فهرست مطالب

فصل اول

عمل گروه‌ها روی مجموعه‌ها و کاربردهای آن

در این فصل عمل گروه روی مجموعه را تعریف می‌کنیم و سپس به اثبات قضایای سیلو می‌پردازیم و نشان می‌دهیم که اگر $m = p^a$ عددی اول است آنگاه عکس قضیه لاگرانژ برقرار است سپس مباحثی را به ساده نبودن گروه‌ها اختصاص می‌دهیم.

1. 1 عمل گروه روی مجموعه

تعریف1.1.1. فرض کنید Gیک گروه و $X \neq f$ یک مجموعه باشد در این صورت گوئیم G روی X عمل می‌کند هرگاه تابع $G: X \times G \to X$ وجود داشته باشد (به جای $(x,y)s$) می‌نویسیم xy به قسمی که:

1- $\forall x \in X; xe = x$

2- $\forall g_1, g_2 \in G, x \in X; x(g_1 g_2) = (xg_1)g_2$

و s را عمل G بر X نامیم.

مثال 1. 1. 2. قرار دهید $G = ¢$ و $X = ¥$ تابع $s : ¥ \times ¢ \to ¥$ $(n\ ,\ m) \to n$ پس داریم:

1- $(n,0)s = n0 = n+0 = n$

2- $((n,m_1)s\ ,m_2)s = (n,m_2)s = n$ و $(n,m_1+m_2)s = n(m_1+m_2) = n$

مثال1. 1. 3. گروه G را در نظر می‌گیریم قرار دهید X=G تابع $X \times G \to X$ $(x,g) \to g^{-1}xg$ داریم:

1- $xe=e^{-1}xe=x$

2- $x(g_1g_2)=(g_1g_2)^{-1}x(g_1g_2)=g_2^{-1}g_1^{-1}xg_1g_2= g_2^{-1}(g_1^{-1}xg_1)g_2=(xg_1)g_2$

به طور مشابه فرض کنید G یک گروه و $N \leq G$ در این صورت نشان دهید که N با عمل زیر یک G مجموعه است.

$$N \times G \to N$$
$$(n,x) \to n^{-1}xn$$

مثال. فرض کنید G یک گروه و $H \leq G$ در این صورت H روی G با عمل زیر را در نظر می‌گیریم.

$$G\times H \to G$$
$$(g,h)\to gh$$

مثال1. 1. 4. گروه S_n را در نظر بگیرید قرار دهید $X=\{1,2,...,n\}$ و

$$s:\quad X\times S_n \to X$$
$$(x,t)\to (x)t$$

در این صورت

1- $(x,e)t=(x)e=x$

2- $(x)t_1t_2=((x)t_1)t_2$

پس S_n روی X عمل می‌کند.

فرض کنید G روی X عمل کند رابطه سه را در بین عناصر X به صورت زیر تعریف می‌کنیم:

$$x_1 \sim x_2 \Leftrightarrow \exists g\in G; x_1g=x_2.$$

در این صورت داریم:

1- $x_1 \sim x_1$ زیرا به ازای $e\in G$ داریم $x_1e=x_1$

2- اگر $x_1 \sim x_2$ آنگاه $\exists g\in G; x_1g=x_2$ پس $(x_1g)g^{-1}=x_1(gg^{-1})=x_1e=x_1$

3- اگر $x_2 \sim x_3$ و $x_1 \sim x_2$ پس

$$\exists g_1,g_2\in G\ s.t.\quad x_2=x_1g_1, x_3=x_2g_2$$

بنابراین $x_3=(x_1g_1)g_2=(x_1)g_1g_2$ در نتیجه رابطه سه یک رابطه هم ارزی است.

به ازای $x\in X$، رده هم ارزی x (یعنی $[x]$) را یک مدار x نامیم و با نماد $\bar{x}$ نشان می‌دهیم. بنابراین $x\in\bar{x}$ و به ازای هر $x,y\in X$ یا $\bar{x}=\bar{y}$ و همچنین $\bar{x}\cap\bar{y}=f$ داریم: $X=\bigcup_{x\in X}\bar{x}$

$$\bar{x}=\{a\in X \mid \exists g\in G\ s.t.\ a=xg\}=xG.$$

مثال1. 1. 5. عمل S_3 روی $\{1,2,3\}$ را در نظر بگیرید مطلوب است محاسبه $\bar{1},\bar{2},\bar{3}$

می‌دانیم $S_3=\{e,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$. پس

$$\bar{1}=1S_3=\{(1)e,(1)(1,2),(1)(1,3),(1)(2,3),(1)(1,2,3),(1)(1,3,2)\}=\{1,2,3\}.$$

و به طور مشابه $\bar{2}=\bar{3}=\{1,2,3\}$ یعنی عمل S_3 روی $X=\{1,2,3\}$ فقط یک مدار دارد.

عمل G روی X را متعدی نامیم هرگاه $\forall x,y\in X,\exists g\in G\ s.t\quad x=yg$

به طور معادل به ازای هر $x \in x$، $\bar{x} = X$ یعنی عمل فقط یک مدار داشته باشد. مثلاً عمل S_n روی $X = \{1,2,...,n\}$ با تابع $s : X \times S_n \to X$ متعدی است زیرا به ازای هر $k_1, k_2 \in S_n$ قرار می‌دهیم $r = (k_1, k_2)$ واضح است که $(k_1)r = k_2$ بنابراین عمل S_n روی X متعدی است.

مثال1. 1. 6. فرض کنید $(G : H) = n, H \le G$ قرار می‌دهیم $R = \{Ha | a \in G\}$ و

$$s : \begin{array}{l} R \times G \to R \\ (Ha, g) \to Hag \end{array}$$

چون s =Ha (Ha,e) و $(Ha)(g_1g_2)=(Hag_1)g_2$ پس G روی R عمل می‌کند. حال به ازای هر دو $Ha, Hb \in R$ داریم $(Ha)(a^{-1}b)=(Haa^{-1})b=Hb$. یعنی عمل فوق متعدی است.

فرض کنید G روی X عمل کند و $x_0 \in X$ قرار می‌دهیم $G_{x_0} = \{g \in G | x_0 g = x_0\}$. می‌توان نشان داد که $G_{x_0} \le G$ که آن را پایدار ساز x_0 نامیم. در مثال 1. 1. 5 به ازای $x_0 = 2$ داریم $G_2 = \{e, (1,3)\}$.

قضیه1.1 7. فرض کنید G یک گروه متناهی که روی X عمل می‌کند و $a \in X$ در این صورت

$$|\bar{a}| = (G : G_a).$$

برهان قرار می‌دهیم $L = \{gG_a | g \in G\}$ حال ضابطه $f : \begin{array}{l} \bar{a} \to L \\ ag \to gG_a \end{array}$ را در نظر می‌گیریم. داریم

1- $ag_1=ag_2$ بنابراین $ag_1g_2^{-1}=a$ یعنی $g_1g_2^{-1} \in G_a$ در نتیجه $g_1G_a=g_2G_a$ پس f خوش تعریف است.

2- فرض کنید $G_ag_1=G_ag_2$ پس $g_1g_2^{-1} \in G_a$ یعنی $ag_1g_2^{-1} = a$ بنابراین $ag_1=ag_2$ یعنی f یکبک است.

پوشا بودن f واضح است بنابراین $L \sim \bar{a}$. پس $|L| = |\bar{a}| = (G : G_a)$ و حکم ثابت می‌شود.

نتیجه1. 1. 8 . فرض کنید G گروه متناهی که روی مجموعه متناهی X عمل کند و $a \in X$ در این صورت $|\bar{a}| \,||G|$ به خصوص اگر عمل G روی X متعدی باشد آنگاه $|G| \,||X|$.

برهان. بنا به قضیه لاگرانژ و قضیه 1. 1. 7 داریم $|\bar{a}| = (G : G_a) \,||G|$ حال اگر عمل متعدی باشد $\bar{a} = X$.

2.1. p – گروه‌ها

در این بخش به مطالعه p - گروه‌ها می‌پردازیم و قضایای سیلو را ثابت می‌کنیم.

تعریف1.2.1. فرض کنید p عددی اول باشد. گروه G را یک p - گروه نامیم هرگاه مرتبه هر عضو G توانی از p باشد.

مثال1. 2. 2.

1- گروه کلاین $k_4=\{e,a,b,c\}$ یک 2- گروه است زیرا $a^2=b^2=c^2=e$

2- گروه‌های $G=Z_3\oplus Z_9$ یک 3- گروه است زیرا $|G|=27$ و حکم از قضیه لاگرانژ به دست می‌آید.

3- اگر $|G|=P^n$ که p عددی اول است آنگاه G یک p - گروه است.

4- گروه تقارن‌های یک n- ضعلی منظم را با D_{2n} نشان می‌دهیم و داریم $|D_{2n}|=2n$ حال اگر n=4 آنگاه $|D_8|=8$ پس گروه تقارن‌های یک 4- ضعلی منظم یک 2- گروه است.

فرض کنید G روی مجموعه X عمل کند. قرار می‌دهیم $X_G=\{x\in X\,|\,xg=x,\forall g\in G\}$ و آن را پایدارنده تحت G نامیم.

لم3.2.1. فرض کنید H یک p - گروه متناهی باشد $(|H|=p^n)$ که روی X عمل می‌کند در اینصورت

$$|X|\equiv|X_H|(mod\ p).$$

برهان. فرض کنید $\overline{x_r},...,\overline{x_2},\overline{x_1}$ کلیه مدارهای مجزای H روی X باشند پس $X=\bigcup_{i=1}^{r}\overline{X_i}$ فرض کنید $\overline{x}_k$ تک عضوی باشد یعنی:

$$\overline{x}_k=\{x_kg\,|\,g\in G,\forall g\in G\}=\{x_k\}\Rightarrow x_kg=x_k,\forall g\in G$$

$$\Rightarrow x_k\in X_H.$$

به طور مشابه اگر $x_k\in X_H$ آنگاه $\overline{x}_k$ تک عضوی است. فرض کنید $\overline{x}_t,...,\overline{x}_1$ تک عضوی باشند پس $|X_H|=t$ و داریم $1\neq(H:H_{x_i})\,||H|$ و $|X|=t+\sum_{i=t+1}^{r}|\overline{x_i}|=t+\sum_{i=t+1}^{r}(H:H_{x_i})$. چون H یک $p-$ گروه است و $p|(H:H_{x_i})$ پس $|X|\equiv|X_H|(mod\ p)$. بنابراین $|X|\equiv|X_H|(mod\ p)$.

حال در شرایطی قرار داریم که قضیه معروف کوشی را ثابت کنیم. در واقع قضیه کوشی نشان می‌دهد که عکس قضیه لاگرانژ به ازای $m=p$ برقرار است.

قضیه 1. 2. 4 (کوشی). فرض کنید G یک گروه متناهی با مرتبه n باشد و $p|n=|G|$ در این صورت G دارای عضوی از مرتبه p است.

برهان. قرار می‌دهیم $X=\{(g_1,g_2,...,g_p)|g_1g_2...g_p=e,g_i\in G\}$ پس $|X|=n^{P-1}$, $p||X|$. حال عمل Z_p روی X را به صورت زیر در نظر می‌گیریم:

$$(g_1,g_2,\ldots,g_p)k=(g_{k+1},\ldots,g_p,g_1,\ldots g_k).$$

فرض کنید $ab=e$ بنابراین $ba=e$ چون $g_1\ldots g_kg_{k+1}\ldots g_p=e$ پس $g_{k+1}\ldots g_pg_1g_2\ldots g_k=e$ یعنی $(g_{k+1},...g_p,g_1,...,g_k)\in X$. همچنین می‌توان نشان داد که در شرایط عمل صدق می‌کند. چون گروه $\mathbb{Z}_p$ یک p - گروه متناهی است، بنا به قضیه قبل داریم $|X|\equiv|X_{Z_p}|(mad\ p)$ چون $(e,...,e)\in X_{Z_p}$ پس $|X_{Z_p}|\geq 1$ از طرفی $p||X|$ پس $|X_{Z_p}|\geq 2$. فرض کنید $(e,...,e)\neq(g_1,g_2,...,g_p)\in X_{Z_p}$. بنابراین

$$(g_1,g_2\ldots,g_p)1=(g_2,\ldots,g_p,g_1)=(g_1,g_2,\ldots,g_p)$$

پس $g_1=g_2=g_3=\ldots=g_p$. چون $(g_1,g_2,...,g_p)\in X$ پس $g_1^p=e$ و حکم ثابت می‌شود.

نتیجه1. 2. 5. فرض کنید G یک گروه متناهی با مرتبه n و $p||G|$ که در این صورت G دارای زیر گروهی از مرتبه p می‌باشد.

برهان. با توجه به اثبات قضیه کوشی، قرار می‌دهیم $H=<g_1>$ و حکم ثابت می‌شود.

نتیجه6.2.1. فرض کنید G یک p - گروه متناهی باشد در این صورت

$$\exists n\in \mathbb{N}\ s.t|G|=p^n.$$

برهان. چون $p||G|$ فرض کنید $q\neq p$ عدد اولی باشد که $q||G|$ بنا به قضیه کوشی G دارای عضوی از مرتبه q می‌باشد که تناقض است.

قضیه1. 2. 7. فرض کنید G یک گروه متناهی و H یک $p-$ زیر گروه G باشد. در این صورت

$$(G:H)\equiv(N(H):H)(\text{mod } p).$$

برهان. قرار می‌دهیم $R=\{Hx|x\in G\}$ در این صورت H روی R با تابع زیر عمل می‌کند. (نشان دهید.)

$$s:\ R\times H\to R$$
$$(Hx,h)\to Hxh$$

بنا لم 1. 2. 3، $(G:H)=|R|\equiv|R_H|(mod\ p)$. چون $He\in R_H$ پس $R_H\neq f$. فرض کنید $Hx\in R_H$ به ازای هر $h\in H$ داریم:

$$Hxh=Hx\Rightarrow xhx^{-1}\in H\Rightarrow xHx^{-1}\subseteq H\Rightarrow xH=Hx$$

$$\Rightarrow x\in N(H)$$

بنابراین $R_H=\{Hx|x\in N(H)\}\Rightarrow|R_H|=(N(H):H)$ و حکم ثابت می‌شود.

نتیجه1. 2. 8. اگر G یک p - گروه متناهی باشد و $H \lneq G$ آنگاه $H < N(H)$.

برهان. چون G یک p - گروه است و $H \lneq G$ پس $p \mid (G:H)$. حال از قضیه 2. 2. 7 داریم $p \mid (N(H):H)$ و حکم ثابت می‌شود.

1. 3 قضایای سیلو

در این بخش به اثبات قضایای سیلو می‌پردازیم که نتایج مهمی را در نظریه گروه‌ها در بردارند. از مهم ترین این نتایج، درستی عکس قضیه لاگرانژ برای $m=p^n$ و استفاده از آنها در ساده نبودن گروه‌ها می‌باشد.

قضیه1. 3. 1. (قضیه اول سیلو). فرض کنید $|G| = p^n m$ که در آن $(P,m) = 1, n \geq 1$ در این صورت:

1- به ازای هر $0 \leq i \leq n$ گروه G دارای زیرگروهی مانند H_i است که $|H_i| = p^i$

2- به ازای هر $0 \leq i \leq n-1$ هر گروه G_i با p^i عضو در یک زیر گروه G با p^{i+1} عضو نرمال است.

برهان 1. به استقرا روی n حکم را ثابت می‌کنیم. اگر 1 یا i=0 حکم برقرار است. فرض کنیم به ازای هر i<n گروه G زیر گروهی با p^i عضو دارد حکم را برای i+1 ثابت می‌کنیم. فرض کنید $|H| = p^i, H < G$ در این صورت $P \mid (G:H)$ و بنا به قضیه 1. 7. 2 $p \mid (N(H):H)$ در نتیجه $\frac{N(H)}{H}$ دارای زیر گروهی مانند K/H است که $|K/H| = p$ بنابراین $|K| = p^{i+1}, K \leq N(H) \leq G$ این مطلب حکم را ثابت می‌کند.

2- با توجه به اینکه $K \leq N(H), H \leq N(H)$ پس $H \leq K$ حکم ثابت می شود.

با شرایط قضیه اول سیلو برای گروه G زنجیری صعودی از p - زیر گروه‌های G به صورت زیر می‌توانیم به دست آوریم. $P_0 \leq P_1 \leq \ldots \leq P_n$ که $|P_i| = p^i$.

تعریف1. 3. 2. فرض کنید G یک گروه باشد در این صورت زیر گروه H را یک p - زیر گروه سیلوی G نامیم هرگاه:

1- H یک p - زیر گروه باشد.

2- اگر K هر p - زیر گروه دیگری باشد که $H \leq K \leq G$ آنگاه K=H

به عبارت دیگر p - زیر گروه ماکزیمال G (نسبت به شمول) را یک p - زیر گروه سیلوی G نامیم.

مثال1. 3. 3.

i - $S_3 = \{4, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ را در نظر بگیرید پس $|S_3| = 2 \times 3$ گروه S_3 دارای یک

3- زیـــر گـــروه ســـیلوی $H=\{e,(1,2,3),(1,3,2)\}$ و ســـه تـــا 2- زیـــر گـــروه ســـیلوی $H_1=\{4,(1,2)\}, H_2=\{4,(1,3)\}, H_3=\{4,(2,3)\}$ است.

ii - اگر $G=Z_3\oplus Z_9$ آنگاه قرار می‌دهیم:

$$H_0=\{0\}, H_1=Z_3\oplus\{0\}, H_2=Z_3\oplus Z_3, H_3=Z_3\oplus Z_9=G.$$

پس یک زنجیر از 3- زیر گروه‌های G به صورت $H_0\leq H_1\leq H_2\leq H_3$ می‌باشد. 3- زیر گروه سیلوی G کدام است؟

iii - اگر $|G|=P^n$ که $n\geq 2$ آنگاه G ساده نیست. زیرا G دارای زنجیری مانند $P_0\leq P_1\leq ...P_{n-1}\leq P_n=G$ که $|P_i|=p^i$ پس $P_{n-1}\leq G$ و G ساده نیست.

با استفاده از قضیه لاگرانژ و قضیه اول سیلو می‌توان نشان داد که اگر G یک گروه باشد که $|G|=p^nm$ که $(p,m)=1$ در این صورت $H\leq G$ یک p - زیر گروه سیلوی G است اگر و فقط اگر $|H|=p^n$.

1. 3. 4 نکته. اگر G یک گروه نامتناهی و p عددی اول باشد آنگاه با استفاده از لم زورن می‌توان نشان داد که p - زیر گروه سیلو G موجود است. البته در مواقعی ممکن است زیر گروه بدیهی $\{e\}$ باشد.

قضیه1. 3. 5 (قضیه دوم سیلو). فرض کنید $|G|=p^nm$ که $(p,m)=1$ در این صورت:

1- هر دو p - زیر گروه سیلوی G مزدوجند.

2- p - زیر گروه سیلوی G نرمال است اگر و فقط اگر G فقط یک $p-$ زیر گروه سیلو داشته باشد. (یعنی منحصر به فرد باشد).

برهان. فرض کنید P_1 و P_2 دو $p-$ زیر گروه سیلوی G باشند. قرار می‌دهیم $R=\{P_1x|x\in G\}$. بنابراین $|R|=(G:P_1)=m$. حال P_2 روی R با تابع زیر عمل می‌کند:

$$s:\ R\times P_2\to R$$
$$(P_1x,g)\to P_1xg$$

چون $|R|=(G:P_1)$، با استفاده از لم 2. 2. 3 داریم:

$$(G:P_1)\equiv |R_{P_2}|\ (mod\ p)$$

از طرفی $p\nmid (G:P_1)=m$ بنابراین $p\nmid |R_{P_2}|$ یعنی $R_{P_2}\neq f$. فرض کنید $P_1x_0\in R_{P_2}$ بنابراین به ازای هر $h\in P_2$ داریم:

$$P_1x_0h=P_1x_0\Rightarrow x_0hx_0^{-1}\in P_1, \forall h\in P_2\Rightarrow x_0P_2x_0^{-1}\subseteq P_1$$

چون $\left|x_0 P_2 x_0^{-1}\right| = \left|P_2\right| = \left|P_1\right|$ پس $P_2^{x_0^{-1}} = P_1$ یعنی P_1 , P_2 مزدوجند.

برهان 2. فرض کنید $H \leq G$ یک p - زیر گروه سیلوی G باشد و K یک p - زیر گروه سیلوی دیگر G بنا به قسمت اول و نرمال بودن، H داریم:

$$\exists g \in G \; s.t. \; K = H^g = H.$$

به عکس ($\Rightarrow$). فرض کنید H تنها p - زیر گروه سیلوی G باشد. به ازای هر $g \in G$ داریم $\left|H^g\right| = \left|H\right| = p^n$ یعنی H^g نیز یک $p-$ زیر گروه سیلوی G است. بنابراین داریم:

$$\forall g \in G; H^g = H \Rightarrow H \leq G.$$

در مثال 1. 3. 3 (i) دیدیم که S_3 فقط یک 3- زیر گروه سیلو دارد (چون هر زیر گروه با اندیس 2 نرمال است) ولی تعداد 2- زیر گروه‌های سیلوی S_3 سه تا می‌باشد.

