

از تابع زتای اویلر تا L - توابع آرتین

علی چراغی

۱ مقدمه

یکی از مسائل بسیار قدیمی در ریاضیات، مطالعه‌ی اعداد اول و بررسی توزیع آن‌ها در اعداد طبیعی است. اقلیدس^۱ اولین کسی بود که اثبات کرد بی‌نهایت عدد اول وجود دارد. بعد از او اویلر^۲ در کتاب مقدمه‌ی *بر آنالیزی نهایی*، [۱]، برای اولین بار با استفاده از آنالیز، بی‌نهایت بودن تعداد اعداد اول را ثابت می‌کند. در واقع اوسری^۱ $\sum_{p \text{ اول}} \frac{1}{p}$ را بررسی کرده و اثبات می‌کند که این سری به بی‌نهایت واگراست و گامی در جهت شناخت بیشتر اعداد اول برداشت. همچنین این اثبات او شروعی برای نظریه تحلیلی اعداد به حساب می‌آید. سپس او تابع زتا را تعریف می‌کند و بعضی از مقادیر آن را بدست می‌آورد. پس از اویلر، دیریکله^۳ در سال ۱۸۴۰، با استفاده از مشخصه‌های اعداد صحیح پیمانه‌ای، تابع زتای اویلر را گسترش می‌دهد و با استفاده از آن قضیه معروف خود را ثابت می‌کند: ”در هر تصاعد حسابی اولیه، بی‌نهایت عدد اول وجود دارد.” او این توابع گسترش یافته را با نماد L نمایش می‌دهد و به همین دلیل این نوع توابع به L - توابع^۴ معروف می‌شوند. ریمان^۵ در مقاله‌ی [۲]، که تنها مقاله‌ی او در نظریه اعداد محسوب می‌شود، تابع زتای اویلر را به اعداد مختلط گسترش می‌دهد و ادعا می‌

کند اگر صفرهای تابع زتا در محدوده‌های خاصی نباشند، آنگاه قضیه اعداد اول (و حتی بهتر از آن) بدست می‌آید. همچنین او در این مقاله مهمترین حدس ریاضیات به نام فرض ریمان را مطرح می‌کند. این حدس در مورد صفرهای تابع زتا در ناحیه‌ی خاصی صحبت می‌کند که در صورت درست بودن، درک بیشتری از توزیع اعداد اول و تعداد بسیاری از مسائل دیگر می‌شود. بعد از او ددکیند^۶ تابع زتا را به میدان‌های عددی گسترش می‌دهد و نشان می‌دهد اطلاعات مهمی از میدان‌های عددی در آن توابع کدگذاری شده‌اند. آرتین^۷ در سال ۱۹۲۳ و در دومین مقاله‌ی منتشر شده از او، [۳]، L - توابع جدیدی را تعریف می‌کند که گسترش L - توابع دیریکله محسوب می‌شوند و مانند توابع زتا و L - توابع درک بالاتری از میدان‌های عددی به ما می‌دهند.

در مقاله پیش رو، روندی تاریخی برای معرفی L - توابع آرتین به کار گرفته شده است. همچنین در بیشتر اثبات‌ها، طرح اثبات داده شده یا خواننده ارجاع داده شده است. همچنین برای سادگی فقط توسیع‌های میدان اعداد گویا در نظر گرفته شده است.

^۱Euclid

^۲Euler

^۳Dirichlet

^۴L-functions

^۵Riemann

^۶Dedekind

^۷Artin

۲ نامتناهی بودن تعداد اعداد اول

به اعداد اول وجود دارد، داریم:

$$P_n = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \dots \quad (1)$$

حال از فرم ضربی P_n لگاریتم می‌گیریم:

$$\log P_n = \log\left(\frac{1}{1-\frac{1}{2^n}}\right) + \log\left(\frac{1}{1-\frac{1}{3^n}}\right) + \log\left(\frac{1}{1-\frac{1}{4^n}}\right) + \dots$$

و از بسط $\log\left(\frac{1}{1-x}\right) = \sum_{m=1}^{\infty} \frac{x^m}{m}$ استفاده می‌کنیم:

$$\begin{aligned} \log P_n = & \left(\frac{1}{2^n} + \frac{1}{2} \left(\frac{1}{2^{2n}}\right) + \frac{1}{3} \left(\frac{1}{2^{3n}}\right) + \dots\right) + \\ & \left(\frac{1}{3^n} + \frac{1}{2} \left(\frac{1}{3^{2n}}\right) + \frac{1}{3} \left(\frac{1}{3^{3n}}\right) + \dots\right) + \\ & \dots \end{aligned}$$

