بعضی چندجمله‌ایهای تحویل‌ناپذیر بر روی Q

حسین صدیقی

عضو هیأت علمی دانشگاه تربیت معلم

چکیده

هدف این مقاله یافتن دسته‌هایی از چندجمله‌ایهای عضو $Q[x]$ است که روی Q تحویل‌ناپذیرند و در پایان شبکه‌ای از زیرگروههای یک چندجمله‌ای روی Q و شبکه‌ای از زیرمیدانهای میدان تجزیه‌ای آن چندجمله‌ای 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

$$\phi_\alpha \; : \; F[x] \longrightarrow F(\alpha)$$
$$f(x) \rightsquigarrow f(\alpha)$$

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

اگر E/F توسیع میدان تجزیه‌ای چندجمله‌ای ناصفر f باشد آنگاه

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

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

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

یک زیرمیدان E می‌باشد که شامل F است. به‌عکس اگر K زیرمیدانی از E و شامل F باشد آنگ $\{\sigma \in \mathrm{Gal}_F(f) | \forall k \in K(\sigma(k)=k)\}$ زیرگروهی از $\mathrm{Gal}_F(f)$ است. چنانچه:

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

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

آنگاه تابع (۱) $\psi : B \longrightarrow A$ با ضابطهٔ $\psi(H) = \phi(H)$ یک تناظر یک‌به‌یک است.

فرض کنید q, p دو عدد خالی از مربع باشند به قسمی که $p \neq (p,q) \neq q$ و $f = (x^۲ - p)(x^۲ - q)$. د این صورت $Q(\sqrt{p}, \sqrt{q})/Q$ یک توسیع میدان تجزیه‌ای f است.

$$Q(\sqrt{p}, \sqrt{q}) = \{a_۰ + a_۱\sqrt{p} + a_۲\sqrt{q} + a_۳\sqrt{pq} | a_i \in Q\}$$

$$|\mathrm{Gal}_Q(f)| = [Q(\sqrt{p}, \sqrt{q}) : Q] = ۴.$$

با فرض $\mathrm{Gal}_Q(f) = \{\sigma_۰, \sigma_۱, \sigma_۲, \sigma_۳\}$، هر یک از σ_i، $(۰ \leq i \leq ۳)$ یک خودریختی روی $Q(\sqrt{p}, \sqrt{q})$ است که هر عضو Q را ثابت نگهمیدارند. برای مشخص کردن یک خودریختی روی $Q(\sqrt{p}, \sqrt{q})$ کافی است $\sigma(\sqrt{p})$ و $\sigma(\sqrt{q})$ را معین نمائیم. از آنجا که $\sigma(\sqrt{p}) = \pm\sqrt{p}$ و $\sigma(\sqrt{q}) = \pm\sqrt{q}$، نتیجه می‌شود که اعضای $\mathrm{Gal}_Q(f)$ به شرح زیر می‌باشند

$$\sigma_۰ : \begin{cases} \sqrt{p} \longrightarrow \sqrt{p} \\ \sqrt{q} \longrightarrow \sqrt{q} \end{cases}, \quad \sigma_۱ : \begin{cases} \sqrt{p} \longrightarrow -\sqrt{p} \\ \sqrt{q} \longrightarrow \sqrt{q} \end{cases}, \quad \sigma_۲ : \begin{cases} \sqrt{p} \longrightarrow \sqrt{p} \\ \sqrt{q} \longrightarrow -\sqrt{q} \end{cases}, \quad \sigma_۳ : \begin{cases} \sqrt{p} \longrightarrow -\sqrt{p} \\ \sqrt{q} \longrightarrow -\sqrt{q} \end{cases}$$

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

$$H_۰ = \{\sigma_۰\}, \quad H_۱ = \{\sigma_۰, \sigma_۱\}, \quad H_۴ = \mathrm{Gal}_Q(f), \quad H_۳ = \{\sigma_۰, \sigma_۳\}, \quad H_۲ = \{\sigma_۰, \sigma_۲\}.$$

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

$$\phi(H_۰) = Q(\sqrt{p}, \sqrt{q})$$

$$\phi(H_۴) = Q, \quad \phi(H_۱) = Q(\sqrt{q}), \quad \phi(H_۲) = Q(\sqrt{p}, \quad \phi(H_۳) = Q(\sqrt{p}q)$$

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

برهان: چون α 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 $Q(\alpha)=Q(\sqrt{p},\sqrt{q})$.▲

قضیه ۲: اگر q,p دو عدد صحیح و مثبت و خالی از مربع باشند به قسمی که $p\nmid q$ و $q\nmid p$ و b,a اعداد گویای ناصفر باشند آنگاه چندجمله‌ای $f(x)=x^۴-۲(a^۲p+b^۲q)x^۲+(a^۲p-b^۲q)^۲$ روی Q تحویل‌ناپذیر است.

