مدرسان شریف

فصل اول

«مقدمات و پیش‌نیازها»

در فصل حاضر مقدمات و پیش‌نیازهای لازم، برای مطالعه مبانی جبر را می‌آموزیم. در ابتدا به مباحثی اشاره می‌کنیم که قطعاً خواننده‌ی این کتاب آن‌ها را در درس مبانی علوم آموخته است. سپس مفاهیمی را ارائه می‌دهیم که پایه‌ی درس مبانی جبر است. در این فصل برای یادآوری به‌طور مختصر مباحث مورد نیاز را مرور می‌کنیم، مباحثی از قبیل اجتماع، اشتراک، تابع، حاصل‌ضرب دکارتی و اصل انتخاب و در فصل‌های آتی خواهیم دید این مطالب، مورد استفاده قرار خواهند گرفت. بحث این فصل را با مفاهیم اجتماع و اشتراک آغاز می‌کنیم و فرض را بر این می‌داریم که خواننده، با مفاهیم مجموعه، زیرمجموعه و انواع سورها آشنایی کامل دارد.

درسنامه (۱): مجموعه‌ها

اجتماع و اشتراک

❖ **تعریف۱:** فرض کنید A و B دو مجموعه باشند. اجتماع دو مجموعه A و B به‌صورت $A\cup B$ نشان داده می‌شود و عبارت است از مجموعه‌ی تمام عضوهایی که حداقل به یکی از دو مجموعه‌ی A و B متعلق باشد، یعنی $x\in A\cup B$ اگر و تنها اگر $x\in A \vee x\in B$. اشتراک دو مجموعه A و B به‌صورت $A\cap B$ نشان داده می‌شود و عبارت است از مجموعه‌ی تمام عضوهایی که هم متعلق به A است و هم متعلق به B، یعنی $x\in A\cap B$ اگر و تنها اگر $x\in A \wedge x\in B$.

مفاهیم اجتماع و اشتراک برای تعداد بیشماری مجموعه نیز قابل تعمیم است. در واقع می‌توانیم آن‌ها را چنین تعمیم دهیم:

❖ **تعریف۲:** فرض کنید $\{A_i\}_{i\in I}$ خانواده‌ای از مجموعه‌ها و I مجموعه اندیس‌گذار باشد. اجتماع و اشتراک خانواده $\{A_i\}_{i\in I}$ به صورت زیر تعریف می‌شود:

$$\bigcup_{i\in I} A_i = \{x \mid x\in A_i \text{ ، به ازای } i\in I \text{ ای}\}$$

$$\bigcap_{i\in I} A_i = \{x \mid x\in A_i \text{ ، } i\in I \text{ به ازای هر}\}$$

در قضیه‌ی بعدی بعضی از خصوصیات مجموعه‌ها را بیان می‌کنیم.

قضیه۱: فرض کنید X یک مجموعه و A، B و C زیرمجموعه‌هایی از X باشند. در این صورت:

۱) $A\cup\varnothing = A$ و $A\cap X = A$ (خصوصیت یکه‌ها)

۲) $A\cup A = A$ و $A\cap A = A$ (خصوصیت خودتوانی)

۳) $A\cup B = B\cup A$ و $A\cap B = B\cap A$ (خصوصیت جابه‌جایی)

۴) $A\cup(B\cup C) = (A\cup B)\cup C$ و $A\cap(B\cap C) = (A\cap B)\cap C$ (خصوصیت شرکت‌پذیری)

۵) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$ و $A\cap(B\cup C) = (A\cap C)\cup(A\cap C)$ (خصوصیت پخش‌پذیری)

۶) اگر $A\subseteq B$، آن‌گاه $A\cup B = B$ و $A\cap B = A$

❖ **تعریف۳:** فرض کنید A یک مجموعه باشد. مجموعه‌ی تمام زیرمجموعه‌های A را مجموعه توانی A می‌نامند و با $P(A)$ نمایش می‌دهند. به‌عنوان مثال، مجموعه‌ی تک عضوی $\{a\}$ را در نظر بگیرید. $\{a\}$ دارای زیرمجموعه‌های $\varnothing$ و $\{a\}$ است. لذا $P(\{a\}) = \{\{a\},\varnothing\}$ مجموعه توانی $\{a\}$ است و یا مجموعه توانی $\{a,b\}$ عبارت است از: $P(\{a,b\}) = \{\varnothing,\{a\},\{b\},\{a,b\}\}$

تا این‌جا چند مطلب بسیار مختصر از نظریه‌ی مجموعه‌ها را مرور کردیم. مبحث آشنای دیگری در نظریه‌ی مجموعه‌ها، متمم‌گیری می‌باشد که مشابه با عمل تفریق در حساب است.

❖ **تعریف۴:** فرض کنید A و B دو مجموعه باشند، متمم B نسبت به A که به‌صورت $A-B$ نمایش داده می‌شود، برابر است با $A-B=\{x\in A \mid x\notin B\}$،

در این تعریف توجه داریم که شرط $B \subseteq A$ لازم نیست. با توجه به متمم دو مجموعه، تعریف دیگری تحت عنوان تفاضل متقارن موجود است. فرض کنید X مجموعه‌ی توانی یک مجموعه‌ی ناتهی U باشد، یعنی $X = P(U)$. در X عمل Δ تفاضل متقارن نامیده می‌شود و به‌صورت زیر تعریف می‌شود:

$$A \Delta B = (A - B) \bigcup (B - A) \; ; \; \forall A, B \in X$$

حاصلضرب دکارتی

❖ **تعریف۵:** فرض کنید A و B دو مجموعه باشند. مجموعه‌ی تمام زوج‌های مرتب (x, y) که در آن $x \in A$ و $y \in B$، حاصل‌ضرب دکارتی A و B نامیده می‌شود. به‌عبارتی $A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$

a مولفه‌ی اول و b مولفه‌ی دوم زوج مرتب (a, b) است.

به‌عنوان مثال، فرض کنید $A = \{۱, ۲\}$ و $B = \{a, b\}$. در این صورت حاصل‌ضرب دکارتی $A \times B$ و $B \times A$ به‌صورت زیر است:

$$A \times B = \{(۱, a), (۱, b), (۲, a), (۲, b)\}$$

$$B \times A = \{(a, ۱), (a, ۲), (b, ۱), (b, ۲)\}$$

با توجه به مثال متوجه می‌شویم که $A \times B \neq B \times A$.

تـابع

❖ **تعریف۶:** فرض کنید A و B دو مجموعه باشند. تابع یا نگاشت f به‌صورت $f : A \to B$ تعریف می‌شود و گویای این است که به هر عضو $a \in A$ یک عضو $b \in B$ مربوط می‌شود. b مقدار تابع f در a یا نقش a نامیده شده و به‌صورت $f(a)$ نشان داده می‌شود. مجموعه‌ی A را دامنه تابع و B را برد یا هم‌دامنه می‌نامند و به ترتیب با نمادهای $Dom(f)$ و $Im(f)$ نشان می‌دهند. اثر تابع f بر عضوهای A به‌فرم $a \mapsto f(a)$ نمایش داده می‌شود.

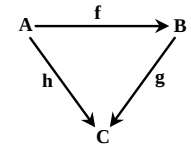
هرگاه A یک مجموعه باشد، تابع ۱_A از A بتوی A به‌صورت $۱_A(x) = x$ تعریف می‌شود و تابع همانی نامیده می‌شود.

مفهوم تابع، مفهومی است که بدون شک هر دانشجوی ریاضی با آن آشنایی دارد. دراین بخش، مفاهیم مرتبط با تابع را یادآوری می‌کنیم و در بین مفاهیم مربوط به تابع، به تعریفی جدید نیز اشاره خواهیم کرد.

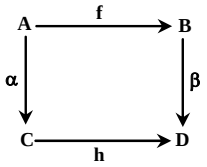
❖ **تعریف۷:** فرض کنید $f : A \to B$ یک تابع باشد و $S \subset A$. اگر تابع f از S به B به‌صورت به ازای هر $a \in S$، $a \mapsto f(a)$ تعریف شود، آن‌گاه این تابع، تحدید f به S نامیده شده و به فرم $f|_S : S \to B$ نشان داده می‌شود.

❖ **تعریف۸:** فرض کنید $f : A \to B$ و $g : B \to C$ دو تابع باشند. ترکیب دو تابع f و g به‌صورت $gof : A \to C$ نشان داده می‌شود و هر عضو از a به $g(f(a))$ برده می‌شود، به‌عبارتی $a \mapsto g(f(a))$. نماد gof گاهی فقط به‌صورت gf نمایش داده می‌شود. حال اگر تابع $h : C \to D$ به این جمع اضافه شود به‌راحتی می‌توان دید $h(gf) = (hg)f$. پس ترکیب توابع خاصیت شرکت‌پذیری دارد.

اکنون می‌خواهیم با توجه به تعریف ترکیب توابع با یک تعریف و نمادگزاری جدید آشنا شویم.



❖ **تعریف۹:** فرض کنید $f : A \to B$، $g : B \to C$ و $h : C \to D$ سه تابع باشند، در این صورت ترسیم نمودار روبرو به این معنی است که $gf = h$.



در چنین حالتی می‌گوییم نمودار، جابه‌جایی (تعویض‌پذیر) است. به‌همین ترتیب نمودار روبرو.

تعویض‌پذیر است هرگاه $\beta f = h\alpha$. بنابراین چنین نمودارهایی تعویض‌پذیر هستند، هرگاه هر مثلث و یا مربع آن تعویض‌پذیر باشد. در ادامه از چنین نمودارهایی استفاده خواهیم کرد. حال به سراغ مباحث آشنای دیگری از توابع می‌رویم.

❖ **تعریف۱۰:** فرض کنید $f : A \to B$ یک تابع باشد. اگر $S \subset A$، آن‌گاه نقش S تحت f به‌صورت مجموعه‌ی $f(S) = \{b \in B \mid b = f(a); \text{ به ازای } a \in S \text{ای}\}$ تعریف می‌شود. مجموعه‌ی $f(A)$ را نقش f می‌نامند و با $Im(f)$ نمایش می‌دهند. حال اگر $T \subset B$، آن‌گاه نقش معکوس T تحت f با مجموعه‌ی $f^{-۱}(T) = \{a \in A \mid f(a) \in T\}$ نشان داده می‌شود.

مثال۱: فرض کنید $f : A \to B$ یک تابع باشد. در این صورت:

۱) اگر $S \subset A$، آن‌گاه $S \subset f^{-۱}(f(S))$

۲) اگر $T \subset B$، آن‌گاه $f(f^{-۱}(T)) \subset T$

☑ **پاسخ:** ۱) فرض کنید $S \subset A$ و عضو $x \in S$ دلخواه باشد. در این صورت $f(x) \in f(S)$، لذا $x \in f^{-۱}(f(S))$. بنابراین $S \subset f^{-۱}(f(S))$.

۲) فرض کنید $T \subset B$ و عضو $x \in f(f^{-۱}(T))$ دلخواه باشد. لذا عضو $y \in f^{-۱}(T)$ موجود است به طوری که $x = f(y)$. پس $x \in T$. بنابراین $f(f^{-۱}(T)) \subset T$.

❖ **تعریف۱۱:** فرض کنید $f:A\to B$ یک تابع باشد. تابع f را یک به یک می‌نامند، هرگاه به ازای هر $a,b\in A$، از تساوی $f(a)=f(b)$ بتوان نتیجه گرفت $a=b$. همچنین تابع f را پوشا می‌نامند، هرگاه به ازای هر $b\in B$ عضو $a\in A$ موجود باشد به طوری که $f(a)=b$. اگر تابع f هم یک به یک و هم پوشا باشد، آن‌گاه f تابع دوسویی یا تناظر یک به یک نامیده می‌شود و به صورت $A\cong B$ نشان داده می‌شود.

توابع یک به یک، پوشا و دوسویی در مبانی جبر دارای اهمیت و کاربردهای بسیاری هستند. در ادامه چند قضیه‌ی کاربردی را بدون اثبات بیان می‌کنیم.

قضیه۲: فرض کنید $f:A\to B$ و $g:B\to C$ دو تابع باشند. در این صورت:

۱) اگر f و g توابع یک به یک باشند، آن‌گاه gf نیز یک به یک است.

۲) اگر f و g توابع پوشا باشند، آن‌گاه gf نیز پوشا است.

۳) اگر gf یک به یک باشد، آن‌گاه f یک به یک است.

۴) اگر gf پوشا باشد، آن‌گاه g پوشا است.

قضیه۳: فرض کنید $f:A\to B$ یک تابع باشد. در این صورت:

۱) f یک به یک است اگر و تنها اگر نگاشت $g:B\to A$ موجود باشد به طوری که $gf=1_A$.

۲) f پوشا است اگر و تنها اگر نگاشت $h:B\to A$ موجود باشد به طوری که $fh=1_B$.

از این قضیه می‌توانیم به یک تعریف بسیار مهم دست یابیم.

❖ **تعریف۱۲:** نگاشت g در قضیه‌ی قبل معکوس چپ و h معکوس راست f نام دارد، هرگاه نگاشت $f:A\to B$ هم معکوس چپ g و هم معکوس راست h داشته باشد، آن‌گاه $g=g.1_B=g(fh)=(gf)h=1_A.h=h$، لذا $g=h$ را معکوس دوطرفه f می‌نامند. به‌راحتی می‌توان بررسی کرد معکوس دوطرفه یک تابع در صورت وجود منحصربه فرد است. معکوس دوطرفه تابع f با f^{-1} نشان داده می‌شود.

نتیجه: هرگاه A یک مجموعه و $f:A\to B$ یک تابع باشد، آن‌گاه f دارای معکوس دوطرفه است اگر و تنها اگر f یک تابع دوسویی باشد.

قضیه۴: فرض کنید A یک مجموعه‌ی m عضوی و B یک مجموعه‌ی n عضوی باشد. در این صورت تعداد توابع از A به B برابر است با n^m.

حاصلضرب

فرض کنید A_1 و A_2 دو مجموعه باشند. حاصل ضرب دکارتی $A_1\times A_2$ را در نظر بگیرید. هر عضو $A_1\times A_2$ زوج مرتبی مانند (a_1,a_2) است که در آن $a_1\in A_1$ و $a_2\in A_2$. بنابراین زوج مرتب (a_1,a_2) تابعی است مانند $f:\{1,2\}\to A_1\cup A_2$ که در آن $f(1)=a_1$ و $f(2)=a_2$. برعکس، هر تابع $f:\{1,2\}\to A_1\cup A_2$ با خاصیت $f(1)\in A_1$ و $f(2)\in A_2$، عضو $(a_1,a_2)=(f(1),f(2))$ از $A_1\times A_2$ را به وجود می‌آورد. لذا یک تناظر یک به یک بین مجموعه‌ی تمام توابع از این نوع و مجموعه‌ی $A_1\times A_2$ موجود است. مباحث ارائه شده، ما را به تعمیم مفهوم حاصل‌ضرب دکارتی هدایت می‌کند.

❖ **تعریف۱۳:** فرض کنید $\{A_i\mid i\in I\}$ خانواده‌ای از مجموعه‌ها و I خانواده‌ی اندیس‌گذار باشد. حاصل‌ضرب دکارتی مجموعه‌های A_i، مجموعه‌ی تمام توابع $f:I\to\bigcup_{i\in I}A_i$ است به طوری که به ازای هر $i\in I$، $f(i)\in A_i$. این حاصل‌ضرب را با $\prod_{i\in I}A_i$ نمایش می‌دهیم. توجه داشته باشید هرگاه $I=\{1,2,...,n\}$، آن‌گاه حاصل‌ضرب $\prod_{i\in I}A_i$ معمولاً به صورت $A_1\times A_2\times...\times A_n$ نشان داده می‌شود و عناصر آن به‌صورت n تایی مرتب $(a_1,a_2,...,a_n)$ است که در آن به ازای هر $i=1,...,n$، $a_i\in A_i$. همانند آنچه قبل از تعریف برای حالت $I=\{1,2\}$ مشاهده کردید.

تذکر۱: اگر به ازای j ای، $A_j=\varnothing$، آن‌گاه تابعی مانند $f:I\to\bigcup A_i$ نمی‌تواند موجود باشد که $f(j)\in A_j$، بنابراین $\prod_{i\in I}A_i=\varnothing$.

اگر $\{A_i\mid i\in I\}$ و $\{B_i\mid i\in I\}$ خانواده‌هایی از مجموعه‌ها باشند به طوری که به ازای هر i، $B_i\subset A_i$، آن‌گاه هر تابع $I\to\bigcup_{i\in I}B_i$ را می‌توان به‌صورت $I\to\bigcup A_i$ نیز در نظر گرفت. لذا $\prod_{i\in I}B_i$ زیرمجموعه‌ای از $\prod_{i\in I}A_i$ است.

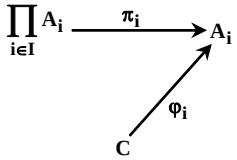
مجدداً حاصل‌ضرب دکارتی A و B را در نظر بگیرید. می‌توانیم توابع $\pi_A:A\times B\to A$ و $\pi_B:A\times B\to B$ را به ترتیب با ضابطه‌های $(a,b)\mapsto a$ و $(a,b)\mapsto b$ تعریف کنیم. حال اگر مجموعه‌های بیشتری داشته باشیم. تعریف چگونه خواهد بود؟ برای پاسخ به این سوال، تعریف تعمیم یافته بعدی را مطالعه می‌کنیم.

❖ **تعریف۱۴:** فرض کنید $\prod_{i\in I}A_i$ حاصل‌ضرب دکارتی باشد. به ازای هر $k\in I$، نگاشت $\pi_k:\prod_{i\in I}A_i\to A_k$ به‌صورت $f\mapsto f(k)$ تعریف می‌شود. π_k **نگاشت تصویری** یا **تصویر کانونی** حاصل‌ضرب روی مولفه‌ی k ام نامیده می‌شود. هرگاه هر A ناتهی باشد، آن‌گاه هر π_k پوشا است. ضابطه π_k با نماد $\{a_i\}\to a_k$ نیز نشان داده می‌شود.

اکنون یکی از مهم‌ترین قضایای این فصل را مطالعه می‌کنیم. ابزار مورد استفاده در این قضیه حاصل‌ضرب $\prod_{i\in I}A_i$ و نگاشت تصویری π_k است. این قضیه، را قضیه‌ی حاصل‌ضرب $\prod_{i\in I}A_i$ به‌وسیله‌ی خاصیت نگاشت عمومی می‌نامیم. این قضیه‌ی در فصل رسته‌ها بسیار مورد استفاده قرار می‌گیرد.

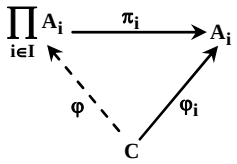
قضیه۵: (حاصل ضرب $\prod_{i\in I}A_i$ به‌وسیله خاصیت نگاشت عمومی) فرض کنید $\{A_i \mid i\in I\}$ خانواده‌ای از مجموعه‌ها و I خانواده‌ی اندیس‌گذار باشد. مجموعه‌ی D با خانواده‌ی نگاشت‌های $\{\pi_i : D\to A_i \mid i\in I\}$ موجود است به طوری که به ازای هر مجموعه‌ی C و هر خانواده از نگاشت‌های $\{\varphi_i : C\to A_i \mid i\in I\}$ نگاشت منحصر به فرد $\varphi : C\to D$ موجود باشد به‌طوری که به ازای هر $i\in I$، $\pi_i o\varphi=\varphi_i$. همچنین D موجود در این خاصیت، منحصر به فرد است.

اثبات: ابتدا نشان می‌دهیم D با شرایط تعریف شده موجود است. فرض کنید $D=\prod_{i\in I}A_i$ و $\pi_i:\prod_{i\in I}A_i\to A_i$ یک نگاشت تصویری باشد و همچنین فرض کنید مجموعه C و خانواده‌ی نگاشت‌های $\{\varphi_i : C\to A_i \mid i\in I\}$ موجود باشند، بنابراین نمودار زیر را داریم:



(۱)

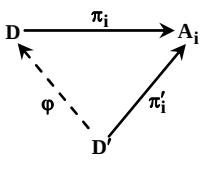
حال لازم است نگاشت φ را طوری پیدا کنیم که نمودار (۱) تعویض‌پذیر باشد، یعنی نمودار:



موجود باشد به طوری که به ازای هر $i\in I$، $\pi_i o\varphi=\varphi_i$. نگاشت $\varphi:\prod_{i\in I}A_i\to C$ را با ضابطه‌ی $\varphi(x)=(\varphi_i(x))_{i\in I}$ تعریف می‌کنیم. بنابراین به ازای هر $i\in I$ و $x\in C$ داریم $(\pi_i o\varphi)(x)=\pi_i(\varphi(x))=\pi_i((\varphi_i(x))_{i\in I}=\varphi_i(x)$، پس $\pi_i o\varphi=\varphi_i$. لذا φ با شرایط مورد نظر ما موجود است. حال نشان می‌دهیم φ منحصر به فرد است. برای این منظور فرض کنید نگاشت $\varphi'.C\to\prod_{i\in I}A_i$ موجود است به طوری که $\pi_i o\varphi'=\varphi'_i$. در این صورت به ازای هر $x\in C$ داریم:

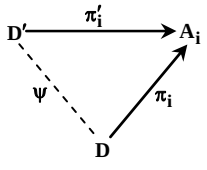
$$\varphi'(x)=((\varphi'(x))_i)_{i\in I}=(\varphi_i(x))_{i\in I}=\varphi(x)$$

بنابراین $\varphi=\varphi'$ و این یعنی φ منحصر به فرد است. در ادامه و برای تکمیل اثبات کافی است نشان دهیم D منحصر به فرد است. برای رسیدن به این هدف کافی است نشان دهیم اگر D' مجموعه‌ی دیگری با این ویژگی باشد، آن‌گاه $D\cong D'$. پس فرض کنید D' همراه با خانواده‌ی نگاشت‌های $\{\pi_i : D'\to A_i \mid i\in I\}$ موجود بوده و در شرایط قضیه‌ی نیز صادق است. چون D در شرایط قضیه‌ی صدق می‌کند پس نگاشت منحصر به فرد $\varphi : D'\to D$ موجود است به طوری که به ازای $i\in I$ داریم $\pi_i o\varphi=\pi'_i$، از طرفی چون D' هم در شرایط قضیه‌ی صدق می‌کند پس نگاشت منحصربه فرد $\psi : D\to D'$ موجود است به طوری که به ازای هر $i\in I$، $\pi'_i o\psi=\pi_i$. بنابراین نمودارهای زیر حاصل می‌شود:



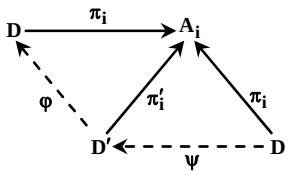
(۲)

و



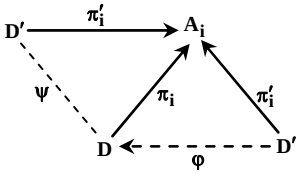
(۳)

حال با در کنار هم قرار دادن نمودارهای (۲) و (۳) خواهیم داشت:



(۴)

و



(۵)

از نمودار (۴) نتیجه روبه‌رو به‌دست می‌آید: $\pi_i o(\varphi o\psi)=(\pi_i o\varphi)o\psi=\pi'_i o\psi=\pi_i \Rightarrow \varphi o\psi=1_D$

و از نمودار (۵) نیز نتیجه روبه‌رو به‌دست می‌آید: $\pi'_i o(\psi o\varphi)=(\pi'_i o\psi)o\varphi=\pi_i o\varphi=\pi'_i \Rightarrow \psi o\varphi=1_{D'}$

پس با به‌دست آمدن نگاشت‌های همانی $1_D : D\to D$ و $1_{D'} : D'\to D'$ نتیجه می‌شود $D\cong D'$ و این یعنی D منحصربه فرد است. بنابراین در

این‌جا اثبات کامل می‌شود.

اصل انتخاب، ترتیب و لم‌زرن

فرض کنید که وارد یک مغازه میوه‌فروشی شده‌اید که تعدادی سبد میوه دارد. اگر از شما خواسته شود از هر سبد یک میوه انتخاب کنید برای شما کار مشکلی نیست. اما سوال زیر که تقریباً شباهت با انتخاب میوه در میوه‌فروشی دارد، در نگاه اول ساده به نظر می‌رسد ولی در عمل دارای پیچیدگی خاصی است. سوال به این صورت مطرح می‌شود، اگر یک مجموعه ناتهی S که عناصرش مجموعه‌های غیرتهی مجزای S_α هستند داده شده باشد، آیا مجموعه‌ای مانند R وجود دارد که عضوهایش از عناصر x_α متعلق به هر S_α تشکیل شده باشد؟ مشکل اصلی وقتی پیش می‌آید که S نامتناهی باشد! برای پاسخ به این سوال تنها راه‌حل ممکن استفاده از اصل موضوعی است که به اصل انتخاب معروف است. اصل انتخاب می‌گوید برای هر مجموعه‌ی ناتهی S که عضوهایش مجموعه‌های ناتهی باشد، تابع $f:S\to\bigcup_{A\in S}A$ به نام تابع انتخاب وجود دارد به طوری که به ازای هر $A\in S$ داشته باشیم $f(A)\in A$.

استفاده از اصل انتخاب برای پاسخ به بسیاری از سوالات کاربرد دارد. در ادامه با مسائلی از این قبیل که جایگاه نو و ویژه‌ای در جبر دارند آشنا می‌شویم.

❖ **تعریف۱۵:** فرض کنید A یک مجموعه‌ی ناتهی باشد. رابطه‌ی «$\le$» روی مجموعه‌ی A رابطه‌ی ترتیب جزئی نامیده می‌شود، هرگاه «$\le$» روی A انعکاسی، متعدی و پادمتقارن باشد. یعنی:

۱) به ازای هر $a\in A$، $a\le a$ (انعکاسی)

۲) به ازای هر $a,b,c\in A$، اگر $a\le b$ و $b\le c$، آن‌گاه $a\le c$ (متعدی)

۳) به ازای هر $a,b\in A$ اگر $a\le b$ و $b\le a$، آن‌گاه $a=b$ (پادمتقارن)

یک مجموعه که رابطه ترتیب جزئی روی آن برقرار باشد مجموعه‌ی جزئاً مرتب نامیده می‌شود و به‌صورت زوج مرتب $(A,\le)$ نشان داده می‌شود که در آن A یک مجموعه و «$\le$» یک رابطه‌ی ترتیب جزئی روی A است.

❖ **تعریف۱۶:** رابطه‌ی ترتیب کلی «$\le$» روی مجموعه‌ی A یک رابطه‌ی ترتیب جزئی است، که به ازای هر دو عضو $a,b\in A$، $a\le b$ یا $b\le a$. یک مجموعه‌ی کلاً مرتب یک زوج مرتب $(A,\le)$ است که در آن A یک مجموعه و «$\le$» یک رابطه‌ی ترتیب کلی است.

✍ **مثال۲: فرض کنید F مجموعه‌ی تمام توابع $f:\mathbf{R}\to\mathbf{R}$ باشد و R به صورت زیر تعریف شود:**

$$\mathbf{R}=\{(f,g)\in F\times F \mid f(x)\le g(x);\forall x\in R\}$$

ثابت کنید (F,R) یک مجموعه‌ی جزئاً مرتب است.

☑ **پاسخ:** کافی است نشان دهیم مجموعه‌ی F یک مجموعه‌ی مرتب جزئی است، یعنی دارای خصوصیات انعکاسی، تعدی و پادمتقارن است. فرض کنید $f\in F$. برای هر $x\in R$ داریم $f(x)\le f(x)$، پس F انعکاسی است. حال فرض کنید $f,g,h\in F$ به طوری که $(f,g),(g,h)\in F\times F$. در این صورت برای هر $x\in R$ داریم $g(x)\le h(x)$ و $f(x)\le g(x)$، پس $f(x)\le h(x)$. لذا خصوصیت تعدی نیز برقرار است. حال عضو $(f,g)\in F\times F$ را در نظر بگیرید. اگر به ازای هر $x\in R$، $f(x)\le g(x)$ و $g(x)\le f(x)$، آن‌گاه $f(x)=g(x)$ و این یعنی F پادمتقارن می‌باشد. بنابراین (F,R) یک مجموعه‌ی جزئاً مرتب است.

◆ ◆ ◆ ◆

اینک آماده‌ایم با استفاده از مفهوم جزئاً مرتب تعاریف دیگری را بیان کنیم.

❖ **تعریف۱۷:** فرض کنید $(A,\le)$ یک مجموعه‌ی جزئاً مرتب و مجموعه‌ی B زیرمجموعه‌ای از A باشد. در این صورت:

۱) عضو $u\in A$ کران بالای B نامیده می‌شود، هرگاه به ازای هر $b\in B$، $b\le u$.

۲) عضو $u_\circ$ کوچکترین کران بالای B نامیده می‌شود، هرگاه به ازای هر کران بالای B مانند u داشته باشیم $u_\circ\le u$، کوچکترین کران بالای B با $\sup B$ نشان داده می‌شود.

۳) عضو $e\in A$ ماکسیمال نامیده می‌شود، هرگاه به ازای هر $a\in A$ اگر $a\ge e$، آن‌گاه $a=e$.

❖ **تعریف۱۸:** فرض کنید $(A,\le)$ یک مجموعه‌ی جزئاً مرتب و B زیرمجموعه‌ای از A باشد. در این صورت:

۱) عضو $v\in A$ کران پایین B نامیده می‌شود، هرگاه به ازای هر $b\in B$، $v\le b$.

۲) عضو $v_\circ$ بزرگترین کران پایین B نامیده می‌شود، هرگاه به ازای هر کران پایین B مانند v داشته باشیم $v_\circ\ge v$، بزرگترین کران پایین B با $\inf B$ نشان داده می‌شود.

فصل دوم

«گروه‌ها»

در فصل قبل با مفهوم دستگاه جامع جبری و نوع جبر آشنا شدیم. همان‌طور که دیدیم مثلاً دستگاه $(\mathbb{Z},\cdot)$ دستگاهی از نوع $\tau=(2)$ است. در این فصل قصد داریم دستگاه جبری از نوع $\tau=(2)$ را بررسی کرده و گروه را که یکی از مهم‌ترین دستگاه‌ها از این نوع است، معرفی کنیم.

درسنامه (۱): گروه

❖ **تعریف۱:** گروهواره $(G,*)$ را یک **نیم‌گروه** می‌نامیم هرگاه $*$ روی G خاصیت شرکت‌پذیری داشته باشد.

❖ **تعریف۲:** نیم‌گروه $(G,*)$ را یک **تکوار یا مونوئید** می‌نامیم هرگاه عضو خنثی یا همانی مانند e در G موجود باشد به طوری که به ازای هر عضو a در G داشته باشیم $a*e=e*a=a$.

توجه داشته باشید که عضو همانی را اغلب با e نمایش می‌دهیم.

به عنوان مثال $(\mathbb{N},+)$ یک نیم‌گروه می‌باشد، چون عمل جمع روی $\mathbb{N}$ خاصیت شرکت‌پذیری دارد، به عبارت دیگر به ازای هر $\mathbf{a,b,c\in\mathbb{N}}$، $a+(b+c)=(a+b)+c$. هم‌چنین $(\mathbb{N},\cdot)$ یک تکوار می‌باشد. چون عمل ضرب روی $\mathbb{N}$ خاصیت شرکت‌پذیری دارد، یعنی به ازای هر $\mathbf{a,b,c\in\mathbb{N}}$، $\mathbf{a(bc)=(ab)c}$. از طرفی ۱ عضو همانی ضرب در مجموعه‌ی $\mathbb{N}$ است.