قضیه. بعد نقش کلیدی در ساده نبودن گروه‌های متناهی دارد.

قضیه 1. 3. 6 (قضیه سوم سیلو). فرض کنید $\left|G\right| = p^n m$ که $(p,m) = 1$ و l تعداد $p-$ زیر گروه‌های سیلوی G باشد. در این صورت:

1- $l \left|\right| G|$

2- $l \equiv 1 (mod\ p)$ به عبارت دیگر l=1+kp

برهان 1. قرار می‌دهیم $X = \{$ G زیرگروه‌های سیلوی $p-\}$ حال عمل G روی X را به صورت زیر تعریف می‌کنیم:

$$X \times G \to X$$
$$(P, g) \to P^g$$

بنا به قضیه دوم سیلو داریم: $\forall P_1, P_2 \in X, \exists g \in G \; s.t. \quad P_1 = P_2^g$ یعنی عمل G روی X متعدی است. حال بنا به نتیجه: $l = \left|X\right| \left|\right| G|$

برای اثبات2. فرض کنید P یک p - زیر گروه سیلوی ثابت G می‌باشد. عمل P روی X با تابع زیر را در نظر می‌گیریم.

$$X \times P \to X$$
$$(P_1, g) \to P_1^g$$

چون P یک p - گروه است. داریم $L = \left|X\right| \equiv \left|X_P\right| (\text{mod } p)$ که $X_P = \left\{P_1 \in X \middle| P_1^g = P_1, \forall g \in P\right\}$ واضح است که $P \in X_P$ حال فرض کنید $Q \in X_P$ بنابراین $\forall g \in P; Q^g = Q \Rightarrow P \subseteq N(Q)$ پس Q, P دو زیر گروه p - سیلوی $N(Q)$ هستند و بنا به تمرین $P = Q$ در نتیجه $\left|X_P\right| = 1$ و حکم ثابت می‌شود.

مثال1. 3. 7. نشان دهید که هر گروه از مرتبه 21 ساده نیست.

راه حل. فرض کنید G یک گروه باشد که $|G| = 21 = 3\times 7$ بنابراین $l_7 = 1+7k \mid 21 \Rightarrow l_7 = 1+7k \mid 3$ در نتیجه فقط $L_7=1$, k=0 یعنی G فقط یک 7- زیر گروه سیلو دارد که بنا به قضیه دوم سیلو نرمال است. پس G ساده نیست.

آیا به روش بالا می‌توانیم نشان دهیم که 3- زیر گروه سیلوی G نرمال است؟

مثال1. 3. 8. نشان دهید که هر گروه از مرتبه 56 ساده نیست.

راه حل. داریم:

$$|G| = 56 = 7\times 2^3 \Rightarrow L_7 = 1+7k \mid 2^3 \Rightarrow L_7 = 1 \text{ یا } 8.$$

اگر $l_7=1$ پس G ساده نیست. فرض کنید $l_7 \neq 1$ بنابراین G دارای 8 زیر گروه سیلو از مرتبه 7 می‌باشد. فرض کنید H_1 , H_2 , ... , H_8 زیر گروه‌های 7- سیلوی متمایز باشد. داریم:

$$H_1 \mathbf{I} H_2 \leq H_1 \Rightarrow |H_1 \mathbf{I} H_2| \mid 7 = |H_1| \Rightarrow |H_1 \mathbf{I} H_2| = 1 \text{ یا } 7.$$

اگر $|H_1 \mathbf{I} H_2| = 7$ آنگاه $H_1 \mathbf{I} H_2 = H_1$ یعنی $H_1 \subseteq H_2$ پس $H_1 = H_2$ که متناقض با متمایز بودن H_1, H_2 است. یعنی $H_1 \mathbf{I} H_2 = \{e\}$ پس هر دو 7- زیر گروه سیلو دارای 12 عضو متمایز از مرتبه 7 هستند. در نتیجه در کل G دارای 48=6 × 8 عضو از مرتبه 7 متمایز دارد. در نتیجه G حداکثر 8 = 48 – 56 عضو از مرتبه توان‌های 2 دارد که با 8 عضو از مرتبه توان‌های 2 فقط یک زیرگروه از مرتبه 8 داریم. بنابراین 2- زیر گروه سیلوی G منحصر به فرد پس نرمال است.

مثال9.3.1. هر گروه از مرتبه 30 ساده نیست.

راه حل. فرض کنید $|G| = 2\times 3\times 5$ پس $l_5 = 1+5k \mid 6 \Rightarrow l_5 = 1$ یا 6.

اگر $l_5 = 1$ پس 5- زیر گروه سیلو نرمال است. فرض کنید $l_5=6$ پس 24 عضو از مرتبه 5 داریم همچنین:

$$l_3 = 1+3k \mid 10 \Rightarrow l_3 = 1 \text{ یا } 10.$$

اگر $L_3=1$ آنگاه 3- زیر گروه سیلو نرمال است. در غیر این صورت G دارای 20 = 2 × 10 عضو از مرتبه 3 می‌باشد. بنابراین G لااقل 44 = 20 + 24 عضو دارد که تناقض است. پس $l_3=1$ یا $l_5=1$ یعنی G ساده نیست.

در تمرینات حالت کلی تری از مثال بالا بیان شده است. (تمرین 7)

قضیه1. 3. 10. فرض کنید $|G|=Pq$ که p و q اعداد اولند و P<q در این صورت:

1- G ساده نیست.

2- اگر $q-1 \nmid p$ آنگاه G دوری است.

برهان 1. داریم $p|q+1=kq$ پس $l_q=1$ و q- زیر گروه سیلو نرمال است.

برای اثبات قسمت دوم $q|kp+1=l_P$ پس $l_P=q$ یا $l_p=1$. اگر $l_p=kp+1=q$ پس $p|q-1$ که تناقض است بنابراین $l_p=1$ یعنی $p-$ زیر گروه سیلو نیز نرمال است. فرض کنید K,H به ترتیب p - زیر گروه و q- زیر گروه سیلوی G باشند. بنابراین $|HK|=\frac{|H||K|}{|H \cap K|}=pq$ یعنی G=HK چون $H \cap K=\{e\},H,K\leq G$ پس داریم $G \; ; \; H\times K \; ; \; Z_p\times Z_q \; ; \; Z_{pq}$ و حکم برقرار است.

از قضیه بالا نتیجه می‌شود که اگر $|G|=15$ آنگاه G دوری است و $G \; ; \; Z_{15}$ و همچنین تنها گروه از مرتبه 85 همان Z_{85} می‌باشد.

مثال1. 3. 11. هر گروه از مرتبه 255 دوری است.

راه حل. فرض کنید $|G|=255=3\times5\times17$ داریم:

$$L_{17}=1+17k|15\Rightarrow L_{17}=1.$$

پس 17- زیر گروه سیلو نرمال است. همچنین داریم:

$$L_5=1+5k|51\Rightarrow L_5=1 \text{ یا } 51.$$

اگر $l_5=1$ آنگاه 5- زیر گروه سیلو نیز نرمال است. فرض کنید $l_5=51$ پس G دارای 204 = 4 ×51 عضو از مرتبه 5 است. حال تعداد 3- زیر گروه سیلوهای G را محاسبه می‌کنیم، داریم:

$$l_3=1+3k|85\Rightarrow l_3=1 \text{ یا } 85$$

اگر $l_3=1$ آنگاه 3- زیر گروه سیلو نرمال است، در غیر این صورت G دارای 170 = 2×85 عضو از مرتبه 3 است. بنابراین $|G|>170+204$ که تناقض است. در نتیجه 5- زیر گروه سیلو یا 3- زیر گروه سیلو حداقل یکی نرمال است. فرض کنید K,H به ترتیب 17- زیر گروه سیلو و 3- زیر گروه سیلو باشند. پس $|G/K|=51=3\times17,|G/H|=15$ که آبلی هستند. در نتیجه $G'\leq K,G'\leq H$ یعنی $G'\leq H \cap K=\{e\}$ پس G آبلی است. چون $|G|=3\times5\times17$ پس $G\simeq Z_3\times Z_5\times Z_{17}\simeq Z_{255}$ و حکم برقرار است.

مثال1. 3. 12. هر گروه از مرتبه 36 ساده نیست.

راه حل داریم:

$$|G| = 2^2 \times 3^2 \Rightarrow L_3 = 1 + 3k | 4 \Rightarrow L_3 = 1 \text{ یا } 4$$

اگر $L_3=1$ آنگاه حکم برقرار است. فرض کنید $L_3=4$ و K,H دو 3- زیر گروه سیلوی متمایز G باشند.

داریم $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{9 \times 9}{|H \cap K|} \leq 36$

چون $|H| = |K| = 9$ و $|H \cap K| \mid |H|$ پس $|H \cap K| = 3$ بنابراین $H \cap K \leq H, K$ یعنی $H, K \leq N(H \cap K)$

در نتیجه $H, K \leq N(H \cap K)$ بنابراین $|N(H \cap K)| \geq |HK| = 27$. چون $N(H \cap K) \leq G$ پس $|N(H \cap K)| \leq |G|$ یعنی $N(H \cap K) = G$. بنابراین $H \cap K \leq G$ یعنی G ساده نیست.

1. 4 معادله رده (کلاس) گروه

فرض کنید X یک مجموعه متناهی و G روی X عمل کند. بنابراین داریم:

$$|X| = |X_G| + \sum_{i=1}^{n} |\overline{x_i}|$$

قرار می‌دهیم X=G و $X \times G \to X$ پس $(x, g) \to x^g$

$$X_G = \{x \in X = G \mid \forall g \in G; x^g = x\}$$

$$= \{x \in G \mid \forall g \in G; xg = gx\} = Z(G).$$

همچنین بنا به $|\overline{x_i}| = (G : G_{x_i})$ که:

$$G_{x_i} = \{g \in G \mid x_i^g = x_i\} = \{g \in G \mid x_i\, g = g x_i\} = C(x_i)$$

در نتیجه $|G| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{C(x_i)}$ که آن را معادله رده‌ای گروه G نامیم.

قضیه1. 4. 1. اگر G یک p - گروه متناهی باشد آنگاه $Z(G) \neq \{e\}$

برهان. داریم $|G| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{C(x_i)}$. از طرفی داریم:

$$G = C(x) \Rightarrow \forall g \in G; xg = gx \Leftrightarrow x \in Z(G).$$

بنابراین $\frac{|G|}{|C(x_i)|} \neq 1$ پس $p \mid \frac{|G|}{|C(x_i)|}$ چون $p \mid |G|$ در نتیجه $p \mid |Z(G)|$ یعنی $|Z(G)| \geq p$ و حکم برقرار است.

نتیجه1. 4. 2. اگر $|G| = p^2$ آنگاه G آبلی است.

برهان. چون $Z(G)\neq\{e\}$ پس p^2 یا $|Z(G)|=P$ اگر $|Z(G)|=P^2$ پس G=Z(G) یعنی G آبلی است. حال فرض کنید $|Z(G)|=p$ پس $\left|G/Z(G)\right|=p$ یعنی $G/Z(G)$ دوری است و حکم به دست می‌آید.

مثال1 . 4. 3. هر گروه از مرتبه p^2 یکریخت با Z_{p^2} یا $Z_p\oplus Z_p$ است.

برهان. چون هر گروه از مرتبه p^2 آبلی است پس حکم برقرار است.

1. 5 قضایای بیشتر برای ساده نبودن گروه‌ها.

فرض کنید G روی X عمل کند و $g\in G$. در اینصورت تابع $\begin{matrix}f_g:X\to X\\ x\to xg\end{matrix}$ یک جایگشت روی X است و $\begin{matrix}f:G\to S_x\\ g\to f_g\end{matrix}$ یک همریختی.

به خصوص اگر $H\le G$، $(G:H)=n$ و $R=\{Hx|x\in G\}$ ، عمل $\begin{matrix}R\times G\to R\\ (Hx,g)\to Hxg\end{matrix}$ متعدی است. داریم: $\begin{matrix}f_g:R\to R\\ \mathrm{H}x\to Hxg\end{matrix}$ که $f_g\in S_n$ حال $Ker f$ را محاسبه می‌کنیم.

$$\begin{aligned}Ker f&=\{g\in G|f_g=e\}=\{g\in G|(Hx)f_g=Hx,\forall Hx\in R\}\\&=\{g\in G|Hxg=Hx,\forall Hx\in R\}=\{g\in G|g\in x^{-1}Hx,x\in G\}\\&=\coprod_{x\in G}H^x.\end{aligned}$$

قرار می‌دهیم $Cor(H)=\coprod_{x\in G}H^x$ که آن را مغز H نامیم. در تمرینات بعضی از خواص مهم Cor(H) را بیان می‌کنیم.

نتیجه1. 5. 1 . فرض G یک گروه ساده و $H\le G$ که (G:H)=n آنگاه $|G|\|n!$

برهان بنا به اطلاعات بالا و قضیه اول یکریختی داریم $\frac{G}{Cor(H)}$; $\mathrm{Im}\,g(f)\le S_n$. چون $Cor(H)\le G$ (تمرین) و G ساده است بنابراین $Cor(H)=\{e\}$ یعنی G ; $\mathrm{Im}\,gf\le S_n$ پس $|G|\|n!$.

به عبارت دیگر نتیجه بالا بیان می‌کند که «**اگر G دارای زیر گروهی مانند H باشد که** $(G:H)=n$ **و** $|G|\nmid n!$ **آنگاه G ساده نیست.**»

مثال1. 5. 2. نشان دهید که هر گروه از مرتبه 80 ساده نیست.

راه حل. داریم $|G|=2^4\times 5$ فرض کنید H یک 2- زیر گروه سیلوی G باشد پس $(G:H)=5,|H|=16$ چون $|G|=80\nmid 5!$ پس G ساده نیست.

نتیجه1. 5. 3. اگر گروه G ساده باشد و $(G:H)=n, H\leq G$ آنگاه $|G|\mid\frac{n!}{2}$

برهان. بنا به برهان نتیجه قبل $G\simeq \mathrm{Im}gf\leq S_n$ حال اگر هر عضو $\mathrm{Im}\,g(f)$ زوج باشد پس $G\simeq \mathrm{Im}gf\leq A_n$ در غیر این صورت $\mathrm{Im}\,g(f)$ دارای عضو از مرتبه فرد است پس G ساده نیست. (بنا به تمرین)

مثال1. 5. 4. نشان دهید که هر گروه از مرتبه 112 ساده نیست.

راه حل. داریم $|G|=2^4\times 7$ فرض کنید $H\in sly_2(G)$ پس $|G|=2^4$ چون $112\nmid\frac{7!}{2}$، G ساده نیست.

قضیه1. 5.5. فرض کنید G یک گروه متناهی و p کوچک ترین عدد اولی باشد که $p||G|$ در این صورت اگر $(G:H)=p,\ H\leq G$ آنگاه $H\leq G$.

برهان. با استفاده از نتیجه داریم $\mathrm{Im}\,gf\leq S_p$; $\frac{G}{Cor(H)}$

می‌خواهیم نشان دهیم که H=Cor(H) داریم

$$(G:Cor(H))=(G:p)\times(H:Cor(H))=p\times|\frac{H}{Cor(H)}|$$

همچنین $p\left|\,|\frac{G}{Cor(H)}\right.$ بنابراین $|\frac{H}{Cor(H)|}\left|\,|\frac{1}{p}\times|\frac{G}{Cor(H)}|\right.$ یعنی $|\frac{H}{Cor(H)}|\left|\,(p-1)!\right.$ فرض کنید q عدد اولی باشد که $q\left|\,|\frac{H}{Cor(H)}|\right.$ پس $q|(p-1)!$ از طرفی $|\frac{H}{Cor(H)}||\,|G|$ که تناقض است.

نتیجه 6.5.1. فرض کنید G یک گروه متناهی و $H\leq G$ که $(G:H)=n$ آنگاه G دارای زیر گروهی مانند H است که $|\frac{H}{N}|\left|\,n!\right.$

برهان. بنا به قضیه داریم که $\mathrm{Im}\,g(f)\leq S_n$; $\frac{G}{Cor(H)}$ ، $Cor(H)\leq G$ و $Cor(H)\leq H$. بنابراین $\frac{H}{Cor(H)}\leq\frac{G}{Cor(H)}$ و $|\frac{H}{Cor(H)}|\left|\,|\frac{G}{Cor(H)}|\right.|\,|G|$. وحکم برقرار است.

تذکر. فرض کنید G یک گروه متناهی $X=\{U\,|f\neq U\subseteq G\}$. در این صورت $\begin{matrix}X\times G\longrightarrow X\\(U,g)\ \to\ U^g\end{matrix}$

داریم $U^e = U$ و $(U^g)^h = U^{gh}$. حال به ازای هر U از X پایدار ساز U بصورت زیر است.

$$st(U) = \{g \in G \mid U^g = U\}.$$

بنابراین $st(U) = N_G(U)$. اکنون $Orb_G(U) = \{U^g \mid g \in G\}$. بنابراین هرگاه مجموعه مزدوج‌های U در G آنگاه $|Orb_G(U)| = (G : N_G(U))$. بخصوص قضیه زیر را داریم:

نتیجه 7.5.1. فرض کنید G یک گروه متناهی و $H \leq G$ در اینصورت تعداد مزدوج‌های متمایز H در G برابر است با $(G : N_G(H))$. بخصوص تعداد مزدوج‌های متمایز H در G، $(G : H)$ را عاد می‌کند.

در ادامه گروه‌های غیر آبلی از مرتبه 8 را طبقه بندی می‌کنیم.

قرار می‌دهیم:

$$D_{2n} = < x, y \mid x^n = y^2 = e, (xy)^2 = e >$$

$$Q_8 = < x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} > .$$

قضیه 1. 5. 6. هر گروه غیر آبلی از مرتبه 8 یکریخت است با D_8 یا Q_8.

برهان. فرض کنید $|G| = 8$ چون هر عضو غیر بدیهی G نمی‌تواند از مرتبه 2 باشد و G عضوی از مرتبه 8 ندارد پس G دارای عضوی مانند a است که $|a| = 4$. قرار می‌دهیم H=<a> پس $|H| = 4, (G : H) = 2$ یعنی $H \leq G$. و داریم $G/H = < Hb > = \{H, Hb\}, H = \{e, a, a^2, a^3\}$ که $|Hb| = 2$ بنابراین:

$$(Hb)^2 = H \Rightarrow b^2 \in H = \{e, a, a^2, a^3\}.$$

اگر a^3 یا b^2=a آنگاه $|a| = 4$ که تناقض است. بنابراین داریم:

b^2=a^2 یا b^2=e (1)

همچنین $H \leq G$ پس $b^{-1}ab \in H = \{e, a, a^2, a^3\}$ حالت‌های زیر را داریم:

1- اگر $b^{-1}ab$=e آنگاه a=e که تناقض است.

2- $b^{-1}ab$=a آنگاه ab=ba پس G آبلی است که تناقض می‌باشد.

با بررسی حالت‌های دیگر می‌توان دریافت که حکم برقرار است. (تمرین)

1. 6 گروه‌های جایگشتی

یادآوری. فرض کنید $p \in S_n, a = (i_1, ..., i_k)$ در این صورت:

$$p^{-1}ap = a^p = (p(i_1), p(i_2), ..., p(i_k))$$

لم1. 6. 1. اگر $n \geq 5$ آنگاه هر دور سه بعدی در A_n مزدوجند.

برهان. فرض کنید $(j_1,j_2,j_3),(i_1,i_2,i_3)$ دو دور سه بعدی باشند. $p \in S_n$ را در نظر می‌گیریم به قسمی که $p(i_3) = j_3, p(i_2) = j_2, p(i_1) = j_1$ داریم:

$$(i_1, i_2, i_3)^p = (p(i_1), p(i_2), p(i_3)) = (j_1, j_2, j_3)$$

اگر $p \in A_n$ آنگاه حکم برقرار است. در غیر این صورت فرض کنید a,b عناصری باشند که مخالف i_1,i_2,i_3 هستند. قرار می‌دهیم $s = (a,b)$ و $p' = ps$ بنابراین داریم:

$$(i_1, i_2, i_3)^{p'} = (p(s(i_1)), ..., p(s(i_3))) = (j_1, j_2, j_3)$$

و حکم ثابت می‌شود.

قضیه1 .2.6. به ازای هر $n \geq 3$ گروه A_n توسط دورهای سه بعدی تولید می‌شود.

برهان. فرض کنید $s = s_1 s_2 ... s_{2k} \in A_n$ که s_i ها ترانهش هستند.

حالت‌های زیر را داریم:

1- اگر $s_i s_{i+1} = (a,b)(b,c)$ آنگاه $s_i s_{i+1} = (a,b,c)$

2- اگر $s_i s_{i+1} = (a,b)(c,d)$

پس s را می‌توان به حاصل ضرب دورهای سه بعدی نوشت.

نتیجه1. 6. 3. اگر $H < S_n, n \geq 5$ که شامل یک دور سه بعدی باشد آنگاه $H = A_n$.

