تقدیم به همسر و فرزند عزیزم سینا

پیش گفتار

در نوشتن این کتاب اهداف زیر مد نظر بوده است.

(۱) ارائه متنی که دانشجویان متوسط با استفاده از آن بتوانند به ادراک عمیقی از جبر مجرد دست یابند،

(۲) حرکتی آهسته و آسان از واقعیت به تجرید،

(۳) آشنایی مختصر با مفاهیم جبری قبل از موعد مقرر،

(۴) آشنایی دانشجویان با شیوهٔ اصل موضوعی، یعنی نحوهٔ استنتاج منطقی از اصول موضوعهٔ معین،

(۵) ایجاد طرز فکر صحیح ریاضی و هدایت دانشجو در جهت تعمیم احکام ریاضی،

(۶) کتابی مناسب جهت داوطلبان شرکت در آزمون‌های کارشناسی ارشد و مسابقات دانشجویی، که در آن ضمن رعایت اختصار، کلیهٔ مطالب ضروری بیان گردیده است.

در پایان هر فصل دو دسته تمرین آورده شده است. دستهٔ اول تمریناتی است که موضوع متن درس را بسط و گسترش می‌دهند. حل این تمرینات برای تسلط یافتن بر مطالب هر فصل مفید است. دستهٔ دوم، تمرینات مبارزه طلب می‌باشند. این تمرینات متناسب با سطح مطالب درسی، دانشجویان مستعد را به مبارزه می‌طلبد و چون حل بعضی از این نوع تمرینات نیاز به نوع‌آوری و خلاقیت دارد، بررسی آنها برای دانشجویان ایجاد انگیزه می‌کند و علاقهٔ دانشجویان را به حل مسائل مشکل تحریک می‌کند.

قطعاً، این کتاب عاری از عیب ونقص نیست امیدوارم همکاران و دانشجویان عزیز از راهنمائیهای ارزشمند خود در جهت رفع نواقص موجود دریغ نفرمایند.

در خاتمه، لازم می‌دانم از همسرعزیزم به خاطر شکیبایی‌اش در زمان نگارش این کتاب تقدیر و تشکر نمایم.

www.mathematic87.blogfa.com

فهرست مطالب

فصل ۱ : گروه‌ها ۱

۱-۱ اعداد صحیح به پیمانه n ۲

۱-۲ حرکت‌ها ۴

۱-۳ عمل دوتایی ۹

۱-۴ ویژگی‌های گروه‌ها ۱۶

۱-۵ زیرگروه‌ها ۱۹

فصل ۲: زیرگروه‌های دوری ۲۹

۲-۱ زیرگروه‌های دوری ۳۰

۲-۲ زیر گروه های یک گروه دوری ۳۳

۲-۳ گروه دایره و ریشه‌های واحد ۳۶

۲-۴ گروه‌های متناهی مولد ۳۸

فصل ۳ : گروه‌های جایگشتی ۴۳

۳-۱ نمایش دو سطری ۴۴

۳-۲ نمایش دوری ۴۶

۳-۳ حاصل ضرب دورها ۴۸

۳-۴ تجزیه به دورها ۴۹

۳-۵ تقارن‌ها ۵۳

www.mathematic87.blogfa.com

فصل ۴: هم‌دسته‌ها و قضیه لاگرانژ ۶۱

۴-۱ هم‌دسته‌ها ۶۲

۴-۲ قضیه لاگرانژ ۶۵

۴-۳ عکس قضیه لاگرانژ ۶۹

۴-۴ قضیه اویلر و قضیه فرما ۷۱

فصل ۵: یکریختی ۷۷

۵-۱ یکریختی ۷۸

۵-۲ قضیه کیلی ۸۴

۵-۳ خودریختی‌ها ۸۶

۵-۴ حاصل‌ضرب‌های مستقیم ۸۸

فصل ۶: زیرگروه‌های نرمال و همریختی‌ها ۱۰۱

۶-۱ زیرگروه‌های نرمال ۱۰۲

۶-۲ همریختی‌ها ۱۱۲

۶-۳ قضایای یکریختی ۱۱۷

۶-۴ ساده بودن $(n \geq 5)A_n$ ۱۲۳

فصل ۷: گروه‌های آبلی متناهی مولد ۱۳۳

۷-۱ قضیهٔ اساسی گروه‌های آبلی متناهی مولد ۱۳۴

۷-۲ مثال‌ها و کاربردها ۱۳۵

۷-۳ اثبات قضیهٔ اساسی گروه‌های آبلی متناهی مولد ۱۳۸

www.mathematic87.blogfa.com

فصل ۸: عمل گروه‌ها و قضایای سیلو ۱۵۳

۸-۱ عمل گروه‌ها ۱۵۴
۸-۲ معادله رده‌ای ۱۵۷
۸-۳ قضایای سیلو ۱۵۹
۸-۴ کاربردهایی از قضایای سیلو ۱۶۶
۸-۵ شمارش مدارها ۱۶۹

فصل ۹: حلقه‌ها ۱۷۹

۹-۱ تعریف‌ها و خواص اساسی ۱۸۰
۹-۲ ایده‌آل‌ها و حلقه‌های خارج قسمتی ۱۹۳
۹-۳ همریختی‌های حلقه ۲۰۳

فصل ۱۰: تجزیه در حلقه‌ها ۲۲۱

۱۰-۱ حلقه چند جمله‌ای ها ۲۲۲
۱۰-۲ حوزه‌های اقلیدسی ۲۲۷
۱۰-۳ میدان کسرها ۲۳۰
۱۰-۴ حوزهٔ تجزیهٔ یکتا ۲۳۲
۱۰-۵ آزمون‌های تحویل‌ناپذیری ۲۴۳

