حل‌پذیری با رادیکال‌ها

در زمان چندجمله‌ای

علیرضا شاولی

مقدمه

- خوارزمی و حل معادله‌ی درجه ۲
- ریاضیدانان ایتالیایی و حل معادله‌ی درجه ۳ و ۴
- آبل و حل ناپذیری معادله‌ی درجه ۵ در حالت کلی
- گالوا و پایان مسئله‌ی حل‌پذیری با رادیکال‌ها از جنبه‌ی نظری
- بررسی حل‌پذیری معادله‌ی درجه n با ضرایب گویا در زمان چندجمله‌ای بر حسب n (لانداو-میلر)
  - سایز ضرایب
  - معادله‌ی چندجمله‌ای روی میدان عددی

سرفصل‌ها

- مروری بر نظریه گالوا
- حل‌پذیری با رادیکال‌ها
- محک گالوا برای حل‌پذیری
- حل‌پذیری با رادیکال‌ها در زمان چندجمله‌ای
- محاسبه‌ی بلوک مینیمال عمل گروه گالوا روی ریشه‌ها

نکات و تعاریف اولیه

- در این ارائه همه‌ی میدان‌هایی که ما در نظر می‌گیریم در واقع زیرمجموعه‌های اعداد مختلط هستند با همان عمل جمع و ضرب مختلط
  - لذا مشخصه همیشه صفر است و مشکل جدایی‌پذیری و … نداریم
- اگر F یک میدان باشد و $\alpha_1, \dots, \alpha_m \in \mathbb{C}$ آنگاه $F(\alpha_1, \dots, \alpha_m)$ کوچکترین میدان شامل F و α_i هاست.
- به عنوان نمونه برای $b \in F$: $F\left(\sqrt[n]{b}\right) = \left\{a_0 + a_1\sqrt[n]{b} + a_2\sqrt[n]{b}^2 + \cdots + a_{n-1}\sqrt[n]{b}^{n-1} : a_i \in F\right\}$
  - مثال) $\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\right\}$ یک توسیع درجه سوم از $\mathbb{Q}$ است.
  - مثال) اگر $\omega = e^{2\pi i/3}$ ریشه سوم واحد باشد $\mathbb{Q}\left(\sqrt[3]{2},\omega\right) = \left\{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} + a_3\omega + a_4\omega\sqrt[3]{2} + a_5\omega\sqrt[3]{4}\right\}$
- برای توسیع K/F مجموعه‌ی خودریختی‌های K که F را ثابت نگه می‌دارند گروه گالوای آن می‌نامیم.

$$Gal(K/F) = \{\sigma \in Aut(K) \mid \forall a \in F : \ \sigma(a) = a\} \subseteq Aut(K)$$

خودریختی میدان‌ها و گروه‌گالوا

- مثال:
  - گروه $Gal(\mathbb{C}/\mathbb{R})$ دارای دو عضو است. همانی و مزدوج کردن مختلط
  - گروه $Gal\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)$ بدیهی است (تنها عنصر آن همانی است)
  - گروه $Gal\left(\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}\right)$ دارای ۶ عضو است
- توسیع (متناهی) K/F را گالوایی می‌نامیم اگر $|Gal(K/F)| = [K:F]$
- قضیه: فرض کنید P یک چندجمله‌ای تحویل‌ناپذیر روی F باشد و $\alpha_1, \dots, \alpha_n$ ریشه‌های آن باشند. آنگاه میدان $F(\alpha_1, \dots, \alpha_n)$ (میدان شکافنده‌ی P) یک توسیع گالوایی F است.
- مثال: اگر F شامل یک ریشه n ام اولیه واحد باشد، $F\left(\sqrt[n]{b}\right)/F$ گالوایی و گروه گالوایش دوری است.
- قضیه: توسیع K/F گالوایی است اگر و تنها اگر $\mathcal{F}ix\left(Gal(K/F)\right) = F$

