**فرهنگ و اندیشهٔ ریاضی**
**شمارهٔ ۳۰(بهار ۱۳۸۲)، صص. ۳۵ تا ۳۸**

# برهانی ساده از قضیهٔ رول برای هیأت‌های متناهی

س. بالانتین و ج. رابرتس

ترجمه: علی معدنشکاف

## ۱. مقدمه

یکی از قضایای اساسی در حساب دیفرانسیل قضیهٔ رول است: ریشه‌های مشتق یک تابع بین ریشه‌های آن تابع قرار دارند. یک نتیجهٔ قضیهٔ رول این است که اگر یک چندجمله‌ای با ضرایب حقیقی روی هیأت اعداد حقیقی شکافته شود آنگاه مشتق آن نیز چنین خواهد شد. این شرط ضعیف‌تر را خاصیت رول می‌گوییم.

از این رو می‌توانیم سؤال کنیم که برای چه هیأت‌های دیگری چند جمله‌ای‌ها از خاصیت رول پیروی می کنند؟ این پرسش نخستین بار توسط کاپلانسکی در [۳، صفحه ۳۰] مطرح شد. به وضوح دیده می‌شود که خاصیت رول برای اعداد مختلط برقرار است ولی برای اعداد گویا برقرار نیست. طبیعی است بپرسیم که آیا این خاصیت برای هیأت‌های متناهی نیز برقرار است یا نه. در [۱] و [۲] توماس کراون و جرج زوردس برای تعیین هیأت‌هایی از مشخصهٔ متناهی که برای آنها خاصیت رول برقرار است از دنباله‌های مضربی بهره بردند. به هر حال، برهان آنها کاملاً تکنیکی بود. ما این پرسش را برای هیأت‌های متناهی تنها با استفاده از نتایج اساسی نظریهٔ هیأت‌های متناهی پاسخ خواهیم داد.

## ۲. مقدمات

برای هر هیأت $F$، فرض کنید $F^{۲} = \{x^{۲} : x \in F\}$ مجموعهٔ همهٔ مربعات در $F$ باشد. فرض کنید $\mathbf{F}_q$ هیأت متناهی با $q$ عنصر باشد. فرض می‌کنیم $F^*$ مجموعه عناصر ناصفر $F$ باشد. یک هیأت فیثاغورثی نامیده می‌شود اگر هر مجموعی از مربعات یک مربع باشد.

**گزارهٔ ۱.** یک هیأت متناهی $F$ از مشخصهٔ فرد فیثاغورثی نیست.

**برهان** گیریم $p$ مشخصهٔ هیأت باشد. فرض کنید به ازای هر عنصر $\alpha$ از $F^{۲}$، $\alpha + ۱$ یک مربع باشد. برای هر عنصر $\beta \in F$، مجموعهٔ $\{\beta, \beta + ۱, \ldots, \beta + p - ۱\}$ یا مشمول در $F^{۲}$ است یا از $F^{۲}$ مجزا است. از این رو تعداد مربعات در $F$ می‌بایست بر $p$ بخش‌پذیر باشد. به هر حال، اگر $|F| = p^n$ آنگاه $|F^{۲}| = (p^n + ۱)/۲$. از آنجا که، $p \nmid (p^n + ۱)/۲$، باید حداقل یک عنصر $\alpha$ از $F$ چنان موجود باشد که $\alpha$ یک مربع باشد ولی $\alpha + ۱$ یک مربع نباشد. پس $\alpha + ۱$ مجموعی از دو مربع است که یک مربع نیست، بنابراین $F$ فیثاغورثی نیست. □

**نتیجهٔ ۲.** اگر $F$ یک هیأت از مشخصهٔ فرد باشد مجموعهٔ $\mathcal{T} = \{\alpha + ۱ : \alpha \in F^{۲}\}$ شامل حداکثر یک مربع و حداقل یک نامربع است.