حال با تغییر دادن آرایش آن داریم:

$$\begin{aligned} \log P_n = & \left(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \dots\right) + \\ & \frac{1}{2} \left(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \dots\right) + \\ & \frac{1}{3} \left(\frac{1}{2^{3n}} + \frac{1}{3^{3n}} + \frac{1}{5^{3n}} + \dots\right) + \\ & \dots \end{aligned} \quad (2)$$

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

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

و از (۲):

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

حال مجموع جملات دوم به بعد سری بالا، مثلا طبق آزمون

اقلیدس در ۳۰۰ سال قبل از میلاد، اثبات خود را از بی نهایت بودن اعداد اول ارائه می‌دهد. البته در اثبات خود اقلیدس، از آنجایی که نمادگذاری برای اعداد مرسوم نبوده، او فقط برای مثال هایی این روش را توضیح می‌دهد ولی مشخص است منظور او برای حالت کلی بوده است.

قضیه. (اقلیدس) بی نهایت عدد اول وجود دارد.

برهان. فرض کنید این طور نباشد و p_1, p_2, \dots, p_n تنها اعداد اول باشند. در این صورت از آنجایی که هر عدد به اعداد اول تجزیه می‌شود، عدد $N = p_1 p_2 \dots p_n + 1$ نیز باید حداقل یکی از این اعداد اول مثل p_i را داشته باشد. در حالی که بوضوح $p_i \nmid p_1 p_2 \dots p_n$ پس

$$p_i \mid N - p_1 p_2 \dots p_n = 1$$

که تناقض است. \square

اوایلر در [۱]، ایده‌ی جدیدی برای اثبات نامتناهی بودن تعداد اعداد اول عرضه می‌کند که دیدگاهی آنالیزی برای حل مسائل "گسسته" نظریه اعداد می‌دهد.

قضیه. (اوایلر) بی نهایت عدد اول وجود دارند.

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

برهان. عدد زیر را در نظر بگیرید:

$$P_n = \left(\frac{1}{1-\frac{1}{2^n}}\right) \left(\frac{1}{1-\frac{1}{3^n}}\right) \left(\frac{1}{1-\frac{1}{5^n}}\right) \dots$$

که اعداد ۲، ۳، ۵، ... روی اعداد اول تغییر می‌کنند. در این صورت از بسط $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ داریم:

$$P_n = \left(1 + \frac{1}{2^n} + \frac{1}{2^{2n}} + \dots\right) \left(1 + \frac{1}{3^n} + \frac{1}{3^{2n}} + \dots\right) \dots$$

و با ضرب این جملات در هم و استفاده از این که تجزیه یکتا

انتگرال، مقداری متناهی خواهد بود و داریم:

$$\log P_n = \log \log \infty \approx \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots$$

و کار تمام است. \square

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:

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

۳ تابع زتای اوایلر

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

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

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

تعریف. تابع زتای اوایلر 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 اوایلر برای حالت کلی تری این فرم ضربی را ارائه می‌دهد:

قضیه. (اوایلر) برای $s > 1$ داریم:

$$\zeta(s) = \prod_{p \text{ اول}} \left(\frac{1}{1 - \frac{1}{p^s}} \right)$$

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

به این فرم ضربی، تجزیه اوایلری^۸ تابع زتا می‌گویند.

اوایلر چند مقدار این تابع را بدست آورد:

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

$$\zeta(2n) = \frac{2^{2n-1} \pi^{2n}}{(2n)!} |B_{2n}|$$

که B_n ها اعداد برنولی هستند.

همچنین اوایلر با بررسی سری $\sum_{n=1}^{\infty} n^k x^n$ 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. (اوایلر)

$$\frac{\zeta(1-n)}{\zeta(n)} = \frac{2^{1-n} \cos\left(\frac{n\pi}{2}\right) n!}{\pi^n}$$

همچنین اوایلر حدس زیر را مطرح می‌کند که به دو طریق در مقاله ریمان اثبات می‌شود.

حدس. (اوایلر) برای هر عدد حقیقی مثبت s ,

$$\frac{\zeta(1-s)}{\zeta(s)} = \frac{2^{1-s} \cos\left(\frac{s\pi}{2}\right) \Gamma(s+1)}{\pi^s}$$

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

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1} dx$$

۴ L - توابع دیریکله

دیریکله 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

^۸Euler factorization

برای s هایی که L - تابع تعریف می شود داریم:

$$L(s, \chi) = \prod_{p \text{ اول}} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

برهان. با استفاده از کاملاً ضربی بودن χ و بسط تیلور $\frac{1}{1-x}$ ، داریم:

$$\begin{aligned} L(s, \chi) &= \prod_{p \text{ اول}} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right) \\ &= \prod_{p \text{ اول}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \dots \right) \\ &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \end{aligned}$$

معمولاً مقدار L - توابع در نقطه $s = 1$ اهمیت زیادی دارد. مثلاً مهم ترین حکمی که دیریکله برای اثبات قضیه خود به آن احتیاج داشت قضیه زیر بود:

قضیه. (دیریکله) اگر χ یک مشخصه دیریکله نابديهی باشد آنگاه $L(1, \chi) \neq 0$.

