مجله‌ی ریاضی شریف

سال اول شماره‌ی سوم

مجله‌ی ریاضی شریف، سال اول شماره‌ی سوم؛ صاحب امتیاز : انجمن علمی و فوق‌برنامه‌ی دانشکده‌ی علوم ریاضی؛ مدیر مسوول : دکتر امیر جعفری؛ سردبیر : خشایار فیلم؛ همکاران : دکتر امیر جعفری، دکتر رسول رمضانیان، خشایار فیلم، ابوالفضل طاهری، مهدی کوره‌چیان، کاوه حسینی، احمدرضا حاج سعیدی، احمدرضا عبدلی، سامان حبیبی؛ طراحی : اوژن غنی‌زاده‌ی خوب؛ طراحی سایت : محسن منصوریار؛ ویراستاری : خشایار فیلم، ابوالفضل طاهری، شهاب ابراهیمی، اوژن غنی‌زاده‌ی خوب؛ با تشکر از دکتر مصطفی اصفهانی‌زاده، دکتر رسول رمضانیان

پیشگفتار

بالاخره شماره سوم "مجله ریاضی شریف" هم منتشر شد. خواستم در ابتدای این شماره درباره‌ی تاخیر به وجود آمده در انتشار شماره‌ی سوم سخن بگویم، اما با نگاهی به سال‌های دورتر[۱] نشریه‌ی دانشکده‌ی علوم ریاضی، دانشگاه صنعتی شریف، به این نتیجه رسیدم که دلایلم برای تاخیر حاصل، چندان دلایل موجهی نیست و گویا این مشکلات همواره بر سر راه این‌چنین نشریاتی وجوددارد. در چنین شرایطی احساس من این است که وظیفه‌ی ماست که با چنین مشکلاتی مقابله کنیم و تسلیم آن‌ها نشویم. بنابراین تاخیر به وجود آمده را تنها به دلیل کوتاهی خود می‌دانم و از این بابت از تمامی خوانندگان که نشریه را دنبال می‌کنند عذرخواهی کرده و امیدوارم آن را بپذیرند.

و اما سخن دیگرم در این باب بود که "مجله ریاضی شریف"، با چه هدفی دوباره احیا شد؟ در پاسخ به این سوال دوباره شما را به گذشته ارجاع می‌دهم. نوشته‌ی زیر مربوط به شماره اول "مجله‌ی ریاضی" است که در پاییز سال ۱۳۶۸ منتشر شد:

" برای بسیاری از دانشجویان ریاضی در سراسر عالم، ریاضیات چیزی بیش از چند درس رسمی است که باید چندسالی با خوب و بدش ساخت و آن را به سرآورد و از آن گذشت. ریاضیات برای این عده جاذبه‌ای دائمی دارد و آنان را همواره در همه جا دنبال می‌کند و به صورت اشتغال دائمی آنان در می‌آید، اشتغالی پس از جذابیت و با رازها و اسرار ویژه. بدین ترتیب است که حرفه‌ی "ریاضیات" علیرغم نشیب و فرازها همیشه، جاذب استعدادهای خوب و پرشوری است که به این گذرگاه زیبا اما صعب‌العبور گام می‌نهند.

مجله‌ی ریاضی که نمودی از علایق دانشجویان دانشکده است، جلوه‌ای از این "جاذبه" است. در این "مجله" بنابر آن است که پا را از حد "توصیف" کمی فراتر گذاریم و به متن ریاضیات نزدیکی بیشتری جوئیم هرچند زبانی نیمه فنی، نیمه توصیفی حفظ شده‌است."

هدف فوق، که در شماره اول، سری اول مجله ریاضی مطرح شده‌است، هدفی والاست. مسلما رسیدن به چنین هدفی بسیار دشوار است و نیاز به کار و تلاش فراوان، تمامی اعضای دانشکده علوم ریاضی دارد. کاری نیست

---

[۱] در یادداشت شماره ششم "مجله ریاضی"، پاییز ۱۳۷۶، از دکتر تابش، می‌خوانیم:

"این ششمین شماره‌ی مجله ریاضی است که منتشر می‌شود، با وقفه‌ای چندساله از پاییز ۱۳۷۳ تاکنون و علت آن یکی مانع‌هایی بود که در را انتشار این نشریات دانشجویی ایجاد شده‌بود و دیگری نوعی بی‌رغبتی بین دانشجویان، که این دومی به سرانجامی نویدبخش انجامیده‌است."

که از عهده یک شخص برآید و در یک شب حاصل شود. بنابراین از تمامی شما عزیزان تقاضا دارم که ما را در این راه یاری دهید و امیدوارم که این همکاری متقابل باعث هر چه پویاتر شدن دانشکده و دانشجویان شود، چرا که چند صباحی است که این پویایی کمتر به چشم می‌خورد.

در این‌جا، جا دارد از دوستانی که تاکنون هیچ‌گونه کمکی را از ما دریغ نکرده‌اند تشکر نمایم. در ابتدا از دکتر جعفری که مسئولیت نشریه را به عهده گرفته‌اند، سپاس‌گزارم که باعث احیای دوباره‌ی مجله ریاضی شدند. از انجمن علمی و فوق برنامه دانشکده که همواره در کارهای علمی و فوق برنامه دانشکده پیش قدم بوده‌است و این بار نیز در تمامی مسیر باری را از دوش ما برداشته‌است. از آقای خشایار فیلُم، که تا کنون با مقالات خود کمک شایانی به نشریه کرده‌است و اکنون با قبول سردبیری نشریه، مسئولیت خطیری را بر عهده گرفته‌است. از آقای اوژن غنی‌زاده خوب، که علاوه بر مقاله‌های‌اش، طرح‌های زیبایش همواره زینت بخش مجله‌ی ریاضی است. از آقای محسن منصوریار که وبگاه مجله را راه‌اندازی نمودند. و از تمامی اساتید و دانشجویان دانشکده علوم ریاضی که به جا آوردن نامشان در این برگ‌ها نمی‌گنجد، سپاس فراوان دارم.

و در پایان بخشی از ترجمه‌ی مقدمه‌ی کتاب جبر و مقابله‌ی ابوعبدالله محمد بن موسی خوارزمی، توسط زنده‌یاد حسین خدیوجم را می‌بینیم که با زیبایی تمام ، نحوه‌ی همکاری با "مجله ریاضی شریف" را بیان می‌کند:

"دانشور سه گونه است:

- یا دانش‌مردی است که برای اولین بار دانشی را ابداع یا کشف می‌کند، و برای آیندگان به یادگار می‌گذارد.
- یا اندیشمندی است که آثار پیشینیان را شرح و تفسیر می‌کند و مطالب مبهم و پیچیده‌ی کتابی را روشن می‌سازد، برای بیان مطلب راه ساده‌تری نشان می‌دهد و نتیجه‌گیری را آسان می‌کند.
- یا خردمندی است که در برخی از کتاب‌ها به نادرستی و آشفتگی برمی‌خورد، پس نادرستی‌ها را اصلاح می‌کند، و آشفتگی‌ها را سامان می‌بخشد، با خوشبینی به کار مولف می‌نگرد، بر او خرده نمی‌گیرد، و از اینکه متوجه خطا و اشتباه دیگران شده به خویشتن نمی‌بالد."

ابوالفضل طاهری
عضو هیئت تحریریه

فهرست مطالب

قضیه‌ی اساسی جبر و اثبات جبری گاوس

دکتر امیر جعفری

حل معادلات جبری به شکل

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0 \qquad (1)$$

که $a_0, \ldots, a_n$ ضرایب عددی مشخص هستند، از دیرباز ذهن بشر را به خود مشغول کرده است. روش حل این معادلات برای معادلات درجه ۲ به زمان‌های باستان باز می‌گردد. روش کلی حل توسط ریاضی‌دان ایرانی، خوارزمی در کتاب جبر و مقابله ارائه شد. حل معادلات درجه ۳ با روش‌های هندسی توسط خیام بررسی شد. روش او حتی برای معادلات درجه ۴ نیز قابل تعمیم است ولی قادر به حل کلی این معادلات نیست. در قرن پانزده و شانزده میلادی، ریاضیدانان ایتالیایی موفق به حل کلی معادلات درجه ۳ و ۴ نیز شدند. آن‌ها برای این منظور مجبور به تعریف مجموعه‌ی بزرگتری از اعداد یعنی همان اعداد مختلط:

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\} \qquad (2)$$

شدند و عدد موهومی $i = \sqrt{-1}$ ریشه‌ی ابداعی آن‌ها برای معادله $x^2 = -1$ بود. این که آیا هر معادله‌ی جبری به شکل (۱) در این مجموعه‌ی بزرگتر از اعداد جواب دارد یا خیر، موضوع قضیه‌ی اساسی جبر است که در این نوشته به آن می‌پردازیم. حل‌ناپذیری کلی معادلات درجه بزرگتر از ۴ نیز موضوعی بسیار جذاب است که در نهایت با تلاش‌های ریاضیدانانی چون رافینی، آبل و گالوا اثبات شد. البته باید تعریفی دقیق از حل‌ناپذیری ارائه شود که از مجال این نوشته کوتاه خارج است.

با اینکه تعریف دقیق پیوستگی و خواص آن، سال‌ها طول کشید که بدست آید ولی از قرن شانزدهم برای ریاضیدانان معلوم بود که معادلات جبری از درجه فرد:

$$x^{2n+1} + a_1 x^{2n} + a_2 x^{2n-1} + \cdots + a_{2n+1} = 0 \qquad (3)$$

در اعداد حقیقی جواب دارند. دلیل ساده این امر آن است که چون جمله غالب معادله فوق x^{2n+1} است برای xهای بسیار بزرگ مثبت، عددی مثبت و برای xهای بسیار بزرگ منفی، عددی منفی خواهد بود و با توجه به خاصیت مقدار میانی توابع پیوسته باید حداقل یک صفر داشته باشد.

نکته‌ی دیگر درباره‌ی اعداد مختلط آن است که فرمول صریح $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ برای ریشه‌های معادله‌ی $ax^2 + bx + c = 0$ نشان می‌دهد که هر معادله درجه ۲ در اعداد مختلط جواب دارد.

گاوس با یک اثبات استقرایی هوشمندانه نشان داد همین دو حقیقت ساده به تنهایی کافی هستند که نشان دهیم:

قضیه اساسی جبر: هر معادله به شکل (۱) و ضرایب حقیقی در اعداد مختلط جواب دارد.

تذکر: اگر معادله (۱) ضرایب مختلط داشته باشد در صورت ضرب در مزدوج آن به معادله‌ای با ضرایب حقیقی می‌رسیم بنابراین در قضیه فوق می‌توان شرط حقیقی بودن ضرایب را حذف کرد. با ادامه استفاده از قضیه‌ی فوق می‌توان ثابت کرد که معادله (۱) قابل تجزیه به صورت

$$a_0 (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

است که $\alpha_1, \ldots, \alpha_n$ اعدادی مختلط ریشه‌های معادله (۱) خواهند بود.

گاوس در طول عمر خود، ۵ اثبات مختلف برای این قضیه ارائه داد. در واقع موضوع رساله دکتری او نیز همین قضیه بود که در سال ۱۷۹۹ به چاپ رسید. البته اثبات اولیه او دارای خلل و فرجی است که بعدها توسط استروفسکی رفع شد.

اثبات جبری گاوس

هر عدد طبیعی n را می‌توان به‌طور یکتا به صورت $2^k m$ که $k \geq 0$ و m عددی فرد است، نوشت. استقراء گاوس روی توان k است. برای $k = 0$ می‌دانیم هر معادله درجه فرد در اعداد حقیقی ریشه دارد.

اگر $f(x)$ یک معادله درجه $2^k m$ باشد گاوس معادله‌ی $F(x)$ از درجه $2^{k-1}m(2^k m - 1) = \frac{2^k m(2^k m-1)}{2} = \binom{2^k m}{2}$ را طوری می‌سازد که وجود ریشه برای آن، وجود ریشه‌ای برای $f(x)$ را نتیجه دهد. اما بنابرفرض استقرا $F(x)$ ریشه دارد و کار تمام می‌شود. روش ساختن $F(x)$ بسیار هوشمندانه است. فرض کنید در یک میدان بزرگ ریشه‌های معادله‌ی $f(x)$، $x_1, \ldots, x_n$ باشند. برای $x \in \mathbb{R}$ (یا $c \in \mathbb{C}$) تعریف کنید:

$$\alpha_{ij}(c) = x_i + x_j + c x_i x_j$$

و تعریف کنید:

$$F_c(x) = \prod_{1 \leq i < j \leq n} (x - \alpha_{ij}(c))$$

چون ضرایب $F_c(x)$ عباراتی متقارن برحسب $x_1, \ldots, x_n$ هستند بنابراین بر حسب ضرایب $f(x)$ قابل بیان بوده و در نتیجه اعدادی حقیقی هستند. بنابر فرض استقرا $F_c(x)$ حداقل یک ریشه‌ی مختلط دارد. چون بی‌نهایت انتخاب برای c داریم می‌توان دو عدد متمایز c_1 و c_2 را یافت به طوری که $i < j$ وجود داشته باشند که $x_i + x_j + c_1 x_i x_j$ و $x_i + x_j + c_2 x_i x_j$ هر دو حقیقی باشند بنابراین با حل یک دستگاه دو معادله دو مجهول (مجهول‌ها $x_i + x_j, x_i x_j$) بدست می‌آید که $x_i + x_j$ و $x_i x_j$ هردو حقیقی هستند پس چون برای $A, B \in \mathbb{R}$

$$\begin{cases} x_i + x_j = A \\ x_i x_j = B \end{cases}$$

آن‌ها ریشه‌های معادله‌ی $x^2 - Ax + B = 0$ هستند و در نتیجه اعدادی مختلط می‌باشند.
این اثبات گاوس قابل تعمیم است.

قضیه ۱. *فرض کنید p یک عدد اول داده شده باشد و K میدانی باشد که هرچندجمله‌ای با ضرایب در K که درجه‌اش نسبت به p اول است حداقل یک ریشه در K داشته باشد. فرض کنید L یک توسیع K باشد که هر معادله با ضرایب در K و درجه p در L ریشه داشته باشد. آنگاه هر معادله با ضرایب در K در L حداقل یک ریشه دارد.*

در حالتی که $p = 2$، $K = \mathbb{R}$، $L = \mathbb{C}$ همان قضیه اساسی خواهد بود.

اثبات. هر عدد n را به‌طور یکتا می‌توان بصورت $p^k m$ نوشت که $k \geq 0$ و m نسبت به p اول است. اثبات با استقرا روی k انجام می‌گیرد. $k = 0$ فرض قضیه است که هر معادله با درجه اول نسبت به p جواب دارد. اگر $f(x)$ یک معادله درجه $p^k m$ باشد یک معادله $F(x)$ از درجه

$$\binom{p^k m}{p} = \frac{p^k m(p^k m - 1)\cdots(p^k m - p + 1)}{p!} = p^{k-1}\frac{m(p^k m - 1)\cdots(p^k m - p + 1)}{(p-1)!}$$

می‌سازیم که بنابر فرض استقرا در K جواب دارد و نشان می‌دهیم این جواب، جوابی برای معادله‌ی $f(x)$ بدست می‌دهد و کار تمام می‌شود. روش ساختن $F(x)$ با تقلید از گاوس خواهد بود.

فرض کنید $x_1, \ldots, x_n$ ریشه‌های معادله $f(x)$ در یک میدان بزرگ باشند. برای هر pتایی $1 \leq i_1 < i_2 < \cdots < i_p \leq n$ و عدد $c \in K$ تعریف کنید:

$$\alpha_{i_1 \ldots i_p}(c) = \sum x_{i_k} + c \sum x_{i_k} x_{i_l} + c^2 \sum x_{i_k} x_{i_l} x_{i_q} + \cdots + c^{p-1} x_{i_p} \ldots x_{i_p}$$

(جملات جمع x_{i_n} جمع ضرب دوتایی آن‌ها، جمع ضرب سه‌تایی آن‌ها، ... تا ضرب همه آن‌ها است.)
دوباره:

$$F_c(x) = \prod (x - \alpha_{i_1 \ldots i_p}(c))$$

را تشکیل می‌دهیم که بنابرفرض استقرا ریشه‌ای در K دارد. چون شرط قضیه نتیجه می‌دهد که K نامتناهی است (چرا؟) آنگاه می‌توان اعداد متمایز $c_1, \dots, c_p$ در K یافت به طوری که $0 \le i_1 < \cdots < i_p \le n$ وجود داشته باشند که $\alpha_{i_1 \dots i_p}(c_k)$ برای $k = 1, \dots p$ در K باشند. با حل یک دستگاه p-معادله p مجهول بدست می‌آید که

$$\begin{cases} \sum x_{i_k} = A_1 \in K \\ \sum x_{i_k} x_{i_l} = A_2 \in K \\ . \\ . \\ . \\ x_{i_1} \cdots x_{i_p} = A_p \in K \end{cases}$$

بنابراین $x_{i_1}, \dots, x_{i_p}$ ریشه‌های معادله $x^p - A_1 x^{p-1} + A_2 x^{p-2} - \cdots \pm A_p = 0$ هستند که مجددا بنابرفرض قضیه جوابی در K دارد، بنابراین یکی از x_{i_k}ها در K است و این همان چیزی است که می‌خواستیم ثابت کنیم. $\square$

تمرین: فرض کنید K یک میدان باشد که هر معادله درجه p که p یک عدد اول دلخواه است، در آن حداقل یک جواب داشته باشد ثابت کنید K بسته جبری است یعنی هر معادله درجه دلخواه در آن جواب دارد. اگر از اعداد اول تنها، یک عدد اول استثنا شود می‌توان مثال نقض برای این حکم پیدا کرد.

اثبات‌هایی بر قضیه‌ی اساسی جبر

احمدرضا حاج سعیدی

چکیده

این مقاله، جمع آوری نه چندان دقیق از اثبات هایی از قضیه اساسی جبر است که سعی شده است که از ایده ها و روش های مختلفی بهره گیرد. اولین اثبات از اطلاعات کمتری نسبت به بقیه اثبات ها استفاده می کند و تنها ایده کار استقراست! در روش‌های بعدی از مفاهیم توابع مختلط، توپولوژی جبری، توپولوژی دیفرانسیل و نظریه‌ی گالوا[۱] بهره می گیریم که سعی شده است که در حد آشنایی و یادآوری، آن ها را بیان کنیم.

قضیه‌ی اساسی جبر. هر چندجمله‌ای غیرثابت باضرایب مختلط در $\mathbb{C}$ ریشه دارد.
یا به عبارتی هر چندجمله‌ای غیرثابت در $\mathbb{C}[x]$، به چندجمله‌ای‌های درجه ۱ تجزیه می‌شود .

روش ۱

نکته جالب این اثبات این است که استقرای ریاضی، اصلی ترین ایده ی آن است:

لم ۱. *اگر هر چندجمله‌ای در $\mathbb{R}[x]$ در $\mathbb{C}$ دارای ریشه باشد، قضیه‌ی اساسی جبر صحیح است.*

اثبات. فرض کنیم $p(x) \in \mathbb{C}[x]$ و $p(x) = \sum_{i=0}^{n} a_i x^i$. در این صورت تعریف می‌کنیم $\bar{p}(x) = \sum_{i=0}^{n} \bar{a}_i x^i$. مشخص است که $p(\alpha) = 0$ اگر و تنها اگر $\bar{p}(\bar{\alpha}) = 0$. به سادگی می‌توان دید که $p(x).\bar{p}(x) \in \mathbb{R}[x]$. پس $p(x).\bar{p}(x)$ ریشه‌ای مثل $\alpha \in \mathbb{C}$ دارد. لذا یکی از $p, \bar{p}$ در $\mathbb{C}$ دارای ریشه است و لذا هر دو دارای ریشه در $\mathbb{C}$ هستند. $\square$

لم ۲. *چندجمله‌ای‌های درجه ۲ و درجه فرد در $\mathbb{R}[x]$، در $\mathbb{C}$ دارای ریشه‌اند.*

اثبات. اثبات این لم ساده است و به خواننده واگذار می‌شود. $\square$

لم ۳. *اگر F یک میدان بوده و $p(x) \in F[x]$، آن‌گاه میدانی مانند E شامل F یافت می‌شود که $p(x)$ در E به چندجمله‌ای‌های درجه ۱ تجزیه می‌شود.*

اثبات. کافی است نشان دهیم میدان E شامل F یافت می‌شود که p در E ریشه دارد؛ چرا که می‌توان با تکرار این روش، $p(x)$ را تجزیه کرد. چون $F[x]$ یک U.F.D. است، می‌توان در آن $p(x)$ را به ضرب عوامل تحویل‌ناپذیر تجزیه کرد. کافی است نشان داد که دست‌کم یکی از این عوامل در توسیعی از F ریشه دارد. پس بدون کاسته شدن از کلیت می‌توان فرض کرد که چندجمله‌ای $p(x)$ در $F[x]$ تحویل‌ناپذیر است. حال اگر قرار دهیم $E = \frac{F[x]}{(p(x))}$ آن‌گاه E یک میدان خواهد بود و با در نظر گرفتن $\alpha = x+(p(x))$ داریم:

$$p(\alpha) = p(x + (p(x)) = p(x) + (p(x)) = (p(x)) = 0_E$$

لذا $p(x)$ در E ریشه دارد. $\square$

[۱] Galois Theory

حال به روش اول می‌پردازیم. اثبات را با استقرا انجام می‌دهیم. فرض کنید $p(x)$ یک چندجمله‌ای درجه d با ضرایب حقیقی باشد. با در نظر گرفتن d به صورت $۲^n(۲k+۱)$، استقرا را روی n در نظر می‌گیریم. بنا به لم ۲، این حکم برای $n=۰$ برقرار است. حال فرض کنید برای $n<N\in\mathbb{N}$، حکم برقرار باشد. بنا به لم ۳ می‌توان میدان E شامل $\mathbb{R}$ یافت به طوری که $x_۱,\dots,x_N\in E$ موجود باشد که

$$p(x)=\prod_{i=۰}^{N}(x-x_i)$$

فرض کنید $k\in\mathbb{N}$. در این صورت تعریف کنید $q_k(x)=\prod_{i<j}(x-x_i-x_j-kx_ix_j)$. می‌توان به سادگی دید که $q_k(x)$ یک چندجمله‌ای در $\mathbb{R}[x]$ است(چون ضرایب $q_k(x)$ به صورت چندجمله‌ای‌هایی حقیقی متقارن از $x_۱,\dots,x_d$ هستند و لذا می‌توان ضرایب $q_k(x)$ را به صورت حاصلضربی از ضرایب چندجمله‌ای $p(x)$ بیان کرد).

اکنون $q_k(x)$ یک چندجمله‌ای با درجه‌ی $d(d-۱)/۲$ می‌باشد و $d(d-۱)/۲=۲^{N-۱}\times(۲k+۱)(۲^N(۲k+۱)-۱)$، و لذا طبق فرض استقرا $q_k(x)$ در $\mathbb{C}$ ریشه دارد، یعنی به ازای i و jای $x_i+x_j+kx_ix_j$ عددی مختلط است.

اکنون چون k می‌تواند هر عدد طبیعی دلخواهی باشد، بنا به اصل لانه‌کبوتری، k و k' طبیعی و i,jای یافت می‌شوند که $x_i+x_j+kx_ix_j$ و $x_i+x_j+k'x_ix_j$ اعدادی مختلط‌اند و لذا x_ix_j و x_i+x_j نیز مختلط‌اند و در نتیجه x_i و x_j مختلط‌اند. پس $p(x)$ نیز ریشه‌ی مختلط دارد و حکم اثبات می‌شود.

در ۳ اثبات بعدی، از روش‌هایی در توابع مختلط استفاده می‌شود.

روش ۲

در این روش با استفاده از قضیه‌ی لیوویل، قضیه‌ی اساسی جبر را اثبات می‌کنیم.

قضیه (لیوویل[۲]): هر تابع تحلیلی و کراندار در $\mathbb{C}$، ثابت است.

اثبات این قضیه را می‌توانید در [۱] ببینید.

لم ۴. *اگر $p(z)$ یک چندجمله‌ای غیرثابت در $\mathbb{C}[x]$ باشد،*

$$\lim_{|z|\to\infty}|\,p(z)\,|=\infty$$

اثبات. فرض کنید $p(z)=\sum_{i=۰}^{n}a_iz^i$ و $a_n\neq ۰$:

$$\lim_{|z|\to\infty}|\,p(z)\,|=\lim_{|z|\to\infty}z^n\,|\,a_n+\frac{a_{n-۱}}{z}+\cdots+\frac{a_۰}{z^n}\,|=\infty\times|\,a_n\,|=\infty$$

□

حال به اثبات روش دوم می‌پردازیم.

فرض کنید $p(z)$ در $\mathbb{C}$ ریشه نداشته باشد. لذا $p(z)$ و $\frac{۱}{p(z)}$ هر دو روی $\mathbb{C}$ تحلیلی‌اند. پس

$$\lim_{|z|\to\infty}|\,\frac{۱}{p(z)}\,|=۰$$

پس به ازای $R>۰$ برای $|\,z\,|>R$ باید $۱>|\,p(z)\,|$ و در نتیجه $p(z)$ روی $|\,z\,|>R$ کراندار است. از طرفی $\frac{۱}{p(z)}$ در ناحیه فشرده‌ی $|\,z\,|\leq R$ نیز کراندار است. پس $\frac{۱}{p(z)}$ در کل $\mathbb{C}$ کراندار است پس بنا بر قضیه لیوویل $\frac{۱}{p(z)}$ و در نتیجه $p(z)$ تابعی ثابت است که تناقض است.

---
[۲] Liouville

روش ۳

در این روش از قضیه‌ی روشه استفاده می‌شود.
قضیه (روشه[۳]): فرض کنید f و g دو تابع تحلیلی درون یک مجموعه‌ی باز که شامل دایره‌ی C و درون آن است، باشد. اگر برای هر $z \in C$، $|g(z)| < |f(z)|$ در این صورت تعداد ریشه‌های f و $f+g$ (با حساب تکرر) درون دایره‌ی C برابرند.

اثبات این قضیه را می‌توانید در [۱] ببینید.

حال به کمک این قضیه اثباتی برای قضیه‌ی اساسی جبر ارائه می‌دهیم.

با فرض $f(z) = \sum_{i=0}^{n} a_i z^i$ و $R > \max(2\frac{\sum_{i=0}^{n-1}|a_i|}{|a_n|}, 1)$ و $g(z) = -\sum_{i=0}^{n-1} a_i z^i$ به سادگی دیده می‌شود که فرض قضیه‌ی روشه برای f و g روی دایره به مرکز ۰ و شعاع R برقرار است لذا f و $f+g = a_n z^n$ درون این دایره به یک تعداد ریشه دارند یعنی f، n ریشه دارد.

روش ۴

این روش نیز از مفاهیم توابع مختلط و توپولوژی جبری بهره می‌گیرد.

اگر D زیرمجموعه ای از $\mathbb{C}$ باشد، دو خم بسته ی γ_1 و γ_2 از بازه $[0,1]$ به D را هوموتوپ می گوییم اگر تابع پیوسته $h : [0,1] \times [0,1] \to D$ موجود باشد که $h(x,0) = \gamma_1(x)$ و $h(x,1) = \gamma_2(x)$.

لم ۵. *دو خم بسته‌ی هموتوپ[۴] در $\mathbb{C}\backslash\{0\}$ دارای یک عدد چرخش حول صفر هستند.*

لم ۶. *اگر γ_1 و γ_2 دو خم بسته در $\mathbb{C}\backslash\{0\}$ باشند که روی $[0,1]$ تعریف شده‌اند و $|\gamma_2(t)| < |\gamma_1(t)|$ برای هر $t \in [0,1]$، آن‌گاه عدد چرخش γ_1 و $\gamma_1 + \gamma_2$ حول صفر یکسان است.*

برای دیدن اثبات این دو لم به [۲] مراجعه کنید.

به کمک این دو لم می‌توانیم اثبات دیگری برای قضیه ارائه دهیم. فرض کنید $p(z) = \sum_{i=0}^{n} a_i z^i$ و $g(z) = -\sum_{i=0}^{n-1} a_i z^i$. مانند اثبات روش سوم، می‌توان $R > 0$ای یافت که برای $|z| \geq R$، $|g(z)| < |p(z)|$. پس با فرض $\gamma_1, \gamma_2 : [0,1] \to \mathbb{C}$، $\gamma_1(t) = p(Re^{2\pi it})$ و $\gamma_2(t) = g(Re^{2\pi it})$، γ_1 و γ_2 در شرایط لم ۶ صدق می‌کنند و لذا $\gamma_1(t)$ و $(\gamma_1+\gamma_2)(t) = a_n R^n e^{2\pi int}$ عدد چرخش یکسان، n، دارند. اگر $p(z)$ دارای ریشه در $\mathbb{C}$ نباشد،

$$h : [0,1] \times [0,1] \to \mathbb{C}\backslash\{0\}$$

$$(t,s) \to p(Rse^{2\pi it})$$

یک هموتوپی بین γ_1 و خم ثابت $p(0)$ است و لذا γ_1 باید عدد چرخش صفر داشته باشد که این تناقض است.

روش ۵

در این اثبات، از روش‌هایی در توپولوژی دیفرانسیل بهره می‌گیریم.

منظور از یک خمینه، یک زیر مجموعه از فضای اقلیدسی است که به طور موضعی وابرسان[۵] با زیرمجموعه‌های باز از فضای اقلیدسی است.

اگر M و N دو خمینه‌ی هموار و هم‌بعد در فضای اقلیدسی باشند و $f : M \to N$ هموار باشد:

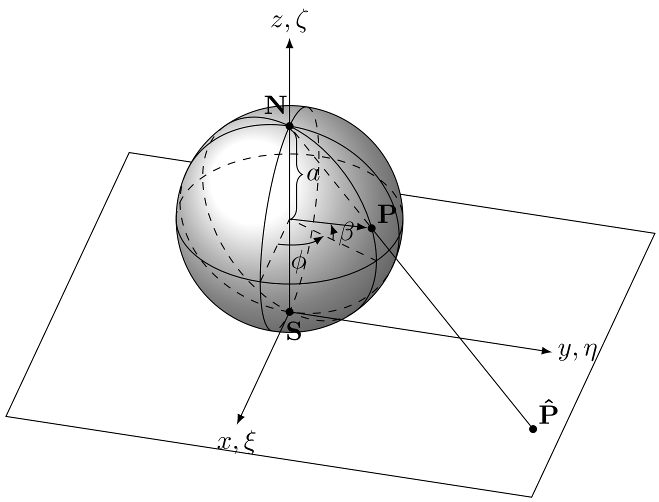
۱) $x \in M$، نقطه‌ی عادی f نامیده می‌شود اگر $\mathrm{df_x}$ یک‌به‌یک و پوشا باشد؛ در غیر این صورت این نقطه بحرانی نامیده می‌شود.

[۳] Rouché
[۴] homotopic
[۵] diffeomorphic

۲) $y \in N$ را مقدار عادی می‌نامیم اگر هیچ یک از اعضای $f^{-1}(y)$ نقطه‌ی بحرانی نباشد در غیر این صورت به آن مقدار بحرانی نامیده می‌گوییم.

لم ۷. *اگر M خمینه‌ای هموار و فشرده در $\mathbb{R}^n$ و N خمینه‌ای هموار در $\mathbb{R}^n$ باشد و $f : M \to N$ تابعی هموار باشد، آن‌گاه $\#f^{-1}(y)$ ($\#A$ نشان دهنده‌ی تعداد اعضای مجموعه‌ی A است) روی مجموعه‌ی مقادیر عادی f متناهی و موضعا ثابت است.*

اثبات این لم را می‌توانید در [۳] ببینید. حال به کمک این لم اثباتی دیگر برای قضیه‌ی اساسی بیان می‌کنیم.
می‌توان $\mathbb{C}$ را با زیرمجموعه‌ی $\mathbb{R}^2 \times \{0\}$ از $\mathbb{R}^3$ یکسان گرفت. ($(x+iy \mapsto (x,y,0)$) فرض کنید $p(z)$ یک چندجمله‌ای باشد. همچنین می‌توان فرض کرد $p(z) : \mathbb{R}^2 \times \{0\} \to \mathbb{R}^2 \times \{0\}$. اکنون فرض کنید $p(z)$ در $\mathbb{C}$ یا در همان $\mathbb{R}^2 \times \{0\}$ ریشه نداشته باشد. نگاشت کنج‌نگاری از قطب شمال را $h_N : S^2 - N \to \mathbb{R}^2 \times \{0\}$ که $N = (0,0,1)$ در نظر بگیرید. (نگاشت کنج‌نگاری[۶] ، نگاشتی است که هر نقطه‌ی غیر از N در S^2 را به نقطه‌ای در $\mathbb{R}^2 \times \{0\}$ می‌برد به طوری که این دو نقطه و N در یک امتداد باشند)



به طور مشابه نگاشت کنج‌نگاری از قطب جنوب را تعریف می‌کنیم و با h_S نمایش می‌دهیم. تابع $f : S^2 \to S^2$ را به صورت زیر تعریف می‌کنیم:

$$f(x) = \begin{cases} N & x = N \\ h_N^{-1} p h_N(x) & x \neq N \end{cases}$$

به راحتی می‌توان دید که h_N یک وابرسانی است و لذا h_N و h_N^{-1} هموار است. پس تابع f در $S^2 - N$ هموار است. اما f در N نیز هموار است. برای دیدن این موضوع تعریف کنید:

$$\phi : \mathbb{R}^2 \times \{0\} \to \mathbb{R}^2 \times \{0\}$$

$$z \mapsto h_S f h_S^{-1}(z)$$

می‌توان دید که $\phi(z) = \frac{z^n}{\sum_{i=0}^{n} \bar{a}_{n-i} z^i}$ (توجه کنید که $p(z) = \sum_{i=0}^{n} a_i z^i$ بود.) پس ϕ در همسایگی ۰ هموار است و لذا $f = h_S^{-1} \phi h_S$ در N هموار است. پس $f : S^2 \to S^2$ هموار است.
از آن‌جا که برد $p(z)$ شامل صفر نیست پس برد f شامل S (که $S = (0,0,-1)$ قطب جنوب است.) نیست. لذا S مقدار عادی است.
اگر $x \neq N$ آن‌گاه $\mathrm{df_x} = (\mathrm{dh_N^{-1}})_{\mathrm{p(h_N(x))}} \mathrm{o} (\mathrm{dp})_{\mathrm{h_N(x)}} \mathrm{o} (\mathrm{dh_N})_{\mathrm{x}}$ پس از آن‌جا که h_N موضعا وابرسانی است $\mathrm{df_x}$ تنها در نقاط متناظر با ریشه‌های $p'(z)$، یک‌به‌یک و پوشا نیست. پس f متناهی نقطه‌ی بحرانی دارد. لذا نقاط عادی (نقاطی که بحرانی نیستند!) f از حذف متناهی نقطه‌ی S^2 به وجود می‌آیند و لذا باز و همبند هستند. پس $\#f^{-1}(y)$ روی مجموعه مقادیر عادی باید مقداری ثابت باشد اما $\#f^{-1}(S) = 0$. یعنی برد f شامل متناهی نقطه است و این یعنی برد f متناهی است که غلط است.

[۶] Stereographic projection

روش ۶

این اثبات نیز از توپولوژی دیفرانسیل استفاده می‌کند. در این اثبات از درجه یک نگاشت هموار میان دو خمینه ی "جهت پذیر"[۷] و قضایا مربوط به آن استفاده می کنیم. برای هر نقطه ی x از خمینه ی n-بعدی هموار M ، می توان زیرفضایی خطی(مماس) n-بعدی از فضای اقلیدسی شامل خمینه، تعریف کرد که فضای مماس بر M در نقطه ی x نامیده می شود و با T_xM نشان داده می شود. اگر بتوان به طور هموار! پایه ای برای فضاهای مماس(T_xM) پیدا کرد این خمینه را جهت پذیر می‌نامیم. برای اطلاعات بیش‌تر مرجع [۶] توصیه می‌شود.

تعریف ۸. *اگر $f : M \to N$ نگاشتی هموار میان دو خمینه هم‌بعد و جهت‌دار M و N باشد و M فشرده و N همبند است. فرض کنید $y \in N$ مقداری عادی باشد.در این صورت اگر $x \in f^{-1}(y)$، می‌گوییم $\mathrm{df_x}$ جهت نگهدار است، اگر این نگاشت پایه القا شده از جهت M روی T_xM به پایه‌ای هم‌جهت با پایه‌ی القایی از جهت N روی $T_{f(x)}N$ ببرد؛ در غیر این صورت آن را جهت برگردان می‌نامیم. درجه‌ی نگاشت f یا $deg f$ برابر است با تعداد نقاط $x \in f^{-1}(y)$ که $\mathrm{df_x}$ جهت نگهدار است منهای تعداد بقیه نقاط $f^{-1}(y)$.*

می‌توان نشان داد که این تعریف مستقل از مقدار عادی $y \in N$ است که در ابتدا انتخاب شد.

لم ۹. *فرض کنید M و N دو خمینه با شرایط قید شده در تعریف بالا باشند و $f, g : M \to N$ دو نگاشت هموار بگیرید. در این صورت اگر f, g هوموتوپ باشند آنگاه $deg(f) = deg(g)$.*

لم ۱۰. *فرض کنیم N و M خمینه با شرایط فوق باشند و $f : M \to N$ نگاشتی هموار باشد. اگر M مرز خمینه ای مانند X باشد و گسترشی هموار مانند $F : M \to N$ از $f : M \to N$ وجود داشته باشد، در این صورت $deg(f) = 0$.*

اکنون فرض کنیم $p(x) = x^n + \cdots + a_1x + a_0$ یک چندجمله ای درجه $n > 0$ مختلط باشد که در $\mathbb{C}$ ریشه ندارد. اگر $R > 0$ را مانند روش ۳ در نظر بگیریم، در این صورت با فرض این که B_R, S_R کره و گوی بسته به شعاع R حول 0 باشند. دقت کنید که S_R مرز خمینه ی B_R است. فرض کنید

$$H : S_R \times [0,1] \to S_1$$

$$H(x,t) = \frac{p(x) - t \times (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)}{| p(x) - t \times (a_{n-1}x^{n-1} + \cdots + a_1x + a_0) |}$$

پس دو نگاشت

$$f : S_R \to S_1, f(x) = p(x)$$

و

$$g : S_R \to S_1, g(x) = \frac{x^n}{R^n}$$

هوموتوپ هستند. لذا چون نگاشت $\mathrm{dg_x}$ برای هر $x \in S_R$ جهت نگهدار است پس $deg(f) = deg(g) = n$. از طرفی نگاشت

$$F : B_R \to S_1 \text{،} F(x) = p(x)$$

گسترشی هموار از نگاشت f است. بنابراین $deg(f) = 0$ که این یک تناقض است. پس $p(x)$ در $\mathbb{C}$ ریشه دارد.

روش ۷

اکنون روشی جبری برای اثبات قضیه‌ی اساسی جبر به کار می‌گیریم. در این روش از مفاهیم نظریه‌ی گالوا بهره می‌گیریم. اگر E و F دو میدان باشند، به طوری که $F \subset E$ آنگاه E توسیع میدانی از F نامیده می شود . این توسیع میدانی را توسیع جبری می نامیم، اگر هر عضو E ریشه یک چندجمله ای در $F[x]$ باشد. اگر $X \subset F[x]$، توسیع میدانی E را میدان شکافنده[۸] X می‌نامیم

[۷] orientable
[۸] Spliting field

اگر اعضای X روی E تجزیه شوند و این میدان یک میدان مینیمال نسبت به این ویژگی باشد. میدان N را بستار نرمال از توسیع جبری میدان E روی F می‌نامیم، اگر N میدان شکافنده‌ی مجموعه‌ی $\{min(F,a) : a \in E\}$ باشد که منظور ما از $min(F,a)$ چندجمله‌ای مینیمال a روی F است. بعد توسیع میدانی E به عنوان یک میدان برداری روی F را با $[E : F]$ نمایش می‌دهیم و درجه ی این توسیع میدانی می‌نامیم. همچنین $Gal(E/F)$ را گروه تمام اتومورفیسم‌های E می‌گیریم که روی F همانی هستند.

یک توسیع متناهی E/F را گالوا می‌نامیم هرگاه هر عنصری از E که توسط تمامی اتومورفیسم‌ها متعلق به $Gal(E/F)$ ثابت نگاه داشته شود در F واقع باشد.

برای آشنایی با ابزارهای این اثبات مطالعه [۴] توصیه می‌شود.

لم ۱۱. *میدان $\mathbb{R}$ توسیع غیربدیهی با درجه‌ی فرد ندارد.*

اثبات. اگر $E \neq \mathbb{R}$ توسیع میدانی $\mathbb{R}$ باشد و $[E : \mathbb{R}]$ فرد باشد؛ با فرض $a \in E\backslash\mathbb{R}$، $[\mathbb{R}(a) : \mathbb{R}]$ نیز فرد خواهد بود. پس $\min(\mathbb{R}, a)$ چندجمله‌ای درجه فرد و تحویل‌ناپذیر روی $\mathbb{R}$ خواهد بود. اما طبق لم ۲ این ناممکن است. $\square$

لم ۱۲. *هیچ توسیع میدانی با درجه‌ی ۲ از $\mathbb{C}$ موجود نیست.*

اثبات. اگر چنین توسیعی موجود باشد باید به فرم $\mathbb{C}(a)$ باشد و $[\mathbb{C}(a) : \mathbb{C}] = ۲$. اما در این صورت a باید ریشه‌ی یک چندجمله‌ای درجه ۲ با ضرایب در $\mathbb{C}$ باشد که در نتیجه a یک عدد مختلط است و $\mathbb{C}(a) = \mathbb{C}$. بنابراین چنین توسیعی وجود ندارد. $\square$

حال می‌توانیم اثباتی جبری ارائه کنیم.

