع تتا می‌زنیم. ما فقط تابع تتای کلاسیک را بررسی می‌کنیم:

$$\theta(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z}$$

حال با استفاده از تبدیل فوریه روی $h(x) = e^{2\pi i x^2 z}$ و فرمول جمع پواسون داریم:

$$\theta(\frac{-1}{4z}) = \sqrt{-2iz}\theta(z)$$

و پس اگر تابع تتا را به توان چهار برسانیم از رابطه‌ی بالا داریم: اگر $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \gamma \in \Gamma_0(4)$ آن‌گاه

$$\theta(\gamma(z))^4 = (cz+d)^2\theta(z)^4$$

حال اگر سری تتا را بنویسیم و به توان چهار برسانیم آنگاه می‌توان تعداد روش‌های نوشتن یک عدد به شکل جمع چهار مربع کامل را حساب کرد (با استفاده از پایه‌ای متشکل از سری‌های آیزنشتاین برای فضایی که این سری تتا در آن است) و مخصوصاً قضیه لاگرانژ را بدست آورد.

۳.۴ بعد فضاهای فرم‌های مدولار

اولاً می‌خواهیم ثابت کنیم که بعد فضاهای فرم‌های مدولار متناهی است.

قضیه. فرض کنید f یک فرم مدولار ناصفر از وزن k روی Γ باشد و V حجم $\mathbb{H}/\Gamma$ باشد (این متناهی است زیرا حجم $\mathbb{H}/SL_2(\mathbb{Z})$ را می‌توان به سادگی حساب کرد و دید که متناهی است). در این صورت داریم:

$$\sum_{P\in\mathbb{H}/\Gamma} \frac{1}{n_p} ord_P(f) + ord_\infty(f) = \frac{KV}{4\pi}$$

همچنین n_P تعداد تثبیت‌کننده نقطه P هستند.

این را می‌توان با استفاده از قضیه کشی[۲۴] در آنالیز مختلط بدست آورد. در واقع باید انتگرال f را روی مرز دامنه بنیادی[۲۵] گرفت در حالی که صفرهای آن را بیرون انداخته‌ایم، سپس با کمی محاسبات این عبارت بدست می‌آید. جزییات آن در [۱۲] می‌توان مطالعه کرد.

حال قضیه متناهی‌بعد بودن این فضاها را حساب می‌کنیم:

قضیه. با نمادگذاری بالا داریم:

$$\dim M_k(\Gamma) \leq \frac{kV}{4\pi} + 1$$

اثبات. به اندازه $\frac{kV}{4\pi} + 2$ فرم مدولار در $M_k(\Gamma)$ انتخاب کنید. باید ثابت کنیم این‌ها وابسته خطی هستند. همچنین به اندازه $\frac{kV}{4\pi} + 1$ نقطه متفاوت در $\mathbb{H}/\Gamma$ مثل P_iها انتخاب کنید (به‌طوری که دارای تثبیت‌کننده تک‌عضوی باشند). حال با ترکیب خطی فرم‌های مدولار، فرمی مدولار مانند f بسازید به‌طوری که در همه‌ی P_iها صفر شود. در این صورت از قضیه بالا بدست می‌آید که $f = 0$. پس ترکیب خطی آن فرم‌های مدولار صفر می‌شود و وابسته‌ی خطی‌اند.

همچنین در حالت $SL_2(\mathbb{Z})$ می‌توان دقیق‌تر این کار را کرد و بعد $M_k(SL_2(\mathbb{Z}))$ را بدست آورد:

قضیه. برای $k < 0$ داریم $M_k(SL_2(\mathbb{Z})) = \{0\}$ و برای $k \geq 0$ و زوج داریم:

$$\dim M_k(SL_2(\mathbb{Z})) \leq \begin{cases} [k/12]+1 & k \not\equiv 2(mod 12) \\ [k/12] & k \equiv 2(mod 12) \end{cases}$$

اثبات. فرم مدولار از وزن ۱۲ Δ را که در بخش قبل معرفی کردیم، در نظر بگیرید.در این صورت تابع

$$M_k(SL_2(\mathbb{Z})) \to S_{k+12}(SL_2(\mathbb{Z}))$$
$$f \mapsto f\Delta$$

[24] Cauchy
[25] Fundamental domain

یک ایزومورفیسم از فضاهای برداری است (این گزاره به سادگی از این نکته بدست می‌آید که Δ روی $\mathbb{H}$ ناصفر است و در بینهایت یک صفر ساده دارد). پس داریم:

$$\dim M_k(SL_2(\mathbb{Z})) = \dim S_{k+12}(SL_2(\mathbb{Z}))$$

حال برای kهای فرد، از قبل می‌دانیم که $M_k(SL_2(\mathbb{Z})) = \{0\}$. برای kهای زوج سری‌های آیزنشتاین را داریم که فرم کاسپ نیستند و پس:

$$\dim M_k(SL_2(\mathbb{Z})) > \dim S_k(SL_2(\mathbb{Z}))$$

از آنجا که $S_k(SL_2(\mathbb{Z}))$ برابر با هسته‌ی تابع $f \mapsto f(\infty)$ است، پس هم‌بعد[۲۶] آن ۱ است. پس از بالا

$$\dim M_k(SL_2(\mathbb{Z})) = \dim M_{k+12}(SL_2(\mathbb{Z})) - 1$$

و قضیه به‌سادگی با استقرا بدست می‌آید (حالت‌های پایه را با استفاده از سری‌های آیزنشتاین و قضیه‌های قبل می‌توان بدست آورد).