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

$$g(\alpha)=۰ \text{ آنگاه } \deg(g(x))\geq ۴ \qquad (۲)$$

$$\alpha=a\sqrt{p}+b\sqrt{q},$$
$$\alpha^۲=a^۲p+b^۲q+۲ab\sqrt{pq},$$
$$\alpha^۲-(a^۲p+b^۲q)=۲ab\sqrt{pq},$$
$$\alpha^۴+(a^۲p+b^۲q)^۲-۲(a^۲p+b^۲q)\alpha^۲=۴a^۲b^۲pq,$$
$$\alpha^۴-۲(a^۲p+b^۲q)\alpha^۲+(a^۲p-b^۲q)^۲=۰$$

بنابراین α صفر $f(x)$ می‌باشد. از این که چندجمله‌ای مینیمال α در Q از درجه ۴ می‌باشد نتیجه می‌شود که $f(x)$ روی Q تحویل‌ناپذیر است. چه در غیر این صورت α صفر یک چندجمله‌ای از درجهٔ کوچکتر از ۴ روی Q می‌باشد که با (۲) تناقض دارد.▲

نتیجه یک: اگر q,p دو عدد خالی از مربع باشند به قسمی که $p\nmid q$ و $q\nmid p$ آنگاه چندجمله‌ای $g(x)=x^۴-۲(p+q)x^۲+(p-q)^۲$ روی Q تحویل‌ناپذیر است.

برهان: با قراردادن $a=b=۱$ در قضیه ۲ نتیجه حاصل می‌شود.▲

نتیجه ۲: اگر q,p دو عدد طبیعی خالی از مربع باشند به قسمی که $p\nmid q$ و $q\nmid p$ و a یک عدد گویای ناصفر باشد آنگاه چندجمله‌ای $h(x)=x^۴-۲(p+q)a^۲x^۲+a^۴(p-q)^۲$ روی Q تحویل‌ناپذیر است.

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

قضیه ۳: اگر m عددی صحیح و مثبت و مربع کامل نباشد (یعنی عددی اول چون p وجود دارد که $p^k|m$ و $p^{k+۱}\nmid m$ و k فرد است) آنگاه چندجمله‌ای $t(x)=x^۴-۲(m-۱)x^۲+(m+۱)^۲$ روی 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 درجهٔ ۴ می‌باشد، در نتیجه اگر $s(x)\in Q[x]$ یک چندجمله‌ای ناصفر باشد به قسمی که $s(i+\sqrt{m}) = ۰$ آنگاه $\deg(s(x)) \geq ۴$. بافرض

$$\begin{aligned}
&\alpha = i+\sqrt{m},\\
&\alpha^{۲} = -۱+m+۲i\sqrt{m},\\
&\alpha^{۴}+(۱-m)^{۲}+۲(۱-m)\alpha^{۲} = -۴m,\\
&\alpha^{۴}+(۱-m)^{۲}+۲(۱-m)\alpha^{۲} = -۴m,\\
&\alpha^{۴}+۲(۱-m)\alpha^{۲}+(m+۱)^{۲} = ۰
\end{aligned}$$

بنابراین α صفر چندجمله‌ای $t(x)$ می‌باشد. در نتیجه $t(x)$ روی Q تحویل‌ناپذیر است چه در غیر این صورت α صفر یک چندجمله‌ای از درجهٔ حداکثر ۳ می‌باشد که غیرممکن است.▲

فرض کنید p، q و t سه عدد اول دوبه‌دو متمایز باشند و $f=(x^{۲}-p)(x^{۲}-q)(x^{۲}-t)$. در این صورت $Q(\sqrt{p},\sqrt{q},\sqrt{t})/Q$ توسیع میدان تجزیه‌ای f روی Q است.