سپس دیریکله با استفاده از L - توابع، اعداد اول به پیمانۀ m جدا می کند و برای هر کدام از آن دسته ها از اعداد اول، ثابت می کند:

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:

$$\sum_{\substack{p \equiv r \\ p \leq x}} \frac{1}{p} = \frac{1}{\phi(m)} \log \log x + A + O\left(\frac{1}{\log x}\right)$$

برهان. رجوع شود به فصل ۷ از [۴].

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

شد. در واقع ایده ی او این بود که اثبات کند $\sum_{p \equiv r}^m \frac{1}{p}$ واگرا به بی نهایت است و با استفاده از آن قضیه اش را نتیجه بگیرد. برای تعریف L - توابع دیریکله باید ابتدا مشخصه های دیریکله را تعریف کنیم:

تعریف. تابع $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ را یک مشخصه دیریکله به پیمانۀ m می نامیم هرگاه خواص زیر را داشته باشد:

- اگر a نسبت به m اول نباشد: $\chi(a) = 0$
- اگر a نسبت به m اول باشد: $|\chi(a)| = 1$
- 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 مشخصه ی دیریکله در واقع یک همومورفیسم از $(\mathbb{Z}/m\mathbb{Z})^*$ به \mathbb{C}^* است. همچنین تابع $\chi \equiv 1$ را مشخصه بدیهی می نامیم.

تعریف. فرض کنید χ یک مشخصه ی دیریکله باشد. L - تابع دیریکله ی وابسته به آن را به شکل زیر تعریف می کنیم:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

اگر χ مشخصه بدیهی باشد، سری بالا برای $s > 1$ همگراست و برابر با تابع زتای اوایلر است.

اگر χ مشخصه بدیهی نباشد، سری بالا برای $s < 0$ همگراست. این تابع این خاصیت را دارد که اعداد متفاوت به پیمانۀ m را از هم "جدا" می کند. مثلاً اگر χ_1 مشخصه ی دیریکله به پیمانۀ ۴ باشد که با $\chi_1(1) = 1$ و $\chi_1(3) = -1$ شناسایی می شود، آنگاه L - تابع وابسته به آن برابر است با:

$$L(s, \chi_1) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s} = \sum_{n \equiv 1} \frac{1}{n^s} - \sum_{n \equiv 3} \frac{1}{n^s}$$

همچنین L - توابع به دلیل کاملاً ضربی بودن χ ، تجزیه اوایلری دارند:

قضیه. اگر $L(s, \chi)$ یک L - تابع دیریکله باشد. در این صورت

۵ تابع زتای ریمان

ریمان در مقاله معروف خود، [۲]، تابع زتای اوایلر 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 $\frac{\pi(x)}{x/\log x} \rightarrow 1$ وقتی x به بی نهایت میل می‌کند.

ابتدا ریمان تابع ζ را به اعداد مختلط s با $Re s > 1$ گسترش می‌دهد. در واقع سری $\sum \frac{1}{n^s}$ برای محدوده $Re s > 1$ به طور مطلق همگراست و تابع زتا را در این ناحیه می‌توان گسترش داد.

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

قضیه. (ریمان) تابع زتای اوایلر را می‌توان به صفحه مختلط گسترش داد بطوری که بجز یک قطب ساده با مانده 1 در نقطه $s = 1$ ، 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 $\{s \in \mathbb{C} | Re s = 1\}$.

برهان. رجوع شود به فصل ۱۳ از [۴].

همچنین ریمان حدسی را در مقاله اش 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^۹) اگر صفری از تابع زتای ریمان روی نوار $\{s \in \mathbb{C} | 0 < Re s < 1\}$ قرار داشته باشد، آن گاه آن صفر روی خط بحرانی $\{\frac{1}{2} + it | t \in \mathbb{R}\}$ 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 سخت‌ترین 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:

نتیجه. اگر فرض ریمان درست باشد و اگر انتگرال لگاریتمی^{۱۰} را برابر $Li(x) = \int_{\frac{1}{2}}^x \frac{dt}{\log t}$ تعریف کنیم، آن گاه:

$$|\pi(x) - Li(x)| < \frac{1}{\lambda\pi} \sqrt{x} \log x$$

برهان. رجوع شود به [۵].