مثال۱: مجموعه‌ی $\mathbb{R}$ با عمل $\mathbf{a*b=2(a+b)}$ نه نیم‌گروه است نه مونوئید، زیرا به ازای هر $\mathbf{a,b,c\in\mathbb{R}}$، خواهیم داشت:

$$\left.\begin{aligned}(a*b)*c&=(2(a+b))*c=2(2(a+b)+c)=4a+4b+2c\\ a*(b*c)&=2(a+(b*c))=2(a+2(b+c))=2a+4b+4c\end{aligned}\right\}\Rightarrow (a*b)*c\neq a*(b*c)\Rightarrow \mathbf{(\mathbb{R},*)}\ \text{خاصیت شرکت‌پذیری ندارد}$$

❖ **تعریف۳:** تکوار $(G,*)$ را یک **گروه** می‌نامیم هرگاه هر عضو G دارای وارون باشد، به عبارت دیگر به ازای هر عضو a در G، عضوی مانند b در G وجود داشته باشد به طوری که $a*b=b*a=e$.

معمولاً وارون عضو a را با a^{-1} نمایش می‌دهیم. البته وقتی گروه جمعی باشد، یعنی عمل جمع در نظر گرفته شود، وارون عضو a با $-a$ نمایش داده می‌شود. برای مثال $(\mathbb{Z},+)$ گروه می‌باشد، زیرا صفر عضو همانی آن است و هر عضو $a\in\mathbb{Z}$ دارای معکوس $-a$ می‌باشد. اما $(\mathbb{Z},\cdot)$ گروه نیست. زیرا اگرچه دارای عضو همانی ۱ است اما اعضای آن نسبت به عمل ضرب وارون‌پذیر نیستند، مثلاً عدد۲ در $\mathbb{Z}$ معکوس ندارد، چون اگر b معکوس ۲ باشد، آن‌گاه باید داشته باشیم $2\times b=1$ یعنی $b=\frac{1}{2}$، اما $\frac{1}{2}\notin\mathbb{Z}$. هم‌چنین $(\mathbb{N},+)$ گروه نیست، زیرا عضو همانی جمعی ندارد. $(\mathbb{N},\cdot)$ نیز گروه نیست زیرا اعضای $\mathbb{N}$ نسبت به ضرب وارون‌پذیر نیستند مثلاً عدد ۳ در $\mathbb{N}$ معکوس‌پذیر نیست، زیرا اگر b معکوس ۳ باشد، آن‌گاه باید داشته باشیم $3\times b=1$ یعنی $b=\frac{1}{3}$، اما $\frac{1}{3}\notin\mathbb{N}$.

مثال۲: به ازای هر دو عدد گویای $\mathbf{a,b\in\mathbb{Q}}$، تعریف می‌کنیم $\mathbf{a*b=\frac{ab}{20}}$. در این‌صورت وارون ۷ در این نیم‌گروه برابر است با: (سراسری ۹۱)

۱) $\frac{200}{7}$ ۲) $\frac{400}{7}$ ۳) $\frac{400}{14}$ ۴) $\frac{7}{400}$

☑ **پاسخ:** گزینه «۲» ابتدا عضو همانی نیم‌گروه را محاسبه می‌کنیم، یعنی عضوی چون b به طوری که به ازای هر $a\neq0\in(\mathbb{Q},*)$، $a*b=a$ بنابراین:

$$\frac{ab}{20}=a\Rightarrow b=20$$

حال به محاسبه وارون یک عنصر می‌پردازیم. (فرض می‌کنیم a ناصفر باشد. به دنبال b ای می‌گردیم که $b*a=۲۰$. بنابراین داریم:

$$\frac{ab}{۲۰}=۲۰\Rightarrow b=\frac{۴۰۰}{a}$$

پس وارون a برابر با $\frac{۴۰۰}{a}$ است و باید وارون ۷ برابر $\frac{۴۰۰}{۷}$ گردد.

مثال۳: کدام‌یک از مجموعه‌های زیر با عمل داده شده گروه نیست؟

۱) $(\mathbb{R},+)$ ۲) $(\mathbb{R},\cdot)$

۳) $\mathbb{R}-\{۰\}$ با عمل دوتایی $a*b=۲ab$ ۴) $(n\mathbb{Z},+)$ که در آن $n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$

☑ **پاسخ:** گزینه «۲» یکی از شروط گروه بودن یک مجموعه، وارون‌پذیر بودن همه‌ی اعضای آن است، در حالی‌که می‌بینیم عدد صفر در $\mathbb{R}$ وارون ضربی ندارد، یعنی عددی مثل $a\in\mathbb{R}$ یافت نمی‌شود که $a\times۰=۰\times a=۱$. بنابراین $(\mathbb{R},\cdot)$ گروه نیست. توجه داشته باشید که اگر صفر را از $\mathbb{R}$ حذف کنیم، یعنی مجموعه‌ی $\mathbb{R}-\{۰\}$ را در نظر بگیریم، آن‌گاه این مجموعه با عمل ضرب یک گروه خواهد بود. گزینه «۱» گروه است زیرا عدد ۰ در آن به عنوان عضو همانی عمل می‌کند یعنی به ازای هر $a\in\mathbb{R}$، $a+۰=۰+a=a$. از طرفی هر عضو $a\in\mathbb{R}$ دارای وارون $-a$ می‌باشد به طوری که $a+(-a)=-a+a=۰$. گزینه «۳» نیز گروه است. عضو همانی این گروه $e=\frac{۱}{۲}$ است زیرا به ازای هر $a\in\mathbb{R}$ داریم $a*e=a*\frac{۱}{۲}=۲\times a\times\frac{۱}{۲}=a$. هم‌چنین هر عضو $a\in\mathbb{R}-\{۰\}$ دارای معکوسی به شکل $a^{-۱}=\frac{۱}{۴a}$ می‌باشد، چون همان‌طور که می‌بینیم $a*a^{-۱}=a*\frac{۱}{۴a}=۲\times a\times\frac{۱}{۴a}=\frac{۱}{۲}=e$. گزینه «۴» هم گروه می‌باشد، زیرا دارای عضو همانی $n\times۰=۰$ است، یعنی به ازای هر $nk\in n\mathbb{Z}$ داریم $nk+۰=nk$. هم‌چنین هر عضو nk از این مجموعه دارای وارونی به فرم $n(-k)$ است.

❖ **تعریف۴:** گروه $(G,*)$ را گروه **آبلی** یا **جابه‌جایی** می‌نامیم، هرگاه به ازای هر دو عضو a و b در G داشته باشیم $a*b=b*a$.
به عنوان مثال گروه‌های جمعی $(\mathbb{Z},+)$، $(\mathbb{Q},+)$، $(\mathbb{R},+)$، $(\mathbb{C},+)$ و گروه‌های ضربی $(\mathbb{Q}-\{۰\},\cdot)$، $(\mathbb{R}-\{۰\},\cdot)$ گروه‌هایی آبلی هستند.

مثال۴: کدام‌یک از گزینه‌های زیر نادرست است؟

۱) مجموعه‌ی ماتریس‌های وارون‌پذیر با درایه‌های حقیقی همراه با عمل ضرب ماتریس‌ها یک گروه غیرآبلی است.
۲) $P(X)$ یعنی مجموعه‌ی توانی مجموعه‌ی X با عمل تفاضل متقارن یک گروه آبلی است.
۳) مجموعه‌ی $\mathbb{Q}(\sqrt{۲})=\{a+b\sqrt{۲}\mid a,b\in\mathbb{Q}\}$ با عمل ضرب معمولی یک گروه آبلی است.
۴) مجموعه‌ی $G=\{f\mid f:A\xrightarrow{\text{دوسویی}}A\}$ با عمل ترکیب توابع یک گروه آبلی است.

☑ **پاسخ:** گزینه «۴» همان‌طور که می‌دانیم تابع همانی $۱_A:A\to A$ تابعی دوسویی است و به ازای هر $f\in G$، داریم $fo۱=۱of=f$، پس تابع ۱_A، عضو همانی مجموعه‌ی G می‌باشد، از طرفی چون توابع این مجموعه دوسویی هستند، وارون‌پذیرند، در نتیجه این مجموعه گروه است، اما چون عمل ترکیب توابع خاصیت جابه‌جایی ندارد، یعنی fog لزوماً با gof برابر نیست، این گروه آبلی نمی‌باشد. بنابراین گزینه «۴» نادرست است. اما در بررسی گزینه‌های دیگر می‌توانیم چنین بگوییم. گزینه «۱» درست است، به ازای هر ماتریس دلخواه A، داریم $AI=IA=A$ که I همان ماتریس همانی است، پس ماتریس همانی I عضو همانی مجموعه‌ی مورد نظر می‌باشد. از طرفی اعضای این مجموعه وارون‌پذیرند، پس این مجموعه یک گروه خواهد بود. اما چون عمل ضرب ماتریس‌ها خاصیت جابه‌جایی ندارد، این گروه نمی‌تواند آبلی باشد. گزینه «۲» نیز درست می‌باشد. یادآوری می‌کنیم که عمل تفاضل متقارن بین دو مجموعه‌ی A و B از $P(X)$ با نماد $A\Delta B$ نمایش داده شده و به صورت $A\Delta B=(A-B)\cup(B-A)$ تعریف می‌شود. مجموعه‌ی تهی، عضو همانی $P(X)$ می‌باشد، زیرا به ازای هر $A\in P(X)$ داریم $A\Delta\varnothing=(A-\varnothing)\cup(\varnothing-A)=A\cup\varnothing=A$، از طرفی هر مجموعه‌ی دلخواه A در $P(X)$ وارون خودش می‌باشد، به عبارت دیگر $A\Delta A=(A-A)\cup(A-A)=\varnothing\cup\varnothing=\varnothing$، پس مجموعه‌ی $P(X)$ با عمل تفاضل متقارن تشکیل یک گروه می‌دهد. هم‌چنین به ازای هر $A,B\in P(X)$ می‌بینیم که $A\Delta B=(A-B)\cup(B-A)=(B-A)\cup(A-B)=B\Delta A$، بنابراین این گروه، آبلی می‌باشد. گزینه «۳» هم درست است. به ازای هر $(a+b\sqrt{۲})\in\mathbb{Q}(\sqrt{۲})$، $(a+b\sqrt{۲})\times۱=a+b\sqrt{۲}$، پس ۱، عضو همانی این مجموعه می‌باشد، از طرفی برای هر عضو $(a+b\sqrt{۲})\in\mathbb{Q}(\sqrt{۲})$ $\frac{a}{a^۲-۲b^۲}-\frac{b}{a^۲-۲b^۲}\sqrt{۲}\in\mathbb{Q}(\sqrt{۲})$ موجود است به طوری که $(a+b\sqrt{۲})(\frac{a}{a^۲-۲b^۲}-\frac{b}{a^۲-۲b^۲}\sqrt{۲})=۱$، لذا همه‌ی اعضای $\mathbb{Q}(\sqrt{۲})$ وارون‌پذیرند، در نتیجه این مجموعه یک گروه می‌باشد. در نهایت، به ازای هر $(a+b\sqrt{۲}),(c+d\sqrt{۲})\in\mathbb{Q}(\sqrt{۲})$ داریم $(a+b\sqrt{۲})(c+d\sqrt{۲})=ac+(ad+bc)\sqrt{۲}+۲bd=(c+d\sqrt{۲})(a+b\sqrt{۲})$ و این نشان می‌دهد که $\mathbb{Q}(\sqrt{۲})$ یک گروه آبلی است.

مثال۵: فرض کنید $(\mathbb{N},*)$ مجموعه اعداد طبیعی همراه با عمل * است که برای هر a و b در $\mathbb{N}$ داریم، $a*b=\max\{a,b\}$، کدام گزاره صحیح است؟ (سراسری ۹۴)

۱) $(\mathbb{N},*)$ غیرآبلی است.　　۲) $(\mathbb{N},*)$ شرکت‌پذیر نمی‌باشد.

۳) $(\mathbb{N},*)$ یک تکواره (منوئید) است.　　۴) هر عضو $(\mathbb{N},*)$ عضو وارون دارد.

☑ **پاسخ:** گزینه «۳» از آنجایی که $\max\{b,a\}=\max\{a,b\}$ نتیجه می‌گیریم گزینه (۱) صحیح نیست. تساوی $\max\{\max\{a,b\},c\}=\max\{a,\max\{b,c\}$ شرکت‌پذیری را نتیجه می‌دهد بنابراین گزینه (۲) صحیح نمی‌باشد. عدد ۱ عضو همانی $(\mathbb{N},*)$ می‌باشد. بنابراین مجموعهٔ مورد نظر به همراه عمل * تشکیل یک تکواره (منوئید) می‌دهد در نتیجه گزینه (۳) گزینه صحیح مورد نظر می‌باشد. نادرست بودن گزینه (۴) واضح می‌باشد.

◆ ◆ ◆ ◆

اکنون به معرفی یک مجموعه‌ی مهم می‌پردازیم که با عمل جمع، یک گروه آبلی و با عمل ضرب، یک تکوار می‌باشد.

❖ **تعریف۵:** همان طور که به خاطر دارید، اگر $\equiv$ رابطه‌ی هم نهشتی به پیمانه‌ی عدد صحیح n روی مجموعه‌ی $\mathbb{Z}$ باشد، آن‌گاه کلاس هم ارزی عضوی مانند a از $\mathbb{Z}$ به صورت $\overline{a}=\{b\in\mathbb{Z}\mid b\overset{n}{\equiv}a\}$ خواهد بود. مجموعه‌ی همه‌ی کلاس‌های هم‌ارزی به پیمانه‌ی n را با $\mathbb{Z}_n$ نمایش داده و به‌صورت $\mathbb{Z}_n=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$ تعریف می‌کنیم. جمع و ضرب اعداد به ازای $\overline{a},\overline{b}\in\mathbb{Z}_n$ به صورت $\overline{a}\cdot\overline{b}=\overline{a\cdot b}$ و $\overline{a}+\overline{b}=\overline{a+b}$ تعریف می‌شود. $\mathbb{Z}_n$ همراه با عمل جمع یک گروه آبلی است. عضو همانی این گروه $\overline{0}$ و معکوس هر عضو آن مانند $\overline{a}$ به صورت $\overline{n-a}=-\overline{a}$ می‌باشد. به عنوان مثال اگر مجموعه‌ی $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$ را در نظر بگیریم، آن‌گاه می‌بینیم که $\overline{1}+\overline{3}=\overline{4}\overset{4}{\equiv}\overline{0}$، $\overline{2}+\overline{2}=\overline{4}\overset{4}{\equiv}\overline{0}$. پس $\overline{0}$ و $\overline{2}$ معکوس خودشان هستند و $\overline{1}$ و $\overline{3}$ معکوس یکدیگرند. توجه داشته باشید که گاهی برای راحتی کار عدد $\overline{a}\in\mathbb{Z}_n$ را با a نمایش می‌دهیم.

$\mathbb{Z}_n$ همراه با عمل ضرب نمی‌تواند گروه باشد، چون اگرچه ۱ عضو همانی $\mathbb{Z}_n$ است ولی همه‌ی اعضای آن وارون‌پذیر نیستند. به عنوان مثال، عضو $\overline{0}$ وارون ضربی ندارد. $\mathbb{Z}_n$ با عمل ضرب یک تکوار جابه‌جایی است. به عنوان مثال اگر $\mathbb{Z}_4$ را با عمل ضرب در نظر بگیریم، آن‌گاه می‌بینیم که ۱ و ۳ معکوس خودشان هستند، $\overline{3}\times\overline{3}=\overline{9}\overset{4}{\equiv}\overline{1}$ و $\overline{1}\times\overline{1}=\overline{1}$. اما ۲ معکوس‌پذیر نیست، چون $\overline{2}\times\overline{0}=\overline{0}\overset{4}{\equiv}\overline{0}$، $\overline{2}\times\overline{1}=\overline{2}\overset{4}{\equiv}\overline{4}\overset{4}{\equiv}\overline{0}$، $\overline{2}\times\overline{2}=\overline{4}\overset{4}{\equiv}\overline{0}$ و $\overline{2}\times\overline{3}=\overline{6}\overset{4}{\equiv}\overline{2}$ یعنی ضرب هیچ‌کدام از اعضای $\mathbb{Z}_4$ در ۲ به پیمانه‌ی ۴، عضو ۱ نمی‌شود. واضح است که۳ و۱ نسبت به۴ اول هستند ولی۲ نسبت به۴ اول نیست. در حالت کلی می‌توانیم بگوییم $a\in(\mathbb{Z}_n,.)$ معکوس‌پذیر است اگر و تنها اگر $(a,n)=1$. برای درک بهتر این مطلب به مثال زیر دقت کنید:

مثال۶: نشان دهید $(\mathbb{Z}_n^*,.)$ گروه است اگر و تنها اگر n عددی اول باشد. $(\mathbb{Z}_n^*=\mathbb{Z}_n-\{\overline{0}\})$

☑ **پاسخ:** اگر u معکوس ضربی عضو $a\in\mathbb{Z}_n^*$ باشد، داریم: $au\overset{n}{\equiv}1\Leftrightarrow au-1=nk,\ k\in\mathbb{Z}\Leftrightarrow au-nk=1,\ k\in\mathbb{Z}\Leftrightarrow(a,n)=1$

بنابراین در تکوار $(\mathbb{Z}_n,\cdot)$، عضو $a\in\mathbb{Z}_n$ معکوس‌پذیر است اگر و تنها اگر $(a,n)=1$. حال اگر n عددی اول باشد، همه‌ی اعضای $\mathbb{Z}_n^*$ نسبت به n اول خواهند بود، در نتیجه همگی معکوس‌پذیر می‌باشند. درنتیجه $\mathbb{Z}_n^*$ همراه با عمل ضرب یک گروه است اگر و تنها اگر n عددی اول باشد.

◆ ◆ ◆ ◆

طبق آنچه که در بالا بیان شد ما می‌توانیم یک گروه جدید بسازیم، این گروه که با U_n نمایش داده می‌شود، برابر است با مجموعه‌ی تمام اعضای وارون‌پذیر $(\mathbb{Z}_n,\cdot)$، در حقیقت $U_n=\{a\in\mathbb{N}\mid a<n,(a,n)=1\}$. به عنوان مثال، $U_{15}=\{1,2,4,7,8,11,13,14\}$.

مثال۷: کدام مجموعه تحت ضرب به پیمانه‌ی ۱۴ تشکیل یک گروه می‌دهد؟ (سراسری ۸۳)

۱) $\{1,3,5\}$　　۲) $\{1,9,11\}$　　۳) $\{1,7,13\}$　　۴) $\{1,3,5,7\}$

☑ **پاسخ:** گزینه «۲» مجموعه‌ای تحت عمل ضرب به پیمانهٔ ۱۴ تشکیل گروه می‌دهد که اعضایش نسبت به ۱۴ اول باشند، پس گزینه‌های (۳) و (۴) نمی‌توانند جواب مسئله باشند، چون ۷ نسبت به ۱۴ اول نیست. در گزینهٔ (۱) می‌بینیم که $5\times5=25\overset{14}{\equiv}11$ اما $11\notin\{1,3,5\}$، پس این مجموعه نسبت به عمل ضرب به پیمانهٔ ۱۴ بسته نیست. تنها گزینه‌ای که باقی می‌ماند، گزینهٔ (۲) است. همهٔ اعضای این گروه نسبت به ۱۴ اول هستند، هم‌چنین $9\times11=99\overset{14}{\equiv}1$، پس این مجموعه نسبت به عمل ضرب به پیمانهٔ ۱۴ بسته است و این گزینه درست می‌باشد.

اکنون در مثال زیر، گروه مهمی را معرفی می‌کنیم که به گروه چهارتایی کلاین معروف می‌باشد.

مثال۸: مجموعه‌ی $G=\{e,a,b,c\}$ را در نظر بگیرید و عمل $*$ را روی آن به صورت زیر تعریف کنید:

$$a*e=e*a=a,\quad b*e=e*b=b,\quad c*e=e*c=c,\quad a*b=b*a=c,\quad a*c=c*a=b,\quad b*c=c*b=a,\quad a^2=b^2=c^2=e$$

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

$(G,*)$ یک گروه آبلی می‌باشد، زیرا دارای عضو همانی e می‌باشد و هر عضو، وارون خودش است. از طرفی همه‌ی اعضا با هم جابه‌جا می‌شوند. همان طور که در بالا اشاره شد، این گروه، **گروه چهارتایی کلاین** نامیده می‌شود. جدول کیلی این گروه به صورت روبرو می باشد:

◆ ◆ ◆ ◆

در این بخش به بیان قضایایی در مبحث گروه‌ها می‌پردازیم که در آن‌ها ویژگی‌های اساسی گروه‌ها بیان می‌شود.

قضایای اساسی گروه‌ها

قضیه۱ (منحصر بودن عضو همانی): فرض کنید $(G,*)$ یک گروه باشد. در این صورت عضو همانی G، منحصر به فرد است.

اثبات: فرض می‌کنیم G دارای دو عضو همانی e_1 و e_2 باشد و ثابت می‌کنیم $e_1=e_2$.

$$\left.\begin{array}{l} e_1 \text{ عضو همانی } G \text{ است} \Rightarrow e_1*e_2=e_2*e_1=e_2 \\ e_2 \text{ عضو همانی } G \text{ است} \Rightarrow e_2*e_1=e_1*e_2=e_1 \end{array}\right\} \Rightarrow e_1=e_2$$

قضیه ۲ (منحصر به فرد بودن عضو معکوس): فرض کنید $(G,*)$ یک گروه باشد و x را به عنوان عضو دلخواهی از آن در نظر بگیرید، در این صورت معکوس x منحصر به فرد است.

اثبات: فرض می‌کنیم $x\in G$ دارای دو معکوس y_1 و y_2 باشد و ثابت می‌کنیم $y_1=y_2$.

$$y_1 \text{ معکوس } x \text{ است} \Rightarrow x*y_1=y_1*x=e \quad (I)$$
$$y_2 \text{ معکوس } x \text{ است} \Rightarrow x*y_2=y_2*x=e \quad (II)$$

بنابراین داریم:

$$y_1=y_1*e \overset{(II)}{=\!=} y_1*(x*y_2)=(y_1*x)*y_2 \overset{(I)}{=\!=} e*y_2=y_2 \Rightarrow y_1=y_2$$

قضیه۳: اگر $(G,*)$ یک گروه باشد، آن‌گاه به ازای هر عضو دلخواه x از G داریم $(x^{-1})^{-1}=x$.

اثبات: $(x^{-1})^{-1}$ وارون عضو x^{-1} است، بنابراین $x^{-1}*(x^{-1})^{-1}=e$. از طرفی x^{-1} وارون x است، پس $x^{-1}*x=e$. لذا بنا بر منحصر به فرد بودن عضو معکوس نتیجه می‌شود $(x^{-1})^{-1}=x$.

قضیه۴: فرض کنید $(G,*)$ یک گروه باشد، در این صورت به ازای هر دو عضو x و y از G داریم $(x*y)^{-1}=y^{-1}*x^{-1}$.

اثبات: $(x*y)^{-1}$ معکوس عضو $(x*y)$ است، بنابراین $(x*y)*(x*y)^{-1}=e$، همچنین داریم:

$$(x*y)*(y^{-1}*x^{-1})=x*(y*y^{-1})*x^{-1}=x*e*x^{-1}=x*x^{-1}=e$$

اکنون طبق قضیه‌ی منحصر به فرد بودن عضو معکوس نتیجه می‌گیریم $(x*y)^{-1}=y^{-1}*x^{-1}$.

قضیه ۵ (قوانین حذف): فرض کنید $(G,*)$ یک گروه باشد. در این صورت قوانین حذف از چپ و راست در G برقرار است، یعنی به ازای $x,y,z\in G$ داریم:

الف) اگر $x*z=x*y$، آن‌گاه $y=z$،

ب) اگر $z*x=y*x$، آن‌گاه $y=z$.

اثبات:

الف) $$x*y=x*z\Rightarrow x^{-1}*(x*y)=x^{-1}*(x*z)\xrightarrow{\text{شرکت‌پذیری}}(\underbrace{x^{-1}*x}_{e})*y=(\underbrace{x^{-1}*x}_{e})*z\Rightarrow e*y=e*z\Rightarrow y=z$$

ب) $$y*x=z*x\Rightarrow (y*x)*x^{-1}=(z*x)*x^{-1}\xrightarrow{\text{شرکت‌پذیری}}y*(\underbrace{x*x^{-1}}_{e})=z*(\underbrace{x*x^{-1}}_{e})\Rightarrow y*e=z*e\Rightarrow y=z$$

فصل سوم

« جایگشت‌ها»

در این فصل، گروه مهمی را که با S_n نمایش داده و گروه جایگشتی نامیده می‌شود، معرفی کرده و سپس به بررسی خواص آن می‌پردازیم.
قبل از این‌که به تعریف گروه‌های جایگشتی S_n بپردازیم، لازم است با مفهوم جایگشت آشنا شویم. فرض کنید X مجموعه‌ای غیرتهی باشد، در این صورت یک جایگشت روی X یک تابع یک به یک و پوشا از X به X است. برای مثال اگر $X=\{x_۱,x_۲,x_۳,x_۴\}$، آن‌گاه می‌توانیم یک جایگشت به صورت زیر روی X تعریف کنیم: $\varphi: X \to X$

$$\varphi(x_۱)=x_۲,\quad \varphi(x_۲)=x_۴,\quad \varphi(x_۳)=x_۳,\quad \varphi(x_۴)=x_۱$$

برای راحتی کار این تابع را به صورت $\varphi=\begin{pmatrix} x_۱ & x_۲ & x_۳ & x_۴ \\ x_۲ & x_۴ & x_۳ & x_۱ \end{pmatrix}$ نمایش می‌دهیم که سطر اول و دوم به ترتیب نشان دهنده‌ی دامنه و برد تابع هستند.

درسنامه (۱) گروه‌های جایگشتی

❖ **تعریف۱:** مجموعه‌ی همه جایگشت‌های تعریف شده روی مجموعه‌ی ناتهی X را با S_X نمایش می‌دهیم. در صورتی که X مجموعه‌ی متناهی از مرتبه‌ی n به شکل $\{x_۱,\dots,x_n\}$ باشد، آن را با $\{۱,\dots,n\}$ و S_X یا با S_n نمایش می‌دهیم. بدین ترتیب اگر φ یک جایگشت روی مجموعه‌ی $\{۱,\dots,n\}$ باشد، آن‌گاه:

$$\varphi=\begin{pmatrix} ۱ & ۲ & \cdots & n \\ \varphi(۱) & \varphi(۲) & \cdots & \varphi(n) \end{pmatrix}$$

در این جا لازم است که مفهوم ترکیب توابع جایگشتی توضیح داده شود. برای این منظور با یک مثال شروع می‌کنیم. فرض کنید φ و ψ دو تابع در $S_۷$ به شکل‌های زیر باشند:

$$\varphi=\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۱ & ۵ & ۶ & ۴ & ۷ & ۳ & ۲ \end{pmatrix},\psi=\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۳ & ۶ & ۷ & ۴ & ۱ & ۵ \end{pmatrix}$$

می‌بینیم که φ، عدد۳ را به۶ و ψ عدد۶ را به۱ می‌برد، در واقع $۳ \xrightarrow{\varphi} ۶ \xrightarrow{\psi} ۱$، پس $\varphi\psi(۳)=۱$. یعنی برای به دست آوردن $\varphi\psi$ از چپ به راست عمل می‌کنیم، بنابراین $\varphi\psi=\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۴ & ۱ & ۷ & ۵ & ۶ & ۳ \end{pmatrix}$ و به همین ترتیب $\psi\varphi$ برابر می‌شود با $\psi\varphi=\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۵ & ۶ & ۳ & ۲ & ۴ & ۱ & ۷ \end{pmatrix}$.
همان طور که مشاهده می‌کنید $\varphi\psi \neq \psi\varphi$، پس جایگشت‌ها روی مجموعه‌ی S_n خاصیت جابه‌جایی ندارند.

❖ **تعریف۲:** به ازای هر عدد طبیعی n، S_n همراه با عمل ترکیب توابع که در بالا توضیح داده شد، تشکیل یک گروه می‌دهد. عضو همانی این گروه که آن را با e یا (۱) نمایش می‌دهیم، به صورت $\begin{pmatrix} ۱ & ۲ & \cdots & n \\ ۱ & ۲ & \cdots & n \end{pmatrix}$ و معکوس هر عضو دلخواه مانند $\begin{pmatrix} ۱ & ۲ & \cdots & n \\ \varphi(۱) & \varphi(۲) & \cdots & \varphi(n) \end{pmatrix}$ به صورت $\begin{pmatrix} \varphi(۱) & \varphi(۲) & \cdots & \varphi(n) \\ ۱ & ۲ & \cdots & n \end{pmatrix}$ می‌باشد. گروه S_n را **گروه جایگشتی از درجه‌ی** n می‌نامیم.

➢ **توجه:** واضح است که گروه‌های تک عضوی و دو عضوی $S_۱$ و $S_۲$ آبلی هستند. اما به ازای $n \geq ۳$، دو جایگشت در S_n لزوماً با هم جابه‌جا نمی‌شوند، پس به ازای $n \geq ۳$، S_n یک گروه ناآبلی است.

قضیه۱: به ازای هر عدد طبیعی n، $o(S_n) = n!$.

اثبات: هر عضو S_n تابعی یک به یک و پوشا از مجموعه‌ی $X = \{۱,۲,\dots,n\}$ به خودش است. اگر $\varphi \in S_n$، آن‌گاه برای تعریف $\varphi(۱)$، به تعداد n تا انتخاب داریم، برای تعریف $\varphi(۲)$ به تعداد $(n-۱)$ تا انتخاب، و به همین ترتیب برای $\varphi(n)$، به تعداد ۱ انتخاب. بنابراین تعداد انتخاب‌ها برای کل جایگشت‌ها مساوی $n(n-۱)\dots ۲\times ۱ = n!$ می‌باشد.

مثال۱: عناصر گروه $S_۳$ را مشخص کرده و مرتبه‌ی هر یک را بیابید.

پاسخ: طبق قضیه‌ی فوق $o(S_۳) = ۳! = ۶$، بنابراین $S_۳$، ۶ عضو دارد، در حقیقت

$$S_۳ = \left\{(۱), \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}, \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix}, \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix}, \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix}, \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۱ & ۲\end{pmatrix}\right\}$$ که مرتبه‌ی اعضای آن به صورت زیر می‌باشد:

$$\alpha_۰ = \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۲ & ۳\end{pmatrix} = (۱) \Rightarrow o(\alpha_۰) = ۱, \quad \alpha_۱ = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}, \quad \alpha_۱^۲ = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix} = \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۲ & ۳\end{pmatrix} = (۱) \quad \Rightarrow o(\alpha_۱) = ۲,$$

$$\alpha_۲ = \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix}, \quad \alpha_۲^۲ = \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix}\begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix} = \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۲ & ۳\end{pmatrix} = (۱) \quad \Rightarrow o(\alpha_۲) = ۲$$

به همین ترتیب با محاسبه‌ای ساده داریم:

$$\alpha_۳ = \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix}, \quad o(\alpha_۳) = ۲, \quad \alpha_۴ = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix}, \quad o(\alpha_۴) = ۳, \quad \alpha_۵ = \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۱ & ۲\end{pmatrix}, \quad o(\alpha_۵) = ۳$$

قرار می‌دهیم $\alpha = \alpha_۱$ و $\beta = \alpha_۴$، می‌توان نشان داد $\alpha_۵ = \beta^۲$، $\alpha_۲ = \alpha\beta$ و $\alpha_۳ = \alpha\beta^۲$، بنابراین $S_۳ = \left\{e, \alpha, \beta, \beta^۲, \alpha\beta, \alpha\beta^۲\right\}$.

مدرسان شریف

فصل چهارم

«زیرگروه‌ها»

در فصل یک با تعریف زیرجبر و $P-$زیرجبر آشنا شدیم. در این فصل قصد داریم مفهوم زیرگروه که نوعی $P-$زیرجبر است را ارائه دهیم. در حقیقت اگر فرض کنیم P مجموعه‌ای متشکل از ویژگی‌های شرکت‌پذیری، دارا بودن عضو همانی و معکوس‌پذیر بودن هر عضو باشد، آن‌گاه مفهوم $P-$زیرجبر بودن معادل با زیرگروه بودن است. پس از آشنایی با این مفهوم و بیان مثال‌های مختلف، به بررسی مفاهیمی هم‌چون گروه‌های دوری، زیرگروه‌های نرمال و خارج قسمتی می‌پردازیم.