۴.۴ عملگرهای هکه

برای سادگی فرض کنید $\Gamma = SL_2(\mathbb{Z})$. اولاً دقت کنید که هر کدام از نقاط بالای صفحه را می‌توان با یک شبکه در $\mathbb{C}$ نمایش داد:

$$\mathbb{H} \to \mathcal{L}$$
$$\alpha \mapsto < \alpha, 1 >$$

که $\mathcal{L}$، مجموعه‌ی همه‌ی شبکه‌هاست و همچنین اگر شبکه‌ها را در حد هموتتی[۲۷] (ضرب در یک عدد مختلط) در نظر بگیریم، تابع بالا یک دوسویی خواهد داد:

$$\mathbb{H} \to \mathcal{L}/Homothety$$

پس فرم‌های مدولار را می‌توان روی شبکه‌ها نیز تعریف کرد. پس یک فرم مدولار از وزن k مثل f فیکس کنید. در این صورت قرار می‌دهیم:

$$f(< \omega_1, \omega_2 >) = (\omega_2)^{-k} f(\omega_1/\omega_2)$$

حال مثلاً یک شبکه L در نظر بگیرید و جمع صوری زیر را در نظر بگیرید ($n \in \mathbb{N}$):

$$T_n L := \sum_{[L:L']=n} L'$$

و برای $f \in M_k(SL_2(\mathbb{Z}))$ قرار دهید:

$$T_n f(L) = n^{k-1} \sum_{[L:L']=n} f(L')$$

در این صورت T_nها عملگرهایی روی $M_k(SL_2(\mathbb{Z}))$ و $S_k(SL_2(\mathbb{Z}))$ خواهند بود. همچنین برای $\lambda \in \mathbb{C}^*$، $[\lambda]$ را برابر با $L \mapsto \lambda L$ تعریف کنید و برای $f \in M_k(SL_2(\mathbb{Z}))$ قرار دهید:

$$([\lambda]f)(L) = f(\lambda L)$$

$[\lambda]$ نیز عملگری از فضاهای فرم‌های مدولار و فرم‌های کاسپ خواهد بود.

[26] Codimension
[27] Homothety

حال می‌توان به‌سادگی چک کرد که T_nها و $[\lambda]$ها با یکدیگر جابجا می‌شوند و T_nها نسبت به ضرب داخلی پترسون:

$$(f,g) := \int_{\mathbb{H}/SL_2(\mathbb{Z})} f(\tau)\bar{g}(\tau)(\square\square\,\tau)^k d\nu(\tau),$$
$$\nu(\tau) = y^{-2}dxdy,\ f,g \in S_k(SL_2(\mathbb{Z}))$$

خودالحاق هستند. پس می‌توان فضای فرم‌های کاسپ از وزن k روی $SL_2(\mathbb{Z})$ را به فرم‌های ویژه همه‌ی T_nها تجزیه کرد (که یکه و عمود هستند). این فرم‌های ویژه را می‌توان صریحاً پیدا کرد و برابر با سری‌های آیزنشتاین[۲۸] می‌شوند. خواص مهمی که عملگرهای هکه دارند عبارتند از:

۱) $[\lambda][\mu] = [\mu][\lambda]$ برای $\lambda, \mu \in \mathbb{C}^*$.

۲) $[\lambda]T_n = T_n[\lambda]$ برای $\lambda \in \mathbb{C}^*$ و $n \in \mathbb{N}$.

۳) $T_nT_m = T_{nm}$ اگر m, n نسبت به هم اول باشند.

۴) $T_{l^n}T_l = T_{l^{n+1}} + lT_{l^{n-1}}[l]$ برای l اول و $n \in \mathbb{N}$.

۵) $a_1(T_nf) = a_n(f)$ که منظور از $a_n(f)$ ضریب n-ام فوریه‌ی f در بی‌نهایت است.

همچنین در حالت کلی‌تر، می‌توان این عملگرهای هکه را تعریف کرد که توابعی خطی از $M_k(\Gamma_1)$ $(S_k(\Gamma_1))$ به $M_k(\Gamma_2)$ $(S_k(\Gamma_2))$ خواهند بود. چیزی که برای ما مهم است، فقط عملگرهای هکه روی $S_k(\Gamma_0(N))$ هست که تعریف آن روشن‌کننده نیست و تعمیمی از حالت قبل خواهد بود (می‌توان به سادگی روی بسط‌های فوریه آن‌ها را تعریف کرد). همچنین خواصی که این عملگرهای هکه کلی‌تر روی $S_k(\Gamma_0(N))$ دارند، مشابه خواص بالا است (برای $l \mid N$ باید حواسمان را بیشتر جمع کنیم).

مثلاً یکی از کاربردهای این عملگرها قسمت‌هایی از حدس رامانوجان[۲۹] بوده است. در واقع تابع

$$\Delta(q) = q\prod_n (1-q^n)^{24},\ q = e^{2\pi iz}$$

بسط فوریه‌ی $\eta(q) = \sum_{n\geq 1}\tau(n)q^n$ را دارد که $\tau(n)$ تابع رامانوجان است. رامانوجان حدس زده بود که

۱) تابع τ ضربی است.