$$Q(\sqrt{p},\sqrt{q},\sqrt{t} = \left\{a+b_{۱}\sqrt{p}+b_{۲}\sqrt{q}+b_{۳}\sqrt{t}+c_{۱}\sqrt{pq}+c_{۲}\sqrt{pt}+c_{۳}\sqrt{qt}+d\sqrt{pqt} \mid a,b_i,c_i,d\in Q\right\},$$

$$\mathrm{Gal}_Q(f) = \{\sigma_۰,\sigma_۱,\sigma_۲,\sigma_۳,\sigma_۴,\sigma_۵,\sigma_۶,\sigma_۷\}.$$

اگر $\sigma\in \mathrm{Gal}_Q(f)$ آنگاه برای هر $q\in Q$ داریم $\sigma(q)=q$. لذا برای مشخص کردن یک خودریختی $\sigma: Q(\sqrt{p},\sqrt{q},\sqrt{t}) \longrightarrow Q(\sqrt{p},\sqrt{q},\sqrt{t})$ 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 ۸ عضو $\mathrm{Gal}_Q(f)$ به شرح زیر است:

$$\sigma_۰:\begin{cases}\sqrt{p}\longrightarrow\sqrt{p}\\ \sqrt{q}\longrightarrow\sqrt{q}\\ \sqrt{t}\longrightarrow\sqrt{t}\end{cases},\quad
\sigma_۱:\begin{cases}\sqrt{p}\longrightarrow-\sqrt{p}\\ \sqrt{q}\longrightarrow\sqrt{q}\\ \sqrt{t}\longrightarrow\sqrt{t}\end{cases},\quad
\sigma_۲:\begin{cases}\sqrt{p}\longrightarrow\sqrt{p}\\ \sqrt{q}\longrightarrow-\sqrt{q}\\ \sqrt{t}\longrightarrow\sqrt{t}\end{cases},\quad
\sigma_۳:\begin{cases}\sqrt{p}\longrightarrow\sqrt{p}\\ \sqrt{q}\longrightarrow\sqrt{q}\\ \sqrt{t}\longrightarrow-\sqrt{t}\end{cases}$$

$$\sigma_۴:\begin{cases}\sqrt{p}\longrightarrow-\sqrt{p}\\ \sqrt{q}\longrightarrow-\sqrt{q}\\ \sqrt{t}\longrightarrow\sqrt{t}\end{cases},\quad
\sigma_۵:\begin{cases}\sqrt{p}\longrightarrow-\sqrt{p}\\ \sqrt{q}\longrightarrow\sqrt{q}\\ \sqrt{t}\longrightarrow-\sqrt{t}\end{cases},\quad
\sigma_۶:\begin{cases}\sqrt{p}\longrightarrow\sqrt{p}\\ \sqrt{q}\longrightarrow-\sqrt{q}\\ \sqrt{t}\longrightarrow-\sqrt{t}\end{cases},\quad
\sigma_۷:\begin{cases}\sqrt{p}\longrightarrow-\sqrt{p}\\ \sqrt{q}\longrightarrow-\sqrt{q}\\ \sqrt{t}\longrightarrow-\sqrt{t}\end{cases}$$

$$[Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) : Q] = |\mathrm{Gal}_Q(f)| = ۸.$$

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

$$H_۰ = \{\sigma_۰\},\ H_۱ = \{\sigma_۰, \sigma_۱\},\ H_۲ = \{\sigma_۰, \sigma_۲\},\ H_۳ = \{\sigma_۰, \sigma_۳\},\ H_۴ = \{\sigma_۰, \sigma_۴\}$$
$$H_۵ = \{\sigma_۰, \sigma_۵\},\ H_۶ = \{\sigma_۰, \sigma_۶\},\ H_۷ = \{\sigma_۰, \sigma_۷\},\ H_۸ = \{\sigma_۰, \sigma_۱, \sigma_۲, \sigma_۴\}$$
$$H_۹ = \{\sigma_۰, \sigma_۱, \sigma_۳, \sigma_۵\},\ H_{۱۰} = \{\sigma_۰, \sigma_۱, \sigma_۶, \sigma_۷\},\ H_{۱۱} = \{\sigma_۰, \sigma_۲, \sigma_۳, \sigma_۶\},$$
$$H_{۱۲} = \{\sigma_۰, \sigma_۲, \sigma_۵, \sigma_۷\},\ H_{۱۳} = \{\sigma_۰, \sigma_۳, \sigma_۴, \sigma_۷\},\ H_{۱۴} = \{\sigma_۰, \sigma_۴, \sigma_۵, \sigma_۶\},$$
$$H_{۱۵} = \mathrm{Gal}_Q(f).$$