فرض کنید N بستار نرمال $\mathbb{C}/\mathbb{R}$ باشد. می‌توان نشان داد که در این صورت به دلیل آن‌که مشخصه‌ی $\mathbb{R}$ صفر است $N/\mathbb{R}$ یک توسیع گالواست و بنابراین می‌توان از احکام مربوط به توسیع‌های گالوایی که در مرجع [۴] آمده‌اند استفاده کرد. اگر نشان دهیم $N = \mathbb{C}$ حکم ثابت شده است. فرض کنید $G = Gal(N/\mathbb{R})$. در این صورت

$$| G |= [N : \mathbb{R}] = [N : \mathbb{C}].[\mathbb{C} : \mathbb{R}] = ۲[N : \mathbb{C}]$$

پس $| G |$ زوج است. فرض کنید P یک زیرگروه ۲-سیلوی G باشد و E میدان ثابت P باشد. بنابراین $[G : P]$ فرد است و از طرفی $[G : P] = [E : \mathbb{R}]$. اما مطابق لم ۱۱ باید $E = \mathbb{R}$. پس $G = P$ و لذا G یک ۲-گروه است. چون $Gal(N/\mathbb{C}) \leq Gal(N/\mathbb{R})$ پس $Gal(N/\mathbb{C})$ نیز یک ۲-گروه است. اگر M زیرگروه سره ماکسیمالی از $Gal(N/\mathbb{C})$ باشد، داریم $[Gal(N/\mathbb{C}) : M] = ۲$. اگر T میدان ثابت M باشد در این صورت $[T : \mathbb{C}] = ۲$. اما این با لم ۱۲ در تناقض است. پس $| Gal(N/\mathbb{C}) |= ۱$، یعنی $N = \mathbb{C}$.

مراجع

[1] Elias M. Stein, Rami Shakarchi, Complex Analysis, 2009.

[2] Henri Cartan, Elementary Theory of Analytic Functions of One Or Several Complex Variables, 1995.

[3] John Willard Milnor, Topology from the Differentiable Viewpoint, 1997.

[4] Patrick Morandi, Field and Galois Theory, 1996.

[5] http://planetmath.org/encyclopedia/ProofOfFundamentalTheoremOfAlgebra2.html

[6] Ian Pollack, Victor Guillemin, Differential Topology, 2010.

نرم‌های کاهش‌یافته از جبرهای ساده روی میدان توابع
گردآوری: ابوالفضل طاهری

چکیده

این مقاله بر اساس مرجع [۱] تنظیم شده‌است و هدف آن بررسی نرم کاهش‌یافته از جبرهای ساده روی میدان توابع[۱] است. توصیفی از گروه تمام نرم‌های کاهش یافته برای میدان‌های کج از توابع گویای ناجابه‌جایی در دست است. در این مقاله می‌خواهیم از آن استفاده کنیم و گروه وایتهد از یک جبر ساده متناهی‌البعد روی میدان دلخواه و از اندیس دلخواه را توصیف کنیم.

۱ مقدمات مورد نیاز

مطالب این بخش از مراجع [۲]، [۳]، [۴]، [۵]، [۶] و [۷] انتخاب شده است. بخش‌های ۳.۱، ۴.۱ و ۵.۱ به طور کامل از [۷] انتخاب شده است.

۱.۱ مدول‌ها و جبرها

تعریف ۱.۱. فرض کنید R حلقه‌ای یکدار و نابدیهی باشد و M مجموعه‌ای ناتهی. مجموعه‌ی M را، همراه با عمل جمع $+ : M \times M \to M$ و ضرب اسکالر $. : R \times M \to M$، R-مدول چپ می‌گوییم اگر:

- $(M, +)$ گروهی آبلی باشد.
- به ازای هر دو عضو از M مثل xو y و هر عضو از R مثل r، $r(x+y) = rx + ry$.
- به ازای هر عضو از M مانند x و هر دو عضو از R مانند r و s، $(r+s)x = rx + sx$.
- به ازای هر عضو از M مانند x و هر دو عضو از R مانند r و s، $(rs)x = r(sx)$.
- به ازای هر عضو از M مثل x، $1x = x$.

مانند تعریف R-مدول چپ، می‌توانیم R-مدول راست را نیز تعریف کنیم. به عنوان مثال هر گروه آبلی یک $\mathbb{Z}$-مدول است.

تعریف ۲.۱. فرض کنید M، R-مدول باشد و N زیرمجموعه‌ای ناتهی از آن باشد. می‌گوییم N زیرمدول M است و می‌نویسیم $N \leq M$، اگر تحدید عمل جمع M به $N \times N$ و تحدید ضرب در اسکالر M به $R \times N$ به ترتیب عمل جمع روی N و ضرب در اسکالر روی N به وجود آورد و به علاوه، N با این عمل جمع و ضرب در اسکالر، R-مدول باشد.

[۱] Function Fields

تعریف ۳.۱. فرض کنید C یک حلقه‌ی جابه‌جایی باشد. یک C-جبر یک حلقه‌ی R است که یک ساختار C-مدولی دارد به طوری که ضرب در اسکالر آن دارای خواص زیر نیز می‌باشد:

$$\forall c \in C, r_1, r_2 \in R, \quad c(r_1r_2) = (cr_1)r_2 = r_1(cr_2)$$

به طور مثال هر حلقه‌ی R یک $\mathbb{Z}$-جبر است.

ساختار جبرها بسیار شبیه حلقه‌ها می‌باشد. اگر R یک C-جبر باشد و A یک ایده‌آل R باشد در این صورت A یک زیرمدول R خواهد بود. بنابراین حلقه‌ی R/A در واقع یک ساختار C-جبر است. به علاوه هر تصویر هومومورفیک از R به صورت طبیعی ساختار C-جبر دارد.

مرکز حلقه‌ی R را تعریف کنید:

$$Z(R) = \{z \in R : rz = zr, \forall r \in R\}$$

با این تعریف، $Z(R)$ زیرحلقه‌ای از R است و R یک جبر روی هر زیرحلقه‌ی $Z(R)$ خواهدبود. برعکس اگر R یک C-جبر باشد، یک هومومورفیسم حلقه‌ای کانونیک مانند $\phi : C \to Z(R)$ که با $\phi(c) = c1$ مشخص می‌شود، وجود دارد.

فرض کنید $A \subset R$ باشد. مرکزساز A در R را به صورت زیر تعریف می‌کنیم

$$C_R(A) = \{r \in R : ra = ar, \forall a \in A\}$$

با این تعریف $C_R(A)$ زیرحلقه‌ای از R است.

گزاره ۴.۱. هر زیرحلقه‌ی ماکسیمال جابه‌جایی C از R مرکزساز خودش است.

اگر C یک میدان باشد در این صورت چون $ker\phi \lhd C$ بنابراین $ker\phi = 0$، پس می‌توانیم C را به عنوان زیرحلقه‌ای از R در نظر بگیریم.

تعریف ۵.۱. حلقه‌ی R را ساده می‌گوییم اگر هیچ ایده‌آل نابدیهی، سره دوطرفه‌ای نداشته‌باشد و یک جبر را ساده می‌گوییم اگر به عنوان یک حلقه ساده باشد.

تعریف ۶.۱. فرض کنید R یک جبر روی میدان k باشد بنابراین $k \subset Z(R)$. اگر $k = Z(R)$ می‌گوییم R یک جبر مرکزی روی k است و اگر R ساده و مرکزی باشد می‌گوییم یک جبر ساده‌ی مرکزی روی k است.

۲.۱ همریختی‌ها

هم‌ریختی بین مدول‌ها نیز مانند حلقه‌ها و گروه‌ها تعریف می‌شود.

تعریف ۷.۱. فرض کنید M و N دو R-مدول باشند. تابع $\phi : M \to N$ را R-هم‌ریختی می‌نامیم هرگاه

۱. برای هر $x, y \in M$، $\phi(x+y) = \phi(x) + \phi(y)$

۲. برای هر $x \in M$ و هر $r \in R$، $\phi(rx) = r\phi(x)$

اگر دو R-مدول M و N داده شده‌باشند، هر R-هم‌ریختی مثل $\phi : M \to N$ که پوشا هم باشد R-بروریختی نامیده می‌شود. اگر یک به یک باشد، R-تک‌ریختی نامیده می‌شود. اگر هم یک به یک و هم پوشا باشد در این صورت به آن R-یک‌ریختی می‌گوییم و M و N را یک‌ریخت می‌گوییم.

۳.۱ دنباله‌های دقیق

تعریف ۸.۱. یک جفت از هم‌ریختی‌های $A \xrightarrow{f} B \xrightarrow{g} C$ در B دقیق است اگر $Im(f) = Ker(g)$. یک دنباله $\cdots \to A_{i-1} \to A_i \to A_{i+1} \to \cdots$ دقیق است اگر برای هر A_i بین دو هم‌ریختی دقیق باشد.

قضیه ۹.۱. یک دنباله $0 \to A \xrightarrow{f} B$ دقیق است اگر وتنها اگر f یک به یک باشد. همچنین، یک دنباله $B \xrightarrow{g} C \to 0$ دقیق است اگر وتنها اگر g پوشا باشد.

اثبات. دقیق بودن در A نتیجه می‌دهد که $Ker(f)$ با تصویر هم‌ریختی $0 \to A$ برابر باشد، که صفر است. این با یک‌به‌یک بودن هم‌ریختی f هم‌ارز است.
به طریق مشابه، هسته هم‌ریختی $C \to 0$ برابر است با C، و $g(B) = C$ اگر و تنها اگر g پوشا باشد □

نتیجه ۱۰.۱. یک دنباله $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ دقیق است اگر و تنها اگر fیک‌به‌یک باشد، g پوشا باشد، و $Im(f) = Ker(g)$. می‌گوییم B یک گسترش[۲] از C توسط A است. این دنباله دقیق را یک دنباله دقیق کوتاه [۳] می‌نامیم.

مثال ۱۱.۱. دو $\mathbb{Z}$-مدول $A = \mathbb{Z}$ و $C = \mathbb{Z}/n\mathbb{Z}$، داده‌شده‌است که با آن‌ها می‌توان دو دنباله‌های دقیق کوتاه متفاوت ساخت.
اول، $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 0$ که $f(a) = (a, 0)$ و $g(a, c) = c$.

$\mathbb{Z}$-مدول $\mathbb{Z}$همچنین یک گسترش از$\mathbb{Z}/n\mathbb{Z}$به$\mathbb{Z}$است. دنباله $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{p} \mathbb{Z}/n\mathbb{Z} \to 0$ در نظر بگیرید، که نگاشت n، z را به nz می‌فرستد، در حالی که p نگاشت تصویر است. توجه داشته‌باشید که حتی هرچند A و C در مثال مدول‌های مشابه‌ای هستند، $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ با$\mathbb{Z}$یک‌ریخت نیست. اهمیت دنباله دقیق کوتاه از آن‌جا ناشی می‌شود که می‌توانیم دنباله دقیق بلند را به دنباله‌های کوتاه دقیق بشکنیم. در یک دنباله دقیق از R-مدول ها

$$\cdots \to A_{n+2} \to A_{n+1} \to A_n \to A_{n-1} \to A_{n-2} \to \cdots$$

اگر

$$C_n \cong Ker(A_n \to A_{n-1}) \cong Im(A_{n+1} \to A_n)$$

آنگاه یک دیاگرام جابه‌جایی به صورت زیر بدست می‌آوریم، در حالی که همه‌دنباله های مورب یک دنباله کوتاه دقیق هستند:

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 & & 0 \arrow[dr] & & 0 & & \\
 & & & C_{n+1} \arrow[ur] \arrow[dr] & & & & C_{n-1} \arrow[ur] \arrow[dr] & & & \\
\cdots \arrow[rr] & & A_{n+2} \arrow[ur] \arrow[rr] & & A_{n+1} \arrow[rr] \arrow[dr] & & A_n \arrow[ur] \arrow[rr] & & A_{n-1} \arrow[rr] \arrow[dr] & & \cdots \\
 & C_{n+2} \arrow[ur] & & & & C_n \arrow[ur] \arrow[dr] & & & & C_{n-2} \arrow[dr] & \\
0 \arrow[ur] & & & & 0 \arrow[ur] & & 0 & & & & 0
\end{tikzcd}$$

درنتیجه، جمله‌های میانی، دنباله‌های دقیق کوتاه که در اینجا هم‌پوشانی دارند، به شکل یک دنباله دقیق است.

تعریف ۱۲.۱. اگر $0 \to A \to B \to C \to 0$ و $0 \to A' \to B' \to C' \to 0$ دو دنباله کوتاه دقیق از مدول ها هستند. یک هم‌ریختی از دنباله‌های کوتاه دقیق یک سه‌تایی f, g, h از همریختی مدول‌ها است بطوریکه دیاگرام زیر جابه‌جایی می‌شود:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & B \arrow[r] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

[۲] Extension
[۳] Short Exact Sequence

اگر f, g, h همه یک‌ریختی باشند، آنگاه این یک‌ریختی از دنباله‌های کوتاه دقیق است، که B و B' گسترش‌های یک‌ریختی هستند.دو دنباله دقیق هم‌ارز هستند اگر:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\approx"'] & B \arrow[r] \arrow[d, "\approx"'] & C \arrow[r] \arrow[d, "\approx"'] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

تعریف ۱.۱۳. اگر $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ دنباله کوتاه دقیق ازR-مدول‌ها است. می‌گوییم دنباله می‌شکافد[۴]، اگر هم‌ارز باشد با $0 \to A \longrightarrow A \oplus C \longrightarrow C \to 0$. یک نگاشت $s : C \to B$ را یک مقطع[۵] از g می‌نامیم اگر $gos = id$. اگر s یک چنین هم‌ریختی باشد، آن‌گاه دنباله‌ی کوتاه دقیق مذکور می‌شکافد.

شکافته شدن با یکی از صورت‌های زیر هم‌ارز است:
(a) یک هم‌ریختی $p : B \to A$ وجود دارد که $pof = 1 : A \to A$.
(b) یک هم‌ریختی $s : C \to B$ وجود دارد که $gos = 1 : C \to C$.

مثال ۱.۱۴. دو دنباله دقیق می‌سازیم که هم‌ارز نباشد. بنا بر تعریف دنباله کوتاه دقیق $0 \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ می‌شکافد. درمقابل، دنباله $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ نمی‌شکافد زیرا یک هم‌ریختی نابدیهی از $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ ندارد. بنابراین این دو دنباله‌ی دقیق کوتاه هم‌ارز نیستند.

۱.۴ تانسور مدول‌ها

تعریف ۱.۱۵. برای حلقه جابه‌جایی R، اگر M مدول راست باشد، و N مدول چپ باشد. ضرب تانسوری $M \otimes N$ روی R یک گروه آبلی $M \times N$است به طوری که که:

$$(m_1 + m_2, n) \sim (m_1, n) + (m_2, n)$$

$$(m, n_1 + n_2) \sim (m, n_1) + (m, n_2)$$

$$(mr, n) \sim (m, rn)$$

برای هر $m, m_1, m_2 \in M$ و $r \in R$.

قضیه ۱.۱۶. اگر L, M, N مدول‌های راست باشند، وD مدول چپ باشد. اگر

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} 0$$

دقیق است،آنگاه دنباله ایجادشده از گروه‌های آبلی

$$L \otimes_R D \xrightarrow{\psi \otimes 1} M \otimes_R D \xrightarrow{\varphi \otimes 1} N \otimes_R D \to 0$$

دقیق است.

[۴] Split
[۵] Section

اثبات. برای نشان دادن پوشایی $1 \otimes \varphi$، می‌دانیم که φ پوشا است. آنگاه برای تعدادی $m \in M, n = \varphi(m)$. اما $n \otimes d = \varphi(m) \otimes d = \varphi(m \otimes d) \otimes 1$. این یعنی این که $(\varphi \otimes 1)$ یک همریختی پوشا از $M \otimes D$ به $N \otimes D$، است، موقعی که گروه‌های آبلی هستند. برای دقیق بودن در $M \otimes_R D$، آن کافی است تا نشان دهیم $\pi : M \otimes D/Im(\psi \otimes 1) \to N \otimes D$ یک یک‌ریختی است. برای ساختن معکوس π یک نگاشت به صورت زیر را تعریف می‌کنیم:

$$p : N \times D \to M \otimes D/Im(\psi \otimes 1)$$

به وسیله $p(n, d) = m \otimes d$ بطوریکه $\varphi(m) = n$. اگر $\varphi(m) = \varphi(m') = n$، آنگاه $m - m' = \psi(l)$ برای هر $l \in L$ باتوجه به دقیق بودن در M. این دلالت می‌کند به این که $m \otimes d - m' = (m - m') \otimes \otimes d = \psi(l) \otimes d \in Im(\psi \otimes 1)$، بنابراین p خوش‌تعریف است.زمانی که p روی هر کلاس هم‌ارزی ثابت است، p القاء می‌کند $p' : N \otimes D \to M \otimes D/Im(\psi \otimes 1)$، یک هم‌ریختی و معکوس π است. $\square$

تعریف ۱.۱۷. یک R-مدول چپ D رایکدست [۶] می‌نامیم اگر آن یکی از دو شرط معادل زیر را داشته‌باشد:

(۱) برای هر مدول راست L, M, N اگر

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

دقیق است، آنگاه

$$0 \to L \otimes D \xrightarrow{\psi \otimes 1} M \otimes D \xrightarrow{\varphi \otimes 1} N \otimes D \to 0$$

دقیق است.

(۲) برای هر مدول راست L, M اگر ψ یک‌به‌یک باشد،آنگاه $1 \otimes \psi$ یک‌به‌یک است.

در نتیجه، برای هر چپ R-مدول D ، تابعگون[۷] $- \otimes D$ از رسته‌ی R-مدول‌های راست به رسته‌ی گروه‌های آبلی از راست دقیق است، این تابعگون دقیق است اگر و تنها اگر D مدولی یکدست باشد.اینجا به بیان تعدادی نتیجه می‌پردازیم:

نتیجه ۱.۱۸. (۱) برای هر R-مدول چپ D ،

$$\mathbb{Z} \otimes_{\mathbb{Z}} D = D$$

(۲) برای هر $m, n \in \mathbb{Z}$

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$$

که d، ب.م.م برای m و n است.

(۳) اگر M, M' R-مدول راست باشند و اگر N, N' R-مدول چپ باشند. آنگاه یک R-یک‌ریختی کانونیک وجود دارد

$$(M \otimes M') \otimes_R N \cong (M \otimes_R N) \otimes (M' \otimes N)$$

به طوری که $(m, m') \otimes n \longmapsto (m \otimes n, m' \otimes n)$. بطور مشابه R-یک‌ریختی $M \otimes_R (N \otimes N') \cong (M \otimes_R N) \otimes_R N'$ تعریف می‌شود.

[۶] Flat
[۷] Functor

۵.۱ مدول تصویری

اگر R یک حلقه یک‌دار باشد، و اگر $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ یک دنباله کوتاه دقیق از R-مدول‌ها باشد. یک همریختی R-مدولی f از D به L وقتی که با ψ ترکیب شود، همان‌گونه که در نمودار زیر می‌بینیم یک همریختی R-مدولی از D به M به‌دست می‌دهد.

$$\begin{tikzcd} D \arrow[d, "f"'] \arrow[dr, dotted, "f'"] & \\ L \arrow[r, "\psi"] & M \end{tikzcd}$$

بنابراین ψ یک هم‌ریختی بین گروه‌های آبلی بصورت زیرالقاء می‌کند:

$$\psi' : Hom_R(D, L) \to Hom_R(D, M)$$

$$f \to f' = \psi o f$$

به طور مشابه، φ هم یک نگاشت

$$\varphi' : Hom_R(D, M) \to Hom_R(D, N)$$

القا می‌کند.

قضیه ۱۹.۱. اگر D, L, M هریک R-مدول باشند. $\psi : L \to M$، نگاشت $\psi' : Hom_R(D, L) \to Hom_R(D, M)$ را القاء می‌کند. اگر $\psi : L \to M$ یک‌به‌یک باشد، آنگاه ψ' هم یک‌به‌یک است، به عبارت دیگر اگر $0 \to L \xrightarrow{\psi} M$ دقیق باشد، آنگاه $0 \to Hom_R(D, L) \xrightarrow{\psi'} Hom_R(D, M)$ هم دقیق است.

اثبات. اگر f, g دو هم‌ریختی متمایز در $Hom_R(D, L)$ باشند. ترکیب $\psi o f, \psi o g : D \to M$ را درنظر می‌گیریم. زمانی که ψ یک‌به‌یک باشد، $\psi o f$ برای هر $f, g \in Hom_R$ متمایز، $\psi o f$ با$\psi o g$ متمایز می‌شود بنابراین یک همریختی ψ' القاء می‌کند که یک‌به‌یک است. $\square$

توجه کنید که دقیق بودن در N موجب نمی‌شود که

$$Hom_R(D, M) \xrightarrow{\varphi'} Hom_R(D, N) \to 0$$

دقیق باشد. یک مثال بارز دنباله دقیق $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{p} \mathbb{Z}/n\mathbb{Z} \to 0$ است. اگر $D = \mathbb{Z}/n\mathbb{Z}$ واگر $f \in Hom(D, N)$ یک نگاشت همانی باشد. از آن جایی که $\mathbb{Z}$ شامل هیچ عنصر از مرتبه متناهی جز صفر نیست، تنها هم‌ریختی صفر $F : D \to M$ وجود دارد. بنابراین $poF = 0 \neq f$.

قضیه ۲۰.۱. اگر D, L, M, N هر یک R-مدول باشند. و دنباله $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ دقیق باشد، آنگاه دنباله زیر

$$0 \to Hom_R(D, L) \xrightarrow{\psi'} Hom_R(D, M) \xrightarrow{\varphi'} Hom_R(D, N)$$

دقیق است.

اثبات. با توجه به قضیه‌ی ۱۹.۱ تنها کافی‌است نشان داد که $im\psi' = ker\varphi'$. به دلیل $\varphi o \psi = 0$، تنها $ker\varphi \subset im\psi'$ نیاز به اثبات دارد. آن هم از آن‌جا نتیجه می‌شود که اگر $f : D \to M$ به گونه‌ای باشد که $\varphi o f = 0$ آن‌گاه باید برد f مشمول در $ker\varphi$ باشد که از طریق ψ می‌توان آن را با L یکی گرفت. $\square$

تعریف ۲۱.۱. یک R-مدول P، تصویری[۸] است اگر هر یک از شرایط هم‌ارز زیر را داشته باشد:

(۱) اگر $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ دقیق باشد، آنگاه

$$0 \to Hom_R(P, L) \xrightarrow{\psi'} Hom_R(P, M) \xrightarrow{\varphi'} Hom_R(P, N) \to 0$$

دقیق است.

(۲) اگر $M \xrightarrow{\varphi} N \to 0$ یک دنباله دقیق از مدول‌ها باشد. برای هر $f : P \to N$ ترفیع $F \in Hom_R(P, M)$ وجود داشته‌باشد به طوری که دیاگرام زیر جابه‌جایی بشود:

$$\begin{tikzcd}
 & P \arrow[dl, dotted, "F"'] \arrow[d, "f"] & \\
M \arrow[r, "\psi"] & N \arrow[r] & 0
\end{tikzcd}$$

(۳) اگر P یک تقسیم R-مدول M باشد، آنگاه هر دنباله کوتاه دقیق بصورت زیر

$$0 \to L \to M \to P \to 0$$

شکافته شود.

(۴) P جمعوند مستقیمی از یک R-مدول آزاد[۹] باشد.

نتیجه ۲۲.۱. مدول‌های آزاد یکدست هستند،مدول‌های تصویری نیز یکدست هستند.

توجه کنید مدول‌های آزاد تصویری هستند. یک مدول به طور متناهی تولیدشده، تصویری است اگر و تنها اگر جمع مستقیم یک مدول آزاد به طور متناهی تولید شده‌باشد. هر مدول یک خارج‌قسمت از یک مدول تصویری است. مدول‌های تصویری را به منظور تعریف کردن گروه‌های همولوژی Tor_n^R با استفاده از تحلیل[۱۰] تصویری تعریف کردیم.

تعریف ۲۳.۱. اگر B یک R -مدول باشد. یک تحلیل تصویری از B دنباله‌ای دقیق بصورت زیر است:

$$\cdots \to P_n \xrightarrow{d_n} P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} 0$$

بطوریکه هر P_i یک R-مدول تصویری باشد.

۶.۱ نرم و تریس

فرض کنید k یک میدان است و A یک k-جبر ساده مرکزی از بعد متناهی از درجه‌ی n ($\sqrt{\dim_k A}$) است. می‌توان نشان داد که یک توسیع میدانی K/k موجود است به قسمی که $A \otimes_k K \cong M_n(K)$. K میدان شکافنده[۱۱] برای A نامیده می‌شود. پس فرض کنید K چنین میدانی باشد و

$$f : A \otimes_k K \to M_n(K)$$

را یکریختی مذکور بگیرید. حال فرض کنید $a \in A$ و $p(x)$ چندجمله‌ای مشخصه‌ی ماتریس $f(a \otimes_k 1)$ باشد. می‌توان نشان داد که $p(x) \in k[x]$ است و به انتخاب میدان K و یکریختی f بستگی ندارد. $p(x)$ را چندجمله‌ای مشخصه کاهش‌یافته a می‌نامند. فرض کنید

$$Prd_A(a, x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in k[x]$$

چندجمله‌ای مشخصه‌ی کاهش یافته‌ی $a \in A$ باشد. نرم کاهش یافته و تریس کاهش یافته را به صورت زیر تعریف می‌کنیم:

$$Trd_A(a) = -\alpha_{n-1}$$

---

[۸] Projective
[۹] Free
[۱۰] Resolution
[۱۱] spliting field

$$Nrd_A(a) = (-1)^n \alpha.$$

در این صورت به نگاشت $Nrd : k \to A$ می‌رسیم که همان نگاشت نرم کاهش یافته است و بر زیرگروه A^* متشکل از عناصر وارون‌پذیر A به یک همریختی گروهی $Nrd : A^* \to k^*$ تحدید می‌شود.

همچنین نگاشت تریس کاهش‌یافته را داریم که یک همریختی جمعی به صورت $Trd : A \to k$ می‌رسیم.

۲ نرم‌های کاهش‌یافته از جبرهای ساده روی میدان توابع

مطالب این بخش براساس [۱] است.

فرض کنید A یک جبر ساده مرکزی متناهی بعد روی میدان k باشد. زیرگروه جابه‌جاگرهای گروه ضربی A^*، $[A^*, A^*]$، را در نظر بگیرید. گروه $A^*/[A^*, A^*]$ را گروه وایتهد[۱۲] A می‌گوییم و با $K_1(A)$ نمایش می‌دهیم. محاسبه‌ی $K_1(A)$ مسئله‌ای بسیار دشوار است زیرا شامل محاسبه‌ی گروه وایتهد کاهش یافته[۱۳]، $SK_1(A)$ است و نیز گروه نرم‌های کاهش یافته، که این گروه به وضوح از روی دنباله‌ی دقیق $1 \to SK_1(A) \to K_1(A) \to Nrd(A^*) \to 1$ با استفاده از هومومورفیسم نرم کاهش یافته Nrd، بدست می‌آید:

$$SK_1(A) = SL(1, A)/[A^*, A^*]$$

که در آن $SL(1, A)$، هسته‌ی Nrd است.

مسئله‌ی تاناکا-آرتین[۱۴] مبنی بر بدیهی بودن گروه $SK_1(A)$ که برای مدت طولانی بدون پاسخ بود، در سال ۱۹۷۵ توسط پلاتونو[۱۵] نقض شد. پلاتون در کارهایش به صورت کمی رفتار گروه وایتهد کاهش یافته را بررسی کرد. غالب نتایجی که بدست آورد روی جبرهای سراسری[۱۶] و میدان‌های هنسل[۱۷] بود.

در مورد نرم‌های کاهش یافته از درجه دلخواه مطلب زیادی نمی‌دانیم و اغلب مطالب در مورد میدان‌های موضعی و سراسری است. در مجموع نتایجی مربوط به ساسلین است. او تمام میدان‌هایی را توصیف کرد که برای تمام جبرهای مرکزی روی آن‌ها و روی توسیع های متناهی از آن‌ها، نرم کاهش یافته پوشاست. جبرهای از درجه مربع روی میدان دلخواه، جایگاه ویژه‌ای دارند. در ۱۹۵۰ ونگ[۱۸] نشان داد در این حالت خاص $SK_1(A) = 1$. از طرف دیگر مرکوری[۱۹] و ساسلین توصیفی کوهمولوژی از گروه $Nrd(A^*)$ بدست آوردند. بنابراین می‌توان نتیجه گرفت که در این حالت گروه $K_1(A)$ محاسبه شده است.

هدف این مقاله توصیف نرم‌های کاهش یافته در حلقه‌های تقسیم از توابع گویای ناجابه‌جایی است که از آن برای محاسبه‌ی $K_1(A)$ برای جبر دلخواه A از درجه دلخواه روی میدان دلخواه k استفاده می‌کنیم. ابتدا نشان می‌دهیم محاسبه‌ی $K_1(A)$، معادل است با محاسبه برای حالت‌هایی که درجه عددی اول است.

مطالبی که در ادامه می‌آید برای توسیع میدانی T/R است و $N_{T/R}$ نرم مربوطه است.

لم ۱.۲. فرض کنید A یک حلقه‌ی تقسیم از درجه n باشد و F/k توسیع متناهی باشد به طوری که $(n, [F : k]) = 1$. در این صورت برای هر $\alpha \in K^* \cap Nrd((A \otimes_k F)^*)$ داریم $\alpha^{[F:k]} \in Nrd(A^*)$.

اثبات. بدون کاسته شدن از کلیت می‌توانیم فرض کنیم توسیع F/K جدایی‌پذیر است. فرض کنید $a \in A \otimes_k F$ و $Nrd(a) = \alpha$. در حالتی که $a \in F$ باشد، حکم بدیهی است. فرض کنید درجه‌ی چندجمله‌ای مینیمال a روی F، $f_F(x)$ برابر $e > 1$ باشد. زیرمیدان ماکسیمال L از $A \otimes_k F$ که شامل است و با ضریب ثابت β از $f_F(x)$. چون $Nrd(a) = N_{L/F}(a)$، بنابراین برای $[L : F] = et$ داریم $\alpha = (-1)^{et}\beta^t$. با استفاده از ضرایب $f_F(x)$ توسیع E/k را بسازید و چندجمله‌ای $f(x) = f_F^{\sigma_1}(x) \cdots f_F^{\sigma_c}(x)$ را درنظر بگیرید که در آن $\sigma_1 \ldots \sigma_c$ نشاندن‌های مجزا از E روی k در بستار جبری‌اش است و

---

[۱۲] Whitehead group

[۱۳] Reduced Whitehead group

[۱۴] Tanaka-Artin

[۱۵] Platonov

[۱۶] global

[۱۷] Henselian

[۱۸] Wang

[۱۹] Merkurev

$c = [E : k]$ و چندجمله‌ای $f_F^{\sigma_i}(x)$ با جایگزین کردن ضرایب $f_F(x)$ تحت اثر σ_i بدست آمده‌است. بنابراین $f(x)$ چندجمله‌ای مینیمال a روی k است.

نشان می‌دهیم $N_{L/k(a)}(a) = \alpha^{[F:k]}$. در واقع در یک طرف داریم $[L : k] = et[F : k]$ و در طرف دیگر داریم $k \subset k(a) \subset F(a) \subset L$ که در آن به تحلیل $[k(a) : k] = ce$ و $[L : F(a)] = t$ برقرار است که نتیجه می‌دهد

$$[F(a) : k(a)] = [F : k]c^{-1}$$

بعلاوه بخش ثابت $f(x)$ برابر است با $\beta_F^{\sigma_1} \cdots \beta_F^{\sigma_c}$، بنابراین $N_{k(a)/k}(\alpha) = \prod_{i=1}^{c}((-1)^e\beta^{\sigma_i})$، پس داریم:

$$N_{L/k}(\alpha) = (N_{k(a)/k}(a)^t)^{[F:k]c^{-1}} = (\alpha^c)^{[F:k]c^{-1}} = \alpha^{[F:k]}$$

چون L میدان شکافنده برای A است، $\alpha^{[F:k]} \in Nrd(A^*)$.

$\square$

در ادامه محاسبه نرم کاهش یافته را به حلقه‌های تقسیم از درجه اعداد اول کاهش می‌دهیم.

گزاره ۲.۲. فرض کنید $A = A_1 \otimes_k \cdots \otimes_k A_r$ باشد به طوری که هر A_i حلقه‌ی تقسیمی از درجه $p_i^{\alpha_i}$ است و p_iها اعداد اول متمایزند. در این صورت $Nrd(A^*) = \cap_{i=1}^{r} Nrd(A_i^*)$.

اثبات. فرض کنید $F_1, \ldots, F_r$ زیرمیدان‌های ماکسیمال متناظر با $A_1, \ldots, A_r$ باشد. فرض کنید L_i کوچکترین میدان روی k شامل $F_1, \ldots, F_{i-1}, F_{i+1}, \ldots, F_r$ باشد. اگر $\alpha \in Nrd(A^*)$، آنگاه $\alpha \in Nrd(A \otimes_k L_i)$ بنابراین

$$\alpha \in Nrd(A_i \otimes_k L_i)$$

. بنا به لم ۱.۲، $\alpha^{[L_i:k]} \in Nrd(A_i^*)$. اول بودن $[L_i : k]$ها نسبت به هم و p_iها نسبت به هم نیتجه می‌دهد $\alpha \in Nrd(A_i^*)$. برعکس، اگر $\alpha \in \cap_{i=1}^{r} Nrd(A_i^*)$ آنگاه $\alpha^{[L_i:k]} \in Nrd(A^*)$. حال از آنجایی که بزرگترین عامل مشترک $[L_i : k]$ها برابر ۱ است پس $\alpha \in Nrd(A^*)$. $\square$

نتیجه‌ی زیر یکی دیگر از نتایج سودمند لم فوق است.

نتیجه ۳.۲. با نمادگذاری لم ۱.۲ داریم $Nrd(A^*) = k^* \cap Nrd((A \otimes_k F)^*)$.

اثبات. واضح است که برای $\alpha \in k^*$ داریم $\alpha^n \in Nrd(A^*)$، که در آن n درجه A است. حال بنابر لم ۱.۲ از

$$\alpha \in k^* \cap Nrd((A \otimes_k F)^*)$$

نتیجه می‌شود $\alpha^{[F:k]} \in Nrd(A^*)$. برای عکس هم که واضح است. $\square$

ملاحظه ۴.۲. به صورت مکرر از این خاصیت معروف استفاده خواهیم‌کرد: اگر $a \in A$، آنگاه $a^n \in Nrd(a)[A^*, A^*]$، که در آن n درجه A است.

حال نشان می‌دهیم محاسبه‌ی $K_1(A)$ به محاسبه‌ی مولفه‌های اول گروه وایتهد وابسته است.

گزاره ۵.۲. با نمادگذاری گزاره ۲.۲، دنباله‌ی دقیق

$$1 \to (k^*)^{(r-1)} \to K_1(A_1) \times \cdots \times K_1(A_r) \to K_1(A) \to 1$$

وجود دارد که در آن $(k^*)^{(r-1)}$، ضرب مستقیم $r - 1$ کپی از k^* است.

اثبات. هomomorfیسم زیر را در نظر بگیرید:

$$f : K_1(A_1) \times \cdots \times K_1(A_r) \to K_1(A)$$

$$f(a_1[A_1^*, A_1^*], \ldots, a_r[A_r^*, A_r^*]) = a_1 \ldots a_r[A^*, A^*]$$

که در آن $a_i \in A_i$، $i = 1, \ldots, r$. فرض کنید $a \in A^*$ بنابراین، بنابه گزاره ۲.۲ داریم $a = bc$ که $b \in A$ و $Nrd(c) = 1$.

حال f پوشاست چون می‌دانیم محدود کردن f به زیرگروه $T = SK_1(A_1) \times \cdots \times SK_1(A_r)$ یک یکریختی بین T و $SK_1(A)$ بدست می‌دهد. بعلاوه $A = A_1 \otimes_k B$، که $B = A_2 \otimes_k \cdots \otimes_k A_r$.

فرض می‌کنیم $a \in A_1$ و $a \notin [A_1^*, A_1^*]$. بعلاوه $b \in B$ به گونه‌ای است که $ab \in [A^*, A^*]$. درجه A_1 را n و درجه B را m بگیرید. در این صورت $(ab)^m \in [A^*, A^*]$. چون $b^m \in Nrd_B(b)[A^*, A^*]$، داریم $a^m \in Nrd_B(b)[A^*, A^*]$. همچنین چون $a^n \in Nrd_{A_1}(a)[A^*, A^*]$ نتیجه می‌شود $\alpha \in k^*$ وجود دارد که $a \in \alpha[A^*, A^*]$. حال به سادگی می‌توان دید که هسته‌ی f شامل اعضایی به شکل $(a_1[A^*, A^*], \dots, a_r[A^*, A^*])$ است که $a_i \in k^*$ و $a_1 \dots a_r \in k^* \cap [A^*, A^*]$.

اگر $\mu \in k^* \cap [A^*, A^*]$، آنگاه μ ریشه‌ی واحد از درجه‌ای است که درجه A را عاد می‌کند. داریم $\mu = \mu_1 \dots \mu_r$ که $\mu_i \in k^*$ ریشه واحد از درجه‌ای است که درجه A_i را عاد می‌کند. نشان می‌دهیم $\mu_i \in k^* \cap [A_i^*, A_i^*]$. در واقع اگر $\mu_i \notin k^* \cap [A_i^*, A_i^*]$ در این صورت $\mu \notin k^* \cap [A^*, A^*]$، زیرا یکریختی $SK_1(A) \cong SK_1(A_1) \times \cdots \times SK_1(A_r)$ و اول بودن p_iها را داریم.

با توجه به مطالب فوق می‌توانیم فرض کنیم $a_1, \dots, a_r$ در خاصیت $a_1 \dots a_r = 1$ صدق می‌کنند. هومورفیسم زیر را در نظر بگیرید:

$$g : k^{*(r)} \to K_1(A_1) \times \cdots \times K_1(A_r)$$

$$g(k_1, \dots, k_r) = (k_1[A_1^*, A_1^*], \dots, k_r[A_r^*, A_r^*])$$

واضح است که هسته‌ی g برابر است با گروه $(k^* \cap [A_1^*, A_1^*]) \times \cdots \times (k^* \cap [A_r^*, A_r^*])$. تحدید g به زیرگروه $G \subset k^{*(r)}$ که با ویژگی $k_1 k_2 \dots k_r = 1$ تعریف می‌شود، دارای این خاصیت خواهدبود که، $g(G)$ هسته‌ی f است و $G \cap Ker(g) = \{1\}$. بنابراین گروه G با هسته‌ی f یک‌ریخت است. بدیهی است که $G \cong k^{*(r-1)}$. □

حال فرض کنید A یک حلقه‌ی تقسیم مرکزی روی $Z(A)$ با خودریختی ϕ از مرتبه بیرونی متناهی r است. در این حالت خوش‌تعریف است که بگوییم حلقه‌ی چندجمله‌ای‌های ناجابه‌جایی، $A[X, \phi]$، حلقه‌ی تقسیم کسرهای $A(X, \phi)$ است که مرکز آن مشابه $k(y^{-1}x^r)$ است که k میدانی است که تحت اثر ϕ در $Z(A)$ ثابت است، $y^\phi = y \in A^*$، و ϕ^r خودریختی درونی A، تولید شده توسط y است. مجموعه‌ی $x = y^{-1}X^r$ را درنظر بگیرید. در این صورت $[A(X, \phi) : k(x)] = n^2 = [A : Z(A)]r$. اگر $P = P_1 \dots P_s$ و $Q = Q_1 \dots Q_s$ تجزیه‌ی P و Q به چندجمله‌ای‌های تحویل‌ناپذیر در $A[X, \phi]$ باشد و تناظری یک به یک و پوشا بین $\{P_1, \dots, P_s\}$ و $\{Q_1, \dots, Q_s\}$ برقرار باشد می‌نویسیم $P \approx Q$ یا معادلا از $\sim$ استفاده می‌کنیم.
در ادامه به لم زیر نیاز خواهیم‌داشت.

لم ۶.۲. فرض کنید $P \in A[X, \phi]$ باشد در این صورت $Nrd(P) \in k[x]$. اگر $P = 1 + XQ$ که $Q \in A[X, \phi]$ آنگاه $Nrd(P) = 1 + xq$ که $q \in k[x]$.

اثبات. فرض کنید $a_1 = 1, a_2, \dots, a_m$ یک پایه برای A روی k باشد و T پایه‌ی $\{a_i X^j\}$ برای $A(X, \phi)$ روی $k(x)$ باشد که $i = 1, \dots, m$ و $j = 0, \dots, r-1$. اگر μ نمایش منظم حلقه‌ی تقسیم $A(X, \phi)$ روی $k(x)$ باشد، آنگاه $\mu(P)$ ماتریسی است که درایه‌های آن چندجمله‌ای‌ها هستند. بنابراین $\det \mu(P)$ چندجمله‌ای است. از آنجایی که $\det \mu(P) = Nrd(P)^n$ و $k[x]$ به درستی در $k(x)$ بسته است می‌توانیم نتیجه بگیریم $Nrd(P) \in k[x]$.
برای حالت $P = 1 + XQ$، کافی است که حلقه‌ی تقسیم $A(X, \phi) \otimes_{k(x)} k(x)_x$ را درنظر بگیریم. □

لم ۷.۲. اگر $a \in [A(X, \phi)^*, A(X, \phi)^*]$ و $a = P\lambda^{-1}$ که $P \in A[X, \phi]$ و $\lambda \in k[x]$، آنگاه $P \approx \lambda$.

نتیجه ۸.۲. اگر $P = Qa$، که $a \in [A(X, \phi)^*, A(X, \phi)^*]$ و $P, Q \in A[X, \phi]$، آنگاه $P \approx Q$.

لم ۹.۲. فرض کنید $g = P_1 \dots P_r$ تجزیه‌ی چندجمله‌ای $g \in k[x]$ به حاصلضرب چندجمله‌ای‌های تحویل‌ناپذیر در $A[X, \phi]$ باشد. اگر $Q \sim Q_i$، در این صورت چندجمله‌ای R وجود دارد به طوری که $g = QR = RQ$.

اثبات. قرار دهید $g = EP_iB$ که در آن $E, B \in A[X, \phi]$، و از تقسیم g بر P_i داریم $g = P_iM + T$. اگر $T \neq 0$ باشد در این صورت از ضرب E در تساوی‌ها بدست می‌آید، $gE = EP_iBE$ و $Eg = EP_iM + ET$، بنابراین داریم $EP_iBE = EP_iM + ET$. بنابراین EP_i عامل ET است، اما این درست نیست زیرا درجه‌ی ET از درجه‌ی EP_i کمتر است و این نتیجه می‌دهد $g = P_iM$.