۲) برای l اول و $n \in \mathbb{N}$ داریم:

$$\tau(l^{n+1}) = \tau(l)\tau(l^n) - l^{11}\tau(l^{n-1})$$

۳) $|\tau(l)| \leq 2l^{11/2}$.

حال می توان دید که فضای $S_{12}(SL_2(\mathbb{Z}))$ یک بعدی است و $S_{12}(SL_2(\mathbb{Z})) =< \Delta >$. پس η باید بردار ویژه‌ی همه‌ی T_nها باشد. پس طبق خاصیت ۵ باید داشته باشیم:

$$a_1(T_n\Delta) = a_n(\Delta) = \tau(n)$$

و از آنجا که $a_1(\Delta) = 1$، پس باید مقدارویژه‌ی متناظر آن $\tau(n)$ باشد و پس از خاصیت ۴ با عمل کردن به روی Δ قسمت دوم حدس بدست می‌آید. همچنین از خاصیت ۳ نیز با همین روند قسمت اول حدس بدست می‌آید.

۵.۴ خم‌های پیمانه‌ای

در این قسمت خم‌های پیمانه‌ای[۳۰] را تعریف می‌کنیم و سپس یک صورت از قضیه مدولاریتی را با استفاده از آنها بیان می‌کنیم.

[28] Eisenstein series
[29] S. Ramanujan
[30] Modular Curves

می‌دانیم که $\Gamma_0(N)$ و در حالت کلی‌تر یک زیرگروه هم‌نهشتی $SL_2(\mathbb{Z})$ (مثلاً Γ) روی نیم‌صفحه بالا عمل می‌کند و پس می‌توان تقسیم $\mathbb{H}/\Gamma$ را در نظر گرفت. در این صورت این یک رویه ریمانی خواهد بود که فشرده نیست ولی با متناهی نقطه می‌توان آن را فشرده کرد پس بدین شکل آن را فشرده می‌کنیم: اول نقاط $\mathbb{P}^1_{\mathbb{Q}}$ را به این فضا اضافه می‌کنیم و با $SL_2(\mathbb{Z})$ روی آن عمل می‌کنیم، بدین شکل که با $\frac{a}{b}$ مانند $\begin{bmatrix} a \\ b \end{bmatrix}$ رفتار می‌کنیم و با ∞ مانند $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ رفتار می‌کنیم. پس فضای زیر را می‌توان تعریف کرد که از نظر توپولوژیک یک رویه‌ی ریمانی فشرده است:

$$X(\Gamma) := (\mathbb{H} \cup \mathbb{P}^1_{\mathbb{Q}})/\Gamma$$

به این چنین فضاهایی خم‌های پیمانه‌ای می‌گویند. حال می‌توان یک صورت از قضیه مدولاریتی را بیان کرد:

قضیه. برای هر خم بیضوی $E/\mathbb{Q}$ یک مورفیسم تعریف شده روی اعداد گویا با ضرایب صحیح و پوشای $f : X_0(N) \to E$ وجود دارد (N به E بستگی دارد).

همچنین برای استفاده‌های آینده، خوب است تعریف ژاکوبین یک خم را در اینجا تعریف کنیم:

تعریف. فرض کنید C یک خم هموار روی اعداد مختلط باشد. در این صورت ژاکوبین را با $J(C)$، نمایش می‌دهیم و مانند زیر تعریف می‌کنیم (می‌توان با استفاده از نگاشت نشاندن و قضیه‌های ژاکوبی و آبل نیز تعریف کرد که معادل این است):

$$J(C) = H^0(\Omega^1_C)^*/H_1(C)$$

۵ نمایش‌های گالوا

در این بخش تا جایی که در فصل‌های آینده نیاز داریم، نمایش‌های گالوا را توضیح می‌دهیم و سعی می‌کنیم در همان حالت کلی‌ای که وایلز نیاز داشت، آنرا تعریف کرده و به کار ببریم.

۱.۵ تعاریف مقدماتی

منظور از یک نمایش گالوا یک هومومورفیسم $\rho : G_{\mathbb{Q}} \to GL_n(A)$ است که $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ و A یک حلقه‌ی جابجایی و یکدار است. یک مثال از نمایش‌های گالوا نمایش دایره‌بر[۳۱] است. این نمایش یک‌بعدی به شکل زیر تعریف می‌شود: یک عدد اول l را فیکس کنید و قرار دهید

$$\chi_l : G_{\mathbb{Q}} \to \mathbb{Z}_l^*$$

به‌طوری که

$$\sigma : \zeta_{l^n} \mapsto \zeta_{l^n}^{\chi_l(\sigma)} , n \in \mathbb{N}$$

همچنین، نمایش‌های شاخه‌ای[۳۲] و غیرشاخه‌ای[۳۳] به معنی زیر هستند:

تعریف. به نمایش ρ در عدد اول l غیرشاخه‌ای گویند هرگاه $\rho(I_l) = \{1\}$ که I_l یک گروه سکون[۳۴] در l است و در غیر این صورت به آن شاخه‌ای در l گویند.