درسنامه (۱): زیرگروه

❖ **تعریف۱:** زیرمجموعه‌ی غیرتهی H از گروه G را **زیرگروه** G می‌نامیم، هرگاه H تحت عمل تعریف شده روی G تشکیل گروه دهد. توجه داشته باشید که عضو همانی H همان عضو همانی G می‌باشد، ضمناً معکوس هر عضو H همان معکوسی است که در G دارد. وقتی H زیرگروه G است، می‌نویسیم $H \leq G$.

به عنوان مثال می‌دانیم $\mathbb{R}^{+} \subseteq \mathbb{R}^{*}$، از طرفی $\mathbb{R}^{*}$ و $\mathbb{R}^{+}$ تحت عمل ضرب تشکیل گروه می‌دهند، پس می‌توانیم بگوییم $(\mathbb{R}^{+},\cdot)$ زیرگروهی از $(\mathbb{R}^{*},\cdot)$است، یا به عبارت دیگر $(\mathbb{R}^{+},\cdot) \leq (\mathbb{R}^{*},\cdot)$. همچنین با در نظر گرفتن عمل جمع $\mathbb{C}$ و چون $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$، و چون $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ تحت عمل جمع تشکیل گروه می‌دهند، پس می‌توان نوشت $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$. هرگروه غیر بدیهی G حداقل دارای دو زیرگروه می‌باشد. این زیرگروه‌ها که خود G و $\{e\}$ می‌باشند، **زیرگروه‌های بدیهی** G نامیده می‌شوند. توجه داشته باشید اگر زیرمجموعه‌ی سره‌ی H از G زیرگروهی از G باشد، آن‌گاه H زیرگروه سره‌ی G نامیده می‌شود.

مثال۱: نشان دهید همه‌ی زیرگروه‌های مجموعه‌ی $(\mathbb{Z},+)$ به شکل $n\mathbb{Z}$ هستند.

☑ **پاسخ:** می‌دانیم به ازای هر $n \in \mathbb{Z}$، $n\mathbb{Z} \subseteq \mathbb{Z}$ و مجموعه‌ی $n\mathbb{Z}$ با عمل جمع تشکیل یک گروه می‌دهد که عضو همانی این گروه 0 و قرینه هر عضو آن مانند nk به شکل $n(-k)$ می‌باشد. بنابراین $n\mathbb{Z}$ زیرگروهی از $\mathbb{Z}$ است. حال نشان می‌دهیم که $(\mathbb{Z},+)$ به غیر از $n\mathbb{Z}$ زیرگروه دیگری ندارد. فرض می‌کنیم H زیرگروه دلخواهی از $\mathbb{Z}$ باشد، بنا به اصل خوش‌ترتیبی، کوچکترین عدد صحیح مثبت در H وجود دارد که آن را n می‌نامیم. اگر $m \in H$، آن‌گاه اعداد صحیحی چون r و q موجودند به‌طوری که $m = nq + r \;,\; 0 \leq r < n$. چون $n \in H$، داریم $nq \in H$. همچنین چون طبق فرض m هم عضوی از H است، اگر $r \neq 0$، آن‌گاه نتیجه می‌شود $m - nq = r \in H$، که این با انتخاب n در تناقض است چون $r < n$، بنابراین $r = 0$ و $m = nq$، در نتیجه $H = n\mathbb{Z}$.

◆ ◆ ◆ ◆

لازم به ذکر است که اگر گروه G گروهی آبلی باشد، آن‌گاه هر زیرگروه H از آن نیز آبلی است، زیرا همه‌ی اعضای H در G قرار دارند و وقتی در G جابه‌جا می‌شوند، در H نیز جابه‌جا خواهند شد. از طرفی اگر $H \leq G$ و $K \leq H$، آن‌گاه $K \leq G$.

توجه داشته باشید ممکن است تشخیص زیرگروه بودن H از G چندان کار ساده‌ای نباشد، بنابراین به روش‌هایی برای تشخیص زیرگروه بودن یک مجموعه از مجموعه‌ای دیگر نیازمندیم. در قضایای نخست از این فصل، روش‌هایی برای این کار ارائه می‌دهیم.

قضیه ۱ (محک زیرگروه): فرض کنید G یک گروه و H زیرمجموعه‌ای غیرتهی از آن باشد. در این صورت H زیرگروه G است اگر و تنها اگر به ازای هر دو عضو a و b از G داشته باشیم: ۱) $a^{-1} \in H$، ۲) $ab \in H$.

اثبات: اگر H زیرگروه G باشد، آن‌گاه شرایط ۱ و ۲ برقرار است. حال فرض می‌کنیم شرایط ۱ و ۲ برقرار باشند، H مخالف تهی است پس عضوی مانند $a \in H$ دارد. طبق فرض $a^{-1} \in H$ حال:

$$a \in H \;,\; a^{-1} \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$$

پس H دارای عضو خنثی هم هست. پس H همه شرایط لازم برای زیر گروه بودن را دارد.
قضیه‌ی فوق را به صورت دیگری نیز می‌توان بیان کرد که آن را در قضیه‌ی زیر می‌بینیم:

قضیه۲: زیرمجموعه‌ی غیرتهی H از گروه G، زیرگروه G است اگر و تنها اگر به ازای هر دو عضو a و b از G داشته باشیم $ab^{-1} \in H$ (در حالت جمع $a - b \in H$).

مثال۲: فرض کنید G یک گروه آبلی است و $H = \{a \in G \mid o(a) = ۱۳ \text{ یا } o(a) = ۱\}$. در این صورت H تحت عمل ضرب، زیرگروهی از G است.

پاسخ: فرض کنید a و b دو عضو دلخواه H باشند، ثابت می‌کنیم $a^{-1}b \in H$ در این صورت اگر $a = e$ یا $b = e$، آن‌گاه حکم واضح است. بنابراین فرض می‌کنیم $a \neq e$ و $b \neq e$. از این رو $o(a) = o(b) = ۱۳$ لذا $o(a^{-1}) = ۱۳$، در نتیجه از آبلی بودن G داریم:

$$(a^{-1}b)^{۱۳} = (a^{-1})^{۱۳}b^{۱۳} = ee = e \Rightarrow o(a^{-1}b) \mid ۱۳ \Rightarrow o(a^{-1}b) = ۱ \text{ یا } o(a^{-1}b) = ۱۳ \Rightarrow a^{-1}b \in H \Rightarrow H \leq G$$

◆ ◆ ◆ ◆

مثال۳: کدام‌یک از مجموعه‌های زیر همراه با عمل‌دوتایی ارائه شده یک گروه نیست؟ (سراسری ۹۳)

۱) $A = \{a \in \mathbb{Q} \mid a > ۰\}$ همراه با عمل دوتایی $a * b = \frac{ab}{۳}$　　۲) $A = \{z \in \mathbb{C} \mid z^{۴} = ۱\}$ همراه با ضرب اعداد مختلط

۳) $A = \{z \in \mathbb{C} \mid ۰ < |z| \leq ۱\}$ همراه با ضرب اعداد مختلط　　۴) $A = \{z \in \mathbb{C} \mid |z| = ۱\}$ همراه با ضرب اعداد مختلط

پاسخ: گزینه «۳» فرض می‌کنیم $z_۱ = ۱$ و $z_۲ = \frac{۱}{۲}$. واضح است که $|z_۱| \leq ۱$ و $|z_۲| \leq ۱$. طبق محک زیرگروه برای اینکه A یک گروه باشد، باید به ازای هر $z_۱, z_۲ \in A$، داشته باشیم $z_۱z_۲^{-1} \in A$، اما برای $z_۱ = ۱$ و $z_۲ = \frac{۱}{۲}$ می‌بینیم که:

$$|z_۱z_۲^{-۲}| = |۱ \times (\frac{۱}{۲})^{-1}| = |۱ \times ۲| = ۲ \xrightarrow{۲>۱} ۲ \notin A \Rightarrow A \text{ زیر گروه } \mathbb{C} \text{ نیست}$$

◆ ◆ ◆ ◆

قضیه۳ (محک زیرگروه متناهی): فرض کنید G یک گروه و H زیرمجموعه‌ی غیرتهی و متناهی از G باشد. در این صورت H زیرگروه G است اگر و تنها اگر به ازای هر $a, b \in H$ داشته باشیم $ab \in G$.

اثبات: طبق قضیه‌ی قبل یعنی محک زیرگروه، کافی است نشان دهیم به ازای هر $a \in H$، $a^{-1} \in H$. مجموعه‌ی $S = \{a, a^{۲}, a^{۳}, \ldots\}$ را در نظر می‌گیریم. چون اعضای S توان‌هایی از عضو $a \in H$ هستند، داریم $S \subseteq H$. با توجه به این که H متناهی است، S هم متناهی می‌باشد، در نتیجه اعضای S متمایز نیستند، لذا به ازای دو عدد صحیح i و j داریم $a^i = a^j$. فرض می‌کنیم $i > j$، بنابراین داریم:

$a^{i-j} = e \Rightarrow aa^{i-j-۱} = e \Rightarrow a^{i-j-۱}$ معکوس a است $\Rightarrow$ هر عضو H دارای معکوس است

مثال۴: فرض کنید $H = \{x \in U_{۴۰} : ۵ \mid x - ۱\}$. در این صورت نشان دهید $H \leq U_{۴۰}$.

پاسخ: H متناهی و ناتهی است. زیرا اعضایش از مجموعه‌ی متناهی $U_{۴۰}$ انتخاب می‌شوند. کافیست برای دو عضو $x, y \in H$ نشان دهیم $xy \in H$. به ازای هر دو عضو x و y داریم $۵ \mid x - ۱$ و $۵ \mid y - ۱$. بنابراین ۵ هر ترکیب خطی از $x - ۱$ و $y - ۱$ را نیز عاد می کند. با توجه به این که $xy - ۱ = xy - y + y + ۱ = y(x - ۱) + (y - ۱)$، نتیجه می‌گیریم $۵ \mid xy - ۱$. بنابراین $xy \in H$ و طبق محک زیرگروه متناهی $H \leq U_{۴۰}$.

◆ ◆ ◆ ◆

قضیه ۴: اگر G یک گروه باشد، آن‌گاه اشتراک هر تعداد از زیرگروه‌های G، زیرگروهی از G می‌باشد.

اثبات: فرض می‌کنیم $\{H_i\}_{i \in I}$ خانواده‌ای از زیرگروه‌های G باشند. در این صورت داریم:

$$a, b \in \bigcap_{i \in I} H_i \Rightarrow \forall i;\ a, b \in H_i \xrightarrow{H_i \leq G} \forall i\ ; ab^{-1} \in H_i \Rightarrow ab^{-1} \in \bigcap_{i \in I} H_i \Rightarrow \bigcap_{i \in I} H_i \leq G$$

توجه: در قضیه‌ی قبل دیدیم که اشتراک هر تعداد از زیرگروه‌های G، زیرگروهی از G می‌شود اما این امر در مورد اجتماع درست نیست، یعنی اگر H و K دو زیرگروه G باشند، آن‌گاه $H \cup K$ لزوماً زیرگروه G نیست. به عنوان مثال $۳\mathbb{Z} = \{۰, \pm ۳, \pm ۶, \ldots\}$ و $۵\mathbb{Z} = \{۰, \pm ۵, \pm ۱۰, \ldots\}$ دو زیرگروه $\mathbb{Z}$ می‌باشند، اما $۳\mathbb{Z} \cup ۵\mathbb{Z}$ زیرگروه $\mathbb{Z}$ نیست، زیرا می‌بینیم که $۳, ۵ \in ۳\mathbb{Z} \cup ۵\mathbb{Z}$ اما $۳ + ۵ = ۸ \notin ۳\mathbb{Z} \cup ۵\mathbb{Z}$. در قضیه‌ی زیر نشان می‌دهیم که تحت چه شرایطی اجتماع زیرگروه‌های G، زیرگروهی از G است.

قضیه ۵: فرض کنید G یک گروه باشد و $H, K \leq G$. در این صورت $H \cup K$ زیرگروهی از G خواهد بود اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.

اثبات: ابتدا فرض می‌کنیم $H \subseteq K$، بنابراین $H \cup K = K \leq G$. حال فرض می‌کنیم $H \cup K \leq G$ و نشان می دهیم $K \subseteq H$ یا $H \subseteq K$. اگر به برهان خلف فرض کنیم این‌طور نباشد یعنی $H \not\subseteq K$ و $K \not\subseteq H$، آن‌گاه عضوی چون $h \in H$ وجود دارد به طوری که $h \notin K$ و عضوی چون $k \in K$ وجود دارد به طوری که $k \notin H$. اما از آن‌جایی که $h \in H$ و $k \in K$ داریم $h, k \in H \cup K$. بنابراین چون $H \cup K$ زیرگروهی از G است، hk هم باید عضوی از $H \cup K$ باشد، یعنی $hk \in H$ یا $hk \in K$. اگر $hk \in H$، آن‌گاه چون $h^{-1} \in H$، داریم $h^{-1}(hk) = h^{-1}hk = k \in H$ که تناقض است و اگر $hk \in K$، آن‌گاه با توجه به این که $k^{-1} \in K$ داریم $(hk)k^{-1} = h(kk^{-1}) = h \in K$ که این هم تناقض است. بنابراین $hk \notin H \cup K$ و از این نتیجه می‌گیریم $H \cup K$ زیرگروه G نیست که این تناقض با فرض می‌باشد.

نتیجه: اگر G یک گروه و $\{H_i\}_{i \in I}$ خانواده‌ای از زیرگروه‌های G باشد و به ازای هر عدد $m \in I$، عدد $n \in I$ موجود باشد به طوری که $H_m \subseteq H_n$، آن‌گاه $\bigcup_{i \in I} H_i \leq G$.

مثال ۵: کدام‌یک از گزینه های زیر نادرست است؟

۱) به ازای هر عددطبیعی n، $A_n \leq S_n$

۲) به ازای دو مجموعه‌ی X و Y که $X \subseteq Y$، مجموعه‌ی $P(X)$ با عمل تفاضل متقارن زیرگروهی از $P(Y)$ است.

۳) $H = \{0, 2, 4\} \leq (\mathbb{Z}_5, +)$

۴) اگر H مجموعه‌ی همه‌ی اعضای از مرتبه‌ی متناهی در گروه آبلی G باشد، آن‌گاه $H \leq G$.

☑ **پاسخ:** گزینه «۳» مجموعه‌ی H متناهی است،پس طبق محک زیرگروه متناهی، H در صورتی زیرگروه $\mathbb{Z}_5$ است که جمع هر دو عضو آن به پیمانه‌ی ۵ در H قرار بگیرند، اما می‌بینیم که $2+4 = 6 \overset{5}{\equiv} 1 \notin H$، پس $H \not\leq \mathbb{Z}_5$. بنابراین گزینه «۳» نادرست است. در بررسی گزینه‌های دیگر می‌توانیم چنین بگوییم. گزینه «۱» درست است. می‌دانیم A_n مجموعه‌ی جایگشت‌های زوج S_n می‌باشد و حاصل‌ضرب هر دو جایگشت زوج جایگشتی زوج است و این یعنی حاصل‌ضرب هر دو عضو A_n در خود A_n قرار می‌گیرد. از طرفی A_n متناهی است،پس طبق محک زیرگروه متناهی، $A_n \leq S_n$. گزینه‌ی «۲» نیز درست است، قبلاً ثابت کردیم که مجموعه‌ی توانی هر مجموعه‌ی دلخواه با عمل تفاضل متقارن تشکیل یک گروه می‌دهد، پس $P(X)$ و $P(Y)$ گروه می‌باشند و چون $Y \subseteq X$ داریم $P(Y) \subseteq P(X)$، در نتیجه $P(Y)$ زیرگروهی از $P(X)$ می‌باشد. گزینه‌ی «۴» هم درست است. فرض می‌کنیم a و b دو عضو H باشند، پس هر دو از مرتبه‌ی متناهی هستند. برای اثبات گروه بودن H کافی است نشان دهیم ab^{-1} از مرتبه‌ی متناهی است. چون a و b از مرتبه‌ی متناهی هستند، اعداد صحیح m و n موجودند به طوری که $a^n = e$ و $b^m = e$. طبق قضیه‌ای $o(a^{-1}) = o(a)$، بنابراین با توجه به این که G آبلی است خواهیم داشت:

$$(a^{-1}b)^{mn} = (a^{-1})^{mn} b^{mn} = ((a^{-1})^n)^m (b^m)^n = e^m e^n = e \Rightarrow o(a^{-1}b) \mid mn \Rightarrow a^{-1}b \text{ متناهی است} \Rightarrow a^{-1}b \in H \Rightarrow H \leq G$$

◆ ◆ ◆ ◆

مثال ۶: فرض کنید به ازای عدد اول p و عدد صحیح مثبت n داشته باشیم $\frac{\mathbb{Z}}{p^n} = \{\frac{a}{p^n} \mid a \in \mathbb{Z}\}$، در این صورت کدام‌یک از گزینه‌های زیر نادرست است؟

۱) $\frac{\mathbb{Z}}{p^n}$ زیرگروهی از گروه جمعی اعداد گویا است.

۲) به ازای هر $n \in \mathbb{N}$، $\frac{\mathbb{Z}}{p^n} \leq \frac{\mathbb{Z}}{p^{n+1}}$

۳) $\bigcup_{n=1}^{\infty} \frac{\mathbb{Z}}{p^n}$ نمی‌تواند زیرگروهی از گروه جمعی اعداد گویا باشد.

۴) $\bigcap_{p} \frac{\mathbb{Z}}{p^n} = \mathbb{Z}$

☑ **پاسخ:** گزینه «۳» ابتدا درستی گزینه‌های ۱ و ۲ را ثابت می‌کنیم، داریم:

گزینه‌ی «۱» درست است $\Rightarrow \frac{a}{p^n}, \frac{b}{p^n} \in \frac{\mathbb{Z}}{p^n} \Rightarrow a, b \in \mathbb{Z} \Rightarrow a - b \in \mathbb{Z} \Rightarrow \frac{a}{p^n} - \frac{b}{p^n} = \frac{a-b}{p^n} \in \frac{\mathbb{Z}}{p^n} \Rightarrow \frac{\mathbb{Z}}{p^n} \leq (\mathbb{Q}, +)$

گزینه‌ی «۲» درست است $\Rightarrow x \in \frac{\mathbb{Z}}{p^n} \Rightarrow \exists a \in \mathbb{Z} \;;\; x = \frac{a}{p^n} = \frac{ap}{p^{n+1}} \in \frac{\mathbb{Z}}{p^{n+1}} \Rightarrow \frac{\mathbb{Z}}{p^n} \subseteq \frac{\mathbb{Z}}{p^{n+1}} \xrightarrow{\frac{\mathbb{Z}}{p^n} \leq \mathbb{Q}} \frac{\mathbb{Z}}{p^n} \leq \frac{\mathbb{Z}}{p^{n+1}}$

گزینه‌ی «۳» نادرست است، زیرا در قضیه‌ای ثابت کردیم که اگر به ازای خانواده‌ی $\{H_i\}_{i \in I}$ از زیرگروه‌های گروه دلخواه G، زیرگروهی چون $H_k \leq G$ موجود باشد به طوری که به ازای هر $i \in I$، $H_i \subseteq H_k$، آن‌گاه $\bigcup_{i \in I} H_i \leq G$، اما در گزینه‌ی «۲» ثابت کردیم به ازای هر $n \in \mathbb{N}$، $\frac{\mathbb{Z}}{p^n} \leq \frac{\mathbb{Z}}{p^{n+1}}$،

فصل پنجم

«همریختی گروه‌ها»

در فصل یک با مفهوم همریختی جبرها آشنا شدیم. همریختی بین دو جبر A و B از نوع τ، نگاشتی چون $\alpha : A \to B$ است که به ازای هر عمل n تایی روی مجموعه‌ی A و $a_1,...,a_n \in A$ داشته باشیم $\alpha(f^A(a_1,....a_n)) = f^B(\alpha(a_1),...,\alpha(a_n))$. حال اگر مجموعه‌های A و B دو گروه باشند، آن‌گاه واضح است که A و B جبرهایی از نوع $\tau = (2)$ هستند، بنابراین تنها یک عمل دوتایی روی A تعریف می‌شود. در این حالت، همریختی موجود بین A و B را همریختی گروه‌ها می‌نامیم. در این فصل، به تفصیل با مفهوم همریختی گروه‌ها آشنا شده و خواص آن را بررسی می‌کنیم. در نهایت قضایایی مهم موسوم به قضایای یکریختی را ارائه می‌دهیم.

درسنامه (۱): همریختی‌ها

❖ **تعریف ۱:** فرض کنید $(G,.)$ و $(H,*)$ دو گروه بوده و $\varphi : G \to H$ یک تابع باشد، در این‌صورت φ را یک **همریختی (هوموورفیسم)** می‌نامیم، هرگاه برای هر دو عضو a و b در G داشته باشیم $\varphi(a.b) = \varphi(a) * \varphi(b)$. برای راحتی کار نماد $.$ و $*$ را حذف کرده و می‌نویسیم $\varphi(ab) = \varphi(a)\varphi(b)$.

توجه داشته باشید که عمل بین a و b عمل تعریف شده روی G و عمل بین $\varphi(a)$ و $\varphi(b)$ عمل تعریف شده روی H می‌باشد.

مثال ۱: فرض کنید H و G دو گروه و $\varphi : G \to H$ نگاشت همانی باشد، یعنی به ازای هر $x \in G$، $\varphi(x) = e_H$. در این صورت φ یک همریختی خواهد بود، زیرا به ازای هر $x,y \in G$ داریم $\varphi(xy) = e_H = e_H e_H = \varphi(x)\varphi(y)$.

◆ ◆ ◆ ◆

مثال ۲: به ازای گروه G، تابع ثابت $\varphi : G \to G$ با ضابطه‌ی $\varphi(x) = x$ یک همریختی خواهد بود، زیرا به ازای هر $x,y \in G$ داریم:

$$\varphi(xy) = xy = \varphi(x)\varphi(y)$$

◆ ◆ ◆ ◆

مثال ۳: کدام‌یک از نگاشت‌های زیر همریختی نمی‌باشد؟

۱) $\varphi : (\mathbb{R},+) \to (\mathbb{R},.)$ با ضابطه‌ی $\varphi(x) = e^x$

۲) $\varphi : (\mathbb{Z},+) \to (\mathbb{Z},+)$ با ضابطه‌ی $\varphi(n) = n^2$

۳) $\varphi : V_4 \to V_4$ با ضابطه‌ی $\varphi(a) = \varphi(e) = e$ و $\varphi(b) = \varphi(c) = a$

۴) $\varphi : G \to (\mathbb{R}^*,.)$ با ضابطه‌ی $\varphi(A) = \det A$، وقتی $G = GL(2,\mathbb{R})$ مجموعه‌ی ماتریس‌های 2×2 با درایه‌های حقیقی باشد.

☑ **پاسخ:** گزینه «۲» زیرا می‌بینیم که به ازای هر $m,n \in \mathbb{Z}$، $\varphi(m+n) = (m+n)^2 \neq m^2 + n^2 = \varphi(m) + \varphi(n)$، پس φ همریختی نیست. گزینه‌ی «۱» درست است، زیرا به ازای هر $x,y \in \mathbb{R}$، $\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$. گزینه‌ی«۳» نیز درست است، به خاطر داریم که در گروه چهارتایی کلاین V_4، $a^2 = b^2 = c^2 = e$، $ab = c$، $ac = b$ و $bc = a$

حال می‌بینیم که:

$$\varphi(ae) = \varphi(a) = e = ee = \varphi(a)\varphi(e),\quad \varphi(be) = \varphi(b) = a = ae = \varphi(b)\varphi(e),\quad \varphi(ce) = \varphi(c) = a = ae = \varphi(c)\varphi(e)$$

$$\varphi(ab) = \varphi(c) = a = ea = \varphi(a)\varphi(b),\quad \varphi(ac) = \varphi(b) = a = ea = \varphi(a)\varphi(c),\quad \varphi(bc) = \varphi(a) = e = aa = \varphi(b)\varphi(c)$$

گزینه‌ی «۴» هم درست است زیرا $\varphi(AB) = \det(AB) = \det A \det B = \varphi(A)\varphi(B)$.

❖ **تعریف ۲:** فرض کنید $\varphi: G \to H$ یک همریختی گروه‌ها باشد، در این صورت:

الف) اگر φ یک به یک باشد، آن را **تکریختی (مونومورفیسم)** می‌نامیم.

ب) اگر φ پوشا باشد، آن را **برووریختی (اپی مورفیسم)** می‌نامیم.

ج) اگر φ یک به یک و پوشا باشد، آن را **یکریختی (ایزومورفیسم)** می‌نامیم. در این صورت G و H با یکدیگر یکریخت می‌باشند و می‌نویسیم $G \cong H$.

حال در مثال زیر، تکریختی، برووریختی و یکریختی بودن چند همریختی را بررسی می‌کنیم.

مثال ۴:

۱ـ همریختی ثابت صفر یعنی $\varphi: G \xrightarrow[a\to e]{} H$ را در نظر می‌گیریم. به ازای هر $a,b \in G$ که $a \neq b$، $\varphi(a) = \varphi(b) = e$. پس φ تکریختی نیست.

۲ـ همریختی همانی یعنی $\varphi: G \xrightarrow[x\to x]{} G$ یک یکریختی است.

۳ـ همریختی $\varphi: (\mathbb{Z},+) \xrightarrow[n\to 2n]{} (\mathbb{Z},+)$ تکریختی است ولی برووریختی نیست. زیرا اگر $3 \in \mathbb{Z}$ را در نظر بگیریم، ۳ در برد φ قرار ندارد.

۴ـ همریختی $\varphi: (\mathbb{Z},+) \xrightarrow[m\to \bar{m}]{} (\mathbb{Z}_n,+)$ تکریختی نیست زیرا مثلاً اگر $\mathbb{Z}_3 = \{\bar{0},\bar{1},\bar{2}\}$ را در نظر بگیریم، آن‌گاه $\varphi(1) = \bar{1} = \bar{4} = \varphi(4)$.

۵ـ همریختی $\varphi: GL(2,\mathbb{R}) \xrightarrow[A\to \det A]{} (\mathbb{R}^*,\cdot)$ تکریختی نیست زیرا اگر دو ماتریس $A = \begin{bmatrix} 1 & 3 \\ 4 & 2 \end{bmatrix}$ و $B = \begin{bmatrix} 2 & 2 \\ 8 & 3 \end{bmatrix}$ را در نظر بگیریم، آن‌گاه می‌بینیم که $\det A = \det B = -10$ در حالی که $A \neq B$.

❖ **تعریف ۳:** اگر $\varphi: G \to G$ یک یکریختی باشد، آن‌گاه آن را **خودریختی (اتومورفیسم)** نامیده و مجموعه تمام خودریختی‌های گروه G را با $\mathbf{AutG}$ نمایش می‌دهیم.

قضیه ۱: رابطه‌ی یکریختی روی هر مجموعه‌ی دلخواه از گروه‌ها، یک رابطه هم‌ارزی است.

اثبات: فرض می‌کنیم X مجموعه‌ی همه‌ی گروه‌ها باشد. روی X رابطه‌ی $\cong$ را به صورت $G,H \in X;\ G \cong H \Leftrightarrow \exists f: G \to H$ تعریف می‌کنیم، که در آن f یک یکریختی است. ثابت می‌کنیم $\cong$ انعکاسی، متقارن و متعدی است. با توجه به این که برای هر گروه G، تابع همانی $i: G \to G$ با ضابطه‌ی $i(x) = x$ یکریختی است، داریم $G \cong G$، پس $\cong$ انعکاسی است. حال فرض می‌کنیم $f: G \to H$ یک یکریختی باشد، چون f دو سویی است، تابع $f^{-1}: G \to H$ وجود دارد، حال نشان می‌دهیم f^{-1} هم یک همریختی است، برای این منظور فرض می‌کنیم $a,b \in H$، بنابراین به ازای $x,y \in G$ داریم $f^{-1}(a) = x$ و $f^{-1}(b) = y$، در نتیجه خواهیم داشت:

$$a = f(x), b = f(y) \Rightarrow ab = f(x)f(y) = f(xy) \Rightarrow f^{-1}(ab) = f^{-1}(f(xy)) = xy = f^{-1}(a)f^{-1}(b) \Rightarrow f^{-1} \text{ یک همریختی است}$$

از این رو $G \cong H$، یعنی $\cong$ رابطه‌ای متقارن است.

حال فرض می‌کنیم $G,H,K \in X$، $G \cong H$ و $H \cong K$. بنابراین یکریختی‌هایی مثل $f: G \to H$ و $g: H \to K$ وجود دارند. $gof: G \to K$ یک تابع دوسویی است، همچنین از همریختی بودن f و g نتیجه می‌شود:

$$\forall x,y \in G;\ (gof)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = gof(x)gof(y) \Rightarrow gof \text{ همریختی است}$$

لذا gof یک یکریختی است و $G \cong K$، یعنی $\cong$ یک رابطه‌ی متعدی است.

نتیجه: فرض کنید G یک گروه باشد. در این صورت مجموعه‌ی $\mathrm{Aut}G$ تحت قانون ترکیب توابع تشکیل یک گروه می‌دهد.

در این‌جا به چند قضیه اشاره کرده و در آنها ویژگی‌های مهمی از همریختی‌ها را بیان می‌کنیم .

قضیه ۲: فرض کنید $\varphi: G \to H$ یک همریختی باشد، در این صورت داریم:

الف) $\varphi(e_G) = e_H$

ب) به ازای هر $x \in G$، داریم $\varphi(x^{-1}) = (\varphi(x))^{-1}$

ج) به ازای هر $x \in G$ و $n \in \mathbb{Z}$، $\varphi(x^n) = (\varphi(x))^n$

د) به ازای هر $x \in G$ داریم $o(\varphi(x)) \mid o(x)$، همچنین اگر φ یک تکریختی باشد، آن‌گاه $o(\varphi(x)) = o(x)$.

اثبات: الف) داریم: $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \xrightarrow{\text{قانون حذف}} \varphi(e_G) = e_H$

ب) $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) \Rightarrow \varphi(x^{-1}) = (\varphi(x))^{-1}$

ج) با استقرار روی n، این قسمت را اثبات می‌کنیم. ابتدا فرض می‌کنیم $n > 0$. درحالت $n = 1$ تساوی واضح است، فرض می‌کنیم برای n هم درست باشد یعنی $\varphi(x^n) = (\varphi(x))^n$ و نشان می‌دهیم برای $n+1$ نیز درست است. از آن‌جایی که $x^{n+1} = xx^n$، داریم:

$\varphi(x^{n+1}) = \varphi(xx^n) = \varphi(x)\varphi(x^n) = \varphi(x)(\varphi(x))^n = (\varphi(x))^{n+1}$

اگر $n = 0$، آن‌گاه طبق قسمت الف داریم $\varphi(x^0) = \varphi(e_G) = e_H = (\varphi(x))^0$.

اگر $n < 0$، آن‌گاه با استفاده از حالت $n > 0$ و قسمت ب قضیه داریم: $\varphi(x^n) = (\varphi(x^{-1})^{-n}) = (\varphi(x^{-1}))^{-n} = (\varphi(x)^{-1})^{-n} = (\varphi(x))^n$

د) فرض می‌کنیم $o(x) = n$، لذا داریم: $x^n = e_G \Rightarrow \varphi(x^n) = \varphi(e_G) \Rightarrow (\varphi(x))^n = e_H \Rightarrow o(\varphi(x)) \mid n$

اکنون فرض می‌کنیم φ یک تکریختی است و $o(\varphi(x)) = m$، در این صورت داریم:

$(\varphi(x))^m = e_H \Rightarrow \varphi(x^m) = \varphi(e_G) \Rightarrow x^m = e_G \Rightarrow o(x) = n \mid m \Rightarrow n = m$

➢ **توجه:** از قضیه‌ی بالا می‌توانیم برای اثبات وجود یا عدم وجود یک تکریختی بین دو گروه استفاده کنیم، به مثال زیر توجه کنید.