با استفاده از $Q \sim P_i$ نتیجه می‌شود چندجمله‌ای‌های u و v با درجه‌ی کمتر از Q وجود دارد که $uP_i = Qv$. حال g را بر Q تقسیم می‌کنیم، داریم $g = QR + T$. اگر $T \neq 0$ باشد، در این صورت داریم $gu = uP_iM = QvM$. به عبارت دیگر

$Q(vM-Ru)=Tu$، بنابراین تجزیه‌ی Tu به چندجمله‌ای‌های تحویل‌ناپذیر شامل عاملی مشابه Q است. اما درجه‌ی T و u از Q کمتر است که تناقض است پس $g=QR$. حال چون g در $A(X,\phi)$ مرکزی است، پس $g=RQ$. □

نتیجه ۱۰.۲. اگر $P\in A[x,\phi]$، در این صورت $P \mid Nrd(P)$.

اثبات. فرض کنید $P=P_1\dots P_s$، که P_iها در $A[X,\phi]$ تحویل‌ناپذیرند. با توجه به ملاحظه ۴.۲، $P_i^n=Nrd(P_i)a_i$ با $a_i\in[A(X,\phi)^*,A(X,\phi)^*]$. بنابر نتیجه‌ی ۸.۲، $P_i^n\approx Nrd(P_i)$. اگر از لم ۹.۲ استفاده کنیم، بدست می‌آید $Nrd(P_i)=P_iQ_i$، که $Q_i\in A[X,\phi]$. بنابراین $Nrd(P_i)=PQ_s\dots P_1$. □

لم ۱۱.۲. فرض کنید $f=P_1\dots P_s$ تجزیه‌ی چندجمله‌ای تحویل‌ناپذیر $f\in k[x]$ به چندجمله‌ای‌های تحویل‌ناپذیر در $A[X,\phi]$ باشد. در این صورت $P_1\sim P_2\sim\dots\sim P_s$ و برای هر $Q\sim P_i$ داریم $Nrd(Q)=af^{n/s}, a\in k^*$.

اثبات. واضح است که $f^n=Nrd(P_1)\cdots Nrd(P_s)$، بنابراین $Nrd(P_i)=af^{n_i}$، در نتیجه $P_i^n=a_if^{n_i}b_i$ که $b_i\in[A(X,\phi)^*,A(X,\phi)^*]$. بنابر نتیجه ۸.۲، $P_i^n\approx f^{n_i}$ پس $P_1\sim\dots\sim P_s$، و این تطابق n_iها و تساوی $n_i=ns^{-1}$ را نتیجه می‌دهد. حال اگر از لم ۹.۲ استفاده کنیم، حکم نتیجه می‌شود. □

لم ۱۲.۲. $A[X,\phi]$ از مرتبه‌ی ماکسیمال روی $k[x]$ است.

اثبات. فرض کنید $\{a_1=1,a_2,\dots,a_m\}$ یک پایه برای A روی k باشد. در این صورت مجموعه‌ی $M=\{a_iX^j\}$ که $i=1,\dots,m$ و $j=0,\dots,r-1$، یک پایه برای $A(X,\phi)$ روی $k(x)$ است. به علاوه نشان می‌دهیم هر چندجمله‌ای $P\in A[X,\phi]$ روی حلقه‌ی $k[x]$ صحیح است. در واقع به سادگی می‌توان دید که P ترکیب خطی از اعضای پایه‌ی M با ضرایب در $k[x]$ است. از آنجایی که ساختار ثابت‌ها در جبر $A(X,\phi)$ نسبت به پایه‌ی M در $k[x]$ قرار دارد، نمایش منظم چندجمله‌ای P ماتریسی با درایه‌های در $k[x]$ است. چندجمله‌ای مشخصه‌ی این ماتریس ضرایبی در $k[x]$ دارد و این با استفاده از قضیه‌ی کیلی-همیلتون[20] نتیجه می‌دهد P روی $k[x]$ صحیح است. بنابراین حلقه‌ی $A[X,\phi]$ مرتبه‌ای در $A(X,\phi)$ روی $k[x]$ دارد.

حال نشان می‌دهیم این مرتبه ماکسیمال است. فرض خلف می‌کنیم. فرض کنید L مرتبه‌ی ماکسیمال در $A(X,\phi)$ روی $k[x]$ دارد که اکیدا شامل $A[X,\phi]$ است. بنابراین L عضوی مانند PQ^{-1} دارد ($P,Q\in A[X,\phi]$) که یک چندجمله‌ای نیست. فرض کنید $P=TQ+R$ که R باقی‌مانده تقسیم از راست P بر Q است. چون PQ^{-1} چندجمله‌ای نیست پس $R\neq 0$. بدیهی است که $RQ^{-1}\in L$. به علاوه درجه‌ی R اکیدا از درجه‌ی Q کمتر است پس درجه‌ی چندجمله‌ای $Nrd(R)$ (نسبت به x) اکیدا از درجه‌ی چندجمله‌ای $Nrd(Q)$ کمتر است. بنابراین $Nrd(RQ^{-1})\notin k[x]$. از آنجایی که $PQ^{-1}\in L$، پس روی $k[x]$ صحیح است. با استفاده از نتیجه‌ی لم گاوس[21]، بخش ثابت چندجمله‌ای مینیمال PQ^{-1} روی $k(x)$ باید در $k[x]$ باشد. حال از آنجایی که $Nrd(RQ^{-1})$ متناسب است با توانی از ۱- در یک ثابت، داریم $Nrd(PQ^{-1})\in k[x]$. اما نشان دادیم که این درست نیست پس $A[X,\phi]$ از مرتبه‌ی ماکسیمال در $A(X,\phi)$ روی $k[x]$ است. □

حال فرض کنید f چندجمله‌ای تکین تحویل‌ناپذیر در $k[x]$ باشد. نماد $k(x)_f$ را برای میدان کامل حاصل از $k(x)$ در نقطه‌ی متناظر با f در نظر می‌گیریم و $O_{<f>}$ را حلقه در این نقطه.

لم ۱۳.۲. $O_{<f>}\mathrm{span}L_{<f>}$ در حلقه‌ی $A[X,\phi]$ دارای مرتبه‌ی ماکسیمال در جبر

$$A(X,\phi)\otimes_{k(x)} k(x)_f$$

روی $O_{<f>}$ می‌باشد.

اثبات. به کمک لم ۱۲.۲ حاصل می‌شود. □

لم ۱۴.۲. دو $A[X,\phi]$-مدول چپ $A[X,\phi]/fA[X,\phi]$ و $L_{<f>}/fL_{<f>}$ یکریختند.

فرض کنید $M_m(D_f)$ جبر ماتریس‌های از درجه‌ی $m\geq 1$ روی حلقه‌ی تقسیم D_f باشد و داشته‌باشیم $A(X,\phi)\otimes_{k(x)} k(x)_f\cong M_m(D_f)$. فرض کنید $\bar{D_f},\bar{k(x)}_f$ به ترتیب حلقه‌های تقسیم کاهش‌یافته‌ی D_f و $k(x)_f$ باشند. قرار دهید $t=[\bar{D_f},\bar{k(x)}_f]$ و $i(f)=\sqrt{e^{-1}t}$، که در آن e درجه انشعابی D_f روی $k(x)_f$ است.

[20] Hamilton-Cauley
[21] Gauss's lemma

لم ۱۵.۲. فرض کنید $aP_1^{\alpha_1}\dots P_s^{\alpha_s} \in Nrd(A(X,\phi))$ که $a \in k^*$ و $P_j(j=1,\dots,s)$ چندجمله‌ای‌های تکین تحویل‌ناپذیر مجزا در $k[x]$ باشند. در این صورت $i(P_j)$ مقسوم‌علیه α_j است.

اثبات. فرض کنید s_f و e_f به ترتیب درجه و درجه انشعابی D_f روی $k(x)_f$ باشند. برای هر زیرمیدان ماکسیمال L از D_f درجه انشعابی L روی $k(x)_f$ درجه e_f را می‌شمارد و زیرمیدان ماکسیمالی وجود دارد که درجه آن e_f است. بنابراین $N_{L/k(x)_f}(L^*) \subset \langle f^{s_f e_f^{-1}} \rangle U_f$ که U_f گروه یکال‌های حلقه‌ی $O_{<f>}$ است و $\langle f^{s_f e_f^{-1}} \rangle$ گروه دوری تولید شده توسط $f^{s_f e_f^{-1}}$ است. بنابراین $N(D_f) \subset \langle f^{s_f e_f^{-1}} \rangle U_f$. با توجه به $Nrd(A(X,\phi)) \subset Nrd(D_f)$، همه چیز ثابت شده‌است. □

برای هر B-مدول M، $\lambda_B(M)$ را طول سری ترکیبی آن در نظر می‌گیریم.

لم ۱۶.۲. فرض کنید P چندجمله‌ای تحویل‌ناپذیر باشد که f را عاد می‌کند. در این صورت $Nrd(P) = \alpha f^{i(f)}$ که $\alpha \in k$.

اثبات. بنا به لم ۱۱.۲ کافی است نشان دهیم تجزیه‌ی f به عامل‌های تحویل‌ناپذیر وجود دارد که طولی برابر $n.i(f)^{-1}$ دارد. می‌دانیم آخرین عدد مطابق است با

$$\mu = \lambda_{A[X,\phi]}(A[X,\phi]/fA[X,\phi])$$

. با توجه به لم ۱۴.۲، $\mu = \lambda_{A[X,\phi]}(L_{<f>}/fL_{<f>})$ و $ni(f)^{-1}$، و آخرین عدد حداقل $\lambda_{L_{<f>}}(L_{<f>}/fL_{<f>})$ و حداکثر $ni(f)^{-1}$ است. حال چون $L_{<f>}$ از مرتبه‌ی ماکسیمال است، $L_{<f>} \cong M_m(O_{D_f})$ که O_{D_f} ارزش[۲۲] حلقه‌ی D_f است. بنابراین

$$L_{<f>}/fL_{<f>} \cong M_m(O_{D_f})/fM_m(O_{D_f}) \cong M_m(O_{D_f}/fO_{D_f})$$

حال به راحتی دیده‌می‌شود که طول سری ترکیبی آخرین مدول برابر است با $ni(f)^{-1}$. □

درجه‌ی چندجمله‌ای f در $k[x]$ را با $\deg f$ نشان می‌دهیم.

لم ۱۷.۲. فرض کنید P چندجمله‌ای تکین تحویل‌ناپذیر در $A[X,\phi]$ باشد. در این صورت برای هر چندجمله‌ای تحویل‌ناپذیر $f \in k[x]$ داریم

$$Nrd(P) = (-1)^{(r+1)i(f)\deg f} N_{k(y)/k}(y)^{i(f)\deg f[k(y):k]^{-1}} f^{i(f)}$$

اثبات. فرض کنید $\alpha f_1^{u_1 i(f_1)}\dots f_s^{u_s i(f_s)}$ تجزیه‌ی $Nrd(P)$ به عامل‌های اول مجزا باشد. بنا به لم ۱۶.۲ چندجمله‌ای‌های تحویل‌ناپذیر P_j وجود دارد به طوری که $Nrd(P_j) = \alpha_j f_j^{i(f_j)}$. بعلاوه $\beta \in k$ وجود دارد با این ویژگی که $\beta Nrd(P) = Nrd(P_1^{u_1}\dots P_s^{u_s})$. با اثر دادن ملاحظه‌ی ۴.۲ و نتیجه‌ی ۸.۲ در تساوی فوق بدست می‌آید $P \sim P_1 \sim \dots \sim P_s$ بنابراین $s=1$ و $u_1=1$. حال قرار دهید $P = (1 + a_{e-1}X^{-1} + \dots + a_0 X^{-e})X^e$ که در آن $a_i \in A$. بنابراین $Nrd(P) = Nrd(1+a_{e-1}X^{-1}+\dots+a_0X^{-e})Nrd(X^e)$. متغیر X^{-1} را بگیرید و لم ۶.۲ را استفاده کنید، خواهیم‌داشت $Nrd(1+a_{e-1}X^{-1}+\dots+a_0X^{-e}) = 1 + x^{-1}q(x^{-1})$. این نتیجه می‌دهد که ضریب پیش‌رو $Nrd(P)$ توان eام ضریب پیش‌رو در $Nrd(X)$ است.

برای کامل شدن اثبات کافی است درجات را نسبت به X به کمک تساوی $e = i(f)\deg f.r.n^{-1}$ مقایسه کنیم. بدست می‌آید:

$$Nrd(X) = (-1)^{n(r+1)r^{-1}} N_{k(y)/k}(y)^{nr^{-1}[k(y):k]^{-1}} x^{nr^{-1}}$$

□

قضیه ۱۸.۲. بگیرید:

$$T = \cup_f (-1)^{(r+1)i(f)\deg f} N_{k(y)/k}(y)^{i(f)\deg f[k(y):k]^{-1}} f^{i(f)}$$

که اجتماع روی تمام چندجمله‌ای‌های تحویل‌ناپذیر f است. بگیرید

$$G = N_{Z(A)/k}(Nrd_A(A^*))$$

و فرض کنید E منوید تولید شده توسط T، G و مجموعه‌ی $(k[x]/fk[x])^{-n}$ باشد. در این صورت $Nrd(L_f) = E \cup \{0\}$ و $Nrd(A(X,\phi)^*)$ زیرگروه تولید شده توسط T و G است. ($L_f = L_{<f>} \cap A(X,\phi)$)

[۲۲] valuation

اثبات. به سادگی می‌توان دید که مجموعه‌ی $k[x]^n$ در $E \cup \{0\}$ قرار دارد. حال حکم برای هر تجزیه چندجمله‌ای دلخواه P به اعضای A که چندجمله‌هایی تکین و تحویل‌ناپذیرند در $A[X,\phi]$ برقرار است. مطلب فوق از لم ۱۷.۲ نتیجه می‌شود. $\square$

حال فرض کنید B حلقه‌ی تقسیم مرکزی روی k از درجه n شامل A باشد به طوری که
$$D = A + At + \cdots + At^{r-1}$$

که $i_t\mid_A = \phi$ و $t^r = y$. در این صورت $X^r - y$ چندجمله‌ای تحویل‌ناپذیر در $A[X,\phi]$ است. در واقع اگر این چنین نباشد پس $X^r - y = f_1 f_2$ است که درجه چندجمله‌ای‌ها کمتر از r است. دو طرف تساوی فوق را در $X = t$ حساب کنید بدست می‌آید $f_1(t) f_2(t) = 0$، اما $f_1(t)$ و $f_2(t)$ هیچکدام در D صفر نمی‌شوند. بنابراین $X^r - y$ تحویل‌ناپذیر است. به علاوه از آنجایی که $X^r - y = y(x-1)$، ایده‌آل $(X^r - y)A[X,\phi]$ دوطرفه است. بنابراین
$$A[X,\phi]/(x-1)A[X,\phi] \cong D$$

برای زیرمجموعه‌ی $S \subset A[X,\phi]$، $\bar{S}$ را مجموعه‌ی تصویر تمام اعضای S تحت هم‌ریختی که توسط چندجمله‌ای ارزیابی در $X = t$ از $A[X,\phi]$ به D حاصل می‌شود، درنظر می‌گیریم.

لم ۱۹.۲. فرض کنید k/M توسیعی جدایی‌پذیر باشد. در این صورت برای هر $P \in A[X,\phi]$ داریم
$$N_{k/M}(Nrd(\bar{P})) = \overline{N_{k(x)/M(x)}(Nrd(P))}$$

اثبات. از آنجایی که $A(X,\phi) \otimes_{k(x)} k(x)_{x-1}$ یک حلقه‌ی تقسیم بدون انشعاب است و نرم کاهش یافته با توسیع‌های مرکز تغییر نمی‌کند بنابراین $Nrd(\bar{P}) = \overline{Nrd(P)}$. مشابها برای $P \in k[x]$ بدست می‌آید $\overline{N_{k(x)/M(x)}(P)} = N_{k/M}(\bar{P})$. $\square$

نتیجه ۲۰.۲. با نمادگذاری لم قبلی داریم:
$$N_{k/M}(Nrd(D)) = \overline{N_{k(x)/M(x)}(Nrd(A[X,\phi]))}$$

اثبات. فرض کنید $\alpha \in N_{k/M}(Nrd(D))$. عنصر $d \in D$ وجود دارد به طوری که $\alpha \in N_{k/M}(Nrd(d))$. اگر a تصویر وارون d در $A[X,\phi]$ باشد در این صورت دیده‌می‌شود که $\alpha \in \overline{N_{k(x)/M(x)}(Nrd(a))}$. بنابراین یک طرف برقرار می‌شود. شمول قسمت دوم از لم ۱۹.۲ نتیجه می‌شود. $\square$

اگر D حلقه‌ی تقسیم با مرکز k از درجه p^m ($p^m \neq 2$ و p اول است) شامل زیرمیدان ماکسیمال L باشد و زنجیر
$$k = L_0 \subset L_1 \subset \cdots \subset L_m = L$$

را داشته باشیم که هر کدام از توسیع‌ها دوری از درجه‌ی p است. مرکزساز L_j در D را با A_j نشان می‌دهیم و ϕ_j خودریختی از A_j است که تحدید آن به L_j مولد گروه گالوای توسیع L_j/L_{j-1} خواهد بود. فرض کنید $y_j \in A_j$ و ϕ_j^p خودریختی درونی حاصل از y_j باشد و $y_j^{\phi_j} = y_j$. در این صورت $A_j(X_j,\phi_j)$ متناظر است با حلقه‌ی تقسیم توابع گویای ناجابه‌جایی. برای چندجمله‌ای تکین و تحویل‌ناپذیر دلخواه $f \in k[x]$، $L_j(f)$ مجموعه‌ی تمام چندجمله‌ای‌های تکین تحویل‌ناپذیر در $L_{j-1}[x]$ است به طوری که $N_{L_{j-1}(x)/k(x)}(l) = f^{\mu_j(l)}$ برای $l \in L_j(f)$. همچنین مجموعه‌ی $N(f) = \cup_{j=1}^{m} N_j(f)$ را داریم که در آن
$$N_j(f) = \cup_{l\in L_j(f)} N_{L_j(y_j)/k}(y_j)^{i(l).\deg l.[L_j(y_j):L_j]^{-1}}.f^{i(l)\mu_j(l)}$$

و $N(f(1))$ مجموعه‌ی مقدارهای اعضای $N(f)$ در $x = 1$ است.

قضیه ۲۱.۲. بگیرید $D(N) = \cup_{f\neq x-1} N(f(1))$. در این صورت $Nrd(D^*)$ منوید تولید شده توسط $D(N)$ و $N_{L/k}(L^*)$ است.

اثبات. فرض کنید T_i مجموعه‌ای برای $A_i(X_i,\phi_i)$ مشابه T که در قضیه‌ی ۱۸.۲ بیان کردیم باشد. با استفاده از قضیه‌ی ۱۸.۲ و لم ۱۷.۲ و نتیجه‌ی ۲۰.۲ داریم:
$$Nrd(D) = \bar{T}_1 \times \overline{N_{L_1(x_2)/k(x_2)}(T_2)} \cdots \overline{N_{L_{m-1}(x_m)/k(x_m)}(T_m)} N_{L_m/k}(L)$$

که بار به معنای ارزش چندجمله‌ای در ۱ است. این نشان می‌دهد که توان (-1) را در تعریف T_i می‌توانیم حذف کنیم. اما مشاهده می‌شود که هنگامی که p فرد است و هنگامی که $p = 2$ این توان به شکل توانی از $(-1)^{2^m(2^m+1)2^{-1}}$ است که برای $m > 1$ برابر ۱ است. $\square$

می‌دانیم برای حلقه‌ی تقسیم D از درجه عدد اول همواره توسیع F از k با درجه‌ی عدد اول p وجود دارد به طوری که حلقه‌ی تقسیم $F \otimes_k D$ دارای زنجیر $F = L_0 \subset L_1 \subset \cdots \subset L_m = L$ است که هر توسیع دوری از درجه‌ی p است و زیرمیدان ماکسیمال L است. حال با استفاده از قضیه‌ی ۱۸.۲ و گزاره‌ی ۲.۲ و نتیجه‌ی ۳.۲، نرم کاهش‌یافته را برای حلقه‌ی تقسیم دلخواه A محاسبه می‌کنیم.

فرض کنید D یک حلقه‌ی تقسیم مرکزی روی k از درجه p^m باشد (p اول) که دارای زیرمیدان Z از درجه‌ی p روی k است. فرض کنید A مرکزساز Z در D و ϕ خودریختی از A باشد که روی Z، مولد گروه گالوای Z روی k باشد. روی $A(X,\phi)$ بگیرید $L_{x-1} = L_{<x-1>} \cap A(X,\phi)$. حال تعریف کنید L^* گروه یکال‌های در L_{x-1} و

$$E = 1 + (x-1)L_{x-1}$$

$$L' = [L^*, L^*]$$

$$H = \{h \in L^* \mid Nrd(h) \in E\}$$

$$A' = [A(X,\phi)^*, A(X,\phi)^*]$$

$$S = SL(1, A(X,\phi))$$

$$N = (EL' \cap S)/L'$$

گزاره‌ی زیر محاسبه‌ی $SK_1(D)$ را به محاسبه‌ی گروه‌های وابسته با میدان $A(X,\phi)$ تبدیل می‌کند.

قضیه ۲۲.۲. دنباله‌ی دقیق زیر وجود دارد:

$$1 \to SK_1(A(X,\phi))/N \to SK_1(D) \to (Nrd(L^*) \cap E)/Nrd(E) \to 1$$

اثبات. از آنجایی که $x-1$ در $A[X,\phi]$ تحویل‌ناپذیر و مرکزی است، $A' = L'$. بعلاوه $L' = [D^*, D^*]$. بنابراین

$$SK_1(D) \cong \bar{H}/\bar{A'} \cong (H/E)(EA'/E) \cong H/EA'$$

زیرگروه $B = SE/EA'$ از گروه H/EA' را در نظر بگیرید. در این صورت

$$B \cong S/(S \cap EA') \cong SK_1(A(X,\phi))/N$$

بگیرید $G = H/ES$، داریم:

$$G \cong (HS)/(ES/S) \cong (Nrd(L^*) \cap E)/Nrd(E)$$

□

ملاحظه ۲۳.۲. $SK_1(A(X,\phi))$ محاسبه شده‌است.

مراجع

[1] V. I. Yanchevskii, *Reduced Norms of Simple Algebras Over Function Fields*, proceedings of the Steklov Institute of Mathematics, Issue 4, 1991.

[2] P. K. Draxl, *Skew Fields*. Cambridge University Press, 1983.

[3] Rowen Louis Halle, *Ring Theory*, Academic Press, 1991.

[4] Philippe Gille and Tamas Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge, Studies in Advanced Mathematics, 2006.

[5] Benson Farb and R.Keith Dennis, *Noncommutative Algebra*, Springer-Verlag, 1993.

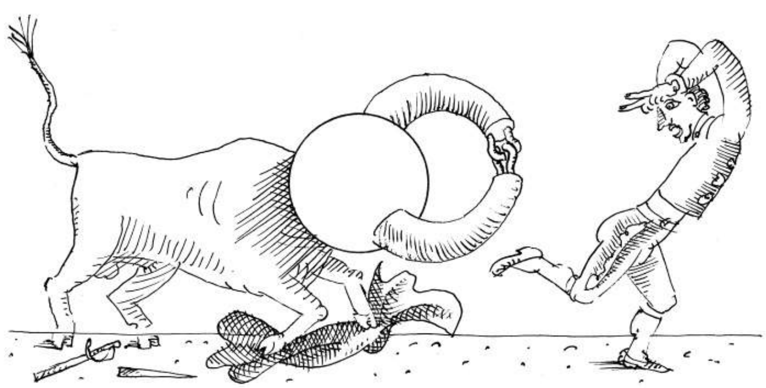
[۶] سیامک یاسمی و محمدرضا پورنکی، *مقدمه‌ای بر نظریه‌ی مدول‌ها*، موسسه‌ی انتشارات علمی دانشگاه صنعتی شریف، چاپ دوم، ۱۳۸۶.

[۷] علی کلامی، *قضیه‌ی ضریب جهانی برای همولوژی*. مجله ریاضی شریف، شماره دوم، سال اول.

کره‌ی شاخدار الکساندر

ترجمه: سامان حبیبی اصفهانی

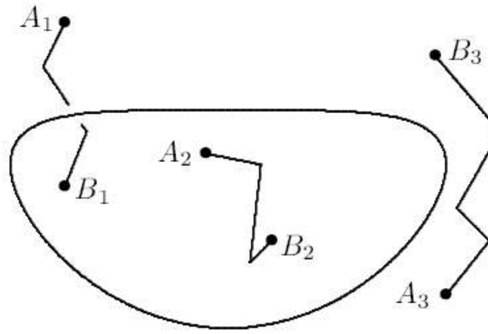
کره شاخدار الکساندر[1] دو ویژگی دارد که به آن ارزش مطالعه می‌دهد . اول اینکه راه حلی برای یک مساله بسیار مهم و مشکل در زمینه توپولوژی ارائه می‌دهد و دوم اینکه واقعا زیباست .



قضیه ژردان-شوئنفلیس[2]: یک خم در یک صفحه اثر[3] یک نقطه متحرک است. اگر مکان اولیه نقطه با مکان انتهایی آن منطبق شود به آن یک خم بسته می‌گوییم. اگر موقعیت نقطه متحرک در هیچ دو لحظه ای (مگر احیانا نقطه اول و آخر) منطبق نشود خم حاصله را خم ساده یا خم ناخود متقاطع می‌نامیم. قضیه ژردان بیان می‌کند خم ساده بسته C واقع در صفحه، صفحه را به دو ناحیه " درون" و "بیرون" تقسیم می‌کند به نحوی که هر دو نقطه که درون یک ناحیه هستند را می‌توان به کمک خطی شکسته[4] به هم متصل کرد طوری که این خط از خم C مجزا باشد در حالیکه هر خط شکسته ای که دو نقطه را از دو ناحیه مختلف به هم وصل می‌کند حتما خم C را قطع خواهد کرد.

این قضیه در آنالیز از اهمیت زیادی برخوردار است برای نمونه در نظریه انتگرال جایی که نیازمندیم تا ناحیه هایی محدود به یک خم بسته ساده در نظر بگیریم. ولی این قضیه سوالی را از خود بر جای می‌گذارد که بیشتر در حوزه توپولوژی جای دارد تا آنالیز: ناحیه‌هایی از صفحه که توسط یک خم ساده بسته تولید می‌شوند چه شکلی دارند؟

---
[1] Alexander's Horned Sphere
[2] Theorem of C. Jordan and A. Schoenflies
[3] trace
[4] Polygonal Line



شکل ۱: یک خم ساده بسته صفحه را به دو ناحیه مجزا تقسیم می‌کند.

در ریاضیات معمولا واژه‌ی نادقیق "هم‌شکل" با واژه‌ی دقیق "همیومورفیک" جای‌گذاری می‌شود: دو ناحیه همیومورفیک هستند اگر یک نگاشت یک‌به‌یک از یکی به دیگری موجود باشد که هم خود آن و هم وارونش پیوسته‌اند. برای نمونه درون یک دایره و درون یک مربع همیومورفیک هستند (با اینکه شاید در ظاهر شبیه هم به نظر نیایند.) در حالی‌که یک حلقه (ناحیه میان دو دایره هم مرکز) با هیچ کدام همیومورفیک نیست .

در سال ۱۹۰۸ شوئنفلیس اثبات کرد که به ازای هر خم ساده بسته ای که در صفحه رسم کنیم، ناحیه درونی خم و ناحیه بیرونی آن با درون و بیرون دایره همیومورفیک است. به طور مشابه می‌توان ثابت کرد که ناحیه میان دو خم ساده بسته که همدیگر را قطع نمی‌کنند با حلقه همیومورفیک است.

تعمیم به ابعاد بالاتر

می‌توان انتظار داشت که قضیه‌ای مشابه قضیه ژردان-شوئنفلیس برای هندسه فضایی هم برقرار باشد. همه چیزی که به آن احتیاج داریم یافتن بیان صحیح است. رویه های های بسته به وضوح باید جای خم های بسته را بگیرند.

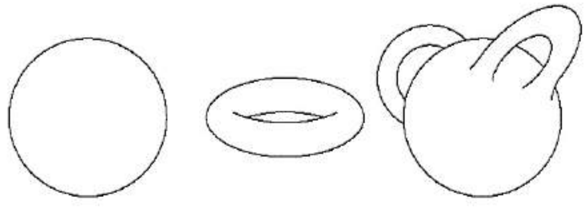
حال با اولین مشکل روبه رو می‌شویم: درحالی که همه‌ی خم‌های بسته به نوعی شبیه به هم هستند (هومیومورفیک‌اند) اما رویه‌های بسته می‌توانند به طور اساسی متفاوت باشند. برای نمونه چنبره ها، کره، کره‌های با دسته و ...هیچ کدام با هم همیومورفیک نیستند. پس باید حالت‌های مختلف جداگانه بررسی شوند. ما از این تنوع چشم‌پوشی می‌کنیم و تمام توجه‌مان را به رویه‌هایی که توسط یک نگاشت پیوسته از کره بدست آمده‌اند بدون اینکه خود را قطع کنند، محدود می‌کنیم. حال برای چنین رویه‌هایی می‌توان انتظار آن را داشت که نتیجه‌ای مشابه قضیه ژردان-شوئنفلیس برقرار باشد.

مشابه قضیه ژردان در دو بعد، حالت فضایی قضیه برای این رویه‌ها درست است یعنی چنین رویه هایی فضا را به دو ناحیه درون و بیرون تقسیم می‌کند. ضمنا ادعای قضیه در حالت دو بعدی اینجا بدون هیچ تغییری کاملا صحیح می‌باشد نه تنها برای رویه‌های مطرح شده همچنین برای کره‌هایی که به آنها دسته یا دسته‌هایی اضافه کرده‌ایم. همچنین برای آن تعمیمی‌کاملا طبیعی به هر بعد دلخواه نیز موجود است .

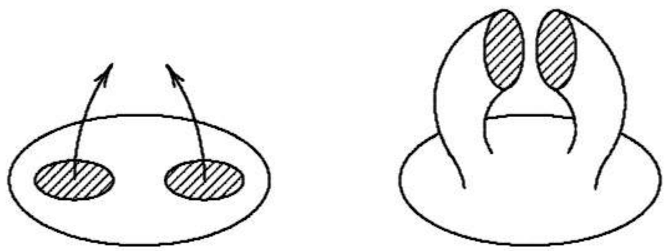
اما قضیه شوئنفلیس چطور؟ تعمیم صورت قضیه به ابعاد بالاتر باید چنین باشد که ناحیه‌های درونی و بیرونی ایجاد شده باید با ناحیه های بیرونی و درونی کره همیومورفیک باشد یعنی به ترتیب با گوی باز و مکمل گوی بسته (مکمل بستار گوی).

اما این توپولوژیست آمریکایی، جان الکساندر بود که برای نخستین بار در سال ۱۹۲۴ اثبات کرد که این حدس، هر چند هم که در نگاه اول پذیرفتنی به نظر می‌رسد، در واقع غلط است. کار الکساندر بسیار متقاعد کننده بود: او یک ساختار صریح از یک کره تغییر شکل یافته ارائه کرد که فضا را به ناحیه های استاندارد تبدیل نمی‌کرد. در زیر این ساختار به تفصیل شرح داده می‌شود.

ساختار الکساندر بسیار زیبا و ساده است. جزء اصلی این ساختار در شکل زیر نمایش داده شده است. دو دیسک مجزا درون یک دیسک بزرگتر در نظر بگیرید.(شکل ۳-ب) از این دو دیسک دو "انگشت" بیرون بکشید و انتهای این دو را به هم نزدیک کنید به طوری که با هم برخوردی نداشته باشند.(شکل۳-الف)

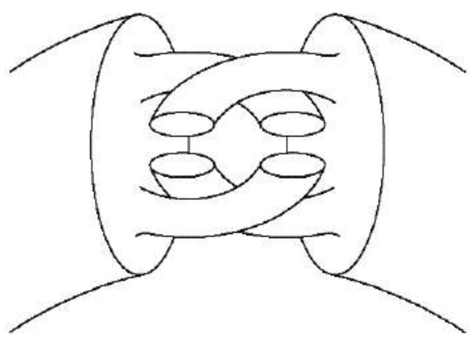


شکل ۲: چند مثال از رویه ها نا همشکل



شکل ۳: ساختن انگشت‌ها

در دو انتهای دو انگشت دو دیسک مسطح داریم. حال همین کار را با این دو دیسک انجام می‌دهیم .درون هر دیسک دو دیسک کوچکتر در نظر گرفته و از آنها "انگشت"هایی را خارج می‌کنیم و به چهار انگشت می‌رسیم که شبیه به یک قفل به نظر می‌آیند. (شکل ۴)

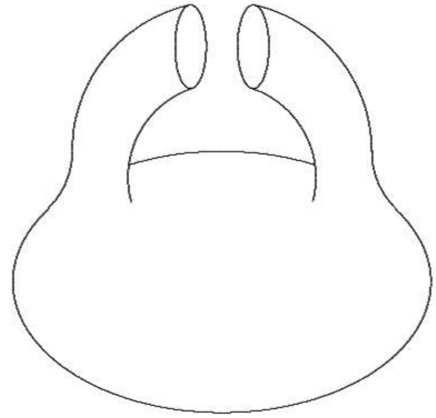


شکل ۴: ساختن انگشت‌ها

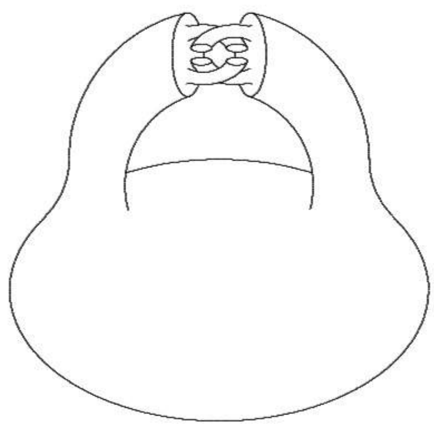
حال می‌توانیم کل ساختار را توضیح بدهیم. یک کره در نظر بگیرید. روی آن دو دیسک انتخاب کنید و از آنها انگشت ها را خارج کنید(بسیار نزدیک به هم ولی بدون برخورد.) (شکل ۵)

حال همانطور که قبلا دیدیم انتهای هر انگشت مشابه یک دیسک است. از هر کدام از این دیسک‌ها دو انگشت دیگرخارج می‌کنیم.

حال ما دو جفت دیسک مسطح نزدیک به هم داریم. مراحل بالا را روی هر جفت از دیسک‌ها انجام می‌دهیم . به همین ترتیب این روند را بی‌نهایت گام ادامه می‌دهیم . ساختاری که به آن می‌رسیم " گوی شاخدار الکساندر" نام دارد . به سختی ممکن به نظر می‌رسد که بتوان طرحی راضی کننده از این ساختار رسم کرد (چرا که انگشت‌ها در هر گام کوچکتر و کوچکتر می‌شوند.) شکل



شکل ۵: قدم اول- دو انگشت از کره خارج شده‌اند.



شکل ۶: قدم دوم- بین انگشتان قفل ایجاد شده است.

بالا تقریبی از این ساختار است.

این ساختار صراحتا یک کره است. در نگاه اول کره بودن این ساختاراندکی شک بر انگیز است. (منظور از کره بودن همیومورفیک بودن با کره است.)

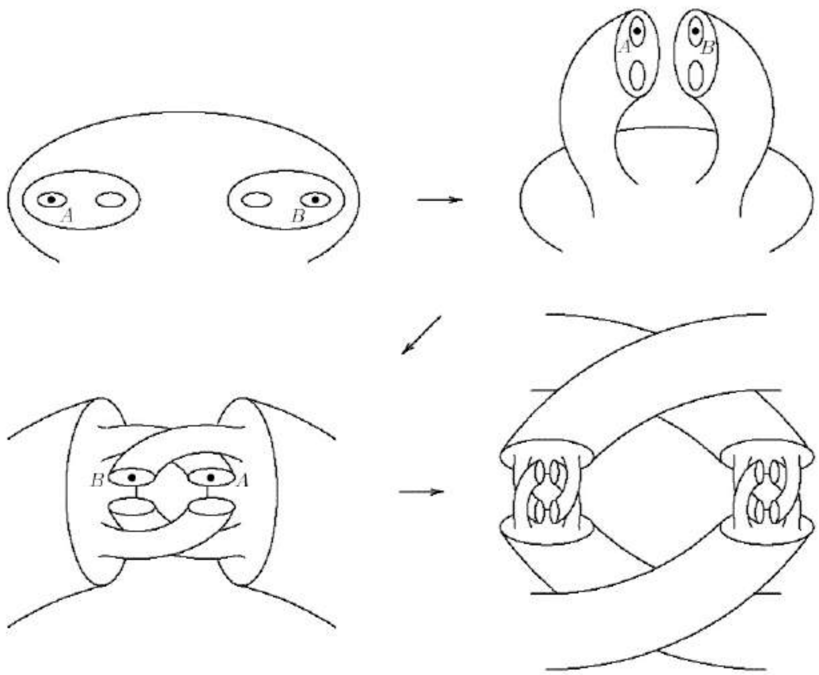
آیا واقعا انتهای انگشت‌ها هرگز با هم برخورد نخواهد کرد؟ ظاهرا آنها به هر اندازه دلخواه به هم نزدیک می‌شوند و در حد به هم می‌پیوندند چرا که در هر گام نیز ما اجزا را به هم نزدیک‌تر می‌کنیم.

اما جواب خیر است و این مشکل کاملا موهومی‌است. ما می‌توانیم همین روند ساخت را به نحوی انجام دهیم که برای هر دو نقطه متفاوت از کره (کره قبل از انجام هر عملی) فاصله‌شان بعد از انجام این عملیات از " مثلا " ۱% فاصله اولی‌شان کمتر نباشد .

عملیات ساخت را قدم به قدم می‌آزماییم . قدم اول ساخت انگشت‌ها، دو دیسک روی یک کره دست نخورده را در بر می‌گیرد. بقیه کره در تمام عملیات دست نخورده باقی می‌ماند. قدم دوم تنها با چهار دیسک کوچکتر کار می‌کند. از مرحله دوم به بعد کل ساختار خارج از این ۴ دیسک بدون تغییر باقی می‌مانند. به طور مشابه ۸ دیسک در مرحله سوم درگیر عملیات هستند، ۱۶ دیسک در مرحله چهارم و ... . دیسک‌های مرحله n ام را با نام دیسک به اندازه n می‌خوانیم. پس ۲^n دیسک از اندازه n داریم و هر دیسک

از اندازه n شامل دو دیسک از اندازه $n+1$ است. نقاطی از کره که در هیچ دیسکی از اندازه n نیستند در عملیات ساخت گوی شاخدار از مرحله n ام به بعد هیچ تغییری نمیکنند.

حال می‌خواهیم فاصله دو نقطه از کره را در طول انجام مراحل بررسی کنیم. دو نقطه متمایز A و B از کره را در نظر بگیرید. اگر نه A و نه B در هیچ دیسکی به اندازه ۱ قرار نداشته باشند فاصله این دو نقطه در طی انجام مراحل تغییر نمی‌کند. اگرفقط یکی از این دو نقطه در دیسکی به اندازه ۱ قرار داشته باشد، آنگاه فاصله آنها به طور محسوسی عوض نمی‌شود به طوری که می‌توانیم فرض کنیم که حتی اگر این فاصله زیاد شود از ۳ برابر مقدار اولیه‌اش بیشتر نمی‌شود. اگر A و B به دو دیسک متمایز از اندازه ۱ متعلق باشند آنگاه بعد از یک گام به طور قابل ملاحظه‌ای به هم نزدیک‌تر می‌شوند ولی می‌توانیم تصور کنیم فاصله شان بیش از ۱۰ مرتبه کاهش نمی‌یابد. بعلاوه اگر دو نقطه به دو دیسک از اندازه ۲ متعلق باشند گام بعدی آن‌ها را باز هم به همدیگر نزدیک‌تر خواهد کرد ولی به طور مشابه نه بیش از ۱۰ مرتبه نزدیکتر. اما حتی اگر دو نقطه به دیسک‌های از اندازه ۲ و ۳ و ... متعلق باشند، نشان می‌دهیم این دو به اندازه کافی به هم نزدیک نخواهند شد.



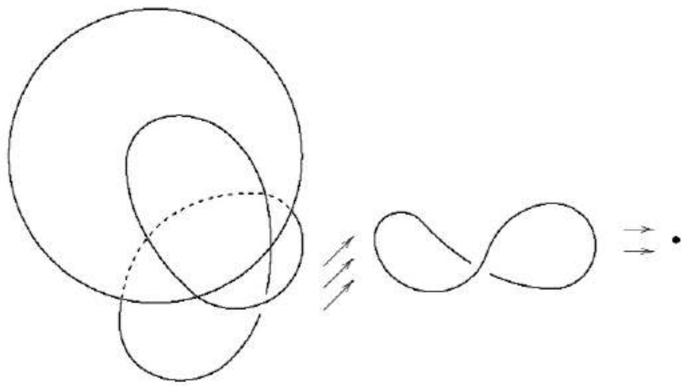
علت این " به‌اندازه کافی به هم نزدیک نشدن " خاصیتی در روش ساخت کره الکساندر است: در مرحله n ام عملیات ما تنها نقاطی را از یک دیسک به‌اندازه $n-1$ به هم نزدیک می‌کنیم.

حال می‌توانیم این خاصیت کلی برای فاصله‌ها را فرموله کنیم. فرض کنیم n بزرگترین عددی باشد که A و B هر دو به یک دیسک به‌اندازه n متعلق باشند. آنگاه فاصله آن دو از گام ۱ ام تا گام n ام بدون تغییر باقی می‌ماند. اگر هیچ کدام به دیسکی به‌اندازه $n+1$ متعلق نباشد فاصله آنها از آن جا به بعد نیز بدون تغییر باقی خواهد ماند پس در کل مراحل فاصله آن‌ها تغییر نمی‌کند. اگر تنها یکی از آن دو به یک دیسک به‌اندازه $n+1$ متعلق باشد فاصله‌شان از ۳ برابر مقدار اولیه بیشتر نمی‌شود. اگر هر دو به دیسک های ازاندازه $n+1$ متعلق باشد (حتما این دو دیسک مختلف‌اند) فاصله‌شان در گام $n+1$ بیش از ۱۰ برابر نخواهد شد. اگر هیچ کدام از دو نقطه به دیسکی ازاندازه $n+2$ متعلق نباشد بعد از گام $n+1$ ام فاصله‌شان بدون تغییر می‌ماند. اگر دقیقا یکی از آن‌ها از دیسکی به‌اندازه $n+2$ باشد در گام $n+2$ فاصله‌شان حداکثر ۳ برابر می‌شود و بعد از آن تغییر محسوسی نمی‌کند. در نهایت اگر A و B هر دو به دیسک‌هایی ازاندازه $n+2$ متعلق باشند در گام $n+2$ ام فاصله‌شان حداکثر ۱۰ برابر شده و بعد آن به طور محسوسی تغییر نخواهد کرد. در همه حالت‌ها فاصله بین A و B از ۱۰۰ برابر فاصله اولیه‌اش بیشتر نخواهد شد.

