

## بعضی چند جمله‌ایهای تحویل‌ناپذیر بر روی $Q$

حسین صدیقی

عضو هیأت علمی دانشگاه تربیت معلم

### چکیده

هدف این مقاله یافتن دسته‌هایی از چند جمله‌ایهای عضو  $Q[x]$  است که روی  $Q$  تحویل‌ناپذیرند و در پایان شبکه‌ای از زیرگروههای یک چند جمله‌ای روی  $Q$  و شبکه‌ای از زیرمیدانهای میدان تجزیه‌ای آن چند جمله‌ای روی  $Q$  جهت مقایسه این دو شبکه رسم شده است.

چنانچه  $E/F$  یک میدان توسیعی و  $\alpha \in E$  روی  $F$  جبری باشد آنگاه تابع

$$\phi_\alpha : F[x] \rightarrow F(\alpha) \\ f(x) \mapsto f(\alpha)$$

یک هم‌ریختی است. با توجه به جبری بودن  $\alpha$  روی  $F$  هسته این هم‌ریختی یک ایده‌آل ناصفر  $F[x]$  است که به وسیله یک چند جمله‌ای تکین تحویل‌ناپذیر منحصر بفرد  $p(x) \in F[x]$  تولید می‌شود،  $p(x)$  را چند جمله‌ای مینیمال یا چند جمله‌ای تحویل‌ناپذیر  $\alpha$  روی  $F$  می‌نامند و  $[F(\alpha) : F] = \deg(p(x))$ .

اگر  $E/F$  توسیع میدان تجزیه‌ای چند جمله‌ای ناصفر  $f$  باشد آنگاه

$$\text{Gal}_F(f) = \{ \phi : E \rightarrow E \mid \phi \text{ یک خودریختی است که هر عضو } F \text{ را ثابت نگه می‌دارد} \}$$

اگر  $H \subseteq \text{Gal}_F(f)$  یک زیرمجموعه دلخواه باشد آنگاه

$$\phi(H) = \{ \alpha \in E \mid \forall \sigma \in H (\sigma(\alpha) = \alpha) \}$$

یک زیرمیدان  $E$  می‌باشد که شامل  $F$  است. به عکس اگر  $K$  زیرمیدانی از  $E$  و شامل  $F$  باشد آنگاه  $\{\sigma \in \text{Gal}_F(f) \mid \forall k \in K (\sigma(k) = k)\}$  زیرگروهی از  $\text{Gal}_F(f)$  است. چنانچه:

$$A = \{K \mid K \text{ زیرمیدانی از } E \text{ که شامل } F \text{ است}\},$$

$$B = \{H \mid H \text{ یک زیرگروه } \text{Gal}_F(f) \text{ است}\},$$

آنگاه تابع  $(1) \psi: B \rightarrow A$  با ضابطه  $\psi(H) = \phi(H)$  یک تناظر یک‌به‌یک است.

فرض کنید  $p, q$  دو عدد خالی از مربع باشند به قسمی که  $q \neq (p, q) \neq p$  و  $f = (x^2 - p)(x^2 - q)$  این صورت  $Q(\sqrt{p}, \sqrt{q})/Q$  یک توسیع میدان تجزیه‌ای  $f$  است.

$$Q(\sqrt{p}, \sqrt{q}) = \{a_0 + a_1\sqrt{p} + a_2\sqrt{q} + a_3\sqrt{pq} \mid a_i \in Q\}$$

$$|\text{Gal}_Q(f)| = [Q(\sqrt{p}, \sqrt{q}) : Q] = 4.$$

با فرض  $\text{Gal}_Q(f) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$  هر یک از  $\sigma_i$  ( $0 \leq i \leq 3$ ) یک خودریختی روی  $Q(\sqrt{p}, \sqrt{q})$  است که هر عضو  $Q$  را ثابت نگاه میدارند. برای مشخص کردن یک خودریختی روی  $Q(\sqrt{p}, \sqrt{q})$  کافی است  $\sigma(\sqrt{p})$  و  $\sigma(\sqrt{q})$  را معین نماییم. از آنجا که  $\sigma(\sqrt{p}) = \pm\sqrt{p}$  و  $\sigma(\sqrt{q}) = \pm\sqrt{q}$  نتیجه می‌شود که اعضای  $\text{Gal}_Q(f)$  به شرح زیر می‌باشند

$$\sigma_0: \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \end{cases}, \quad \sigma_1: \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \end{cases}, \quad \sigma_2: \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \end{cases}, \quad \sigma_3: \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \end{cases}$$

