نظریه جبری اعداد

علی چراغی

یادداشت‌های درس کوتاه ارائه شده در دانشگاه شیراز

تابستان ۱۳۹۷

فهرست مطالب

◦ مقدمه

این یادداشت‌ها خلاصه‌ای از آنچه در دانشکده علوم دانشگاه شیراز از ۶ تا ۱۱ مرداد سال ۱۳۹۷ ارائه شده است، می‌باشد. در این ارائه‌ها تلاش شد تا مقدماتی در مورد نظریه جبری اعداد و سپس هندسه جبری، قضیه‌ها و مفهوم‌های شناخته شده در هندسه حسابی، مخصوصاً خم‌های بیضوی بیان شود.

در فصل اول، یک تصویر کلی از نظریه اعداد تحلیلی و جبری داده می‌شود، نظریه اعداد تحلیلی از اثبات اویلر از نامتناهی بودن اعداد اول شروع می‌شود و با تعریف زتا و کارهای اویلر روی آن به معرفی Lـ توابع دیریکله می‌رسیم و قضیه دیریکله را در مورد اعداد اول توزیع شده به پیمانه اعداد بیان می‌کنیم. سپس کارهای ریمان روی قضیه اعداد اول و تابع زتای ریمانـ که در تنها مقاله‌ی نظریه اعداد او چاپ شده استـ را توضیح می‌دهیم و سپس فرض ریمان را بیان می‌کنیم. همچنین زیربخش دوم آن به مقدمه‌ای بر نظریه جبری اعداد می‌پردازد و بعضی تعاریف پایه‌ای مانند میدان عددی ، حلقه‌ی اعداد صحیح یک میدان عددی و عدد کلاسی در روند اثبات حالت خاصی از قضیه فرما (که توسط کومر ثابت شده است) توضیح داده می‌شود.

در فصل دوم، هندسه جبری مقدماتی با روندی مانند فصل اول [Har77] توضیح داده شده است یعنی در ابتدا واریته‌های آفین و تناظر آن با Kـ جبرهای متناهی تولید تحویل‌یافته بیان شده، سپس مقدمه‌ای در مورد واریته‌های تصویری داده شده است.

در فصل سوم، خود را محدود به خم‌های جبری می‌کنیم . دسته‌بندی آنها توسط گوناهایشان را بیان کرده و همچنین قضیه ریمانـ رخ را معرفی می‌کنیم.

در فصل چهارم، خود را به خم‌های گونای یک، یعنی خم‌های بیضوی، محدود می‌کنیم و خواص تحلیلی و حسابی آنها را مورد بررسی قرار می‌دهیم. قضیه‌هایی مانند قضیه ناگلـ لوتز، میزر، موردلـ وی ، هسه در مورد تعداد نقاط خم بیضوی روی میدان‌های متناهی و حدس ساتوـ تیت در اینجا گفته شده‌اند.

در فصل آخر، قضیه‌های مهمی مانند حدس‌های وی (که الآن یک قضیه است)، قضیه فالتینگز، سوال دوازدهم هیلبرت و نقش ضرب مختلط در آن گفته شده و در آخر روند اثبات قضیه آخر فرما را شرح می‌دهیم.

در اینجا بر خود لازم می‌دانم از زحمات مریم نوروزی، جلال پیردایه، فاطمه شریفی، انجمن علمی ریاضی دانشگاه شیراز و همه کسانی که برگزاری این درس کوتاه را میسر کردند، تشکر کنم.

علی چراغی

شهریور ۱۳۹۷

۱ نگاهی از بالا به نظریه اعداد

در این بخش ابتدا با شاخه‌های مختلف نظریه اعداد آشنا می‌شویم و مسائل مربوط به بعضی از شاخه‌هایش را مورد بررسی قرار می‌دهیم و در نهایت به صورت مفصل به نظریه جبری اعداد می‌پردازیم و روند پیشرفت آن را خصوصاً در قضیه آخر فرما دنبال می‌کنیم. نظریه اعداد به چندین بخش مختلف تقسیم می‌شود که مهم‌ترین آن‌ها نظریه جبری اعداد، نظریه تحلیلی اعداد و نظریه اعداد ترکیبیاتی و ... است.

۱.۱ نظریه تحلیلی اعداد

نظریه تحلیلی اعداد از تکنیک‌های آنالیز برای حل مسائل در نظریه اعداد استفاده می‌کند. در این بخش چند مثال و قضیه از نظریه تحلیلی اعداد ارائه داده که در آن‌ها روش حل مسائل را به اختصار توضیح می‌دهیم.

قضیه. *تعداد اعداد اول نامتناهی است.*

اثبات اقلیدس[1] را همه می‌دانیم. پس در اینجا روشی دیگر منسوب به اویلر[2] را توضیح می‌دهیم که یکی از اولین تکنیک‌های استفاده از آنالیز در نظریه اعداد به حساب می‌آید. این اثبات به شکل زیر انجام می‌شود:

تبصره. این اثبات، اثبات خود اویلر است و دقت کافی را ندارد، ولی می‌توان آنرا دقیق کرد.

برهان. عدد زیر را در نظر بگیرید:

$$P_n = (\frac{۱}{۱-\frac{۱}{۲^n}})(\frac{۱}{۱-\frac{۱}{۳^n}})(\frac{۱}{۱-\frac{۱}{۵^n}})\cdots$$

که اعداد ۲، ۳، ۵، ... روی اعداد اول تغییر می‌کنند. در این صورت از بسط $\frac{۱}{۱-x} = \sum_{n=۰}^{\infty} x^n$ داریم:

$$P_n = (۱+\frac{۱}{۲^n}+\frac{۱}{۲^{۲n}}+\cdots)(۱+\frac{۱}{۳^n}+\frac{۱}{۳^{۲n}}+\cdots)\cdots$$

و با ضرب این جملات در هم و استفاده از این که تجزیه یکتا به اعداد اول وجود دارد، داریم:

$$P_n = ۱+\frac{۱}{۲^n}+\frac{۱}{۳^n}+\frac{۱}{۴^n}+\cdots \qquad (۱)$$

حال از فرم ضربی P_n لگاریتم می‌گیریم:

$$\log P_n = \log(\frac{۱}{۱-\frac{۱}{۲^n}}) + \log(\frac{۱}{۱-\frac{۱}{۳^n}}) + \log(\frac{۱}{۱-\frac{۱}{۵^n}}) + \cdots$$

و از بسط $\log(\frac{۱}{۱-x}) = \sum_{m=۱}^{\infty} \frac{x^m}{m}$ استفاده می‌کنیم:

$$\begin{aligned}\log P_n = &(\frac{۱}{۲^n}+\frac{۱}{۲}(\frac{۱}{۲^{۲n}})+\frac{۱}{۳}(\frac{۱}{۲^{۳n}})+\cdots)+\\ &(\frac{۱}{۳^n}+\frac{۱}{۲}(\frac{۱}{۳^{۲n}})+\frac{۱}{۳}(\frac{۱}{۳^{۳n}})+\cdots)+\\ &\cdots\end{aligned}$$

[1] Euclid
[2] Euler

حال با تغییر دادن آرایش آن داریم:

$$\begin{aligned}\log P_n = &(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \cdots) + \\ &\frac{1}{2}(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \cdots) + \\ &\frac{1}{3}(\frac{1}{2^{3n}} + \frac{1}{3^{3n}} + \frac{1}{5^{3n}} + \cdots) + \\ &\cdots\end{aligned} \tag{2}$$

حال n را برابر ۱ قرار می‌دهیم و داریم از (۱):

$$P_1 = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \log(\frac{1}{1-1}) = \log\ \infty$$

و از (۲) :

$$\begin{aligned}\log P_1 = &(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots) + \\ &\frac{1}{2}(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \cdots) + \\ &\frac{1}{3}(\frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{5^3} + \cdots) + \\ &\cdots\end{aligned}$$

حال مجموع جملات دوم به بعد سری بالا، مثلا طبق آزمون انتگرال، مقداری متناهی خواهد بود و داریم:

$$\log P_1 = \log\ \log\ \infty \approx \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots$$

و کار تمام است.

واضح است که اثبات بالا دقت کافی را ندارد ولی هر گام آن را می‌توان با همین روند دقیق کرد و پس از دقیق کردن متوجه می‌شویم که:

$$\sum_{p \le x} \frac{1}{p} \sim \log\ \log\ x$$

اویلر در اثبات قضیه قبل، از موجودی به نام P_n استفاده می‌کند که

$$P_n = \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \cdots$$

پس اویلر تعریف زیر را برای تابع زتای خود ارائه می‌دهد:

تابع زتای اویلر برای اعداد حقیقی $s > 1$ به شکل زیر تعریف می‌شود:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

پس در واقع، در اثبات قضیه قبل داشتیم $P_n = \zeta(n)$ و همچنین برای P_n یک فرم ضربی داشتیم که اویلر برای حالت کلی‌تری این فرم ضربی را ارائه می‌دهد:

قضیه. *(اویلر) برای $s > ۱$ داریم:*

$$\zeta(s) = \prod_{p \text{ اول}} \left(\frac{۱}{۱ - \frac{۱}{p^s}}\right)$$

برهان. مانند قبل، به دلیل تجزیه یکتای اعداد طبیعی بزرگتر از ۱ به اعداد اول.

به این فرم ضربی، تجزیه اویلری [۳] تابع زتا می‌گویند.

اویلر چند مقدار این تابع را در اعداد زوج بطور صریح بدست آورد:

قضیه. *(اویلر) برای $n \in \mathbb{N}$ داریم:*

$$\zeta(۲n) = \frac{۲^{۲n-۱}\pi^{۲n}}{(۲n)!}|B_{۲n}|$$

که B_nها اعداد برنولی هستند.

همچنین اویلر با بررسی سری $\sum_{n=۱}^{\infty} n^k x^n$، سعی کرد مقادیر تابع ζ را برای اعداد منفی پیدا کند. اگرچه او تعریف دقیقی برای تابع زتا در اعداد منفی نداشت ولی احتمالاً می‌دانست که آنرا مانند تابع فاکتوریل می‌توان به کل اعداد حقیقی گسترش داد.

قضیه. *(اویلر)*

$$\frac{\zeta(۱-n)}{\zeta(n)} = \frac{۲^{۱-n}\cos(\frac{n\pi}{۲})(n-۱)!}{\pi^n}$$

همچنین اویلر حدس زیر را مطرح می‌کند که به دو طریق در مقاله ریمان[۴] اثبات می‌شود.

حدس. *(اویلر) برای هر عدد حقیقی مثبت s،*

$$\frac{\zeta(۱-s)}{\zeta(s)} = \frac{۲^{۱-s}\cos\left(\frac{s\pi}{۲}\right)\Gamma(s)}{\pi^s}$$

که تابع $\Gamma(s)$ توسیع فاکتوریل به کل اعداد حقیقی است و با رابطه زیر تعریف می‌شود:

$$\Gamma(s) = \int_{۰}^{\infty} e^{-x}x^s\frac{dx}{x}$$

دیریکله[۵] در سال ۱۸۴۰، قضیه‌ی معروف خود را ثابت می‌کند:

قضیه. *(دیریکله) اگر r و m دو عدد طبیعی نسبت به هم اول باشند، آنگاه در تصاعد حسابی $\{mk+r|k \in \mathbb{N}\}$ بی‌نهایت عدد اول وجود دارد.*

برای اثبات این قضیه، دیریکله مجبور به تعمیم دادن تابع زتا شد. در واقع ایده‌ی او این بود که اثبات کند $\sum_{p \overset{m}{\equiv} r} \frac{۱}{p}$ واگرا به بی‌نهایت است و با استفاده از آن قضیه‌اش را نتیجه بگیرد. برای تعریف Lـ توابع دیریکله باید ابتدا مشخصه‌های دیریکله را تعریف کنیم:

تعریف. *تابع $\chi : \mathbb{Z} \to \mathbb{C}$ را یک مشخصه دیریکله به پیمانه m می‌نامیم هرگاه خواص زیر را داشته باشد:*

- *اگر a نسبت به m اول نباشد: $\chi(a) = ۰$*

[3] Euler factorization
[4] Riemann
[5] Dirichlet

- *اگر a نسبت به m اول باشد:* $|\chi(a)| = ۱$
- *اگر* $a, b \in \mathbb{Z}$ *آنگاه* $\chi(a)\chi(b) = \chi(ab)$ *(کاملاً ضربی بودن)*
- *برای همه* $k \in \mathbb{Z}$ *داریم:* $\chi(k+m) = \chi(k)$

پس مشخصه‌ی دیریکله در واقع یک هومومورفیسم از $(\mathbb{Z}/m\mathbb{Z})^*$ به $\mathbb{C}^*$ است. همچنین تابع $\chi_۰ \equiv ۱$ را مشخصه بدیهی می‌نامیم.

تعریف. *فرض کنید χ یک مشخصه‌ی دیریکله باشد. Lـ تابع دیریکله‌ی وابسته به آن را به شکل زیر تعریف می‌کنیم:*

$$L(s,\chi) = \sum_{n=۱}^{\infty} \frac{\chi(n)}{n^s}$$

اگر χ مشخصه بدیهی باشد، سری بالا برای $s > ۱$ همگراست و برابر با تابع زتای اویلر است.

اگر χ مشخصه بدیهی نباشد، سری بالا برای $s > ۰$ همگراست.

این تابع این خاصیت را دارد که اعداد متفاوت به پیمانه m را از هم "جدا" می‌کند. مثلا اگر $\chi_۱$ مشخصه‌ی دیریکله به پیمانه ۴ باشد که با $\chi_۱(۱) = ۱$ و $\chi_۱(۳) = -۱$ شناسایی می‌شود، آنگاه Lـ تابع وابسته به آن برابر است با:

$$L(s,\chi_۱) = \sum_{n=۱}^{\infty} \frac{\chi_۱(n)}{n^s} = \sum_{n \equiv ۱ \pmod ۴} \frac{۱}{n^s} - \sum_{n \equiv ۳ \pmod ۴} \frac{۱}{n^s}$$

همچنین Lـ توابع به دلیل کاملاً ضربی بودن χ، تجزیه اویلری دارند:

قضیه. *اگر $L(s,\chi)$ یک Lـ تابع دیریکله باشد. در این صورت برای sهایی که Lـ تابع تعریف می‌شود، داریم:*

$$L(s,\chi) = \prod_{p \text{ اول}} \left(\frac{۱}{۱ - \frac{\chi(p)}{p^s}}\right)$$

برهان. با استفاده از کاملاً ضربی بودن χ و بسط تیلور $\frac{۱}{۱-x}$، داریم:

$$\begin{aligned} L(s,\chi) &= \prod_{p \text{ اول}} \left(\frac{۱}{۱ - \frac{\chi(p)}{p^s}}\right) \\ &= \prod_{p \text{ اول}} \left(۱ + \frac{\chi(p)}{p^s} + \frac{\chi(p^۲s)}{p^{۲s}} + \cdots\right) \\ &= \sum_{n=۱}^{\infty} \frac{\chi(n)}{n^s} \end{aligned}$$

معمولاً مقدار Lـ توابع در نقطه $s = ۱$ اهمیت زیادی دارد. مثلاً مهم‌ترین حکمی که دیریکله برای اثبات قضیه خود به آن احتیاج داشت قضیه زیر بود:

قضیه. *(دیریکله) اگر χ یک مشخصه دیریکله نابدیهی باشد آنگاه* $L(۱,\chi) \neq ۰$.