۲.۵ نمایش‌های گالوا روی خم‌های بیضوی

یک خم بیضوی $E/\mathbb{Q}$ را در نظر بگیرید. دیدیم که عمل گروه روی E داریم و پس می‌توان نقاط تابی[۳۵] روی آن را در نظر گرفت:

$$E[n] = \{p \in E(\bar{Q}) \mid [n]p = O\}$$

در این صورت داریم:

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

حال مدول تیت[۳۶] را به شکل زیر تعریف می‌کنیم:

$$T_l(E) := \varprojlim E[l^n] \cong \mathbb{Z}_l \times \mathbb{Z}_l$$

که $\mathbb{Z}_l$ گروه اعداد l-تایی[۳۷] هاست.

با استفاده از مدول تیت می‌توان یک نمایش گالوا معرفی کرد، در واقع برای هر نقطه‌ی $P = (x, y) \in E[l^n]$ می‌توان $\sigma \in G_{\mathbb{Q}}$ را روی آن اثر داد و $P^\sigma = (\sigma(x), \sigma(y))$ را بدست آورد که از آنجا که عمل گروه، به شکل توابع گویا تعریف شده است، P^σ باید در $E[l^n]$ باشد. پس می‌توان نمایشی به شکل $\rho : G_{\mathbb{Q}} \to GL(E[l^n]) = GL_2(\mathbb{Z}/l^n\mathbb{Z})$ تعریف کرد که این‌ها با سیستم وارون سازگارند و پس نمایش گالوا روی مدول تیت پیدا می‌کنیم:

$$\rho_{E,l} : G_{\mathbb{Q}} \to GL(T_l(E)) \cong GL_2(\mathbb{Z}_l)$$

[31] Cyclotomic
[32] Ramified
[33] Unramified
[34] Inertia group
[35] Torsion points
[36] Tate module
[37] l-adic numbers

۳.۵ نمایش‌های گالوا روی فرم‌های مدولار

تعریف این کمی دشوارتر از حالت قبل است. در واقع برای ساخت آن ابتدا باید یک خم بیضوی (واریته آبلی در حالت کلی) بسازیم و سپس نمایش گالوا روی آن را مساوی با نمایش این فرم مدولار تعریف کنیم. پس فرض کنید $f \in S_2(\Gamma_0(N))$ طوری باشد که تابع ویژه‌ی همه‌ی عملگرهای هکه باشد، و نرمال باشد و همچنین همه‌ی ضرایب بسط فوریه‌ی آن صحیح باشند. در این صورت با استفاده از آن می‌توان یک خم بیضوی E_f ساخت:

دلیل این ساختن را در فصل L-توابع توضیح می‌دهیم. ژاکوبین $X_0(N)$ را در نظر بگیرید و آن را با $J_0(N)$ نمایش دهید. در این صورت این یک واریته آبلی خواهد بود. حال I_f را هسته‌ی تابع $\lambda : \mathbb{T} \to \mathbb{Z}$ (تابع مقادیر ویژه) قرار دهید، در این صورت خارج‌قسمت $J_0(N)/I_f J0(N)$ خم بیضوی مورد نظر خواهد بود که با E_f نمایش می‌دهیم و سپس قرار می‌دهیم:

$$\rho_{f,l} := \rho_{E_f,l}$$

حال صورت دومی از قضیه مدولاریتی را بیان می‌کنیم:

قضیه. فرض کنید E یک خم بیضوی روی $\mathbb{Q}$ باشد. در این صورت $f \in S_2(\Gamma_0(N))$ (که f جدید و فرم‌ویژه‌ی همه‌ی عملگرهای هکه و دارای ضرایب فوریه گویا) وجود دارد که برای همه lهای اول:

$$\rho_{f,l} \sim \rho_{E,l}$$

علامت $\sim$ به معنی مزدوج است.

همچنین نمایش گالوایی که چنین fی برای آن موجود باشد، نمایش گالوای مدولار گوییم.

روندی که وایلز برای اثبات قضیه آخر فرما در پیش گرفت، صورتی از قضیه مدولاریتی بود که با نمایش‌های گالوا فرمول‌بندی شده بود و کاری که او کرد این بود که قضیه مدولاریتی را برای همه‌ی خم‌های بیضوی نیمه‌پایدار اثبات کرد که برای اثبات قضیه آخر فرما کافی بود.

۴.۵ دگردیسی‌های نمایش‌های گالوا

فرض کنید یک خم بیضوی روی اعداد گویا داریم و می‌خواهیم نمایش‌های گالوا روی آن را بررسی کنیم. در این صورت اگر نمایش روی کل مدول تیت را در نظر بگیریم، بررسی آن به نظر کار بسیار سختی است. پس ما ابتدا نمایش روی نقاط l-تابی را بررسی می‌کنیم و سعی می‌کنیم با ایده‌ای با بررسی این نمایش، کار را تمام کنیم.

در این قسمت نمایش‌های گالوا را کلی‌تر می‌نویسیم و سعی می‌کنیم شرط‌های محدودکننده‌ای روی آن قرار دهیم (شرط‌هایی که مطمئن باشیم برای نمایش‌های گالوا روی خم‌های نیمه‌پایدار درست باشند).