فصل ۱۱: مباحثی پیشرفته‌تر در نظریهٔ حلقه‌ها ۲۵۳

۱۱-۱ مجموعه‌های بسته ضربی ۲۵۴
۱۱-۲ حلقه کسره ۲۵۶
۱۱-۳ رادیکال‌ها ۲۶۱

www.mathematic87.blogfa.com

۱۱-۴ مدول ها..... ۲۶۵

فصل ۱۲: مباحثی پیشرفته‌تر در نظریهٔ گروه‌ها **۲۹۱**

۱۲-۱ سری گروه‌ها..... ۲۹۲
۱۲-۲ گروه‌های حل‌پذیر..... ۲۹۷
۱۲-۳ گروه‌های پوچ‌توان..... ۳۰۱
۱۲-۴ نمایش آزاد گروه‌ها..... ۳۰۶
۱۲-۵ برخی رده‌بندی‌ها..... ۳۱۰

حل تمرینهای فرد **۳۱۹**

فهرست نمادها **۳۵۹**

واژه نامه فارسی به انگلیسی و فهرست راهنما **۳۶۵**

www.mathematic87.blogfa.com

فصل ۱

گروه‌ها

در این فصل می‌خوانید:

۱-۱ اعداد صحیح به پیمانه n
۱-۲ حرکت‌ها
۱-۳ عمل دوتایی
۱-۴ ویژگی‌های گروه‌ها
۱-۵ زیرگروه‌ها

مقدمه

با ساختار مجموعه اعداد صحیح $\mathbb{Z}$ همراه با عمل جمع و همچنین مجموعه ماتریس‌های معکوس‌پذیر 2×2 همراه با عمل ضرب آشنا هستید. اینها مثال‌های آشنایی از یک ساختار جبری به نام گروه می‌باشند. مفهوم گروه یکی از مهم‌ترین مفاهیم ریاضیات می‌باشد که از زمان‌های قدیم، در قالب تقارن اشکال هندسی و حرکت در فضا مطرح بوده است، اما نظریهٔ گروه نوین از کوشش برای پیدا کردن ریشه‌های یک چند جمله‌ای برحسب ضرایب آن پدید آمده است. نظریه گروه‌ها هم اکنون نقشی بسیار اساسی در موضوعاتی از قبیل کدگذاری، ترکیبیات، شمارش و مطالعه تقارن‌ها و همچنین بسیاری از شاخه‌های علوم از قبیل زیست‌شناسی، شیمی و فیزیک ایفا می‌کند.

www.mathematic87.blogfa.com

۱-۱ اعداد صحیح به پیمانه n

همان‌طوری که می‌دانید همنهشتی به پیمانه n یک رابطه هم‌ارزی روی $\mathbb{Z}$ است. مجموعه رده‌های هم‌ارزی مربوطه را با $\mathbb{Z}_n$ نمایش می‌دهیم. این رده‌ها عبارتند از:

$$\overline{0} = [0] = \{nk | k \in \mathbb{Z}\} = \{..., -n, 0, n, ...\}$$
$$\overline{1} = [1] = \{1 + nk | k \in \mathbb{Z}\} = \{..., 1 - n, 1, 1 + n, ...\}$$
$$\vdots \quad \vdots$$
$$\overline{n-1} = [n-1] = \{(n-1) + nk | k \in \mathbb{Z}\} = \{..., -1, n-1, 2n-1, ...\}$$

■ اعمال جمع و ضرب در $\mathbb{Z}_n$

فرض کنید $[a], [b] \in \mathbb{Z}_n$، جمع و ضرب در $\mathbb{Z}_n$ را به صورت زیر تعریف می‌کنیم:

$$[a] +_n [b] = [a + b] \qquad \text{و} \qquad [a] \bullet_n [b] = [ab]$$

نشان می‌دهیم که اعمال $+_n$ و $\bullet_n$ (جمع و ضرب) در $\mathbb{Z}_n$ خوش تعریف می‌باشند. برای این منظور فرض کنید $[a] = [a']$ و $[b] = [b']$. در این‌صورت اعداد صحیح k, k' چنان موجودند که $a = a' + nk$ و $b = b' + nk'$. بنابراین

$$a + b = a' + b' + n(k + k'),$$
$$ab = a'b' + n(a'k' + kb' + nkk').$$

درنتیجه $[a + b] = [a' + b']$ و $[ab] = [a'b']$. یعنی اعمال $+_n$ و $\bullet_n$ در $\mathbb{Z}_n$ خوش تعریف می‌باشند.

گزاره ۱-۱

فرض کنید $[a], [b], [c] \in \mathbb{Z}_n$. در این صورت گزاره‌های زیر در $\mathbb{Z}_n$ برقرارند.

(۱) $[a] +_n [b] = [b] +_n [a]$ (عمل جمع دارای خاصیت جابجایی است)،

$[a] \bullet_n [b] = [b] \bullet_n [a]$ (عمل ضرب دارای خاصیت جابجایی است).

(۲) $([a] +_n [b]) +_n [c] = [a] +_n ([b] +_n [c])$(عمل جمع دارای خاصیت شرکت‌پذیری است)،

www.mathematic87.blogfa.com

$([a]\bullet_n[b])\bullet_n[a]=[a]\bullet_n([b]\bullet_n[c])$(عمل ضرب دارای خاصیت شرکت‌پذیری است).