**برهان.** همان‌گونه که در برهان گزارهٔ قبل مشاهده شد، مجموعهٔ $\mathcal{T}$ شامل یک نامربع است. از آنجا که تنها $(p^n - ۱)/۲$ نامربع موجود است، $\mathcal{T}$ که دارای عدد اصلی $(p^n + ۱)/۲$ است می‌بایست شامل یک مربع باشد. □

## ۳. قضیهٔ اصلی

اکنون آماده‌ایم که قضیهٔ اصلی‌مان را بیان و اثبات کنیم.

**قضیهٔ ۳.** تنها هیأت‌های متناهی که از خاصیت رول پیروی می‌کنند $\mathbf{F}_{۲}$ و $\mathbf{F}_{۴}$ هستند.

**برهان.** ابتدا نشان می‌دهیم که برای یک هیأت $F$ از مشخصهٔ فرد باید یک چندجمله‌ای $f(x) \in F[x]$ موجود باشد که در $F$ شکافته شود و مشتقش در $F$ شکافته نشود.

فرض کنیم $F$ هیأتی از مشخصه فرد باشد. خانوادهٔ چندجمله‌ای‌های

$$f(x) = (x - ۲)(x + ۲)(x - ۲a)(x + ۲a)$$

که در آن $a \in F$ را در نظر بگیرید. بنابراین

$$f'(x) = ۴x(x^{۲} - ۲(a^{۲} + ۱)),$$

که در $F[x]$ شکافته می‌شود اگر و تنها اگر مبین $8(a^2+1)$ از عامل دوم آن یک مربع در $F$ باشد. بنابراین $2(a^2+1)$ باید یک مربع باشد. اگر $2 \in F^2$ آنگاه باید به ازای هر $a \in F$ داشته باشیم $a^2+1 \in F^2$، و اگر $2 \notin F^2$ آنگاه باید به ازای هر $a \in F$ داشته باشیم $a^2+1 \notin F^2$. بنا بر نتیجهٔ ۲ هر دو وضعیت غیرممکن می‌باشند. بنابراین باید $a \in F$ای چنان موجود باشد که $f'(x)$ در $F$ شکافته نشود. از این رو هر هیأت متناهی از مشخصه فرد خاصیت رول را ندارد.

حال یک هیأت $F$ از مشخصهٔ ۲ را که حداقل ۸ عضو دارد در نظر می‌گیریم. فرض کنیم

$$f(x) = x(x+1)(x+a)(x+a+1)(x+b)(x+b+1) \quad , \quad a, b \in F$$

یک خانواده از چندجمله‌ای‌ها باشد. پس

$$f'(x) = x^4 + x^2 + (a^2+a)(b^2+b).$$

فرض کنیم برای هر $a, b \in F$، $f'(x)$ شکافته شود. پس چندجمله‌ای $x^2 + x + (a^2+a)(b^2+b)$ نیز برای هر $a, b \in F$ شکافته می‌شود و بنابراین برای هر $a$ و $b$ می‌توانیم $A, B \in F$ را چنان بیابیم که

$$x^2 + x + (a^2+a)(b^2+b) = (x+A)(x+B)$$

باید $A + B = 1$ و $AB = (a^2+a)(b^2+b)$ و بدین ترتیب $(a^2+a)(b^2+b) = A^2 + A$.

بنابراین اگر $f'(x)$ در $F$ به ازای هر $a, b \in F$ شکافته شود نتیجه می‌شود که مجموعهٔ