سپس دیریکله با استفاده از Lـ توابع، اعداد اول به پیمانه m جدا می‌کند و برای هر کدام از آن دسته‌ها از اعداد اول، ثابت می‌کند:

قضیه. *(دیریکله) اگر m و r دو عدد طبیعی نسبت به هم اول باشند، آنگاه ثابت A (وابسته به r و m) وجود دارد که:*

$$\sum_{p \overset{m}{\equiv} r, p \leq x} \frac{۱}{p} = \frac{۱}{\phi(m)} \log\log x + A + O\left(\frac{۱}{\log x}\right)$$

برهان. رجوع شود به فصل ۷ از [Apo76] .

این قضیه، قضیه دیریکله را نتیجه می‌دهد و در واقع اثبات می‌کند "چگالی" اعداد اول برای r های نسبت به m اول متفاوت نیز یکسان است.

ریمان در مقاله معروف خود، [Rie59]، تابع زتای اویلر را به تمام اعداد مختلط گسترش می‌دهد و با استفاده از آن تلاشی برای اثبات "قضیه اعداد اول" می‌کند:

قضیه. (*قضیه اعداد اول*) *فرض کنید x یک عدد حقیقی مثبت باشد و تابع $\pi(x)$ را برابر با تعداد اعداد اول از ۱ تا x تعریف کنید. در این صورت داریم:*

$$\pi(x) \sim \frac{x}{\log\ x}$$

که این یعنی $\frac{\pi(x)}{x/\log\ x} \to ۱$ وقتی x به بی‌نهایت میل می‌کند.

ابتدا ریمان تابع ζ را به اعداد مختلط s با $Re\ s > ۱$ گسترش می‌دهد. در واقع سری $\sum \frac{۱}{n^s}$ برای محدوده‌ی $Re\ s > ۱$ به طور مطلق همگراست و تابع زتا را در این ناحیه می‌توان گسترش داد.

ریمان در آنالیز مختلط بسیار قوی بود و توانست تابع زتا را به شکلی انتگرالی به کل صفحه‌ی مختلط گسترش دهد و حدس اویلر (که اکنون به معادله تابعی تابع زتا معروف است) را با دو روش اثبات کند.

قضیه. (*ریمان*) *تابع زتای اویلر را می‌توان به صفحه مختلط گسترش داد به طوری که به جز یک قطب ساده با مانده‌ی ۱ در نقطه $s = ۱$ ، در بقیه نقاط تحلیلی باشد.*

همچنین با قضیه نسبتاً ساده‌ای در آنالیز مختلط می‌توان نتیجه گرفت که این گسترش یکتا نیز هست.

حال می‌توان قضیه اعداد اول را به کمک تابع زتای ریمان به شکل دیگری بیان کرد:

قضیه. *قضیه اعداد اول معادل است با صفر نشدن تابع زتای ریمان روی خط $\{s \in \mathbb{C} | Re\ s = ۱\}$.*

برهان. رجوع شود به فصل ۱۳ از [Apo76].

همچنین ریمان حدسی را در مقاله‌اش مطرح می‌کند و در مورد آن می‌نویسد:

"... ممکن است کسی به اثبات دقیقی از این موضوع علاقه داشته باشد، ولی من تلاش برای پیدا کردن اثبات آن را کنار گذاشته‌ام، زیرا این موضوع برای هدف تحقیق من نیاز نیست."

این حدس "فرض ریمان" نام گرفته و ادعا می‌کند:

حدس. (*فرض ریمان*[۶]) *اگر صفری از تابع زتای ریمان روی نوار $\{s \in \mathbb{C} | ۰ < Re\ s < ۱\}$ قرار داشته باشد، آنگاه آن صفر روی خط بحرانی $\{\frac{۱}{۲} + it | t \in \mathbb{R}\}$ قرار دارد.*

برای این حدس تاکنون تلاش‌های بسیاری شده است و معادل‌های بسیاری برای آن یافت شده است، ولی با این وجود تاکنون حل نشده است و جزء سخت ترین مسائل حل نشده ریاضیات به حساب می‌آید.

فرض ریمان نتایج بسیاری دارد که از جمله آن‌ها می‌توان به تقریب بهتری از $\pi(x)$ اشاره کرد:

[6] Riemann Hypothesis (RH)

نتیجه. *اگر فرض ریمان درست باشد و اگر انتگرال لگاریتمی*[7] *را برابر* $Li(x) = \int_{۲}^{x} \frac{dt}{\log\ t}$ *تعریف کنیم، آنگاه:*

$$|\pi(x) - Li(x)| < \frac{۱}{۸\pi}\sqrt{x}\ \log\ x$$

.

برهان. رجوع شود به [Sho76] .

Lـ توابع دیریکله را نیز مانند تابع زتا، می‌توان به طور مرومورفیک [8] به کل صفحه گسترش داد و حدسی مانند فرض ریمان برای آن ها فرمول‌بندی کرد:

حدس. *(فرض تعمیم‌یافته ریمان*[9] *) اگر* χ *یک مشخصه دیریکله باشد و صفری از تابع* $L(s,\chi)$ *روی نوار بحرانی* $\{s \in \mathbb{C} | ۰ < Re\ s < ۱\}$ *قرار داشته باشد، آنگاه آن صفر روی خط بحرانی* $\{\frac{۱}{۲} + it | t \in \mathbb{R}\}$ *قرار گرفته است.*

۲.۱ قضیه آخر فرما و نظریه جبری اعداد

با معادله دیوفانتی $y^۲ + ۲ = x^۳$ شروع می‌کنیم. در حلقه‌ی $\mathbb{Z}[\sqrt{-۲}]$ آن را به شکل زیر تجزیه می‌کنیم:

$$(y + \sqrt{-۲})(y - \sqrt{-۲}) = x^۳$$

برای حل این معادله و استفاده از معادله بالا، ما نیاز به مفهومی مانند ب‌م‌م در حلقه‌ی $\mathbb{Z}[\sqrt{-۲}]$ داریم و برای داشتن چنین مفهومی نیاز داریم بدانیم که $\mathbb{Z}[\sqrt{-۲}]$ حلقه‌ی تجزیه یکتا است یا خیر. قضیه زیر این را برای ما اثبات می‌کند:

قضیه. $\mathbb{Z}[\sqrt{-۲}]$ *یک دامنه‌ی اقلیدسی است.*

برهان. تابع $N : \mathbb{Z}[\sqrt{-۲}] \to \mathbb{N} \cup \{۰\}$ را با ضابطه‌ی $N(x + \sqrt{-۲}y) = x^۲ + ۲y^۲$ تعریف کنید. در این صورت برای تقسیم $a + \sqrt{-۲}b$ بر $c + \sqrt{-۲}d$، خارج‌قسمت را به شکل زیر انتخاب کنید:

$$a + \sqrt{-۲}b = (c + \sqrt{-۲}d)(q_۱ + \sqrt{-۲}q_۲) + (r_۱ + \sqrt{-۲}r_۲)$$

که $q_۱$ و $q_۲$ نزدیکترین اعداد صحیح به ترتیب به $\frac{ac+۲bd}{c^۲+۲d^۲}$ و $\frac{bc-ad}{c^۲+۲d^۲}$ هستند.

دقت کنید که

$$\frac{a + \sqrt{-۲}b}{c + \sqrt{-۲}d} = \frac{ac + ۲bd}{c^۲ + ۲d^۲} + \sqrt{-۲}\frac{bc - ad}{c^۲ + ۲d^۲}$$

در این صورت

$$\frac{a + \sqrt{-۲}b}{c + \sqrt{-۲}d} - (q_۱ + \sqrt{-۲}q_۲) = \frac{r_۱ + \sqrt{-۲}r_۲}{c + \sqrt{-۲}d}$$

پس

$$N(\frac{r_۱ + \sqrt{-۲}r_۲}{c + \sqrt{-۲}d}) = |\frac{a + \sqrt{-۲}b}{c + \sqrt{-۲}d} - (q_۱ + \sqrt{-۲}q_۲)|^۲ \leq (\frac{۱}{۲})^۲ + ۲(\frac{۱}{۲})^۲ = \frac{۳}{۴}$$

[7] Logarithmic integral

[8] Meromorphic

[9] Generalized Riemann Hypothesis (GRH)

پس

$$N(r_1 + \sqrt{-2}r_2) \leq \frac{3}{4}N(c + \sqrt{-2}d) < N(c + \sqrt{-2}d)$$

پس $\mathbb{Z}[\sqrt{-2}]$ یک حلقه‌ی تجزیه یکتا است. حال به معادله دیوفانتی باز می‌گردیم. اولاً y باید فرد باشد زیرا اگر زوج باشد، سمت چپ معادله $4k+2$ خواهد بود و پس x باید زوج باشد و پس سمت راست $8k$ است که تناقض است. حال اگر $d|y+\sqrt{-2}$ و $d|y-\sqrt{-2}$. در این صورت

$$d|2\sqrt{-2},\ \ d|2y$$

از آنجا که $\sqrt{-2}$ در $\mathbb{Z}[\sqrt{-2}]$ یک عدد اول است، پس d باید توانی از $\sqrt{-2}$ (در حد یک وارونپذیر) باشد، ولی از طرفی $d|y+\sqrt{-2}$ که از آنجا که y فرد است، تناقض است. پس هر کدام از $y+\sqrt{-2}$ و $y-\sqrt{-2}$ باید توان سوم باشند و پس

$$(y+\sqrt{-2}) = (a+\sqrt{-2}b)^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$$

پس

$$1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$$

و پس $b = 1, a = \pm 1$ بنابراین $(3,5), (3,-5)$ تنها جوابهای این معادله هستند.

این مثال نشان می‌دهد که کار کردن در میدان‌ها و حلقه‌های بزرگتر از $\mathbb{Q}$ و $\mathbb{Z}$، اگر خوش‌رفتار باشند، می‌توانند مفید باشند (مثلاً حلقه‌ی تجزیه صحیح هستند و ...).

از آنجایی که معادله دیوفانتی بالا با توسیع میدان از $\mathbb{Q}$ به $\mathbb{Q}(\sqrt{-2})$ حل شد، ما توسیع میدان‌ها روی $\mathbb{Q}$ را در حالت کلی‌تری بررسی می‌کنیم.

تعریف. *میدان K را یک میدان عددی گوییم هرگاه یک توسیع متناهی از $\mathbb{Q}$ باشد.*

همچنین مجموعه‌ی همه‌ی اعضای K که در یک چندجمله‌ای تکین با ضرایب صحیح صدق می‌کنند را حلقه‌ی اعداد صحیح می‌گویند و با O_K نشان می‌دهند.

حال با مقدماتی که ارائه شد قضیه‌ی آخر فرما[10] را با بهره‌گیری از یافته‌ها و دستاوردهای کومر[11] اثبات می‌کنیم و نظریه جبری اعداد را بصورت مفصل‌تری بررسی می‌کنیم:

قضیه. (*قضیه آخر فرما*) *فرض کنید $n \geq 3$، در این صورت $x^n + y^n = z^n \Leftarrow xyz = 0$.*

در سال ۱۶۳۷، در ویرایشی از کتاب حساب[12] فرما ادعای زیر را نوشت: "غیرممکن است که یک مکعب را به دو مکعب تجزیه کرد، یا یک توان چهارم را به دو توان چهارم، و در حالت کلی هر توان بزرگ‌تر از دو را به دو توان شبیه هم، من یک اثبات شگفت‌انگیز از این پیدا کرده‌ام که این حاشیه کوچک‌تر از آن است که آن را قرار دهم." پس از او ریاضیدان‌های بسیاری برای اثبات این موضوع تلاش کردند و به نتایج جزئی نیز رسیدند. مثلاً:

۱) فرما در سال ۱۶۴۰، حالت توان چهارم را حل کرد.

۲) اویلر بین سال‌های ۱۷۵۸ و ۱۷۷۰ حالت توان سوم را حل کرد.

۳) سوفی ژرمن[13] در اوایل قرن ۱۹، راه‌حلی ایجاد کرد که حداقل برای همه توان‌های اول فرد کمتر از ۱۰۰، حالت اول قضیه فرما را ثابت می‌کرد $(x^n + y^n = z^n \Rightarrow n \mid xyz)$.

[10] Fermat
[11] Kummer
[12] Arithmetica
[13] Sophie Germain

۴) کومر با استفاده از نظریه اعداد جبری قضیه را برای حدود ۶۰ درصد (حدسی!) از اعداد اول ثابت کرد.

۵) در سال ۱۹۷۷، ترجانیان[14] حالت اول قضیه را برای همه‌ی توان‌های زوج (غیر ۲!) اثبات کرد.

ولی در سال ۱۹۸۴ بود که فری[15] یک ارتباط بین این حدس و خمی بیضوی یافت و احساس کرد که غلط بودن قضیه آخر فرما باعث رد حدسی معروف از شیمورا و تانیاما می‌شود. دو سال پس از آن، ریبت این روند را ادامه داد و با اثبات حدسی از سر ، به نام حدس اپسیلون [16]، اثبات قضیه آخر فرما را به حدس شیمورا[17] ـ تانیاما[18] کاهش داد. بعد از او، ریاضیدان انگلیسی، اندرو وایلز[19]، که از زمان کودکی آرزوی حل این مسئله را داشت، ۶ سال روی این مسئله کار کرد و در نهایت، در سال ۱۹۹۳ موفق به اثبات مقداری از حدس شیمورا ـ تانیاما شد که برای اثبات قضیه آخر فرما کافی بود. پس از آن اشکالی در اثبات وایلز پیدا شد که باعث شد وایلز و تیلور[20] (شاگرد قدیمی او) یک سال دیگر تلاش کنند تا آن اشکال را برطرف نمایند. در انتها، در سال ۱۹۹۵، قضیه آخر فرما به‌طور کامل اثبات شد. همچنین با قوی‌تر کردن ایده‌های وایلز، تعدادی ریاضیدان دیگر، بروی[21] و کنراد[22] و دایموند[23] و تیلور، توانستند حدس شیمورا ـ تانیاما را به‌طور کامل اثبات کنند و پس از آن، نام آن تبدیل به قضیه مدولاریتی[24] شد.