(۳) $[a]+_n[0]=[a]$ (عمل جمع دارای عنصر خنثی (همانی) می‌باشد)،

$[a]\bullet_n[1]=[a]$(عمل ضرب دارای عنصر خنثی (همانی) می‌باشد).

(۴) $[a]\bullet_n([b]+_n[c])=[a]\bullet_n[b]+_n[a]\bullet_n[c]$ (خاصیت توزیع‌پذیری ضرب روی جمع).

(۵) $[a]+_n[-a]=[0]$ (وجود عنصر قرینه نسبت به عمل جمع).

(۶) عنصر $[a]\in\mathbb{Z}_n$ دارای معکوس ضربی است اگر و فقط اگر $(a,n)=1$.

اثبات: گزاره‌های ۱ تا ۵ بدیهی‌اند. به اثبات گزاره ۶ می‌پردازیم.

(۶): فرض کنید $(a,n)=1$. در این صورت اعداد صحیح $b,r\in\mathbb{Z}$ چنان موجودند که $ab+nr=1$. بنابراین $[ab]=[1]$ و در نتیجه $[a]\bullet_n[b]=[ab]=[1]$. برعکس، فرض کنید $[a]$ دارای معکوس ضربی باشد. یعنی $[b]\in\mathbb{Z}_n$ به‌گونه‌ای موجود است که $[a]\bullet_n[b]=[1]$. از اینرو برای یک $r\in\mathbb{Z}$، خواهیم داشت $ab=nr+1$، و لذا $(a,n)=1$.

■■■

تذکر: اگر جای هیچ گونه ابهامی نباشد، برای راحتی کار از نوشتن اندیس n برای $\bullet_n,+_n$ صرف نظر می‌کنیم. همچنین $[a]$ را با a نمایش می‌دهیم.

مثال۱: جدول زیر عمل ضرب در $\mathbb{Z}_8$ را به طور کامل نشان می‌دهد.

$\mathbb{Z}_8$

$\bullet$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

www.mathematic87.blogfa.com

همان‌طوری که از جدول مشاهده می‌شود عناصر $4,2,0$ و 6 معکوس ضربی ندارد.

■

۱- ۲ حرکت‌ها

■ جایگشت‌ها

تعریف ۱- ۱ (جایگشت)

فرض کنید X یک مجموعه ناتهی باشد. تابع یک به یک و پوشای $\delta : X \to X$ را یک **جایگشت** از X گوییم. مجموعه تمام جایگشت‌های X را با S_X نمایش می‌دهیم.

❖ **تذکر:** در صورتی که $X = \{1,2,...,n\}$ به جای S_X از نماد S_n استفاده می‌کنیم.

مثال۲: اگر $X = \{1,2\}$ آنگاه، عناصر $S_2 = S_X$ عبارتند از:

$$\delta_1 : \begin{cases} 1 \to 1 \\ 2 \to 2 \end{cases} \qquad \delta_2 : \begin{cases} 1 \to 2 \\ 2 \to 1 \end{cases}$$

■

مثال۳: عناصر S_3 عبارتند از:

$$\delta_1 : \begin{cases} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{cases} \quad \delta_2 : \begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases} \quad \delta_3 : \begin{cases} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{cases}$$

$$\delta_4 : \begin{cases} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{cases} \quad \delta_5 : \begin{cases} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{cases} \quad \delta_6 : \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases}$$

■

www.mathematic87.blogfa.com

در حالت کلی اگر $X = \{x_1, x_2, ..., x_n\}$ آنگاه $\delta \in S_X$ مشخص است اگر و فقط اگر $\delta(x_i)$ برای هر $1 \le i \le n$ مشخص باشد. بنابراین راه ساده‌تر برای نمایش دادن $\delta \in S_X$ این است که اعضای $x_n, ..., x_2, x_1$ را به ترتیب در سطری بین دو پرانتز قرار داده، سپس زیر هر عنصر تصویر آن را تحت δ می‌نویسیم. یعنی:

$$\delta = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \delta(x_1) & \delta(x_2) & \dots & \delta(x_n) \end{pmatrix}$$

به عنوان مثال δ_5 و δ_6 مثال فوق را می‌توان چنین نوشت:

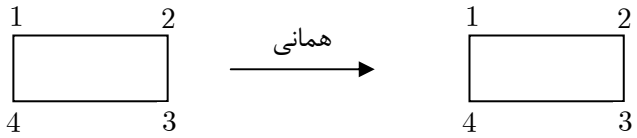
$$\delta_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ و } \delta_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

■ حرکت‌های یک شکل هندسی

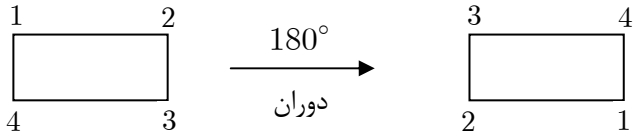
تعریف ۱- ۲

منظور از یک **شکل هندسی**، مجموعه‌ای از نقاط موسوم به رئوس است که بعضی از آنها دو به دو به کمک خط‌های مستقیم به هم متصل شده باشند. منظور از یک **حرکت** از یک شکل هندسی، جایگشتی است از مجموعهٔ رئوس آن که توسط حرکت صلبی در فضا معین می‌شود.