مثال ۵: نشان دهید هیچ تکریختی از گروه $(\mathbb{Z}_4, +)$ به گروه $(\mathbb{Z}_{10}, +)$ وجود ندارد.

اثبات: فرض کنیم $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_{10}$ یک همریختی باشد. $t \in \mathbb{Z}_4$ عضوی از مرتبه‌ی ۴ است. اگر φ تکریختی باشد باید داشته باشیم $o(\varphi(t)) = o(t) = 4$، اما $\varphi(t)$ عضوی از $\mathbb{Z}_{10}$ است. در $\mathbb{Z}_{10}$ عنصری از مرتبه ۴ وجود ندارد. پس φ نمی‌تواند تکریختی باشد.

◆ ◆ ◆ ◆

مثال ۶: فرض کنید G و H دو گروه باشند به طوری که $(o(G), o(H)) = 1$. در این صورت چند همریختی بین G و H وجود دارد؟

۱) ۱　　۲) $(o(G))^{o(H)}$　　۳) $(o(H))^{o(G)}$　　۴) $o(G) \times o(H)$

☑ **پاسخ:** گزینه «۱» فرض می‌کنیم $\varphi : G \to H$ یک همریختی باشد. چون مرتبه‌ی هر عضو مرتبه‌ی گروه را عاد می‌کند، به ازای هر $x \in G$ داریم $o(x) \mid o(G)$ و $o(\varphi(x)) \mid o(H)$. اما مطابق قضیه‌ی فوق، $o(\varphi(x)) \mid o(x)$ پس $o(\varphi(x)) \mid o(G)$. در نتیجه:

$o(\varphi(x)) \mid (o(G), o(H)) = 1 \Rightarrow o(\varphi(x)) = 1 \Rightarrow \varphi(x) = e \quad \forall x \in G \Rightarrow$ تنها همریختی ثابت صفر بین G و H وجود دارد

◆ ◆ ◆ ◆

مثال ۷: فرض کنید p و q دو عدد اول متمایز باشند، تعداد همریختی‌ها از گروه $\mathbb{Z}_{p^2}$ به گروه $\mathbb{Z}_{q^2}$ برابر است با: (سراسری ۹۱)

۱) ۰　　۲) ۱　　۳) p　　۴) q

☑ **پاسخ:** گزینه «۲» طبق مثال قبل چون $(p^2, q^2) = 1$، بنابراین تنها همریختی همانی بین $\mathbb{Z}_{p^2}$ و $\mathbb{Z}_{q^2}$ وجود دارد.

◆ ◆ ◆ ◆

مثال ۸: تعداد همریختی‌ها از گروه دوری مرتبه ۶۰ به گروه دوری مرتبه ۴۵ چندتاست؟ (سراسری ۸۹)

۱) ۵　　۲) ۱۵　　۳) ۱۲　　۴) ۱۶

☑ **پاسخ:** گزینه «۲» فرض می‌کنیم G و H دو گروه دوری باشند به طوری که $o(G) = 60$ و $o(H) = 45$. در این صورت به ازای یک $a \in G$ و $b \in H$ داریم $G = \langle a \rangle = \{e, a, ..., a^{59}\}$ و $H = \langle b \rangle = \{e, b, ..., b^{44}\}$. اگر $\varphi : G \to H$ یک همریختی باشد، آنگاه چون عناصر H توان‌هایی از b هستند، می‌توانیم ضابطه‌ی φ را به صورت $\varphi(a) = b^n$ که $0 \le n < 45$ تعریف کنیم. طبق قضیه‌ای $o(b^n) = o(\varphi(a)) \mid o(a) = 60$، بنابراین $b^{60n} = (b^n)^{60} = e$، از طرفی چون $o(b) = 45$، داریم:

$45 \mid 60n \Rightarrow \frac{45}{15} \mid \frac{60n}{15} \Rightarrow 3 \mid 4n \xrightarrow{(3,4)=1} 3 \mid n \xrightarrow{0 \le n < 45} n = 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42$

در نتیجه ۱۵ همریختی به صورت $b^0 = e, b^3, b^6, b^9, b^{12}, b^{15}, b^{18}, b^{21}, b^{24}, b^{27}, b^{30}, b^{33}, b^{36}, b^{39}, b^{42}$ بین G و H وجود دارد.

◆ ◆ ◆ ◆

قضیه ۳: فرض کنید $\varphi : G \to H$ یک همریختی باشد، در این صورت:

الف) اگر $K \le G$، آن‌گاه $\varphi(K) = \{\varphi(k) \mid k \in K\}$ زیرگروهی از H است.

ب) اگر $L \le H$، آن‌گاه $\varphi^{-1}(L) = \{g \in G \mid \varphi(g) \in L\}$ زیرگروهی از G است.

ج) اگر φ پوشا باشد و $K \trianglelefteq G$، آن‌گاه $\varphi(K) \trianglelefteq H$.

د) اگر $L \trianglelefteq H$، آن‌گاه $\varphi^{-1}(L) \trianglelefteq G$.

اثبات: الف) چون $\varphi(e_G) = e_H$، داریم $e_H \in \varphi(K)$، پس $\varphi(K)$ ناتهی است، از طرفی به ازای هر $\varphi(a)\ \varphi(b) \in \varphi(K)$، که در آن $a, b \in K$ داریم:

$$(\varphi(a))^{-1}\varphi(b)=\varphi(a^{-1})\varphi(b)=\varphi(a^{-1}b)\in\varphi(K)$$

بنابراین طبق محک زیرگروه $\varphi(K)\le H$.

ب) چون $\varphi(e_G)=e_H$ داریم $e_G\in\varphi^{-1}(L)$، پس $\varphi^{-1}(L)$ ناتهی است، همچنین به ازای هر $x,y\in\varphi^{-1}(L)$، داریم $\varphi(x)\ \varphi(y)\in L$، بنابراین خواهیم داشت:

$$(\varphi(x))^{-1}\varphi(y)\in L\Rightarrow\varphi(x^{-1})\varphi(y)\in L\Rightarrow\varphi(x^{-1}y)\in L\Rightarrow x^{-1}y\in\varphi^{-1}(L)$$

در نتیجه طبق محک زیرگروه $\varphi^{-1}(L)\le G$.

ج) برای این که ثابت کنیم $\varphi(K)\trianglelefteq H$، باید نشان دهیم به ازای هر $x\in H$ و هر $y\in\varphi(K)$، $xyx^{-1}\in\varphi(K)$. چون $y\in\varphi(K)$ عضو $a\in K$ موجود است به طوری که $\varphi(a)=y$ و چون φ پوشا است، عضو $b\in G$ موجود است به طوری که $\varphi(b)=x$. در این صورت از آن‌جایی که $K\trianglelefteq G$ داریم:

$$xyx^{-1}=\varphi(b)\varphi(a)(\varphi(b))^{-1}=\varphi(b)\varphi(a)\varphi(b^{-1})=\varphi(\underbrace{bab^{-1}}_{\in K})\in\varphi(K)\Rightarrow\varphi(K)\trianglelefteq G$$

د) برای این‌که ثابت کنیم $\varphi^{-1}(L)\trianglelefteq G$ کافی است نشان دهیم به ازای هر $x\in G$ و $y\in\varphi^{-1}(L)$، $xyx^{-1}\in\varphi^{-1}(L)$. چون $\varphi(y)\in L$ و $L\trianglelefteq H$، داریم:

$$\varphi(xyx^{-1})=\varphi(x)\varphi(y)\varphi(x^{-1})=\varphi(x)\varphi(y)(\varphi(x))^{-1}\in L\Rightarrow xyx^{-1}\in\varphi^{-1}(L)\ \Rightarrow\varphi^{-1}(L)\trianglelefteq G$$

تذکر۱: شرط پوشا بودن در قسمت ج قضیه‌ی فوق الزامی است. برای درک بهتر مطلب به مثال زیر توجه کنید.

مثال۹: اگر $G=(\mathbb{Z}_4,+)$، $H=S_3$ و $\varphi:G\to H$ به صورت $\varphi(\circ)=e$ و $\varphi((23))=(1)$ تعریف شود، آن‌گاه φ یک همریختی است اما پوشا نمی‌باشد، چون مثلاً برای $(12)\in S_3$ عضوی چون g در $\mathbb{Z}_4$ موجود نیست که $\varphi(g)=(12)$. قرار می‌دهیم $K=G$، در این صورت $K\trianglelefteq G$، اما $\{e,(23)\}=<(23)>=\varphi(K)$ در S_3 نرمال نیست، زیرا می‌بینیم که $(13)=(12)(23)(12)^{-1}\notin\varphi(K)$.

قضیه ۴: فرض کنید $\varphi:G\to H$ یک همریختی باشد، در این صورت

الف) اگر H آبلی و φ تکریختی باشد، آن‌گاه G آبلی است. **ب) اگر G آبلی و φ بروریختی باشد، آن‌گاه H آبلی است.**

اثبات: (الف) به ازای هر $a,b\in G$، داریم $\varphi(a),\varphi(b)\in H$. چون H آبلی است، $\varphi(a)\varphi(b)=\varphi(b)\varphi(a)$، لذا می‌بینیم که:

$$\varphi(ab)=\varphi(a)\varphi(b)=\varphi(b)\varphi(a)=\varphi(ba)\xrightarrow{\varphi\text{ تکریختی است}}ab=ba\Rightarrow G\text{ آبلی است}$$

(ب) فرض می‌کنیم $a,b\in H$، چون φ پوشاست، اعضای $x,y\in G$ موجودند به طوری که $\varphi(x)=a$ و $\varphi(y)=b$. از آبلی بودن G نتیجه می‌گیریم $xy=yx$، بنابراین داریم:

$$ab=\varphi(x)\varphi(y)=\varphi(xy)=\varphi(yx)=\varphi(y)\varphi(x)=ba\ \Rightarrow\ H\text{ آبلی است}$$

تذکر۲: با توجه به قضیه‌ی بالا می‌توانیم بگوییم اگر $\varphi:G\to H$ یک یکریختی باشد، آن‌گاه G آبلی است اگر و تنها اگر H آبلی باشد و از این حکم می‌توانیم برای تشخیص یکریختی بین گروه‌ها استفاده کنیم، به طور مثال با وجود این که مرتبه‌ی S_3 و $\mathbb{Z}_6$ یکی است اما چون $(\mathbb{Z}_6,+)$ آبلی است و S_3 آبلی نیست، طبق قضیه‌ی قبل، هیچ یکریختی بین S_3 و $\mathbb{Z}_6$ وجود ندارد.

مثال ۱۰: کدام یک از گزینه‌های زیر صحیح می‌باشد؟

۱) $(\mathbb{R},+)\cong(\mathbb{R}^+,\cdot)$ ۲) $(\mathbb{Q},+)\cong(\mathbb{Q}^+,\cdot)$ ۳) $(\mathbb{R}^*,\cdot)\cong GL(2,\mathbb{R})$ ۴) $(\mathbb{Z}_4,+)\cong V_4$

☑ **پاسخ:** گزینه «۱» همریختی $\varphi(x)=e^x$ یک یکریختی از $(\mathbb{R},+)$ به $(\mathbb{R}^+,\cdot)$ می‌باشد. گزینه‌ی «۲» نادرست است زیرا همان طور که می‌بینیم هر عضو $q\in(\mathbb{Q},+)$ دارای ریشه دوم $\frac{q}{2}$ می‌باشد. در حالی که بعضی از اعضای $(\mathbb{Q}^+,\cdot)$ ریشه دوم ندارند، مثلاً عضوی مانند x در $(\mathbb{Q}^+,\cdot)$ وجود ندارد که $x^2=3$. اگر فرض کنیم $\varphi:(\mathbb{Q},+)\to(\mathbb{Q}^+,\cdot)$ یک یکریختی باشد، آن‌گاه به ازای $3\in(\mathbb{Q}^+,\cdot)$ حتماً عضوی چون $q\in(\mathbb{Q},+)$ وجود دارد به طوری که $\varphi(q)=3$، اما می‌دانیم $\varphi(q)=3=\varphi(\frac{q}{2}+\frac{q}{2})=\varphi(\frac{q}{2})\varphi(\frac{q}{2})=(\varphi(\frac{q}{2}))^2$، یعنی ریشه دوم۳ در $(\mathbb{Q}^+,\cdot)$ وجود دارد که این تناقض می‌باشد. پس φ نمی‌تواند یکریختی باشد. گزینه‌ی «۳» نادرست است، زیرا می‌دانیم $\mathbb{R}$ گروهی آبلی است ولی از آن‌جایی‌که ضرب ماتریس‌ها خاصیت جابه‌جایی ندارد، $GL(2,\mathbb{R})$ ناآبلی است، پس $\mathbb{R}^*$ و $GL(2,\mathbb{R})$ نمی‌توانند یکریخت باشند.

فصل ششم

«حاصل‌ضرب مستقیم گروه‌ها»

در این فصل به معرفی یک نوع گروه جدید می‌پردازیم که از حاصل‌ضرب گروه‌های دیگر ساخته می‌شود. در ادامه خواص این نوع گروه را بیان کرده و به بررسی این موضوع می‌پردازیم که آیا حاصل ضرب گروه‌های آبلی و دوری، آبلی و دوری می‌باشد یا نه.

درسنامه: حاصل‌ضرب مستقیم خارجی گروه‌ها

❖ **تعریف ۱:** فرض کنید $G_1, G_2, \ldots, G_n$، n گروه باشند که لزوماً متمایز نیستند، **حاصل‌ضرب مستقیم خارجی** به صورت زیر تعریف می‌شود:

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i, 1 \le i \le n\}$$

مثال۱: دو گروه جمعی $\mathbb{Z}_2$ و $\mathbb{Z}_4$ را در نظر بگیرید و حاصل ضرب مستقیم آنها را بیابید.

☑ **پاسخ:** مطابق تعریف حاصل‌ضرب مستقیم داریم $\mathbb{Z}_4 \times \mathbb{Z}_2 = \{0,1,2,3\} \times \{0,1\} = \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1),(3,0),(3,1)\}$

◆ ◆ ◆ ◆

قضیه ۱: برای گروه‌های $G_1, G_2, \ldots, G_n$، حاصل ضرب مستقیم خارجی گروه‌ها با عمل $*$ که به صورت زیر تعریف می‌شود، یک گروه خواهد بود.

$$\forall (g_1, \ldots, g_n), (g'_1, \ldots, g'_n) \in G_1 \times \cdots \times G_n \ , \ (g_1, \ldots, g_n) * (g'_1, \ldots, g'_n) = (g_1 * g'_1, \ldots, g_n * g'_n)$$

عضو همانی این گروه به صورت $(e, \ldots, e)$ و معکوس هر عضو مانند $(g_1, \ldots, g_n)$ به صورت $(g_1^{-1}, \ldots, g_n^{-1})$ می‌باشد.

مثال۲: گروه $\mathbb{Z} \times \mathbb{Z}$ را در نظر بگیرید و عضو همانی و معکوس هر عضو آن را مشخص کنید.

☑ **پاسخ:** گروه $\mathbb{Z} \times \mathbb{Z}$ به صورت $\{(k,k') \mid k,k' \in \mathbb{Z}\}$ می‌باشد. عضو همانی این گروه $(0,0)$ و معکوس هر عضو (k,k') به صورت $(-k,-k')$ خواهد بود.

◆ ◆ ◆ ◆

مثال ۳: کدام مجموعه همراه با عمل داده شده تشکیل یک گروه می‌دهد؟ (سراسری ۹۴)

۱) $(\mathbb{R}, \times)$

۲) $a * b = \frac{a}{5}, (\mathbb{Q}, *)$

۳) $(a,b) * (c,d) = (ad + bc, bd), (\mathbb{Z} \times \mathbb{Z}, *)$

۴) $A = \{x \in \mathbb{R} \mid 0 \le x < 1\}$ و $x * y = x + y - [x + y]$ که در آن $[z]$ جزء صحیح z است.

☑ **پاسخ :گزینه «۴»** در مجموعه $(\mathbb{R}, 0)$، صفر دارای وارون ضربی نمی‌باشد. بنابراین گزینه (۱) صحیح نمی‌باشد.

در مجموعه $(\mathbb{Q}, *)$ عمل $*$ شرکت‌پذیر نمی‌باشد زیرا: $x * (y * z) = \frac{x}{5}$ و $(x * y) * z = \frac{(x * y)}{5} = \frac{x}{25}$

بنابراین $x * (y * z) \neq (x * y) * z$، پس گزینه (۲) نادرست است.

با فرض گروه بودن $(\mathbb{Z} \times \mathbb{Z}, *)$ عضو خنثی عمل گروه و عضو وارون هر عنصر دلخواه را جستجو می‌کنیم: اگر (e_1, e_2) عضو خنثی گروه باشد باید:

$$(x,y) \times (e_1, e_2) = (x,y) \Rightarrow (xe_2 + ye_1, ye_2) = (x,y) \Rightarrow e_2 = 1 \ x + ye_1 = x \Rightarrow (0\ ,\ 1) = (e_1, e_2)$$

اینک با فرض اینکه $(0,1)$ عنصر خنثی است به دنبال یافتن وارون $(2,2)$ هستیم:

$$(2,2)(x,y) = (0,1) \Rightarrow (2x + 2y, 2y) = (0,1) \Rightarrow y = \frac{1}{2} \notin z$$

پس $(2,2)$ دارای عضو وارون نمی‌باشد، در نتیجه گزینه (۳) صحیح نمی‌باشد.

بررسی گزینه (۴): واضح است مجموعه A تحت عمل مورد نظر بسته می‌باشد.

$$x*(y*z)=x+y*z-[x+y*z]=x+y+z-[y+z]-[x+y+z-[y+z]]=x+y+z-[x+y+z]$$
$$=x+y-[x+y]+z-[x+y-[x+y]+z]=x*y+z-[x*y+z]=(x*y)*z.$$

محاسبات بالا شرکت‌پذیری عمل $*$ را نتیجه می‌دهد. عدد 0 عضو همانی است زیرا: $x*0=x+0-[x+0]=x-[x]=x$

همچنین هر عضو $x\in A-\{0\}$ دارای معکوسی به شکل $x^{-1}=(1-x)$ می‌باشد، چون همان‌طورکه می‌بینیم $x*(1-x)=x+(1-x)-[x+1-x]=0$.
بنابراین گزینه (۴) گزینه مورد نظر است.

مثال۴: کدام‌یک از گزینه‌های زیر نادرست است؟

۱) اگر G' و H' به ترتیب زیرگروه‌های G و H باشند، آن‌گاه $G'\times H'$ زیرگروه $G\times H$ می‌باشد.
۲) هر زیرگروه $G\times H$ به صورت $G'\times H'$ می‌باشد که $H'\le H$ و $G'\le G$.
۳) برای n گروه متناهی $G_1,G_2,...,G_n$ داریم $o(G_1\times\cdots\times G_n)=o(G_1)\times\cdots\times o(G_n)$
۴) برای n گروه $G_1,G_2,...,G_n$ داریم $Z(G_1\times\cdots\times G_n)=Z(G_1)\times\cdots\times Z(G_n)$

☑ **پاسخ:** گزینه «۲» گروه $\mathbb{Z}_2=\{0,1\}$ فقط دارای دو زیرگروه بدیهی $\langle 0\rangle$ و $\mathbb{Z}_2$ می‌باشد، اما گروه $\mathbb{Z}_2\times\mathbb{Z}_2=\{(0,0),(0,1),(1,0),(1,1)\}$ علاوه بر زیرگروه‌های $\langle 0\rangle\times\langle 0\rangle$، $\mathbb{Z}_2\times\langle 0\rangle$، $\langle 0\rangle\times\mathbb{Z}_2$ و $\mathbb{Z}_2\times\mathbb{Z}_2$ زیرگروه دیگری دارد که این زیرگروه $\langle(1,1)\rangle=\{(0,0),(1,1)\}$ می‌باشد. پس ممکن است گروه $G\times H$ علاوه بر زیرگروه‌هایی به فرم $G'\times H'$ که $H'\le H$ و $G'\le G$، زیرگروه‌های دیگری هم داشته باشد. لذا گزینه‌ی «۲» نادرست است.
گزینه‌ی «۱» درست است. اگر e_H و e_G به ترتیب عضو همانی H و G باشد، آن‌گاه $e_H\in H'$ و $e_G\in G'$، بنابراین داریم $(e_G,e_H)\in G'\times H'$، لذا $G'\times H'$ دارای عضو همانی می‌باشد. از طرفی به ازای هر $(g_1,h_1),(g_2,h_2)\in G'\times H'$ داریم:

$$\begin{matrix}g_1,g_2\in G'\Rightarrow g_1g_2^{-1}\in G'\\ h_1,h_2\in H'\Rightarrow h_1h_2^{-1}\in H'\end{matrix}\Rightarrow (g_1,h_1)(g_1,h_1)^{-1}=(g_1,h_1)(g_2^{-1},h_2^{-1})=(g_1g_2^{-1},h_1h_2^{-1})\in G'\times H'$$

در نتیجه $G'\times H'$ زیرگروهی از $G\times H$ می‌باشد. گزینه‌ی ۳ هم درست است. به استقرا روی n حکم را ثابت می‌کنیم. فرض می‌کنیم $n=2$، $o(G_1)=m_1$ و $o(G_2)=m_2$، داریم $o(G_1\times G_2)=m_1m_2=o(G_1)o(G_2)$. حال فرض می‌کنیم به ازای $n=k$ حکم برقرار باشد، یعنی $o(G_1\times\cdots\times G_k)=o(G_1)\cdots o(G_k)$، برای $n=k+1$ خواهیم داشت:

$$o(G_1\times\cdots\times G_k\times G_{k+1})=o(G_1\times\cdots\times G_k)o(G_{k+1})=o(G_1)\cdots o(G_k)o(G_{k+1})$$

گزینه‌ی «۴» نیز درست است. داریم:

$$(x_1,\ldots,x_n)\in Z(G)\Leftrightarrow (x_1,\ldots,x_n)(y_1,\ldots,y_n)=(y_1,\ldots,y_n)(x_1,\ldots,x_n),\forall(y_1,...y_n)\in G\Leftrightarrow(x_1y_1,\ldots,x_ny_n)=$$
$$(y_1x_1,\ldots,y_nx_n)\Leftrightarrow x_1y_1=y_1x_1,\ldots,x_ny_n=y_nx_n\Leftrightarrow x_1\in Z(G_1),\ldots,x_n\in Z(G_n)\Leftrightarrow(x_1,\ldots,x_n)\in Z(G_1)\times\cdots\times Z(G_n)$$

مثال۵: اگر π یک ترانهش در گروه متقارن S_n و $n\ge 2$، فرض شود، آن‌گاه $C_{S_n}(\pi)$ با کدام گروه زیر یکریخت است؟ (دکتری ۹۲)

۱) S_{n-2}　　۲) S_{n-1}　　۳) $\mathbb{Z}_2\times S_{n-2}$　　۴) $\mathbb{Z}_2\times S_{n-1}$

☑ **پاسخ :گزینه «۳»** یادآوری می‌کنیم که:

اگر α دوری به طول m در گروه S_n باشد، آن‌گاه مرتبه‌ی مرکز ساز α در S_n یعنی $C_{S_n}(\alpha)$ برابر با $m(n-m)!$ است.

با توجه به مطلب فوق و این که هر ترانهش یک دور به طول ۲ است، داریم $|C_{S_n}(\pi)|=2(n-2)!$.

اما در گزینه‌ها، از بین گروه‌های داده شده فقط $\mathbb{Z}_2\times S_{n-2}$ است که $2(n-2)!$ عضو دارد. بنابراین تنها این گزینه می‌تواند جواب باشد. پس گزینه (۳) پاسخ مورد نظر سوال می‌باشد.

مثال۶: کدام‌یک از گزینه‌های زیر نادرست است؟

۱) به ازای هر دو گروه H و G داریم $G\times H\cong H\times G$
۲) به ازای هر سه گروه H، K و G داریم $(G\times H)\times K\cong G\times(H\times K)$
۳) اگر به ازای گروه‌های G، G'، H و H' داشته باشیم $G\cong G'$ و $H\cong H'$، آن‌گاه $G\times H\cong G'\times H'$
۴) اگر به ازای گروه‌های G، G'، H و H' داشته باشیم $G\times H\cong H'\times G'$، آن‌گاه $G\cong G'$ و $H\cong H'$

☑ **پاسخ:** گزینه «۴» ابتدا درستی گزینه‌های «۱» و «۲» و «۳» را نشان می‌دهیم. گزینه‌ی «۱» درست می‌باشد. نگاشت $\varphi: G\times H \to H\times G$ را با ضابطه‌ی $\varphi(x,y)=(y,x)$ در نظر می‌گیریم. به ازای هر $(x,y),(x',y')\in G\times H$ داریم:

φ یک تابع یک به یک است $\Leftrightarrow (x,y)=(x',y')\Leftrightarrow x=x', y=y' \Leftrightarrow (y,x)=(y',x')\Leftrightarrow \varphi(x,y)=\varphi(y,x)$

φ پوشا است $\Rightarrow \varphi(G\times H)=\{\varphi(x,y)\mid x\in G, y\in H\}=\{(y,x)\mid y\in H, x\in G\}=H\times G$

φ یک همریختی است $\Rightarrow \varphi((x,y)(x',y'))=\varphi(xx',yy')=(yy',xx')=(y,x)(y',x')=\varphi(x,y)\varphi(x',y')$

در نتیجه φ یک یکریختی خواهد بود، پس $G\times H\cong H\times G$.

گزینه‌ی «۲» نیز درست می‌باشد. نگاشت $\varphi: G\times(H\times K)\to (G\times H)\times K$ را با ضابطه‌ی $\varphi(g,(h,k))=((g,h),k)$ در نظر می‌گیریم. φ یک همریختی است، زیرا به ازای هر $(g_1,(h_1,k_1)),(g_2,(h_2,k_2))\in G\times(H\times K)$ داریم:

$$\varphi((g_1,(h_1,k_1)).(g_2,(h_2,k_2)))=\varphi(g_1g_2,(h_1,k_1)(h_2,k_2))=\varphi(g_1g_2,(h_1h_2,k_1k_2))=((g_1g_2,h_1h_2),k_1k_2)$$
$$=((g_1,h_1)(g_2,h_2),\ k_1k_2)=((g_1,h_1),k_1)((g_2,h_2),k_2))=\varphi(g_1,(h_1,k_1))\varphi(g_2,(h_2,k_2))$$

هم‌چنین φ یک به یک است، زیرا به ازای هر $(g_2,(h_2,k_2)),(g_1,(h_1,k_1))\in G\times(H\times K)$ داریم:

$$\varphi(g_1,(h_1,k_1))=\varphi(g_2,(h_2,k_2))\Rightarrow((g_1,h_1),k_1)=((g_2,h_2),k_2)\Rightarrow(g_1,h_1)=(g_2,h_2),k_1=k_2\Rightarrow g_1=g_2,h_1=h_2,k_1=k_2$$
$$\Rightarrow(g_1,(h_1,k_1))=(g_2,(h_2,k_2))$$

از طرفی اگر $(g,(h,k))\in G\times(H\times K)$، آن‌گاه $g\in G$، $h\in H$ و $k\in K$، پس عضو $((g,h),k)\in(G\times H)\times K$ موجود است به طوری که $\varphi((g,h),k)=(g,(h,k))$، و این یعنی φ پوشا است، بدین ترتیب $G\times(H\times K)\cong(G\times H)\times K$.

گزینه‌ی «۳» درست است. نگاشت $\varphi: G\times H\to G'\times H'$ را به ازای هر $(a,b)\in G\times H$، با ضابطه‌ی $\varphi(a,b)=(f(a),g(b))$ در نظر می‌گیریم به طوری که $f: G\to G'$ و $g: H\to H'$ دو یکریختی باشند. چون f و g دوسویی است، φ هم یک تابع دوسویی می‌باشد. حال نشان می‌دهیم φ یک همریختی است. از آن‌جایی‌که f و g دو همریختی است، به ازای هر $a,a'\in G$ و $b,b'\in H$ داریم:

$$\varphi((a,b)(a',b'))=\varphi(aa',bb')=(f(aa'),g(bb'))=(f(a)f(a'),g(b)g(b'))=(f(a),g(b))(f(a'),g(b'))=\varphi(a,b)\varphi(a',b')$$

در نتیجه φ یک یکریختی است. گزینه‌ی (۴) نادرست می‌باشد، به طور مثال اگر $G=\mathbb{Z}_2$، $G'=\mathbb{Z}_2\times\mathbb{Z}_2$، $H=\mathbb{Z}_6$ و $H'=\mathbb{Z}_3$، آن‌گاه چون $<(1,1)>=\mathbb{Z}_2\times\mathbb{Z}_3$ پس $\mathbb{Z}_2\times\mathbb{Z}_3$ گروهی دوری از مرتبه‌ی ۶ می‌باشد، بنابراین از آن‌جایی که **گروه‌های دوری هم‌مرتبه یکریختند** داریم $\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$. از طرفی طبق گزینه‌ی ۲، $\mathbb{Z}_6\cong\mathbb{Z}_2\times\mathbb{Z}_3\cong(\mathbb{Z}_2\times\mathbb{Z}_2)\times\mathbb{Z}_3$. پس می‌توانیم یکریختی $\varphi: \mathbb{Z}_2\times\mathbb{Z}_6\to(\mathbb{Z}_2\times\mathbb{Z}_2)\times\mathbb{Z}_3$ را تعریف کنیم. توجه داشته باشید که $\varphi((1,0))=((1,0),0)$ و $\varphi((0,1))=((0,1),1)$. اما چنان‌چه می‌بینید $\mathbb{Z}_2$ با $\mathbb{Z}_2\times\mathbb{Z}_2$ و $\mathbb{Z}_6$ با $\mathbb{Z}_3$ یکریخت نیستند، چون از مرتبه‌های یکسان نیستند.

قضیه۲: فرض کنید $G=G_1\times\cdots\times G_n$. در این صورت G آبلی است اگر و تنها اگر به ازای هر $1\le i\le n$، G_i آبلی باشد.

اثبات: ابتدا فرض می‌کنیم G آبلی باشد. اگر x_i و y_i به ازای $1\le i\le n$، دو عضو از G_i باشند، آن‌گاه $(e,\ldots,e,x_i,e,\ldots,e)$ و $(e,\ldots,e,y_i,e,\ldots,e)$ دو عضو G می‌باشند. بنابراین چون G آبلی است، داریم:

$$(e,\ldots,e,x_iy_i,e,\ldots,e)=(e,\ldots,e,x_i,e,\ldots,e)(e,\ldots,e,y_i,e,\ldots,e)=(e,\ldots,e,y_i,e,\ldots,e)(e,\ldots,e,x_i,e,\ldots,e)$$
$$=(e,\ldots,e,y_ix_i,e,\ldots,e)$$

در نتیجه $x_iy_i=y_ix_i$، یعنی به ازای هر $1\le i\le n$، G_i آبلی است.

به عکس فرض می‌کنیم به ازای $1\le i\le n$، G_iها آبلی باشند، در این صورت اگر $(x_1,\ldots,x_n)$ و $(y_1,\ldots,y_n)$ دو عضو از G باشند، آن‌گاه خواهیم داشت:

$$(x_1,\ldots,x_n)(y_1,\ldots,y_n)=(x_1y_1,\ldots,x_ny_n)=(y_1x_1,\ldots,y_nx_n)=(y_1,\ldots,y_n)(x_1,\ldots,x_n)\Rightarrow G \text{ آبلی است}$$

مثال ۷: با توجه به این که گروه Q_8 آبلی نیست، طبق قضیه‌ی فوق، گروه $Q_8\times\mathbb{Z}_3\times V_4$ نمی‌تواند آبلی باشد.

