بررسی و حل

مسائل برگزیده در جبر

برای

دانشجویان و داوطلبان کنکور کارشناسی ارشد رشته ریاضی

تألیف: ناصر عزیزی

ابراهیم رحمانی

بررسی و حل:

مسائل برگزیده در جبر

برای

(دانشجویان و داوطلبان کنکور کارشناسی ارشد رشته ریاضی)

تألیف: ناصر عزیزی زیر نظر: دکتر جواد توکّلی

بررسی و حل مسائل برگزیده در جبر

ناصر عزیزی

چاپ اوّل مرداد ۷۲

ناشر: مؤلّف

تیراژ: ۳۰۰۰ نسخه

حروفچینی: کامپیوتر زمان

چاپ : نهضت

حضرت علی علیه‌السّلام:

«کار کن و اطمینان داشته باش که

کامیاب خواهی شد»

ادیسون:

«نود و نه درصد نبوغ عرق پیشانی

است و یک درصد آن الهام روح»

فهرست

عنوان	صفحه
پیشگفتار مؤلّف	۵
فصل ۱ ـ یادآوری و پیشنیاز	۹
فصل ۲ ـ گروهها	
الف ـ تمرینات بخش گروهها	۳۵
ب ـ حل تمرینات بخش گروهها	۵۰
فصل ۳ ـ حلقه‌ها	
الف ـ تمرینات بخش حلقه‌ها	۱۰۷
ب ـ حل تمرینات بخش حلقه‌ها	۱۱۳
فصل ۴ ـ میدانها و حوزه‌های تجزیه یکتا	
الف ـ تمرینات بخش میدانها و حوزه‌های تجزیه یکتا	۱۳۵
ب ـ حل تمرینات بخش میدانها وحوزه‌های تجزیه یکتا	۱۳۷
فصل ۵ ـ مسائل بدون حل	۱۴۷
ضمیمه علائم و قراردادها	۱۵۳

بنام آنکه جان را فکرت آموخت

پیشگفتار مؤلّف:

کتابی که هم اکنون به لطف خدا موفّق شدم در دسترس شما دانش پژوهان و دانشجویان عزیز قرار دهم شامل سؤالاتی از مباحث نظریه گروهها، حلقه‌ها و میدانها می‌باشد.

کمبود کتاب در این زمینه به زبان انگلیسی و فارسی مرا بر آن داشت تا در جهت رفاه شما دانشجویان گرامی کتاب حاضر را که گلچینی از سئوالات مسابقات ریاضی، کنکور کارشناسی ارشد و سئوالاتی در همان سطح از کتب معتبر جبر می‌باشد، تدوین نمایم.

برای استفاده بهتر ازکتاب تعاریف، قضایا و نکات مهّم جبر به عنوان یادآوری آمده است و در پایان کتاب هم تعداد پنجاه مسئله حل نشده به عنوان خودآزمایی در نظر گرفته شده است. در ضمن سعی شده در هر بخش ازکتاب ابتداء سئوالات مربوط به آن بخش مطرح شود و در پایان همان بخش راه حلّی برای سئوالات آن پیشنهاد کرده‌ایم.

توصیه می‌نمایم که ابتدا با دقّت کامل و فکر متمرکز خود به سئوالات جواب دهید سپس به راه حل پیشنهادی مراجعه نمایید.

از شما می‌خواهیم به ضمیمه علائم و قراردادها در صفحات ۱۵۳ و ۱۵۴ توجّه نمایید.

در اینجا لازم می‌دانم از استادگرامی آقای دکتر جواد توکّلی که هم مشوّق من بوده‌اند و هم از لحاظ علمی در تهیّه این کتاب مرا یاری نموده‌اند تشکّر و قدردانی

نمایم و همچنین از همکاری صمیمانه آقایان محمد حسن حسنی و مسعود والی‌تبار تشکّر نمایم.

با اینکه کوشش شده است تا کتاب بی نقص تهیّه شود ولی مسلماً خالی از اشکال نخواهد بود. لذا خواهشمندم تا با یادآوری ایرادها مؤلّف را مرهون خود سازید.

ناصر عزیزی

فصل ۱

یادآوری و پیشنیاز

هدف این بخش از کتاب یادآوری خلاصه‌ای از مطالب جبر می‌باشد که در حل مسائل نقش اساسی و کلیدی دارند و به آنها نیاز مبرم داریم ولی از اثبات و توضیح دربارهٔ آنها پرهیز می‌نمایم.

نظریه گروهها:

۱ ـ تعریف: ساختمان جبری $(G, *)$ راکه G در آن یک مجموعه و $*$ یک عمل دو تایی روی آن است **گروه** نامند. اگر به ازای هر x و y و z در G داشته باشیم:

الف ـ (شرکت پذیری) $x*(y*z) = (x*y)*z$

ب ـ (عضو همانی) به ازای هر x در G عضوی مانند e در G موجود باشد بطوریکه:

$$x*e = e*x = x$$

ج ـ (وارون پذیری) به ازای هر x در G، عضوی چون y از G وجود داشته باشد بطوریکه $y*x = x*y = e$

تذکّر: چون وارون هر عضو یکتا است بنا بر این، وارون x را با نماد x^{-1} نمایش می‌دهیم و برای سادگی به جای $x*y$، xy می‌نویسیم.

۲ ـ گروه G را آبلی (جابجائی) گویند اگر به ازای هر y و x متعلّق به G داشته

باشیم

$$xy = yx$$

۳ـ تعداد اعضای مجموعهٔ G را مرتبه گروه G می‌نامند و آنرا با $|G|$ یا $O(G)$ نمایش می‌دهند.

۴ـ اگر H یک زیر مجموعه G باشد آنگاه H را یک زیرگروه G نامند اگر H همراه با عمل دوتایی G خود یک گروه باشد. در اینحالت می‌نویسیم $H \leq G$

تذکّر: $\{e\}$ و G زیرگروههای بدیهی، G نامیده می‌شوند.

۵ـ قضیه: فرض کنیم G یک گروه باشد و H زیر مجموعه‌ای از G، در اینصورت H زیرگروه G است. اگر و فقط اگر (۱) $e \in G$ (۲) به ازای هر $a, b \in H$، $ab \in H$ (۳) به ازای هر $a \in H$، $a^{-1} \in H$

۶ـ فرکنیم X یک زیر مجموعه‌ای از G باشد کوچکترین زیرگروه G شامل X را زیرگروه تولید شده توسط X نامند و با $< X >$ نمایش می‌دهند.

۷ـ تعریف: گروه G را یک گروه دوری نامند در صورتیکه، عضوی چون a از G وجود داشته باشد بطوریکه: $G = < a >$

۸ـ قضیه: فرض کنیم $G = < a >$ یک گروه دوری باشد.

الف ـ اگر G نا متناهی باشد آنگاه a و a^{-1} تنها مولدهای G می‌باشند

ب ـ اگر G متناهی و از مرتبهٔ n باشد آنگاه به ازای هر r که $(r, n) = ۱$، a^r یک مولد G خواهد بود و بالعکس اگر a^r یک مولد G باشد $(r, n) = ۱$ خواهد بود.

۹ـ اگر G یک گروه و a عضوی از آن باشد، کوچکترین عدد طبیعی چون n را که $a^n = e$، مرتبه a گوییم و با $o(a)$ نشان می‌دهیم.

۱۰ ـ تعریف: دو گروه $G_۱$ و $G_۲$ را یکریخت نامند اگر تابع دوسوئی $\varphi: G_۱ \longrightarrow G_۲$ وجود داشته باشد بطوریکه:

$\forall x, y \in G_1 , (xy)\varphi = (x\varphi)(y\varphi)$

و می‌نویسند: $G_1 \cong G_2$

۱۱ ـ قضیه:

الف ـ هر گروه دوری نامتناهی با گروه $\mathbf{Z}$ یکریخت است.

ب ـ هر گروه دوری متناهی از مرتبه n با گروه $\mathbf{Z_n}$ یکریخت است.

ج ـ زیرگروه هر گروه دوری، دوری است.

۱۲ ـ قضیه: اگر G یک گروه باشد و $a \in G$ آنگاه $o(a) = |< a >|$

۱۳ ـ تعریف : اگر G_1 و G_2 دو گروه باشند آنگاه $G_1 \times G_2$ را گروه حاصلضرب G_1 در G_2 نامند در صورتیکه عمل دوتایی زیر در آن تعریف شود.

$\forall x_1, y_1 \in G_1$

$\forall x_2, y_2 \in G_2$

$$(x_1 , x_2) . (y_1 , y_2) = (x_1y_1 , x_2y_2)$$

۱۴ ـ تعریف: فرض کنید H زیرگروه G و $a \in G$ مجموعه

$$aH = \{ ah \mid h \in H \}$$

را یک همرده چپ H در G نامند و به همین ترتیب $Ha = \{ ha \mid h \in H \}$ یک همرده راست H در G می‌باشد.

۱۵ ـ قضیه:

الف ـ به ازای هر a و b از G، $aH = bH$ اگر و تنها اگر $a^{-1} b \in H$ و $Ha = Hb$ اگر و تنها اگر $ab^{-1} \in H$.

ب ـ به ازای هر a در G، $|aH| = |H| = |Ha|$

تذکّر: تعداد همرده‌های راست یا تعداد همرده‌های چپ H در G را اندیس H در G نامند و با $[G : H]$ نمایش می‌دهند.

۱۶ ـ تعریف : فرض کنیم G یک گروه باشد و به ازای هر i از I، $a_i \in G$ کوچکترین زیرگروه G شامل $\{ a_i \mid i \in I \}$ زیرگروه تولید شده توسط $\{ a_i \mid i \in I \}$ نامیده می‌شود

اگر این زیرگروه خود G باشد، گفته می‌شود $\{ a_i \mid i \in I \}$، G را تولید کرده است.

اگر مجموعه‌ای متناهی مانند $\{ a_i \mid i \in I \}$، گروه G را تولید کند آنگاه G یک گروه متناهیاً تولید شده نامیده می‌شود.

۱۷ ـ قضیه: اگر G یک گروه باشد و به ازاء هر i از I و $a_i \in G$ آنگاه زیر گروه H از G تولید شده توسط $\{ a_i \mid i \in I \}$ دقیقاً از تمام اعضایی از G تشکیل می‌شود که بصورت حاصلضرب متناهی از توانهای صحیح a_iها باشند. در اینجا توانهای یک a_i ثابت می‌تواند چندین بار در حاصلضرب ظاهر شود.

۱۸ ـ تعریف: گروه G یک گروه تابی است در صورتیکه هر عضو آن از مرتبهٔ متناهی باشد. G بدون تاب است در صورتیکه به جز عضو همانی عضوی از مرتبهٔ متناهی نداشته باشد.

۱۹ ـ قضیه: در هر گروه آبلی G، مجموعه T متشکل از همهٔ اعضای از مرتبه متناهی G یک زیرگروه G است، که آن را زیرگروه تابی G نامیم.

۲۰ ـ قضیه لاگرانژ: اگر H زیرگروه G باشد آنگاه $o(G)=[G:H]\, o(H)$ و اگر G متناهی باشد آنگاه $o(H) \mid o(G)$

نتیجه: مرتبهٔ هر عضو یک گروه متناهی، مرتبهٔ گروه را می‌شمارد به عبارت دیگر اگر G متناهی باشد و $a \in G$، $a^{o(G)} = e$

۲۱ ـ قضیه: هر گروه متناهی از مرتبه یک عدد اوّل p دوری است و لذا یکریخت با $\mathbf{Z}_p$ می‌باشد.

۲۲ ـ تعریف: اگر $H \leq G$ باشد، H را نرمال گویند اگر $\forall a \in G : a^{-1}Ha \subseteq H$ و بصورت $H \trianglelefteq G$ نمایش می‌دهند.

۲۳ ـ قضیه: اگر $\varphi : G_1 \longrightarrow G_2$ یک همریختی گروهی باشد واضح است $G_1\varphi$ زیرگروه G_2 است و $\operatorname{Ker}\varphi = \{ a \in G_1 \mid a\varphi = e_2 \}$ یک زیرگروه نرمال G_1 خواهد بود ($\ker\varphi$ را هسته φ نامند).

۲۴ ـ قضیه اساسی همریختی

اگر $\varphi : G_1 \longrightarrow G_2$ همریختی باشد و $k = \ker\varphi$ آنگاه یکریختی یکتا $f: G_1/k \longrightarrow G_2\varphi$ وجود دارد بطوریکه به ازای هر a از G_1، $(ak)f = a\varphi$.

۲۵ ـ قضیه: اگر $H \trianglelefteq G$، آنگاه هر زیرگروه G/H به صورت K/H است بطوریکه $H \leq K \leq G$ به علاوه K/H در G/H نرمال است اگر و تنها اگر $K \trianglelefteq G$.

۲۶ ـ اگر G یک گروه باشد و $x, y \in G$ آنگاه $x\,y\,x^{-1}\,y^{-1}$ را یک برگرداننده گویند. و زیرگروه G' از G را که توسط مجموعهٔ همه برگردانندههای G تولید شده، را زیرگروه برگرداننده یا مشتق G نامند. در اینصورت احکام زیر بدست می‌آید $G' \trianglelefteq G$ و G/G' آبلی است و همچنین اگر $H \trianglelefteq G$ و $\frac{G}{H}$ آبلی باشد آنگاه $G' \leq H$.

قضایای یکریختی و سری گروهها

۱ ـ قضیه اوّل یکریختی:

فرض کنید G و G' دو گروه دلخواه و $\varphi : G \longrightarrow G'$ یک همریختی با هستهٔ K باشد و فرض کنید $\gamma : G \longrightarrow G/K$ برو ریختی متعارف باشد، در اینصورت وجود دارد یکریختی یکتا $f : G/K \longrightarrow G\varphi$ بطوریکه :

$$\forall x \in G \quad \varphi(x) = f\gamma(x)$$

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G\varphi \leq G' \\ & {\scriptstyle\gamma}\searrow \quad \nearrow{\scriptstyle f} & \\ & G/K & \end{array}$$

۲ ـ قضیه دوّم یکریختی: فرض کنید G یک گروه، $H \leq G$ و $N \trianglelefteq G$

آنگاه $\dfrac{HN}{N} \cong \dfrac{H}{H \cap N}$.

۳ ـ قضیه سوّم یکریختی: فرض کنید K و H دو زیرگروه نرمال در G باشند بطوریکه $K \leq H$ در اینصورت یکریختی زیر برقرار است.

$$\frac{G}{H} \cong \frac{G/K}{H/K}$$

۴ ـ تعریف: یک سری زیر نرمال از گروه G عبارتست از دنبالهٔ متناهی H_0 و H_1 و .... و H_n از زیرگروههای G به قسمی که به ازای هر i که $0 \leq i \leq n-1$ داشته باشیم $H_i \trianglelefteq H_{i+1}$ و $\langle e \rangle = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_n = G$

اگر هر یک از H_i ها در G نیز نرمال باشند، سری را نرمال گویند.

نتیجه: بنا به تعریف بالا و با توجّه به خواص گروههای آبلی نتیجه می‌شود که اگر G یک گروه آبلی باشد آنگاه هر سری زیر نرمال، نرمال خواهد بود.

۵ـ تعریف: دو سری زیر نرمال (نرمال) $\{ H_i \}$ و $\{ K_j \}$ را یکریخت گویند، اگرکه یک تناظر یک به یک بین مجموعه $\{ \frac{H_{i+1}}{H_i} \}$ و $\{ \frac{K_{j+1}}{K_j} \}$ موجود باشد به نحوی که عوامل متناظر یکریخت باشند.

۶ـ قضیه شریر:

دو سری زیر نرمال (نرمال) از گروه G دارای تظریفهای یکریخت هستند.

۷ ـ تعریف: گروه G را ساده گویند اگر G هیچ زیر گروه نرمال غیر بدیهی نداشته باشد.

۸ـ تعریف: سری زیر نرمال $\langle e \rangle = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = H$ را یک سری ترکیب گویند، اگر $\frac{H_{i+1}}{H_i}$ یک گروه ساده باشد $(i = 1, 2, \dots, n)$

۹ـ قضیه جردن هُلدر:

هر دو سری ترکیب برای گروهی مانند G یکریختند.

۱۰ ـ تعریف: گروه G را حلپذیر گویند، اگر برای G یک سری زیرنرمال $\{ H_i \}$ وجود داشته باشد بطوریکه $\frac{H_{i+1}}{H_i}$ آبلی باشد. $(i = 1,2,\dots, n)$

عمل گروه روی یک مجموعه و قضایای سیلو

۱ ـ تعریف: فرض کنید G یک گروه و X یک مجموعه دلخواه باشد: عمل گروه G بر روی X عبارتست از تابع $* : X \times G \longrightarrow X$ بطوریکه ضابطه آن بصورت:

$$\forall x \in X , \forall g \in G : * (x , g) = x . g$$

و با خاصیت زیر باشد (توجه کنید $x . g$ یعنی عمل g بر x)

$$x (g_1 g_2) = (x g_1) g_2 \qquad (2) \qquad x . e = x \quad (1)$$

که $g_1 , g_2 \in G$ و e عضو همانی G است. در اینحالت X را یک G - مجموعه گویند.

۲ ـ زیرگروههای ایزتروپی (پایدارکننده):

فرض کنید G یک گروه و X یک G - مجموعه باشد و $x \in X$، $g \in G$ مجموعه تمام عناصری از X که تحت عمل گروه، ثابت می‌مانند را به G_x نشان می‌دهیم یعنی:

$$G_x = \{ g \in G \mid x.g = x \} \text{ و } X_g = \{ y \in X \mid y . g = y \}$$

در اینصورت طبق تعریف مجموعه‌های بالا واضح است که $G_x \subseteq G$ و $X_g \subseteq X$ قضیه زیر خواص دیگری را برای G_x بیان می‌کند.

۳ ـ قضیه : فرض کنید X یک G - مجموعه باشد، در اینصورت

$$\forall x \in X : G_x \leq G$$

۴ ـ تعریف: فرض کنید X یک G - مجموعه و $x \in X$ در اینصورت G_x را زیرگروه ایزتروپی x گویند.

۵ ـ فرض کنید X یک G - مجموعه باشد برای $x_1, x_2 \in X$، $x_1 \sim x_2$ (x_1 را هم ارز x_2 گوئیم) اگر و تنها اگر وجود داشته باشد عضوی چون g از G به قسمی که $x_1 . g = x_2$ در اینصورت رابطه $\sim$ یک رابطه هم ارزی روی X است.

۶ ـ تعریف: فرض کنید X یک G - مجموعه باشد، به ازای هر x از X، مجموعه xG را به صورت زیر تعریف می‌کنیم و آن را مدار X می‌نامیم.

$$xG = \{ xg \mid g \in G \}$$

با توجه با تعریف بالا داریم:

$xG = yG \Leftrightarrow x \sim y$ و $xG \cap yG = \phi \Leftrightarrow$ (x و y هم ارز نباشند)

و

$$X = \bigcup_{x \in X} xG$$

۷ ـ قضیه: فرض کنید X یک G - مجموعه باشد آنگاه: $|xG| = [G : G_x]$

۸ ـ قضیه برنساید: فرض کنید G یک گروه متناهی و X یک G - مجموعه متناهی باشد اگر تعداد مدارها در X برابر r باشد آنگاه:

$$r \mid G \mid = \sum_{g \in G} \mid X_g \mid$$

نتیجه: اگر G یک گروه متناهی و X یک G - مجموعه متناهی باشد در اینصورت

$$\text{تعداد مدارهای } X = \frac{1}{|G|} \sum_{g \in G} \mid X_g \mid$$

۹ ـ تعریف: فرض کنید p یک عدد اوّل باشد، G را یک p -گروه گویند، اگر مرتبهٔ هر عنصر آن توانی از p باشد.

بنا به تعریف بالا واضح است که مرتبهٔ هر p -گروه متناهی توانی از p است.

۱۰ ـ قضیه: فرض کنید مرتبه G به صورت p^n باشد (p عدد اوّل است) و فرض کنید X یک G - مجموعه متناهی باشد، آنگاه (هنگ p) $|X_G| \equiv |X|$ که در آن

$$X_G = \{ x \in X \mid x.g = x \quad \forall g \in G \}$$

۱۱ ـ قضیهٔ کشی: فرض کنید G یک گروه متناهی و p یک عدد اوّل باشد بطوریکه $p \mid\mid |G| = n$ آنگاه G حداقل یک عنصر از مرتبه p دارد و در نتیجه یک زیرگروه از مرتبه p دارد.

۱۲ ـ قضیه: اگر H یک p زیرگروه ازگروه متناهی G باشد بطوریکه

$p \mid [G:H]$ آنگاه $(H \neq N_G(H)) \; H \lhd N_G(H)$

۱۳ ـ قضیه اوّل سیلو: فرض کنید G یک گروه متناهی از مرتبه $P^n m$ باشد که p یک عدد اوّل است و $n \geq ۱$، $(p , m) = ۱$ آنگاه به ازای هر i که $۱ \leq i \leq n$، G یک زیرگروه از مرتبه p^i دارد و زیرگروه p^i عضوی در زیرگروه از مرتبه $p^{i+۱}$ نرمال می‌شود.

۱۴ ـ تعریف: فرض کنید G یک گروه و $P \mid\mid |G|$ آنگاه P را یک p - زیر گروه سیلو گویند اگر نسبت به مرتبه‌اش ماکزیمال باشد، یعنی اگر H یک P - زیر گروه G باشد و $P \leq H \leq G$ آنگاه $P = H$

۱۵ ـ قضیه دوّم سیلو: اگر G یک گروه از مرتبه $p^n m$ که $(p , m) = ۱$ و P یک p - زیرگروه سیلوی G باشد آنگاه $x \in G$ وجود دارد بطوریکه

$H \leq x\ p\ x^{-1}$ بخصوص هردو زیرگروه سیلو مزدوج یکدیگرند.

۱۶ ـ قضیهٔ سوّم سیلو:

اگر G یک گروه متناهی و p یک عدد اوّل باشد بطوریکه $p \mid |G|$ در اینصورت تعداد p - زیرگروههای سیلو G، مرتبهٔ G را عاد می‌کند و برابر $k\,P+1$ ($k \in Z^+$) می‌باشد.

نتیجه: اگر G فقط یک p - زیرگروه سیلو داشته باشد، در اینصورت این زیر گروه در G نرمال است.

۱۷ ـ قضیه: هر p -گروه متناهی حلپذیر است.

۱۸ ـ قضیه: مرکز هر p -گروه متناهی غیر بدیهی است.

۱۹ ـ قضیه: هرگروه از مرتبه p^2 آبلی است (p یک عدد اوّل است).

نظریه حلقه‌ها

۱ ـ تعریف: مجموعه غیر تهی R همراه با دو عمل دو تایی + و ۰ را یک حلقه می‌نامند اگر:

(الف) $(R, +)$ گروه آبلی باشد.

(ب) شرکت پذیری : به ازای هر a و b و c از R $a(bc) = (ab)c$

(ج) به ازای هر $a, b, c \in R$، $a(b + c) = ab + ac$

و $(b + c)a = ba + ca$

۲ ـ حلقه R را تعویض پذیر (جابجائی) می‌گوئیم اگر به ازای هر a و b از R، $ab = ba$ اگر R نسبت به عمل ضرب دارای عضو همانی باشد، آنگاه این عضو را با 1_R یا بطور اختصار با ۱ نشان می‌دهیم و آنرا عنصر یکه R می‌گوئیم اگر R حلقه یکدار باشد همچنین a و b اعضایی از R باشند که $ab = 1$ آنگاه a را واحد یا عضو وارون پذیر می‌نامند.

۳ ـ تعریف: اگر F یک حلقه تعویض پذیر و یکدار بدون مقسوم علیه صفر باشد همچنین هر عضو نا صفر آن واحد باشد آنگاه F را یک میدان گویند.

۴ ـ تعریف: می‌گوئیم حلقه R بدون مقسوم علیه صفر است اگر به ازای هر a و b از R

$ab = 0 \Rightarrow a = 0$ یا $b = 0$

هر حلقه تعویض پذیر، یکدار بدون مقسوم علیه صفر را دامنه (حوزه) صحیح گویند.

۵ـ تعریف: زیر مجموعه S از حلقه R یک زیر حلقه R است اگر S نا تهی باشد و به ازای هر a و b از S، a.b و a - b اعضایی از S باشند.

۶ـ زیر حلقه I از R را ایده‌آل R گویند هرگاه به ازای هر $a \in I$ و $r \in R$، ar و ra در I باشند. بنابر این $I \subseteq R$ یک ایده‌آل R است اگر و فقط اگر:

(الف) $I \neq \phi$ (ب) $\forall a, b \in I : a-b \in I$

(ج) $\forall a \in I, \forall r \in R : ar, ra \in I$

۷ـ تعریف: فرض کنید R یک حلقه و $a \in R$ باشد. آنگاه کوچکترین ایده‌آل R را که شامل a باشد ایده‌آل اصلی با مولد a گویند و آنرا با $<a>$ نشان می‌دهند.

اگر حلقه R تعویض پذیر، یکدار باشد آنگاه $< a > = aR = Ra$ به عبارت دیگر $< a > = \{ ra \mid r \in R \}$

۸ـ قضیه: اگر I یک ایده‌آل از حلقه یکدار R باشد آنگاه $I = R$ اگر و تنها اگر I شامل یک عضو واحد باشد بویژه $I = R$ اگر و تنها اگر $1 \in I$

تذکّر: ایده‌آلها در نظریه حلقه‌ها همتای زیرگروههای نرمال در نظریه گروهها می‌باشند به عبارت دیگر اگر I یک ایده‌آل حلقه R باشد آنگاه:

$$\frac{R}{I} = \{ a + I \mid a \in R \}$$

همراه با اعمال جمع و ضرب

$$a, b \in R \quad (a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

یک حلقه است، $\frac{R}{I}$ را حلقه خارج قسمت R بر I گویند.

اگر R تعویض پذیر، یکدار باشد آنگاه $\frac{R}{I}$ نیز چنین است.

۹ـ تعریف: ایده‌آل I از حلقه R ماکسیمال نامیده می‌شود اگر $I \neq R$ و به

ازای هر ایده‌آل K از R

$$I \leq K < R \Rightarrow I = K \text{ یا } K = R$$

۱۰ ـ تعریف: ایده‌آل I از حلقه تعویض پذیر R را اوّل گویند اگر به ازای هر a و b از R

$$ab \in I \Rightarrow a \in I \text{ یا } b \in I$$

۱۱ ـ قضیه: فرض کنیم حلقه R تعویض پذیر و یکدار باشد آنگاه:

الف ـ ایده‌آل M از R ماکسیمال است اگر و تنها اگر $\frac{R}{M}$ میدان باشد.

ب ـ ایده‌آل P از R اوّل است اگر و تنها اگر $\frac{R}{P}$ دامنه صحیح باشد.

۱۲ ـ تعریف: فرض کنیم R و S دو حلقه باشند تابع $\varphi : R \longrightarrow S$ را همریختی حلقه‌ای گویند اگر به ازای هر a و b از R

$$(a + b)\varphi = a\varphi + b\varphi \quad \text{و} \quad (ab)\varphi = (a\varphi)(b\varphi)$$

اگر همریختی φ دو سویی باشد آنگاه φ را یکریختی نامند در اینحالت R را یکریخت S گویند و می‌نویسند: $R \cong S$

۱۳ ـ تعریف: اگر I ایده آل حلقه R باشد آنگاه $\gamma : R \longrightarrow \frac{R}{I}$ با تعریف $a\gamma = a + I$ و $a \in R$ یک همریختی پوشا است.

در این صورت γ را همریختی طبیعی نامند.

۱۴ ـ اگر $\varphi : R \longrightarrow S$ همریختی حلقه‌ای باشد آنگاه $R\varphi$ زیر حلقه S و $\ker\varphi = \{ a \in R \mid a\varphi = 0 \}$ ایده آل R است.

۱۵ ـ قضیه اساسی همریختی (برای حلقه‌ها)

اگر $\varphi : R \longrightarrow S$ همریختی حلقه‌ای باشد و $K = \ker\varphi$ آنگاه یکریختی منحصر بفرد $\psi : \frac{R}{K} \longrightarrow R\varphi$ وجود دارد بطوریکه به ازای هر a از R،

$$(a + K)\psi = a\varphi$$

۱۶ ـ تعریف: فرض کنیم R یک حلقه باشد در اینصورت کوچکترین عدد طبیعی n را بطوریکه به ازای هر a در R، $na = 0$ مشخصه R گویند.

اگر چنین عددی وجود نداشت، آنگاه مشخصه R برابر صفر تعریف می‌شود.

۱۷ ـ قضیه: مشخصه هر دامنه صحیح (بویژه هر میدان) برابر با صفر یا عدد اوّل است .

۱۸ ـ قضیه: اگر حلقه R یکدار باشد، آنگاه مشخصه R برابر با $n > 0$ است اگر و تنها اگر n کوچکترین عدد طبیعی باشد بطوریکه $n.1 = 0$.

۱۹ ـ قضیه: هر میدان با مشخصه صفر (P) زیر میدانی یکریخت با Q (Z_p) دارد.

۲۰ ـ تعریف: میدانهای Q و Z_p را میدانهای اوّل گویند.

حلقه چند جمله‌ایها

۱ ـ تعریف: فرض کنیم R یک حلقه باشد، یک چند جمله‌ای $f(x)$ با ضرایب در R عبارتست از سری نامتناهی $f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots$ که

$a_i \in R$

$a_i = 0$ به جز تعداد متناهی از a_iها که احتمالاً مخالف صفرند.

a_iها را ضریب چند جمله‌ای گویند و بزرگترین اندیس i که $a_i \neq 0$ را درجهٔ $f(x)$ گویند، اگر چنین iای وجود نداشت، $f(x)$ درجه ندارد و اگر $i = 0$ گوئیم درجه $f(x)$ صفر است.

۲ ـ قضیه: مجموعه تمام چند جمله‌ایها بر روی حلقه R که با $R[x]$ نشان می‌دهیم با اعمال جمع و ضرب زیر، یک حلقه است.

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

$$g(x) = b_m x^m + \ldots + b_1 x + b_0$$

فرض کنیم $m < n$،

$$f_{(x)} + g_{(x)} = a_n x^n + \ldots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \ldots + a_0 + b_0$$

$$f_{(x)} g_{(x)} = \sum_{k=0}^{m+n} c_k x^k \qquad : c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

اگر R تعویض پذیر و یکدار باشد، $R[x]$ نیز چنین است.

۳ ـ قضیه: فرض کنید E و F دو میدان و $F \subseteq E$ و $\alpha \in E$، x نیز یک متغیر

است در اینصورت تابع $\varphi_\alpha : F[x] \longrightarrow E$ را که با ضابطه $\varphi_\alpha (f(x)) = f(\alpha)$

تعریف می‌شود یک همریختی حلقه‌ای است ضمناً $\varphi_\alpha(x) = \alpha$.

$\varphi_\alpha (a) = a \quad \forall a \in F$: یعنی φ_α روی F همانی است.

۴ـ قضیه الگوریتم تقسیم در $F [x]$:

فرض کنید $f(x) = a_n x^n + ... + a_0$ و $g(x) = b_m x^m + ... + b_0$

بطوریکه $a_n , b_m \neq 0$ دو عنصر $F[x]$ باشند آنگاه عناصر یکتای $q(x)$ و $r(x)$ در $F [x]$ وجود دارند بطوریکه:

$f(x) = g(x) q(x) + r(x)$ که $r(x) = 0$ یا $0 \leq \deg r(x) < m$

۵ـ قضیه: عنصر a در F ریشه (صفر) چند جمله‌ای $f(x) \in F[x]$ است اگر و تنها اگر $(x - a)$ عاملی از $f(x)$ باشد یعنی $f(x) = (x - a) g(x)$

۶ـ قضیه: فرض کنید $f(x) \in F[x]$ یک چند جمله‌ای باشد که $\deg f(x) = n$ در اینصورت $f(x)$ حداکثر n ریشه در میدان F دارد.

۷ـ قضیه: اگر $f(x) = x^n + a_{n-1} x^{n-1} + ... + a_0$ عضوی از $\mathbf{Z}[x]$ باشد که $a_0 \neq 0$ اگر $f(x)$ یک ریشه در $\mathbf{Q}$ داشته باشد در اینصورت یک ریشه در $\mathbf{Z}$ نیز دارد و اگر ریشهٔ آن b باشد آنگاه $b | a_0$

۸ـ تعریف: چند جمله‌ای غیر ثابت $f(x)$ در $F[x]$ را بر روی F تحویل ناپذیر گویند اگر $f(x)$ را نتوان به صورت حاصلضرب دو چند جمله‌ای غیر ثابت نوشت.

۹ـ فرض کنید $f(x) \in F[x]$ و درجه $f(x)$، ۲ یا ۳ باشد در اینصورت $f(x)$ تحویل پذیر است اگر و تنها اگر در F یک ریشه داشته باشد.

۱۰ـ قضیه (محك آیزنشتاین):

فرض کنید p عدد اوّل باشد و $f(x) = a_n x^n + ... + a_0$ عضوی از $\mathbf{Z}[x]$ باشد که p، a_n را عاد نمی‌کند و $\forall i \quad 0 \leq i < n : p \mid a_i$ و p^2، a_0 را

عاد نمی‌کند در اینصورت $f(x)$ بر روی Q تحویل‌ناپذیر است.

۱۱ ـ قضیه: اگر F یک میدان باشد در اینصورت تمام ایده‌آلهای $F[x]$ اصلی هستند.

۱۲ ـ ایده‌آل نا صفر $<p(x)>$ در $F[x]$ ماکزیمال است اگر و تنها اگر $p(x)$ تحویل ناپذیر باشد.