قضیه‌ی اساسی گالوا

- برای هر توسیع (متناهی) گالوایی K/F یک تناظر یک به یک و وارون‌کننده‌ی شمول بین میدان‌های بینابینی $K \supseteq L \supseteq F$ و زیرگروه‌های گروه $G = Gal(K/F)$ وجود دارد که ضابطه‌ی آن به این صورت است:
  - به میدان L بین K و F زیرگروه $Gal(K/L)$ از G نسبت داده می‌شود.
  - به زیرگروه H از G میدان بینابینی $\mathcal{F}ix(H) = \{x \in K | \forall \sigma \in H: \sigma(x) = x\}$ نسبت داده می‌شود.
- به علاوه زیرگروه $H = Gal(K/L)$ از G نرمال است اگر و تنها اگر $L = \mathcal{F}ix(H)$ یک توسیع گالوایی از F باشد و در این صورت داریم $Gal(L/F) \cong G/H$ (دقت کنید K/L همیشه گالوایی هست)

حل‌پذیری با رادیکال‌ها

- می‌دانیم معادله‌ی درجه‌ی ۲ و ۳ و ۴ را می‌توان با کمک رادیکال‌ها حل کرد. به عنوان مثال یک جواب معادله‌ی درجه سوم $x^3+ax+b=0$ برابر $\sqrt[3]{-\frac{b}{2}-\sqrt[2]{\frac{b^2}{4}+\frac{a^3}{27}}}+\sqrt[3]{-\frac{b}{2}+\sqrt[2]{\frac{b^2}{4}+\frac{a^3}{27}}}$ است.
- به طور کلی می‌گوییم چندجمله‌ای f با ضرایب در میدان F توسط رادیکال‌ها قابل حل است اگر زنجیری از میدان‌های $F=F_0\subseteq F_1\subseteq\cdots\subseteq F_m$ وجود داشته باشد که $F_i=F_{i-1}\left(\sqrt[n_i]{a_i}\right)$ که n_i ها طبیعی و $a_i\in F_{i-1}$ به نحوی که تمام ریشه‌های f درون F_m باشد (f در F_m شکافته شود)
  - دقت کنید در تعریف بالا می‌توان فرض کرد F_i روی F_{i-1} گالوایی است (با افزودن ریشه‌های واحد مناسب)
  - همچنین می‌توان فرض کرد F_m/F گالوایی است (با گرفتن یک بستار نرمال)
- دقت کنید در تعریف بالا لازم نیست F_m میدان شکافنده‌ی f باشد بلکه شامل میدان شکافنده است.

گروه حل‌پذیر

- با کمک تناظر موجود در قضیه اساسی گالوا، زنجیر ساخته‌شده از میدان‌های قبل به زنجیری از زیرگروه‌های گروه $G = Gal(F_m/F)$ تبدیل می‌شود مانند

$$\{id\} = G_m \subseteq G_{m-1} \subseteq \cdots \subseteq G_0 = G$$

فرض گالوایی بودن هر میدان روی میدان قبلی به نرمال بودن هر زیرگروه در زیر گروه بعدی تبدیل می‌شود.
به علاوه گروه گالوای F_i/F_{i-1} برابر G_{i-1}/G_i است و لذا G_{i-1}/G_i دوری است.

- وجود چنین زنجیری از زیرگروه‌ها برای یک گروه دلخواه نابدیهی است و برای هر گروهی درست نیست

- به یک گروه متناهی G حل‌پذیر می‌گوییم اگر زنجیر $\{id\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ یافت شود که فاکتورهای G_{i-1}/G_i همگی دوری باشند.

- قضیه: هر خارج قسمت یک گروه حل‌پذیر خود حل‌پذیر است.

محک گالوا برای حل‌پذیری با رادیکال‌ها

- تا اینجا نشان داده‌ایم اگر $f \in F[x]$ با رادیکال‌ها حل‌پذیر باشد آنگاه توسیع گالوایی F_m از F شامل میدان شکافنده‌ی f وجود دارد که $Gal(F_m/F)$ گروهی حل‌پذیر است. اگر K میدان شکافنده‌ی f باشد طبق قضیه‌ی اساسی گالوا، $Gal(K/F) = {}^{Gal(F_m/F)}/_{Gal(F_m/K)}$ و لذا $Gal(K/F)$ حل‌پذیر است.

  می‌توان نشان داد عکس این حکم نیز درست است:

- قضیه (گالوا): چندجمله‌ای $f \in F[x]$ با رادیکال‌ها حل‌پذیر است اگر و تنها اگر $Gal(K/F)$ گروهی حل‌پذیر باشد.