بنابراین  $\text{Gal}_Q(f)$  دارای زیرگروه‌های

$$H_0 = \{\sigma_0\}, \quad H_1 = \{\sigma_0, \sigma_1\}, \quad H_2 = \text{Gal}_Q(f), \quad H_3 = \{\sigma_0, \sigma_2\}, \quad H_4 = \{\sigma_0, \sigma_3\}.$$

در نتیجه زیرمیدانهای متناظر  $H_i$ ها بنابر رابطه (۱) که تمام زیرمیدانهای  $Q(\sqrt{p}, \sqrt{q})$  نیز می‌باشند به شرح زیر می‌باشند:

$$\phi(H_0) = Q(\sqrt{p}, \sqrt{q})$$

$$\phi(H_1) = Q(\sqrt{q}), \quad \phi(H_2) = Q(\sqrt{p}), \quad \phi(H_3) = Q(\sqrt{pq})$$

لم ۱: اگر  $a, b$  اعداد گویای ناصفر و  $p, q$  دو عدد خالی از مربع باشند به قسمی که  $q \neq (p, q) \neq p$  آنگاه  $\alpha = a\sqrt{p} + b\sqrt{q}$   $Q(\alpha) = Q(\sqrt{p}, \sqrt{q})$ .

برهان: چون  $\alpha$  به هیچیک از زیرمیدانهای  $Q(\sqrt{p})$ ،  $Q(\sqrt{q})$ ،  $Q(\sqrt{pq})$  و  $Q$  تعلق ندارد، و  $Q(\alpha)$  زیرمیدانی از  $Q(\sqrt{p}, \sqrt{q})$  است که با هیچیک از این چهار زیرمیدان برابر نیست پس  $Q(\alpha) = Q(\sqrt{p}, \sqrt{q})$ .  $\blacktriangle$

قضیه ۲: اگر  $p, q$  دو عدد صحیح و مثبت و خالی از مربع باشند به قسمی که  $\lambda p$  و  $\lambda q$  و  $a, b$  اعداد گویای ناصفر باشند آنگاه چندجمله‌ای  $f(x) = x^4 - 2(a^2p + b^2q)x^2 + (a^2p - b^2q)^2$  روی  $\mathbb{Q}$  تحویل‌ناپذیر است.

برهان: با فرض  $\alpha = a\sqrt{p} + b\sqrt{q}$  بنا بر لم یک داریم  $Q(\alpha) = Q(\sqrt{p}, \sqrt{q})$ . بنابراین  $[Q(\alpha) : Q] = [Q(\sqrt{p}, \sqrt{q}) : Q] = 4$ . در نتیجه چندجمله‌ای مینیمال  $\alpha$  روی  $\mathbb{Q}$  از درجه ۴ می‌باشد. لذا اگر  $g(x) \in Q[x]$  یک چندجمله‌ای ناصفر باشد به قسمی که

$$\deg(g(x)) \geq 2 \quad \text{آنگاه} \quad g(\alpha) = 0 \quad (2)$$

$$\alpha = a\sqrt{p} + b\sqrt{q}$$

$$\alpha^2 = a^2p + b^2q + 2ab\sqrt{pq}$$

$$\alpha^2 - (a^2p + b^2q) = 2ab\sqrt{pq}$$

$$\alpha^4 + (a^2p + b^2q)^2 - 2(a^2p + b^2q)\alpha^2 = 4a^2b^2pq$$

$$\alpha^4 - 2(a^2p + b^2q)\alpha^2 + (a^2p - b^2q)^2 = 0$$

بنابراین  $\alpha$  صفر  $f(x)$  می‌باشد. از این که چندجمله‌ای مینیمال  $\alpha$  در  $\mathbb{Q}$  از درجه ۴ می‌باشد نتیجه می‌شود که  $f(x)$  روی  $\mathbb{Q}$  تحویل‌ناپذیر است. چه در غیر این صورت  $\alpha$  صفر یک چندجمله‌ای از درجه کوچکتر از ۴ روی  $\mathbb{Q}$  می‌باشد که با (۲) تناقض دارد.  $\blacktriangle$

