Notes

تابع و پیوسته بودن

تعریف: فرض کنید $G\neq\phi$ ، $*$ را یک عمل دوتایی گویند.

$*: G\times G \longrightarrow G$ تابع

برای راحتی $\longleftarrow$ $*(a,b) = (a*b)$

مثال:

$+ : \mathbb{R}\times\mathbb{R} \longrightarrow \mathbb{R}$

$(a,b) \longmapsto (a+b)$

مثال:

ضرب $\cdot : \mathbb{R}\times\mathbb{R} \longrightarrow \mathbb{R}$

$(a,b) \longmapsto ab$

مثال: اگر $X\neq\phi$ و (کل زیرمجموعه های X) مجموعه توانی $= P(X)$

$\Delta : P(X)\times P(X) \longrightarrow P(X)$

$(A\cup B)-(A\cap B) \equiv (A-B)\cup(B-A)$

واضح است $\cup$ ، $\cap$ ، Δ یک عمل دوتایی هستند.

!! $a^2 = a*a \longrightarrow A^2 = A\Delta A = \phi$

مثال: اگر $X\neq\phi$ ، $S=\{f: X\to X\}$ تابع ، عمل ترکیب توابع روی S یک عمل دوتایی است.

$\circ : S\times S \longrightarrow S$

$(f,g) \longmapsto f\circ g$

مثال: آیا عمل $*$ در $\mathbb{Q}$ یک عمل دوتایی است؟ خیر!

$$*: \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$$
$$(a,b) \longrightarrow \frac{a}{b}$$
$$a*0$$

جایش: $\mathbb{Q} = \mathbb{Q}-\{0\}$

مثال: فرض کنید $G=\{a,b\}$ تعداد عمل های ۲تایی روی G را تعیین کنید.

$$*: G\times G \longrightarrow G$$
$$(a,b) \longrightarrow a*b$$

*	a	b
a	۲	۲
b	۲	۲

$\# *$ ۲×۲×۲×۲ = ۱۶

نکته: تعداد عمل های دوتایی روی یک مجموعه n عضوی برابر است با n^{n^2}

تمرین: فرض کنید $*$ یک عمل دوتایی در G باشد برای راحتی $a\times a = a^2$ نشان می‌دهیم $(a^2\times a = a^3)$

• قاعدهٔ جبر از ریاضی عمومی تبعیت می کند

$$a^m\times a^n = a^{m+n}$$
$$(a^m)^n = \underbrace{a^m\times\cdots\times a^m}_{n\text{ بار}}$$

تمرین: فرض کنید $G\neq\phi$ و $*$ یک عمل دوتایی است.

$(G,*)$ را یک گروه گویند اگر در خواص زیر صدق کند:

۱- شرکت پذیر باشد $(a*b)*c=a*(b*c)$

۲- $\exists e\in G \ \text{s.t.}\ \forall a\in G \quad a*e=e*a=a$

۳- $\forall a\in G, \exists a'\in G \ \text{s.t.}\ a*a'=a'*a=e$

تعریف: گروه G را آبلی گویند درصورتی که $*$ خاصیت جابه جایی داشته باشد.

مثال: $(\mathbb{R},+)$ و $(\mathbb{R}^*,\cdot)$ گروه آبلی هستند.

تذکر: فرض کنید G و $*$ یک گروه باشند معکوس a را با علامت a^{-1} نشان می‌دهیم.

مثال: فرض کنید $n\in\mathbb{R}$ ، $M_n(\mathbb{R}) = \{$ماتریس های $n\times n$ با درایه‌ی $\mathbb{R}\}$ واضح است $M_n(\mathbb{R})$ با جمع ماتریس‌ها گروه آبلی است.

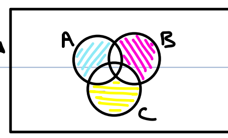
$AB \in M_n(\mathbb{R})$ $\quad$ X

$\det(AB) = \det(A)\cdot\det(B)$

$\neq 0 \quad \neq 0$

مثال: فرض کنید $X\neq\emptyset$ در این صورت $(P(X),\Delta)$ یک گروه آبلی است.

1- $(A\Delta B)\Delta C = A\Delta(B\Delta C)$



2- $A\Delta\emptyset = A$

3- $A\Delta A = \emptyset$

4- $A\Delta B = B\Delta A \longrightarrow$ آبلی است

مثال: فرض کنید $X=\{1,2,3\}$ و $S=\{f: X\to X \mid 1\text{-}1 ,\ \text{پوشا}\}$ واضح است S و ترکیب توابع تشکیل گروه می‌دهند.

$X \xrightarrow{f} X \xrightarrow{g} X$

$f\circ(g\circ h) = (f\circ g)\circ h$

$id(x) = x$

$f\,id(x) = f(x)$

$id\,f(x) = f(x)$

$f\,id = f$ همانی

واضح است با یک محاسبه ساده S و ترکیب توابع تشکیل یک گروه نا آبلی می‌دهند که عضو همانی آن توابع همانی است، با توجه به شرکت‌پذیری ترکیب توابع مجموعه S تشکیل یک گروه می‌دهند.

در ادامه مرتبه S_3 ، ساختار اعضای آن را بدست می‌آوریم.

$f:\{1,2,3\} \longrightarrow \{1,2,3\}$

S_3:

- $1 \longrightarrow$ ۳ حالت
- $2 \longrightarrow$ ۲ حالت $\xrightarrow[\text{اصل ضرب}]{}$ $\#f = 3\times 2\times 1 = 6$
- $3 \longrightarrow$ ۱ حالت

• با توجه به تعمیم نتیجه بالا اگر X مجموعه n عضوی باشد و به صورت $\{1,2,\dots,n\}$ باشد در این صورت مجموعه توابع یک به یک و پوشا از X به X را با S_n نشان می‌دهند و به راحتی دیده می‌شود که S_n از مرتبه $n!$ است.

$|S_n| = n!$

شکل اعضای S_3 به صورت زیر است.

$f:\{1,2,3\} \longrightarrow \{1,2,3\}$

$f_1: 1\to 1,\ 2\to 2,\ 3\to 3$ $\qquad f_2: 1\to 2,\ 2\to 1,\ 3\to 3$ $\qquad f_3: 1\to 3,\ 2\to 1,\ 3\to 2$

$f_4: 1\to 1,\ 2\to 3,\ 3\to 2$ $\qquad f_5: 1\to 2,\ 2\to 3,\ 3\to 1$ $\qquad f_6: 1\to 3,\ 2\to 2,\ 3\to 1$

• نماد بازگشتی:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

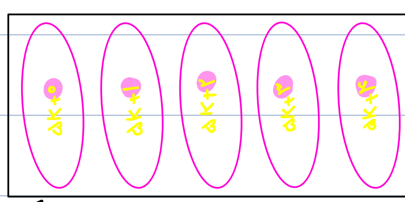
$\vdots$

مثال: فرض کنید n عدد طبیعی باشد باقی‌مانده اعداد بر n را در نظر بگیرید. این اعداد عبارتند از $\{0,1,2,\dots,n-1\}$، این مجموعه را با $\mathbb{Z}_n$ نشان می‌دهیم.

عمل جمع را در $\mathbb{Z}_n$ به صورت رو به رو تعریف می‌کنیم: $a +_n b := $ باقی‌مانده $a+b$ بر n

با عمل فوق $\mathbb{Z}_n$ یک گروه است.

- $(a +_n b) +_n c = a +_n (b +_n c)$
- $a +_n 0 = a$
- $a +_n a' = 0 \qquad a' = n - a$
- $a +_n b = b +_n a \longrightarrow$ گروه آبلی هست



$n = 5$

فشرده سازی ، هر کاری روی آن انجام شد روی نماینده‌ها نیز انجام می‌شود!

از هر مجموعه ناسازها نماینده را برمی‌داریم.

مثال: فرض کنید n عدد طبیعی باشد مجموعه U_n را به صورت زیر تعریف می کنیم:

$$U_n = \{a \in \mathbb{N} \mid a<n ,\ (a,n)=1\}$$

$U_6 = \{1,5\}$ $\qquad$ $U_5 = \{1,2,3,4\}$ $\qquad$ * ضرب $3\times4 = 12$

تو U_5 نیست ولی نماینده اش

یعنی باقی مانده اش ۲ هست.

- U_n با ضرب اعداد به پیمانه n تشکیل یک گروه می دهند:

که عضو خنثی این گروه ۱ و عضو وارون هر عضو درون خودش است.

معکوس ضرب دارد

$(a,b)=d \implies (a,n)=1$

$\exists r,s\in\mathbb{Z} \quad ra+sb=d \qquad ra+sn=1 \implies ra \overset{n}{\equiv} 1$

مثال: گروه ۴ تایی کلاین:

فرض کنید $G=\{e,a,b,c\}$ باشد

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

$aa=e$

$ab=c$

$ac=b$

آبلی ✓

→ معکوس $a^{-1}=a ,\ b^{-1}=b ,\ c^{-1}=c$

→ همانی

→ شرکت پذیری $\longrightarrow \begin{cases} a(\overset{a}{\overline{bc}}) = e \\ (\overset{c}{\overline{ab}})c = e \end{cases}$

$\begin{cases} \text{جزء} \xrightarrow{\times} \text{کل} \\ \text{کل} \xrightarrow{\checkmark} \text{جزء} \end{cases}$

قضیه: فرض کنید $(G, *)$ یک گروه باشد در این صورت عضو همانی گروه و وارون هر عضو منحصر به فرد است.

برهان: فرض کنید در گروه G، e_1 و e_2 همانی باشند. نشان می‌دهیم $e_1 = e_2$:

$$\underset{}{\overset{\text{همانی}}{e_1}} * e_2 = \overset{\text{همانی}}{e_2} * e_1 = e_2$$

$$\longrightarrow e_1 = e_2$$

$$\overset{\text{همانی}}{e_2} * e_1 = \overset{\text{همانی}}{e_1} * e_2 = e_1$$

برهان: فرض کنید در گروه G، b و c عضو وارون a اند

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c \longrightarrow c = b$$

نکته: اگر $(G, *)$ یک گروه باشد، عضو خنثی آن را (منحصر به فرد) با e و عضو وارون آن را (منحصر به فرد) با a^{-1} نشان می‌دهیم

نکته: فرض کنید $(G, *)$ یک گروه باشند در این صورت:

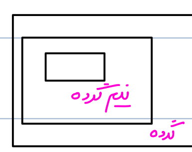
۱- $(a^{-1})^{-1} = a$ **برهان:** $aa^{-1} = e$، $a^{-1}(a^{-1})^{-1} = e$ $\longrightarrow$ و چون معادل یکتاست: $a = (a^{-1})^{-1}$

۲- $(ab)^{-1} = b^{-1}a^{-1}$ **برهان:** $(ab)(b^{-1}a^{-1}) \overset{\text{شرکت‌پذیری}}{\Longrightarrow} a(\overbrace{bb^{-1}}^{e})a^{-1} = aa^{-1} = e$

و چون معادل یکتاست: $(ab)^{-1} = b^{-1}a^{-1}$

تعریف: فرض کنید G یک مجموعه ناتهی و $*$ یک عمل دوتایی باشد به طوری که $*$ شرکت‌پذیر است در این صورت $(G, *)$ را یک نیم‌گروه گوییم.

گروه = عضو خنثی + عضو وارون + نیم‌گروه



این ضرب که می‌شناسیم نیست!

نتیجه: فرض کنید $(G, *)$ یک گروه باشد از این به بعد اگر دچار مشکل نشویم $*$ را عمل ضرب در نظر می‌گیریم.

$$a * b = ab$$

نتیجه: اگر G یک گروه باشد در این صورت اگر a و b دو عضو دلخواه گروه باشند در این صورت هر یک از معادلات $\overset{ba^{-1}}{y}a = b$ و $ax = b$ دارای جواب است.

$$a \in G \Longrightarrow a^{-1} \in G \left.\begin{matrix} \\ b \in G \end{matrix}\right\} a^{-1}b \in G \longrightarrow a(\underbrace{a^{-1}b}_{x}) = b$$

نکته: درمورد ماتریس‌ها حتما باید وارون پذیر باشد.

قضیه: فرض کنید $(G, *)$ یک نیم گروه باشد. در این صورت $(G, *)$ یک گروه است اگر و تنها اگر هر یک از معادلات خطی دارای جواب باشد

$(G, *)$ یک گروه است $\Longleftrightarrow$ $ya = b$, $ax = b$

تعریف: فرض کنید G یک نیم گروه باشد اگر از تساوی $ab = ac$ بتوان نتیجه گرفت $b = c$ می‌توان نتیجه گرفت قانون حذف از چپ برقرار است.

تعریف: فرض کنید G یک نیم گروه باشد اگر از تساوی $ba = ca$ بتوان نتیجه گرفت $b = c$ می‌توان نتیجه گرفت قانون حذف از راست برقرار است.

تذکر: اگر G یک گروه باشد قوانین حذف از چپ و راست برقرار است.

برهان: $ab = ac \longrightarrow a^{-1}(ab) = a^{-1}(ac) \longrightarrow \overset{e}{\overline{(a^{-1}a)}}\, b = \overset{e}{\overline{(a^{-1}a)}}\, c \longrightarrow b = c$

نکته: فرض کنید G یک نیم گروه متناهی باشد به طوری که قوانین حذف راست و چپ برقرار باشد در این صورت G گروه است.

حل: فرض کنیم $G = \{a_1, a_2, \dots, a_n\}$ و $a, b \in G$ دلخواه، هدف این است که معادلات $ax = b$, $ya = b$ برقرار شوند اعضای $T = \{aa_1, aa_2, \dots, aa_n\}$ را در نظر بگیریم واضح است $\underset{n}{T} \subseteq \underset{n}{G}$ و اعضای T دو به دو متمایز است. $\forall i, j \quad aa_i = aa_j \xrightarrow[\text{قوانین حذف}]{\text{طبق برقراری}} a_i = a_j$

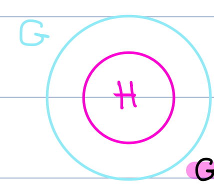
پس $T = G$. چون $b \in G$ پس $b \in T$ است لذا i ای است $aa_i = b$ پس معادله $ax = b$ حل پذیر است.

مثال: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

بدیهی

$\{0\}$ ✓ گروه $\{0, 1\}$ ✗ $1+1=2$ نوشتنیست

$\{0, 2\}$ ✓ گروه $\{0, 1, 2\}$ ✗



$G \leqslant H$
زیرگروه

۱۶ تا زیرمجموعه ←   مطمئن هستیم ۲ تا از این زیرمجموعه‌ها زیرگروه اند → های وخودگروه

تعریف: فرض کنید G یک گروه باشد و H زیر مجموعه ناتهی G. اگر H و عمل گروه تشکیل یک گروه بدهند H را زیرگروه G گویند و می نویسیم

$$H \leqslant G$$

H را زیرگروه واقعی گویند درصورتی که $H \neq G$ و می نویسیم $H < G$

!! هر گروه دارای حداقل ۲ زیرگروه می باشند ← $\{e\}$, $\{G\}$

مثال: $(\mathbb{Z},+) \leqslant (\mathbb{Q},+) \leqslant (\mathbb{R},+)$

چه جوری بفهمیم زیرگروه ؟ وارون و همانی و بسته بودن را باید چک کنیم

قضیه: فرض کنید G یک گروه، H زیر مجموعه ناتهی G باشد $(H \subseteq G)$ آنگاه H زیرگروه است $(H \leqslant G)$ اگر و تنها اگر $ab^{-1} \in H$

$$\forall a,b \in H \quad ab^{-1} \in H \longleftrightarrow H \leqslant G$$

$$b \in H \longrightarrow b^{-1} \in H, \quad a \in H \longrightarrow ab^{-1} \in H$$

وجود همانی: $a = b \longrightarrow ab^{-1} \in H \longrightarrow aa^{-1} \in H \longrightarrow e \in H$

وجود معکوس: $a = e\ ,\ b = H \longrightarrow eb^{-1} \in H \longrightarrow b^{-1} \in H$

بسته بودن: $\forall a,b \in H \longrightarrow ab \in H$

$a,b \in H \longrightarrow b^{-1} \in H \longrightarrow a(b^{-1})^{-1} \in H \longrightarrow ab \in H$

مثال: $n \in \mathbb{Z} = n$ مضارب $= \{nk \mid k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \dots\}$ ← $(n\mathbb{Z},+) \leqslant \mathbb{Z}$ واضح است

$+G$	معکوس دومی، عمل گروه، اولی	G ضرب
$a-b \in H$		$ab^{-1} \in H$

تذکر: اگر عمل گروه G جمعی باشد عضو خنثی را با 0 و عضو معکوس را با $-b$ نشان می دهیم بنابراین اگر بخواهیم زیرگروه بودن H را بررسی کنیم

کافی است ثابت کنیم به ازای هر $a,b \in H$ ، $a-b \in H$

$a + (-b)$: اولی ← ، عمل گروه ← ، معکوس دومی ←

$$a = nk_1,\quad b = nk_2 \longrightarrow a-b = n(k_1-k_2) \in n\mathbb{Z}$$

تذکر: تعداد زیرگروه $\mathbb{Z}$ بی نهایت است. مثلاً: $2\mathbb{Z}, 3\mathbb{Z}, \ldots$

تعداد زیرگروه های $\{0,1,2,3\}$ $\longleftarrow$ $\{0, 2^3\}$: 2^{n-1}

باید باشد

۳ عضو دیگر می توانند باشند
می توانند نباشند

مثال: تمام زیرگروه های ۴ کلاین را مشخص کنید. $\{e,a,b,c\}$ $\quad a^2=b^2=c^2=e$

مرتبه زیرگروه باید مرتبه گروه را عاد کند

۵ تا زیرگروه ها $\longleftarrow$ $\{e,c\}\quad \{e,b\}\quad \{e,a\}\quad \{e\}\quad \{e,a,b,c\}$

$\{e,a,b\}$ ✗ ۳ تایی نداریم

$\{a,b\}\quad \{b,c\}$ ✗

تعریف: فرض کنید G یک گروه باشد و a عضوی از آن قرار دهیم

$$H := \{a^n \mid n \in \mathbb{Z}\} = \{e, e^{\pm 1}, e^{\pm 2}, \ldots\}$$

توجه کنید که این مجموعه یک زیرگروه G است

این زیرگروه را زیرگروه دوری تولید شده با a گویند و

با علامت $\langle a \rangle$ نشان می دهیم.

$$a^0 = e, \quad \underset{\downarrow\; a^{-2}}{a^2 = aa}, \quad \underset{\downarrow\; a^{-3}}{a^3 = a^2 a}, \quad \ldots$$

$$a = a^n \longrightarrow a^n (a^m)^{-1} = a^n a^{-m} = a^{n-m}$$

$$b = a^m$$

$\longrightarrow ab^{-1} \in H$

مثال: دوران ها یک زیرگروه دوری اند.