بنابراین کره شاخدار الکساندر واقعا یک کره (همیومورفیک با یک کره) است.

ناحیه بیرونی کره شاخدار الکساندر

اثبات این گزاره سخت نیست که درون کره شاخدار الکساندر با یک گوی عادی بدون مرز همیومورفیک است ولی ما به آن نیازی نداریم. آنچه که از اهمیت زیادی برخوردار است این است که ناحیه خارجی کره شاخدار الکساندر مشابه (همیومورفیک) با ناحیه خارجی کره عادی نیست. اثبات ادعای اخیر ساده ولی جالب است (از آنجایی که نمونه‌ی خوبی برای یک اثبات توپولوژیک است). ناحیه خارجی کره عادی (مثل درون آن) دارای یک خاصیت توپولوژیک است که همبندی ساده نام دارد: هر خم پیوسته را می‌توان به طور پیوسته به یک نقطه تبدیل کرد. با اینکه بدیهی به نظر می‌آید ولی اثبات دقیق آن به چند تکنیک احتیاج دارد.



شکل ۷: درون کره شاخدار همبند ساده است.

همبندی ساده یک خاصیت توپولوژیک است پس اگر دو ناحیه همیومورفیک باشند و یکی همبند ساده باشد دیگری نیز چنین خواهد بود . ناحیه خارجی کره شاخدار همبند ساده نیست: اگر یک خم بسته دور یک دسته داشته باشیم نمی‌توانیم آن را به طور پیوسته به نقطه ای خارج دسته بکشیم(شکل ۸). (برای بیرون کشیدن این خم بسته باید آن را از میان جفت دیسک‌های موازی از هراندازه رد کنیم بنابراین در فرآیند تغییر شکل خم بسته به نقطه، خم به هراندازه دلخواه به کره شاخدار نزدیک می‌شود که معنی آن این است که بالاخره در لحظه‌ای به کره شاخدار برخورد خواهد کرد که نباید چنین می‌شد چرا که فرآیند تغییر فرم باید در ناحیه خارج کره شاخدار اتفاق بیافتد)

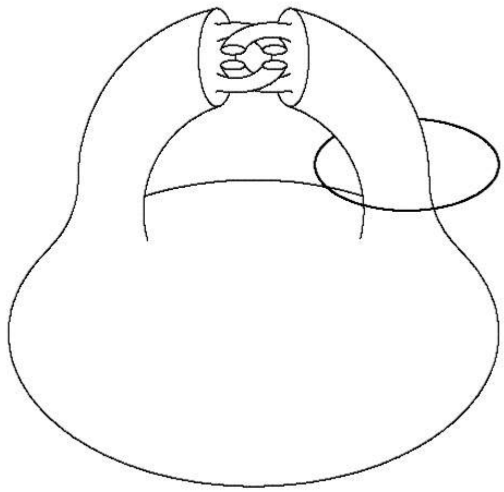
پس خارج کره شاخدار همبند ساده نیست بنابراین با خارج کره عادی همیومورفیک نیست و این نشان می‌دهد که نسخه فضایی قضیه شوئنفلیس صحیح نمی‌باشد.

کمی‌بیشتر از بیرون کره!

حال به راحتی می‌توان باهوش بود! می‌توان شاخ‌ها را به جای بیرون کشیدن از کره به درون آن کشید. آنگاه کره‌ای خواهیم داشت که به جای بیرون آن، درونش همبند ساده نیست و در نتیجه با درون کره عادی همیومورفیک نیست یا می‌توانستیم از ابتدا به جای یک جفت شاخ، دو جفت شاخ از کره خارج کنیم. یک جفت به بیرون کره بکشیم و یک جفت به درون آن. در این صورت هم ناحیه بیرونی کره شاخدار و هم ناحیه درونی کره شاخدار همبند ساده نیستند و با ناحیه بیرونی و درونی کره عادی متفاوت (غیر همیومورفیک) خواهند بود.

نتیجه

پیشرفت های بیشتر: ده‌ها سال از اکتشاف الکساندر می‌گذرد. هنوز توپولوژی‌دان‌ها امیدوارند که نسخه‌ای از قضیه شوئنفلیس برای حالت سه بعدی نیز برقرار باشد: "شاید فقط کافی باشد که شکل‌های بسیار پیچیده را از قضیه مستثنی کرد" یا "اگر فقط اشکال



شکل ۸: خارج کره شاخدار الکساندر همبند ساده نیست.

چندوجهی[۵] را در نظر گرفت آیا قضیه صادق خواهد بود" و ... ولی در این حالت‌ها مساله باز هم بسیار سخت می‌باشد. در سال ۱۹۶۰ مورتن براون[۶] قضیه شوئنفلیس را برای چندوجهی‌ها اثبات کرد.(در حقیقت نتایج براون دسته بیشتری از رویه‌ها را شامل می‌شود.) هم‌چنین قضیه براون در ابعاد بالاتر نیز برقرار می‌باشد. با این وجود در ابعاد بالاتر چندوجهی‌ها هم گاهی ما را شگفت زده می‌کنند. برای نمونه در سال ۱۹۷۰ کربی[۷] و سیبنمان[۸] نشان دادند که دو چندوجهی در فضای ۴ بعدی که یکی درون دیگری است می‌توانند ناحیه‌ای تولید کنند که با ناحیه تولید شده توسط دو کره عادی هم مرکز متفاوت است که البته همه‌ی این‌ها تا جایی فراتر از محدوده این نوشته پیش می‌روند.

مراجع

[1] Dimitry Fuchs and Serge Tabachnikov, Mathematical Omnibus: Thirty Lecture on Classic Mathematics

[۵] polyhedral
[۶] Morton Brown
[۷] Kirby
[۸] L. Siebenmann

پیچش و کاربردهای آن در نظریه های نوین گرانشی

مهدی کوره‌چیان

بعد از گالیله در طول ۲۰۰ سال علم نوین فیزیک پیشرفت های چشمگیری کرد و دانشمندان توانستند با زبان ریاضی بسیاری از پدیده های جهان را تبیین و یا پیش بینی کنند اما یک استثنا وجود داشت. با آنکه پدیده گرانش به زیبایی به زبان ریاضیات فرمول بندی شده بود ، دانشمندان از تفسیر چرایی وجود داشتن گرانش و این خاصیت که ذرات مختلف با جرم های گوناگون در یک میدان گرانشی همگی شتاب ثابتی را اکتساب می کنند عاجز بودند. تا آنکه در سال ۱۹۱۷ آلبرت انشتین توانست بوسیله نظریه نسبیت عام چرایی و علت گرانش را توضیح دهد. او در این نظریه میدان گرانشی را به انحنا که یک خصوصیت هندسی فضا می باشد ربط داد. بر اساس این نظریه فضای خلا به تنهایی تخت مینکوفسکیایی می باشد و وجود ماده در این فضا انحنا ایجاد می کند که به نوبه خود این امر در ساختار ژئودزیک های فضا تغییر ایجاد می کند و باعث می شود اجرام و حتی نوری که در یک میدان گرانشی قرار می گیرند به جای حرکت بر روی مسیر مستقیم ، که خاصیت چارچوب های لخت در فضای مینکوفسکیایی هست، بر روی مسیرهای منحنی وار (ژئودزیک های فضای دارای انحنا) حرکت کنند.

با آنکه نظریه نسبیت عام توانسته بود توجیه مناسبی از پدیده گرانش ارائه کرده و بسیاری از پدیده های کیهان شناختی را با دقت بالایی پیش بینی کند با این حال به دو دلیل زیر به نظریه های نوین گرانشی که دارای مفاهیم جدیدی مانند پیچش هستند احساس نیاز می شد.

۱) به موازات نظریه نسبیت عام ، نظریه مکانیک کوانتومی با ایده های نوین و شگرفش توانسته بود بسیاری از پدیده ها در مقاسه اتمی و ریز اتمی را که مکانیک کلاسیک از تبیین آن عاجز بود توضیح دهد. هر دو نظریه نسبیت عام و مکانیک کوانتومی دو برداشت کاملا متفاوتی از جهان پیرامون ما ارائه می دهند اما چه از لحاظ فلسفی و چه از لحاظ ساختاری ناسازگاری های بزرگی بین این دو نظریه وجود دارد که بخاطر آن ها نمی توان همانند نظریه الکترو مغناطیسی ، که در واقع تلفیق موفقی از دو نظریه الکترواستاتیک و مغناطیس است ، براحتی نظریه واحدی برای آن ها ارائه کرد. مثلا تمام پیش بینی هایی که نظریه مکانیک کوانتومی انجام می دهد بر این اصل که فضای اطراف ما فضای تخت اقلیدسی است استوار شده است حتی برای نظریه کوانتوم فیلد که توسط آن سعی شده اثرهای نسبیتی در آن لحاظ شود رویدادها در فضای تخت مینکوفسکیایی رخ می دهند که این مسئله برخلاف این اصل نسبیت عام می باشد که ماده با ایجاد انحنا در ساختار فضا تغییر ایجاد می کند. در دهه ۲۰ میلادی ریاضیدانان و فیزیکدانان بسیاری تلاش کردند که این تناقض را برطرف کنند مانند کارتان که برای این کار مفهوم پیچش را برای اولین بار وارد مبحث هندسه دیفرانسیل کرد و تلاش کرد آن را جایگزین مفهوم انحنا در نظریه نسبیت عام کند. او این گونه فرض کرد که ماده موجود در عالم به جای انحنا در فضا پیچش ایجاد می کند که در این صورت ساختار فضا تخت می ماند. به زبان ریاضی در فضایی که کارتان درست کرد برعکس فضای ریمانی مولفه های تانسور انحنا برابر صفر و تانسور پیچش مخالف صفر می باشد. با انجام محاسبات ریاضی معلوم شد که نظریه نوین کارتان نتایج کاملا مشابه نظریه نسبیت عام ارائه می دهد و در واقع این دو معادل یکدیگر می باشند. خواننده علاقه مند جهت آشنایی بیشتر با این نظریه می تواند به منبع شماره یک مراجعه کند.

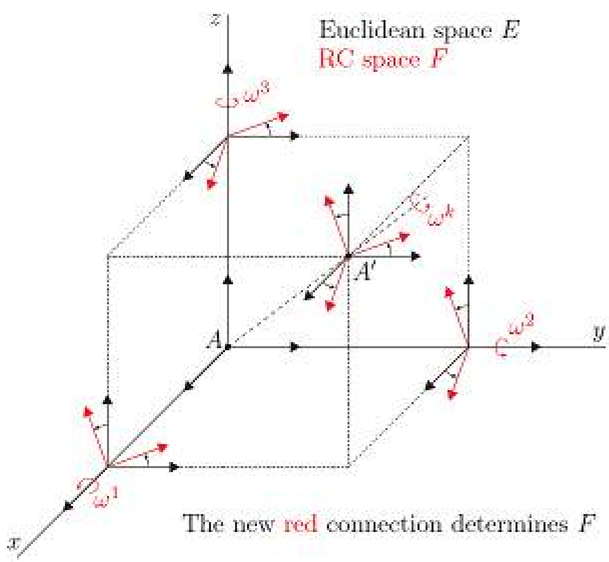
۲) با آن که بسیاری از پیش بینی ها و محاسبات نظریه نسبیت عام در ابعاد کیهانی مشاهده شده تا به امروز دانشمندان نتوانستند به علت ضعیف بودن گرانش نسبت به سایر نیروها آن را تصدیق یا رد کنند. با این همه نظریه ای که بتواند هم شامل اثرات گرانشی و هم اثرات کوانتومی مانند اسپین باشد کامل تر بوده و می تواند دید ما گسترش دهد. برای حصول چنین امری لازم

است که نظریه فوق از درجه آزادی کافی برخوردار باشد تا بتوان توسط آن تاثیرات کوانتومی به همراه ویژگی های نسبیت عام را در یک نظریه واحد لحاظ کرد. نظریه نوین گرانشی که به نظریه کارتان– انشتین معروف است دارای ویژگی بالا می باشد. در این نظریه بر خلاف نسبیت عام و نظریه کارتان فضا هم دارای انحنا و هم پیچش می باشد. بنتبراین نسبت به آن دو تعداد درجات آزادی بیشتری دارد. اما متاسفانه تا کنون آزمایشی طراحی نشده که توسط آن بتوان پیش بینی ها و نتایج حاصله از این نظریه را در بوته آزمایش قرار داد. جهت آشنایی بیشتر با این مطلب می توان به منبع شماره دو مراجعه کرد.

حال که مختصری راجع به نظریه های گرانشی و رابطه آن با پیچش صحبت شد در قسمت بعدی به تاریخچه و مفهوم شهودی هندسی پیچش می پردازیم.

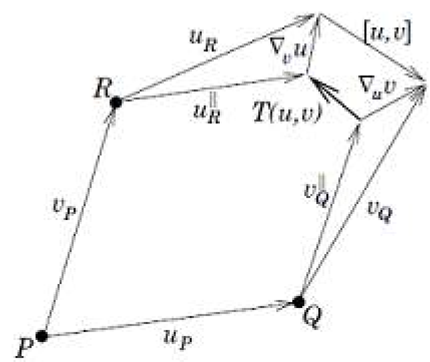
پیچش چیست؟

در سال ۱۹۲۲ ، الی کارتان مفهوم پیچش را در مبحث هندسی دیفرانسیل پایه گزاری کرد. او مفهوم هندسه ریمانی را که بر مبنای تانسور متریک متقارن $g_{ij} = \mathrm{g_{ji}}$ و تانسور انحنای ریمانی R^l_{ijk} بنا شده را به یک مفهوم کلی تر تعمیم داد بطوری که علاوه بر تانسورهای فوق شامل تانسور مرتبه ۳ $T^k_{ij} = -T^k_{ji}$، که توسط کارتان تانسور پیچش نامیده شد ، نیز می باشد.
با آن که به راحتی می توان یک فضای ریمانی دوبعدی را به عنوان یک رویه دوبعدی که در فضای تخت ۳ بعدی اقلیدسی نشانده شده در ذهن تجسم کرد اما هیچ شهود ذهنی ساده ای از یک فضای پیچش دار وجود ندارد. با این حال در اولین مقاله کارتان او از یک فضای ۳ بعدی با یک پیچش همگن به عنوان یک مثال استفاده کرد. این مثال با آنکه برای بدست آوردن یک شهود ذهنی از پیچش بسیار مفید است اما به مرور زمان فراموش شده است. ایده کلی کارتان بصورت زیر است:
یک نقطه دلخواه مانند A را از یک فضای سه بعدی اقلیدسی در دستگاه مختصاتی دکارتی همان گونه که در شکل زیر نمایش داده شده است در نظر می گیریم. نقطه A' را حول همسایگی A انتخاب می‌کنیم.



برداری که A را به A' وصل می‌کند AA' می‌نامیم. حال دستگاه سه‌تایی مختصاتی در A' در راستای برداری $\vec{W} = \alpha AA'$ در جهت راست‌گرد می‌چرخانیم که در اینجا α یک ثابت عددی است. دستگاه مختصاتی سه‌تایی جدید را می‌توان به عنوان یک پایه از فضای پیچشی F در نظر گرفت. فرق یک فضای اقلیدسی که گروه دوران بر روی نقاط اثر کرده با یک فضای پیچشی در این است که در فضای اقلیدسی دوران یافته عمل گروه دوران بر روی تمام نقاط به صورت یکسان عمل می‌کند و فضا همسان‌گرد باقی می‌ماند اما در فضای پیچشی همان‌گونه که از شکل بالا پیداست این‌گونه نمی‌باشد. یک بردار در فضای پیچشی F در نقطه‌ی

A' را موازی یک بردار در نقطه‌ی A گوییم هرگاه مولفه‌های آن در A نسبت به دستگاه مختصاتی ۳تایی موضعی برابر با مولفه‌های آن در دستگاه پیچش یافته در نقطه A' باشد. حال اگر بردار $\vec{W}$ را به مولفه‌های آن در راستای محورهای مختصاتی x, y, z تجزیه کرده و آن‌ها را $w_۱, w_۲, w_۳$ بنامیم و سپس از A' به سمت A حرکت کرده و سپس از آن دور شویم دستگاه مختصاتی سه‌تایی بر روی هریک از محورها بر روی یک مسیر مارپیچ حرکت می‌کند. حال به مفهوم توازی دو بردار را در فضای پیچش F در نقطه A' موازی یک بردار در نقطه A گوییم هرگاه مولفه‌های آن در A نسبت به دستگاه مختصاتی دکارتی موضعی برابر با مولفه‌های آن در نقطه A' در دستگاه مختصاتی پیچش یافته باشد. با آن که تعریف توازی دو بردار در فضای پیچ‌دار F کاملا مشابه فضای اقلیدسی می‌باشد اما یک تفاوت شهودی بین این دو فضا وجود دارد. در فضای اقلیدسی موازی بودن دو بردار معادل هم راستا بودن آن‌ها می‌باشد. اما به علت ساختار فضای پیچ‌دار F از لحاظ شهودی ممکن است دو بردار دارای مولفه‌های برابر باشند اما جهت آن‌ها در یک راستا نباشد. از طرفی دیگر فضای پیچشی دارای یک خاصیت نامتعارف دیگر نیز می‌باشد. فرض کنیم U و V دو بردار دلخواه باشند. در نقطه‌ی دلخواه P این دو را در طول یکدیگر به‌صورت موازی انتقال می‌دهیم و بردارهای حاصله را ${U_R}^{||}$ و ${V_R}^{||}$ می‌نامیم. اگر تانسور پیچش فضا مخالف صفر باشد نمودار حاصله بسته نمی‌شود. شکل زیر این مسئله را به روشنی نشان می‌دهد.



تا این قسمت مقاله سعی شد تا یک درک شهودی از مفهوم پیچش ارائه شود. در قسمت پایانی مقدمه ای از ویژگی های هندسی یک فضای پیچش دار با زبان دقیق ریاضی می پردازیم.

ویژگی هندسی هر نظریه گرانشی کلاف مماسی[۱] که یک ساختار طبیعی بر رزی فضا زمان می باشد. در هر نقطه از این فضا — زمان همیشه یک فضای مماسی وجود دارد که بر روی آن گروه انتقال فضا — زمان عمل می کند. در مورد گروه لورنتز فضای مماسی یک نمایش را برای گروه فراهم می کند که همان نمایش برداری می باشد. در ادامه مقاله ما از حروف یونانی($\mu, \rho, \nu = ۱, ۲, ۳$) برای نمایش اندیس‌های مربوط به فضا-زمان و حروف لاتین کوچک ($a, b, c, \ldots$) برای اندیس‌های فضای مماس استفاده می‌کنیم که همان فضای مینکوفسکی تخت با متریک

$$\eta_{ab} = \mathrm{diag}(+1, -1, -1, -1)$$

اندیس‌های لاتین($i, j, k = ۱, ۲, ۳$) برای نمایش قسمت برای نمایش مختصات فضایی از مختصات فضا-زمان بکار برده می‌شود که با نماد $\{x^\mu\}$ نمایش داده می‌شود در حالی که مختصات فضای مماس را با نماد $\{x^a\}$ نشان خواهیم داد. این سیستم های مختصاتی بر روی دامنه تعریفشان یک پایه برای فضای برداری که توسط مجموعه های

$$\{\partial_\mu\} = \{\frac{\partial}{\partial x^\mu}\} \quad \text{و} \quad \{\partial_a\} = \{\frac{\partial}{\partial x^a}\}$$

درست همانند پایه‌های $\{\mathrm{dx}^\mu\}$ و $\{\mathrm{dx^a}\}$ که به عنوان پایه برای فضای هم بردارها تعریف می‌کند. این پایه‌ها دوگان همدیگر هستند به طوری که

$$\mathrm{dx}^\nu(\partial_\mu) = \delta^\mu_\nu \quad \text{و} \quad \mathrm{dx}^\mu(\partial_\nu) = \delta^\mu_\nu$$

بر روی دامنه تعریف متناظر هر میدان برداری یا میدان هم‌برداری توسط ترکیبی از این پایه‌ها به وجود می‌آید. یک پایه هولونوم مانند $\{\partial_a\}$ که با مختصات رابطه دارد یک مثال خاص از پایه‌های خطی می‌باشد. هر میدان مستقل خطی چهارتایی $\{e^a\}$ یک پایه‌ی

[۱] tangent bundle

دیگر تشکیل می‌دهند که دوگان آن‌ها به صورت $\{e_a\}$ می‌باشند و در خاصیت $e^a(e_b) = \delta^a_v$ صدق می‌کنند. این چارچوب ها حالت کلی پایه های خطی روی یک منیفلد دیفرانسیل پذیر فضا — زمان می باشند. البته بر روی دامنه مشترک اعضای یک پایه را می توان بر اساس پایه ای دیگر نوشت که از قانون زیر تبعیت می کنند.

$$e_a = e^\mu_a \partial_\mu \qquad \text{و} \qquad e^a = e^a_\mu \mathrm{dx}^\mu$$

این چارچوب ها به همراه کلاف هایشان اجزای تشکیل دهنده فضا — زمان می باشند. آن ها بصورت خودکار هنگامی که فضا زمان را بصورت یک منیفلد دیفرانسیل پذیر ظاهر می شوند. از این به بعد از علامت های $\{h^a, h_a\}$ برای یک میدان چهارتایی نوعی استفاده می کنیم. یک میدان از چارچوب های خطی که به حضور یک میدان گرانشی ربط داده شده است. فرض کنیم g متریک فضا-زمان با اجزای $g_{\mu\nu}$ باشد که در یک پایه هولونوم دوگان $\{\mathrm{dx}^\mu\}$ به‌صورت

$$g = g_{\mu\nu} \mathrm{dx}^\mu \otimes \mathrm{dx}^\nu = \mathrm{g}_{\mu\nu} \mathrm{dx}^\mu \mathrm{dx}^\nu$$

نشان داده می‌شود. یک میدان چهارتایی $h_a = h^\mu_a \partial_\mu$ متریک g را به فضای متریک مماسی $\eta = \eta_{ab} \mathrm{dx^a dx^b}$ را از طریق رابطه‌ی $\eta_{ab} = g(h_a, h_b) = g_{\mu\nu} h^\mu_a h^\nu_b$ تبدیل می‌کند.

این بدان معناست که یک میدان چهارتایی یک چهارچوب خطی است که اعضای آن h_aها در متریک g شبه عمود هستند. اجزای مولفه‌های پایه دوگان در شرط $h_a = h^\mu_a \mathrm{dx}^\mu$ و روابط

$$h^\mu_a h^a_\nu = \delta^\mu_\nu \qquad \text{و} \qquad h^a_\mu h^\nu_a = h^\nu_\mu$$

نیز صدق می‌کنند. در نتیجه با توجه به روابط بالا داریم:

$$g_{\mu\nu} = \eta_{ab} h^a_\mu \nu$$

ناهولونومی که خاصیت یک فرم دیفرانسیل است که دیفرانسیل هیچ چیزی نیست یا یک میدان برداری که گرادیان نیست در بسیاری از بخش های فیزیک مانند گرما یا کار کلربرد فراوانی دارد. در مورد گرانش ناهولونوم بودن با اصل هم ارزی نسبیت عام و میدان گرانشی ارتباط نزدیکی دارد. اگر یک متریک ریمانی داده شده باشد بودن یا نبودن یک میدان گرانشی متناظر با ویژگی هولونوم و یا ناهولونوم بودن فرم های $h_a = h^\mu_a \mathrm{dx}^\mu$ می‌باشد. ما می‌توانیم تغییر مختصات $\{x^a \to x^\mu\}$ که به وسیله‌ی رابطه‌های $\mathrm{dx}^\mu = (\partial_\mathrm{a} \mathrm{x^a}) \mathrm{dx^a}$ و $\mathrm{dx^a} = (\partial_\mu \mathrm{x^a}) \mathrm{dx}^\mu$ بدست می‌آید. یک فرم $\mathrm{dx^a}$ هولونوم است که در واقع همان مشتق مختصات x^a می‌باشد و موجوداتی مانند $\partial_\mu x^a$ مولفه‌های فرم هولونومیک $\mathrm{dx^a}$ که در پایه dx^μ نوشته می‌شود. در نتیجه تغییر مختصات فقط یک تغییر در پایه هولونومیک از یک فرم‌ها می‌باشد. برای پایه دوگان رابطه‌های

$$\partial_\mu = (\partial_\mu x^a) \partial_a \qquad \text{و} \qquad \partial_a = (\partial_\mu x^\mu) \partial_\mu$$

حال یک پایه دوگان مانند h^a را طوری در نظر می‌گیریم به طوری که $\mathrm{dh^a} \neq 0$ باشد. به بیان دیگر دیفرانسیل هیچ فرمی نباشد. حال اگر یک فرم ناهولونوم h^a را روی $\frac{\partial}{\partial_\mu}$ اثر دهیم نتیجه آن یعنی $h^a_\mu = h^a(\partial_\mu)$ مولفه‌های $h^a = h^a_\mu \mathrm{dx}^\mu$ در طول dx^μ می‌باشند. این دستورالعمل را می‌توان هنگامی که h^a مستقل خطی هستند به‌صورت معکوس انجام داد و میدان‌های برداری $h_a = h^\mu_a \partial_\mu$ که گرادیان هیچ برداری نیستند را تعریف کرد. چون فرم‌های بسته به صورت موضعی دقیق هستند معیار هولونوم بودن یا ناهولونوم بودن را می‌توان این‌گونه تعریف کرد:

یک فرم دیفرانسیل هولونوم است اگر و تنها اگر مشتق خارجی آن برابر صفر شود. یک چهارتایی هولونوم همیشه بصورت $h^a = \mathrm{dx^a}$ از یک مجموعه مختصاتی $\{x^a\}$ می‌باشند. برای این چهارتایی تانسور $g_{\mu\nu}$ به سادگی همه اجزای متریک لورنتز η را در دستگاه مختصاتی $\{\mathrm{dx}^\mu\}$ ارائه می‌کند. یک پایه ناهولونوم $\{h_a\}$ در شرط

$$[h_a, h_b] = f^c_{ab} h_c$$

صدق می‌کند که f^c_{ab} را ضرائب ساختار یا ضرائب ناهولونومی می‌نامند. چارچوب $\{\partial_\mu\}$ که در بالا ذکر شده را کاملا هولونوم در نظر می‌گیریم چرا که اعضای آن با هم جابه‌جا می‌شوند. عبارت دوگان جدول جابه‌جاگر بالا همان ساختار معادله کارتان

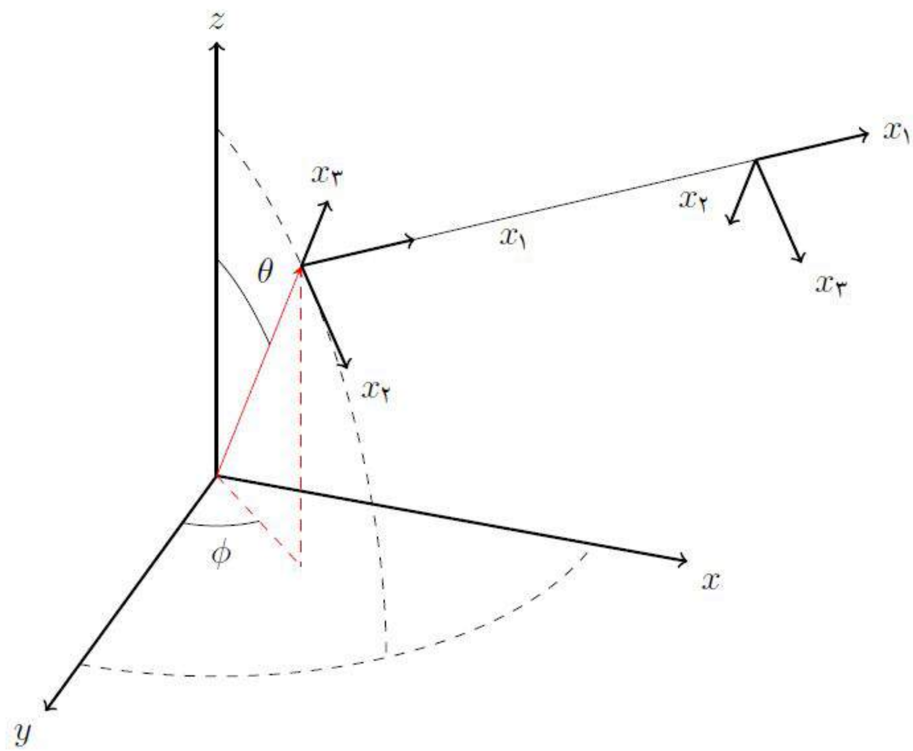
$$\mathrm{dh^c} = -\frac{1}{2} \mathrm{f^c_{ab} h_a} \wedge \mathrm{h_b} = \frac{1}{2} (\partial_\mu \mathrm{h}^\mathrm{c}_\nu - \partial_\nu \mathrm{h}^\mathrm{c}_\mu) \mathrm{dx}^\mu \wedge \mathrm{dx}^\nu$$

می‌باشند. ضرائب ساختاری نمایانگر هسته اجزای پایه هستند.

$$f^c_{ab} = h^c([h_a, h_b]) = h^\mu_a h^\nu_b (\partial_\mu h^c_\nu - \partial_\nu h^c_\mu) = h^\mu_c (h_a(h^\mu_b) - h_b(h^\mu_a))$$

اگر $f^c_{ab} = ۰$ باشند، آنگاه $\mathrm{dh^a} = 0$ می‌شود که این امر وجود توابع مختصاتی موضعی x^a را به‌طوری که $h^a = \mathrm{dx^a}$ تضمین می‌کند که این همان مسئله (چهارتایی هنگامی گرادیان است که هسته آن برابر صفر باشد) را تداعی می‌کند.

حال که با شهود هندسی پدیده‌ی پیچش آشنا شدیم، برای درک بهتر مسئله آن را به بیان دقیق ریاضی برای فضای $\mathbb{R}^3$، محاسبه می‌کنیم و هموستار[2] متناظرش را به دست می‌آوریم. فرض کنیم نقطه‌ی دلخواه A داده شده است و می‌خواهیم دستگاه راستگرد مختصاتی را به نقطه‌ی B انتقال موازی دهیم. برای سهولت در انجام محاسبات فرض می‌کنیم محور x در راستای $\frac{\bar{AB}}{|\bar{AB}|}$ به‌صورت موازی منتقل می‌شود. پیچش باعث می‌شود تا محور متعامد $(z-y)$ در این انتقال موازی در راستای محور x به اندازه‌ی α دوران کند. که در شکل زیر می‌توان مشاهده کرد.



حال اگر رابطه‌ی $\nabla = \nabla^{\parallel} + \nabla^{\perp}$ را در نظر بگیریم، نمایش ماتریس متناظر با این انتقال موازی به صورت

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

از طرفی با توجه به رابطه $\nabla_X^Y = \lim_{t\to 0} \frac{1}{t}(p^{-1}(\gamma(a(t)) - \gamma(0)))$ که در اینجا p انتقال موازی بردار γ در راستای خم $a(t)$ با شرایط اولیه $a(0) = A$، $a'(0) = X$ و همچنین رابطه

$$\nabla_{\frac{\partial}{\partial x_j}}^{\frac{\partial}{\partial x_i}} = \sum_{k=1}^{n} \Gamma_{ij}^k \frac{\partial}{\partial x_k}$$

داریم:

$$\nabla_{\frac{\partial}{\partial x_1}}^{\frac{\partial}{\partial x_2}} = \lim_{\theta\to 0} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\sin\theta & \cos\theta \\ 0 & \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \sum_{k=1}^{3} \Gamma_{12}^k \frac{\partial}{\partial x_k}$$

[2] Connection

$$\nabla_{\frac{\partial}{\partial x_1}} \frac{\partial}{\partial x_2} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \frac{\partial}{\partial x_3} = \sum_{k=1}^{3} \Gamma_{12}^{k} \frac{\partial}{\partial x_k}$$

$$\Gamma_{12}^{1} = \Gamma_{12}^{2} = 0 \ , \quad \Gamma_{12}^{3} = 1$$

با استفاده از این روش می‌توان تمام ضرایب کریستوفر Γ_{ij}^{k}ها را به‌دست آورد. Γ_{ij}^{k} دارای خاصیت تانسوری نمی‌باشد، چرا که اگر فرض کنیم Γ_{ij}^{k} ضرایب کریستوفر متناظر با هموستار ∇ بر روی باز $\mathcal{U}$ با بردارهای پایه $\{\frac{\partial}{\partial u_1}, \cdots, \frac{\partial}{\partial u_n}\}$ و ${\Gamma_{ij}^{k}}'$ مربوط به هموستار ∇' بر روی باز $\mathcal{V}$ با بردارهای پایه $\{\frac{\partial}{\partial v_1}, \cdots, \frac{\partial}{\partial v_n}\}$ باشند به طوری که $\mathcal{U} \cap \mathcal{V} \neq \emptyset$ آن‌گاه تحت تغییر مختصات اجزای هموستار ∇' از رابطه‌ی

$${\Gamma_{ik}^{j}}' = \Gamma_{pr}^{q} \frac{\partial v^j}{\partial u^q} \frac{\partial u^p}{\partial v^i} \frac{\partial u^r}{\partial v^k} + \frac{\partial^2 u^p}{\partial v^i \partial v^k} \frac{\partial v^j}{\partial u^p}$$

به دست می‌آید و عبارت $\frac{\partial^2 u^p}{\partial v^i \partial v^k} \frac{\partial v^j}{\partial u^p}$ عبارت اضافی است. اما اگر تفاضل دو مولفه Γ_{ij}^{k} و Γ_{ji}^{k} در نظر بگیریم، این عبارت زائد حذف شده و عبارت حاصل از قانون تغییر مختصات یک تانسور ۲-هموورد،۱-ناهموورد تبعیت می‌کند. این تانسور را با T_{ij}^{k} نمایش می‌دهیم:

$$T_{ij}^{k} = \Gamma_{ij}^{k} - \Gamma_{ji}^{k}$$

واضح است که T_{ij}^{k} یک تانسور پادمتقارن است. خواننده‌ی علاقه‌مند می‌تواند مولفه‌های این تانسور را برای فضای $\mathbb{R}^3$ به‌دست آورد.

هموستار همراه با پیچش

هنگامی که بخواهیم عمل مشتق را با یک رابطه تانسوری خوش تعریف تعریف کنیم ، بسیار حیاتی است که هموستار $\Gamma_{\nu\mu}^{\lambda}$ را معرفی بکنیم که در اندیس آخر دارای خاصیت برداری هستند ولی قسمتی از آن ها که رفتار تانسوری ندارند همان دو مولفه اول این هموستار می باشند. هموستارهای خطی دارای خصوصیات زیادی از فضا — زمان هستند چرا که بر روی کلاف چارچوب های خطی تعریف شده اند که یک قسمت تشکیل دهنده از ساختار منیفلد می باشند. هموستارهای خطی بخصوص هموستارهای لورنتزی همیشه دارای پیچش مخالف صفر هستند . یادآوری این مسئله که انحنا و پیچش خصوصیات هموستار فضا هستند بسیار مهم می باشد. به بیان دیگر چیزی بنام انحنا و پیچش در فضا - زمان وجود ندارد بلکه این دو ویژگی های مفهوم محض هموستار می باشند و می توانیم بر روی یک فضا هموستارهای گوناگونی تعریف کرد. البته وقتی به مورد نسبیت عام محدود می شویم که تنها هموستار موجود هموستار لوی— چیوتاست ، فراگیر بودن گرانش این اجازه را می دهد که به عنوان یکی از خصوصیات فضا — زمان تفسیر بشود. اما در حضور هموستارهای مختلف به همراه انحنا و پیچش های گوناگون بسیار منطقی به نظر می رسد که فضا— زمان را به عنوان یک منیفلد و هموستارها را به عنوان یک ساختار اضافی که روی آن منیفلد تعریف می شود در نظر بگیریم.

هموستار اسپین‌دار A یک هموستار به‌صورت

$$A_\mu = \frac{1}{2} A_{ab}^{\mu} S_{ab} \tag{1}$$

با خاصیت $S_{ab} = -S_{ba}$ مولدهای لورنتز در یک نمایش داده شده می‌باشند. از طرف دیگر یک میدان چهارتایی تانسورهای داخلی با خارجی را مربوط می‌کند. به‌طور مثال اگر V^α یک بردار لورنتزی باشد آن‌گاه

$$V^\rho = h_a^\rho V^a \tag{2}$$

یک بردار فضا— زمان خواهد بود. با این حال در یک مورد خاص از هموستارها یک شرط خلا اضافی وقتی که اندیس وقتی که می خواهیم از اندیس داخلی به اندیس خارجی تغییر دهیم ظاهر می شود که برعکس این امر نیز صادق می باشد. در واقع یک هموستار خطی عمومی مانند $\Gamma_{\mu\nu}^{\rho}$ به هموستار اسپینی A_{ab}^{μ} از طریق رابطه

$$\Gamma_{\mu\nu}^{\rho} = h_a^\rho \partial_\mu h_a^\mu + h_a^\rho A_{b\mu}^{a} h_b^\mu \tag{3}$$

و همچنین با توجه به معادلات ۱ و ۲ و معکوس رابطه ۳ از معادله

$$A_{b\mu}^{a} = h_\nu^a \partial_\mu h_\nu^b + h_\nu^a \Gamma_{\rho\mu}^{\nu} h_b^\rho \tag{4}$$

مربوط می شوند. معادلات ۳ و ۴ در واقع راه های گوناگون از بیان این خاصیت که مشتق هموردا برای هر دو اندیس وقتی که روی چهار بردار فضا زمان اثر می کند همه جا برابر صفر می شود.

$$\partial_\mu h^a_\nu - \Gamma^\rho_{\mu\nu} h^a_\rho + A^a_{b\mu} h^b_\nu = 0 \quad (5)$$

یک هموستار $\Gamma^\rho_{\lambda\mu}$ را سازگار با متریک گوییم هرگاه

$$\partial_\lambda g_{\mu\nu} - \Gamma^\rho_{\mu\lambda} g_{\rho\nu} - \Gamma^\rho_{\nu\lambda} g_{\mu\rho} = 0 \quad (6)$$

اگر از نقطه نظر یک چهاربردار به مسئله نگاه کنیم و با توجه به معادلات ۳ و ۴، رابطه فوق را می توان بصورت

$$h_\mu(\eta_{ab}) - A^d_{a\mu}\eta_{db} - A^d_{b\mu}(\eta_{ad}) = 0 \quad (7)$$

نوشت، به طوری که $h_\mu = h^a_\mu \partial_a$ است. چون $h_\mu(\eta_{ab}) = 0$ داریم

$$A_{ba\mu} = -A_{ab\mu} \quad (8)$$

انحنا و پیچش هموستار $A^a_{b\mu}$ به صورت مشابه توسط معادلات

$$R^a_{b\mu\nu} = \partial_\nu A^a_{b\mu} - \partial_\mu A^a_{b\nu} + A^a_{e\nu} A^e_{b\mu} - A^a_{e\mu} A^e_{b\nu} \quad (9)$$

و

$$T^a_{\mu\nu} = \partial_\nu h^a_\mu - \partial_\mu h^a_\nu + A^a_{e\mu} A^e_{b\nu} - A^a_{e\nu} A^e_{b\nu} \quad (10)$$

بدست می آید. اگر از رابطه ۴ در روابط بالا استفاده کنیم روابط بالا را می توانیم کاملا بر حسب فرم فضا — زمان بنویسیم که به معادله

$$R^\rho_{\lambda\nu\mu} = h^\rho_a h^\lambda_b R^a_{b\nu\mu} = \partial_\nu \Gamma^\rho_{\lambda\mu} - \partial_\mu \Gamma^\rho_{\lambda\nu} + \Gamma^\rho_{\nu\eta}\Gamma^\eta_{\lambda\mu} - \Gamma^\rho_{\eta\mu}\Gamma^\eta_{\lambda\nu} \quad (11)$$

$$T^\alpha_{\mu\nu} = h^\rho_a T^\alpha_{\mu\nu} = \Gamma^\rho_{\nu\mu} - \Gamma^\rho_{\mu\nu} \quad (12)$$

می رسیم. ضرائب هموستار را می توان به دو قسمت تجزیه کرد

$$\Gamma^\rho_{\mu\nu} = \Gamma^{\dot\rho}_{\mu\nu} + K^\rho_{\mu\nu} \quad (13)$$

به‌طوری که

$$\Gamma^{\dot\rho}_{\mu\nu} = \frac{1}{2} g^{\sigma\rho}(\partial_\mu g_{\rho\nu} + \partial_\nu g_{\rho\nu} - \partial_\rho g_{\mu\nu}) \quad (14)$$

همان قسمت بدون پیچش هموستار ریمانی لوی چیوتا در نسبیت عام و

$$K^\rho_{\mu\nu} = \frac{1}{2}(T^\rho_{\nu;\mu} + T^\rho_{\mu;\nu} - T^\rho_{\mu\nu}) \quad (15)$$

تانسور هم پیچش[3] می باشد. در مورد هموستار اسپینی تجریه معادله ۱۳ به‌صورت

$$A^c_{a\mu} = A^{\dot c}_{a\mu} + K^c_{a\mu} \quad (16)$$

که $A^{\dot c}_{a\mu}$ ضریب ریچی از دوران همان هموستار اسپینی در نسبیت عام فرض می شود. چون هموستار اسپینی در اندیس آخرش خاصیت تانسوری دارد می توانیم آن را به فرم معادله

$$A^a_{bc} = A^a_{b\mu} h^\mu_c \quad (17)$$

بنویسیم. به راحتی می توان مشاهده کرد در پایه ناهولونوم h_a مولفه های انحنا و پیچش بترتیب از طریق روابط

$$R^a_{bcd} = h_c(A^a_{bd}) - h_d(A^a_{bc}) + A^a_{ec} A^a_{bd} - A^a_{ed} A^e_{bc} + f^e_{cd} A^a_{be} \quad (18)$$

و

$$T^a_{bc} = -f^a_{bc} + A^a_{cb} - A^a_{bc} \quad (19)$$

[3]cotorsion

بدست می آیند. در نتیجه پیچش شامل ناهولونومی است. اگر معادله بالا را برای سه ترکیب مختلف از اندیس ها بکار ببریم داریم

$$A^a_{bc} = -\frac{۱}{۲}(f^a_{bc} + T^a_{bc} + f^a_{bc} + T^a_{bc} + f^a_{cb} + T^a_{cb}) \quad (۲۰)$$

وقتی پیچش همانند نظریه نسبیت عام محو می شود ما به همتن ضرائب ریچی از دوران در پایه ناهولونوم

$$A^{\dot a}_{bc} = -\frac{۱}{۲}(f^a_{bc} + f^a_{bc} + f^a_{cb}) \quad (۲۱)$$

می‌رسیم.