تعریف. فرض کنید K یک توسیع متناهی $\mathbb{Q}_l$ باشد و O حلقه‌ی اعداد صحیح K باشد. رسته $\mathcal{C}_O$ را تعریف کنید: اشیا از همه O-جبرهای نوتری موضعی A (با ایدآل ماکسیمال $\mathfrak{m}_A$) به همراه نگاشتی پوشا (نگاشت تشدید[۳۸]) $\pi : A \to O$ تعریف کنید به‌طوری که $A/\mathfrak{m}_A \cong O/\mathfrak{m}_O = \mathbb{F}_q$ و نگاشت‌های بین این اشیا را برابر O-جبر هوموفیسم‌های روی O تعریف کنید (نمودار زیر جابجا شود):

$$\begin{array}{ccc} A & \longrightarrow & A' \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_{A'}} \\ O & \xrightarrow{1_O} & O \end{array}$$

حال یک شیء از رسته بالا مثل A را فیکس کنید. می‌خواهیم دگردیسی[۳۹] نمایش‌های گالوا را تعریف می‌کنیم:

تعریف. ۱) یک نمایش گالوا $\rho_0 : G_{\mathbb{Q}} \to GL_m(\mathbb{F}_q)$ فیکس کنید. منظور از یک بالابری[۴۰] ρ از این نمایش گالوا یک نمایش $\rho : G_{\mathbb{Q}} \to GL_m(A)$

[38] Augmentation
[39] Deformation
[40] Lift

است به‌طوری که ρ به پیمانه‌ی $\mathfrak{m}_A$ برابر ρ_0 شود.

۲) دو بالابری ρ, ρ' از ρ_0 را اکیداً معادل[41] گوییم هرگاه یک ماتریس C وجود داشته باشد که به پیمانه‌ی $\mathfrak{m}_A$ همانی شود و داشته باشیم:

$$\rho(g) = C^{-1}\rho'(g)C,\ g \in G_{\mathbb{Q}}$$

۳) منظور از یک دگردیسی ρ_0 یک مولفه‌ی هم‌ارزی از رابطه‌ی هم‌ارزی بالا است.

حال شرط‌هایی که گفتیم را باید روی دگردیسی‌های نمایش‌های گالوا قرار دهیم: پس یک نمایش گالوا $\rho_0 : G_{\mathbb{Q}} \to GL_m(\mathbb{F}_q)$ فیکس کنید و S را مجموعه‌ی اعداد اولی قرار دهید که ρ_0 در آن‌ها شاخه‌ای است. این یک مجموعه‌ی متناهی است. حال فرض کنید Σ یک مجموعه‌ی متناهی از اعداد اول باشد.

تعریف. دگردیسی ρ را از نوع D_Σ گوییم هرگاه:

۱) ρ بیرون از $\Sigma \cup S \cup \{p\}$ غیرشاخه‌ای باشد.

۲) $\det \rho = \chi_p$.

۳) برای هر $l \in S$،

$$\rho|_{I_l} \sim \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$$

این شرط نیمه‌پایداری در l است.

۴) تحدید $\rho|_{D_p}$ یا "صاف" باشد یا "معمولی"[42]. این‌ها دو شرط موضعی هستند که اولی یعنی این که این نمایش از یک گروه اسکیمی[43] متناهی و صاف آمده باشد و معمولی تعریف تکنیکال‌تری دارد.

همچنین به دگردیسی‌ای، مجاز[44] گوییم هرگاه برای Σیی D_Σ باشد. حال مجموعه‌های همه‌ی دگردیسی‌های از نوع D_Σ و دگردیسی‌های مدولار از نوع D_Σ را به ترتیب با $DA_\Sigma(A)$ و $DM_\Sigma(A)$ نشان می‌دهیم. در این صورت می‌توان ثابت کرد که این‌ها دو مجموعه‌ی متناهی هستند و اگر به آن‌ها به عنوان فانکتور[45] نگاه کنیم:

$$DM_\Sigma \subseteq DA_\Sigma : \mathcal{C}_O \to \mathbf{FiniteSets}$$

نمایش‌پذیر[46] خواهند بود. پس دو عضو از $\mathcal{C}_O$ وجود دارند مثل R_Σ و $\mathbb{T}_\Sigma$ به‌طوری که

$$DM_\Sigma(A) = \square\square\square(\mathbb{T}_\Sigma, A) \subseteq DA_\Sigma(A) = \square\square\square(R_\Sigma, A)$$

حال با قرار دادن $A = \mathbb{T}_\Sigma$ یک تابع کانونی $\phi_\Sigma : R_\Sigma \to \mathbb{T}_\Sigma$ پیدا می‌کنیم. حال می‌توانیم نمایش‌های زیر را پیدا می‌کنیم:

$$\rho_\Sigma^{univ} : G_{\mathbb{Q}} \to GL_2(R_\Sigma)$$
$$\rho_\Sigma^{univ.mod} : G_{\mathbb{Q}} \to GL_2(\mathbb{T}_\Sigma)$$

به‌طوری که با ϕ_Σ به هم مربوط می‌شوند. کاری که وایلز برای اثبات این قضیه می‌کند، اثبات قضیه زیر است:

قضیه. (قضیه اصلی) ϕ_Σ ایزومورفیسم در رسته $\mathcal{C}_O$ است.