مثال ۸: اگر D_8 گروه تقارن‌های مربع و Q_8 گروه کواترنیون‌های هشت عضوی باشند در این صورت در کدام گزینه مشتق گروه با بقیه فرق دارد؟
(سراسری ۹۴)

۱) $\mathbb{Z}_4\times Q_8$ ۲) $\mathbb{Z}_3\times Q_8$ ۳) $\mathbb{Z}_4\times S_3$ ۴) $\mathbb{Z}_{12}\times D_8$

☑ **پاسخ:گزینه «۳»** ابتدا لازم به ذکر است از آنجا که گروهای $\mathbb{Z}_n$ آبلی هستند، همواره مشتق آن‌ها گروه بدیهی $\{e\}$ می‌باشد. از طرفی بنابر قضیه لاگرانژ مرتبه گروه مشتق باید مرتبه گروه را عاد کند. بنابراین مشتق گروه‌های Q_8، $\mathbb{Z}_4\times Q_8$، $\mathbb{Z}_3\times D_8$ و $\mathbb{Z}_{12}\times D_8$ به ترتیب برابرند با $\{e\}$، $\{e\}\times(Q_8)'$، $\{e\}\times(D_8)'$ و $(D_8)'\times\{e\}$، که همگی از مرتبه زوج هستند اما مشتق $\mathbb{Z}_4\times S_3$ برابر است با $\{e\}\times A_3$ که از مرتبه فرد می‌باشد. بنابراین گزینه (۳) صحیح می‌باشد.

مثال۹: کدام گزینه در مورد گروه $\mathbb{Z}_4\times S_3$ صحیح است؟ (سراسری ۹۳)

۱) این گروه حداقل ۳ زیرگروه ناآبلی دارد.　　۲) این گروه دقیقاً ۳ زیرگروه آبلی دارد.

۳) تمام زیرگروه‌های آن نرمال است.　　۴) تمام زیرگروه‌های نرمال آن آبلی است.

☑ **پاسخ: گزینه «۱»** می‌دانیم گروه S_3 دارای ۶ زیرگروه به صورت $<e>$، $<(12)>$، $<(13)>$، $<(23)>$، $<(123)>$ و S_3 است که با وجود اینکه S_3 گروهی ناآبلی است، همهٔ زیرگروه‌های سره‌اش دوری و آبلی هستند. همچنین $\mathbb{Z}_4$ دارای سه زیرگروه $<0>$، $<2>$ و $\mathbb{Z}_4$ است که چون $\mathbb{Z}_4$ آبلی است، همهٔ زیرگروه‌هایش هم آبلی هستند. $\mathbb{Z}_4\times S_3$ حداقل ۱۸ زیرگروه دارد که از ضرب زیرگروه‌های S_3 در زیرگروه‌های $\mathbb{Z}_4$ به دست می‌آیند. اما $\mathbb{Z}_4\times S_3$ زیرگروه‌های دیگری هم دارد، مثلاً زیرگروه $<((12),(2,0))>$. از بین ۱۸ زیرگروه تولید شده توسط زیرگروه‌های S_3 و $\mathbb{Z}_4$، به غیر از $<e>\times S_3$، $S_3\times<2>$ و $\mathbb{Z}_4\times S_3$، همگی آبلی هستند، پس این گروه بیش از ۳ زیرگروه آبلی دارد، بنابراین گزینه ۲ رد می‌شود. اما چون S_3 ناآبلی است و اعضایش با هم جابجا نمی‌شوند، هر زیرگروه غیردوری دیگری که از ضرب اعضای $\mathbb{Z}_4$ در اعضای S_3 به دست بیایند، ناآبلی است، پس این گروه بیش از ۳ زیرگروه ناآبلی دارد. پس گزینه ۱ درست می‌باشد. گزینه ۳ نادرست است، زیرا مثلاً برای زیرگروه $<(12)>\times<2>$ می‌بینیم که به ازای عضو $((1,(13)),0)\in\mathbb{Z}_4\times S_3$، داریم:

$$((1,(13)),0)((0,(12)),0)((1,(13)),0)^{-1}=((1,(13))(0,(12))(3,(13)),0)=((0,(23)),0)\notin<2>\times<(12)>$$

پس $<(12)>\times<2>$ نرمال نیست. گزینه (۴) هم نادرست است. مثلاً $S_3\times<0>$ زیرگروه نرمال $\mathbb{Z}_4\times S_3$ است، ولی چون S_3 ناآبلی است، پس $S_3\times<0>$ هم ناآبلی خواهد بود.

اکنون قصد داریم به بررسی این موضوع بپردازیم که آیا دوری بودن $G_1\times\cdots\times G_n$ با دوری بودن G_iها مرتبط می‌باشد یا نه. به مثال‌های زیر توجه کنید.

مثال ۱۰: گروه $\mathbb{Z}\times\mathbb{Z}=\{(g_1,g_2)\mid g_1,g_2\in\mathbb{Z}\}$ را در نظر می‌گیریم. می‌دانیم که $\mathbb{Z}$ گروهی دوری با مولدهای ۱ و ۱− است اما $(1,1)$ و $(-1,-1)$ مولدهای $\mathbb{Z}\times\mathbb{Z}$ نیستند، زیرا همان طور که می‌بینیم عدد صحیحی چون k موجود نیست به طوری که $k(1,1)=(1,0)$ یا $k(-1,-1)=(0,1)$، در کل هیچ عضوی در $\mathbb{Z}\times\mathbb{Z}$ یافت نمی‌شود که $(1,0)$ یا $(0,1)$ را تولید کند، پس $\mathbb{Z}\times\mathbb{Z}$ دوری نیست.

مثال ۱۱: فرض کنید $G_1=G_2=(\mathbb{Z}_2,+)$، در این صورت $\mathbb{Z}_2\times\mathbb{Z}_2=\{(0,0),(0,1),(1,0),(1,1)\}$. می‌بینیم که $o(\mathbb{Z}_2\times\mathbb{Z}_2)=4$، اما مرتبه‌ی هر عضو غیرهمانی آن۲ می‌باشد:

$$(1,1)+(1,1)=(0,0)\quad,\quad(1,0)+(1,0)=(0,0)\quad,\quad(0,1)+(0,1)=(0,0)$$

بنابراین $\mathbb{Z}_2\times\mathbb{Z}_2$ دوری نیست.

مثال ۱۲: فرض کنید $G_1=(\mathbb{Z}_2,+)$ و $G_2=(\mathbb{Z}_3,+)$، در این صورت داریم $\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$. مشاهده می‌شود که $o(\mathbb{Z}_2\times\mathbb{Z}_3)=6=o((1,1))$، پس $\mathbb{Z}_2\times\mathbb{Z}_3$ گروهی دوری می‌باشد.

همچنانکه در مثال‌های بالا دیدیم، حاصل ضرب گروه‌های دوری لزوماً دوری نمی‌باشد، در قضایای زیر شرط دوری بودن حاصل ضرب مستقیم گروه‌ها بیان می‌شود.

قضیه۳: فرض کنید $G=G_1\times\cdots\times G_n$، در این صورت

الف) اگر به ازای هر $1\le i\le n$ داشته باشیم $g_i\in G_i$ به طوری که $o(g_i)=n_i$، آن‌گاه $o(g_1,\ldots,g_n)$ برابر است با کوچکترین مضرب مشترک $o(g_i)$ها یعنی $o((g_1,\ldots,g_n))=[o(g_1),\ldots,o(g_n)]$.

ب) اگر G دوری باشد، آن‌گاه به ازای هر $1\le i\le n$، G_i دوری خواهد بود.

ج) اگر به ازای هر $1\le i\le n$، G_i گروهی دوری باشد، آن‌گاه G دوری است اگر و تنها اگر به ازای هر $i\neq j$، $o(G_i)$ و $o(G_j)$ نسبت به هم اول باشند.

اثبات: الف) به ازای هر عدد صحیح مثبت m، داریم $(g_1,g_2,\ldots,g_n)^m=(g_1^m,g_2^m,\ldots,g_n^m)$. از طرفی اگر $(g_1,g_2,\ldots,g_n)^m=(g_1^m,g_2^m,\ldots,g_n^m)=(e_{G_1},e_{G_2},\ldots,e_{G_n})$، آن‌گاه $o(g_1)\mid m$، $o(g_2)\mid m$، ...، $o(g_n)\mid m$، بنابراین m کوچکترین عددی است که به ازای هر i، $o(g_i)\mid m$ یعنی $o(g_1,g_2,\ldots,g_n)=[o(g_1),o(g_2),\ldots,o(g_n)]$.

فصل هفتم

«حلقه‌ها»

در فصل مقدمات و پیش‌نیازها با مفهوم جبر و نوع آن آشنا شدیم، همچنین در فصول گروه‌ها جبرهایی از نوع $\tau(۲)$ را معرفی کردیم و به بررسی خواص آن‌ها پرداختیم، همانند $(\mathbb{Z},+)$، $(\mathbb{Q},+)$ و $(\mathbb{R},+)$. در فصل‌های آتی به مطالعه جبرهایی از نوع $\tau(۲,۲)$ می‌پردازیم که از اهمیت بسیاری برخوردار هستند. در فصل حاضر با مفهوم حلقه آشنا می‌شویم و به مطالعه مثال‌ها و خصوصیات اساسی حلقه‌ها می‌پردازیم. در ابتدا به تعریفی اشاره خواهیم کرد که برای تعریف حلقه لازم است.

درسنامه (۱): تعریف حلقه‌ها و مثال های مهم

❖ **تعریف۱:** فرض کنید $(S,*,\circ)$ یک دستگاه جامع جبری باشد. عمل $\circ$ را نسبت به $*$ توزیع‌پذیر (پخشی) می‌نامیم، هرگاه به ازای هر $a,b,c\in S$ داشته باشیم:

$a\circ(b*c)=(a\circ b)*(a\circ c)$ (توزیع‌پذیری از چپ)

$(b*c)\circ a=(b\circ a)*(c\circ a)$ (توزیع‌پذیری از راست)

اگر عمل $\circ$ جابه‌جایی باشد، آن‌گاه توزیع‌پذیری از راست و چپ یکسان خواهد بود.

مثال۱: فرض کنید $*$ و $\circ$ روی $\mathbb{Z}$ به صورت $a\circ b=۲ab$ و $a*b=\frac{a+b}{۲}$ تعریف شده باشد. نشان دهید $\circ$ نسبت به $*$ از چپ توزیع‌پذیر است.

☑ **پاسخ:** فرض می‌کنیم $a,b,c\in\mathbb{Z}$ عناصر دلخواه باشند. حال روابط زیر را بررسی می‌کنیم:

$$\left.\begin{aligned} a\circ(b*c)&=a\circ(\frac{b+c}{۲})=a(b+c)=ab+ac\\ (a\circ b)*(a\circ c)&=(۲ab)*(۲ac)=\frac{۲ab+۲ac}{۲}=ab+ac\end{aligned}\right\}\Rightarrow a\circ(b*c)=(a\circ b)*(a\circ c)$$

و این یعنی $\circ$ نسبت به $*$ از چپ توزیع‌پذیر است.

همان‌گونه که وعده داده بودیم، حال که با مفهوم توزیع‌پذیری آشنا شدیم، با استفاده از این تعریف به سراغ بیان تعریف حلقه می‌رویم و به مطالعه مثال‌های مربوط به حلقه‌ها می‌پردازیم.

❖ **تعریف۲:** فرض کنید R یک مجموعه ناتهی همراه با دو عمل دوتایی که معمولاً اعمال جمع و ضرب در نظر گرفته می‌شود، باشد. در این صورت دستگاه جامع جبری $(R,+,\cdot)$ را یک حلقه می‌نامیم، هرگاه:

۱) $(R,+)$ یک گروه آبلی باشد؛

۲) $(R,\cdot)$ یک نیم‌گروه باشد؛

۳) ضرب نسبت به جمع توزیع‌پذیر باشد. یعنی:

$\forall\ a,b,c\in R;\quad a\cdot(b+c)=a\cdot b+a\cdot c$ (توزیع‌پذیری از چپ)

$(b+c)\cdot a=b\cdot a+c\cdot a$ (توزیع‌پذیری از راست)

پس توجه داشته باشید که حلقه‌ها، همان جبرهایی از نوع $\tau(۲,۲)$ هستند که در آن دو عمل دوتایی تعریف می‌شود و معمولاً اعمال جمع و ضرب را در نظر می‌گیریم. به عنوان مثال، هر یک از دستگاه‌های جامع جبری $(\mathbb{Z},+,\cdot)$، $(\mathbb{Q},+,\cdot)$، $(\mathbb{R},+,\cdot)$ و $(\mathbb{C},+,\cdot)$ با جمع و ضرب معمولی تشکیل یک حلقه می‌دهند.

مثال۲: فرض کنید $(R,+,\cdot)$ یک حلقه باشد، کدام‌یک از گزینه‌های زیر از اصول حلقه R نمی‌باشد.

۱) $(R,+)$ یک گروه آبلی می‌باشد. ۲) $(R,\cdot)$ یک گروه آبلی می‌باشد.

۳) $(R,\cdot)$ یک نیم‌گروه می‌باشد. ۴) ضرب نسبت به جمع توزیع‌پذیر می‌باشد.

☑ **پاسخ:** گزینه «۲» گزینه‌های (۱)، (۳) و (۴) با توجه به تعریف حلقه از اصول حلقه هستند. اما گزینه (۲) از اصول یک حلقه نیست، توجه داشته باشید در یک حلقه، $(R,\cdot)$ باید یک نیم‌گروه و $(R,+)$ یک گروه آبلی باشد.

◆ ◆ ◆ ◆

تذکر۱: از این به بعد هرگاه هیچ ابهامی وجود نداشته باشد، حلقه $(R,+,\cdot)$ را فقط با R نمایش می‌دهیم.

در تعریف حلقه R دیدیم باید $(R,+)$ یک گروه آبلی باشد. از طرفی در فصل گروه‌ها آموختیم، اگر $(R,+)$ یک گروه آبلی باشد، آن‌گاه گروه R دارای عضو خنثی (همانی) و عضو قرینه (معکوس یا وارون) است. در تعریف بعدی بیان می‌کنیم عضو خنثی و عضو قرینه گروه R در مفهوم حلقه چه نام‌هایی خواهند داشت.

❖ **تعریف۳:** الف) عضو خنثی عمل «+» را **صفر حلقه** می‌نامیم و با «$\circ$» نشان می‌دهیم.

ب) وارون هر عضو a از حلقه نسبت به عمل «+»، **قرینه a** نامیده می‌شود و با «$-a$» یا «a^{-1}» نشان می‌دهیم.

❖ **تعریف۴:** الف) اگر عمل ضرب حلقه جابه‌جایی باشد، حلقه را **جابه‌جایی (تعویض‌پذیر)** می‌نامیم.

ب) اگر عمل ضرب حلقه دارای عضو خنثی باشد، این عضو را **یکه‌ی حلقه** می‌نامیم و آن را با «**۱**» نمایش می‌دهیم، در چنین حالتی حلقه را **حلقه یکدار** می‌نامیم. به عنوان مثال، هر یک از دستگاه‌های جامع جبری $(\mathbb{Z},+,\cdot)$، $(\mathbb{Q},+,\cdot)$ و $(\mathbb{R},+,\cdot)$ با اعمال جمع و ضرب معمولی تشکیل حلقه جابه‌جایی یکدار می‌دهند.

ج) در یک حلقه‌ی یکدار هر عضو وارون‌پذیر را **یکال** می‌نامیم و مجموعه‌ی یکال‌های حلقه‌ی R را با $U(R)$ نمایش می‌دهیم.

➢ **توجه:** هر حلقه، الزاماً یکدار نیست. به عنوان مثال، فرض کنید $\mathbb{Z}_e$ مجموعه اعداد صحیح زوج باشد، $(\mathbb{Z}_e,+,\cdot)$ تشکیل یک حلقه جابه‌جایی می‌دهد. اما $\mathbb{Z}_e$ نسبت به عمل ضرب دارای عضو خنثی نمی‌باشد. بنابراین $(\mathbb{Z}_e,+,\cdot)$ غیر یکدار است.

مثال۳: (حلقه زیرمجموعه‌های X) فرض کنید X مجموعه ناتهی و $P(X)$ مجموعه‌ی همه زیرمجموعه‌های X باشد. در فصل گروه‌ها دیدیم $(P(X),\Delta)$ یک گروه آبلی است که در آن $B\Delta C=(B-C)\cup(C-B)$. از طرف دیگر $(P(X),\cap)$ یک نیم‌گروه جابه‌جایی با عضو خنثی X می‌باشد. حال نشان می‌دهیم $\cap$ نسبت به Δ توزیع‌پذیر است. لذا داریم:

$$A\cap(B\Delta C)=A\cap[(B-C)\cup(C-B)]=[(A\cap(B-C)]\cup[(A\cap(C-B)]=[(A\cap B)-(A\cap C)]\cup[(A\cap C)-(A\cap B)]=(A\cap B)\Delta(A\cap C)$$

بنابراین $(P(X),\Delta,\cap)$ تشکیل یک حلقه جابه‌جایی یکدار می‌دهد، این حلقه را حلقه زیرمجموعه‌های X می‌نامیم.

◆ ◆ ◆ ◆

مثال۴: (حلقه اعداد صحیح همنهشت با n) در مباحث گروه‌ها با گروه آبلی $(\mathbb{Z}_n,+)$ آشنا شدیم. یادآوری می‌کنیم ضرب رده‌های همنهشتی روی $\mathbb{Z}_n$ به صورت زیر تعریف می‌شود:

$$\forall\,[a],[b]\in\mathbb{Z}_n \quad ; \quad [a]\cdot[b]=[ab]$$

این ضرب جابه‌جایی است. زیرا:

$$[a]\cdot[b]=[ab]=[ba]=[b]\cdot[a]$$

همچنین جمع روی رده‌های همنهشتی نیز به صورت زیر تعریف می‌شود:

$$\forall\,[a],[b]\in\mathbb{Z}_n \quad ; \quad [a]+[b]=[a+b]$$

نشان دهید $(\mathbb{Z}_n,+,\cdot)$ یک حلقه جابه‌جایی یکدار است.

☑ **پاسخ:** ابتدا نشان می‌دهیم $(\mathbb{Z}_n,\cdot)$ یک نیم‌گروه است. یعنی کافی است نشان دهیم $\mathbb{Z}_n$ نسبت به عمل ضرب شرکت‌پذیر است. فرض می‌کنیم $[a],[b],[c]\in\mathbb{Z}_n$ و تساوی‌های زیر را به دست می‌آوریم:

$$\left.\begin{array}{l}[a].([b].[c])=[a].[bc]=[abc]\\([a].[b]).[c]=[ab].[c]=[abc]\end{array}\right\}\Rightarrow[a].([b].[c])=([a].[b]).[c]$$

در نتیجه $(\mathbb{Z}_n,\cdot)$ نیم‌گروه است. در ادامه به بررسی خصوصیت توزیع‌پذیری ضرب نسبت به جمع می‌پردازیم. برای بررسی این خصوصیت فرض می‌کنیم $[a],[b],[c]\in\mathbb{Z}_n$ و عملیات زیر را با توجه به جمع و ضرب رده‌های همنهشتی انجام می‌دهیم:

$$[a].([b]+[c]) \underset{\text{رده‌های همنهشتی}}{\overset{\text{با توجه به جمع}}{=\!=}} [a].[b+c] \underset{\text{رده‌های همنهشتی}}{\overset{\text{با توجه به ضرب}}{=\!=}} [a(b+c)]=[ab+ac]=[ab]+[ac]=[a][b]+[a][c]$$

بنابراین $[a].([b]+[c])=[a].[b]+[a].[c]$ و این تساوی نشان‌دهنده توزیع‌پذیری ضرب نسبت به جمع از چپ می‌باشد. با انجام عملیات مشابه می‌توان نشان داد توزیع‌پذیری از راست نیز برقرار است. بنابراین خصوصیت توزیع‌پذیری ضرب نسبت به جمع از چپ و راست نیز برقرار هستند.

همچنین $[1]$ عضو یکه‌ی عمل ضرب است. زیرا: $\forall\,[a]\in\mathbb{Z}_n \quad ; \quad [a]\cdot[1]=[a\cdot 1]=[a]$

بنابراین به ازای هر عدد صحیح مثبت n، دستگاه جامع جبری $(\mathbb{Z}_n,+,\cdot)$ یک حلقه جابه‌جایی یکدار است. این حلقه را، **حلقه اعداد صحیح همنهشت با n** می‌نامیم.

◆ ◆ ◆ ◆

تذکر۲: در بعضی از کتاب‌ها حلقه اعداد صحیح همنهشت با n، که در مثال قبل تعریف شد، به صورت $(\mathbb{Z}_n,\oplus,\odot)$ که در آن به ازای هر $a,b\in\mathbb{Z}_n$; $a\odot b=\overline{ab}$ و $a\oplus b=\overline{a+b}$، نشان داده می‌شود.

مثال۵: (حلقه درون‌ریختی‌های یک گروه آبلی) فرض کنید $(G,+)$ یک گروه آبلی و HomG مجموعه‌ی همه‌ی درون‌ریختی‌های گروه آبلی G با عمل ترکیب توابع یک نیم‌گروه با عضو خنثی باشد. روی HomG عمل + را به صورت زیر تعریف می‌کنیم:

$$\forall f,g\in \mathbf{HomG} \quad , \quad \forall x\in G \quad ; \quad (f+g)(x)=f(x)+g(x)$$

و ترکیب توابع g و f که برابر است با $fg(x)=f(g(x))$ را فقط با fg نشان می‌دهیم و ضرب در نظر می‌گیریم. پس توجه داریم در HomG عمل ضرب همان ترکیب توابع است که با fg نشان داده می‌شود. ثابت کنید $(\mathbf{HomG},+,\cdot)$ یک حلقه یکدار است.

☑ **پاسخ:** در ابتدا ثابت می‌کنیم $f+g,fg\in \mathrm{HomG}$. یعنی HomG نسبت به جمع و ضرب بسته است. به ازای هر $f,g\in \mathrm{HomG}$ و $x,y\in G$ داریم:

$$(f+g)(x+y)=f(x+y)+g(x+y)=[f(x)+f(y)]+[g(x)+g(y)] \overset{\text{G یک گروه آبلی}}{=\!=\!=} [f(x)+g(x)]+[f(y)+g(y)]$$
$$=(f+g)(x)+(f+g)(y)\Rightarrow f+g\in \mathrm{HomG}$$
$$(fg)(x+y)=f[g(x+y)]=f[g(x)+g(y)]=f(g(x))+f(g(y))=fg(x)+fg(y)\Rightarrow fg\in \mathrm{HomG}$$

در گام بعدی نشان می‌دهیم $(\mathrm{HomG},+)$ یک گروه آبلی است. برای رسیدن به این هدف به ترتیب مراحل زیر را انجام می‌دهیم.

۱) نشان می‌دهیم $(\mathrm{HomG},+)$ یک نیم‌گروه است. پس فرض کنید $f,g,h\in \mathrm{HomG}$ و $x\in G$. لذا داریم:

$$[(f+g)+h](x)=(f+g)(x)+h(x)=[f(x)+g(x)]+h(x)=f(x)+[g(x)+h(x)]=f(x)+[(g+h)(x)]=[f+(g+h)](x)$$

بنابراین $(f+g)+h=f+(g+h)$.

۲) اگر $\circ$ عضو خنثی G باشد، می‌توانیم همریختی w را به صورت زیر تعریف کنیم:

$$\begin{cases} w:G\to G \\ w(x)=\circ \quad \forall x\in G \end{cases} \Rightarrow w\in \mathrm{HomG}$$

حال به ازای هر $f\in \mathrm{HomG}$ و $x\in G$ می‌توانیم حاصل $f+w$ را بررسی کنیم، لذا داریم:

$$(f+w)(x)=f(x)+w(x)=f(x)+\circ=f(x)\Rightarrow f+w=f \Rightarrow \text{HomG عضو خنثی } w \text{ است}$$

۳) به ازای هر $f\in \mathrm{HomG}$، همریختی « $-f$ » را به صورت زیر تعریف می‌کنیم:

$$\begin{cases} -f:G\to G \\ (-f)(x)=-f(x) \qquad \forall x\in G \end{cases}$$

« $-f$ » یک همریختی گروه‌های آبلی است. زیرا:

$$\forall x,y\in G;\quad (-f)(x+y)=-f(x+y)=-[f(x)+f(y)]=-f(x)+[-f(y)]=(-f)(x)+(-f)(y)$$

بعد از تعریف همریختی« $-f$»، نشان می‌دهیم« $-f$» عضو قرینه (وارون) f است. پس به ازای هر $x\in G$ حاصل $f+(-f)$ را بررسی می‌کنیم، لذا داریم:

$$[f+(-f)](x)=f(x)+[-f(x)]=\circ=w(x)\Rightarrow \text{« } -f \text{ » قرینه (وارون) } f \text{ است}$$

۴) در گام آخر ثابت می‌کنیم $(\mathrm{HomG},+)$ جابه‌جایی است. فرض کنید $f,g\in \mathrm{HomG}$. بنابراین:

$$\forall x\in G;\ (f+g)(x)=f(x)+g(x)=g(x)+f(x)=(g+f)(x)\Rightarrow f+g=g+f$$

با انجام مراحل ۱ تا ۴ به این نتیجه می‌رسیم که $(\mathrm{HomG},+)$ یک گروه آبلی است. در مرحله دوم اثبات، نشان می‌دهیم $(\mathrm{HomG},\cdot)$ یک نیم‌گروه است. فرض کنید $f,g\in \mathrm{HomG}$ و $x\in G$، به طوری که:

$$\left.\begin{aligned}[(fg)h](x)&=(fg)[h(x)]=f(g[h(x)])\\ [f(gh)](x)&=f[(gh)(x)]=f(g[h(x)])\end{aligned}\right\}\Rightarrow (fg)h=f(gh)$$

مدرسان شریف

فصل هشتم

«زیرحلقه‌ها و ایده‌آل‌ها»

نظریه حلقه‌ها همانند دیگر ساختارهای جبری، دارای زیرساختار است. در واقع می‌توان برای حلقه‌ها، زیرحلقه را تعریف نمود. در نظریه گروه‌ها با مفهوم زیرگروه‌های نرمال آشنا شدیم و دیدیم این مفهوم دارای چه نقش اساسی در نظریه گروه‌ها است. در حلقه‌ها با مفهوم ایده‌آل آشنا می‌شویم و خواهیم دید ایده‌آل‌ها همانند زیرگروه‌های نرمال که در نظریه گروه‌ها حائز اهمیت هستند، برای حلقه‌ها چه نقش اساسی و مهمی خواهند داشت.

درسنامه (۱): زیرحلقه‌ها

❖ **تعریف۱:** فرض کنید $(R,+,\cdot)$ یک حلقه و S زیرمجموعه‌ای ناتهی از R باشد. اگر زیرمجموعه‌ی S همراه با عمل جمع و ضرب حلقه R، تشکیل یک حلقه بدهد، در این صورت $(S,+,\cdot)$ را **زیرحلقه‌ای** از $(R,+,\cdot)$ می‌نامیم و آن را با $\mathbf{S \leq R}$ نمایش می‌دهیم.

تذکر ۱: توجه کنید که S به طور طبیعی شرکت‌پذیری ضرب و توزیع‌پذیری جمع نسبت به ضرب را از R به ارث می‌برد، لذا برای نشان دادن زیرحلقه بودن مجموعه ناتهی S از حلقه R کافی است به محک زیر توجه کنیم.

قضیه۱ (محک زیرحلقه): فرض کنید R یک حلقه و S زیرمجموعه ناتهی از R باشد. S زیرحلقه R است اگر و تنها اگر:

۱ـ به ازای هر $a,b \in S$، $a-b \in S$؛ یعنی $(S,+)$ زیرگروه $(R,+)$ باشد.

۲ـ به ازای هر $a,b \in S$، $ab \in S$؛ یعنی $(S,\cdot)$ یک دستگاه جامع جبری باشد.

هر حلقه به طور طبیعی دارای دو زیرحلقه است. $\{0\}$ و دیگری خود R، این زیرحلقه‌ها را **زیرحلقه بدیهی** حلقه می‌نامیم.

حلقه $\mathbf{(\mathbb{Z},+,\cdot)}$ را در نظر بگیرید. اینک با استفاده از محک زیرحلقه نشان می‌دهیم $(n\mathbb{Z},+,\cdot)$ زیرحلقه $(\mathbb{Z},+,\cdot)$ است. می‌دانیم $n\mathbb{Z}=\{0,\pm n,\pm 2n,\ldots\}$. حال فرض کنید $a,b \in n\mathbb{Z}$. بنابراین عناصر $m,m' \in \mathbb{Z}$ موجود هستند به طوری که $a=m\mathbb{Z}$ و $b=m'\mathbb{Z}$. با توجه به محک زیرحلقه کافی است نشان دهیم $a-b \in n\mathbb{Z}$ و $ab \in n\mathbb{Z}$. بنابراین داریم:

$$\left.\begin{array}{l} a-b=m\mathbb{Z}-m'\mathbb{Z}=(m-m')\mathbb{Z}\in n\mathbb{Z} \\ ab=(m\mathbb{Z})(m'\mathbb{Z}) \xrightarrow[\text{یک گروه دوری}]{(n\mathbb{Z},+)} (mm')\mathbb{Z}\in n\mathbb{Z} \end{array}\right\} \Rightarrow \text{است } (\mathbb{Z},+,\cdot) \text{ زیرحلقه } (n\mathbb{Z},+,\cdot)$$

در ادامه نشان می‌دهیم $(\mathbb{Z}_e,+,\cdot)$ نیز زیرحلقه‌ای از $(\mathbb{Z},+,\cdot)$ است.

می‌دانیم $\mathbb{Z}_e=\{\ldots,-4,-2,0,2,4,\ldots\}=\{2k \mid k\in\mathbb{Z}\}$. حال فرض کنید $a,b \in \mathbb{Z}_e$. لذا عناصر $k,k' \in \mathbb{Z}$ موجود هستند به طوری که $a=2k$ و $b=2k'$. برای نشان دادن زیرحلقه بودن $\mathbb{Z}_e$ به صورت زیر می‌نویسیم:

$$\left.\begin{array}{l} a-b=2k-2k'=2(k-k')\in\mathbb{Z}_e \\ ab=(2k)(2k')=2(2kk')\in\mathbb{Z}_e \end{array}\right\} \Rightarrow (\mathbb{Z}_e,+,\cdot) \text{ زیرحلقه‌ای از } (\mathbb{Z},+,\cdot) \text{ است}$$

ممکن است این سؤال به وجود آید که آیا زیرحلقه‌ی یک حلقه جابه‌جایی، جابه‌جایی است؟

برای پاسخ به این سؤال فرض می‌کنیم R یک حلقه و S زیرحلقه‌ای از R باشد. اگر R حلقه جابه‌جایی باشد، آن‌گاه به ازای هر $a,b \in R$ داریم $ab=ba$. بدین‌ترتیب به ازای هر $a,b \in S$ نتیجه می‌شود، $ab=ba$. بنابراین S نیز جابه‌جایی است و این یعنی پاسخ سؤال ما مثبت است. در ادامه یکی از مهمترین مثال‌های این مبحث را مطالعه خواهیم کرد.

مثال۱: نشان دهید $m\mathbb{Z}$ زیرحلقه‌ای از حلقه $n\mathbb{Z}$ است اگر و تنها اگر $n|m$.

☑ **پاسخ:** ابتدا فرض می‌کنیم $m\mathbb{Z}$ زیرحلقه‌ای از حلقه $n\mathbb{Z}$ باشد. بنابراین $m\mathbb{Z}\subseteq n\mathbb{Z}$. حال فرض کنید $m\in m\mathbb{Z}$. با توجه به این‌که $\mathbb{Z}$ حلقه یکدار است، نتیجه می‌شود $m=m.1$. با توجه به تعریف زیرحلقه، نتیجه می‌شود $m\in n\mathbb{Z}$. لذا عدد صحیح مثبت $x\in\mathbb{Z}$ موجود است به طوری که $m=nx$. بنابراین $n|m$. و این یعنی n عاد می‌کند m را. حال برعکس، فرض می‌کنیم $n|m$. بنابراین عدد صحیح مثبت $d\in\mathbb{Z}$ موجود است به طوری که $m=dn$. حال عناصر دلخواه $x,y\in m\mathbb{Z}$ را در نظر بگیرید. در این صورت با توجه به محک زیرحلقه سه حالت زیر را نشان می‌دهیم:

۱ـ $m\in n\mathbb{Z}$ (در این صورت $m\mathbb{Z}\subseteq n\mathbb{Z}$)

۲ـ $x-y\in m\mathbb{Z}$ (در این صورت $m\mathbb{Z}$ گروه آبلی است)

۳ـ $xy\in m\mathbb{Z}$ (در این صورت $m\mathbb{Z}$ نسبت به عمل ضرب بسته است)

برای حالت اول، اگر $x\in m\mathbb{Z}$ باشد، آن‌گاه عدد صحیح مثبت $b\in\mathbb{Z}$ موجود است به طوری که $x=bm$. حال از این‌که $m=dn$ نتیجه می‌شود:

$$x=b(dn)=(bd)n\Rightarrow x\in n\mathbb{Z}$$

بنابراین $m\mathbb{Z}\subseteq n\mathbb{Z}$ و حالت اول ثابت می‌شود.