مراجع

[1] Gravitation in search of missing torsion .R.Aldrovandi, Arxiv :0801.4148v1

[2] Cartan's theory in geometry and field theory , an essay. Friedrich W. Hehl

[3] Cartan's spiral staircase in physics and in particular in gauge theory of dislocations. Marcus Lazar and Friedrich W. Hehl

مسایلی در اُریگامی‌محاسباتی

کاوه حسینی

مسائل مربوط به تا کردن و باز کردن کاغذ از از اوایل سده‌ی پانزدهم میلادی مورد توجه بوده ولی تا سالهای های اخیر به شکل جدی از لحاظ ریاضیات مورد مطالعه قرار نگرفته بود. این مسایل در چند سال اخیر در حوزه‌ی هندسه‌ی گسسته و محاسباتی مورد توجه قرار گرفته است. در ادامه شرح مختصری از کارهای اصلی انجام شده در این حوزه را ارایه‌ی دهیم. بیشتر مطالب این مقاله در رساله‌ی دکتری اریک دیمین [D۰۱] آمده است.

در واقع هدف کلی بررسی نحوه‌ی تغییر شکل دادن اشیایی هندسی با توجه به محدودیتهای خاص وابسته به شئ است. مانند پیوند[۱] ،قطعه‌ی کاغذ و چند ضلعی.

در ادامه این سه نوع شیئ هندسی را به طور جداگانه بررسی می‌کنیم.

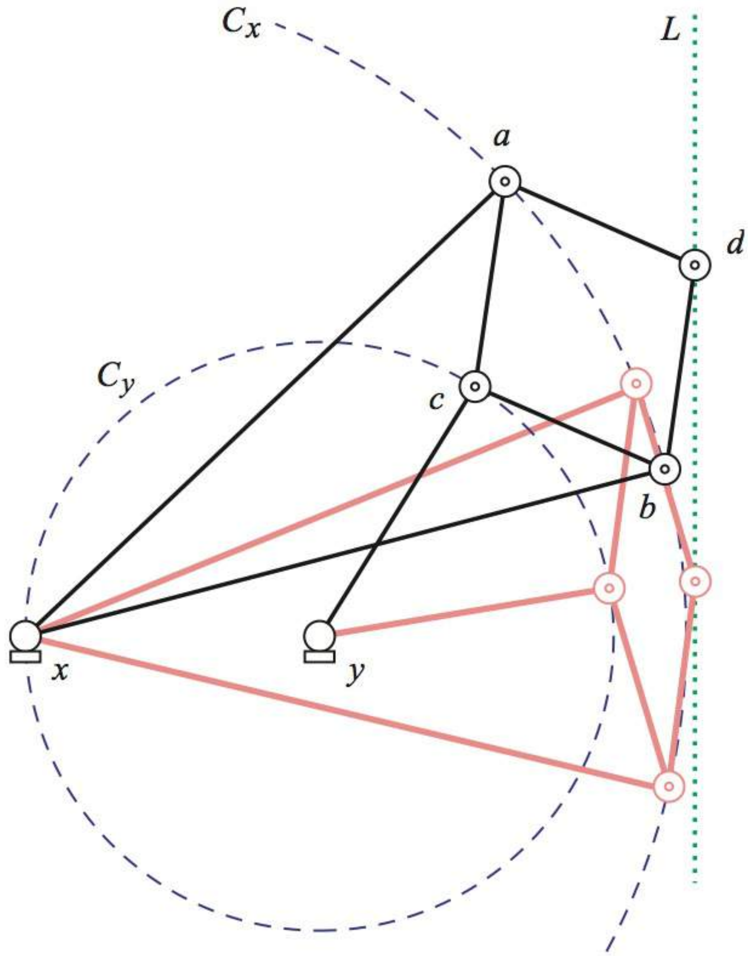
پیوند یا چارچوب[۲] به مجموعه ای از پاره خط ها گفته می‌شود که از نقاط انتهایی(رئوس) به هم وصل شده اند و یک گراف را به وجود آورده اند. یک پیوند را می‌توان در فضای $\mathbb{R}^d$ تاکرد[۳] به این مفهوم که می‌توان رئوس را طوری حرکت داد که طول پاره خط ها تغییر نکند. یک مثال از تا کردن پیوند را در شکل ۱ می‌بینید.

در حالتی که پاره خط ها بتوانند هم دیگر را قطع کنند این مسئله بسیار مطالعه شده است. البته این پیوند ها حتی در صفحه می‌توانند بسیار پیچیده شوند. در ۱۸۷۶ کمپ[۴] [Kem۷۶] نشان داد که یک پیوند مسطح پیوند وجود دارد که یک راس آن روی نمودار یک تابع چند جمله ای دلخواه قرار حرکت می‌کند. هوپکرافت[۵]، جوزف[۶] و وایتسایدز[۷] [HJW۸۴] نشان دادند مسئله‌ی تعیین اینکه آیا یک پیوند دلخواه را می‌توان به یک پیکربندی دلخواه داده شده تبدیل کرد یک مسئله‌ی PSPACE-Complete است. یک نشاندن یک پیوند در فضای $\mathbb{R}^d$ یک پیکربندی یا یک حالت می‌نامیم و به مجموعه‌ی همه‌ی پیکربندی‌های یک پیوند، فضای پیکربندی[۸] می‌گوییم. جوردن[۹] و اشتاینر[۱۰] [JS۹۹] ثابت کردند برای هر چندگونای جبری حقیقی[۱۱] دلخواه Z با توپولوژی اقلیدسی ، یک پیوند مسطح[۱۲] وجود دارد که فضای پیکر بندی آن با Z هم ریخت است. بنابراین پیوند های مسطح با نظریه‌ی حل دستگاه نامساوی چندجمله ای ها روی اعداد حقیقی یکسان است. از طرفی برای هر پیوندی که گراف آن یک دور است ، هر عضوی از فضای پیکر بندی آن را می‌توان با دنباله ای از حرکت ها (تا کردن و انتقال) در فضای $\mathbb{R}^d, d > ۲$ روی یک پیکر بندی دلخواه اولیه بدست آورد [Salv۳ ، LW۹۵]

اخیرا کارهای زیادی روی حالتی که پیوند باید ساده باشد (هیچ دو پاره خطی همدیگر را قطع نکنند.) انجام شده است[۱۳].

[۱] Linkage
[۲] Framework
[۳] Fold
[۴] Kempe
[۵] Hopcroft
[۶] Joseph
[۷] Whitesides
[۸] Configuration Space
[۹] Jordan
[۱۰] Steiner
[۱۱] Real Algebraic variaty
[۱۲] Planar Linkage

[۱۳] البته پاره خط ها می‌توانند مماس باشند.



شکل ۱: یک مثال از تا کردن پیوند

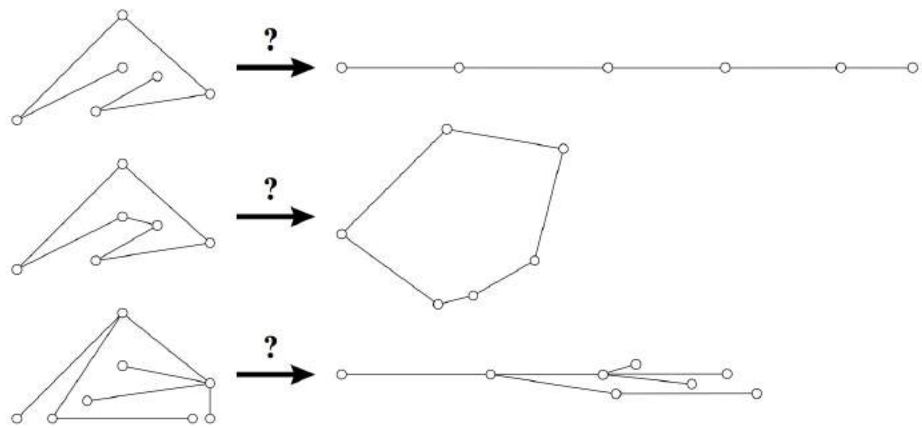
این نسخه از مسئله کاربردهایی درخم کردن لوله های آب[۱۴] [O'R۹۸] و برنامه‌ریزی حرکت[۱۵] بازوی ربات ها دارد. همچنین این مسئله در تا کردن پروتئین[۱۶] ها در زیست شناسی مولکولی هم کاربردهای مهمی‌پیدا کرده است.

شاید بنیادی ترین مسئله ای که راجع به تا کردن پیوند ها بتوان مطرح کرد این است که آیا می‌توان با تا کردن و انتقال از هر پیکربندی به پیکر بندی دیگر رسید؟ حال با توجه به اینکه این حرکت ها برگشت پذیراند سوال را می‌توان به شکل دیگری بیان کرد. آیا می‌توان هر پیکربندی را به یک پیکربندی کانونی[۱۷] تبدیل کرد؟ البته تعریف پیکر بندی کانونی به نوع پیوند بستگی دارد.

در حالتی که پاره خط ها نمی‌توانند همدیگر را قطع کنند سه نوع پیوند (با توجه به ساختار گراف مربوطه) به طور معمول مطالعه می‌شوند: یک مسیر چندضلعی باز ، درخت چندضلعی و دور چند ضلعی یا همان چند ضلعی ساده. در زیر پیکر بندی های کانونی ذکر شده را می‌بینید.

حال مسئله‌ی اولیه به این تبدیل می‌شود: آیا هر زنجیری را می‌توان راست ، هر چند ضلعی را محدب و هر درخت را مسطح کرد؟ جواب این مسئله به بعد فضای اولیه‌ی پیوند و بعد فضایی که پیوند را در آن تا می‌کنیم بستگی دارد. در سالهای اخیر این دسته

[۱۴] hydraulic tube bending
[۱۵] motion planning
[۱۶] protein folding
[۱۷] Canonical configuration

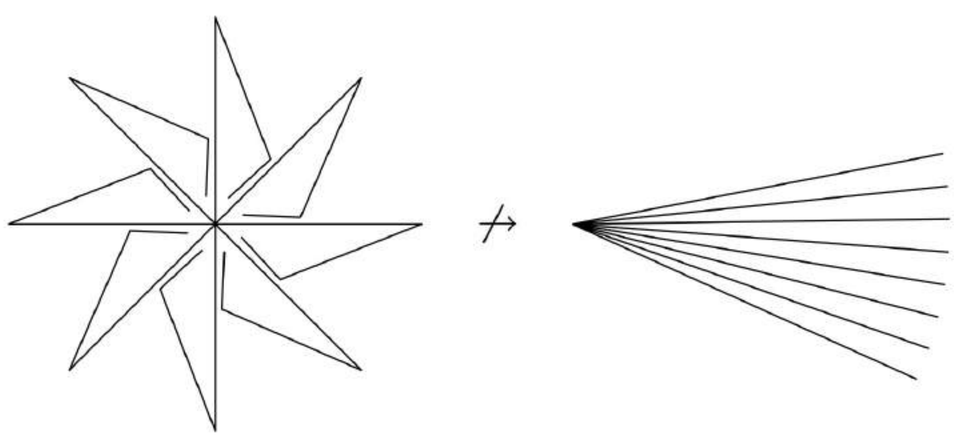


از مسایل به طور کامل حل شده‌اند. در جدول زیر برای حالتی که فضای اولیه و فضای تا کردن هم بعد باشند نتایج را میبینید.

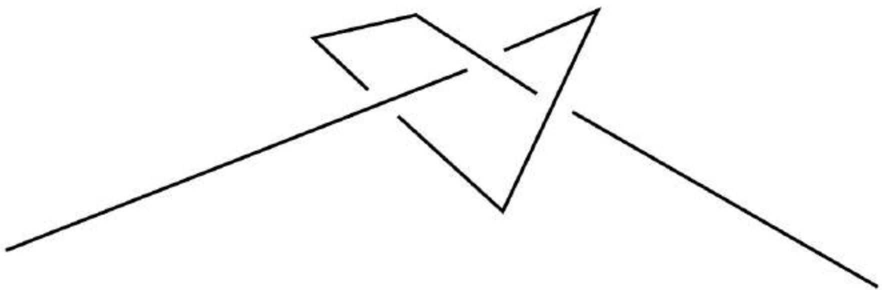
بعد	آیا هر زنجیری را می‌توان راست کرد؟	آیا هر چندضلعی را می‌توان محدب کرد؟	آیا هر درخت را می‌توان مسطح کرد؟
۲	بله(در ادامه)	بله(در ادامه)	خیر[BDD+۰۱b]
۳	خیر[CJ۹۸،BBD+۰۱a]	خیر[CJ۹۸،BBD+۰۱a]	خیر
بالاتر	بله[CO۹۹،CO۰۱]	بله[CO۹۹،CO۰۱]	بله[CO۰۱]

مسئله‌ی خط‌کش‌نجار: زنجیرهای چندضلعی در صفحه

مسئله‌ی راست کردن زنجیر با نام مسئله‌ی خط کش نجار شناخته شده است. زیرا خط کش نجار ها مانند یک زنجیر چند ضلعی تا میشود. این مسئله را بعدا بررسی می‌کنیم.
بیدل و بقیه[BDD+۰۱b] نشان دادند همه‌ی درخت ها را نمی‌توان مسطح کرد. مثال نقض آنها را در زیر می‌بینید.



در واقع به طور شهودی می‌توان گفت هیچ پاره خطی را نمی‌توان حرکت داد مگر اینکه فضای کافی برای دوران آن موجود باشد.
مسایل مربوطه در بعد ۳ توسط اردوش [Erd۳۵] در ۱۹۳۵ برای اولین بار مطرح شد. فرض کنید پیوند اولیه در فضای ۳ بعدی باشد. به طور کلی یک زنجیر چندضلعی یا یک چند ضلعی بدون گره در فضای ۳ بعدی را نمی‌توان به پیکر بندی کانونی تبدیل کرد [CJ۹۸،Tou۰۱،BDD+۰۱a] . شکل زیر یک گره را در ۳ بعد نشان می‌دهد.



مسئله‌ی تعیین اینکه یک مسیر چندضلعی یا یک دور چندضلعی بدون گره را می‌توان به ترتیب راست یا محدب شود هنوز باز است و تنها کران بالای موجود الگوریتمی PSpace است[Can۸۷،Can۸۸].
در ابعاد ۴ و بالاتر همه‌ی گره ها را می‌توان باز کرد ، به عبارتی هر مسیر چندضلعی را می‌توان راست و هر دور چند ضلعی را می‌توان محدب کرد.[CO۹۹،CO۰۱]

کاربرد در تا کردن پروتئین

تا کردن پروتئین مسئله‌ی مهمی‌در زیست شناسی مولکولی است به طوری که نحوه‌ی تا شدن پروتئین به طور کلی رفتار آن را تعیین می‌کند.
پروتئین را می‌توان با یک پیوند مدل کرد به طوری که رئوس نشان دهنده‌ی آمینو اسید ها و پاره خط ها نشان دهنده‌ی پیوند های شیمیایی بین آمینو اسید هاست. معمولا طول پیوند های شیمیایی در حد یک ضریب دو به هم نزدیک هستند. میتوان پروتئین را به شکل یه درخت (با جزئیات بیشتر) یا یک زنجیر(با جزئیات کمتر).
یکی از ویژگی های جالب پروتئین۲ها این است که سریعا به پیکربندی با انرژی کمینه تا می‌شوند.
مدل دقیق ریاضی از پروتئین ها با پیوند های معمولی انجام نمی‌شود و به جای آن از پیوند پیچیده[۱۸] استفاده می‌شود که در آن زاویه‌ی هر راس ثابت است. این محدودیت زاویه ای به طور کلی تعداد درجه های آزادی پیوند را نصف می‌کند. عمل اصلی به دوران دادن بخشی از پیوند حول یکی از میله های آن تبدیل می‌شود[ST۰۰،Sos۰۱]. نشان داده شده که مسئله‌ی تعیین اینکه یک زنجیر چندضلعی پیچیده مسطح می‌شود یا نه مسئله‌ای NP-Complete است[ST۰۰].

کاغذ

اریگامی‌کاغذ در حدود ۲۵ سال اخیر به مسائل ریاضیاتی و محاسباتی جالبی رسیده است. یک قطعه کاغذ ، یک چندضلعی ساده مانند مربع یا مستطیل است و آن را می‌توان با هر عملی که فاصله ها در کاغذ را حفظ کرده و کاغذ را نبرد تا کرد. به عبارت دیگر کاغذ را نباید پاره کرد، کشید یا چسباند. به طور رسمی‌یک عمل تا کردن دنباله ای از جاسازی[۱۹] های هم اندازه‌ی قطعه‌ی کاغذ در $\mathbb{R}^3$ است. البته استفاده از اصطلاح "جاسازی" ضعیف است زیرا دو بخش از کاغذ را می‌توان بر هم مماس کرد. همچنین یک تا کردن مسطح کاغذ را به شکل مسطح در می‌آورد. معمولا به حرکت پیوسته‌ی تا کردن توجهی نمی‌کنیم و حالت نهایی تا کردن مورد توجه است.

طراحی اریگامی

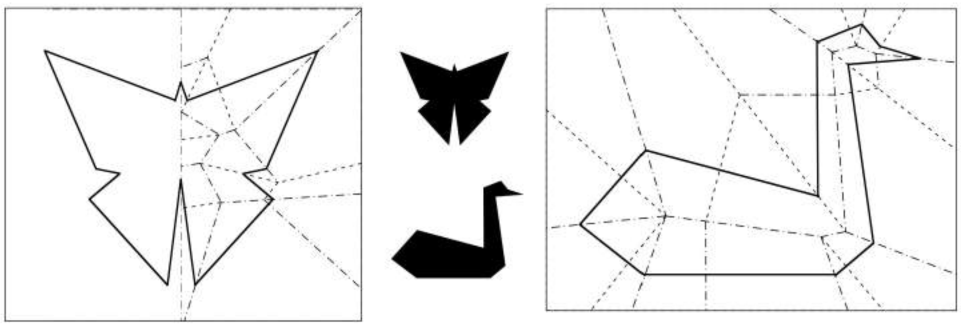
طراحی اریگامی‌به عمل تا کردن کاغذ به شیئی با ویژگی خاصی (مثلا یک شکل خاص)اطلاق می‌شود.
یکی از موضوعات طراحی اریگامی‌را در زیر بررسی می‌کنیم.

[۱۸] Revolute linkages
[۱۹] Embedding

یک برش مستقیم

یک قطعه کاغذ را تا کنید ، آن را مسطح کنید، روی یک خط مستقیم کاغذ را ببرید. و قطعه ها را جدا کنید. این مسئله‌ی تا کردن و برش ابتدا توسط مارتین گاردنر در ۱۹۶۰ مطرح شد. البته مسئله بسیار قدیمی‌تر است و به یک کتاب معمای ژاپنی بر می‌گردد.

به عبارت دیگر ، فرض کنید یک گراف مسطح رسم شده روی کاغذ به شما داده شده است. آیا می‌توان کاغذ را طوری مسطح تا کرد که همه‌ی پاره خط های گراف روی یک خط قرار بگیرند؟ پاسخ این است که برای هر مجموعه ای از پاره خط ها در صفحه می‌توان این کار را انجام داد. دو روش کلی برای حل این مسئله وجود دارد. روش اول(حل جزئی)[DDL۹۸،DDL۹۹b] بر اساس ساختاری به نام اسکلت راست[۲۰] که دو مثال از آن در شکل پایین نشان داده شده است.



شکل ۲: اسکلت راست

روش دوم (حل کامل) [BDEH۰۱] بر اساس بسته بندی دیسک[۲۱] انجام می‌شود و کران های پایینی روی تعداد تا کردن های لازم می‌یابد.

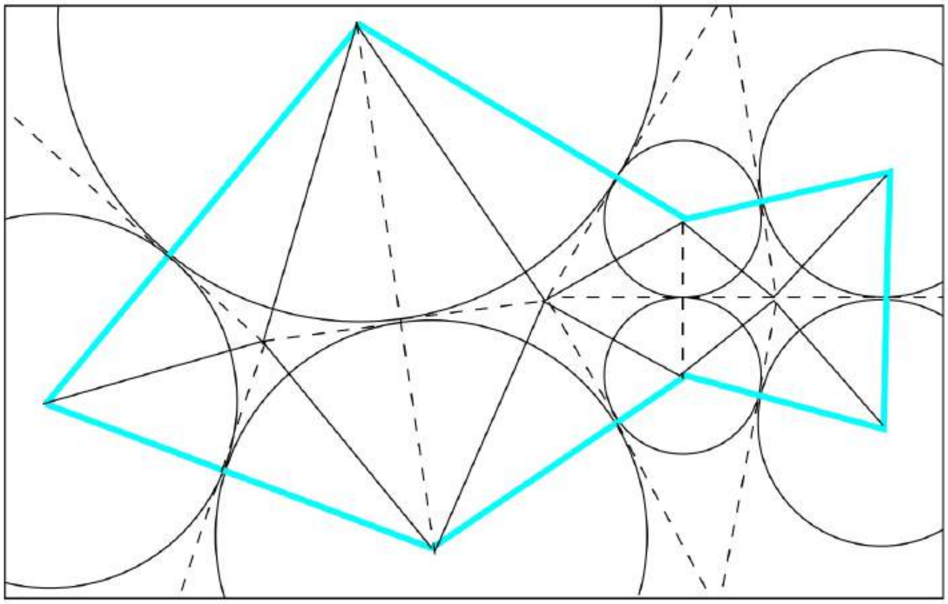
چندوجهی

یکی از روش های استاندارد برای ساخت چند وجهی این است که ابتدا یک شبکه مسطح (یا همان گسترده‌ی چندوجهی) می‌سازیم ، سپس آن را تا کرده و لبه ها را با چسب وصل می‌کنیم. برای یک چندوجهی داده شده یک سوال طبیعی پیدا کردن گسترده‌ی چندوجهی است. از طرف دیگر فرض کنید یک چند ضلعی داده شده است. این سوال ممکن است پیش بیاید که آیا می‌توانیم چند ضلعی را تا کرده و یک چند وجهی محدب از آن بسازیم؟ به سوال اول در بخش بعد پاسخ می‌دهیم.

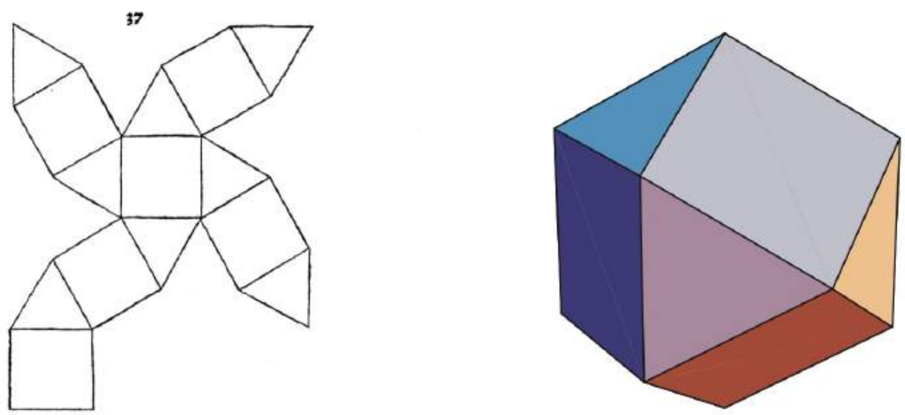
یکی از مسایل کلاسیک باز در این زمینه این است: آیا می‌توان یک چند وجهی محدب را از روی ضلع هایش طوری برید و سپس چند وجهی را باز کرد به طوری که گسترده‌ی آن مسطح بوده و همپوشانی نداشته باشد؟[She۷۵،O'R۹۸] این مسئله دارای کاربردهای مهمی‌در تاکردن صفحات فلزی دارد. حدس کلی در مورد این مسئله پاسخ مثبت است ولی همه‌ی تلاشها برای حل آن تا به حال به شکست منجر شده است. آزمایشهای شون[۲۲] نشان داده است که یک بازکردن تصادفی از چند وجهی تصادفی با احتمال ۱ دارای همپوشانی خواهد بود.

به جای پاسخ دادن به این مسئله‌ی سخت می‌توان تعمیم هایی از آن را بررسی کرد. یک چندوجهی را محدب توپولوژیکی[۲۳] می‌گوییم اگر گراف یک-اسکلت[۲۴] آن گراف یک-اسکلت یک چند وجهی محدب باشد. آیا هر چندوجهی محدب توپولیژیکی دارای یک گسترده‌ی ضلعی است؟ به طور خاص هر چندوجهی که از وجه های محدب ساخته شده باشد و با کره هم ریخت باشد، محدب توپولوژیکی است. آیا اینها دارای گستره‌ی ضلعی هستند؟ [Sch۸۷]

[۲۰] straight skeleton
[۲۱] Disk packing
[۲۲] Schevon
[۲۳] topologically convex
[۲۴] Edge unfolding



شکل ۳: بسته‌بندی دیسک



شکل ۴: آیا می‌توانیم چند ضلعی را تا کرده و یک چند وجهی محدب از آن بسازیم؟

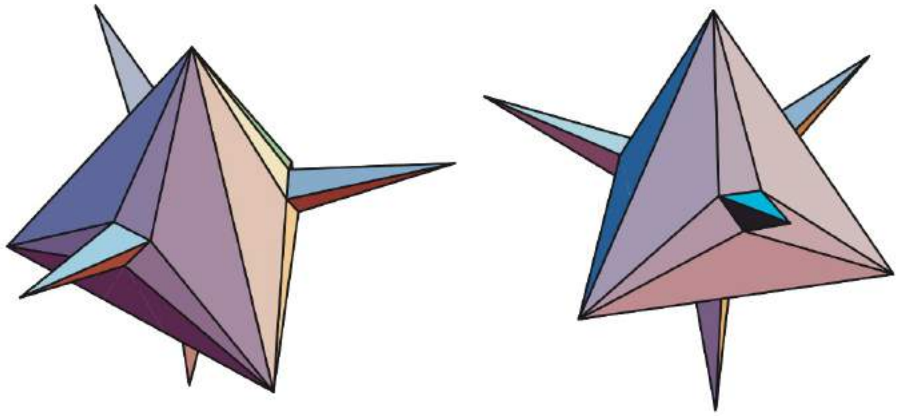
برن و بقیه نشان[BDE+۰۱] داده اند که پاسخ هر دوی این سوالات منفی است. چندوجهی شکل پایین را به عنوان مثال نقض در نظر بگیرید. که در گستره‌ی نشان داده شده برش ها از وجه ها هم عبور کرده اند.

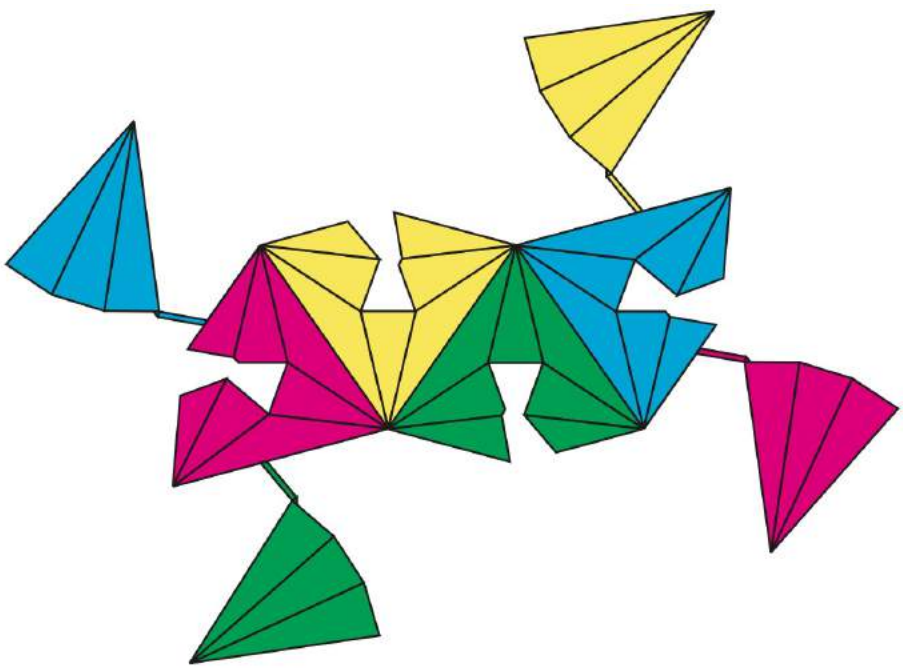
پیچیدگی تعیین اینکه آیا یک چندوجهی محدب توپولوژیکی داده شده دارای گستره‌ی ضلعی است هنوز مسئله ای باز است.

یکی از مسایل باز دیگر در این زمینه این است که آیا هر چندوجهی همریخت با کره دارای یک گستره‌ی همبند است یا نه؟(لزومی‌ندارد برش ها روی ضلعها باشد.) می‌دانیم که هر چندوجهی محدب این خاصیت را دارد. به طور خاص در تاکردن ستاره ای[25] [AAOS۹۷،AO۹۲] مجموعه ای از مسیر های برش داریم که همه در یک راس چندوجهی به هم می‌رسند. در این روش گستره‌ی حاصل همپوشانی نخواهد داشت.

[25] star unfolding

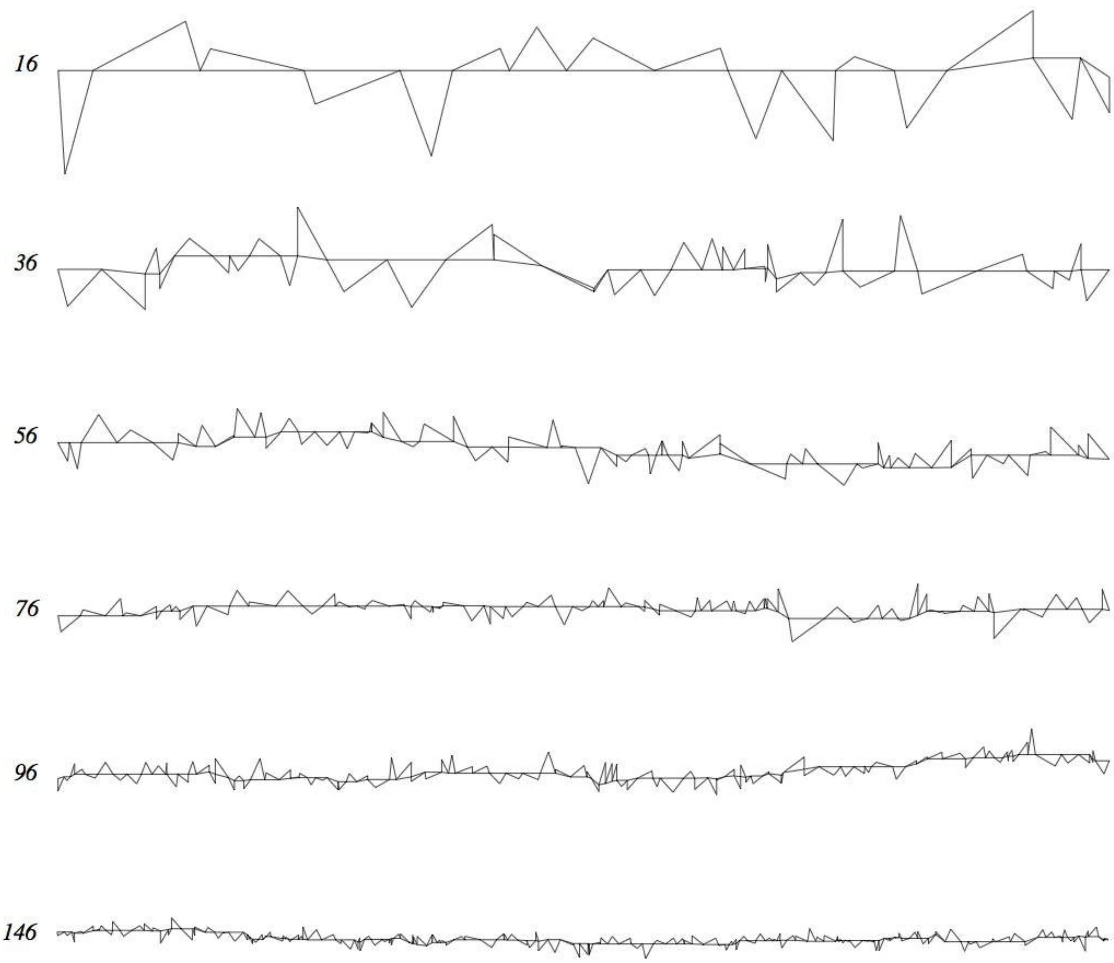
اما بسیاری از چندوجهی های غیر محدب هم دارای چنین گسترده هایی هستند. شکل پایین را ببینید. بیدل و بقیه [BDD+۹۸] روش هایی برای باز کردن بسیاری از چند وجهی های متعامد را ارایه کرده اند. گرچه مسئله‌ی تعیین این دسته از این چندوجهی ها نیز هنوز باز است.





یکی از روش های اخیر در مورد گسترده های ضلعی و گسترده های کلی از چندوجهی های غیرمحدب باز کردن[۲۶] راسی است [DEE+۰۱] (گستره‌ی حاصل را گستره‌ی راسی می‌نامیم). شکل پایین را ببینید که گستره‌ی راسی تعدادی از چند وجهی ها با تعداد مختلف وجه مثلثی را نشان می‌دهد. البته در باز کردن راسی میتوان فقط روی ضلعها برش داد ولی در این روش وجه هایی که تنها در یک راس اشتراک دارند در مولفه‌ی همبندی محسوب می‌شوند. بنابراین گستره‌ی حاصل همبند است ولی ممکن است درون آن ناهمبند باشد.

[۲۶] vertex-unfolding



تغییر پیکربندی چندضلعی های محدب

در اینجا نشان می‌دهیم هر (دور) چندضلعی محدب را به چندضلعی محدب دلخواه دیگر می‌توان تبدیل کرد به شرطی که دنباله‌ی پادساعتگرد ضلعهای چندضلعی ها یکسان باشد. تبدیل انجام شده هم طول ضلعها را حفظ کرده و چند ضلعی در طول تبدیل محدب باقی می‌ماند. این کار مربوط به دیمین و بقیه [ADE+۰۰] است.

راس های چندوجهی P را با دنباله‌ی $v_1, \dots, v_n$ نشان می‌دهیم که در آن رئوس به صورت پادساعت‌گرد مرتب شده‌اند. ضلع‌ها را به صورت $e_i = (v_i, v_{i+1})$ و طول ضلع‌ها را با $l_i = | e_i | = | v_i - v_{i+1} |$ نشان می‌دهیم که اندیس‌ها به هنگ n هستند. یک پیکربندی محدب از $l_1, \dots, l_n$ یک چندضلعی محدب است که طول اضلاع آن به ترتیب پادساعت‌گرد، $l_1, \dots, l_n$ باشد.

چندضلعی محدب می‌تواند رئوس با زاویه‌ی π داشته باشد و اضلاع می‌توانند همپوشانی داشته باشند.

لم ۱. ([LW۹۵]) *طول‌های $l_1, \dots, l_n$ طول اضلاع یک چند ضلعی محدب می‌توانند باشند اگر و تنها اگر*

$$l_i \leq \sum_{j \neq i} l_j$$

یک حرکت[۲۷] یا تغییر پیکربندی[۲۸] یک تابع پیوسته از بازه‌ی $[۰,۱]$ (به عنوان زمان) به یک پیکربندی است به طوری که هر پیکربندی یک چندضلعی با دنباله‌ی پادساعتگرد اضلاع یکسان است. یک حرکت زاویه-یکنوا حرکتی است که زاویه‌ی هر راس تابعی صعودی نسبت به زمان است.

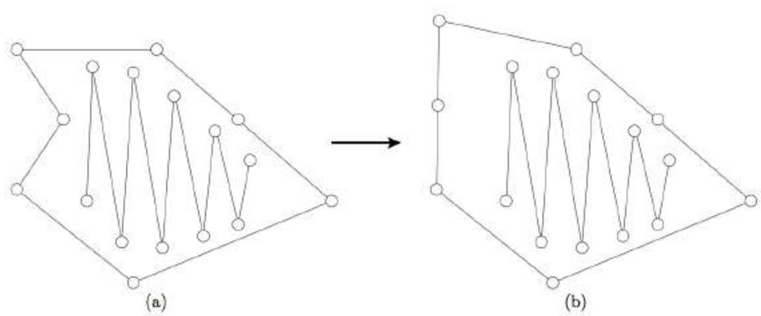
لم ۲. *یک چهارضلعی $v_۱, v_۲, v_۳, v_۴$ داده شده است. حرکتی وجود دارد که زاویه‌ی $v_۱$ و $v_۳$ را کاهش داده و زاویه‌ی $v_۲$ و $v_۴$ را افزایش می‌دهد. حرکت را می‌توان تا زمانی که یکی از زاویه‌ها ۰ یا π شود، ادامه داد.*

قضیه ۳. *دو پیکربندی C و C' با دنباله‌ی طول اضلاع یکسان $l_۱, \dots, l_n$ داده شده است. یک حرکت زاویه یکنوا از C به C' با $O(n)$ حرکت، که هر کدام زاویه‌ی چهار راس را تغییر می‌دهند وجود دارد.*

اثبات. مراجعه کنید به .[D۰۱] □

راست کردن مسیرهای چندضلعی و محدب سازی دورهای چندضلعی

یک پیوند مسطح را در نظر بگیرید که شامل تعدادی دور و مسیر چندضلعی مجزا است با این ویژگی که هیچ دوری ، مسیر یا دور دیگر را احاطه نمی‌کند. در این بخش نشان می‌دهیم همواره مسیرها را می‌توان راست و دور ها را محدب کرد به طوری که در طول عمل محدب سازی اضلاع همدیگر را قطع نکنند و دورها ،محدب باقی بمانند[CDR۰۰].
برای دور چند ضلعی در این روش از یک حرکت توسیع[۲۹] استفاده می‌کنیم که فاصله‌ی رئوس را افزایش می‌دهد.همچنین نشان می‌دهیم که مساحت چند ضلعی در طول حرکت افزایش می‌یابد. وضعیت کلی تری را در نظر می‌گیریم که به آن مجموعه‌ی مسیر-دور A می‌گوییم که شامل تعداد متناهی از دور و مسیر چند ضلعی است به طوری که هیچکدام همدیگر را قطع نمی‌کنند .
می‌گوییم A در یک پیکربندی محدب-بیرونی[۳۰] است اگر هر مولفه‌ی A که در هیچ دوری از A قرار ندارد یا محدب(اگر دور باشد) و یا راست(اگر مسیر باشد) باشد. بهترین انتظاری که می‌توان داشت این است که A را به وضعیت محدب-بیرونی در آورد زیرا بقیه‌ی مولفه ها که در دور قرار دارند را ممکن است نتوان راست یا محدب کرد. شکل زیر را ببینید.



یک حرکت را توسیعی[۳۱] می‌گوییم اگر در طول حرکت فاصله‌ی هیچ دو راسی از A کاهش نیابد. با این تعریف هر زمان که دو ضلع هم خطی می‌شوند در طول ادامه‌ی هر حرکت توسیعی دیگر نیز هم خطی باقی می‌مانند. به یک حرکت توسیعی اکید می‌گوییم اگر فاصله‌ی دو راس که بین آنها یک ضلع یا یک مسیر مستقیم از اضلاع وجود دارد ثابت باقی بماند . همچنین فاصله‌ی رئوس روی مرز یا داخل یک دور ثابت باقی بماند.
می‌گوییم مجموعه‌ی A جداشده[۳۲] است اگر خط L در صفحه وجود داشته باشد به طوری که L با A تقاطع نداشته و حداقل یک مولفه از A در طرف دیگر از L قرار دارد.
نتیجه‌ی اصلی قضیه‌ی زیر است:

---
[۲۷] motion
[۲۸] reconfiguration
[۲۹] Expansion motion
[۳۰] Outer-convex
[۳۱] expansive
[۳۲] seperated

قضیه ۴. *هر مجموعه‌ی دور- مسیر دارای یک حرکت معتبر قطعه قطعه پیوسته است که آن را به یک حالت محدب- بیرونی می‌برد. همچنین حرکت توسیعی اکید است تا زمانی که A جدا می‌شود.*

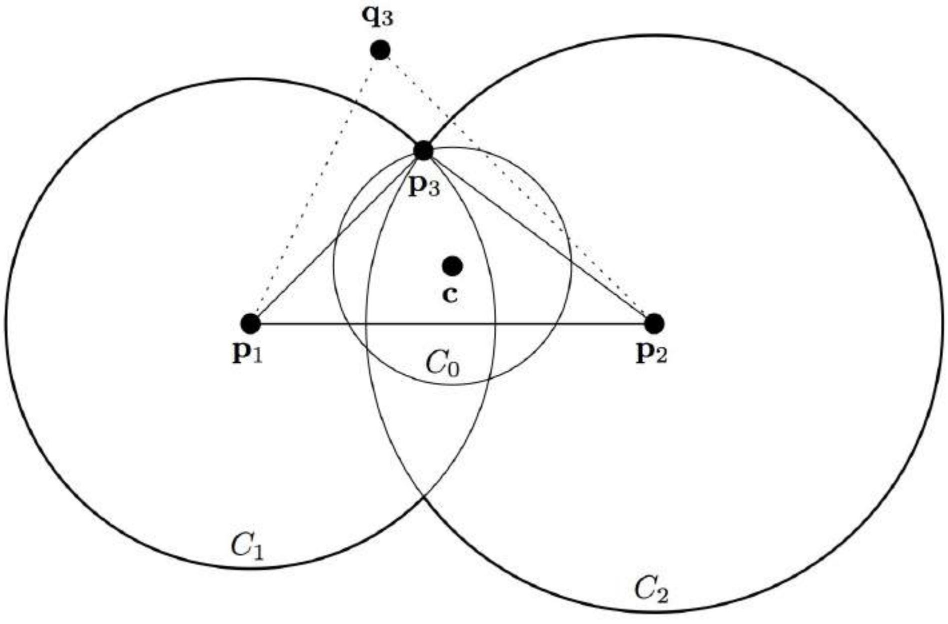
ابزار لازم برای اثبات قضیه از نظریه‌ی مکانیزم ها و چارچوب های صلب می‌آید.[۳۳] مسیر و دور را می‌توان به عنوان چارچوب در نظر گرفت.