[41] Strictly equivalent
[42] Ordinary
[43] Group scheme
[44] Admissible
[45] Functor
[46] Representable

این قضیه کار را تمام می‌کند، زیرا نشان می‌دهد که تعداد اعضای مجموعه‌های $DM_{\Sigma}(A)$ و $DA_{\Sigma}(A)$ برای همه‌ی Aها یکی است و پس همه‌ی دگردیسی‌های مجاز، مدولار هستند و پس قضیه مدولاریتی خم‌های نیمه‌پایدار را میتوان به اتمام رساند.

۶ L-توابع

همانند حالت کلاسیک L-توابع دیریکله و ددکیند، L-توابعی می‌توان برای اشیایی که تاکنون توضیح داده‌ایم، ساخت. در این بخش L-توابع خم‌های بیضوی و فرم‌های مدولار و خواص آنها را توضیح می‌دهیم.

۱.۶ L-توابع خم‌های بیضوی

فرض کنید $E/\mathbb{Q}$ یک خم بیضوی باشد. در این صورت می‌توان کاهش $\bar{E}$ به پیمانه l (عدد اول خوبی) را در نظر گرفت و مورفیسم فروبنیوس روی آن عمل می‌کند:

$$\phi_p : \bar{E} \to \bar{E}$$
$$(x, y) \mapsto (x^p, y^p)$$

و پس می‌توان چندحمله‌ای مشخصه عمل آن روی مدول‌های تیت را در نظر گرفت و از آنجا که درجه ϕ_p، p است و $tr\phi_p = p + 1 - |E(\mathbb{F})_p| =: a_p$ خواهیم داشت:

$$\det(I - t\phi_p) = 1 - a_p t + pt^2$$

پس L-تابع خم بیضوی را در قسمت خوب به شکل زیر تعریف می‌کنیم:

$$L_{good}(E, s) = \prod_p \frac{1}{\det(I - p^{-s}\phi_p)}$$

و در قسمت‌های بد نیز اگر p ضربی باشد قرار می‌دهیم $\frac{1}{1 \pm a_p p^{-s}}$ (اگر تجزیه‌ای[۴۷] باشد + و در غیر این صورت -) و اگر جمعی باشد ۱ قرار می‌دهیم، پسدر کل، L-تابع را به شکل زیر تعریف می‌کنیم:

$$L(E, s) = \prod_p \frac{1}{1 \pm a_p p^{-s}} \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

به سادگی می‌توان چک کرد که از قضیه هسه ($|a_p| \leq 2\sqrt{p}$) بدست می‌آید که این تابع برای $Res > \frac{3}{2}$ همگرا است.

۲.۶ L-توابع فرم‌های مدولار

فرض کنید f یک فرم کاسپ از وزن k روی $SL_2(\mathbb{Z})$ باشد و فرض کنید دارای بسط فوریه‌ی

$$f = \sum_{n=1}^{\infty} c_n q^n$$

در این صورت L-تابع را می‌توان با استفاده از تبدیل ملین [۴۸] بدست آورد:

$$g(s) = \int_0^{\infty} F(t) t^{s-1} dt$$

پس

$$g(s) = \int_0^{\infty} f(i\sigma)\sigma^{s-1} d\sigma = \int_0^{\infty} \sum_{n=1}^{\infty} c_n e^{-2\pi\sigma} \sigma^{s-1} ds = (2\pi)^{-s}\Gamma(s) \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

و L-تابع را برابر با $L(s, f) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$ تعریف می‌کنیم.

[47] Split
[48] Mellin

در این صورت، می‌توان به سادگی ثابت کرد که $|c_n| \leq Cn^{\frac{k}{2}}$ (مثلاً قضیه‌ی ۵ از فصل ۷ در [۱۱]) و خواهیم داشت که این L-تابع برای $Res > \frac{k}{2} + 1$ همگراست.

قضیه. اگر f یک فرم کاسپ از وزن k برای $SL_2(\mathbb{Z})$ باشد، آن‌گاه L-تابع را می‌توان گسترش تحلیلی داد. علاوه بر این، تابع

$$\Lambda(s, f) = (2\pi)^{-s}\Gamma(s)L(s, f)$$

معادله تابعی زیر را دارد:

$$\Lambda(s, f) = (-1)^{\frac{k}{2}}\Lambda(k - s, f)$$

برهان. طبق فرم کاسپ بودن f روی $SL_2(\mathbb{Z})$ داریم:

$$f(\frac{i}{\sigma}) = i^k\sigma^k f(i\sigma)$$

و

$$\Lambda(s, f) = \int_0^\infty f(i\sigma)\sigma^{s-1}d\sigma$$

از بالا (برای $Res > \frac{k}{2} + 1$) پس

$$\Lambda(s, f) = \int_0^1 f(i\sigma)\sigma^{s-1}d\sigma + \int_1^\infty f(i\sigma)\sigma^{s-1}d\sigma$$
$$\int_0^1 f(\frac{i}{\sigma})\frac{1}{\sigma^{s-1}}d\frac{1}{\sigma} + \int_1^\infty f(i\sigma)\sigma^{s-1}d\sigma =$$
$$\int_1^\infty i^k f(i\sigma)\sigma^{k-s-1}d\sigma + \int_1^\infty f(i\sigma)\sigma^{s-1}d\sigma$$

حال با $s \mapsto k - s$ در بالا داریم:

$$\int_1^\infty i^k f(i\sigma)\sigma^{s-1}d\sigma + \int_1^\infty f(i\sigma)\sigma^{k-s-1}d\sigma$$

اما چون $S_k(SL_2(\mathbb{Z}))$ برای kهای فرد صفر است، پس فرض می‌کنیم k زوج است و پس:

$$i^k\Lambda(k - s, f) = \int_1^\infty i^k f(i\sigma)\sigma^{k-s-1}d\sigma + \int_1^\infty f(i\sigma)\sigma^{s-1}d\sigma = \Lambda(s, f)$$

پس تمام است.