فرض کنید $A = \{H_i | ۰ \leq i \leq ۱۵\}$ و $B = \{K | Q \leq K \leq Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$ و

$$\psi : A \longrightarrow B.$$
$$H_i \rightsquigarrow \phi(H_i)$$

و c, b, a 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 $(۱ \leq i \leq ۱۵)$، $\alpha \notin \phi(H_i)$، زیرا برای هر چنین i زیرگروه H_i عضوی دارد که α را روی خودش تصویر نمی‌کند. بنابراین $(۱ \leq i \leq ۱۵)$، $Q(\alpha) \neq \phi(H_i)$ و در نتیجه $Q(\alpha) = Q(\sqrt{p}, \sqrt{q}, \sqrt{t})$. لذا

$$[Q(\alpha) : Q] = [Q(\sqrt{p}, \sqrt{q}, \sqrt{t}) : Q] = ۸.$$

بنابراین چندجمله‌ای مینیمال α روی Q از درجه ۸ می‌باشد، در نتیجه اگر $g(x) \in Q[x]$. یک چند جمله‌ای ناصفر باشد به قسمی که $g(\alpha) = ۰$ آنگاه $\deg(g(x)) \geq ۸$.

قضیه ۴: اگر p، q و t سه‌عدد اول دوبه‌دو متمایز باشند آنگاه

$$\begin{aligned} f(x) = x^۸ &- ۴(p+q+t)x^۶ + ۲[(p+q+t)^۲ + ۲(p^۲+q^۲+t^۲)]x^۴ \\ &- ۴[(p+q+t)(p^۲+q^۲+t^۲ - ۲pq - ۲pt - ۲qt) + ۱۶pqt]x^۲ \\ &+ (p^۲+q^۲+t^۲ - ۲pq - ۲pt - ۲qt)^۲, \end{aligned}$$

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 $[Q(\gamma) : Q] = ۸$ و در نتیجه چندجمله‌ای مینیمال γ روی Q از درجه ۸ می‌باشد. لذا اگر $h(x) \in Q[x]$ یک چندجمله‌ای ناصفر باشد به قسمی که $h(\gamma) = ۰$ آنگاه $\deg(h(x)) \geq ۸$.

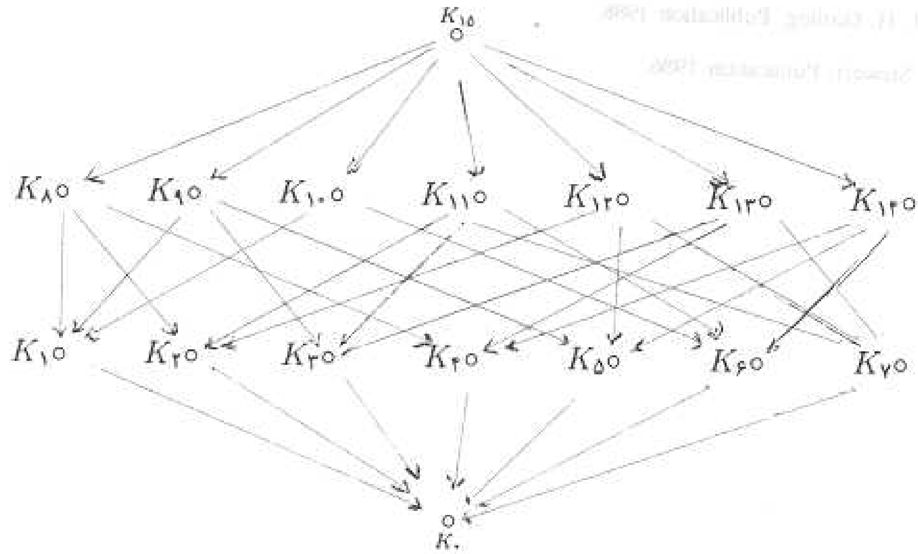
$$\begin{aligned}
&\gamma = \sqrt{p}+\sqrt{q}+\sqrt{t},\\
&\gamma - \sqrt{p} = \sqrt{q}+\sqrt{t},\\
&\gamma^۲ + p - ۲\gamma\sqrt{p} = q + t + ۲\sqrt{qt},\\
&(\gamma^۲ + p - q - t)^۲ = ۲(\gamma\sqrt{p} + \sqrt{qt}),\\
&\gamma^۴ + ۲(p-q-t)\gamma^۲ + (p-q-t)^۲ = ۴(\gamma^۲ p + qt + ۲\gamma\sqrt{pq}),\\
&\gamma^۴ - ۲(p+q+t)\gamma^۲ + (p^۲+q^۲+t^۲ - ۲pt - ۲pq - ۲qt) = ۸\gamma\sqrt{pqt}.\\
&\gamma^۸ - ۴(p+q+t)\gamma^۶ + [۲(p^۲+q^۲+t^۲-۲pq-۲pt-۲qt) + ۴(p+q+t)^۲]\gamma^۴\\
&\quad - [۴(p+q+t)(p^۲+q^۲+t^۲-۲pq-۲pt-۲qt) + ۶۴pqt]\gamma^۲\\
&\quad + (p^۲+q^۲+t^۲-۲pq-۲pt-۲qt) = ۰.
\end{aligned}$$