برای حالت دوم، از این‌که $y\in m\mathbb{Z}$ است، نتیجه می‌شود عدد صحیح مثبت $c\in\mathbb{Z}$ موجود است به طوری که $y=cm$. بنابراین داریم:

$$x-y=bm-cm=(b-c)m\in m\mathbb{Z}$$

و در نهایت برای حالت سوم، با توجه به این‌که $n\mathbb{Z}$ و $m\mathbb{Z}$ گروه‌های دوری هستند، نتیجه می‌شود:

$$xy=(bm)(cm)=(bcm)m\in m\mathbb{Z}$$

بنابراین با توجه به مطالب مذکور نتیجه می‌شود $m\mathbb{Z}$ زیرحلقه $n\mathbb{Z}$ است.

قضیه۲: فرض کنید R یک حلقه و $Z(R)$ مرکز حلقه باشد. در این‌صورت $Z(R)$ زیرحلقه‌ای از R است و همچنین برای هر $x\in R$، اگر $x^۲+x\in Z(R)$، آن‌گاه R حلقه جابه‌جایی است.

اثبات: فرض کنید $Z(R)=\{r\in R\mid rx=xr,\forall x\in R\}$ مرکز حلقه R باشد و همچنین فرض کنید $r,s\in Z(R)$. بنابراین برای هر $x\in R$، $rx=xr$ و $sx=xs$. ابتدا نشان می‌دهیم $r+s\in Z(R)$.

$$(r+s)x=rx+sx=xr+xs=x(r+s)\Rightarrow r+s\in Z(R)$$

از این‌که $r\in Z(R)$، داریم $rx=xr$. لذا برای نشان دادن این‌که $-r\in Z(R)$ است به صورت زیر عمل می‌کنیم:

$$(-r)x=-(rx)=(-rx)=(-xr)=x(-r)\Rightarrow -r\in Z(R)$$

بنابراین $Z(R)$ یک گروه آبلی است. حال نشان می‌دهیم $rs\in Z(R)$. برای هر $x\in R$ داریم:

$$(rs)x=r(sx)=r(xs)=(rx)s=(xr)s=x(rs)\Rightarrow rs\in Z(R)$$

پس با توجه به این‌که $(Z(R),+)$ یک زیرگروه آبلی و $rs\in Z(R)$، به این نتیجه می‌رسیم که $Z(R)$ یک زیرحلقه R است.

حال نشان می‌دهیم اگر $x^۲+x\in Z(R)$، آن‌گاه R جابه‌جایی است. فرض کنید $a,b\in R$. در این صورت $\left((a+b)^۲+(a+b)\right)\in Z(R)$.

عبارت $(a+b)^۲+(a+b)$ را به صورت زیر محاسبه می‌کنیم:

$$a^۲+ab+ba+b^۲+a+b=(a^۲+a)+(b^۲+b)+ab+ba\xrightarrow{(b^۲+b),(a^۲+a)\in Z(R)}ab+ba\in Z(R)$$

از این‌که $ab+ba\in Z(R)$، نتیجه می‌شود $ab+ba$ با جملات دیگری چون $b\in R$، جابه‌جا می‌شود، یعنی داریم:

$$(ab+ba)b=b(ab+ba)\Rightarrow ab^۲+bab=bab+b^۲a\Rightarrow ab^۲=b^۲a\quad(*)$$

از طرفی داشتیم $b^۲+b\in Z(R)$. لذا $b^۲+b$ با $a\in R$ نیز جابه‌جا می‌شود. پس می‌توانیم بنویسیم:

$$a(b^۲+b)=(b^۲+b)a\Rightarrow ab^۲+ab=b^۲a+ba\xrightarrow{\text{با توجه به رابطه }(*)}ab=ba\Rightarrow R\text{ یک حلقه جابه‌جایی است}$$

ممکن است این سؤال برای شما مطرح شود که آیا یک زیرحلقه از حلقه ناجابه‌جایی، جابه‌جایی است، یا نه؟ برای پیدا کردن پاسخ این سؤال، مثال بعدی را مطالعه می‌کنیم.

مثال۲: نشان دهید حلقه ماتریس‌های $M_{۲\times۲}(\mathbb{Q})$ دارای زیرحلقه‌ای جابه‌جایی یکدار است.

☑ **پاسخ:** از فصل قبل می‌دانیم حلقه $M_{۲\times۲}=\left\{\begin{bmatrix} x & y \\ z & t \end{bmatrix}\middle| x,y,z,t\in\mathbb{Q}\right\}$ حلقه‌ای ناجابه‌جایی یکدار است.حال قرار دهید $S=\left\{\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}\middle| a,b\in\mathbb{Q}\right\}$. نشان می‌دهیم S زیرحلقه‌ای جابه‌جایی یکدار ازحلقه ماتریس‌های $M_{۲\times۲}(\mathbb{Q})$ است. پس فرض کنید $A=\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}\in S$, $B=\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}$. لذا داریم:

$$\left.\begin{array}{l} A-B=\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}-\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}=\begin{bmatrix} a-c & ۰ \\ ۰ & b-d \end{bmatrix}\in S\Rightarrow A-B\in S \\ AB=\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}=\begin{bmatrix} ac & ۰ \\ ۰ & bd \end{bmatrix}\in S\Rightarrow AB\in S \end{array}\right\}\Rightarrow S \text{ زیرحلقه } M_{۲\times۲}(\mathbb{Q}) \text{ است}$$

و ماتریس همانی $I_{۲\times۲}=\begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix}$ عضو یکه‌ی زیرحلقه S می‌باشد. حال نشان می‌دهیم به ازای دو عضو $A=\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}\in S$ ، $B=\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}\in S$ جابه‌جایی است. یعنی $AB=BA$. لذا داریم:

$$AB=\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}=\begin{bmatrix} ac & ۰ \\ ۰ & bd \end{bmatrix}=\begin{bmatrix} ca & ۰ \\ ۰ & db \end{bmatrix}=\begin{bmatrix} c & ۰ \\ ۰ & d \end{bmatrix}\begin{bmatrix} a & ۰ \\ ۰ & b \end{bmatrix}=BA$$

پس S یک زیرحلقه جابه‌جایی یکدار است. بنابراین یک زیرحلقه از یک حلقه ناجابه‌جایی می‌تواند جابه‌جایی باشد.

◆ ◆ ◆ ◆

✍ **مثال۳: فرض کنید حلقه یکدار $(\mathbb{Z}_۶,+,۰)$ مفروض باشد. نشان دهید $S=\{۰,۲,۴\}$ زیرحلقه $\mathbb{Z}_۶$ است.**

☑ **پاسخ:** برای نشان دادن $S\leq\mathbb{Z}_۶$ از جدول کیلی نسبت به اعمال جمع و ضرب مقابل استفاده می‌کنیم.

$+$	۰	۲	۴
۰	۰	۲	۴
۲	۲	۴	۰
۴	۴	۰	۲

$\cdot$	۰	۲	۴
۰	۰	۰	۰
۲	۰	۴	۲
۴	۰	۲	۴

با مشاهده جدول جمع می‌بینیم مجموع هر ۲ عضو از S به S تعلق دارد. به عنوان مثال، $۲+۲=۴\in S$ و $۲+۴=۶\equiv_{۶}۰\in S$ و همین‌طور در جدول ضرب نیز حاصلضرب هر دو عضو از S به S تعلق دارد. به عنوان مثال، $۲.۲=۴\in S$ و $۲.۴=۸\equiv_{۶}۲\in S$

بنابراین با توجه به جداول می‌توان نتیجه گرفت، S زیرحلقه‌ای از $\mathbb{Z}_۶$ است.

◆ ◆ ◆ ◆

خواننده عزیز همان‌طور که در مثال قبل دیدید حلقه $\mathbb{Z}_۶$ حلقه‌ای یکدار با یکه‌ی ۱ است. ولی زیرحلقه‌ی $S=\{۰,۲,۴\}$ دارای عضو یکه‌ی حلقه‌ی $\mathbb{Z}_۶$ نیست. پس **اگر R حلقه یکدار باشد، آن‌گاه الزاماً هر زیرحلقه آن یکدار نیست.** در مبحث بعدی به یک نتیجه‌ی جالب در این خصوص اشاره می‌کنیم.

قضیه۳: فرض کنید R حلقه‌ای یکدار باشد و یکه‌ی R را با ۱_R نمایش می‌دهیم. اگر S زیرحلقه‌ای یکدار از R با یکه‌ی ۱_S باشد، به طوری که $۱_S\neq۱_R$، آن‌گاه ۱_S مقسوم علیه صفر حلقه R است.

اثبات: فرض کنید ۱_S یکه‌ی زیرحلقه S باشد، به طوری که $۱_S\neq۱_R$. حال عضو دلخواه $a\in R$ را طوری در نظر می‌گیریم که $a\cdot۱_S\neq a$. داریم:

$$(a\cdot۱_S)\cdot۱_S=a(۱_S\cdot۱_S)=a\cdot۱_S\Rightarrow(a\cdot۱_S)\cdot۱_S-a.۱_S=۰\Rightarrow(a.۱_S-a)۱_S=۰$$

چون $a.۱_S-a\neq۰$ و $۱_S\neq۰$ لذا ۱_S یک مقسوم علیه صفر حلقه R است.

✍ **مثال4: فرض کنید $R=\{(a,b)\in\mathbb{R}\times\mathbb{R}\,|\,a,b\in\mathbb{R}\}$ حلقه‌ای با جمع و ضرب زیر باشد.**

$(a,b)+(c,d)=(a+c,b+d)$ و $(a,b)\cdot(c,d)=(ac,bd)$

به‌راحتی می‌توانید نشان دهید R با جمع و ضرب تعریف شده، یک حلقه یکدار با یکه‌ی $(۱,۱)$ است. پس اثبات حلقه بودن R به خواننده واگذار می‌شود. حال فرض کنید $R'=\{(a,۰)\,|\,(a,۰)\in\mathbb{R}\times\{۰\}\}$. نشان دهید R' زیرحلقه‌ای از R است و یکه‌ی R' را بدست آورید.

☑ **پاسخ:** برای اثبات زیرحلقه بودن R' از محک زیرحلقه استفاده می‌کنیم. پس فرض کنید عناصر $(a,۰),(b,۰)\in R'$ دلخواه باشند به طوری که:

$$\left.\begin{array}{l}(a,۰)-(b,۰)=(a-b,۰)\in R' \\ (a,۰)(b,۰)=(ab,۰)\in R'\end{array}\right\}\Rightarrow R' \text{ زیرحلقه‌ای از } R \text{ است}$$

حال نشان می‌دهیم R' دارای یکه است. فرض کنید به ازای هر $(a,۰)\in R'$ عضو $(e,۰)\in R'$ موجود است به طوری که:

$(a,۰)(e,۰)=(ae,۰)=(a,۰)\Rightarrow ae=a\Rightarrow e=۱\Rightarrow$ است R' یکه‌ی زیرحلقه $(۱,۰)$

فصل نهم

«ایده‌آل‌های اول و ماکسیمال و همریختی حلقه‌ها»

در این فصل ابتدا با مفهوم ایده‌آل اول و ایده‌آل ماکسیمال که از اساسی‌ترین مفاهیم در نظریه حلقه‌ها هستند، آشنا می‌شویم. ایده‌آل‌های اول و ماکسیمال به ویژه در نظریه جبر جابه‌جایی کاربردهای اساسی دارند. در انتهای این فصل با کاربردهایی در این خصوص آشنا می‌شویم.

درسنامه (۱): ایده‌آل‌های اول

❖ **تعریف۱:** ایده‌آل سره P از حلقه جابه‌جایی R را **اول** می‌نامیم، هرگاه به ازای هر $a,b\in R$ به طوری که $ab\in P$، داشته باشیم $a\in P$ یا $b\in P$.

به عنوان مثال، ایده‌آل $\langle ۳\rangle=\{۳k\,|\,k\in\mathbb{Z}\}$ از حلقه اعداد صحیح $\mathbb{Z}$ را در نظر بگیرید. نشان می‌دهیم $\langle ۳\rangle$ ایده‌آل اول $\mathbb{Z}$ است. فرض کنید عناصر $a,b\in\mathbb{Z}$ موجود باشند به طوری که $ab\in\langle ۳\rangle$. از این‌که $ab\in\langle ۳\rangle$ نتیجه می‌شود:

$$۳\,|\,ab\Rightarrow ۳\,|\,a \text{ یا } ۳\,|\,b\Rightarrow \exists k,k'\in\mathbb{Z};\ a=۳k \text{ یا } b=۳k'\Rightarrow a\in\langle ۳\rangle \quad \text{یا} \quad b\in\langle ۳\rangle$$

از این رو $\langle ۳\rangle$ ایده‌آل اول $\mathbb{Z}$ است با توجه به مثال ارائه شده، در حالت کلی می‌توانیم بگوییم، **هر ایده‌آل بفرم $\langle p\rangle=\{pn\,|\,n\in\mathbb{Z}\}$ که در آن p عدد اول باشد، یک ایده‌آل اول حلقه $\mathbb{Z}$ است.**

حال نشان می‌دهیم در حلقه اعداد صحیح $\mathbb{Z}$، ایده‌آل $\langle ۰\rangle$ اول است.

فرض کنید عناصر $a,b\in\mathbb{Z}$ موجود باشند به طوری که $ab\in\langle ۰\rangle$، از طرفی $\mathbb{Z}$ یک حوزه صحیح است، بنابراین داریم:

$$ab=۰\ \Rightarrow a=۰ \text{ یا } b=۰\Rightarrow a\in\langle ۰\rangle \quad \text{یا} \quad b\in\langle ۰\rangle$$

لذا $\langle ۰\rangle$ ایده‌آل اول $\mathbb{Z}$ است بدین‌ترتیب با توجه به این مثال می‌توان گفت، **در هر حوزه صحیح، ایده‌آل صفر، ایده‌آل اول** است.

مثال ۱: ایده‌آل‌های اول حلقه $\mathbb{Z}$ به‌صورت $n\mathbb{Z}$ است که: (سراسری ۹۷)

۱) $n=۰$
۲) n یک عدد اول است.
۳) n مربع یک عدد اول است.
۴) $n=۰$ یا n یک عدد اول است.

☑ **پاسخ:** گزینه «۴» همان‌گونه که در مباحث قبل نشان دادیم در حلقه $\mathbb{Z}$، صفر ایده‌آل اول است و همچنین اگر $I=\langle n\rangle$ ایده‌آلی از $\mathbb{Z}$ باشد، در این صورت I ایده‌آل اول است اگر n یک عدد اول باشد. پس گزینه (۴) پاسخ مورد نظر است.

◆ ◆ ◆ ◆

قضیه۱: فرض کنید R یک حلقه جابه‌جایی و P ایده‌آلی از R باشد. در این صورت گزاره‌های زیر معادلند:

۱ـ P ایده‌آل اول است.

۲ـ اگر $a,b\in R$ به طوری که $\langle a\rangle\langle b\rangle\subseteq P$، آن‌گاه $a\in P$ یا $b\in P$.

۳ـ اگر I و J ایده‌آل‌هایی از حلقه R باشند به طوری که $IJ\subseteq P$، آن‌گاه $I\subseteq P$ یا $J\subseteq P$.

اثبات: ۲ $\Rightarrow$ ۳ و ۱ $\Rightarrow$ ۲ با توجه به تعریف ایده‌آل اول مستقیماً بدست می‌آیند. حال نشان می‌دهیم ۳ $\Rightarrow$ ۱ برقرار است. فرض کنید P ایده‌آل اول، I و J ایده‌آل‌هایی از R باشند، به طوری که $IJ\subseteq P$ و $I\not\subseteq P$. بنابراین عضو $a\in I$ موجود است به طوری که $a\notin P$. با توجه به این‌که $IJ\subseteq P$ پس به ازای $b\in J$ و این‌که فرض کرده بودیم $a\in I$، داریم $ab\in P$. حال چون P ایده‌آل اول است و $a\notin P$، داریم $b\in P$. بنابراین $J\subseteq P$.

مثال۲: فرض کنید R یک حلقه جابه‌جایی و P ایده‌آلی از R باشد، کدام گزینه با گزینه‌های دیگر معادل نیست.

۱) P ایده‌آل اول است.

۲) اگر $a,b\in R$ به طوری که $ab\in P$، آن‌گاه $a\in P$ یا $b\in P$.

۳) اگر I و J ایده‌آل‌هایی از R باشند، به طوری که $IJ\subseteq P$، آن‌گاه $I\subseteq P$ یا $J\subseteq P$.

۴) اگر $a,b\in R$ به طوری که $ab\in P$ و $ab\neq 0$، آن‌گاه $a\in P$ یا $b\in P$.

☑ **پاسخ:** گزینه «۴» گزینه‌های (۱)، (۲) و (۳) با توجه به قضیه (۱) که در مورد شرایط معادل در خصوص ایده‌آل‌های اول بیان می‌شود، معادلند. حال حلقه $M_{2\times 2}(\mathbb{R})$ و ایده‌آل $I=\langle 0\rangle$ را در نظر بگیرید. I در شرایط گزینه (۴) صدق می‌کند، اما به ازای عناصر $\begin{bmatrix}0&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix}\in M_{2\times 2}(\mathbb{R})$ داریم:

$$\begin{bmatrix}0&0\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}\in I \quad \text{ولی} \quad \begin{bmatrix}0&0\\0&1\end{bmatrix}\notin I \ \text{و}\ \begin{bmatrix}1&0\\0&0\end{bmatrix}\notin I$$

بنابراین گزینه (۴) با (۱) معادل نیست.

❖ **تعریف۲:** فرض کنید R یک حلقه جابه‌جایی باشد، مجموعه‌ی تمام ایده‌آل‌های اول حلقه R را **طیف اول R** می‌نامیم و با **Spec(R)** نمایش می‌دهیم.

مثال۳: Spec($\mathbb{Z}$) و Spec($\mathbb{R}$) را بدست آورید.

☑ **پاسخ:** با توجه به تعریف، $\mathrm{Spec}(\mathbb{Z})$ برابر می‌شود با مجموعه‌ی ایده‌آل‌های اول $\mathbb{Z}$. از طرفی نشان دادیم که ایده‌آل‌های $\langle 0\rangle$ و $\langle p\rangle$ که p عدد اول است ایده‌آل‌های اول حلقه $\mathbb{Z}$ هستند. بنابراین $\mathrm{Spec}(\mathbb{Z})=\{0\}\cup\{\langle p\rangle \mid p>1 \text{ اول}\}$.

برای حلقه اعداد حقیقی $\mathbb{R}$ می‌توانیم چنین نتیجه بگیریم، $\mathbb{R}$ یک میدان است و هر میدان یک حوزه صحیح است. چون هر میدان فقط دارای ایده‌آل‌های بدیهی است پس $\mathbb{R}$ تنها دارای دو ایده‌آل $I=\langle 0\rangle$ و $J=\mathbb{R}$ است. از طرفی در هر حوزه صحیح، $\langle 0\rangle$ ایده‌آل اول است. بنابراین تنها ایده‌آل اول $\mathbb{R}$، ایده‌آل $\langle 0\rangle$ است. پس $\mathrm{Spec}(\mathbb{R})=\{0\}$.

در ادامه با قضیه‌ای آشنا می‌شویم که یکی از مهمترین قضیه‌ها در مبحث ایده‌آل‌های اول است. لازم به ذکر است در قضیه بعدی از خصوصیات حلقه‌های خارج قسمتی استفاده خواهیم نمود.

قضیه۲: فرض کنید R یک حلقه جابه‌جایی یکدار باشد. در این صورت P یک ایده‌آل اول است اگر و تنها اگر $\frac{R}{P}$ یک حوزه صحیح باشد.

اثبات: فرض کنید P یک ایده‌آل اول باشد، می‌خواهیم نشان دهیم $\frac{R}{P}$ یک حوزه صحیح است. فرض کنید به ازای $a+P\in\frac{R}{P}$ عضو $b+P\neq P$ موجود باشد به طوری که $(a+P)(b+P)=P$. پس $ab+P=P$ و از این‌جا نتیجه می‌شود $ab\in P$. از این‌که $b+P\neq P$، نتیجه می‌شود $b\notin P$. از طرفی P ایده‌آل اول است، لذا $a\in P$ و در نتیجه $a+P=P$. همچنین R یک حلقه جابه‌جایی یکدار است، پس $\frac{R}{P}$ نیز یک حلقه جابه‌جایی یکدار می‌باشد. بنابراین $\frac{R}{P}$ یک حوزه صحیح است.

برعکس، فرض کنید $\frac{R}{P}$ یک حوزه صحیح باشد. نشان می‌دهیم P یک ایده‌آل اول است. چون $\frac{R}{P}\neq 0$ پس $P\neq R$، یعنی P ایده‌آل سره R است. حال فرض کنید به ازای عناصر $a,b\in R$، داشته باشیم $ab\in P$. از این‌که $ab\in P$ نتیجه می‌شود:

$$P \text{ یک ایده‌آل اول است} \Rightarrow a\in P \text{ یا } b\in P \xrightarrow{\frac{R}{P} \text{ یک حوزه صحیح}} a+P=P \text{ یا } b+P=P \Leftarrow ab+P=(a+P)(b+P)=P$$

➢ **توجه:** اگر R یک صفحه جابه‌جایی و یکدار و P ایده‌آل اول R باشد، آنگاه $\frac{R}{P}$ الزاماً دارای مقسوم علیه صفر نابدیهی نمی‌باشد. برای درک بهتر این مطلب حلقه خارج قسمتی $\frac{\mathbb{Z}}{3\mathbb{Z}}=\{0+3\mathbb{Z},1+3\mathbb{Z},2+3\mathbb{Z}\}$ را در نظر بگیرید. $3\mathbb{Z}$ ایده‌آل اول $\mathbb{Z}$ است، ولی $\frac{\mathbb{Z}}{3\mathbb{Z}}$ دارای مقسوم علیه صفر نابدیهی نیست.

در فصل قبل با مفهوم رادیکال ایده‌آل و رادیکال پوچ آشنا شدیم. این مفاهیم را در این‌جا یادآوری می‌کنیم.

ـ فرض کنید R حلقه‌ای جابه‌جایی و I ایده‌آلی از R باشد. رادیکال ایده‌آل I را به صورت $\sqrt{I}=\{r\in R \mid r^n \in I; n$ وجود دارد عدد طبیعی $\}$ تعریف می‌کنیم.

ـ مجموعه تمام اعضای پوچ‌توان حلقه جابه‌جایی R را به صورت $Nil(R)=\{r\in R \mid r^n = 0$، n وجود دارد عدد طبیعی $\}$ نشان می‌دهیم.

در ادامه با توجه به این دو مفهوم به ارائه مطالبی در حیطه ایده‌آل‌های اول می‌پردازیم.

قضیه۳: اگر P ایده‌آل اول از حلقه جابه‌جایی R باشد، آن‌گاه P ایده‌آل رادیکال است. یعنی $\sqrt{P}=P$.

اثبات: برای اثبات لازم است نشان دهیم $P\subseteq\sqrt{P}$ و $\sqrt{P}\subseteq P$. می‌دانیم همواره $P\subseteq\sqrt{P}$. پس کافی است ثابت کنیم $\sqrt{P}\subseteq P$. فرض کنید $a\in\sqrt{P}$. لذا عدد طبیعی n موجود است به طوری که $a^n\in P$. اگر $n=1$، آن‌گاه $a\in P$. پس فرض کنید $n\neq 1$. لذا داریم:

$$a^n = a.a^{n-1}\in P \xrightarrow{P \text{ ایده‌آل اول}} a\in P \text{ یا } a^{n-1}\in P$$

اگر $a\in P$ باشد، آن‌گاه حکم ثابت می‌شود. پس می‌توانید فرض کنید $a\notin P$، لذا $a^{n-1}\in P$. بنابراین داریم:

$$a^{n-1} = a.a^{n-2}\in P \xrightarrow{P \text{ ایده‌آل اول}} a\in P \text{ یا } a^{n-2}\in P$$

دوباره اگر $a\in P$ باشد، حکم برقرار می‌شود. پس دوباره می‌توانید فرض کنید $a\notin P$، پس $a^{n-2}\in P$. این روند را تا $n-2$ مرتبه دیگر تکرار کنید، در نهایت به این نتیجه می‌رسیم که $a\in P$. بنابراین $\sqrt{P}\subseteq P$، لذا حکم برقرار می‌باشد.

مثال۴: فرض کنید P ایده‌آل اول از حلقه جابه‌جایی R باشد. در این صورت به ازای هر عدد صحیح مثبت n، $\sqrt{P^n}=P$.

پاسخ: برای اثبات کافی است نشان دهیم $P\subseteq\sqrt{P^n}$ و $\sqrt{P^n}\subseteq P$. ابتدا فرض کنید $a\in P$. پس $a^n\in P^n$. لذا $a\in\sqrt{P^n}$. در نتیجه $P\subseteq\sqrt{P^n}$.

حال فرض کنید $a\in\sqrt{P^n}$. پس عدد صحیح مثبت m موجود است به طوری که $a^m\in P^n$. از طرفی همواره داریم $P\subseteq\sqrt{P}$، بنابراین $P^n\subseteq P$. لذا $a^m\in P$. حال اگر $m=1$ باشد، آن‌گاه $a\in P$ و کار تمام است. پس فرض کنید $m\neq 1$ و به صورت زیر نتیجه می‌گیریم:

$$a^m = a.a^{m-1}\in P \xrightarrow{P \text{ ایده‌آل اول}} a\in P \text{ یا } a^{m-1}\in P$$

اگر $a\in P$ باشد، آن‌گاه کار تمام است. پس دوباره می‌توانید فرض کنید $a\notin P$. لذا $a^{m-2}\in P$. این روند را تا $m-2$ مرتبه دیگر تکرار کنید، در نهایت به این نتیجه می‌رسیم که $a\in P$. پس داریم $\sqrt{P^n}\subseteq P$. بنابراین با توجه به موارد اثبات شده نتیجه می‌شود $\sqrt{P^n}=P$ و حکم ثابت می‌شود.

◆ ◆ ◆ ◆

قضیه۴: فرض کنید R حلقه‌ای جابه‌جایی یکدار باشد. اگر P_1 و P_2 ایده‌آل‌های اول R باشند به طوری که $P_1\not\subseteq P_2$ و $P_2\not\subseteq P_1$، آن‌گاه $P_1\cap P_2$ ایده‌آل اول نیست.

اثبات: فرض می‌کنیم $P_1\cap P_2$ ایده‌آل اول باشد، نشان می‌دهیم $P_1\subseteq P_2$ یا $P_2\subseteq P_1$. می‌دانیم همواره $P_1P_2\subseteq P_1\cap P_2$. چون $P_1\cap P_2$ ایده‌آل اول است، بنابراین $P_1\subseteq P_1\cap P_2$ یا $P_2\subseteq P_1\cap P_2$. لذا $P_1\subseteq P_2$ یا $P_2\subseteq P_1$ و حکم برقرار می‌شود.

قضیه قبل برای ایده‌آل‌های اول $P_1,\cdots,P_n$ از یک حلقه جابه‌جایی R نیز برقرار است.

قضیه۵: فرض کنید R حلقه‌ای جابه‌جایی یکدار و $P_1,\cdots,P_n$ ایده‌آل‌های حلقه R باشند. در این صورت $\bigcap_{i=1}^{n}P_i$ اول است اگر و تنها اگر به ازای یک $1\le j\le n$ داشته باشیم $P_j\subseteq\bigcup_{i\neq j}P_i$.

توجه: اگر R یک حلقه، P_1 و P_2 ایده‌آل‌های اول R باشند، آن‌گاه الزاماً $P_1\cap P_2$ ایده‌آل اول نیست. برای درک بهتر این مطلب به عنوان مثال، فرض کنید $\mathbb{Z}$ حلقه اعداد صحیح باشد. $2\mathbb{Z}=\{\ldots,-4,-2,0,2,4,\ldots\}$ و $3\mathbb{Z}=\{\ldots,-6,-3,0,3,6,\ldots\}$ ایده‌آل‌های اول $\mathbb{Z}$ هستند، زیرا گفته بودیم ایده‌آل‌های حلقه $\mathbb{Z}$ بفرم $p\mathbb{Z}$ هایی هستند که p عدد اول است. ولی $6\mathbb{Z}=3\mathbb{Z}\cap 2\mathbb{Z}$ که می‌توان گفت اعضای $6\mathbb{Z}$ بفرم $\{\ldots,-12,-6,0,6,12,\ldots\}$ است، ایده‌آل اول $\mathbb{Z}$ نمی‌باشد. زیرا به ازای عناصر $2,3\in\mathbb{Z}$ داریم $2.3=6\in 6\mathbb{Z}$، ولی $2,3\notin 6\mathbb{Z}$.

مثال ۵: فرض کنید R حلقه‌ای جابه‌جایی و یکدار و P_1,P_2 ایده‌آل‌های R باشند. اگر $P_1\cap P_2$ ایده‌آلی اول باشد، در این صورت: (سراسری ۹۶)

۱) $P_1\subseteq P_2$ ۲) $P_1\not\subseteq P_2$ و $P_2\not\subseteq P_1$ ۳) $P_1=P_1P_2$ ۴) $P_1\subseteq P_2$ یا $P_2\subseteq P_1$

پاسخ: گزینه «۴» با توجه به آنچه در متن درس مطالعه کردیم، اگر R یک حلقه جابه‌جایی یکدار و P_1 و P_2 ایده‌آل‌های اول R باشد، در این صورت اگر $P_1\cap P_2$ ایده‌آل اول باشد، آن‌گاه $P_1\subseteq P_2$ یا $P_2\subseteq P_1$.

مدرسان شریف

فصل دهم

«میدان کسرها و حلقه چندجمله‌ای‌ها»

در یک حلقه ممکن است تمام شرایط مورد نیاز برای حل مسائل خاصی موجود نباشد، ولی می‌توان حلقه بزرگتری ساخت که دارای خواص مورد نیاز برای حل مسئله مورد نظر باشد. به عنوان مثال، معادله $3x=5$ روی $\mathbb{Z}$ دارای جواب نیست. ولی اگر میدان F را در نظر بگیریم، همیشه معادلاتی به فرم $ax=b$ دارای جواب $x=a^{-1}b$ است. در این بخش با میدان کسرهای گویای یک حلقه و مباحث وابسته به آن آشنا می‌شویم و خواهیم دید میدان کسرها در بررسی چنین مسائلی مورد استفاده قرار می‌گیرد.

درسنامه (۱): میدان کسرها

❖ **تعریف۱:** فرض کنید D یک حوزه صحیح باشد. مجموعه $(a,b)=\frac{a}{b}=\{\frac{a}{b}\,|\,a\in D;b\in D-\{0\}\}$ را در نظر بگیرید.

اگر به ازای عناصر (c,d) و (a,b) داشته باشیم $(a,b)\sim(c,d)\Leftrightarrow ad=bc$، به عبارت دیگر $\frac{a}{b}=\frac{c}{d}\Leftrightarrow ad=bc$، در این صورت مجموعه مذکور را **مجموعه رده‌های هم ارزی روی $D^*=D\times D-\{0\}$** می‌نامیم.

قضیه ۱: « $\sim$ » یک رابطه هم ارزی روی D^* است.