روش کومر برای حل این مسأله بدین شکل است: ابتدا این معادله را فقط باید برای حالت خاص n اول در نظر بگیریم، زیرا اگر $p|n$ یک عامل اول n باشد می‌توان مسئله را به شکل $(x^{\frac{n}{p}})^p + (y^{\frac{n}{p}})^p = (z^{\frac{n}{p}})^p$ نوشت و پس اگر قضیه آخر فرما برای اعداد اول درست باشد قضیه نتیجه می‌شود. پس از این به بعد n را به p تغییر می‌دهیم. حال فرض می‌کنیم x, y, z نسبت به هم اول هستند (این فرض از کلیت مسأله کم نمی‌کند) سمت راست را تجزیه می‌کنیم و معادله به صورت زیر در می‌آید:

$$(x+y)(x+\zeta_p y)(x+\zeta_p^2 y)...(x+\zeta_p^{p-1} y) = z^p$$

که ζ_p ریشه‌ی pام واحد است. پس ما توسیع میدانی از $\mathbb{Q}$ به $\mathbb{Q}(\zeta_p)$ را در نظر گرفته‌ایم. می‌توان اثبات کرد که حلقه‌ی اعداد صحیح $\mathbb{Q}(\zeta_p)$، $\mathbb{Z}[\zeta_p]$ است (رجوع شود به کتاب [Was82] فصل ۱). مسأله را در این حلقه بررسی می‌کنیم.

$\mathbb{Z}[\zeta_p]$ لزوماً یک حلقه‌ی تجزیه یکتا نیست اما کومر قضیه‌ای ثابت کرده است که نشان می‌دهد به جای یافتن تجزیه یکتا برای اعضا، تجزیه یکتا برای ایدآل‌ها وجود دارد:

قضیه. *(کومر) فرض کنید K یک میدان عددی باشد و O_K حلقه‌ی اعداد صحیح K باشد. حال اگر $I \neq 0$ یک ایدآل سره از O_K باشد، آنگاه به شکل یکتا (در حد جایگشت) می‌توان نوشت*

$$I = \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2}...\mathfrak{P}_n^{\alpha_n}$$

که $\mathfrak{P}_i$ها ایدآل‌های اول و α_iها اعداد صحیح مثبت هستند.

در اینجا ابتدا گریز کوتاهی می‌زنیم به تجزیه ایدآل‌های اول. فرض کنید p عدد اولی باشد و تجزیه ایدآل $(p)O_K$ در O_K را در نظر بگیرید:

$$(p)O_K = \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2}...\mathfrak{P}_g^{\alpha_g}$$

[14] Terjanian
[15] Frey
[16] Epsilon conjecture
[17] Shimura
[18] Taniyama
[19] Andrew Wiles
[20] R. Taylor
[21] Breuil
[22] Conrad
[23] Diamond
[24] Modularity theorem

در این صورت، به α_i اندیس شاخه‌ای[25] $e_i = \mathfrak{P}_i/p$ می‌گویند و همچنین اگر $p^{f_i} = |O_K/\mathfrak{P}_i|$، f_i را درجه مانده‌ی[26] $\mathfrak{P}_i/p$ گویند. اگر همه‌ی e_iها یک باشند، به این توسیع غیرشاخه‌ای در p می‌گوییم و عدد اول p را غیرشاخه‌ای در این توسیع می‌گوییم. اگر توسیع $K/\mathbb{Q}$ گالوا باشد، آنگاه $\forall i,j \quad e_i = e_j, f_i = f_j$ و پس به هرکدام از e_iها اندیس شاخه‌ای p در K گویند. در این حالت، یک دنباله کوتاه به شکل زیر خواهیم داشت:

$$\circ \to I_{\mathfrak{P}_i/p} \to D_{\mathfrak{P}_i/p} \to \mathrm{Gal}(\frac{O_K}{\mathfrak{P}_i}/\mathbb{F}_p) \to \circ$$

که

$$D_{\mathfrak{P}_i/p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) | \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$$

و گروه تجزیه[27] نامیده می‌شود و $I_{\mathfrak{P}_i/p}$ هسته‌ی تابع به پیمانه $\mathfrak{P}_i$ گرفتن $D_{\mathfrak{P}_i/p} \to \mathrm{Gal}(\frac{O_K}{\mathfrak{P}_i}/\mathbb{F}_p)$ است و به آن گروه اینرسی[28] گویند که تعداد اعضایش برابر e_i است. پس $\mathfrak{P}_i/p$ غیرشاخه‌ای است اگر و تنها اگر $I_{\mathfrak{P}_i/p} = \{1\}$.

حال به بحث اصلی بازمی‌گردیم؛ در معادله‌ی بالا در دو طرف، ایدآل تولید شده توسط طرفین را در نظر می‌گیریم. بنابراین خواهیم داشت که ضرب ایدآل‌های اصلی به فرم $(x + \zeta_p^i y)$ $(\circ \le i \le p-1)$ برابر با ایدآل اصلی $(z)^p$ شده است. حال قضیه مهمی در نظریه اعداد داریم که در این گونه مواقع قابل استفاده است (این حالت قضیه‌ای که ما می‌نویسیم فقط برای $\mathbb{Z}$ و حلقه‌های تجزیه یکتا درست است).

قضیه. *اگر a و b اعداد صحیح باشند بطوری که ab توان nام کامل است و $(a,b) = 1$، در این صورت در حد ± 1، a و b توان‌های nام کامل هستند.*

برهان. a و b را به اعداد اولشان تجزیه می‌کنیم و در آنجا توان‌های اعداد اولشان باید بر n بخش‌پذیر باشند پس خود آن‌ها نیز باید توان nام باشند.

پس این قضیه فقط با این فلسفه که می‌دانیم تجزیه یکتا به اعداد اول وجود دارد اثبات می‌شود، پس با استفاده از قضیه کومر می‌توان همین قضیه را برای ایدآل‌ها اثبات کرد.

نتیجه. *اگر $I, J \subseteq O_K$ دو ایدآل سره و ناصفر باشند و IJ توان nام ایدآلی باشد و I, J ایدآل‌های اول یکسانی در تجزیه‌شان به ایدآل‌های اول نداشته باشند (یا معادلاً $I + J = (1)$، در این حالت می‌گوییم این دو ایدآل نسبت به هم اول هستند) در این صورت هر دوی I و J توان nام کامل خواهند بود.*

پس تلاش می‌کنیم اثبات کنیم ایدآل‌های $(x + \zeta_p^i y)$ نسبت به هم اول هستند تا بتوانیم از این قضیه استفاده کنیم. فرض کنیم ایدآل اولی مثل $\mathfrak{P}$ دوتا از آنها را عاد می‌کند:

$$\mathfrak{P} | (x + \zeta_p^i y),\ \mathfrak{P} | (x + \zeta_p^j y)$$

پس

$$\mathfrak{P} | (\zeta_p^i - \zeta_p^j)(y) = (1 - \zeta_p^{j-i})(y)$$

حال داریم که $\frac{1-\zeta_p^{j-i}}{1-\zeta_p}$ یک عضو وارون‌پذیر در $\mathbb{Z}[\zeta_p]$ است (چرا؟) و پس

$$\mathfrak{P} | (1 - \zeta_p)(y)$$

[25] Ramification index
[26] Residue degree
[27] Decomposition group
[28] Inertia group

حال $(1-\zeta_p)$ یک ایدآل اول در $\mathbb{Z}[\zeta_p]$ است که $(p) = (1-\zeta_p)^{p-1}$ چون

$$p = (1-\zeta_p)(1-\zeta_p^2)...(1-\zeta_p^{p-1})$$

پس یا $(1-\zeta_p) = \mathfrak{P}$ یا $\mathfrak{P}|(y)$. اگر $\mathfrak{P}|(y)$ از $\mathfrak{P}|(x+\zeta_p^i y)$ نتیجه می‌شود $\mathfrak{P}|(x)$ و پس x, y, z نسبت به یکدیگر اول نیستند (در واقع اگر q عدد اولی باشد که $q|N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\mathfrak{P}$ در این صورت $q|\gcd(x,y)$ و پس از معادله $x^p + y^p = z^p$ نتیجه می‌شود $q|\gcd(x,y,z)$) که تناقض است.

پس $\mathfrak{P} = 1-\zeta_p$ و پس

$$1-\zeta_p|x+\zeta_p^i y \Rightarrow 1-\zeta_p|x+y \Rightarrow p|x+y \Rightarrow p|z$$

این تناقض ایجاد نمی‌کند ولی نشان می‌دهد که با این روش می‌توان قضیه آخر فرما را در حالت خاص‌تری حل کرد. در واقع از این به بعد تلاش می‌کنیم حالت اول قضیه آخر فرما را حل کنیم:

قضیه. (*حالت اول قضیه آخر فرما*)

$$x^p + y^p = z^p,\ x, y, z \in \mathbb{Z} \Rightarrow p|xyz$$

پس در این حالت فرض $\mathfrak{P}|(1-\zeta_p)$ نیز منجر به تناقض می‌شود (زیرا از بالا $p|z$) و پس ایدآل‌های $(x+\zeta_p^i y)$ نسبت به هم اول هستند. حال چون ضرب آن‌ها توان pام کامل شده، همگی آن‌ها توان pام کامل هستند، مخصوصاً

$$(x+\zeta_p y) = I^p$$

برای ایدآل سره و ناصفر I از $\mathbb{Z}[\zeta_p]$.

حال ما علاقه داریم به این که که I ایدآلی اصلی باشد که بتوان با این معادله کاری روی اعضا (به جای ایدآل‌ها) انجام داد. برای این کار باید مفهوم عدد کلاسی[۲۹] را تعریف کنیم:

مجموعه‌ی همه‌ی O_Kـ زیرمدول‌های متناهی تولید ناصفر K را در نظر بگیرید (این همه‌ی ایدآل‌های ناصفر O_K را شامل می‌شود چون O_K نوتری است) و با $\mathcal{I}$ نشان دهید و مجموعه‌ی همه‌ی O_Kـ زیرمدول‌های ناصفر تولید شده توسط یک عنصر را با $\mathcal{P}$ نشان دهید. در این صورت $\mathcal{I}$ با ضرب (ضرب زیرمدول‌ها مانند ضرب ایدآل‌ها تعریف می‌شود) یک گروه تشکیل می‌دهد با عضو خنثی (۱)، در این صورت طبق قضیه‌ای از مینکوفسکی $|\mathcal{I}/\mathcal{P}|$ متناهی است و به آن عدد کلاسی K گفته می‌شود، همچنین به گروه $\mathcal{I}/\mathcal{P}$ گروه کلاسی[۳۰] حلقه O_K گفته می‌شود.

حال در حالت $\mathbb{Q}(\zeta_p)$ که مورد توجه ماست، اگر فرض کنیم p عدد کلاسی $\mathbb{Q}(\zeta_p)$ را عاد نکند (به اعداد اول p که این خاصیت را دارند را اعداد اول منظم[۳۱] گویند، از نظر آماری حدود ۶۰% از اعداد اول، اعداد اول منظم هستند). حال فرض کنید در بالا p یک عدد اول منظم باشد. در این صورت از معادله بالا داریم که I^p یک ایدآل اصلی است و در گروه $\mathcal{I}/\mathcal{P}$ خنثی است پس از آنجا که این گروه متناهی و عدد اصلیش نسبت به p اول است، خود I یک ایدآل اصلی است.

پس

$$(x+\zeta_p y) = (a_0 + a_1\zeta_p + ... + a_{p-2}\zeta_p^{p-2})^p$$

و پس به عنوان اعضا $x+\zeta_p y = u(a_0 + a_1\zeta_p + ... + a_{p-2}\zeta_p^{p-2})^p$ که u یک عضو وارون‌پذیر در $\mathbb{Z}[\zeta_p]$ است.

حال قضیه‌ای داریم:

[29] Class number
[30] Class group
[31] Regular

قضیه. *اگر u یک عضو وارون‌پذیر $\mathbb{Z}[\zeta_p]$ باشد، آنگاه $u = \epsilon(\pm\zeta_p^i)$ برای یک ϵ حقیقی.*

برهان. رجوع شود به کتاب [Was82] فصل ۱.

حال معادله بالا را به پیمانه p می‌گیریم و پس

$$x + \zeta_p y = u(a_0^p + a_1^p + ... + a_{p-2}^p) \pmod{p}$$

پس

$$x + \zeta_p y = un = \epsilon(\pm\zeta_p^i)n \pmod{p}$$

که $n \in \mathbb{Z}$. پس با در نظر گرفتن مزدوج مختلط داریم

$$x + \zeta_p^{-1} y = \epsilon(\pm\zeta_p^{-i})n \pmod{p}$$

و پس

$$\pm\zeta_p^{-i}(x + \zeta_p y) = \epsilon n = \pm\zeta_p^i(x + \zeta_p^{-1} y) \pmod{p}$$

پس

$$x + \zeta_p y + \zeta_p^{2i} x + \zeta_p^{2i-1} y = 0 \pmod{p}$$

بنابراین

$$p | x + \zeta_p y + \zeta_p^{2i} x + \zeta_p^{2i-1} y$$

و پس p باید ضرایب را عاد کند و پس $p|x, y$ که تناقض با فرض است.

پس بعد از همه‌ی این‌ها قضیه زیر را بدست می‌آوریم:

قضیه. *اگر p عدد اول منظمی باشد، در این صورت*

$$x^p + y^p = z^p \Rightarrow p | xyz$$

۲ هندسه جبری مقدماتی

در این بخش به هندسه جبری مقدماتی می‌پردازیم و با واریته‌های آفین و تصویری آشنا می‌شویم.