یک روش حل مسئله این است که نشان دهیم برای هرپیکربندی یک حرکت جزئی وجود دارد که فاصله ها را افزایش می‌دهد.سپس می‌توان نشان داد این حرکت های موضعی را می‌توان به یک حرکت کامل تبدیل کرد.

یک پیوند[۳۴] یا چارچوب میله ای[۳۵] $G(p)$ یک گراف متناهی $G=(V,E)$ بدون ضلع چندگانه و طوقه به همراه پیکربندی مربوط به آن است. $p=(p_1,\dots,p_n)$ برای n نقطه که در صفحه که p_i متناظر با راس $i\in V$ است.(فرض می‌کنیم $V=\{1,\dots,n\}$) اعضای E متناظر با اضلاع چارچوب هستند. مجموعه های دور-مسیر یک نوع خاص از چارچوب ها هستند که گراف مربوط به آنها اجتماعی از مسیر ها و دور هاست. یک خم کردن[۳۶] یا حرکت[۳۷] از $G(p)$، مجموعه‌ای از توابع پیوسته‌ی $p(t)=(p_1(t),\dots,p_n(t))$ روی $0\le t\le 1$ است به طوری که $p(0)=p$ و $||p_i(t)-p_j(t)||$ برای هر $\{i,j\}\in E$ ثابت بماند. می‌خواهیم حرکتی روی مجموعه‌ی دور-مسیر بیابیم که توسیعی اکید باشد.

برخی از ویژگی های اولیه‌ی حرکت های توسیعی را نشان می‌دهیم.

لم ۵. *فرض کنید نقطه‌ی c داخل مثلث $p_1p_2p_3$ باشد و فرض کنید نقطه‌ی دیگر q_3 طوری انتخاب شده است که $||q_3-p_1||\ge||p_3-p_1||$ و $||q_3-p_2||\ge||p_3-p_2||$، در اینصورت داریم $||q_3-c||\ge||p_3-c||$ که تساوی دقیقا زمانی برقرار است که تساوی در هر دو طرف نامساوی های بالا برقرار باشد. شکل ۵ را ببینید.*



شکل ۵: لم ۵

[۳۳] theory of mechanisms and rigid frameworks
[۳۴] linkage
[۳۵] Bar framework
[۳۶] flex
[۳۷] motion

اثبات. مراجعه کنید به .[D۰۱] □

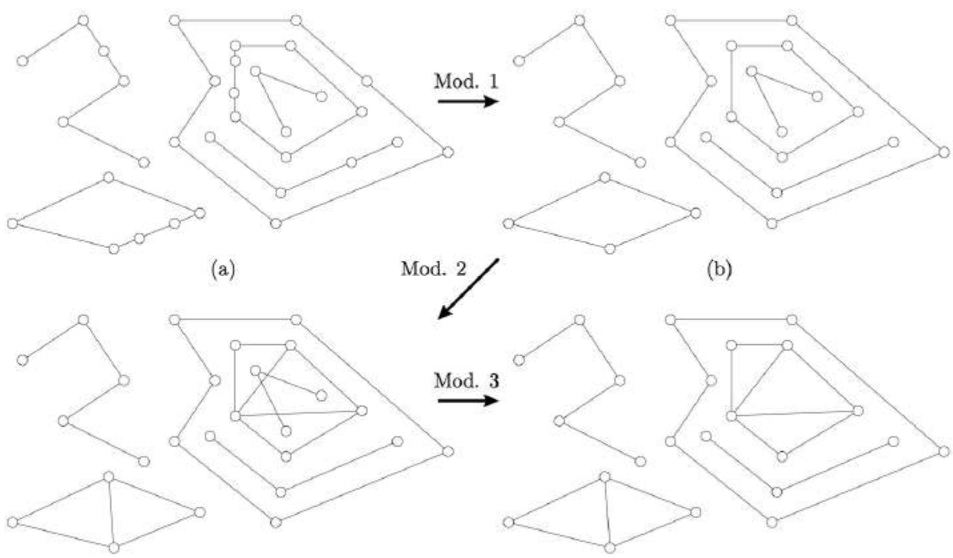
می‌خواهیم مجموعه‌ی دور-مسیر داده شده‌ی A را به پیکربندی محدب-بیرونی تبدیل کنیم. ابتدا A را کمی‌تغییر میدهیم .این کار در چهار مرحله صورت می‌گیرد.

مرحله‌ی ۱. **حذف رئوس راست.** نشان می‌دهیم می‌توان فرض کرد A هیچ راس راستی (با زاویه‌ی نیم صفحه) ندارد. به علاوه اگر در طول حرکت یک راس راست شود می‌توانیم با استقرا ادامه دهیم. اگر یک پاره خط در واقع از دو پاره خط تشکیل شده باشد می‌توانیم آنها را ادغام کنیم.

مرحله‌ی ۲. **صلب کردن[۳۸] چندضلعی های محدب.** از زمانی که یک چندضلعی محدب می‌شود دیگر نیازی به توسعه دادن آن نداریم ، در واقع این کار ممکن هم نیست. پس از این نظر آن را صلب می‌گیریم.و دیگر نمی‌توان زاویه های آن را تغیر داد.

مرحله‌ی ۳. **حذف مولفه های درون دورها.** زمانی که یک دور محدب می‌شود به علاوه می‌توانیم مولفه های درون آن را نیز صلب کنیم. در واقع این مولفه ها را می‌توان حذف کرد.

مرحله‌ی ۴. **اضافه کردن بست[۳۹].** برای مدل کردن بهتر از بست هم استفاده می‌کنیم که در طول حرکت طولش می‌تواند افزایش یابد یا ثابت بماند. در این مرحله بین هر دو راس از A که بین آنها ضلع وجود نداشته باشد یا روی یک دور چند ضلعی نباشند ، بست اضافه می‌کنیم.

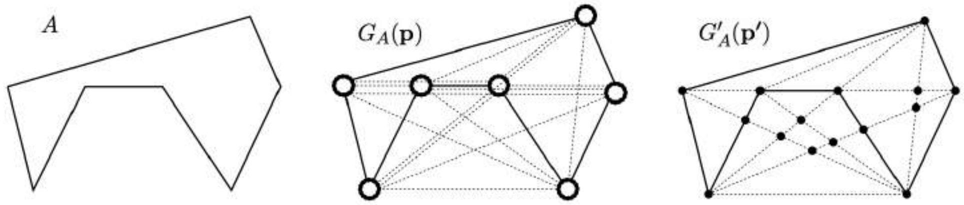


شکل ۶: تبدیل به پیکربندی محدب-بیرونی

شکل ۷ را ببینید. $G'_A(p')$ را بعدا تعریف می‌کنیم.
برای اثبات قضیه ۴، می‌خواهیم حرکتی پیدا کنیم که در آن طول همه‌ی اضلاع ثابت بماند و طول بست‌ها افزایش یابد. به عبارت دیگر حرکت $p(t)$ که $۰ \leq t \leq ۱$ را می‌خواهیم بیابیم که $p(۰) = p$ و

$$\frac{\mathrm{d}}{\mathrm{dt}}||p_j(t) - p_i(t)|| = ۰ \quad for\{i, j\} \in B$$

[۳۸] rigidify
[۳۹] struts



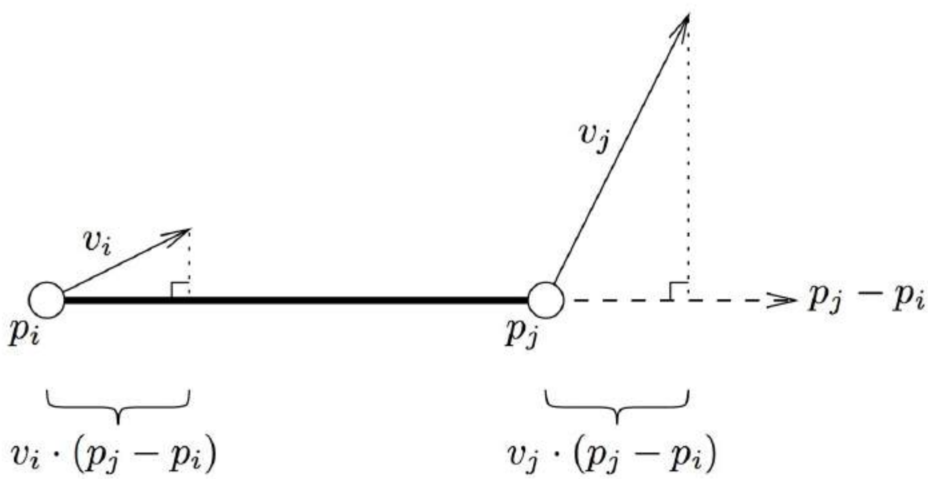
شکل ۷:

$$\frac{\mathrm{d}}{\mathrm{dt}}||p_j(t)-p_i(t)|| > 0 \quad for\{i,j\} \in S$$

$v_i(t) := \frac{\mathrm{d}}{\mathrm{dt}} p_i(t)$:

$$(v_j(t)-v_i(t)).(p_j(t)-p_i(t)) = 0 \quad for\{i,j\} \in B$$
$$(v_j(t)-v_i(t)).(p_j(t)-p_i(t)) > 0 \quad for\{i,j\} \in S$$

یک حرکت کوچک اکید $v = (v_1, \ldots, v_n)$ مشتق حرکت توسیعی اکید را در زمان ۰ تعیین می‌کند.(شکل ۸)



شکل ۸:

باید داشته باشیم:

$$(v_j - v_i).(p_j - p_i) = 0 \quad for\{i,j\} \in B \tag{1}$$
$$(v_j - v_i).(p_j - p_i) > 0 \quad for\{i,j\} \in S \tag{2}$$

که p_i مکان اولیه‌ی راس i است.

قضیه ۶. *برای هر مجموعه کاهش یافته ی A حرکت کوچک v برای $G_A(p)$ وجود دارد که معادلات ۱ و ۲ در آن برقرار است.*[D01]

$$\sum_{j:\{i,j\}\in B\cup S} \omega_{ij}(p_j - p_i) = 0 \tag{3}$$

دوگان ۳ را در نظر می‌گیریم و بر اساس تنش آن را بیان می‌کنیم. تنش[۴۰] در چارچوب $G(p)$ یک مقداردهی $\omega_{ij} = \omega_{ji}$ به همه‌ی زوج‌های $\{i, j\}$ است (ضلع‌ها وبست‌ها). برای مثال مقدار مثبت به این معنی است که یال به دو راس آن به اندازه‌ی یکسان نیروی بیرونی وارد می‌کند. تنش ω را یک تنش تعادلی می‌گوییم اگر هر راس i از G در تعادل باشد.(یال را بجای ضلع و بست به کار میبریم.)

تنش ω را معتبر می‌گوییم اگر برای همه‌ی بست های $\{i, j\}$، $\omega_{ij} \geq 0$.

تنش صفر[۴۱] را که یک تنش تعادلی است تنشی می‌گیریم که به هر ضلع و بست مقدار صفر نسبت داده شده است.

لم ۷. *اگر تنها تنش تعادلی معتبر یک چارچوب ضلع-بست ، تنش صفر باشد ، در این صورت چارچوب دارای حرکت کوچک است.*

$D01$. را ببینید. □

قضیه ۸. *چارچوب $G_A(p)$ مربوط به مجموعه‌ی کاهش یافته‌ی A تنها دارای تنش معتبر صفر است.*

$D01$. را ببینید. □

برای اثبات قضیه ۸ از قضیه‌ی ماکسول-کرمونا[۴۲] استفاده می‌کنیم. برای استفاده از این قضیه ابتدا $G_A(p)$ را به یک چارچوب مسطح $G'_A(p')$ تبدیل می‌کنیم. برای همه‌ی نقاط تقاطع در $G_A(p)$ یک راس تعریف می‌کنیم و اضلاع و بست های متناظر را تقسیم می‌کنیم.

یک تنش را صفر-بیرونی می‌گوییم اگر اضلاعی که تنش نا صفر دارند اضلاع دور های چند ضلعی محدب یا اضلاع داخل آنها باشند. در غیر این صورت تنش را ناصفر-بیرونی می‌نامیم.

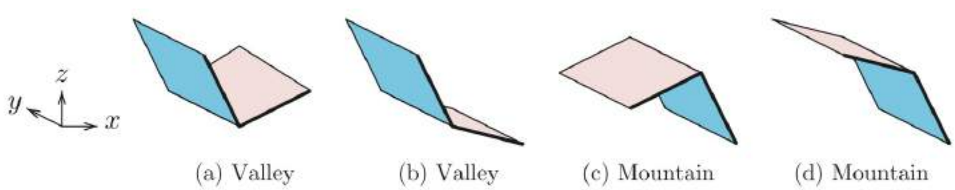
لم ۹. *اگر $G_A(p)$ دارای تنش معتبر نا صفر ω باشد $G'_A(p')$، دارای تنش ناصفر-بیرونی معتبر ω' است.*

اثبات. برای اثبات به [D01] مراجعه کنید. □

قضیه‌ی ماکسول-کرمونا

یک گراف چند وجهی Γ از اختصاص دادن یک مولفه‌ی سوم z به رئوس یک چارچوب مسطح به دست می‌آید به طوری که نقاط هر ناحیه از چندضلعی هم صفحه باقی بمانند. بدین ترتیب هر ناحیه از چندضلعی به یک چندضلعی در فضا تبدیل می‌شود.

یال $\{i, j\}$ ازیک چارچوب مسطح را در نظر بگیرید که دو وجه F و F' را از هم جدا می‌کند. بین حالاتی که که این یال در Γ به "دره"، "کوه" یا "سطح" تبدیل می‌شود تمایز قائل می‌شویم. شکل ۹ را ببینید.

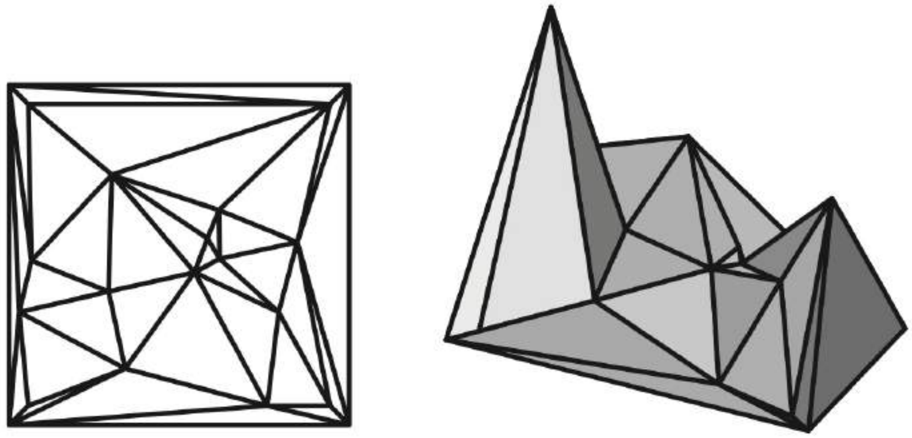


شکل ۹: دره، کوه، سطح

حال فرض کنید:

$$z(p) = a.p + b, z'(p) = a'.p + b'$$

[۴۰] stress
[۴۱] zero stress
[۴۲] Maxwell-Cremona theorem



دو تابع خطی باشند که Γ را به ترتیب روی F' و F تعیین می‌کنند. a و a' در $\mathbb{R}^۲$ و b و b' اعداد حقیقی هستند. باید داشته باشیم:

$$a' - a = \omega_{ij} e_{ij}^{\perp} \quad (۴)$$

که $e_{ij}^{\perp}$ بردار عمود بر $p_j - p_i$ و با طول برابر با طول $p_j - p_i$ و جهت آن از F به F' است. $\{i, j\}$ را دره می‌نامیم اگر $\omega_{ij} > ۰$، کوه اگر $\omega_{ij} < ۰$ و سطح اگر $\omega_{ij} = ۰$.

قضیه ۱۰. *(قضیه‌ی ماکسول- کرمونا)*

۱) *برای هر گراف چندوجهی Γ که به یک چارچوب مسطح $G(p)$ تصویر می‌شود تنش ω تعریف شده با ۴ یک تنش تعادلی روی $G(p)$ تعریف می‌شود.*

۲) *برای هر تنش تعادل معتبر ω روی $G(p)$، $G(p)$ را می‌توان به یک گراف چندوجهی Γ تبدیل کرد که ۴ برای همه‌ی یال‌ها برقرار باشد. به علاوه Γ در حد اضافه کردن یک تابع خطی-آفینی یکتاست.*

اثبات. مرجع [CW۹۴] را ببینید. □

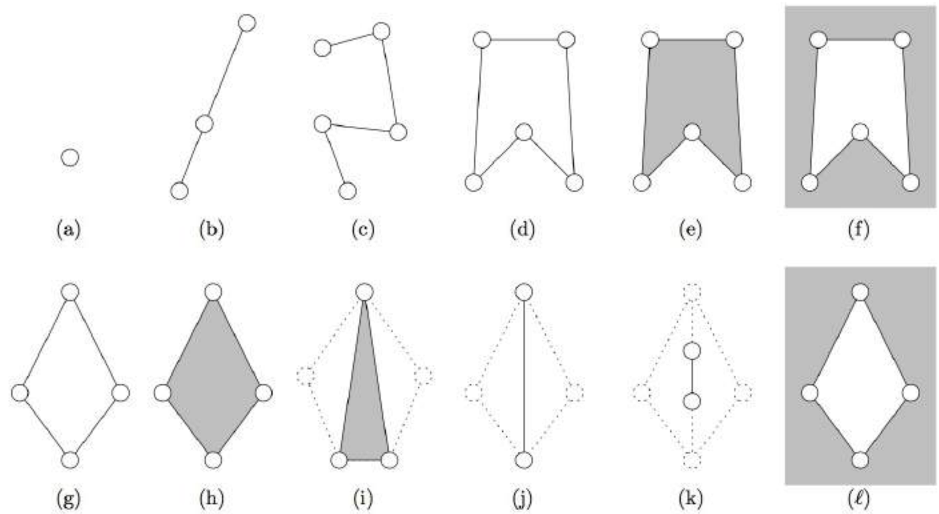
لم ۱۱ (HJW۸۴)**.** *هر کوه در گراف چندوجهی Γ در چارچوب مسطح $G'_A(p')$ به یک ضلع تصویر می‌شود.*

اثبات. بست تنها می‌توان تنش منفی داشته باشد . پس بنا بر قضیه‌ی ۱۰ بست تنها می‌توان به دره یا سطح تبدیل شود. □

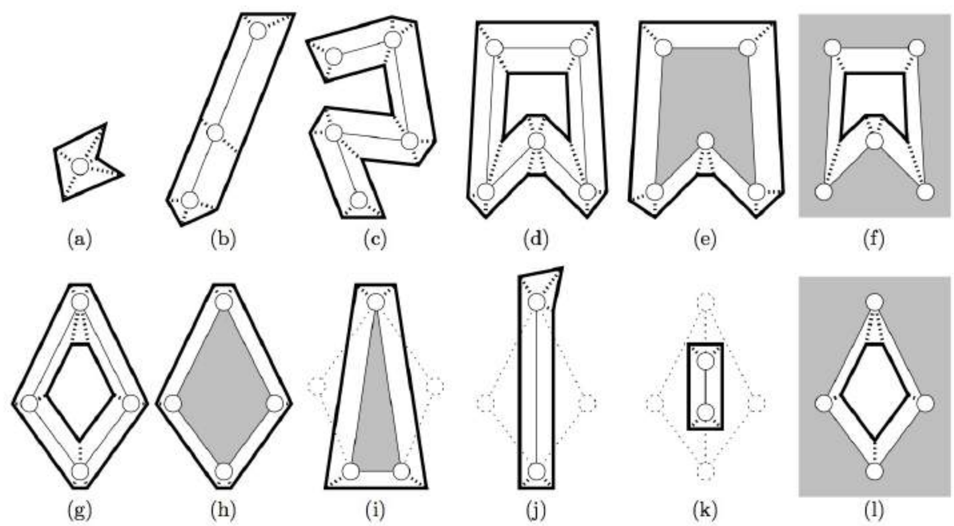
قضیه اصلی برای اثبات قضیه‌ی ۴ قضیه ی زیر است.

قضیه ۱۲. *فرض کنید M بخشی از صفحه‌ی xy باشد که مقدار z روی گراف چندوجهی Γ ماکسیمم است. در این صورت M شامل همه‌ی صفحاتی از $G'_A(p')$ است که بیرون از همه‌ی دورهای محدب قرار دارند.*

∂M را مرز M بگیرید. با توجه به اینکه نقاط M به ارتفاع بیشینه می‌رسند، نقاط ∂M باید به کوه تبدیل شوند. پس بنابر لم ۱۱ همه‌ی یال‌های ∂M باید اضلاع چارچوب باشند. شکل ۱۰ را ببینید.
در همه‌ی حالتهای بالا به جز l برش گراف چندوجهی است. صفحه‌ی Π موازی با xy و زیر بالاترین z را در نظر بگیرید که بالاتر از همه‌ی نقاط دیگر باشد. اشتراک Π با سطح Γ را بگیرید و اشتراک را روی xy تصویر کنید. تصویر حاصل X برای حالت‌های مختلف در شکل ۱۱ نشان داده شده است.
X بسیاری از ویژگی‌های گراف چندوجهی را دارد. با توجه به اینکه X مرز همسایگی کوچکی از M است اجتماعی مجزا از دور ها است. به علاوه چند وجهی است. هر یال X به یک ناحیه از Γ و هر راس از X به یک یال از Γ مربوط است.



شکل ۱۰:



شکل ۱۱: تصویر حاصل

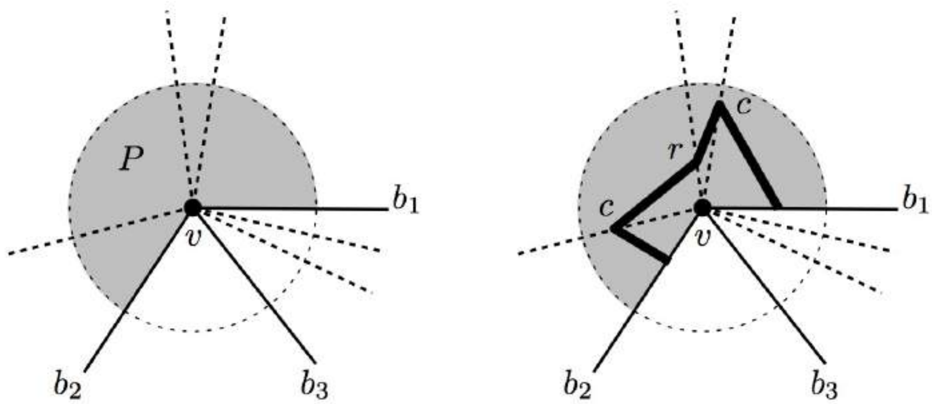
ایده‌ی اصلی این است نشان دهیم X دارای تعداد زیادی زاویه‌ی محدب است و سپس از لم ۱۱ استفاده کنیم برای اثبات اینکه چارچوب دارای ضلع های زیادی است. کلید اصلی در اثبات قضیه این است که مجموعه‌ی دور مسیر اولیه دارای درجه‌ی ضلعی حداکثر دو است. در $G'_A(p')$ تنها رئوس v از دورهای محدب می‌توانند درجه‌ی ضلعی بیش از دو داشته باشند.
در لم زیر نشان می‌دهیم حالت های a تا k نمی‌توانند وجود داشته باشند.

لم ۱۳. *فرض کنید v راسی روی مرز M باشد و $b_1, \ldots, b_k$ اضلاع متصل به v در جهت ساعتگرد باشند. یک گوی کوچک D حول v در نظر بگیرید.*

۱) *اگر بین دو ضلع متوالی از بین $b_1, \ldots, b_k$ مثل b_i و b_{i+1} زاویه حداقل π باشد، در این‌صورت بخش سایه‌دار در شکل ۱۲*

به M تعلق دارد.

۲) *اگر حداکثر یک ضلع مجاور v وجود داشته باشد، همه‌ی D در M است.*



شکل ۱۲: لم ۱۳

اثبات. ۱) با توجه به اینکه هیچ ضلعی در P وجود ندارد، P باید کاملا داخل M باشد یا از آن مجزا باشد. فرض کنید P با M مجزا باشد. در این صورت اشتراک X با P یک مسیر چندضلعی ستاره‌ای شکل حول v است که از b_i شروع شده و به b_{i+1} ختم می‌شود. نقاط محدب این مسیر مربوط به کوه هایی است که یک سر آنها v بوده است. باتوجه به اینکه زاویه‌ی P حداقل π است، مسیر باید حداقل شامل یک راس محدب در P باشد. بنابر لم ۱۱ یک ضلع باید در P باشد که تناقض است.

۲) اگر $k = 1$ که b_i و b_{i+1} یکی هستند و همان اثبات کار می‌کند. مسیر ستاره ای چندضلعی به دور ستاره ای چندضلعی تبدیل می‌شود که باید حداقل دو راس محدب غیر از $b_{i+1} - b_i$ داشته باشد. اگر $k = 0$، X یک دور چندضلعی حول v دارد که باید حداقل ۳ راس محدب داشته باشد ولی v هیچ ضلع مجاوری ندارد.

□

توجه کنید که این لم روی هر راس از $G'_A(p')$ کار می‌کند.
با استفاده از این لم به راحتی می‌توان نشان داد که حالت‌های $a - k$ با آن متناقض هستند.

اثبات قضیه‌ی ۱۲

ابتدا یک راس v درجه ۰ یا ۱ را در ∂M در نظر بگیرید. بنابر لم ۱۳ می‌دانیم ناحیه‌ای دو بعدی حول v به M تعلق دارد که با اینکه v در ∂M درجه‌ی ۰ یا ۱ دارد متناقض است.
بنابراین ∂M اجتماعی از دورهاست. یک مولفه از ∂M می‌تواند به دو صورت باشد:

۱. اگر از یک دور محدب و مثلث‌بندی آن به‌دست آمده باشد لم ۱۳ به هر راس آن اعمال می‌شود، نتیجه می‌گیریم M شامل ناحیه ای از چارچوب است که بیرون دور است.بدین ترتیب حالتهای $g - i$ حذف می‌شوند.

۲. اگر شامل یک دور غیر محدب است ، لم ۱۳ را می‌توانیم به یک راس محدب و به یک راس بازتاب[۴۳] اعمال کرده و نتیجه می‌گیریم M شامل دو ناحیه‌ی چارچوب مجاور داخل و خارج دور است .بدین ترتیب حالتهای $d - f$ حذف می‌شوند.

[۴۳] Reflex vertex

حرکت سرتاسری

در این بخش حرکت های کوچک را ترکیب کرده و به یک حرکت سرتاسری می‌رسیم که به اثبات قضیه‌ی ۴ منجر می‌شود. قضیه‌ی ۶ وجود یک جهت حرکت v را تضمین می‌کند. بردار یکتای $v-f(p)$ را برای هر پیکربندی p به عنوان جواب مسئله‌ی بهینه‌سازی محدب انتخاب می‌کنیم. سپس معادله دیفرانسیل زیر را در نظر بگیرید.

$$\frac{\mathrm{d}}{\mathrm{dt}}p(t) = f(p(t))$$

جواب این معادله دیفرانسیل پیکربندی فعلی را به حالتی می‌رساند که زاویه‌ی بین دو ضلع راست شود.در این حالت دو ضلع را ادغام کرده و کار را ادامه می‌دهیم ، بدین ترتیب هر بار یک راس کم می‌شود.

حال وارد جزئیات اثبات می‌شویم. از مسئله‌ی بهینه سازی غیرخطی زیر برای تعریف جهت یکتای v برای هر پیکر بندی p از یک مجموعه‌ی دور-مسیر کاهش یافته استفاده می‌کنیم.

$$\text{minimize} \quad \sum_{i\in V} ||v_i||^۲ + \sum_{\{i,j\}\in S} \frac{۱}{(v_i - v_j).(p_i - p_j) - ||p_j - p_i||} \tag{۵}$$

$$\text{to subject} \quad (v_j - v_i).(p_j - p_i) > ||p_j - p_i||, \quad for\{i,j\} \in S \tag{۶}$$

$$(v_j - v_i).(p_j - p_i) = ۰, \quad for\{i,j\} \in B \tag{۷}$$

$$v_۱ = v_۲ = ۰ \tag{۸}$$

محدودیت‌های ۶ یک محدودیت یکنواخت روی افزایش بست های S اعمال می‌کند. مشتق طول هر بست باید بیش از ۱ باشد.با توجه به اینکه دستگاه معادلات ۱ و ۲ همگن است، دستگاه ۶ و ۷ برای هر انتخاب طرف راست ۶، جواب دارد.

در تابع هدف نرم v به توان دو به اضافه‌ی یک عامل خطا که جواب را از مرز مجموعه جواب ۶ دور نگه می‌دارد. این خطا برای وابسته بودن هموار جواب نسبت به داده ضروری است. تابع هدف محدب اکید است زیرا مجموع تعدادی تابع محدب اکید است.همچنین با توجه به اینکه تابع هدف با نزدیک شدن v به مرز به بی نهایت نزدیک می‌شود، دقیقا یک جواب یکتا برای هر p وجود دارد که آن را با $f(p)$ نشان می‌دهیم.

تابع $f(p)$ روی یک زیرمجموعه‌ی باز $U\subset\mathbb{R}^{۲n}$ تعریف می‌شود که با شرایط قضیه‌ی ۶ تعریف می‌شود.

نشان می‌دهیم f روی U مشتق پذیر است. این از نظریه‌ی پایداری بهینه سازی محدب با محدودیت های به شکل تساوی ناشی می‌شود که روی مسئله‌ی بهینه سازی به شکل زیر اعمال می‌کنیم.

$$\min\{g(p,x) : x\in\Omega(p)\subset\mathbb{R}^n, A(p)x = b(p)\} \tag{۹}$$

که $A(p)$ یک ماتریس $m\times n$ و $b(p)$ یک بردار m-تایی است. تابع هدف g، دامنه‌ی $\Omega(p)$ و محدودیت‌های خطی (A,b) به پارامتر p بستگی دارند که روی ناحیه‌ی باز $U\subset\mathbb{R}^k$ تغییر می‌کند.

برای این مسئله‌ی بهینه سازی لم زیر وابستگی هموار بردار جواب بر حسب $A(p)$ و $b(p)$ را بیان می‌کند.

لم ۱۴. *فرض کنید شرایط زیر در مسئله‌ی بهینه سازی ۹ ارضا شده باشد:*

- الف) *تابع هدف $g(p,x)$ دوبار مشتق‌پذیر پیوسته و محدب اکید به عنوان تابعی از $x\in\Omega(p)$ باشد که ماتریس هسیان H_g برای هر $p\in U$ مثبت و معین است.*
- ب) *دامنه‌ی $\Omega(p)$ برای هر $p\in U$ مجموعه‌ای باز است.*
- ج) *راس‌های ماتریس $A(p)$ برای هر $p\in U$ مستقل خطی است.*
- د) *$b(p)$ و $A(p)$ و گرادیان ∇_g نسبت به x مشتق‌پذیر با مشتق پیوسته نسبت به p هستند، برای هر $p\in U$.*
- ه) *نقطه‌ی بهینه‌ی $x^*(p)$ از مسئله‌ی ۹ برای هر $x^*(p)$ موجود است.*

در این صورت $x^*(p)$ روی U مشتق‌پذیر با مشتق پیوسته است.

اثبات. اثبات بر اساس قضیه‌ی تابع ضمنی است .[BS۷۴]

x^* را می‌توان به عنوان جواب یکتای (x^*,λ) دستگاه معادلات $h(p,x,\lambda)$ در نظر گرفت که شرط‌های درجه اول ضروری بهینگی را ارضا می‌کند. به طور دقیق‌تر λ بردار k-تایی ضرایب لاگرانژ $h : U \times \mathbb{R}^{n+k} \to \mathbb{R}^{n+k}$ است که:

$$h = \begin{pmatrix} \nabla_g - \lambda^T A^T \\ Ax - b \end{pmatrix}$$

قضیه‌ی تابع ضمنی وجود جواب موضعی $x(p)$ را به عنوان جواب $h(p,x(p),\lambda(p)) = 0$ در یک همسایگی x تضمین می‌کند، اگر ماتریس ژاکوبیان $J = \partial h/\partial(x,\lambda)$ برای هر $p \in U$ معکوس‌پذیر باشد. همچنین $x(p)$ مشتق‌پذیر است اگر h مشتق‌پذیر با مشتق پیوسته باشد. ماتریس ژاکوبی به شکل زیر است:

$$J = \frac{\partial h(p,x,\lambda)}{\partial(x,\lambda)} = \begin{pmatrix} H_g & A^T \\ A & 0 \end{pmatrix}$$

مشتق‌پذیری h از فرض (د) حاصل می‌شود. باید معکوس‌پذیری J را چک کنیم. بنابر الف داریم:

$$\det J = \det H_g . \det(-A H_g^{-1} A^T)$$

بنابر ج AA^T مثبت معین است و با توجه به اینکه H_g مثبت معین است، پس برای $AH^{-1}A^T$ هم همین‌طور. پس $\det J \neq 0$. $\square$

لم ۱۵. *f روی U مشتق‌پذیر است.*

اثبات. اثبات را در [D۰۱] ببینید. $\square$

حل معادله‌ی دیفرانسیل و اثبات قضیه‌ی ۴

با توجه به لم ۱۵ درمی‌یابیم که معادله‌ی مقدار اولیه‌ی

$$\frac{\mathrm{d}}{\mathrm{dt}} p(t) = f(p(t)), \quad p(0) = p_0 \qquad (۱۰)$$

دارای جواب یکتای ماکسیمال $p(t)$، $0 \leq t < T$ است. یکی از حالت‌های زیر ممکن است رخ دهد:

الف) T برای هر t وجود دارد. ($T = \infty$)

ب) T متناهی است و $p(t)$ با $t \to T$ بی‌کران افزایش می‌یابد.

ج) T متناهی است و $p(t)$ با $t \to T$ به مرز U نزدیک می‌شود.

حالت الف و ب را می‌توان کنار گذاشت.[D۰۱]
می‌توان نشان داد $p(t)$ با $t \to T$ همگرا می‌شود.[D۰۱]
بنابراین قضیه‌ی ۴ ثابت می‌شود.

مراجع

[AAOS97] Pankaj K. Agarwal, Boris Aronov, Joseph O'Rourke, and Catherine A. Schevon. Star unfolding of a polytope with applications. SIAM Journal on Computing, 26(6):1689–1713, December 1997.

[AO92] Boris Aronov and Joseph O'Rourke. Nonoverlap of the star unfolding. Discrete & Computational Geometry, 8(3):219–250, 1992.

[BDD+01a] T. Biedl, E. Demaine, M. Demaine, S. Lazard, A. Lubiw, J. O'Rourke, M. Over- mars, S. Robbins, I. Streinu, G. Toussaint, and S. Whitesides. Locked and un- locked polygonal chains in three dimensions. Discrete & Computational Geom- etry, 26(3):283–287, October 2001. The full version is Technical Report 060, Smith College, 1999, and arXiv:cs.CG/9910009, http://www.arXiv.org/abs/cs. CG/9910009.

[BDD+01b] Therese Biedl, Erik Demaine, Martin Demaine, Sylvain Lazrd, Anna Lubiw, Joseph O'Rourke, Steve Robbins, Ileana Streinu, Godfried Toussaint, and Sue Whitesides. A note on reconfiguring tree linkages: Trees can lock. Discrete Applied Mathematics, 2001. To appear. The full version is Technical Report SOCS-00.7, School of Computer Science, McGill University, September 2000, and Computing Research Repository paper cs.CG/9910024. http://www.arXiv.org/abs/cs.CG/ 9910024.

[BDE+ 01] Marshall Bern, Erik D. Demaine, David Eppstein, Eric Kuo, Andrea Mantler, and Jack Snoeyink. Unufoldable polyhedra with convex faces. Computational Geometry: Theory and Applications, 2001. To appear.

[CDR00] Robert Connelly, Erik D. Demaine, and Gu ̈nter Rote. Straightening polygonal ar cs and convexifying polygonal cycles. In Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pages 432–442, Redondo Beach, California, November 2000.

[CJ98] Jason Cantarella and Heather Johnston. Nontrivial embeddings of polygonal in- tervals and unknots in 3-space. Journal of Knot Theory and Its Ramifications, 7(8):1027–1039, 1998.

[CO99] Roxana Cocan and Joseph O'Rourke. Polygonal chains cannot lock in 4D. In Pro- ceedings of the 11th Canadian Conference on Computational Geometry, Vancouver, Canada, August 1999. http://www.cs.ubc.ca/conferences/CCCG/elec_proc/c17.ps.gz.

[CO01] Roxana Cocan and Joseph O'Rourke. Polygonal chains cannot lock in 4D. Techni- cal Report 063, Smith College, February 2001. http://www.arXiv.org/abs/cs. CG/9908005.

[D01] Erik D. Demaine, Folding and Unfolding ,PhD Thesis, University of Waterloo, 2001 Main Reference .Some of Figures from here , with permission

[HJW84] John Hopcroft, Deborah Joseph, and Sue Whitesides. Movement problems for 2- dimensional linkages. SIAM Journal on Computing, 13(3):610–629, August 1984.

[JS99] D. Jordan and M. Steiner. Configuration spaces of mechanical linkages. Discrete & Computational Geometry, 22:297–315, 1999.

[Kem76] A. B. Kempe. On a general method of describing plane curves of the nth degree by linkwork. Proceedings of the London Mathematical Society, 7:213–216, 1876.

[LW95] W. J. Lenhart and S. H. Whitesides. Reconfiguring closed polygonal chains in Euclidean d-space. Discrete & Computational Geometry, 13:123–140, 1995.

[O'R98] Joseph O'Rourke. Folding and unfolding in computational geometry. In Revised Papers from the Japan Conference on Discrete and Computational Geometry, vol- ume 1763 of Lecture Notes in Computer Science, pages 258–266, Tokyo, Japan, December 1998.

[Sal73] G. T. Sallee. Stretching chords of space curves. Geometriae Dedicata, 2:311–315, 1973.

[ST00] Michael Soss and Godfried T. Toussaint. Geometric and computational aspects of polymer reconfiguration. Journal of Mathematical Chemistry, 27(4):303–318, 2000.

لگاریتم گسسته

احمدرضا عبدلی

در این مقاله ابتدا به معرفی مفاهیمی از جبر مجرد پرداخته که در معرفی مفهوم لگاریتم گسسته نیاز بوده سپس لگاریتم گسسته را تعریف میکنیم. در ادامه دو روش برای حل مساله لگاریتم گسسته بیان کرده و به توضیح آنها میپردازیم. نظر به اینکه لگاریتم گسسته نقش به سزایی در حل روش رمزنگاری RSA دارد جز مسایل داغ روز به حساب آمده و همواره اهمیت خاصی برای روش‌های هر چه بهتر برای حل آن مدنظر قرار گرفته است.

لگاریتم گسسته و مفاهیم جبری

در این بخش ابتدا به تعریف لگاریتم گسسته و روش هایی برای محاسبه‌ی آن می‌پردازیم.

تعریف ۱. *فرض کنید $(G, .)$ گروهی ضربی و متناهی باشد. گروه دوری تولید شده توسط عنصر a از گروه G را $< a >$ می‌نامیم و آنرا به شکل زیر تعریف می‌کنیم:*

$$< a >= \{a^i \mid a \in G, i \in \mathbb{N}\}$$

واضح است که متناهی بودن گروه G، متناهی بودن $< a >$ را نتیجه می‌دهد. حال اگر $|< a >| = n$، در این‌صورت:

$$< a >= \{e, a, a^۲, \dots, a^{n-۱}\}$$

زیرگروه بودن $< a >$ به سادگی از تعریف بدست می‌آید.

از تعریف نتیجه می‌شود اگر $g \in < a >$ در این‌صورت $j \in \{۰, \dots, n-۱\}$ وجود دارد به‌طوری که $g = a^j$.

تعریف ۲. *منظور از لگاریتم گسسته عنصر g، از گروه ضربی $(G, .)$، از مرتبه‌ی n در مبنای b عبارت است از عدد $۰ \leq i \leq n-۱$، به طوری که $b^i = g$، یا به صورت معادل $\log_b^g = i$ می‌باشد. مشخصه لگاریتم گسسته در آن است که محاسبه آن سخت ولی چک کردن جواب به غایت آسان است.*

الگوریتم‌های محاسبه لگاریتم گسسته

حال به بررسی الگوریتم‌هایی برای محاسبه‌ی لگاریتم گسسته خواهیم پرداخت. فرض کنید $(G, .)$ گروه ضربی و $< \alpha >$ زیرگروهی دوری از آن باشد به طوری‌که $\beta \in < \alpha >$ باشد. هدف بر آن است که i را طوری پیدا کنیم که $\beta = \alpha^i$ و i یکتا باشد.اولین الگوریتم و ساده‌ترین روش، چک کردن یک‌به‌یک عنصرها خواهد بود. زمان مورد نیاز برای هر ضرب در گروه G، از $O(۱)$ می‌باشد. اگر $|< \alpha >| = n$ آنگاه محاسبه‌ی لگاریتم گسسته از $O(n)$ خواهد بود.

به این صورت که با داشتن فضایی از $O(۱)$ هر دفعه که α^i محاسبه شد، آن را ذخیره کرده و با مقدار β چک می‌کنیم و در صورت یکی نبودن، مقدار α^i را در α ضرب کرده و دوباره مقایسه می‌کنیم.