برهان. کافی است نشان دهیم که هر دور سه بعدی به H متعلق است. فرض کنید $d \in H$ یک دور سه بعدی باشد و s یک دور سه بعدی دلخواه در A_n بنابراین داریم $\exists a \ \ s.t. \ \ s = d^a$

چون $d \in H, H \leq G$ پس $d \in H$ یعنی H شامل همه دورهای 3- بعدی است چون A_n توسط دورهای سه بعدی تولید می‌شود و تنها زیر گروه نرمال غیر بدیهی S_n است. (تمرین.....) پس $H = A_n$

می‌توان نشان داد که A_n به ازای $n \geq 5$ ساده است (برای اثباتی از این به [ ] مراجعه نمود.)

1. 7 گروه‌های خطی

فرض کنید F یک میدان و n عددی طبیعی باشد. هر ماتریس n×n را به صورت $A=(a_{ij})_{n\times n}$ می‌نویسیم که $a_{ij} \in F$ مجموعه همه ماتریس‌های معکوس پذیر n×n را با GL(n,F) نشان می‌دهیم. یعنی $GL(n,F)=\{A_{n\times n} | \det A_{n\times n} \neq 0\}$. همچنین $SL(n,F)=\{A\in GL(n,F) | \det A=1\}$ را در نظر می‌گیریم. در این صورت واضح است که $SL(n,F)$ یک گروه است و $SL(n,F)\leq GL(n,F)$.

تعریف1. 7. 1. گروه‌های $GL(n,F)$ و $SL(n,F)$ را به ترتیب گروه‌های خطی عام (از درجه n بر F) و گروه-های خطی خاص (از درجه n بر F) نامیم.

فرض کنید V یک فضای برداری روی میدان F باشد. مجموعه همه تبدیلات خطی معکوس پذیر F را با GL(F) نشان می‌دهیم در این صورت GL(F) با عمل ترکیب یک گروه است و داریم GL(F) ≅ GL(n,F) در واقع هر تبدیل خطی معکوس پذیر متناظر با ماتریس نمایش آن بر یک پایه V می‌باشد.

لم1. 7. 2. فرض کنید F یک میدان و n یک عدد طبیعی مفروض باشد. در این صورت $\frac{GL(n,F)}{SL(n,F)} \cong F^*$ که F^*، گروه ضربی میدان F است.

برهان. تابع $f: GL(n,F) \to F^*$, $A \to \det A$ را در نظر می‌گیریم واضح است که f همریختی پوشا است و $Ker f = SL(n,F)$ پس حکم از قضیه اول یکریختی به دست می‌آید.

قرارداد. فرض کنید F یک میدان متناهی باشد و $|F|=q$ (از جبر 2 می‌دانیم که q به صورت توان مثبتی از یک عدد اول است) در این صورت گروه‌های GL(n,F) ,SL(n,F), GL(n,F) را به ترتیب با GL(n,F), SL(n,q) نشان می-دهیم. به عنوان مثال GL(2,3) ماتریس‌های معکوس پذیر 2×2 روی میدان Z_3 می‌باشد و $\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} \in SL(2,3)$.

قضیه1. 7. 3. فرض کنید n یک عدد طبیعی مفروض و $|F|=q$ در این صورت

i - $|GL(n,q)| = (q^n-1)(q^n-q)...(q^n-q^{n-1})$.

ii - $|SL(n,q)| = \frac{|GL(n,q)|}{q-1}$.

برهان. ماتریس $A=\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ را در نظر می‌گیریم که به ازای $1 \le j \le n$ $v_j=(v_{j1},v_{j2},...,v_{jn})$ می‌دانیم که A معکوس پذیر است. اگر و فقط اگر $v_1, v_2, \ldots, v_n$ مستقل خطی باشند. تعداد انتخاب‌های v_1 مساوی q^n است و اگر $\{v_1\}$ مستقل خطی باشد آنگاه تعداد انتخاب‌های v_1 مساوی q^n-1 است. حال باید v_2 را طوری انتخاب کنیم که $\{v_1,v_2\}$ مستقل خطی باشد پس $v_2 \neq cv_1$ به ازای هر $c \in F$ پس تعداد انتخاب‌های v_2 به طوری که $\{v_1,v_2\}$ مستقل خطی باشند برابر است با q^n-q و با ادامه فرایند تعداد انتخاب‌های v_n به طوری که $\{v_1,v_2,...,v_n\}$ مستقل خطی باشد برابر است با q^n-q^{n-1} حال بنا به اصل ضرب تعداد A های معکوس پذیر برابر است با $(q^n-1)(q^n-q)....(q^n-q^{n-1})$.

برای اثبات قسمت (ii) از قسمت اول و لم 1. 5. 2 استفاده می‌کنیم.

نکته: می‌توان نشان داد که $Z(SL(n,F))=\{aI_{n\times n} \mid a \in F^*\}$ قرار می‌دهیم $PSL(n,F)=\frac{SL(n,F)}{Z(SL(n,F))}$ که آن را گروه خطی خاص تصویری از درجه n روی F نامیم و داریم $|PSL(n,F)|=\frac{|SL(n,F)|}{(n,q-1)}$.

.

اثبات قضیه زیر را می‌توان در [ ] ملاحظه نمود.

قضیه1. 7. 4. اگر n=2 یا n>2 و $|F|>3$ آنگاه $PSL(n,F)$ ساده است.

مثال‌ها1. 7. 5 .

1- داریم $|SL(2,2)|=6$ و $SL(2,2)=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}0&1\\1&0\end{bmatrix},\begin{bmatrix}1&1\\1&0\end{bmatrix},\begin{bmatrix}0&1\\1&1\end{bmatrix}\right\}$.

می‌توان نشان داد که $PSL(2,2)$; $SL(2,2)$; S_3.

2- می‌دانیم $|SL(2,3)|=24$ قرار می‌دهیم $a=\begin{bmatrix}0&1\\2&1\end{bmatrix}$ با محاسبه معلوم می‌شود که $a^3=-I_{2\times 2}$ پس a عضوی از مرتبه 6 می‌باشد.

تمرینات

1- فرض کنید G روی X عمل می‌کند به ازای هر $g \in G$ تابع $\begin{matrix} f_g : X \to X \\ x \to xg \end{matrix}$ را در نظر می‌گیریم نشان دهید که

الف) f یک جایگشت است.

ب) تابع $\begin{matrix} f : G \to S_x \\ g \to f_g \end{matrix}$ یک همریختی است.

ج) $Ker f$ را مشخص کنید.

د) به‌خصوص اگر $H \leq G, R = \{Hx | x \in G\}$ آنگاه $Ker f$ را محاسبه کنید.

2- اگر P عددی اول $|G| = p^n m$ که $(p,m) = 1$ نشان دهید کـه H یـک p - زیـر گـروه سـیلوی G اسـت $\Leftrightarrow |H| = p^n$

3- نشان دهید که به ازای هر عدد اول p و گروه G , p – زیر گروه سیلوی G وجود دارد.

4- نشان دهید که P تنها p – زیر گروه سیلوی N(P) است.

5- نشان دهید که هر گروه از مرتبه 88 ساده نیست.

6- اگر $|G| = P^n m$ که $p \geq m$ و $(p,m) = 1$ آنگاه G ساده نیست.

7- اگر $|G| = pqr$ که r,q,p سه عدد اول متمایزند آنگاه G ساده نیست.

8- اگر $H, K \subseteq N(H \cap K)$ آنگاه $HK \subseteq N(H \cap K)$

9- فرض کنید G یک گروه باشد و $H \leq G$ در این صورت:

الف) $Cor(H) \leq G$ و $Cor(H)$ بزرگ ترین زیر گروه نرمال G مشمول H است.

ب) $Cor(H) = H \Leftrightarrow H \leq G$.

10- فرض کنید G یک گروه باشد و $H \leq G$ در این صورت H را زیرگروه مشخصه‌ی G نامیم هرگاه $\forall f \in Aut(G);\ f(H) \subseteq H$

نشان دهید:

الف) $\{e\}, G$ زیرگروه مشخصه‌ی G هستند.

ب) هر زیرگروه مشخصه G زیرگروه نرمال است ولی عکس آن لزوما برقرار نیست.

ج) هر p–زیرگروه سیلوی نرمال G، زیرگروه مشخصه G است.

11- فرض کنید $H \leq S_n$ در این صورت تمام عناصر G زوجند یا نیمی از عناصر G زوج و نیم دیگر فردند.

12- با شرایط **قضیه**1. 5، 6 نشان دهید که $G = H \cup Hb = \{e, a, a^2, a^3, b, ab, ..., a^3b\}$.

13- نشان دهید که A_n تنها زیر گروه نرمال غیر بدیهی S_n است.

14- نشان دهید که S_3 ; $SL(2,2)$; $PSL(2,2)$.

15- نشان دهید که S_4 ; $SL(2,3)$ ولی A_4 ; $PSL(2,3)$.

فصل دوم گروههای حل‌پذیر و پوچتوان

1.2 معرفی سری گروهها

تعریف 1.1.2. فرض کنید G یک گروه باشد و $G_k ..., G_1, G_0$ زیر گروه‌های G باشند به قسمی‌که

$$\{e\} = G_0 < G_1 < ... < G_k = G \qquad (1)$$

در این‌صورت

الف) زنجیر (1) را یک **سری زیر نرمال** G نامیم هرگاه

$$\forall 1 \le i \le k; G_{i-1} < G_i$$

گاهی از اوقات سری زیر نرمال فوق را به صورت زیر نشان می دهیم:

$$\{e\} = G_0 < G_1 < ... < G_k = G$$

ب) زنجیر (1) را یک **سری نرمال** G نامیم هر گاه

$$\forall\ 0 \le i \le k;\ G_i < G$$

ج) در تعریف های الف و ب): هر گاه G_i را **یک جمله سری**، k را **طول سری** و هر $\frac{G_i}{G_{i-1}}$ را یک **عامل سری** می نامیم.

واضح است که هر سری نرمال یک سری زیر نرمال است. همچنین اگر G آبلی باشد آنگاه دو مفهوم سری زیر نرمال و سری نرمال یکسان هستند.

مثالها2.1.2

1) سری های $\mathbb{C} > 2\mathbb{C} > 16\mathbb{C} > \{0\}$ و $\mathbb{C} > 5\mathbb{C} > \{0\}$ دو سری نرمال گروه $\mathbb{C}$ هستند و عامل های آنها عبارتند از:

$$\frac{\mathbb{C}}{2\mathbb{C}}\ ;\ Z_2, \frac{2\mathbb{C}}{16\mathbb{C}}\ ;\ Z_8, \frac{16\mathbb{C}}{\{0\}}\ ;\ 16\mathbb{C};$$

$$\frac{\mathbb{C}}{5\mathbb{C}}\ ;\ Z_5, \frac{5\mathbb{C}}{\{0\}}\ ;\ 5\mathbb{C}.$$

2) اگر $n \ge 3$ آنگاه $\{e\} < A_n < S_n$ یک سری نرمال S_n است.

3) گروه S_4 و زیر گروه‌های $U = \langle (1,2)(3,4) \rangle, V = \langle (1,2)(3,4), (2,3)(1,4) \rangle$ از آن را در نظر می‌گیریم. در این صورت هر یک از سری های زیر یک سری نرمال S_4 هستند.

(1) $\{e\} < V < S_4$

(2) $\{e\} < U < V < S_4$

(3) $\{e\} < U < V < A_4 < S_4$

از این سریها فقط سری اولی نرمال است.

4) گروه تقارنهای مربع، D_8، را در نظر بگیرید. قرار دهید:

$a = (1,2,3,4), \quad b = (1,2)(3,4)$

در این صورت هر یک از سری‌های زیر یک سری زیر نرمال D_8 است.

$\{e\} < < a^2 > < < a > < D_8$

$\{e\} < < b > < < b, a^2 > < D_8.$

تعریف 3.1.2. فرض کنید

(1) $\{e\} = G_0 < G_1 < ... < G_r = G,$

(2) $\{e\} = H_0 < H_1 < ... < H_s = G.$

دو سری زیر نرمال G باشند. در این صورت

الف) سری (2) را یک **تظریف سری** (1) نامیم هرگاه هر جمله سری (1)، یک جمله از سری (2) باشد.

ب)دوسری (1) و (2) را **معادل** (یا هم ارز) گوئیم هر گاه $s = r$ و تناظر یکبیکی بین مجموعه عاملهای سری (1) و مجموعه عاملهای سری (2) وجود داشته باشد به قسمی که هر عامل (1) یا عامل متناظرش در (2) یکریخت باشد.

مثال 4.1.2 الف) در مثال قبل قسمت سوم؛ سری (3) تظریف سریهای (1) و (2) است. همچنین سری (2) تظریف سری (1) می باشد.

ب) دو سری $Z_6 > < 2 > < < 0 > < < 3 > < Z_6$ و $Z_6 > < 3 > < < 0 > < < 2 > < Z_6$ معادل هستند. زیرا

$$|\frac{< 3 >}{< 0 >}| = 2, \ |\frac{Z_6}{< 3 >}| = 3$$

و

$$|\frac{< 2 >}{< 0 >}| = 3, \quad |\frac{Z_6}{< 2 >}| = 2$$

بنابراین $\frac{< 2 >}{< 0 >} ; \frac{Z_6}{< 3 >}, \ \frac{Z_6}{< 2 >} ; \frac{< 3 >}{< 0 >}.$

ج) دو سری زیـر نرمـال $\mathbb{C} > 4\mathbb{C} < 8\mathbb{C} < \{0\}$ و $\mathbb{C} > 9\mathbb{C} < \{0\}$ را از گـروه $\mathbb{C}$ در نظـر بگیریـد. در ایـن صورت سریهای

(1) $\{0\} < 72\mathbb{C} < 8\mathbb{C} < 4\mathbb{C} < \mathbb{C}$

(2) $\{0\} < 72\mathbb{C} < 18\mathbb{C} < 9\mathbb{C} < \mathbb{C}$

به ترتیب تظریفهای دو سری داده شده می باشند و عاملهای سری های (1) و (2) به صورت زیر می باشند.

عاملهای سری (1):

$$\frac{72\mathbb{C}}{\{0\}} ; 72\mathbb{C}, \frac{8\mathbb{C}}{72\mathbb{C}} ; Z_9, \frac{4\mathbb{C}}{8\mathbb{C}} ; Z_2, \frac{\mathbb{C}}{4\mathbb{C}} ; Z_4$$

عاملهای سری (2):

$$\frac{72\mathbb{C}}{\{0\}} ; 72\mathbb{C}, \frac{18\mathbb{C}}{72\mathbb{C}} ; Z_4, \frac{9\mathbb{C}}{18\mathbb{C}} ; Z_2, \frac{\mathbb{C}}{9\mathbb{C}} ; Z_9$$

واضح است که سری های (1) و (2) معادلند.

لم زیر تعمیمی از قضیه دوم یکریختی در گروه‌ها است.

لم 5.1.2 فرض کنید G یک گروه باشد. اگر C, B, A زیـر گـروه هـای G باشـند بـه طـوری کـه $C \leq G$ و $B \leq A$ آنگاه

$$\frac{AC}{BC} ; \frac{A}{B(A \cap C)}$$

برهان. معلوم است که $BC \leq AC$. اینک بنا بر قضیه دوم یکریختی داریم:

$$\frac{AC}{BC} ; \frac{(AB)C}{BC} ; \frac{A(BC)}{BC} ; \frac{A}{A \cap BC} ; \frac{A}{B(A \cap C)}$$

لم زیر به قضیه چهارم یکریختی گروه ها مشهور است.

لم 6.1.2. (لم شور) فرض کنیـد G یـک گـروه باشـد. اگـر K_1, H_1, K, H زیـر گروههـایی از G باشـند کـه $H_1 \leq H$ و $K_1 \leq K$ آنگاه

$$\frac{H_1(H \cap K)}{H_1(H \cap K_1)} ; \frac{K_1(H \cap K)}{K_1(H_1 \cap K)}$$

برهان. قرار می دهیم $C = H_1, B = H \cap K_1, A = H \cap k, L = H$. بموجب لم قبل

$$\frac{H_1(H \cap K)}{H_1(H \cap K_1)} ; \frac{H \cap K}{(H \cap K_1)(H_1 \cap K)}$$

به طریق مشابه

$$\frac{K_1(H \mathbf{I} K)}{K_1(H_1 \mathbf{I} K)} ; \frac{H \mathbf{I} K}{(H_1 \mathbf{I} K)(H \mathbf{I} K_1)}$$

حال حکم از مقایسه دو رابطه فوق به دست می آید.

قضیه 7.1.2.(قضیه تظریف شرایر). هر دو سری زیر نرمال گروه G دارای تظریفهای معادل هستند.

برهان. دو سری زیر نرمال ذیل را برای G در نظر می گیریم:

(1) $\{e\} = G_0 < G_1 < ... < G_r = G$

(2) $\{e\} = H_0 < H_1 < ... < H_s = G$

فرض کنید i عددی ثابت باشد با استفاده از H_jها می خواهیم بین G_{i-1} و G_iجملاتی درج کنیم. می‌دانـیم که

$$G_{i-1}(G_i \mathbf{I} H_{j-1}) < G_{i-1}(G_i \mathbf{I} H_j)$$

بنابراین داریم:

$$G_{i-1} = G_{i-1}(G_i \mathbf{I} H_0) < G_{i-1}(G_i \mathbf{I} H_1) < ... < G_{i-1}(G_i \mathbf{I} H_6) = G_i$$

با تغییر i $(1 \le i \le r)$ تظریفی از سری (1) بدست می آوریم که طول آن rs است. به‌طور مشابه بدلیل این‌که

$$H_{j-1} = H_{j-1}(H_j \mathbf{I} G_0) < H_{j-1}(H_j \mathbf{I} G_1) < ... < H_{j-1}(H_j \mathbf{I} G_r) = H_j .$$

پس با تغییر j تظریفی از سری (2) بدست می‌آوریم که طول آن rs است و بنا به لم شور دو تظریف حاصـل معادلند.

2.2 سری ترکیبی و قضیه ژردان – هولدر

تعریف1.2.2. فرض کنید G یک گروه باشد. دراین‌صورت سری زیرنرمال

$$\{e\} = G_0 < G_1 < ... < G_r = G$$

را یک سری ترکیب G نامیم هر گاه به ازای هر $(1 \le i \le r)$، عامل $\frac{G_i}{G_{i-1}}$ یک گروه ساده (غیر بدیهی) باشد.

می‌توان نشان داد که هرگروه متناهی دارای یک سری ترکیبی است (G/H ساده است اگرو فقط اگر H زیر گروه نرمال ماکزیمال G باشد). بنابراین سری

$$\{0\} = H_0 < H_1 < ... < H_r = G$$

یک سری ترکیب برای $G \neq \{e\}$ است اگر و تنها اگر H_{i-1} زیر گروه نرمال ماکزیمال H_i باشد. نشان دهید که چنین زیر گروهی وجود دارد). ولی ¢ فاقد سری ترکیبی است. در مثال‌های قبل سری‌های ترکیب را مشخص کنید.

اکنون قضیه زیر که به قضیه ژردان – هولدر معروف است، را اثبات می‌کنیم.

قضیه 2.2.2. فرض کنید گروه G دارای یک سری ترکیبی باشد. در این‌صورت هر دو سری ترکیبی G معادلند.

برهان. اگر $\{e\} < G_1 < ... < G_r = G$ یک سری ترکیبی G باشد آن را نمی توان به طور اکید تظریف کرد. زیرا اگر به ازای عدد i زیر گروه نرمال H بین G_i, G_{i-1} باشد آنگاه $\frac{H}{G_{i-1}} < \frac{G_i}{G_{i-1}}$. چون $\frac{G_i}{G_{i-1}}$ ساده است. پس $H = G_i$ یا $H = G_{i-1}$. حال با این توضیح و استفاده از قضیه شرایر حکم ثابت می شود.

نتیجه3.2.2. هر دو سری ترکیب یک گروه متناهی معادلند.

فرض کنید $\{e\} = G_0 < G_1 < ... < G_r = G$ یک سری ترکیبی باشد. در این صورت G_2را می توان از توسیع G_1 با $\frac{G_2}{G_1}$ ساخت. سپس G_3 را از توسیع G_2 با $\frac{G_3}{G_2}$ به دست می آوریم با تکرار این فرایند سرانجام G بدست می‌آید. توجه شود که G ممکن است دارای سریهای ترکیبی متعددی باشد.ولی بنا به قضیه، عاملهای این سریها یکسانند.

قضیه هولدر حداقل در دو مورد زیر کاربرد دارد.

1)رده بندی همه گروههای ساده متناهی

2)یافتن توسیعهای مکرر ممکن از گروه های ساده

یادآوری4.2.2. فرض کنید K, H دو گروه باشند. گروه Gرا یک توسیع K با H نامیم هر گاه G زیر گروه نرمالی مانند N داشته باشد که $H,\ N$; K ; $\frac{G}{N}$.

به عنوان مثال Z_6 و S_3 توسیعهای (غیریکریخت) از Z_3 با Z_2 هستند.