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

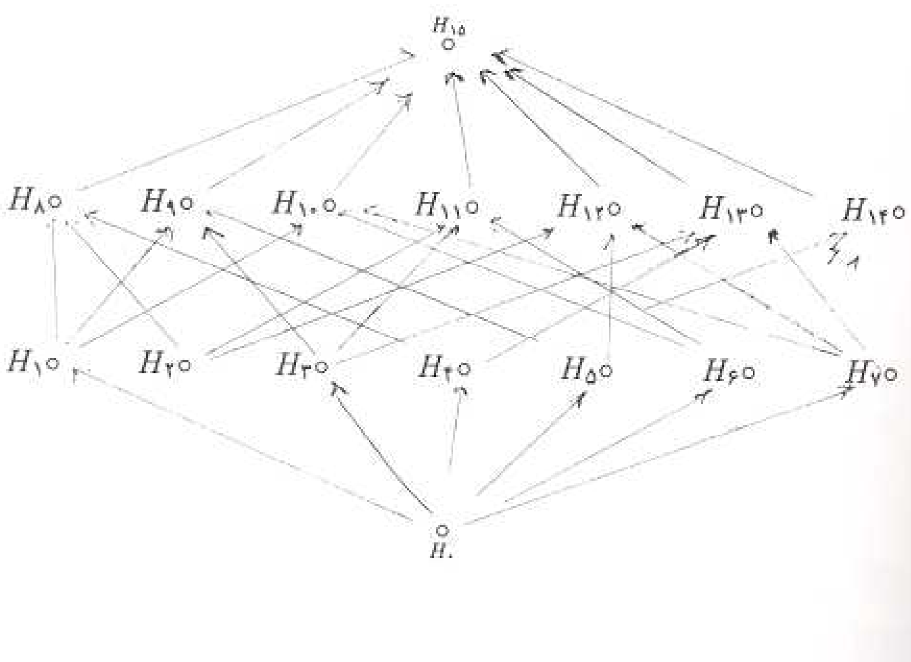
با فرض $K_i = \phi(H_i)$، $(۰ \leq i \leq ۱۵)$ خواهیم داشت

$$\begin{aligned}
&K_۰ = Q(\sqrt{p}, \sqrt{q}, \sqrt{t}),\ K_۱ = Q(\sqrt{q}, \sqrt{t}),\ K_۲ = Q(\sqrt{p}, \sqrt{t}),\ K_۳ = Q(\sqrt{p}, \sqrt{q})\\
&K_۴ = Q(\sqrt{t}, \sqrt{pq}),\ K_۵ = Q(\sqrt{q}, \sqrt{pt}),\ K_۶ = Q(\sqrt{p}, \sqrt{qt}),\ K_۷ = Q(\sqrt{pq}, \sqrt{pt}, \sqrt{qt}),\\
&K_۸ = Q(\sqrt{t}),\ K_۹ = Q(\sqrt{q}),\ K_{۱۰} = Q(\sqrt{qt}),\ K_{۱۱} = Q(\sqrt{p}),\ K_{۱۲} = Q(\sqrt{pt})\\
&K_{۱۳} = Q(\sqrt{pq}),\ K_{۱۴} = Q(\sqrt{pqt}), K_{۱۵} = Q.
\end{aligned}$$

در صفحه بعد شبکه زیرگروههای $\mathrm{Gal}_Q(f)$ 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 زیر گروههای $\mathrm{Gal}_Q(f)$

References:

[1]. Galois Theory, Joseph Rotman, Publication 1990.

[2]. Galois Theory, D. J. H. Garling, Publication 1986.

[3]. Galois Theory, Ian Stewert, Publication 1986.