L -توابع دیریکله را نیز مانند تابع زتا، می‌توان به طور مرمورفیک^{۱۱} به کل صفحه گسترش داد و حدسی مانند فرض ریمان برای آن‌ها فرمول بندی کرد:

حدس. (فرض تعمیم یافته ریمان^{۱۲}) اگر χ یک مشخصه دیریکله باشد و صفری از تابع $L(s, \chi)$ روی نوار بحرانی $\{s \in \mathbb{C} | 0 < Re s < 1\}$ قرار داشته باشد، آن گاه آن صفر روی خط بحرانی $\{\frac{1}{2} + it | t \in \mathbb{R}\}$ قرار گرفته است.

^۹Riemann Hypothesis (RH)

^{۱۰}Logarithmic integral

^{۱۱}Meromorphic

^{۱۲}Generalized Riemann Hypothesis (GRH)

۶ نظریه جبری اعداد

موجود در آن حلقه تجزیه نمی شوند، بلکه تجزیه یکتا برای ایدال های حلقه اعداد صحیح درست است:

قضیه. فرض کنید $\mathbb{Q} \subseteq K$ یک میدان عددی و R_K حلقه ی اعداد صحیح موجود در آن میدان باشد. در این صورت هر ایدال ناصفر $I \subseteq R_K$ را می توان به شکل زیر نوشت.

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

که \mathfrak{P}_i ها ایدال هایی اول از R_K و α_i ها اعداد صحیح مثبت هستند. این تجزیه در حد جایگشت یکتاست.

برهان. رجوع شود به [۷].

حال فرض کنید $\mathbb{Q} \subseteq K$ یک توسیع میدان عددی و R_K حلقه اعداد صحیح موجود در آن میدان باشد و $p \in \mathbb{Z}$ یک عدد اول گویا (منظور عدد اولی در \mathbb{Z} است)، در این صورت pR_K یک ایدال ناصفر در R_K تشکیل می دهد و ما علاقه مند به تجزیه این ایدال به ایدال های اول موجود در R_K هستیم. این ایدال در R_K مثلاً به شکل زیر تجزیه می شود:

$$pR_K = \mathfrak{P}_1^{e_{\mathfrak{P}_1/p}} \mathfrak{P}_2^{e_{\mathfrak{P}_2/p}} \dots \mathfrak{P}_n^{e_{\mathfrak{P}_n/p}}$$

که \mathfrak{P}_i ها ایدال های اول در R_K هستند و $e_{\mathfrak{P}_i/p}$ ها اعداد صحیح مثبت. ایدال های اول \mathfrak{P}_i ، ایدال های اول روی p نامیده می شوند. به عدد اول $p \in \mathbb{Z}$ ، شاخه ای گوئیم اگر برای i ای، $1 < e_{\mathfrak{P}_i/p}$ و در غیر این صورت به آن عدد اول، غیر شاخه ای گوئیم. همچنین به اعداد $e_{\mathfrak{P}_i/p}$ اندیس انشعاب \mathfrak{P}_i روی p گفته می شود. می توان ثابت کرد که تعداد اعداد اول شاخه ای در یک توسیع متناهی، متناهی است. همچنین عدد مهم دیگری در نظریه انشعاب وجود دارد به نام درجه مانده ای \mathfrak{P}_i روی p ، که به این شکل تعریف می شود:

تعریف. اگر \mathfrak{P} روی p باشد، آن گاه $\mathbb{Z}/p\mathbb{Z} \subseteq R_K/\mathfrak{P}$ میدان هایی متناهی خواهند بود و $[R_K/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$ درجه مانده ای \mathfrak{P} روی p گفته می شود و با $f_{\mathfrak{P}/p}$ نمایش داده می شود.

از اینجا به بعد، فرض می کنیم K/\mathbb{Q} توسیعی گالوا باشد. در این حالت می توان اثبات کرد که درجه مانده ای و اندیس انشعاب، برای همه ایدال های اول روی p عددی ثابت است.

نظریه جبری اعداد قسمتی از نظریه اعداد است که با استفاده از تکنیک های جبر مجرد، به مطالعه ی اعداد صحیح، اعداد گویا و توسیع های آن ها می پردازد. سوالات نظریه اعداد را می توان با استفاده از نظریه جبری اعداد فرمول بندی جدیدی کرد و با استفاده از خواص جبری ساختارهای جبری متنوع به بررسی آن ها پرداخت. نظریه جبری اعداد مخصوصاً در حل بسیاری از معادلات دیوفانتی^{۱۳} کمک می کند.

در اینجا فرض می کنیم خواننده با بعضی ایده ها و ساختارهای جبری معمولی مثل حلقه، ایدال، میدان، توسیع میدان ها، نظریه گالوا^{۱۴} آشنا است.

خواننده برای درک این مفاهیم می تواند به [۶] رجوع کند. برای سادگی ما فقط با توسیع های اعداد گویا کار می کنیم و تعریف می کنیم:

تعریف. منظور از یک میدان عددی جبری، توسیعی متناهی از میدان اعداد گویا است.