فرض کنید K میدان باشد. در این صورت فرض کنید تعدادی چندجمله‌ای $f_1, f_2, ..., f_m \in K[x_1, x_2, ..., x_n]$ در اختیار دارید و صفرهای مشترک این چندجمله‌ای‌ها را پیدا می‌کنیم که زیرمجموعه‌ای از فضای K^n می‌شود و با $X = Z(f_1, f_2, ..., f_m)$ نشان می‌دهیم. به این مجموعه یک واریته آفین[۳۲] می‌گویند. اولاً اگر ما ایدآل تولید شده توسط $f_1, f_2, ..., f_m$ را در نظر بگیریم و مجموعه‌ی صفرهای مشترک همه‌ی چندجمله‌ای‌های درون ایدآل را در نظر بگیریم، به همان مجموعه‌ی X می‌رسیم. بنابراین می‌توانیم فقط زیرمجموعه‌های به فرم $Z(I)$ برای ایدآل‌های متناهی‌تولید $I \trianglelefteq K[x_1, x_2, ..., x_n]$ را در نظر بگیریم. همچنین طبق قضیه پایه‌ی هیلبرت[۳۳] که در زیر آمده، هر $Z(I)$ را نیز می‌توان به شکل $Z(f_1, f_2, ..., f_m)$ برای متناهی چندجمله‌ای $f_1, f_2, ..., f_m$ نوشت:

قضیه. (*قضیه پایه هیلبرت*) *اگر R نوتری باشد، $R[x]$ نیز نوتری است. پس اگر K یک میدان باشد (یا یک حلقه نوتری) $K[x_1, x_2, ..., x_n]$ نوتری است.*

پس طبق این قضیه، هر ایدآل توسط متناهی عنصر تولید می‌شود و

$$I = (f_1, f_2, ..., f_m) \Rightarrow Z(I) = Z(f_1, f_2, ..., f_m)$$

در این صورت بوضوح $Z((0)) = K^n$ و $Z((1)) = \varnothing$. همچنین داریم:

$$\bigcap_{i \in I} Z(I_i) = Z(\bigoplus_{i \in I} I_i)$$

$$\bigcup_{i=1}^{m} Z(I_i) = Z(I_1 I_2 ... I_m)$$

پس اگر فضای K^n را همراه با توپولوژی بسته‌های $Z(I)$ برای $I \trianglelefteq K[x_1, x_2, ..., x_n]$ در نظر بگیریم، یک فضای توپولوژیک بدست می‌آید که با $\mathbb{A}^n_K$ (فضای آفین n بعدی) نشان می‌دهند. به این توپولوژی، توپولوژی زاریسکی[۳۴] می‌گویند.

پس واریته‌های آفین در $\mathbb{A}^n_K$، زیرمجموعه‌های بسته $\mathbb{A}^n_K$ هستند.

حال به شکل معکوس اگر ما یک زیرمجموعه‌ی $X \subseteq K^n$ داشته باشیم می‌توان ایدآل $I(X)$، را به شکل زیر تعریف کرد

$$I(X) = \{f \in K[x_1, x_2, ..., x_n] | \forall p \in X; f(p) = 0\}$$

حال می‌خواهیم بدانیم چقدر این دو عمل I, Z معکوس یکدیگر هستند.

در این صورت به سادگی می‌توان چک کرد که حکم زیر درست است.

حکم. *اگر $X \subseteq K^n$ آنگاه $Z(I(X)) = \bar{X}$.*

طرح برهان. اولاً ثابت کنید $X \subseteq Z(I(X))$. برای شمول برعکس به سادگی ثابت می‌شود

$$Z(I(Z(J))) = Z(J)$$

[32] Affine variety
[33] Hilbert
[34] Zariski

برای همه‌ی ایدآل‌های J و این که I, Z شمول برگردان هستند. حال فرض کنید $X \subseteq V$ یک بسته روی X باشد. در این صورت $V = Z(J)$ برای ایدآلی مثل J. پس

$$X \subseteq V = Z(J) \Rightarrow I(X) \supseteq I(Z(J)) \Rightarrow Z(I(X)) \subseteq Z(I(Z(J))) = Z(J) = V$$

پس $Z(I(X)) = \bar{X}$

از این به بعد فرض می‌کنیم که میدان K بسته جبری است. در این صورت هیلبرت برای عکس آن (یعنی برای $I(Z(J))$) نیز قضیه معروف زیر را ثابت کرد:

قضیه. *اگر $J \trianglelefteq K[x_1, x_2, ..., x_n]$ آنگاه $I(Z(J)) = \sqrt{J}$ که*

$$\sqrt{J} = \{a \in K[x_1, x_2, ..., x_n] | \exists n \in \mathbb{N}; a^n \in J\}$$

تذکر. *به $\sqrt{J}$، رادیکال J می‌گویند و به ایدآل‌هایی که با رادیکال خود برابرند، ایدآل‌های رادیکال می‌گویند مثلاً ایدآل‌های اول رادیکالند.*

پس اگر $X \subseteq K^n$ها را از بسته‌های K^n و $J \trianglelefteq K[x_1, x_2, ..., x_n]$ها را از ایدآل‌های رادیکال انتخاب کنیم، یک تناظر یک به یک مانند زیر میگیریم:

$$\{\text{زیرمجموعه‌های بسته‌ی } \mathbb{A}^n_K\} \leftrightharpoons \{\text{ایدآل‌های رادیکال } K[x_1, x_2, ..., x_n]\}$$

$$\begin{array}{ccc} J & \rightarrow & Z(J) \\ I(X) & \leftarrow & X \end{array}$$

تعریف. *اگر X یک واریته آفین در $\mathbb{A}^n_K$ باشد، در این صورت به $\frac{K[x_1,x_2,...,x_n]}{I(X)}$ حلقه‌ی مختصات[35] X گویند.*

حال یک تعادل رسته‌ها[36] بین رسته‌ی همه‌ی Kـجبرهای متناهی‌تولید و بدون پوچ‌توان و همه‌ی واریته‌های آفین وجود دارد با

$$\{K\text{ـجبرهای متناهی‌تولید و بدون پوچ‌توان}\} \leftrightharpoons \{\text{واریته‌های آفین }\}$$

$$\begin{array}{ccc} X & \rightarrow & \dfrac{K[x_1, x_2, ..., x_n]}{I(X)} \\ Z(J) & \leftarrow & A \cong \dfrac{K[x_1, x_2, ..., x_n]}{J} \end{array}$$

حال واریته‌های تصویری را تعریف می‌کنیم. در ابتدا باید $\mathbb{P}^n_K$ را تعریف کنیم.

تعریف. *فضای همه‌ی خطوط گذرنده از مبدا در $\mathbb{A}^{n+1}_K$ را $\mathbb{P}^n_K$ تعریف می‌کنیم. با نمادها:*

$$\mathbb{P}^n_K = \mathbb{A}^{n+1}_K - \{0\} / \sim$$

که $x \sim y$ اگر $x = \lambda y$ برای $\lambda \in K^*$.

در این صورت اگر بخواهیم مانند قبل صفرهای چندجمله‌ای‌های در $K[x_0, x_1, ..., x_n]$ (به حلقه‌ی چندجمله‌ای‌ها یک متغیر اضافه کرده‌ایم زیرا در $\mathbb{A}^{n+1}_K$ زندگی می‌کنیم) را در این فضا در نظر بگیریم به مشکل برمی‌خوریم، زیرا ممکن است یک چندجمله‌ای روی یک نقطه از یک خط

[35] Coordinate ring
[36] Equivalence of categories

گذرنده از مبدا صفر باشد ولی کاملاً روی آن خط صفر نباشد. پس برای این که این مشکل پیش نیاید باید فقط چندجمله‌ای‌هایی را در نظر بگیریم که اگر روی نقطه‌ای از یک خط صفر باشند، روی کل خط صفر باشند.

پس اگر f یک چندجمله‌ای باشد که روی $p \in \mathbb{A}_K^{n+1} - \{0\}$ صفر باشد، می‌خواهیم که روی λp هم صفر باشد. بنابراین اگر

$$f = f_0 + f_1 + ... + f_d$$

تجزیه f به قسمت‌های همگن خود باشد، داریم:

$$0 = f(\lambda p) = f_0(p) + \lambda f_1(p) + \lambda^2 f_2(p) + ... + \lambda^d f_d(p)$$

و پس این باید برای همه‌ی λها درست باشد که از آنجا که میدان K نامتناهی است (هر میدان بسته‌ی جبری نامتناهی است (چرا؟)) نشان می‌دهد که همه‌ی ضرایب صفر هستند یعنی همه‌ی مولفه‌های همگن f نیز روی p صفر می‌شوند و پس برای اینکه مشکل پیش نیاید باید فقط $Z(I)$هایی را در نظر بگیریم که I توسط تعدادی چندجمله‌ای همگن تولید شده باشد. به این ایدآل‌ها، ایدآل‌های همگن گوییم. پس به واریته‌هایی که به شکل $Z(I)$ برای یک ایدآل همگن $I \trianglelefteq K[x_0, x_1, ..., x_n]$ باشند، واریته‌های تصویری[37] می‌گویند. برای واریته‌های تصویری نیز مانند واریته‌های آفین یک تناظر وجود دارد که از آنجا بدان نیاز نداریم به آن نمی‌پردازیم. در اینجا تعریف بعد یک واریته را تعریف می‌کنیم:

تعریف. *فرض کنید V یک واریته آفین (تصویری) باشد، در این صورت به طول زنجیر ماکسیمال از بسته‌های $\varnothing \neq A_0 \subsetneq A_1 \subsetneq ... \subsetneq A_n = V$ در فضای آفین (تصویری) بعد V گویند و با $\dim V$ نشان دهند.*

[37] Projective varieties

۳ خم‌های جبری

منظور ما از یک خم جبری، همواره، یک واریته تصویری با بعد ۱ روی میدان کامل[۳۸] K است که با C/K نمایش می‌دهیم. خم‌های جبری را می‌توان با استفاده از گونای[۳۹] آن‌ها دسته‌بندی کرد. در بخش‌های بعدی سعی شده است همه خم‌ها با گونای داده شده را در حد ایزومورفیسم پیدا کنیم. قضیه ریمان‌ـ رخ[۴۰] از مهم‌ترین ابزارها برای این کار است. در ابتدا، مقدمات قضیه ریمان‌ـ رخ را بیان می‌کنیم.

۱.۳ قضیه ریمان‌ـ رخ

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 گونایشان طبقه‌بندی کرد. در واقع، گونا، یک ناوردای دوگویا[۴۱] است که مقادیر نامنفی می‌گیرد. همچنین برای هر $g > ۰$ داده شده، یک واریته تحویل‌ناپذیر $\mathcal{M}_g$ به نام "واریته مدولی خم‌های گونای g" وجود دارد که همه‌ی خم‌های هموار را در حد تعادل دوگویا[۴۲] طبقه‌بندی می‌کند، به عبارت دیگر، هر نقطه از آن به یک خم گونای g تناظر داده می‌شود. پس در واقع همه‌ی خم‌های هموار با یک مولفه‌ی "گسسته" (گونا) و یک مولفه‌ی "پیوسته" (واریته مدولی) داده می‌شوند. خم‌های هموار با گونای ۱ با نقاط Kـ گویا، خم‌های بیضوی روی K نامیده می‌شوند. (البته در ابتدا خم‌های بیضوی 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 گونای ریمانی تعداد سوراخ‌های آن است و این تعریف گونا را می‌توان به همه‌ی خم‌های جبری تعمیم داد. این قضیه تعمیم‌های بسیاری داده شده است. ما قضیه ریمان‌ـ رخ را برای خم‌های جبری بیان و در بخش‌های بعدی از آن استفاده می‌کنیم.

برای بیان کردن قضیه ریمان‌ـ رخ نیاز به تعریف مقسم[۴۳] داریم که توضیحاتی را در ادامه راجع به آن بیان می‌کنیم:

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 $n_P = ۰$ 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 $f \in \bar{K}(C)$ 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 و برای $f = ۰$ قرار می‌دهیم:

$$div\ ۰ = \sum_{P \in C} \infty(P)$$

که بینهایت آن صوری است.

[38] Perfect
[39] Genus
[40] Riemann-Roch theorem
[41] Birational
[42] Birational Equivalence
[43] Divisor

حکم. *برای هر* $f \in \bar{K}(C)$ *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[44] 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[45] است و با $D \geq 0$ نمایش می‌دهیم، هرگاه $n_P \geq 0$ برای هر $P \in C$.

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 [Ful69].

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[46] مثل $t_P \in \bar{K}(C)$ انتخاب کنید. در این صورت از آن‌جا که بعد فضای برداری فرم‌های دیفرانسیل روی $\bar{K}(C)$ برابر ۱ است، پس برای هر $p \in C$ می‌توان $f_P \in \bar{K}(C)$ 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[47] دو مقسم را بدین صورت تعریف می‌کنیم:

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

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

از آن‌جا که بعد فضای برداری فرم‌های دیفرانسیلی روی $\bar{K}(C)$، ۱ است، پس هر دو مقسم که از فرم‌های دیفرانسیلی بدست آمده‌اند با یکدیگر هم‌ارز خطی هستند.

تعریف. *منظور از مقسم کانونی*[48] ، $div\, \omega$ *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:

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

[44] Bezout
[45] Effective
[46] Uniformizer
[47] linear equivalence
[48] Canonical divisor

زیرا $L(div\,\omega' + div\,f) \cong L(div\,\omega')$

حال می‌توان قضیه ریمان‌ـ رخ را بیان کرد:

قضیه. *(ریمان‌ـ 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 گونا وجود دارد بطوری که:*

$$l(D) - l(W - D) = \deg D + ۱ - g$$

برهان. رجوع شود به بخش ۶.۸ از [Ful69].

در واقع این قضیه تقریبی برای محاسبه $l(D)$ بدست می‌دهد زیرا می‌گوید $l(D) \approx \deg D + ۱ - g$ با جمله خطای $l(W - D)$.

نتیجه. *اگر W خم جبری هموار C و g گونای آن باشد، آنگاه $\deg W = ۲g - ۲$.*

برهان. ابتدا در قضیه ریمان‌ـ رخ قرار دهید $D = ۰$، در این صورت:

$$\begin{aligned} l(۰) - l(W - ۰) &= \deg ۰ + ۱ - g \Rightarrow \\ ۱ - l(W) &= ۱ - g \Rightarrow \\ l(W) &= g \end{aligned}$$

حال در قضیه ریمان‌ـ رخ قرار دهید $D = W$ بنابراین:

$$\begin{aligned} l(W) - l(۰) &= \deg W + ۱ - g \Rightarrow \\ g - ۱ &= \deg W + ۱ - g \Rightarrow \\ \deg W &= ۲g - ۲ \end{aligned}$$

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

مثال. می‌خواهیم ثابت کنیم گونای $\mathbb{P}^۱_K$ برابر ۰ است. در واقع اگر $\mathbb{P}^۱_K$ را با $\{[t : ۱] \mid t \in K\} \cup \{\infty\}$ مختصه‌بندی کنیم و فرم دیفرانسیلی dt را در نظر بگیریم داریم:

$$div\,dt = -۲(\infty)$$

و پس

$$۲g - ۲ = \deg(div\,dt) = -۲ \Rightarrow g = ۰$$

همچنین قضیه‌ای برای محاسبه گونای خم‌های جبری صفحه‌ای (قابل نشاندن در $\mathbb{P}^۲_K$) وجود دارد که در زیر بیان می‌کنیم:

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

$$g = \frac{(n-۱)(n-۲)}{۲} - \sum_{P_i} \frac{r_{P_i}(r_{P_i} - ۱)}{۲}$$

برهان. رجوع شود به بخش ۳.۸، نتیجه‌ی ۱ از [Ful69].