۱۳ ـ تعریف: اگر $f(x)$ و $g(x)$ اعضایی از $F[x]$ باشند بطوریکه $q(x)$ ای از $F[x]$ وجود داشته باشد که $f(x) = q(x)\, g(x)$ در اینصورت گویند $g(x)$، $f(x)$ را عاد می‌کند و با نماد $g(x) \mid f(x)$ نشان می‌دهند.

۱۴ ـ قضیه: فرض کنید $p(x)$ یک چند جمله‌ای تحویل ناپذیر باشد و $p(x) \mid r(x)\, s(x)$ آنگاه $p(x) \mid r(x)$ یا $p(x) \mid s(x)$

۱۵ ـ اگر a و b اعضایی از حوزه صحیح D باشند آنها را وابسته (شریک) گوییم هرگاه عضو واحدی مانند u در D باشد بطوریکه $a = bu$.

۱۶ ـ تعریف: یک حوزه صحیح را با تجزیه یکتا (U F D)گوییم هرگاه :

الف ـ هر عنصر D که صفر و واحد نباشد، بتوان به حاصلضرب عناصر تحویل ناپذیر (متناهی) تجزیه کرد.

ب ـ اگر $p_1 , \dots , p_r$ و $q_1 , \dots , q_s$ دو تجزیه مختلف برای عنصر d در D باشند در اینصورت $r = s$ و p_i و q_i وابسته باشند.

۱۷ ـ تعریف: حوزه صحیح با ایده‌آلهای اصلی عبارتست از حوزه صحیحی که هر ایده‌آل آن اصلی باشد و آنرا با نماد PID نشان می‌دهیم.

۱۸ ـ تعریف: فرض کنید D یک حوزه صحیح باشد عنصر غیر صفر و غیر واحد p از D را اوّل گویند اگر $p \mid ab$ آنگاه $p \mid a$ یا $p \mid b$.

۱۹ ـ قضیه: در هر PID هر عنصر تحویل ناپذیر، اوّل است، توجه شود که

عکس این مطلب فقط در UFD درست است. (بطور کلی در UFD تحویل ناپذیری و اوّل بودن معادلند).

۲۰ ـ قضیه: هر PID یک UFD است.

نتیجه: $\mathbf{Z}$ و $F[x]$ هر دو UFD هستند.

۲۱ ـ قضیه: فرض کنید D یک UFD و F میدان خارج قسمت D باشد، اگر $f(x) \in D[x]$ تحویل ناپذیر باشد آنگاه $f(x)$ در $F[x]$ تحویل ناپذیر است.

۲۲ ـ قضیه: اگر D یک UFD باشد آنگاه $D[x]$ نیز یک UFD است.

حوزه‌های اقلیدسی

۲۳ ـ تعریف: فرض کنید D یک حوزه صحیح باشد، یک ارزیاب اقلیدسی بر روی D عبارتست از یک تابع چون $\gamma : D \longrightarrow \mathbf{Z}$ که در شرایط زیر صدق کند.

الف ـ $\forall a \in D \quad \gamma(a) \geq 0$

ب ـ $\forall a,b \in D \; \exists q,r \in D : a = bq+r$

$: r = 0$ یا $0 \leq \gamma(r) < \gamma(b)$

ج ـ $\forall a,b \in D \; , \; a \neq 0 \neq b \; , \; \gamma(a) \leq \gamma(ab)$

اگر D دارای یک ارزیاب اقلیدسی باشد آن را یک حوزه اقلیدسی (ED) گویند.

۲۴ ـ قضیه: هر حوزه اقلیدسی (ED) یک PID و یک UFD است.

۲۵ ـ هر میدانی یک حوزه اقلیدسی بوده و هر حوزه اقلیدسی یک PID است، هر PID، UFD بوده و لذا بطور خلاصه می‌توان توسط دیاگرام زیر نشان

داد.

$$F \subseteq ED \subseteq PID \subseteq UFD \subseteq ID \subseteq R$$

توجه: ID حوزه صحیح و R حلقه است.

مختصری در بارهٔ میدانها

۱ ـ تعریف: فرض کنید F یک میدان باشد یک توسیع برای این میدان عبارتست از میدان E بقسمی که همریختی یک به یک از F به F وجود داشته باشد و در اینحالت می‌نویسند $F \leq E$

۲ ـ قضیهٔ (کرونکر): فرض کنید F یک میدان و $f(x) \in F[x]$ یک چند جمله‌ای غیر ثابت باشد آنگاه توسیعی از F مانند E و $\alpha \in E$ وجود دارد بطوریکه $f(\alpha) = 0$

۳ ـ تعریف: فرض کنید $F \leq E$ یک توسیع باشد عنصر $\alpha \in E$ را روی F جبری گویند اگر چند جمله‌ای غیر صفر $f(x)$ در $F[x]$ وجود داشته باشد بطوریکه $f(\alpha) = 0$ در غیر اینصورت α را متعالی گویند.

۴ ـ قضیه: فرض کنید $F \leq E$ یک توسیع از F باشد و $\alpha \in E$ روی F جبری باشد آنگاه چند جمله‌ای تحویل ناپذیر $p(x) \in F[x]$ وجود دارد بطوریکه $p(\alpha) = 0$ ، $\forall f(x) \in F[x] : f(\alpha) = 0 \Rightarrow p(x) \mid f(x)$ ، $p(x)$ را چند جمله‌ای می‌نیمال برای α روی F گویند و می‌توان $p(x)$ را تکین نیز فرض کرد.

۵ ـ قضیه: فرض کنید $F \leq E$ و $E \leq K$ دو توسیع متناهی باشند آنگاه توسیع $F \leq K$ متناهی می‌شود و داریم $[K : F] = [K : E]\,[E : F]$

۶ ـ قضیه: هر توسیع متناهی جبری است.

۷ ـ قضیه: اگر $F \leq E$ یک توسیع و $\alpha \in E$ روی F جبری باشد و $\beta \in F(\alpha)$ آنگاه:

$[F(ß) : F] \mid [F(\alpha) : F]$

۸ـ تعریف: میدان F را بطور جبری بسته گویند اگر هر چند جمله‌ای بر روی F در F بطور خطی تجزیه شود یعنی :

$$\forall f(x) \in F[x] \qquad f(x) = (x - c_1)^{d1} \ldots (x - c_n)^{dn}$$

فصل ۲

گروهها

تمرینات بخش گروهها

۱ ـ فرض کنید R^* مجموعهٔ تمام اعداد حقیقی نا صفر باشد در R^* عمل o را با ضابطهٔ $aob = |a|b$ تعریف کنید.

الف) نشان دهید o عمل دوتایی شرکت پذیری را در R^* به دست می‌دهد.

ب) نشان دهید که نسبت به o در R^* عضو همانی چپ وجود دارد و هر عضو دارای معکوس راست نیز می‌باشد.

ج) آیا R^* با این عمل دوتایی یک گروه است؟

د) فایده این تمرین را بیان کنید.

۲ ـ اگر در مجموعه‌ای چون S، o عمل دوتایی باشد آنگاه عضو x از S را نسبت به o **خودنما** می‌نامیم در صورتی که $xox = x$. ثابت کنید که هر گروه دقیقاً یک عضو خود نما دارد.

۳ ـ نشان دهید که هر گروه G با عضو همانی e که از آن برای هر x از G، $xox = e$ آبلی است. (o عمل دوتایی G است).

۴ ـ ثابت کنید که مجموعه‌ای چون G با عمل دوتایی چون o شرکت پذیر بوده و عضو همانی چپ و هر عضو آن معکوس چپ داشته باشد، G یک گروه است.

۵ ـ ثابت کنید هر مجموعهٔ نا تهی G با عمل دوتایی شرکت پذیری چون o واجد این خاصیّت که به ازای هر a و b از G معادله‌های $aox = b$ و $yoa = b$ در G دارای جواب باشند یک گروه است.

✓ ۶ ـ فرض کنید S یک مجموعه n عضوی باشد چند عمل دوتایی متمایز می‌توان روی S تعریف کرد، چند تا از این اعمال جابجائی هستند.

✓ ۷ ـ نشان دهید که مجموعه { ۱,۲,۳ } تحت عمل ضرب به هنگ ۴ گروه نیست ولی { ۱,۲,۳,۴ } تحت ضرب به هنگ ۵ یک گروه است.

✓ ۸ ـ مجموعه متناهی G تحت یک عمل دوتایی چون (∘) شرکت پذیر بوده و قانون حذف از چپ و راست در آن برقرار است ثابت کنید G یک گروه است.

۹ ـ نشان دهید که ماتریس $\begin{bmatrix} ۲ & ۲ \\ ۱ & ۱ \end{bmatrix}$ وارون ضربی ندارد و از آنجا نتیجه بگیرید که ماتریس‌های ۲×۲ روی اعداد حقیقی و با دترمینان صفر با ضرب ماتریسها تشکیل یک گروه نمی‌دهد.

۱۰ ـ فرض کنید D_n گروه تقارنهای n وجهی باشد، برای $n \geq ۳$ عناصر D_n را توصیف کنید، D_n چند عضو دارد؟

۱۱ ـ آیا گروه $GL(۲, R)$ آبلی است؟ چرا؟

✓ ۱۲ ـ نشان دهید اگر a عضوی از گروه متناهی G با عضو همانی e باشد آنگاه عدد طبیعی مانند n وجود دارد که $a^n = e$

۱۳ ـ اگر G گروهی از مرتبهٔ زوج باشد. ثابت کنیدکه G دارای عضوی چون $a \neq e$ است که در $a^۲ = e$ صدق می‌کند.

۱۴ ـ همهٔ زیرگروههای $Z_۶$ را بدست آورید و نمودار لاتیس آنرا رسم کنید.

۱۵ ـ نشان دهید اگر H و K زیرگروههایی ازگروه آبلی G باشند آنگاه $A = \{ hk : h \in H, k \in K \}$ زیرگروهی از G است.

۱۶ ـ نشان دهید که هر زیر مجموعهٔ ناتهی H از گروهی چون G یک زیر گروه G است اگر و فقط اگر برای هر a و b از H، $ab^{-۱} \in H$

۱۷ ـ اگر H و K دو زیرگروه از G باشند نشان دهید که $H \cap K$ زیرگروه G است.

۱۸ ـ شرط لازم و کافی برای آنکه $\mathbf{Z}_m - \{ 0 \}$ تحت عمل ضرب گروه شود آنستکه m عدد اوّل باشد.

۱۹ ـ فرض کنید G یک گروه و a متعلق به G باشد ثابت کنید $< a^{-1} > = < a >$

۲۰ ـ ثابت کنید که هر گروه دوری با تنها یک مولد، حد اکثر دو عضو دارد.

✓ ۲۱ ـ ثابت کنید اگر G گروهی آبلی با عضو همانی e باشد، آنگاه مجموعهٔ H متشکّل از تمام عضوهایی چون x از G که در معادلهٔ $x^2 = e$ صدق می‌کنند یک زیرگروه G است.

✓ ۲۲ ـ ثابت کنید اگر G گروهی آبلی با عضو همانی e باشد، آنگاه مجموعهٔ H متشکل از تمام عضوهایی چون x از G که در معادلهٔ $x^n = e$ صدق می‌کنند یک زیرگروه G است که n عدد طبیعی ثابت می‌باشد.

✓ ۲۳ ـ فرض کنید زیر مجموعهٔ نا تهی و متناهی H از گروه G تحت عمل G بسته باشد. ثابت کنید که H زیرگروه G است.

✓ ۲۴ ـ با یک مثال نشان دهید که در گروهی چون G با عضو همانی e معادلهٔ درجهٔ دوّم $x^2 = e$ می‌تواند بیش از دو جواب هم داشته باشد.

۲۵ ـ اگر G یک گروه و a متعلّق به G و $k \in \mathbf{N}$ نشان دهید که

$$o(a^k) = \frac{o(a)}{(o(a),k)}$$

که در آن $o(a)$ عبارتست از مرتبه a و $(o(a), k)$ بزرگترین مقسوم علیه مشترک k و $o(a)$ می‌باشد.

۲۶ ـ فرض کنید G یک گروه بوده و x متعلّق به G و مرتبه x مساوی n باشد

اگر $< x^r > = < x^s >$ آنگاه نشان دهید که $(n , r) = (n , s)$

۲۷ ـ فرض کنید p و q دو عدد اوّل باشند تعداد مولدهای Z_{pq} را پیدا کنید.

۲۸ ـ نشان دهید که در گروهی دوری چون G از مرتبه n، به ازاء هر عدد طبیعی m که $m \mid n$ معادلهٔ $x^m = e$ دارای m جواب در G است.

۲۹ ـ ثابت کنید هرگاه G یک گروه و a، b و ab از مرتبهٔ ۲ باشند آنگاه :

$ab = ba$

۳۰ ـ فرض کنید a و b اعضایی از یک گروه باشند نشان دهید مرتبه ab با مرتبه ba برابر است.

۳۱ ـ فرض کنید a و x اعضایی از یک گروه باشند نشان دهید که مرتبه a با مرتبه $x^{-1} a x$ برابر است.

۳۲ ـ اگر گروه G فقط یک عنصر از مرتبهٔ n داشته باشد ثابت کنید اگر آن عنصر a باشد آنگاه $a \in Z(G)$ که در آن $Z(G)$ مرکز G می‌باشد.

۳۳ ـ فرض کنیم x عضوی از یک گروه و از مرتبه mn باشد که $(m , n) = ۱$ نشان دهید y و z را می‌توان چنان اختیار کرد که $x = yz$ که y و z اعضائی از آن گروه بوده که به ترتیب از مراتب m و n می‌باشند.

۳۴ ـ هرگاه G یک گروه و $H \neq \phi$ یک زیر مجموعه متناهی از G باشد در اینصورت H یک زیرگروه است اگر $H^2 = H$ باشد.

۳۵ ـ نشان دهید که برای $n \geq ۳$، S_n گروهی نا آبلی است.

۳۶ ـ ثابت کنید اگر $n \geq ۳$ آنگاه تنها عضوی از S_n که برای هر γ از S_n در $\sigma\gamma = \gamma\sigma$ صدق می‌کند $\sigma = I$ جایگشت همانی است یا به عبارت دیگر $Z(S_n) = \{ I \}$ (Z مرکز S_n است)

۳۷ ـ تعداد جایگشتهای زوج و فرد S_n مساوی است.

۳۸ ـ نشان دهید که برای هر زیرگروه H از S_n، $n \geq 2$، یا تمام جایگشتهای H یا دقیقاً نصف آنها زوج هستند.

۳۹ ـ گروه S_n را برای $n \geq 2$ در نظر بگیرید و فرض کنید σ جایگشت فرد ثابتی از S_n باشد، نشان دهید که هر جایگشت فردی از S_n برابر است با حاصلضرب σ در عضوی از A_n

۴۰ ـ ثابت کنید S_4 هیچ عنصری از مرتبه بزرگتر از ۴ ندارد.

۴۱ ـ ثابت کنید تعداد دورهای مجزّا با طول $r \leq n$ در S_n برابر $\frac{n!}{r(n-r)!}$ می‌باشد.

۴۲ ـ ثابت کنید A_4 زیرگروهی از مرتبه شش ندارد که در اینجا A مجموعه جایگشتهای زوج S_4 می‌باشد.

۴۳ ـ اوّلاً برای $n \geq 3$ نشان دهید A_n هر دور به طول سه را شامل می‌شود ثانیاً برای $n \geq 3$ نشان دهید که A_n بوسیله دورهای به طول سه تولید می‌شود.

۴۴ ـ اگر G یک گروه و a متعلّق به G و $N(a)$ نرمالساز a باشد که به صورت زیر تعریف می‌شود. $N(a) = \{ x \in G \mid xa = ax \}$

نشان دهید:

الف) $N(a)$ زیرگروه G است. ب) در چه صورتی $a \in Z(G)$ می‌باشد.

۴۵ ـ فرض کنید H زیرگروهی از گروه G و g عضوی از G از مرتبه n باشد و g^m متعلّق به H باشد بطوریکه $(m, n) = 1$ ثابت کنید g متعلّق به H است.

۴۶ ـ نشان دهید گروهی که تعداد متناهی زیرگروه دارد خود لزوماً گروهی متناهی است.

۴۷ ـ فرض کنیم در یک گروه دلخواه G مرتبه عضو b برابر n باشد نشان دهید $b^k = e$ اگر و فقط اگر n، k را بشمارد.

۴۸ ـ نشان دهید که اگر p عددی اوّل باشد آنگاه Z_p زیرگروه واقعی نابدیهی ندارد.

۴۹ ـ فرض کنید که G گروه آبلی باشد و H و K زیرگروههایی دوری از آن باشند و مرتبه H و K بترتیب r و s باشد نشان دهید اگر $(r , s) = ۱$ آنگاه G زیرگروهی دوری از مرتبه rs دارد.

۵۰ ـ اگر H و K دو زیرگروه از گروه G باشند ثابت کنید:

$H \cup K$ زیرگروه G است اگر و فقط اگر $K \subseteq H$ یا $H \subseteq K$

۵۱ ـ مثالی از یک گروه غیر دوری بیاورید که هر زیرگروه سرهٔ آن دوری باشد.

۵۲ ـ مثالی از یک گروه همراه با دو زیرگروه آن ارائه کنید که اجتماع آن دو زیر گروه یک گروه نباشد به عبارت دیگر نشان دهید اجتماع دو زیرگروه یک زیرگروه نمی‌شود.

۵۳ ـ اگر G گروهی دوری از مرتبه فرد باشد نشان دهید حاصلضرب اعضای G برابر e است (e عضو همانی G است).

۵۴ ـ نشان دهید هر گروه از مرتبه عددی اوّل دوری است.

۵۵ ـ فرض کنید H و K زیرگروههایی از G باشند و x و y اعضایی از G بطوریکه $Hx = Ky$ ثابت کنید $H = K$

۵۶ ـ فرض کنیم G گروهی دوری با مولد a و G' گروهی ایزومورف با G باشد نشان دهید اگر $\varphi : G \longrightarrow G'$ یک ایزومورفیسم باشد آنگاه برای هر x از G عضو $x\varphi$ از G' توسط $a\varphi$ کاملاً تعیین می‌شود.

۵۷ ـ فرض کنیم $\varphi : G \longrightarrow H$ ایزومورفیسمی است بین گروهی چون G و گروهی چون H و $\psi : H \longrightarrow K$ هم ایزومورفیسمی است از H با گروهی چون K نشان دهید که $\varphi\psi : G \longrightarrow K$ ایزومورفیستی از G به K است.

۵۸ ـ ثابت کنید که هر گروه دوری از مرتبهٔ n با Z_n ایزومورف است.

۵۹ ـ فرض کنیم G یک گروه و g عضو ثابتی از G باشد نشان دهید که نگاشت φ_g با تعریف $x\varphi_g = gxg^{-1}$ برای هر x از G یک ایزومورفیسم از G به خودش یعنی اتومورفیسمی از G می‌باشد این اتومورفیسم را اتومورفیسم داخلی گروه نامند.

۶۰ ـ نشان دهید گروه مجموعهٔ اعداد گویا با عمل جمع دوری نیست.

۶۱ ـ اگر φ تابع اویلر باشد نشان دهید اگر $(m , n) = 1$ آنگاه:

$$\varphi(n\,m) = \varphi(n)\,\varphi(m)$$

۶۲ ـ ثابت کنید که هر حاصلضرب مستقیم خارجی گروههای آبلی خود یک گروه آبلی است.

۶۳ ـ فرض کنید $n = rs$ و $(r , s) = 1$ نشان دهید که Z_n حاصلضرب مستقیم داخلی زیرگروه $< r >$ و $< s >$ است.

۶۴ ـ اگر G یک گروه و H زیرگروهی از آن باشد تعریف می‌کنیم:

$N_G(H) = \{ x \in G \mid x^{-1} H x = H \}$ و $N_G(H)$ را نرمالساز H می‌نامیم ثابت کنید $N(H)$ زیرگروه G است.

۶۵ ـ فرض کنید G یک گروه باشد و H زیرگروهی از G و $x \in G$ که $x^{-1}Hx$ مزودج H باشد که بصورت $x^{-1}Hx = \{ x^{-1}hx \mid h \in H \}$ تعریف می‌شود ثابت کنید:

الف) $x^{-1}Hx$ زیرگروهی از G است. ب) اگر H دوری باشد $x^{-1}Hx$ دوری است. ج) اگر H آبلی باشد $x^{-1}Hx$ آبلی است.

۶۶ ـ فرض کنید G یک گروه باشد و $Z(G)$ را بصورت زیر تعریف کنیم.

$Z(G) = \{ x \in G \mid xg = gx \quad \forall g \in G \}$ و $Z(G)$ را مرکز G می‌نامند

ثابت کنید $Z(G)$ زیرگروه نرمال G می‌باشد.

۶۷ـ اگر G یک گروه باشد و $Z(G)$ مرکز آن باشد ثابت کنید اگر $G/Z(G)$ دوری باشد آنگاه G آبلی است.

۶۸ـ اگر G یک گروه باشد بطوریکه مرتبه آن بیست و پنج باشد ثابت کنید G دوری است یا برای هر g متعلّق به G داریم $g^5 = e$

۶۹ـ اگر هر زیرگروه دوری، گروه G در G نرمال باشد، آنگاه هر زیرگروه G در G نرمال است.

۷۰ـ فرض کنید G یک گروه آبلی با مرتبهٔ فرد باشد، ثابت کنید معادلهٔ $x^2 = a$ به ازای هر a منعلّق به G فقط یک جواب دارد.

۷۱ـ فرض کنید p یک عدد اوّل و G یک گروه بابیش از ۱ ـ p عضو از مرتبه p باشد، چرا G نمی‌تواند دوری باشد؟

۷۲ـ نشان دهید هیچ گروهی بصورت اجتماع دو زیرگروه خودش نیست. (البتّه منظور زیرگروه سره می‌باشد)

۷۳ـ فرض کنیم G یک گروه با مرتبهٔ فرد باشد، ثابت کنید که به ازاء هر $a \in G$ معادلهٔ $x^2 = a$ فقط یک جواب دارد.

۷۴ـ اگر G یک گروه غیر آبلی از مرتبه p^3 که p عددیست اوّل نشان دهید که $| Z(G) | = p$ ($Z(G)$ مرکز G است)

۷۵ـ ثابت کنید که زیر مجموعه متشکّل از عناصر از مرتبه متناهی در یک گروه آبلی یک زیرگروه است (این زیرگروه را زیرگروه تابی می‌نامند)

۷۶ـ فرض کنید H زیرگروهی از G و g عنصری از G باشد ثابت کنید:

$$N (g^{-1}Hg) = g^{-1} N(H) g$$

(در اینجا $N(H)$ نرمالساز H در G می‌باشد)

۷۷ـ فرض کنیم که G یک گروه و H و K زیرگروههایی از G باشند بطوریکه:

$H \cap K = \{ e \}$ ثابت کنید $| K | = ۵$ و $| H | = ۱۲$

۷۸ـ فرض کنید p و q دو عدد اوّل متمایز باشند و G یک گروه از مرتبه pq باشد ثابت کنید که هر زیرگروه واقعی G دوری است.

۷۹ـ اگر G یک گروه آبلی و H متشکّل از تمام $x^۲$هایی باشد که x متعلّق به G است ثابت‌کنید H در G نرمال است.

۸۰ـ اگر K و H دو زیرگروه نرمال G باشند ثابت کنید HK زیرگروه نرمال G است.

۸۱ـ اگر H و K دو زیرگروه نرمال ازگروه متناهی G باشند که $|H|$ و $|K|$ متباینند نشان دهید که به ازای هر h از H و هر k از K، $hk = kh$

۸۲ـ اگر n عدد صحیح مثبت باشد و a نیر نسبت به n اوّل باشد نشان دهید (هنگ n) $a^{\varphi(n)} \equiv ۱$ که $\varphi(n)$ تعداد اعداد کوچکتر از n است که نسبت به n اولند.

۸۳ـ اگر R^* گروه اعداد حقیقی غیر صفر با عمل ضرب باشد نشان دهید $(R^* , .)$ با $(R , +)$ ایزومورف نیست.

۸۴ـ اگر G یک گروه دلخواه باشد زیرگروه G' که زیرگروه مشتق یا زیرگروه برگردان نامیده می‌شود بصورت زیر تعریف می‌شود.

$$G' = < \{ xyx^{-۱}y^{-۱} \mid x,y \in G \} >$$

نشان دهید $\frac{G}{N}$ آبلی است اگر و فقط اگر $G' \subseteq N$ (N زیرگروه نرمال G است)

۸۵ـ فرض کنید N یک زیرگروه نرمال ازگروه G باشد که مرتبه $\frac{G}{N}$ متناهی است و H یک زیرگروه G با مرتبه متناهی باشد اگر $(| H | , [G:N]) = ۱$ نشان دهید که $H \subseteq N$

۸۶ـ اگر H زیرگروهی از S_n، $n > ۱$ باشد بطوریکه H شامل یک

جایگشت فرد باشد، نشان دهید که مجموعهٔ همهٔ جایگشتهای زوج در H، یک زیر گروه نرمال H با اندیس ۲ است.

۸۷ ـ ثابت کنید هر گروه از مرتبهٔ p^2 که در آن p عدد اوّل می‌باشد، آبلی است.

۸۸ ـ ثابت کنید هر گروه از مرتبه p^2 که p عدد اوّل باشد، بایستی زیر گروه نرمال از مرتبه p داشته باشد.

۸۹ ـ برای گروه دلخواه چون G ثابت کنید $Inn(G)$ یک زیر گروه نرمال $Aut(G)$ است و $G/Z(G)$ یکریخت با $Inn(G)$ می‌باشد.

($Z(G)$ مرکز G، $Inn(G)$ گروه خود ریختیهای داخلی G و $Aut(G)$ گروه خود ریختیهای G می‌باشند)

۹۰ ـ فرض کنید G یک گروه دلخواه و N زیر گروه نرمالی از آن باشد بطوریکه $N \cap G' = \{ e \}$ نشان دهید $N \subseteq Z(G)$. (G' زیر گروه مشتق و $Z(G)$ مرکز G است)

۹۱ ـ G گروهی از مرتبه p^2 است که در آن p یک عدد اوّل می‌باشد، نشان دهید G دوری است یا به صورت حاصل جمع مستقیم دو گروه دوری است که هر کدام از مرتبه p هستند. (توجه: در صورت مسئله اصلی که از کتاب جبر گالیان اخذ شده حاصل جمع مستقیم به زبان اصلی بیان شده‌بود که با علائم آن کتاب همان حاصلضرب مستقیم خارجی می‌باشد)

✓ ۹۲ ـ اگر T یک اتومورفیسم گروه G باشد بطوریکه $\forall x \in G \quad xT = x^{-1}$ آنگاه ثابت کنید G آبلی است.

✓ ۹۳ ـ فرض کنید G یک گروه آبلی متناهی از مرتبهٔ n و m یک عدد صحیح مثبت باشد بقسمی که $(m, n) = 1$ آنگاه نشان دهید که $f: x \longrightarrow x^m$ یک اتومورفیسم G است.

۹۴ـ فرض کنید T یک خود ریختی از گروه متناهی G باشد بطوریکه $T(x) = x$ اگر و فقط اگر $x = e$ $(x \in G)$ همچنین $T^{r} = I$ که I عضو همانی $Aut(G)$ است. نشان دهید که G آبلی است. (راهنمایی: نخست ثابت کنید که هر g از G را می توانیم بر حسب $x^{-1}T(x)$ که x در G است بیان کنیم)

۹۵ـ اگر $G = < a >$ و $H = < b >$ دو گروه دوری هم مرتبه باشند و $f : G \longrightarrow H$، $f(a^{r}) = b^{r}$ برای هر عدد صحیح مثبت r نشان دهید که f خوش تعریف بوده و یک ایزومورفیسم است.

۹۶ـ اگر m یک عدد صحیح مثبت باشد که مرتبه یک گروه دوری متناهی را عاد کند، ثابت کنید یک و تنها یک زیرگروه از مرتبه m وجود دارد.

۹۷ـ اگر G یک گروه متناهی و T یک زیرگروه دوری از G باشد، ثابت کنید که اگر T در G نرمال باشد هر زیرگروه T در G نرمال است.

۹۸ـ نشان دهید که تابع $f : C \longrightarrow C$ که با ضابطه $\forall z \in C \quad f(z) = \bar{z}$ تعریف می‌شود یک اتومورفیسم است. ($\bar{z}$ مزدوج z و C اعداد مختلط می‌باشد)

۹۹ـ فرض کنید G یک گروه و h و g اعضایی از G باشند که اتومورفیسمهای داخلی متناظر با g و h یکسان هستند ثابت کنید که gh^{-1} متعلّق به $Z(G)$ است.

۱۰۰ـ فرض کنید $\varphi : G \longrightarrow H$ یک همریختی گروهی باشد ثابت کنید φ یک به یک است اگر و فقط اگر $\forall x \in G \quad o(x) = o(x\varphi)$

۱۰۱ـ فرض کنید $\varphi : G \longrightarrow G$ یک همریختی گروهی باشد و فرض کنید K زیرگروه G و دوری باشد بطوریکه $K\varphi \subseteq K$ ثابت کنید اگر H زیرگروه K باشد آنگاه $H\varphi \subseteq H$

۱۰۲ـ فرض کنید G یک گروه و H زیرگروه از G و همچنین a عضوی از G باشد ثابت کنید که $aH = H$ اگر و فقط اگر $a \in H$

۱۰۳ ـ فرض کنید G گروهی از مرتبه pq باشد بطوریکه p و q دو عدد اوّل متمایزند ثابت کنید G دوری است.

۱۰۴ ـ G یک گروه با بیش از یک عضو می‌باشد بطوریکه هیچ زیرگروه غیر بدیهی ندارد ثابت کنید G دوری و مرتبهٔ G عدد اوّل است.

۱۰۵ ـ فرض کیند $G = GL(۲, \mathbf{R})$ و H زیرگروه ماتریسهای ۲×۲ با دترمینان یک و منفی یک باشد. اگر a و b اعضایی از G باشند و $aH = bH$ در مورد دترمینان a و دترمینان b چه می‌توانیم بگوییم؟ آیا عکس موضوعی که بیان می‌کنید درست است؟

۱۰۶ ـ نشان دهید $SL(۲, \mathbf{R})$ در $GL(۲, \mathbf{R})$ نرمال می‌باشد.

✓ ۱۰۷ ـ ثابت کنید گروه خارج قسمت هر گروه دوری، دوری است.

✓ ۱۰۸ ـ نشان دهید که گروه خارج قسمت یک گروه آبلی، آبلی است.

۱۰۹ ـ فرض کنید G یک گروه متناهی و H زیرگروه نرمال از G باشد، ثابت کنید که مرتبه عضو gH از G/H مرتبه g از G را می‌شمارد.

۱۱۰ ـ فرض کنید N و H دو زیرگروه G و N نرمال در G باشند اگر N زیر گروه نرمال H باشد، ثابت کنید $\frac{H}{N}$ زیرگروه نرمال $\frac{G}{N}$ است اگر و فقط اگر H در G نرمال باشد.

۱۱۱ ـ نشان دهید اشتراک دو زیرگروه نرمال G، زیرگروه نرمالی از G است.

✓ ۱۱۲ ـ نشان دهید اگر M و N دو زیرگروه نرمال G باشند و $N \cap M = \{e\}$ آنگاه $mn = nm$ به ازای هر m از M و هر n از N.

۱۱۳ ـ H زیرگروه نرمال از گروهی متناهی چون G است و $(o(x), |G/H|) = ۱$ نشان دهید $x \in H$

۱۱۴ ـ H زیرگروه نرمال از گروه متناهی G است، اگر G/H یک عنصر از

مرتبه n داشته باشد نشان دهید که G یک عنصر از مرتبه n دارد.

۱۱۵ ـ H و K دو زیرگروه نرمال ازگروه متناهی چون G هستند و مرتبه H و مرتبه K نسبت به هم اوّلند نشان دهید که به ازای هر h متعلّق به H و هر t متعلّق به K، $ht = th$

۱۱۶ ـ فرض کنید G یک گروه آبلی و H زیر مجموعه‌ای متشکّل از عضو همانی همراه با تمام اعضایی از G که مرتبه آنها سه است، نشان دهید که H زیرگروه G است آیا به جای سه ، چهار قرار دهیم باز هم حکم فوق برقرار است؟ به ازای چه مقادیری از عدد طبیعی n مجموعهٔ متشکّل از عضو همانی و تمام اعضای از مرتبه n همواره یک زیرگروه G است؟

۱۱۷ ـ G یک گروه متناهی و دارای فقط یک زیرگروه از مرتبه‌ای مفروض باشد آنگاه نشان دهید آن زیرگروه در G نرمال است.

۱۱۸ ـ اگر m عدد صحیح مثبت باشد نشان دهید Z_m با $\frac{Z}{mZ}$ ایزومورف است.

۱۱۹ ـ G گروه غیر آبلی و متناهی است نشان دهید که مرتبه $\frac{G}{Z(G)}$ بزرگتر یا مساوی ۴ است.

۱۲۰ ـ فرض کنید G یک گروه و $Z(G)$ مرکز آن باشد، ثابت کنید که اگر T یک اتومورفیسم G باشد آنگاه $T \subseteq Z(G)$ [$Z(G)$]

۱۲۱ ـ ثابت کنید مرتبه $Inn(G)$ برابر یک است اگر و فقط اگر G آبلی باشد.

۱۲۲ ـ G یک گروه غیر آبلی است، ثابت کنید $Aut(G)$ گروه اتومورفیسمهای G نمی‌تواند دوری باشد.