تذکر: اگر G یک گروه باشد علاوه بر زیرگروه هایی، زیرگروه های دوری نیز ساخته می شود.

تعریف: گروه G را گروه دوری گوییم هرگاه که عضوی مانند a داشته باشد به طوری که $\langle a \rangle = G$

اگر عمل جمع بود $\longleftarrow$ ۲تا $\longleftarrow$ $2a$

اگر عمل ضرب بود $\longleftarrow$ ۲تا $\longleftarrow$ a^2

مثال: $(\mathbb{Z}, +)$ گروه دوری است.

$$(\mathbb{Z}, +) = \langle 1 \rangle$$
$$= \{1k \mid k \in \mathbb{Z}\}$$

تذکر:

$\langle a \rangle = \{0, \pm a, \pm 2a, \dots\}$

$H = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \dots\}$

G را دوری گویند: $\exists a \in G \;\; s.t. \;\; \langle a \rangle = G$

نکته:

$\mathbb{Z} = \langle 1 \rangle = \{0, \pm 1, \pm 2, \dots\}$

$\mathbb{Z} = \langle -1 \rangle$

$2\mathbb{Z} = \langle 2 \rangle = \{0, \pm 2, \pm 4, \dots\}$

$3\mathbb{Z} = \langle 3 \rangle = \{0, \pm 3, \pm 6, \dots\}$

مثال: آیا $(\mathbb{Q}, +)$ دوری است؟ خیر!

$\langle \frac{m}{n} \rangle \;,\; (m, n) = 1$

$\langle \frac{2}{3} \rangle = \{0, \pm \frac{2}{3}, \pm \frac{4}{3}, \pm \frac{6}{3}, \dots\}$

$\frac{1}{5} \notin \langle \frac{2}{3} \rangle$

فرض کنیم هست

$\frac{1}{5} = m \frac{2}{3} \longrightarrow 3 = m \times 2 \times 5$

۵ سمت چپ را عاد نمی‌کند ، سمت راست را عاد می‌کند

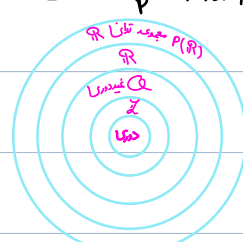
هیچ وقت تمام نمی‌شه ← مثلا: $\frac{1}{11} \notin \langle \frac{3}{35} \rangle \longleftarrow \frac{1}{11} = m \frac{3}{35} \longleftarrow 35 = 3 \times 11 \times m$ مضرب ۱۱ نیست

• با تعداد متناهی تولید نمی‌کند

$(\mathbb{Q}, +)$ دوری نیست زیرا اگر فرض کنیم دوری باشد لذا با عضوی مانند $\frac{m}{n}$ تولید می شوند فرض کنید m و n نسبت به هم اول باشند از نماد $\pi(n)$ به عنوان اعداد اول ظاهر شده در تجزیه n استفاده می کنیم $(\pi(12) = 2, 3)$ می دانیم $\pi(n)$ متناهی است فرض کنید p عدد اولی باشد که عضو $\pi(n)$ نباشد $(p \notin \pi(n))$ ادعا می کنیم $\frac{1}{p} \notin \langle \frac{m}{n} \rangle$ زیرا اگر این طور باشد n مضرب p نیست.

$$\frac{1}{p} = \frac{m}{n} k \longrightarrow \underbrace{n}_{\text{مضرب} \; p \; \text{نیست}} = \underbrace{p \times m \times k}_{\text{مضرب} \; p}$$

نکته ←



مثال: در مورد مولدهای گروه های $\mathbb{Z}_4$ ، $\mathbb{Z}_5$ ، $\mathbb{Z}_6$ بحث کنید.

$\mathbb{Z}_4 = \{0,1,2,3\}$ $\langle 1\rangle = \mathbb{Z}_4$, $\langle 2\rangle = \{0,2\}$, $\langle 3\rangle = \{0,3,2,1\}$

$3\times3 = 9 \,|\, 4$ → 1

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ $\langle 1\rangle = \mathbb{Z}_5$, $\langle 2\rangle = \{0,2,4,1,3\}$, $\langle 3\rangle = \{0,3,1,4,2\}$

$2\times 2 = 4 \,|\, 5$

$\langle 4\rangle = \{0,4,3,2,1\}$

نکته: $\mathbb{Z}_n = \langle i\rangle \quad (i,n)=1$

- تعداد / اعداد طبیعی کوچکتر از n که نسبت به n اول اند $= \phi(n)$ فی - اویلر
- $\phi(p) = p-1$ (p عدد اول)
- $(m,n)=1 \longrightarrow \phi(m.n) = \phi(m)\phi(n)$
- $\phi(p^n) = p^n - \left[\frac{p^n}{p}\right] = p^n - p^{n-1}$
- $(i,p^n)=1 \longrightarrow (i,p)=1$ $\quad 1,2,3,\dots,p,p+1,p+2,\dots,2p,2p+1,\dots$

سوال ارشد: تعداد مولدهای گروه دوری $\mathbb{Z}_{12}$ کدام است؟

$\phi(12) = \phi(2^2\times 3) = \underbrace{\phi(2^2)}_{(2^2-2)}\times\underbrace{\phi(3)}_{2} = 4$

مثال: $\phi(100) = \phi(2^2\times5^2) = (2^2-2)(5^2-5) = 2\times20 = 40$

تعریف: فرض کنید G یک گروه باشد. تعداد اعضای G را مرتبه G ، و با علامت $|G|$ نشان می دهیم

و اگر نامتناهی باشد می نویسیم: $|G| = \infty$

تعریف: فرض کنید G یک گروه متناهی باشد. $a\in G$ در این صورت کوچکترین عدد طبیعی مانند n که a^n برابر همانی شود $(a^n = e)$

مرتبه عضو گوئیم و با علامت $o(a)=n$ نشان می دهند. با توجه به تعریف نتیجه می شود اگر گروهی متناهی باشد مرتبه عضوش

متناهی است.

$a \in G \quad , \quad T = \{e, a^1, a^2, \dots\} \underset{\text{متناهی}}{\subseteq} G$

چون G مجموعه متناهی است. لذا T نیز متناهی است بنابراین نباید اعضای آن غیر متمایز باشند.

پس $i \neq j$ وجود دارد که $a^i = a^j$ است $\quad a^i = a^j \longrightarrow a^{i-j} = e$ در نتیجه همان n وجود دارد

مثال: گروهی را مثال بزنید که نامتناهی باشد و مرتبه هر عضو آن متناهی باشد.

A نامتناهی $\qquad A \Delta B = (A \cup B) - (A \cap B)$

$(P(A), \Delta) \qquad \underset{\text{همانی}}{A \Delta A = \phi} \longrightarrow A^2 = e \quad , \quad o(A) = 2$

مثال: $(\mathbb{Z}, +)$ هیچ عضو مرتبه متناهی ندارند.

$(G, +) \qquad 2n \neq 0$

مرتبه $= na = 0 \qquad o(2) = \infty$

تمرین: اشکال استدلال زیر را بیابید.

$0 = \underbrace{0 + 0 + \dots + 0}_{\text{بی‌نهایت}}$

$= (1-1) + \dots + (1-1)$

$= 1 + (-1+1) + (-1+1) + \dots$

$= 1 + 0 + 0 + \dots$

$= 1$

یادآوری:

$G = \langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \dots\}$

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$

$o(a) = m \qquad a^m = e$ $\quad m$ کوچکترین توانی است که a به توان آن همانی شود

نتیجه: اگر G یک گروه باشد، مرتبه عضو همانی برابر ۱ است.

$e^1=e \quad , \quad o(e)=1$

مثال:

$\mathbb{Z}_{12}=\langle 1\rangle$ همانی

$o(1)=12 \quad , \quad o(5)=12 \quad , \quad o(7)=12 \quad , \quad o(11)=12$

$o(2)=\frac{12}{(2,12)}=6 \quad , \quad o(3)=\frac{12}{(3,12)}=4 \quad , \quad o(6)=\frac{12}{(6,12)}=2$

نتیجه: فرض کنیم $o(a)=n$, $a^m=e$ آنگاه $n|m$

حل. حل الگوریتم تقسیم: $m=nq+\overset{\text{باقی‌مانده}}{r}$ که $0\leq r<n$

$e=a^m=a^{nq+r}=(\underbrace{a^n}_{e})^q a^r=a^r \longrightarrow a^r=\cancel{e} \longrightarrow r=0 \longrightarrow m=nq \longrightarrow n|m$

چون n کوچک‌ترین است $r<n$

نتیجه: گروه های دوری آبلی هستند.

حل: $G=\langle a\rangle$ فرض کنیم $x,y\in G$ پس $x=a^i$, $y=a^j$ که $i,j\in\mathbb{Z}$

$xy=a^ia^j=a^{i+j}=a^ja^i=yx$

$V=\{e,a,b,c\}$

$a^2=e=b^2=c^2$

$a^3=a^2a=a$

توان های زوج همانی را می‌دهند و توان های فرد a را

در نتیجه c, b تولید نمی‌شوند پس دوری نیست

ولی آبلی هست

$|G| \longrightarrow P(G)$ اضافی!

```
for H in P(G) do :
    for a and b in H do :
        t := ab^-1 in H
        if t = false then
            break
        :
    odj
odj
```

$x = y z$ نکته:

$\in G \quad \in G$

قضیه: هر زیرگروه دوری ، دوری است.

برهان: فرض کنید $G=\langle a\rangle$ و $H\leqslant G$ باشد ، می دانیم اعضای H توان‌هایی از a می باشند این توان ها مثبت و منفی است.

فرض کنید n کوچکترین عدد طبیعی باشد که a^n عضو H باشد. ادعا می‌کنیم $H=\langle a^n\rangle$

فرض کنیم: $\underset{\text{دلخواه}}{x\in H} \longrightarrow x\in G \longrightarrow \exists m\in\mathbb{Z}\ \ s.t.\ \ x=a^m$

$0\leqslant r<n \qquad m=nq+r \qquad \underset{\in H}{a^m}=(\underset{\in H}{a^n})^q a^r \longrightarrow \underset{\text{چون } n \text{ کوچکترین است}}{a^r\in H} \longrightarrow r=0 \longrightarrow \underline{n\mid m}$

$a^m=(a^n)^q\in\langle a^n\rangle \longleftarrow m=nq \longleftarrow$

نتیجه: تمام زیرگروه های $\mathbb{Z}$ دوری است و به صورت $n\in\mathbb{Z}$ $\quad n\mathbb{Z}$ است

مضارب یک

$1\mathbb{Z},\ 2\mathbb{Z},\ 3\mathbb{Z},\ ...$

نتیجه: اگر G گروه دوری باشد و G با a تولید شود اگر مرتبه G نامتناهی باشد نتیجه می شود $o(a)=\infty$

نکته: اگر $G=\langle a\rangle,\ |G|<\infty \Longrightarrow |G|=o(a)$

نکته: اگر $G=\langle a\rangle,\ |G|=\infty \Longrightarrow o(a)=\infty$

ساختار یکسان

نکته: فقط یک گروه دوری از مرتبه n داریم که آن $\mathbb{Z}_n$ است. توجه شود هر گروه دوری از مرتبه n یکریخت است

همچنین فقط یک گروه دوری نامتناهی داریم که آن هم $\mathbb{Z}$ است.

فعلا بدون برهان برای یکریختی

$\mathbb{Z}_n=\{0,1,2,...,n-1\}$

$G=\langle a\rangle=\{e,a,a^2,...,a^{n-1}\}$

هدف: شمارش تعداد زیرگروه های یک گروه دوری

نکته: اگر $G=\langle a\rangle$ که $|G|=n$ $(G \cong \mathbb{Z}_n)$ ← فقط یک گروه دوری داریم که $|G|=n$

تناظر یک به یک بین زیرگروه های G و مجموعه مقسوم علیه های n وجود دارد.

$n=12 \qquad G=\langle a\rangle \qquad |a|=12$

مقسوم علیه ها $=\{1,2,3,4,6,12\}$

G دارای ۶ زیرگروه است

$H_1=\langle a\rangle = G$

$H_2=\langle a^2\rangle \longrightarrow |H_2| = \dfrac{12}{(2,12)}=6$

$\{1, a^2, (a^2)^2, (a^2)^3, (a^2)^4, (a^2)^5\}$

$H_3=\langle a^3\rangle \longrightarrow |H_3| = \dfrac{12}{(3,12)}=4$

$\{1, (a^3)^1, (a^3)^2, (a^3)^3\}$

$H_4=\langle a^4\rangle \longrightarrow |H_4| = \dfrac{12}{(4,12)}=3$

$\{1, a^4, (a^4)^2\}$

$H_5=\langle a^6\rangle \longrightarrow |H_5| = \dfrac{12}{(6,12)}=2$

$\{1, (a^6)^1\}$

$H_6=\langle a^{12}\rangle \longrightarrow |H_6| = \dfrac{12}{(12,12)}=1$

$\{a^{12}\}=\langle 1\rangle=1$

مثال: تعداد زیرگروه ها:

$G=\langle a\rangle \qquad \dfrac{n}{(n,i)} = \dfrac{n}{i}$

نکته: فرض کنید n دارای عددی باشد که تجزیه‌ای به صورت $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ در این صورت هر مقسوم علیه n به صورت d می باشد
که در آن $d = p_1^{\beta_1} \times \cdots \times p_t^{\beta_t}$ باشد که در آن $0 \leq \beta_i \leq \alpha_i$

$$\# d = \# \beta_1 \times \cdots \times \# \beta_t = (\alpha_1+1) \cdots (\alpha_t+1)$$

مثال: تعداد زیرگروه های دوری گروه از مرتبه ۱۰۰۰ را پیدا کنید

$$1000 = 2^3 \times 5^3$$

تعداد زیرگروه ها : $(3+1)(3+1) = 16$

نکته: فرض کنید G با a تولید شود به طوری که مرتبه a شود n در این صورت مرتبه a_i به صورت زیر به دست می آید

$G = \langle a \rangle \quad , \quad |a| = n$

$$o(a_i) = \frac{o(a)}{(o(a), i)}$$

مثال: فرض کنیم $G = \langle a \rangle$, $|a| = 36$ مطلوب است:

$$o(a^2) = \frac{36}{(2,36)} = 18 \qquad o(a^3) = \frac{36}{(3,36)} = 12 \qquad o(a^5) = \frac{36}{(5,36)} = 36$$

نکته: فرض کنیم $G = \langle a \rangle$ و مرتبهٔ a ، n باشد در این صورت سایر مولدهای G به صورت a^i می باشند که در آن $(i,n) = 1$

$$G = \langle a \rangle \xrightarrow{\text{مولد}} \{a^1, a^5, a^7, a^{11}\}$$

$|a| = 12$

تعداد را با تابع اویلر می توانیم پیدا کنیم

تعریف: فرض کنید G یک گروه باشد و H یک زیرگروه G, $a\in G$ — $Ha=\{ha \mid h\in H\}$

از تعریف همدسته نتیجه می‌شود که $a\in Hxa$

تعریف: فرض کنید G یک گروه باشد و H زیرگروه G رابطه ~ را به صورت زیر تعریف می‌کنیم.

$a\sim b \longleftrightarrow ab^{-1}\in H$

• رابطهٔ تعریف شده یک رابطهٔ هم ارزی است.

انعکاسی $\quad a\sim a \longleftrightarrow aa^{-1}=e\in H$

تقارنی $\quad$ if $a\sim b \longrightarrow \underbrace{ab^{-1}\in H}_{\text{زیرگروه}} \longrightarrow (ab^{-1})^{-1}\in H \longrightarrow b^{-1}a\in H \Longrightarrow b\sim a$ $\quad$ وارون بگیر

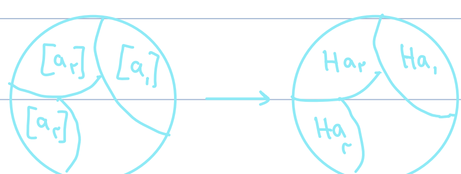
تعدی $\quad a\sim b,\ b\sim c \longrightarrow ab^{-1}\in H,\ bc^{-1}\in H \longrightarrow a\underbrace{b^{-1}b}_{e}c^{-1}\in H \longrightarrow ac^{-1}\in H \longrightarrow a\sim c$

با توجه به اینکه رابطهٔ تعریف شده یک رابطهٔ هم ارزی است بنابراین رابطهٔ مذکور مجموعه G را به کلاس های هم ارزی افراز می‌کنیم اما طبق قراردادهای مبانی ریاضی کلاس هم ارزی A را با نماد $[a]$ نشان می‌دهیم، که به صورت زیر محاسبه می‌شود.

$$[a]=\{b\in G \mid a\sim b\}=\{b\in G \mid ab^{-1}\in H\}=\{b\in G \mid b^{-1}a\in H\}=\{b\in G \mid b=ha\}=\underbrace{Ha}_{\text{همدسته!}}$$

$b^{-1}a=h$

$b=ah$



با توجه به اینکه G را می‌توان اجتماعی از کلاس های مجزا نوشت

بنابراین $\quad G=\overset{\text{مجزا}}{\dot{\bigcup_{i\in I}}}[a_i]=\dot{\bigcup_{i\in I}}Ha_i$

کلاس بندی را پیدا کردن = هم دسته بردن

نکته: اگر زیرگروه داشته باشیم حتما باید مرتبه گروه را عاد کند

$$|G| = |Ha_1| + \dots + |Ha_n| = n|Ha_1| = n|H|$$

$$|G| = n|H|$$

$|H| \mid |G|$ ⟵ بنابر این مرتبه H ، مرتبه G را عاد می‌کند

قضیه لاگرانژ:

فرض کنید G یک گروه متناهی و H زیرگروه آن باشد. با توجه به بحث انجام شده در بالا مرتبه H ، مرتبه G را عاد می‌کند

تذکر: فرض کنیم G یک گروه است و $H \leq G$ در این صورت $\forall a,b \in G : |Ha| = |Hb| = |H|$

حل:

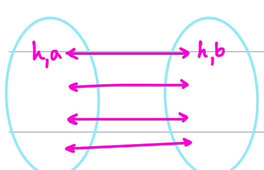
سای $\psi : Ha \longrightarrow Hb$

$ha \longmapsto hb$

ψ یک به یک است زیرا: $\psi(ha) = \psi(hb)$ ⟵ $hb = h'b$ $\xleftarrow[\text{حذف گروه ها}]{\text{طبق قانون}}$ $h = h'$ ⟵ پس $ha = h'a$

ψ پوشاست زیرا: فرض کنیم $hb \in Hb$ (دلخواه) واضح است $\psi(ha) = hb$

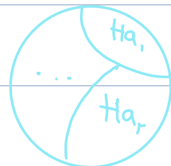
با قرار دادن $b = e$ تساوی دوم نتیجه می‌شود.