نتیجه یک: اگر  $p, q$  دو عدد خالی از مربع باشند به قسمی که  $\lambda p$  و  $\lambda q$  آنگاه چندجمله‌ای  $g(x) = x^2 - 2(p+q)x^2 + (p-q)^2$  روی  $\mathbb{Q}$  تحویل‌ناپذیر است.

برهان: با قراردادن  $a = b = 1$  در قضیه ۲ نتیجه حاصل می‌شود.  $\blacktriangle$

نتیجه ۲: اگر  $p, q$  دو عدد طبیعی خالی از مربع باشند به قسمی که  $\lambda p$  و  $\lambda q$  و  $a$  یک عدد گویای ناصفر باشد آنگاه چندجمله‌ای  $h(x) = x^2 - 2(p+q)a^2x^2 + a^2(p-q)^2$  روی  $\mathbb{Q}$  تحویل‌ناپذیر است.

برهان: با قراردادن  $a = b$  در قضیه ۲ نتیجه حاصل می‌شود.  $\blacktriangle$

قضیه ۳: اگر  $m$  عددی صحیح و مثبت و مربع کامل نباشد (یعنی عددی اول چون  $p$  وجود دارد که  $p^k | m$  و  $p^{k+1} \nmid m$  و  $k$  فرد است) آنگاه چندجمله‌ای  $t(x) = x^2 - 2(m-1)x^2 + (m+1)^2$  روی  $\mathbb{Q}$  تحویل‌ناپذیر است.



برهان:  $Q(i, \sqrt{m}) = Q(i + \sqrt{m})$  : لذا

$$[Q(i + \sqrt{m}) : Q] = [Q(i, \sqrt{m}) : Q] = ۴$$

بنابراین چندجمله‌ای مینیمال  $i + \sqrt{m}$  روی  $Q$  از درجه ۴ می‌باشد. در نتیجه اگر  $s(x) \in Q[x]$  یک چندجمله‌ای ناصفر باشد به قسمی که  $s(i + \sqrt{m}) = 0$  آنگاه  $\deg(s(x)) \geq ۴$  . با فرض

$$\alpha = i + \sqrt{m},$$

$$\alpha^2 = -۱ + m + ۲i\sqrt{m},$$

$$\alpha^3 + (۱ - m)\alpha^2 + ۲(۱ - m)\alpha = -۴m,$$

$$\alpha^3 + (۱ - m)\alpha^2 + ۲(۱ - m)\alpha = -۴m,$$

$$\alpha^3 + ۲(۱ - m)\alpha^2 + (m + ۱)\alpha = 0.$$

بنابراین  $\alpha$  صفر چندجمله‌ای  $t(x)$  می‌باشد. در نتیجه  $t(x)$  روی  $Q$  تحویل‌ناپذیر است چه در غیر این صورت  $\alpha$  صفر یک چندجمله‌ای از درجه حداکثر ۳ می‌باشد که غیرممکن است.  $\blacktriangle$

فرض کنید  $p, q$  و  $t$  سه عدد اول دوه‌دو متمایز باشند و  $f = (x^2 - p)(x^2 - q)(x^2 - t)$  در این صورت  $Q(\sqrt{p}, \sqrt{q}, \sqrt{t})/Q$  توسیع میدان تجزیه‌ای  $f$  روی  $Q$  است.