نگاه محاسباتی

- قضیه‌ی گالوا به لحاظ نظری به نوعی مسئله‌ی حل‌پذیری با رادیکال‌ها را تمام می‌کند. با این حال از نظر محاسباتی مسئله هنوز قابل بررسی است. در واقع برای یک چندجمله‌ای درجه n گروه گالوای میدان شکافنده‌ی آن ممکن است از مرتبه‌ی $n!$ بزرگ باشد. بنابراین قاعدتا بررسی حل‌پذیری آن با بررسی مستقیم این گروه ممکن نیست.
- الگوریتمی به نام الگوریتم Sims وجود دارد که با داشتن یک مجموعه مولد برای گروه به همراه روابط آن‌ها، در زمان چندجمله‌ای (بر حسب تعداد مولدها و و تعداد و طول روابط) بررسی می‌کند که یک گروه حل‌پذیر هست یا نه. ولی هیچ الگوریتم در زمان چندجمله‌ای برای یافتن چنین نمایش مناسبی از گروه گالوا موجود نیست. با این حال لانداو و میلر در مقاله‌ای در ۱۹۸۵ نشان دادند که بدون محاسبه‌ی مستقیم گروه گالوا می‌توان حل‌پذیری چندجمله‌ای را در زمان چندجمله‌ای (بر حسب درجه و سایز ضرایب) بررسی کرد و حتی در صورت وجود جواب رادیکالی، آن را یافت.
- حال فرض کنید چندجمله‌ای درجه n با ضرایب گویا مثل f داده شده‌است و میدان شکافنده را K بنامید.
  - دقت کنید می‌توان از اول فرض کرد چندجمله‌ای داده شده تحویل ناپذیر است (به دلیل وجود الگوریتم‌هایی مثل LLL برای تجزیه)

نکاتی از نظریه گروه‌ها

- قضیه: فرض کنید N زیرگروه نرمالی از گروه G باشد. آنگاه G حل‌پذیر است اگر و تنها اگر N و G/N حل‌پذیر باشند.
- فرض کنید گروه G روی مجموعه‌ی $\Omega = \{\alpha_1, \dots, \alpha_m\}$ به طور تراگذر عمل کند. به زیرمجموعه‌ی B از Ω یک بلوک می‌گوییم اگر برای هر $\sigma \in G$ داشته باشیم $\sigma B = B$ یا $\sigma B \cap B = \emptyset$. کل Ω و تک عضوی‌ها را بلوک بدیهی گوییم.
- می‌گوییم عمل گروه G اولیه است اگر هیچ بلوک نابدیهی نداشته باشد.
- قضیه: عمل G اولیه است اگر و تنها اگر برای یک (هر) $\alpha \in \Omega$، G_α (پایدارساز α) زیرگروهی ماکسیمال باشد.
- در واقع قضیه خیلی کلی‌تری درست است. تناظر یک به یک و حافظ شمول بین گروه‌های بین G_α و G و بلوک‌های شامل α برقرار است که به بلوک B گروه G_B را نسبت می‌دهد و به گروه H بلوک $H\alpha$ را نسبت می‌دهد.

ایده‌های اصلی

- قضیه Palfy: اگر G گروهی حل‌پذیر باشد که روی یک مجموعه‌ی n عضوی به طور اولیه عمل‌کند آنگاه $|G| \leq n^4$
- این قضیه یکی از ایده‌های اصلی مقاله لانداو و میلر است. دقت کنید اگر مرتبه گروه گالوا از بزرگی چندجمله‌ای باشد با استفاده از الگوریتم Sims کار تمام است. مشکل این است که عمل گروه گالوا روی ریشه‌ها لزوماً اولیه نیست.
- اولیه بودن عمل گروه گالوا معادل این است که برای یک ریشه‌ی f مانند α زیرگروه G_α ماکسیمال باشد. حال دقت کنید $G_\alpha = Gal(K/\mathbb{Q}(\alpha))$ بنابراین طبق تناظر گالوا معادل این است که بین $\mathbb{Q}$ و $\mathbb{Q}(\alpha)$ میدانی نداریم.
- نکته قابل توجه بعدی این است که با اینکه گالوایی بودن خاصیت تراگذری نیست اما حل‌پذیری به یک معنی چنین است:
- لم: $F(\alpha) \subseteq F(\beta) \subseteq F$ و $h(x) = \min_{F(\beta)}(\alpha)$ و $g(x) = \min_{F}(\beta)$ و $f(x) = \min_{F}(\alpha)$. آنگاه f با رادیکال‌ها حل‌پذیر است اگر و تنها اگر h و g چنین باشند.
- در نتیجه هدف ما ساختن زنجیر $\mathbb{Q} \subset \mathbb{Q}(\beta_1) \subset \cdots \subset \mathbb{Q}(\beta_r) \subset \mathbb{Q}(\alpha)$ است که میدان بینابینی نداشته باشیم.