مثال هایی مهم از میدان های عددی، میدان های $\mathbb{Q}(\sqrt{d})$ ، $\mathbb{Q}(\zeta_n)$ هستند که d یک عدد صحیح و ζ_n یک ریشه ی n -ام اولیه واحد است. این میدان ها در حل بسیاری از معادلات دیوفانتی مثل قضیه آخر فرما کمک می کنند.

تعریف. به $\mathbb{C} \ni z$ یک عدد صحیح جبری می گوئیم هرگاه در یک چندجمله ای به فرم زیر صدق کند:

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \quad (a_i \in \mathbb{Z})$$

منظور از "حلقه اعداد صحیح یک میدان عددی"، مجموعه ی اعداد صحیح موجود در آن میدان است. می توانید بررسی کنید که حلقه اعداد صحیح در یک میدان عددی، با جمع و ضرب معمولی اعداد مختلط، ساختار یک حلقه را تشکیل می دهند. "حلقه اعداد صحیح میدان اعداد گویا" همان اعداد صحیح معمولی، \mathbb{Z} هستند و در این حالت \mathbb{Z} خواص بسیاری مانند تجزیه به اعداد اول و ... را دارد. ولی برخلاف این حالت خاص، اعداد صحیح در یک میدان عددی لزوماً به اعداد اول

^{۱۳}Diophantine equations

^{۱۴}Galois

به عبارت دیگر با نمادگذاری بالا:

$$e_{\mathfrak{P}_i/p} = e_{\mathfrak{P}_j/p}, \quad f_{\mathfrak{P}_i/p} = f_{\mathfrak{P}_j/p}$$

برای همه i, j ها.

حال گروه‌هایی را تعریف می‌کنیم که در نظریه انشعاب نقش مهمی را ایفا می‌کنند:

تعریف. فرض کنید $Gal(K/\mathbb{Q})$ گروه گالوای توسعه K/\mathbb{Q} باشد و $pR_K = \mathfrak{P}_1^{e_{\mathfrak{P}_1/p}} \mathfrak{P}_2^{e_{\mathfrak{P}_2/p}} \dots \mathfrak{P}_n^{e_{\mathfrak{P}_n/p}}$ تجزیه عدد اول p به ایدال‌های اول R_K باشد. در این صورت برای هر \mathfrak{P}_i گروهی به نام گروه تجزیه^{۱۵} به شکل زیر تعریف می‌شود:

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

حال می‌توان همومورفیسم $f: D_{\mathfrak{P}_i} \rightarrow Gal(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}})$ را در نظر گرفت که به شکل زیر تعریف می‌شود:

فرض کنید $\sigma \in D_{\mathfrak{P}_i}$ در این صورت σ ، \mathfrak{P}_i را ثابت نگه می‌دارد و پس اتومورفیسمی از R/\mathfrak{P}_i می‌دهد بطوری که $\mathbb{Z}/p\mathbb{Z}$ را ثابت نگه می‌دارد. پس می‌توان عضو $f(\sigma)$ را برابر با این اتومورفیسم از $Gal(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}})$ تعریف کرد. همچنین می‌توان ثابت کرد که f پوشاست.

حال گروه دیگری را با استفاده از این همومورفیسم می‌توان تعریف کرد (این گروه در تعریف مولفه‌های شاخه‌ای L - توابع آرتین به کار می‌آید):

تعریف. گروه اینرسی^{۱۶} $\mathfrak{I}_{\mathfrak{P}_i}$ را برابر با هسته‌ی همومورفیسم f تعریف می‌کنیم و با $\mathfrak{I}_{\mathfrak{P}_i}$ نشان می‌دهیم. در واقع:

$$\mathfrak{I}_{\mathfrak{P}_i} = \{\sigma \in D_{\mathfrak{P}_i} \mid \forall r \in R_K, \sigma(r) - r \in \mathfrak{P}_i\}$$

با استفاده از قضیه اول یکریختی داریم:

$$\frac{D_{\mathfrak{P}_i}}{\mathfrak{I}_{\mathfrak{P}_i}} \cong Gal\left(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$$

همچنین به سادگی می‌توان دید که $D_{\mathfrak{P}_i}$ ($I_{\mathfrak{P}_i}$) مزدوج $D_{\mathfrak{P}_j}$ ($I_{\mathfrak{P}_j}$) است برای همه i, j ها.