۱۲۳ ـ اگر m و n عناصری ازگروه جمعی Z باشند، یک مولد برای

$< n > \cap < m >$ بیابید.

۱۲۴ـ اگر $\varphi : G \longrightarrow H$ یک همریختی گروهی باشد ثابت کنید φ، یک به یک است اگر و فقط اگر $\mathrm{Ker}\varphi = \{ e \}$

۱۲۵ـ فرض کنید $G = H \times K$ (حاصلضرب خارجی) که $H \neq \{ e \}$ و $K \neq \{ e \}$ اگر G غیر آبلی باشد نشان دهید که $| G | \geq ۱۲$

۱۲۶ـ زیرگروه K از گروه G مفروض است ثابت کنید K در G نرمال است اگر و فقط اگر K هسته یک همریختی گروهی مانند $f: G \longrightarrow H$ باشد.

۱۲۷ـ فرض کنید N زیرگروه G با اندیس دو باشد اگر x و y اعضایی از G باشند همچنین x و y متعلّق به N نباشند ثابت کنید xy متعلّق به N است.

۱۲۸ـ $G \neq \{ e \}$ یک گروه دوری است که $G = < a >$ آنگاه ثابت کنید هر هوموموفیسم چون $f : G \longrightarrow G$ یک اتوموفیسم است اگر و فقط اگر $f(a)$ یک مولد G باشد.

۱۲۹ـ مثالی از یک گروه و عناصر a و b از آن ارائه دهید بطوریکه مرتبه a و b متناهی باشند ولی مرتبه ab نامتناهی باشد.

۱۳۰ـ فرض کنید G یک گروه و p کوچکترین عدد اوّلی باشد که مرتبه G را عاد کند نشان دهید اگر H زیرگروه G بوده و $[G : H] = p$ آنگاه H در G نرمال است.

۱۳۱ـ فرض کنید G متناهی و $p \mid\mid |G|$ به علاوه $\mathbf{P}$ یک P زیرگروه سیلو G باشد نشان دهید که $N [N(P)] = N(P)$

۱۳۲ـ فرض کنید p عدد اوّل و $| G | = p^n$ و H زیرگروه G باشد و $[G : H] = p$ نشان دهید H در G نرمال است.

۱۳۳ـ G یک گروه و K زیرگروه نرمال G و متناهی است همچنین P

یک p زیرگروه سیلو K باشد نشان دهید $G = N(p) . K$

۱۳۴ ـ G گروه متناهی و p عدد اوّلی باشد که مرتبه G را می‌شمارد

الف) به ازای هر p زیرگروه سیلو چون P از G نشان که P تنها P زیرگروه سیلو $N(p)$ است.

ب) فرض کنید P یک p زیرگروه سیلو G باشد و H زیرگروه G که $N(p) \subseteq H$ نشان دهید که $N(H) = H$

۱۳۵ ـ نشان دهید که اگر H یک زیرگروه نرمال از گروه متناهی G باشد و p عدد اوّلی باشد که مرتبه G را می‌شمارد بطوریکه $([G : H] , p) = ۱$) آنگاه H تمام p زیرگروههای سیلو G را شامل می‌شود.

۱۳۶ ـ نشان دهید که گروه G، یک p گروه متناهی است اگر و فقط اگر یک زیرگروه نرمال چون N داشته باشد بطوریکه N و G/N هر دو p گروه باشند.

۱۳۷ ـ گروه G از مرتبه p^n است که p عدد اوّل است و G دقیقاً یک زیرگروه $p^{n-۱}$ عضوی دارد، نشان دهید G دوری است.

۱۳۸ ـ گروه آبلی G سری ترکیب دارد اگر و تنها اگر G متناهی باشد.

۱۳۹ ـ اگر G گروهی از مرتبه $p^۲q$ باشد که p و q دو عدد اوّل متمایز می‌باشند و $q > p$ همچنین q عاملی از $p^۲ - ۱$ نیست، ثابت کنید G آبلی است.

۱۴۰ ـ کنش یک گروه G روی G ـ مجموعه‌ای چون X صادقانه است اگر عضو همانی تنها عضوی از G باشد که هر عضو X را ثابت نگه می‌دارد.

حال فرض کنید X یک G ـ مجموعه باشد نشان دهید که کنش G روی X صادقانه است اگر و فقط اگر هیچ دو عضو متمایزی از G برهر عضو X کنش یکسان نداشته باشند.

۱۴۱ ـ نشان دهید هیچ گروه از مرتبه ۴۸ ساده نیست.

حل تمرینات بخش گروهها

۱ ـ الف) فرض کنیم a و b و c دلخواه از R^* باشند داریم:

$$a \circ b = |a|\, b \text{ و } b \circ c = |b|\, c$$

$$(aob)oc = (|a|b)oc = ||a|b|c = ao(|b|c) = ao(boc)$$

ب) عضو خنثی چپ موجود و برابر یک است زیرا

$$1 \circ b = |1|\, b = b$$

$$a \circ b = 1 \Rightarrow |a|\, b = 1 \Rightarrow b = \frac{1}{|a|}$$

برای هر a از R^* معکوس راست $\frac{1}{|a|}$ موجود بوده و عبارتست از زیرا:

$$a \circ \frac{1}{|a|} = |a|\, \frac{1}{|a|} = \frac{|a|}{|a|} = 1$$

ج) خیر، زیرا عضو همانی راست ندارد.

د) هرگاه مجموعهٔ G تحت عمل o شرکت پذیر باشد و عضو همانی راست (چپ) هر عضو معکوس راست (چپ) داشته باشد آنگاه G تحت عمل o گروه است ولی اگر G شرکت پذیر بوده و عضو همانی راست (چپ) و هر عضو معکوس چپ (راست) داشته باشد G گروه نیست. این مطلب در تمرین ۴ همین بخش ثابت شده است.

۲ ـ می‌دانیم در هر گروه با عضو همانی e، $e \circ e = e$ پس کافی است منحصر بفرد بودن عضو خودنما را ثابت کنیم، فرض کنیم x و y دو عنصر خودنما نسبت به o باشند داریم: $xox = x$ و $yoy = y$

$xox=x \Rightarrow x^{-1}o(xox) = x^{-1}ox \Rightarrow (x^{-1}ox)ox = e \Rightarrow eox=e \Rightarrow x=e$

$yoy=y \Rightarrow y^{-1}o(yoy)=y^{-1}oy \Rightarrow (y^{-1}oy)oy=e \Rightarrow eoy=e \Rightarrow y=e$

پس داریم: $x = y = e$ در نتیجه عضو خودنما منحصر بفرد است.

۳ـ داریم: (۱) $(a\,o\,b)^{-1} = b^{-1}\,o\,a^{-1}$

از طرفی داریم: (۲) $a\,o\,b = (a\,o\,b)^{-1}$ چون معکوس هر عضو طبق فرض خودش می‌باشد.

از (۱) و (۲) داریم: (۳) $a\,o\,b = b^{-1}\,o\,a^{-1}$

از طرفی بنا به فرض داریم $a = a^{-1}$ و $b = b^{-1}$ از اینجا و رابطه (۳) داریم:

$a\,o\,b = b\,o\,a$

۴ـ فرض کنیم a عضو دلخواه از G باشد و b معکوس چپ a همچنین c معکوس چپ b باشد داریم:

$boa = e \quad , \quad cob = e$

$boa = e \Rightarrow co(boa) = coe \Rightarrow (cob)oa = coe \Rightarrow eoa = coe$

$\Rightarrow a = coe \qquad (1)$

با توجه به (۱) داریم: $aob = (coe)ob = co(eob) = cob = e = boa$

پس هر عضو در G معکوس دارد.

حال نشان می‌دهیم که e عضو همانی راست نیز می‌باشد.

فرض کنیم x عضو دلخواهی از G باشد خواهیم داشت:

$xoe = xo(x^{-1}ox) = (xox^{-1})ox = eox = x$

۵ـ عضو دلخواهی از G چون a را انتخاب می‌کنیم معادلهٔ $yoa = a$ جواب دارد. جوابی از آن را e می‌نامیم بنابراین $eoa = a$، اکنون فرض کنیم b عضو دلخواهی از G باشد معادلهٔ $aox = b$ در G جواب دارد جوابی از آن را c می‌نامیم

پس $aoc = b$

$$eob = eo(aoc) = (eoa)oc = aoc = b$$

پس e عضو همانی چپ گروه است، اکنون فرض کنیم a عضو دلخواهی از G باشد معادله $yoa = e$ در G جواب دارد جوابی از آنرا d می‌نامیم می‌دانیم $doa = e$ پس d معکوس چپ a است لذا بنا به مسئله قبل G با عمل o یک گروه است.

۶ـ از تئوری مجموعه‌ها میدانیم که اگر $f : A \longrightarrow B$ و $|A| = n$ و $|B| = m$ در اینصورت m^n تابع از A به B وجود دارد چون $o : S \times S \longrightarrow S$ در اینصورت n^{n^2} تابع متمایز می‌توان تعریف کرد، در مجموعه $S \times S$ ، n تا عنصر (x,x) وجود دارد پس $n^2 - n$ عنصر از $S \times S$ می‌ماند که مؤلفه‌های اوّل و دوّم متمایز دارند و چون $xoy = yox$ پس $\frac{n^2 - n}{2}$ عضو باقی می‌ماند لذا $\frac{n^2 + n}{2} = \frac{n^2 - n}{2} + n$ پس تعداد اعمال دوتایی جابجائی $n^{\frac{n^2+n}{2}}$ می‌باشد.

۷ـ در مجموعه $Z_4 - \{o\} = \{ ۱ , ۲ , ۳ \}$ عضو ۲ وارون ضربی ندارد زیرا داریم:

$۲ \times ۱ = ۲ \not\equiv ۱$ (هنگ ۴)

$۳ \times ۲ = ۶ \equiv ۲ \not\equiv ۱$ (هنگ ۴)

ولی $Z_5 - \{o\} = \{ ۱ , ۲ , ۳ , ۴ \}$ دارای عضو همانی ۱ بوده و داریم:

$۲ \times ۳ = ۶ \equiv ۱$ (هنگ ۵)

$۴ \times ۴ = ۱۶ \equiv ۱$ (هنگ ۵)

پس هر عضو $Z_5 - \{o\}$ دارای معکوس بوده و لذا مجموعه فوق یک گروه است. البتّه توجّه داریم که بدیهی است $Z_5 - \{o\}$ باعمل ضرب به‌هنگ ۵ شرکت‌پذیر است.

۸ـ چون G متناهی است فرض کنیم $G = \{ a_1 , ... , a_n \}$

حال عضو a متعلق به G را در نظر می‌گیریم و اعضای $aa_1, \dots, aa_n$ با توجه به اینکه G نسبت به عمل دوتایی بسته است، متعلق به G می‌باشند و همچنین متمایز نیز هستند زیرا در غیر اینصورت داریم:

وجود دارد $i \neq j$ بطوریکه $aa_i = aa_j$ و چون قانون حذف برقرار است لذا $a_i = a_j$ در نتیجه این مخالف با متمایز بودن $a_1, \dots, a_n$ می‌باشد پس $aa_1, \dots, aa_n$ متمایزند و لذا چون $a \in G$ پس یک 1 ای وجود دارد بطوریکه $a=aa_1$ و داریم $a^2 = aa_1a$ طبق قانون حذف $a_1a = a$ حال نشان می‌دهیم به ازای هر x متعلق به G، $xa_1 = a_1x = x$ چون $x \in G$ پس $x = aa_i$ به ازای یک i ای و بنا بر این داریم:

$$a_1x = a_1aa_i = aa_i = x$$

بنا به قانون حذف

$$xa = x(a_1a) = (xa_1)a \Rightarrow x = xa_1$$

بنابر این: $xa_1 = a_1x = x$ و $e = a_1$ عضو همانی می‌باشد.

امّا برای اثبات اینکه هر عضو G وارون دارد بدین ترتیب عمل می‌کنیم چون $e \in G$ پس یک t ای وجود دارد بطوریکه $e = aa_t$ پس a وارون دارد ولی چون a دلخواه بود پس هر عضو G وارون دارد و بنابر این G گروه است.

۹ ـ فرض کنیم ماتریس $\begin{bmatrix} ۲ & ۲ \\ ۱ & ۱ \end{bmatrix}$ وارون ضربی داشته باشد پس وارون آن ماتریسی چون $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ می‌باشد و داریم:

$$\begin{bmatrix} ۲ & ۲ \\ ۱ & ۱ \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix} \Rightarrow$$

$$\begin{cases} ۲(a+c) = ۱ \\ ۲(b+d) = ۰ \end{cases}$$

$$\begin{cases} a + c = ۰ \\ b + d = ۱ \end{cases}$$

پس داریم $a + c = ۰$ و از طرفی $a + c = \frac{۱}{۲}$ و این تناقض است پس ماتریس

$\begin{bmatrix} ۲ & ۲ \\ ۱ & ۱ \end{bmatrix}$ وارون ضربی ندارد و لذا مجموعه ماتریسهای ۲×۲ روی اعداد حقیقی با دترمینان صفر تشکیل یک گروه نمی‌دهد.

۱۰ ـ این گروه دارای $۲n$ عضو می‌باشد، زیر اگر n فرد باشد n جایگشت متمایز از دوران حول $\frac{۲\pi}{n}$ بدست می‌آید و n جایگشت دیگر نیز از دوران حول خط گذرنده از هر رأس و وسط ضلع مقابل آن بدست می‌آید و اگر n زوج باشد متشابهاً n جایگشت متمایز از دوران حول مرکز به اندازه $\frac{۲\pi}{n}$ و $\frac{n}{۲}$ جایگشت از دوران حول خطوطی که از رئوس n ضلعی می‌گذرند و آن را به دو قسمت مساوی تقسیم می‌کنند بدست می‌آید. و همچنین $\frac{n}{۲}$ جایگشت باقیمانده از دوران حول عمود منصفهای اضلاع بدست می‌آید که جمعاً $۲n$ جایگشت می‌شود.

۱۱ ـ البته می‌دانیم که $GL(۲, R)$ ماتریسهای ۲×۲ با درآیه‌های حقیقی و دترمینان مخالف صفر بوده و با عمل ضرب ماتریسها یک گروه است حال نشان می‌دهیم که آبلی نیست دو ماتریس $A=\begin{bmatrix} ۲ & ۰ \\ ۱ & ۲ \end{bmatrix}$ و $B=\begin{bmatrix} ۱ & ۱ \\ ۰ & ۲ \end{bmatrix}$ را در نظر می‌گیریم دترمینان A برابر ۴ بوده و همچنین دترمینان B برابر ۲ بوده و هر دو مخالف صفرند بنابر این A و B هر دو متعلق به $GL(۲, R)$ می‌باشند و داریم.

$$AB = \begin{bmatrix} ۲ & ۲ \\ ۱ & ۵ \end{bmatrix} \quad \text{و} \quad BA = \begin{bmatrix} ۳ & ۲ \\ ۲ & ۴ \end{bmatrix} \quad \Rightarrow AB \neq BA$$

۱۲ ـ اگر $G = \{ e \}$ باشد که مسئله بدیهی است ولی اگر $G \neq \{ e \}$ و a متعلق به G باشد چون G نسبت به عمل دوتایی بسته است پس $a, a^۲, a^۳, \ldots$ همگی متعلق به G هستند و این مجموعه اگر نامتناهی باشد تناقض با متناهی بودن G می‌باشد پس این مجموعه متناهی بوده و وجود دارد i و j ای بطوریکه $a^i = a^j$ حال فرض کنیم $i > j$ پس $a^{i-j} = e$ و $i - j > 0$ لذا حکم ثابت است.

۱۳ ـ فرض کنیم هیچ عضوی از G مانند a وجود نداشته باشد بطوریکه $a^2 = e$ باشد پس هر عوض G با معکوسش متمایز می‌باشد اگر اینها را دو بدو یعنی هر عضو را با معکوسش کنار بگذاریم تعداد این عناصر زوج خواهد بود و یک عضو همانی باقی می‌ماند که معکوس آن با خودش برابر است اگر این عضو را به مجموعه جدا شده بیفزاییم تعداد فرد خواهد شد و این مخالف با فرض زوج بودن مرتبهٔ G می‌باشد.

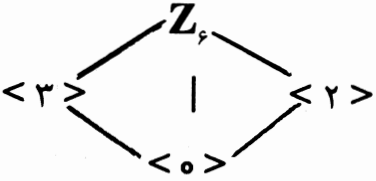
پس عضوی چون $a \neq e$ وجود دارد بطوریکه $a^2 = e$

۱۴ ـ تمام زیرگروههای Z_6 دوری هستند زیرا خود Z_6 دوری است.

و داریم: $<1> = <5> = Z_6$ $<0> = \{0\}$

$<3> = \{0, 3\}$ $<2> = <4> = \{0, 2, 4\}$

نمودار لاتیس آن عبارتست از:



۱۵ ـ فرض کنیم x و y اعضای دلخواهی از A باشند داریم $x = h_1 k_1$ و $y = h_2 k_2$ که در آن h_2 و h_1 در H و k_2 و k_1 در K هستند

$$xy = (h_1k_1)(h_2k_2) = (h_1k_1)(k_2h_2) = h_1 (k_1k_2) h_2 = (h_1h_2)(k_1k_2)$$

پس چون H و K زیرگروههایی از G هستند $h_1h_2 \in H$ و $k_1k_2 \in K$ و لذا xy متعلق به A می‌باشد پس A نسبت به عمل بسته است.

حال چون $e = e.e$ پس e متعلق به A می‌باشد.

فرض کنیم $x \in A$ دلخواه باشد پس $x = hk$ که $h \in H$ و $k \in K$ در نتیجه:

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in A$$

لذا A زیرگروه G است و این زیرگروه را با HK نشان می‌دهیم.

۱۶ - چون H ناتهی است عضوی مانند a از H انتخاب می‌کنیم، داریم:

$e = aa^{-1}$ و لذا $e \in H$.

فرض کنیم a عضو دلخواهی از H باشد چون $e \in H$ پس $a^{-1} = ea^{-1}$ و لذا a^{-1} متعلق به H می‌باشد پس داریم $a\ (b^{-1})^{-1} = ab \in H$ لذا H نسبت به عمل بسته است لذا H زیرگروه G است.

حال فرض کنیم H زیرگروه G باشد و a و b متعلق به H باشند در نتیجه b^{-1} متعلق به H خواهد بود و چون H زیرگروه G است لذا ab^{-1} متعلق به H می‌باشد و حکم ثابت است.

۱۷ - چون H و K زیرگروههای G هستند پس e متعلق به H و همچنین e متعلق به K است و لذا e متلعق به $H \cap K$ است و حال فرض کنیم y و x متعلق به $H \cap K$ باشند داریم:

$$\begin{cases} x \in H \wedge y \in H \\ x \in K \wedge y \in K \end{cases} \Rightarrow \begin{cases} xy \in H \\ xy \in K \end{cases} \Rightarrow xy \in H \cap K$$

پس $H \cap K$ نسبت به عمل بسته است.

فرض کنیم x متعلق به $H \cap K$ باشد داریم:

$$\begin{cases} x \in H \Rightarrow x^{-1} \in H : \text{چون } H \text{ زیرگروه } G \text{ است.} \\ \wedge \\ x \in K \Rightarrow x^{-1} \in K \text{. چون } K \text{ زیرگروه } G \text{ است.} \end{cases}$$

در نتیجه x^{-1} متعلق به $H \cap K$ است و لذا $H \cap K$ زیرگروه G است.

۱۸ - در مورد این مسئله توجه شود که منظور از o کلاس o می‌باشد یا مثلاً منظور از عنصر ۱ از Z_m کلاس ۱ می‌باشد که ما به اختصار به ۱ نشان می‌دهیم.

فرض کنیم m اوّل باشد خاصیت شرکت پذیری بنا به خاصیت شرکت پذیری اعداد صحیح نسبت به ضرب بدیهی است.

و چون به ازای هر a متعلق به $\mathbf{Z}_m - \{ 0 \}$ داریم $a \cdot 1 = a$ پس ۱ عضو خنثی آن می‌باشد.

فرض کنیم $x \in \mathbf{Z}_m - \{ 0 \}$ داریم $(x , m) = 1$ یعنی x و m نسبت به هم اوّلند لذا وجود دارد s و t ای بطوریکه $xs + mt = 1$ و لذا $xs \equiv 1$ (هنگ m) پس s وارون x می‌باشد.

به عکس فرض می‌کنیم $\mathbf{Z}_m - \{ 0 \}$ گروه باشد نشان می‌دهیم m اوّل است فرض کنیم m اوّل نباشد پس $m = m_1 m_2$ که $m_2 \leq m$ و $m_1 \leq 1$ پس m_2 و m_1 متعلق به $\mathbf{Z}_m - \{ 0 \}$ بوده و وارون دارند پس وجود دارند t و s در $\mathbf{Z}_m - \{ 0 \}$ بطوریکه :

$m_1 s \equiv 1$ (هنگ m)

$m_2 t \equiv 1$ (هنگ m)

لذا $m_1 m_2 st \equiv 1$ (هنگ m) پس $mst \equiv 1$ (هنگ m) و این تناقض است زیرا $mst \equiv 0$ (هنگ m) پس m اوّل است.

۱۹ـ $< a > = \{ a^n \mid n \in \mathbf{Z} \} = \{ a^{-n} \mid -n$ یا $n \in \mathbf{Z} \}$

$= \{ (a^{-1})^n \mid n \in \mathbf{Z} \} = < a^{-1} >$

۲۰ـ اگر $G = \{ e \}$ آنگاه مسئله واضح است ولی اگر $G \neq \{ e \}$ در اینصورت بنا به تمرین ۱۹ همین بخش اگر a مولد G باشد آنگاه a^{-1} نیز مولد G است و بنابر این چون G تنها یک مولد دارد $a = a^{-1}$ و G دارای دو عضو e و a می‌باشد و حکم ثابت است.

$G = < a > = \{ a, a^2, \ldots \} = \{ a, e \}$

۲۱ـ فرض کنیم x و y اعضایی دلخواه از H باشند

$(xy)(xy) = (xy)(yx) = x(yy)x = xex = xx = e \in H$

$e \in H \neq \emptyset$

$(xy^{-1})^2 = xy^{-1}xy^{-1} = e$

پس H تحت عمل بسته است.

چون $ee = e$ لذا $e \in H$

فرض کنیم $x \in H$ چون $x^2 = e$ پس معکوس x، خودش می‌باشد لذا $x = x^{-1} \in H$ پس H یک زیرگروه G است.

۲۲ ـ ابتدا ثابت می‌کنیم در هرگروه آبلی $(ab)^n = a^n b^n$ استقراء برای $n = 1$ برقرار است و همچنین داریم $ab = ba$.

فرض کنیم برای $n = k$ برقرار باشد داریم : $(ab)^k = a^k b^k$

حال برای اثبات حکم استقراء چنین عمل می‌کنیم:

$$(ab)^{k+1} = (ab)^k ab = (a^k b^k)(ab) = (a^k b^k)(ba) =$$

$$a^k(b^k b)a = a^k(b^{k+1} a) = a^k(a\, b^{k+1}) = a^{k+1} b^{K+1}$$

پس حکم استقراء ثابت شد و لذا حکم کلی ثابت است.

حال اگر a و b دو عضو دلخواه از H باشند داریم $(ab)^n = a^n b^n = ee = e$ لذا H تحت عمل بسته است. همواره داریم $(ee)^n = e$ لذا $e \in H$ برای هر a از H داریم $a^n = e$ لذا $aa^{n-1} = a^{n-1}a = a^n = e$ پس $a^{-1} = a^{n-1} \in H$ زیرگروه G است.

۲۳ ـ فرض کنیم a عضو دلخواهی از H باشد (H غیر تهی است) قرار می‌دهیم $K = < a >$ چون H تحت عمل القایی G بسته است پس، $K \subseteq H$ چون H متناهی است پس K متناهی است. و در نتیجه توانی از a برابر e می‌باشد فرض کنید $a^m = e$ در اینصورت $a^m = a.a^{m-1} = e$ یعنی:

$$a^{-1} = a^{m-1} \in K$$

در نتیجه چون $K \subseteq H$ پس $a^{-1} \in H$ و مطلب تمام است زیرا

$$a \in H \wedge a^{-1} \in H \Rightarrow aa^{-1} = e \in H$$

۲۴ ـ برای مثال این مسئله ساختمان گروه چهار عضوی همراه با جدول کیلی آن را معرفی می‌کنیم که به گروه چهارهٔ کلاین مشهور است.

جدول این‌گروه به قرار زیر است:

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

همانطور که در جدول ملاحظه می‌شود معادلهٔ $x^2 = e$ دارای چهار جواب می‌باشد.

۲۵ ـ فرض کنیم $o(a) = n$ و $(o(a), k) = d$ داریم:

$$(a^k)^{n/d} = (a^n)^{k/d} = (a^n)^t = e^t = e$$

که در آن چون $d|k$ داریم $k = dt$ و در نتیجه $k/d = t$.

حال فرض کنیم $s \in N$ و داشته باشیم: $(a^k)^s = e$

لذا $a^{ks} = e$ در نتیجه $n|ks$ پس $n/d|k/d \cdot s$ و چون $(n/d, k/d) = 1$ لذا $n/d|s$ پس $o(a^k) = n/d$ و اثبات کامل است.

۲۶ ـ فرض کنیم $\langle x^r \rangle = \langle x^s \rangle$ پس $o(x^r) = o(x^s)$ و بنا به تمرین ۲۵ داریم $o(x^s) = \frac{n}{(n,s)}$ و $o(x^r) = \frac{n}{(n,r)}$ لذا $(n,r) = (n,s)$

۲۷ ـ می‌دانیم که تعداد مولدهای Z_n برابر $\varphi(n)$ می‌باشد که در آن φ تابع اویلر می‌باشد زیرا تمام اعداد از ۱ تا n که با n متباین هستند Z_n را تولید می‌کنند پس داریم:

$$\text{تعداد مولدهای } Z_{pq} = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

۲۸ ـ اوّلاً معادله دارای جواب است زیرا e یک جواب آن می‌باشد حال چون

$m|n$ پس $mq = n$ و حال $e, a^q, a^{2q}, \ldots, a^{(m-1)q}$، m جواب معادله $x^m = e$ می‌باشند و مطلب تمام است.

۲۹ ـ برای اثبات مسئله چنین عمل می‌کنیم:

$$(ab)^2 = (ab)(ab) = e \Rightarrow a(ba)b = e \Rightarrow aa(ba)bb = aeb \Rightarrow e(ba)e = ab \Rightarrow ba = ab$$

۳۰ ـ فرض کنیم $o(ab) = n$ و $o(ba) = m$ و $n<m$ داریم:

$$e = (ba)^m = b(ab)^{m-1}a = b(ab)^n(ab)^{n-(m-1)}a = b(ab)^{n-m+1}a = (ba)^{n-m+2}$$

پس بنا به فرض $m \leq n-m+2$ و لذا $2m \leq n+2 < m+2$ در نتیجه $m < 2$ یعنی $m = 1$ پس $n<1$ و تناقض با مرتبه بودن n می‌باشد زیرا n بایستی عدد طبیعی باشد پس حکم ثابت شده است.

۳۱ ـ بنا به تمرین ۳۰ همین بخش داریم:

$$o(x^{-1}ax) = o(xx^{-1}a) = o(ea) = o(a)$$

پس $o(x^{-1}ax) = o(a)$ و اثبات کامل است.

۳۲ ـ با توجه به مسئله ۳۱ داریم:

به ازای هر x متعلّق به G: $o(a) = o(x^{-1}ax)$ و چون طبق فرض مسئله a تنها عنصر از مرتبه n است لذا بایستی داشته باشیم $a = x^{-1}ax$ در نتیجه $xa = ax$ و لذا $a \in Z(G)$

۳۳ ـ چون $(m, n) = 1$ پس اعدادی صحیح چون a و b وجود دارند بطوریکه $ma + nb = 1$ در نتیجه $(n, a) = 1$ و $(m, b) = 1$ و داریم:

$$x = x^{ma+nb} = x^{ma} \cdot x^{nb} = zy \quad x = x^{nb+ma} = x^{nb}x^{ma} = yz$$

حال طبق مسئله شماره ۲۵ داریم:

$$o(x^{ma}) = \frac{mn}{(mn, ma)} = \frac{mn}{m(n, a)} = \frac{n}{(n, a)} = \frac{n}{1} = n$$

$$o(x^{nb}) = \frac{mn}{(mn, nb)} = \frac{mn}{n(m, b)} \frac{m}{(m, b)} = m$$

پس کافی است $z = x^{ma}$ و $y = x^{nb}$ اختیار کنیم، مسئله حل خواهد شد.

۳۴ـ فرض کنیم $H^2 = H$ و a و b دو عضو دلخواه H باشند داریم:

$$ab \in H^2 = H \Rightarrow ab \in H$$

و لذا H نسبت به عمل دو تایی القاء شده بسته است و چون H ناتهی و متناهی است بنابه مسئله شماره ۲۳ همین بخش H زیرگروه G است.

۳۵ـ در S_3، $\rho_1 = (1\ 2\ 3)$ ، $\mu_1 = (1\ 2)$

$$\rho_1 \mu_1 = (2\ 3) \qquad \mu_1 \rho_1 = (1\ 3)$$

چون $\mu_1 \rho_1 \neq \mu_2 \rho_2$، با در نظر گرفتن همین جایگشتها در S_n مطلب حاصل می‌شود.

۳۶ـ فرض کنیم σ همانی نباشد در اینصورت عضوی چون a هست که $a\sigma = b$ فرض کنیم $b\sigma = c$ ($b \neq c$ چون σ جایگشت است) حال جایگشت γ از S_n را چنین ارائه می‌کنیم $\gamma = (b, c)$ داریم:

$$a(\gamma\sigma) = (a\ \gamma)\sigma = a\sigma = b$$

$$a(\sigma\gamma) = (a\ \sigma)\gamma = b\gamma = c$$

در نتیجه چون $b \neq c$ پس $\gamma\sigma \neq \sigma\gamma$ لذا با فرض تناقض ایجاد می‌شود پس σ همانی می‌باشد.

۳۷ ـ فرض کنیم B_n مجموعهٔ جایگشتهای فرد S_n باشد و A_n مجموعهٔ جایگشتهای زوج آن، تابع $f: A_n \to B_n$ را با ضابطهٔ $\sigma f = (۱\ ۲)\sigma$ در نظر می‌گیریم.

اوّلاً f خوش تعریف است زیرا اگر $\sigma_۱ = \sigma_۲$ آنگاه

$$\sigma_۱ f = (۱\ ۲)\sigma_۱ = (۱\ ۲)\sigma_۲ = \sigma_۲ f$$

ثانیاً f یک به یک است زیرا اگر $\sigma_۱ f = \sigma_۲ f$ آنگاه

$$(۱\ ۲)\sigma_۱ = (۱\ ۲)\sigma_۲ \Rightarrow \sigma_۱ = \sigma_۲$$

ثالثاً f پوشاست، فرض کنیم $\alpha \in B_n$ و $\sigma = (۱\ ۲)\alpha$ اکنون

$$\sigma f = (۱۲)(۱۲)\alpha = \alpha$$

۳۸ ـ فرض کنیم H یک زیرگروه از S_n باشد اگرتمام جا یگشتهای H زوج باشند حکم برقرار است، پس فرض کنیم چنین نباشد یعنی جایگشت فردی چون $\alpha \in H$ وجود دارد.

مجموعهٔ جایگشتهای زوج H را $H_۲$ و مجموعهٔ جایگشتهای فرد آن را $H_۱$ می‌نامیم و تابع $f: H_۱ \to H_۲$ را در نظر می‌گیریم، داریم:

$$\sigma \to \alpha\sigma$$

آ) f خوش تعریف است زیرا اگر $\sigma_۱ = \sigma_۲ \in H_۱$ داریم:

$$\sigma_۱ f = \alpha\sigma_۱ = \alpha\sigma_۲ = \sigma_۲ f$$

ب) f یک به یک است زیرا اگر $\sigma_۱ f = \sigma_۲ f$ در اینصورت داریم $\alpha\sigma_۱ = \alpha\sigma_۲$ در نتیجه $\sigma_۱ = \sigma_۲$

ج) f پوشاست زیرا اگر $\gamma \in H_۲$ در اینصورت قرار می‌دهیم $\sigma = \alpha^{-۱}\gamma \in H_۱$

$$\sigma f = (\alpha^{-۱}\gamma) f = \alpha\alpha^{-۱}\gamma = \gamma$$

پس تعداد جایگشتهای زوج و فرد H باهم برابرند.

۳۹ ـ فرض کنیم حکم برقرار نباشد در اینصورت داریم:

وجود دارد یک جایگشت فرد مانند σ_1 که به ازای هر جایگشت زوج چون σ_2 بطوریکه $\sigma_1 \neq \sigma\sigma_2$.

فرض کنیم $\sigma_2 = \sigma^{-1}\sigma_1$ واضح است که $\sigma_2 \in A_n$ برای این σ_2 باید داشته باشیم $\sigma_1 = (\sigma\sigma^{-1})\sigma_1 = \sigma(\sigma^{-1}\sigma_1) = \sigma\sigma_2 \neq \sigma_1$ یعنی $\sigma_1 \neq \sigma_1$ که این تناقض آشکار است .