ساخت زنجیر ماکسیمال

- در ادامه روش ساخت اولین میدان یعنی $F=\mathbb{Q}(\beta_r)$ را توضیح می‌دهیم. روش ساخت بقیه مشابه است.
- فرض کنید $B=\{\alpha_1,\dots,\alpha_k\}$ یک بلوک مینیمال شامل α باشد. لذا این بلوک متناظر زیرگروه G_B است که بین G_B و G_α زیرگروهی نیست پس بین $\mathbb{Q}(\alpha)$ و $\mathcal{Fix}(G_B)$ میدانی نیست و کافیست این میدان را برابر F قرار دهیم.
  - دقت کنید لازم است این میدان را صریحاً محاسبه کنیم و سپس به فرم $\mathbb{Q}(\theta)$ بنویسیم.
- فرض کنید $h(x)=(x-\alpha_1)\dots(x-\alpha_k)$ و پس از پخش کردن $h(x)=x^k+\cdots+\beta_1x+\beta_0$ در این صورت هر عضو G_B چندجمله‌ای h و لذا β_i ها را ثابت نگه می‌دارد. به عکس هر عضو G که β_i را ثابت نگه دارد B را به خودش می‌نگارد پس عضو G_B است. پس $F=\mathbb{Q}(\beta_0,\dots,\beta_{k-1})$.
- برای نمایش این میدان به فرم $\mathbb{Q}(\theta)$ کافیست توجه کنید اگر α یک عدد جبری درجه n و β درجه m باشد آنگاه عدد طبیعی $\lambda\le mn+1$ یافت می‌شود که $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\alpha+\lambda\beta)$
- حال کافی است همین روند را برای θ به جای α تکرار کنیم.

محاسبه‌ی بلوک مینیمال

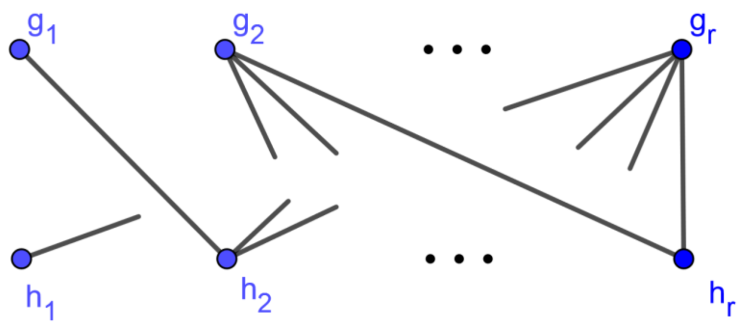
- بنابر اسلاید قبلی کافیست یک بلوک مینیمال را محاسبه کنیم که شامل α باشد.
- الگوریتم اتکینسون: اگر گروه n عضوی G روی یک مجموعه به طور تراگذر عمل کند در زمان چندجمله‌ای بر حسب n می‌توان یک بلوک مینیمال شامل عضو دلخواهی از مجموعه برای این عمل یافت.
  - دقت کنید این الگوریتم مستقیماً مشکل ما را حل نمی‌کند چون سایز گروه گالوا بزرگ است.
- چندجمله‌ای f را روی $\mathbb{Q}(\alpha)[x]$ تجزیه می‌کنیم. فرض کنید علاوه بر عامل $(x-\alpha)$ عوامل خطی دیگری مانند $\left(x-p_i(\alpha)\right)$ نیز ظاهر شوند که $p_i \in \mathbb{Q}[x]$. فرض کنید $p_i(\alpha)=\alpha_i$ و $1 \leq i \leq r$
- به سادگی $\Lambda=\{\alpha_1,\ldots,\alpha_r\}$ یک بلوک است ($\alpha_1=\alpha$) و از آنجا که عمل یک عضو G روی آن با عملش روی α مشخص می‌شود (چون بقیه چندجمله‌ای‌هایی بر حسب α هستند) لذا این عمل معادل عمل r تا جایگشت از S_Λ است و لذا با الگوریتم اتکینسون یک بلوک مینیمال آن را می‌توان یافت.