$$Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) = \{a + b_1\sqrt{p} + b_2\sqrt{q} + b_3\sqrt{t} + c_1\sqrt{pq} + c_2\sqrt{pt} + c_3\sqrt{qt} + d\sqrt{pqt} \mid a, b_i, c_i, d \in Q\},$$

$$\text{Gal}_Q(f) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}.$$

اگر  $\sigma \in \text{Gal}_Q(f)$  آنگاه برای هر  $q \in Q$  داریم  $\sigma(q) = q$  . لذا برای مشخص کردن یک خودریختی  $\sigma : Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) \rightarrow Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$  کافی است  $\sigma(\sqrt{p}), \sigma(\sqrt{q})$  و  $\sigma(\sqrt{t})$  را معین کنیم. از آنجا که  $\sigma(\sqrt{p}) = \pm\sqrt{p}$  و  $\sigma(\sqrt{q}) = \pm\sqrt{q}$  و  $\sigma(\sqrt{t}) = \pm\sqrt{t}$  نتیجه می‌شود که  $\sigma$  عضو  $\text{Gal}_Q(f)$  به شرح زیر است:

$$\sigma_0 : \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \\ \sqrt{t} \rightarrow \sqrt{t} \end{cases}, \sigma_1 : \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \\ \sqrt{t} \rightarrow \sqrt{t} \end{cases}, \sigma_2 : \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \\ \sqrt{t} \rightarrow \sqrt{t} \end{cases}, \sigma_3 : \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \\ \sqrt{t} \rightarrow -\sqrt{t} \end{cases}$$

$$\sigma_4 : \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \\ \sqrt{t} \rightarrow \sqrt{t} \end{cases}, \sigma_5 : \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow \sqrt{q} \\ \sqrt{t} \rightarrow -\sqrt{t} \end{cases}, \sigma_6 : \begin{cases} \sqrt{p} \rightarrow \sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \\ \sqrt{t} \rightarrow -\sqrt{t} \end{cases}, \sigma_7 : \begin{cases} \sqrt{p} \rightarrow -\sqrt{p} \\ \sqrt{q} \rightarrow -\sqrt{q} \\ \sqrt{t} \rightarrow -\sqrt{t} \end{cases}$$

$$[Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) : Q] = |\text{Gal}_Q(f)| = 8.$$

لذا  $\text{Gal}_Q(f)$  دارای ۱۶ زیرگروه به شرح زیر است:

$$\begin{aligned} H_0 &= \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_1\}, H_2 = \{\sigma_0, \sigma_2\}, H_3 = \{\sigma_0, \sigma_3\}, H_4 = \{\sigma_0, \sigma_4\} \\ H_5 &= \{\sigma_0, \sigma_5\}, H_6 = \{\sigma_0, \sigma_6\}, H_7 = \{\sigma_0, \sigma_7\}, H_8 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\} \\ H_9 &= \{\sigma_0, \sigma_1, \sigma_2, \sigma_5\}, H_{10} = \{\sigma_0, \sigma_1, \sigma_6, \sigma_7\}, H_{11} = \{\sigma_0, \sigma_2, \sigma_3, \sigma_6\}, \\ H_{12} &= \{\sigma_0, \sigma_2, \sigma_5, \sigma_7\}, H_{13} = \{\sigma_0, \sigma_3, \sigma_2, \sigma_7\}, H_{14} = \{\sigma_0, \sigma_3, \sigma_5, \sigma_6\}, \\ H_{15} &= \text{Gal}_Q(f). \end{aligned}$$

فرض کنید  $A = \{H_i \mid 0 \leq i \leq 15\}$  و  $B = \{K \mid Q \leq K \leq Q(\sqrt{p}, \sqrt{q}, \sqrt{t})\}$  و

$$\psi : A \rightarrow B.$$

$$H_i \rightsquigarrow \phi(H_i)$$

و  $a, b, c$  اعداد گویای ناصفری باشند و  $\alpha = a\sqrt{p} + b\sqrt{q} + c\sqrt{t}$  در این صورت  $Q(\alpha)$  زیرمیدانی از  $Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$  است و برای هر  $(1 \leq i \leq 15)$ ،  $\alpha \notin \phi(H_i)$ ، زیرا برای هر چنین  $i$  زیرگروه  $H_i$  عضوی دارد که  $\alpha$  را روی خودش تصویر نمی‌کند. بنابراین  $(1 \leq i \leq 15)$ ،  $Q(\alpha) \neq \phi(H_i)$  و در نتیجه  $Q(\alpha) = Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$ . لذا

$$[Q(\alpha) : Q] = [Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) : Q] = 8.$$

بنابراین چندجمله‌ای مینیمال  $\alpha$  روی  $Q$  از درجه ۸ می‌باشد. در نتیجه اگر  $g(x) \in Q[x]$  یک چندجمله‌ای ناصفر باشد به قسمی که  $g(\alpha) = 0$  آنگاه  $\deg(g(x)) \geq 8$ .