مثال5.2.2. سریهای $\langle 3\mathbb{Q} \rangle < \langle 0 \rangle < \mathbb{Q}$ و $\langle 5\mathbb{Q} \rangle < \langle 0 \rangle < \mathbb{Q}$ دو سری نرمال $\mathbb{Q}$ (با طول‌های مساوی) که معادل نیستند.

3.2 گروه‌های حل‌پذیر

تعریف1.3.2. فرض کنید G یک گروه باشد

الف) سری زیر نرمال $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_r = G$ از G را **سری حلپذیر** نامیم هرگاه به ازای هر $1 \leq i \leq r$، عاملهای $\frac{G_i}{G_{i-1}}$ آبلی باشد.

ب) گروه G **را حلپذیر** نامیم هر گاه دارای یک سری حلپذیر باشد.

مثال ها2.3.2

1) هرگروه آبلی G حلپذیر است. زیرا $\{e\} \leq G$ یک سری حلپذیر است.

2)سری $\{e\} < A_3 < S_3$ یک سری حلپذیر S_3 است. زیرا $\frac{S_3}{A_3}$ و $\frac{A_3}{\{e\}}$ آبلی هستند. پس S_3 حلپذیر است.

3) گروه S_4 حلپذیر است. زیرا $\{e\} < V < A_4 < S_4$ یک سری آبلی است که $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ و داریم $|\frac{A_4}{V}| = 3$. یعنی $\frac{A_4}{V}$ آبلی است.

4) گروه D_8 حلپذیر است. (چرا؟)

تعریف3.3.2. فرض کنید G یک گروه حلپذیر باشد. در این صورت طول کوتاه‌تری سری حلپذیر G را **طول حلپذیری** (طول مشتق) G نامیم.

توجه4.3.2. 1) طول مشتق گروه حلپذیر G مساوی صفر است $\Leftrightarrow G = \{e\}$

2) هر گروه با طول مشتق 1، آبلی است.

3)گروه حلپذیر $G \neq \{e\}$ ساده است $\Leftrightarrow |G|$ عددی اول باشد.

قضیه5.3.2. فرض کنید G یک گروه حلپذیر باشد. در این صورت

الف) اگر $H \leq G$ آنگاه H حلپذیر است.

ب) اگر $H \leq G$ آنگاه $\frac{G}{H}$ نیز حلپذیر است.

برهان. فرض کنید $\{e\} = G_0 \leq G_1 \leq ... \leq G_r = G$ یک سری حلپذیر G باشد. برای اثبات الف) داریم:

$$\{e\} = H \mathbf{I} G_0 \leq H \mathbf{I} G_1 \leq ... \leq H \mathbf{I} G_r = H \mathbf{I} G = H. \qquad (2)$$

به دلیل اینکه $G_{i-1} \leq G_i$ پس $H \mathbf{I} G_{i-1} \leq H \mathbf{I} G_i$. از طرفی

$$\frac{H \mathbf{I} G_i}{H \mathbf{I} G_{i-1}} = \frac{H \mathbf{I} G_i}{(H \mathbf{I} G_i) \mathbf{I} G_{i-1}} \; ; \; \frac{(H \mathbf{I} G_i) G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}$$

چون $\frac{G_i}{G_{i-1}}$ آبلی است، $\frac{H \mathbf{I} G_i}{H \mathbf{I} G_{i-1}}$ نیز آبلی است. در نتیجه سری (2) برای H سری حل پذیر است.

برای اثبات ب) قرار می دهیم $H_i = \frac{HG_i}{H}$. چون $G_{i-1} \leq G_i$ داریم $HG_{i-1} \leq HG_i$. بنابراین سری زیر نرمال زیر را برای G/H به دست می آوریم:

$$\frac{HG_0}{H} = \{H\} \leq \frac{HG_1}{H} \leq ... \leq \frac{HG_r}{H} = \frac{HG}{H} = \frac{G}{H}$$

حال کافی است نشان دهیم که به ازای هر $1 \leq i \leq r$ عاملهای $\frac{H_i}{H_{i-1}}$ آبلی است. با استفاده از قضیه سوم یکریختی ولم داریم:

$$\frac{H_i}{H_{i-1}} = \frac{\frac{HG_i}{H}}{\frac{HG_{i-1}}{H}} \; ; \; \frac{HG_i}{HG_{i-1}} \; ; \; \frac{G_i}{G_{i-1}(G_i \mathbf{I} H)} \; ; \; \frac{\frac{G_i}{G_{i-1}}}{\frac{G_{i-1}(G_i \mathbf{I} H)}{G_{i-1}}}$$

بدلیل آبلی بودن $\frac{G_i}{G_{i-1}}$ عامل $\frac{H_i}{H_{i-1}}$ نیز آبلی است و حکم ثابت می شود.

قضیه5.3.2. فرض کنید G یک گروه باشد و $H \leq G$. در این صورت اگر H، G/H حلپذیر باشند آنگاه G حلپذیر است.

برهان. فرض کنید H و $\frac{G}{H}$ دارای سریهای حلپذیر زیر باشند.

$$\{e\} = H_0 \leq H_1 \leq ... \leq H_r = H$$

$$\{H\} = \frac{G_0}{H} \leq \frac{G_1}{H} \leq ... \leq \frac{G_t}{H} = \frac{G}{H}$$

اینک سری زیر یک سری حلپذیر برای G است (تحقیق کنید!).

$$\{e\} = H_0 \le H_1 \le \ldots \le H_r = H = G_0 \le G_1 \le \ldots \le G_t = G.$$

نتیجه6.3.2 الف) تصویر همریختی هر گروه حلپذیر، حلپذیر است.

ب) اگر G_1 و G_2 گروه های حلپذیر باشند آنگاه $G = G_1 \times G_2$ حل پذیر است.

برهان الف) فرض کنید Gیک گروه حلپذیر و $f : G \to S$ همریختی باشد. باید نشان دهیم که $f(G)$ حلپذیر است. بااستفاده از قضیه اول یکریختی داریم:

$$\frac{G}{Kerf} \; ; \; f(G)$$

چون $Kerf \le G$، حکم از قسمت دوم قضیه5.3.2 به دست می آید.

ب) داریم $\frac{G}{G_1} \; ; \; G_2$. به دلیل اینکه G_1 و G_2 حل پذیرند،پس G_1 و $\frac{G}{G_1}$ حلپذیر هستند. اینک حکم از قضیه5.3.2 نتیجه می شود

مثال7.3.2. اگر $n \ge 5$ آنگاه A_n و S_n حلپذیر نیستند.

راه حل: فرض کنید A_n حل پذیر باشد. چون به ازای $n \ge 5$ گروه A_nساده است پس $\{e\} < A_n$تنها سری حل پذیر A_n می باشد و در نتیجه A_n آبلی است که تناقض می باشد. به دلیل اینکه $A_n \le S_n$، S_n نیز حلپذیر نیست.

فیت- تامپسون [6] در سال 1936 ثابت کردند که:

"هر گروه متناهی از مرتبه فرد حلپذیر است"

تعریف8.3.2. فرض کنیم G یک گروه باشد. دنباله $\{G^{(n)}\}$ از زیرگروههای G را به استقراء چنین تعریف می‌کنیم:

$$G^{(0)}=G, \quad G^{(n)}=[G^{(n-1)}, G^{(n-1)}] \quad (n \ge 1)$$

به آسانی و به استقراء ثابت می شود که هر G^n یک زیرگروه مشخص G است و در نتیجه به ازای هر n

صحیح نامنفی، $G^{(n)} \leq \mathrm{G}^{(\mathrm{n}-1)}$. مطابق قرارداد، $G^{(1)}$، $G^{(2)}$، $G^{(3)}$ را به ترتیب با G' ، G'' ، G''' نشان می‌دهیم.

تعریف9.3.2 فرض کنیم G یک گروه باشد. سری

$$G \geq G^1 \geq G^2 \geq G^3 \geq \mathbf{L}$$

را سری مشتق G می نامند.

۴.۲ گروه های پوچتوان

تعریف1.4.2. فرض کنید G یک گروه باشد. سری نرمال

$$\{e\} = G_0 \leq G_1 \leq \ldots \leq G_r = G$$

را یک **سری مرکزی** G گوییم هر گاه به ازای هر i که $1 \leq i \leq r$ داشته باشیم

$$\frac{G_i}{G_{i-1}} \leq Z(\frac{G}{G_{i-1}}).$$

گروه G را **پوچتوان** نامیم در صورتی که یک سری مرکزی داشته باشد. طول کوتاه ترین سری مرکز G را **رده پوچتوانی** G نامیم و با $Cl(G)$ نشان می‌دهیم.

مثال ها 2.4.2:

1) فرض کنید $G \neq \{e\}$ یک گروه آبلی باشد. در این صورت G پوچتوان از رده پوچتوانی 1 می باشد (زیرا $G_0 = \{e\} \leq Z(G) = G$ یک سری مرکزی برای G است). وقتی $G = \{e\}$ آنگاه طبق قرارداد رده پوچتوانی G مساوی صفر است.

2) در گروه دو وجهی D_8، قرار می دهیم $a = (1,2,3,4)$ و $G_1 = < a^2 >$ بنابراین $\{e\} < \langle a^2 \rangle < D_8$ یک سری مرکزی D_8 است.یعنی رده پوچتوانی D_8 مساوی2 می باشد.

3) به ازای $n \geq 3$ می دانیم که $Z(S_n) = \{e\}$، اینک داریم

$$G_0 = \{e\}, \quad \frac{G_1}{G_0} \leq (\frac{S_n}{\{e\}}) = Z(S_n) = \{e\} \Rightarrow G_1 = G_0 = \{e\}$$

با ادامه فرآیند $\forall r \geq 2$ داریم $G_r = \{e\}$. یعنی S_n پوچتوان نیست.

تذکر 3.4.2. 1) اگر $G \neq \{e\}$ پوچتوان باشد آنگاه $Z(G) \neq \{e\}$.

2)با توجه به اینکه هر سری مرکزی یک سری نرمال است، پس هر گروه پوچتوان، حلپذیر است. ولی عکس آن برقرار نیست.

3) فرض کنید $A \leq B, A \leq G$. در این صورت $\frac{B}{A} \leq Z(\frac{G}{A})$ اگر و فقط اگر $[B,G] \leq A$. که $[B,G] = \langle [x,y] \mid x \in B, y \in G \rangle$ (ثابت کنید).

به موجب قسمت سوم تذکر قبل، لم زیر به دست می آید.

لم 4.4.2. گروه G پوچتوان است اگر و تنها اگر سری نرمالی مانند

$$\{e\} = G_0 \leq G_1 \leq \ldots \leq G_r = G$$

داشته باشیم که به ازای هر i که $1 \leq i \leq n$، $[G, G_i] \leq G_{i-1}$.

قضیه 5.4.2. فرض کنید G یک گروه پوچتوان از رده r باشد. دراین صورت

1)هر زیر گروه G پوچتوان از رده حداکثر r است.

2) هر تصویر همریخت G پوچتوان از رده حداکثر r است.

برهان 1) فرض کنید $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_r = G$ یک سری مرکزی G باشد و $H \leq G$. قرار می‌دهیم $H_i = G_i \cap H$ پس داریم.

$$\{e\} = H_0 \leq H_1 \leq \ldots \leq H_r = G_r \cap H = G \cap H = H$$

واضح است که $H_i \leq H$. همچنین داریم:

$$[H, H_i] \leq [G, G_i] \leq G_{i-1},\ [H, H_i] \leq G_{i-1} \cap H = H_{i-1}.$$

یعنی سری $\{e\} = H_0 \leq H_1 \leq \ldots \leq H_r = H$ یک سری مرکزی برای H است. پس H پوچتوان است.

2) فرض کنید K یک گروه $q : G \longrightarrow K$ یک همزیختی پوشا باشد. داریم:

$$\{e\} = q(G_0) \leq q(G_1) \leq \ldots \leq q(G_r) = q(G) = K$$

واضح است که سری فوق، یک سری نرمال برای K است (بنا به اینکه q پوشا و $G_i \leq G$ آنگاه $q(G_i) \leq K$). اینک ملاحظه می شود که

$\forall 1 \le i \le r;\ [k, q(G_i)] = [q(G), q(G_i)] = q([G, G_i]) \le q(G_{i-1})$

بنابراین سری فوق، مرکزی و K پوچتوان است.

نتیجه6.4.2. اگر G پوچتوان باشد و $N \le G$ آنگاه $\frac{G}{N}$ پوچتوان است.

برهان. حکم از قسمت دوم قضیه قبل و اینکه $\Pi : \underset{x}{G} \longrightarrow \underset{xN}{G/N}$ همریختی پوشا است، به دست می آید.

قضیه7.4.2. حاصل ضرب مستقیم هر تعداد متناهی از گروه های پوچتوان، پوچتوان است.

برهان. کافی است حکم را برای دو گروه پوچتوان ثابت کنیم.

فرض کنید K, H دو گروه پوچتوان و سریهای

$\{e_1\} = H_0 \le H_1 \le ... \le H_r = H;$

$\{e_2\} = K_0 \le K_1 \le ... \le K_r = K.$

به ترتیب سریهای مرکزی برای K, H باشد (با درج جملات تکراری می توان طول دو سری را یکسان گرفت) حال معلوم است که

$\{e_1\} \times \{e_2\} = H_0 \times K_0 \le H_1 \times K_1 \le ... H_r \times K_r = H \times K$

یک سری مرکزی $K \times H$ است.

تذکر8.4.2. فرض کنید G یک گروه و $H \le G$ به قسمی که H و $\frac{G}{H}$ پوچتوان باشند. در این صورت G لزوما پوچتوان نیست (می دانیم $A_3 \le S_3$ و A_3 و $\frac{S_3}{A_3}$ پوچتوان هستند ولی S_3 پوچتوان نیست) اما قضیه زیر برقرار است:

"اگر G یک گروه باشد و $H \le G$ بقسمی که H و $\frac{G}{H'}$ پوچتوان باشند،آنگاه G پوچتوان است".

تمرینات

1- الف) یک سری نرمال برای D_8 بیابید که از 4 زیرگروه تشکیل شود.

ب) تمام سریهای ترکیبی گروه‌های D_8، A_4 و $S_3 \times Z_3$ را بیابید.

پ) تمام عوامل سریهای ترکیبی D_8، A_4 و S_4 را بیابید.

2- گروه $G = ¢$ در نظر بگیرید.

الف) دو سری نرمال با طول‌های غیرمساوی از G بنویسید؛

ب) دو سری نرمال با طول‌های مساوی از G بنویسید که معادل نباشند؛

ج) دو سری نرمال از G بنویسید که معادل باشند.

3- ثابت کنید که هر گروه متناهی دارای یک سری ترکیب است.

4- ثابت کنید که هر $p-$گروه متناهی از مرتبه p^n دارای یک سری ترکیب از طول n است.

5- ثابت کنید که گروه آبلی G دارای یک سری ترکیب است اگر وفقط اگر G متناهی باشد.

6- گروههای G ، H و $G_1 \leq G$ ، $H_1 \leq H$ را در نظر بگیرید که $H_1 \cong G_1$ و $\frac{G}{G_1} \cong \frac{H}{H_1}$. آیا $G \cong H$؟ ادعای خود را ثابت کنید.

7- نشان دهید اگر G گروهی ناآبلی وساده باشد، انگاه G حل‌پذیر نیست.

8- نشان دهید اگر G گروهی حل‌پذیر وساده باشد، انگاه G متناهی و از مرتبه اول است.

9- سری مشتق گروه G را در نظر بگیرید. نشان دهید:

الف) به‌ازای هر k ، $G^k \leq G$

ب) $\frac{G^k}{G^{k+1}}$ آبلی است.

10- فرض کنید $\{e\} = G_0 \leq G_1 \leq ... \leq G_n = G$ یک سری حلپذیر G باشد.

الف) به استقرا روی i نشان دهید که به‌ازای هر $0 \leq i \leq n$، داریم $G^i \leq G_{n-i}$؛

ب) $G^n = \{e\}$؛

11- الف) نشان دهید گروه G حلپذیر است اگروتنها اگر عدد صحیح نا منفی مانند n موجود باشد به‌طوری که $G^n = \{e\}$.

ب) اگر k کوچکترین عدد صحیح نامنفی باشد که $G^k = \{e\}$. دراین‌صورت k برابر طول حلپذیری G است.

12- فرض کنید G یک گروه باشد که $\frac{G}{Z(G)}$ پوچتوان است، نشان دهید G پوچتوان است. کلاس پوچتوانی G را برحسب کلاس پوچتوانی $\frac{G}{Z(G)}$ بدست آورید.

13- فرض کنید G یک گروه متناهی باشد که $Inn(G)$ آبلی است، نشان دهید G پوچتوان از کلاس حداکثر دو است

14- فرض کنید G یک گروه متناهی باشد که $Aut(G)$ آبلی است، نشان دهید G پوچتوان از کلاس حداکثر دو است.

15- فرض کنید G یک گروه متناهی باشد که $Aut(G)$ پوچتوان است، نشان دهید G پوچتوان است.

فصل سوم حلقه‌های ویژه

در این فصل F همه‌جا نماد میدان است.

1.3 حلقه چندجمله‌ایها

فرض کنید R یک حلقه باشد. قرار می دهیم:

$R[x]=\{(a_0,a_1,...,a_n,...)\,|\,a_i\in R, a_i=0$ {بازای هر i، جز تعداد متناهی

در این صورت $R[x]$ همراه با اعمال $+,\times$ زیر، یک حلقه است.

$$(a_0,a_1,...)+(b_0,b_1,...)=(a_0+b_0,a_1+b_1,...);$$

$$(a_0,a_1,...)\times(b_0,b_1,...)=(c_0,c_1,...)$$

که $C_i=\sum_{k=0}^{i}a_k b_{i-k}$.

واضح است که اگر R حلقه جابجایی و یکدار باشد، آنگاه $R[x]$ نیز حلقه جابجایی و یکدار است که $1_{R[x]}=(1_R,0,0,0,...)$. قرار می‌دهیم $x=(0,1_R,0,0,0,...)$ در این صورت $x^n=(0,0,...,0,1_R,0,0,...)$ که 1_R مولفه $(n+1)$–ام است. همچنین به ازای هر $r\in R$ و به ازای هر $n\geq 0$، $rx^n=(0,0,...0,r,0,0,...)$ که در آن مولفه $(n+1)$–ام مساوی r است.

بامفاهیم بالا، فرض کنید $f=(a_0,a_1,...,a_n,0,0,...)\in R[x]$ دراین‌صورت داریم: $f=a_0x^0+a_1x+...+a_nx^n$ و اگر R یکدار باشد $x^0=1_R$ و $f=a_0+a_1x+...+a_nx^n$.

بحث قبل روشی بود برای ساختن حلقه چند جمله ایهای $R[x]$ روی R. دراینجا حلقه چند جمله ایهای $R[x]$ روی R را به روش آشنای زیر تعریف می کنیم.

فرض کنید R یک حلقه باشد و x یک مجهول در این صورت قرار می‌دهیم:

$$R[x]=\left\{a_0+a_1x+...+a_nx^n\,|\,n\in \mathbb{N}\cup\{0\};\ a_0,a_1,\mathbf{L},a_n\in R\right\}.$$

اعمال جمع و ضرب را در آن به‌صورت زیر تعریف می‌کنیم:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$(\sum_{i=0}^{n} a_i x^i)(\sum_{i=0}^{m} b_i x^i) = \sum_{i=0}^{m+n} c_i x^i,$$

که $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

هرگاه $f(x) = a_0 + a_1 x + ... + a_n x^n \in R[x]$ که $a_n \neq 0$. در این صورت n را درجه $f(x)$ می نامیم (می نویسیم $\deg f(x) = n$) و a_n را ضریب پیشرو $f(x)$. اگر R حلقه یکدار باشد و $a_n = 1$ آنگاه $f(x)$ را چند جمله‌ایی تکین گوییم.

لازم به ذکراست که اگر x_1 و x_2 دو مجهول باشند. حلقه چند جمله‌ایهای دو متغیره $R[x_1, x_2]$ را به صورت زیر تعریف می کنیم.

$$R[x_1, x_2] = (R[x_1])[x_2]$$

و این تعریف را می توان (با استفاده از استقرا) برای هر $n \in \mathbb{N}$، تعمیم داد.

نکته. با توجه به تعریف، درجه برای هر چند جمله ای ثابت ناصفر مساوی صفر است، ولی مفهوم درجه برای چند جمله ایی صفر، تعریف نشده است. هر چند در برخی منابع درجه چند جمله‌ایی صفر، برابر $-\infty$ تعریف می شود.

با استفاده از مفاهیم بالا قضیه زیر به سادگی ثابت می‌شود.

قضیه1.1.3. فرض کنید R یک حلقه باشد و $f, g \in R[x]$ که $f + g, fg \neq 0$ در این صورت

الف) $\deg(f + g) \leq \max\{\deg f, \deg g\}$

ب) $\deg(fg) \leq \deg f + \deg g$

مثال 2.1.3. فرض کنید $f = 3 + x^2 + 2x^3 \in Z_4[x]$ و $g = 2 + 2x^3$. مطلوبست محاسبه

$f + g, fg, g^2$

راه حل. داریم:

$$.f+g=1+x^2, fg=2+2x^2+2x^3+2x^5,\ g^2=0$$

نتیجه3.1.3. اگر D دامنه صحیح باشد و $g\in D[x]$, $f\neq 0$ دراین صورت

الف) $D[x]$ دامنه صحیح است.