۴۰ ـ فرض کنید $\sigma \neq I \in S_4$ پس $\sigma = \sigma_1\sigma_2 \ldots \sigma_t$ که $\sigma_1, \ldots, \sigma_t$ دورهای دو بدو مجزا و طولشان بیشتر از **یک** است چون اعضای دامنه σ_i از مجموعه $\{1,2,3,4\}$ انتخاب می‌شوند پس σ ها طولشان نمی‌تواند از ۴ بیشتر باشد و σ_i و σ_j که $i \neq j$ هیچ عضو مشترکی ندارند پس $t \leq 2$ پس σ یا خود یک دور است یا به حاصلضرب دوترانهش تجزیه می‌شود که اگر σ دور باشد پس با طول ۲ ، ۳ یا ۴ است لذا ۴ و ۳ و ۲ = $o(\sigma)$ اگر σ حاصلضرب دوترانهش باشد آنگاه

۲ = $o(\sigma)$ پس در هر حالت S_4 عضوی از مرتبه بزرگتر از چهار نخواهد داشت.

۴۱ ـ تعداد آرایشهای متمایز r تایی از n شی برابر $\frac{n!}{(n-r)!}$ می‌باشد و چون داریم $(a_1 \ldots a_r) = (a_2 \ldots a_r a_1) = \ldots = (a_r a_1 \ldots a_{r-1})$

پس تعداد دورهای مجزا با طول r برابر است با $\frac{n!}{r(n-r)!}$

۴۲ ـ چون هرکدام از سیکلهای به طول سه یک جایگشت زوج هستند پس تمام سیکلهای به طول سه از S_4 متعلق به A_4 هستند با توجه به تمرین قبل تعداد دورهای به طول سه (مجزا) در A_4 برابر ۸ می‌باشد حال فرض کنیم مجموعهٔ H زیر گروه A_4 و مرتبه H برابر شش باشد همهٔ دورهای به طول سه از A_4 به H متعلق نیستند مثلاً فرض کنیم ، x یک دور به طول سه باشد که x متعلق به H نیست ، چون

مرتبه x برابر سه است پس $K = \{ e , x , x^2 \}$ یک زیرگروه S_n می‌باشد اکنون چون x متعلّق به H نیست پس $x^2 = x^{-1} \notin H$ لذا: $k \cap H = \{e\}$ و داریم:

$$Hk \subseteq A_4 \text{ پس } |HK| = \frac{|H| \cdot |K|}{|K \cap H|} = \frac{6 \times 3}{1} = 18$$

و $|HK| = 18$، بیشتر از مرتبه A_4 می‌باشد و تناقض است پس A_4 زیرگروهی از مرتبه شش ندارد

۴۳ ـ اگر $(a\ b\ c)$ یک دور به طول سه و دلخواه باشد داریم:

$(a\ b\ c) = (a\ b)(a\ c)$ پس $(a\ b\ c)$ متعلّق به A_n می‌باشد.

حال اگر σ عضوی دلخواهی از A_n باشد داریم $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$ که k زوج بوده و σ_1 و ... و σ_k ترانهش می‌باشند $\sigma_i \sigma_{i+1}$ را در نظر می‌گیریم دو حالت وجود دارد یا σ_i و σ_{i+1} مجّزا هستند که در اینصورت داریم

$(a\ b)(c\ d) = (a\ c\ d)(a\ c\ b)$

اگر مجّزا نباشند داریم: $(a\ b)(a\ c) = (a\ b\ c)$

و در هر حالت $\sigma_i \sigma_{i+1}$ حاصلضربی از دورهای بطول سه است لذا σ حاصلضربی از دورهای به طول سه بوده و اثبات کامل است.

۴۴ ـ (آ) فرض کنیم $x , y \in N(a)$ در اینصورت داریم:

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

$$\Rightarrow xy \in N(a)$$

فرض کنیم e عضوهمانی G باشد: $ea = ae = e \Rightarrow e \in N(a)$

بالاخره فرض کنیم x متعلّق به $N(a)$ باشد داریم:

$$xa = ax \Rightarrow x^{-1}x\,a\,x^{-1} = x^{-1}axx^{-1} \Rightarrow ax^{-1} = x^{-1}a \Rightarrow x \in N(a)$$

پس $N(a)$ زیرگروه G است.

ب)

$$a \in Z(G) \Leftrightarrow N(a) = G$$

زیرا $Z(G)$ تمام xهایی از G است که با همهٔ اعضای G جابجا می‌شوند پس a متعلّق به $Z(G)$ است اگر و فقط اگر با تمام اعضای G جابجا شود و طبق تعریف $N(a)$، a متعلّق به $Z(G)$ اگر $N(a) = G$ باشد.

۴۵ - چون $(m, n) = 1$ پس بنابه قضیه بزو، x و yای در اعداد صحیح وجود دارند بطوریکه $mx + ny = 1$ و لذا خواهیم داشت:

$$g = g^{mx+ny} = g^{mx} \cdot g^{ny} = (g^m)^x \cdot (g^n)^y = (g^m)^x \cdot e$$
$$= (g^m)^x \in H \Rightarrow g \in H$$

۴۶ - عکس نقیض هرگزارهٔ شرطی معادل خود آن است و لذا برای اثبات این مسئله عکس نقیض آنرا اثبات می‌کنیم یعنی:

«اگر G گروهی نامتناهی باشد در آن صورت به تعداد نامتناهی زیرگروه دارد»

برای این منظور فرض کنیم G گروهی نامتناهی باشد برای هر a متعلّق به G زیرگروههایی از G به صورت $< a >$ را در نظر می‌گیریم اگر تعداد این زیرگروهها نامتناهی باشد که حکم برقرار است، در غیر اینصورت یکی از $< a >$ ها دارای تعداد متناهی عضو نیست به عبارت دیگر یکی از آنها نامتناهی است و چون از مرتبهٔ نامتناهی تنها یك گروه در حد ایزومورفیسم وجود دارد و آن گروه اعداد صحیح با عمل جمع می‌باشد لذا $< a >$ با $\mathbf{Z}$ ایزومورف بوده و بنابراینکه گروه اعداد صحیح با عمل جمع دارای تعداد نامتناهی زیرگروه است $< a >$ نیز چنین است یعنی تعداد زیرگروههای $< a >$ نامتناهی است و لذا حکم ثابت شده است.

۴۷ - برای اثبات لزوم فرض کنیم $b^k = e$ بنابه قضیه تقسیم داریم:

$k = nq + r \quad 0 \leq r < n$ از طرفی داریم:

$e = b^k = b^{nq+r} = (b^n)^q . b^r = eb^r = b^r$

اگر $r = o$ مسئله حل است واگر $r \neq o$ پس از رابطه فوق نتیجه می‌گیریم که $b^r = e$ ولی چون $r < n$ لذا تناقض با اینست که n مرتبه b است پس $r = o$ لذا $n \mid k$

برای اثبات کفایت فرض کنیم $n \mid k$ دراینصورت قرار می‌دهیم $k = nl$ لذا خواهیم داشت $b^k = b^{nl} = (b^n)^l = e^l = e$ پس اثبات در اینجا کامل شده است.

۴۸ ـ چون Z_p یک گروه دوری است لذا هر زیرگروه آن دوری است و بنابر متناهی بودن آنها، هرکدام با Z_kای ایزومورف است ولی می‌دانیم که چون p عددی اوّل است Z_p دارای $p - ۱$ مولد می‌باشد و $\{o\}$ زیرگروه بدیهی آن است لذا Z_p زیرگروه واقعی و نابدیهی ندارد.

۴۹ ـ فرض کنیم که $H = < a >$ و $K = < b >$ در اینصورت ثابت می‌کنیم $o(ab) = rs$ در نتیجه $M = < ab >$ زیرگروه G از مرتبه rs خواهد بود امّا برای اثبات اینکه $o(ab) = rs$ چنین عمل می‌کنیم:

$(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e$

حال فرض کنیم $o(ab) = t$ پس بنابه رابطه فوق $t \mid rs$ در نتیجه $t \leq rs$

$a^{st} = a^{st} e = a^{st} b^{st} = (ab)^{st} = e \Rightarrow r \mid st$

$b^{rt} = eb^{rt} = a^{rt}b^{rt} = (ab)^{rt} = e \Rightarrow s \mid rt$

از رابطه $r \mid st$ و اینکه $(r , s) = ۱$ نتیجه می‌گیریم $r \mid t$.

از رابطه $s \mid rt$ و اینکه $(r , s) = ۱$ نتیجه می‌گیریم $s \mid t$.

چون $(r , s) = ۱$ لذا کوچکترین مضرب مشترک r , s مساوی rs می‌باشد و ازطرفی $t \mid r$ و $t \mid s$ بنابراین $rs \mid t$ در نتیجه $rs \leq t$ وقبلاً داشتیم $t \leq rs$

در نتیجه $t = rs$ و مطلب تمام است .

۵۰ـ اگر $K \subseteq H$ یا $H \subseteq K$ در اینصورت $H \cup K$ برابر K یا H خواهد بود ولذا $H \cup K$ زیرگروه G خواهد بود.

به عکس فرض کنیم $H \cup K$ زیرگروه G باشد و $H \not\subset K$ و $K \not\subset H$ لذا وجود دارد xای متعلّق به K که x متعلّق به H نیست و همچنین وجود دارد yای متعلّق به H که y متعلّق به K نیست.

بنابراین x و y هر دو متعلّق به $H \cup K$ بوده و چون $H \cup K$ زیرگروه است لذا x^{-1} , y^{-1} هر دو متعلّق به $H \cup K$ خواهند بود و در نتیجه xy^{-1} نیز متعلّق به $H \cup K$ بوده و لذا

$$\begin{cases} xy^{-1} \in H \rightarrow xy^{-1}\, y = x \in H \\ xy^{-1} \in K \rightarrow x^{-1}xy^{-1} = y^{-1} \in K \rightarrow y \in K \end{cases}$$

که در هر حالت تناقضی آشکار است ولذا فرض خلف باطل است یعنی $H \subseteq K$ یا $K \subseteq H$

۵۱ ـ در تمرین ۲۴ همین بخش گروه چهارهٔ کلاین معرّفی شد که در اینجا دوباره برای یاد آوری جدول کیلی آن را رسم می‌کنیم و ملاحظه می‌شود که این گروه دوری نیست زیرا توسط هیچکدام از اعضا تولید نمی‌شود ولی هر زیرگروه آن دوری است.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\langle a \rangle = \{e , a\}$$
$$\langle b \rangle = \{e , b\}$$
$$\langle c \rangle = \{e , c\}$$
$$\langle e \rangle = \{e\}$$

۵۲ـ در تمرین ۵۱ اگر گروه چهارهٔ کلاین را همراه با دو زیرگروه $\langle a \rangle$ و $\langle b \rangle$ در نظر بگیریم واضح است که $\langle a \rangle \cup \langle b \rangle$ زیرگروه نیست

زیرا $a \in < a > \cup < b >$ و b ولی $ab = c$ و متعلّق نیست به

$< a > \cup < b >$

یا به عنوان مثالی دیگر می‌توان $\mathbf{Z}$ را همراه با دو زیرگروه $۲\mathbf{Z}$ و $۳\mathbf{Z}$ از آن را در نظر گرفت که $۲\mathbf{Z} \cup ۳\mathbf{Z}$ زیرگروه نیست زیرا:

$۲ \in ۲\mathbf{Z} \cup ۳\mathbf{Z} \wedge ۳ \in ۲\mathbf{Z} \cup ۳\mathbf{Z}$

ولی $۲ - ۳ = ۱$ متعلّق به این مجموعه نیست پس اجتماع $۲\mathbf{Z}$ و $۳\mathbf{Z}$ نسبت به عمل بسته نبوده و زیرگروه نیست.

۵۳ـ فرض کنیم $G = < a >$ و مرتبه G مساوی عدد فرد n باشد داریم:

$G = \{ a , a^{۲} , \dots , a^{n-۱} , e \}$

$$aa^{۲}a^{۳} \dots a^{n} = a^{\frac{n(n+۱)}{۲}} = (a^{n})^{\frac{n+۱}{۲}} = e^{\frac{n+۱}{۲}} = e$$

۵۴ـ چون مرتبه گروه G عدد اوّل می‌باشد پس $G \neq \{e\}$ و لذا G دارای یک عضو غیر همانی چون a است و مطابق نتیجه‌ای از قضیه لاگرانژ می‌دانیم که

$| G | \; | \; o (a)$ و چون $o(a) \neq ۱$ و مرتبه G عدد اوّل است لذا

$| G | \; | \; o (a)$ درنتیجه $G = < a >$ و لذا G دوری بوده ومطلب تمام است.

۵۵ـ فرض کنیم $Hx = Ky$ داریم:

$$Hx = Ky \Rightarrow Hxy^{-۱} = K \Rightarrow exy^{-۱} = k \in K$$

$$\Rightarrow xy^{-۱} \in K \Rightarrow (xy^{-۱})^{-۱} = yx^{-۱} \in K$$

$$Hx = Ky \Rightarrow H = Kyx^{-۱} = K \Rightarrow H = K$$

۵۶ـ فرض کنیم x عضو دلخواهی از G باشد چون G دوری با مولد a است پس وجود دارد n ای بطوریکه $x = a^{n}$ و لذا خواهیم داشت

$x\varphi = a^n\varphi = (a\varphi)^n$

و مطلب تمام است.

۵۷ ـ فرض برآنست که φ و ψ ایزومورفیسم هستند پس یک به یک و پوشا هستند لذا ترکیب آنها یعنی $\varphi\psi$ یک به یک و پوشاست.

فرض کنیم x و y اعضای دلخواه از G باشند داریم:

$$(xy)\varphi\psi = [(xy)\varphi]\psi = [(x\varphi)(y\varphi)]\psi$$

$$= [(x\varphi)\psi][(y\varphi)\psi] = (x\varphi\psi)(y\varphi\psi)$$

پس $\varphi\psi$ هممورفیسم بوده و لذا $\varphi\psi$ ایزومورفیسم از G به K می‌باشد.

۵۸ فرض کنیم $G = \langle a \rangle$ گروه دوری دلخواه از مرتبهٔ n باشد تابع $\varphi : \mathbf{Z}_n \to G$ را با ضابطه $k\varphi = a^k$ در نظر می‌گیریم

فرض کنیم $x\varphi = y\varphi$ یعنی $a^x = a^y$ و از آنجا $x = y$ پس φ یک به یک است.

فرض کنیم a^m عضو دلخواهی از G باشد در اینصورت $m \in \mathbf{Z}_n$ و $m\varphi = a^m$ پس φ پوشاست.

اگر x و y اعضای دلخواه از $\mathbf{Z}_n$ باشند داریم:

$$(x + y)\varphi = a^{x+y} = a^x a^y = (x\varphi)(y\varphi)$$

پس φ هممورفیسم می‌باشد در نتیجه φ یک ایزومورفیسم است.

۵۹ ـ $\varphi_g : G \to G$، $x\varphi_g = gxg^{-1}$ فرض کنیم $x\varphi_g = y\varphi_g$ در اینصورت $gxg^{-1} = gyg^{-1}$ در نتیجه $g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$ و بنابراین $exe = eye$ و لذا $x = y$ پس φ_g یک به یک می‌باشد.

فرض کنیم x عضو دلخواهی از G باشد در اینصورت $g^{-1}xg \in G$ و داریم $(g^{-1}xg)\varphi_g = x$ پس φ_g پوشاست.

اگر a و b اعضای دلخواهی از G باشند داریم:

$(ab)\varphi_g = g(ab)g^{-1} = g(ag^{-1}gb)g^{-1} = (gag^{-1})(gbg^{-1}) = (a\varphi_g)(b\varphi_g)$

۶۰ـ فرض کنیم که گروه اعداد گویا با عمل جمع دوری باشد و توسط $a \neq 0$ تولید شود در اینصورت $a/2$ هیچ مضربی از آن نخواهد بود (البته مضرب منظور مضرب صحیح است) و این تناقض است پس گروه اعداد گویا با عمل جمع دوری نیست.

۶۱ـ اگر $(m , n) = 1$ آنگاه $\mathbf{Z}_n \times \mathbf{Z}_m$ دوری است و با $\mathbf{Z}_{nm}$ ایزومورف است، از طرف دیگر اگر a یک مولد $\mathbf{Z}_n$ و b یک مولد $\mathbf{Z}_m$ باشد (a , b) یک مولد $\mathbf{Z}_n \times \mathbf{Z}_m$ است بنابراین داریم:

$\varphi(m)\varphi(n) =$ تعداد مولدهای $\mathbf{Z}_n \times \mathbf{Z}_m$، از طرف دیگر تعداد مولدهای $\mathbf{Z}_{nm}$ برابر $\varphi(nm)$ می‌باشد و چون دو گروه بالا ایزومورف هستند پس

$$\varphi(nm) = \varphi(n)\varphi(m)$$

۶۲ـ $\pi_{i=1}^{n} G_i$ بر طبق قضیه گروه است فرض کنیم x و y دو عضو دلخواهی از $\pi_{i=1}^{n} G_i$ باشند قرار می‌دهیم:

$$x = (a_1 , a_2 , \dots , a_n) \qquad y = (b_1 , b_2 , \dots , b_n)$$

$$xy = (a_1 , a_2 , \dots a_n)(b_1 , \dots , b_n) = (a_1b_1 , a_2 b_2 , \dots a_nb_n)$$

$$= (b_1a_1 , b_2a_2 , \dots , b_na_n) = (b_1,b_2,\dots,b_n)(a_1 , a_2 , \dots , a_n) = yx$$

۶۳ـ تابع $f : \langle r \rangle \times \langle s \rangle \to \mathbf{Z}_n$ که باضابطه $f[(xr , ys)] = xr + ys$ داده شده در نظر می‌گیریم ثابت می‌کنیم f ایزومورفیسم است.

ابتدا نشان می‌دهیم $\langle r \rangle \cap \langle s \rangle = \{0\}$ برای این منظور فرض کنیم

$x \in < r > \cap < s >$ دلخواه باشد لذا $x = mr$ و $x = ks$ چون

$(r , s) = ۱$ لذا برای x و yای داریم $rx + sy = ۱$ چون $x = mr$ و $x = ks$

پس $mr = ks$ در نتیجه $r \mid ks$ و لذا $r \mid k$ بنابراین $k = tr$ و حال توجه می‌کنیم

که $x = ks = trs = t'n = ۰$ لذا $< r > \cap < s > = \{۰\}$ از این مطلب

می‌توان نتیجه گرفت که f یک به یک است.

و چون دامنه و هم دامنه f متناهی است لذا f پوشاست ثابت می‌کنیم f حافظ ساختار گروه است.

$$[(x_۱r , y_۱s) + (x_۲r , y_۲s)]f = (x_۱r + x_۲r , y_۱s + y_۲s)f$$

$$= (x_۱ r + x_۲r) + (y_۱s + y_۲s) = (x_۱r + y_۱s) + (x_۲r + y_۲s)$$

$$= (x_۱r , y_۱s)f + (x_۲ r , y_۲ s)f$$

پس f یک ایزومورفیسم می‌باشد.

بنابراین Z_n حاصلضرب مستقیم داخلی $< r >$, $< s >$ است.

۶۴ـ فرض کنیم x و y اعضائی از $N_G(H)$ باشند در اینصورت

$x^{-۱}Hx = H$ و $y^{-۱}Hy = H$ و درنتیجه $y^{-۱}x^{-۱}Hxy = y^{-۱}Hy$ بنابراین

$(xy)^{-۱}Hxy = H$ و لذا xy متعلّق به $N_G(H)$ می‌باشد پس $N_G(H)$ نسبت به عمل بسته است.

حال چون $eHe = H$ پس e متعلّق به $N_G(H)$ می‌باشد.

فرض کنیم x متعلّق به $N_G(H)$ باشد در اینصورت $x^{-۱}Hx = H$ در نتیجه

$x H x^{-۱} = xx^{-۱} H xx^{-۱}$ بنابراین $xHx^{-۱} = H$ پس $x^{-۱}$ متعلّق به $N_G(H)$ بوده ولذا $N_G(H)$ زیرگروه G می‌باشد.

۶۵ـ الف) به ازای هر z و y متعلّق به $x^{-۱}Hx$، h و h'ای متعلّق به H است که $z = x^{-۱}hx$ و $y = x^{-۱}h'x$

$yz = (x^{-1}h\acute{x})\,(x^{-1}hx) = x^{-1}h\acute{h}x \in x^{-1}Hx$

پس H نسبت به عمل بسته است.

حال چون $e = x^{-1}ex$ پس e متعلّق به $x^{-1}Hx$ می‌باشد.

فرض کنیم y متعلّق به $x^{-1}Hx$ باشد پس h ای متعلّق به H وجود دارد بطوریکه $y = x^{-1}hx$ و داریم

$y^{-1} = (x^{-1}hx)^{-1} = x^{-1}h^{-1}x \in x^{-1}Hx$

پس $x^{-1}Hx$ زیرگروه G است.

ب ـ فرض کنیم $H = <h>$ ادعا می‌کنیم $x^{-1}Hx = <x^{-1}hx>$ برای این منظور فرض کنیم $y \in x^{-1}Hx$ پس h' متعلّق به H وجود دارد بطوریکه $y = x^{-1}h'x$ چون $H = <h>$ پس $h' = h^k$ لذا $y = x^{-1}h^kx$ در نتیجه $y = (x^{-1}hx)^k$ پس $x^{-1}Hx = <x^{-1}hx>$

ج ـ فرض کنیم H آبلی باشد و z و y اعضای از $x^{-1}Hx$ باشند پس h و h' ای متعلّق به H وجود دارند بطوریکه $y = x^{-1}hx\ ,\ z = x^{-1}h'x$

و داریم: $yz = (x^{-1}hx)(x^{-1}h\acute{x}) = x^{-1}h(xx^{-1})\,h'x$

$= x^{-1}hh'x = x^{-1}h'hx = x^{-1}h'ehx = x^{-1}h'xx^{-1}hx = zy$

پس $x^{-1}Hx$ آبلی است.

۶۶ ـ اوّلاً ثابت می‌کنیم $\mathbf{Z}(G)$ زیرگروه G می‌باشد.

فرض کنیم x و y اعضایی از $\mathbf{Z}(G)$ باشند داریم:

$\forall g \in G : (xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$

پس $\mathbf{Z}(G)$ نسبت به عمل بسته است.

چون به ازای هر g از G داریم $g = eg = ge$ پس e متعلّق به $\mathbf{Z}(G)$ می‌باشد

فرض کنیم x عضوی از $\mathbf{Z}(G)$ باشد و g عضو دلخواهی از G باشد در اینصورت

داریم، $xg = gx \Rightarrow x^{-1}xgx^{-1} = x^{-1}gxx^{-1} \Rightarrow gx^{-1} = x^{-1}g$

و بنابراین x^{-1} عضوی از $Z(G)$ است پس $Z(G)$ زیر گروه G می‌باشد.

حال برای اثبات نرمال بودن $Z(G)$ فرض کنیم x عضوی از $Z(G)$ و g عضوی از G باشد باید نشان دهیم $g^{-1}xg \in Z(G)$، فرض کنیم y عضوی از G باشد

$$(g^{-1}xg)y = (g^{-1}gx)y = g^{-1}gyx = g^{-1}ygx = yg^{-1}gx = y(g^{-1}xg)$$

پس بنابراین $g^{-1}xg \in Z(G)$ و مطلب تمام است.

۶۷ ـ بنابه تمرین ۶۶ همین بخش چون $Z(G)$ در G نرمال می‌باشد لذا $\frac{G}{Z(G)}$ یک گروه است حال فرض کنیم $\frac{G}{Z(G)}$ دوری باشد در نتیجه $\frac{G}{Z(G)} = <gZ(G)>$ حال فرض کنیم x و y اعضایی از G باشند لذا $xZ(G) = g^m Z(G)$ و $yZ(G) = g^n Z(G)$ به ازای یک m و n ای.

حال از دو رابطه اخیر داریم $x = g^m h$ و $y = g^n t$ که t و h اعضای از $Z(G)$ هستند پس خواهیم داشت.

$$xy = (g^m h)(g^n t) = g^m(hg^n)t = g^m(g^n ht)$$

$$g^m g^n(ht) = g^{m+n}(ht) = g^n g^m(th) = g^n(g^m t)h$$

$$= g^n(tg^m)h = (g^n t)(g^m h) = yx$$

توجه: در روابط فوق از اینکه h و t اعضایی از $Z(G)$ هستند استفاده شده است.

پس G آبلی است.

۶۸ ـ اگر G دوری باشدکه حکم ثابت است ولی اگر G دوری نباشد پس G هیچ عنصری از مرتبه ۲۵ ندارد و چون طبق نتیجه‌ای از قضیه لاگرانژ می‌دانیم که به ازای هر g از G مرتبه g، مرتبه G را می‌شمارد لذا ۵ یا ۱ $= o(g)$ می‌باشد در نتیجه اگر $g \neq e$ آنگاه $o(g)$ برابر پنج بوده و لذا $g^5 = e$ و اگر $g = e$ آنگاه $e^5 = e$ و اثبات کامل است.

۶۹ ـ فرض کنیم H زیرگروه G باشد و h عضوی از H و g عضوی از G باشد طبق فرض زیرگروه $< h >$ در G نرمال بوده ولذا $g^{-1} < h > g = < h >$ در نتیجه $g^{-1} < h > g \subseteq H$ بنابراین چون می‌دانیم $g^{-1}hg \in < h >$ پس $g^{-1}hg \in H$ در نتیجه $g^{-1}Hg \subseteq H$ و چون $H \subseteq g^{-1}Hg$ پس $g^{-1}Hg = H$ و لذا H در G نرمال می‌باشد چون H دلخواه بود پس هر زیرگروه G در G نرمال می‌باشد.

۷۰ ـ این مسئله نتیجه‌ای از مسئله تعمیم یافته زیراست.

« فرض کنید G یک گروه آبلی از مرتبه n باشد و $(r,n) = ۱$ نشان دهید معادلهٔ $x^r = a$ به ازای هر a از G فقط یک جواب دارد »

قبل از اثبات این مسئله تعمیم یافته متذکّر می‌شویم که چون در مسئله اصلی مرتبه G فرد است پس مرتبه G و ۲ متباینند و لذا در شرایط مسئله تعمیم یافته صادق است حال به اثبات مسئله تعمیم یافته می‌پردازیم.

اوّلاً نشان میدهیم که معادله $x^r = a$ به ازای هر a جواب دارد، چون $(r,n) = ۱$ پس اعداد صحیحی چون k و m وجود دارند بطوریکه $rk + nm = ۱$ حال داریم: $(a^k)^r = a^{kr} = a^{kr}e = a^{kr}(a^n)^m = a^{kr}a^{nm} = a^{kr+nm} = a$

پس معادله دارای جواب است.

حال فرض کنیم c و b دو جواب $x^r = a$ باشند بنابراین $c^r = a$ و $b^r = a$ در نتیجه $b^r = c^r$ لذا $b^rc^{-r} = e$ نهایتاً چون G آبلی است خواهیم داشت

$$(bc^{-1})^r = e \qquad (۱)$$

چون $(r,n) = ۱$ لذا $bc^{-1} = e$ بنابراین $b = c$.

توجّه: از رابطه (۱) نتیجه می‌گیریم $o(bc^{-1}) \mid n$ و $o(bc^{-1}) \mid r$ پس چون $(r,n) = ۱$ لذا $o(bc^{-1}) = ۱$ پس $bc^{-1} = e$.

۷۱ ـ اگر گروه G نامتناهی باشند و دوری نیز باشد در اینصورت هیچ عضوی

از مرتبه عدد اوّل ندارد. اگر دوری و متناهی باشد در اینصورت از مرتبه هر عددی که مرتبه G را عاد کند فقط یک زیرگروه دارد، حال اگر یک زیرگروه از مرتبه p دقیقاً $p-1$ عنصر از مرتبه p داشته‌باشد و بقیّه عناصر از مرتبه p از G متعلّق به زیر گروههای دیگری از مرتبهٔ p می‌باشند و چون زیرگروهی دیگر از مرتبه p وجود ندارد لذا G نمی‌تواند دوری باشد.

۷۲ ـ فرض کنیم H و K دو زیرگروه G باشند و $G = H \cup K$ حال x متعلّق به H را طوری در نظر می‌گیریم که $x \notin K$ و $y \in K$ را در نظر می‌گیریم که $y \notin H$ چون y و x اعضایی از $H \cup K$ هستند و $G = H \cup K$ لذا xy عضوی از $H \cup K$ بوده و لذا xy متعلّق به K یا xy متعلّق به H می‌باشد

فرض کنیم xy عضوی از K باشد پس xyy^{-1} نیز عضوی از K می‌باشد یعنی x عضوی از K است و این تناقض است.

فرض کنیم xy عضوی از H باشد پس $x^{-1}xy$ عضوی از H بوده یعنی y عضوی از H است و این تناقضی آشکار است پس فرض خلف باطل است یعنی

$G \neq H \cup K$.

۷۳ ـ فرض کنیم G یک گروه با مرتبه n باشد که n عددیست فرد پس $(n$ و $۲) = ۱$ در نتیجه وجود دارد دو عدد صحیحی چون k و m بقسمی که $۲k + mn = ۱$.

$$(a^k)^۲ = a^{۲k} = a^{۲k}e = a^{۲k}(a^n)^m = a^{۲k}a^{nm} = a^{۲k+nm} = a$$

پس a^k یک جواب معادله است، حال فرض کنیم که b یک جواب دیگر معادله فوق باشد پس $b^۲ = a$ ولذا $b^{۲k} = (b^۲)^k = a^k$ از طرفی می‌دانیم

$$(b^k)^۲ = b^{۲k} = b^{۲k}e = b^{۲k}b^{mn} = b^{۲k+mn} = b$$

پس $b = a^k$ در نتیجه جواب $x^۲ = a$ منحصر بفرد و a^k می‌باشد.

۷۴ـ می‌دانیم مرکز هر p گروه متناهی غیر بدیهی است پس $Z(G) \neq \{e\}$، از تمرین شماره شصت و شش می‌دانیم که $Z(G)$ زیر گروه نرمال G می‌باشد و بنابراین طبق قضیه لاگرانژ مرتبه $Z(G)$ مرتبه G را می‌شمارد پس مرتبه $Z(G)$ یکی از اعداد p، p^2 یا p^3 می‌باشد اگر p باشد که حکم ثابت است اگر p نباشد یکی از اعداد p^3 یا p^2 خواهد بود حال اگر p^3 باشد چون $Z(G) \subseteq G$ پس $Z(G)=G$ و لذا G آبلی است و این خلاف فرض است اگر مرتبه $Z(G)$ برابر p^2 باشد آنگاه مرتبه $\frac{G}{Z(G)}$ برابر با p^1 بوده و مطابق تمرین پنجاه و چهارهمین بخش $\frac{G}{Z(G)}$ دوری بوده و لذا مطابق تمرین شمارهٔ شصت و هفت همین بخش G آبلی است و این نیز خلاف فرض است پس مرتبه $Z(G)$ همان p می‌باشد.

۷۵ـ فرض کنیم H مجموعه متشکل از عناصر از مرتبه متناهی از یک گروه آبلی باشد و x، y اعضایی از H باشند که $o(x) = m$ و $o(y) = n$

$$(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = ee = e$$

پس مرتبه xy متناهی بوده و لذا xy متعلّق به H می‌باشد. چون $o(e) = 1$ پس e عضوی از H است.

فرض کنیم x عضوی از H باشد چون مرتبه معکوس x با مرتبه x برابر است لذا معکوس x متعلّق به h می‌باشد و در نتیجه H زیر گروه G می‌باشد.

۷۶ـ فرض کنید $x \in N(g^{-1}Hg)$ پس $x^{-1}(g^{-1}Hg)x = g^{-1}Hg$ لذا

$$(gxg^{-1})^{-1} Hgxg^{-1} = H \Rightarrow gxg^{-1} \in N(H)$$

$$\Rightarrow x \in g^{-1} N(H) g \Rightarrow N(g^{-1} H g) \subseteq g^{-1} N(H) g \qquad (1)$$

حال فرض کنیم $x \in g^{-1} N(H) g$ خواهیم داشت.

$$g x g^{-1} \in N(H) \Rightarrow (gxg^{-1})^{-1} H (gxg^{-1}) = H$$

$$\Rightarrow (gx^{-1}g^{-1}) H (gxg^{-1}) = H \Rightarrow x^{-1}(g^{-1}Hg) x = g^{-1}Hg$$

$\Rightarrow x \in N(g^{-1}Hg) \Rightarrow g^{-1}N(H)g \subseteq N(g^{-1}Hg)$ (۲)

$g^{-1}N(H)g = N(g^{-1}Hg)$ از روابط (۱) و (۲) داریم

۷۷ ـ فرض کنیم x عضوی از $H \cap K$ باشد، طبق قضیه لاگرانژ داریم:

$o(x) \mid |H| \wedge o(x) \mid |K| \Rightarrow o(x) \mid (|H|, |K|)$

$\Rightarrow o(x) \mid (۵, ۱۲) \Rightarrow o(x) \mid ۱ \Rightarrow o(x) = ۱ \Rightarrow x = e$

پس $H \cap K = \{e\}$.

۷۸ ـ فرض کنیم H زیرگروه G و سره باشد طبق قضیه لاگرانژ $|H| \mid |G|$

لذا $p \mid |H|$ یا $q \mid |H|$ پس $|H| = p$ یا $|H| = q$ و در هر حالت چون H گروهی از مرتبه عدد اوّل می‌باشد لذا H دوری است.

۷۹ ـ ابتدا نشان می‌دهیم که H زیرگروه G می‌باشد برای این منظور فرض کنیم که x و y اعضایی از H باشند پس $x = a^۲$ و $y = b^۲$ که a و b متعلّق به G هستند حال داریم: $xy = a^۲b^۲ = (ab)^۲ \in H$

چون $e = e^۲$ پس $e \in H$ و اگر $x \in H$ باشد آنگاه وجود دارد a ای از G بطوریکه $x = a^۲$ لذا $x^{-1} = (a^{-1})^۲ \in H$ پس $x^{-1} = (a^۲)^{-1} = (a^{-1})^۲$ لذا H زیرگروه G است.