همچنین قضیه زیر را داریم:

$$|D_{\mathfrak{P}_i}| = e_{\mathfrak{P}_i/p} f_{\mathfrak{P}_i/p} \quad \text{و} \quad |I_{\mathfrak{P}_i}| = e_{\mathfrak{P}_i/p}$$

حال در موقعیتی هستیم که اتومورفیسم فروبنیوس را تعریف کنیم:

معمول است که $\mathbb{Z}/p\mathbb{Z}$ را با \mathbb{F}_p نمایش دهند. پس $\frac{R}{\mathfrak{P}_i} / \mathbb{F}_p$ یک توسعه متناهی از میدان‌های متناهی است و با نظریه میدان‌های متناهی می‌توان نشان داد که این توسعه‌ها همواره گالوا هستند و گروه گالوای آن‌ها دوری است و با عنصر $\sigma: x \mapsto x^p$ تولید می‌شود. به این عنصر، اتومورفیسم فروبنیوس این توسعه گفته می‌شود. پس $Gal(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}})$ گروهی دوری است که با $Frob_{\mathfrak{P}_i/p}: x \mapsto x^p$ تولید می‌شود. حال فرض کنید p عدد اولی غیرشاخه‌ای باشد و مانند قبل $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_n$ ایدال‌های اول روی p باشند. در این صورت از قضیه بالا $I_{\mathfrak{P}_i} = \{1\}$ برای همه i ها و داریم:

$$Gal(K/\mathbb{Q}) \supseteq D_{\mathfrak{P}_i} \cong Gal\left(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$$

پس می‌توان اتومورفیسم موجود در $Gal(\frac{R}{\mathfrak{P}_i} / \frac{\mathbb{Z}}{p\mathbb{Z}})$ را به عنوان عنصری در $Gal(K/\mathbb{Q})$ نگاه کرد و از آنجایی که $D_{\mathfrak{P}_i}$ ها $(0 \leq i \leq n)$ مزدوج یکدیگرند، پس مولد‌های آنها نیز مزدوج یکدیگرند و می‌توان اتومورفیسم فروبنیوس عدد اول p (به ایدال‌های اول روی p وابسته نیست) را برابر با آن مولفه‌ی ازدواج در $Gal(K/\mathbb{Q})$ تعریف کرد که ما با $Frob_p$ نشان می‌دهیم.

۷ توابع زتای ددکیند

ددکیند تابع زتای ریمان را برای میدان‌های عددی گسترش داد و با استفاده از آن تعدادی از خواص موجود در اعداد صحیح را به حلقه اعداد صحیح میدان‌های عددی گسترش داد. همچنین فرض ریمان گسترش یافته^{۱۷} نیز برای آن فرمول بندی شده است

^{۱۵}Decomposition group

^{۱۶}Inertia group

^{۱۷}Extended Riemann Hypothesis (ERH)

^{۱۸}Norm

۸ نمایش خطی گروه‌های متناهی

ما برای تعریف L - توابع آرتین به یک توسیع از مشخصه‌های دیریکله به نام نمایش‌های خطی گروه‌ها نیاز داریم که در این بخش به مقدمات آن پرداخته می‌شود.

در این بخش همیشه فرض می‌کنیم G یک گروه متناهی است. **تعریف.** منظور ما از یک نمایش خطی از G ، یک عمل خطی گروه G بر یک فضای برداری V متناهی بعد روی اعداد مختلط است. به عبارت دیگر، یک نمایش خطی گروه G یک همومورفیسم $\rho: G \rightarrow GL_n(V)$ است. به V ، یک G -فضا گفته می‌شود.

درجه یک نمایش خطی، طبق تعریف، بُعد V است. نمایش (ρ, V) یک نمایش تحویل ناپذیر است هرگاه هیچ زیرفضای سره پایا تحت عمل G نداشته باشد. دو نمایش خطی (ρ, V) و (ρ', V') معادل نامیده می‌شوند هرگاه V و V' به عنوان G -فضا یکی باشند، این مفهوم به این معناست که یک ایزومورفیسم خطی $f: V \rightarrow V'$ باشد بطوری که:

$$f \circ \rho(g) = \rho'(g) \circ f$$

هر نمایش خطی (ρ, V) به جمع مستقیم نمایش‌های تحویل ناپذیر خطی تجزیه می‌شود. به عبارت دیگر:

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_s$$

که V_i ها G -فضا هستند و V_i ها نمایش‌هایی تحویل ناپذیرند. مشخصه‌ی یک نمایش (ρ, V) برابر با تابع زیر است:

$$\chi: G \rightarrow \mathbb{C}, \quad \chi(\sigma) = \text{Tr}(\rho(\sigma))$$

است که از آن جایی که اثر^{۲۰} یک ماتریس فقط به مولفه‌ی ازدواج آن بستگی دارد، پس χ در حد ازدواج ثابت می‌ماند. دو نمایش معادلند اگر و تنها اگر مشخصه‌های آن‌ها مساوی باشند. مشخصه‌ی اصلی^{۲۱} همواره برابر ۱ است، مشخصه‌ی اصلی^{۲۱} نامیده می‌شود.