۲.۳ خم های با گونای ۰

در بخش پیش ثابت کردیم که $\mathbb{P}^1_K$ گونای 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 گونای C ۰ باشد آن‌گاه C با $\mathbb{P}^1_{\bar{K}}$ ایزومورف است.*

برهان. فرض کنید $p \in C$ و در قضیه ریمان‌ـرخ 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 Kـگویا روی آن، همین اثبات کار می‌کند و نتیجه می‌گیریم $C \cong \mathbb{P}^1_K$.

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

۳.۳ خم های با گونای ۱

حال به قسمتی اصلی از خم‌های بررسی شده در این بخش می‌پردازیم. به یک خم جبری هموار با گونای ۱ و نقاط Kـگویا، خم بیضوی[49] گویند. پس تلاش براین است که 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[50] زیر بیان کرد:*

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

برهان. فرض کنید نقطه‌ی Kـگویای ∞ در E باشد. برای آن با قضیه ریمان‌ـرخ 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

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

[49] Elliptic curve
[50] Weierstrass

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

$$c_۱ + c_۲x + c_۳y + c_۴x^۲ + c_۵xy + c_۶y^۲ + c_۷x^۳ = ۰$$

همچنین به دلیل خواص x, y ، باید داشته باشیم که $c_۶c_۷ \neq ۰$. (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 $\phi : C \to \mathbb{P}^۲_K$ به شکل زیر می‌گیریم :

$$\phi : \begin{cases} p \mapsto [x(p) : y(p) : ۱] & p \neq \infty, \\ \infty \mapsto [۰ : ۱ : ۰] \end{cases}$$

حال تابع $[x : ۱]$، درجه‌ی ۲ دارد (زیرا x یک قطب مرتبه‌ی ۲ در ∞ دارد) و همچنین تابع $[y : ۱]$ درجه‌ی ۳ دارد و پس داریم:

$$[K(E) : K(x, y)] \mid [K(E) : K(x)] = ۲$$
$$[K(E) : K(x, y)] \mid [K(E) : K(y)] = ۳$$

پس $K(E) = K(x, y)$ و پس ϕ از درجه ۱ است و پس ایزومورفیسم است. همچنین برای میدان‌های با $char\, K \neq ۲, ۳$ 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:

$$y^۲ = x^۳ + Ax + B \quad (A, B \in K)$$

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

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

$$E : y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶$$

در این صورت گونای E برابر ۱ است.

برهان. فرم دیفرانسیلی $\frac{dx}{۲y+a_۱x+a_۳} = \frac{dy}{۳x^۲+۲a_۲x+a_۴-a_۱y}$ را در نظر بگیرید. به سادگی می‌توان چک کرد که این فرم هلومورف است و جایی صفر نمی‌شود. حال طبق قضیه ریمان‌ـرخ درجه‌ی مقسم آن برابر با $۲g - ۲$ است و پس داریم:

$$۲g - ۲ = \deg(div\, w) = \deg(۰) = ۰$$

پس $g = ۱$.

۴.۳ خم‌های با گونای بزرگتر از ۱

برای خم‌های با گونای بزرگتر از ۱ نیز می‌توان مدل‌هایی مانند مدل‌های بخش قبل پیدا کرد. مثلاً خم‌های هموار با گونای ۲ به همراه نقطه‌ی Kـ گویا روی میدان با مشخصه صفر K را می‌توان به شکل خم ابربیضوی[۵۱] زیر نوشت:

$$y^۲ = x^۵ + a_۴x^۴ + a_۳x^۳ + a_۲x^۲ + a_۱x + a_۰$$

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

موردل[۵۲] در سال ۱۹۲۲ حدسی را بیان می‌کند بدین مضمون که هر خم با گونای بزرگتر یا مساوی ۲ حداکثر متناهی نقطه تعریف شده روی اعداد

[51] Hyperelliptic curve
[52] Mordell

گویا می‌تواند داشته باشد. این حدس ۶۰ سال بعد توسط فالتینگز[۵۳] به اثبات رسید.

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

این قضیه اثبات‌های متعددی دارد. خود فالتینگز از یک کاستن به حدس تیت[۵۴] و ابزارها و ایده‌های هندسه جبری و مدل‌های نرون[۵۵] استفاده کرد. پس از او ویتا[۵۶] با استفاده از تقریب دیوفانتی و به شکلی کاملاً متفاوت آن را ثابت کرد. همچنین یک اثبات مقدماتی‌تر توسط بمبیری[۵۷] بدست آمد.

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

مثال. *فرض کنید $n \geq ۴$ 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 $\mathbb{P}^۲_{\mathbb{Q}}$ در نظر بگیرید. در این صورت از قضیه‌ی آخر بخش ۱.۳ داریم که گونای آن برابر با $\frac{(n-۱)(n-۲)}{۲} \geq ۲$ است. پس از قضیه فالتینگز حکم نتیجه می‌شود.*

[53] Faltings
[54] Tate
[55] Neron models
[56] Vojta
[57] Bombieri

۴ خم‌های بیضوی

همان طور که گفته شد، خم بیضوی روی میدان K یک خم جبری هموار روی K با نقطه‌ای Kـ 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 موردل‌ـ وی[۵۸] روی میدان‌های عددی را با استفاده از کوهمولوژی گالوا[۵۹] ثابت می‌کنیم و در بررسی آن گروه‌های سلمر[۶۰] و شفرویچ‌ـ تیت[۶۱] را معرفی می‌کنیم. سپس در مورد نقاط صحیح روی خم‌های بیضوی صحبت می‌کنیم و نحوه‌ی بدست آوردن آن‌ها را با گفتن قضایای ناگل‌ـ لوتز[۶۲] 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 Lـ توابع آن‌ها را در بخش‌های بعدی بررسی می‌کنیم.

۱.۴ تعاریف مقدماتی

در بخش ۳.۳ ثابت کردیم که هر خم بیضوی E روی میدان K را می‌توان به شکل زیر نمایش داد:

$$E : y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶$$

با $a_۱, a_۲, a_۳, a_۴, a_۶ \in K$ که البته در حالت $char\ K \neq ۲, ۳$ با یک تغییر مختصات ساده می‌توان آن‌را به شکل ساده‌تر زیر درآورد:

$$E : y^۲ = x^۳ + Ax + B \quad (A, B \in K)$$

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[۶۳] خم E با مختصات بالا را به شکل زیر تعریف می‌کنیم. قرار دهید:*

$$b_۲ = a_۱^۲ + ۴a_۴, \quad b_۴ = ۲a_۴ + a_۱a_۳, \quad b_۶ = a_۳^۲ + ۴a_۶$$

در این صورت تفکیک‌کننده برابر است با

$$\Delta_E = -b_۲^۲b_۸ - ۸b_۴^۳ - ۲۷b_۶^۲ + ۹b_۲b_۴b_۶$$

در حالت $char\ K \neq ۲, ۳$ این عبارت به حالت ساده‌تر $\Delta_E = -۱۶(۴A^۳ + ۲۷B^۲)$ در می‌آید. می‌توان به سادگی بررسی کرد که $\Delta_E = ۰$ اگر و تنها اگر E ناهموار باشد.

همچنین "ناوردایی" وجود دارد به نام jـ ناوردا[۶۴] که خم بیضوی را در حد ایزومورفیسم روی $\bar{K}$ مشخص می‌کند و به صورت زیر تعریف می‌شود:

تعریف. *با نمادگذاری‌های تعریف بالا، jـ ناوردا را برابر مقدار زیر تعریف می‌کنیم:*

$$j_E = \frac{(b_۲^۲ - ۲۴b_۴)^۳}{\Delta_E}$$

[58] Mordell-Weil theorem
[59] Group cohomology
[60] Selmer
[61] Shafarevich-Tate
[62] Nagell-Lutz
[63] Discriminant
[64] j-invariant

که در حالت $char\ K \neq ۲, ۳$ داریم:

$$j_E = -۱۷۲۸\frac{(۴A)^۳}{\Delta_E}$$

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

قضیه. ۱) *دو خم بیضوی ایزومورف هستند (با ایزومورفیسم تعریف شده روی $\bar{K}$)، اگر و تنها اگر jـ ناوردای آنها با هم یکسان باشند.*

۲) *فرض کنید $j_۰ \in \bar{K}$، در این صورت خم بیضوی E تعریف شده روی $K(j_۰)$ وجود دارد بطوری که $j_E = j_۰$*

برهان. ۱) فرض می‌کنیم $char\ K \neq ۲, ۳$ (در حالت‌های کنار گذاشته شده نیز می‌توان به سادگی این کارها را انجام داد)، در این صورت فرض کنید برای $E : y^۲ = x^۳ + Ax + B$ و $E' : y^۲ = x^۳ + A'x + B'$ داشته باشیم $j_E = j_{E'}$. در این صورت:

$$j_E = j_{E'} \Leftrightarrow -۱۷۲۸\frac{(۴A)^۳}{\Delta_E} = -۱۷۲۸\frac{(۴A')^۳}{\Delta'_E} \Leftrightarrow \frac{A^۳}{۴A^۳ + ۲۷B^۲} = \frac{A'^۳}{۴A'^۳ + ۲۷B'^۲} \Leftrightarrow$$
$$A^۳B'^۲ = A'^۳B^۲ \Leftrightarrow (\frac{A}{A'})^۳ = (\frac{B}{B'})^۲$$

(حالت‌های $A' = ۰$ یا $B' = ۰$ را نیز می‌توان به همین شکل بررسی کرد)

حال $\lambda \in \bar{K}$ را طوری انتخاب کنید که $\lambda^۶ = \frac{B}{B'}$ (از آن‌جایی که $\bar{K}$ بسته جبری است چنین λ یافت می‌شود). در این صورت روی E، تغییر مختصات زیر را انجام بدهید:

$$x \mapsto \lambda^۲xy \mapsto \lambda^۳y$$

در این صورت داریم:

$$E \cong \hat{E} : \lambda^۶y^۲ = \lambda^۶x^۳ + A\lambda^۲x + B \Leftrightarrow y^۲ = x^۳ + \frac{Ax}{\lambda^۴} + \frac{B}{\lambda^۶}$$

پس از رابطه‌ی بالا:

$$\lambda^{۱۲} = (\frac{B}{B'})^۲ = (\frac{A}{A'})^۳ \Rightarrow' \lambda^۴ = \frac{A}{A'}$$

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:

$$\hat{E} : y^۲ = x^۳ + \frac{Ax}{\lambda^۴} + \frac{B}{\lambda^۶} \Leftrightarrow y^۲ = x^۳ + A'x + B' : E'$$

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:

$$x \mapsto u^۲x + r, \quad y \mapsto u^۳y + u^۲sx + t$$

با $u, r, s, t \in \bar{K}$ و $u \neq ۰$، پس از اعمال تغییر مختصات و چک کردن jـ ناوردای بدست آمده می‌توان بررسی کرد که آنها با یکدیگر برابرند.

۲) فرض کنید $j_۰ \neq ۰, ۱۷۲۸$، برای این قسمت کافی است خمی را پیدا کنیم که خواص بالا را داشته باشد. قرار دهید: $E : y^۲ + xy = x^۳ - \frac{۳۶}{j_۰ - ۱۷۲۸}x - \frac{۱}{j_۰ - ۱۷۲۸}$ در این صورت $j_E = j_۰$ و این خم هموار است چون

$$\Delta_E = \frac{j_۰^۳}{(j_۰ - ۱۷۲۸)^۳}$$

همچنین برای حالات دیگر داریم:

$$E_۱ : y^۲ + y = x^۳, \quad j_E = ۰ E_۲ : y^۲ = x^۳ + x, \quad j_E = ۱۷۲۸$$

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:

$$\omega = \frac{dx}{۲y + a_۱x + a_۳} = \frac{dy}{۳x^۲ + ۲a_۲x + a_۴ - a_۱y}$$

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

قضیه. *برای این فرم دیفرانسیلی داریم* $div\ \omega = ۰$.

برهان. رجوع شود به حکم ۵.۱ از [Sil86].

۲.۴ عمل گروه

بچت[۶۵] با استفاده از روش وتر ـ مماس[۶۶]، 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 می‌کند. 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.

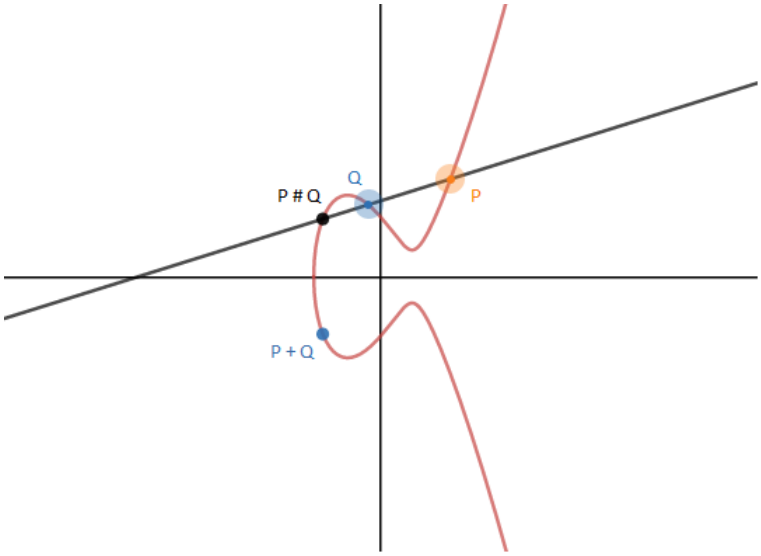
در این بخش فرمول‌بندی بهتری برای این روش روی خم بیان می‌کنیم و یک عمل گروه روی خم بیضوی با استفاده از این روش می‌سازیم.