حال نشان می‌دهیم H در G نرمال است، برای این منظور فرض کنیم:

$h \in H \wedge x \in G \quad x^{-1}hx = x^{-1}hx^{-1}h(x^{-1}h)^{-1}x = (x^{-1}h)^۲ h^{-1}(x^{-1})^{-1}x$

$= (x^{-1}h)^۲ h^{-1}x^۲$

چون $(x^{-1}h)^۲$ و h^{-1} , $x^۲$ هر سه متعلّق به H هستند بنابراین از تساوی فوق داریم $x^{-1}hx$ متعلّق به H است پس H در G نرمال است.

۸۰ ـ در تمرین پانزده نشان دادیم که HK زیرگروه است حال کافی است

نشان دهیم که HK نرمال است.

فرض کنیم x متعلّق به G و t متعلّق به HK باشد در اینصورت خواهیم داشت

$$x^{-1}tx = x^{-1}hkx = x^{-1}hxx^{-1}kx = (x^{-1}hx)(x^{-1}kx)$$

چون H نرمال است لذا $(x^{-1}hx) \in H$ و چون K نرمال است لذا $(x^{-1}kx) \in K$

پس از تساوی فوق داریم $(x^{-1}tx) \in HK$ لذا HK در G نرمال است.

۸۱ـ چون $H \cap K = \{e\}$ زیرا اگر $(|K| \text{ و } |H|) = 1$ لذا

$H \cap K \neq \{e\}$ پس $|H \cap K| \geq 2$ و چون $H \cap K$ زیرگروه H می‌باشد

لذا $|H| \mid |H \cap K|$ و $|K| \mid |H \cap K|$ پس $|H \cap K| \neq 1$ و $(|H|, |K|)$

تناقض است پس $H \cap K = H$ حال چون H و K در G نرمال هستند پس

داریم: $\forall h \in H \wedge \forall k \in K : hkh^{-1}k^{-1} \in H \cap K$

زیرا hkh^{-1} عضوی از K است و k^{-1} عضوی از K است پس $hkh^{-1}k^{-1}$ عضوی از K

است و بهمین ترتیب عضوی از H است، لذا $hkh^{-1}k^{-1} = e$ در نتیجه $hk = kh$.

۸۲ـ مجموعه اعداد از ۱ تا n که نسبت به n اوّلند با عمل ضرب به هنگ n

تشکیل یک گروه می‌دهند و معمولاً این گروه را با U_n نمایش می‌دهند حال اگر a

عضوی از این گروه باشد طبق نتیجه‌ای از قضیه لاگرانژ می‌دانیم:

$$a^{\varphi(n)} = e \quad \text{پس} \quad a^{|U_n|} = e$$

۸۳ـ می‌دانیم ۱ـ عضوی از R^* و از مرتبه ۲ است حال اگر این دو ایزومورف

باشند و ایزومورفیسم بین آنها f باشد آنگاه بایستی $f(-1)$ نیز دارای مرتبه دو باشد

ولی برای هر a متعلّق به R اگر $na = 0$ آنگاه $a = 0$ یا $n = 0$ بنابراین

$(R, +)$ هیچ عضوی از مرتبه دو ندارد و لذا این دو ایزومورف نیستند.

۸۴ـ برای اثبات این مسئله کافی است ثابت کنیم که $\frac{G}{N}$ آبلی است اگر وفقط

اگر به ازای هر x و y از G، $xyx^{-1}y^{-1}$، متعلّق به N باشد،

فرض کنیم برای هر x و y از G، $xyx^{-1}y^{-1} \in N$ پس

$$xyx^{-1}y^{-1}N = N \Rightarrow xNyN(xN)^{-1}(yN)^{-1} = N$$

$$\Rightarrow (xN)(yN) = (yN)(xN) \Rightarrow$$ $\frac{G}{N}$ آبلی است.

به عکس فرض کنیم $\frac{G}{N}$ آبلی باشد پس برای هر x و y از G داریم:

$$xNyN = yNxN \Rightarrow xNyN(xN)^{-1}(yN)^{-1} = N$$

$$\Rightarrow xN(xN)^{-1}yN(yN)^{-1} = N \Rightarrow xyx^{-1}y^{-1}N = xNyNx^{-1}Ny^{-1}N$$

$$= xNyN(xN)^{-1}(yN)^{-1} = N \Rightarrow xyx^{-1}y^{-1}N = N \Rightarrow xyx^{-1}y^{-1} \in N$$

۸۵ـ فرض کنیم $|H| = m$ و $[G : N] = n$ و $h \in H$ چون

$(m, n) = ۱$ پس اعداد صحیحی چون x و y هستند بطوریکه $mx + ny = ۱$

$$h = h^{mx+ny} = h^{mx}\, h^{ny} = (h^m)^x h^{ny} = eh^{ny} = h^{ny} \qquad (۱)$$

از طرفی داریم: $h^{ny}N = (h^yN)^n = N \Rightarrow h^{ny} \in N$

از اینجا و رابطه (۱) داریم: $h = h^{ny} \in N \Rightarrow H \subseteq N$

۸۶ـ قرار می‌دهیم $X = \{۱ ، -۱\}$ می‌دانیم X یک زیرگروه اعداد حقیقی تحت عمل ضرب می‌باشد.

تعریف می‌کنیم $\varphi: H \to X$

$$\varphi(f) = \begin{cases} ۱ & \text{اگر } f \text{ یک جایگشت زوج در } H \text{ باشد} \\ -۱ & \text{اگر } f \text{ یک جایگشت فرد در } H \text{ باشد} \end{cases}$$

ابتدا نشان می‌دهیم که φ یک همریختی است برای این منظور حالتهای زیر را در نظر می‌گیریم.

الف) $f_۱$ و $f_۲$ دو جایگشت زوج باشند داریم: $\varphi(f_۱)\varphi(f_۲) = ۱ \cdot ۱ = ۱ = \varphi(f_۱f_۲)$

($f_۱ f_۲$ توجه زوج است)

ب) f_1 و f_2 هر دو جایگشت فرد باشند در اینصورت $f_1 f_2$ زوج بوده و خواهیم داشت

$$\varphi(f_1 f_2) = 1 = (-1)\cdot(-1) = \varphi(f_1)\,\varphi(f_2)$$

ج) f_1 یک جایگشت فرد و f_2 جایگشت زوج باشد در اینصورت $f_1 f_2$ فرد است و

$$\varphi(f_1 f_2) = -1 = (-1)\cdot 1 = \varphi(f_1)\,\varphi(f_2)$$

پس φ یک همریختی است.

همچنین φ پوشاست زیرا طبق فرض مسئله H دارای یک جایگشت فرد مانند α است لذا $\varphi(\alpha) = -1$ وچون H زیرگروه است لذا $\alpha^2 \in H$ و $\varphi(\alpha^2) = 1$.

واضح است که هسته φ برابر مجموعه جایگشتهای زوج می‌باشد و چون $\ker\varphi$ در H نرمال است پس یک قسمت مسئله ثابت شده است حال بنابه قضیه اساسی هوموورفیسم چون X یکریخت با $\frac{H}{\ker\varphi}$ می‌باشد پس $\left|\frac{H}{\ker\varphi}\right| = 2$ و لذا $\ker\varphi$ دارای اندیس ۲ در H می‌باشد.

۸۷- بنابه تمرین شصت و شش همین بخش می دانیم که اگر G یک گروه و $Z(G)$ مرکز آن باشد آنگاه $Z(G)$ زیرگروه نرمال G است.

پس اگر G یک گروه از مرتبهٔ p^2 باشد و $Z(G)$ مرکز آن باشد، بنابه یکی از کاربردهای قضایای سیلو می‌دانیم که $Z(G) \neq \{e\}$ پس چون طبق قضیه لاگرانژ مرتبه $Z(G)$ مرتبه G رامی‌شمارد، لذا مرتبه $Z(G)$، p یا p^2 می‌باشد اگر p^2 باشد در آنصورت $Z(G) = G$ و G آبلی و حکم ثابت است ولی اگر p^2 نباشد برابر p بوده و لذا مرتبه $\frac{G}{Z(G)}$ برابر p می‌باشد و مطابق تمرین پنجاه و چهار همین بخش $\frac{G}{Z(G)}$ دوری و باز بنابه تمرین شماره شصت و هفت همین بخش داریم G آبلی است و لذا تناقض است با اینکه مرتبه $Z(G)$ برابر p می‌باشد پس مرتبه $Z(G)$، p نمی‌تواند باشد و همان p^2 است و لذا G آبلی است.

۸۸ـ بنابه به تمرین هشتاد وهفت همین بخش، هرگروه از مرتبهٔ p^2 آبلی است و چون $p \mid p^2$ و p عدد اوّل است لذا بنابه قضیه کوشی یک زیرگروه از مرتبه p دارد ولی چون گروه آبلی است، هر زیرگروه آن نرمال بوده و لذا حکم ثابت است.

۸۹ـ اولاً نشان می‌دهیم که $Inn(G)$ زیرگروه $Aut(G)$ می‌باشد برای این منظور داریم:

$\forall f_a, f_b \in Inn(G)$

$f_a f_b(x) = f_a(b^{-1} x b) = a^{-1}b^{-1}xba = (ba)^{-1}xba = f_{ba}(x) \Rightarrow f_a f_b = f_{ab}$

پس $Inn(G)$ نسبت به عمل بسته است.

چون $I(x) = x = exe = f_e$ که درآن I تابع همانی است پس $I \in Inn(G)$

فرض کنیم f_a عضوی از $Inn(G)$ باشد ابتدا نشان می‌دهیم که $f_b^{-1} f_b = I$ برای این منظور چنین عمل می‌کنیم:

$f_b^{-1} f_b (x) = f_b^{-1}(bxb^{-1}) = (b^{-1}bxb^{-1}b) = x \Rightarrow f_b^{-1} f_b = I$

چون عضو وارون منحصر بفرداست لذا $(f_b)^{-1} = f_b^{-1}$ پس $(f_b)^{-1} \in Inn(G)$ لذا $Inn(G)$ زیرگروه $Aut(G)$ می‌باشد.

حال نشان می‌دهیم که $Inn(G)$ در $Aut(G)$ نرمال است فرض می‌کنیم φ عضوی از $Aut(G)$ باشد و f_a عضوی از $Inn(G)$ داریم:

$\varphi f_a \varphi^{-1}(x) = \varphi(a\varphi^{-1}(x)a^{-1}) = \varphi(a)x\ \varphi(a^{-1})$

$= \varphi(a)\, x\, (\varphi(a))^{-1} = f_{\varphi(a)}(x)$

بنابراین

$\varphi f_a \varphi^{-1} = f_{\varphi(a)}$ پس $\varphi f_a \varphi^{-1}$ عضوی از $Inn(G)$

بوده و لذا $Inn(G)$ در $Aut(G)$ نرمال است.

حال برای اثبات قسمت بعد مسئله داریم:

$g : G \longrightarrow Inn(G)$

$g(a) = f_a$

اوّلا g پوشاست زیرا اگر f_a عضوی از $Inn(G)$ باشد داریم $g(a) = f_a$

g همریختی است زیرا $g(ab) = f_{ab} = f_a f_b = g(a)\, g(b)$

حال بنابه قضیه اساسی هوموورفیسم داریم، $Inn(G)$ یکریخت با $\frac{G}{kerg}$ پس

چون $kerg \{ a \mid g(a) = f_a = I \} \Rightarrow f_a(x) = I(x)$

آنگاه: $a \in kerg \Leftrightarrow g(a) = I \Leftrightarrow f_a = I \Leftrightarrow f_a(x) = I(x)$

$\Leftrightarrow axa^{-1} = x \Leftrightarrow a \in Z(G)$

لذا $kerg = Z(G)$ و مسئله حل شده‌است.

۹۰ـ چون $G' = < \{ xgx^{-1}g^{-1} \mid x , g \in G \} >$ لذا به ازای هر x از N و هر g از G، $xgx^{-1}g^{-1}$ عضوی از G' می‌باشد، از طرفی N در G نرمال است لذا $gx^{-1}g^{-1}$ و در نتیجه $xgx^{-1}g^{-1}$ متعلّق به N می‌باشد لذا $xgx^{-1}g^{-1} \in N \cap G'$ بنابراین $xg = gx$ در نتیجه x پس $xgx^{-1}g^{-1} = e$ متعلّق به $Z(G)$ و بنابراین N زیر مجموعه $Z(G)$ می‌باشد.

۹۱ـ اگر G دوری باشد که حکم ثابت است، اگر G دوری نباشد پس هیچ عضوی از مرتبهٔ p^2 ندارد و لذا اگر a عضوی از G و مخالف عضوهمانی باشد در اینصورت طبق نتیجه‌ای از قضیه لاگرانژ $o(a) \mid |G|$ لذا $o(a) = p$ حال $H = <a>$ را در نظر می‌گیریم اگر عضو غیر همانی b از G را طوری در نظر بگیریم که b متعلّق به H نباشد آنگاه قرار می‌دهیم $K = <b>$، K زیرگروه دوری از مرتبهٔ p بوده و $H \cap K = \{e\}$ در نتیجه چون $|HK| = \frac{|H||K|}{|H \cap K|}$

ولذا خواهیم داشت $|HK| = p^2$ پس $G = HK$ وچون G آبلی است بنابراین H و K در G نرمال هستند پس بطور خلاصه G حاصلضرب داخلی H و K خواهد بود، طبق یکی از قضایا $G \cong H \times K$ ($\times$ حاصلضرب خارجی).

۹۲ ـ فرض کنیم x و y اعضایی از G باشند $(xy)T = (xy)^{-1} = y^{-1}x^{-1}$

$$(xy)T = (xT)(yT) = x^{-1}y^{-1}$$

از دو رابطه فوق داریم: $x^{-1}y^{-1} = y^{-1}x^{-1}$ در نتیجه $xx^{-1}y^{-1} = xy^{-1}x^{-1}$ بنابراین $y^{-1} = xy^{-1}x^{-1}$ بالاخره $e = yxy^{-1}x^{-1}$ در نهایت خواهیم داشت $xy = yx$ ولذا G آبلی است.

۹۳ ـ چون m و n متباین هستند، اعداد صحیح u و v وجود دارند بطوریکه $mu + nv = ۱$.

فرض کنیم x عضوی از G باشد در اینصورت

$$x = x^{mu + nv} = x^{mu}x^{nv} = x^{mu}$$

از تساوی فوق داریم $f(x^u) = x^{mu} = x$ پس f پوشاست.

فرض کنیم x عضوی از هسته f باشد پس داریم:

$$f(x) = x^m = e \Rightarrow x^{mu} = e \Rightarrow x^{mu} \cdot x^{nv} = e \Rightarrow x^{mu + nv} = e \Rightarrow x = e$$

پس $\ker f = \{e\}$ در نتیجه f یک به یک است.

$$\forall x, y \in G \qquad f(xy) = (xy)^m = x^m y^m = f(x) f(y)$$

پس f هموморفیسم است و نهایتاً از شرایط اثبات شده داریم f ایزومورفیسم است.

۹۴ ـ ابتدا راهنمایی مسئله را ثابت می‌کنیم.

ادّعا می‌کنیم $x^{-1}(xT) = y^{-1}yT \Leftrightarrow x = y$ برای اثبات این ادّعا داریم:

$$x^{-1}(xT) = y^{-1}(yT) \Rightarrow (yx^{-1})(xT)(y^{-1}T) = e$$

$$\Rightarrow (yx^{-1})(xy^{-1}T) = e \Rightarrow xy^{-1} = (xy^{-1})T \Rightarrow xy^{-1} = e \Rightarrow x = y$$

$\Rightarrow G = \{x^{-1}(xT) \mid x \in G\}$

حال برای حل مسئله داریم:

$g = [x^{-1}(xT)]T^{r} = [(x^{-1}T)(xT^{r})]T$

$= [(x^{-1}T)x]T = [x^{-1}(xT)]^{-1}T$

بنابراین به ازای هر g از G داریم: $g = g^{-1}T$

وبنابه تمرین شماره نودودو همین بخش G آبلی است.

۹۵ ـ اولاً برای اثبات خوش تعریفی فرض کنیم $x, y \in G$ پس $y = a^{k}$ و $x = a^{r}$ حال اگر داشته باشیم $x = y$ پس $a^{r} = a^{k}$ در نتیجه $a^{r-k} = e$ چون H و G هم مرتبه‌اند فرض کنیم مرتبه آنها n باشد دراینصورت $r - k \mid n$ پس $b^{r-k} = e$ در نتیجه $b^{r} = b^{k}$ ونهایتاً داریم $f(a^{r}) = f(a^{k})$ و f خوش تعریف است.

حال فرض کنیم $f(a^{r}) = f(a^{k})$.

$f(a^{r}) = f(a^{k}) \Rightarrow b^{r} = b^{k} \Rightarrow b^{r-k} = e \Rightarrow r - k \mid n \Rightarrow a^{r-k} = e$

$\Rightarrow a^{r} = a^{K}$

پس f یک به یک است.

فرض کنیم x عضوی از H باشد پس $x = b^{r}$ و در نتیجه $f(a^{r}) = b^{r}$ و لذا f پوشاست.

f هممورفیسم است زیرا:

$f(a^{r}a^{k}) = f(a^{r+k}) = b^{r+k} = b^{r}b^{k} = f(a^{r})f(a^{k})$

لذا f ایزومورفیسم است.

۹۶ ـ فرض کنیم G یک گروه دوری با مولد a باشد و $|G| = n$ چون $m \mid n$

پس عددی صحیح چون q هست که $n = mq$، $H = \langle a^{q} \rangle$ یک زیرگروه دوری G از مرتبه m می‌باشد، فرض کنیم K زیرگروه دلخواه G از مرتبه m باشد، اگر t

کوچکترین عدد صحیح مثبتی باشد که a^t متعلّق به K است در آنصورت $K = <a^t>$ و برای هر عدد صحیح s که a^s متعلّق به K باشد نتیجه می‌گیریم که $t \mid s$.

چون داریم $a^n = e \in k$ پس $t \mid n$ و $o(a^t) = \frac{n}{t}$ (بنابه تمرین ۲۵)

بنابراین چون $|K| = m$ و $|H| = \frac{n}{t}$ پس $o(a^t) = \frac{n}{t}$ لذا $m = \frac{n}{t}$ و $n = mt$

چون $n = mq$ پس $q = t$ لذا $K = <a^t> = <a^q> = H$ بنابراین H تنها زیرگروه G از مرتبه m می‌باشد.

۹۷ ـ فرض کنیم H زیرگروه T باشد بنابه قضیه لاگرانژ داریم $|H| \mid |T|$

(فرض کنیم $|H| = m$) بنابه تمرین قبل T دقیقاً دارای یک زیرگروه از مرتبه m می‌باشد ولی چون $|xHx^{-1}| = H$ پس $xHx^{-1} = H$ و لذا H در G نرمال است.

۹۸ ـ اولاً f هموморفیسم است زیرا $f(z_1z_2) = \overline{z_1.z_2} = \overline{z}_1.\overline{z}_2 = f(z_1)\, f(z_2)$

ثانیاً f پوشاست زیرا $\forall z \in C \quad f(\overline{z}) = \overline{\overline{z}} = z$

ثالثاً f یک‌به‌یک است زیرا $f(z_1) = f(z_2) \Rightarrow \overline{z}_1 = \overline{z}_2 \Rightarrow \overline{\overline{z}}_1 = \overline{\overline{z}}_2$

$\Rightarrow z_1 = z_2$ پس f اتومورفیسم است.

۹۹ ـ $\forall x \in G \quad x\varphi_h = x\varphi_g \Rightarrow h^{-1}xh = g^{-1}xg$

$\Rightarrow gh^{-1}xhg^{-1} = x \Rightarrow gh^{-1}x = x(hg^{-1})^{-1} = xgh^{-1}$

بنابراین به ازای هر x از G داریم: $gh^{-1}x = xgh^{-1}$ پس gh^{-1} عضوی از $Z(G)$ بوده و مطلب تمام است.

۱۰۰ ـ ابتدا فرض کنیم φ یک همریختی یک به یک باشد پس داریم $\ker\varphi = \{e\}$ حال اگر $o(x) = n$ نشان می‌دهیم که $o(x\varphi) = n$ برای این کار چنین عمل می‌کنیم $(x\varphi)^n = x^n\varphi = e\varphi = e'$

حال فرض کنیم $(x\varphi)^s = e'$ در نتیجه $x^s\varphi = e'$ بنابراین چون $\ker\varphi = \{e\}$

خواهیم داشت $x^s = e$ و چون $o(x) = n$ پس $n|s$ لذا $o(x\varphi) = n$ (توجه، e عضوهمانی G و e' عضوهمانی H می‌باشد)

به عکس فرض کنیم $o(x) = o(x\varphi)$ نشان می‌دهیم که φ یک به یک است.

اگر $x\varphi = e'$ آنگاه $o(x\varphi) = o(e')$ پس $o(x\varphi) = 1$ ولی چون $o(x) = o(x\varphi)$ پس $o(x) = 1$ لذا $x = e$ بنابراین $\ker\varphi = \{e\}$ و φ یک به یک است.

۱۰۱ ـ فرض کنیم $K = \langle a\rangle$ چون K زیرگروه H است پس $H = \langle a^k\rangle$ لذا $h\varphi \in H$ و $h\varphi = (a^k)^m\varphi = a^{mk}\varphi \in K\varphi \subseteq K$

بنابراین $H\varphi \subseteq K$ حال کافی است ثابت کنیم که $a^k\varphi \in H$

$$a^k\varphi = (a\varphi)^k = (a^m)^k = a^{mk} = (a^k)^m \in H$$

چون مولد $H\varphi$ متعلّق به H است پس $H\varphi \subseteq H$ و مطلب تمام است.

۱۰۲ ـ فرض کنیم $a \in H$ ابتدا نشان می‌دهیم $aH \subseteq H$

$ah \in aH \Rightarrow ah = h' \in H$ (چون a و h هر دو متعلّق به H هستند)

$\Rightarrow aH \subseteq H$

حال نشان می‌دهیم: $H \subseteq aH$

$$h \in H \wedge a^{-1} \in H \Rightarrow a^{-1}h \in H \Rightarrow a(a^{-1}h) \in aH \Rightarrow h \in aH$$

پس $H \subseteq aH$ بنابراین $H = aH$

به عکس فرض کنیم $aH = H$ پس چون e متعلّق به H است لذا $a = ae \in H$ پس $a \in H$.

۱۰۳ ـ این مسئله را به دو روش حل می‌کنیم.

روش اوّل، چون $q||G|$ و $p||G|$ بنابه قضیه کوشی G زیرگروههایی و همچنین عناصری از مرتبه p و q دارد پس فرض کنیم a و b اعضایی از G بترتیب

از مراتب p و q باشند در اینصورت $H = < a >$ و $K = < b >$ زیرگروههایی از مراتب p و q هستند که $(p , q) = ۱$ لذا بنابه تمرین شماره چهل‌ونه همین بخش $o (ab) = pq$ در نتیجه $G = <ab>$

روش دوّم: H و K روش قبل را در نظر می‌گیریم، $H \cup K$ دارای $p + q - ۱$ عضو می‌باشد، چون $pq > p + q - ۱$ فرض کنیم m عضوی باشد که در G هست ولی در $H \cup K$ نیست پس مطابق قضیه لاگرانژ مرتبه m برابر p یا q یا pq است، حال مرتبه m مخالف p است زیرا در غیر اینصورت $H = <m>$ و همچنین مرتبه m مخالف q است زیرا در غیر اینصورت $K = <m>$ پس مرتبه m برابر pq است و $G = <m>$

۱۰۴ ـ فرض کنیم a عضوی از G وغیرهمانی باشد آنگاه $H = <a>$ یک زیرگروه G است و چون $H \neq \{e\}$ و G زیرگروه نابدیهی ندارد لذا $G = H$ پس G دوری است.

حال اگر مرتبه G متناهی نباشد پس مرتبه a متناهی نیست لذا داریم $K = <a^۲>$ حال اگر $K = \{ e \}$ آنگاه مرتبه a متناهی بوده و تناقض است پس $K \neq \{ e \}$ و $K = G$ و لذا $a=(a^۲)^m = a^{۲m}$ لذا $a^{۲m-۱}=e$ پس مرتبه a متناهی است.

حال فرض کنیم $o(a)= n$ و n عدد اوّل نباشد پس $n= n_۱n_۲$ که $n_۲<n$ و $۱<n_۱$ بنابه تمرین شماره نودوشش همین بخش G زیرگروهی چون H از مرتبه $n_۱$ دارد و $۱ < n_۱ < n$ پس H زیرگروه غیر بدیهی G است و متناقض با فرض اوّلیه است پس n عدد اوّل است.

۱۰۵ ـ توجّه شود که عکس مطلبی که بیان می‌کنیم نیز درست می‌باشد و لذا مطلب را بصورت شرط لازم و کافی بیان می‌کنیم یعنی:

$aH = bH$ اگر وفقط اگر $\pm \det (a) = \det (b)$

برای اثبات نخست فرض می‌کنیم $aH = bH$ پس داریم ab^{-1} متعلّق به H یعنی

$\det(ab^{-1}) = \pm 1$ و چون $\det(ab^{-1}) = \det(a)\det(b^{-1})$ پس

$\det(a) = \pm \det(b)$ حال $\frac{\det(a)}{\det(b)}$ برابر ۱ یا ۱- می‌باشد و لذا

فرض کنیم $\det(a) = \pm \det(b)$ داریم $\frac{\det(a)}{\det(b)} = \pm 1$ پس

$\det(ab^{-1}) = \det(a)\det(b^{-1}) = \pm 1$ لذا ab^{-1} متعلّق به H بوده و

$aH = bH$

۱۰۶ - اوّلاً ثابت می‌کنیم $SL(۲, \mathbf{R})$ زیر گروه $GL(۲, \mathbf{R})$ می‌باشد

فرض کنیم A و B اعضایی از $SL(۲, \mathbf{R})$ باشند پس $\det(A) = ۱$ و

$\det(B) = ۱$ و چون $\det(AB) = \det(A)\det(B) = ۱$ پس AB عضوی از

$SL(۲, \mathbf{R})$ بوده ولذا نسبت به عمل بسته است.

چون دترمنیان ماتریس همانی برابر یک است لذا ماتریس همانی عضو $SL(۲, \mathbf{R})$

است.

فرض کنیم A عضوی از $SL(۲, \mathbf{R})$ باشد چون $\det(A)\det(A^{-1}) = \det(I)$

پس $\det(A^{-1}) = \frac{۱}{\det(A)}$ پس $\det(A^{-1}) = ۱$ ولذا A^{-1} متعلّق به $SL(۲, \mathbf{R})$

است پس $SL(۲, \mathbf{R})$ زیرگروه است.

حال برای اثبات نرمال بودن فرض کنیم $A \in SL(۲, \mathbf{R})$ و $M \in GL(۲, \mathbf{R})$

داریم:

$$\det(M^{-1}AM) = \det(M^{-1})\det(A)\det(M)$$

$$= \frac{۱}{\det M} \times \det(A) \times \det(M) = \det(A) = ۱$$

پس $M^{-1}AM$ عضوی از $SL(۲, \mathbf{R})$ بوده ولذا $SL(۲, \mathbf{R}) = M^{-1}SL(۲, \mathbf{R})M$

پس $SL(۲, \mathbf{R})$ نرمال می‌باشد.

۱۰۷ - فرض کنید $G = \langle a \rangle$ یک گروه دوری باشد و H یک زیرگروه

نرمال G باشد حال نشان می‌دهیم که $\frac{G}{H} = <aH>$. فرض کنیم $bH \in \frac{G}{H}$ چون $b \in G$ پس وجود دارد عدد صحیحی چون m بطوریکه $b = a^m$ ولذا

$$bH = a^mH = (aH)^m$$

پس هر عضو دلخواه $\frac{G}{H}$ مانند bH توانی از aH است بنابراین $G = <aH>$

۱۰۸ ـ نشان دهیم که اگر G یک گروه آبلی باشد و H زیر گروه نرمال آن آنگاه $\frac{G}{H}$ آبلی است.

فرض کنیم aH و bH اعضایی از $\frac{G}{H}$ باشند داریم:

$$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$$

پس $\frac{G}{H}$ آبلی است.

۱۰۹ ـ فرض کنیم مرتبه g برابر n و مرتبه gH برابر m باشد.

$$(gH)^n = g^nH = eH = H \Rightarrow (gH)^n = H$$

چون $o(gH) = m$ لذا $m \mid n$.

۱۱۰ ـ فرکنیم $\frac{H}{N}$ زیرگروه نرمال $\frac{G}{N}$ باشد پس داریم:

$$\forall gN \in \frac{G}{N} \wedge hN \in \frac{H}{N} \qquad \forall g \in G, \forall h \in H$$

$$(gN)^{-1}hN(gN) \in \frac{H}{N} \Rightarrow (g^{-1}hg)N \in \frac{H}{N} \Rightarrow g^{-1}hg \in H$$

بنابراین $g^{-1}Hg \subseteq H$ پس H در G نرمال است.

حال فرض کنیم H در G نرمال باشد پس

$$\forall gN \in \frac{G}{N}, \forall hN \in \frac{H}{N}:$$

$$(gN)^{-1}hN(gN) = (g^{-1}hg)N$$

چون H در G نرمال است لذا $(g^{-1}hg) \in H$ و $(g^{-1}hg)N \in \frac{H}{N}$ بوده پس

در $\frac{G}{N}$ نرمال می‌باشد.

۱۱۱ ـ قبلاً در یکی از تمرینات نشان دادیم که اشتراک دو زیر گروه، زیرگروه می‌باشد حال نشان می‌دهیم اگر H و N دو زیرگروه نرمال G باشند آنگاه $H \cap N$ در G نرمال است.

$\forall g \in G\ ,\ \forall k \in H \cap N : g^{-1}kg \in H$ (چون H در G نرمال است)

$g^{-1}kg \in N$ (چون N در G نرمال است)

بنابراین $g^{-1}kg \in H \cap N$ لذا $H \cap N$ زیرگروه نرمال G است.

۱۱۲ ـ چون N زیرگروه نرمال G است لذا به ازای هر m از M و هر n از N، عضو mnm^{-1} متعلّق به N می‌باشد در نتیجه $mnm^{-1}n^{-1}$ متعلّق به N است.

چون M زیرگروه نرمال G است پس به ازای هر m از M وهر n از N عضو $nm^{-1}n^{-1}$ عضوی است از M و لذا $mnm^{-1}n^{-1}$ متعلّق به M است پس نهایتاً داریم:

$$mnm^{-1}n^{-1} \in M \cap N = \{e\}$$

لذا: $mnm^{-1}n^{-1} = e \Rightarrow mnm^{-1} = n \Rightarrow mnm^{-1}m = nm \Rightarrow mn = nm$

۱۱۳ ـ فرض کنیم مرتبه x برابر m ومرتبه $\frac{G}{H}$ برابر n باشد چون $(m,n) = ۱$

پس اعداد صحیحی چون s و y وجود دارند بطوریکه $ms + ny = ۱$ بنابراین

$$x = x^{ms+ny} = (x^m)^s x^{ny} = ex^{ny} = x^{ny}$$

پس $xH = x^{ny}H$ ولی $x^{ny}H = (x^yH)^n$ و چون n مرتبه $\frac{G}{H}$ می‌باشد و $x^yH \in \frac{G}{H}$ پس

$x^{ny}H = (x^yH)^n = H$ و لذا $xH = x^{ny}H = H$ بطورخلاصه $xH = H$ و در نتیجه $x \in H$ و مطلب تمام است.

۱۱۴ ـ فرض کنیم مرتبه عضو gH از $\frac{G}{H}$ برابر n باشد بنابه تمرین شماره صدوهشت همین بخش داریم، $o(g) = n.t$ لذا $n \mid o(g)$ و مطابق تمرین شماره

بیست وپنیج همین بخش می‌دانیم

$$o(g^t) = \frac{o(g)}{(t, o(g))} = \frac{o(g)}{t} = o(gH) = n$$

بنابراین g^t عضوی از G و دارای مرتبه n می‌باشد.

۱۱۵ ـ فرض کنیم $|H| = m$ و $|K| = n$ باشد، اوّلاً نشان می‌دهیم $H \cap K = \{e\}$ اگر x عضوی از $H \cap K$ باشد در اینصورت طبق نتیجه‌ای از قضیه لاگرانژ مرتبه x ، m و n را می‌شمارد ولی چون m و n نسبت به هم اوّلند پس مرتبه x برابر یك می‌باشد ولذا $x = e$ پس $H \cap K = \{e\}$.

حال بنابه مسئله شماره صدودوازده همین بخش به ازای هر h از H و هر t از K $ht = th$ می‌باشد و حکم ثابت شده است.

۱۱۶ ـ فرض کنیم H زیر مجموعه‌ای از G متشکّل از عضوهمانی همراه با تمام اعضای از مرتبه سه باشد و x و y اعضایی از H و غیرهمانی باشند.

$$(xy)^3 = x^3y^3 = ee = e$$

حال فرض کنیم $e = (xy)^s$ و s مرتبه xy باشد و چون $(xy)^3 = e$ پس $s \mid 3$ لذا s که در هر حالت xy عضوی از H است ولذا H نسبت به عمل بسته است چون طبق فرض داریم $e \in H$ وهمچنین $o(x) = o(x^{-1})$ پس اگر $x \in H$ آنگاه $x^{-1} \in H$ لذا H زیرگروه G است.