مثال: گروه از مرتبه ۲۵ ، زیرگروه از مرتبه ۱۵ ندارد. زیرگروه های آن می‌تواند از مرتبه (۲۵ ، ۵ ، ۱) باشد

همانی — $\mathbb{Z}_5$ — خودش $\mathbb{Z}_{25}$

تعریف: فرض کنید G یک گروه متناهی باشد و H زیرگروه آن باشد. در این صورت تعداد همدسته‌های H در G را اندیس یا شاخص H در G گویند (index) و با علامت $|G:H|$ نشان می‌دهند.



$$G=\bigcup_{i=1}^{n} Ha_i = Ha_1+\dots+Ha_n$$

$$|G|=n|H|$$

index = $\dfrac{\text{مرتبه گروه}}{\text{مرتبه زیرگروه}}$

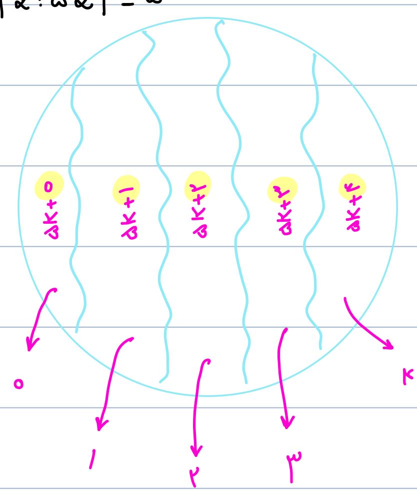
تذکر: اگر G یک گروه متناهی باشد و H زیرگروه آن گاه:

$$|G:H|=\frac{|G|}{|H|}$$

مثال: می‌دانیم کلیه زیرگروه‌های $\mathbb{Z}$ به صورت $n\mathbb{Z}$ است. قرار دهیم $G=\mathbb{Z}$ و $H=n\mathbb{Z}$. مطلوب است محاسبه $|\mathbb{Z}:n\mathbb{Z}|$

$\longrightarrow n$

$|\mathbb{Z}:۵\mathbb{Z}|=۵$



$Ha \longrightarrow$ همدسته راست

$aH \longrightarrow$ همدسته چپ

اگر $|G| = 15$ ، $H \leqslant G$ باشد آنگاه $|H| \mid 15$

$|H| = 1 \longrightarrow H = \langle e \rangle$

$|H| = 3 \longrightarrow H \cong \mathbb{Z}_3$

$|H| = 5 \longrightarrow H \cong \mathbb{Z}_5$

$|H| = 15 \longrightarrow H \cong G$

نتایجی از قضایای لاگرانژ:

۱- اگر G یک گروه متناهی و $a \in G$ در این صورت $o(a) \mid |G|$ (مرتبه عضو) پس $a^{|G|} = e$

حل: $H = \langle a \rangle$ واضح است $|H| = o(a)$. طبق لاگرانژ $|H| \mid |G|$ لذا $o(a) \mid |G|$

از طرفی $k \in \mathbb{N}$ است که $|G| = o(a)k$ ، $a^{|G|} = a^{o(a)k} = (\underbrace{a^{o(a)}}_{e})^k = e$

۲- هر گروه از مرتبه عدد اول دوری است. (مهم)

$|G| = 23 \xrightarrow{\text{متناهی}} G \cong \mathbb{Z}_{23}$

حل: فرض کنیم $|G| = p$ که p عدد اول است. $e \neq a \in G$ قرار دهیم $H = \langle a \rangle$

واضح است $H \neq e$ ، طبق لاگرانژ $|H| \mid |G| = p$ پس $|H| = |G|$

از طرفی $H \leqslant G$ پس $H = G = \langle a \rangle$

تعریف: فرض کنید $n \in \mathbb{N}$ باشد. U_n را به صورت زیر تعریف می‌کنیم:

$$U_n = \{ i \in \mathbb{N} \ , 1 \leqslant i < n \mid (i,n) = 1 \} \longrightarrow |U_n| = \phi(n)$$

عمل ضرب به پیمانه n را به U_n تحدید می‌کنیم

$U_{10} = \{1, 3, 7, 9\}$ $\quad \phi(10) = \phi(2)\phi(5) = 4$

$a * b =$ باقی‌مانده حاصل‌ضرب ab بر n $= \overline{ab}^{\,n} = ab \equiv_n$

برای بررسی عمل بودن توجه شود فقط بسته بودن بررسی شود

فرض کنید $(a,n) = 1$ ، $(b,n) = 1$ واضح است $(a,b,n) = 1$

گروه U_n را گروه یکانی به پیمانه n گویند

قضیه اویلر:

فرض کنید $n\in\mathbb{N}$ ، $(a,n)=۱$ در این صورت $a^{\phi(n)}\equiv_n ۱$ است.

$(۲,۱۷) \longrightarrow ۲^{\phi(n)}\equiv_n ۱ \longrightarrow ۲^{۱۶}\equiv_n ۱$

باقیمانده

حل: $(a,n)=۱ \longrightarrow \bar{a}\in U_n \xrightarrow[\text{لاگرانژ}]{\text{نتیجه}} a^{\phi(n)}=۱$

سلام

قضیه فرما:

فرض کنید p عدد اول باشد ، $(a,p)=۱$ آنگاه $a^{p-1}\equiv_p ۱$

حل: با توجه به قضیه اویلر داریم $a^{\phi(p)}\equiv_p ۱$ پس $a^{p-1}\equiv_p ۱$

نتیجه: اگر p عدد اول باشد همواره $a^p\equiv_p a$ است.

تمرین: ثابت کنید هر گروه مرتبه کمتر از ۶ آبلی است.

$|G|=۱ \longrightarrow G=\langle e\rangle$

$|G|=۲ \longrightarrow G\underset{\text{دوری}}{\cong}\mathbb{Z}_۲$

$|G|=۳ \longrightarrow G\cong\mathbb{Z}_۳$

$|G|=۴ \longrightarrow G\cong\mathbb{Z}_۴$

$\qquad\quad \searrow V$ ۴-کلاین

$|G|=۵ \longrightarrow G\cong\mathbb{Z}_۵$

S ، با ترکیب توابع گروه است

$X=\{۱,۲,۳\}$ $\quad S=\{f: X\longrightarrow X \mid$ پوشا ، $۱\text{-}۱\ f\}$

S آبلی نیست.

$fg\neq gf$

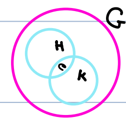
$f: ۱\longrightarrow ۱,\ ۲\longrightarrow ۳,\ ۳\longrightarrow ۲$

$g: ۱\longrightarrow ۲,\ ۲\longrightarrow ۱,\ ۳\longrightarrow ۳$

$fg: ۱\longrightarrow ۳,\ ۲\longrightarrow ۱,\ ۳\longrightarrow ۲$

$gf: ۱\longrightarrow ۲,\ ۲\longrightarrow ۳,\ ۳\longrightarrow ۱$

تعریف: فرض کنید H و K زیرگروه های G باشند در این صورت ضرب نقطه‌ای HK را به صورت زیر تعریف می‌کنیم:



$$HK = \{hk \mid h \in H, k \in K\}$$

$$H \times K = \{(h,k) \mid h \in H, k \in K\} \longrightarrow |H \times K| = |H||K|$$

توجه شود! $HK \subseteq G$

دلیل: نیازه ضرب ۲ تا زیرگروه زیرگروه شود

سوال مهمی که مطرح می‌شود اینکه تحت چه شرایطی HK تشکیل زیرگروه می‌دهد.

در قضیه زیر شرط لازم و کافی برای آنکه ضرب ۲ زیرگروه، تشکیل زیرگروه بدهد را بررسی می‌کنیم.

$$\underbrace{HK = KH}_{\text{تساوی مجموعه}} \Longleftrightarrow HK \leqslant G$$

$$\overbrace{h_1k_1}^{a}\ \overbrace{h_2k_2}^{b} = h_3k_3$$

$$\in KH = HK \quad = h_1h'k'k_2 \in HK$$

لزوما همان h_3k_3 نیست اما در HK وجود دارد.

نکته: اگر گروه G آبلی باشد آنگاه حاصل ضرب هر دو زیرگروه یک زیرگروه می‌شود

نتیجه: اگر $H, K \leqslant G$ در این صورت

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

نکته: فرض کنیم G یک گروه باشد در این صورت اشتراک هر تعداد زیرگروه باز هم باهم زیرگروه است

می‌تواند متناهی یا نامتناهی باشد (مجموعه اندیس گذاره) $I = \{1, \ldots, \infty\}$ یا $I = \{1, \ldots, n\}$

حل: $H_i \leqslant G \ (i \in I)$ قرار می‌دهیم: $K = \bigcap_{i \in I} H_i$

$$a, b \in K \xrightarrow{\text{حکم}} ab^{-1} \in K$$

$$a, b \in K \longrightarrow a, b \in H_i \underset{i \in I}{} \leqslant G \longrightarrow ab^{-1} \in H_i \underset{i \in I}{} \longrightarrow ab^{-1} \in \bigcap_{i \in I} H_i = K$$

تعریف: فرض کنیم G یک گروه باشد، $N \leqslant G$ ، زیرگروه N را ، زیرگروه نرمال گوئیم.

درصورتی که $\forall g \in G, \forall n \in N \quad g^{-1}ng \in N$

$$g^{-1}ng \in N \iff g^{-1}Ng \subseteq N \iff g^{-1}Ng = N \iff Ng = gN$$

$$\varphi : g^{-1}Ng \longrightarrow N$$

$$g^{-1}ng \longmapsto n$$

$$\varphi(g^{-1}ng) = \varphi(g^{-1}yg) \implies n = y$$

$|Ha| = |Hb| \qquad \varphi : Ha \longrightarrow Hb \qquad$ 1.1 ، پوشا

تذکر: با توجه به تعریف بالا N زیرگروه نرمال است ، اگر و تنها اگر همدسته‌های چپ و راست باهم برابر باشند

یعنی به ازای هر $g \in G \longleftarrow Ng = gN$

تعریف: (گروه خارج قسمتی)

فرض کنید G یک گروه و N زیرگروه نرمال آن $\{Ng \mid g \in G\}$ عمل زیر را روی این مجموعه تعریف می‌کنیم

هم همدسته‌ها اینجا هم راست هم چپ

$$Ng_1 Ng_2 = Ng_1g_2$$

a b

$$n_1g_1\, n_2g_2 = n_1g_1n_2g_2 = \underbrace{n_1}_{\in N}\overbrace{\underbrace{g_1n_2g_1^{-1}}_{\in N}}^{\in N}g_1g_2 = Ng_1g_2$$

• لازم به توضیح است خوش تعریفی عمل فوق به نرمال بودن N ربط دارد.

مجموعه تعریف شدهٔ بالا را باعلامت $\{Ng \mid g \in G\} = \frac{G}{N}$ نشان می‌دهیم.

گروه $\frac{G}{N}$ باعمل تعریف شده بالا را ، گروه خارج قسمتی گوئیم.

$$Ng_1Ng_2 = Ng_1g_2$$

نکات زیر را از تعریف گروه خارج قسمتی بدست می آوریم:

متناهی

۱- $\left|\frac{G}{N}\right| = |G:N| = \frac{|G|}{|N|}$

۲- اگر گروه G آبلی باشد آنگاه هر زیرگروه آن نرمال است.

$N \leqslant G$ $\quad Ng = gN$ $\quad ng = gn$

۳- اگر گروه G دوری باشد آنگاه هر خارج قسمتی آن دوری است.

حل ۳:

$G = \langle a \rangle \quad H \leqslant G \quad \frac{G}{H} = \{Hg \mid g\in G\} = \{Ha^i \mid i \in \mathbb{Z}\}$

$$g\in G = \langle a \rangle \longrightarrow g = a^i = \{Ha^0, Ha^{\pm 1}, Ha^{\pm 2}, \dots\} = \langle Ha \rangle$$

$(Ha)^1 = Ha$

$(Ha)^2 = HaHa = Ha^2$

$(Ha)^3 = Ha^3$

۴- اگر N زیرگروه نرمال باشد می توانیم گروه $\frac{G}{N}$ را تشکیل دهیم و اعضای این گروه به صورت Ng می باشد

$NNa = Na$

$e = N$ اولین مجموعه عضوهای $\frac{G}{O}$ مفروض

$(Na)^{-1} = Na^{-1}$ معکوس اینجوری ساخته می شود

$NaNa^{-1} = N$

مثال: می دانیم $\mathbb{Z}$ یک گروه آبلی است و $7\mathbb{Z}$ زیرگروه است، بنابراین زیرگروه نرمال می شود و می دانیم گروه خارج قسمتی $\frac{\mathbb{Z}}{7\mathbb{Z}}$ را تشکیل می دهیم

$$\frac{\mathbb{Z}}{7\mathbb{Z}} = \{\overset{e}{7\mathbb{Z}}, \overset{a_1}{7\mathbb{Z}+1}, \overset{a_2}{7\mathbb{Z}+2}, \overset{a_3}{7\mathbb{Z}+3}, \overset{a_4}{7\mathbb{Z}+4}, \overset{a_5}{7\mathbb{Z}+5}, \overset{a_6}{7\mathbb{Z}+6}\}$$

$$(7\mathbb{Z}+2)^{-1} = 7\mathbb{Z} - 2$$

$$\underbrace{7\mathbb{Z}}_{e} + \underbrace{(7\mathbb{Z}+3)}_{a_3} = \underbrace{7\mathbb{Z}+3}_{a_3}$$

تذکر: اگر N زیرگروه نرمال باشد آن را با علامت $N \trianglelefteq G$ نشان می‌دهیم. General linear group

مثال: فرض کنید همه ماتریس های $n\times n$ و معکوس پذیر روی $\mathbb{R}$ را با علامت $Gl(n,\mathbb{R})$ نشان می‌دهیم. همچنین $Sl(n,\mathbb{R})$ را به صورت زیر تعریف می‌کنیم: $Sl(n,\mathbb{R}) = \{A\in Gl(n,\mathbb{R}) \mid \det A = 1\}$

در این صورت $Sl(n,\mathbb{R})$ زیرگروه نرمال $Gl(n,\mathbb{R})$ است.

$Sl(n,\mathbb{R}) \trianglelefteq Gl(n,\mathbb{R})$

مثال از Sl

$\begin{pmatrix} 2 & & & \\ & \frac{1}{2} & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$

$\begin{pmatrix} a & & & \\ & a^{-1} & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$

$A, B \in Sl(n,\mathbb{R})$

$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \underbrace{\det A}_{1}(\underbrace{\det B}_{1})^{-1} = 1$

$AB^{-1}\in Sl(n,\mathbb{R})$ اثبات زیرگروه بودن

$B\in Gl(n,\mathbb{R})$ $\qquad B^{-1}AB\in Sl(n,\mathbb{R})$

$A\in Sl(n,\mathbb{R})$ $\qquad \longrightarrow Sl(n,\mathbb{R}) \trianglelefteq Gl(n,\mathbb{R})$

$\det(B^{-1}AB) = (\det B)^{-1}\det A \det B = 1$ اثبات نرمال بودن

یادآوری:

$N \trianglelefteq G$

کاربردی ترین رابطه

$\forall g\in G\ \forall n\in N\quad g^{-1}ng\in N \iff g^{-1}Ng = N \iff Ng = gN$

$N \trianglelefteq G \longrightarrow \frac{G}{N}$

$\frac{G}{N} = \{Ng \mid g\in G\}$ $\qquad Ng_1 Ng_2 = Ng_1g_2$

نرمال بودن باعث خوش تعریفی می‌شود

با عمل بالا $\frac{G}{N}$ تشکیل گروه می‌دهد که به آن گروه خارج قسمتی می‌گوییم.

تعریف: (مرکز گروه) Center of group

فرض کنید G یک گروه باشد. مرکز گروه را با علامت $Z(G)$ نشان می‌دهیم، که به صورت زیر تعریف می‌شود:

$Z(G)=\{x\in G \mid \forall y\in G \quad xy=yx\}$ = اعضایی که با کل اعضای گروه جابه‌جا شوند

واضح است $e\in Z(G)$ $\quad (\forall y\in G \quad ey=ye)$

لذا $Z(G)\neq\phi$

قضیه: اگر G یک گروه باشد $Z(G)\trianglelefteq G$ (زیرگروه نرمال)

برهان: اول ثابت می‌کنیم $Z(G)$ زیرگروه است.

فرض کنید $a,b\in Z(G)$ نشان می‌دهیم: $ab^{-1}\in Z(G)$

دلخواه

$y\in G\ ,\ b\in Z(G) \longrightarrow by=yb \xrightarrow[b^{-1}\text{ ضرب کرده}]{\text{طرفین از چپ در}} y=b^{-1}yb \xrightarrow[b^{-1}\text{ ضرب کرده}]{\text{طرفین را از راست در}} yb^{-1}=b^{-1}y$

لذا $b^{-1}\in Z(G)$

چون b^{-1} توی مرکز افتاده جابه‌جا می‌شوند — a در مرکز گروه پس جابه‌جا می‌شود

$ab^{-1}y=a(b^{-1}y)=ayb^{-1}=(ay)b^{-1}=yab^{-1}$

پس $ab^{-1}\in Z(G)$ لذا $Z(G)\leqslant G$ است

حال ثابت می‌کنیم $Z(G)\trianglelefteq G$

$g\in G\ ,\ x\in Z(G)$

x جابه‌جا شده چون توی مرکز

$g^{-1}xg=\underbrace{g^{-1}g}_{e}x=x$

الان ثابت کردیم $\longrightarrow$ $\forall g\in G,\ \forall x\in Z(G) \quad g^{-1}xg=x\in Z(G)$

پس $Z(G)\trianglelefteq G$

واسه اثبات نرمال بودن می‌توانستیم از همدسته‌ها نیز استفاده کنیم

$Z(G)g=gZ(G)$

همدسته راست = همدسته چپ

مثال: $\mathcal{M}_n(\mathbb{R})$ (ماتریس های nxn با درایه‌های $\mathbb{R}$)

$$\lambda I = \begin{bmatrix} \lambda & & \\ & \lambda & \\ & & \ddots \lambda \end{bmatrix} \qquad \lambda \in \mathbb{R}$$

$$(\lambda I)A = \lambda(IA) = A(\lambda I)$$

$$Z(\mathcal{M}_n(\mathbb{R})) = \{\lambda I \mid \lambda \in \mathbb{R}\}$$

تمرین: اگر G یک گروه باشد، $H \leqslant Z(G)$ در این صورت $H \trianglelefteq G$ (مهم)

یعنی اعضای H همه چیز جابجا می‌شوند

$\in H \leqslant Z(G)$

$$g^{-1}hg = \underbrace{g^{-1}g}_{e}h = h \in H$$

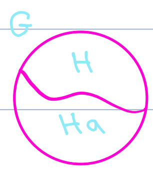
$$\forall g \in G,\ \forall h \in H \longrightarrow g^{-1}hg = g^{-1}gh = h \longrightarrow h \in H \Rightarrow g^{-1}hg \in H \Rightarrow \underline{H \trianglelefteq G}$$

$h \in Z(G)$ ← چون

نکته: اگر $N \trianglelefteq G$ باشد می دانیم $|G:N| =$ تعداد همدسته ها $= \left|\frac{G}{N}\right|$

قضیه: فرض کنیم $H \leqslant G$ به طوری که $|G:H| = 2$ در این صورت $H \trianglelefteq G$.