که نتایجی در نحوه‌ی تجزیه اعداد اول به ایدآل‌های اول در آن میدان عددی دارد. برای تعریف تابع زتای ددکیند ابتدا باید مفهومی به نام نُرم^{۱۸} را تعریف کنیم:

تعریف. فرض کنید K یک میدان عددی با حلقه اعداد صحیح R_K باشد و I یک ایدآل ناصفر R_K . در این صورت منظور از نُرم I ، اندیس I در R_K است و با $N_{K/\mathbb{Q}}(I)$ نمایش داده می‌شود.

حال می‌توان تابع زتای ددکیند را تعریف کرد:

تعریف. تابع زتای ددکیند برای میدان عددی K ، به شکل زیر تعریف می‌شود:

$$\zeta_K(s) = \sum_{I \subseteq R_K} \frac{1}{(N_{K/\mathbb{Q}}(I))^s}$$

که I روی ایدآل‌های ناصفر R_K حرکت می‌کند.

این تابع برای s مختلط با $\text{Re } s > 1$ همگراست.

اولا به سادگی می‌توان دید که در حالت $K = \mathbb{Q}$ تابع زتای ددکیند، همان تابع زتای ریمان است.

برای تابع زتای ددکیند، نیز به دلیل ضربی بودن تابع نُرم می‌توان تجزیه‌ای به فرم اوایلر پیدا کرد:

قضیه. برای s مختلط با $\text{Re } s > 1$ داریم:

$$\zeta_K(s) = \prod_{P \subseteq R_K} \left(\frac{1}{1 - N_{K/\mathbb{Q}}(P)^{-s}} \right)$$

که P روی ایدآل‌های اول ناصفر R_K حرکت می‌کند.

هکه^{۱۹} توانست این تابع را به کل صفحه مختلط به طور مرمورفیک گسترش دهد و همچنین معادله‌ای تابعی برای آن پیدا کند و پس حدسی مانند فرض ریمان برای آن فرمول بندی شد:

حدس. (فرض ریمان گسترش یافته) برای هر میدان عددی K ، اگر صفری از $\zeta_K(s)$ در $\{s \in \mathbb{C} \mid 0 < \text{Re } s < 1\}$ باشد، آن گاه آن صفر روی خط $\text{Re } s = \frac{1}{2}$ قرار دارد.

^{۱۹}Hecke

^{۲۰}Trace

^{۲۱}Principal character

۹ L - توابع آرتین

دریافت می‌کنیم:

$$L(s, \chi_0, K) = \zeta(s)$$

(۲) اگر $L \supseteq K \supseteq \mathbb{Q}$ توابع های گالوای \mathbb{Q} باشند، آن گاه

$$L(s, \chi, K/\mathbb{Q}) = L(s, \chi, L/\mathbb{Q})$$

که مشخصه χ از $Gal(K/\mathbb{Q})$ را به عنوان یک مشخصه از $Gal(L/\mathbb{Q})$ ببینیم.

(۳) اگر χ_1 و χ_2 دو مشخصه از $Gal(K/\mathbb{Q})$ باشند، آن گاه

$$L(s, \chi_1 + \chi_2, K/\mathbb{Q}) = L(s, \chi_1, K/\mathbb{Q})L(s, \chi_2, K/\mathbb{Q})$$

(۴) اگر χ_α ها مشخصه های تحویل ناپذیر نمایش های $Gal(K/\mathbb{Q})$ باشند، آنگاه $r_\alpha \in \mathbb{C}$ وجود دارند بطوری که:

$$\zeta_K(s) = \zeta(s) \prod L(s, \chi_\alpha, K/\mathbb{Q})^{r_\alpha}$$

برهان. رجوع شود به قضیه ۲، ۴ از فصل ۵ در [۸].

L - تابع آرتین در حالتی که توسیع آبلی باشد (توسیع گالوای متناهی با گروه گالوای آبلی)، با L - تابع دیریکله یکسان می شود اما از آنجایی که اثبات آن به کمی نظریه میدان های رده ای نیاز دارد خواننده علاقمند می تواند به کتاب [۸] رجوع کند.

همچنین L - توابع آرتین به طور مرمورفیک به صفحه مختلط گسترش می یابد و یک معادله ی تابعی مانند معادله ی تابعی تابع زتا دارند. همچنین حدس آرتین ادعا می کند که اگر مشخصه غیر اصلی باشد، آنگاه L - تابع آرتین وابسته به آن به طور تحلیل گسترش می یابد:

حدس. (آرتین) برای هر مشخصه تحویل ناپذیر غیر اصلی، L - تابع آرتین $L(s, \chi, K/\mathbb{Q})$ یک گسترش تحلیلی به کل صفحه مختلط دارد.