ب) $\deg(fg)=\deg f+\deg g$.

برهان. فرض کنید a_n و b_m ضریب پیشرو $D[x]$ (به ترتیب) باشند در این صورت حکم با توجه به اینکه $a_nb_m\neq 0$ به دست می آید.

مثال4.1.3. چند جمله ایی $3x_1^2x_2^2x_3^2+3x_1^3x_2^4-6x_2^3x_3\in \mathbb{C}[x_1,x_2,x_3]$ را در نظر بگیرید. در این صورت درجه آن نسبت به x_1 مساوی 3، نسبت به x_2 مساوی 4 و نسبت به x_3 مساوی 2 است. همچنین درجه کل آن مساوی 7 می باشد.

قضیه5.1.3 (الگوریتم تقسیم). فرض کنید R حلقد یکدار بوده و $g(x)\in R[x]$ و $f(x)$ چند جمله ایهای باشند به قسمی که ضریب پیشرو $g(x)$ در R وارون پذیر باشد. در این صورت چند جمله ایهای منحصر به فردی مانند $q(x)\in R[x]$ و $r(x)$ وجود دارند که

$r(x)=0$ یا $\deg r(x)<\deg g(x)$ و $f(x)=q(x)g(x)+r(x)$.

برهان. ابتدا وجود $q(x)$و $r(x)$ را نشان می دهیم.

اگر $f(x)=0$ یا $f(x)\neq 0$ و $\deg f(x)<\deg g(x)$ قرار می دهیم:

$$f(x)=0\times g(x)+f(x)$$

لذا حکم برقرار است.

حال فرض کنید $f(x)\neq 0$ و $\deg f(x)\geq \deg g(x)$. حکم را به روش استقرار روی $\deg f(x)$ اثبات می کنیم.

اگر $\deg f(x)=0$آنگاه $\deg g(x)=0$. پس $f(x)$ و $g(x)$ هر دو ثابت هستند. فرض کنید $f(x)=a$ و $g(x)=b$. قرار می دهیم.

$$a=f(x)=(ab^{-1})g(x)+0$$

و لذا مساله حل می شود(توجه شود بنا به فرض b^{-1} وجوددارد).

حال فرض کنید حکم برای تمام چند جمله ایها از درجه کمتر از n برقرار باشد و $f(x)$ چند جمله ایی باشد که $\deg f(x) = n$. همچنین فرض کنید

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n,\ a_n \neq 0$$
$$g(x) = b_0 + b_1 x + \ldots + b_m x^m,\quad b_m \neq 0,\quad n \geq m.$$

چند جمله ای $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ را در نظر می گیریم. واضح است که $h(x) = 0$ یا $\deg h(x) < \deg f(x) = n$.

اگر $h(x) = 0$ آنگاه $f(x) = a_n b_m^{-1} x^{n-m} g(x) + 0$ و شرایط برقرار است. در غیر از این صورت بنا به فرض استقرا چند جمله ایهای $r(x)$ و $s(x)$ وجود دارند به قسمی که

$$h(x) = s(x)g(x) + r(x)$$

که $r(x) = 0$ یا $\deg r(x) < \deg g(x)$. در نتیجه داریم:

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + h(x) \\ &= a_n b_m^{-1} x^{n-m} g(x) + s(x) g(x) + r(x) \\ &= (a_n b_m^{-1} x^{n-m} + s(x)) g(x) + r(x) \end{aligned}$$

و شرایط برقرار است.

برای منحصر بفرد بودن $r(x)$ و $g(x)$، فرض کنید

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

و شرایط حکم برقرار باشد. در این صورت داریم:

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$$

اگر $q_1(x) \neq q_2(x)$ آنگاه $r_1(x) \neq r_2(x)$ (زیرا ضریب پیشرو $g(x)$ وارون پذیر است). داریم

$$\deg(r_2(x) - r_1(x)) = \deg(q_1(x) - q_2(x)) + \deg g(x) \geq \deg g(x)$$

که تناقض است. پس $q_1(x) = q_2(x)$ و در نتیجه $r_1(x) = r_2(x)$ و قضیه ثابت می شود.

چند جمله ایها $q(x),\ r(x)$ در قضیه قبل را به ترتیب خارج قسمت و باقی مانده تقسیم $f(x)$ بر $g(x)$ می‌نامیم. گوییم $g(x)$ چند جمله ایی $f(x)$ را در $R(x)$ عاد می کند (بخش می کند) هرگاه $r(x) = 0$ می نویسیم $g(x) \mid f(x)$.

نتیجه6.1.3. فرض کنید R حلقه یکدار و $f(x)=\sum_{i=0}^{n} a_i x^i \in R[x]$. در این صورت به ازای هر $c\in R$ وجود دارد $q(x)\in R[x]$ منحصر بفرد بقسمی که

$$f(x)=(x-c)q(x)+f(c)$$

برهان. بنا به قضیه قبل چندجمله ایهای منحصر بفرد $q(x), r(x)$ وجود دارند، بقسمی که

$$f(x)=(x-c)q(x)+r(x),\ \deg r(x)<1,\ r(x)=0$$

پس $f(x)=(x-c)q(x)+d$ که d عددی ثابت است. حال $d=f(c)$ و حکم برقرار است.

2.3 تجزیه چندجمله‌ایها

از این به بعد فرض کنید F یک میدان باشد و به بررسی خواص $F[x]$ می پردازیم.

تعریف 1.2.3. فرض کنید E یک میدان و F زیر میدان E باشد. اگر $f(x)\in F[x]$ آنگاه $c\in E$ را یک ریشه f نامیم هر گاه

$$f(c)=0$$

نتیجه 2.2.3. فرض کنید F یک میدان باشد و $f(x)\in F[x]$. در این صورت $c\in F$ یک ریشه $f(x)$ است اگر و فقط اگر $x-a \mid f(x)$.

برهان. بنا به نتیجه داریم:

$$f(x)=(x-c)q(x)+f(c)$$

پس $x-c \mid f(x) \Leftrightarrow f(c)=0$.

نتیجه 3.2.3. فرض کنید F یک میدان باشد و $f(x)\in F[x]$.اگر $\deg f(x)=n$آنگاه تعداد ریشه های متمایز $f(x)$ حداکثر مساوی nاست.

برهان. اثبات به استقرا روی n. اگر $n=1$ آنگاه $f(x)=ax+b$ که $a\neq 0$. لذا $x=-ba^{-1}$ تنها ریشه $f(x)$ است. فرض کنید حکم برای هر چند جمله ایی از درجه $n-1$ برقرار باشد و $\deg f(x)=n>1$. اگر $f(x)$ در F ریشه نداشته باشد حکم برقرار است. فرض کنید a یک ریشه $f(x)$ باشد در این صورت $f(x)=(x-a)g(x)$ و $\deg g(x)\leq n-1$ و بنا به فرض استقرا تعداد ریشه های $g(x)$ حداکثر $n-1$ است.

نتیجه4.2.3. فرض کنید F میدان نامتناهی باشد $f(x),g(x)\in F[x]$ بقسمی که به ازای زیر مجموعه نامتناهی S و هر $a\in S$ داشته باشیم $f(a)=g(a)$ آنگاه $f=g$.

مثال5.2.3 .الف)چند جمله‌ایی $f(x)=2x+2x^2$ روی Z_4 دارای چهار ریشه متمایز است.

ب)حلقه چهارگانه و چند جمله ایی $f(x)=x^2+1$ را در نظر بگیرید. حداقل عناصر k,j,i ریشه‌های آن هستند (این چند جمله نامتناهی ریشه دارد)

نکته6.2.3. توجه شود که نتایج این بخش برای هر دامنه صحیح D نیز برقرار است.

تعریف 7.2.3. فرض کنید $f(x)\in F[x]$ یک چند جمله ایی غیر ثابت باشد. در این صورت $f(x)$ را تحویل ناپذیر (یا تجزیه ناپذیر) گوییم هرگاه $f=gh$ آنگاه $g=f$ یا $h=f$.

به عبارت دیگر $f(x)$ را تحویل ناپذیر گوییم هرگاه $f(x)$ را نتوان به حاصلضرب دو چند جمله ایی با درجه کمتر از درجه $f(x)$ تجزیه کرد. واضح است که اگر $\deg f(x)\leq 3$آنگاه $f(x)$ روی Fتحویل ناپذیر است اگر و فقط اگر در F ریشه نداشته باشد.

قضیه زیر نشان می دهد $f(x)\in ¤[x]$ در ¤ تحویل‌پذیر است اگر و فقط $f(x)$ در ¢ تحویل پذیرباشد. مثال زیر را در نظر بگیرید:

$$f(x)=9x^3+18x^2+4x+8=(\frac{3}{2}x+3)(6x^2+\frac{8}{3})=\frac{1}{2}(3x+6)\times\frac{1}{3}(18x^2+8)$$
$$=\frac{1}{6}[3(x+2)][2(9x^2+4)]=\frac{1}{6}\times 6(x+2)(9x^2+4)]=(x+2)(9x^2+4).$$

قضیه 8.2.3. فرض کنید $f(x)\in \mathbb{C}[x]$ چند جمله ای غیرثابت باشد. در این صورت $f(x)$ در $\mathbb{R}[x]$ به حاصلضرب دو چند جمله ایی g,h تجزیه‌پذیر است اگر و فقط اگر $f(x)$ در $\mathbb{C}[x]$ به حاصلضرب دو چند جمله ای با درجه g,h تجزیه پذیر باشد.

برهان. ($\Rightarrow$)حکم بدیهی است. زیرا $\mathbb{R}[x]\subseteq\mathbb{C}[x]$. فرض کنید $f=gh$ که در آن g و $h\in\mathbb{R}[x]$ و $\deg f,\deg g>0$. فرض کنید d',d (به ترتیب) کوچکترین مضرب مشترک، مخرج‌های ضرایب ناصفر h,g باشند. پس $dd'f=(dg)(d'h)$. اکنون فرض کنید g,b,a (به ترتیب) بزرگترین مقسوم مشترک ضرایب ناصفر $f,d'h$ باشند. در این صورت $dd'gf^*=abg^*h^*$ که در آن $g^*,h^*\in\mathbb{C}[x]$ و بزرگترین مقسوم علیه مشترک ضرایب f^*,h^*,g^* برابر یک است. می توان نشان داد که $ab=dd'g$. بنابراین

$$dd'f=abg^*h^*=dd'gg^*h^*\Rightarrow f=gg^*h^*$$

و حکم برقرار است.

قضیه 9.2.3. (محک آبزنشتاین). فرض کنید $f(x)=a_0+a_1x+\ldots+a_nx^n\in\mathbb{C}[x]$. اگر p عدد اولی باشد که

$$p\mid a_0,\mathbf{L}\ p\mid a_1,\ldots,p\mid a_{n-1};\ p\nmid a_n,p^2\nmid a_0$$

آنگاه $f(x)$ در $\mathbb{R}[x]$ تحویل ناپذیر است.

برهان. واضح است که $\deg f(x)>0$. با توجه به قضیه کافی است نشان دهیم که $f(x)$ در $\mathbb{C}[x]$ تحویل ناپذیر است. به برهان خلف فرض کنید $f(x)=g(x)h(x)$ که $g(x),h(x)\in\mathbb{C}[x]$ غیر ثابت هستند. قرار می دهیم:

$$g(x)=b_0+b_1x+\ldots+b_sx^s$$
$$h(x)=C_0+C_1x+\ldots+C_tx^t$$

که در آن $1<s,t<n$. بنابراین $a_0=b_0c_0$ و p فقط یکی از دو عضو c_0 یا b_0 را عاد می کند. (زیرا $p^2\nmid a_0,p\mid a_0$). فرض کنید $p\mid b_0$ و $p\nmid c_0$. به دلیل اینکه $a_n=b_sc_t$، واضح است که $p\nmid b_s$. فرض کنید k کوچکترین اندیسی باشد که $p\nmid b_k$. چون $p\mid b_0$ و $p\nmid b_s$ پس

$0 < k \le s < n$. حال ضریب

$$a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0$$

را در نظر می گیریم. با توجه به انتخاب k و بنا به فرض داریم:

$$p \mid a_k - (b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1) = b_k c_0$$

که تناقض است (زیرا $p \nmid b_k, c_0$).

نتیجه10.2.3. فرض کنید $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in ¢[x]$ و p عددی اول باشد. که $P \nmid a_n$ قرار می دهیم:

$$\overline{f}(x) = \overline{a}_0 + \overline{a_1} x + \ldots + \overline{a_n} x^n$$

که $\overline{a_i} = a_i (mod\ p)$. در این صورت اگر $\overline{f}(x)$ در $Z_p[x]$ تحویل ناپذیر باشد آنگاه $f(x)$ در ¤$[x]$ تحویل ناپذیر است.

برهان. فرض کنید $f(x) = g(x)h(x)$ پس $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ و حکم ثابت می‌شود زیرا $p \nmid a_n$

تذکر11.2.3. فرض کنید $f(x) \in ¢[x]$ در این صورت $f(x) = g(x)h(x)$ اگر و تنها اگر به ازای هر $a \in ¢$ داشته باشیم:

$$f(x+a) = g(x+a)h(x+a)$$

مثال 12.2.3. نشان دهید که به ازای هر عدد اول p، $f(x) = x^{P-1} + x^{P-2} + \ldots + x^2 + x + 1$ تحویل ناپذیر است.

راه حل داریم:

$$f(x) = \frac{x^P - 1}{x - 1} = x^{P-1} + x^{P-2} + \ldots + x^2 + x + 1$$

و

$$f(x+1) = \frac{(x+1)^P - 1}{x} = x^{P-1} + \binom{p}{1} x^{P-2} + \ldots + p$$

چون به ازای هر $1 \le i \le p$، $p \mid \binom{p}{i}$ حکم از تذکر قبل و لم آیزنشتاین به دست می آید.

مثال 13.2.3. نشان دهید که $f(x)=8x^3+x^2+7x+22$ روی $\mathbb{Q}$ تحویل ناپذیر است.

راه حل. به ازای $p=5$ داریم $\overline{f}(x)=3x^3+x^2+2x+2$ حال اگر $\overline{f}(x)$ در $Z_5[x]$ تحویل پذیر باشد باید در Z_5 ریشه داشته باشد. ولی

$$\overline{f}(0)=2, \overline{f}(1)=3, \overline{f}(2)=4, \overline{f}(3)=3, \overline{f}(4)=3$$

یعنی $\overline{f}(x)$ در Z_5 ریشه ندارد و بنابراین $\overline{f}(x)$ در $Z_5[x]$ (در نتیجه در $\mathbb{Q}[x]$) تحویل ناپذیر دارد.

به عنوان تمرین نشان دهید که $f(x)=\dfrac{x^{p^2}-1}{x^p-1}$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

مثال 14.2.3. $f(x)=x^4+1$ را در نظر می گیریم. داریم

$$f(x+1)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$$

و با انتخاب $p=2$ و استفاده از لم آیزنشتاین $f(x)$ تحویل ناپذیر است.

3.3.ایده ال‌های $F[x]$.

تعریف1.3.3. فرض کنید R یک حلقه حابجایی و یکدار باشد و $a\in R$ در این صورت $<a>=\{ra \mid r\in R\}$ را یک ایده آل اصلی نامیم. دامنه صحیح D را $P.I.D$ (دامنه با ایده آل اصلی) نامیم هرگاه هر ایده آل آن اصلی باشد.

مثال 1-2.3.3) اگر F میدان باشد. آنگاه F یک $P.I.D$ است. زیرا $\{0\}$ و F تنها ایده آل های F هستند و داریم $F=<1>, \{0\}=<0>$.

2) چون هر ایده آل $\mathbb{C}$ به صورت $n\mathbb{C}$ است که $n\in\mathbb{C}$، $\mathbb{C}$ یک $P.I.D$ است.

قضیه3.3.3. اگر F میدان باشد آنگاه $F[x]$ یک $P.I.D$ است.

برهان. فرض کنید $I\leq F[x]$. اگر $I=\{0\}$ پس $I=<0>$ و حکم برقرار است. فرض کنید $0\neq g(x)\in I$ قرار می دهیم:

$$S=\{\deg f_1(x) \mid f_1(x)\in I,\ f_1(x)\neq 0\}$$

پس $f \neq S \subseteq \mathbf{¥U}\{0\},\ \deg g(x) \in S$ و $n = \min S$. به موجب اصل خوش ترتیبی فرض کنید $f(x) \in I$ چند جمله ایی باشد که $\deg f(x) = n$ نشان می دهیم:

$$I = < f(x) > = \{q(x) f(x) \mid q(x) \in F[x]\}$$

واضح است که $< f(x) > \subseteq I$ (زیرا $f(x) \in I$). فرض کنید $h(x) \in I$.

بنا بر قضیه الگوریتم تقسیم

$$h(x) = q_1(x) f(x) + r(x)$$

$$0 \leq \deg r(x) < n = \deg f(x) \text{ یا } r(x) = 0$$

حال $r(x) = h(x)_{\in I} - q_1(x) f(x)_{\in I} \in I$ و این تناقض است با اینکه $n = \min(S)$، زیرا $0 \leq \deg r(x) < n$. پس $r(x) = 0$ و $h(x) = q_1 f(x) \in < f(x) >$.

قضیه زیرا شرایط ایده ال ماکزیمال را در $F[x]$ مشخص می کند.

قضیه 4.3.3. فرض کنید F میدان باشد. در این صورت ایده آل $M = < f(x) >$ ماکزیمال است اگر و تنها اگر $f(x)$ تحویل ناپذیر باشد.

برهان. فرض کنید $M = < f(x) >$. چون $< 0 > \subsetneq < x > \subsetneq F[x]$ پس $F[x]$ میدان نیست و داریم $< 0 > \subsetneq < f(x) > \subsetneq F[x]$. پس $f(x)$ غیرثابت است. حال فرض کنید $f(x) = g(x)h(x)$. بنابراین داریم

$$< f(x) > \subseteq < g(x) > \subseteq F[x]$$

چون $< f(x) >$ ماکزیمال است پس $< f(x) > = < g(x) >$ یا $< g(x) > = F[x]$ اگر $< f(x) > = < g(x) >$ آنگاه داریم:

$$g(x) = f(x)h_1(x) \Rightarrow f(x) = f(x)h_1(x)h(x) \Rightarrow h_1(x)h(x) = 1$$

یعنی $h(x)$ واحد است پس $f(x)$ تحویل ناپذیر است.

اگر $< g(x) > = F[x]$ پس $g(x)$ واحد است یعنی $f(x)$ تحویل ناپذیر است.

بعکس. فرض کنید $f(x)$ تحویل ناپذیر باشد و $< f(x) > \subseteq N \subseteq F[x]$. چون $< f(x) > \subseteq N = < q(x) > \subseteq F[x]$. پس $f(x) = q(x)t(x)$. بنابراین $q(x) = f(x)$ یا $t(x) = f(x)$. در نتیجه $N = < f(x) >$ یا $N = F[x]$.

مثال 5.3.3-1) x^2-3 در $\mathbb{Q}[x]$ تحویل ناپذیر است. پس $<x^2-3>$ در $\mathbb{Q}[x]$ ماکزیمال و در نتیجه $\frac{\mathbb{Q}[x]}{<x^2-3>}$ میدان است.

2) x^2+x+1 در Z_2 تحویل ناپذیر است پس

$$\frac{Z_2[x]}{<x^2+x+1>}=\{a+bx \mid a,b\in Z_2\}$$

میدان 4 عضوی است.

3) چون x^2+1 در Z_{11} تحویل ناپذیر است. آنگاه

$$\frac{Z_{11}[x]}{<x^2+1>}=\{a+bx \mid a,b\in Z_{11}\}$$

میدان 121 عضوی است.

4) $<x^2+1>$ در $\mathbb{Z}[x]$ ماکزیمال است ولی در $\mathbb{Q}[x]$ ماکزیمال نیست.

قضیه 6.3.3. فرض کنید $p(x)\in F[x]$ تحویل ناپذیر باشد و $p(x)\mid r_1(x)r_2(x)$. در این صورت $p(x)\mid r_1(x)$ یا $p(x)\mid r_2(x)$.

برهان. چون $p(x)$ تحویل ناپذیر است، $<p(x)>$ ماکزیمال و در نتیجه اول است. اکنون داریم $r_1(x)r_2(x)\in<p(x)>$. بنابراین $r_1(x)\in<p(x)>$ یا $r_2(x)\in<p(x)>$ و درنتیجه حکم برقرار است.

واضح است که قضیه فوق به ازای $n\geq 3$ نیز قابل تعمیم است.

قضیه 7.3.3. (تجزیه چند جمله ایها). فرض کنید F یک میدان باشد. آنگاه هر چند جمله ایی غیرثابت در $F[x]$ تحویل ناپذیراست یا آن را می توان به حاصلضرب عوامل تحویل ناپذیر تجزیه کرد که این تجزیه در حد ترتیب منحصربفرد است.