منظور سوال ← اگر ۲ تا همدسته بود حتما نرمال است



حل: $H = He, Ha$ دو همدسته هست که $a \notin H$ (اگر عضوش باشد جذبش میشه)

برای اینکه بگیم نرمال ← همدسته چپ = همدسته راست

چون همدسته ها افراز ایجاد می کنند پس $aH \cap H = \emptyset$

(در غیر این صورت اگر $aH \cap H \neq \emptyset$ باشد داریم $aH = H$)

$a \in aH, \quad a \notin H$

$\downarrow$

$a = a \times e$

aH

$\hookrightarrow aH \cap H = \emptyset \Rightarrow aH = Ha$

چون افراز $aH \cap H = \emptyset$

$aH \neq H \longleftarrow aH, H$

$\hookrightarrow aH = G - H$

$Ha \cap H = \emptyset$

$Ha \neq H \longleftarrow Ha, H$

$Ha = G - H$

$\hookrightarrow Ha = aH$

یادآوری: اگر $H, K \leqslant G$ باشد آنگاه $HK \leqslant G \iff HK = KH$

نکته: فرض کنیم G یک گروه، $H \trianglelefteq G$ ، $K \leqslant G$ در این صورت $HK \leqslant G$

حل:

$hk \in HK \xrightarrow{\text{حکم}} hk \in KH$

$H \trianglelefteq G$

$$hk = \underbrace{k}_{\in K}\underbrace{k^{-1}hk}_{\in H \trianglelefteq G} \in kh \implies HK \subseteq KH$$

برعکس به مشابه حل می‌شود پس $HK = KH$ لذا $HK \leqslant G$

تمرین: فرض کنیم G یک گروه، $H \trianglelefteq G$ ، $K \trianglelefteq G$. نشان دهید $HK \trianglelefteq G$.

حل:

$g^{-1}hkg \overset{?}{\in} HK$

$$\underbrace{g^{-1}hg}_{\in H}\,\underbrace{g^{-1}kg}_{\in K} \in HK$$

تعریف (همریختی) Homomorphism

فرض کنیم $(G_1, *_1)$ و $(G_2, *_2)$ دو گروه باشند $f: G_1 \to G_2$ را همریختی گوئیم $f(a *_1 b) = f(a) *_2 f(b)$

تابع f را همریختی گوئیم هرگاه حافظ عمل باشد

کل همریختی‌های از G_1 به G_2 را با علامت $\mathrm{Hom}(G_1, G_2)$ نشان می دهیم.

مثال: تابع $\phi: G \to G$, $x \mapsto e$ یک همریختی است.

$$\left.\begin{aligned} \phi(xy) &= e \\ \underbrace{\phi(x)}_{e}\underbrace{\phi(y)}_{e} &= e \end{aligned}\right\} \longrightarrow \phi(xy) = \phi(x)\phi(y)$$

مثال: تابع $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $x \mapsto 2x$ یک همریختی است.

$$\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$$

همریختی:

تابع $f: G_1 \longrightarrow G_2$

$G_1 \to *_1$ ، $G_2 \to *_2$

$\forall a,b \in G_1 \qquad f(a *_1 b) = f(a) *_2 f(b)$

اگر مشکلی نباشد هر دو عمل را ضرب می‌گیریم.

$f: G_1 \longrightarrow G_2$

$f(ab) = f(a)f(b)$

ضرب داخل G_1 ، ضرب داخل G_2

مثال: $\phi: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +_n)$ ، ϕ یک همریختی است.

$x \longmapsto \bar{x}$ (باقی‌مانده x بر n)

$\phi(x+y) = \overline{x+y} = \bar{x} \oplus_n \bar{y} = \phi(x) +_n \phi(y)$

$n=11 \quad , \quad x=9$

$y=4 \longrightarrow \overline{9+4} = 2 \qquad , \qquad \bar{9} +_n \bar{4} = 9 +_n 4 = 2$

$y=13 \longrightarrow \overline{9+13} = 0 \qquad , \qquad 9 +_n 2 = 0$

$\overline{x+y} = \bar{x} +_n \bar{y}$

مثال: $\phi: Gl(n, \mathbb{R}) \longrightarrow (\mathbb{R}^*, \cdot)$ ، ϕ یک همریختی و پوشا است.

ماتریس های $n \times n$ معکوس پذیر ، $\mathbb{R}^* = \mathbb{R} - \{0\}$ ، ضرب اعداد حقیقی

$A \longmapsto \det A \quad (A \in Gl \longrightarrow \det A \neq 0)$

ضرب ماتریس

$\phi(AB) = \det(AB) = \det(A)\det(B) = (\det A)(\det B) = \phi(A)\phi(B)$

پوشا بودن ϕ: فرض کنیم $a \in \mathbb{R}^*$ ، نشان می‌دهیم ماتریس مانند A عضو $Gl(n,\mathbb{R})$ هست به طوری که

$\phi(A) = a$

$$A = \begin{bmatrix} a & & 0 \\ & 1 & \\ 0 & & \ddots \; 1 \end{bmatrix}$$

$\det A = a \neq 0 \longrightarrow A \in Gl(n,\mathbb{R}) \;,\; \phi(A) = \det A = a$

مثال مهم: فرض کنیم G یک گروه و $N \trianglelefteq G$. تابع $\gamma : G \longrightarrow \boxed{\frac{G}{N}}$ در این صورت γ همریختی پوشا است.

$g \longmapsto Ng$ این همریختی را همریختی کانونی گویند.

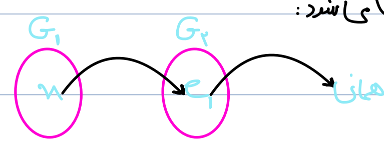
$$\gamma(g_1 g_2) = N g_1 g_2 = N g_1 N g_2 = \gamma(g_1)\gamma(g_2)$$

پوشا بودن γ: فرض کنیم $Ng \in \frac{G}{N}$ (دلخواه) واضح است $g \in G$, $\gamma(g) = Ng$

تعریف: (هسته عمل) kernel

فرض کنیم $\overset{e_1}{G_1} \xrightarrow{\phi} \overset{e_2}{G_2}$ ، $\phi : G_1 \to G_2$ همریختی باشد. هسته عمل ϕ را با علامت $Ker(\phi)$ نشان می‌دهیم به صورت زیر تعریف می‌شود:

$$Ker(\phi) = \{ x \in G_1 \mid \phi(x) = e_2 \} \neq \emptyset$$



توجه شود

همانی G_1

$$\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)\phi(e_1) \longrightarrow \cancel{\phi(e_1)} = \cancel{\phi(e_1)}\phi(e_1) \xrightarrow[\text{حذف}]{\text{قانون}} \boxed{e_2 = \phi(e_1)}$$

همریختی همانی را به همانی می‌برد

$۲x = ۲ \longrightarrow x = ۱$

$$e_1 \in Ker\phi \longrightarrow Ker\phi \neq \emptyset$$

ثابت می‌کنیم $\boxed{Ker\phi \trianglelefteq G_1}$

زیرگروه بودن:

$$a, b \in Ker\phi \overset{?}{\longleftrightarrow} ab^{-1} \in Ker\phi \overset{?}{\longleftrightarrow} \phi(ab^{-1}) = e_2$$

$$b \in Ker\phi \longrightarrow \phi(b) = e_2$$

$$e_2 = \phi(e_1) = \phi(bb^{-1}) = \phi(b)\phi(b^{-1}) \longrightarrow e_2 = \phi(b^{-1})$$

$$\phi(ab^{-1}) = \overset{e_2}{\overline{\phi(a)}}\,\overset{e_2}{\overline{\phi(b^{-1})}} = e_2 \longrightarrow ab^{-1} \in Ker\phi \xrightarrow{\text{یعنی}} Ker\phi \leqslant G$$

نرمال بودن:

$$\forall g \in G, \forall a \in Ker\phi \xrightarrow{\text{حکم؟}} g^{-1}ag \in Ker\phi$$

$$\phi(g^{-1}ag) = \phi(g^{-1})\underbrace{\phi(a)}_{e_2}\phi(g) = \phi(g^{-1})\phi(g) = \phi(\underbrace{gg^{-1}}_{e_1}) = e_2$$

$$\longrightarrow g^{-1}ag \in Ker\phi \longrightarrow Ker\phi \trianglelefteq G$$

نکات زیر را داریم:

لم: فرض کنیم $\phi: G_1 \to G_2$ یک همریختی باشد در این صورت:

۱- $\phi(e_1) = e_2$ (بالا اثبات کردیم)

۲- $Ker\,\phi \trianglelefteq G$ (بالا اثبات کردیم)

۳- $\phi(x^n) = (\phi(x))^n$

برهان: $\phi(x^2) = \phi(xx) = \phi(x)\phi(x) = \phi(x)^2$

$$\phi(x^3) = \phi(x^2x) = \phi(x^2)\phi(x) = \phi(x)^2\phi(x) = \phi(x)^3$$

$\vdots$

استقرا $\longrightarrow \phi(x^n) = \phi(x)^n$

۴- $\phi(a^{-1}) = (\phi(a))^{-1}$

برهان: $e_2 = \phi(e_1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$

$$e_2 = \phi(a)\phi(a^{-1}) \longrightarrow (\phi(a))^{-1}\underbrace{e_2}_{\text{های}} = \phi(a^{-1}) \longrightarrow (\phi(a))^{-1} = \phi(a^{-1})$$

در معکوس

مثال: $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$، می دانیم ϕ یک همریختی است. هسته این همریختی را محاسبه کنید.

عضو همانی ۰   عضو همانی ۰

$x \mapsto 2x$

$$x \in Ker\,\phi \longrightarrow \phi(x) = 0 \longrightarrow 2x = 0 \longrightarrow x = 0 \longrightarrow Ker\,\phi = \{0\}$$

مثال: $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}_n, +_n)$، می دانیم ϕ همریختی پوشا است. هسته این همریختی را محاسبه کنید.

عضو همانی ۰   عضو همانی ۰

$x \mapsto \bar{x}$

باقیمانده بر n

$$x \in Ker\,\phi \longrightarrow \phi(x) = 0 \longrightarrow \bar{x} = 0 \longrightarrow x \in n\mathbb{Z}$$

$$\longrightarrow Ker\,\phi = n\mathbb{Z}$$

مثال: $\phi : Gl(n,\mathbb{R}) \longrightarrow (\mathbb{R}^*, .)$ همانی! ، می دانیم ϕ همریختی پوشا است. هسته این همریختی را محاسبه کنید.

$$A \longmapsto \det A$$

$$A \in Ker\phi \longrightarrow \phi(A) = 1 \longrightarrow \det A = 1 \Longrightarrow Ker\phi = Sl(n,\mathbb{R})$$

$A \in Sl$

$Sl(n,\mathbb{R}) = \{A \in Gl \mid \det A = 1\}$

مثال دوم: همریختی کانونی

تابع $\gamma : G \longrightarrow \frac{G}{N}$ ، می دانیم γ یک همریختی پوشا است. هسته این همریختی را محاسبه کنید.

عضوهای N

$$g \longmapsto Ng$$

$g \in Ker\gamma \longrightarrow \gamma(g) = \frac{G}{N}$ همانی $\longrightarrow Ng = N \longrightarrow g \in N$

اعضای در هسته است که داخل N باشد $\longleftarrow$ $Ker\gamma = N$

یادآوری:

فرض کنید $H \leqslant G$

$$a \sim b \iff ab^{-1} \in H$$

$$Ha = Hb \iff ab^{-1} \in H$$

دو همدسته یا باهم برابر است یا دو تهی اند

$$Ha = Hb \overset{\sim}{\iff} ab^{-1} \in H$$

$$Ha = H = He \longrightarrow ae^{-1} \in H \longrightarrow a \in H$$

همدسته

سپس $\longrightarrow Ha = H \longrightarrow a \in H$

قضیه: فرض کنیم $\phi : G_1 \longrightarrow G_2$ یک همریختی باشد. در این صورت ϕ 1-1 است اگر و تنها اگر $Ker\phi = \{e_1\}$

برهان:

← فرض یک به یک، $x \in Ker\phi$

$$\left.\begin{array}{l}\phi(x) = e_2 \\ \phi(e_1) = e_2\end{array}\right\} \longrightarrow \phi(x) = \phi(e_1) \xrightarrow{1-1} x = e_1 \longrightarrow Ker\phi = \{e_1\}$$

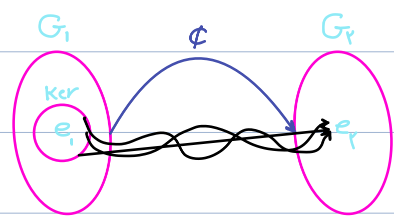
→ فرض کنیم $Ker\phi = \{e_1\}$ ، نشان دهید ϕ یک به یک است. فرض کنیم:

$$\phi(x) = \phi(y) \longrightarrow \phi(x)(\phi(y))^{-1} = e_2 \longrightarrow \phi(x)\,\phi(y^{-1}) = e_2 \longrightarrow \phi(xy^{-1}) = e_2$$

پس $xy^{-1} \in Ker\phi$ اما $Ker\phi = \{e_1\}$

پس $xy^{-1} = e_1$ پس $x = y$ ← ϕ یک به یک است

خلاصه:



تعریف: (یکریختی) Isomorphism

فرض کنید $\phi : G_1 \to G_2$ یک همریختی یک به یک و پوشا باشد در این صورت ϕ را یک ایزومورفیسم (یکریختی) گویند $G_1 \cong G_2$

یادآوری:

تابع $\phi : G_1 \to G_2$ (با عمل $*_1$ روی G_1 و $*_2$ روی G_2)

همریختی $\longrightarrow$ $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$

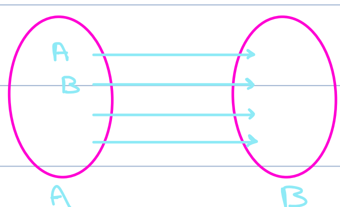
راحتی

$$\phi(ab) = \phi(a)\phi(b)$$

تعریف: یکریختی (Isomorphism)

همریختی $\phi : G_1 \to G_2$ را یکریختی هستند درصورتی که 1-1 و پوشا باشد

می نویسیم G_1 با G_2 یکریخت است و $G_1 \cong G_2$



• $\phi : \mathbb{Z}, + \longrightarrow$ ماتریس ۲x۲

$a \longmapsto \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ $\longrightarrow$ ۲+۳ $\longrightarrow$ ۵

$$\begin{bmatrix} ۲ & ۰ \\ ۰ & ۲ \end{bmatrix} + \begin{bmatrix} ۳ & ۰ \\ ۰ & ۳ \end{bmatrix} = \begin{bmatrix} ۵ & ۰ \\ ۰ & ۵ \end{bmatrix}$$

عدد مختلط

• $\mathbb{R}^2 \times (0,0) \cong \mathbb{R}^2 \cong \mathbb{C}$ $\quad a+bi$

ابسا

a, bi را میبره به زوج مرتب (a, bi)

مثال: نشان دهید $(\mathbb{R},+) \cong (\mathbb{R}^+,\cdot)$ یک به یک است

$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$

$\psi : (\mathbb{R},+) \longrightarrow (\mathbb{R}^+,\cdot)$

$x \longmapsto e^x$ (نمایی + و منفی نمی‌شد)

همریختی:

$\psi(a+b) = e^{a+b} = e^a e^b = \psi(a)\psi(b)$

یک به یک بودن ψ:

راه اول $\psi(a) = \psi(b) \longrightarrow e^a = e^b \longrightarrow a = b$

راه دوم $a \in \ker\psi \longrightarrow \psi(a) = 1 \longrightarrow e^a = 1 \longrightarrow a = 0$

پس $\ker\psi = \{0\}$

پوشا بودن ψ:

$y \in \mathbb{R}^+ \longrightarrow a = \ln y$

$\psi(a) = e^a = e^{\ln y} = y$

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

مثال: اگر G یک گروه باشد آن گاه:

i) اگر $|G| = n$ باشد آن گاه $G \cong \mathbb{Z}_n$

ii) اگر $|G| = \infty$ باشد آن گاه $G \cong \mathbb{Z}$

حل i: فرض کنیم $G = \langle a \rangle$ ، $|a| = n$ $(G = \{1, a, a^2, \dots, a^{n-1}\})$

$\varphi : \mathbb{Z}_n \longrightarrow G$

$i \longmapsto a^i$

پوشا بودن واضح است

همریختی بودن:

$\varphi(i +_n j) = a^{i +_n j} = a^i a^j = \varphi(i)\varphi(j)$

یک به یک بودن:

$i \in \ker\varphi \longrightarrow \varphi(i) = 1 \longrightarrow a^i = 1$

پس $o(a) | i$ لذا $n | i$ پس $i = 0$

لذا $\ker\varphi = \{0\}$ پس یک به یک است

لذا $G \cong \mathbb{Z}_n$

حل ii: $G = \{1, a^1, a^2, \dots, a^{-1}, a^{-2}, \dots\}$

$\varphi : \mathbb{Z} \longrightarrow G$

$i \longmapsto a^i$

مثل قسمت i بالا حل می شود

مسأله: $\phi : G_1 \longrightarrow G_2$ یک همریختی و $a \in G_1$ ثابت کنید $o(\phi(a)) \mid o(a)$

واسه عاد کردن همیشه همین کار را باید کرد

حل: $o(a) = m \ , \ o(\phi(n)) = n$

$a^m = e_1 \longrightarrow \phi(a^m) = \phi(e_1) = e_2$

$\phi(a^m) = e_2 \longrightarrow \phi(a)^m = e_2$

$o(\phi(a)) \mid m \longrightarrow \underline{\underline{n \mid m}}$

مسأله: اگر $\phi : G_1 \rightarrow G_2$ یک همریختی یک به یک باشد آنگاه $o(\phi(a)) = o(a)$

حل: $o(a) = m \ , \ o(\phi(a)) = n$

داریم $n \mid m$ از بالا

$o(\phi(a)) = n \longrightarrow (\phi(a))^n = e_1 \longrightarrow \phi(a^n) = e_2$

پس $a^n \in \ker\phi$ ، ϕ یک به یک است پس $a^n = e_1$ پس $m \mid n$

درنتیجه $\underline{\underline{m = n}}$

نکته: فرض کنید G_1 و G_2 دو گروه همریختی باشند در این صورت خواص زیر تحت یکریختی حفظ می شوند