برای این کار یک خم بیضوی E با نقطه‌ی گویای $O = [۰ : ۱ : ۰]$ در نظر بگیرید. 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 مشاهده کرد که یک خم بیضوی همواره دقیقاً یک نقطه در بی‌نهایت دارد که دارای مختصه‌های همگن $O = [۰ : ۱ : ۰] \in E(K)$ داده می‌شود. این نقطه را همواره به عنوان نقطه گویای خم در نظر می‌گیریم و پس در عمل گروه پس از به دست آوردن $P \nparallel Q$ باید آن را نسبت به محور x تقارن بدهیم تا $P + Q$ را بدست آوریم (در حالت کلی باید $P \nparallel Q$ 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 [Sil92]). 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 مقسم‌ها[۶۷] انجام می‌شود. ابتدا گروه $Pic^{\circ}(C)$ را برای یک خم جبری C تعریف می‌کنیم:

[65] Bachet
[66] Chord-tangent
[67] Divisors



شکل ۱: عمل گروه روی خم بیضوی

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

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

و گروه $Piv^{\circ}(C)$ را برابر با زیرگروه مقسم‌های درجه ۰ از $Pic(C)$ است:

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

حال قضیه‌ای بیان می‌کنیم که نشان می‌دهد گروه $Pic^{\circ}(E)$ برای هر خم بیضوی E، 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:*

$$\sigma : E \to Pic^{\circ}(E)$$
$$P \mapsto (P) - (O)$$

برهان. رجوع شود به لم ۳.۳ و حکم ۴.۳ از [Sil86]

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

در اینجا سوالی که پیش می‌آید این است 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 گونای 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 ریمان‌ـرخ:

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

۳.۴ نقاط تابی

از آن‌جا که عمل گروه خم بیضوی روی میدان K، یک گروه آبلی بدست می‌دهد، پس بررسی نقاط تابی[۶۸] 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 nـ 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

$$\exp : T_eG \to G$$

[68] Torsion points

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

به طور موضعی یک دیفیومورفیسم می‌دهد و تصویر آن باز و بسته است (چون exp در این‌جا هومومورفیسم 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:*

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

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 می‌کنیم. 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 ـ لوتز*) *خم بیضوی* $E : y^2 = x^3 + Ax + B$ *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[69] است که همه حالات نقاط تابی روی اعداد گویا را می‌دهد:

[69] Mazur

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[70] 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 $d = [K : \mathbb{Q}]$ داریم:*

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

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

می‌توانید از اثبات این قضیه عبور کنید، زیرا آسیبی به بقیه مطالب نمی‌رساند و من کوهمولوژی گروه‌ها را در اینجا فرض کرده‌ام.

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

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

در این صورت $G_K = \mathrm{Gal}(\bar{K}/K)$ 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:

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

حال قضیه زیر را داریم.

[70] Merel

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 می‌شود که $E(K)[m] \to E(\mathbb{F}_{N\mathfrak{p}})$ یک‌به‌یک است. پس اگر یک هم‌دور[71] 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:

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

و پس اگر 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، $\mathrm{Gal}(L/K)$ باید آبلی باشد. حال طبق قضیه‌ی هرمیت‌ـ مینکوفسکی می‌دانیم که متناهی توسیع Sـ غیرشاخه‌ای از درجه کراندار یک میدان عددی وجود دارد. پس برای همه‌ی هم‌دورها متناهی‌تا توسیع L/K یافت می‌شود. پس همه‌ی توابع $\mathrm{Gal}(L/K) \to E[m]$ برای همه‌ی چنین توسیع‌هایی متناهی است و پس همچنین تعداد هم‌دور ها متناهی است.

پس اثبات قضیه ضعیف موردلـ وی انجام می‌شود. حال برای این‌که قضیه موردلـ وی را اثبات کنیم، نیاز به یک تابع "ارتفاع[72]" 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 $h(mP) = m^2 h(P) + O(1)$*

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

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

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:

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

می‌توان چک کرد که تحدید این تابع به خم بیضوی در خواص بالا صدق می‌کند.

برای رهایی از $O(1)$ها نیز می‌توان ارتفاع کانونی (نرونـ 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 موردلـ وی را کامل می‌کنیم. قضیه ضعیف موردلـ 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: $Q = P_i + 2R$

حال به دلیل خاصیت مینیمال Q داریم:

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

و پس

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

[71] Cocycle
[72] Height

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).

۵.۴ 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[۷۳] داشته باشیم، که به آن یک کاستن ضربی می‌گوییم.

۲)به پیمانه آن ایدآل اول، یک نوک هلال[۷۴] داشته باشیم که به آن کاستن جمعی گوییم.

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 هومومورفیسم طبیعی*

$$E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$$

یک‌به‌یک است.

در مثال‌ها از این قضیه برای پیدا کردن نقاط تابی یک خم بیضوی روی اعداد گویا استفاده شده است.

۶.۴ خم‌های بیضوی روی میدان‌های متناهی

فرض کنید $E/\mathbb{F}_q$ یک خم بیضوی باشد. در این صورت تعداد نقاط آن روی $\mathbb{F}_{q^n}$ متناهی است و علاقه‌مندیم که تعداد این نقاط را بشماریم. در این صورت هسه[۷۵] کرانی به ما داده است.

قضیه. (هسه) *داریم:*

$$|\sharp E(\mathbb{F}_{q^n}) - (q^n + 1)| \leq 2\sqrt{q^n}$$

[73] Node
[74] Cusp
[75] Hasse

این را آرتین[۷۶] در تز دکترایش حدس زد و در آخر توسط هسه اثبات شد.

پس این قضیه می‌گوید که فاصله تعداد نقاط خم بیضوی از تعداد نقاط یک خط تصویری "کم" است. همچنین وی توانست برای خم‌های جبری دیگر نیز قضیه مشابهی را ثابت کند:

قضیه. *(وی) اگر C یک خم جبری از گونای g باشد،*

$$|\sharp C(\mathbb{F}_{q^n}) - (q^n + ۱)| \leq ۲g\sqrt{q^n}$$

در واقع این قضیه حالت خاصی از حدس‌های وی (رجوع شود به بخش ۵) برای خم‌های جبری است. حال برای فهمیدن میزان دقیق بودن این نامساوی باید ببینیم که چقدر به کران‌ها نزدیک می‌شویم. ساتو و تیت حدسی را در این مورد صورت‌بندی کردند که نحوه‌ی توزیع $\sharp C(\mathbb{F}_p)$ وقتی p تغییر می‌کند را به ما می‌دهد:

حدس. *(ساتو[۷۷]ـ تیت) اگر E یک خم بیضوی بدون ضرب مختلط (این شرط بزرگی نیست و بعداً توضیح داده می‌شود) باشد و $۰ \leq \theta_p \leq \pi$ زاویه‌ای باشد که*

$$\cos\theta_p = \frac{\sharp E(\mathbb{F}_p - (p+۱))}{۲\sqrt{p}}$$

در این صورت

$$\lim_{x\to\infty} \frac{\sharp\{p \leq x | \alpha \leq \theta_p \leq \beta\}}{\pi(x)} = \frac{۲}{\pi}\int_\alpha^\beta \sin^۲(\theta)d\theta$$

این حدس توسط ریچارد تیلور در سال ۲۰۰۸ اثبات شده است و پس این قضیه به ما می‌گوید که نامساوی دقیق است و به اندازه کافی (به معنی بالا) به کران‌ها نزدیک می‌شویم.

۷.۴ یک‌جنسی

از این به بعد یک خم بیضوی E با نقطه Kـ 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 $(E_۱, O_۱)$ و $(E_۲, O_۲)$ دو خم بیضوی باشند. اگر $\phi : E_۱ \to E_۲$ مورفیسمی جبری (به عنوان دو خم جبری) باشد که $\phi(O_۱) = O_۲$، 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 می‌کنیم. در واقع نمودار زیر را در نظر بگیرید:

$$\begin{array}{ccc} E_۱(\bar{K}) & \xrightarrow{\sim} & Pic^\circ(E_۱) \\ \downarrow f & & \downarrow g \\ E_۲(\bar{K}) & \xrightarrow{\sim} & Pic^\circ(E_۲) \end{array}$$

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

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

[76] E. Artin
[77] Sato

برای هر مقسم. می‌توان به سادگی چک کرد که g خوش‌تعریف و هوموورفیسم است و با نمودار بالا جابجا می‌شود. پس از آن‌جا که هوموورفیسم‌های افقی ایزوموورفیسم هستند، f نیز باید هوموورفیسم و پس مورفیسمی از گروه‌های جبری باشد.

تعریف. یک‌جنسی[78] $f : (E_1, O_1) \to (E_2, O_2)$ *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 Kـ گویا تشکیل می‌دهیم به همراه یک‌جنسی‌ها به عنوان مورفیسم‌ها.

پس $\mathrm{Hom}(E_1, E_2)$ را برابر با همه‌ی یک‌جنسی‌ها از (E_1, O_1) به (E_2, O_2) قرار می‌دهیم. همچنین، $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. مجموعه‌ی یک‌جنسی‌های وارون‌پذیر در $\mathrm{End}(E)$ را با $\mathrm{Aut}(E)$ نمایش می‌دهیم. همچنین $\mathrm{Hom}_L(E_1, E_2)$ و $\mathrm{End}_L(E)$ و $\mathrm{Aut}_L(E)$ 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* 0 *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.

[78] Isogeny

۸.۴ ضرب مختلط

در این بخش خم‌های بیضوی با ضرب مختلط[۷۹] را توضیح می‌دهیم و نشان می‌دهیم که خواص شگفت‌انگیزی دارند. مرجع اصلی این بخش [Sil94] و [Ser67] است.

روی یک خم بیضوی همواره درون‌ریختی‌های $[n]$ برای $n \in \mathbb{Z}$ وجود دارد. این که آیا درون‌ریختی‌های دیگری 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*[۸۰] *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*[۸۱] *در اعداد مختلط (دو بعدی روی اعداد حقیقی) باشد و قرار دهید:*

$$g_۲(\Lambda) = ۶۰ \sum_{۰ \neq \omega \in \Lambda} \frac{۱}{\omega^۴}, \quad g_۳(\Lambda) = ۱۴۰ \sum_{۰ \neq \omega \in \Lambda} \frac{۱}{\omega^۶}$$

و همچنین قرار دهید

$$\wp_\Lambda(z) = \frac{۱}{z^۲} + \sum_{۰ \neq \omega \in \Lambda} \left(\frac{۱}{(z-\omega)^۲} - \frac{۱}{\omega^۲} \right)$$

در این صورت قرار دهید:

$$E : y^۲ = ۴x^۳ - g_۲(\Lambda)x - g_۳(\Lambda)$$

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

$$\wp : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad z \mapsto [\wp(z) : \wp'(z) : ۱]$$

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 $\mathrm{End}(E)$ 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

[79] Complex multiplication
[80] Order
[81] Lattice

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 ــ این توابع همان $[n]$ها هستند که در حالت جبری بررسی کردیم ــ 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:

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

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 $\mathrm{End}(E) \otimes \mathbb{Q}$ 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 $Cl(R)$ (گروه کلاسی حلقه R) دارد.*

ایده‌ی برهان. یک عمل متعدی ساده از $\mathrm{Cl}(R)$ 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 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[82] 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 jــ 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:*

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

[82] Hilbert class field

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

برای برهان این قضایا به [Ser67] 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.*

۹.۴ مثال‌ها

۱ــ **استفاده از میدان‌های متناهی برای نقاط تابی.** خم بیضوی $E : y^2 = x^3 + 3$ روی اعداد گویا در نظر بگیرید. تفکیک‌کننده‌ی این خم برابر $-2^4 3^5$ است و پس هومومورفیسم‌های یک به یک

$$E(\mathbb{Q})_{tors} \to E(\mathbb{F}_5), \quad E(\mathbb{Q})_{tors} \to E(\mathbb{F}_7)$$

وجود دارند، اما تعداد اعضای $E(\mathbb{F}_5)$ و $E(\mathbb{F}_7)$ به ترتیب برابر ۶ و ۱۳ است. پس از آنجا که این دو عدد نسبت به هم اول هستند، $E(\mathbb{Q})_{tors}$ گروه تک‌عضوی است و پس نقطه تابی روی اعداد گویا ندارد.

۲ــ **استفاده از قضیه هسه.** در این مثال، فرض کنید $p \neq 3$ یک عدد اول باشد و $a \in \mathbb{Z}$، در این صورت معادله‌ی

$$x^3 + y^3 + z^3 = a$$

روی $\mathbb{F}_p$ جواب دارد. در واقع، ابتدا اگر $a = 1 \pmod{p}$ آنگاه $(1, 0, 0)$ یک جواب معادله بالاست. پس فرض کنید

$$a \neq 1 \pmod{p}$$

و خم تصویری زیر را در نظر بگیرید:

$$f(x, y, z) = x^3 + y^3 + (1 - a)z^3 = 0$$

در این صورت این یک خم بیضوی روی $\mathbb{F}_p$ است زیرا اولاً نقطه‌ی تکین ندارد زیرا اگر $(x : y : z)$ یک نقطه‌ی تکین (مثلاً با $z \neq 1$ باشد) در این صورت باید

$$f(x, y, z) = 0, \frac{\partial f}{\partial x} = 3x^2 = 0, \quad \frac{\partial f}{\partial y} = 3y^2 = 0$$

که نتیجه می‌دهد $x, y = 0$ و پس $z = 0$ که تناقض است. در چارت‌های $x = 1$ و $y = 1$ نیز به همین شکل می‌توان اثبات کرد که نقطه‌ی تکین وجود ندارد. پس گونای آن طبق فرمول گونا برابر $1 = \frac{(3-1)(3-2)}{2}$ است. حال طبق قضیه هسه این خم بیضوی روی $\mathbb{F}_p$ حداقل $(\sqrt{p} - 1)^2$ نقطه دارد. حال میخواهیم ثابت کنیم جوابی با $z \neq 0$ وجود دارد. در واقع یک جواب با $z = 0$، نقطه‌ی $(0 : 0 : 1)$ داریم و بقیه‌ی جوابها، جوابهای تصویری $-1 = (\frac{x}{y})^3$ است که برابر ۰ یا ۳ است. پس اگر $p \geq 11$ داریم:

$$4 < (\sqrt{p} - 1)^2$$

و پس حداقل یک جواب با $z \neq 0$ داریم که در نهایت به ما یک جواب به شکل زیر میدهد:

$$f(x, y, z) = x^3 + y^3 + (1 - a)z^3 = 0 \Rightarrow (\frac{x}{z})^3 + (\frac{y}{z})^3 + (1 - a) = 0$$

و پس $(\frac{x}{z}, \frac{y}{z}, 1)$ یک جواب معادله اصلی است. برای $p \leq 7$ نیز به سادگی می‌توان به سادگی چک کرد که برای همه‌ی aها جواب وجود دارد.

۵ قضیه‌ها و حدس‌های مهم

در این بخش تلاش می‌کنیم تا قضیه‌ها و حدس‌های مهم در نظریه جبری اعداد را توضیح دهیم. در ابتدا با واریته‌ها روی میدان‌های متناهی شروع کرده و حدس‌های وی در مورد تابع زتای آنها را بیان می‌کنیم، سپس سوال دوازدهم هیلبرت را برای میدان اعداد گویا و سپس با استفاده از مباحث توضیح داده شده در مورد ضرب مختلط، برای میدان‌های مربعی مختلط توضیح می‌دهیم. در آخر هم روند اثبات قضیه آخر فرما (البته به شکل کاملاً نادقیق) توضیح داده می‌شود.