اثبات: برای این‌که نشان دهیم « $\sim$ » یک رابطه هم‌ارزی است کافی است ثابت کنیم. خصوصیات بازتابی، تقارنی و تعدی بر روی عناصر D^* برقرار هستند. پس ابتدا به ازای عناصر $a\in D$ و $b\in D-\{0\}$ فرض کنید $ab=ba$. لذا $(a,b)\sim(b,a)$. بنابراین خاصیت بازتابی برقرار است. همچنین فرض کنید $(a,b)\sim(c,d)$، لذا $ad=bc$. پس $cb=da$ و در نتیجه $(c,d)\sim(a,b)$. بنابراین خاصیت تقارنی برقرار است.
حال فرض کنید $(a,b)\sim(c,d)$ و $(c,d)\sim(e,f)$. بنابراین $ad=bc$ و $cf=de$ و از این روابط چنین نتیجه می‌گیریم:

$$\left.\begin{array}{l} ad=bc \xrightarrow{\text{با ضرب طرفین در } f} adf=bcf \\ cf=de \xrightarrow{\text{با ضرب طرفین در } b} bcf=bde \end{array}\right\} \Rightarrow adf=bde \Rightarrow d(af-be)=0$$

و چون $d\neq 0$ لذا با استفاده از قانون حذف روی $D-\{0\}$ داریم $af=be$ و این یعنی $(a,b)\sim(e,f)$. بنابراین خاصیت تعدی نیز برقرار می‌باشد. پس « $\sim$ » یک رابطه هم‌ارزی روی D^* است.

➢ **توجه:** با توجه به تعریف رابطه هم ارزی « $\sim$ » روی $D\times D-\{0\}$ به ازای عناصر ناصفر $a,b,c\in D$ می‌توانیم موارد زیر را نتیجه بگیریم:
$(ac,bc)\sim(a,b)$ و $(a,a)\sim(b,b)$ و $(0,a)\sim(0,b)$

❖ **تعریف۲:** فرض کنید D یک حوزه صحیح باشد. مجموعه رده‌های هم ارزی روی D^* را در نظر بگیرید. مجموعه رده هم ارزی (a,b) را با F نشان می‌دهیم و به ازای عناصر ناصفر $b,d,bd\in D-\{0\}$ جمع و ضرب روی F را به صورت زیر تعریف می‌کنیم:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd} \quad \text{و} \quad (\frac{a}{b})(\frac{c}{d})=\frac{ac}{bd}$$

تذکر۱: در تعریف (۲) نماد $[a,b]$ به عنوان نماد مجموعه F نیز تعریف می‌شود. لذا جمع و ضرب روی F با توجه به نماد $[a,b]$ به صورت $[a,b].[c,d]=[ac,bd]$ و $[a,b]+[c,d]=[ad+cb,bd]$ می‌باشد، ولی ما برای راحتی کار از فرم تعریف شده در تعریف (۲) استفاده می‌کنیم.

در ادامه می‌خواهیم نشان دهیم $(F,+,0)$ یک میدان است ولی هنوز نمی‌دانیم که آیا جمع و ضرب تعریف شده برای F خوش‌تعریف است یا نه؟
پس بهتر است ابتدا خوش‌تعریفی جمع و ضرب را بررسی کنیم و به سراغ قضیه بعدی می‌رویم.

قضیه ۲: فرض کنید D یک حوزه صحیح و F مجموعه رده‌های هم ارزی روی D^* باشد. در این صورت جمع و ضرب روی F خوش‌تعریف است.

اثبات: فرض کنید $\frac{a}{b}=\frac{a'}{b'}$ و $\frac{c}{d}=\frac{c'}{d'}$. بنابراین داریم:

$$\left.\begin{array}{l} ab'=a'b \xrightarrow{\text{با ضرب طرفین در } dd'} (ab')(dd')=(a'b)(dd') \\ cd'=c'd \xrightarrow{\text{با ضرب طرفین در } bb'} (cd')(bb')=(c'd)(bb') \end{array}\right\} \Rightarrow (ab')(dd')+(cd')(bb')=(a'b)(dd')+(c'd)(bb')$$

لذا نتیجه می‌شود:

$$(ad+cb)(b'd')=(a'd'+c'b')(bd) \Rightarrow \frac{ad+cb}{bd}=\frac{a'b'+c'b'}{b'd'}$$

برای نشان دادن خوش‌تعریفی ضرب مجدداً از روابط $ab'=a'b$ و $cd'=c'd$ استفاده می‌کنیم، بنابراین داریم:

$$\left.\begin{array}{l} ab'=a'b \xrightarrow{\text{با ضرب طرفین در } cd'} (ab')(cd')=(a'b)(cd') \\ cd'=c'd \xrightarrow{\text{با ضرب طرفین در } a'b} (cd')(a'b)=(c'd)(a'b) \end{array}\right\} \Rightarrow (ab')(cd')=(a'b)(c'd) \Rightarrow (ac)(b'd')=(a'c')(bd) \Rightarrow \frac{ac}{bd}=\frac{a'c'}{b'd'}$$

بنابراین جمع و ضرب روی F خوش‌تعریف هستند.

با توجه به تعریف « $\sim$ » توانستیم نتیجه بگیریم $(\circ,a)\sim(\circ,b)$، $(a,a)\sim(b,b)$ و $(ac,bc)\sim(a,b)$. حال که با فرم دیگری از نمایش رابطه « $\sim$ » آشنا شدیم، می‌توایم سه نتیجه را به فرم دیگری هم نمایش دهیم این نمایش‌های جدید به شرح زیر هستند.

۱ـ به ازای هر $\circ\neq a\in D$ داریم، $\frac{a}{a},\frac{\circ}{a}\in F$ و $\frac{\circ}{a}\neq\frac{a}{a}$.

۲ـ به ازای هر $\circ\neq a,b\in D$ داریم، $\frac{\circ}{a}=\frac{\circ}{b}$ و به ازای هر $\circ\neq c$ داریم، $\frac{a}{b}=\frac{ac}{bc}$.

۳ـ به ازای هر $\circ\neq a,b,c\in D$، اگر $\frac{a}{b}=\frac{\circ}{c}$، آن‌گاه $a=\circ$.

اینک آماده‌ایم ثابت کنیم $(F,+,\cdot)$ یک میدان است.

قضیه ۳: فرض کنید D یک حوزه صحیح و F مجموعه رده‌های هم ارزی باشد. در این صورت $(F,+,\cdot)$ یک میدان است.

اثبات: ابتدا نشان می‌دهیم $(F,+)$ یک گروه جابه‌جایی است. بنابراین شرکت‌پذیری و جابه‌جایی را بررسی می‌کنیم. پس فرض کنید $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$.

برای نشان دادن شرکت‌پذیر بودن جمع خواهیم داشت:

$$(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}=\frac{a(df)+b(cf+de)}{b(df)}=\frac{a}{b}+\frac{cf+de}{df}=\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})$$

لذا با توجه به این‌که تساوی $(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})$ برقرار است، نتیجه می‌شود جمع شرکت‌پذیر است. برای نشان دادن جابه‌جایی بودن جمع نیز خواهیم داشت:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{bc+ad}{bd}=\frac{c}{d}+\frac{a}{b}$$

همان‌طور که می‌بینید $\frac{a}{b}+\frac{c}{d}=\frac{c}{d}+\frac{a}{b}$ و این تساوی نشان‌دهنده جابه‌جایی بودن عمل جمع است. در ادامه به سراغ نشان دادن خصوصیات عضو خنثی و عضو قرنیه برای یک گروه می‌رویم. فرض کنید به ازای $\circ\neq c\in D$ داریم $\frac{\circ}{c}\in F$. لذا $\frac{a}{b}+\frac{\circ}{c}=\frac{ac}{bc}=\frac{a}{b}$، پس $\frac{\circ}{c}\in F$ عضو خنثی جمع است.

حال فرض کنید به ازای هر $\frac{a}{b}\in F$ عضو $(-\frac{a}{b})\in F$ وجود دارد به طوری که: $\frac{a}{b}+(\frac{-a}{b})=\circ$

$$\frac{a}{b}+(-\frac{a}{b})=\frac{ab-ba}{b^2}=\frac{\circ}{b^2}=\frac{\circ}{c} \Rightarrow \frac{a}{b}+(\frac{-a}{b})=\circ$$

توجه داشته باشید $(\frac{a}{b})-=(\frac{-a}{b})$. پس $(\frac{a}{b})-$ قرینه عضو $\frac{a}{b}$ در F است. لذا $(F,+)$ یک گروه جابه‌جایی است.

حال نشان می‌دهیم $(F-\{\circ\},\cdot)$ یک نیم‌گروه جابه‌جایی است. برای اثبات این بخش ابتدا به سراغ بررسی شرکت‌پذیری و جابه‌جایی عمل ضرب می‌رویم.

پس فرض کنید $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$. برای نشان دادن شرکت‌پذیری، تساوی زیر را بررسی می‌کنیم، لذا داریم:

$$(\frac{a}{b}\frac{c}{d})(\frac{e}{f})=(\frac{ac}{bd})(\frac{e}{f})=\frac{(ac)e}{(bd)f}=\frac{a(ce)}{b(df)}=\frac{a}{b}(\frac{c}{d}\frac{e}{f})$$

بنابراین با توجه به تساوی $(\frac{a}{b}\frac{c}{d})(\frac{e}{f})=(\frac{a}{b})(\frac{c}{d}\frac{e}{f})$، نتیجه می‌شود ضرب شرکت‌پذیر است. همچنین برای اثبات جابه‌جایی بودن عمل ضرب نیز می‌توانیم به ازای عناصر $\frac{a}{b},\frac{c}{d}\in F$ به بررسی روابط زیر بپردازیم، بنابراین خواهیم داشت:

$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\frac{a}{b}\Rightarrow$ ضرب جابه‌جایی است

حال فرض کنید $\circ\neq c\in D$ به طوری که $\frac{c}{c}\in F$، لذا داریم:

$(\frac{a}{b})(\frac{c}{c})=\frac{ac}{bc}=\frac{a}{b}\Rightarrow$ $\frac{c}{c}$ عضو یکه عمل ضرب است

تا این‌جای اثبات نشان دادیم $(F-\{\circ\},\cdot)$ نیم‌گروه جابه‌جایی با عضو یکه‌ی $\frac{c}{c}$ است. در همین مرحله که هستیم به سراغ بررسی خصوصیت عضو وارون می‌رویم. زیرا برای این‌که F یک میدان باشد لازم است نسبت به عمل ضرب وارون‌پذیر باشد. پس فرض کنید عناصر ناصفر $\frac{a}{b}$ و $\frac{b}{a}$ دلخواه باشند به طوری که $a,b\neq\circ$ و $\frac{a}{b},\frac{b}{a}\in F$. در این صورت خواهیم داشت $(\frac{a}{b})(\frac{b}{a})=\frac{ab}{ba}=\frac{c}{c}=1$. بنابراین $\frac{b}{a}\in F$ عضو وارون $\frac{a}{b}\in F$ است. لذا F نسبت به عمل ضرب وارون‌پذیر است. در نهایت، اثبات می‌کنیم ضرب نسبت به جمع توزیع‌پذیر است. پس به ازای عناصر $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$ مقادیر $\frac{a}{b}(\frac{c}{d}+\frac{e}{f})$ و $(\frac{a}{b})(\frac{c}{a})+(\frac{a}{b})(\frac{e}{f})$ را به فرم زیر به دست می‌آوریم:

$$\frac{a}{b}(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}(\frac{cf+ed}{df})=\frac{a(cf+ed)}{bdf}=\frac{acf+aed}{bdf}$$

$$(\frac{a}{b})(\frac{c}{d})+(\frac{a}{b})(\frac{e}{f})=\frac{ac}{bd}+\frac{ae}{bf}=\frac{(ac)(bf)+(ae)(bd)}{(bd)(bf)}=\frac{(acf+aed)b}{(bdf)b}=\frac{acf+aed}{bdf}$$

لذا $\frac{a}{b}(\frac{c}{d}+\frac{e}{f})=(\frac{a}{b})(\frac{c}{d})+(\frac{a}{b})(\frac{e}{f})$، و این تساوی یعنی ضرب نسبت به جمع از چپ توزیع‌پذیر است. به طور مشابه می‌توانیم نشان دهیم ضرب نسبت به جمع از راست نیز توزیع‌پذیر است. بنابراین با توجه به همه مراحل مذکور نتیجه می‌شود $(F,+,\cdot)$ یک میدان است.

در قضیه‌ای که اثبات آن را با هم مطالعه کردیم، دیدیم $(F,+,\cdot)$ یک میدان است، این قضیه ما را به ارائه تعریف بسیار مهمی رهنمود می‌سازد.

❖ **تعریف۳:** فرض کنید D یک حوزه صحیح باشد. مجموعه رده‌های هم ارزی F را در نظر بگیرید. در این صورت میدان $(F,+,\cdot)$ را **میدان کسرهای گویای D** می‌نامیم.

❖ **تعریف۴:** فرض کنید R و T دو حلقه باشند، می‌گوئیم می‌توان حلقه R را در حلقه T **نشاند یا محاط کرد،** هرگاه همریختی یک به یک $f:R\to T$ موجود باشد، به عبارت دیگر R در T نشانده می‌شود، هرگاه R با هر زیرحلقه T یکریخت باشد. در این صورت حلقه T را یک **توسیع** حلقه R می‌نامیم.

قضیه۴: فرض کنید R یک حلقه باشد و همچنین فرض کنید $T=R\times\mathbb{Z}=\{(r,n)\mid r\in R,n\in\mathbb{Z}\}$، به طوری که قوانین جمع و ضرب به صورت زیر تعریف می‌شوند: $(r,n)(s,m)=(rs+ns+mr,nm)$ و $(r,n)+(s,m)=(r+s,n+m)$

در این صورت T با جمع و ضرب مذکور یک حلقه یکدار با یکه‌ی $(\circ,1)$ است.

اثبات: به سادگی می‌توان نشان داد $(T,+)$ یک گروه جابه‌جایی است و $(\circ,\circ)$ عضو صفر و $-(r,n)=(-r,-n)$ عضو قرینه $(T,+)$ است. حال نشان می‌دهیم $(T,\cdot)$ شرکت‌پذیر است. فرض کنید عناصر (t,q)، (s,m) و (r,n) دلخواه باشند و برای روابط $(r,n)[(s,m)(t,q)]$ و $[(r,n)(s,m)](t,q)$ داریم:

$$(r,n)[(s,m)(t,q)]=(r,n)(st+mt+qs,mq)=(rst+rmt+rqs+nst+nmt+nqs+rmq,nmq)$$

و

$$[(r,n)(s,m)](t,q)=(rs+ns+mr,nm)(t,q)=(rst+nst+mrt+nmt+rsq+nsq+mrq,nmq)$$

همان‌طور که می‌بینید $(r,n)[(s,m)(t,q)]=[(r,n)(s,m)](t,q)$. بنابراین $(T,\cdot)$ شرکت‌پذیر است.

حال به بررسی توزیع‌پذیری ضرب نسبت به جمع می‌پردازیم، فرض کنید عناصر $(r,n),(s,m),(t,q)\in T$ دلخواه باشند به طوری که:

$$(r,n)\big[(s,m)+(t,q)\big]=(r,n)(s+t,m+q)=(r(s+t)+n(s+t)+r(m+q),n(m+q))=(rs+rt+ns+nt+rm+rq,nm+nq)$$

همچنین برای رابطه $(r,n)(s,m)+(r,n)(t,q)$ خواهیم داشت:

$$(r,n)(s,m)+(r,n)(t,q)=(rs+ns+rm,nm)+(rt+nt+rq,nq)=(rs+ns+rm+rt+nt+rq,nm+nq)$$

بنابراین $(r,n)\big[(s,m)+(t,q)\big]=(r,n)(s,m)+(r,n)(t,q)$، و این تساوی نشان دهنده توزیع‌پذیری ضرب نسبت به جمع از چپ است. به همین

نحو می‌توانیم نشان دهیم توزیع‌پذیری از راست نیز برقرار است. حال نشان می‌دهیم $(۰,۱)$ یکه‌ی این حلقه است. پس به ازای عضو $(r,n)\in T$ داریم:

$(r,n)(۰,۱)=(r\cdot ۰+n\cdot ۰+r,n\cdot ۱)=(r,n)$ و $(۰,۱)(r,n)=(۰\cdot r+r+۰\cdot n,۱\cdot n)=(r,n)$

بدین‌ترتیب نشان دادیم $(T,+,\cdot)$ یک حلقه یکدار با یکه‌ی $(۰,۱)$ است.

تا به این مرحله با میدان کسرهای گویای D ، تعریف نشاندن یک حلقه در حلقه دیگر و حلقه $T=R\times\mathbb{Z}=\{(r,n)\,|\,r\in R,n\in\mathbb{Z}\}$ آشنا شدیم. در ادامه می‌خواهیم از این مفاهیم برای بیان قضایا و مباحث بسیار مهمی استفاده کنیم. اولین قضیه که می‌توان بحث را با آن شروع کرد این است که چگونه می‌توان یک حلقه را در حلقه‌ای دیگر نشاند؟ و شرایط مورد نیاز چیست؟ برای پاسخ به این سؤال‌ها قضیه‌ی بعدی را مطالعه می‌کنیم.

قضیه ۵: هر حلقه را می‌توان در یک حلقه یکدار نشاند.

اثبات: فرض کنید R یک حلقه باشد. نشان می‌دهیم می‌توان حلقه R را در $S=R\times\{۰\}=\{(r,۰)\,|\,r\in R\}$ نشاند. به‌وضوح S زیرحلقه T با جمع و ضرب $(r,۰)+(s,۰)=(r+s,۰)$ و $(r,۰)(s,۰)=(rs,۰)$ است. نگاشت $f:R\to S$ با ضابطه‌ی $f(r)=(r,۰)$ $\forall r\in R;$ را در نظر بگیرید. f یک همریختی است، زیرا به ازای عناصر $r,s\in R$ داریم:

$$f(r+s)=(r+s,۰)=(r,۰)+(s,۰)=f(r)+f(s)$$
$$f(rs)=(rs,۰)=(r,۰)(s,۰)=f(r)\cdot f(s)$$

f یک به یک است، زیرا با فرض $f(r)=f(s)$ داریم $(r,۰)=(s,۰)$. لذا $r=s$. بنابراین f یک همریختی یک به یک از R به S است. در نتیجه R در حلقه یکدار S با یکه‌ی $(۰,۱)$ نشانده می‌شود.

قضیه۶: فرض کنید D یک حوزه صحیح و $(F,+,\cdot)$ یک میدان باشد. در این صورت D در F نشانده می‌شود.

اثبات: نگاشت $f:D\to F$ با ضابطه‌ی، $\forall a\in D, f(a)=\frac{ac}{c}, c\neq ۰$ را در نظر بگیرید. f یک همریختی است. زیرا به ازای عناصر $a,b\in D$ داریم:

$$f(a+b)=\frac{(a+b)c}{c}=\frac{ac+bc}{c}=\frac{ac}{c}+\frac{bc}{c}=f(a)+f(b)$$
$$f(ab)=\frac{(ab)c}{c}=\frac{(ab)c^{۲}}{c^{۲}}=\frac{(ac)(bc)}{c^{۲}}=\frac{ac}{c}\cdot\frac{bc}{c}=f(a)\cdot f(b)$$

f یک به یک است. زیرا به ازای هر $a,b\in D$ داریم:

$$f(a)=f(b)\ \Rightarrow\frac{ac}{c}=\frac{bc}{c}\ \Rightarrow ac^{۲}=bc^{۲}\ \Rightarrow a=b$$

بنابراین D در میدان F نشانده می‌شود.

قضیه۷: فرض کنید D یک حوزه صحیح و F میدان کسرهای گویای D باشد. اگر F' کوچکترین زیرمیدان شامل F باشد، آن‌گاه F و F' یکریختند.

اثبات: فرض کنید F میدان کسرهای گویای D باشد. بنابراین چون می‌توان حوزه صحیح D را در میدان F نشاند پس می‌توان D را در F تحت همریختی $\theta_۱$ نشاند. فرض کنید F' میدان دیگری از D باشد به طوری که D در F' تحت همریختی $\theta_۲$ نشانده می‌شود. حال فرض کنید $\varphi:F\to F'$ با ضابطه $\varphi(\frac{a}{b})=\frac{\theta_۲(a)}{\theta_۲(b)}$ به ازای $\frac{a}{b}\in F$ و $b\neq ۰$ موجود باشد. نشان می‌دهیم φ یک، یکریختی است. ابتدا نشان می‌دهیم ضابطه φ خوش‌تعریف است.

پس فرض کنید به ازای عناصر $a,b,a',b'\in D$ و $b,b'\neq ۰$ داشته باشیم $\frac{\theta_۱(a)}{\theta_۱(b)}=\frac{\theta_۱(a')}{\theta_۱(b')}$. در نتیجه:

$$\theta_۱(a)\theta_۱(b')=\theta_۱(a')\theta_۱(b)\xrightarrow{\text{همریختی }\theta_۱}\theta_۱(ab')=\theta_۱(a'b)\xrightarrow{\text{یک به یک }\theta_۱}ab'=a'b\to\theta_۲(ab')=\theta_۲(a'b)$$
$$\xrightarrow{\text{همریختی }\theta_۲}\theta_۲(a)\theta_۲(b')=\theta_۲(a')\theta_۲(b)\Rightarrow\frac{\theta_۲(a)}{\theta_۲(b)}=\frac{\theta_۲(a')}{\theta_۲(b')}$$

بنابراین $\varphi(\frac{a}{b})=\varphi(\frac{a'}{b'})$ و این نشان می‌دهد φ خوش تعریف است. حال نشان می‌دهیم φ یک همریختی است. قرار دهید $x=\frac{\theta_۱(a)}{\theta_۱(b)}$ و $y=\frac{\theta_۱(c)}{\theta_۱(d)}$ بنابراین داریم:

$$\varphi(x+y)=\varphi(\frac{\theta_۱(a)}{\theta_۱(b)}+\frac{\theta_۱(c)}{\theta_۱(d)})\overset{\text{همریختی }\theta_۱}{=\!=}\varphi(\frac{\theta_۱(ad+bc)}{\theta_۱(bd)})=\frac{\theta_۲(ad+bc)}{\theta_۲(bd)}\overset{\text{همریختی }\theta_۲}{=\!=}\frac{\theta_۲(a)}{\theta_۲(b)}+\frac{\theta_۲(c)}{\theta_۲(d)}=\varphi(x)+\varphi(y)$$

و

$$\varphi(xy)=\varphi(\frac{\theta_۱(a)}{\theta_۱(b)}\cdot\frac{\theta_۱(c)}{\theta_۱(d)})\overset{\text{همریختی }\theta_۱}{=\!=}\varphi(\frac{\theta_۱(ac)}{\theta_۱(bd)})=\frac{\theta_۲(ac)}{\theta_۲(bd)}\overset{\text{همریختی }\theta_۲}{=\!=}\frac{\theta_۲(a)}{\theta_۲(b)}\cdot\frac{\theta_۲(c)}{\theta_۲(d)}=\varphi(x)\cdot\varphi(y)$$

فصل یازدهم

«رسته و مشبکه»

در فصل‌های گذشته با انواع ساختمان‌های جامع جبری به طور کامل آشنا شدیم. در این فصل با مفاهیم رسته و مشبکه آشنا خواهیم شد.

درسنامه (۱): رسته‌ها و گروه‌های آزاد

در این بخش به معرفی مفهوم **رسته (کاتاگوری)** خواهیم پرداخت و با مثال‌های مهم و چند قضیه اساسی آشنا می‌شویم. برای این‌که از لحاظ ذهنی آمادگی بیشتری پیدا کنیم بهتر است ابزار کارمان را بشناسیم. نظریه رسته‌ها در واقع زبان سودمند و عامیانه‌ای برای پرداختن به اشیاء مختلف ریاضی است. «اشیاء؟!» با دیدن این واژه متعجب نشوید. منظور از اشیاء در واقع همان دستگاه‌های جامع جبری آشنایی هستند که قبلاً در فصل‌های گذشته آن‌ها را مطالعه کردیم، در واقع همان مجموعه‌ها، گروه‌ها و حلقه‌ها همراه با نگاشت‌های مناسبی که بین این اشیاء وجود دارد. همانند توابع برای مجموعه‌ها، همریختی گروهی برای گروه‌ها و همریختی حلقه‌ای برای حلقه‌ها که از خواص مشترکی چون ترکیب، شرکت‌پذیری و نگاشت همانی برخوردار هستند. بنابراین ابزار کارمان همان مطالبی هستند که تا این‌جا در مبانی جبر آموختیم. حال می‌خواهیم این مفاهیم را در قالب جدید و ارتباط جدید در مفهوم رسته بیاموزیم.

❖ **تعریف۱:** یک **رسته** خانواده‌ای است متشکل از اشیاء (مانند مجموعه‌ها، گروه‌ها، حلقه‌ها، فضاهای برداری و ...) که معمولاً آن‌ها را با A، B، C، D و ... نمایش می‌دهیم به طوری که دارای ویژگی‌های زیر باشد:

۱ـ به ازای هر دو شیء A و B مجموعه‌ای مانند $\mathrm{Hom}(A,B)$ نسبت داده می‌شود (یک عضو $f \in \mathrm{Hom}(A,B)$ را یک **ریختار** از A به B می‌نامیم و با $f:A \to B$ نمایش می‌دهیم.) و دارای این خاصیت است که به ازای هر چهار شیء A، B، C و D که $(A,B) \neq (C,D)$، آن‌گاه $\mathrm{Hom}(A,B) \cap \mathrm{Hom}(C,D) = \phi$؛

۲ـ به ازای هر سه شیء مثل A، B و C نگاشت

$$\mathrm{Hom}(B,C) \times \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,C)$$
$$(g,f) \mapsto gf$$

موجود است به طوری که:

الف ـ به ازای هر چهار شیء A، B، C و D اگر $f:A \to B$، $g:B \to C$ و $h:C \to D$ آن‌گاه $h(gf) = (hg)f$، در واقع خصوصیت شرکت‌پذیری برقرار باشد.

ب ـ به ازای هر شیء A عضو $1_A:A \to A$ موجود باشد به طوری که به ازای هر $f:A \to B$ و $g:C \to A$ داشته باشیم $f \circ 1_A = f$ و $1_A \circ g = g$.

یک رسته (کاتاگوری) را با $\mathcal{C}$ نشان می‌دهیم.

به عنوان مثال، فرض کنید $\mathcal{C}$ خانواده تمام مجموعه‌ها باشد. به ازای هر دو مجموعه A و B، $\mathrm{Hom}(A,B)$ را مجموعه تمام توابع از A به B در نظر می‌گیریم و تابع زیر را به صورت

$$\mathrm{Hom}(B,C) \times \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,C)$$
$$(g,f) \mapsto gf$$

تعریف می‌کنیم که در آن gf در واقع ترکیب دو تابع f و g است. در این صورت $\mathcal{C}$ یک رسته است که در این رسته هر تابع از A به B یک ریختار است و هر عضو $f \in \mathrm{Hom}(A,B)$ در واقع تابع $f:A \to B$ محسوب می‌شود. این رسته به رسته‌ی مجموعه‌ها معروف است و آن را با $\mathbb{S}\mathrm{et}$ نمایش می‌دهیم.

❖ **تعریف۲:** فرض کنید $\mathcal{C}$ یک رسته باشد. ریختار $f:A \to B$ را **هم‌ارزی** می‌نامیم، هرگاه ریختاری مانند $g:B \to A$ موجود باشد به طوری که $fog = 1_B$ و $gof = 1_A$.

در ادامه با توجه به تعریف رسته و هم‌ارزی به بیان مثال‌های بیشتری در این راستا می‌پردازیم.

مثال۱: فرض کنید G یک گروه ضربی و $\mathcal{C}$ یک خانواده تک عضوی باشد. پس تنها عضو $\mathcal{C}$ گروه G است. لذا $\mathrm{Hom}(G,G)$ یک مجموعه از اعضای G است. در فصل حلقه‌ها با $\mathrm{Hom}(G,G)$ بطور کامل آشنا شدیم. حال نگاشت

$$\mathrm{Hom}(G,G) \times \mathrm{Hom}(G,G) \to \mathrm{Hom}(G,G)$$
$$(a,b) \mapsto ab$$

که در آن ab، ضرب دو عضو a و b در گروه G است، را تعریف می‌کنیم. نشان دهید $\mathcal{C}$ یک رسته است. آیا هر ریختار این رسته هم‌ارزی است؟

☑ **پاسخ:** با توجه به این‌که $\mathcal{C}$ یک خانواده تک عضوی و فقط شامل گروه ضربی G است، لذا هر عضو از گروه G ریختار محسوب می‌شود در واقع $a \in Hom(G,G)$ را با نماد $a:G \to G$ نشان می‌دهیم و این یعنی a عضوی از G است. حال برای نشان دادن رسته بودن خانواده $\mathcal{C}$ به تعریف رسته مراجعه می‌کنیم. حال فرض می‌کنیم عناصر $a:G \to G$، $b:G \to G$ و $c:G \to G$ دلخواه باشند. در این صورت داریم $a(bc) = (ab)c$. از طرفی نگاشت همانی $1_G : G \to G$ عضو خنثی مجموعه‌ی $Hom(G,G)$ می‌باشد. لذا به ازای هر $a:G \to G$ داریم $a o 1_G = a$. بنابراین با توجه به مطالب ارائه شده نتیجه می‌شود $\mathcal{C}$ یک رسته است. از طرف دیگر با توجه به این‌که هر عضو گروه ضربی G دارای وارون است، لذا در رسته $\mathcal{C}$ ریختار $a:G \to G$ هم‌ارزی است.

مثال۲: فرض کنید $\mathcal{C}$ خانواده تمام گروه‌ها باشد. به ازای هر دو گروه H و G مجموعه $Hom(G,H)$ همان مجموعه تمام همریختی‌های گروهی $f:G \to H$ در نظریه گروه‌ها است. به ازای گروه‌های H، G و K نگاشت

$$Hom(H,K) \times Hom(G,H) \to Hom(G,K)$$
$$(g,f) \mapsto gf$$

که در آن gf ترکیب دو همریختی گروهی است را در نظر بگیرید. نشان دهید $\mathcal{C}$ یک رسته و دارای ریختار هم‌ارزی است.

☑ **پاسخ:** اشیاء H، G، K و T را در نظر بگیرید. اگر $(G,H) \neq (K,T)$ آن‌گاه $Hom(G,H) \cap Hom(K,T) = \phi$.
حال فرض کنید $f \in Hom(G,H)$، $g \in Hom(H,K)$ و $h \in Hom(K,T)$. در این صورت داریم $f:G \to H$، $g:H \to K$ و $h:K \to T$، لذا $h(gf) = (hg)f$. بنابراین خصوصیت شرکت‌پذیری برقرار است.
از طرفی به ازای هر شیء G، عضو $1_G : G \to G$ موجود است به طوری که به ازای $f:G \to H$ داریم $f o 1_G = f$ و به ازای $g:K \to G$ داریم $1_G o g = g$. بنابرین با توجه به مطالب ارائه شده نتیجه می‌شود $\mathcal{C}$ یک رسته است. در این مثال رسته‌ی $\mathcal{C}$ به **رسته گروه‌ها** معروف است و آن را با $\mathbb{G}rp$ نمایش می‌دهیم.
حال اشیاء G و G' را از رسته $\mathcal{C}$ در نظر بگیرید. در این صورت ریختار $f:G \to G'$ موجود است. با توجه به این‌که $f \in Hom(G,G')$ و $\mathcal{C}$ رسته گروه‌ها است، لذا f یک همریختی گروهی است. پس ریختار $f^{-1}:G' \to G$ موجود است به طوری که $f o f^{-1} = 1_{G'}$ و $f^{-1} o f = 1_G$. در این صورت f یک به یک و پوشا است. لذا g یک، یکریختی گروه‌ها است. بنابراین ریختار $f:G \to G'$ در رسته گروه‌های $\mathcal{C}$ هم‌ارزی است.

➢ **توجه:** در مثال قبل اگر به جای گروه، گروه‌های آبلی در نظر گرفته شود، رسته بدست آمده به رسته گروه‌های آبلی معروف است و با $\mathbb{A}b$ نشان داده می‌شود.