مثال۴: فرض کنید F یک مستطیل و $X = \{1,2,3,4\}$ مجموعه رئوس این مستطیل باشد. مجموعه حرکت‌های این شکل هندسی با نماد K_4 نمایش داده می‌شود. عناصر K_4 عبارتند از:

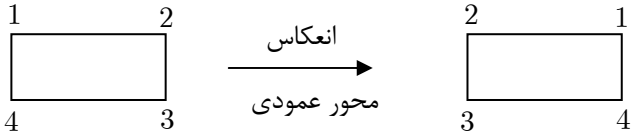


$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

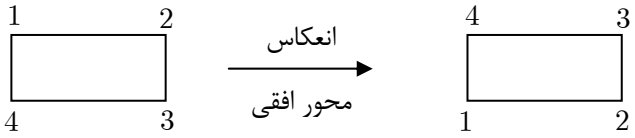


$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

www.mathematic87.blogfa.com



$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$



$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

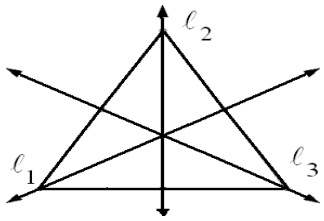
■

تذکر: توجه داشته باشیم که دوران به اندازه $90°$ یک حرکت نمی‌باشد مگر این که چهار ضلعی مربع باشد.

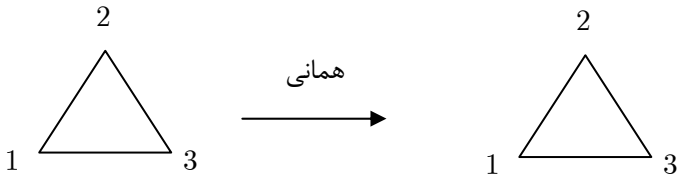
مثال ۵ : فرض کنید F یک مثلث متساوی الا ضلاع باشد. F دارای دو نوع حرکت است:

نوع اول: دوران به اندازه زاویه‌های $0°, 120°$ و $240°$ در جهت عقربه‌های ساعت.

نوع دوم: انعکاس نسبت به خطوط (نیمسازهای) ℓ_1, ℓ_2 و ℓ_3. (شکل زیر ملاحظه شود).

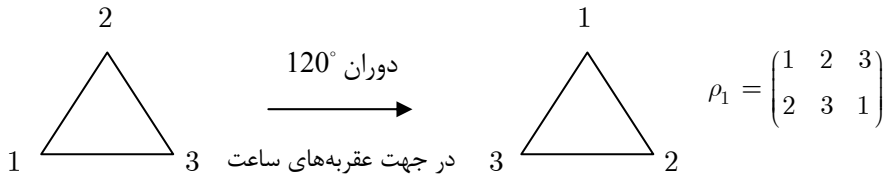


حال فرض کنید $X = \{1,2,3\}$ مجموعه رئوس این مثلث باشد. حرکت‌های این شکل هندسی عبارتند از:

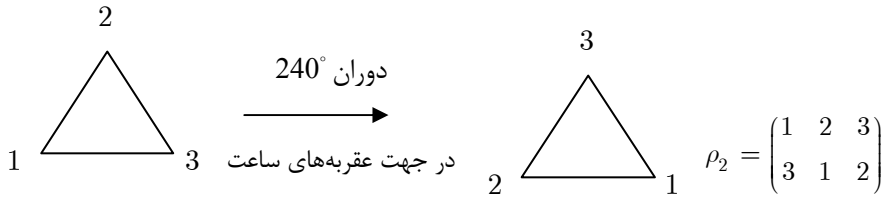


$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

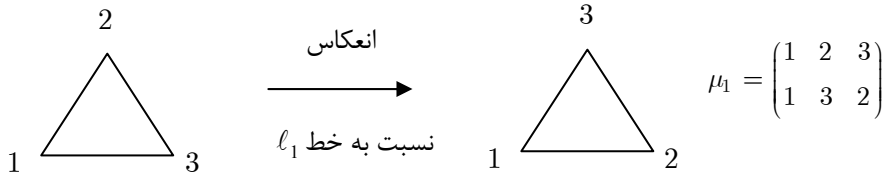
www.mathematic87.blogfa.com



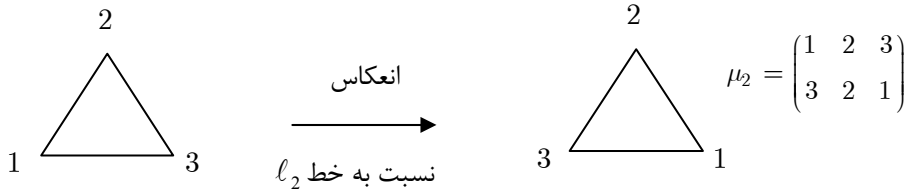
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$



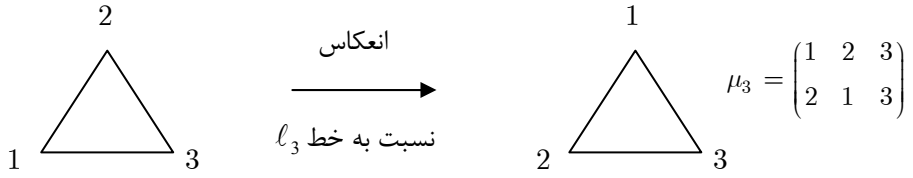
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

همان طوری که ملاحظه می‌شود هر جایگشت از $X = \{1,2,3\}$، یا به عبارت معادل هر عنصر S_3، یک حرکت از F است، یعنی:

www.mathematic87.blogfa.com

مجموعه حرکت‌های مثلث متساوی‌الاضلاع $= S_3$

خواننده باید توجه داشته باشد که این مطلب در مورد حرکت‌های یک مستطیل برقرار نمی‌باشد.