چون حداکثر n بار ضرب نیاز است، زمان محاسبه از $O(n)$ خواهد بود و به $O(۱)$ فضا نیاز داریم. راه دیگر این است که تمام مقادیر را قبلاً محاسبه و به صورت جفت مرتب منظم کنیم و سپس با جستجویی مانند جستجوی دودویی به مقایسه کردن بپردازیم.

این راه $O(n)$ برای محاسبه زمان نیاز دارد و در صورت استفاده از روش منظم کردن بهینه مانند quick sort به $O(n\log n)$ زمان نیز برای مرتب کردن نیاز دارد. فضایی از $O(n)$ برای ذخیره‌ی مقادیر و زمانی از $O(n)$ برای جستجو در این مقادیر، و در پایان با فضایی از $O(n)$ و زمانی از $O(n\log n)$ امکان‌پذیر خواهد بود.

الگوریتم‌های دیگر برای اینکار الگوریتم شنک[۱] و الگوریتم پولارد رو[۲] هستند که به بررسی کوتاهی در باب آن می‌پردازیم.

الگوریتم شنک

فرض کنید β عنصری است که می‌خواهیم لگاریتم گسسته‌ی آن را در مبنای α حساب کنیم. برای jهای کوچکتر از $\sqrt{n}$ و بزرگتر یا مساوی صفر، α^{mj} را حساب کرده که در آن $m=[\sqrt{n}]+۱$ و سپس آن‌ها را در زوج مرتب‌های (j,α^{mj}) بر حسب مولفه‌ی دوم مرتب می‌کنیم ولیست $L_۱$ به وجود می‌آید. سپس $\beta\alpha^{-j}$ را نیز حساب کرده، به همان شکل مرتب می‌کنیم و در $L_۲$ می‌گذاریم و بین این دو لیست زوجی را پیدا می‌کنیم که مولفه‌ی دوم‌شان یکی باشد.

به این‌صورت که اگر $(i,y)\in L_۲$ و $(j,y)\in L_۱$ باشند آنگاه

$$\alpha^{mj}=\beta\alpha^{-i}\Rightarrow\alpha^{mj+i}=\beta$$

و اگر $\beta\in<\alpha>$ در نتیجه $۰\le\log_\alpha\beta\le n-۱$. حال $\log^{\beta}_{\frac{\alpha}{m}}$ را محاسبه می‌کنیم و $\log_\alpha\beta=mj+i$.

به وضوح جستجو در قسمت آخر تمام می‌شود چون اگر نشود $\beta\notin<\alpha>$.

SHANKS(G,n,α,β)
 $m\leftarrow\lceil\sqrt{n}\rceil$
 for $j\leftarrow 0$ to $m-1$
  do compute α^{mj}
 Sort the m ordered pairs (j,α^{mj}) with respect to their second coordinates, obtaining a list L_1
 for $i\leftarrow 0$ to $m-1$
  do compute $\beta\alpha^{-i}$
 Sort the m oredered pairs $(i,\beta\alpha^{-1})$ with respect to their second coordinates, obtaininig in a list L_2
 Find a pair $(j,y)\in L_1$ and a pair $(i,y)\in L_2$ (i.e., find two pairs having identical second coordinates)
 $\log_\alpha\beta\leftarrow(mj+i)\bmod n$

حال به آنالیز مقدار زمان و فضای مورد نیاز می‌پردازیم. ضرب کردن توان‌های α از ۱ تا $\sqrt{n}$ از $O(m)$ بوده و مانند الگوریتم ابتدایی $O(m)$ حافظه نیاز دارد. به وضوح در حساب کردن $L_۲$ نیز $O(m)$ فضا و زمان نیاز است، و منظم کردن از $O(m\log m)$ زمان نیاز دارد. همچنین مقایسه کردن لیست‌ها هم $O(m)$ زمان نیاز دارد. بنابراین الگوریتم شنک از لحاظ فضا و زمان، بسیار موثرتر از الگوریتم قبلی می‌باشد.

---
[۱] Shank
[۲] Pollord Rho

الگوریتم پولارد رو

این الگوریتم مشابه الگوریتم قبلی است با این تفاوت که در اینجا اعضای G، به سه قسمت با کاردینال‌های تقریبا مساوی افراز می‌شود.

$$G = S_1 \cup S_2 \cup S_3, \mid S_1 \mid \cong \mid S_2 \mid \cong \mid S_3 \mid$$

حال تابعی از ضرب دکارتی $\mathbb{Z}_n$ و $\mathbb{Z}_n$ و $<\alpha>$ به خودش تعریف کرده و سعی در ساختن دنباله‌ای می‌کنیم که پس از پیدا کردن عناصر تکراری $\log_\alpha \beta$ بدست خواهد آمد.

$$f :<\alpha> \times \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow <\alpha> \times \mathbb{Z}_n \times \mathbb{Z}_n$$

حال تابع زیر را در نظر بگیرید:

$$f(x,a,b) = \begin{cases} (\beta x, a, b+1) & x \in S_1 \\ (x^2, 2a, 2b) & x \in S_2 \\ (\alpha x, a+1, b) & x \in S_3 \end{cases}$$

شرط زیر را بر ورودی (x,a,b) در نظر بگیرید:

$$x = \alpha^a \beta^b \tag{1}$$

با مقدار اولیه‌ی $(1,0,0)$، اگر ورودی خاصیت (۱) را داشته باشد خروجی f هم این خاصیت را دارد. با شروع از مقدار اولیه‌ی $(1,0,0)$ به دنباله‌ای از عناصر $<\alpha> \times \mathbb{Z} \times \mathbb{Z}$ می‌رسیم که به روش بازگشتی با $(x_{i+1}, a_{i+1}, b_{i+1}) = f(x_i, a_i, b_i)$ تعریف می‌شوند.

عناصر (x_i, a_i, b_i) و (x_{2i}, a_{2i}, b_{2i}) بررسی می‌شوند تا زمانی که مولفه‌ی اول‌شان برابر شود.

اگر تساوی برقرار شود یعنی $\alpha^{a_i}\beta^{b_i} = x_i = x_{2i} = \alpha^{a_{2i}}\beta^{b_{2i}}$ با جای‌گذاری $\alpha^c = \beta$ $(c = \log_\alpha^\beta)$ به تساوی $\alpha^{a_i+cb_i} = \alpha^{a_{2i}+cb_{2i}}$ می‌رسیم و در نتیجه $a_i + cb_i \equiv a_{2i} + cb_{2i}$ به پیمانه n.

$$\Rightarrow (a_{2i} - a_i) \equiv -c(b_{2i} - b_i) \mod n$$

و اگر

$$(b_{2i} - b_i, n) = 1$$

آنگاه

$$c = (a_i - a_{2i})(b_{2i} - b_i)^{-1}$$

و در حالتی که $(b_{2i} - b_i, n) = d$ و $d > 1$ به d جواب برای معادله می‌رسیم که در صورت بزرگ بودن نمی‌توان همه ی اینها را محاسبه نمود و در غیر این‌صورت لگاریتم گسسته محاسبه می‌شود. مادامی که $\mid <\alpha> \mid = n$، با محاسبات می‌توان نشان داد که در شرایط ایده آل شامل رندوم بودن تابع f و ... می‌توان در $O(\sqrt{n})$ این الگوریتم را انجام داد.

POLLARD RHO DISCRETE LOG ALGORITHM (G, N, α, β)
procedure $f(x,a,b)$
if $x \in S_1$
then $f \leftarrow (\beta.x, a, (b+1) \bmod n)$
else if $x \in S_2$
then $f \leftarrow (x^2, 2a \bmod n, 2b \bmod n)$
else $f \leftarrow (\alpha.x, (a+1) \bmod n, b)$
return (f)

```
main
 define the partition G = S_1 ∪ S_2 ∪ S_3
  (x, a, b) ← f(1, 0, 0)
  (x', a', b') ← f(x, a, b)
 while x ≠ x' do
    (x, a, b) ← f(x, a, b)
    (x', a', b') ← f(x', a', b')
    (x', a', b') ← f(x', a', b')
  if gcd(b' − b, n) ≠ 1
   then return ("failure")
    else return ((a − a')(b − b')^{-1} mod n)
```

در پایان شایان ذکر است که مساله لگاریتم گسسته کاربرد گسترده‌ای در علم رمزنگاری داشته و همواره جستجو برای الگوریتم‌هایی با زمان بهتر در جریان بوده است.

P vs NP

دکتر رسول رمضانیان

در کاری که انجام شده است دو مفهوم اساسی وجود دارد که این دو مفهوم به نحوی در هم تنیده‌اند:

۱- از پیش تعیین شده نبودن معنای یک واژه (یک کد ماشین تورینگ)،

۲- تغییر پایای یک معنا.

اثبات چیست؟

ما می‌خواهیم مساله دشوار P vs NP را حل کنیم. یعنی یا اثباتی در رد آن یا اثباتی در موافقت آن ارائه دهیم. اما یک اثبات چیست؟ اثبات یک گزاره عبارت است از آغاز کردن از یک سری اصول بدیهی واضح (که بدون اثبات پذیرفته می‌شوند؛ چون اصل استقرا، اصل لانه کبوتری و ...) و استفاده از قواعد استنتاج منطقی و رسیدن به گزاره مورد نظر. از اصول بدیهی می‌توان به اصل لانه کبوتری و اصل استقرا اشاره کرد (که بدون اثبات پذیرفته می-شوند و دلیل این است که برای انسان کنونی این اصول واضح هستند، یعنی برای ما واضح است! که اگر سه کبوتر را بخواهیم در دو لانه بنشانیم حتما در یکی از دو لانه دو کبوتر باید بنشیند). انسان ۱۰ هزار سال پیش غار نشین را لحاظ کنید که هنوز توان تکلم نداشت. آیا برای او نیز اصل لانه کبوتری واضح بوده است؟ در واقع واضح و بدیهی شدن یک اصل در نتیجه تکامل انسان رخ می‌دهد!!! حال فرض کنید ما می‌خواهیم یک گزاره را ثابت یا رد کنیم. اما این گزاره از هیچیک از اصولی که برای ما واضح و بدیهی به نظر می‌رسند قابل استخراج نیست. بلکه لازم است که اصلی بدیهی پیدا شود تا از آن اصل بتوان مساله را ثابت یا رد کرد. نحوه اندیشیدن در این نوشتار در مورد مساله P vs NP به همین نحوه است.

فرض کنید که یک جعبه سیاه داریم که دارای دو نوار ورودی و خروجی است. روی نوار ورودی یک عدد طبیعی a می‌نویسم و جعبه سیاه روی نوار خروجی عدد طبیعی b را می نویسد.

گوییم جعبه سیاه خوش‌تعریف است هرگاه اگر در مرحله‌ای از زمان عدد طبیعی c را به جعبه وارد کردیم، و جعبه عدد d را در خروجی نوشت، آنگاه هرگاه در آینده دوباره همان عدد c را به جعبه وارد کنیم، جعبه دوباره همان عدد d را در خروجی چاپ کند.

گوییم جعبه سیاه ایستا است هرگاه خروجی‌ها به ترتیب ورودی‌ها وابسته نباشد.

پرسش: آیا اگر یک جعبه خوش‌تعریف عمل کند، آنگاه حتما ایستا است؟

پاسخ: خیر . کد زیر را در داخل جعبه سیاه قرار دهید.

1. Input x;
2. Check to see whether there exists a pair (x,y) in MEMORY, for some y, if there exists output y, goto line 1;
3. If [(x=5 or there exists a pair (5,2) in Memory) and there exists no pair (13,3) in MEMORY] output 2, save (x,2) in Memory, goto line 1;

4. If [(x=13 or there exists a pair (13,3) in Memory) and there exists no pair (5,2) in MEMORY] output 3, save (x,3) in Memory, goto line 1;

5. If (x≠5 and x≠13) output 1, save (x,1) in MEMORY, goto line 1;

جعبه خوش‌تعریف عمل می‌کند، اما وابسته به اینکه شما عدد ۱۳ را قبل از عدد ۵، یا عدد ۵ را قبل از عدد ۱۳ به جعبه وارد کنید، جعبه سیاه دارد توابع متفاوتی را محاسبه می‌کند. اگر تابع محاسبه شده توسط کد بالا را معنای[1] کد در نظر بگیریم، کد بالا یک معنای از پیش‌تعیین‌شده [2] ندارد، و معنای کد در اثر کنشگری با کاربر در طی گذر زمان شکل می‌گیرد!! معنای کد به اراده کاربر وابسته است (این همان نقطه کلیدی اثبات مساله اصلی است)

برای بهتر روشن شدن موضوع مثالی دیگر را در نظر بگیرید. فرض کنید E یک زبان برنامه نویسی است و من یک کامپایلر C برای زبان برنامه نویسی E طراحی کردم که این زبان را به زبان ماشین تبدیل می‌کند. به این ترتیب که، نحوه ترجمه آن بطور پایستاری (خوش‌تعریفی) تغییر می‌کند. یعنی اگر شما پیش‌تر دستوری در زبان E را توسط کامپایلر اجرا کرده باشید و از نتیجه آن آگاه شده باشید، هرگاه دوباره همان دستور را اجرا کنید، نتیجه همان چیزی خواهد بود که پیش‌تر از آن آگاه شده بودید. اما ترتیبی که شما دستورات را اجرا می‌کنید، سبب می‌شود که کامپایلر بطور پایایی تغییر کند. به این ترتیب، برنامه‌هایی که شما در زبان E می‌نویسید روی کامپایلر C معنایی از پیش‌تعیین شده ندارند! هر چند اگر شما به نحوه کارکرد کامپایلر توجه نکنید، هیچگاه از این موضوع آگاه نخواهید شد. (در مقاله [۱] ، نشان داده شده است که می‌توان یک زبان برنامه نویسی E و یک کامپایلر C برای آن معرفی کرد، بطوریکه بتوان در این محیط همه ماشین‌های تورینگ را پیاده‌سازی کرد، و به علاوه برنامه‌ای نوشت که زبان آن متعلق به NP هست ولی متعلق به P نیست)

اصل عدم تمییز: اگر معنای یک واژه (در یک زبان) برای انسان بطور پایستاری (با حفظ خوش-تعریفی) تغییر کند، انسان نمی‌تواند تفاوتی بین اینکه آیا معنا از پیش-تعیین‌شده است، یا معنا دینامیک است و در اثر کنشگری در طی زمان شکل می-یابد، قائل شود. (مقاله [۲] را ببینید)

در واقع این شبکه عصبی مغز ما است که به کدهای ماشین‌های تورینگ معنا می-بخشد. کدهای ماشین تورینگ همانند کدهای زبان برنامه‌نویسی E در مثال بالا هستند، اما برای آنکه مغز ما آنها را درک کند، باید به زبان شبکه عصبی (زبان ماشین مغز انسان) تبدیل شوند، حال چگونه می‌توان مطمئن بود که این فرآیند کامپایل کردن به طور پایستاری تغییر نمی‌کند؟ در واقع اگر شبکه عصبی مغز را نادید بگیریم، هیچ راهی برای تمییز قائل شدن بین ایستایی و تغییر پایا نخواهیم داشت، زیرا ما نمی‌توانیم به گذشته برگردیم و نمی-توانیم ترتیب‌های گوناگون را آزمون کنیم که ببینیم آیا یک ماشین تورینگ، معنایش وابسته به نحوه اجرا شبکه عصبی مغز ما است یا نه! در واقع ما با دو زبان روبرو هستیم، زبان برنامه نویسی، و زبان ماشین. یک کامپایلر زبان اول را به دومی ترجمه می‌کند. تز چرچ تورینگ می‌گوید، کدهای ماشین تورینگ زبان برنامه نویسی شبکه عصبی مغز ما هستند. زبان ماشین مغز ما برای ما ناشناخته است. هیچ دلیلی هم نداریم که فرض کنیم که کامپایلری که کدهای تورینگی را به زبان ماشین ترجمه می‌کند، بطور پایستاری تغییر نمی-کند.

بنابراین

۱. کدینگی که تورینگ ارائه می‌دهد، در واقع یک زبان برنامه‌نویسی است که CPU آن شبکه عصبی مغز انسان است. این زبان برنامه‌نویسی باید به زبان ماشین توسط یک کامپایلر ترجمه شود، حال ممکن است که کامپایلر مغز انسان، بطور پایستاری تغییر کند، زبان و تابعی که (معنایی که) یک ماشین تورینگ آن را توصیف و نمایندگی می‌کند، از پیش تعیین شده نیست!

۲. اگر زبان یک ماشین تورینگ از پیش تعیین شده نیست، اراده آزاد انسان در این که کدام برنامه را اجرا کند، سبب می‌شود که او بتواند معناهای ممکن بسیاری را (البته تنها یکی از آنها را، چون نمی تواند به گذشته برگردد) تحقق بخشد.

پس دو جهان ممکن پیش رو داریم

۱. معنای یک واژه (ماشین تورینگ) از پیش تعیین شده است

۲. معنای یک واژه (ماشین تورینگ) از پیش تعیین شده نیست.

[1] semantics
[2] Predetermined

در حالت دوم ثابت می‌شود که P مساوی NP نیست (مقاله [۱] را ببینید). بنابر اصل عدم تمییز ، چون نمی‌توان بین دو حالت ۱ و ۲ تمییز گذاشت، پس نمی‌توانیم هیچگاه ثابت کنیم P=NP.

مراجع

[1] R. Ramezanian, Computation Environment 1, An interactive Semantics for Turing Machines (which P is not equal to NP considering it), arXiv, 1205.5994v1. 2012.

[2] R. Ramezanian, Computation Environment 2, Persistently Evolutionary Semantics, arXiv, 1207.0051v1. 2012.

[3] R. Ramezanian, Computation Environment 3, P=NP Conflicts with the Free Will, http://sharif.edu/ ramezanian/cela.pdf

سوالات مسابقه دانشجویی ریاضی دانشگاه صنعتی شریف، اسفند ۱۳۹۰

روز اول

سوال ۱. ۲۰۱۲ نقطه در $\mathbb{R}^2$ داریم. ثابت کنید یک چندجمله‌ای غیرصفر با درجه حداکثر ۶۲ و ضرایب حقیقی مانند $P(x,y)$ وجود دارد که همه‌ی این نقاط روی منحنی $P(x,y)=0$ واقع باشند.

سوال ۲. فرض کنید A یک ماتریس $n\times n$ با درایه‌های در یک میدان دلخواه F باشد. ثابت کنید ماتریس قطری D با درایه‌های در F موجود است به طوری که $A+D$ وارون‌پذیر باشد.

سوال ۳. دنباله‌ی $\{a_n\}_{n=1}^{\infty}$ با جملات مثبت که $\lim_{n\to\infty} a_n = \infty$ داده شده است. نشان دهید دنباله‌ی نزولی $\{b_n\}_{n=1}^{\infty}$ با جملات مثبت وجود دارد به طوری که $\sum_{n=1}^{\infty} b_n < \infty$ و $\sum_{n=1}^{\infty} a_n b_n = \infty$.

سوال ۴. اعداد طبیعی n و m به طوری که $2m \leq n$ داده شده‌اند و f تابعی است که به هر زیرمجموعه m عضوی

$$N=\{1,\dots,n\}$$

یک عدد حقیقی منسوب می‌کند. اگر برای هر زیرمجموعه $m-1$ عضوی K از N داشته باشیم

$$\sum_{j\in N-K} f(K\cup\{j\}) = 0$$

نشان دهید برای هر زیرمجموعه m عضوی A از N داریم

$$\sum f(B) = (-1)^m f(A)$$

که این جمع روی تمام زیرمجموعه‌های m عضوی B از N که با A اشتراک ندارند، زده می‌شود.

سوال ۵. فرض کنید $\mathbb{D}=\{z\in\mathbb{C} : |z|<1\}$ و $\partial\mathbb{D}=\{z\in\mathbb{C} : |z|=1\}$. ثابت کنید هر تابع تحلیلی $f:\mathbb{D}\to\mathbb{D}$ که به طور پیوسته به $\partial\mathbb{D}$ گسترش می‌یابد و $f(\partial\mathbb{D})\subset\partial\mathbb{D}$ به صورت حاصلضرب توابع موبیوس است (تابع موبیوس تابعی به شکل $z\mapsto e^{i\theta}\frac{z-\alpha}{1-\bar{\alpha}z}$ است که $\theta\in\mathbb{R}$ و $\alpha\in\mathbb{D}$).

روز دوم

سوال ۶. اگر $f:[0,1]\to\mathbb{R}$ تابعی پیوسته باشد که برای هر $0\le x,y\le 1$،
$$xf(y)+yf(x)\le 1$$
ثابت کنید $\int_0^1 f(x)\mathrm{d}x\le\frac{\pi}{4}$ و با ذکر مثال نشان دهید $\frac{\pi}{4}$ کرانی دقیق است.

سوال ۷. برای $n=1,2,\dots$ فرض کنید $C_n\subset\mathbb{R}^n$ یک زیرمجموعه‌ی فشرده و ناتهی باشد به طوری که $C_{n+1}\subset C_n\times\mathbb{R}$. ثابت کنید دنباله‌ی حقیقی $x_1,x_2,x_3,\dots$ وجود دارد به طوری که برای هر n، $(x_1,x_2,\dots,x_n)\in C_n$.

سوال ۸. فرض کنید برای گروه G نگاشت $x\to x^n$ یک ایزومورفیسم باشد. ثابت کنید برای هر $x,y\in G$ داریم
$$x^{n-1}y=yx^{n-1}$$
(n یک عدد طبیعی داده شده است.)

سوال ۹. اعداد صحیح a,b,c به‌طوری‌که c فرد و خالی از مربع است و $a^2+bc=-1$ داده شده است. نشان دهید اعداد صحیح A,B,C,D وجود دارد به طوری که $AD-BC=1$ و $AC+BD=a$ و $C^2+D^2=c$ به طور همزمان برقرار شوند.

سوال ۱۰. فرض کنید G یک زیرگروه از $GL_n(\mathbb{Z})$ (ماتریس‌های $n\times n$ با درایه‌های صحیح و $\det=\pm1$) است که برای هر $g\in G$ عدد $m\ge1$ وجود دارد به طوری که $g^m=1$. ثابت کنید:

الف) عدد طبیعی N وجود دارد به طوری که برای هر $g\in G$ داریم $g^N=1$

ب) G یک گروه متناهی است و یک کران برای مرتبه‌ی آن برحسب تابعی از n بیابید.

پاسخ سوالات مسابقه دانشجویی ریاضی دانشگاه صنعتی شریف، اسفند ۱۳۹۰

گردآوری: خشایار فیلُم

روز اول

سوال ۱. ۲۰۱۲ نقطه در $\mathbb{R}^2$ داریم. ثابت کنید یک چندجمله‌ای غیرصفر با درجه حداکثر ۶۲ و ضرایب حقیقی مانند $P(x,y)$ وجود دارد که همه‌ی این نقاط روی منحنی $P(x,y)=0$ واقع باشند. (طراح: عرفان صلواتی)

پاسخ سوال ۱. مجموعه‌ی همه‌ی چندجمله‌ای‌های دومتغیره با ضرایب حقیقی و درجه‌ی حداکثر ۶۲ را با Π نمایش می‌دهیم. نگاشت $T:\Pi\to\mathbb{R}^{2012}$ را نگاشتی می‌گیریم که به هر عضو Π مقادیر آن را در نقاط مذکور در مساله نسبت می‌دهد. به وضوح Π یک فضای برداری و T نگاشتی خطی است. از طرفی مجموعه‌ی زیر یک پایه برای Π تشکیل می‌دهد:

$$\{x^iy^j \mid i,j\geq 0, i+j\leq 62\}$$

که ۲۰۱۶ عضوی است(تعداد اعضای آن تعداد جواب‌های نامنفی نامعادله‌ی $i+j\leq 62$ است و لذا برابر $\binom{64}{2}$ است.) بنابراین $\dim(\Pi)=2016$. پس $\ker(T)$ عضوی ناصفر مانند $P(x,y)$ دارد که همان چندجمله‌ای مطلوب است.

سوال ۲. فرض کنید A یک ماتریس $n\times n$ با درایه‌های در یک میدان دلخواه F باشد. ثابت کنید ماتریس قطری D با درایه‌های در F موجود است به طوری که $A+D$ وارون‌پذیر باشد. (طراح: دکتر جعفری، روزبه فرهودی)

پاسخ سوال ۲. حکم را با استقرا بر $n\in\mathbb{N}$ ثابت می‌کنیم. در پایه‌ی استقرا، حالت $n=1$ بدیهی است؛ کافی است قرارداد:

$$D=\begin{cases}[1] & A=0\\ [0] & A\neq 0\end{cases}$$

فرض کنید حکم برای n درست باشد. درستی آن را برای $n+1$ ثابت می‌کنیم: یک ماتریس $(n+1)\times(n+1)$، $A=[a_{ij}]_{1\leq i,j\leq n+1}$ با درایه‌های در F در نظر بگیرید. بلوک $n\times n$ پایین و راست A را $A'\in M_n(F)$ می‌گیریم (شکل ۱).

بنابر فرض استقرا، به ازای یک ماتریس قطری $n\times n$، D' با درایه‌های در F؛ $\det(A'+D')\neq 0$.

ماتریس‌های قطری $(n+1)\times(n+1)$ای به صورت شکل ۲ تعریف می‌کنیم.

برای اثبات حکم استقرا کافی است نشان داد که حداقل یکی از $\det(A+D_1)$ و $\det(A+D_0)$ ناصفر است که این هم از آن‌جا نتیجه می‌شود که با بسط دترمینان نسبت به سطر اول:

$$\det(A+D_1)-\det(A+D_0)=\det(A'+D')\neq 0$$

سوال ۳. دنباله‌ی $\{a_n\}_{n=1}^{\infty}$ با جملات مثبت که $\lim_{n\to\infty}a_n=\infty$ داده شده است. نشان دهید دنباله‌ی نزولی $\{b_n\}_{n=1}^{\infty}$ با جملات مثبت وجود دارد به طوری که $\sum_{n=1}^{\infty} b_n<\infty$ و $\sum_{n=1}^{\infty} a_nb_n=\infty$. (طراح: علی خزلی)

$$A = \left(\begin{array}{c|ccc} a_{11} & a_{12} & \cdots & a_{1(n+1)} \\ \hline a_{21} & & & \\ \vdots & & A' & \\ a_{(n+1)1} & & & \end{array}\right)$$

شکل ۱: ماتریس A

$$D_1 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & D' \end{array}\right), D_0 = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & D' \end{array}\right)$$

شکل ۲: ماتریس‌های قطری تعریف شده

پاسخ سوال ۳. چون $\lim_{n\to\infty}$، از جایی به بعد a_nها از ۱ بیشتراند، مثلا با شروع از مکان k_1+1ام و به دلیل مثبت بودن جملات دنباله می‌توان نوشت: $a_n > 0$ برای $1 \leq n \leq k_1$. با استفاده‌ی مجدد از $\lim_{n\to\infty} a_n = \infty$، اگر از مکان k_1+1ام به اندازه‌ی کافی، مثلا k_2 واحد جلو برویم، a_n از ۲ بیشتر می‌شود. لذا برای $k_1+1 \leq n \leq k_1+k_2$ داریم $a_n > 1$ (به دلیل روش انتخاب k_1) در حالی که اگر $n \geq k_1+k_2+1$، a_n از ۲ بیشتر می‌شود. دوباره به دلیل $\lim_{n\to\infty} a_n = \infty$، اگر در میان nهایی که از k_1+k_2 بیشترند، n به اندازه‌ی کافی بزرگ شود، a_n از ۳ هم بیشتر خواهد بود. پس عدد طبیعی k_3ای موجود است که برای $n \geq k_1+k_2+k_3+1$ داریم $a_n > 3$ در حالی که اگر $k_1+k_2+1 \leq n \leq k_1+k_2+k_3$، $a_n > 2$.

با تکرار این روند، به دنباله‌ی $\{k_m\}_{m=1}^{\infty}$ از اعداد طبیعی می‌رسیم، با این ویژگی که برای $\sum_{j=1}^{m-1} k_j + 1 \leq n \leq \sum_{j=1}^{m} k_j$ داریم $a_n > (m-1)$. بنابراین در واقع دنباله حالتی به صورت زیر دارد:

$$\underbrace{a_1, \ldots, a_{k_1}}_{\text{جملات بزرگتر از ۰}}, \underbrace{a_{k_{1+2}}, \ldots, a_{k_1+k_2}}_{\text{جملات بزرگتر از ۱}}, \underbrace{a_{k_1+k_2+1}, \ldots, a_{k_1+k_2+k_3}}_{\text{جملات بزرگتر از ۲}}, \ldots$$

از این روند ساختن k_jها به طور استقرایی، واضح است که اگر $k_1, \ldots, k_m$ انتخاب شده باشند، چون از جایی به بعد a_nها از $m+1$ بیشترند، می‌توان k_{m+1} را (که تنها باید ویژگی $n > \sum_{j=1}^{m+1} k_j \Leftarrow a_n > m+1$ را برآورده کند) آنقدر بزرگ گرفت که

$$m^2 k_m < (m+1)^2 k_{m+1}$$

لذا دنباله‌ی $\{k_m\}_{m=1}^{\infty}$ از اعداد طبیعی را داریم، به قسمی که $\{m^2 k_m\}_{m=1}^{\infty}$ صعودی است و برای $n > \sum_{j=1}^{m} k_j$ خواهیم داشت $a_n > m$.

حال قرار می‌دهیم:

$$b_n := \frac{1}{m^2 k_m} \quad \sum_{j=1}^{m-1} k_j + 1 \leq n \leq \sum_{j=1}^{m} k_j \text{ برای}$$

در نتیجه $\{b_n\}_{n=1}^{\infty}$ دنباله‌ای نزولی و با جملات مثبت خواهد بود که:

$$\sum_{n=1}^{\infty} b_n = \sum_{m=1}^{\infty} k_m \left(\frac{1}{m^2 k_m}\right) = \sum_{m=1}^{\infty} \frac{1}{m^2} < \infty$$

تنها ویژگی باقی‌مانده بررسی واگرا بودن سری $\sum_{n=1}^{\infty} a_n b_n$ است. توجه کنید که برای هر $m \in \mathbb{N}$:

$$\sum_{\sum_{j=1}^{m-1} k_j + 1 \leq n \leq \sum_{j=1}^{m} k_j} a_n b_n = \frac{1}{m^2 k_m} \sum_{\sum_{j=1}^{m-1} k_j + 1 \leq n \leq \sum_{j=1}^{m} k_j} a_n > \frac{m-1}{m^2}$$

و نامساوی آخر به این دلیل است که در مجموع k_m تا جمله داریم که همگی از $m-1$ بیشترند. بنابراین

$$\sum_{m=1}^{\infty}\sum_{\sum_{j=1}^{m-1}k_j+1\le n\le\sum_{j=1}^{m}k_j}a_nb_n>\sum_{m=1}^{\infty}\frac{m-1}{m^2}=\infty$$

چون تمامی a_nb_nها مثبت‌اند، این واگرایی سری $\sum_{n=1}^{\infty}a_nb_n$ را به دست می‌دهد.

سوال ۴. اعداد طبیعی n و m به طوری که $2m\le n$ داده شده‌اند و f تابعی است که به هر زیرمجموعه m عضوی
$$N=\{1,\dots,n\}$$
یک عدد حقیقی منسوب می‌کند. اگر برای هر زیرمجموعه $m-1$ عضوی K از N داشته باشیم
$$\sum_{j\in N-K}f(K\cup\{j\})=0$$
نشان دهید برای هر زیرمجموعه m عضوی A از N داریم
$$\sum f(B)=(-1)^m f(A)$$
که این جمع روی تمام زیرمجموعه‌های m عضوی B از N که با A اشتراک ندارند، زده می‌شود. (طراح: خشایار فیلُم)

پاسخ سوال ۴. برای هر $0\le r\le m$ قرار می‌دهیم $S_r=\sum_{|B|=m,|B\cap A|=r}f(B)$ (توجه کنید که چون $2m\le n$، حتما چنین زیرمجموعه‌ی Bای از N موجود است). خواسته‌ی مساله اثبات $S_n=(-1)^m f(A)$ است، به علاوه اگر زیرمجموعه‌ی m عضوی B از $N=\{1,\dots,n\}$ چنان باشد که $|B\cap A|=m$، آن‌گاه $B=A$ و لذا $S_m=f(A)$. پس به منظور حل مساله، نسبت S_{r+1}/S_r را می‌یابیم. بدین منظور $0\le r<m$ را تثبیت کنید. کمیت زیر را به دو روش می‌شماریم:
$$(*)T=\sum_{|B|=m,|B\cap A|=r}\ \sum_{x\in N-B,y\in B-A}f(B\cup\{x\}-\{y\})$$

روش اول محاسبه‌ی مجموع T در (*): روی $x\in N-B$ دو حالت داریم. حالت اول آن‌که x در $A-B$ باشد و حالت دوم آن‌که در $N-A\cup B$ باشد. در حالت اول که $x\in A-B$ و $y\in B-A$، اشتراک زیرمجموعه‌ی m عضوی $B\cup\{x\}-\{y\}$ از N با A برابر $r+1=|A\cap B|+1$ است و در حالت دوم که $x\in N-A\cup B$ و $y\in B-A$، اشتراک زیرمجموعه‌ی m عضوی $B\cup\{x\}-\{y\}$ از N با A برابر $r=|A\cap B|$ است. حال تعیین می‌کنیم که زیرمجموعه‌ی m عضوی‌ای همچون C از $N=\{1,\dots,n\}$ که اشتراک‌اش با A، r یا $r+1$ عضوی باشد، چندبار در مجموع (*) به صورت $B\cup\{x\}-\{y\}$ ظاهر می‌گردد. پس فرض کنید که به ازای زیرمجموعه‌ی m عضوی B از N با $|A\cap B|=r$ و عناصر $x\in N-B$ و $y\in B-A$ داشته باشیم $C=B\cup\{x\}-\{y\}$. حالت اول آن است که $x\in A-B$. پس اشتراک $C=B\cup\{x\}-\{y\}$ با A برابر است با $(A\cap B)\cup\{x\}$ و لذا $r+1$ عضوی است. چون با تعیین x و y، B معین می‌گردد، تنها تعداد حالاتی که (با تثبیت C) برای چنین x و yای رخ می‌دهد را می‌شماریم. همان‌گونه که گفتیم، x به مجموعه‌ی $r+1$ عضوی $A\cap C$ تعلق دارد و لذا برای آن $r+1$ حالت داریم. چون $y\in B-A$ و $y\notin C$، برای y به تعداد
$$|N-(A\cup C)|=|N|-|A|-|C|+|A\cap C|=n-2m+r+1$$
حالت داریم. لذا در مجموع (*)، هر C با $|C|=m$ و $|A\cap C|=r+1$، $(r+1)(n-2m+r+1)$ بار ظاهر می‌گردد. حالت دیگر آن است که در $C=B\cup\{x\}-\{y\}$ داشته باشیم $x\in N-(A\cup B)$ و $y\in B-A$. دوباره چون با تعیین چنین x و yای زیرمجموعه‌ی m عضوی B به طور یکتا تعیین می‌گردد، تعداد حالت‌های x و y را می‌شماریم. اینجا $A\cap C=A\cap B$ و لذا r عضوی است. باید $x\in C-A$ ولذا برای x
$$|A-C|=|A|-|A\cap C|=m-r$$
حالت داریم. در مورد y هم توجه کنید که مشابه بالا $y\in N-(A\cup C)$ که اینجا به دلیل $|A\cap C|=r$، به تعداد
$$|N-(A\cup C)|=|N|-|A|-|C|+|A\cap C|=n-2m+r$$

حالت دارد. در نتیجه در مجموع (*)، هر C با $|C|=m$ و $|A\cap C|=r$، $(m-r)(n-2m+r)$ ظاهر می‌گردد. از این موارد:

$$T=(r+1)(n-2m+r+1)S_{r+1}+(m-r)(n-2m+r)$$

روش دوم محاسبه‌ی مجموع T در (*):

$$T=\sum_{|B|=m,|B\cap A|=r}\ \sum_{y\in B-A}\ \sum_{x\in N-B} f((B-\{y\})\cup\{x\})$$

با اعمال فرض مساله به زیرمجموعه‌ی $n-1$ عضوی $B-\{y\}$ از $N=\{1,\dots,n\}$ داریم:

$$0=\sum_{x\in N-(B-\{y\})} f((B-\{y\})\cup\{x\})=f(B)+\sum_{x\in N-B} f((B-\{y\})\cup\{x\})$$

حال با قرار دادن در بالا:

$$T=-\sum_{|B|=m,|B\cap A|=r}\ \sum_{y\in B-A} f(B)=-\sum_{|B|=m,|B\cap A|=r} |B-A|.f(B)=-(m-r)S_r$$

با مقایسه‌ی دو مقداری که برای T حاصل شد:

$$(r+1)(n-2m+r+1)S_{r+1}+(m-r)(n-2m+r)S_r=-(m-r)S_r$$

$$\Rightarrow (r+1)(n-2m+r+1)S_{r+1}=-(m-r)(n-2m+r+1)S_r$$

(چون $0\le r<m$، $n-2m+r+1$ ناصفر است.)

$$\Rightarrow (r+1)S_{r+1}=-(m-r)S_r$$

حال با ضرب تمامی تساوی‌های $(r+1)S_{r+1}=-(m-r)S_r$ برای $0\le r<m$ خواهیم داشت $S_m=(-1)^m S_0$ که همان حکم مطلوب است.

سوال ۵. فرض کنید $\mathbb{D}=\{z\in\mathbb{C}:|z|<1\}$ و $\partial\mathbb{D}=\{z\in\mathbb{C}:|z|=1\}$. ثابت کنید هر تابع تحلیلی $f:\mathbb{D}\to\mathbb{D}$ که به طور پیوسته به $\partial\mathbb{D}$ گسترش می‌یابد و $f(\partial\mathbb{D})\subset\partial\mathbb{D}$ به صورت حاصلضرب توابع موبیوس است (تابع موبیوس تابعی به شکل $z\mapsto e^{i\theta}\frac{z-\alpha}{1-\bar{\alpha}z}$ است که $\theta\in\mathbb{R}$ و $\alpha\in\mathbb{D}$). (طراح: دکتر خاندانی، عرفان صلواتی)

پاسخ سوال ۵. ابتدا توجه کنید که تعداد صفرهای f درون D متناهی است، چرا که اگر این‌گونه نباشد و f در یک دنباله‌ی نامتناهی $\{a_n\}_{n=1}^{\infty}$ از نقاط دو به دو متمایز D صفر شود، به دلیل فشردگی $\bar{D}=D\cup\partial D$، با جایگزین کردن $\{a_n\}_{n=1}^{\infty}$ با زیردنباله‌ای از آن در صورت لزوم، دنباله‌ی مذکور از ریشه‌های دو به دو متمایز f به یک $a\in\bar{D}=D\cup\partial D$ همگرا می‌شود که آن هم به دلیل پیوستگی نگاشت $\bar{D}\to\bar{D}$ حاصل از توسیع $f:D\to D$، باید ریشه‌ی f باشد. ولی به دلیل $f(\partial D)\subset\partial D$ که در مفروضات مساله آمده، f نمی‌تواند بر ∂D صفر شود. پس $\lim_{n\to\infty}a_n=a\in D$ و لذا صفرهای تابع هولومورف $f:D\to D$، در a نقطه‌ی انباشتگی دارند. از آن‌جا که a_nها ریشه‌های دو به دو متمایزی از f بودند، هر همسایگی محذوف به دلخواه کوچک حول a ریشه‌ای از f را دربردارد. پس بنابر اصل یگانگی $f:D\to D$ متحد با صفر می‌شود، ولی در این صورت گسترش یافته‌ی پیوسته‌ی $f:\bar{D}\to\bar{D}$ از آن هم باید متحد با صفر باشد که دوباره با $f(\partial D)\subset\partial D$ در تناقض است. بنابراین $f:D\to D$ حداکثر متناهی‌تا ریشه دارد که آن‌ها را $\alpha_1,\dots,\alpha_k$ می‌نامیم. تکرر هر α_i به عنوان ریشه‌ای از f متناهی و عددی همچون $m_i\ge 0$ است، چرا که دوباره اگر تمامی مشتقات f در ریشه‌ی α_i از آن صفر شوند، با در نظر گرفتن سری تیلور حول α_i، به $f\equiv 0$ می‌رسیم که دیدیم امکان‌پذیر نیست. از طرف دیگر می‌دانیم که برای هر $\alpha\in D$،

$$\begin{cases} D\to D\\ z\mapsto \frac{z-\alpha}{1-\bar{\alpha}z}\end{cases}$$

تابع موبیوس و نگاشت هولومورفی است که به صورت نگاشت پیوسته‌ی $\bar{D}\to\bar{D}$ای که ∂D را به درون ∂D تصویر می‌کند، گسترش می‌یابد. به علاوه تنها ریشه‌ی آن $\alpha\in D$ است. پس

$$g(z):=\frac{f(z)}{\prod_{i=1}^{k}(\frac{z-\alpha_i}{1-\bar{\alpha}_i z})^{m_i}}$$

یک نگاشت هولومورف $g: D \to D - \{0\}$ ارائه می‌دهد (چرا که تنها ریشه‌های f، $\alpha_1, \dots, \alpha_k \in D$ بودند و آن هم با تکرر $m_1, \dots, m_k \geq 0$.) که توسیع پیوسته‌ی $g: \bar{D} \to \mathbb{C}$ از آن با $g(\partial D) \subset \partial D$ موجود است. پس اگر نشان دهیم که چنین gای باید تابع ثابت با مقدار $e^{i\theta}$ $(\theta \in \mathbb{R})$ باشد، نتیجه می‌شود که:

$$\forall z \in D: f(z) = e^{i\theta} \prod_{i=1}^{k} (\frac{z - \alpha_i}{1 - \bar{\alpha}_i z})^{m_i}$$

و لذا f همان‌گونه که می‌خواستیم، ضرب توابع موبیوس می‌شود. از آن‌جا که به دلیل $g(\partial D) \subset \partial D$، g حداکثر یک مقدار ω با $|\omega| = 1$ را می‌پذیرد. تنها کافی است ثابت بودن g را نشان داد و بنابراین مساله به حکم زیر تقلیل می‌یابد:

(*) $g: D \to D - \{0\}$ را تابع هولومورفی بگیرید که می‌توان آن را به طور پیوسته بر نقاط ∂D هم تعریف کرد به قسمی که $g(\partial D) \subset \partial D$. چنین تابعی باید ثابت باشد.