۱- متناهی بودن

۲- آبلی بودن

۳- دوری بودن

۴- تعداد جواب معادله

۵- داشتن عضو از مرتبه n

حل ۲:

آبلی

$$G_1 \cong G_2$$

$$\psi : G_1 \xrightarrow[\text{متناهی}]{\text{پوشا}} G_2$$

$$b_1 , b_2 \in G_2$$

پوشا

$$\phi(a_1) \qquad \phi(a_2)$$

آبلی بودن

پوشا بودن

$$b_1 b_2 = \phi(a_1)\phi(a_2) = \phi(a_1 a_2) = \phi(a_2 a_1) = \phi(a_2)\phi(a_1) = b_2 b_1$$

مثال: نشان دهید

$$\underbrace{(\mathbb{Z},+)}_{\text{دوری}} \not\cong \underbrace{(\mathbb{Q},+)}_{\text{غیردوری}}$$

$$\underbrace{(\mathbb{Q}^*,\cdot)}_{x^2=2\ \text{حل ناپذیر}} \not\cong \underbrace{(\mathbb{R}^*,\cdot)}_{x^2=2\ \text{حل پذیر است}}$$

$$(\mathbb{R}^*,\cdot) \not\cong (\mathbb{R},+)$$

$(-1)^2=1$ — $2x=0$

$o(-1)=2$ — $x=0$

یعنی یک عضو از مرتبه ۲ دارد. — $o(a)=1$

$$\underbrace{(\mathbb{C},\cdot)}_{x^2=-1\ \text{حل پذیر}} \not\cong \underbrace{(\mathbb{R},\cdot)}_{x^2=-1\ \text{حل ناپذیر}}$$

$$(\mathbb{Z},+) \cong (2\mathbb{Z},+)$$

حل کنید $(\mathbb{Z},+) \cong (n\mathbb{Z},+)$

$\varphi : (\mathbb{Z},+) \longrightarrow (2\mathbb{Z},+)$

۱-۱ و پوشا $\quad x \mapsto 2x$

تعریف : (مرکز گروه) Center of group

فرض کنید G یک گروه باشد. مرکز گروه را با علامت $Z(G)$ نشان می‌دهیم که به صورت زیر تعریف می‌شود:

$$Z(G) = \{g\in G \mid \forall y\in G \quad gy = yg\}$$ = اعضایی که با کل اعضای گروه جابه‌جا می‌شوند

واضح است $e\in Z(G)$ $\quad (\forall y\in G \quad ey = ye)$

لذا $Z(G)\neq\phi$

مثال: $Z(S_3) = ?$

$$f_1: \begin{array}{l} 1\to 1 \\ 2\to 2 \\ 3\to 3 \end{array} \qquad f_3: \begin{array}{l} 1\to 2 \\ 2\to 1 \\ 3\to 3 \end{array} \qquad f_5: \begin{array}{l} 1\to 3 \\ 2\to 1 \\ 3\to 2 \end{array}$$

$$f_2: \begin{array}{l} 1\to 1 \\ 2\to 3 \\ 3\to 2 \end{array} \qquad f_4: \begin{array}{l} 1\to 2 \\ 2\to 3 \\ 3\to 1 \end{array} \qquad f_6: \begin{array}{l} 1\to 3 \\ 2\to 2 \\ 3\to 1 \end{array}$$

$$Z(G) = f_1$$

$$f_2f_6 \left| \begin{array}{l} 1\to 2 \\ 2\to 3 \\ 3\to 1 \end{array} \right. \qquad f_3f_5 \left| \begin{array}{l} 1\to 3 \\ 2\to 2 \\ 3\to 1 \end{array} \right. \qquad f_3f_5 \neq f_5f_3$$

$$f_6f_2 \left| \begin{array}{l} 1\to 3 \\ 2\to 1 \\ 3\to 2 \end{array} \right. \qquad f_2f_6 \neq f_6f_2 \qquad f_2, f_6 \notin Z(S_3) \qquad f_5f_3 \left| \begin{array}{l} 1\to 1 \\ 2\to 3 \\ 3\to 2 \end{array} \right. \qquad f_3, f_5 \notin Z(S_3)$$

مثال: مرکز ماتریس های $n\times n$ بی نهایت عضو دارد که برخی از اعضای آن ماتریس های اسکالر هستند.

برخی λI

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \ddots \end{pmatrix}$$

قضایای ایزومرفیسم:

قضیه اول:

فرض کنید $f: G_1 \to G_2$ یک همریختی باشد در این صورت $\frac{G_1}{\ker f} \cong Im(f)$

$\frac{G}{N} = \{Nn \mid n \in G\}$. $\ker f = \{n \in G_1 \mid f(n) = e_2\}$. $Im(f) = \{f(n) \mid n \in G_1\}$.

$NnNy = Nny$

برهان: برای راحتی $\ker f = K$ می‌گیریم، $\psi: \frac{G_1}{K} \to Im(f)$

$Kg \longmapsto f(g)$

اول ثابت می‌کنیم ψ خوش تعریف است

$Kg_1 = Kg_2 \longrightarrow g_1 g_2^{-1} \in K \longrightarrow f(g_1 g_2^{-1}) = e \xrightarrow{\text{همریختی}} f(g_1) f(g_2^{-1}) = e$

$f(g_1) = f(g_2) \longleftarrow f(g_1) f(g_2)^{-1} = e \longleftarrow$

ψ همریختی است

$\psi(Kg_1 Kg_2) = \psi(Kg_1 g_2) \longrightarrow f(g_1 g_2) = f(g_1) f(g_2) = \psi(Kg_1)\psi(Kg_2)$

ψ پوشا است

$y \in Im f$ پس $y = f(g)$

$y = f(g) = \psi(Kg)$

چون روابط تابع بودن برگشت پذیر است لذا یک به یک است

مثال: $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

$f: \overset{G_1}{\mathbb{Z}} \longrightarrow \overset{G_2}{\mathbb{Z}_n}$

$n \longmapsto \bar{n} \longrightarrow$ باقی‌مانده n بر n

f همریختی است و f پوشاست.

$\ker f = \{n \in \mathbb{Z} \mid \bar{n} = 0\} = n\mathbb{Z}$

$\xrightarrow[\text{اول تکریختی}]{\text{طبق قضیه}} \dfrac{\mathbb{Z}}{\text{هسته}} \cong \operatorname{Im} f \quad \Rightarrow \quad \dfrac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

مثال: $\dfrac{Gl(n,\mathbb{R})}{Sl(n,\mathbb{R})} \cong \mathbb{R}^*$

$\mathbb{R}^* = \mathbb{R} - \{0\}$

$f: \overset{G_1}{\overbrace{Gl(n,\mathbb{R})}} \longrightarrow \overset{G_2}{\overbrace{\mathbb{R}^*}}$

$A \longmapsto \det A$

$f(AB) = \det AB = \det A \cdot \det B = f(A)f(B)$ f همریختی است.

$\ker f = \{A \in Gl(n,\mathbb{R}) \mid \det A = 1\} = Sl(n,\mathbb{R})$

f پوشاست

$$\begin{pmatrix} \sqrt{2} & & 0 \\ & 1 & \\ 0 & & \ddots \ 1 \end{pmatrix}$$

طبق قضیه اول $\Rightarrow \dfrac{Gl(n,\mathbb{R})}{\text{هسته}} \cong \operatorname{Im} f$

$\longrightarrow \dfrac{Gl(n,\mathbb{R})}{Sl(n,\mathbb{R})} \cong \mathbb{R}^*$

قضیه دوم:

فرض کنیم G یک گروه و $H,K \leq G$, $H \trianglelefteq G$ در این صورت $\frac{HK}{H} \cong \frac{K}{H\cap K}$

(اگر H زیرگروه نرمال باشد $\Leftarrow$ HK زیرگروه)

برای اثبات تابعی از HK به $\frac{K}{H\cap K}$

مثال: $\frac{\overset{K}{2\mathbb{Z}}\,\overset{H}{3\mathbb{Z}}}{\underset{H}{3\mathbb{Z}}} \cong \frac{2\mathbb{Z}}{2\mathbb{Z}\cap 3\mathbb{Z}} = \frac{2\mathbb{Z}}{6\mathbb{Z}}$

$$\boxed{\frac{m\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_{\frac{n}{m}}}$$

$\frac{G}{N} = \{Ng \mid g\in G\}$

$\frac{2\mathbb{Z}}{6\mathbb{Z}} = 6\mathbb{Z}+0 \ , \ 6\mathbb{Z}+2 \ , \ 6\mathbb{Z}+4 \ , \ 6\mathbb{Z}+6 \ , \ 6\mathbb{Z}+8 \ , \ 6\mathbb{Z}+10$ $\quad \underline{\mathbb{Z}_3}$

تذکر مهم: فرض کنید $N \trianglelefteq G$ در این صورت زیرگروه های $\frac{G}{N}$ به صورت $\frac{H}{N}$ که $N \leq H \leq G$.

مثال: تعداد زیرگروه های $\mathbb{Z}_6$ را بیان کنید.

$\mathbb{Z}_6 \cong \frac{\mathbb{Z}}{6\mathbb{Z}}$

کافی است زیرگروه های $\frac{\mathbb{Z}}{6\mathbb{Z}}$ را بررسی کنید

$\frac{H}{6\mathbb{Z}} \leq \frac{\mathbb{Z}}{6\mathbb{Z}} \xrightarrow{\text{۲ شرط مهم}} H \leq \mathbb{Z}$

$6\mathbb{Z} \leq H \leq \mathbb{Z} \longrightarrow \# \frac{H}{\mathbb{Z}} = 4$

$H = 6\mathbb{Z} \qquad H = 2\mathbb{Z}$

$H = 3\mathbb{Z} \qquad H = \mathbb{Z}$

مقسوم علیه ۶ $= \{1,2,3,6\}$

نکته: زیرگروه های $\mathbb{Z}$ که به شامل $n\mathbb{Z}$ می باشند به صورت $d\mathbb{Z}$ که $d \mid n$.

بنابراین تعداد آن ها برابر با تعداد مقسوم علیه های n است.

فرض کنید n تجزیه‌ای به صورت $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ باشد آن گاه تعداد مقسوم علیه های آن برابر با $(\alpha_1+1) \cdots (\alpha_t+1)$ است.

مثال: تعداد زیرگروه های $\mathbb{Z}$ که شامل $\mathbb{Z}_{100}$ است چند تا است؟

$100 = 2^2 \times 5^2$

تعداد مقسوم علیه $= (2+1)(2+1) = 9$

تعریف (زیرگروه ماکسیمال) Maximal Subgroup

فرض کنید G یک گروه باشد. زیرگروه M را زیرگروه ماکسیمال گوئیم درصورتی که بین M، گروه، زیرگروه واقعی وجود نداشته باشد.

$M \leqslant H \leqslant G \longrightarrow M = H$ یا $H = G$

مثال: $5\mathbb{Z}$ یک زیرگروه ماکسیمال $\mathbb{Z}$ است ولی $4\mathbb{Z}$ نمی باشد.

$4\mathbb{Z} < \mathbb{Z}$

$2\mathbb{Z}, 3\mathbb{Z}$

مثال: اگر p عدد اول باشد $p\mathbb{Z}$ زیرگروه ماکسیمال است.

نکته: هر گروه متناهی حداقل یک زیرگروه ماکسیمال دارد.

تعریف (زیرگروه مشتق) Derived subgroup

فرض کنید G یک گروه باشد و $X \subseteq G$ در این صورت زیرگروه تولید شده توسط X با نماد $\langle X \rangle$

نشان می دهیم و به صورت زیر تعریف می شود:

(این چیزی که به ذهن می رسه ورد های یکسان ضربی، تمام های مثبت، توان های منفی و ترکیبات شان با جابجایی)

$$\langle X \rangle = \{ x_1^{\alpha_1} \cdots x_t^{\alpha_t} \mid x_i \in X \,,\, t \geq 0 \,,\, \alpha_i \in \{\pm 1\} \}$$

$$\hookrightarrow (1, x, x^{-1}, xy, yx, x^2, x^3, \dots, x^{-2}, x^{-3}, \dots, \dots, \dots)$$

$$xy^2x^{-1} = xyyx^{-1}$$

حالت خاص:

اگر $\langle X \rangle = \{x\}$ باشد. در این صورت گروه تولید شده توسط X همان $\langle x \rangle$ گروه دوری است.

$$\langle x \rangle = \{1, x^{\pm 1}, x^{\pm 2}, \dots\}$$

$$\left\langle \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} m & n \\ 0 & 0 \end{bmatrix} \right\}$$

$$\left\langle \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \longrightarrow$$ ماتریس های ۲×۲

با پایه یا مولد

تعریف: (جابه‌جاگر) Commutator

فرض کنید G یک گروه باشد، $a,b\in G$، جابه‌جاگر a,b را با $[a,b]$ نشان می‌دهیم:

$$[a,b]=a^{-1}b^{-1}ab$$

لذا گروه مشتق G را با علامت G' نشان می‌دهیم، به صورت زیر تعریف می‌شود:

$$G'=\langle [a,b] \mid a,b\in G\rangle$$

$$G'=\langle a\rangle$$

برنامه:

```
X := [ ]
For a in G do :
    For b in G do :
        Add(X,[a,b]);
    od;
od;
```

نکته: اگر G یک گروه آبلی باشد به ازای هر دو عضو آن مانند a,b جابه‌جاگر آن همانی است.

$[a,b]=a^{-1}b^{-1}ab$

G آبلی است $\iff G'=1$ این راسته!

G آبلی است $\iff Z(G)=G$

یادآوری:

$G = \langle x \rangle$

$G = \langle a, b \rangle$ $\quad a, b, ab, ba, aba \dots$

$a^{-1}, b^{-1}, a^{-1}b, \dots$

$G' = \langle [a,b] \mid a, b \in G \rangle$

$a^{-1}b^{-1}ab = e$

زیرگروه نرمال

قضیه: فرض کنید G یک گروه باشد و $H \trianglelefteq G$ در این صورت:

$\frac{G}{H}$ آبلی است $\iff G' \leqslant H$

برهان:

فرض کنید $a, b \in G$ نشان می‌دهیم $[a,b] \in H$

$$Ha, Hb \in \frac{G}{H} \xrightarrow{\frac{G}{H} \text{ آبلی}} HaHb = HbHa \longrightarrow Hab = Hba$$

$$\longrightarrow ab(ba)^{-1} \in H \longrightarrow aba^{-1}b^{-1} \in H \longrightarrow [a^{-1}, b^{-1}] \in H$$

کافی است a^{-1}, b^{-1} انتخاب شود

برای اثبات ← منفی بالای زیرگروه مخرج خارج قسمتی شود

$$\longrightarrow [a,b] \in H \longrightarrow G' \leqslant H$$

مثال:

- $(\mathbb{Z}_n)' = e$
- $(\mathbb{Z})' = e$
- $(S_3)' = ?$

جمع‌بندی:

- G آبلی است $\iff Z(G)=G$
- G آبلی است $\iff G'=1$
- $\frac{G}{H}$ آبلی است $\iff G' \leq H$

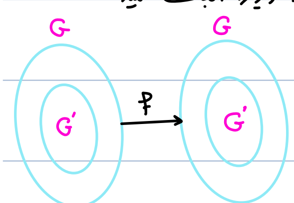
مثال: فرض کنید $f: G \longrightarrow G$ همریختی باشد، $N \trianglelefteq G$ در این صورت $f(N) \trianglelefteq f(G)$.

$x \in f(G) \quad \exists g \in G \quad s.t \quad f(g)=x$

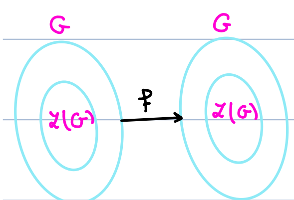
$y \in f(N) \quad \exists n \in N \quad s.t \quad f(n)=y$

$$x^{-1} y x = (f(g))^{-1} f(n) f(g) = f(g^{-1}) f(n) f(g) = f(\underbrace{g^{-1}ng}_{\in N}) \in f(N)$$

مثال مشابه: فرض کنید G یک گروه، $f: G \longrightarrow G$ همریختی پوشا باشد در این صورت موارد زیر را اثبات کنید.



۱- $f(G') \leq G'$



۲- $f(Z(G)) \leq Z(G)$

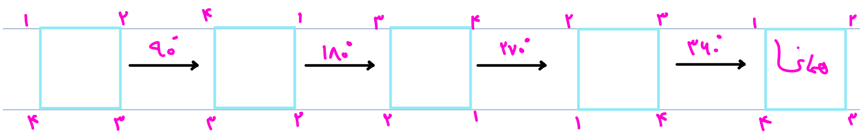
تعریف: گروه خودریختی ها (Automorphism)

فرض کنیم G یک گروه باشد گروه خودریختی های G را با علامت $Aut(G)$ نشان می دهیم و به صورت روبه رو تعریف می کنیم

$$Aut(G) = \{ f: G \longrightarrow G \mid f \text{ همریختی ۱-۱ و پوشا} \}$$

یکریختی

نکته: واضح است $Aut(G)$ با ترکیب توابع تشکیل گروه می دهد.



تعریف: خودریختی داخلی Inner Automorphism

فرض کنید G یک گروه باشد خودریختی های داخلی را با علامت $Inn(G)$ نشان می دهیم و به صورت زیر تعریف می شود:

$$Inn(G) = \{ i_g \mid g \in G \}$$

تابع

$$i_g : G \longrightarrow G$$
$$x \longmapsto g^{-1} x g$$

توجه: i_g یکریختی است.

i_g همریختی: $i_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = i_g(x)\, i_g(y)$

۱-۱: $x \in Ker\, i_g \longrightarrow i_g(x) = 1 \longrightarrow g^{-1}xg = 1 \longrightarrow x = 1 \Rightarrow Ker\, i_g = 1$

پوشا: $h \in G \quad i_g(ghg^{-1}) = g^{-1}ghg^{-1}g = h$

نکته: طبق تمرینات انجام شده: $Inn(G) \leq Aut(G)$

لم: فرض کنید ~~بدیهیه که؟!~~

۱- $Inn(G) \trianglelefteq Aut(G)$ (بدون برهان)

۲- $Inn(G) \cong \dfrac{G}{Z(G)}$

برهان ۲: $\varphi : G \longrightarrow Inn(G)$

$$g \longmapsto i_g$$

✓ پوشا ، ✓ 1-1

قضیه اول یکریختی $\dfrac{G}{Ker\,\varphi} \cong Im(G)$

$g \in Ker\,\varphi \longrightarrow \varphi(g) = i_g =$ همانی

$\forall x \in G \quad i_g(x) = x \longrightarrow g^{-1}xg = x \longrightarrow xg = gx$

$Ker\,\varphi = Z(G) \longleftarrow g \in Z(G)$

تعریف: (گروه های جایگشتی) Permutation group

هر تابع یک به یک و پوشا از $A \to A$ را یک جایگشت گویند، مجموعه تمام جایگشت‌های A را $S_{|A|}$ نشان می‌دهند.