برای قسمت بعد چون اگر $x \in H$ و از مرتبه ۴ باشد $o(x^2) = \frac{4}{(2 \text{ و } 4)} = 2$ پس $x^2 \notin H$ و لذا H بسته نیست و H زیرگروه نیست.

بطورکلّی برای n هایی که n عدد اوّل باشد H زیرگروه خواهد بود.

۱۱۷ ـ فرض کنیم H یک زیرگروه از مرتبه مفروض n باشد چون می‌دانیم مرتبه H با مرتبه $x^{-1}Hx$ به ازای هر x از G برابر است لذا با توجّه به فرض مسئله بایستی $x^{-1}Hx = H$ باشد ولذا H در G نرمال است.

۱۱۸ ـ تابع $\varphi : \mathbf{Z} \to \mathbf{Z}_m$ را با ضابطه $x\varphi = \bar{x}$ که در آن $\bar{x}$ باقیمانده تقسیم x بر m می‌باشد را در نظر می‌گیریم

$$\forall x, y \in \mathbf{Z}: (xy)\varphi = \overline{xy} = \bar{x}\,\bar{y} = (x\varphi)(y\varphi)$$

پس φ همریختی است.

واضح است که φ پوشاست لذا طبق قضیه اساسی هوموموفیسم $\mathbf{Z}_m$ با $\frac{\mathbf{Z}}{\ker\varphi}$ یکریخت است ولی

$$\operatorname{Ker}\varphi = \{x \in \mathbf{Z} \mid x\varphi = o\} = \{x \in \mathbf{z} \mid x = mt \text{ ، } t \in \mathbf{Z}\} = m\mathbf{Z}$$

لذا $\mathbf{Z}_m$ با $\frac{\mathbf{Z}}{m\mathbf{Z}}$ یکریخت است.

۱۱۹ ـ اگر مرتبه $\frac{G}{Z(G)}$ بزرگتر یا مساوی چهار نباشد پس مرتبه آن یک یا دو یا سه می‌باشد اگر یک باشد در آنصورت $|Z(G)|$ برابر مرتبه G بوده ولذا $G = Z(G)$ پس G آبلی است وتناقض است. اگر ۲ = $\left|\frac{G}{Z(G)}\right|$ یا ۳ = $\left|\frac{G}{Z(G)}\right|$ باشد بنابه تمرین شماره شصت وهفت همین بخش $\frac{G}{Z(G)}$ دوری و بنابه تمرین شماره شصت وهفت همین بخش G آبلی است و خلاف فرض است پس فرض خلف باطل و حکم ثابت است.

۱۲۰ ـ فرض کنیم x عضوی از $Z(G)$ باشد پس xT عضوی از $[Z(G)]T$ است.

حال فرض کنیم g عضوی از G باشد چون T پوشاست پس عضوی مانند h از G وجود دارد بطوریکه $g = hT$ لذا

$$(xT)g = (xT)(hT) = (xh)T = (hx)T = (hT)(xT) = g(xT)$$

$$\Rightarrow xT \in Z(G) \Rightarrow [Z(G)]\,T \subseteq Z(G)$$

۱۲۱ ـ فرض کنیم G آبلی باشد پس $Z(G) = G$ و از تمرین شماره

هشتاد ونه همین بخش داریم $\frac{G}{Z(G)}$ یکریخت با $Inn(G)$، پس مرتبه $Inn(G)$ برابر یک است به عکس فرض کنیم $|Inn(G)| = 1$ پس $|\frac{G}{Z(G)}| = 1$ لذا $G = Z(G)$ و G آبلی است.

۱۲۲ ـ فرض کنیم گروه $Aut(G)$ دوری باشد پس $Inn(G)$ که زیرگروه آن است نیز دوری بوده و بنابه تمرین شماره هشتادو نه همین بخش چون $Inn(G)$ با $\frac{G}{Z(G)}$ یکریخت است پس $\frac{G}{Z(G)}$ دوری است و از تمرین شصت و هفت همین بخش نتیجه می‌شود که G آبلی است و این خلاف فرض است پس فرض خلف باطل و $Aut(G)$ دوری نیست.

۱۲۳ ـ ادعا می‌کنیم که کوچکترین مضرب مشترک m و n یک مولد برای $< m > \cap < n >$ می‌باشد برای اثبات اوّل فرض کنیم کوچکترین مضرب مشترک m و n برابر k باشد، حال فرض کنیم x متعلّق به $< m > \cap < n >$ لذا چون $x \in < n >$ و $x \in < m >$ پس $n \mid x$ و $m \mid x$ پس $k \mid x$ در نتیجه $x \in < k >$ لذا $< m > \cap < n > \subseteq < k >$ (۲)

حال فرض کنیم x عضوی از $< k >$ باشد پس $k \mid x$ در نتیجه $m \mid x$ و $n \mid x$ پس x متعلّق به $< m >$ و همچنین متعلّق به $< n >$ بوده لذا x متعلّق به $< m > \cap < n >$ می‌باشد پس $< k > \subseteq < m > \cap < n >$ و نهایتاً ازاینجا و رابطه (۲) داریم $< k > = < m > \cap < n >$.

۱۲۴ ـ فرض کنیم e عضو همانی G و e' عضو همانی H باشد.

حال فرض کنیم φ یک به یک باشد چون داریم $\forall x \in \ker\varphi : x\varphi = e'$ و $e' = e\varphi$ پس $x\varphi = e\varphi$ ولذا $x = e$ بنابراین $\ker\varphi = \{e\}$

به عکس فرض کنیم $\ker\varphi = \{e\}$ و داشته باشیم $x\varphi = y\varphi$ و لذا $(x\varphi)(y\varphi)^{-1} = e'$ درنتیجه $(x\varphi)(y^{-1}\varphi) = e'$ پس $(xy^{-1})\varphi = e'$ لذا

xy^{-1} متعلّق به $\ker\varphi$ و برابر e است پس $xy^{-1} = e$ در نتیجه $x = y$

۱۲۵ ـ چون G غیر آبلی است پس بایستی حداقل یکی از H و K غیر آبلی باشد لذا چون کوچکترین گروه غیر آبلی از مرتبه شش می‌باشد پس بایستی حداقل یکی از H و K مرتبه‌ای بیشتر یا مساوی شش داشته باشد و چون آن دیگری غیر بدیهی است پس حداقل مرتبه دیگری نیز دو می‌باشد پس حداقل مرتبه $H \times K$ ، دوازده بوده و لذا $|G| \geq 12$

۱۲۶ ـ اولاً نشان می‌دهیم که هسته هر همریختی زیرگروه نرمال می‌باشد

فرض کنیم $f : G \to H$ یک همریختی گروهی باشد و $K = \ker f$

اگر x و y اعضایی از K باشند آنگاه $(xy)f = (xf)(yf) = e'$ (e' عضو همانی H و e عضو همانی G است) پس K نسبت به عمل بسته است. چون $e\varphi = e'$ پس e متعلّق به K است.

اگر x عضوی از K باشد آنگاه $x^{-1}f = (xf)^{-1} = (e')^{-1} = e'$ پس x^{-1} عضوی از K است و لذا K زیرگروه G است، حال نشان می‌دهیم که در G نرمال است.

$$\forall g \in G \ \wedge\ x \in K : (g^{-1}xg)f = (g^{-1})f\,(x)f\,(g)f$$

$$(gf)^{-1}\,(xf)\,(gf) = (gf)^{-1}\,e'\,(gf) = e'$$

پس $g^{-1}xg$ متعلّق به K است پس $g^{-1}Kg = K$ پس K در G نرمال است.

به عکس فرض کنیم K در G نرمال باشد، گروه خارج قسمت $\frac{G}{K}$ را تشکیل می‌دهیم

γ از G به $\frac{G}{K}$ را با ضابطه $\forall x \in G \quad \gamma(x) = xK$ تعریف می‌کنیم

یک همریختی طبیعی (متعارف) است زیرا

$$(xy)\gamma = (xy)K = (xK)(yK) = (x\gamma)(y\gamma)$$

حال چون $\ker\gamma = \{x \in G \mid x\gamma = xK = K\} = K$ پس مطلب تمام است.

۱۲۷ ـ چون $[G : N] = ۲$ پس N دارای دو همدسته در G است که یکی از آنها خود N است وچون x و y متعلّق به N نیستند پس $xN \neq N$ و $yN \neq N$ لذا چون N دارای دو همدسته است پس $xN = yN$ از طرفی چون $y \notin N$ پس $y^{-۱} \notin N$ و در نتیجه $xN = y^{-۱}N$ پس $xy \in N$ و حکم ثابت است.

۱۲۸ ـ فرض کنیم f اتومورفیسم باشد و $x \in G$ چون f پوشاست لذا وجود دارد y متعلّق به G بطوریکه $x = f(y)$

می‌دانیم که $G = < a >$ لذا kای متعلّق به $\mathbf{Z}$ هست بطوریکه $y = a^k$ بنابراین

$$x = f (a^k) = [f(a)]^k$$

در نتیجه $G = < f (a) >$

به عکس فرض کنیم $G = < f (a) >$ و x متعلّق به G پس t متعلّق به اعداد صحیح موجود است بطوریکه $x = [f (a)]^t$ در نتیجه $x = f (a^t)$ که a^t متعلّق به $G = < a >$ بوده و لذا f پوشاست.

حال اگر G متناهی باشد از مبانی ریاضیات می‌دانیم که هر تابع پوشا از یک مجموعه متناهی به آن مجموعه یک به یک نیز می‌باشد لذا طبق این مطلب f یک به یک بوده پس یک اتومورفیسم از G است.

اگر G نامتناهی باشد فرض کنیم $f(x) = f(y)$ که x و y اعضایی از G هستند پس r و sای از اعداد صحیح موجودند بطوریکه $x = a^r$ و $y = a^s$ پس $f(a^r) = f(a^s)$ یعنی $[f(a)]^r = [f(a)]^s$ پس $[f(a)]^{r-s} = e$ چون G نامتناهی است پس $r - s = ۰$ یا $r = s$ ولذا $x = y$، f یک به یک و مطلب ثابت شده است.

۱۲۹ ـ گروه تابعهای یک به یک و پوشا از $\mathbf{R}$ به $\mathbf{R}$ و عناصر a و b رااز این گروه به صورت $a (x) = -x$ و $b (x) = ۱ - x$ را در نظر می‌گیریم

$a^2 = -(-x) = x \Rightarrow a^2 = I \Rightarrow o(a) = 2$

$b^2(x) = 1 - (1 - x) = x \Rightarrow b^2 = I \Rightarrow o(b) = 2$

$o(ab)$ نامتناهی است چون،

$ab(x) = -1 + x \qquad (ab)^n(x) = -n + x \neq x \qquad \forall n \geq 1$

۱۳۰ ـ اولاً ادعا می‌کنیم که اگر x متعلّق به H نباشد آنگاه

$\forall 1 \leq i \leq p \quad x^i \notin H$ زیرا اگر چنین نباشد و x^iای متعلّق به H باشد کوچکترین این iها را در نظر می‌گیریم و آنرا j می‌نامیم فرض کنیم $o(x) = m$ می‌دانیم که m ، j را عاد نمی‌کند (زیرا $1 < j < p$ و $m \mid n = o(G)$ و p کوچکترین عدد اوّلی است که $p \mid n$)

پس طبق الگوریتم تقسیم $m = jq + r \quad r < j$ ولذا:

$x^m = (x^j)^q \; (x^r) = e \in H \Rightarrow x^r \in H$

و این تناقض است پس $\forall 1 \leq i \leq p \quad x^i \notin H$

حال فرض کنیم H در G نرمال نباشد پس وجود دارد hای در H و xای در G بطوریکه $x^{-1}hx \notin H$ لذا $x \notin H$

پس طبق نتیجه فوق $1 < i < p \quad x^i \notin H$ پس $\forall i, j \mid 1 \leq i < j \leq p - 1$ و داریم: $x^i H \neq x^j H$ (زیرا در غیر اینصورت $x^{i-j} \notin H$ و تناقض است)

لذا همرده‌های متمایز H عبارتنداز $\{ H, Hx, \ldots, Hx^{p-1} \}$

حال چون $y = x^{-1} hx \notin H$ لذا $\{ H, Hy, \ldots, Hy^{p-1} \}$

همرده‌های متمایز H در G هستند، لذا این دو مجموعه مساویند بنابراین وجود دارد $0 \leq r \leq p - 1$ بطوریکه $Hx = Hy^r$ بنابراین $x = h' y^r$ بطوریکه h' عضوی از H است.

$x = h' x^{-1} h^r x \Rightarrow h' x^{-1} = h^{-r} \Rightarrow h^r h' = x \Rightarrow x \in H$

این تناقض است پس فرض خلف باطل و H زیرگروه نرمال G است.

۱۳۱ ـ واضح است که $N[P] \subseteq N[N(P)]$ حال نشان می‌دهیم $N[N(P)] \subseteq N[P]$

$$g \in N[N(P)] \Rightarrow g^{-1} N(P) g = N(P)$$

P زیرگروه $N(P)$ است پس $g^{-1}Pg$ زیرگروه $N(P)g = g^{-1} N(P)$ (۱) چون P یک p زیرگروه سیلو است و $g^{-1}Pg$ نیز یک p زیرگروه سیلو است.

چون رابطه (۱) را داریم پس $g^{-1}Pg$ یک p زیرگروه سیلو $N(P)$ است ولی P زیرگروه نرمال $N(P)$ است پس $P = g^{-1}Pg$ یعنی $g \in N(P)$ پس $N[N(P)] \subseteq N[P]$

۱۳۲ ـ چون $[N(H) : H]$ | p و $[N(H) : H]$ غیر صفر است پس $p = [N(H) : H]$ لذا مرتبه G با مرتبه $N(H)$ برابر است لذا چون $N(H) \subseteq G$ پس $N(H) = G$ بنابراین H در G نرمال است.

۱۳۳ ـ بدیهی است که $N(P).K \subseteq G$ حال نشان می‌دهیم $G \subseteq N(P).K$

فرض کنیم g عضوی از G باشد چون P زیرگروه K است لذا $g^{-1}Pg$ زیرگروه $g^{-1}Kg$ است امّا K در G نرمال است لذا $K = g^{-1}Kg$ بنابراین $g^{-1}Pg \subseteq K$ امّا چون $|g^{-1}Pg| = |P| : \forall g \in G$ پس $g^{-1}Pg$ یک p زیرگروه سیلو K است.

بنابه قضیه دوّم سیلو tای از K وجود دارد بطوریکه $g^{-1}Pg = t^{-1}Pt$ بنابراین

$$tg^{-1}Pgt^{-1} = P \Rightarrow (gt^{-1})^{-1} Pgt^{-1} = P \Rightarrow gt^{-1} \in N(P)$$

پس g متعلّق به $N(P)K$ و لذا حکم ثابت است.

۱۳۴ ـ الف) چون P زیرگروه نرمال $N(P)$ است در نتیجه P تنها p زیرگروه سیلو G است، چون P، p زیرگروه سیلو G است بنابراین p زیرگروه

سیلو $N(P)$ است.

ب) چون $N(P)$ زیرگروه H می‌باشد پس P زیرگروه H است.

پس p زیرگروه سیلو G، p زیرگروه سیلو H نیز می‌باشد.

حال چون شرایط مسئله قبل برقراراست لذا $N[H] = N[P].H = H$

۱۳۵ ـ فرض کنیم $p^k \mid\mid G$ و P^{k+1} مرتبه G را عاد نکند.

چون $[G : H] = 1$ و P) و داریم: $|H| . \left|\frac{G}{H}\right| \mid\mid P^k$ لذا $p^k \mid\mid |H|$

(زیرا $[G : H] = 1$ و p^k)

پس H بزرگترین توان p را داراست پس H یک p زیرگروه سیلو چون P از G را داراست یعنی P زیرگروه H است.

حال فرض کنیم Q یک p زیرگروه سیلو G باشد نشان می‌دهیم Q زیرگروه H است.

چون P و Q، p زیرگروههای سیلو G هستند پس وجود دارد gای در G بطوریکه $g^{-1}Pg = Q$

$$P \leq H \Rightarrow g^{-1}Pg \leq g^{-1}Hg$$

چون H زیرگروه نرمال G است پس $g^{-1}Pg \leq H$

بنابراین $Q \leq H$ ($\leq$ زیرگروه بودن)

پس H شامل تمام p زیرگروههای سیلو G است.

۱۳۶ ـ فرض کنیم G یک pگروه متناهی باشد لذا nای وجود دارد بطوریکه $|G| = p^n$ بنابه قضیه اوّل سیلو G زیرگروه نرمال از مرتبه p^{n-1} مانند N دارد پس $|\frac{G}{N}| = p$ بنابراین N و $\frac{G}{N}$ هر دو Pگروه هستند.

به عکس فرض کنیم N و $\frac{G}{N}$ هر دو P گروه باشند پس

$\forall\ g \in G\ \ (gN)^{pk} = N \Rightarrow\ g^{pk}N = N \Rightarrow\ g^{pk} \in N$

بنابراین $g^{pk} \in N$ و N یک p گروه است لذا $(g^{pk})^{pt} = e$ پس $g^{pk+t} = e$ به ازای هر g از G بنابراین G یک p گروه است.

۱۳۷ ـ فرض کنیم $|G| = p^n$ و H تنها زیرگروه G ازمرتبه p^{n-1} باشد چون تنها زیرگروه p^{n-1} عضوی است لذا H در G نرمال است و چون مرتبه $\frac{G}{H}$ برابر p است و هر گروه از مرتبه عدد اوّل دوری است پس $\frac{G}{H}$ دوری است لذا وجود دارد gای در G بقسمی که $\frac{G}{H} = <gH>$ حال ادعا می‌کنیم $G = <g>$.

اگر مرتبه g، p^n باشد که حکم ثابت است، اگر p^n نباشد قرار می‌دهیم $K = <g>$ چون $o(g) | p^n$ پس $o(g) = p^t$ اگر $t = n - 1$ آنگاه $H = K$ پس $g \in H$ وتناقض است اگر $t < n - 1$ آنگاه $K \leq H$ بنابراین $g \in H$ و تناقض است پس مرتبه g همان p^n بوده و حکم ثابت است.

۱۳۸ ـ فرض کنیم G گروه آبلی باشد و $G = H_1 \triangleright H_2 \triangleright \dots \triangleright H_s \triangleright H_{s+1} = \{e\}$ یک سری ترکیب G باشد در این صورت $\frac{H_i}{H_{i+1}}$ها گروههای آبلی و ساده هستند در نتیجه هر یک ازگروههای $\frac{H_i}{H_{i+1}}$ یک گروه دوری و با پایان است و از مرتبه اوّل (زیرا اگر G یک گروه آبلی و ساده باشد آنگاه تنها زیرگروههای G همان $\{e\}$ و خود G هستند چون هر زیرگروه یک گروه آبلی نرمال است پس G دوری و از مرتبه اوّل است) پس $\frac{H_1}{H_2}$ نیز از مرتبه اوّل است در نتیجه $G = H_1$ یک گروه با پایان است.

به طورکلّی اگرگروه G دارای یک سری ترکیب باشد که گروههای خارج قسمتی آن گروههای متناهی باشند آنگاه G متناهی است.

به عکس فرض کنیم G یک گروه متناهی باشد، اگر تنها زیرگروههای G فقط زیرگروههای بدیهی باشند آنگاه $G \triangleright \{e\}$ یک سری ترکیب برای G می‌باشد. فرض کنیم G دارای زیرگروهی مانند H_1 و غیربدیهی باشد پس $G \triangleright H^{-1} \triangleright \{e\}$

حال اگر بین G و H_1 زیرگروه دیگری از G مانند H^2 باشد در اینصورت $\{e\} \subseteq H_1 \subseteq H \lhd G$ به همین ترتیب می‌توان ادامه داد، چون G متناهی است پس زیرگروهی مانند H_{n-1} هست که در G نرمال ماکسیمال است پس

$$\{e\} \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_{n-2} \lhd G$$

که $\frac{G}{H_{n-1}}$ ساده است. حال به همین روش بین H_{n-1} و H_{n-2} می‌توان آنقدر زیرگروه اضافه کرد تا خارج قسمت H_{n-1} و آن زیرگروه نرمال ماکسیمال ساده شود وچون G متناهی است این روش منجر به بدست آمدن یک سری ترکیب می‌شود (البته از این قضیه که $H \lhd G$ در اینصورت $\frac{G}{H}$ ساده است اگر وفقط اگر H زیرگروه نرمال ماکسیمال G باشد)

۱۳۹ ـ تعداد p زیرگروههای سیلو G بنابه قضیه سوّم سیلو برابر $kp + 1$ می‌باشد که $| G | \mid kp + 1$ و $k = 0, 1, \ldots$ با توجه به اینکه $q < p$ پس تعداد p زیرگروههای سیلو G یکی است.

با توجه به اینکه q ، $p^2 - 1$ رانمی‌شمارد لذا تعداد q زیرگروههای سیلو G برابر یکی است. ولذا اگر H تنها p زیرگروه سیلو G و K تنها q زیرگروه سیلو G باشند آنگاه H و K در G نرمال خواهند بود پس H یک زیرگروه نرمال G از مرتبه p^2 است ولذا بنا به یکی از تمرینات همین بخش آبلی است و K یک زیرگروه نرمال G از مرتبه q بوده ولذا دوری و در نتیجه آبلی است.

$H \cap K = \{e\}$ زیرا اگر x عضوی از $H \cap K$ باشد آنگاه مرتبه x، مرتبه H و همچنین مرتبه K را می‌شمارد و چون $(p^2, q) = 1$ پس $o(x) = 1$ لذا $x = e$.

حال داریم $|HK| = \frac{|H||K|}{|H \cap K|}$ لذا $G = HK$ پس چون H و K زیرگروههای نرمال G هستند و $H \cap K = \{e\}$ بنابراین G حاصلضرب

داخلی H و K است وبنابه قضیه $G \cong H \times K$ و چون H و K آبلی هستند لذا G آبلی است.

۱۴۰ ـ فرض کنیم کنش G بر X صادقانه باشد، g و h دو عضو از G باشند که

$$\forall x \in X : xg = xh$$

بنابراین به ازای هر x از X داریم $x(gh^{-1}) = x$ بنابراین $(gh^{-1}) = e$ پس $g = h$

برای اثبات کفایت چون می‌دانیم که هیچ دو عضوی از G بر تمام اعضای X تأثیر یکسان ندارند پس اثر هیچ عضوی مانند عضو همانی نیست یعنی تنها عضوهمانی است که تمام اعضاء X راثابت نگه می‌دارد.

۱۴۱ ـ فرض کنیم گروه G داری مرتبه ۴۸ باشد.نشان می‌دهیم G زیر گروه نرمال ۸ یا ۱۶ عضوی دارد.

از قضیه سوّم سیلو می‌دانیم که تعداد ۲ـ زیرگرو ههای سیلوی G برابر با ۱ یا ۳ است. اگر G تنهایک ۲ـزیرگروه سیلو داشته باشد،

این زیرگروه ۱۶ عصوی در G نرمال است. فرض کنیم G سه ۲ـزیرگروه سیلو دارد و $H \neq K$ دو تا از این زیرگروهها باشند. در این صورت مرتبه $H \cap K$ مرتبه H یعنی ۱۶ را بخش می‌کند. حال ادعا می‌کنیم

$|H \cap K| \leq ۴$ آنگاه $|H \cap K| = ۸$ زیرا اگر

$$|HK| = \frac{۱۶ \times ۱۶}{|H \cap K|} \geq ۶۴$$

که متناقض $|G| = ۴۸$ می‌باشد. چون اندیس $H \cap K$ در H و K برابربا ۲ است پس $H \cap K$ در H و در K نرمال است بنابراین $N[H \cap K]$ هر دو گروه H و K را شامل می‌شود. پس $HK \subseteq N[H \cap K]$ ولذا

$$| N[H \cap K] | \geq | HK | = \frac{۱۶ \times ۱۶}{۸} = ۳۲$$

چون مرتبه $N[H \cap K]$ مرتبه G یعنی ۴۸ را می‌شمارد پس مرتبه آن برابر ۴۸ بوده و لذا $N[H \cap K] = G$ و از اینجا نتیجه می‌گیریم که $H \cap K$ در G نرمال است و لذا G ساده نیست.

فصل ۳

حلقه‌ها

تمرینات بخش حلقه‌ها

۱ ـ نشان دهید مجموعهٔ { ۴ و ۲ و ۰ } تحت عمل جمع و ضرب به هنگ ۶ یک حلقه یکدار است.

۲ ـ نشان دهید حلقه‌ای که تحت عمل جمع گروه دوری باشد، حلقه جابجائی است.

۳ ـ نشان دهید عنصر یکال در حلقه، هر عضو حلقه را عاد می‌کند. (عنصر یکال عنصری است که نسبت به عمل ضرب حلقه وارون داشته باشد).

۴ ـ فرض کنید a و b اعضایی از یک حلقه جابجائی باشند و a عنصر یکال، $b^2 = 0$ باشد نشان دهید که $a + b$ عضو یکالی از حلقه است.

۵ ـ ثابت کنید اشتراک هر گردایه از زیر حلقه‌های، حلقه‌ای چون R یک زیر حلقه R است.

۶ ـ فرض کنید عدد صحیح زوجی چون n وجود داشته باشد بقسمی که $a^n = a$ برای هر عنصر a از یک حلقه چون R، نشان دهید که به ازای هر a از R داریم $-a = a$

۷ ـ نشان دهید اگر در یک حلقه قانون حذف برقرار باشد، حلقه مقسوم علیه صفر ندارد.

۸ ـ R یک حلقه و a عنصر پوچ توانی از R است ثابت کنید a وارون ضربی ندارد ولی $(a - 1)$ وارون ضربی دارد.

۹ ـ نشان دهید عناصر خودتوان یک حوزه صحیح ۰ و ۱ می‌باشند.

۱۰ ـ آیا $\mathbf{Z} \times \mathbf{Z}$ یک حوزه صحیح است؟

۱۱ ـ فرض کنید a و b اعضایی از یک حوزه صحیح باشند، اگر $a^m = b^m$، $a^n = b^n$ که m و n اعداد صحیحی باشند و $1 = (m \text{ و } n)$ ثابت کنید $a = b$

۱۲ ـ فرض کنید R حلقه جابجائی بدون مقسوم علیه صفر باشد نشان دهید که مشخصهٔ R، صفر یا عدد اوّل می‌باشد.

۱۳ ـ فرض کنید R حلقه جابجائی بدون مقسوم علیه صفر باشد، نشان دهید که همه عناصر R مرتبه جمعی یکسان دارند.

۱۴ ـ فرض کنید D یک حوزه صحیح و φ یک تابع غیر ثابت از D به اعداد صحیح نامنفی باشد، نشان دهید اگر $\varphi(xy) = \varphi(x)\varphi(y)$ و x یکال در D باشد آنگاه $\varphi(x) = 1$

۱۵ ـ اگر n عدد صحیح مثبت و بزرگتر از یک باشد نشان دهید $n\mathbf{Z} = \langle n \rangle$ ایده‌آل اوّلی از $\mathbf{Z}$ است اگر و فقط اگر n عدد اوّل باشد.

۱۶ ـ اگر A ایده‌آلی از حلقه یکدار R باشد و عنصریکّه R متعلّق به A باشد نشان دهید $A = R$

۱۷ ـ R حلقه جابجائی یکدار است، نشان دهید هر ایده‌آل ماکزیمال آن ایده‌آل اوّل است.

۱۸ ـ اگر R حلقه جابجائی با بیش از یک عضو باشد، ثابت کنید اگر برای هر عضو غیر صفر چون a از R داشته باشیم $aR = R$ آنگاه R یک میدان است.

۱۹ ـ فرض کنید A و B و C ایده‌آلهای حلقه R باشند همچنین C ایده‌آل اوّل و $AB \subseteq C$ نشان دهید $A \subseteq C$ یا $B \subseteq C$

۲۰ ـ F حلقه جابجائی یکدار است نشان دهید F یک میدان است اگر و فقط

اگر ایده‌آلهای آن ایده‌آل صفر و خود F باشد.

۲۱ ـ فرض کنید R یک حلقه و J ایده‌آلی از آن باشد و همچنین I ایده‌آلی از J باشد ثابت کنید اگر I یکدار باشد آنگاه I ایده‌آل R است.

(توجّه : شاید عنصریکّه I با عنصریکّه R متفاوت باشد.)

۲۲ ـ در هر حوزه صحیح با ایده‌آلهای اصلی (PID) نشان دهید که هر ایده‌آل اوّل ، ماکزیمال است.

۲۳ ـ فرض کنیم R یک حوزه صحیح با مشخصه غیر صفر باشد، اگر A یک ایده‌آل از R باشد نشان دهید که مشخصهٔ $\frac{R}{A}$ همان مشخصه R است.

۲۴ ـ R حلقه جابجائی یکدار و متناهی است، ثابت کنید هر ایده‌آل اوّل R یک ایده‌آل ماکزیمال R است.

۲۵ ـ F یک میدان و R یک حلقه است، $\varphi : F \longrightarrow R$ یک همریختی حلقه‌ای غیر صفر باشد آنگاه φ یک به یک است.

۲۶ ـ فرض کنید

$$S = \{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a , b \in R \}$$

نشان دهید که یکریختی حلقه‌ای از C به S وجود دارد.

۲۷ ـ آیا هموморفیسم حلقه‌ای از اعداد حقیقی به یک حلقه چون M وجود دارد که هستهٔ آن مجموعهٔ اعداد صحیح باشد؟

۲۸ ـ نشان دهید هر همریختی پوشا از یک میدان به یک حلقه با بیش از یک عضو یکریختی است.

۲۹ ـ آیا میدان اعداد حقیقی با میدان اعداد مختلط یکریخت است؟

۳۰ ـ مثالی از یک حلقه غیر یکدار ارائه کنید که در داخل یک میدان قرار داشته باشد.

۳۱ ـ اگر F یک میدان باشد ثابت کنید:

الف) اگر مشخصه F مخالف صفر باشد آنگاه مشخصه F عدد اوّل است.

ب) اگر همریختی پوشا $\varphi : \mathbf{Z} \longrightarrow F$ وجود داشته باشد ثابت کنید F متناهی و مرتبه F عدد اوّل است.

ج) یک حوزه صحیح مثال بزنید که نامتناهی باشد ولی مشخصه آن متناهی باشد.

۳۲ ـ فرض کنید F یک میدان متناهی باشد ثابت کنید به ازای هر a از F $a^{p^n} = a$ که مرتبه F برابر p^n بوده و p عدد اوّل است.

۳۳ ـ فرض کنیم R یک حلقه با بیش از یک عضو و به ازای هر a از R عضو منحصر بفرد b از R وجود داشته باشد بطوریکه $aba = a$ ثابت کنید:

الف) R مقسّم صفر (مقسوم علیه صفر) ندارد.

ب) $bab = b$.

ج) R عضو یکّه دارد.

د) R یک حلقه تقسیم (بخشی) است.

۳۴ ـ فرض کنید R حلقه‌ای جابجائی و یکدار باشد بطوریکه برای هر x از R داشته باشیم $x^n = x$ که در آن $n > 1$ عدد طبیعی ثابتی است، ثابت کنید هر ایده‌آل اوّل R ماکزیمال نیز می‌باشد.

۳۵ ـ اگر R حلقهٔ جابجائی یکدار با ایده‌آلهای اصلی باشد همچنین p و q دو ایده‌آل اوّل R باشند بطوریکه $p \subsetneq q$ آنگاه q ایده‌آل ماکزیمال است.

۳۶ ـ فرض کنید R حلقهٔ تعویض پذیر یکدار باشد، نشان دهید اگر f یک همریختی پوشا از R به یک میدان باشد آنگاه $\ker f$ یک ایده‌آل ماکزیمال R است.

۳۷ ـ D یک حوزه صحیح با ایده‌آلهای اصلی و I ایده‌آل D است، نشان دهید هر ایده‌آل $\frac{D}{I}$ اصلی است، آیا $\frac{D}{I}$ لزوماً یک PID است؟

۳۸ ـ با ذکر دلیل بگویید آیا حوزه صحیحی از مرتبه شش وجود دارد؟

۳۹ ـ نشان دهید حلقهٔ

$$\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Q} \} = M_2(\mathbf{Q})$$

ایده‌آل دو طرفه ندارد.

۴۰ ـ اگر M یک ایده‌آل سرهٔ حلقه بول R باشد (یعنی $\forall x \in R : x^2 = x$) که R یکدار است ثابت کنید:

الف) $\frac{R}{M}$ یک حلقه بول است.

ب) $\frac{\mathbf{Z}}{<2>}$ با $\frac{R}{M}$ یکریخت است اگر و فقط اگر M ایده‌آل ماکزیمال در R باشد.

۴۱ ـ اگر R حلقهٔ بدون عضو پوچ توان غیر صفر باشد آنگاه برای هر عضو خود توان چون e از R، ثابت کنید به ازای هر x از R، $ex = xe$.

۴۲ ـ R یک حلقه و A، B دو ایده‌آل باشند نشان دهید:

$$A+B = < A \cup B >$$

۴۳ ـ فرض کنید هر ایده‌آل حلقه جابجائی و یکدار R اصلی است، $f : R \longrightarrow R$ یک همریختی پوشا باشد آنگاه ثابت کنید f یکریختی است.

۴۴ ـ فرض کنیم F میدانی نامتناهی و K زیر مجموعه‌ای نامتناهی از F است اگر $f(x) \in F[x]$ و به ازای هر t از K، $f(t) = 0$ آنگاه نشان دهید که $f(x)$ چند جمله‌ای صفر است.