می‌توان حداقل سه اثبات برای (*) ارائه کرد:

اثبات اول) از ایده‌ی استاندارد "اصل انعکاس شوارتز[1]" استفاده می‌کنیم. چون برای هر $z \in \partial D$ داریم $|g(z)| = 1$، اگر $|z| = 1$ آن‌گاه $g(z) = 1/\overline{g(\frac{1}{\bar{z}})}$. پس چون $g: D \to D - \{0\}$ تابعی هولومورف بود،

$$\begin{cases} h: \mathbb{C} \to \mathbb{C} - \{0\} \\ h(z) = \begin{cases} g(z) & |z| \leq 1 \\ 1/\overline{g(\frac{1}{\bar{z}})} & |z| \geq 1 \end{cases} \end{cases}$$

هم این‌گونه است. ولی توجه کنید که:

$$\lim_{|z| \to \infty} h(z) = \lim_{|z| \to \infty} 1/\overline{g(\frac{1}{\bar{z}})} = 1/\overline{g(0)} \in \mathbb{C}$$

پس تابع هولومورف $h: \mathbb{C} \to \mathbb{C} - \{0\}$ کراندار است و بنابراین، بنابر قضیه‌ی لیوویل باید ثابت باشد. از آن‌جا که $h|_D = g$، این ثابت بودن g را هم نتیجه می‌دهد.

اثبات دوم) فرض کنید تابع هولومورف $g: D \to D - \{0\}$ ثابت نباشد. پس بنابر قضیه‌ای یک نگاشت باز خواهد بود: $g(D)$ بازی از $D - \{0\}$ است. ولی توجه کنید که بستار $g(D)$ در $\mathbb{C}$، یعنی $\overline{g(D)}$، به جز $g(D)$ تنها نقاط

$$\partial D = \{z \in \mathbb{C} : |z| = 1\}$$

را می‌تواند دربر داشته باشد. چرا که اگر $\{g(b_n)\}_{n=1}^{\infty}$ دنباله‌ای از اعضای $g(D)$ باشد که در آن $\{b_n\}_{n=1}^{\infty}$ دنباله‌ای از اعضای D است و $\lim_{n\to\infty} g(b_n) = c$ آنگاه $c \in g(D) \cup \partial D$. چرا که به دلیل فشردگی $\bar{D} = \{z \in \mathbb{C} \mid |z| \leq 1\}$، دنباله‌ی مذکور از نقاط D، زیردنباله‌ای به شکل $\{b'_n\}_{n=1}^{\infty}$ دارد که به عضوی از $\bar{D}$ همچون b' همگراست: $\lim_{n\to\infty} b'_n = b' \in \bar{D}$. پس چون g به طور پیوسته به کل $\bar{D}$ گسترش می‌یابد $c = g(b')$ و حال اگر $b' \in D$ آن‌گاه $c \in D$ (چرا که $g: D \to D - \{0\}$ بود) و اگر $b' \in \partial D$، از فرض (*)، یعنی $g(\partial D) \subset \partial D$ نتیجه می‌شود $c \in \partial D$. لذا $g(D)$ بازی از $D - \{0\}$ است که بستار آن $\overline{g(D)}$، به جز $g(D)$ حداکثر می‌تواند اعضای ∂D را دربر داشته باشد. باید وجود چنین بازی را به تناقض کشاند: از آن‌جا که $\overline{g(D)}$ فشرده است، نقطه‌ای از آن مانند $x \in \overline{g(D)}$ موجود است که فاصله‌اش از $0 \in \mathbb{C}$ حداقل ممکن است. همان‌گونه که گفتیم $\overline{g(D)} \subset g(D) \cup \partial D$، $g(D)$ بازی از $D - \{0\}$ و لذا فاصله‌ی اعضایش از مبدا کمتر از یک است در حالی که $\partial D = \{z \in \mathbb{C} \mid |z| = \}$. پس $x \in g(D)$. با استفاده از باز بودن $g(D)$، اگر $\epsilon > 0$ به اندازه‌ی کافی کوچک باشد $(1 - \epsilon)x \in g(D)$. این در حالی است که

$$|(1 - \epsilon)x| = (1 - \epsilon).|x| < |x|$$

که با روش انتخاب x تناقض دارد.

اثبات سوم) (این اثبات ممکن است اندکی فراتر از سطح استاندارد دروس دوره‌ی کارشناسی باشد.) در نمودار زیر

[1] Schwarz reflection principal

$$\begin{tikzcd}
 & \mathbb{C} \arrow[d, "z\mapsto e^{2\pi i z}"] \\
\bar{D} \arrow[r, "g"] \arrow[ur, dotted, "\tilde{g}"] & \mathbb{C}-\{0\}
\end{tikzcd}$$

نگاشت عمودی

$$\begin{cases}\mathbb{C}\to\mathbb{C}-\{0\}\\ z\mapsto e^{2\pi i z}\end{cases}$$

یک نگاشت پوششی است و $g:\bar{D}\to\mathbb{C}-\{0\}$ همان نگاشت پیوسته‌ی حاصل از توسیع $g:D\to D-\{0\}$ در (*) است. لذا چون $\bar{D}$ همبند ساده (و در واقع انقباض‌پذیر) است، یک ترفیع پیوسته‌ی $\tilde{g}:\bar{D}\to\mathbb{C}$ که در نمودار با خط‌چین نمایش داده شده، موجود است: نگاشت پیوسته‌ی $\tilde{g}:\bar{D}\to\mathbb{C}$ که نمودار را جابه‌جایی می‌کند. تحدید $\tilde{g}$ به درون $\bar{D}$ یعنی دیسک واحد $D=\{z\in\mathbb{C}\mid |z|<1\}$ هولومورف است، چرا که

$$\begin{tikzcd}
 & \mathbb{C} \arrow[d, "z\mapsto e^{2\pi i z}"] \\
\bar{D} \arrow[r, "g|_D"] \arrow[ur, "\tilde{g}|_D"] & \mathbb{C}-\{0\}
\end{tikzcd}$$

جابه‌جایی، $g|_D$ هولومورف و نگاشت عمودی ظاهر شده در نمودار، موضعا همیومورفیسم است. تجزیه‌ی $\tilde{g}$ به جمع جزء حقیقی و موهومی‌اش را به صورت $\tilde{g}=u+iv$ بگیرید. با توجه به نمودار جابه‌جایی فوق، برای $z\in\partial D$:

$$|g(z)|=|e^{2\pi i\tilde{g}(z)}|=|e^{2\pi i(u(z)+iv(z))}|=|e^{-v(z)}|=1\Rightarrow v(z)=0$$

حال $v:\bar{D}\to\mathbb{R}$ تابعی پیوسته است که $v|_D$ هارمونیک است یعنی لاپلاسین آن صفر است (چرا که جزء موهومی تابع هولومورف $\tilde{g}:D\to\mathbb{C}$ است) و بر ∂D؛ $v=0$. در این صورت باید $v\equiv 0$ چرا که توابع هارمونیک در اصل ماکسیمم صدق می‌کنند. یک روش دیگر بیان آن این است که v جواب معادله‌ی لاپلاس بر D است که بر ∂D صفر است و در نتیجه $v\equiv 0$. پس جزء موهومی تابع هولومورف $\tilde{g}:D\to\mathbb{C}$ صفر است و بنابراین $\tilde{g}$ و لذا $g=e^{2\pi i\tilde{g}}$ ثابت هستند.

سوال ۱. اگر $f:[0,1]\to\mathbb{R}$ تابعی پیوسته باشد که برای هر $0\le x,y\le 1$،
$$xf(y)+yf(x)\le 1$$
ثابت کنید $\int_0^1 f(x)\mathrm{d}x \le \frac{\pi}{4}$ و با ذکر مثال نشان دهید $\frac{\pi}{4}$ کرانی دقیق است. (طراح: سوال مسابقه‌ی *IMC* در ۱۹۹۸)

پاسخ سوال ۱. انتگرال $\int_0^1 f(x)\mathrm{d}x$ را با تغییر متغیرهای $x=\cos\theta$ و $x=\sin\theta$ بازنویسی می‌کنیم و معادلات زیر بدست می‌آید:
$$\int_0^1 f(x)\mathrm{d}x=\int_0^{\frac{\pi}{2}} f(\sin\theta)\cos\theta\mathrm{d}\theta$$
$$\int_0^1 f(x)\mathrm{d}x=\int_{\frac{\pi}{2}}^0 f(\cos\theta)(-\sin\theta)\mathrm{d}\theta=\int_0^{\frac{\pi}{2}} f(\cos\theta)\sin\theta\mathrm{d}\theta$$
از جمع دو تساوی فوق داریم:
$$2\int_0^1 f(x)\mathrm{d}x=\int_0^{\frac{\pi}{2}}[f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta]\mathrm{d}\theta\le\frac{\pi}{2}\Rightarrow\int_0^1 f(x)\mathrm{d}x\le\frac{\pi}{4}$$
زیرا که با استفاده از نامساوی صورت مسئله داریم:
$$f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta\le 1$$
برای برقراری تساوی توجه کنید که با توجه به بالا کافی است
$$\forall\theta\in[0,\frac{\pi}{2}]: f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta=1$$
لذا با توجه به اتحاد $\cos^2\theta+\sin^2\theta=1$، یک ایده تعریف $f:[0,1]\to\mathbb{R}$ به قسمی که $f(\sin\theta)=\cos\theta$ و $f(\cos\theta)=\sin\theta$ برای هر $\theta\in[0,\frac{\pi}{2}]$. پس $f(x)=\sqrt{1-x^2}$ باید تساوی را برقرار کند. این را در ادامه تحقیق خواهیم کرد:
$$\forall 0\le x,y\le 1: xf(y)+yf(x)=x\sqrt{1-y^2}+y\sqrt{1-x^2}$$
$$=\sin(\arcsin(x))\cos(\arcsin(y))+\sin(\arcsin(y))\cos(\arcsin(x))$$
$$=\sin(\arcsin(x)+\arcsin(y))\le 1$$
$$\int_0^1 f(x)\mathrm{d}x=\int_0^1\sqrt{1-x^2}\mathrm{d}x=\text{مساحت ربع دایره به شعاع ۱}=\frac{\pi}{4}$$

سوال ۲. برای $n=1,2,\ldots$ فرض کنید $C_n\subset\mathbb{R}^n$ یک زیرمجموعه‌ی فشرده و ناتهی باشد به طوری که $C_{n+1}\subset C_n\times\mathbb{R}$. ثابت کنید دنباله‌ی حقیقی $x_1,x_2,x_3,\ldots$ وجود دارد به طوری که برای هر n، $(x_1,x_2,\ldots,x_n)\in C_n$. (طراح: علی خزلی)

پاسخ سوال ۲. برای هر $i\le k$، $\pi_i:\mathbb{R}^k\to\mathbb{R}^i$ را نگاشت تصویر بر i مولفه‌ی اول می‌گیریم:
$$\pi_i(y,\ldots,y_k)=(y_1,\ldots,y_i)$$
دنباله‌ی مطلوب در صورت مساله را به طور استقرایی می‌سازیم. توجه کنید که برای هر $i\le k$، $\pi_i(C_k)$ زیرمجموعه‌ای فشرده از $\mathbb{R}^i$ است. برای هر $n\ge 1$، $C_{n+1}\subset C_n\times\mathbb{R}$ و در نتیجه با اعمال نگاشت پیوسته‌ی π_1؛ $\pi_1(C_{n+1})\subset\pi_1(C_n)$. پس دنباله‌ی تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}$ داریم:
$$\cdots\subset\pi_1(C_3)\subset\pi_1(C_2)\subset\pi_1(C_1)$$

و لذا $\cap_{j=1}^{\infty}\pi_1(C_j)$ ناتهی است؛ x_1 را عضوی از آن بگیرید. حال x_2 را چنان می‌گیریم که $(x_1, x_2) \in \cap_{j=2}^{\infty}\pi_2(C_j)$. برای هر $n \geq 2$، $C_{n+1} \subset C_n \times \mathbb{R}$ و در نتیجه با اعمال نگاشت پیوسته‌ی π_2؛ $\pi_2(C_{n+1}) \subset \pi_2(C_n)$ و بنابراین به دنباله‌ای تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}^2$ داریم:

$$\cdots \subset \pi_2(C_4) \subset \pi_2(C_3) \subset \pi_2(C_2)$$

اشتراک هر یک از این‌ها با زیرمجموعه‌ی بسته‌ی $\{x_1\} \times \mathbb{R}$ از $\mathbb{R}^2$ ناتهی است، چرا که از روش انتخاب x_1، برای هر $n \geq 1$، C_n عضوی با مولفه اول x_1 دارد. پس دنباله‌ی تودرتوی دیگری از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}^2$ داریم:

$$\cdots \subset \pi_2(C_4) \cap \{x_1\} \times \mathbb{R} \subset \pi_2(C_3) \cap \{x_1\} \times \mathbb{R} \subset \pi_2(C_2) \cap \{x_1\} \times \mathbb{R}$$

و لذا دوباره این اشتراک ناتهی است یا معادلا به ازای x_2ای؛ $(x_1, x_2) \in \cap_{j=2}^{\infty}\pi_2(C_j)$. ادامه‌ی فرآیند ساختن x_iها با همین روند استقرایی پیش می‌رود؛ فرض کنید $x_1, \ldots, x_i$ چنان ساخته شده باشند که:

$$\forall 1 \leq k \leq i : (x_1, \ldots, x_k) \in \cap_{j=k}^{\infty}\pi_k(C_j)$$

x_{i+1} را چنان می‌یابیم که این برای $k = i+1$ هم برقرار شود:

$$(x_1, \ldots, x_{i+1}) \in \cap_{j=i+1}^{\infty}\pi_{i+1}(C_j)$$

از همان ایده‌ی بالا استفاده می‌کنیم: دنباله‌ی زیر از زیرمجموعه‌های فشرده و تودرتو $\mathbb{R}^{i+1}$ را داریم(تودرتو بودن به دلیل $C_{n+1} \subset C_n \times \mathbb{R}$):

$$\cdots \subset \pi_{i+1}(C_{i+3}) \cap \{(x_1, \ldots, x_i)\} \times \mathbb{R} \subset \pi_{i+1}(C_{i+2}) \cap \{(x_1, \ldots, x_i)\} \times \mathbb{R} \subset \pi_{i+1}(C_{i+1}) \cap \{(x_1 \ldots, x_i)\} \times \mathbb{R}$$

که تمامی آن‌ها به دلیل آن‌که $(x_1, \ldots, x_i) \in \cap_{j=i}^{\infty}\pi_i(C_j)$ یا معادلا اینکه هر یک از C_nها که $n \geq i$، عضوی دارند که i مولفه‌ی اولش همان $(x_1, \ldots, x_i)$ است ناتهی هستند. پس اشتراک زیرمجموعه‌های فشرده‌ی فوق، ناتهی است و لذا به ازای x_{i+1} مناسبی:

$$(x_1, \ldots, x_i, x_{i+1}) \in \cap_{j=i+1}^{\infty}\pi_{i+1}(C_j)$$

پس دنباله‌ی $x_1, x_2, \ldots$ را ساختیم به قسمی که برای هر $i \geq 1$، $(x_1, \ldots, x_i) \in \cap_{j=i}^{\infty}\pi_i(C_j)$. علی‌الخصوص $(x_1, \ldots, x_i) \in \pi_i(C_i) = C_i$ (توجه کنید که $C_i \subset \mathbb{R}^i$ بود) برای هر $i \geq 1$ و بنابراین این همان دنباله‌ی مطلوب است که حل را تکمیل می‌کند.

تذکر ۱. ایده‌ی این سوال از "قضیه‌ی توسیع کولموگروف[۲]" در نظریه‌ی احتمال گرفته شده است.

تذکر ۲. اگر به جای فضای اقلیدسی $\mathbb{R}^n$، مکعب فشرده‌ی I^n در صورت مساله قرار گیرد، می‌توان حکم را به سادگی از قضیه‌ی تیخونوف[۳] نتیجه گرفت: فرض کنید برای هر عدد طبیعی n، $C_n \subset I^n$ فشرده باشد ($I = [0, 1]$ بازه‌ی واحد) و $C_{n+1} \subset C_n \times I$. هدف اثبات وجود دنباله‌ی $x_1, x_2, \ldots$ از عناصر I است، با این ویژگی که برای هر $n \in \mathbb{N}$؛ $(x_1, \ldots, x_n) \in C_n$. بنابر قضیه‌ی تیخونوف در توپولوژی عمومی، فضای

$$I^{\infty} = \{(y_j)_{j=1}^{\infty} \in I^{\infty} \mid \forall j \in \mathbb{N} : y_j \in I\}$$

در توپولوژی حاصلضربی فشرده است. حال کافی است زیر مجموعه‌ی بسته‌ی زیر از آن را در نظر گرفت:

$$\tilde{C}_n = \{(y_j)_{j=1}^{\infty} \in I^{\infty} \mid (y_1, \ldots, y_n) \in C_n\}$$

(مکمل $\tilde{C}_n$، $(I^n - C_n) \times I \times I \cdots$ و لذا در توپولوژی حاصلضربی بر I^{∞} باز است). این‌ها زیرمجموعه‌های بسته‌ی فضای توپولوژیک فشرده و هاسدورف I^{∞} هستند و لذا فشرده‌اند و به علاوه به دلیل شرط $C_{n+1} \subset C_n \times I$، تودرتو و به دلیل ناتهی بودن C_nها، ناتهی هم هستند. بنابراین

$$\cdots \subset \tilde{C}_3 \subset \tilde{C}_2 \subset \tilde{C}_1$$

دنباله‌ای تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی فضای فشرده‌ی I^{∞} می‌شود و بنابراین یک عنصر $(x_j)_{j=1}^{\infty}$ از I^{∞} در اشتراک $\cap_{n=1}^{\infty}\tilde{C}_n$ واقع است. این همان دنباله‌ی مطلوب است، چرا که از تعریف $\tilde{C}_n$ داریم:

$$(x_j)_{j=1}^{\infty} \in \tilde{C}_n \iff (x_1, \ldots, x_n) \in C_n$$

[۲] Kolmogorov extension theorem
[۳] Tychonoff's theorem

تذکر ۳. *با اندکی ویرایش راه‌حلی که در بالا برای حالت خاصی که در آن C_nها زیرمجموعه‌های فشرده‌ی I^n اند بیان شد، می‌توان برای مساله در همان صورت اولیه‌اش، حلی جدید مبتنی بر قضیه‌ی تیخونوف ارائه کرد: هر $C_n \subset \mathbb{R}^n$ فشرده است. پس می‌توان بازه‌ی بسته‌ی $[a_n, b_n]$ را یافت به قسمی که مولفه‌ی nام تمامی عناصر C_n در $[a_n, b_n]$ واقع باشد. $C_{n+1} \subset C_n \times \mathbb{R}$، $C_{n+2} \subset C_{n+1} \times \mathbb{R}$ و ... نشان می‌دهند که حکم مشابهی برای مولفه‌ی nام عناصر هر C_k با $k \geq n$ برقرار است. پس بازه‌های بسته‌ی $[a_1, b_1], [a_2, b_2], \ldots$ را خواهیم داشت به قسمی که:*

$$\forall n \in \mathbb{N} : C_n \subset [a_1, b_1] \times \cdots \times [a_n, b_n]$$

حال کافی است همان استدلال بیان شده در تذکر ۲ را، به فضای توپولوژیک $\prod_{n=1}^{\infty}[a_n, b_n]$ در توپولوژی حاصلضربی (که بنابر قضیه‌ی تیخونوف، فشرده است) اعمال کرد.

سوال ۳. *فرض کنید برای گروه G نگاشت $x \to x^n$ یک ایزومورفیسم باشد. ثابت کنید برای هر $x, y \in G$ داریم*

$$x^{n-1}y = yx^{n-1}$$

(n یک عدد طبیعی داده شده است.) (*طراح: سوال معروفی است!*)

پاسخ سوال ۳. *به دلیل همریختی بودن*

$$\begin{cases} G \to G \\ x \mapsto x^n \end{cases}$$

برای هر $b, c \in G$ داریم: $(bc)^n = b^n c^n$. با تثبیت یک عنصر دلخواه $x \in G$، این نتیجه می‌دهد که:

$$\forall a \in G : (xax^{-1})^n = x^n a^n (x^{-1})^n \Rightarrow xa^n x^{-1} = x^n a^n x^{-n} \Rightarrow a^n x^{n-1} = x^{n-1} a^n$$

پس x^{n-1} با هر عنصر G که به شکل a^n باشد، جابه‌جایی می‌شود. ولی به دلیل پوشایی همریختی مذکور، اگر $y \in G$ دلخواه باشد، به ازای $a \in G$ای $y = a^n$ و حال با قرار دادن در تساوی $a^n x^{n-1} = x^{n-1} a^n$ داریم:

$$x^{n-1}y = yx^{n-1}$$

سوال ۴. *اعداد صحیح a, b, c به‌طوری‌که c فرد و خالی از مربع است و $a^2 + bc = -1$ داده شده است. نشان دهید اعداد صحیح A, B, C, D وجود دارد به طوری که $AD - BC = 1$ و $AC + BD = a$ و $C^2 + D^2 = c$ به طور همزمان برقرار شوند.*
(*طراح: به توضیحات پس از راه‌حل مراجعه کنید!*)

پاسخ سوال ۴. *ایده‌ی حل استفاده از حلقه‌ی اعداد صحیح گاوسی یا $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ است. خواص مقدماتی این حلقه را یادآوری می‌کنیم:*

$\mathbb{Z}[i]$ یک .P.I.D است و برای هر $a + bi$ متعلق به آن می‌توان نرم را به صورت $N(a + bi) = a^2 + b^2$ تعریف کرد و اگر عددی اول باشد، $a + bi$ در $\mathbb{Z}[i]$ عنصری تحویل‌ناپذیر یا معادلا اول است. به علاوه اگر p یک عدد اول به فرم $p \overset{4}{\equiv} 1$ باشد، قضیه‌ای استاندارد حکم می‌کند که $x, y \in \mathbb{Z}$ موجودند به قسمی که $x^2 + y^2 = p$. پس در $\mathbb{Z}[i]$، $(x + iy)(x - iy) = p$. لذا $N(x + iy) = N(x - iy) = \sqrt{N(p)} = p$ و بنابراین $x \pm iy$ هر دو عناصری اول از $\mathbb{Z}[i]$اند. پس تجزیه‌ی عدد اول p با $p \overset{4}{\equiv} 1$ در $\mathbb{Z}[i]$ به صورت $p = \alpha\bar{\alpha}$ خواهد بود که α عنصری اول از $\mathbb{Z}[i]$ است.

حال مساله را حل می‌کنیم: $a^2 + bc = -1$ و لذا $b, c \mid a^2 + 1$. پس هیچ‌یک از b و c عامل اولی مانند q با $q \overset{4}{\equiv} 3$ ندارد. چرا که آنگاه $q \mid a^2 + 1$ و بنابراین $q \mid 1$ که تناقض است. پس تمامی عوامل فرد b و c به فرم $4k + 1$اند. اگر هر دوی b و c فرد باشند $b, c \overset{4}{\equiv} 1$ و لذا $bc \overset{4}{\equiv} 2 - 1 - 1 \overset{4}{\equiv} a^2$ که امکان‌پذیر نیست. پس چون c بنابر فرض مساله فرد است باید b زوج باشد. اگر $4 \mid b$ آنگاه $-1 \overset{4}{\equiv} a^2 + bc \overset{4}{\equiv} a^2$ که امکان‌پذیر نیست. پس b به شکل $4k + 2$ است. در جمع‌بندی این موارد، اعداد اول $p_1, \ldots, p_r$ و $q_1, \ldots, q_s$ با $p_1, \ldots, p_r, q_1, \ldots, q_s \overset{4}{\equiv} 1$ موجودند که $b = \pm 2q_1 \ldots q_s$ و $c = \pm p_1 \ldots p_r$. از آن‌چه که درباره‌ی تجزیه‌ی اعداد اول به فرم $4k + 1$ در $\mathbb{Z}[i]$ بیان گردید، اعداد $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}[i]$ و $\beta_1, \ldots, \beta_s \in \mathbb{Z}[i]$ موجودند که عناصری اول از $\mathbb{Z}[i]$اند و:

$$\forall 1 \leq t \leq r : \alpha_t \bar{\alpha}_t = p_t, \forall 1 \leq j \leq s : \beta_j \bar{\beta}_j = q_j \Rightarrow N(\alpha_t) = p_t, N(\beta_j) = q_j$$

حال در $\mathbb{Z}[i]$ می‌توان نوشت:

$$a^۲+۱=-bc \Rightarrow (a+i)(a-i)=-bc=\pm ۲(\alpha_۱\bar{\alpha}_۱)\cdots(\alpha_r\bar{\alpha}_r)(\beta_۱\bar{\beta}_۱)\cdots(\beta_s\bar{\beta}_s)$$
$$=\pm((۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s)(\overline{(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s})$$

چون برای هر $۱\leq t\leq r$ و $۱\leq j\leq s$، α_t و β_j عناصر اولی از $\mathbb{Z}[i]$ هستند، $\alpha_t|(a+i)(a-i)$ و $\beta_j|(a+i)(a-i)$ که از تساوی فوق حاصل می‌شوند نشان می‌دهند که $\alpha_t|a+i$ یا $\alpha_t|a-i$ یا معادلا با توجه به $\overline{a+i}=a-i$: $\alpha_t|a+i$ یا $\bar{\alpha}_t|a+i$ و به طور مشابه $\beta_j|a+i$ یا $\bar{\beta}_j|a+i$.

پس با جابه‌جا کردن α_t و $\bar{\alpha}_t$ یا β_j و $\bar{\beta}_j$ در صورت لزوم، فرض می‌کنیم که برای هر $۱\leq t\leq r$ و $۱\leq j\leq s$؛ $\alpha_t|a+i$ و $\beta_j|a+i$. به علاوه $۱\pm i$ هم در $\mathbb{Z}[i]$ به دلیل $N(۱\pm i)=۲$ اول‌اند. پس $۱+i|a+i$ یا $۱-i|a+i$ که دوباره بنابر تقارن و عوض کردن جای a و $-a$ در صورت لزوم، فرض می‌کنیم که $۱+i|a+i$. پس $۱+i,\alpha_۱,\ldots,\alpha_r$ و همچنین $\beta_۱,\ldots,\beta_s$ عوامل اولی از $a+i$ در $\mathbb{Z}[i]$ هستند.

حال اگر تجزیه‌ی $a+i$ در $\mathbb{Z}[i]$ را به صورت $a+i=\gamma_۱\cdots\gamma_u$ بگیریم، از بالا:

$$(\gamma_۱\cdots\gamma_u)(\overline{\gamma_۱\cdots\gamma_u})$$
$$=\pm((۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s)(\overline{(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s})$$

حال از یکتایی تجزیه به سادگی نتیجه می‌گردد که

$$\gamma_۱\cdots\gamma_u=\pm(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s$$

چرا که هر γ_i باید در سمت راست هم ظاهر شود و اگر یکی از $\bar{\alpha}_t$ یا $\bar{\beta}_j$ باشد، چون α_t یا β_j هم عوامل اول $a+i$ هم بودند، باید α_t یا β_j، هردوی $a\pm i$ و لذا a را بشمارند. در هر حال چون α_t عامل c در $\mathbb{Z}[i]$ و β_j عامل b در $\mathbb{Z}[i]$ بودند، a و c یا a و b در $\mathbb{Z}[i]$ نسبت به هم اول نیستند. ولی این تناقض است چرا که $a^۲+bc=-۱$ نشان می‌دهد که a و b و همچنین a و c در $\mathbb{Z}$ نسبت به هم متباین‌اند. پس

$$a+i=\gamma_۱\cdots\gamma_u=\pm(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s$$

حال قرار می‌دهیم

$$\alpha_۱\cdots\alpha_r=C+Di$$

$$\pm(۱+i)\beta_۱\cdots\beta_s=A-Bi$$

که در آن A، B، C و D صحیح‌اند. پس $a+i=(A-Bi)(C+Di)$. لذا با در نظر گرفتن اجزا حقیقی و موهومی $AC+BD=a$ و $AD-BC=۱$. به علاوه

$$C^۲+D^۲=N(Ci+D)=N(\alpha_۱\cdots\alpha_r)=p_۱\cdots p_r=c$$

پس $A,B,C,D\in\mathbb{Z}$ خواص مطلوب را برآورده می‌کنند.

تذکر. ایده‌ی این سوال در ابتدا از عمل گروه $SL(۲,\mathbb{Z})$ بر نیم‌صفحه‌ی بالا یعنی $\mathcal{H}=\{z\in\mathbb{C}\mid Imz>۰\}$ گرفته شد. عضو

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL(۲,\mathbb{Z})$$

بر $\mathcal{H}$ با تبدیلات خطی-کسری به صورت $z\mapsto\frac{az+b}{cz+d}$ عمل می‌کند. در این عمل اعضایی از $SL(۲,\mathbb{Z})$ (به جز $\pm I$) بیضوی[۴] نامیده می‌شوند که نقطه‌ی ثابتی در عمل بر $\mathcal{H}$ داشته باشند و می‌توان نشان داد که شرط لازم و کافی برای برآورده شدن این شرط آن است که تریس این ماتریس به $\{۰,\pm۱\}$ تعلق داشته باشد. می‌توان نشان داد که نقاطی از $\mathcal{H}$ که بیضوی یعنی نقطه‌ی ثابت عنصری به جز $\pm I$ از $SL(۲,\mathbb{Z})$ باشند، یا در مدار عمل iاند یا در مدار عمل $\exp(\frac{۲\pi i}{۶})$.

ایده‌ی طرح سوال این بود که عنصری از $SL(۲,\mathbb{Z})$ با تریس صفر که لاجرم به شکل

$$\begin{pmatrix} a & b\\ c & -a\end{pmatrix}$$

[۴] elliptic

با $a^2+bc=-1$ خواهد بود، در نظر گرفته شود و نقطه‌ی ثابت تبدیل خطی-کسری $z\mapsto \frac{az+b}{cz+d}$ متناظر محاسبه گردد و اینکه این نقطه از $\mathcal{H}$ در مدار i باشد، معادل است با وجود $A,B,C,D\in\mathbb{Z}$ با خواص مذکور.

البته پس از امتحان متوجه شدیم که متاسفانه سوال تکراری است و یک بار در دوره‌های المپیاد ریاضی دبیرستانی مطرح شده است!

سوال ۵. *فرض کنید G یک زیرگروه از $GL_n(\mathbb{Z})$ (ماتریس‌های $n\times n$ با درایه‌های صحیح و $\det=\pm 1$) است که برای هر $g\in G$ عدد $m\geq 1$ وجود دارد به طوری که $g^m=1$. ثابت کنید:*

الف) عدد طبیعی N وجود دارد به طوری که برای هر $g\in G$ داریم $g^N=1$

ب) G یک گروه متناهی است و یک کران برای مرتبه‌ی آن برحسب تابعی از n بیابید.

(*طراح:* دکتر غلامزاده محمودی)

پاسخ سوال ۵. *حل قسمت الف:* هر $g\in G$ ماتریسی $n\times n$ با درایه‌های صحیح است که $g^m=I_n$ و لذا چندجمله‌ای مینیمال g چندجمله‌ای x^m-1 را می‌شمارد. ولی این چندجمله‌ای و در نتیجه چندجمله‌ای مینیمال g ریشه‌ی تکراری ندارند و بنابراین g قطری‌پذیر است و درایه‌های روی قطر آن باید ریشه‌های واحد باشند، چرا که مقادیر ویژه‌ی g باید در $x^m-1=0$ صدق کنند. پس هر $g\in GL(n,\mathbb{Z})$ را می‌توان بر $\mathbb{C}$ قطری کرد و درایه‌های روی قطر، ریشه‌های واحد خواهند بود. ولی این ریشه‌ها باید در چندجمله‌ای مشخصه‌ی g هم که چندجمله‌ای تکین از درجه‌ی n و با ضرایب صحیح است صدق کنند. لذا باید چندجمله‌ای مینیمال ریشه‌ی واحد مذکور بر $\mathbb{Q}$، چندجمله‌ای درجه‌ی nای را بشمارد. ولی می‌دانیم که اگر $\omega\in\mathbb{C}$ یک ریشه‌ی اولیه‌ی kام واحد باشد، یعنی k کوچکترین عددی باشد که $\omega^k=1$، آن‌گاه چندجمله‌ای مینیمال ω از چندجمله‌ای‌های موسوم به دایره‌بُر[5] و از درجه‌ی $\phi(k)$ است. پس اگر یک ریشه‌ی اولیه‌ی kام واحد، مقدار ویژه‌ی یکی از عناصر G باشد، باید $\phi(k)\leq n$. ولی $\lim_{m\to\infty}\phi(m)=\infty$. پس تعداد kهایی از این دست متناهی است و لذا اگر N' را بزرگترین عدد طبیعی‌ای بگیریم که $\phi(N')\leq n$، هر مقدار ویژه‌ی یکی از عناصر $g\in G$ مانند ω، باید $\omega^{N'!}=1$ را برآورده کند. چرا که اگر k کوچکترین عدد طبیعی‌ای باشد که برای این ω، $\omega^k=1$ (یعنی ω ریشه‌ی اولیه‌ی kام واحد باشد) چندجمله‌ای مینیمال ω بر $\mathbb{Q}$ چندجمله‌ای از درجه‌ی $\phi(k)\leq n$ خواهد بود و لذا $k\leq N'$. پس چون $k\mid N'!$:

$$\omega^k=1\Rightarrow\omega^{N'!}=1$$

حال قرار می‌دهیم $N:=N'!$. آن‌چه بیان شد نشان می‌دهد که برای هر $g\in G$، مقادیر ویژه‌ی $g^N\in GL(n,\mathbb{Z})$ همگی ۱ اند. ولی این ماتریس قطری‌پذیر است چرا که g این‌گونه بود و ماتریس قطری‌پذیری که تمامی مقادیر ویژه‌اش ۱ باشند همانی است. پس این N خاصیت مطلوب را برآورده می‌کند: $g^N=I_n$ برای هر $g\in G$.

حل قسمت ب:

راه‌حل اول(دکتر غلامزاده) - $GL(n,\mathbb{Z})$ و به تبع آن G را می‌توان زیرمجموعه‌ای از فضای برداری متناهی‌البعد $M(n,\mathbb{Q})$ متشکل از ماتریس‌های $n\times n$ با درایه‌های گویا گرفت. پس زیرمجموعه‌ای متناهی از G مانند $\{A_1,\dots,A_l\}$ موجود است به قسمی که هر عنصر G را می‌توان به صورت ترکیب خطی با ضرایب گویا از $A_1,\dots,A_l$ نوشت(در واقع برای انتخاب A_iها کافی است زیرمجموعه‌ای از G با حداکثر تعداد عضو ممکن را در نظر گرفت که عناصرش بر $\mathbb{Q}$ مستقل باشند). با توجه به اینکه G زیرگروهی از $GL(n,\mathbb{Z})$ است، نگاشتی به صورت زیر داریم:

$$(*)\begin{cases}G\to\mathbb{Z}^l\\ A\mapsto(tr(AA_1),\dots,tr(AA_l))\end{cases}$$

(tr نماد تابعک تریس است). برد این نگاشت متناهی است زیرا از (الف) به ازای Nای، $g^N=I_n$ برای هر $g\in G$ و لذا مقادیر ویژه‌ی هر عنصر g به مجموعه‌ی متناهی $\{e^{\frac{2\pi ik}{N}}\mid 0\leq k<N\}$ تعلق دارند و بنابراین $tr(g)$ که جمع n مقدار ویژه‌ی g است، حداکثر N^n حالت دارد. پس در نگاشت $G\to\mathbb{Z}^l$ که در (*) تعریف شد، هر مولفه حداکثر N^n حالت دارد و لذا تعداد اعضای برد این نگاشت از N^{nl} تجاوز نمی‌کند. پس اگر یک‌به‌یک بودن $G\to\mathbb{Z}^l$ ثابت شود، نتیجه می‌شود که G متناهی است و

[5] Cyclotomic

$| G | \leq N^{nl}$. برای اثبات یک‌به‌یک بودن فرض کنید $A, B \in G$ چنان باشند که برای هر $1 \leq i \leq l$: $tr(AA_i) = tr(BA_i)$.
لذا چون روش انتخاب $\{A_1, \ldots, A_l\}$ هر عنصر G را می‌توان به صورت یک ترکیب خطی A_iها با ضرایب گویا توصیف کرد:

$$\forall g \in G : tr(Ag) = tr(Bg)$$

علی‌الخصوص برای $g = B^{-1} \in G$: $tr(AB^{-1}) = tr(I_n)$. پس جمع n مقدار ویژه (با حساب تکرر) از $AB^{-1} \in G$، n است. ولی دیدیم که تمامی این مقدار ویژه‌ها ریشه‌های Nام واحد هستند ولذا از $AB^{-1} = I_n$ نتیجه می‌شود $A = B$. پس نشان دادیم که $| G | \leq N^{nl}$.

چون زیرمجموعه‌ی $\{A_1, \ldots, A_l\}$ از $M(n, \mathbb{Q})$ مستقل خطی بود پس $l \leq n^2$. N هم باید تنها این ویژگی را داشته باشد که برای هر $g \in G$، $g^N = I_n$ و در حل (الف) دیدیم که بدین منظور کافی است قرار داد $N = \prod_{\{k \in \mathbb{N} | \phi(k) \leq n\}} k$. لذا کرانی برای $| G |$ بدین شرح است:

$$|G| \leq N^{nl} \leq N^{n^3} \Rightarrow |G| \leq (\prod_{\{k \in \mathbb{N} | \phi(k) \leq n\}} k)^{n^3}$$

راه‌حل دوم(دکتر جعفری) - دوباره N را مشابه قسمت (الف) عدد طبیعی‌ای بگیرید با این ویژگی که برای هر $g \in G$، g^N همانی باشد. p را عدد اولی بگیرید که نسبت به N اول است. با در نظر گرفتن درایه‌های عناصر $GL(n, \mathbb{Z})$ به پیمانه‌ی p، به یک همریختی گروهی $G \to GL(n, \mathbb{Z}_p)$ می‌رسیم که درایه‌های هر $A \in G$ را به پیمانه‌ی p در نظر می‌گیرد. ادعا می‌کنیم که این همریختی گروهی یک‌به‌یک است و این امر نتیجه خواهد داد که $|G| \leq |GL(n, \mathbb{Z}_p)|$.

فرض کنید $A \in G$ در هسته‌ی این همریختی باشد، یعنی با درایه‌های بر میدان $\mathbb{Z}_p$: $\bar{A} = I_n$. لذا ماتریس $n \times n$، B با درایه‌های صحیح موجود است که $A = I_n + pB$. با نوشتن آن به صورت $A = I_n + p^k B$ به ازای $k \geq 1$ مناسبی، می‌توان فرض کرد که حداقل یک درایه‌ی B بر p بخش‌پذیر نیست، چرا که اگر چنین kای موجود نباشد، $B = 0$ و لذا $A = I_n$ که همان چیزی است که در پی آنیم. پس A را به شکل $I_n + p^k B$ که $k \geq 1$ و B را با ویژگی مذکور بگیرید. چون در $GL(n, \mathbb{Z})$، $A^N = I_n$، داریم:

$$(I_n + p^k B)^N = I_n \Rightarrow \sum_{i=1}^{N} \binom{N}{i} p^{ki} B^i = 0 \Rightarrow NB = -\sum_{i=2}^{N} \binom{N}{i} p^{k(i-1)} B^i$$

با توجه به اینکه این تساوی‌ها میان ماتریس‌های با درایه‌های صحیح هستند، نتیجه می‌شود که p^k همه‌ی درایه‌های NB را می‌شمارد. ولی p نسبت به N اول بود و حداقل یکی از درایه‌های B را عاد نمی‌کرد. بنابراین به تناقض می‌رسیم و یک‌به‌یک بودن

$$G \to GL(n, \mathbb{Z}_p)$$

ثابت می‌شود. کران $|G|$ را هم می‌توان تعداد اعضای $GL(n, \mathbb{Z}_p)$ گرفت.

مجله شفاهی

دانشکده علوم ریاضی دانشگاه صنعتی شریف

چهارشنبه آخر هر ماه

ریاضیات فرهنگ گسترده‌ای دارد. یکی از نیازهای هر ریاضیدان آشنایی با این فرهنگ است. مجله‌ی شفاهی فعالیتی است که توسط جمعی از اساتید و دانشجویان دانشکده‌ی علوم ریاضی دانشگاه صنعتی شریف پایه‌گذاری شده‌است و هدف اصلی آن افزایش دانش عمومی افراد در زمینه‌های گوناگون ریاضیات است. مخاطبین اصلی مجله‌ی شفاهی دانشجویان تحصیلات تکمیلی هستند. از دیگر اهداف مجله‌ی شفاهی، گسترش ارتباط و همکاری علمی خصوصا در بین رشته‌های مختلف در دانشکده و افزایش روحیه‌ی جمعی از طریق مشارکت اساتید و دانشجویان است.

در هر شماره‌ی مجله‌ی شفاهی تعدادی سخنرانی ریاضی ارائه خواهد شد که مشخصه‌ی اساسی آن‌ها توصیفی بودن در عین فنی بودن و کیفیت بالای علمی آن‌ها است. از آن‌جا که تولید چنین سخنرانی‌هایی دشوار است، یکی از راه‌بردهای مجله‌ی شفاهی استفاده از مقالات نشریات مکتوبی است که معیارهای مورد نظر را دارند.

مجله‌ی شفاهی از مقولات جنبی ریاضی هم غافل نمی‌ماند. به همین منظور در هر شماره نشستی با موضوعاتی چون آموزش، پژوهش، تاریخ و فلسفه‌ی ریاضی و نقد و بررسی نشر، اخبار و موضوعات روز جامعه‌ی ریاضی برگزار می‌شود.

مجله‌ی ریاضی شریف از هر گونه همکاری در تمامی زمینه‌ها از جمله تهیه یا معرفی مطالب علمی و توصیفی وهمچنین همکاری در زمینه کارهای اجرایی مجله از جانب دانشجویان و اساتید استقبال به عمل می‌آورد. لازم به ذکر است که اکثر همکاران فعلی این مجله به‌صورت کاملا داوطلبانه با مجله همکاری می‌کنند و اساس کار این نشریه بر مبنای همکاری داوطلبانه‌ی اهالی دانشکده‌ی ریاضی قرار گرفته‌است.

تماس با ما:

mathematicsjournal@gmail.com
www.sharifmathjournal.ir

[illegible]