به وضوح $S_{|A|}$ با ترکیب توابع تشکیل گروه می‌دهد آن را گروه جایگشتی متناظر با A گویند.

$f : A \to A$

$f^{-1} : A \to A$

$id : A \to A$
عضو یکه
$n \mapsto n$

حالت خاص: اگر $A = \{1, 2, \dots, n\}$ در این صورت $S_{|A|}$ را با علامت S_n نشان می‌دهند واضح است: $|S_n| = n!$

∇

$1 \longrightarrow \# n$

$2 \longrightarrow \# n-1$

$\vdots$

$n \longrightarrow \# 1$

اصل ضرب $\# \nabla = n(n-1)(n-2)\dots(2)(1) = n!$

گروه متقارن از درجه n

تذکر: اگر A مجموعه n عضوی باشد $S_{|A|} \cong S_n$

$$A = \{a_1, \dots, a_n\}$$
$$\downarrow \qquad \downarrow$$
$$1 \quad \dots \quad n$$

مثال: S_3 اولین گروه ناآبلی از مرتبهٔ ۶ است.

$|S_3| = 3! =$

ارتبه به ۲، ۲ رفته به ۱، ۳ ثابت		ارفته به ۳، ۳ رفته به ۲، ۲ رفته به ۱
id	$(1,2)$	$(1,3,2)$
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$(2,3)$	$(1,2,3)$	$(1,3)$
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

معکوس

$S_3 = \{ e, (12), (13), (23), (123), (132) \}$

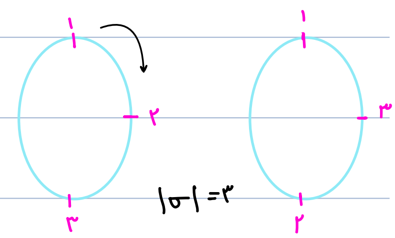
$\binom{3}{2} = 3$ معکوس ۲ تایی‌ها خودشان هستند

توی ۳ تایی‌ها بحث انتخاب نیست

ترتیب است

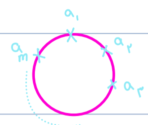
$e = \overset{f}{(123)}\overset{g}{(132)}$

$$f \circ g(1) \begin{cases} 1 \xrightarrow{g} 3 \xrightarrow{f} 1 \\ 2 \xrightarrow{g} 1 \xrightarrow{f} 2 \\ 3 \xrightarrow{g} 2 \xrightarrow{f} 3 \end{cases}$$



تعریف (دور) cycle

فرض کنید $\sigma \in S_n$ باشد و $\{a_1, a_2, \dots, a_n\} \subseteq \{1, 2, \dots, n\}$, $\sigma(a_3) = a_3$, $\sigma(a_2) = a_2$, $\sigma(a_1) = a_1$



در این صورت σ را یک دور به طول m گویند و به فرم $(a_1, \dots, a_m)$ نشان می دهند.

* با توجه به تعریف مرتبه یک دور به طول m برابر m است.

مثال: S_4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \rightarrow (1\,2\,4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \rightarrow \underbrace{(1\,4)}_{\alpha}\underbrace{(2\,3)}_{\beta} = \beta\alpha = (2\,3)(1\,4)$$

مثال:

$$\alpha\beta(1) = 4$$
$$\beta\alpha(1) = 4$$

$\rightarrow (\alpha\beta)^2 = \alpha^2\beta^2 = e$

$\rightarrow$ ک.م.م

مثال:

$$\alpha\beta(2) = 3$$
$$\beta\alpha(2) = 3$$

تعریف (دور مجزا)

فرض کنید $\sigma=(a_1,\dots,a_m)$ ، $\tau=(b_1,\dots,b_n)$ دو دور σ و τ را مجزا گوئیند در صورتی که $(a_1,\dots,a_m)\cap(b_1,\dots,b_n)=\phi$

بنابراین $order(\sigma\tau)$ میشه کوچکترین مضرب مشترک σ , τ

قضیه: (بدون اثبات)

هر جایگشت از S_n را می‌توان به حاصل ضربی از دورهای مجزا تجزیه کرد

حرفی رو انتخاب می‌کنیم که توی اولی نباشه

اثبات: $(a_1,a_2,\dots,a_m)(\;—\;)$

تعریف (ترانهش)

هر دور را به طول ۲ را یک ترانهش گوئیند.

مثال: (۱ ۲ ۳)

دلیلی نداره ترانهش ها مجزا باشند

(۱ ۲ ۳) = (۱ ۳)(۱ ۲)

۱ → ۲

۲ → ۳

۳ → ۱

$n \in$ ۱,۲,۳,۴

(۱ ۲ ۳ ۴) = (۱ ۴)(۱ ۳)(۱ ۲)(n) ⟶ (۱ ۴)(۱ ۳)(۱ ۲) (۳|
۲
۱
۴

۳ → ۱

۲ → ۳

۱ → ۲

۴ → ۱

نکته: با توجه به مثال بالا هر دور را می‌توان به حاصل ضربی از ترانهش ها تجزیه کرد اما دلیلی ندارد ترانهش ها مجزا باشند

بنابراین هر دور را می‌توان با ترانهش ها تولید کرد

تذکر: با توجه به بحث های بالا هر عضو S_n (عضو جایگشت ها) با ترانهش تولید می‌شود.

مثال: مولد S_n ؟ ترانهش ها

هر معادله‌ای توی $\mathbb{R}$ از درجه ۲ به بالا قابل تجزیه به درجه یک یا دو است.

هر معادله‌ای توی $\mathbb{C}$ به درجه یک‌ها تجزیه می‌شوند.

برای اینکه بفهمیم معادله درجه n حل‌پذیر است یا نه

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

جابجایی‌ها یک گروه می‌سازند

گروه گالوا G

$H = G' \longrightarrow H' \quad G'' \quad \dots \quad G^{(n)} = 1$ حل‌پذیر (solvable group)

قضیه اساسی: معادله حل‌پذیر است $\iff G^{(n)} = 1$

تعریف:

جایگشت $\sigma \in S_n$ را جایگشت زوج گویند درصورتی‌که در تجزیه به ترانهش‌ها تعداد ترانهش‌ها زوج باشد در غیر این صورت فرد گویند.

$\sigma = (1,2)$ فرد

$\sigma = (1,2,3) = (1\,3)(1\,2)$ زوج — طول فرد ← زوج

$\sigma = (1,2,3,4) = (1\,4)(1\,3)(1\,2)$ فرد — طول زوج ← فرد

مثال: نوع کلی جایگشت روبه‌رو

$$\sigma = \underbrace{(1,2,3)}_{\text{زوج}}\underbrace{(4,5)}_{\text{فرد}}\underbrace{(1,2,3,5)}_{\text{فرد}} \longrightarrow \text{زوج}$$

تعریف:

مجموعه کلیه جایگشت‌های زوج از S_n را با علامت A_n نشان می‌دهند به وضوح A_n زیرگروهی از S_n است.

$e = (1,2)(2,1) \in A_n$

$\sigma, \tau \in A_n \longrightarrow \sigma = \alpha_1\alpha_2 \cdots \alpha_{2t}$ ترانهش α_i

$\tau = \beta_1\beta_2 \cdots \beta_{2r}$ ترانهش β_i

$$\sigma\tau^{-1} = \alpha_1 \cdots \alpha_{2t}\beta_{2r}^{-1} \cdots \beta^{-1}$$

$$= \underline{\alpha_1 \cdots \alpha_{2t}\beta_{2r} \cdots \beta_r}$$

تعداد زوج $\longrightarrow \sigma\tau^{-1} \in A_n$

۲ مورد مثال

- $\sigma = (1,2)(1,3)$

$\sigma^{-1} = (1,3)^{-1}(1,2)^{-1}$

$= (1,3)(1,2)$

- $\sigma = (1,2)(3,4)$

$\sigma^{-1} = (3,4)^{-1}(1,2)^{-1}$

$= (3,4)(1,2) = (1,2)(3,4)$

گروه A_n را گروه متناوب از درجه n گویند

لم: نشان دهید $A_n \trianglelefteq S_n$ و $|S_n : A_n| = 2$ ، $|A_n| = \frac{n!}{2}$

برهان:

$\varphi : S_n \longrightarrow \{1, -1\}$ واضح است φ همریختی پوشاست.

$\varphi(\alpha_1\alpha_2) \overset{?}{=} \varphi(\alpha_1)\varphi(\alpha_2)$

$$\varphi \quad \sigma \longmapsto \begin{cases} 1 & \text{اگر } \sigma \text{ زوج باشد} \\ -1 & \text{اگر } \sigma \text{ فرد باشد} \end{cases}$$

۴ حالت: ۱- α_1 زوج، α_2 فرد ۳- α_1 فرد، α_2 زوج

۲- α_1 زوج، α_2 زوج ۴- α_1 فرد، α_2 فرد

$\varphi(\text{زوج}, \text{فرد}) = -1 = \varphi(\text{زوج})\varphi(\text{فرد})$

$\varphi(\text{زوج}, \text{زوج}) = 1 = \varphi(\text{زوج})\varphi(\text{زوج})$

$\varphi(\text{فرد}, \text{فرد}) = 1 = \varphi(\text{فرد})\varphi(\text{فرد})$

پوشا بودن:

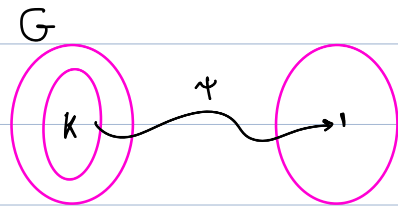
$$\left.\begin{array}{l} \varphi(e) = 1 \ \text{(زوج)} \\ \varphi(1,2) = -1 \end{array}\right] \quad \varphi \text{ پوشاست}$$

استفاده از قضیه ۱ یکریختی:

$\sigma \in \ker\varphi \longleftrightarrow \varphi(\sigma) = 1 \longleftrightarrow \sigma \in A_n$

قضیه اول یکریختی $\frac{S_n}{A_n} \cong \underbrace{\{\pm 1\}}_{\text{مرتبه ۲}} \Longrightarrow |S_n : A_n| = 2 \;,\; A_n \trianglelefteq S_n$

$K \trianglelefteq G$

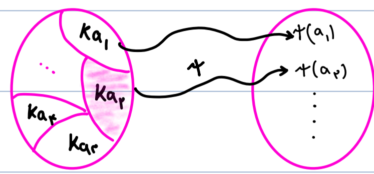


$G = Ka_1 \cup Ka_2 \cup \dots \cup Ka_t$

$\psi(a_1)$ $\psi(a_2)$ هرکدام به نماینده‌اش می‌رود!

$Ka = \{ka \mid k \in K\}$

$\psi(Ka) = \psi(a)$



مثال: در گروه S_3 زیرگروه A_3 را مشخص کنید.

$|S_3| = 6$

$|S_3 : A_3| = 2 \longrightarrow |A_3| = \frac{3!}{2} = 3$

$(1,3)$

$(1,2)$??

$(2,3)$

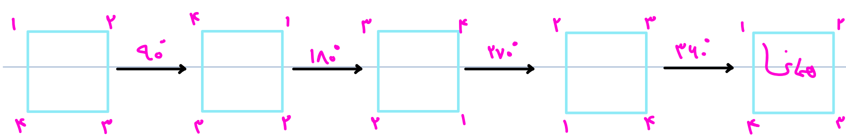
$A_3 = \{e, (1,2)(1,3), (1,2)(2,3)\}$

$(1,3)(2,3) = (1,2)(1,3)$

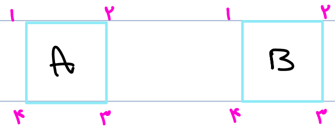
$1 \to 3 \qquad 1 \to 3$

$2 \to 1 \qquad 2 \to 1$

$3 \to 2 \qquad 3 \to 2$



$$\begin{cases} \sigma_{90} = (1,2,3,4) \\ \sigma_{180} = (1,3)(2,4) \\ \sigma_{270} = (1,4,3,2) \\ \sigma_{360} = id \end{cases}$$



$$\begin{cases} \sigma_{90} = (1,2,3,4) = \sigma \\ \sigma_{180} = (1,3)(2,4) = \sigma^2 \\ \sigma_{270} = (1,4,3,2) = \sigma^3 \\ \sigma_{360} = id = \sigma^4 \end{cases}$$

با نرم اولی تولید شد

$$\sigma^2 = \sigma\underbrace{\sigma(1)}_{2} = 3$$

$$\sigma\sigma(2) = 4$$

$$\sigma\sigma(3) = 1$$

$$\sigma\sigma(4) = 2$$

$$\sigma^3 = \sigma^2\underbrace{\sigma(1)}_{2} = 4$$

یک حالت دیگه $\longrightarrow$ ۳,۴ ثابت $\longrightarrow$ ۱,۲ را با هم جابجا کنیم

$\tau = (2,4)$

$\sigma\tau = (1,2)(3,4)$

$\sigma^2\tau = (1,3)$

$\sigma^3\tau = (1,4)(2,3)$

هر حالت دیگری که فکر کنیم یکی از این ۸ حالت است

تقارن های مربع:

D_{2n}

$$D_{2\times 4} = \langle \sigma, \tau \mid \sigma = (1,2,3,4), \tau = (2,4) \rangle$$

$$= \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

مثال: ثابت کنید با توجه به تعریف گروه تقارن $\sigma^i\tau$ $(0\le i\le 3)$ بود مرتبه آن ۲ است $o(\sigma^i\tau)=2$

$D_8=\{1,\sigma,\sigma^2,\sigma^3,\tau,\sigma\tau,\sigma^2\tau,\sigma^3\tau\}$

مرتبه ۱   مرتبه ۴   مرتبه ۲   مرتبه ۴   مرتبه ۲

برای $i=0$ برقرار است

$\sigma=(1,2,3,4)$ $\sigma^3=(1\ 4\ 3\ 2)$

$\sigma^2=(1\ 3)(2\ 4)$ $\tau=(1\ 3)$

برای $i=1$ $\longleftarrow$ $\underline{\sigma\tau}\,\underline{\sigma\tau}$

$$=(1\ 2)(3\ 4)(1\ 2)(3\ 4)$$
$$=(1\ 2)(1\ 2)(3\ 4)(3\ 4)$$
$$=(1\ 2)^2(3\ 4)^2$$
$$=1$$

قضیه کیلی: (بدون برهان)

هر گروه متناهی داخل یک گروه جایگشتی قرار می‌گیرد.

نکته:

با توجه به قضیه کیلی، همه گروه‌ها را می‌توان به عنوان گروه جایگشتی در نظر گرفت و از نمادهای معین خارج شد.

$|G|=1024 \longrightarrow G\leqslant S_{1024}$ $|S_{1024}|=1024!$

تو این باید دنبال زیرگروه‌ها با مرتبه ۱۰۲۴ بگردیم

تمرین (حاصل ضرب مستقیم گروه ها) Direct Product

فرض کنید $G_1, G_2, \dots, G_n$ ، n تا گروه باشند.

حاصل ضرب مستقیم آن ها را با

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

$$(g_1, \dots, g_n) * (g_1', \dots, g_n') = (g_1 g_1', g_2 g_2', \dots, g_n g_n')$$

$Mat_{m\times n}(\mathbb{R})$

$([\,], g)([\,], h)$ → ?

توجه شود:

با توجه به عمل تعریف شده در بالا حاصل ضرب مستقیم تشکیل یک گروه می دهد و خواص زیر را داریم:

۱- بسته بودن

۲- عضو همانی $e = (e_1, e_2, \dots, e_n)$

۳- عضو معکوس $g^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$

۴- شرکت پذیری — چرا از هم اند

قضیه اساسی گروه آبلی: بدون اثبات

فرض کنید G یک گروه آبلی متناهی باشد به طوری که تجزیه مرتبه G به صورت $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ باشد که در آن p_i ها اعداد اول متمایزند. در این صورت G با حاصل ضرب مستقیمی از گروه های دوری یکریخت است.

?

مثال: تعداد گروه های آبلی مرتبهٔ ۴ را پیدا کنید.

افراز

$|G| = p^2 \rightarrow p$

افرازهای ۲ با جمع اعداد طبیعی

$$\begin{cases} 2 = 2 & \longrightarrow \mathbb{Z}_{2^2} \\ 2 = 1+1 & \longrightarrow \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \end{cases}$$

آبلی

$|G| = 8 = 2^3 \rightarrow p=2$

$$\begin{cases} 3 & \xrightarrow{\text{۱ عامل ضرب}} \mathbb{Z}_{2^3} \\ 2+1 & \xrightarrow{\text{۲ عامل ضرب}} \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \\ 1+1+1 & \xrightarrow{\text{۳ عامل ضرب}} \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \end{cases}$$

آبلی

$|G| = 81 = 3^4$

$$\begin{cases} 4 & \xrightarrow{\text{۱ عامل ضرب}} \mathbb{Z}_{3^4} \\ 3+1 & \xrightarrow{\text{۲ عامل ضرب}} \mathbb{Z}_{3^3} \times \mathbb{Z}_{3^1} \\ 2+2 & \xrightarrow{\text{۲ عامل ضرب}} \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \\ 2+1+1 & \xrightarrow{\text{۳ عامل ضرب}} \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \\ 1+1+1+1 & \xrightarrow{\text{۴ عامل ضرب}} \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \end{cases}$$

تعداد گروه های آبلی ⟵ تعداد افرازها

$\# G = 5$

نکته:

تعداد گروه های آبلی از مرتبهٔ p^n = تعداد افرازهای n به اعداد طبیعی

مثال: تعداد گروه‌های آبلی از مرتبهٔ ۱۰۰ را پیدا کنید

$۱۰۰ = ۵^۲ \times ۲^۲$

آبلی $|H_۱| = ۴ = ۲^۲ \longrightarrow$ تا ۲ $\longrightarrow \mathbb{Z}_۲ \times \mathbb{Z}_۲ \ , \ \mathbb{Z}_{۲^۲}$

$\# G = ۲ \times ۲ = \underline{\underline{۴}}$

آبلی $|H_۲| = ۲۵ = ۵^۲ \longrightarrow$ تا ۲ $\longrightarrow \mathbb{Z}_۵ \times \mathbb{Z}_۵ \ , \ \mathbb{Z}_{۵^۲}$

- $\mathbb{Z}_{۲^۲} \times \mathbb{Z}_{۵^۲}$
- $\mathbb{Z}_{۲^۲} \times \mathbb{Z}_۵ \times \mathbb{Z}_۵$
- $\mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_۵ \times \mathbb{Z}_۵$
- $\mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_{۵^۲}$

مثال: تعداد گروه‌های آبلی از مرتبهٔ ۶۰ ؟

$|G| = ۲^۲ \times ۳^۱ \times ۵^۱ \longrightarrow ۲ \times ۱ \times ۱ = \underline{\underline{۲}}$

$|۳۶| = |۶۰|$

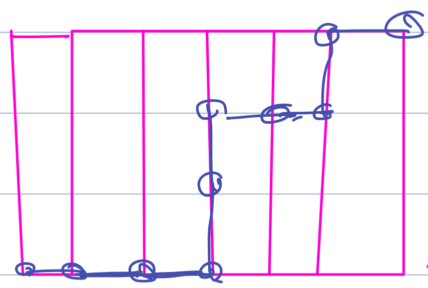
مثال:

تعداد گروه آبلی از مرتبه ۶۰

$|G| = ۲^{\boxed{۲}} \times ۳^{۱} \times ۵^{۱}$

|۳۶| = |۶۰| → ?