۱.۵ حدس‌های وی

فرض کنید $V/\mathbb{F}_q$ یک واریته تصویری هموار از بعد d باشد. در این صورت یک تابع به اسم تابع زتای واریته V به شکل زیر تعریف می‌شود:

$$\zeta(V,s) = \exp(\sum_{n\geq 1} \frac{\sharp V(\mathbb{F}_{q^n})}{n} q^{-ns})$$

حال حدس‌های وی متشکل از چهار حدس هستند که می‌گویند:

۱ـ (حدس گویایی) تابع زتا را برای چندجمله‌ای‌هایی مثل $p_0(t), p_1(t), ..., p_{2d}(t) \in \mathbb{Z}[t]$ می‌توان به فرم زیر نوشت:

$$\zeta(V,s) = \frac{p_1(q^{-s})p_3(q^{-s})...p_{2d-1}(q^{-s})}{p_0(q^{-s})p_2(q^{-s})...p_{2d}(q^{-s})}$$

همچنین $p_0(t) = 1 - t$ و $p_{2d}(t) = 1 - q^d t$.

۲ـ (معادله‌ی تابعی و دوگانگی پوانکاره[۸۳]) تابع زتا در معادله‌ی زیر صدق می‌کند:

$$\zeta(V, n-s) = \pm q^{\frac{n\chi}{2} - \chi s} \zeta(V,s)$$

که χ یک عدد صحیح به نام مشخصه اویلر واریته V است.

۳ـ (فرض ریمان) اگر بنویسیم $p_i(t) = \Pi_j(1 - \alpha_{ij}t)$ برای $\alpha_{ij} \in \mathbb{C}$، آنگاه $|\alpha_{ij}| = q^{\frac{i}{2}}$.

۴ـ (عدد بتی[۸۴]) اگر W یک واریته هموار تصویری روی یک میدان عددی باشد به طوری که کاهش خوب آن به پیمانه ایدآل اولی برابر V شود، درجه p_i با عدد بتی iام $Y(\mathbb{C})$ یکی می‌شود.

این حدس‌ها اطلاعات زیادی در مورد تعداد نقاط یک واریته روی میدان‌های متناهی می‌دهد، مثلاً قضیه هسه از این نتیجه می‌شود (چرا؟) یا این که مقادیر $\sharp V(\mathbb{F}_{q^n})$ برای nهای مختلف از مقادیر اولیه n بدست می‌آید. البته ارزش بیشتر این حدس‌ها در روند توسعه‌ی یک نظریه کوهمولوژی (به نام کوهمولوژی اتال[۸۵]) برای واریته‌هاست.

این حدس‌ها همگی ثابت شده‌اند. در ابتدا دوورک[۸۶] حدس اول را با استفاده از آنالیز پی‌ـادیک حل کرد، سپس گروتندیک[۸۷] با پیشرفت دادن کوهومولوژی اتال، این حدس‌ها را بجز فرض ریمان اثبات کرد. مثلاً گویایی معادل فرمول لفشتز[۸۸] برای این نظریه کوهمولوژی است. در آخر دلین[۸۹] با بهره‌گیری از ایده‌های گروتندیک و قضیه ابرصفحه‌ی لفشتز[۹۰] این حدس را نیز اثبات کرد.

[83] Poincare duality
[84] Betti number
[85] Etale cohomology
[86] Dwork
[87] Grothendieck
[88] Lefschetz
[89] Deligne
[90] Lefschetz hyperplane theorem

۲.۵ مسأله‌ی دوازدهم هیلبرت

تاریخچه این مسئله به قوانین تقابل[۹۱] ، مانند تقابل مربعی گاوس[۹۲]، باز میگردد در زیر ابتدا کمی در مورد قوانین تقابل صحبت می‌کنیم و انگیزه‌ی سوال دوازدهم هیلبرت را بیان می‌کنیم.

در ابتدا نماد لژاندر[۹۳] را تعریف می‌کنیم:

تعریف. *اگر p,q دو عدد اول فرد باشند، در این صورت نماد لژاندر را به صورت زیر تعریف می‌کنیم:*

$$\left(\frac{p}{q}\right) = \left\{ \begin{array}{ll} ۱, & \exists x; x^۲ = p \pmod q \\ -۱, & \nexists x; x^۲ = p \pmod q \\ ۰, & p = q \end{array} \right\}$$

حال گاوس اولین کسی بود که توانست قانون تقابل زیر را اثبات کند:

قضیه. *(گاوس) برای p,q اعداد اول فرد متفاوت داریم:* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-۱)^{\frac{(p-۱)(q-۱)}{۴}}$.

حال اگر در این قضیه ما p را با عدد اول دیگری مثل p' عوض کنیم که $p = p' \pmod{۴q}$ ، در این صورت از قانون تقابل نتیجه می‌شود که

$$\left(\frac{q}{p}\right) = \left(\frac{q}{p'}\right)$$

و پس تابع $\left(\frac{q}{\cdot}\right)$ تناوب $۴q$ دارد. حال این را می‌توان جور دیگری تفسیر کرد طبق قضیه زیر از کومر:

قضیه. *(کومر) فرض کنید $\mathbb{Q}(\alpha)$ یک میدان عددی باشد به طوری که $\mathbb{Z}[\alpha]$ حلقه‌ی اعداد صحیح آن باشد و فرض کنید f چندجمله‌ای مینیمال α باشد. در این صورت اگر p یک عدد اول باشد، و $f = \prod_i f_i^{\alpha_i}$ تجزیه‌ی f به پیمانه‌ی p باشد، در این صورت تجزیه p به شکل زیر خواهد بود:*

$$(p) = \prod_i \mathfrak{p}_i^{\alpha_i}$$

که $\mathfrak{p}_i$ ایدآل‌های اول $\mathbb{Z}[\alpha]$ هستند و درجه مانده $\mathfrak{p}_i$ برابر درجه f_i است.

حال می‌خواهیم با استفاده از این قضیه قانون تقابل مربعی را به شکل دیگری بیان کنیم. میدانیم که $\left(\frac{p}{q}\right) = ۱$ اگر و تنها اگر معادله‌ی $x^۲ - p = ۰$ به پیمانه q جواب داشته باشد اگر و تنها اگر (طبق قضیه کومر) ایدآل (q) در حلقه‌ی اعداد صحیح $\mathbb{Q}(\sqrt{p})$ به دو ایدآل اول تجزیه شود. پس می‌توان قانون تقابل مربعی را به شکل زیر بیان کرد:

قضیه. *اگر عددهای اول غیرشاخه‌ای در $\mathbb{Q}(\sqrt{p})$ (آنهایی که تجزیه‌شان به ایدآل‌های اول فقط توان ۱ دارد، این‌ها همه‌ی اعداد اول بجز احتمالاً $۲, p$ هستند) را تجزیه کنیم، نوع تجزیه (این که اول می‌مانند یا تجزیه به ضرب دو ایدآل اول می‌شوند) آنها متناوب به پیمانه $۴p$ است.*

حال ما علاقه‌مندیم بدانیم این تجزیه متناوب بجز در میدان‌های مربعی حقیقی دیگر در کجاها اتفاق میفتد و در اینجا قضیه‌ای داریم که کاملاً آنها را مشخص می‌کند:

قضیه. *اگر $K/\mathbb{Q}$ یک توسیع گالوا باشد، در این صورت تجزیه متناوب اعداد اول را داریم اگر و تنها اگر $Gal(K/\mathbb{Q})$ آبلی باشد.*

[91] Reciprocity laws
[92] Gauss's quadratic reciprocity law
[93] Legendre symbol

تذکر. *به توسیع‌های گالوا با گروه گالوای آبلی، توسیع‌های آبلی گوییم.*

پس برای این که این انواع تجزیه و قوانین تقابل را بدست آوریم، باید توسیع‌های آبلی $\mathbb{Q}$ را بدست آوریم. از طرفی واضح است که اگر ما ζ_n (ریشه‌ی nام واحد) را به $\mathbb{Q}$ اضافه کنیم، یک توسیع آبلی دریافت می‌کنیم با گروه گالوای $(\mathbb{Z}/n\mathbb{Z})^*$ و اعضای به فرم $\zeta_n \mapsto \zeta_n^i$ که i نسبت به n اول است.

حال قضیه کرونکر_وبر[۹۴] عکس این را برای ما اثبات می‌کند:

قضیه. *(کرونکر_ وبر) هر توسیع آبلی $K/\mathbb{Q}$ درون یکی از $\mathbb{Q}(\zeta_n)$ها است.*

پس قوانین تقابل به فرم تناوبی برای توسیع‌های به فرم بالا وجود دارد.

حال می‌توان همین سوال را برای میدان‌های عددی پایه‌ای دیگر کرد. بدین معنی که $\mathbb{Q}$ را در بالا با یک میدان عددی K عوض می‌کنیم و تلاش می‌کنیم توسیع‌های آبلی آن را شناسایی کنیم (زیرا در این حالت هم می‌توان ایدآل‌های اول را تجزیه کرد و به معنی‌ای تناوب معادل آبلی بودن می‌شود). این سوال، سوال دوازدهم هیلبرت نام دارد و هیلبرت حدس می‌زند که یک تابع تحلیلی $f : \mathbb{C} \to \mathbb{C}$ وجود دارد که مقادیر خاصی از این تابع توسیع‌های آبلی را تولید می‌کنند. مثلاً، در بالا برای توسیع‌های آبلی $\mathbb{Q}$ مقادیر خاص تابع $\exp$ در $\frac{2\pi i}{n}$ها توسیع‌های آبلی را تولید می‌کنند. همچنین همانطور که در بخش ضرب مختلط گفتیم، در نظر گرفتن مختصه‌های نقاط تابی خم‌های بیضوی، توسیع‌های آبلی میدان‌های مربعی مختلط را می‌سازد. در مورد بقیه میدان‌ها اطلاعات بسیار کمی بدست آمده است. شیمورا برای ساختن توسیع‌های آبلی میدان‌های "ضرب مختلط" (مثلاً میدان‌های دایره‌بر [۹۵])، از نقاط تابی واریته‌های آبلی[۹۶] استفاده می‌کند. همچنین دارمون[۹۷] از معادل نقاط هیگنر[۹۸] روی نیم‌صفحه‌ی بالای درینفلد[۹۹] برای ساختن توسیع‌های آبلی میدان‌های مربعی حقیقی استفاده می‌کند.

همچنین برای بررسی این مطالب و زودتر از نتایج بالا نظریه میدان‌های رده‌ای به وجود آمده و این نظریه قضیه‌های کلی‌ای در مورد این توسیع‌ها اثبات می‌کند. برای اطلاعات بیشتر می‌توانید به کتاب [CaF65] مراجعه کنید.

۳.۵ قضیه آخر فرما

این قسمت، چند زیربخش دارد که برای روند اثبات قضیه آخر فرما نیاز است بیان شود، با فرمهای مدولار شروع می‌کنیم و سپس در مورد نمایش‌های گالوا و دگردیسی‌های آن صحبت می‌کنیم، و در انتها ایده‌ی اثبات را با استفاده از این‌ها می‌دهیم.

۱.۳.۵ فرم‌های مدولار

منظور از یک فرم مدولار روی $\mathrm{SL}_2(\mathbb{Z})$ با وزن k، یک تابع $f : \mathbb{H} \to \mathbb{C}$ است ($\mathbb{H}$ نیم‌صفحه‌ی بالای $\mathbb{C}$ است)، به‌طوری که

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z), z \in \mathbb{H}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \qquad (۳)$$

[94] Kronecker-Weber
[95] Cyclotomic fields
[96] Abelian varieties
[97] Darmon
[98] Heegner points
[99] Drinfeld upper half plane

و روی همه‌ی نقاط $\mathbb{H}$ و همچنین در "∞" تحلیلی باشد. شرط آخر به این معنی است که بسط فوریه[100] f (چون داریم $f(z) = f(z+1)$ از رابطه بالا) در بی‌نهایت از صفر شروع شود:

$$f(q) = \sum_{n \geq 0} a_n q^n, \quad q = e^{2\pi i z},\ a_n \in \mathbb{C}$$

همه‌ی فرم‌های مدولار از وزن k روی $\mathrm{SL}_2(\mathbb{Z})$ را با $M_k(\mathrm{SL}_2(\mathbb{Z}))$ نمایش می‌دهیم. همچنین واضح است که این تعریف را می‌توان زیرگروه‌هایی از $\mathrm{SL}_2(\mathbb{Z})$ مثل Γ تعمیم داد به این شکل که در شرط (۳) به جای $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ داشته باشیم $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. فرض می‌کنیم Γ خیلی کوچک نباشد یعنی $\Gamma \supseteq \Gamma(N)$ برای Nی که

$$\Gamma(N) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N\}$$

هم‌چنین قرار می‌دهیم:

$$\Gamma_0(N) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N\}$$

در این صورت $\Gamma(N)$ از اندیس متناهی در $\mathrm{SL}_2(\mathbb{Z})$ است (چرا؟) و پس Γ و $\Gamma_0(N)$ نیز از اندیس متناهی هستند. به چنین زیرگروه‌هایی از $\mathrm{SL}_2(\mathbb{Z})$ زیرگروه‌های هم‌نهشتی[101] گوییم. پس مانند قبل، فرم‌های مدولار در این فضا را با $M_k(\Gamma)$ نمایش می‌دهیم. فرم‌های مدولار این خاصیت مهم را دارند که هر کدام از $M_k(\Gamma)$ها متناهی‌بعد هستند (پس مثلاً اگر یک فرم مدولار داشته باشیم، می‌توانیم آن را برحسب پایه‌ای در این فضا بنویسیم و ضرایب فوریه آن فرم مدولار را بهتر بشناسیم).

منظور از یک فرم کاسپ[102] از وزن k روی Γ، یک فرم مدولار با وزن k روی Γ است به‌طوری که در همه‌ی "کاسپ"های Γ صفر شود: اگر Γ یک زیرگروه هم‌نهشتی باشد، می‌توان فضای $\mathbb{H}/\Gamma$ را در نظر گرفت. در این صورت این یک رویه ریمانی باز است بطوری که فشرده‌سازی[103] آن به متناهی نقطه نیاز دارد. به این متناهی نقطه، کاسپ‌های Γ گوییم. فضای همه‌ی فرم‌های کاسپ از وزن k روی Γ را با $S_k(\Gamma)$ نمایش می‌دهیم. همچنین منظور از یک فرم مدولار (فرم کاسپ) از وزن k و مرحله‌ی n، یک فرم مدولار (فرم کاسپ) در $M_k(\Gamma_0(N))$ ($S_k(\Gamma_0(N))$) است.