به‌وضوح مشاهده می‌شود که ترکیب دو حرکت یک حرکت است. به عنوان مثال $\mu_1\rho_1$ را می‌یابیم.

$$(\mu_1\rho_1)(1) = \mu_1(\rho_1(1)) = \mu_1(2) = 3,$$
$$(\mu_1\rho_1)(2) = \mu_1(\rho_1(2)) = \mu_1(3) = 2,$$
$$(\mu_1\rho_1)(3) = \mu_1(\rho_1(3)) = \mu_1(1) = 1.$$

یعنی $\mu_1\rho_1 = \mu_2$. جدول زیر قانون ترکیب حرکت‌های F را به طور کامل نشان می‌دهد.

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

به آسانی از جدول مشاهده می‌شود که برای هر $\alpha \in S_3$، عنصر $\alpha' \in S_3$ چنان موجود است که $\alpha\alpha' = \alpha'\alpha = \mathrm{id}$. همچنین قانون ترکیب در S_3 دارای خاصیت جابجایی نیست. مثلاً $\rho_1\mu_1 \neq \mu_1\rho_1$.

■

▼ **یادداشت:** مجموعه اعداد صحیح به پیمانه n (یعنی $\mathbb{Z}_n$) همراه با عمل جمع، مجموعه حرکت‌های مستطیل (یعنی K_4) و مثلث متساوی‌الاضلاع (یعنی S_3) همراه با عمل ترکیب توابع مثال‌هایی از گروه می‌باشند. اکنون به تعریف دقیق گروه می‌پردازیم:

www.mathematic87.blogfa.com

۱-۳ عمل دوتایی

تعریف ۱- ۳ (عمل دوتایی)

اگر G یک مجموعه ناتهی باشد، یک **عمل دوتایی** بر G تابعی است مانند $* : G \times G \to G$. معمول است که نقش (x,y) تحت این عمل دوتایی، یعنی $*(x,y)$ ، با $x * y$ نمایش داده شود.

برای نشان دادن نقش (x,y) در صورتی که صحبت از یک عمل دوتایی نامعینی باشد، نمادهای مختلفی به کار می‌روند:

xy (نماد ضربی)، $x + y$ (نماد جمعی)، $x.y$، $x \circ y$ و غیره. برای راحتی در سراسر این کتاب عموماً از نماد ضربی استفاده می‌کنیم و xy را **حاصل ضرب** y, x می‌نامیم. بر یک مجموعه ممکن است چند عمل دوتایی تعریف شده باشد، (مثلاً جمع و ضرب معمولی در $\mathbb{Z}$ که به ترتیب با $(x,y) \mapsto x + y$ و $(x,y) \mapsto xy$ داده می‌شوند).

مثال۶ : عمل ضرب روی $\mathbb{R}$، مجموعه اعداد حقیقی، که به ازای هر $x, y \in \mathbb{R}$ به صورت $x.y = |x + y|$ تعریف می‌شود یک عمل دوتایی روی $\mathbb{R}$ است.

■

تعریف ۱- ۴

فرض کنید A و B دو زیر مجموعه از مجموعهٔ X باشند **تفاضل متقارن** A و B چنین تعریف می‌شود:

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

مثال ۷ : فرض کنید X یک مجموعه دلخواه و $G = P(X)$ مجموعه زیر مجموعه‌های X باشد. اعمال $\cup$ (اجتماع) و $\cap$ (اشتراک) و Δ (تفاضل متقارن) اعمال دوتایی روی مجموعه G هستند.

■

تعریف ۱- ۵ (نیم گروه)

یک **نیم گروه** عبارت است از مجموعه‌ای ناتهی مانند G همراه با عملی دو تایی بر G که:

شرکت‌پذیر (یا **انجمنی**) باشد. یعنی

$$x(yz) = (xy)z \qquad \forall x, y, z \in G$$

تعریف ۱- ۶ (تکوار)

یک **تکوار** (یا **مونوئید**) عبارت است از یک نیم گروه G که شامل یک عنصر $e \in G$ است به طوری که

$$xe = ex = x, \quad \forall x \in G$$

این عنصر e را یک **عنصر همانی** (دوطرفه) برای تکوار G می‌نامند.

■ گروه

تعریف ۱- ۷ (گروه)

یک **گروه** عبارت است از یک تکوار G به طوری که به ازای هر $x \in G$ یک $y \in G$ وجود داشته باشد

طوری که $xy = yx = e$.

تعریف ۱- ۸ (گروه آبلی)

گروه G را **آبلی** یا **جابجایی** گوییم اگر به ازای هر $x, y \in G$ $xy = yx$ و در غیر این صورت G را یک گروه **غیر آبلی** یا **غیر جابجایی** می‌نامند.

اصطلاح گروه آبلی به یادبود ریاضی دان، N. Abel مورد استفاده قرار می‌گیرد.

❖ **تذکر:** نیم گروه آبلی نیز به طریق مشابه تعریف می‌گردد.

تعریف ۱- ۹ (مرتبه یک گروه)

مرتبه یک گروه G عبارت است از عدد اصلی (کاردینال) مجموعه G که آن را با $|G|$ نمایش می‌دهند. اگر $|G|$ متناهی باشد، G را یک **گروه متناهی** و در غیر این صورت آن را یک **گروه نامتناهی** می‌نامند.

■ مثال‌هایی از نیم گروه

هرگاه یک عمل دوتایی معین $*$ روی یک نیم گروه G تعریف شده باشد به منظور مشخص کردن این که G دارای عمل دوتایی $*$ است، آن را با $(G,*)$ نشان می‌دهیم.