حال می‌توان یک صورت جدید برای قضیه مدولاریتی می‌توان بیان کرد:

قضیه. فرض کنید $E/\mathbb{Q}$ یک خم بیضوی باشد. فرض کنید l یک عدد اول باشد. در این صورت قرار دهید $a_l = l + 1 - \bar{E}(\mathbb{F}_l)$ (برای pهای با کاهش خوب) در این صورت $f \in S_2(\Gamma_0(N))$ وجود دارد که نرمال ($a_1(f) = 1$) و "جدید" و فرم ویژه‌ی همه‌ی عملگرهای هکه باشد و $a_l(f) = a_l$ برای همه بجز متناهی l (این معادل است با $L(s, f) = L(E, f)$).

"جدید" یعنی این‌که f از $S_2(\Gamma_0(d))$ $(d \mid N)$ نیامده باشد: در واقع، اگر $g \in S_2(\Gamma_0(d))$ باشد، آن‌گاه $h : z \mapsto g(\frac{N}{d}z)$ یک فرم کاسپ در $S_2(\Gamma_0(N))$ هست و منظور از جدید یعنی f ترکیب خطی تعدادی از این خم‌های $S_2(\Gamma_0(d))$ برای dهای کمتر نباشد.

۳.۶ نظریه آیشلر شیمورا

همانطور که گفته بودیم در اینجا قضیه‌ای در مورد ساخت خم بیضوی ارائه می‌دهیم.

فرض کنید f یک فرم کاسپ از وزن ۲ و مرحله‌ی N جدید باشد که فرم ویژه‌ی همه‌ی عملگرهای هکه روی $\Gamma_0(N)$ باشد. در این صورت می‌توان یک خم بیضوی با استفاده از آن ساخت که در قضیه بالا صدق کند. در واقع برای ساختن آن کافیست $J(X_0(N))/I_f J(X_0(N))$ را در نظر بگیریم که I_f هسته‌ی تابع مقدار ویژه‌ی $\lambda : \mathbb{T} \to \mathbb{Z}$ است که $\mathbb{T}$ جبر هکه است. در این صورت این تقسیم یک خم بیضوی خواهد بود که L-تابع یکسانی با f دارد، پس در قضیه بالا صدق می‌کند.

۷ قضیه آخر فرما

در این بخش روند اثبات قضیه آخر فرما توسط وایلز را توضیح می‌دهیم. در واقع کاری که او کرد این بود که قضیه مدولاریتی را برای خم‌های نیمه پایدار ثابت کرد و قضیه آخر فرما را با استفاده از قضیه ریبت (در پایین توضیح داده شده) و مدولاریتی خم‌های نمیه پایدار نتیجه می‌گیرد.

۱.۷ نتیجه گرفتن قضیه آخر فرما

در ابتدا باید قضیه‌ای از ریبت را بیان کنیم. این حدس را اولین بار سر مطرح کرد و ریبت آن را اثبات کرد و اثبات قضیه آخر فرما را به حدس شیمورا-تانیاما کاهش داد. این قضیه در مورد کاهش دادن مرحله‌ی یک فرم کاسپ حرف می‌زند:

قضیه. (قضیه ریبت) فرض کنید q عدد اولی باشد و f در $S_2(\Gamma_0(lN))$ یک فرم کاسپ جدید نرمال $(a_1(f)=1)$ و فرم‌ویژه همه‌ی عملگرهای هکه باشد به‌طوری که دارای نمایش‌های "مطلقاً تحویل‌ناپذیر"[۴۹] $\rho_{f,q}$ باشد و این نمایش در l غیرشاخه‌ای ("متناهی" و "صاف"[۵۰]) باشد اگر $l \neq q$ $(l=q)$. آن‌گاه $g \in S_2(\Gamma_0(N))$ نرمال و جدید وجود دارد که داریم:

$$\rho_{f,q} \sim \rho_{g,q}$$

اثبات. رجوع شود به [۴].

متناهی و صاف معانی جزئی دارند که توضیح آنها از سطح این مقاله بالاتر است. مطلقاً تحویل‌ناپذیر یعنی به عنوان نمایش‌های به $GL_2(\overline{\mathbb{F}}_p)$ تحویل‌ناپذیر باشند.