$$S = \{\gamma^2 + \gamma : \gamma \in F\}$$

تحت ضرب بسته است. فرض کنید $\alpha \in S^*$. چون $F^*$ یک گروه متناهی است عدد صحیح $m$ای موجود است که برای آن $\alpha^m = 1$. بنابراین ۱ به $S$ متعلق است و معکوس هر عنصر ناصفر $S$ در $S$ است. چون $\mathrm{char}(F) = 2$ ، $S$ تحت جمع تشکیل یک گروه می‌دهد. بنابراین $S$ یک زیرهیأت $F$ است. به علاوه، اگر $F$ دارای $2^n$ عنصر باشد و $n \geq 3$، آنگاه $S$ دارای $2^{n-1}$عنصر خواهد بود زیرا دقیقاً زمانی که $\alpha = \beta$ یا $\alpha = \beta + 1$ باشد، $\alpha^2 + \alpha = \beta^2 + \beta$ خواهد بود. این ایجاب می‌کند که $n - 1 | n$ که یک تناقض است. بنابراین $S$ تحت ضرب بسته نیست و باید $a, b \in F$ موجود باشند که به ازای آنها $f'(x)$ شکافته نشود و بنابراین $F$ دارای خاصیت رول نخواهد بود.

اکنون نشان خواهیم داد که $\mathbf{F}_2$ و $\mathbf{F}_4$ در خاصیت رول صدق می‌کنند. اگر $f(x)$ یک چندجمله‌ای در $\mathbf{F}_2[x]$ باشد که روی $\mathbf{F}_2$ شکافته می‌شود آنگاه $f(x) = x^a(x+1)^b$، که $a$ و $b$ اعداد صحیح نامنفی می‌باشند. از آنجا که مشتق $f(x) = (h(x))^2 k(x)$، $f'(x) = (h(x))^2 k'(x)$ می‌باشد. کافی است حالتی را در نظر بگیریم که $f(x)$ بدون مربع است، به عبارت دیگر $a, b \leq 1$. چهار امکان وجود دارد.

| $a$ | $b$ | $f'(x)$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

در هر حالت، $f'(x)$ روی $\mathbf{F}_۲$ شکافته می‌شود، بنابراین $\mathbf{F}_۲$ خاصیت رول را دارد.

اگر $\mathbf{F}_۴$ یک هیأت متناهی با ۴ عنصر باشد آنگاه $F_۴ = \{۰, ۱, \alpha, \alpha + ۱\}$ که $\alpha^۲ = \alpha + ۱$. اگر یک چندجمله‌ای $f(x)$ در $F_۴$ شکافته شود، می‌تواند به صورت

$$f(x) = x^b(x+۱)^c(x+\alpha)^d(x+\alpha+۱)^e$$

نوشته شود که $b$، $c$، $d$ و $e$ اعداد صحیح نامنفی هستند. همانند حالت $\mathbf{F}_۲$، چون مشتق $f(x) = (h(x))^۲k(x)$، $f'(x) = (h(x))^۲k'(x)$ می‌باشد کافی است حالتی را در نظر بگیریم که $b, c, d, e \leq ۱$. اگر یکی از $b$، $c$، $d$، $e$ برابر ۰ باشند آنگاه $f(x) = Ax^۳ + Bx^۲ + Cx + D$ که $A, B, C, D \in \mathbf{F}_۴$ و $f'(x) = Ax^۲ + C$. از آنجا که هر عنصر در $\mathbf{F}_۴$ یک مربع است $f'(x)$ در $\mathbf{F}_۴$ شکافته می‌شود. اگر $b = c = d = e = ۱$ آنگاه $f(x) = x^۴ + x$ و $f'(x) = ۱$ در $\mathbf{F}_۴$ شکافته می‌شود.

چون $f'(x)$ در هر حالت شکافته می‌شود $\mathbf{F}_۴$ خاصیت رول دارد. □

# مراجع


[1] T. Craven and G. Csordas, Multiplier sequences for fields, *Illinois J. Math.* 21 (1977) 801-817.

[2] T. Craven, A weak version of Rolle's theorem, *Proc. Amer. Math. Soc.* 125 (1997) 3147-3153.

[3] I. Kaplansky, *Fields and Rings,* 2nd. ed., University of Chicago Press, Chicago, 1972.



ترجمه: علی معدنشکاف

دانشگاه سمنان، دانشکدهٔ تربیت دبیر مهدی‌شهر، گروه ریاضی

پست الکترونیک: amadanshekaf@semnan.ac.ir