مثال ۸ : اعمال جمع و ضرب معمولی روی مجموعه‌ای $\mathbb{C},\mathbb{R},\mathbb{Q},\mathbb{Z},\mathbb{N}$ اعمال دو تایی‌اند، مجموعه‌های فوق همراه با این اعمال دوتایی نیم گروه‌های آبلی هستند.

■

مثال۹: $\mathbb{Z}_n$ همراه با هر یک از اعمال جمع و ضرب تشکیل نیم گروه آبلی می‌دهد. به عبارت معادل $(\mathbb{Z}_n,+_n),(\mathbb{Z}_n,\bullet_n)$ نیم گروه‌های آبلی‌اند.

■

مثال۱۰: S_3 همراه با عمل ترکیب یک نیم گروه غیر آبلی است.

■

مثال۱۱: به ازای یک مجموعه دلخواه $X, P(X)$ همراه با هر یک از اعمال $\cup$ (اجتماع)، $\cap$ (اشتراک)، Δ (تفاضل متقارن) یک نیم گروه است.

■

مثال۱۲: هیچ یک از مجموعه‌های مثال ۸ همراه با عمل تفریق یک نیم گروه نمی‌باشد.

■

■ مثال‌هایی از تکوار

مثال۱۳: فرض کنید X یک مجموعه ناتهی باشد. مجموعه $\mathrm{Map}(X,X)$ را چنین تعریف می‌کنیم:

$$\mathrm{Map}(X,X)=\{f|f:X\to X\}$$

به سادگی می‌توان بررسی کرد که $\mathrm{Map}(X,X)$ همراه با عمل ترکیب توابع یک نیم گروه است. نگاشت id که به صورت $\mathrm{id}(x)=x$ برای تمام $x\in X$ تعریف می‌شود عنصر خنثی $\mathrm{Map}(X,X)$ بوده و در نتیجه $\mathrm{Map}(X,X)$ یک تکوار است.

■

❖ **تذکر:** $\mathrm{Map}(X,X)$ لزوماً یک گروه نیست. چرا؟

مثال ۱۴: مجموعه اعداد صحیح زوج همراه با عمل ضرب یک نیم گروه می‌باشد، در صورتی که یک تکوار نیست.

■

■ مثال‌هایی از گروه‌ها

مثال۱۵: هر یک از مجموعه‌های $\mathbb{C},\mathbb{R},\mathbb{Q},\mathbb{Z}$ همراه با عمل جمع، و همچنین هر یک مجموعه‌های $\mathbb{Q}^*=\mathbb{Q}-\{0\},\mathbb{R}^*=\mathbb{R}-\{0\}$ و $\mathbb{C}^*=\mathbb{C}-\{0\}$ همراه با عمل ضرب یک گروه آبلی نامتناهی‌اند.

■

مثال۱۶: مجموعه حرکت‌های مثلث متساوی‌الاضلاع، S_3، همراه با عمل ترکیب توابع مثال آشنایی از یک گروه غیر آبلی متناهی است.

■

مثال۱۷: مجموعه حرکت‌های مستطیل،یعنی K_4، یک گروه آبلی 4 عنصری است. این گروه به **چهارتایی کلاین** معروف است. (بعضی از کتب این گروه را با نماد V برگرفته از لغت آلمانی Vieregruppe به معنی چهار-گروه نمایش می‌دهند).

www.mathematic87.blogfa.com

■

مثال۱۸: در حالت کلی S_n همراه با عمل ترکیب توابع یک گروه است. S_n را گروه **متقارن درجه** n می‌گوییم.

■

به علت این که یک گروه یک مجموعه همراه با عمل دو تایی است، یک گروه متناهی را می‌توان توسط جدول ضرب آن **(جدول کیلی)** به طور کامل مشخص کرد. به کار بردن اصطلاح جدول کیلی در این مورد متداول‌تر است. این اصطلاح به نام آرتورکیلی، ریاضیدانی که پیشتاز استفاده از چنین جدول‌هایی است، می‌باشد. در این جا مثالی از جدول کیلی $(\mathbb{Z}_5,+)$ ارایه می‌دهیم:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

مثال۱۹ : $\mathbb{Z}_n$ با عمل ضرب گروه نیست، چرا که 0 دارای معکوس ضربی نیست. در حقیقت برای هر $k \in \mathbb{Z}_n$ داریم $0.k = k.0 = 0$. در حالت کلی حتی اگر 0 را از $\mathbb{Z}_n$ برداریم، باز هم مجموعه حاصل یعنی، $\mathbb{Z}_n - \{0\}$ همراه با عمل ضرب گروه نیست. به عنوان مثال $2 \in \mathbb{Z}_6$ دارای معکوس ضربی نیست.

■

مثال۲۰ : مجموعه همه عناصر ناصفر $\mathbb{Z}_n$ که دارای معکوس ضربی‌اند با عمل ضرب تشکیل یک گروه می‌دهند. این گروه را با $U(n)$ نشان می‌دهیم و آن را گروه **یکال‌های** $\mathbb{Z}_n$ می‌نامیم. جدول زیر، جدول کیلی گروه $U(8)$ می‌باشد.

www.mathematic87.blogfa.com

•	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

■

مثال۲۱ : فرض کنید $\mathrm{M}_2(\mathbb{R})$ نشان دهنده همه ماتریس‌های 2×2 با درایه‌های حقیقی باشد. $\mathrm{M}_2(\mathbb{R})$ همراه با عمل جمع ماتریسها یک گروه آبلی است. زیر مجموعه $\mathrm{GL}_2(\mathbb{R})$ از $\mathrm{M}_2(\mathbb{R})$ را به صورت زیر تعریف می‌کنیم:

$$\mathrm{GL}_2(\mathbb{R})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| ad-bc\neq 0\right\}.$$

یعنی ماتریس‌های 2×2 ای که دترمینان آنها غیرصفراند (ماتریس‌های معکوس‌پذیر). به آسانی می‌توان دید که $\mathrm{GL}_2(\mathbb{R})$ همراه با عمل ضرب ماتریس‌ها تشکیل یک گروه می‌دهد (البته یک گروه غیر آبلی). این گروه را **گروه خطی عمومی از درجه ۲** روی میدان اعداد حقیقی $\mathbb{R}$ می‌نامیم.