مثال۳: فرض کنید $\mathcal{C}$ خانواده تمام حلقه‌ها باشد. به ازای هر دو حلقه R و S مجموعه $Hom(R,S)$ همان مجموعه تمام همریختی‌های حلقه‌ای $f:R \to S$ در نظریه حلقه‌ها است. حال به ازای حلقه‌های R، S و T نگاشت

$$Hom(S,T) \times Hom(R,S) \to Hom(R,T)$$
$$(g,f) \mapsto gf$$

که در آن gf ترکیب دو همریختی حلقه‌ای است را در نظر بگیرید. نشان دهید $\mathcal{C}$ یک رسته و دارای ریختار هم‌ارزی است.

☑ **پاسخ:** فرض کنید R، S، T و U اشیاء $\mathcal{C}$ باشند. بنابراین به ازای $f:R \to S$، $g:S \to T$ و $h:T \to U$ داریم $h(gf) = (hg)f$. از طرفی همریختی همانی $1_R : R \to R$ موجود است به طوری که به ازای $f:R \to S$ داریم $f o 1_R = f$ و به ازای $g:S \to R$ داریم $1_R o g = g$. بنابراین $\mathcal{C}$ یک رسته است. این رسته به **رسته حلقه‌ها** معروف است و آن را با نماد $\mathbb{R}ing$ نمایش می‌دهیم. همچنین به‌راحتی می‌توان نشان داد اگر f یک، یکریختی حلقه‌ای باشد، آن‌گاه ریختار $f:R \to S$ در رسته $\mathcal{C}$ هم‌ارزی است.

مثال۴: یک مجموعه نقطه‌ای، جفتی مانند (S,x) است که در آن S یک مجموعه و $x \in S$. همچنین یک ریختار از مجموعه‌های نقطه‌ای مانند $(S,x) \to (S',x')$، سه‌تایی است مانند (f,x,x') که در آن $f:S \to S'$ تابعی است مانند $f(x) = x'$. نشان دهید مجموعه‌های نقطه‌ای تشکیل یک رسته می‌دهد.

☑ **پاسخ:** ابتدا فرض می‌کنیم سه‌تایی $(f,S,T):(S,x) \to (T,y)$ با ضابطه $f(x) = y$ و سه‌تایی $(g,T,U):(T,y) \to (U,z)$ با ضابطه $g(y) = z$ موجود باشند. بدین ترتیب داریم:

$$(gf,S,U):(S,x) \to (U,z)$$
$$gf(x) = g(y) = z$$

بنابراین ترکیب در سه‌تایی مذکور برقرار است. حال سه‌تایی‌های (f,S,T)، (g,T,U) و (h,U,V) را در نظر بگیرید. لذا داریم:

$$(f,S,T)[(g,T,U)(h,U,V)] = (f,S,T)(hg,T,V) = (hgf,S,V)$$

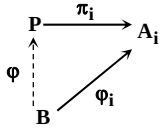
و همچنین $[(f,S,T)(g,T,U)](h,U,V) = (gf,S,U)(h,U,V) = (hgf,S,V)$. بنابراین خصوصیت شرکت‌پذیری برقرار است.
حال ریختار همانی $(1_S,x,x):(S,x) \to (S,x)$ را با ضابطه $1_S(x) = x$ در نظر بگیرید. فرض کنید $(f,x,y):(S,x) \to (T,y)$ با ضابطه $f(x) = y$ و $(g,y,x):(T,y) \to (S,x)$ با ضابطه $g(y) = x$ موجود باشند. بنابراین داریم:

$$(f,x,y)(1_S,x,x) = (1_S.f,x,y) = (f,x,y) \quad \text{و} \quad (1_S,x,x)(g,y,x) = (g.1_S,y,x) = (g,y,x)$$

با توجه به توضیحات مذکور نتیجه می‌شود (S,x) یک رسته شامل ریختارهایی بفرم سه‌تایی (f,x,y) با ضابطه $f(x) = y$ می‌باشد.

در تعاریف بعدی می‌خواهیم با مفهومی آشنا شویم که با استفاده از رسته‌ها و حاصلضرب که درفصل مقدمات و پیش‌نیازها اشاره کردیم، بیان می‌شود.

❖ **تعریف۳:** فرض کنید $\mathcal{C}$ یک رسته و $\{A_i \mid i\in I\}$ خانواده‌ای از اشیا باشد. شیء P در $\mathcal{C}$ را یک **ضرب** برای خانواده $\{A_i \mid i\in I\}$ می‌نامیم، هرگاه ریختار $\{\pi_i : P\to A_i \mid i\in I\}$ موجود باشد به طوری که به ازای هر شیء B در $\mathcal{C}$ و هر خانواده $\{\varphi_i : B\to A_i \mid i\in I\}$ ریختار یکتای $\varphi : B\to P$ موجود باشد به طوری که به ازای هر $i\in I$، $\pi_i\varphi=\varphi_i$. به عبارتی نمودار روبرو تعویض‌پذیر باشد:

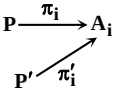


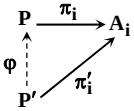
به عنوان مثال، $\prod_{i\in I} A_i$ یک ضرب برای خانواده $\{A_i \mid i\in I\}$ از مجموعه‌ها است.

بلافاصله بعد از تعریف ضرب قضیه‌ای را بیان می‌کنیم که یکی از خصوصیات اساسی این مبحث را ارائه می‌کند.

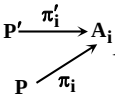
قضیه۱: (یکتایی ضرب) در هر رسته $\mathcal{C}$، ضرب برای خانواده $\{A_i \mid i\in I\}$ از اشیاء یکتاست.

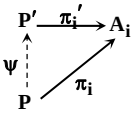
اثبات: نشان می‌دهیم اگر به ازای اشیاء P و P' و ریختارهای π_i و π'_i، جفت‌های (P,π_i) و (P',π'_i) ضرب برای خانواده $\{A_i \mid i\in I\}$ باشند، آن‌گاه P و P' در $\mathcal{C}$ هم‌ارز هستند.

ابتدا فرض کنید P یک ضرب برای خانواده $\{A_i \mid i\in I\}$ و P' یک شیء دلخواه باشد. لذا نمودار  موجود است. بنابراین ریختار منحصر بفرد $\varphi : P'\to P$ موجود است به طوری که نمودار تعویض‌پذیر می‌باشد. یعنی داریم:



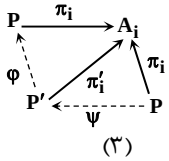
$$\pi_i\varphi=\pi'_i \qquad (۱)$$

حال فرض کنید P' یک ضرب برای خانواده $\{A_i \mid i\in I\}$ و P یک شیء دلخواه در $\mathcal{C}$ باشد. بنابراین نمودار  موجود است. لذا ریختار منحصر به فرد $\psi : P\to P'$ موجود است به طوری که نمودار بالا تعویض‌پذیر خواهد شد. یعنی داریم:



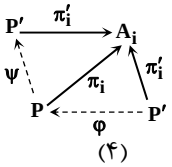
$$\pi'_i\psi=\pi_i \qquad (۲)$$

حال با ترکیب دو نمودار (۱) و (۲) نمودارهای زیر به دست می‌آیند.



(۳)

و



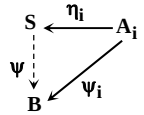
(۴)

از نمودارهای (۳) و (۴) روابط زیر نتیجه می‌شود:

$$\pi_i(\varphi\psi)=(\pi_i\varphi)\psi=\pi'_i\psi=\pi_i \quad\text{و}\quad \pi'_i(\psi\varphi)=(\pi'_i\psi)\varphi=\pi_i\varphi=\pi'_i \qquad (۵)$$

با توجه به این‌که $\varphi\psi=1_P$ و $\psi\varphi=1_{P'}$ و با قرار دادن این روابط در عبارات (۵) نتیجه می‌شود $\pi_i 1_P=\pi_i$ و $\pi'_i 1_{P'}=\pi'_i$. بنابراین $P\cong P'$ و این یعنی P و P' هم‌ارز هستند. لذا در هر رسته مانند $\mathcal{C}$ ضرب برای خانواده‌ای از اشیاء مانند $\{A_i \mid i\in I\}$ یکتاست.

❖ **تعریف۴:** فرض کنید $\mathcal{C}$ یک رسته و $\{A_i \mid i\in I\}$ خانواده‌ای از اشیاء باشد. شیء S را یک **هم‌ضرب** برای $\{A_i \mid i\in I\}$ می‌نامیم، هرگاه ریختار $\{\eta_i : A_i\to S \mid i\in I\}$ موجود باشد به طوری که به ازای هر شیء B از $\mathcal{C}$ و هر خانواده از ریختارهای $\{\psi_i : A_i\to B \mid i\in I\}$ ریختار منحصر بفرد $\psi : S\to B$ موجود باشد به طوری که به ازای هر $i\in I$، $\psi\eta_i=\psi_i$. به‌عبارتی نمودار زیر تعویض‌پذیر است:



تذکر۱: همان‌طور که متوجه شدید تعریف هم‌ضرب، همانند تعریف ضرب است با این تفاوت که جهت فلش‌ها در تعریف هم‌ضرب عوض شدند. پس این مطلب یک نکته جالب و قابل توجه خواهد بود. مشابه قضیه‌ی یکتایی که برای ضرب بیان کردیم برای هم‌ضرب هم داریم.

قضیه۲: (یکتایی هم‌ضرب) در هر رسته $\mathcal{C}$، هم‌ضرب برای خانواده $\{A_i \mid i\in I\}$ در صورت وجود یکتاست.

اثبات: این قضیه هم مشابه با آنچه برای ضرب بیان کردیم اثبات می‌شود با این تفاوت که برای هم‌ضرب کافی است جهت فلش‌ها را عوض کنیم.

مثال۵: کدام‌یک از موارد زیر صحیح است؟

فرض کنید $\mathcal{C}$ یک رشته باشد، در این صورت:

الف ـ اگر $\mathcal{C}$ یک رسته از گروه‌ها باشد، آن‌گاه گروه $G_1\times G_2$. با همریختی‌های $\pi_1 : G_1\times G_2\to G_1$ و $\pi_2 : G_1\times G_2\to G_2$ یک ضرب است.

ب ـ اگر $\mathcal{C}$ یک رسته از گروه‌های آبلی باشد، آن‌گاه $A_1\times A_2$ همراه با همریختی‌های $\eta_1 : A_1\to A_1\times A_2$ و $\eta_2 : A_2\to A_1\times A_2$ یک هم‌ضرب است.

ج ـ فرض کنید $\{A_i \mid i\in I\}$ خانواده از مجموعه‌ها باشد، آن‌گاه هر رسته از مجموعه‌های $\{A_i \mid i\in I\}$ یک هم‌ضرب است.

۱) فقط الف　　۲) الف و ب　　۳) الف، ب و ج　　۴) ب و ج

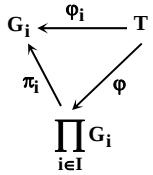
☑ **پاسخ:** گزینه «۳» برای پاسخ به این مثال به بررسی هر یک از موارد الف، ب و ج می‌پردازیم. ابتدا فرض کنید $\mathcal{C}$ رسته‌ای از گروه‌ها باشد. لذا این

رسته شامل همریختی‌های گروهی است که همان ریختارهای مورد نیاز ما هستند. فرض کنید $\{G_i \mid i \in I\}$ خانواده‌ای از گروه‌ها باشد. لذا ابتدا حالت (الف) را روی خانواده $\{G_i \mid i \in I\}$ بررسی می‌کنیم. گروه T را طوری در نظر بگیرید که خانواده‌ای از همریختی‌های گروهی $\{\varphi_i : T \to G_i \mid i \in I\}$ موجود باشد. حال همریختی $\varphi : T \to \prod_{i\in I} G_i$ را تعریف کنید. با توجه به قضیه‌ی **حاصل‌ضرب** $\prod_{i\in I} A_i$ **بوسیله خاصیت نگاشت عمومی**، که در فصل مقدمات و پیش‌نیازها بیان کردیم، نتیجه می‌شود φ یک همریختی منحصرد بفرد است.

از طرفی از قبل با نگاشت $\pi_i : \prod_{i\in I} G_i \to G_i$ آشنا شده بودیم. نشان می‌دهیم π_i یک همریختی است. پس فرض کنید عناصر دلخواه f و g از $\prod_{i\in I} G_i$ موجود هستند. لذا داریم $f : I \to \bigcup_{i\in I} G_i$ به طوری که $f(i) \in G_i$ و $g : I \to \bigcup_{i\in I} G_i$ به طوری که $g(i) \in G_i$. بنابراین $fg : I \to \bigcup G_i$ موجود است به طوری که $fg(i) = f(i)g(i) \in G_i$. حال داریم:

$$\pi_i(fg) = fg(i) = f(i)g(i) = \pi_i(f)\pi_i(g)$$

بنابراین نگاشت پوشای π یک همریختی است. لذا با توجه به **قضیه یکتایی ضرب** در رسته‌ها داریم:



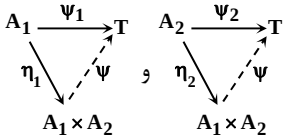
$$\forall i \in I\ ;\ \pi_i \varphi = \varphi_i$$

اگر بتوانیم نشان دهیم φ یک همریختی است در آن صورت $\mathcal{C}$ یک رسته خواهد بود. نگاشت $\varphi : T \to \prod_{i\in I} G_i$ تعریف شده است. با اشاره دوباره به قضیه‌ی حاصل‌ضرب $\prod_{i\in I} A_i$ بوسیله خاصیت نگاشت عمومی که در فصل مقدمات و پیش‌نیازها بیان کردیم، نتیجه می‌شود $\varphi(x) = f_x$ به طوری که $f_x(i) = \varphi_i(x)$. بنابراین $\varphi(xy) = f_{xy}$ به طوری که $f_{xy}(i) = \varphi_i(xy) = \varphi_i(x)\varphi_i(y) = f_x(i)f_y(i)$. پس $\varphi(xy) = f_{xy} = f_x f_y = \varphi(x)\varphi(y)$. لذا φ یک همریختی است. پس $\prod_{i\in I} G_i$ یک ضرب در رسته گروه‌ها است. بنابراین قسمت (الف) درست است.

حال فرض کنید $\mathcal{C}$ یک رسته از گروه‌های آبلی باشد. نشان می‌دهیم گروه $A_1 \times A_2$ همراه با همریختی $\eta_1 : A_1 \to A_1 \times A_2$ و $\eta_2 : A_2 \to A_1 \times A_2$ یک هم‌ضرب است. ابتدا نگاشت $\eta_1 : A_1 \to A_1 \times A_2$ با ضابطه $a \mapsto (a, \circ)$ و نگاشت $\eta_2 : A_2 \to A_1 \times A_2$ با ضابطه $b \mapsto (\circ, b)$ را تعریف می‌کنیم. نشان می‌دهیم η_1 یک همریختی گروه‌ها است. لذا با فرض $a, b \in A_1$ داریم:

$$\eta_1(a+b) = (a+b, \circ) = (a, \circ) + (b, \circ) = \eta_1(a) + \eta_1(b)$$

بنابراین η_1 همریختی گروه‌های آبلی می‌باشد. به طریقی مشابه می‌توان نشان داد η_2 نیز یک همریختی گروه‌های آبلی است. حال گروه آبلی T و دو همریختی $\psi_1 : A_1 \to T$ و $\psi_2 : A_2 \to T$ را طوری در نظر بگیرید که $\psi : A_1 \times A_2 \to T$. بنابراین نمودارهای حاصل

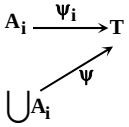


می‌شوند. لذا به ازای $i = ۱,۲$ نتیجه می‌شود $\psi\eta_i = \psi_i$. اگر عناصر $a \in A_1$ و $b \in A_2$ را در نظر بگیریم نتیجه می‌شود $\psi_1(a) = \psi\eta_1(a) = \psi(a, \circ)$ و $\psi_2(b) = \psi\eta_2(b) = \psi(\circ, b)$. بنابراین $\psi(a,b) = \psi((a,\circ)+(\circ,b)) = \psi(a,\circ) + \psi(\circ,b) = \psi_1(a) + \psi_2(b)$ که نشان می‌دهد نگاشت $\psi : A_1 \times A_2 \to T$ با ضابطه $(a,b) \to \psi_1(a)\psi_2(b)$ موجود است. حال اگر نشان دهیم ψ یک همریختی است آن‌گاه با توجه به تعریف هم‌ضرب‌ها، $\mathcal{C}$ موجود در قسمت (ب) یک هم‌ضرب از رسته گروه‌های آبلی خواهد بود. پس کافی است همریختی بودن ψ برای تکمیل اثبات بررسی شود. فرض کنید $(c,d) \in A_1 \times A_2$ و (a,b) به طوری که داریم:

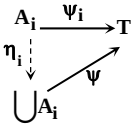
$$\psi((a,b)+(c,d)) = \psi(a+c, b+d) = \psi_1(a+c) + \psi_2(b+d) = \psi_1(a) + \psi_1(c) + \psi_2(b) + \psi_2(d)$$
$$= \psi_1(a) + \psi_2(b) + \psi_1(c) + \psi_2(d) = \psi(a,b) + \psi(c,d)$$

بنابراین ψ یک همریختی است پس یک رسته از گروه‌های آبلی خواهد بود. لذا $A_1 \times A_2$ یک هم‌ضرب در رسته گروه‌های آبلی با اشیاء A_1 و A_2 می‌باشد. پس قسمت (ب) نیز درست می‌باشد.

برای بررسی بند (ج) فرض کنید $\{A_i \mid i \in I\}$ خانواده‌ای از مجموعه‌ها باشد. مجموعه‌ی $\bigcup_{i\in I} A_i = \{(a,i) \in (\bigcup A_i) \times I \mid a \in A_i\}$ را همراه با نگاشت $\eta_i : A_i \to \bigcup_{i\in I} A_i$ با ضابطه $a \mapsto (a,i)$ در نظر بگیرید. فرض کنید T یک مجموعه و $\{\psi_i : A_i \to T \mid i \in I\}$ خانواده‌ای از توابع باشد و تابع $\psi : \bigcup A_i \to T$ را با توجه به خصوصیات هم‌ضرب‌ها در نظر می‌گیریم. لذا نمودار



بوجود می‌آید. بنابراین تابع منحصر بفرد $\eta_i : A_i \to \bigcup A_i$ موجود است به طوری که نمودار



تعویض‌پذیر است. یعنی به ازای هر $i \in I$، $\psi\eta_i = \psi_i$ به طوری که به ازای هر

$a \in A_i$ داریم $\psi\eta_i(a) = \psi(\eta_i(a)) = \psi(a,i)$. پس $\psi: \bigcup A_i \to T$ بفرم $(a,i) \mapsto \psi_i(a)$ می‌باشد. بنابراین رسته تمام مجموعه‌ها یک هم‌ضرب در نظریه رسته‌ها است. لذا بند (ج) هم درست است. با توجه به تمام مطالب ارائه شده نتیجه می‌شود گزینه ۳ پاسخ مورد نظر است.

در بخش بعدی می‌خواهیم با مفهوم شیء آزاد در یک رسته آشنا شویم. برای این منظور نیاز به تعریف بعدی داریم.

❖ **تعریف۵:** رسته‌ای مانند $\mathcal{C}$ را **رسته‌ی ملموس** می‌نامیم، هرگاه تابعی مانند σ موجود باشد که به هر شیء مانند A، مجموعه‌ای مانند $\sigma(A)$ را متناظر کند به طوری که دارای ویژگی‌های زیر باشد:

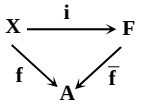
۱ـ هر ریختار مانند $f: A \to B$، تابعی از مجموعه‌ی $\sigma(A)$ به مجموعه‌ی $\sigma(B)$ باشد.

۲ـ به ازای هر شیء مثل A، ریختار 1_A، تابع همانی روی مجموعه $\sigma(A)$ باشد.

۳ـ ترکیب دو ریختار همانند $f: A \to B$ و $g: B \to C$ همان ترکیب آن‌ها به عنوان توابعی از $\sigma(A)$ به $\sigma(B)$ و $\sigma(B)$ به $\sigma(C)$ است.

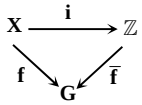
به عنوان مثال، رسته‌های $\mathbb{S}et$، $\mathbb{G}rp$، $\mathbb{A}b$ و $\mathbb{R}ing$ که آن‌ها را مطالعه کردیم هر کدام یک رسته ملموس هستند، ولی رسته گروه ضربی شامل تنها یک عضو یک رسته ملموس نیست. زیرا هرگاه تابع σ به گروه G، $\sigma(G)$ را نسبت دهد، آن‌گاه ریختار حاصله یک تابع نیست. بنابراین رسته مورد بحث یک رسته ملموس نمی‌باشد.

❖ **تعریف۶ (شیء آزاد):** فرض کنید F یک شیء در رسته‌ی ملموس $\mathcal{C}$ باشد، X یک مجموعه و $i: X \to F$ یک نگاشت بین مجموعه‌ها باشد. گوییم F روی مجموعه‌ی X آزاد است، هرگاه برای هر شیء A از $\mathcal{C}$ و نگاشت (بین مجموعه‌ها) $f: X \to A$، یک ریختار یکتا مثل $\bar{f}: F \to A$ موجود باشد به طوری که $\bar{f}i = f$. به عبارتی نمودار مقابل تعویض‌پذیر است.



مثال۶: نشان دهید مجموعه‌ی اعداد صحیح $\mathbb{Z}$ روی مجموعه‌ی $X = \{1\}$ آزاد است.

☑ **پاسخ:** فرض می‌کنیم G یک گروه باشد و $g \in G$. همچنین فرض می‌کنیم $f: \mathbb{Z} \to G$ با ضابطه $f(1) = g$ یک همریختی باشد. واضح است که تابع شمول $\begin{cases} i: X \to \mathbb{Z} \\ 1 \mapsto 1 \end{cases}$ موجود می‌باشد. اکنون می‌توانیم همریختی یکتای $\bar{f}: \mathbb{Z} \to G$ را با ضابطه $\bar{f}(n) = g^n$ تعریف کنیم به طوری که $\bar{f}(i(1)) = \bar{f}(1) = g$. به عبارتی نمودار روبرو را خواهیم داشت.



مثال۷: نشان دهید در رسته‌ی گروه‌ها، مجموعه‌ی اعداد گویا روی هیچ مجموعه‌ای آزاد نیست.

☑ **پاسخ:** فرض می‌کنیم $\mathbb{Q}$ روی مجموعه‌ی X آزاد و $i: X \to \mathbb{Q}$ یک نگاشت باشد، پس به ازای گروه S_3 و نگاشت $f: X \to S_3$، همریختی $\bar{f}: \mathbb{Q} \to S_3$ وجود دارد که $\bar{f}i = f$. طبق اولین قضیه‌ی یکریختی‌ها داریم $\frac{\mathbb{Q}}{\ker\bar{f}} \cong \mathrm{Im}\bar{f} \le S_3$. چون S_3 متناهی است، پس $\frac{\mathbb{Q}}{\ker\bar{f}}$ هم متناهی خواهد بود. اما در فصول گروه‌ها ثابت کردیم $\mathbb{Q}$ زیرگروهی با شاخص متناهی ندارد، بنابراین باید داشته باشیم $\ker\bar{f} = \mathbb{Q}$، یعنی $\bar{f}$ همریختی همانی است، در نتیجه به ازای هر $e \neq x \in X$، $f(x) = \bar{f}(i(x)) = e$ که تناقض می‌باشد. در نتیجه $\mathbb{Q}$ روی هیچ مجموعه‌ای در رسته‌ی گروه‌ها آزاد نیست.

قضیه۳: فرض کنید $\mathcal{C}$ یک رسته‌ی ملموس باشد. اگر F و F' دو شیء از این رسته باشند که به ترتیب روی مجموعه‌های X و X' آزادند و $|X| = |X'|$، آن‌گاه F و F' هم‌ارز هستند.

اکنون قصد داریم تعریف نیم‌گروه و گروه آزاد را ارائه دهیم، اما قبل از آن لازم است تعریف کلمه را ارائه دهیم.

❖ **تعریف۷:** فرض می‌کنیم A یک مجموعه‌ی دلخواه باشد که در اینجا آن را الفبا می‌نامیم. یک **کلمه** روی الفبای A یک دنباله چون $w = (a_1, a_2, ..., a_n)$ از اعضای A که حرف نامیده می‌شوند، است. توجه داشته باشید که هر کلمه $w = (a_1, a_2, ..., a_n)$ به صورت $w = a_1, a_2, ..., a_n$ هم نوشته می‌شود. طول این کلمه برابر است با n.

❖ **تعریف۸:** فرض می‌کنیم A یک الفبا باشد. مجموعه‌ی تمام کلمات به شکل $w = (a_1, a_2, ..., a_n)$ روی الفبای A را با A^* نمایش می‌دهیم. عمل دوتایی بین اعضای این مجموعه، عمل توالی است که به صورت زیر تعریف می‌شود:

$$\forall (a_1, a_2, ..., a_m), (b_1, b_2, ..., b_n) \in A^* ; (a_1, a_2, ...a_m)(b_1, b_2, ..., b_n) = (a_1, a_2, ..., a_m, b_1, b_2, ..., b_n)$$

واضح است که این عمل شرکت‌پذیر می‌باشد. دنباله‌ی تهی، کلمه‌ی تهی نامیده می‌شود که آن را با «۱» نمایش می‌دهند، در حقیقت به ازای هر $w \in A^*$ داریم $w1 = 1w = w$، بنابراین ۱ عضو همانی این مجموعه می‌باشد. در نتیجه A^* با عمل توالی یک تکواره است که آن را **تکواره آزاد** می‌نامیم.

❖ **تعریف۹:** فرض می‌کنیم A یک الفبا باشد. مجموعه‌ی تمام کلمه‌های غیرتهی به شکل $w=(a_1,a_2,...,a_n)$ را با A^+ نمایش می‌دهیم، در حقیقت $A^+=A^*-\{1\}$. چون A^+ با عمل توالی خاصیت شرکت‌پذیری دارد، یک نیم‌گروه می‌باشد که آن را **نیم‌گروه آزاد** می‌نامیم.

➢ **توجه:** هر نیم‌گروه آزاد A^+، روی رسته‌ی همه‌ی نیم‌گروه‌ها، یک شیء آزاد است.

قضیه۴: اگر A^+ یک نیم‌گروه باشد، آن‌گاه شرایط زیر معادلند:

۱ـ A^+ آزاد است.

۲ـ A^+ یک مجموعه‌ی مولد چون X دارد، به طوری که هر عضو A^+ به طور منحصر به فرد به صورت حاصل‌ضرب اعضای X نوشته می‌شود.

۳ـ قانون حذف روی A^+ برقرار است ولی A^+ شامل خودتوان‌ها نیست. هر عضو A^+ شامل تعداد متناهی از مقسوم‌علیه‌هاست و برای هر $u,u',w,w'\in A^+$، اگر $uw=u'w'$، آن‌گاه $u=u'$ یا یکی از u و u' مقسوم‌علیه چپ دیگری است.

مبحث بعدی مربوط به تعریف گروه آزاد است. اما قبل از ارائه این تعریف لازم است مطالب زیر را بدانیم.

فرض می‌کنیم X یک مجموعه‌ی دلخواه باشد. به ازای هر $x\in X$، عضو معکوس مرتبط با x یعنی x^{-1} را در نظر می‌گیریم و فرض می‌کنیم $X^{-1}=\{x^{-1}\mid x\in X\}$. همچنین فرض می‌کنیم $w=(a_1,a_2,...)$ یک کلمه‌ی نامتناهی روی X باشد به طوری که به ازای هر $i\in\mathbb{N}\cup\{0\}$، $a_i\in X\cup X^{-1}\cup\{1\}$ و به ازای یک $n\in\mathbb{N}\cup\{0\}$، داشته باشیم $a_k=1$، $\forall k\ge n$. کلمه‌ی $w=(a_1,a_2,...)$ را **کلمه‌ی تحویل یافته** می‌نامیم، هرگاه به ازای هر $x\in X$، x و x^{-1} پشت سرهم قرار نگیرند، یعنی اگر $a_i=x$، آن‌گاه $a_{i+1}\neq x$ و اگر $a_i=x$، آن‌گاه $a_{i+1}\neq x$ و به ازای هر $i\ge k$ از $a_k=1$ نتیجه بگیریم $a_i=1$، به عبارت دیگر یک کلمه‌ی تحویل یافته به صورت $(x_1^{\lambda_1},x_2^{\lambda_2},...,x_n^{\lambda_n},1,1,...)$ می‌باشد، به طوری که $n\in\mathbb{N}\cup\{0\}$، $x_i\in X$ و $\lambda_i=\pm1$. دو کلمه‌ی تحویل یافته‌ی $(x_1^{\lambda_1},x_2^{\lambda_2},...,x_m^{\lambda_m},1,1,...)$ و $(y_1^{\delta_1},y_2^{\delta_2},...,y_n^{\delta_n},1,1,...)$ با هم برابرند اگر و تنها اگر $m=n$ و به ازای هر $1\le i\le n$، $x_i=y_i$ و $\lambda_i=\delta_i$. حال نگاشت $\begin{cases}f:X\to F(X)\\ x\mapsto x^1=x\end{cases}$ را که در آن $F(X)$ مجموعه‌ی تمام کلمات تحویل‌پذیر است، در نظر می‌گیریم. واضح است که این نگاشت یک به یک است. فرض می‌کنیم عمل دوتایی بین اعضای $F=F(X)$، عمل توالی باشد، یعنی به ازای هر $(x_1^{\lambda_1},...,x_m^{\lambda_m},1,1,...),(y_1^{\delta_1},...,y_m^{\delta_m},1,1,...)\in F(X)$ داشته باشیم:

$$(x_1^{\lambda_1},...,x_m^{\lambda_m},1,1,...)(y_1^{\delta_1},...,y_n^{\delta_n},1,1,...)=x_1^{\lambda_1}...x_m^{\lambda_m}\ y_1^{\delta_1}...y_n^{\delta_n}$$

اما اگر $x_m^{\lambda_m}=y_1^{-\delta_1}$، آن‌گاه حاصل‌ضرب فوق نمی‌تواند تحویل یافته باشد. برای رفع این مشکل، تمام اعضای به شکل xx^{-1} یا $x^{-1}x$ را حذف می‌کنیم. همچنین اگر $x_1^{\lambda_1}...x_m^{\lambda_m}$ و $y_1^{\delta_1}...y_n^{\delta_n}$ دو کلمه‌ی تحویل یافته غیرتهی روی X باشند به طوری که $m\le n$، آن‌گاه فرض می‌کنیم k بزرگترین عدد صحیحی باشد که $0\le k\le m$ و $x_{m-j}^{\lambda_{m-j}}=y_{i+j}^{-\delta_{i+j}}$ $(0\le j\le k-1)$. در این صورت تعریف می‌کنیم:

$$(x_1^{\lambda_1}...x_m^{\lambda_m})(y_1^{\delta_1}...y_n^{\delta_n})=\begin{cases}x_1^{\lambda_1}...x_{m-k}^{\lambda_{m-k}}y_{k+1}^{\delta_{k+1}}...y_n^{\delta_n} & k<m\\ y_{m+1}^{\delta_{m+1}}...y_n^{\delta_n} & k=m<n\\ 1 & k=m=n\end{cases}$$

حال آماده هستیم گروه آزاد را تعریف کنیم.

❖ **تعریف۱۰:** اگر X یک مجموعه‌ی دلخواه باشد، آن‌گاه $F=F(X)$ یعنی مجموعه‌ی همه‌ی کلمه‌های تحویل یافته روی مجموعه‌ی X تحت عمل توالی یک گروه است که آن را **گروه آزاد** می‌نامیم.

قضیه۵: فرض کنید F مجموعه‌ی تمام کلمه‌های تحویل یافته روی مجموعه‌ی X باشد، در این صورت $F=\langle X\rangle$.