شبکه = رخی در ترکیبیات



۶ = ۳+۲+۱

نفهمیدم که چرا مرتبه را به رخی ربط داد

تازه آخرش هم به نتیجه نرسید.

فکر کنم خودش هم حوصلش سر رفته [redacted]

الان ساعت ۱۱:۲۵ دقیقه است [redacted]

خلاصه: تعداد افراز ها رابطه مشخص نداره ولی این میگه به تعداد آپ ها در رخی مربوط است

یادآوری :

آبلی

• $|G| = ۴۵ = ۳^۲ \times ۵$

$۱ = ۱ \quad \mathbb{Z}_۵$

$۲ = ۲ \quad \mathbb{Z}_{۳^۲}$

$۲ = ۱ + ۱ \quad \mathbb{Z}_۳ \times \mathbb{Z}_۳$

$$\begin{cases} G = \mathbb{Z}_{۳^۲} \times \mathbb{Z}_۵ \cong \mathbb{Z}_{۴۵} \\ G = \mathbb{Z}_۳ \times \mathbb{Z}_۳ \times \mathbb{Z}_۵ \cong \mathbb{Z}_۳ \times \mathbb{Z}_{۱۵} \end{cases}$$

آبلی

• $|G| = ۲^۲ \times ۳^۳ \times ۵^۲$

$۲ = ۲ \quad \mathbb{Z}_{۵^۲}$

$۲ = ۱ + ۱ \quad \mathbb{Z}_۵ \times \mathbb{Z}_۵$

$۲ = ۲ \quad \mathbb{Z}_{۲^۲}$

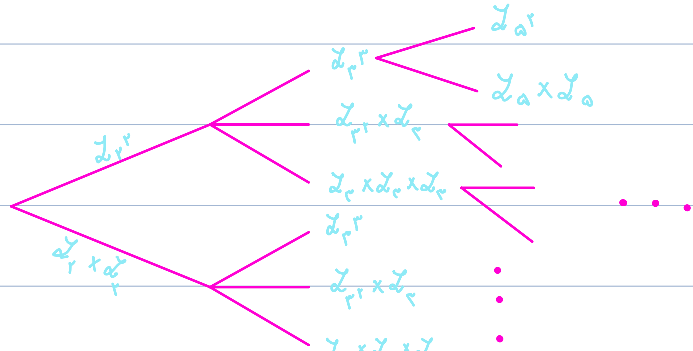
$۲ = ۱ + ۱ \quad \mathbb{Z}_۲ \times \mathbb{Z}_۲$

$۳ = ۳ \quad \mathbb{Z}_{۳^۳}$

$۳ = ۲ + ۱ \quad \mathbb{Z}_{۳^۲} \times \mathbb{Z}_۳$

$۳ = ۱ + ۱ + ۱ \quad \mathbb{Z}_۳ \times \mathbb{Z}_۳ \times \mathbb{Z}_۳$

$\# G = ۲ \times ۳ \times ۲ = ۱۲$



تمرین: فرض کنید m, n اعداد طبیعی باشند $(m,n)=1$ در این صورت $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

مثال: $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{30}$ یا $\mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{45}$

برهان: فرض کنیم $\mathbb{Z}_{mn} = \langle a \rangle$ $(|a| = o(a) = mn)$

قرار دهیم $H = \langle a^m \rangle$, $K = \langle a^n \rangle$ داریم

$$|H| = \frac{o(a)}{(o(a), m)} = \frac{mn}{(mn, m)} = \frac{mn}{m} = n$$

مرتبه

$$|K| = \frac{o(a)}{(o(a), n)} = \frac{mn}{n} = m$$

لذا $H \cong \mathbb{Z}_n$, $K \cong \mathbb{Z}_m$

$$\varphi : H \times K \longrightarrow \mathbb{Z}_{mn}$$
$$(x,y) \longmapsto xy$$

φ همریختی، 1-1، پوشاست.

$$\varphi((x,y)(x',y')) = \varphi(xx', yy') = xyx'y' = \varphi(x,y)\varphi(x',y')$$ همریختی

نکته: برای اینکه بگیم یک به یک است نتوانیم بگوییم تابع پوشا و مرتبه آن ها برابر است.

$\varphi : A \longrightarrow B$ پوشا و $|A| = |B|$

پوشا $\varphi \iff$ یک به یک

پوشا بودن

$$\varphi : H \times K \longrightarrow \mathbb{Z}_{mn} = \langle a \rangle$$

دلخواه $a^t \in \mathbb{Z}_{mn}$

$H = \langle a^m \rangle$ ، $K = \langle a^n \rangle$

$(m,n) = 1 \xrightarrow{\text{تعلیم اعداد}} rm + sn = 1$

$x = (a^m)^{rt} \in H$ ، $y = (a^n)^{st} \in K$

$\times t$: $m(rt) + n(st) = t$

$$\varphi(x,y) = a^{mrt} a^{nst} = a^{mrt + nst} = a^t$$

پس یک به یک است.

تعریف : حلقه ها (Ring)

مجموعهٔ ناتهی R همراه با ۲ عمل $+$ و $\times$ تشکیل حلقه می دهد در صورتی که روابط و خواص زیر برقرار باشند $(R, +, .)$

۱- $(R, +)$ گروه آبلی باشند — ۴ تا خاصیت — شرکت پذیر و همانی و معکوس و تعویض پذیر

۲- $(R, .)$ نیم گروه باشند (نیم گروه : عمل $a.b$ و $a.(b.c) = (a.b).c$)

۳- توزیع پذیری نسبت به جمع

$a(b+c) = ab + ac$

$(b+c)a = ba + ca$

مثال های زیر نمونه های حلقه ها هستند

۱- $(\mathbb{Z}, +, .)$

۲- $(\mathbb{Q}, +, .)$

۳- $(\mathbb{R}, +, .)$

۴- $(\mathbb{C}, +, .)$

۵- $(M_n(\mathbb{R}), +, .)$ $\times$ جابجایی نیست

تعریف: حلقه‌ی جابه‌جایی (Commutative ring)

حلقه‌ی $(R,+,\cdot)$ را حلقه‌ی جابه‌جایی گویند در صورتی که: $\forall a,b\in R \quad ab=ba$

مثال: $(\mathbb{Z}_n, +_n, \cdot_n)$

$a\cdot b \overset{n}{\equiv}$

$a+b \overset{n}{\equiv}$

حلقه‌ی جابه‌جایی است

عضو خنثی ضرب!

$(\mathbb{Z}_{10}, +, \cdot)$

$3+7=0$

$3\times 7=21=1$

نکته: $(\mathbb{Z}_p, +_p, \cdot_p)$ که p عدد اول است $\Leftarrow$ میدان ✓

تعریف:

حلقه‌ی $(R,+,\cdot)$ را حلقه‌ی یکدار گویند در صورتی که نسبت به عمل ضرب دارای عضو خنثی باشند، عضو خنثی ضرب را با علامت 1 نشان می‌دهند.

- $(\mathbb{Z}_n, +, \cdot)$ — یکدار ✓ — جابه‌جایی ✓
- $(M_n(R), +, \cdot)$ — یکدار ✓ — جابه‌جایی ✗

تعریف میدان Field

فرض کنید $(R,+,\cdot)$ یک حلقهٔ جابه‌جایی و یکدار باشد به طوری که با عمل ضرب هر عضو مخالف صفر آن وارون داشته باشد در این صورت R را یک میدان گویند.

$(R,+)$ گروه آبلی

$(R-\{0\},\cdot)$ گروه آبلی

توزیع‌پذیری
$$\begin{cases} a(b+c) = ab+ac \\ (b+c)a = ba+ca \end{cases}$$

مثال: مثال‌هایی از میدان

- $(\mathbb{Z},+,\cdot)$ ✗ → معکوس ضربی ✗
- $(\mathbb{R},+,\cdot)$ ✓
- $(\mathbb{Q},+,\cdot)$ ✓
- $(M_n(\mathbb{R}),+,\cdot)$ ✗ جابه‌جایی ضربی ✗
- $(Gl(n,\mathbb{R}),+,\cdot)$ ✗ جابه‌جایی!

تمرین: $(\mathbb{Z}_n,+,\cdot)$ میدان است $\Leftrightarrow$ n اول است

حل:

$\Leftarrow$ $(\mathbb{Z}_n,+,\cdot)$ میدان است و فرض کنیم n اول نباشد پس $n=kl$ که $1<\cancel{n}\,l, k<n$

ادعا کنیم k معکوس ضربی ندارد $kk'=1$

طرفین در l ضرب شود $\underbrace{kl}_{0}k'=l \longrightarrow l=0$ ✗

$\mathbb{Z}_{10}$ $\quad 10=2\times5$

$2\cdot0=1 \quad 2\cdot0\cdot5=5$

$\underbrace{2\times5}_{0}\cdot0=5 \longrightarrow 5=0$ ✗

$\Rightarrow$ (n اول) $0\neq a\in\mathbb{Z}_n$ پس $(a,n)=1$ لذا $a^{n-1}\equiv_n 1$ پس $a\underbrace{a^{n-2}}_{a^{-1}}\equiv_n 1$

یادآوری:

حلقه: $(R,+,.)$ → $(R,+)$ آبلی، $(R,.)$ نیم گروه

حلقهٔ جابجایی: $ab=ba$

حلقهٔ یکدار: $1a=a1$

میدان: $(R,+,.)$ → $(R,+)$ آبلی، $(R,.)$ آبلی

مثال: حلقهٔ کواترنیون ها ← فرض کنید $R=\{a_0+a_1i+a_2j+a_3k \mid 0\leq i\leq 3,\ a_i\in R\}$ که در آن i، j، k سه نماد هستند.

برای ضرب i، j، k در یکدیگر در جهت عقربه ساعت علامت + $(ki=j\ ,\ jk=i\ ,\ ij=k)$

و در خلاف جهت ساعت علامت − $(ji=-k,\ kj=-i\ ,\ ik=-j)$

همچنین $i^2=j^2=k^2=-1$ ، $ijk=-1$

چون a_i ها توی R می‌توانند جابجا بشن. شرکت‌پذیری هم از R

$$(a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k)=a_0+b_0+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k$$

$$(a_0+a_1i+a_2j+a_3k).(b_0+b_1i+b_2j+b_3k)=$$ مشابه بالا

$a_0b_0+a_0b_1i+a_0b_2j+a_0b_3k$
$a_1ib_0+a_1b_1i^2+a_1b_2ij+a_1b_3ik$
$a_2b_0j+a_2b_1ij+a_2b_2jj+a_2b_3jk$
$a_3b_0k+a_3b_1ik+a_3b_2jk+a_3b_3kk$

حلقه

واضح است که $(R,+)$ گروه آبلی هستند

$(R,.)$ نیم گروه → $(R^*,.)$ گروه نا آبلی

یکدار است $(1+0i+0j+0k)$

$$x=a_0+a_1i+a_2j+a_3k\neq 0$$

$$|x|=\sqrt{a_0^2+a_1^2+a_2^2+a_3^2}\neq 0$$

$$x^{-1}=y=\frac{a_0}{|x|}+\frac{a_1}{|x|}i+\frac{a_2}{|x|}j+\frac{a_3}{|x|}k\in R$$

$$xy=1$$

جابجایی نیست $(ij\neq ji)$

تعریف حلقه تقسیم

حلقهٔ $(\mathbb{R},+,\cdot)$ را حلقه تقسیم گویند درصورتی که $(\mathbb{R}^*,\cdot)$ گروه شوند

- $(\mathbb{R},+,\cdot) \longrightarrow (\mathbb{R},+)$ آبلی
- $(\mathbb{R},+,\cdot) \longrightarrow (\mathbb{R}^*,\cdot)$ گروه ← تفاوت با میدان: آبلی نیست
- توزیع پذیری

مثال: حلقهٔ کواترنیون‌ها، حلقه تقسیم هستند که میدان نمی‌باشند.

$(\mathbb{Z},+,\cdot)$ حلقهٔ تقسیم نمی‌باشد

خواص مقدماتی:

حلقه $(\mathbb{R},+,\cdot)$

۱- $a0 = 0a = 0$

$a0 = a(0+0) = a0+a0 \longrightarrow a0 = a0+a0 \xrightarrow{\text{حذف}} a0 = 0$

۲- $a(-b) = (-a)b = -ab$

$ab + a(-b) \overset{\text{توزیع پذیری}}{=} a(b+(-b)) = a0 = 0$

$ab + a(-b) = 0$ ← قرینه جمعی ← یکتا ← $-ab = a(-b)$

۳- $a(b-c) = ab - ac$

$a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$

۴- $(-1)a = -a$

$a+(-1)a = 1a+(-1)a = (1+(-1))a = 0 \longrightarrow a+(-1)a = 0 \longrightarrow (-1)a = -a$

۵- $(-1)(-1) = 1$

$(-1)+(-1)(-1) = (-1)1+(-1)(-1) = (-1)(1+(-1)) = 0$

$\hookrightarrow (-1)+1 = 0 \longrightarrow 1 = (-1)(-1) \longrightarrow ?$

۶- $m(na) = (mn)a$

۷- $ma + na = (m+n)a$

بازکن

$-7a = 7(-a) = -a-a-\dots-a$

تعریف مقسوم الیه صفر

فرض کنید R یک حلقه . عنصر $x \neq 0$ را مقسوم الیه چپ صفر گویند در صورتی که عنصری ناصفر مانند y وجود داشته باشد

به طوری که : $xy=0$

مشابه تعریف بالا : $x \neq 0$ را مقسوم الیه راست صفر گویند در صورتی که عنصری ناصفر مانند y وجود داشته باشد به طوری که $yx=0$

مثال : در حلقهٔ ماتریس ها $x=\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$ مقسوم الیه چپ صفر است .

$y=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \hookrightarrow \underline{xy=0}$

تعریف حوزهٔ صحیح

فرض کنید $(R,+,\cdot)$ حلقه جابجایی باشد که مقسوم الیه صفر ندارد . در این صورت R را یک حوزهٔ صحیح گویند

$(\mathbb{Z},+,\cdot)$

$(R,+,\cdot) \longrightarrow$ توزیع پذیری ✓

آبلی $(R,+)$ ✓

نیم گروه $(R,\cdot)$ ✓

جابجایی ✓

مقسوم الیه صفر ✗

حوزهٔ صحیح

لم : هر حوزهٔ صحیح متناهی ، یک میدان است .

برهان : کافی است ثابت کنیم که $(R,\cdot)$ نیم گروه متناهی است ، تشکیل گروه می دهد .

برای این منظور با توجه به متناهی بودن آن ثابت می کنیم قوانین حذف در آن برقرار است .

$a \neq 0$

$ab=ac \longrightarrow ab-ac=0 \longrightarrow a(b-c)=0 \xrightarrow{\text{حوزهٔ صحیح}} b-c=0 \longrightarrow \underline{b=c}$

حوزهٔ صحیح $\longrightarrow xy=0 \longrightarrow x=0$ یا $y=0$

یادآوری:

حوزه صحیح — حلقه $(R,+)$ آبلی

$(R,\cdot)$ نیم‌گروه

$\to xy=0 \longrightarrow x=0$ یا $y=0$

حلقه تقسیم — میدان $(R,+)$ آبلی

$(R,\cdot)$ آبلی

$\to (R^*,\cdot)$ گروه شوند

تعریف: (مشخصه حلقه)

فرض R یک حلقه باشد کوچک‌ترین عدد طبیعی مانند n که به ازای هر $na=0$ $\forall a\in R$

$(\underbrace{a+a+\dots+a}_{n \text{ بار}}=0)$

مشخصه حلقه گویند و می‌نویسیم: $\mathrm{char}\, R = n$

اگر چنین حلقه‌ای وجود نداشت مشخصه حلقه را صفر می‌گیریم.

$\mathrm{char}\, \mathbb{Q} = 0$ $\qquad$ $\mathrm{char}\, \mathbb{Z}_n = n$ $\qquad$ $\mathbb{Z}_7 = \{0,1,2,\dots,6\}$

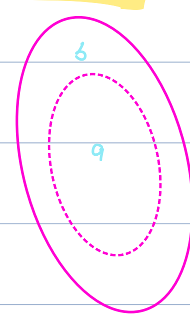
$\mathrm{char}\, \mathbb{Z} = 0$ $\qquad$ $2n=0 \quad n|2n$ $\qquad$ $\mathrm{char}\, \mathbb{Z}_7 = 7$

نکته: برای پیدا کردن مشخصه حلقه یکدار کافی است ببینیم $n1$ به چه موقعی صفر است کوچک‌ترین n

جواب مسئله هست.

$n1=0$

$(na) = n(1a) = \underbrace{(n1)}_{0}a = 0$



$\mathrm{Arccos}[-1,1] \longrightarrow [0,\pi]$

$\mathrm{Arccos}(0) = \frac{\pi}{2}$

$n2 = n(1+1)$

$= \underbrace{n1}_{0} + \underbrace{n1}_{0}$

مسأله: فرض کنید D یک حوزه صحیح باشد، $0 \neq a \in D$ ، $na = 0$ در این صورت به ازای هر $b \in D$ داریم $nb = 0$

حل:

فرض کنید nb باشد (خلاف) $nb \neq 0$

$$\underbrace{a(nb)}_{\neq 0} = \underbrace{(na)}_{0} b = 0 \longrightarrow a(\underbrace{nb}_{\neq 0}) = 0 \xrightarrow{\text{حوزه صحیح}} a = 0 \quad \times$$

قضیه: مشخصه یک حوزه صحیح صفر یا عدد اول است.

برهان: فرض کنید $n = char\, R \neq 0$ ادعای کنیم n اول است در این صورت $n = rs$ که $1 < r,s < n$ داریم

$12 = 3\times 4$

$$0 = na = (rs)a = r(\overbrace{sa}^{a'})$$

حالات زیرا اتفاق میافتد

• $sa = 0$ پس طبق مسأله قبل به ازای هر $b \in R$ داریم $sb = 0$ اما $s < n$ که این با انتخاب n به عنوان کوچکترین عدد در تناقض است.