برهان. **فرض کنید** $f(x)$ یک چند جمله‌ای از درجه‌ی $n\geq 1$ باشد. اگر $f(x)$ تحویل ناپذیر باشد، حکم برقرار است. در غیراین‌صورت، **فرض کنید** $f(x)=g(x)h(x)$ که $1\leq \deg g(x), \deg h(x)<n$ و $\deg g(x)+\deg h(x)=n$ حال اگر $g(x)$ و $h(x)$ تحویل ناپذیر باشد که حکم برقرار است. در غیراین‌صورت با ادامه فرآیند داریم $f(x)=p_1(x)\,p_2(x)\ldots p_k(x)$

که $p_i(x)$ تحویل ناپذیر است. برای منحصربفرد بودن: **فرض کنید** $f(x)=p_1(x)p_2(x)...p_k(x)=q_1(x)q_2(x)...q_r(x)$ **دو** تجزیه $f(x)$ به تحویل ناپذیرباشند. بدلیل این‌که $p_i(x)\mid f(x)$، وجود دارد $q_j(x)$ بقسمی که $p_i(x)=u_jq_j(x)$ و $0\neq u_j\in F$. اکنون با قرار دادن $u_jq_j(x)$ به جا ی $p_i(x)$ و خذف $q_j(x)$ داریم:

$$1=u_1u_2...u_kq_{k+1}(x)...q_r(x)$$

واضح است که این وقتی امکان دارد که $k=r$.

تعریف 8.3.3. فرض کنید D یک دامنه صحیح باشد و $a,b\in D$. گوییم b بر a در D **بخشپذیر** است (می نویسیم $a\mid b$) هر گاه

$$\exists c\in D;\ b=ac.$$

همچنین گوییم b وابسته a است هر گاه عضو واحد $u\in D$ وجود داشته باشد بقسمی که $b=ua$.

اثبات قضیه زیر به دانشجویان واگذار می شود.

قضیه9.3.3. فرض کنید $a,b,c\in D$ دراین صورت

1) $a\mid a$

2) اگر $a\mid b$ و $b\mid c$ آنگاه $a\mid c$

3) اگر $a\mid b$و $b\mid c$ آنگاه aوابسته bاست.

4) رابطه وابسته بودن در D یک رابطه هم ارزی است.

5) اگر $a\mid b$و $x\in D$ آنگاه $a\mid bx$.

6) اگر $a\mid b$ و $a\mid c$آنگاه $a\mid(b-c)$.

تعریف10.3.3. فرض کنید $a,b\in D$در این صورت

الف) $d\in D$را بزرگترین مقسوم علیه مشترک aو b نامیم (می نویسیم $d=(a,b)$)هرگاه

1) $a\mid b$ و $d\mid b$.

2)اگر $c\in D$و $c\mid a$و $c\mid b$آنگاه $c\mid d$.

ب) $m \in D$ را یک کوچکترین مضرب مشترک a و b در D نامیم(می نویسیم $m=[a,b]$) هرگاه:

1) $a,b \mid m$

2) اگر $a,b \mid l$ آنگاه $m \mid l$.

واضح است که بزرگترین مقسوم علیه مشترک و کوچکترین مضرب مشترک لزوما منحصر بفرد نیست ولی در حد وابسته بودن منحصر بفرد است.

تعریف11.3.3. فرض کنید D یک دامنه صحیح باشد و $p \in D$ عضوی غیرصفر و غیرواحد در این صورت

الف) p را تحویل ناپذیر گوئیم هر گاه $p=ab$ که $a,b \in D$ آنگاه a یا b واحد است.

ب) عضو p را اول گوییم هر گاه به ازای هر $a,b \in D$ که $p \mid ab$ آنگاه $p \mid a$ یا $p \mid b$.

مثال12.3.3. $f(x)=2x+4$ در $[x]$ ¤ تحویل ناپذیر است ولی در $[x]$ ¢ تحویل‌پذیر.

لم 13.3.3. در هر دامنه صحیح D، هر عضو اول تحویل ناپذیر است.

برهان. فرض کنید $p \in D$ اول باشد. نشان می دهیم که p در D تحویل ناپذیر است. فرض کنید $p=ab$. چون $p \mid ab$ و p اول است، $p \mid a$ یا $p \mid b$. فرض کنید $p \mid a$ آنگاه وجود دارد $a \in D$ بقسمی که $a=pa_1$ بنابراین

$$p=ab=pa_1b \xrightarrow[p\neq 0]{} a_1b=1$$

پس b واحد و p تحویل ناپذیر است.

4.3 حلقه های اقلیدسی($E.D$)

تعریف زیر در واقع تعمیم قضیه الگوریتم تقسیم به دامنه صحیح D است.

تعریف 1.4.3. فرض کنید D یک دامنه صحیح باشد و $D^*=D-\{0\}$. تابع $s: D^* \to$ ¢ را یک ارزیاب اقلیدسی روی D می‌نامیم، هر گاه

1) به ازای هر $a \in D^*$، $s(a) \geq 0$؛

2) به ازای هر $a, b \in D^*$، $s(ab) \geq s(b)$.

3) به ازای هر $a \in D$ و $b \in D^*$، وجود دارند $r, q \in D$ بقسمی که

$$a = bq + r; \quad r = 0 \text{ یا } s(r) < s(b)$$

اگر s یک ارزیاب اقلیدسی روی D باشد آنگاه (D, s) را یک **دامنه اقلیدسی** نامیم و بـه اختصـار با ED نشان می‌دهیم.

مثال2.4.3-1. تابع $s : \mathbb{C}^* \longrightarrow \mathbb{C}$, $n \longrightarrow |n|$ باشد یک ارزیاب اقلیدسی روی $\mathbb{C}$ است. زیرا

i) $\forall n \in \mathbb{C}^*; \quad s(n) = |n| \geq 0$

ii) $\forall m, n \in \mathbb{C}^*; \quad s(mn) = |mn| = |m||n| \geq |n| = s(n)$

iii) به ازای $m \in \mathbb{C}$; $n \in \mathbb{C}^*$ بنا به الگوریتم تقسیم داریم:

$$\exists r, q \; s.t. \quad m = nq + r; \; r = 0 \text{ یا } |r| < |n|$$

بنابراین $r = 0$ یا $s(r) < s(n)$. پس $(\mathbb{C}, s)$ یک دامنه اقلیدسی است.

2- بااستفاده از الگوریتم تقسیم در $F[x]$، تابع $s : F[x] \longrightarrow \mathbb{C}$, $f(x) \longrightarrow \deg f(x)$ یک ارزیاب اقلیدسی است. بنابراین $(F[x], s)$ یک دامنه اقلیدسی است.

3- اگر F میدان باشد آنگاه تابع $s(f(x)) = 2\deg f(x)$ یک ارزیاب اقلیدسی است.

مشابه قضیه 3.3.3 می‌توان نشان داد که هر $E.D$ یک $P.I.D$ است.

تمرینات

1- باقی‌مانده تقسیم چندجمله‌ایی $x^3 + 3x^2 + 4$ را بر $3x + 2$ در Z_5 بدست آورید.

2- کدامیک از حلقه های زیر میدان است:

الف) $\dfrac{Z_5[x]}{< x^2 - 2 >}$ ب) $\dfrac{Z_7[x]}{< x^2 - 2 >}$ ج) $\dfrac{\mathbb{Q}[x]}{< x^4 + x^3 + x^2 + x + 1 >}$ د) $\dfrac{F[x]}{< x >}$.

3- کوچکترین زیر میدان (در حد یکریختی) را در میدانهای زیر مشخص کنید.

الف) $\mathbb{F}$ ب) $\frac{\mathbb{Z}[x]}{<x^2+1>}$ ج) $\frac{Z_{11}[x]}{<x^2+1>}$ د) یک میدان 81 عضوی

4-حلقه $F[x]$ وچند جمله‌ایهای $f(x), g(x) \in R[x]$ را در نظر بگیرید. نشان دهید که گزاره‌های زیر معادلند:

الف) $f(x)$ و $g(x)$ وابسته‌اند.

ب) $<f(x)>=<g(x)>$.

ج) $f(x)|g(x)$ و $g(x)|f(x)$.

5- حلقه $F[x]$ را در نظر بگیرید. نشان دهید

الف) تعدادعناصر تحویل‌ناپذیر آن نامتناهی است.

ب) تعداد ایده‌الهای اول آن نامتناهی است.

5- اگر عدد گویای $\frac{r}{s}$ (که $(r,s)=1$) ریشه چندجمله‌ایی گویای

$$f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

باشد، آنگاه $r|a_0$ و $s|a_n$.

6-کدامیک از چندجمله‌ایهای زیر در میدان‌های داده شده تحویل‌ناپذیر است.

الف) x^3+3x+2 در $\mathbb{Q}[x]$ ؛

ب) $3x^3+2x^2-1$ در $\mathbb{Q}[x]$ ؛ در $\mathbb{C}[x]$ چطور؟

ج) x^4-5x^2+x+1 در $\mathbb{Q}[x]$ ؛

د) $x^6+x^4+x^2+1$ در $\mathbb{Z}[x]$ ؛

ه) $x^5+x^4+x^3+x^2+x+1$ در $\mathbb{Q}[x]$.

7- نشان دهید که به‌ازای $n \in \mathbb{N}$، چندجمله‌ایی $f(x)=x^{n-1}+x^{n-2}+\mathbf{L}+x+1$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است

اگر و فقطاگر n عددی اول باشد.

8- نشان دهید که به‌ازای $n \in \mathbb{N}$،چندجمله‌ایی $f(x)=(x-1)(x-2)\mathbf{L}(x-n)-1$ در $\mathbb{Q}[x]$ تحویل ناپذیر است

فصل چهارم توسیع میدان وکاربرد آن

1.4 بیان مفاهیم مقدماتی

تعریف 1.1.4. فرض کنید E و F دو میدان باشند. در این صورت E را یک توسیع F نامیم، هرگاه همریختی یکبیکی مانند $s : F \to E$ وجود داشته باشد.

با توجه به تعریف توسیع میدان واضح است که $s(F) \leq E$; F. به طور معادل داریم که E یک توسیع Fاست هر گاه F زیر میدان E باشد.

اگر E یک توسیع F باشد می نویسیم $F \leq E$. مثلا ¡ ≤ ¤□ £ ≤ ¡ و £ ≤ ¤ . واضح است که اگر E یک توسیع Fباشد آنگاه $1_F = 1_E$.

مثال 2.1.4. فرض کنید $p(x)$ یک چند جمله ایی تحویل ناپذیر روی میدان F باشد در این صورت $\frac{F(x)}{< p(x) >}$ یک میدان است. اینک تابع $s : F \longrightarrow \frac{F(x)}{< p(x) >}$ با ضابطه

$$s(a) = a + < P(x) >$$

یک همریختی است. زیرا

$$s(ab) = ab + < p(x) > = (a + < p(x) >)(b + < p(x) >) = s(a)s(b)$$
$$s(a+b) = s(a) + s(b).$$

حال فرض کنید $s(a) = 0 = < P(x) >$ پس داریم:

$$a + < p(x) > = < p(x) > \Rightarrow a \in < p(x) > \Rightarrow p(x) | a \Rightarrow a = 0$$

یعنی s همریختی یکبیک و در نتیجه $\frac{F(x)}{< p(x) >}$ یک توسیع میدان F است.

قضیه 3.1.4. (کرونکر) فرض کنید $f(x)$ یک چند جمله ایی غیرثابت روی میدان F باشد. در این صورت توسیعی چون K از F و $a \in K$ وجود دارد که $f(a)=0$.

برهان. اگر $f(x)$ در F ریشه داشته باشد، قرار می‌دهیم $K=F$. در غیراین صورت فرض کنید $p(x)=a_0+a_1x+...+a_nx^n$ ، یک عامل تحویل ناپذیر $f(x)$ باشد. بنا به مثال 2.1.4 $K=\frac{F(x)}{<p(x)>}$ یک توسیع میدان F است و $s(p(x))=\bar{p}(x)=\bar{a}_0+\bar{a}_1x+...+\bar{a}_nx^n$ که به ازای هر $0\le i\le n$، $\bar{a}_i=a_i+<p(x)>$. اینک نشان می دهیم $a=x+<p(x)>$ یک ریشه $\bar{p}(x)$ است. داریم:

$$\bar{p}(x+<p(x)>)=a_0+<p(x)>+(a_1+<p(x)>)(x+>p(x)>)+...+(a_n+<p(x)>)$$
$$+(x+<p(x)>)^n=a_0+a_1x+...+a_nx^n+<p(x)>=<p(x)>=0_K$$

بنابراین $\bar{p}(a)=s(p(a))=0_K$. چون s یکبیک است، $p(a)=0$ و در نتیجه $f(a)=0$.

مثال 4.1.4. چند جمله ایی $p(x)=x^2+x+1$ در $Z_2[x]$ تحویل ناپذیر است. بنابراین

$$K=\frac{Z_2[x]}{<p(x)>}=\{<p(x)>+a_0+a_1x+...+a_nx^n \mid a_i\in Z_2\}$$
$$=\{<p(x)>+b_0+b_1x \mid b_0,b_1\in Z_2\}.$$

حال $s:Z_2\longrightarrow K$ و $s(P(x))=\bar{1}x^2+\bar{1}x+\bar{1}$ را در نظر می گیریم که
$a \longrightarrow a+<p(x)>$

$\bar{1}=1+<p(x)>$

قرار می دهیم $a=x+<p(x)>$ و داریم:

$$\bar{p}(x)=(1+<p(x)>)(x+<p(x)>)^2+(1+<p(x)>)+(x+<p(x)>$$
$$+1+<p(x)>=1\times x^2+x+1+<p(x)>=<p(x)>=0_K.$$

2.4 اعداد جبری و متعالی

تعریف 1.2.4. فرض کنید E یک توسیع میدان F باشد. در این صورت $a \in E$ را روی F **جبری** نامیم هر گاه

$$\exists f(x) \in F[x] \ s.t. \ f(a) = 0$$

در این غیراین صورت a را روی F **متعالی** نامیم.

هر عضو £ را که روی ¤ جبری باشد یک **عدد جبری** می نامیم. یک عدد **متعالی**، عضوی از £ است که روی ¤ متعالی باشد.

مثال 1-2.2.4. میدان ¡ یک توسیع ¤ است. واضح است که هر عدد گویا روی ¤ جبری است. همچنین $\sqrt{3}$ یک عضو جبری است زیرا $\sqrt{3}$ یک ریشه $f(x) = x^2 - 3 \in ¤[x]$ میباشد.

2. عدد حقیقی $a = \sqrt{1+\sqrt{3}}$ را در نظر می گیریم. داریم:

$$a^2 = 1+\sqrt{3} \Rightarrow a^2 - 1 = \sqrt{3} \Rightarrow a^4 - 2a^2 + 1 = 3$$

بنابراین a یک ریشه $f(x) = x^4 - 2x^2 - 2 \in ¤[x]$ است. یعنی a روی ¤ جبری است.

3. £ $i \in$ یک عدد جبری است. زیرا ریشه $x^2 + 1 \in ¤[x]$ می باشد.

4. می‌توان نشان داد (نه به سادگی) اعداد p و e (عدد نپر) روی ¤ متعالی هستند.

قضیه 3.2.4. فرض کنید E یک توسیع میدان F باشد. در این صورت $a \in E$ روی F متعالی است اگر و تنها اگر همریختی ارزیاب $f_a : F[x] \to E$ یکبیک باشد.

برهان. f_a یکبیک است اگر و فقط اگر $Ker f_a = \{0\}$ به ازای $0 \neq f(x) \in F[x]$ داشته باشیم $f(a) \neq 0$ یعنی a متعالی است.

قضیه 4.2.4. فرض کنید E یک توسیع میدان F باشد که $a \in E$ روی F جبری است. در اینصورت چند جمله ایی تکین و تحویل ناپذیر منحصربفردی مانند $p(x) \in F[x]$ وجود بقسمی که $p(a) = 0$. بعلاوه اگر $0 \neq f(x) \in F[x]$ که $f(a) = 0$ آنگاه $p(x) | f(x)$ و $\deg p(x) \leq \deg f(x)$.

برهـان. همریختـی ارزیـاب $f_a : F[x] \to E$ را در نظـر مـی گیـریم. واضـح اسـت کـه $g(a)=0 \Leftrightarrow g(x) \in Ker f_a$. چون $F(x)$ یک $P.I.D$ است و $Ker f_a \leq F[x]$ پس وجـود دارد $p(x) \in F[x]$ بقســمی کــه $Ker f_a =< p(x) >$. بنــابراین اگــر $f(x) \in F[x]$ کــه $f(a)=0$ آنگاه $f \in Ker f_a$ ودرنتیجه $p(x) | f(x)$. حال فرض کنید $p(x)=p_1(x)p_2(x)$. چون $\mathrm{Im} g f_a \leq E$ دامنه صحیح است، داریم:

$$0=P(a)=P_1(a)P_2(a) \Rightarrow P_1(a)=0 \quad \text{یا} \quad P_2(a)=0.$$

بنابراین $p(x) | p_1(x)$ یا $p(x) | p_2(x)$. یعنی $p(x)$ تحویل ناپذیر است و با ضرب کردن عدد مناسبی در $p(x)$، چند جمله ایی تکین به دست می آید.

تعریف 5.2.4. فرض کنید E یـک توسـیع میـدان F باشـد و $a \in E$ روی F جبـری در ایـن صورت چند جمله ایی تکین یکتای $p(x)$ در قضیه قبل را چند جمله ایی **تحویل ناپذیر** a بـر روی F نـامیم و بـا $P(a,F)$ را نشـان مـی دهـیم. همچنـین درجـه $p(x)$ را درجـه a بـر F گوییم و به صورت $\deg(a,F)$ نمایش می د هیم.

مثال 6.2.4. داریم:

$$P(\sqrt{2}, ¡) = x - \sqrt{2}, P(\sqrt{2}, ¤) = x^2 - 2,$$
$$P(\sqrt{1+\sqrt{3}}, ¤) = x^4 - 2x^2 - 2, P(i, ¤) = x^2 + 1,$$
$$\deg(\sqrt{2}, ¡) = 1, \deg(\sqrt{2}, ¤) = \deg(i, ¤) = 2, \deg(\sqrt{1+\sqrt{3}}, ¤) = 4.$$

نمادگذاری 7.2.4. فرض کنید $F \leq E$, $S \subseteq E$ در این صورت

الف) کوچکترین زیر حلقه E شامل $F \cup S$ را با $F[S]$ نشان می دهیم.

ب) کوچکترین زیر میدان E شامل $F \cup S$ را با $F(S)$ نشان می دهیم.

واضح است $F[S]$ دامنه صحیح است و داریم:

$$F[S] \subseteq F(S) \subseteq E$$

با توجه به اینکه $F[S]$ دامنه صحیح است و $F(S)$ کوچکترین میدان شامل $F \cup S$ پس $F(S)$ همان میدان کسرهای $F[S]$ می باشد. یعنی $F(S)=\{\frac{u}{u};u,u\in F[s]\}$.

حال فرض کنید $S=\{a\}$ در این صورت به سادگی می توان نشان داد که

$$F[s]=F[a]=\{f(a);\ f(x)\in F[x]\}$$

و بنابراین $F(S)=\left\{\frac{f(a)}{g(a)};\ f(x),g(x)\in F[x]\right\}$.

فرض کنید a روی F جبر ی باشد. قضیه زیر عناصر $F(a)$ را مشخص می کند.

قضیه 8.2.4. فرض کنید $F\le E$ و $a\in E$ بروی F جبری باشد. در این صورت اگر $\deg(a,F)=n$ آنگاه $F(a)=\{b_0+b_1a+...+b_{n-1}a^{n-1}\mid b_i\in F\}$.

برهان همریختی ارزیاب $f_a : F[x]\to E$ را با تعریف

$$\forall f(x)\in F[x];\quad f_a(f(x))=f(a)$$

در نظر می گیریم. در این صورت می دانیم که $f_a(F[x])$; $K=\frac{F[x]}{\ker f_a}$ میدان است و $\ker f_a =< P(x) >$ که $P(x)$ چند جمله ای مینمال a است. به ازای هر $f(x)\in F[x]$ داریم:

$$\exists r(x),\ g(x)\in F[x]\ s.t.\ f(x)=P(x)g(x)+r(x)$$

که $r(x)=0$ یا $\deg r(x)<\deg P(x)$

حال داریم:

$$\begin{aligned}K\ ;\ f_a(F[x])&=\{f_af(x);\ f(x)\in F[x]\}\\&=\{f(a);\ f(x)\in F[x]\}=\{r(a);\ r(x)=0,\ \deg r(x)<n\}\\&=\{b_0+b_1a+...+B_{n-1}a^{n-1}\mid b_i\in F\}.\end{aligned}$$

زیرا $P(a)=0$ پس $f(a)=p(a)g(a)+r(a)=r(a)$.