حدس آرتین در صورت درست بودن، نتایج بسیار زیادی دارد، مثلا تحلیلی بودن $\frac{\zeta_L(s)}{\zeta_K(s)}$ برای توسیع L/K از میدان های عددی.

فرض کنید K/\mathbb{Q} یک توسیع گالوا با گروه گالوای G باشد و فرض کنید (ρ, V) یک نمایش خطی از G باشد. برای $\sigma \in G$ و $v \in V$ ، عمل $\rho(\sigma)v$ را با σv نمایش می دهیم.

فرض کنید $p \in \mathbb{Z}$ یک عدد اول و \mathfrak{P} یک ایدال اول روی p باشد. در این صورت اگر $D_{\mathfrak{P}}$ گروه تجزیه و $I_{\mathfrak{P}}$ گروه اینرسی \mathfrak{P}/p باشد، آن گاه از نتایج بخش های قبل، $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ با عنصر فروبنیوس $\text{Frob}_{\mathfrak{P}/p}$ تولید می شود و پس اتومورفیسم فروبنیوس یک درون ریختی فضای متناهی بعد

$$V^{I_{\mathfrak{P}}} := \{v \in V \mid \forall i \in I_{\mathfrak{P}}; iv = v\}$$

است و می توان "چندجمله ای مشخصه" اتومورفیسم $\text{Frob}_{\mathfrak{P}/p}$ را با تابع زیر تعریف کرد:

$$\text{Charpol}(\text{Frob}_{\mathfrak{P}/p})(t) = \text{Det}(I - t\text{Frob}_{\mathfrak{P}/p})$$

تعریف می کنیم. از بخش های قبل می دانیم که $\text{Frob}_{\mathfrak{P}/p}$ در حد ازدواج با خود p مشخص می شود. پس از آنجا که چندجمله ای مشخصه ماتریس های مزدوج یکی است، پس این چندجمله ای مشخصه، فقط با p مشخص می شود و به انتخاب ایدال اول روی آن بستگی ندارد.

حال می توان L - توابع آرتین را تعریف کرد:

تعریف. فرض کنید K/\mathbb{Q} یک توسیع گالوای متناهی با گروه گالوای G باشد. فرض کنید (ρ, V) یک نمایش خطی G با تابع مشخصه χ باشد. آن گاه L - تابع آرتین وابسته به ρ یا χ با فرم ضربی زیر تعریف می شود:

$$L(s, \chi, K/\mathbb{Q}) = \prod_{\text{اول } p} \frac{1}{\text{Charpol}(\text{Frob}_p)(N(p)^{-s})}$$

برای هر $\delta > 0$ ، L - تابع آرتین به طور یکنواخت و مطلق روی ناحیه $Re s \geq 1 + \delta$ همگراست.

قضیه. (۱) برای مشخصه ی اصلی $\chi_0 \equiv 1$ ، تابع زتای ریمان را

مراجع

- [1] Euler L. *Introduction to Analysis of the Infinite - Book I*, Springer, 1988.
- [2] Riemann B. *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, 1859.
- [3] Artin E. *Über eine neue art von L-Reihen*, 1923.
- [4] Apostol T. M. *Introduction to Analytic Number Theory*, Springer, 1976.
- [5] Shoenfeld, L. *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II*, Mathematics of Computation, **30** (134): 337 - 360.
- [6] Hungerford, W. H. *Algebra*, Springer, 1974.
- [7] Samuel P. *Algebraic Theory of Numbers*, Translated by Allan J. Silberger. Mineola, NY: Dover, 2008.
- [8] Neukirch J. *Class Field Theory*, Springer, 1986.

همچنین L - توابع آرتین کاربردهای بسیار زیادی دارد. مثلاً همان گونه که L - توابع دیریکله در اثبات قضیه دیریکله به ما کمک می کنند، L - توابع آرتین در حل قضیه دیریکله گسترش یافته (قضیه چگالی چبوتاروف^{۲۲}) کاربرد دارند. همچنین آن ها در مشخص کردن توسیع های جبری میدان های عددی، با استفاده از ایدال های موجود در خود آن میدان عددی کمک می کنند. این برنامه توسط کرونگر^{۲۳} پیشنهاد شده بود و کاربردهای زیادی در نظریه جبری اعداد و نظریه تحلیلی اعداد دارند و نتایجی دارند که به فرمول بندی یک برنامه بسیار فعال در نظریه اعداد به نام "برنامه لنگلندز^{۲۴}" منجر می شوند.

۱۰ قدردانی

با تشکر از محمدامین حیدرشاهی برای کمک به حروفچینی مطالب.

^{۲۳}Kronecker

^{۲۴}Langlands program