محاسبه‌ی بلوک مینیمال (ادامه)

- پس فرض می‌کنیم $f(x)$ در تجزیه‌اش در $\mathbb{Q}(\alpha)[x]$ عامل خطی به غیر از $x-\alpha$ ندارد. ابتدا به یک قضیه ساده نیاز داریم:
- قضیه: فرض کنید G روی Ω تراگذر عمل کند و G_α هیچ نقطه ثابتی جز α نداشته باشد (تجزیه f در $\mathbb{Q}(\alpha)[x]$ عامل خطی به غیر از $x-\alpha$ نداشته باشد) و Λ یک بلوک مینیمال شامل α باشد. آنگاه برای هر $\alpha \neq \theta \in \Lambda$ خواهیم داشت $\Lambda = \{\sigma(\alpha) : \sigma \in \langle G_\alpha, G_\theta \rangle\}$
- اثبات: کافیست دقت کنید $\{\sigma(\alpha) : \sigma \in \langle G_\alpha, G_\theta \rangle\}$ بلوک است و شامل Λ است.
- این قضیه روشی برای محاسبه‌ی بلوک مینیمال به دست می‌دهد (در صورت وجود). کافیست برای همه‌ی θها $\{\sigma(\alpha) : \sigma \in \langle G_\alpha, G_\theta \rangle\}$ را حساب کنیم و ببینیم کدام یک زیرمجموعه‌ی هیچ کدام دیگر نیست. اگر هم همه این بلوک‌ها بدیهی بودند بلوک مینیمال وجود ندارد (عمل اولیه است)

محاسبه‌ی بلوک مینیمال (ادامه)

- فرض کنید α و θ دو ریشه f باشند. هدف ما محاسبه‌ی $\{\sigma(\alpha) : \sigma \in \langle G_\alpha, G_\theta \rangle\}$ است.
- $f(x) = (x-\alpha)g_2(x) \ldots g_r(x)$ و $f(x) = (x-\theta)h_2(x) \ldots h_r(x)$ تجزیه‌ی f به ترتیب روی $\mathbb{Q}(\alpha)$ و $\mathbb{Q}(\theta)$ هستند. هدف ما شناسایی عناصری به فرم $\tau_1\sigma_1 \ldots \tau_n\sigma_n(\alpha)$ است که σ_i ها در G_θ و τ_i ها در G_α هستند. α ریشه‌ی یکی از h_i ها مثلا h_2 است. لذا $\sigma_n(\alpha)$ تنها می‌تواند ریشه دیگری از h_2 باشد (چون σ_n هر h_i را به خودش می‌برد) و در واقع همه‌ی آن‌ها می‌تواند باشد. حال باید ببینیم ریشه‌های h_2 تحت عمل τ_i ها به کجاها می‌توانند بروند و ...
- بنابر حرف‌های بالا لازم است h_i ها و g_j هایی که ریشه مشترک دارند پیدا شوند که با تجزیه کردن f روی $\mathbb{Q}(\alpha, \beta)$ به سادگی بدست می‌آید. سپس از این اطلاعات یک گراف دو بخشی حاصل می‌شود و ریشه‌های مولفه همبندی شامل $x - \alpha$ در این گراف همان چیزی است که می‌خواستیم.



منابع

[1] Landau, Susan, and Gary Lee Miller. *Solvability by radicals is in polynomial time.* Journal of Computer and System Sciences 30.2 (1985)

[2] Morandi, Patrick. *Field and Galois theory*. Vol. 167. Springer Science & Business Media, 2012

[3] Lenstra, Arjen K., Hendrik Willem Lenstra, and László Lovász. *Factoring polynomials with rational coefficients.* Mathematische annalen 261. (1982)

[4] Cohen, Henri. *A course in computational algebraic number theory*. Vol. 138. Springer Science & Business Media, 2013