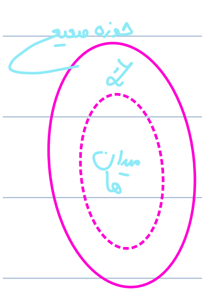
• $sa \neq 0$ لذا $a' \neq 0$ و $ra' = 0$ طبق مسأله قبل $rb = 0$ $\forall b \in R$ که این نیز با کوچکترین بودن عدد n در تناقض است.

پس n اول است.

مسأله: $\mathbb{Z}_{15}$ حوزه صحیح نیست زیرا $char\, \mathbb{Z}_{15} = 15$ می شود و 15 عدد اول نمی باشد.

مسأله: $\mathbb{Z}_n$ حوزه صحیح است اگر و تنها اگر $\mathbb{Z}_n$ میدان باشد اگر و تنها اگر n عدد اول باشد.

مسأله: میدان ها حوزه صحیح هستند.



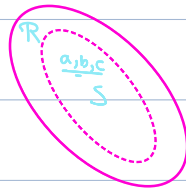
حل:

$$ab = 0 \xrightarrow{a \neq 0} a^{-1}(ab) = 0 \longrightarrow (\underbrace{a^{-1}a}_{1})b = 0 \longrightarrow b = 0$$

(میدان a^{-1} وجود دارد)

تعریف: زیرحلقه

فرض کنید $(R,+,.)$ حلقه باشد S زیرمجموعه‌ی ناتهی R است S را زیرحلقه گوئیم در صورتی که با ۲ عمل حلقه‌ی R تشکیل حلقه دهند.



* شرکت‌پذیری را چون بالایی داره اینم داره و بدیهی است

پس برای زیرحلقه بودن ۲ تا چیز باید چک شود:

۱- بسته بودن نسبت به جمع ab^{-1}

۲- بسته بودن ضرب نسبت به ضرب

$1-\ a,b\in S \longrightarrow a-b\in S$

$2-\ \forall a,b\in S \longrightarrow ab\in S$

مثال: $2\mathbb{Z}$ زیرحلقه‌ی $\mathbb{Z}$ است.

$$2\mathbb{Z} \leqslant (\mathbb{Z},+,.)$$

$$1-\quad \left.\begin{array}{l} a=2k \\ b=2k' \end{array}\right\} \quad a-b=2k-2k'=2(k-k')\in 2\mathbb{Z}$$

$$2-\ ab=2k2k'=2(\underbrace{2kk'}_{k''})\in 2\mathbb{Z}$$

نکته: کلیه زیرحلقه‌های $\mathbb{Z}$، $m\mathbb{Z}$ است.

تعریف: مرکز حلقه

فرض کنید R یک حلقه باشد در این صورت مجموعه‌ی

$$\mathbb{Z}(R)=\{a\in R \mid \forall n\in R \quad an=na\}$$

را مرکز حلقه‌ی R می‌نامند.

نکته: مرکز هر حلقه یک زیرحلقه از آن است.

مسأله: $Z(R)$ زیر حلقه است.

برهان:

۱- $a,b \in Z(R) \longrightarrow a-b \in Z(R)$

$\forall x \in R \longrightarrow (a-b)x = ax - bx = xa - xb = x(a-b) \longrightarrow a-b \in Z(R)$

۲- $a,b \in Z(R) \longrightarrow ab \in Z(R)$

$\forall x \in R \longrightarrow (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \longrightarrow ab \in Z(R)$

نکته: اگر R حلقه باشد، ۰ و R زیرحلقه‌های بدیهی اند.

مسأله: حلقه‌ی R را بولی گوئیم درصورتی که $\forall a \in R \quad a^2 = a$

بولی

بولی

مسأله: ثابت کنید حلقه‌های بولی جابه‌جایی هستند.

حل:

$(a+b)^2 = a+b$

$(a+b)^2 = a^2+b^2+ab+ba$

$\cancel{a}+\cancel{b} = \cancel{a^2}+\cancel{b^2}+ab+ba$

$\hookrightarrow ab = -ba \longrightarrow ab = ba$

$a = a^2 = \underbrace{(-a)^2 = -a}_{\text{بولی}}$

مثال: فرض کنید M مجموعه ناتهی باشد. $(P(M), \Delta, \cap)$

- $A, B \in P(M) \longrightarrow A \cap B \in P(M)$
- $A \cap (B \cap C) = (A \cap B) \cap C$

- $A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
- $A \Delta \underset{}{\overset{\text{خنثی}}{\phi}} = A$
- $A \Delta A = \phi \longrightarrow A^{-1} = A$

حلقه‌ی بولی $A^2 = A \cap A = A$

تعریف: ایده‌آل

فرض کنید $(R, +, .)$ یک حلقه باشد، I زیرمجموعه ناتهی R ، $\phi \neq I \subseteq R$ را ایده‌آل گوئیم درصورتی که ۲ شرط زیر برقرار باشند:

۱- $a, b \in I \quad a - b \in I$ (گروه آبلی می‌شود $(I, +)$)

۲- $\forall r \in R, \forall a \in I \quad ra \in I$

ایده‌آل‌ها حتما زیرحلقه اند. اما عکس آن برقرار نیست!

در این صورت با توجه به اینکه ضرب اعضای آن از سمت چپ انجام شده، I را یک ایده‌آل چپ می‌گوئیم.

اگر R حلقه جابه‌جایی باشد، ایده‌آل چپ و راست یکی است.

مثال: R و 0 ایده‌آل های بدیهی هستند.

$0, R$

$a, b \in \{0\} \longrightarrow a - b \in \{0\}$

$\forall r \in R, a \in \{0\} \longrightarrow ra = 0 \in \{0\}$

نکته: در $\mathbb{Z}$ ایده‌آل هایش همان $n\mathbb{Z}$ است.

$\mathbb{Z} \xrightarrow{\text{زیرگروه}} n\mathbb{Z}$

$\mathbb{Z} \xrightarrow{\text{زیرحلقه}} n\mathbb{Z}$

$\mathbb{Z} \xrightarrow{\text{ایده‌آل}} n\mathbb{Z}$

مسأله: فرض کنیم R حلقه و $I \trianglelefteq R$ (علامت ایده‌آل) ایده‌آل آن به طوری که $a \in I$ ، a معکوس پذیر باشد در این صورت $I = R$

$$a \in I,\ aa^{-1} = 1 \quad \Big\{ \quad \underbrace{a^{-1}}_{r}\underbrace{a}_{I} \in I \longrightarrow 1 \in I$$

$$\forall r \in R \quad \underbrace{R}_{\in R}\underbrace{1}_{\in I} \in I \longrightarrow r \in I \longrightarrow R \subseteq I \ ,\ \text{می‌دانیم: } I \subseteq R \longrightarrow R = I$$

مسأله: ایده‌آل های یک میدان را مشخص کنید

حل: فرض کنید R یک میدان باشد، I ایده‌آلش باشد، $0 \neq I \trianglelefteq R$ لذا $0 \neq a \in I$. چون R یک میدان است پس a معکوس ضربی دارد.

طبق مسأله قبل $I = R$

پس هر میدان فقط ۲ ایده‌آل بدیهی دارد.

مسأله: اگر R یک حلقه، I و J دو ایده‌آل های آن باشند در این صورت $I+J$ ، IJ را به صورت زیر تعریف می‌کنیم:

- $I + J = \{a + b \mid a \in I, b \in J\}$

برهان:

$$x = a + b,\quad y = a' + b' \quad \Big\{ \quad x - y = a + b - a' - b' = \underbrace{a - a'}_{\in I} + \underbrace{b - b'}_{\in J} \in I + J$$

$$r(a + b) = \underbrace{ra}_{\in I} + \underbrace{rb}_{\in J} \in I + J$$

- $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$

برهان:

$$x = a_1b_1 + \cdots + a_nb_n,\quad y = a'_1b'_1 + \cdots + a'_nb'_n \quad \Big\{ \quad x - y = a_1b_1 + \cdots + a_nb_n + (-a'_1)b'_1 + \cdots + (-a'_n)b_n \longrightarrow x - y \in IJ$$

$$r \in R \ ,\quad x = a_1b_1 + \cdots + a_nb_n$$

$$rx = \underbrace{ra_1}_{\in I}\underbrace{b_1}_{\in J} + \cdots + \underbrace{ra_n}_{\in I}\underbrace{b_n}_{\in J} \in IJ$$

نکته: اگر I, J ایده‌آل های R باشد در این صورت داریم:

i) $I \leq I+J$

برهان i: $i = i+0 \in I+J \longrightarrow I \leq I+J$

ii) $J \leq I+J$

برهان ii: $j = j+0 \in I+J \longrightarrow J \leq I+J$

iii) $IJ \subseteq I \cap J$

برهان iii:

$$\left.\begin{array}{l} x = \underbrace{a_1}_{\in I,\ \in R}\ \underbrace{b_1}_{\in J,\ \in J} \in J \\ \\ x = \underbrace{a_1}_{\in I,\ \in I}\ \underbrace{b_1}_{\in J,\ \in R} \in I \end{array}\right\} IJ \subseteq I \cap J$$

مسئله: $m\mathbb{Z} + n\mathbb{Z} = \overset{\text{ب.م.م}}{(m,n)}\,\mathbb{Z}$

$(m,n) = d$ حتما داخلش هست چون ایده‌آل هست پس مضارب آن هم داخلش هست! $\Leftarrow$

یک ترکیب خطی است

$\exists r,s \in \mathbb{Z} \quad \underbrace{rm}_{\in m\mathbb{Z}} + \underbrace{sn}_{\in n\mathbb{Z}} = d \in m\mathbb{Z} + n\mathbb{Z}$

$m\mathbb{Z} \cdot n\mathbb{Z} = \overset{\text{ک.م.م}}{[m,n]}\,\mathbb{Z}$

مثال: • $2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z}$ • $6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$ • $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$

حلقه خارج قسمتی: فرض کنید R یک حلقه و I ایده‌آلی از آن باشد، حلقه خارج قسمت آن را به صورت زیر تعریف می‌کنیم:

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

$$(I+x)+(I+y) := I+x+y$$

$$(I+x)(I+x) := I+xy$$

توجه شود $\frac{R}{I}$ با عمل اول یک گروه آبلی است زیرا $(I,+) \leq (R,+)$ است

چون $(R,+)$ گروه آبلی است لذا هر زیرگروه آن نرمال است

طبق بحث‌های انجام شده در گروه‌ها $(\frac{R}{I},+)$ گروه آبلی است.

عضو خنثی:

$$\underbrace{I}_{\text{عضو خنثی جمع}} = I+0$$

$$I+x+I+0 = I+x$$

$$I+x+\underbrace{I-x}_{\text{معکوس جمعی}} = I$$

توجه شود: اگر $I+x = I+x'$ ($x-x' \in I$) و $I+y = I+y'$ ($y-y' \in I$) طبق تساوی همدسته‌ها چون I ایده‌آل است به سهولت دیده می‌شود عمل ضرب خوش تعریف است.

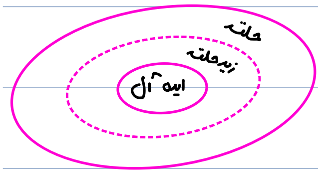
?

نکته: اگر R حلقه جابه‌جایی باشد، $\frac{R}{I}$ نیز حلقه جابه‌جایی است.

اگر R یکدار باشد، $\frac{R}{I}$ نیز یکدار است، یکه آن $I+1$ است.

$$(I+1)(I+x) = I+x$$

یادآوری:



$I \trianglelefteq R$

$\frac{R}{J} = \{ J + x \mid x \in R \}$

۲ همسته برابر

P

$J + x = J + y \iff x - y \in J$

$Nx = Ny \iff xy^{-1} \in N$

- $J + x + J + y = J + x + y$
- $(J+x)(J+y) = J + xy$ ایده‌آل

- $J + 0 = J$ عضو خنثی جمع
- $J - x$ معکوس جمعی
- $J + 1$ یکدار

تذکر: فرض کنید R حلقه، I ایده‌آلی از آن باشد. در این صورت:

i) اگر R جابه‌جایی باشد آن‌گاه $\frac{R}{I}$ جابه‌جایی است. عکس این برقرار نیست!

حل i: $(I+x)(I+y) = I + xy = I + yx = (I+y)(I+x)$ پس $\frac{R}{I}$ جابه‌جایی

ii) اگر R یکدار باشد آن‌گاه $\frac{R}{I}$ نیز یکدار است.

حل ii: $(I+x)(I+1) = I + x$

یکای حلقهٔ خارج‌قسمتی است

تعریف (همریختی حلقه‌ها)

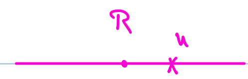
یادآوری:

پوشا و یک به یک + همریختی ← یکریختی $G_1 \cong G_2$

همریختی $\begin{cases} f: G_1 \longrightarrow G_2 \\ f(xy) = f(x)f(y) \end{cases}$

• $\mathbb{Z} \neq \mathbb{Z} \times \{0\}$

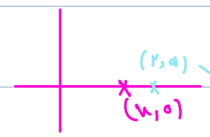
$\mathbb{Z} \cong \mathbb{Z} \times \{0\}$



$2+3=5 \qquad (2,0)+(3,0)=(5,0)$ ۱-۱ و پوشا

• $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$

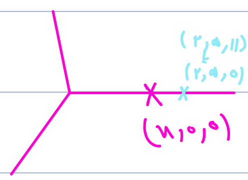
$f: \mathbb{C} \longrightarrow \mathbb{R}\times\mathbb{R}$



$a+bi \mapsto (a,b)$

$\mathbb{C} \cong \mathbb{R}\times\mathbb{R}$

• میشدند نقطه‌ی ۳ بعدی هم باشد



نباید اون یکی‌ها را

نداشتی

تعریف: فرض کنید R_1, R_2 دو حلقه باشند. تابع $f: R_1 \to R_2$ را یک همریختی حلقه گویند در صورتی که:

$f: \underset{+,\cdot}{R_1} \longrightarrow \underset{+,\cdot}{R_2}$

۱- $f(x+y) = f(x) + f(y)$

۲- $f(xy) = f(x)f(y)$

- اگر f یک به یک باشد آن را تک ریختی گویند — Monomorphism
- اگر f پوشا باشد آن را بروریختی گویند — Epimorphism
- اگر f یک به یک و پوشا باشد آن را یکریختی گویند — Isomorphism
- اگر $R_1 = R_2$ و f یکریختی باشد آن را خودریختی گویند — Automorphism

تعریف:

اگر $f: R_1 \to R_2$ یک همریختی حلقه باشد هسته f (Ker) را با علامت $\ker f$ نشان می‌دهیم به صورت زیر تعریف می‌کنند:

$$\ker f = \{ x \in f \mid f(x) = 0 \}$$

تذکر: با توجه به تعریف بالا نتایج زیر را داریم:

۱- اگر $f: R_1 \to R_2$ همریختی باشد $\Leftarrow$ $f(0) = 0$

برهان: $f(x) = f(x+0) = f(x) + f(0) \longrightarrow f(0) = 0$

۲- $f(-a) = -f(a)$

برهان: $0 = f(a+(-a)) = f(a) + f(-a) \longrightarrow f(-a) = -f(a)$

۳- $\ker f$ یک ایده‌آل R_1 است. $I \trianglelefteq R$ اثبات

برهان: $1.\ \forall x,y \in I \longrightarrow x-y \in I \quad 2.\ \forall r \in R,\ \forall x \in I \quad rx \in I$

$f: R_1 \longrightarrow R_2$

$x,y \in \ker f \longrightarrow f(x-y) = f(x+(-y)) = f(x) + f(-y) = \underbrace{f(x)}_{0} - \underbrace{f(y)}_{0} = 0 \longrightarrow x-y \in \ker f$

$f(\underset{\in R}{r}\underset{\in \ker f}{x}) = f(r)\underbrace{f(x)}_{0} = 0 \longrightarrow rx \in \ker f$

۴- f یک به یک است اگر و تنها اگر $\ker f = 0$

برهان: فرض کنید $\ker f = \{0\}$ ثابت می‌کنیم f یک به یک است

$f(x) = f(y) \longrightarrow f(x) - f(y) = 0 \longrightarrow f(x-y) = 0 \longrightarrow x-y \in \ker f = \{0\}$

f ۱-۱ است. $\longleftarrow x = y \longleftarrow x - y = 0$

قضیه اول یکریختی حلقه‌ها:

فرض کنید R و S دو حلقه باشند و $f: R \longrightarrow S$ یک همریختی حلقه‌ها باشد لذا $\frac{R}{\ker f} \cong \underbrace{\operatorname{Im} f}_{\text{برد تابع}}$

یکریختی حلقه‌ها

قضیه دوم یکریختی حلقه‌ها:

فرض کنید R یک حلقه و I و J ایده‌آل های آن باشند در این صورت

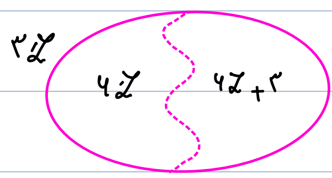
$$\frac{I+J}{I} \cong \frac{J}{I\cap J}$$

مثال:

$$\frac{2\mathbb{Z}+3\mathbb{Z}}{2\mathbb{Z}} \cong \frac{3\mathbb{Z}}{6\mathbb{Z}}$$

$3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$

$6\mathbb{Z} = \{0, \pm 6, \pm 12, \dots\}$



$$\frac{4\mathbb{Z}+6\mathbb{Z}}{4\mathbb{Z}} = \frac{2\mathbb{Z}}{4\mathbb{Z}}$$

نکته:

فرض کنید R یک حلقه باشد و I ایده‌آلی از (R) آن، در این صورت ایده‌آل های $\frac{R}{I}$ به شکل $\frac{J}{I}$ است که $I \subseteq J$ و J ایده‌آل R باشد.

مثال: می‌دانیم $(\mathbb{Z}_{10}, +, \cdot)$ تشکیل حلقه می‌دهند. کلیه ایده‌آل های آن را بدست آورید.

$$\mathbb{Z}_{10} \cong \frac{\mathbb{Z}}{\mathbb{Z}_{10}} \longrightarrow J = m\mathbb{Z} \longrightarrow \begin{cases} m=1 \\ m=2 \\ m=5 \\ m=10 \end{cases}$$

واقعی

قضیه سوم یکریختی حلقه‌ها:

فرض کنید R یک حلقه و I, J ۲ ایده‌آل از آن باشند به طوری که $I \subseteq J$ در این صورت

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

مثال:

$$\frac{4\mathbb{Z}}{28\mathbb{Z}} \cong \mathbb{Z}_7$$

$28\mathbb{Z}+8$ $\quad$ $28\mathbb{Z}$

$0, 4, 8, 12, 16, 20, 24, 28$

$28\mathbb{Z}+4$ $\quad$ تعداد ۷ تا