قضیه ۴: اگر  $p, q, t$  سه عدد اول دوه‌دو متمایز باشند آنگاه

$$\begin{aligned} f(x) &= x^8 - 4(p+q+t)x^6 + 2[(p+q+t)^2 + 2(p^2+q^2+t^2)]x^4 \\ &\quad - 4[(p+q+t)(p^2+q^2+t^2) - 2pq - 2pt - 2qt]x^2 \\ &\quad + (p^2+q^2+t^2 - 2pq - 2pt - 2qt)^2. \end{aligned}$$

روی  $Q$  تحویل‌ناپذیر است.

برهان: بنابر بحث‌های قبل از قضیه ۴ اگر  $\gamma = \sqrt{p} + \sqrt{q} + \sqrt{t}$  آنگاه  $Q(\gamma) = Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$ . بنابراین  $[Q(\gamma) : Q] = 8$  و در نتیجه چندجمله‌ای مینیمال  $\gamma$  روی  $Q$  از درجه ۸ می‌باشد. لذا اگر  $h(x) \in Q[x]$  یک چندجمله‌ای ناصفر باشد به قسمی که  $h(\gamma) = 0$  آنگاه  $\deg(h(x)) \geq 8$ .

$$\gamma = \sqrt{p} + \sqrt{q} + \sqrt{t},$$

$$\gamma - \sqrt{p} = \sqrt{q} + \sqrt{t},$$

$$\gamma^2 + p - 2\gamma\sqrt{p} = q + t + 2\sqrt{qt},$$

$$(\gamma^2 + p - q - t)^2 = 4(\gamma\sqrt{p} + \sqrt{qt})^2,$$

$$\gamma^4 + 2(p - q - t)\gamma^2 + (p - q - t)^2 = 4(\gamma^2 p + qt + 2\gamma\sqrt{pq}),$$

$$\gamma^4 - 2(p + q + t)\gamma^2 + (p^2 + q^2 + t^2 - 2pt - 2pq - 2qt) = 8\gamma\sqrt{pqt}.$$

$$\gamma^8 - 4(p + q + t)\gamma^6 + [2(p^2 + q^2 + t^2 - 2pq - 2pt - 2qt) + 4(p + q + t)^2]\gamma^4$$

$$- [4(p + q + t)(p^2 + q^2 + t^2 - 2pq - 2pt - 2qt) + 64pqt]\gamma^2$$

$$+ (p^2 + q^2 + t^2 - 2pq - 2pt - 2qt) = 0.$$

بنابراین  $\gamma$  صفر  $f(x)$  است. از این که چندجمله‌ای مینیمال  $\gamma$  روی  $Q$  از درجه ۸ می‌باشد نتیجه می‌شود که  $f(x)$  روی  $Q$  تحویل‌ناپذیر است. چه در غیراین صورت  $\gamma$  صفر یک چندجمله‌ای از درجه کوچکتر از ۸ می‌باشد که غیرممکن است. ▲