زیر مجموعه $\mathrm{SL}_2(\mathbb{R})$ از $\mathrm{GL}_2(\mathbb{R})$ را به صورت زیر تعریف می‌کنیم:

$$\mathrm{SL}_2(\mathbb{R})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| ad-bc=1\right\}$$

$\mathrm{SL}_2(\mathbb{R})$ همراه با عمل ضرب ماتریس‌ها یک گروه می‌باشد. این گروه را گروه **خطی ویژه ازدرجه ۲** روی میدان اعداد حقیقی $\mathbb{R}$ می‌نامیم.

■

❖ **تذکر:** $\mathrm{M}_n(R)$، $\mathrm{GL}_n(R)$ و $\mathrm{SL}_n(R)$، که R می تواند یکی از مجموعه‌های $\mathbb{C},\mathbb{Q},\mathbb{R}$ یا $\mathbb{Z}_n$ باشد، به طریق مشابه تعریف می‌شوند.

مثال۲۲ : فرض کنید

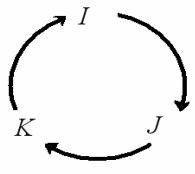
www.mathematic87.blogfa.com

$$I=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \text{ و } 1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$
$$K=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} \text{ و } J=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

که در این جا $i^2=-1$. به آسانی می‌توان مشاهده کرد که روابط زیر برقرارند:

$$I^2=J^2=K^2=-1,\ JK=I,\ KI=J,\ JI=-K,\ \ KJ=-I,\ \ IK=-J.$$

مجموعه $\{\pm 1,\pm I,\pm J,\pm K\}$ یک گروه است، که گروه **کواترنیون** از مرتبهٔ 8 نامیده و با علامت Q نمایش می‌دهیم. به سادگی می‌توان فرمول‌های بالا را به خاطر سپرد. حاصل‌ضرب هر دو عنصر متوالی در جهت عقربه‌های ساعت عنصر بعدی آنها است و حاصل‌ضرب هر دو عنصر متوالی در جهت خلاف عقربه‌های ساعت منفی عنصر بعدی است. (شکل زیر ملاحظه شود).



■

▼ **یادداشت:** هرگاه G یک تکوار بوده و عمل دوتایی آن به صورت جمع نوشته شود، آنگاه:

(۱) عنصر همانی با 0 نمایش داده می‌شود،

(۲) معکوس $x\in G$ با $-x$ نشان داده می‌شود،

(۳) برای هر $x,y\in G$ قرار می‌دهیم $x-y:=x+(-y)$.

نوعی توافق محترمانه هم وجود دارد که نماد $+$ فقط برای عمل‌های آبلی (جابجایی) به کار می‌رود. مشاهده $a+b\neq b+a$ برای یک جبردان بسیار ناراحت کننده است و در حقیقت به خاطر همین است که اگر عمل ما معین نباشد از نماد ضربی استفاده می‌کنیم.

www.mathematic87.blogfa.com

۱-۴ ویژگی‌های گروه‌ها

هر چند توجه اصلی ما به گروه‌ها است. با این حال برای بیان قضایا در منتهای کلیت، نیم‌گروه‌ها و تکوار ها مناسب می‌باشند.

قضیه ۱-۱(یکتایی عنصر همانی

اگر G یک تکوار باشد، آنگاه عنصر همانی e منحصر به فرد است.

اثبات: هرگاه e', e دو عنصر همانی دو طرفه باشند، آنگاه $e = ee' = e'$.

■■■

تعریف ۱- ۱۰ (معکوس)

فرض کنید G یک تکوار باشد.

(۱) اگر برای $x \in G$ عنصر $x' \in G$ چنان موجود باشد که $xx' = e$ ($x'x = e$) آنگاه x' را یک **معکوس راست (چپ)** x نامیم،

(۲) اگر برای $x \in G$ عنصر $y \in G$ چنان موجود باشد که $xy = yx = e$ آنگاه y را یک **معکوس** (دوطرفه) x نامیم. اگر $x \in G$ دارای معکوس باشد، آنگاه این عنصر را **معکوس‌پذیر** گوییم.

قضیه ۱-۲(یکتایی معکوس)

فرض کنید G یک تکوار باشد.

(۱) اگر $x \in G$ دارای معکوس راست x' و معکوس چپ x'' باشد، آنگاه $x' = x''$،

(۲) $x \in G$ معکوس‌پذیر است اگر و فقط اگر x دارای معکوس راست وچپ باشد،

(۳) اگر $x \in G$ دارای معکوس باشد، آنگاه این معکوس یکتا است.

اثبات (۱): $x'' = x''e = x''(xx') = (x''x)x' = ex' = x'$.

(۲) به آسانی از قسمت (۱) نتیجه می‌شود.