واضح است که K یک میدان شامل $F\cup\{a\}$ است. کافی است نشان دهیم که K کوچکترین میدان شامل $F\cup\{a\}$ است. اگر L یک میدان شامل $F\cup\{a\}$ باشد پس شامل $b_0+b_1a+...+b_{n-1}a^{n-1}$ است یعنی $K\subseteq L$.

مثال 9.2.4 -1) می دانیم که $\sqrt{2} \in$ ¡ روی ¤ جبری است. پس

$¤[\sqrt{2}] = ¤(\sqrt{2}) = \{b_0 + b_1\sqrt{2} \mid b_0, b_1 \in ¤\}$.

2) واضح است که $i \in$ £ روی ¡ جبری است $(x^2 + 1 = 0)$ در این صورت

$¡[i] = ¡(i) = \{a + bi \mid a, b \in ¡\}$

3) می دانیم $p \in$ ¡ روی ¤ جبری نیست. بنابراین

$¤[p] = \{f(p) \mid f(x) \in ¤[x]\}$

$¤(p) = \{\frac{f(p)}{g(p)} \mid f(x), g(x) \in ¤[x]\}$

مثلا $\frac{1}{p} \notin ¤[p]$ ولی $\frac{1}{p} \in ¤(p)$.

تعریف 10.2.4. فرض کنید E یک توسیع F باشد. در این صورت E را توسیع ساده F نامیم هرگاه $\exists a \in E \; s.t. \; E = F(a)$.

مثال11.2.4-1) £ یک توسیع ساده ¡ است. زیرا $¡(i) =$ £

2) $¤(\sqrt{2})$ یک توسیع ساده ¤ است.

3.4 توسیع های جبری و توسیع های متناهی

توسیع میدان E را روی F در نظر می گیریم. واضح است که E یک فضای برداری روی میدان F است.

تعریف 1.3.4. توسیع E را روی F، یک **توسیع متناهی** نامیم هر گاه E به عنوان یک فضای برداری روی F از بعد متناهی n باشد. در این صورت n را **درجه** E روی F نامیم و می نویسیم $[E:F] = n$.

مثال 2.3.4. فرض کنید a روی F جبری باشد که $\deg(a, F) = k$. یعنی

$F(a) = \{b_0 + b_1 a + ... + b_{k-1} a^{k-1} \mid b_i \in F\}$

بنابراین $S = \{1, a, ..., a^{k-1}\}$ یک پایه $F(a)$ روی F است و $[F(a):F] = k$.

تعریف 3.3.4. توسیع میدان E روی F را یک **توسیع جبری** نامیم، هر گاه هر عضو E روی F جبری باشد.

قضیه 4.3.4. هر توسیع متناهی، یک توسیع جبری است.

برهان. فرض کنید E یک توسیع متناهی از میدان F باشد که $[E:F]=n$ و $a \in E$ دراین صورت $S=\{1,a,...,a^n\}$ وابسته خطی است. بنابراین وجود دارند $c_0,c_1,...,c_n \in F$ بقسمی که $c_0\times 1+c_1\times a+...+c_n a^n=0$. با قرار دادن $f(x)=c_0+c_1x+...+c_nx^n$ داریم $f(a)=0$ وحکم برقرار است.

بنابراین a روی F جبری است $\Leftrightarrow$ $[F(a):F]$ متناهی باشد.

قضیه 5.3.4. اگر E یک توسیع متناهی میدان F و K توسیع متناهی روی E باشد، آنگاه K یک توسیع متناهی روی F است و داریم:

$$[K:F]=[K:E]\times[E:F]$$

برهان. فرض کنید $a=\{a_1,a_2,...,a_n\}$ و $b=\{b_1,b_2,...,b_m\}$ به ترتیب پایه ایی برای فضای E روی F و فضای K روی E باشند. کافی است نشان دهیم:

$$g=\{a_i b_j \mid 1\le i\le n,\ 1\le j\le m\}$$

یک مبنای K روی F است.

فرض کنید $u\in K$ پس داریم:

$$\exists c_i \in E \ \ s.t. \ \ u=\sum_{j=1}^{m} c_j b_j$$

چون $c_j \in E$ داریم:

$$\exists t_{ij} \in F \ \ s.t. \ \ c_j=\sum_{i=1}^{n} t_{ij} a_i$$

بنابراین

$$u=\sum_{j=1}^{m} c_j b_j=\sum_{j=1}^{m}(\sum_{i=1}^{n} t_{ij} a_i)b_j=\sum_{i.j} t_{ij} a_i b_j$$

یعنی هر عضو K ترکیب خطی از عناصر g است. برای استقلال خطی g، فرض کنید $\sum t_{ij}a_i b_j = 0$ بنابراین

$$\sum_{j=1}^{m}(\sum_{i=1}^{n}t_{ij}a_i)b_j = 0 \Rightarrow \sum_{i=1}^{n}t_{ij}a_i = 0, \qquad \forall j = 1,2,...,m$$

بنابراین به ازای هر i, j داریم $t_{ij} = 0$. زیرا a و b مستقل خطی هستند.

نتیجه 6.3.4- 1) اگر $E_1 \le E_2 \le E_3 \le E_4$، آنگاه

$$[E_4 : E_1] = [E_4 : E_3] \times [E_3 : E_2][E_2 : E_1]$$

2) فرض کنید $F \le E$ و $a \in E$ روی F جبری باشد. در این صورت اگر $b \in F(a)$ آنگاه $\deg(b, F) \mid \deg(a, F)$.

برهان 1) به سادگی از تعمیم قضیه قبل به دست می آید.

برای اثبات 2) داریم $F \le F(b) \le F(a)$ پس

$$[F(a) : F] = [F(a) : F(b)] \times [F(b) : F]$$

بنابراین

$$\deg(b, F) = [F(b) : F] \mid [F(a) : F] = \deg(a, F)$$

مثال 7.3.4. چند جمله ایی $x^3 - 2$ در $¤(\sqrt{2})$ ریشه ندارد. زیرا اگر $a \in ¤(\sqrt{2})$ یک ریشه $x^3 - 2$ باشد، آنگاه $\deg(\sqrt{2}, ¤) = 2 \mid \deg(a, ¤) = 3$ که تناقض است.

تذکر 8.3.4. فرض کنید E یک توسیع میدان F باشد و $a_1, a_2 \in E$. بنا به تعریف کوچکترین زیر میدان E شامل $F \cup \{a_1, a_2\}$ را با $F\{a_1, a_2\}$ نشان می دهیم. بنابراین $F(a_1, a_2) = (F(a_1))(a_2)$. به طور مشابه اگر $a_1, a_2, ..., a_n \in E$ آنگاه $F\{a_1, ..., a_n\}$ تعریف می شود.

مثال 9.3.4. میدان $¤(\sqrt{2}, \sqrt{3})$ را در نظر می گیریم. می دانیم که $\{1, \sqrt{2}\}$ یک مبنای $¤(\sqrt{2})$ است. از طرفی $p(\sqrt{2} + \sqrt{3}, ¤) = x^4 - 10x^2 + 1$ پس $\deg(\sqrt{2} + \sqrt{3}, ¤) = 4$، یعنی $\sqrt{3} \notin ¤(\sqrt{2})$. با توجه به اثبات قضیه $S = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ یک مبنای $¤(\sqrt{2}, \sqrt{3})$ است.

بنابراین $\sqrt{2}+\sqrt{3}\in ¤(\sqrt{2},\sqrt{3})$ و با توجه به قضیه داریم:

$$[¤(\sqrt{2},\sqrt{3}):¤]=[¤(\sqrt{2},\sqrt{3}):¤(\sqrt{2}+\sqrt{3})][¤(\sqrt{2}+\sqrt{3}),¤]$$

از طرفی

$$[¤(\sqrt{2},\sqrt{3}):¤]=[¤(\sqrt{2}+\sqrt{3}):¤]=4.$$

بنابراین

$$[¤(\sqrt{2},\sqrt{3}):¤(\sqrt{2}+\sqrt{3})]=1\Rightarrow ¤(\sqrt{2},\sqrt{3})=¤(\sqrt{2}+\sqrt{3})$$

و در نتیجه $¤(\sqrt{2},\sqrt{3})$ یک توسیع ساده است.

به طور مشابه نشان دهید که $¤(\sqrt{2},\sqrt[3]{2})=¤(\sqrt[6]{2})$.

تعریف 10.3.4. فرض کنید $F\le E$. در این صورت اگر وجود داشته باشند $a_1,a_2,...,a_k\in E$ بقسمی که $E=F(a_1,a_2,...,a_k)$ آنگاه گوییم E یک توسیع متناهی تولید شده است.

مثال 11.3.4-1) می دانیم $¡(i)=£$ پس $£$ یک توسیع متناهی تولید شده است.

2) $¡(p)$ روی یک توسیع متناهی تولید شده است که توسیع متناهی نیست.

قضیه زیر نشان می دهد که هر توسیع متناهی از میدان F یک توسیع با تولید متناهی از میدان F است. آیاعکس این حکم برقرار است؟

قضیه12.3.4. فرض کنید E یک توسیع متناهی از میدان F باشد آنگاه E یک توسیع با تولید متناهی از F است.

برهان. فرض کنید $[E:F]=n$. اگر $n=1$ پس $E=F=F(1)$.

فرض کنید $n\ge 2$ پس $a_1\in E-F$. اگر $[F(a_1):F]\ge 2$ آنگاه حکم برقرار است. در غیر این صورت $a_2\in E-F(a_1)$ را انتخاب می کنیم.بنابراین

$$[F(a_1,a_2):F(a_1)]\ge 2$$

اگر $E = F(a_1, a_2)$ که حکم برقرارا ست، در غیر این صورت با ادامه فرآیند $a_1, a_2, ...a_k \in E$ وجود دارند که $E = F(a_1, ...a_k)$. زیرا

$n = [E : F] = [F(a_1) : F][F(a_1, a_2) : F(a_1)] \times ... \times [E : F(a_1, ..., a_t)]$.

قضیه 13.3.4. اگر $a_1, a_2, ..., a_n$ روی F جبری باشند آنگاه $E = F(a_1, ..., a_n)$ یک توسیع جبری روی F است.

برهان. به ازای $i \geq 2$، a_i روی F جبری است. پس a_i روی $F(a_1, ..., a_{i-1})$ نیز جبری است. بنابراین $[F(a_1, ..., a_i) : F(a_1, ..., a_{i-1})]$ متناهی می باشد. در نتیجه $[F(a_1, ..., a_n) : F]$ توسیع متناهی است و اینک حکم از قضیه 4.3.4 به دست می آید.

قبلا ثابت شد که هر توسیع متناهی یک توسیع جبری است. مثال زیر نشان می دهد که عکس آن ممکن است، برقرار نباشد.

مثال 14.3.4. فرض کنید p عدد اول باشد. در این صورت $E = ¤(\sqrt{2}, \sqrt{3}, ..., \sqrt{p}, ...)$ یک توسیع جبری $¤$ است که توسیع متناهی نیست

راه حل. فرض کنید $a \in E$. بنابراین اعداد اول $P_1, ..., P_k$ وجود دارند که $a \in E_r = ¤(\sqrt{p_1}, ..., \sqrt{p_r})$. چون $\sqrt{p_i}$ روی $¤$ جبری است پس E_r (در نتیجه a) جبری است. بنابراین E جبری است.

حال زنجیر صعودی اکید زیر متوقف نمی شود.

$¤ < ¤(\sqrt{2}) < ¤(\sqrt{2}, \sqrt{3}) < ¤(\sqrt{2}, \sqrt{3}, \sqrt{5}) < ...$

بنابراین E متناهی نیست.

4.4 میدان بسته جبری

فرض کنید $F \leq E$ و a, b روی F جبری باشند. بنابراین $F(b, a)$ روی F جبری است. چون $a \pm b \in F(a, b)$، $\frac{a}{b}$ $(b \neq 0)$، پس قضیه زیر را داریم:

قضیه 1.4.4. فرض کنید $F < E$ در این صورت $\{ a$ روی F جبری است ; $a \in E\} = \overline{F}$ زیر میدانی از E است. که آنرا بستار جبری F در E نامیم. درنتیجه مجموعه تمام اعداد جبری تشکیل یک میدان میدهد.

تعریف 2.4.4. میدان F را **بسته جبری** نامیم، هر گاه هر چند جمله ایی غیرثابت از $F[x]$ در F ریشه داشته باشد.

قضیه 3.4.4. میدان F بسته است اگر و فقط اگر هر چند جمله ایی غیرثابت از $F[x]$ به حاصل ضرب عوامل خطی (درجه اول)تجزیه شود.

برهان فرض کنید $f(x) \in F[x]$ چند جمله ایی غیر ثابت باشد. پس $f(x)$ در F ریشه ایی مانند a دارد. بنابراین $f(x) = (x-a)g(x)$. اکنون اگر $g(x)$ غیر ثابت باشد، ریشه ایی چون b دارد و در نتیجه $f(x) = (x-a)(x-b)h(x)$. با ادامه فرآیند حکم ثابت می شود.

بعکس. فرض کنید $ax+b$ یکی از عوامل غیرثابت تجزیه $f(x)$ باشد. پس $x = -\frac{b}{a}$ یک ریشه $f(x)$ است.

بااستفاده از لم زورن می توان نشان داد که هر میدان F دارای یک بستار جبری است.

قضیه زیرا را از دو روش جبری و تحلیلی می توان ثابت نمود که از حوصله این درس خارج است.

قضیه 4.4.4. (اساسی جبر). میدان اعداد مختلط $\mathbb{C}$، بسته جبری است.

5.4 ترسیم با خط کش و پرگار

در این بخش با استفاده از توسیع های میدان ، خط کش غیرمدرج و پرگار می خواهیم چند مساله قدیمی مشهور را سامان دهیم:

1)آیا می توان مکعبی رسم کرد که حجم آن دو برابر حجم مکعب مفروض باشد.

2) آیا می توان مربعی رسم کرد که مساحت آن برابر مساحت دایره مفروض باشد.

3) آیا می توان یک زاویه دلخواه را تثلیث کرد (یعنی بر سه قسمت مساوی تقسیم کرد).
البته فرض بر این است که با ترسیم های استاندارد با خط کش و پرگار که در هندسه مسطحه می آیند، آشنایی داریم. بخصوص اگر P نقطه ایی غیرواقع بر خط l باشد می توان از این نقطه خطی موازی بر l (عمود بر l) رسم کرد.

تعریف 1.5.4. فرض کنید پاره خطی به طول واحد داده باشد. عدد حقیقی a را رسم پذیر نامیم هر گاه بتوان پاره خطی به طول $|a|$ با استفاده از خط کش و پرگار و پاره خط به طول واحد، رسم کرد.

قضیه 2.5.4. اگر a و b اعداد حقیقی رسم پذیر باشند آنگاه $a+b,\ a-b,\ ab,\ \frac{a}{b}\ (b\neq 0)$ ترسیم پذیرند.

برهان. پاره خط های به طول $|a|$ و $|b|$ داده شده اند. برای $a,b>0$ با خط کش پاره خط به طول a را امتداد دهیم و سپس با استفاده از پرگار از یک طرف پاره خط a، پاره خطی به طول b جدا می کنیم. این کار پاره خط $a+b$ را رسم می کند. بروش مشابه پاره خط $a-b$ جدا می شود.

اعداد ab و a/b با استفاده از شکل های زیر ساخته می شوند.

حال حکم از تشابه مثلثها به دست می آید، که داریم:

$$\frac{1}{|a|}=\frac{|b|}{|OQ|}\Rightarrow|oQ|=|a||b|;$$

$$\frac{|OQ|}{1}=\frac{|a|}{|b|}\Rightarrow|OQ|=\frac{|a|}{|b|}$$

نتیجه 3.5.4. مجموعه تمام اعداد رسم پذیر زیر میدانی از اعداد حقیقی است.

تذکر 4.5.4. با توجه به اینکه ¤ کوچکترین زیر میدان ¡ است. (¤ میدان اول ¡ است). پس میدان اعداد رسم پذیر شامل ¤ می باشد.

مثال 5.5.4. نقاط $¤\times¤$ رسم پذیرند.

راه حل. فرض کنید $(a,b)\in ¤\times¤$. با توجه به اینکه $a,b\in ¤$ پس نقاط $(a,0)$ و $(0,b)$ رسم پذیرند. در نتیجه با توجه به نمودار زیر نقطه (a,b) رسم پذیر است.

فرض کنید l خطی باشد که از دو نقطه گویای مشخص می گذرد (پس معادله l به صورت $ax+by+c=0$ است که $a,b,c\in ¤$. همچنین معادله دایره به شعاع و مختصات مرکز گویا نیز به صورت $x^2+y^2+dx+ey+f=0$ است. واضح است که چنین خطوط و دایره هایی قابل رسم است با کمی تامل متوجه می شویم که نقاط زیر نیز قابل رسم است.

الف) تقاطع دو خط به صورت بالا

ب) تقاطع دو دایره به فرم بالا

ج) تقاطع یک خط و یک دایره به فرم بالا.

نقاط حالت‌های اول و دوم، دارای مقادیر گویا برای $y.x$ هستند. بنابراین عضو $¤\times¤$ می باشند. یعنی نقاط رسم پذیر جدیدی به دست نیم آوریم.

اکنون به بررسی نقاط حالت سوم می پردازیم. برای این کار نقاط تقاطع خط $dx+ey+f=0$ و دایره $x^2+y^2+ax+by+c=0$ را به دست می آوریم. حالتهای زیر داریم:

1) اگر $d=0$ داریم $y=\frac{-f}{e}$ و بنابراین

$$0=x^2+(\frac{-f}{e})^2+ax+b(\frac{-f}{e})+c=Ax^2+Bx+C$$

که $A,B,C\in ¤$.

وقتی که $A=0$ پس $x=\frac{-C}{B}\in ¤$. چون $y=\frac{-f}{C}\in ¤$ پس $(x,y)\in ¤\times ¤$.

اگر $A=0$ با حل معادله $Ax^2+Bx+C=0$ داریم که $x\in ¤(\sqrt{u})$, $[¤(u):¤]=2$

2) اگر $d\neq 0$ (که در این حالت می توانیم فرض کنیم $d=1$). در نتیجه $x=-ey-f$ و با جایگذاری در معادله دایره معادله $Ay^2+By+C=0$ به دست می آید که مشابه حالت (1) داریم $x,y\in ¤(\sqrt{u})$.

یعنی حالت سوم می تواند شامل نقاط رسم پذیر غیر از نقاط $¤\times ¤$ باشد.

لم 6.5.4. فرض کنید $c>0$ عددی رسم پذیر باشد آنگاه $\sqrt{c}$ رسم پذیر است.

برهان: نمودار زیر را در نظر می گیریم:

داریم: $\frac{|OQ|}{|OA|}=\frac{|OP|}{|OQ|}$ و بنابراین

$$|OQ|^2=|OA|\times|OP|=c\Rightarrow|OQ|=\sqrt{c}$$

قضیه 7.5.4. هر گاه عدد حقیقی c رسم پذیر باشد، آنگاه c روی میدان اعداد گویا جبری و از درجه توانی از 2 می باشد.

برهان. چون c رسم پذیر است بنابراین نقطه $(c,0)$را میتوان با استفاده از دنباله متناهی از ترسیم ها (نقاط الف تا ج) به دست آورد. اولین عضو دنباله به $¤(u_1)$ تعلق دارد که $u_1^2 \in ¤$ یعنی $t=0$ یا 1 و $[¤(u_1):¤]=2^t$ به همین نحو دومین نقطه به $¤(u_1,u_2)=(¤(u_1))(u_2)$ متعلق است که $u_2^2 \in ¤(u_1)$. با ادامه فرآیند سرانجام به c می رسیم. یعنی وجود دارند $u_i^2 \in ¤(u_1,u_2,...,u_{i-1})$ که $c \in ¤(u_1,u_2,...,u_n)$ و داریم:

$$[¤(u_1,...,u_n):¤]=2^k$$

اینک نشان می دهیم که بعضی از ترسیم ها غیر ممکن هستند.

قضیه 8.5.4. تضعیف مکعب غیر ممکن است. یعنی در صورتی که طول ضلع مکعبی داده شده باشد. نمی توان فقط با استفاده از خط کش و پرگار ضلع مکعبی رابه دست آورد که حجم آن دو برابر حجم مکعب داده شده باشد.

برهان. فرض کنید طول ضلع داده شده مساوی 1 باشد. پس حجم آن مساوی 1 می باشد. یعنی بایدمکعبی رسم کنیم که حجم آن 2 باشد. در واقع طول ضلع آن با $\sqrt[3]{2}$ باشد که این کار ممکن نیست زیرا

$$[Q(\sqrt[3]{2}):Q]=3\neq 2$$

یعنی $\sqrt[3]{2}$) ساختنی نیست.

مثال 9.5.4. رسم مربعی که مساحت آن برابر مساحت دایره ایی به شعاع یک باشد ممکن نیست.

راه حل چون مساحت باید مساوی pباشد پس باید ضلعی به طول $\sqrt{p}$رسم کنیم. چون p روی Q جبری نیست پس $\sqrt{p}$ نیز جبری نیست، یعنی حکم برقرار است.