حال عملگرهای هکه[104] را مختصراً توضیح می‌دهیم. برای سادگی فرض کنید $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. 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[105] (ضرب در یک عدد مختلط) در نظر بگیریم، تابع بالا یک دوسویی خواهد داد:

$$\mathbb{H} \to \mathcal{L}/\text{homothety}$$

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

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

[100] Fourier expansion
[101] Congruence subgroups
[102] Cusp form
[103] Compactification
[104] E. Hecke
[105] Homothety

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 $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ قرار دهید:

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

در این صورت T_nها عملگرهایی روی $M_k(\mathrm{SL}_2(\mathbb{Z}))$ و $S_k(\mathrm{SL}_2(\mathbb{Z}))$ خواهند بود. همچنین برای $\lambda \in \mathbb{C}^*$، $[\lambda]$ را برابر با $L \mapsto \lambda L$ تعریف کنید و برای $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ قرار دهید:

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

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

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

$$(f,g) := \int_{\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})} f(\tau)\bar{g}(\tau)(\mathrm{Im}\,\tau)^k d\nu(\tau),$$
$$\nu(\tau) = y^{-2}dxdy, f, g \in S_k(\mathrm{SL}_2(\mathbb{Z}))$$

خودالحاق هستند. پس می‌توان فضای فرم‌های کاسپ از وزن k روی $\mathrm{SL}_2(\mathbb{Z})$ 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[106] 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) $T_n T_m = T_{nm}$ 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) $a_1(T_n f) = a_n(f)$ که منظور از $a_n(f)$ ضریب nـام 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[107] بوده است. در واقع تابع

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

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:

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

[106] Eisenstein series
[107] S. Ramanujan

۳) $|\tau(l)| \leq 2l^{11/2}$.

حال می‌توان دید که فضای $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ یک بعدی است و $S_{12}(\mathrm{SL}_2(\mathbb{Z})) =< \Delta >$. 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. قسمت سوم حدس سخت‌تر است و از حدس‌های وی بدست می‌آید.

یک فرم کاسپ $f \in S_k(\Gamma_0(N))$ در نظر بگیرید به‌طوری که فرم ویژه‌ی همه‌ی T_nها ($n \nmid N$) باشد. در این صورت خواص ۳ و ۴ عملگرهای هکه پیشنهاد می‌کنند که ما Lـ تابع ضرایب بسط فوریه‌ی آن را در نظر بگیریم:

اگر $f = \sum_{n\geq 1} a_n q^n$ قرار دهید:

$$L(f,s) = \sum_{p\nmid N} \frac{a_n}{n^s}$$

و پس از ۳ و ۴ و بسط تیلور داریم که این تابع حاصلضرب اویلری زیر را دارد:

$$L(f,s) := \prod_{p\nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

این حاصلضرب اویلری ما را یاد Lـ تابع خم‌های بیضوی می‌اندازد. پس احتمالاً رابطه‌ای بین فرم‌های ویژه و خم‌های بیضوی وجود دارد.

حال می‌توان یک بیان ساده از قضیه مدولاریتی را گفت:

قضیه. *فرض کنید $E/\mathbb{Q}$ یک خم بیضوی باشد. برای pهای اول که E در آنها کاهش خوب دارد قرار دهید $a_p = p + 1 - \bar{E}(\mathbb{F}_p)$. در این صورت $N \in \mathbb{Z}$ و $f \in S_2(\Gamma_0(N))$ وجود دارند که f نرمال ($a_1(f) = 1$) و "جدید" و فرم ویژه‌ی همه‌ی عملگرهای هکه باشد و $a_p = a_p(f)$ برای همه بجز متناهی p.*

"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.

با فرض این قضیه خواهیم داشت:

$$L(E,s) = L(f,s)$$

(روی متناهی عدد اول کنار گذاشته شده می‌توان این توابع را جوری تعریف کرد که رابطه بالا درست باشد) و پس خواص خوب (معادله تابعی و گسترش تحلیلی و ...) که برای Lـ توابع فرم‌های کاسپ ساده است به Lـ توابع خم‌های بیضوی می‌رسد.

۲.۳.۵ نمایش‌های گالوا

در این‌جا نمایش‌های گالوا[108] روی خم‌های بیضوی و فرم‌های مدولار را توضیح می‌دهیم (مساوی بودن نمایش‌های گالوا نیز صورتی دیگر از قضیه مدولاریتی خواهد بود). منظور از یک نمایش گالوا یک هوموورفیسم $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$ است که $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ و A یک حلقه‌ی جابجایی و یکدار است. یک مثال از نمایش‌های گالوا نمایش دایره‌بر است. این نمایش یک‌بعدی به شکل زیر تعریف می‌شود: یک عدد اول l را فیکس کنید و قرار دهید

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

[108] Galois representations

به‌طوری که

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

همچنین، نمایش‌های شاخه‌ای و غیرشاخه‌ای به معنی زیر هستند:

تعریف. *به نمایش ρ در عدد اول l غیرشاخه‌ای گویند هرگاه $\rho(I_l) = \{۱\}$ که I_l یک گروه اینرسی در l است و در غیر این صورت به آن شاخه‌ای در l گویند.*

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 روی آن را در نظر گرفت:

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

در این صورت داریم:

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

حال مدول تیت 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 lـ تایی است.

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 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(E[l^n]) = \mathrm{GL}_۲(\mathbb{Z}/l^n\mathbb{Z})$ تعریف کرد که این‌ها با سیستم وارون سازگارند و پس نمایش گالوا روی مدول تیت پیدا می‌کنیم:

$$\rho_{E,l} : G_{\mathbb{Q}} \to \mathrm{GL}(T_l(E)) \cong \mathrm{GL}_۲(\mathbb{Z}_l)$$

نمایش‌های گالوا روی فرم‌های مدولار.

تعریف این کمی دشوارتر از حالت قبل است و قسمت اصلی ساخت آن را ارجاع می‌دهیم. 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 $f \in S_۲(\Gamma_۰(N))$ طوری باشد که همه‌ی ضرایب بسط فوریه‌ی آن گویا هستند. در این صورت با استفاده از آن می‌توان یک خم بیضوی E_f ساخت به‌طوری که مدولار باشد (به معنی صورت قضیه مدولاریتی بالا) و سپس قرار می‌دهیم:

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

برای دیدن نحوه ساخت آن خم بیضوی می‌توانید به بخش ۵.۲ از [Dar03] رجوع کنید.

حال صورت دومی از قضیه مدولاریتی را بیان می‌کنیم:

قضیه. *فرض کنید E یک خم بیضوی روی $\mathbb{Q}$ باشد. در این صورت $f \in S_۲(\Gamma_۰(N))$ (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.

روندی که وایلز برای اثبات قضیه آخر فرما در پیش گرفت همین صورت از قضیه مدولاریتی بود و کاری که او کرد این بود که قضیه مدولاریتی را برای همه‌ی خم‌های بیضوی نیمه‌پایدار[109] (از جمله خم فری) اثبات کرد که برای اثبات قضیه آخر فرما کافی بود.

۳.۳.۵ حدس اپسیلون (قضیه ریبت)

این حدس را اولین بار سر مطرح کرد و ریبت آن را اثبات کرد و اثبات قضیه آخر فرما را به حدس شیمورا ـ 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 $S_۲(\Gamma_۰(lN))$ یک فرم کاسپ جدید نرمال $(a_۱(f)=۱)$ و فرم‌ویژه همه‌ی عملگرهای هکه باشد به‌طوری که دارای نمایش‌های "مطلقاً تحویل‌ناپذیر"[110] $\rho_{f,q}$ باشد و این نمایش در l غیرشاخه‌ای ("متناهی" و "صاف"[111]) باشد اگر $l\neq q$ $(l=q)$. آنگاه $g\in S_۲(\Gamma_۰(N))$ نرمال و جدید وجود دارد که داریم:*

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

اثبات. رجوع شود به [Rib90].

متناهی و صاف معانی جزئی دارند که توضیح آنها از سطح این نوشته‌ها بالاتر است. مطلقاً تحویل‌ناپذیر یعنی به عنوان نمایش‌های به $\mathrm{GL}_۲(\overline{\mathbb{F}}_p)$ تحویل‌ناپذیر باشند. نحوه‌ی استفاده از این قضیه را در بخش آخر توضیح می‌دهیم.

۴.۳.۵ 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 ـ 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) و مدولاریتی آن‌ها را اثبات کنیم.

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 ـ جبرهای نوتری موضعی A (با ایدآل ماکسیمال $\mathfrak{m}_A$) به همراه نگاشتی پوشا (نگاشت تشدید[112]) $\pi : A\to O$ تعریف کنید به‌طوری که $A/\mathfrak{m}_A\cong O/\mathfrak{m}_O=\mathbb{F}_q$ و نگاشت‌های بین این اشیا را برابر O ـ جبر هومومورفیسم‌های روی O تعریف کنید (نمودار زیر جابجا شود):*

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

حال یک شیء از رسته بالا مثل A را در نظر بگیرید. می‌خواهیم دگردیسی[113] نمایش‌های گالوا را تعریف می‌کنیم:

[109] Semistable elliptic curves
[110] Absolutely irreducible
[111] flat
[112] Augmentation
[113] Deformation

تعریف. ۱) *یک نمایش گالوا* $\rho_\circ : G_{\mathbb{Q}} \to GL_m(\mathbb{F}_q)$ *در نظر بگیرید. منظور از یک بالابری*[۱۱۴] ρ *از نمایش گالوای روی میدان متناهی* $\rho_\circ$*، یک نمایش* $\rho : G_{\mathbb{Q}} \to GL_m(A)$ *است به‌طوری که* ρ *به پیمانه‌ی* $\mathfrak{m}_A$ *برابر* $\rho_\circ$ *شود.*

۲) *دو بالابری* ρ, ρ' *از* $\rho_\circ$ *را اکیداً معادل*[۱۱۵] *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* $\rho_\circ$ *یک مولفه‌ی هم‌ارزی از رابطه‌ی هم‌ارزی بالا است.*

حال شرط‌هایی که گفتیم را باید روی دگردیسی‌های نمایش‌های گالوا قرار دهیم: پس یک نمایش گالوا $\rho_\circ : G_{\mathbb{Q}} \to \mathrm{GL}_m(\mathbb{F}_q)$ فیکس کنید و S را مجموعه‌ی اعداد اولی قرار دهید که $\rho_\circ$ در آن‌ها شاخه‌ای است. این یک مجموعه‌ی متناهی است (چرا؟). 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"*[۱۱۶]*. این‌ها دو شرط موضعی هستند تعریف آن‌ها از سطح این نوشته‌ها بالاتر است.*

همچنین به دگردیسی‌ای، مجاز[۱۱۷] 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[۱۱۸] نگاه کنیم:

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

نمایش‌پذیر[۱۱۹] خواهند بود. پس دو عضو از $\mathcal{C}_O$ وجود دارند مثل R_Σ و $\mathbb{T}_\Sigma$ به‌طوری که

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

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:

$$\rho_\Sigma^{univ} : G_{\mathbb{Q}} \to \mathrm{GL}_2(R_\Sigma)$$
$$\rho_\Sigma^{univ.mod} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_\Sigma)$$

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

[114] Lift
[115] Strictly equivalent
[116] Ordinary
[117] Admissible
[118] Functor
[119] Representable

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

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 به اتمام می‌رسد. نحوه‌ی اثبات وایلز به این شکل است که او از استقرا روی تعداد اعضای Σ استفاده می‌کند و R_Σ و T_Σ را به‌طور صریح می‌سازد و انتخاب هوشمندانه‌ای برای توابع تشدید آن‌ها می‌کند و سپس با تکنیک‌های جبر این مسئله را به یک نامساوی درباره تعداد اعضای یک ناوردا در این حلقه‌ها تبدیل می‌کند و آن را اثبات می‌کند. شکافی که در اثبات ابتدایی وایلز وجود داشت باعث شد که او و تیلور یک سال دیگر روی آن زمان بگذارند تا آنرا اثبات کنند. برای خواندن اثبات دقیق آن می‌توانید به مقاله وایلز [Wil95] رجوع کنید.

۵.۳.۵ اتمام اثبات

پس فرض کنیم که معادله‌ی فرما یک جواب نابدیهی دارد و $A^p + B^p = C^p$. در این صورت خم فری را به شکل زیر تعریف می‌کنیم:

$$F : y^۲ = x(x - A^p)(x + B^p)$$

و نمایش‌های گالوای روی آن را در نظر گرفتیم. می‌توان دید که این نمایش‌ها مجاز هستند. بنابراین با توجه به قضیه اصلی وایلز، مدولار هستند و پس یک فرم مدولار نرمال در $S_۲(\Gamma_۰(N))$ برای Nی پیدا می‌کنیم که N عددی خالی از مربع خواهد بود که $N \mid ۲ABC$ (این از ترکیب قضیه‌ای از میزر و ریبت بدست می‌آید که آن را بیان نکردیم. می‌توانید این را در [Man05] پیدا کنید). حال با استفاده از تفکیک‌کننده یک خم می‌توان شرطی روی نمایش‌های گالوای بدست آمده از نقاط lـ تابی قرار داد. اگر این کار را برای خم فری انجام دهیم نتیجه می‌شود که همه‌ی اعداد اول فردی 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 $S_۲(\Gamma_۰(۲))$ پیدا کرد. اما داریم $S_۲(\Gamma_۰(۲)) = \{۰\}$ (این به‌سادگی از این‌که فشرده‌سازی $\mathbb{H}/\Gamma_۰(۲)$ گونای صفر دارد بدست می‌آید) و پس فرم مدولار نرمالی در آن وجود ندارد. این همان تناقضی بود که دنبالش بودیم!

مراجع

[Apo76] Apostol T. M., *Introduction to Analytic Number Theory*, Springer, 1976.

[Art23] Artin E., *Üb er eine neue art von L-Reihen*, 1923.

[CaF65] Cassels J.W.S., Frohlich A., *Algebraic Number Theory*, London Mathematical Society, 1965.

[Dar03] Darmon H., *Rational Points on Modular Elliptic Curves*, 2003.

[Eul88] Euler L., *Introduction to Analysis of the Infinite - Book I*, Springer, 1988.

[Ful69] Fulton W., *Algebraic curves*, 1969.

[Har77] Hartshorne R., *Algebraic Geometry*, Springer, 1977.

[Man05] Manin, Yu. I., Panchishkin, Alexei A., *Introduction to Modern Number Theory*, 2005.

[Rib90] Ribet K., *From the Taniyama-Shimura Conjecture to Fermat's Last Theorem* , 1990.

[Rie59] Riemann B., *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, 1859.

[Ser67] Serre J.P., *Complex Multiplication*, in: Cassels-Frohlich, ed., Algebraic Number Theory, Academic Press, 1967.

[Ser73] Serre J.P., *A Course in Arithmetic*, Springer, 1973.

[Sho76] Shoenfeld L., *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II* , Mathematics of Computation, **30** (134): 337 - 360,1976.

[Sil92] Silverman J., Tate J.T., *Rational Points on Elliptic Curves*, Springer, 1992.

[Sil86] Silverman J. *The Arithmetic of Elliptic Curves*, Springer, 1986.

[Sil94] Silverman J., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[Was82] Washington L.C., *Introduction to Cyclotomic Fields*, Springer, 1982.

[Wil95] Wiles A., *Modular Elliptic curves and Fermat's Last Theorem*, 1995.

[Zag08] 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.