حال با استفاده از این قضیه و مدولاریتی خم‌های نیمه پایدار بدین شکل می‌توان قضیه آخر فرما را ثابت کرد:

پس فرض کنیم که معادله‌ی فرما یک جواب نابدیهی دارد: $A^p+B^p=C^p$ حال خم فری را به شکل زیر تعریف می‌کنیم: $F: y^2=x(x-A^p)(x+B^p)$ و نمایش‌های گالوای روی آن را در نظر گرفتیم. می‌توان دید که این نمایش‌ها مجاز هستند و پس از قضیه اصلی وایلز، مدولار هستند و پس یک فرم مدولار نرمال در $S_2(\Gamma_0(N))$ برای Nی پیدا می‌کنیم که N عددی خالی از مربع خواهد بود که $N \mid 2ABC$ (این از ترکیب قضیه‌ای از میزر[۵۱] و ریبت بدست می‌آید که آن را بیان نکردیم. می‌توانید این را در [۶] پیدا کنید). حال با استفاده از تفکیک‌کننده یک خم می‌توان شرطی روی نمایش‌های گالوای بدست آمده از نقاط l-تابی قرار داد. اگر این کار را برای خم فری انجام دهیم نتیجه می‌شود که همه‌ی اعداد اولی که ABC را عاد می‌کنند در شروط قضیه‌ی ریبت صدق می‌کنند (به عنوان q در قضیه). پس طبق قضیه ریبت می‌توان فرم کاسپی نرمال در $S_2(\Gamma_0(2))$ پیدا کرد. اما داریم $S_2(\Gamma_0(2))=\{0\}$ (این به‌سادگی از این‌که فشرده‌سازی $\mathbb{H}/\Gamma_0(2)$ گونه[۵۲] صفر دارد بدست می‌آید) و پس فرم مدولار نرمالی در آن وجود ندارد. این همان تناقضی بود که دنبالش بودیم!

در بخش‌های بعد در مورد اثبات وایلز از قضیه آخر فرما توضیح می‌دهیم و با نمادگذاری آخر بخش نمایش‌های گالوا ادامه می‌دهیم.

۲.۷ ایده‌ی اثبات وایلز

در اینجا به طور مختصر ایده‌ی اثبات وایلز را توضیح می‌دهیم. گفتیم که حلقه‌های R_Σ و $\mathbb{T}_\Sigma$ وجود دارند. وایلز در ابتدا آن‌ها را می‌سازد و شناسایی می‌کند. سپس برای این که اثبات کند تابع بین آنها ایزومورفیسم است، پوشایی را به سادگی ثابت می‌کند و برای یک به یک بودن آن معیارهایی می‌دهد. در ابتدا باید یک نوع حلقه را تعریف کنیم:

تعریف. یک O-جبر موضعی نوتری A کاملاً اشتراکی[۵۳] گوییم هرگاه :

[49] Absolutely irreducible
[50] flat
[51] B. Mazur
[52] Genus
[53] Complete intersection

۱) A یک O-مدول آزاد از بعد متناهی باشد.

۲) $A \cong O[[X_1, X_2, \cdots, X_n]]/(f_1, f_2, \cdots, f_n)$.

حال ناورداهای زیر را در نظر می‌گیریم:

$$I_A = (f_1, f_2, \cdots, f_n) \quad \Phi_A = I_A/I_A^2 \quad \eta_A = Ann(I_A) \subseteq O$$

حال معیارها را بیان می‌کنیم:

قضیه. فرض کنید $\phi : A \to B$ یک مورفیسم پوشا در کتگوری C_O باشد. در این صورت اینها معادلند:

۱) ϕ یک ایزومورفیسم از O-جبرهای موضعی کاملاً اشتراکی[۵۴] است.

۲) $|\Phi_A| \leq |O/\eta_B| < \infty$

۳) $|\Phi_A| = |O/\eta_B| < \infty$

همچنین معیار دوم بدین شکل است:

قضیه. فرض کنید ϕ یک مورفیسم پوشا در C_O باشد. اگر ϕ یک J-ساختار[۵۵] (این یک تعریف تکنیکال جبری دارد) در این صورت ϕ یک ایزومورفیسم از حلقه‌های موضعی کاملاً اشتراکی است.

پس از این اثبات می‌کند (با استفاده از ساخت این حلقه‌ها) که R_Σ و $\mathbb{T}_\Sigma$ حلقه‌های کاملاً اشتراکی هستند و با استقرا بروی تعداد اعضای Σ و استفاده از این معیارها (با محاسبه‌ی ناورداهای این حلقه‌ها) ثابت می‌کند که ϕ_Σ ایزومورفیسم است و کار تمام می‌شود و مدولاریتی خم‌های نیمه‌پایدار و پس از بالا قضیه آخر فرما ثابت می‌شود.

[54] Local complete intersection

[55] J-structure

مراجع

[1] Fulton W., *Algebraic curves*, 1969.

[2] Hartshorne R., *Algebraic Geometry*, Springer, 1977.

[3] Darmon H., *Rational Points on Modular Elliptic Curves*, 2003.

[4] Ribet K., *From the Taniyama-Shimura Conjecture to Fermat's Last Theorem* , 1990.

[5] Wiles A., *Modular Elliptic curves and Fermat's Last Theorem*, 1995.

[6] Manin, Yu. I., Panchishkin, Alexei A., *Introduction to Modern Number Theory*, 2005.

[7] Silverman J., Tate J.T., *Rational Points on Elliptic Curves*, Springer, 1992.

[8] Silverman J. *The Arithmetic of Elliptic Curves*, Springer, 1986.

[9] Silverman J., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[10] Serre J.P., *Complex Multiplication*, in: Cassels-Frohlich, ed., Algebraic Number Theory, Academic Press, 1967.

[11] Serre J.P., *A Course in Arithmetic*, Springer, 1973.

[12] Zagier D., van der Geer G., Harder G. Bruinier J.H., *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*, Springer, 2008.