با فرض  $K_i = \phi(H_i)$ ,  $(0 \leq i \leq 15)$  خواهیم داشت

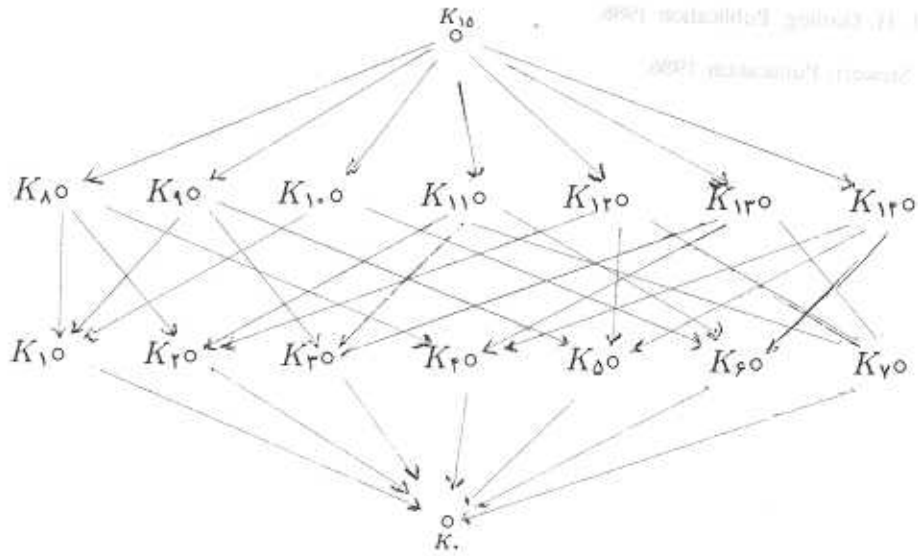
$$K_0 = Q(\sqrt{p}, \sqrt{q}, \sqrt{t}), K_1 = Q(\sqrt{q}, \sqrt{t}), K_2 = Q(\sqrt{p}, \sqrt{t}), K_3 = Q(\sqrt{p}, \sqrt{q})$$

$$K_4 = Q(\sqrt{t}, \sqrt{pq}), K_5 = Q(\sqrt{q}, \sqrt{pt}), K_6 = Q(\sqrt{p}, \sqrt{qt}), K_7 = Q(\sqrt{pq}, \sqrt{pt}, \sqrt{qt}),$$

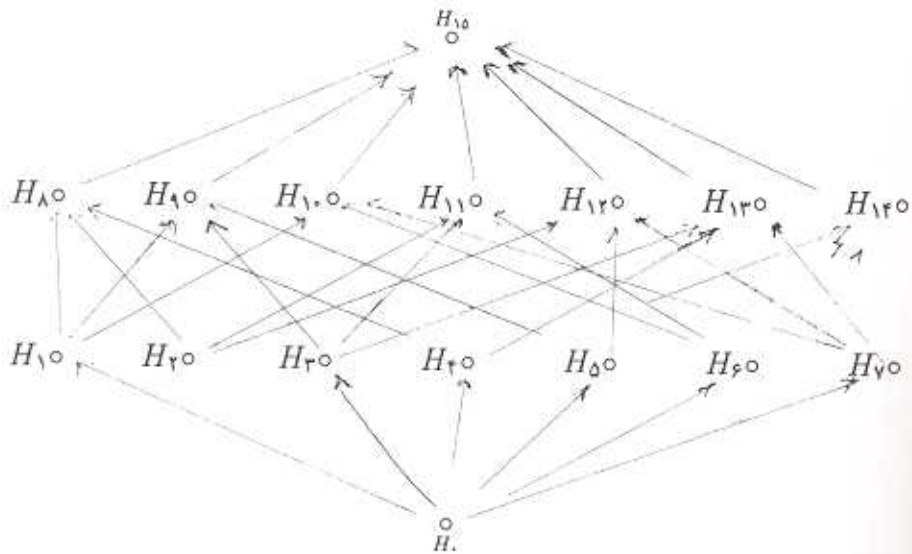
$$K_8 = Q(\sqrt{t}), K_9 = Q(\sqrt{q}), K_{10} = Q(\sqrt{qt}), K_{11} = Q(\sqrt{p}), K_{12} = Q(\sqrt{pt})$$

$$K_{13} = Q(\sqrt{pq}), K_{14} = Q(\sqrt{pqt}), K_{15} = Q.$$

در صفحه بعد شبکه زیرگروه‌های  $\text{Gal}_Q(f)$  و شبکه زیرمیدانهای  $Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$  را جهت مقایسه نشان می‌دهیم.



شبکه زیر میدانهای  $Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$



شبکه زیرگروههای  $Gal_Q(f)$



References:

- [1]. Galois Theory, Joseph Rotman, Publication 1990.
- [2]. Galois Theory, D. J. H. Garling, Publication 1986.
- [3]. Galois Theory, Ian Stewart, Publication 1986.