تعریف 10.5.4. زاویه q(اندازه بر حسب رادیان است) را رسم پذیر نامیم هر گاه نقاط رسم Pو Q وجود داشته باشد که اندازه زاویه POQبر حسب رادیان برابر q باشد.

لم 11.5.4. فرض کنید $q \in R$یک زاویه بر حسب رادیان باشد در این صورت گزاره های زیر معادلند

1)زاویه q ساخت پذیر است.

2) $Cosq$ساخت پذیر است.

3) $Sinq$ساخت پذیر است.

برهان. $1 \Leftarrow 2$و $1 \Leftarrow 3$از نمودار زیر به دست می آید.

برای اثبات $2 \Leftarrow 3$چون $Cosq$ ساختنی است. پس $Sinq = \sqrt{1-\cos q}$ نیز ساختنی است.

و اثبات $3 \Leftarrow 1$به عنوان ترین واگذار می شود.

مثال 12.5.4. تثلیث زاویه 60 درجه با خط کش پرگار ممکن نیست.

راه حل. با توجه به فرمول $Cos3q = 4Cos^3 q - 3Cosq$، قرار می دهیم $q = 20$و $a = Cos20$ داریم:

$$4a^3 - 3a = \frac{1}{2}$$

بدلیل اینکه $8a^3 - 6a = 1$ تحویل ناپذیر است پس

$$[¤(a):¤] = 3$$

یعنی $a = Cos\frac{p}{12}$ ساختنی نیست و در نتیجه زاویه 20^oدرجه قابل ساختن نیست.

اینک مساله رسم یک n - ضلعی منظم کافی است زاویه $q_n = \frac{2p}{n}$را رسم کنیم. زیرا هر n ضلعی منظم را می توان در دایره ای به شعاع وحد محاط کنیم و بنابراین کافی است نشان دهیم $Cosq_n$ ساختنی است.

قضایای زیر را برای رسم یک n - ضلعی منظم می توان نشان داد.

قضیه. فرض کنید $n>1$ عدد طبیعی باشد و $n=P_1^{a_1}P_2^{a_2}...P_n^{a_n}$ یک تجزیه به عوامل اول باشد. در این صورت n - ضلعی منظم ساخت پذیر است اگر و فقط اگر برای هر i که $1\le i\le s$ چند ضلعی با p^i ضلع ساخت پذیر باشد.

قضیه. فرض کنید $n\in ¥$ و z یک ریشه n -ام واحد باشد. در این صورت n - ضلعی منظم ساخت پذیر است $\Leftrightarrow [¤(z):¤]$ توانی از 2 باشد.

قضیه. فرض کنید p عددی اول و فرد باشد. در این صورت p - ضلعی ساخت پذیر است $\Leftrightarrow p=2^m+1$ (به این اعداد، اعداد اول فرما گوییم).

نتیجه. اگر $n=2^k p_1...p_t$ که $k\ge 0$ و $p_1,p_2,...,p_t$ اعداد اول فرد متمایز باشند. آنگاه n - ضلعی منظم ساخت پذیر است.

6.4 قضیه اساسی گالوا

در این فصل گروه گالوای یک توسیع میدان دلخواه را تعریف نموده و شرایط مورد نیاز برای اثبات قضیه اساسی نظریه گالوا را فراهم می کنیم. این قضیه مسایل مربوط به میدان ها، چند جمله ایی ها و توسیع ها را به زبان نظریه گروه ها بیان می کند.

فرض کنید F یک میدان باشد. تابع $s:F\to F$ رایک خودریختی میدان F نامیم هر گاه به ازای هر $a,b\in F$ داشته باشیم:

$$\begin{cases} s(a+b)=s(a)+s(b) \\ s(ab)=s(a)\times s(b) \end{cases}$$

مجموعه همه خودریختی های میدان F با عمل ترکیب یک گروه است که با نماد $Aut(K)$ نشان می دهیم.

فرض کنید G زیر گروهی از $Aut(K)$ باشد. قرار می دهیم.

$$K_G = \{a \in K \mid s(a) = a; \forall s \in G\}$$

لم 1.6.4. با نمادهای بالا K_G زیر میدان K است.

برهان. فرض کنید $a, b \in K_G$ در این صورت

$$s(a-b) = s(a) - s(b) = a - b \Rightarrow a - b \in K_G$$
$$s(ab) = s(a)s(b) = ab \Rightarrow ab \in K_G$$

هرگاه $b \neq 0$ آنگاه

$$s(b^{-1}) = (s(b))^{-1} = b^{-1} \Rightarrow b^{-1} \in K_G$$

زیر میدان K_G را زیر میدان ثابت G نامیم.

فرض کنید F یک توسیع میدان K باشد. قرار می دهیم:

$$Aut(F, K) = \{s \in Aut(F) \mid s(a) = a, \forall a \in K\}$$

در این صورت $Aut(F, K)$ زیر گروه $Aut(F)$ است.

مثال 2.6.4. می دانیم که $\mathbb{C} \leq \mathbb{i}$. فرض کنید $s \in Aut(\mathbb{C}, \mathbb{i})$ پس

$$(s(i))^2 = s(i^2) = s(-1) = -1 \Rightarrow s(i) = \pm i$$

و

$$s(a+ib) = s(a) + s(i)s(b) = a \pm ib.$$

پس $Aut(\mathbb{C}, \mathbb{i}) = \{s_1, s_2\}$ که $s_i : \mathbb{C} \longrightarrow \mathbb{C}$ و

$$s_1(a+ib) = a+ib$$
$$s_2(a+ib) = a-ib$$

حال می خواهیم ببینیم $\mathbb{C}_{Aut(\mathbb{C}, \mathbb{i})} = ?$.

$$s_2(a+ib) = a+ib \Rightarrow a+ib = a-ib \Rightarrow b = 0 \Rightarrow \mathbb{C}_{Aut(\mathbb{C}, \mathbb{i})} = \mathbb{i}.$$

مثال 3.6.4. می دانیم که $\sqrt[3]{2}$ یک ریشه چند جمله ایی $f(x) = x^3 - 2$ است که روی $\mathbb{Q}$ تحویل ناپذیر است. قرار می دهیم $F = \mathbb{Q}(\sqrt[3]{2})$. بنابراین

$$F = \left\{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \,\middle|\, a_i \in \mathbb{Q}\right\}$$

اگر $s \in Aut(F, ¤)$ آنگاه $(s(\sqrt[3]{2}))^3 = s(\sqrt[3]{2})^3 = s(2) = 2$ یعنی $s(\sqrt[3]{2})$ نیز یک ریشه $f(x)$ است. چون $f(x)$ فقط یک ریشه حقیقی دارد. پس $s(\sqrt[3]{2}) = \sqrt[3]{2}$ و بنابراین

$$s(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2) = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$$

یعنی $s = id$. در نتیجه $Aut(F, ¤) = \{id\}$ و $F_{Aut(F,¤)} = F$.

قضیه 4.6.4. فرض کنید F یک توسیع میدان K باشد و $f(x) \in K[x]$. هرگاه $u \in F$ یک ریشه f باشد و $s \in Aut(F, K)$ آنگاه $s(u) \in F$ نیز یک ریشه f است.

برهان. فرض کنید $f = \sum_{i=1}^{n} c_i x^i$ و پس $f(u) = 0$ و داریم:

$$0 = s(f(u)) = s(\sum_{i=1}^{n} c_i u^i) = \sum_{i=1}^{n} s(c_i)(s(u))^i = \sum_{i=0}^{n} c_i (s(u))^i$$

و حکم ثابت می شود.

مثـــال 5.6.4. مـــی دانـــیم کـــه بـــه ازای $1 \le i \le 4$؛ $w = e^{\frac{2pi}{5}}$ ریشـــه چنـــد جملـــه ایـــی $x^4 + x^3 + x^2 + x + 1$ است که روی ¤ تحویل ناپذیر است. قرار مـی دهـیم $F = ¤(w)$. اگـر $s \in Aut(F, ¤)$ آنگاه $s(w) = w^i$ که $1 \le i \le 4$ (چون $s(1) = 1$ پس $s(w) \neq 1$) . در نتیجـه داریم:

$$s_i(a_0 + a_1 w + a_2 w^2 + a_3 w^3) = a_0 + a_1 w^i + a_2 (w^i)^2 + a_3 (w^i)^3 .$$

پس $Aut(F, ¤) = \{s_1, s_2, ..., s_4\}$ که s_1 عنصر همانی است و

$$s_2^4 = s_1 \text{ و } s_2^3 = s_3, s_2^2 = s_4$$

یعنی $Aut(F, ¤)$ یک گروه دوری از مرتبه 4 می باشد.

قرار می دهیم $H = \{s_1, s_4\}$. پـس $s_4^2 = s_2^4 = s_1$. یعنـی H یـک زیـر گـروه $Aut(F, ¤)$ است. حال $K_H = ?$

$$s_4(a_0 + a_1 w + a_2 w^2 + a_3 w^3) = a_0 + a_1 w + a_2 w^2 + a_4 w^3$$

بنابراین داریم:

$$a_0 + a_1 w^4 + a_2 w^8 + a_3 w^{12} = a_0 + a_1 w + a_2 w^2 + a_3 w^3$$

$$\Rightarrow a_0 + a_1 w^4 + a_2 w^3 + a_3 w^2 = a_0 + a_1 w + a_2 w^2 + a_3 w^3 \Rightarrow a_1 = 0,\ a_2 = a_3$$

در نتیجه

$$K_H = \{a_0 + a_2(w^2 + w^3) | a_0, a_2 \in \text{¤}\}.$$

تعریف 6.6.4. فرض کنید F یک توسیع جبری F باشد. دو عضو $a, b \in F$ را روی E **مزدوج** نامیم، هر گاه چندجمله‌ایی تحویل ناپذیر a و b مساوی باشند.

مثال 7.6.4- 1) توسیع £ روی ¡ را در نظر می گیریم. چون $a+ib$ و $a-ib$ ریشه های چند جمله ایی تحویل ناپذیر $x^2 + 2ax + a^2 + b^2$ هستند پس $a+ib$ و $a-ib$ مزدوجند.

2) $w_i = e^{\frac{2p\,i}{5}}$ به ازای $i = 1, 2, 3, 4$ ریشه های چند جمله ای تحویل ناپذیر $x^4 + x^3 + x^2 + x + 1$ می باشند. پس w_i مزدوجند.

قضیه 8.6.4. فرض کنید a, b روی میدان F جبری باشند و $\deg(F, a) = n$ در اینصورت $y_{a,b} : F(a) \to F(b)$ با ضابطه

$$y_{a,b} : (c_. + c_1 a + \ldots + c_{n-1} a^{n-1}) = c_. + c_1 b + \ldots + c_{n-1} b^{n-1}$$

که $c_i \in F$ از $F(a)$ به $F(b)$ یکریختی است اگر فقط اگر a و b مزدوج باشند.

برهان. فرض کنید $y_{a,b}$ یکریختی باشد و f , g چند جمله ایی های تحویل ناپذیر تکین که $f(a) = g(b) = 0$ بنابراین داریم:

$$0 = y_{a,b}(f(a)) = f(b) \Rightarrow g(x) \mid f(x)$$

چون $f(x)$ تحویل ناپذیر و تکین است پس $f = g$ یعنی a, b مزدوجند.

بعکس. فرض کنید $p(x)$ چند جمله ای تحویل ناپذیر تکین باشد که $p(a) = p(b) = 0$ حال $f_a : F[X] \to F(a),\ f_b : F[X] \to F(b)$ همریختی پوشا هستند که نتیجه می شود

$f_a : \frac{F(x)}{<p(x)} \to F(a)$ و $f_b : \frac{F[x]}{<p(x)} \to F(b)$ یکریختی هستند. بنابراین $f_b f_a^{-1} : F(a) \to F(b)$ یکریختی است.

تعریف 9.6.4. فرض کنید E یک توسیع متناهی Fباشد. در این صورت E را یک **توسیع نرمال** F نامیم، هرگاه $E_{G(E,F)} = F$.

به عبارت دیگر داریم:

$$\forall x \in E - F, \exists s \in G(E,F) \; s.t. \;\; s(x) \neq x.$$

تعریف 10.6.4. فرض کنید Fیک میدان و $f(x) \in F[x]$ یک چند جمله‌ایی با درجه مثبت باشد. گوییم $f(x)$ در $F[x]$ **تجزیه** می‌شود، اگر $f(x)$ را بتوان به صورت حاصل ضربی از عوامل خطی در $F[x]$ نوشت. یعنی

$$f(x) = u(x - a_1)...(x - a_n)$$

که در آن $u, a_i \in F$.

فرض کنید $f(x) \in F[x]$ یک چند جمله ای با درجه مثبت باشد. گوییم توسیع میدان E از F **میدان تجزیه‌گر** چند جمله‌ایی $f(x)$ روی Fاست هر گاه $f(x)$ در $E[x]$ تجزیه شده و $E = F(u_1,...,u_h)$، که در آن $u_n,...,u_2,u_1$ ریشه های $f(x)$ در E هستند.

فرض کنید S مجموعه‌ایی از چند جمله‌ایی‌های از درجه مثبت در $F[x]$ باشد. گوییم توسیع میدان E از Fمیدان تجزیه‌گر عناصر Sدر $F[x]$است هرگاه هر چند جمله‌ایی از S در $E[x]$ تجزیه شود و E روی F توسط ریشه‌های همه چند جمله ایی های در S تولید گردد.

مثال 11.6.4- 1). $x^2 - 2 \in ¤[x]$ را در نظر می‌گیریم. می دانیم که $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. بنابراین $¤(\sqrt{2}) = ¤(\sqrt{2}, -\sqrt{2})$ یک میدان تجزیه‌گر $x^2 - 2$ روی ¤ است.

2) چند جمله‌ایی $x^3-2\in$ ¤$[x]$ را در نظر می گیریم. می دانیم که $\sqrt[3]{2}$ یک ریشه آن است. ولی $Q(\sqrt[3]{2})$ میدان تجزیه گر آن نیست زیرا دو ریشه دیگر آن مختلط هستند.

تبصره 12.6.4. هر گاه E میدان تجزیه‌گر S روی F باشد و $E=F(X)$ که X مجموعه همه ریشه های چند جمله ایی ها در S است. چون هر عضو X روی F جبری است، پس E روی F جبری است.
اکنون اگر $S=\{f_1,f_2,...,f_k\}$ متناهی باشد. بنابراین $[E:F]$ متناهی است و می توان نشان داد که میدان تجزیه گر S با میدان تجزیه‌گر $g=f_1f_2...f_k$ برابر می باشد. لذا میدان تجزیه گر S در دو حالت S فقط متشکل از یک چند جمله ای باشد یا S نامتناهی باشد بحث میشود.

حال فرض کنید K میدان تجزیه گر $f(x)$ در $F[x]$ و $p(x)$ یک عامل تحویل ناپذیر $f(x)$ در $F[x]$ باشد که $a_1, a_2, ...$ و a_n ریشه های آن هستند، آنگاه به ازای هر i خودریختی مانند $s_i\in G(K,F)$ وجود دارد که $s_i(a_1)=a_i$ (با استفاده از قضایای...)
همچنین می توان نشان داد که هر گاه $f(x)\in F[x]$ از درجه $n\geq 1$ باشد، آنگاه میدان تجزیه گری مانند E از F وجود دارد که $[E:F]\leq n!$.

تعریف 13.6.4. فرض کنید $f(x)\in F[x]$ و E میدان تجزیه گر آن روی F باشد. در این صورت گروه $G(E,F)$، گروه خودریختی های E که هر عنصر F را ثابت نگه می دارد، را **گروه گالوای** $f(x)$ نامیم.

توجه شود که گروه گالوای $f(x)$ را می توان به عنوان گروهی از جایگشتهای ریشه هایش در نظر گرفت. زیرا اگر a ریشه ایی از $f(x)$ باشد و $s\in G(E,F)$ آنگاه $s(a)$ ریشه ایی از $f(x)$ خواهد بود.

حال قضیه ایی را بیان می کنیم که به قضیه **اساسی گالوا** معروف است. این قضیه تناظری یک به یک بین زیرمیدانهای، میدان تجزیه گر $f(x)$ و زیرگروه های گروه گالوای آن به وجود می آورد. همچنین برای به دست آوردن شرطهایی جهت حل پذیری ریشه های یک چند جمله ایی به وسیله رادیکالها به کار می رود.

قضیه14.6.4. فرض کنید که $f(x)\in F[x]$ یک چندجمله با میدان تجزیه گر E و گروه گالوای $G(E,F)$ باشد. به ازای هر زیر میدان T از E که حاوی F باشد، فرض کنید که

$$G(E,T)=\{s\in G(E.F)\mid s(t)=t,\forall t\in T\}$$

و به ازای هر $H\le G(E,F)$، قرار می دهیم:

$$E_H=\{x\in E\mid s(x)=x,\forall s\in H\}$$

در این صورت تناظر یک به یکی از مجموعه همه زیر میدانهای E شامل F به روی مجموعه زیرگروه های $G(E,F)$ وجود دارد $(f(T)=G(E,T))$ که

1) $T=E_G(E,T)$ ،

2) $H=G(E,E_H)$ و $(G(E,F):G(ET))=[T:F]$؛

3) T یک توسیع نرمال F است اگر و فقط اگر $G(E,T)\le G(E.F)$؛

4) اگر T یک توسیع نرمال F باشد آنگاه $\frac{G(E,F)}{G(E,T)}$; $G(T,F)$.

مثال 15.6.4. فرض کنید $E=¤(\sqrt{2},\sqrt{3})$. پس E توسیع نرمال ¤ است و

$$X=\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$$

یک مبنای E روی ¤. بنابراین $G(E,F)=\{s_1,s_2,s_3,s_4\}$ که

1) $s_1=i_d$؛

2) $s_2(\sqrt{2})=-\sqrt{2}$، $s_2(\sqrt{6})=-\sqrt{6}$ و s_2 اعضای دیگر را ثابت نگه می دارد.

3) $s_3(\sqrt{3})=-\sqrt{3}$، $s_3(\sqrt{6})=-\sqrt{6}$ و s_3 بقیه اعضا را ثابت نگه می دارد.

4) $s_4(\sqrt{2}) = -\sqrt{2}$ ، $s_4(\sqrt{3}) = -\sqrt{3}$ و s_4 بقیه اعضا را ثابت نگه می دارد.

و تناظر یک‌به‌یک موردنظر در قضیه گالوا به صورت زیر است:

$\text{¤} \leftrightarrow \{s_1, s_2, s_3, s_4\}$; $\text{¤}(\sqrt{3}) \leftrightarrow \{s_1, s_2\}$

$\text{¤}(\sqrt{2}) \leftrightarrow \{s_1, s_3\}$; $\text{¤}(\sqrt{2}, \sqrt{3}) \leftrightarrow \{s_1\}$.

چون K_4 ; $G(E,F)$، هر زیر گروه $G(E,F)$ نرمال و در نتیجه تمام میدانهای واسطه‌ایی نیز نرمال می‌باشند.

تمرینات

1- میدان تجزیه‌گر چندجمله‌ایی‌های $x^3 - 2, x^4 - 5x^2 + 6 \in \text{¤}[x]$ و $S = \{x^2 - 3, x^2 + 1\}$ را بدست آورید.

2- چندجمله‌ایی منیمال $a = \sqrt{1+\sqrt{3}}$, $b = \sqrt{2} + \sqrt{3}$ را روی ¤ بدست آورید.

3- قرار دهید $u = \sqrt[3]{a + \sqrt{b}}$ که $a, b \in \text{¤}$. مقدار a و b را طوری مشخص کنید که

$\deg(u, \text{¤}) = 1, 2, 3, 6$

آیا ممکن است $\deg(u, \text{¤}) = 4$؟ دلیل خود رابیان کنید.

4- اگر F یک توسیع میدان K و $a \in F$ روی K غیر جبری باشد و $f(x) \in K[x]$ چندجمله‌ایی از درجه بزرگتر یا مساوی یک. ثابت کنید $b = f(a)$ نیز روی K غیر جبری است.

5- اگر ح عددی اول باشد، میدان تجزیه‌گر چندجمله‌ایی $x^p - 2 \in \text{¤}[x]$ را بدست آورید ودرجه توسیع آنرا مشخص کنید.

6- قرار دهید $u = \sqrt[3]{2}$. اولا فرم عناصر $\text{¤}(u)$ را بنویسید. ثانیا عناصر $u^4 - u^3 - u$ ، $\frac{3}{u}$ و $\frac{u-2}{u+2}$ را به‌فرم عناصر $\text{¤}(u)$ بنویسید.

7- نشان دهید که $\text{¤}(\sqrt{2}, i)$ توسیع ساده ¤ است.

8- نشان دهید که هر میدان متناهی بسته جبری نیست.

9- مرتبه‌ی گروه گالوای اعداد مختلط £ را روی میدان اعداد خقیقی ¡ بدست آورید

10- گروه گالوای چندجمله‌ایی های $x^4 - 5x^2 + 6,\ (x^2 - 3)(x^2 + 1) \in \text{¤}[x]$ را روی ¤ بدست آورید.