۴۵ ـ فرض کنید $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ در $\mathbf{Z}[x]$ است نشان دهید اگر $\frac{r}{s}$ که در آن $1 = (r, s)$ ریشه $f(x)$ در $\mathbf{Q}$ باشند آنگاه $r \mid a_0$ و $s \mid a_n$

۴۶ ـ فرض کنید حلقه R تعویض پذیر است و a عضوی از R است نشان دهید $N = \{ ra + na \mid r \in R \text{ و } n \in Z \}$ کوچکترین ایده‌آل R است که شامل a می‌باشد.

۴۷ ـ اگر در حلقه‌ای یکدار چون R داشته باشیم $x^{۱۳۷۰} = x$ ثابت کنید:

الف) به ازای هر x از R ، $۲x = 0$

ب) R عنصر پوچ توان غیر صفر ندارد

ج) به ازای هر x و y از R $x^{۱۳۶۹}y = yx^{۱۳۶۹}$

د) هر ایده‌آل اوّل R ایده‌آل ماکزیمال است.

۴۸ ـ فرض کنید F یک میدان و a عضوی از آن باشد نشان دهید a ریشه $f(x) \in F[x]$ است اگر و فقط اگر $(x-a) \mid f(x)$

۴۹ ـ نشان دهید $\frac{Z_۲[x]}{\langle x^۲+x+۱ \rangle}$ یک میدان ۴ عضوی است. اعضای آن را مشخص کنید.

۵۰ ـ چند جمله‌ای $x^۴ + ۴$ را به دو صورت به حاصلضرب عوامل تحویل‌ناپذیر در $Z_۵[x]$ تجزیه کنید.

حل تمرینات بخش حلقه‌ها

۱ ـ می‌دانیم که $Z_۶$ یک حلقه است حال چون $\{۰ و ۲ و ۴\} \subseteq Z_۶$ نشان می‌دهیم که مجموعه فوق زیر حلقه $Z_۶$ است.

$۴ - ۲ = ۲ \in \{۰ و ۲ و ۴\}$

$۲ - ۰ = ۲ \in \{۰ و ۲ و ۴\}$ $\quad$ $۴ - ۰ = ۴ \in \{۰ و ۲ و ۴\}$

$۲ - ۴ \equiv ۴ \text{ (هنگ ۶)} \Rightarrow (۲ - ۴) \in \{۰ و ۲ و ۴\}$

پس $\{۰ و ۲ و ۴\}$ زیر حلقه $Z_۶$ است.

حال نشان می‌دهیم که چهار عنصر یکّه آن است،

$۲ \times ۴ = ۸ \equiv ۲ \quad (\text{هنگ } ۶)$

$۴ \times ۴ = ۱۶ \equiv ۴ \quad (\text{هنگ } ۶)$

پس ۴ عنصر یکّه آن است.

(توجّه: از این تمرین نتیجه می‌شود که امکان دارد عنصر یکّه حلقه با عنصر یکّه زیر حلقه متفاوت باشد).

۲ ـ فرض کنیم R حلقه‌ای باشد که تحت عمل جمع گروه دوری بوده و a مولد R باشد

$\forall x و y \in R \Rightarrow x = na \text{ و } y = ma \quad m و n \in Z$

$xy = (na)(ma) = (nm)a^۲ = (ma)(na) = yx$

بنابراین R حلقه جابجائی است.

۳ ـ فرض کنیم a عضو یکالی از یک حلقه باشد پس اگر عنصر یکّه حلقه ۱

باشد داریم: $aa^{-1} = 1$.

فرض کنیم b عضو دلخواهی از حلقه باشد پس $b = a(a^{-1}b)$ لذا a، b را می‌شمارد.

$(a+b)(a^{-1}-a^{-2}b) = aa^{-1} - a^{-1}b + ba^{-1} - a^{-2}b^2 = aa^{-1} = 1 - 4$

پس $a + b$ عضو یکال حلقه است.

۵ـ فرض کنیم H_iها زیر حلقه‌های R باشند.

$$\forall x, y \in \bigcap_{i \in I} H_i \Rightarrow x, y \in H_i \quad \forall i \in I$$

$$\Rightarrow x - y \in H_i \ \forall i \in I \Rightarrow x - y \in \bigcap_{i \in I} H_i$$

پس $\bigcap_{i \in I} H_i$ زیر حلقه R است.

۶ـ فرض کنیم a عضوی از R باشد و $n = 2k$ در این صورت داریم:

$-a = (-a)^{2k} = [(-a)^2]^k = (a^2)^k = a^{2k} = a$

بنابراین $a = -a$ و لذا حکم ثابت است.

۷ـ فرض کنیم a و b اعضایی از این حلقه باشند و داشته باشیم $ab = 0$ همچنین فرض کنیم a مخالف صفر باشد بنابراین $ab = a.0$ پس $b = 0$ و حکم ثابت است.

۸ـ فرض کنیم $a^n = 0$ و a^{-1} موجود باشد در این صورت $a^{-1}a^n = 0$ پس $a^{n-1} = 0$ و اگر a^{-1} را $n - 2$ بار بترتیب در توانهای a که برابر صفر می‌شود ضرب کنیم نهایتاً خواهیم داشت $a = 0$ و این خلاف این است که a وارون دارد پس a وارون پذیر نیست.

چون

$(1+a+...+a^{n-1})(1-a) = (1-a)(1+a+...+a^{n-1}) = 1-a^n = 1$

پس $(1-a)$ وارون پذیر است و $(1+a+...+a^{n-1})$ وارون آن می‌باشد.

۹ـ فرض کنیم a عضوی خود توان از یک حوزه صحیح باشد پس $a^2 = a$ لذا $a^2 - a = 0$ بنابراین $a(a-1) = 0$ چون a و $a-1$ عناصری از حوزه صحیح هستند لذا $a = 0$ یا $a-1 = 0$ پس $a = 0$ یا $a = 1$ و مطلب تمام است.

۱۰ـ $\mathbb{Z} \times \mathbb{Z}$ حوزه صحیح نیست زیرا $(0,0) = (0,1).(1,0)$ ولی $(0,0) \neq (1,0)$ و $(0,0) \neq (0,1)$.

۱۱ـ چون $(m,n) = 1$ پس اعداد صحیحی چون x و y وجود دارند بطوریکه $mx + ny = 1$ لذا

$$a = a^{mx+ny} = a^{mx}.a^{ny} = (a^m)^x (a^n)^y = (b^m)^x . (b^n)^y$$
$$= b^{mx}.b^{ny} = b^{mx+ny} = b \Rightarrow a = b$$

۱۲ـ فرض کنیم مشخصه R برابر n باشد و n مخالف صفر باشد.

اگر n اوّل باشد که مسئله حل است و اگر n اوّل نباشد پس s , t ای از اعداد صحیح هستند بطوریکه $n = s.t$ که $1 < s, t < n$

$$\forall x \in R \quad 0 = n.x = (st)(x) = s(tx) \Rightarrow tx = 0$$

پس بطور خلاصه داریم به ازای هر x از R، $tx = 0$ ولی چون t کوچکتر از n است این مخالف با مشخصه بودن n است، پس n اوّل می‌باشد.

۱۳ـ فرض کنیم x و y اعضایی از R باشند و x و y به ترتیب از مراتب جمعی n و m باشند که $n \leqslant m$ داریم:

$$0 = n(xy) = (nx)y = x(ny) \Rightarrow ny = 0 \Rightarrow m \leqslant n$$

و چون داشتیم $n \leqslant m$ پس $m = n$ و لذا همه عناصر R دارای مرتبه جمعی یکسان هستند.

$\varphi(x) = \varphi(x.1) = \varphi(x)\varphi(1) \Rightarrow \varphi(x) - \varphi(x)\varphi(1) = 0$ ـ ۱۴

$\Rightarrow \varphi(x)[1 - \varphi(1)] = 0 \Rightarrow \varphi(1) = 1$

از طرفی داریم:

$\varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) \Rightarrow \varphi(x) = 1$ و $\varphi(x^{-1}) = 1$

(در مورد این قسمت آخر توجه شود که $\varphi(x)$ و $\varphi(x^{-1})$ هر دو اعداد صحیح نامنفی می‌باشند)

۱۵ ـ فرض کنیم $< n >$ ایده‌آل اوّلی از $\mathbf{Z}$ باشد، نشان می‌دهیم n عدد اوّل است اگر n اوّل نباشد پس اعداد صحیحی چون r و s وجود دارند بقسمی که $n = r.s$ و $n > s > 1$ و $n > r > 1$ حال چون $n \in < n >$ لذا $rs \in < n >$ چون $< n >$ اوّل است پس $n \mid r$ یا $n \mid s$ و این تناقض با این است که $1 < r,s < n$ پس n اوّل می‌باشد.

به عکس فرض کنیم n عدد اوّل باشد و $ab \in < n >$ لذا $n \mid ab$ و چون n اوّل است پس $n \mid a$ یا $n \mid b$ لذا $a \in < n >$ یا $b \in < n >$.

۱۶ ـ فرض کنیم 1 عنصر یکه R باشد و $1 \in A$ همچنین a عضوی از A و r عضوی از R باشد چون A ایده‌آلی از R است پس $a.r \in A$ ، حال فرض کنیم $a = 1$ پس $r \in A = r.1$ لذا به ازای هر r از R داریم r متعلّق به A پس R زیر مجموعه A است و از طرفی می‌دانیم A زیر مجموعه R است پس $A = R$.

۱۷ ـ فرض کنیم I ایده‌آل ماکزیمال R باشد بنابراین می‌دانیم R / I میدان است در نتیجه R / I حوزهٔ صحیح بوده و بنا به قضیه، I ایده‌آل اوّل است.

۱۸ ـ باید نشان دهیم که R یکدار بوده و هر عنصر غیر صفر آن وارون دارد چون $aR = R$ به ازای هر a متعلّق به R، لذا عضوی چون x از R وجود دارد بطوریکه $ax = a$ حال ادعا می‌کنیم که x عضو یکّه R است.

$\forall b \in R: xb = bx = ayx = yax = ya = ay = b \Rightarrow$

پس x عضو همانی R است.

(توجه : چون $aR = R$ و $b \in R$ پس $x\,(b = ay)$ را با ۱ نشان می‌دهیم.

حال نشان می‌دهیم که هر عضو غیر صفر R وارون ضربی دارد.

فرض کنیم a عضو غیر صفری از R باشد چون $aR = R$ و ۱ متعلق به R است.

پس عضوی چون a^{-1} از R وجود دارد بطوریکه $aa^{-1} = 1$ ولذا چون a دلخواه بود

پس هر عضو غیر صفر R وارون ضربی دارد. بنابراین R میدان است.

۱۹ ـ فرض کنیم $A \not\subset C$ و $B \not\subset C$ لذا عضوی از A چون a و عضوی از B چون b وجود دارند بطوریکه $a \notin C$ و $b \notin C$ چون $AB \subseteq C$ پس $ab \in C$

بنابه اینکه C ایده‌آل اوّل است لذا a متعلّق به C یا b متعلّق به C می‌باشد که تناقض است پس $A \subseteq C$ یا $B \subseteq C$ و مطلب تمام است.

۲۰ ـ اوّلاً فرض کنیم F یک میدان باشد و I یک ایده‌آل F باشد بنابراین اگر $I \neq \{0\}$

$0 \neq a \in I \quad \Rightarrow aa^{-1} = 1 \in I$

بنابه تمرین شماره شانزده همین بخش $I = R$

به عکس فرض کنیم F یک حلقه جابجائی یکدار باشد که ایده‌آلهای آن ایده‌آل صفر و خود F باشند، بنابراین $\{0\}$ ایده‌آل ماکزیمال F است در نتیجه $\frac{F}{\{0\}}$ میدان است ولی چون F یکریخت با $\frac{F}{\{0\}}$ می‌باشد پس F یک میدان است.

۲۱ ـ فرض کنیم R یک حلقه و I ایده‌آلی از J و J ایده‌آلی از R باشد.

ثابت می‌کنیم I ایده‌آل R است برای این منظور با توجه به فرض مسئله واضح است که $I \subseteq R$ باید نشان دهیم به ازای هر a و b از I ، $a - b$ متعلّق به I است و همچنین به ازای هر a از I و هر r از R ، ar متعلّق به I است.

فرض کنیم ۱ عنصر یکّه I باشد در نتیجه چون I ایده‌آل J است پس ۱ متعلّق به J بوده و لذا به ازای هر r از R داریم (۱۰ r)عضوی از J می‌باشد چون I ایده‌آل J است پس (۱۰r) a عضوی از I است لذا ۰r(a۰۱) عضوی از I است چون r = a۰r (a۰۱) پس a۰r عضوی از I است و یک قسمت ثابت شد.

فرض کنیم b و a اعضایی از I باشند چون I ایده‌آلی از J است پس a - b عضوی از I است.

بنابراین I ایده‌آل R است.

۲۲ ـ فرض کنیم D یک PID باشد و I ایده‌آل D همچنین I اوّل باشد.

فرض کنیم J ایده‌آل D باشد بطوریکه $I \subsetneq J \subseteq D$

چون D یک حوزه صحیح با ایده‌آلهای اصلی است پس x و y ای از D وجود دارند بطوریکه $I = \langle x \rangle$ و $J = \langle y \rangle$ چون x متعلّق به J است پس t ای از R است بطوریکه $x = yt$ چون $x \in I$ پس yt متعلّق به I ولی $y \notin I$ پس $t \in I$ لذا z ای وجود دارد بطوریکه $t = xz$ بنابراین $t = ytz$ پس $0 = yz - ۱$ و لذا $yz = ۱$ بنابراین ۱ متعلّق به J است پس $J = R$

توجّه: این حکم در مورد حوزه صحیح درست نیست زیرا $\langle x \rangle$ ایده‌آل اوّل $\mathbf{Z}[x]$ است ولی ماکزیمال نیست.

۲۳ ـ فرض کنیم $r + A$ عضو دلخواهی از $\frac{R}{A}$ باشد و مشخصه R برابر p باشد می‌دانیم که p یک عدد اوّل می‌باشد و همچنین می‌دانیم مشخصه $\frac{R}{A}$ برابر مرتبه جمعی $۱ + A$ است لذا چون $O(۱) = p$ | $O(۱ + A)$ پس $O(۱ + A) = p$ لذا مشخصه $\frac{R}{A}$ برابر p و همچنین برابر مشخصه R است.

۲۴ ـ فرض کنیم I ایده‌آل اوّل R باشد پس $\frac{R}{I}$ حوزه صحیح است. و چون R

متناهی است. پس $\frac{R}{I}$ متناهی است و چون هر حوزه صحیح متناهی میدان است بنابراین $\frac{R}{I}$ میدان بوده و لذا I ایده‌آل ماکزیمال R است.

۲۵ ـ می‌دانیم که $\ker\varphi$ ایده‌آل F است و چون F یک میدان بوده و تنها ایده‌آلهای آن F، $\{0\}$ هستند و از طرفی φ همریختی صفر نیست لذا $\ker\varphi = \{0\}$ در نتیجه φ یک به یک می‌باشد.

۲۶ ـ

$$\varphi : C \longrightarrow S$$

$$(a + bi)\varphi = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

۱) φ خوش تعریف است

$$(a_2 + b_2 i) = (a_1 + b_1 i) \Rightarrow \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \Rightarrow$$

$$\Rightarrow (a_2 + b_2 i)\varphi = (a_1 + b_1 i)\varphi$$

۲) φ یک به یک است

$$(a_1 + b_1 i)\varphi = (a_2 + b_2 i)\varphi \Rightarrow \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$\begin{cases} a_1 = a_2 \\ \Rightarrow \\ b_1 = b_2 \end{cases} \Rightarrow \quad a_1 + b_1 i = a_2 + b_2 i$$

۳) φ پوشا است

$$\forall \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in S \quad (a + bi)\varphi = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

۴) φ هممورفسیم است

$$[(a_1+b_1 i)(a_2+b_2 i)]\varphi = [(a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2)]\varphi$$

$$\begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -a_1b_2 - b_1a_2 & a_1a_2 - b_1b_2 \end{bmatrix} - \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$= (a_1 + b_1 i)\varphi(a_2 + b_2 i)\varphi$$

۲۷ ـ خیر ـ زیرا هسته همریختی ایده‌آلی از $\mathbf{R}$ است و چون تنها ایده‌آلهای $\mathbf{R}$ خود $\mathbf{R}$ و $\{0\}$ می‌باشد، بنابراین چنین همریختی وجود ندارد.

۲۸ ـ باید نشان دهیم که φ، همریختی مذکور یک به یک می‌باشد. برای این منظور باید نشان دهیم $\ker\varphi = \{0\}$ امّا چون $\ker\varphi$ ایده‌آل F است. (F میدان است) و تنها ایده‌آلهای F، خود F و $\{0\}$ می‌باشند، همچنین φ پوشا است و مرتبه M بزرگتر از یک است. (M همان حلقهٔ ذکر شده می‌باشد) لذا $\ker\varphi = \{0\}$ و حکم ثابت است.

۲۹ ـ خیر، زیرا معادله $x^4 = 1$ در $\mathbf{R}$ دو جواب ولی در $\mathbf{C}$ چهار جواب دارد.

۳۰ ـ $2\mathbf{Z}$ یک حلقه غیر یکدار است که در داخل میدان اعداد گویا قرار دارد. ($2\mathbf{Z} \subseteq \mathbf{Q}$).

۳۱ ـ الف) فرض کنیم مشخصهٔ F برابر n باشد که n مخالف صفر است حال فرض کنیم n اوّل نباشد لذا اعداد صحیح s و t وجود دارد بطوریکه $n = s \cdot t$ و $1 < s, t < n$

$$n.1 = 0 \Rightarrow (s.t).1 = 0 \Rightarrow (s.1)(t.1) = 0 \Rightarrow s.1 = 0 \text{ یا } t.1 = 0$$

و در هر حالت با مشخصه بودن n در تناقض است.

ب) طبق قضیه اساسی همریختی می‌دانیم F با $\frac{\mathbf{Z}}{\ker\varphi}$ یکریخت است و چون $\ker\varphi$ ایده‌آل $\mathbf{Z}$ می‌باشد بنابراین عدد صحیحی چون m موجود است بقسمی که $\ker\varphi = m\mathbf{Z}$ لذا F با $\frac{\mathbf{Z}}{m\mathbf{Z}}$ یکریخت است ولی $\mathbf{Z}_m$ با $\frac{\mathbf{Z}}{m\mathbf{Z}}$ یکریخت است لذا

Z_m با F یکریخت است چون F میدان است لذا m عدد اوّل است. پس F متناهی و از مرتبه عدد اوّل است.

ج) در حوزه صحیح $Z_p[x]$ که خود نا متناهی است مشخصه آن برابر p است. (البتّه p عدد اوّل است)

۳۲ ـ $F - \{0\}$ با عمل ضرب گروه است که مرتبه آن $p^n - 1$ است و طبق نتیجه‌ای از قضیه لاگرانژ می‌دانیم به ازای هر a از F $a^{p^n-1} = 1$ پس $a^{p^n} = a$ و حکم ثابت است.

۳۳ ـ الف) فرض کنیم c و d اعضایی از R باشند و داشته باشیم $cd = 0$ و c مخالف صفر باشد نشان می‌دهیم $d = 0$.

طبق فرض می‌دانیم یک b ی منحصر بفرد وجود دارد بطوریکه $cbc = c$ امّا داریم

$$c(b+d)c = cbc + cdc = cbc + 0 = cbc = c$$

چون b منحصر بفرد است پس $b + d = b$ لذا $d = 0$ و حکم ثابت است یعنی R مقسوم علیه صفر ندارد.

ب) به ازای هر a مخالف صفر، یک b ی منحصر بفرد از R وجود دارد بطوریکه:

$aba = a$ لذا $baba = ba$ بنابراین $bab = b$.

ج) اوّلاً R یک عضو خود توان دارد، زیرا $bab = b \Rightarrow (ba)^2 = ba$

حال این عنصر خود توان را e می‌نامیم و نشان می‌دهیم که به ازای هر x از R

$$x.e = e.x = x$$

$$(xe - x)e = xe^2 - xe = xe - xe = 0 \Rightarrow xe - x = 0 \Rightarrow xe = x$$

$$e(ex - x) = e^2x - ex = ex - ex = 0 \Rightarrow ex = x$$

بنابراین $ex = xe = x$ و حکم ثابت است.

د) فرض کنیم، x عضو غیر صفری از R باشد لذا b ی منحصر بفرد وجود دارد بطوریکه $xbx = x$ چون R مقسوم علیه صفر ندارد لذا $bx = ۱$.

چون $bxb = b$ پس $xb = ۱$ لذا $bx = xb = ۱$ پس x وارون پذیر است بنابراین R حلقه تقسیم است.

۳۴ـ فرض کنیم I ایده‌آل اوّلی از R باشد و K ایده‌آلی از R باشد بطوریکه

$$I \subsetneq K \subseteq R$$

چون $K \neq I$ پس وجود دارد x‌ای متعلّق به K بطوریکه x متعلّق به I نباشد طبق فرض داریم $x^n = x$ در نتیجه داریم:

$$x^n - x = ۰ \Rightarrow x(x^{n-۱} - ۱) = ۰ \in I \Rightarrow (x^{n-۱} - ۱) \in I$$

(چون I اوّل است و $x \notin I$)

بنابراین $x^{n-۱} - ۱$ متعلّق به K است پس ۱ متعلّق به K است لذا $K = R$ بنابراین I ماکزیمال است.

۳۵ـ فرض کنیم V ایده‌آل R باشد بطوریکه $q \subsetneq V \subseteq R$ ثابت می‌کنیم $V = R$ چون هر ایده‌آل R اصلی است لذا

$$q = \langle y \rangle \text{ و } p = \langle x \rangle \text{ و } V = \langle z \rangle$$

چون $p \neq q \neq V$ در نتیجه $z \notin q$ و $y \notin p$

حال چون $y \in V = \langle z \rangle$ لذا وجود دارد t ای از R بطوریکه $y = zt$ پس $y=zt$ چون y متعلّق به q و q اوّل است همچنین z متعلّق به q نیست پس t متعلّق به q است بنابراین u ای از R وجود دارد بطوریکه $t = yu$.

$$y = zt = zyu \Rightarrow y - zyu = ۰ \Rightarrow y(۱ - zu) = ۰ \in p$$

چون p اوّل بوده و $y \notin p$ پس $(۱ - zu)$ متعلّق به p بوده لذا $(۱ - zu)$ متعلّق به

V است لذا ۱ متعلّق به V است پس $V = R$ بنابراین q ماکزیمال است.

۳۶ـ بنابه قضیه اساسی همریختی می‌دانیم که F با $\frac{R}{kerf}$ یکریخت است (F همان میدانی است که f از R به روی آن است)

ولی چون F میدان است لذا $\frac{R}{kerf}$ میدان بوده و در نتیجه $kerf$ در R ماکزیمال است.

۳۷ـ می‌دانیم که هر ایده‌آل $\frac{D}{I}$ به فرم $\frac{K}{I}$ است که در آن K ایده‌آل D است و چون D یک حوزه صحیح با ایده‌آلهای اصلی است لذا xای از D هست که $K = < x >$ و ادعا می‌کنیم که $\frac{K}{I} = < x + I >$.

زیرا اگر $(y + I)$ عضوی از $\frac{K}{I}$ باشد آنگاه y عضوی از K است بنابراین عضوی از D چون r هست که $y = x.r$ پس $y + I = (x.r) + I = (x + I)(r + I)$

بنابراین $\frac{K}{I} = < x + I >$ لذا هر ایده‌آل $\frac{D}{I}$ اصلی است.

امّا $\frac{D}{I}$ لزوماً یک PID نیست زیرا برای مثال:

$$(۳ + ۶\mathbf{Z}) \in \frac{\mathbf{Z}}{۶\mathbf{Z}} \quad و \quad (۲ + ۶\mathbf{Z}) \in \frac{\mathbf{Z}}{۶\mathbf{Z}}$$

و داریم $(۳ + ۶\mathbf{Z})(۲ + ۶\mathbf{Z}) = ۶\mathbf{Z}$ که می‌بینیم $\frac{\mathbf{Z}}{۶\mathbf{Z}}$ مقسوم علیه صفر دارد و حوزه صحیح نیست.

۳۸ـ وجود ندارد.

اگر وجود داشته باشد با عمل جمع یک گروه آبلی است و چون از مرتبه شش دو گروه $S_۳$ و $\mathbf{Z}_۶$ را داریم لذا با $\mathbf{Z}_۶$ یکریخت بوده و در نتیجه ۲ عنصر a و b به ترتیب

از مراتب دو و سه دارد لذا $2ba = 0$ که در آن a مخالف صفر و همچنین 2b مخالف صفر است.

بنابراین حوزه صحیح از مرتبه شش وجود ندارد.

۳۹ـ فرض کنیم A مخالف صفر ایده‌آلی از $M_2(Q)$ باشد نشان می‌دهیم

$$A = M_2(Q)$$

چون $A \neq \{0\}$ پس X غیر صفری از A وجود دارد فرض کنیم

$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ چون A ایده‌آل است و ماتریسهای :

$$X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ و } X_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ و } X_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ و } X_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

متعلّق به $M_2(Q)$ هستند لذا

$$X_1 . X_2 + X_3 . X_4 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in A$$

از طرفی چون: $\begin{bmatrix} a^{-1} & 0 \\ 0 & a^{-1} \end{bmatrix} \in A$ لذا $\begin{bmatrix} a^{-1} & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

پس $A = M_2(Q)$

۴۰ـ الف) $\forall (x+M) \in \frac{R}{M} \quad (x+M)^2 = x^2 + M = x+M$

پس $\frac{R}{M}$ حلقه بول است.

ب) اگر $\frac{Z}{<2>}$ با $\frac{R}{M}$ یکریخت باشد چون $\frac{Z}{<2>}$ یک میدان است لذا $\frac{R}{M}$ میدان

بوده بنابراین M ایده‌آل ماکزیمال R است به عکس فرض کنیم M ایده‌آل ماکزیمال R باشد آنگاه $\frac{R}{M}$ میدان است

$$\forall x \in R \qquad (x + M)^{۲} = x+M$$

$$(x+M)[(x+M) - (۱+M)] = M \Rightarrow x + M = M$$

یا $\qquad (x+M) - (۱+M) = M \Rightarrow x + M = ۱ + M$

بنابراین به ازای هر x در R، $\quad x + M = M \quad$ یا $\quad x + M = ۱ + M$

لذا $\frac{R}{M}$ دو عنصر بیشتر ندارد. حال تابع زیر را در نظر می‌گیریم

$$f : \frac{R}{M} \longrightarrow \frac{Z}{<۲>} \qquad f(M) = <۲> \text{ و } f(۱+M) = ۱ + <۲>$$

واضح است که f یک ایزومورفیسم است پس $\frac{Z}{<۲>}$ یکریخت با $\frac{R}{M}$ است و لذا مطلب تمام است.

۴۱ ـ فرض کنیم x عضو دلخواهی از R باشد.

$$(exe - xe)^{۲} = exe^{۲}xe - exexe - xe^{۲}xe + xexe =$$

$$exexe - exexe - xexe + xexe = ۰$$

چون R عضو پوچ توان غیر صفر ندارد پس

$$exe - xe = ۰ \Rightarrow exe = xe \quad (۱)$$

از طرفی داریم:

$$(ex - exe)^{۲} = exex - exexe$$

$$- exeex + exe^{۲}xe = exex - exexe - exex + exexe = ۰$$

بنابراین $ex - exe = ۰$ پس $ex = exe$ (۲)

از رابطه (۱) و (۲) داریم $ex = xe$ و حکم ثابت است.

۴۲ ـ اولاً می‌دانیم که $A + B \subseteq A , B$ و $A + B$ ایده‌آل R است پس

$A \cup B \subseteq A + B$

حال اگر $A \cup B \subseteq X$ و X ایده‌آل R باشد، نشان می‌دهیم که $A + B \subseteq X$

برای این منظور فرض کنیم z عضوی از $A + B$ باشد پس aای از A و bای از R وجود دارد بطوریکه $z = a + b$ لذا $a + b$ متعلّق به $A \cup B$ در نتیجه a و b اعضایی از X هستند بنابراین $a + b$ متعلّق به X بوده پس $z \in X$ لذا

$(A + B) \subseteq X$

پس $< A \cup B > = A + B$

۴۳ ـ زنجیر صعودی

$\ker f \subseteq \ker f^2 \subseteq ... \subseteq \ker f^n \subseteq ...$

از ایده‌آلهای R را در نظر می‌گیریم، چون ایده‌آلهای R اصلی هستند پس در شرط زنجیر صعودی صدق می‌کند بنابراین عدد طبیعی مانند k موجود است که به ازاء هر $n \geq k$، $\ker f^n = \ker f^k$.

حال فرض کنیم $f(x) = 0$ پس y ای از R وجود دارد بطوریکه $x = f^k(y)$ لذا $0 = f(x) = f^{k+1}(y)$ بنابراین y متعلّق به $\ker f^{k+1}$ بوده پس $y \in \ker f^k$ لذا $x = f^k(y) = 0$ پس $\ker f = \{0\}$ لذا f یک به یک است.

۴۴ ـ اگر $f(x)$ مخالف صفر باشد آنگاه اگر درجه $f(x)$ برابر n باشد می‌دانیم که $f(x)$ حداکثر n ریشه متمایز در F دارد و لذا همه اعضای مجموعه نامتناهی K نمی‌توانند ریشه آن باشند پس $f(x)$ چند جمله‌ای صفر است.

۴۵ ـ چون $\frac{r}{s}$ ریشه $f(x)$ است پس

$a_0 + a_1 (\frac{r}{s}) + ... + a_n (\frac{r}{s})^n = 0$

بنابراین

$a_0 s^n + a_1 r s^{n-1} + \ldots + a_n r^n = 0$

چون $r \mid 0$ و $r \mid a_1 r s^{n-1} + \ldots + a_n r^n$ پس $r \mid a_0 s^n$ ولی چون

$(r,s) = 1$ پس $(r,s^n) = 1$ و لذا $r \mid a_0$.

چون $s \mid 0$ و $s \mid a_0 s^n + a_1 r s^{n-1} + \ldots + a r^{n-1}_{n-1} s$ پس $s \mid a_n r^n$ ولی چون

$(r,s) = 1$ پس $(s,r^n) = 1$ لذا $s \mid a_n$ و حکم ثابت است.

۴۶ ـ ابتدا نشان می‌دهیم N ایده‌آل R است. واضح است که

$a = 0a + 1a \in N$ پس N غیر تهی است.

فرض کنیم $x = ra + na$ و $y = sa + ma$ در N باشند و t عضوی از R باشد

در اینصورت

$$x - y = (ra + na) - (sa + ma)$$

$$= (r - s)a + (n - m)a \in N$$

$$tx = t(ra + na) = (tr)a + (nt)a$$

$$= (tr + nt)a + 0a \in N$$

همچنین چون R تعویض پذیر است پس xt عضوی از N بوده و لذا N یک ایده‌آل R است و $a \in N$.

برای این که نشان دهیم N کوچکترین ایده‌آل R است که شامل a است فرض کنیم M یک ایده‌آل R باشد و $a \in M$ چون M ایده‌آل است پس به ازای هر r از R و n از $\mathbf{Z}$،

$$(ra + na) \in M$$

بنابراین $N \subseteq M$

توجّه کنید که اگر R دارای عنصریکه باشد، آنگاه

$ra + na = (r + n1)a = sa$ که در آن $s = (r + n1) \in R$ در نتیجه

$N = \langle a \rangle = \{ sa \mid s \in R \}$

۴۷ ـ الف) بنا به مسئله شماره شش همین بخش داریم $x = -x$ به ازای هر x از R پس $2x = 0$

ب) فرض کنیم x پوچ توان باشد پس عدد صحیح مثبتی چون n وجود دارد بطوریکه $x^n = 0$ حال اگر $n > 1370$ باشد با استفاده از الگوریتم تقسیم داریم $n = 1370\, q + r$ که $r = 0$ یا $0 < r < 1370$ پس

$$0 = x^n = x^{1370q} \cdot x^r = x^{q+r}$$

$$x^q \cdot x^r = 0 \Rightarrow x^{-q} \cdot x^q \cdot x^r = 0 \Rightarrow x^r = 0$$

$$\Rightarrow x^{1370-r} \cdot x^r = 0 \Rightarrow x^{1370} = 0 \Rightarrow x = 0$$

پس تنها عضو پوچ توان R عضو صفر است.

ج) $(x^{1369} y - x^{1369} yx^{1369})^2 = x^{1369} y x^{1369} y - x^{1369} yx^{1369} yx^{1369}$

$- x^{1369} yx^{2738} y + x^{1369} y x^{2738} yx^{1369} = 0$

بنابراین $0 = x^{1369} y - x^{1369} y x^{1369} = (x^{1369} y - x^{1369} yx^{1369})^3$

لذا $x^{1369} y - x^{1369} yx^{1369} = 0$

در نتیجه $x^{1369} y = x^{1369} yx^{1369}$

بهمین ترتیب نشان می‌دهیم که $yx^{1369} = x^{1369} y x^{1369}$ پس

$$x^{1369} y = y x^{1369}$$

د) اگر در تمرین شماره سی و چهار همین بخش n را مساوی ۱۳۷۰ بگیریم نتیجه حاصل می‌شود.

۴۸ ـ فرض کنیم $(x - a) \mid f(x)$ پس وجود دارد $g(x)$ ای از $F[x]$ بطوریکه

$f(x) = (x-a)\, g(x)$ پس $f(a) = (a - a)\, g(x) = 0$ لذا a ریشه $f(x)$

است.

حال فرض کنیم $f(a) = 0$ بنابه الگوریتم تقسیم داریم

$$f(x) = (x - a) g(x) + r(x)$$

که $r(x) = 0$ یا درجه $r(x)$ از درجه $(x - a)$ یعنی ۱ کمتر است پس $r(x)$ چند جمله‌ای صفر یا یک چند جمله‌ای ثابت است.

چون $f(a) = 0$ پس $r(a) = 0$ لذا $0 = f(a) = (a - a)g(x) + r(a)$ و چون $r(x)$ اگر صفر نباشد چند جمله‌ای ثابت است پس $r(x) = 0$ و لذا خواهیم داشت $f(x) = (x - a) g(x)$ پس $(x - a) \mid f(x)$

۴۹ ـ چون $x^2 + x + 1$ در $\mathbf{Z}_2$ ریشه ندارد، پس در $\mathbf{Z}_2[x]$ تحویل ناپذیر است.

در نتیجه ایده‌آل $< x^2 + x + 1 >$ در $\mathbf{Z}_2[x]$ ماکسیمال و لذا

$E = \frac{\mathbf{Z}_2[x]}{< x^2 + x + 1 >}$ میدان است. حال فرض کنیم $f(x) \in \mathbf{Z}_2[x]$، بنابه الگوریتم تقسیم در $\mathbf{Z}_2[x]$، چند جمله‌ایهای $g(x)$ و $r(x)$ در $\mathbf{Z}_2[x]$ وجود دارند به طوری که

$$f(x) = g(x) (x^2 + x + 1) + r(x)$$

که در آن $r(x) = 0$ یا $\deg r(x) \leq 1$ بنابراین

$$r(x) = ax + b \qquad a,b \in \mathbf{Z}_2$$

پس هر عضو E به صورت زیراست:

$$f(x) + <x^2+x+1> = r(x) + g(x)(x^2 + x + 1) + <x^2 + x + 1>$$

$$= (ax + b) + < x^2 + x + 1 >$$

چون $\mathbf{Z}_2 = \{ 0 , 1 \}$، پس ۲ انتخاب برای a و برای هر انتخاب a، ۲ انتخاب برای b وجود دارد یعنی مرتبه E برابر ۴ است در واقع اعضای E عبارتند از

$< x^2 + x + 1 >$ و $x + < x^2 + x + 1 >$ و $1 + < x^2 + x + 1 >$

$(x + 1) + < x^2 + x + 1 >$

۵۰ـ به سادگی دیده می‌شود که ۱ و ۲ و ۳ و ۴ ریشه‌های $x^4 + 4$ در Z_5 هستند پس

$$x^4 + 4 = (x - 1)(x - 2)(x - 3)(x - 4)$$

این تجزیه را به صورت

$$x^4 + 4 = (2x - 2)(3x - 1)(x - 3)(x - 4)$$

نیز می‌توان نوشت. توجه می‌کنیم که $2(x-1) = 2x - 2$ و $3(x-2) = 3x - 1$

فصل ٤

میدانها و حوزه‌های تجزیه یکتا

تمرینات بخش میدانها و حوزه تجزیه یکتا

۱ـ فرض کنید چند جمله‌ای $p(x)$ در $F[x]$ تحویل ناپذیر است و $p(x) \mid r(x)s(x)$ که در آن $r(x)$ و $s(x)$ در $F[x]$ هستند در اینصورت نشان دهید $p(x) \mid r(x)$ یا $p(x) \mid s(x)$

۲ـ نشان هید اگر d و d' دو ب.م.م. a و b در D باشند آن‌گاه عضو واحد u در D وجود دارد بطوریکه $d = ud'$ (D حوزه صحیح است).

۳ـ فرض کنید a و b دو عضو غیر صفر در D هستند (D حوزه صحیح است) نشان هید:

الف) a و b وابسته اند اگر و تنها اگر $b \mid a$ و $a \mid b$

ب) a و b وابسته اند اگر و تنها اگر $<a> = <b>$

۴ـ فرض کنیم D یک حوزهٔ تجزیه یکتا باشد و p عضوی از D در اینصورت p اوّل است اگر و تنها اگر تحویل ناپذیر باشد.

۵ـ فرض کنید F میدان، x و y دو مجهول روی F باشند، نشان دهید $F[x,y]$ یک PID نیست.

۶ـ فرض کنید R حلقه‌ای با یک ارزیاب اقلیدسی باشد نشان دهید هر ایده‌آل R اصلی است (تابع $f: R - \{0\} \to \mathbf{Z}$ را یک ارزیاب اقلیدسی روی R گوییم هرگاه (الف) به ازای هر a از $R - \{0\}$، $f(a) \geq 0$ (ب) به ازای هر a و b از $R - \{0\}$، $f(a) \geq f(ab)$ (ج) به ازای هر a از R و هر b از $R - \{0\}$ اعضای r و q از D باشند که $a = bq + r$ که در آن $r = 0$ یا $f(r) < f(b)$

۷ـ فرض کنید R یک حلقه جابجائی و $f: R - \{0\} \to \mathbf{Z}$ یک ارزیاب

اقلیدسی باشد، نشان دهید R یکداراست.

۸ ـ نشان دهید $\alpha \in E$ روی F غیر جبری است اگر و تنها اگر همریختی ارزیاب $\varphi_\alpha : F[x] \to E$ ، $\varphi_\alpha [\, f(x) \,] = f(\alpha)$ یک به یک باشد.

۹ ـ نشان دهید α متعلّق به E روی F جبری است اگر و تنها اگر $[F : F(\alpha)]$ متناهی باشد.

۱۰ ـ نشان دهید اگر E توسیع متناهی F باشد، آنگاه E توسیع متناهیاً تولید شده از F است.

۱۱ ـ اگر E یک توسیع متناهی F باشد و D یک حوزه صحیح که $F \subseteq D \subseteq E$ نشان دهید که D یک میدان است.

۱۲ ـ فرض کنید F یک میدان با مشخصه غیر دو باشد ، a و b اعضایی از F باشند آنگاه $F(\sqrt{a}\,\sqrt{b}) = F(\sqrt{a} + \sqrt{b})$

۱۳ ـ حوزه صحیح مثال بزنید که UFD نباشد.

۱۴ ـ نشان دهید هر توسیع متناهی جبری است.

۱۵ ـ فرض کنیم D یک PID است و $p \in D$ در اینصورت p اوّل است. اگر و تنها اگر در D تحویل ناپذیر باشد.

حل تمرینات بخش میدانها و حوزه تجزیه یکتا

۱ ـ فرض کنیم $p(x) \mid r(x)s(x)$ دراین صورت $r(x)\ s(x) \in \langle p(x) \rangle$، چون $P(x)$ روی F تحویل ناپذیر است پس ایده‌آل $\langle p(x) \rangle$ در $F[x]$ ماکسیمال است و لذا اوّل است در نتیجه $r(x) \in \langle p(x) \rangle$ یا $s(x) \in \langle p(x) \rangle$ بنابراین $p(x) \mid r(x)$ یا $p(x) \mid s(x)$

۲ ـ فرض کنیم d و d' دو ب. م. م. a و b باشند بنابه تعریف ب. م. م. نتیجه می‌گیریم که $d' \mid d$ و $d \mid d'$ لذا x و y ای از D وجود دارند بطوریکه $d' = dx$ یا $d = d'y$ پس $d' = dx = d'yx$ لذا $yx = ۱$ یعنی x واحد (یکال) است. پس $d' = dx$ که x یکال است.

۳ ـ (الف) فرض کنیم a و b وابسته باشند در اینصورت عضو واحد u از D وجود دارد به طوریکه $a = bu$ پس $b \mid a$ همچنین چون $b = au^{-۱}$ پس $a \mid b$ برعکس اگر $a \mid b$ و $b \mid a$ آن‌گاه x و y از D وجود دارند به طوری که $b = ax$ و $a = by$ درنتیجه $a = by = axy$ ولذا $xy = ۱$ یعنی x واحد است، حال چون $b = ax$ و x واحد است پس b و a وابسته اند.

(ب) بنابه قسمت (الف) a و b وابسته‌اند اگر و تنها اگر $a \mid b$ و $b \mid a$ در نتیجه a و b وابسته اند اگر وتنها اگر $a \in \langle b \rangle$ و $b \in \langle a \rangle$ بنابراین داریم: a و b وابسته‌اند اگر تنها اگر $\langle a \rangle = \langle b \rangle$

۴ ـ فرض کنیم p از D اوّل باشد و $p = ab$ که در آن a و b اعضایی از D هستند، چون p اوّل است بنابراین $p \mid a$ یا $p \mid b$ (چون $p \mid ab$) اگر $p \mid a$

آنگاه d از D وجود دارد به طوریکه $a = pd$ در اینصورت $p = ab = adp$ چون D دامنه صحیح است و p غیر صفر پس $ad = ۱$ و لذا a یکال است به همین ترتیب می‌توان نشان داد که اگر $p \mid b$ آنگاه b واحد است در نتیجه p یک عضو تحویل ناپذیر D می‌باشد

به عکس فرض کنیم $p \in D$ ، تحویل ناپذیر باشد پس p غیر صفر و غیر واحد است، فرض کنیم $p \mid ab$ که در آن a و b اعضایی از D در اینصورت $c \in D$ وجود دارد به طوریکه $ab = cp$ اگر a واحد باشد، آنگاه $b = pca^{-۱}$ و لذا $p \mid b$ به همین نحو اگر b واحد باشد نتیجه می‌گیریم که $p \mid a$، فرض کنیم هر دو عنصر a و b غیر واحد هستند در این صورت چون D یک UFD است می‌نویسیم

$$a = p_۱ \dots p_m \quad و \quad b = q_۱ \dots q_m$$

که در آن p_i ها و q_i ها در D تحویل ناپذیرند، c نیز واحد نیست، زیرا در غیر اینصورت $P = (c^{-۱}a)b$ حال چون p تحویل ناپذیر و b غیر واحد است پس $c^{-۱}a$ و لذا a باید واحد باشد که متناقض فرض است.

در نتیجه داریم $c = r_۱ \dots r_s$ که در آن r_i ها در D تحویل ناپذیرند. بنابراین ، چون $ab = cp$ داریم

$$p_۱ \dots p_n q_۱ \dots q_m = r_۱ \dots r_s\, p$$

بنابه یکتایی تحزیه در UFD، p وابسته یک P_i یا وابسته یک q_t است.

در این صورت $p \mid p_i$ یا $p \mid q_t$ و لذا $p \mid a$ یا $p \mid b$ پس p اوّل است.

۵ - چون $F[x,y] = (F[x])[y]$ بنابراین $F[x,y]$ یک حوزه صحیح با ایده‌آلهای اصلی است اگروتنها اگر $F[x]$ یک میدان باشد، چون $F[x]$ میدان نیست پس $F[x,y]$ یک PID نیست.

(توجّه : $\langle x,y \rangle$ یک ایده‌آل غیر اصلی $F[x,y]$ است).

۶ ـ فرض کنیم R با ارزیاب f باشد و I ایده‌آل R اگر $I = \{0\}$ آنگاه $I=<0>$ و لذا اصلی است ، بنابراین فرض می‌کنیم که I غیر صفر باشد و مجموعه K را به صورت $K = \{ f(x) \mid x \in I \text{ و } x \neq 0 \}$ در نظر می‌گیریم واضح است که K یک زیر مجموعه غیر تهی از اعداد صحیح نا منفی است، بنابه اصل خوش ترتیبی، K دارای عضو ابتدا یا به عبارتی کوچکترین عضو است.

فرض کنید a مخالف صفر در I باشد بطوریکه به ازای هر عضو غیر صفر b از I $f(a) \leq f(b)$ ادعا می‌کنیم که $I = < a > \subseteq I$ واضح است که $< a >$ حال فرض کنیم $x \in I$ ، چون R با ارزیاب f است پس q و r از R هستند بطوریکه $x = aq + r$ که در آن $r = 0$ یا $f(r) < f(a)$ چون I ایده‌آل است و همچنین x و a متعلّق به I هستند پس $r = (x - aq) \in I$

بنابه انتخاب a ، $f(r) \geq f(a)$ لذا $r = 0$ در نتیجه $x \in < a >$ یعنی ایده‌آل $I = < a >$ اصلی است و حکم ثابت است.

۷ ـ بنا به تمرین قبل هر ایده‌آل R اصلی است پس چون R یک ایده‌آل خودش می‌باشد c متعلّق به R وجود دارد بطوریکه $R = < c >$ چون c متعلّق به R پس e ای در R هست بطوریکه $c = ce$ ادّعا می‌کنیم که e عضویکّه R است. فرض کنیم x متعلّق به R دلخواه باشد چون $R = < c >$ پس y ای در R هست بقسمی که $x = cy$ ، حال داریم:

$$xe = cye = (ce)y = cy = x$$

پس e عضویکّه R است.

۸ ـ α روی F غیر جبری است اگر و تنها اگر چند جمله‌ای غیر صفر $f(x) \in F[x]$ وجود نداشته باشد بطوریکه $f(x) = 0$ یعنی اگر وتنها اگر هیچ چند جمله‌ای غیر صفر $f(x)$ در $F[x]$ وجود نداشته باشد به طوریکه $\varphi_\alpha(f(x)) = 0$

یعنی اگر و تنها اگر $\ker\varphi_\alpha = \{0\}$ پس α روی F غیر جبری است اگر و تنها اگر همریختی $\varphi_\alpha: F[x] \to E$ یک به یک باشد.

۹ ـ فرض کنیم α روی F جبری است در اینصورت

$$[F(\alpha):F] = \deg(\alpha \text{ و } F)$$

و چون $\deg(\alpha$ و $F)$ متناهی است پس $[F(\alpha):F]$ متناهی است

به عکس فرض کنیم $[F(\alpha):F] = n$ متناهی باشد. در اینصورت هر زیر مجموعه با بیش از n عضو در $F(\alpha)$ روی F وابسته خطی است. لذا مجموعه $n+1$ عضوی $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ روی F وابسته خطی است. در نتیجه عناصر c_0 و c_1 و ... و c_n در F وجود دارند به طوریکه حداقل یکی از آنها مخالف صفر است و

$c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0$ یعنی α ریشه چند جمله‌ای غیر صفر

$f(x) = c_0 + c_1 x + \ldots + c_n x^n$ روی F است لذا α روی F جبری می‌باشد.

۱۰ ـ فرض کنیم E توسیع متناهی F است و $[E:F] = n$ فرض کنیم $\{\alpha_1, \ldots, \alpha_n\}$ پایه‌ای برای E روی F باشد. در این صورت برای هر $\alpha \in E$ داریم $c_i \in F$ و $\alpha = c_1\alpha + \ldots + c_n\alpha_n$ پس α در $F(\alpha_1, \ldots, \alpha_n)$ است.

لذا $E = F(\alpha_1, \ldots, \alpha_n)$

۱۱ ـ چون E توسیع متناهی از F است پس E روی F جبری است لذا اگر d مخالف صفر عضوی از D باشد چون $d \in E$ پس چند جمله‌ای می‌نیمال و تحویل‌ناپذیر $p(x)$ از $F[x]$ هست که $p(d) = 0$ فرض کنیم درجه $p(x)$ برابر n باشد پس داریم:

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$a_0 + a_1 d + a_2 d^2 + \ldots + a_n d^n = 0$$

چون a_0 مخالف صفر است پس

$$a_n d^n + \dots a_1 d = - a_0$$

چون $-a_0$ عضوی از F است لذا

$$(-a_0)^{-1} a_n d^n + \dots + (-a_0)^{-1} d = (- a_0)(-a_0)^{-1} = 1$$

$$d[(-a_0)^{-1} a_n d^{n-1} + \dots + (-a_0)^{-1}] = 1$$

پس چون a_0 ، a_i ها و d اعضایی از D هستند لذا

$[(-a_0)^{-1} a_n d^{n-1} + \dots + (-a_0)^{-1}]$ عضوی از D است پس عضو دلخواه d از D وارون دارد لذا D میدان است.

توجّه: a_0 مخالف صفر است زیرا اگر a_0 صفر باشد آنگاه

$$d(a_1 + \dots a_n d^{n-1}) = 0$$

چون $d \neq 0$ پس $a_1 + \dots + a_n d^{n-1} = 0$ و این تناقض با مینیمال بودن $p(x)$ است.

۱۲ - بدیهی است که $F(\sqrt{a} + \sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b})$

$$(\sqrt{a} + \sqrt{b})^2 = a^2 + b^2 + 2\sqrt{ab} \in F(\sqrt{a} + \sqrt{b})$$

$$0 \neq a-b = (\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b})$$

$$1 = (\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b})(a - b)^{-1} \in F(\sqrt{a} + \sqrt{b})$$

$$(\sqrt{a} - \sqrt{b})(a - b)^{-1} \in F(\sqrt{a} + \sqrt{b}) \Rightarrow (\sqrt{a} - \sqrt{b}) \in F(\sqrt{a} + \sqrt{b})$$

$$\begin{cases} (\sqrt{a} - \sqrt{b}) \in F(\sqrt{a} + \sqrt{b}) \\ (\sqrt{a} + \sqrt{b}) \in F(\sqrt{a} + \sqrt{b}) \end{cases}$$

بنابراین:

$$2\sqrt{a} \in F(\sqrt{a} + \sqrt{b}) \Rightarrow \sqrt{a} \in F(\sqrt{a} + \sqrt{b})$$

$$\begin{cases} \sqrt{a} \cdot \sqrt{b} \in F(\sqrt{a}+\sqrt{b}) \\ \sqrt{a} \in F(\sqrt{a}+\sqrt{b}) \end{cases}$$

بنابراین $\sqrt{b} \in F(\sqrt{a}+\sqrt{b})$

پس چون $\sqrt{b}$ و $\sqrt{a}$ اعضایی از $F(\sqrt{a}+\sqrt{b})$ هستند لذا

$$F(\sqrt{a}\ ,\sqrt{b}) \subseteq F(\sqrt{a}+\sqrt{b})$$

پس $F(\sqrt{a}\ ,\sqrt{b}) = F(\sqrt{a}+\sqrt{b})$

۱۳ ـ $\mathbf{Z}[\sqrt{-6}]$ یک حوزه صحیح است ولی UFD نیست زیرا عنصر ۱۰ در آن دارای دو تجزیه است.

$$10 = 2 \times 5$$

$$10 = (2-\sqrt{-6})(2+\sqrt{-6})$$

در تجزیه فوق ۲ و ۵ یکال نیستند

۱۴ ـ فرض کنیم E توسیع متناهی از F باشد و $[E:F] = n$ همچنین α عضوی از E باشد می‌دانیم که مجموعهٔ بابیش از n عضو وابسته خطی است پس مجموعه $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ وابسته است پس $c_0, c_1, \ldots, c_n$ وجود دارند که حداقل یکی از آنها مخالف صفر بوده و $c_0 + c_1\alpha + \ldots c_n\alpha^n = 0$ پس α روی F جبری است، چون α دلخواه بود پس E توسیع جبری است.

(توجّه: c_i ها متعلّق به F هستند)

۱۵ ـ فرض کنید $p \in D$ اوّل باشد. نشان می‌دهیم p در D تحویل ناپذیر است.

فرض کنیم $p = ab$ که در آن $a, b \in D$، چون p اوّل است و $p \mid ab$ پس $p \mid a$ یا $p \mid b$ اگر $p \mid a$، آنگاه $a_1 \in D$ وجود دارد به طوری که $a = pa_1$ در این صورت

$$p = ab = aa_1\, p$$

چون D دامنه صحیح است و $p \neq 0$ پس $aa_1 = 1$ ولذا a واحد است.

به همین نحو می توان نشان داد که اگر $p \mid b$ آنگاه b واحد است. در نتیجه p یک عضو تحویل ناپذیر D می‌باشد

به عکس فرض کنیم p در D تحویل ناپذیر باشد و $p \mid ab$ که در آن a و b از D هستند. ایده‌آل $< p > + < b >$ را در نظر می‌گیریم، چون D یک PID است پس $d \in D$ وجود دارد به طوریکه $< p > + < b > = < d >$

چون $< p > \subseteq < d >$ پس $p = dd_1$ که در آن $d_1 \in D$، چون p در D تحویل ناپذیر است پس d یا d_1 واحد است.

اگر d واحد باشد آنگاه $< d > = D$ ولذا $1 \in < p > + < b >$ یعنی $1 = pr + bs$ که در آن r و s اعضایی از D هستند در نتیجه $a = apr + abs$، چون $p \mid ab$ پس p عبارت $(apr + abs)$ ولذا a را بخش می‌کند اگر d_1 واحد باشد آنگاه $d = pd_1^{-1}$ ولذا $< d > \subseteq < P >$ درنتیجه $< p > = < d >$ ولذا $< P > = < d > + < P >$ در این صورت $< p > \subseteq < b >$ ولذا $P \mid b$ بنابراین حکم ثابت شده است.

فصل ۵

مسائل بدون حل

۱ ـ اگر A و B دو زیرگروه G و $[G:B]$ متناهی باشد ثابت کنید $[G:B] \leq [A:A\cap B]$، همچنین نشان دهید تساوی برقرار است اگر و فقط اگر $G = AB$

۲ ـ H و K زیرگروههایی از گروه متناهی G هستند $|H|>\sqrt{|G|}$ و $|K|>\sqrt{|G|}$ نشان دهید که $|H\cap K| > 1$

۳ ـ اگر H زیرگروهی از گروه G باشد بطوریکه $x^2 \in H$ برای هر $x \in G$ ثابت کنید $\frac{G}{H}$ آبلی است.

۴ ـ ثابت کنید هر گروه دوری نامتناهی با $\mathbf{Z}$ و هر گروه دوری متناهی از مرتبه n با گروه خارج قسمتی $\frac{\mathbf{Z}}{<n>}$ یکریخت است.

۵ ـ گروه دوری نامتناهی چند مولد دارد، گروهی دوری متناهی از مرتبه n چند مولد دارد؟

۶ ـ اگر G یک گروه دوری باشد در هریک از حالتهای زیر مرتبه $\mathrm{Aut}(G)$ را مشخص کنید: (الف) G نامتناهی است. (ب) G متناهی از مرتبه n است.

۷ ـ یک زیرگروه H از گروه G، زیرگروه مشخصه گفته می‌شود اگر برای هر اتومورفیسم f از G، $f(H) \subseteq H$.

ثابت کنید

الف) اگر H یک زیرگروه نرمال G باشد، آنگاه هر زیرگروه مشخصه H چون K در G نرمال است.

ب) اگر G یک گروه آبلی و n یک عدد مثبت ثابت باشد، نشان دهید $H = \{x \in G \mid x^n = e\}$ زیرگروه مشخصه G است. (e عضو همانی G است)

ج) یک مثال از یک زیرگروه نرمال که زیرگروه مشخصه نباشد ارائه دهید.

۸ ـ فرض کنید G یک گروه متناهی با بیش از دو عضو باشد و همچنین وجود داشته باشد عضوی چون x از G بطوریکه $x^2 \neq e$ ثابت کنید G بایستی اتومورفیسم غیر همانی داشته باشد، به عبارت دیگر نشان دهید $Aut(G) \neq \{I\}$ که I تابع همانی است.

۹ ـ اگر G یک گروه از مرتبه p^n باشد که p عدد دیست اوّل، همچنین $N \neq \{e\}$ یک زیرگروه نرمال از G باشد ثابت کنید $N \cap Z(G) \neq \{e\}$ [$Z(G)$ مرکز G است]

۱۰ ـ اگر G یک گروه باشد و $f: G \to G$ باضابطه $f(x) = x^n$ یک اتومورفیسم G باشد نشان دهید برای هر a از G، a^{n-1} متعلّق به $Z(G)$ است.

۱۱ ـ فرض کنیم دو عضو a و b از گروه آبلی و متناهی G به ترتیب از مرتبه‌های m و n باشند، ثابت کنید:

الف) اگر $(m \text{ و } n) = ۱$ آنگاه ab از مرتبه mn است

ب) اگر مرتبه هر عضو G از m نا بیشتر باشد آنگاه $b^m = e$

۱۲ ـ عناصر a و b را از یک گروه طوری پیدا کنید که $o(ab) = ۵$ و $o(a) = ۲$ و $o(b) = ۳$

۱۳ ـ آیا هر گروه آبلی دوری است؟ آیا عکس این مطلب درست است؟ چرا؟

۱۴ ـ فرض کنید G یک گروه دلخواه باشد که حداقل یک زیرگروه از مرتبه n داشته باشد ثابت کنید اشتراک همه زیرگروههای مرتبه n از G، زیرگروه نرمال G است

۱۵ ـ فرض کنید G یک گروه متشکل از اجتماع خانواده‌ای از زیرگروههای نرمال که اشتراک دو بدو آنها فقط زیرگروه همانی باشد، نشان دهید G آبلی است.

۱۶ ـ فرض کنید گروه دوری G از مرتبه m توسط a تولید شود ثابت کنید a^k مولد G است اگر وفقط اگر m و k نسبت به هم اوّل باشند

۱۷ ـ کوچکترین زیرگروه نرمال از گروهی چون G را بطوریکه شامل زیر مجموعه ثابتی مانند X از G باشد، تعیین کنید.

۱۸ ـ نشان دهید مفهوم نرمال بودن از خاصیت تعّدی پیروی نمی‌کند به عبارت دیگر مفهوم نرمال بودن دارای خاصیّت تعّدی نیست.

۱۹ ـ فرض کنید G و H دو گروه دوری متناهی باشند نشان دهید $G\times H$ دوری است اگر وتنها اگر $(|H|$ و $|G|) = 1$ ($\times$ حاصلضرب خارجی است)

۲۰ ـ فرض کنید G یک گروه آبلی و f یک هموморفیسم از G به G باشد بطوریکه $f^2 = f$ ثابت کنید $G = \ker f \otimes \mathrm{Im} f$ (حاصلضرب مستقیم خارجی است)

۲۱ ـ ثابت کنید گروه جمعی اعداد حقیقی $(\mathbf{R})$ دارای زیرگروه ماکسیمال نمی‌باشد

۲۲ ـ ثابت کنید هر زیرگروه، گروه دوری مشخصه است (N زیرگروهی از G را مشخصه گوییم هرگاه $N\varphi \subseteq N \quad \forall \varphi \in \mathrm{Aut}(G)$)

۲۳ ـ ثابت کنید $Z(G)$ و G' زیرگروههای مشخصه گروه G هستند ($Z(G)$ مرکز G و G' زیرگروه مشتق G است)

۲۴ ـ فرض کنید a و b عناصری از یک گروه آبلی و از مراتب m و n باشند ثابت کنید که گروه شامل یک عنصر از مرتبهٔ کوچکترین مضرب مشترک n و m می‌باشد

۲۵ ـ نشان دهید تنها همریختی گروهی از $\mathbf{Q}$ به $\mathbf{Z}$ همریختی صفراست.

۲۶ ـ گروه نامتناهی مثال بزنید که هر عضو آن مرتبه متناهی داشته باشد.

۲۷ ـ ثابت کنید هر حوزه صحیح با تعداد متناهی ایده‌آل میدان است.

۲۸ ـ فرض کنید R یک حلقه و به ازای هر a از R، $(a^2 + a)$ عضوی از مرکز R باشد نشان دهید که R جابجائی است.

۲۹ ـ ثابت کنید که هر گروه از مرتبه p^2q که p و q اعداد اوّل متمایز هستند، ساده نیست.

۳۰ ـ نشان دهید که یک گروه متناهی از مرتبه p^n به ازای هر $1 \leq i \leq n$ یک زیرگروه نرمال H_i دارد که مرتبه H_i برابر p^i بوده و H_i زیرگروه H_{i+1} است.

۳۱ ـ نشان دهید که یک p زیرگروه نرمال از یک گروه متناهی در هر p زیر گروه سیلو خود قرار دارد.

۳۲ ـ ثابت کنید S_n بوسیله ترانهشهای $(1\ 2)$ و ... و $(n-1)$ تولید می‌شود

۳۳ ـ نشان دهید A_5 زیرگروه از مرتبهٔ ۱۵ ندارد.

۳۴ ـ فرض کنید $\mathbf{Z}$ حلقهٔ اعداد صحیح و $\mathbf{Z}[x]$ حلقهٔ چند جمله‌ایهای روی $\mathbf{Z}$ باشد. نشان دهید که $\mathbf{Z}[x]$ یک حوزه صحیح با ایده‌آلهای اصلی نیست.

۳۵ ـ فرض کنید E یک توسیع میدان F و $\alpha \in E$ روی F جبری و از درجه n باشد اگر $m < n$ و $(n, m!) = 1$ آنگاه نشان دهید $F(\alpha) = F(\alpha^m)$

۳۶ ـ فرض کنید G یک گروه آبلی متناهی و H زیرگروهی از آن باشد، بعلاوه، فرض کنید به ازای هر عدد طبیعی مانند n و هر h از H، معادلهٔ $x^n = h$ فقط و فقط وقتی جوابی در G داشته باشد که جوابی در H داشته باشد. ثابت کنید در هر xH عضوی مانند y وجود دارد که مرتبهٔ آن با مرتبه xH مساوی است.

۳۷ـ فرض کنیم R یک حوزه صحیح نامتناهی، یکدار و مجموعه یکالهای R متناهی باشد نشان دهید که:

الف) اشتراک همه ایده‌آلهای ماکسیمال R برابر ایده‌آل صفر است.

ب) مجموعه ایده‌آلهای ماکسیمال R یک مجموعه نامتناهی است.

۳۸ـ نشان دهید که چند جمله‌ای

$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ از $Z[x]$

روی Q تحویل ناپذیر است.

۳۹ـ فرض کنید $f : G \to H$ یک همریختی گروهی باشد و H گروه آبلی، N زیرگروهی از G شامل هسته f باشد، نشان دهید N در G نرمال است.

۴۰ـ نشان دهید که هر حاصلضرب مستقیم خارجی تعداد متناهی گروه حلپذیر خود حلپذیر است.

۴۱ـ نشان دهید که هر زیرگروه از گروهی حلپذیر چون G حلپذیر است.

۴۲ـ اگر R حلقه‌ای یکدار باشد که در آن هر ایده‌آل چپ یک ایده‌آل راست هم باشد آنگاه ثابت کنید که اشتراک تمام ایده‌آلهای اوّل R با مجموعه عناصر پوچ توان مساوی است.

۴۳ـ ثابت کنید در هر PID هر ایده‌آل سره درون یک ایده‌آل ماکزیمال قرار دارد.

۴۴ـ فرض کنید I ایده‌آل $Z[i]$ است، نشان دهید که $\frac{Z[i]}{I}$ حلقه متناهی با ایده‌آلهای اصلی است.

۴۵ـ فرض کنید N یک نرم ضربی روی دامنه صحیح D است بطوریکه $N(\alpha) = 1$ اگر و تنها اگر α در D واحد باشد. نشان دهید هر عضو غیر صفر و غیرواحد در D به عوامل تحویل ناپذیز تجزیه می‌شود.

۴۶ـ فرض کنید E توسیعی از F باشد، b و a اعضایی از E و a روی F غیر جبری ولی روی $F(b)$ جبری است نشان دهید b روی $F(a)$ جبری است.

۴۷ـ فرض کنید E توسیع جبری است. نشان دهید E توسیع متناهی F است اگر و تنها اگر توسیع متناهیاً تولید شده F باشد.

۴۸ـ اگر E توسیع میدان F و α متعلّق به E روی F جبری با درجه فرد باشد نشان دهید که α^2 نیز روی F جبری با درجه فرد است و $F(\alpha) = F(\alpha^2)$ می‌باشد.

۴۹ـ فرض کنید E توسیع $\mathbf{R}$ و $[E : \mathbf{R}]$ متناهی است نشان دهید $E = \mathbf{R}$ یا $E = \mathbf{C}$ ($\mathbf{C}$ اعداد مختلط و $\mathbf{R}$ اعداد حقیقی است).

۵۰ـ اگر G یک گروه از مرتبه ۶۰ باشد ثابت کنید $|Z(G)| \neq 4$

ضمیمه علائم و قرار دادها

وارون x	x^{-1}
هم نهشتی	$\equiv$
مجموعه ماتریسهای $n \times n$ بادرآیه‌های متعلّق به F و دترمینان مخالف صفر	$GL(n,F)$
مجموعه ماتریسهای $n \times n$ بادرآیه های متعلّق به F ودترمینان یک	$SL(n,F)$
تولید شده توسط a	$< a >$
مرتبهٔ a	$o(a)$
a عاد می‌کند b را	$a \mid b$
جایگشتهای زوج S_n	A_n
جایگشتهای فرد S_n	B_n
مرکز G	$Z(G) = \{ x \in G \mid xg = gx \ \ \forall g \in G \}$
تعداد همرده‌های H در G یا اندیس H در G	$[G : H]$
گروه جایگشتهای روی n حرف	S_n
هسته φ	$\ker\varphi$

ایزمورف یا یکریخت	$\cong$
گروه خودریختیهای G یا گروه اتومورفیسهای G	$Aut(G)$
گروه خودریختیهای داخلی G	$Inn\ (G)$
حوزه صحیح با ایده‌آلهای اصلی	PID
حوزه تجزیهٔ یکتا	UFD

هم مجموعه = همدسته = همرده

بهنجار = نرمال

خودسانی = خودریختی = اتومورفیسم

همسانی = همریختی = هممورفیسم

ترانهش = دور به طول ۲

سیکل = دور

معکوس = وارون

همانی = خنثی

ماکسیمال = ماکزیمال

Problems in Algebra

by

Nasser Azizi

قیمت: ۲۰۰۰ ریال