(۳): فرض کنید x' و x'' معکوس های x باشند. بنابراین داریم:

$$y' = y'e = y'(xy'') = (y'x)y'' = ey'' = y''.$$

www.mathematic87.blogfa.com

■■■

نمادگـــذاری: فـرض کنیـد G یـک تکـوار و $x \in G$ دارای معکـوس باشـد. در این‌صورت معکوس یکتای x را با x^{-1} نشان می‌دهیم.

قضیه ۱-۳ (ویژگی معکوس‌ها)

فرض کنید G یک تکوار و $x \in G$ دارای معکوس باشد. در این‌صورت

(۱) $(x^{-1})^{-1} = x$،

(۲) $(xy)^{-1} = y^{-1}x^{-1}$.

اثبـــات (۱): چـون $xx^{-1} = x^{-1}x = e$ و معکـوس x^{-1} منحـصر بـه فـرد اسـت، پس $\left(x^{-1}\right)^{-1} = x$.

(۲):

$$(xy)\left(y^{-1}x^{-1}\right) = x\left(yy^{-1}\right)x^{-1} = xex^{-1} = xx^{-1} = e$$

به طریق مشابه داریم $\left(y^{-1}x^{-1}\right)(xy) = e$. بنابراین $(xy)^{-1} = y^{-1}x^{-1}$.

■■■

قضیه ۱-۴ (قوانین حذف)

فرض کنید G یک گروه و $x, y, g \in G$.

(۱) (قانون حذف از چپ) $gx = gy \Rightarrow x = y$،

(۲) (قانون حذف از راست) $xg = yg \Rightarrow x = y$.

اثبـــــات: فـــــرض کنیـــــد $gx = gy$. بنـــــابراین $g^{-1}(gx) = g^{-1}(gy)$. در نتیجه $\left(g^{-1}g\right)x = \left(g^{-1}g\right)y$، یعنی $x = y$. با برهانی مشابه قانون حـذف از راسـت نیـز برقرار است.

■■■

■ حاصل ضرب‌ها

در یک نیم گروه G فقط می‌توانیم دو عنصر را، به یک باره در هم ضرب کنیم. اکنون این پرسش پیش می‌آید که آیا می‌توانیم تعداد بیشتری را نیز در هم ضرب کنیم؟ برای انجام این کار باید با به کار بردن پرانتزها به طور پی در پی در هر بار زوجی از اعضا را در هم ضرب کنیم. در واقع به خاطر وجود قانون شرکت‌پذیری نتیجه به دست آمده مستقل از نحوه قرار دادن پرانتزها است. به عنوان مثال برای عبارت $xyzw$ پنج روش پرانتزگذاری وجود دارد که عبارتند از:

$$x(y(zw)),\ x((yz)w),\ (xy)(zw),\ (x(yz))w,\ ((xy)z)w$$

به سادگی می‌توان نشان داد که همگی این پنج حاصل ضرب مساویند. در حالت کلی در این مورد قضیه زیر وجود دارد که اثبات آن به استقرای ریاضی است که به عهده خواننده واگذار می‌شود.

قضیه ۱-۵

فرض کنید G یک نیم گروه و $x_1,...,x_n \in G$. در این صورت عبارت $x_1x_2...x_n$ مستقل از روش پرانتزگذاری برای محاسبه آن است.

■ توان‌ها

فرض کنید G یک تکوار و $x \in G$. قرار می‌دهیم $x^0 = e$ و برای هر $n \in \mathbb{N}$ تعریف می‌کنیم:

$$x^n = \underbrace{x...x}_{n\text{ مرتبه}}.$$

در ضمن اگر x دارای معکوس x^{-1} باشد، برای هر $n \in \mathbb{N}$ تعریف می‌کنیم:

$$x^{-n} = \underbrace{x^{-1}...x^{-1}}_{n\text{ مرتبه}}.$$

توجه داشته باشید که این تعاریف با توجه به قضیه فوق خوش تعریف‌اند.

www.mathematic87.blogfa.com

❖ **تذکر:** وقتی عمل دوتایی به صورت جمع نوشته شده باشد به جای x^n می‌نویسیم nx لذا:

$$\begin{aligned} 0x &= 0, \\ 1x &= x, \\ &\vdots \\ nx &= (n-1)x + x. \end{aligned}$$

قضیه ۱-۶

هرگاه G گروه (نیم گروه یا تکوار) بوده و $x \in G$ آنگاه به ازای هر $m,n \in \mathbb{Z}$.

(۱) $x^m x^n = x^{m+n}$ (با نماد جمعی: $mx + nx = (m+n)x$)،

(۲) $(x^m)^n = x^{mn}$ (با نماد جمعی: $n(mx) = mnx$).

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

۱- ۵ زیرگروه‌ها

بعضی مواقع خواهان بررسی گروه‌های کوچکی که جزء گروه بزرگتری هستند می‌باشیم. برای مثال، گروه $\mathbb{Z}$ تحت عمل جمع جزء گروه $\mathbb{Q}$ تحت عمل جمع است که خود جزء گروه $\mathbb{R}$ تحت عمل جمع می‌باشد. وقتی که گروه $(\mathbb{Z},+)$ را به عنوان جزئی از $(\mathbb{R},+)$ در نظر می‌گیریم، توجه بدین نکته بسیار مهم است که عمل $+$ روی دو عدد صحیح n,m به عنوان عناصر $(\mathbb{Z},+)$ همان عمل جمع دو عدد حقیقی n,m به عنوان عناصر $(\mathbb{R},+)$ می‌باشد. به عبارت دیگر ما نه تنها لازم می‌دانیم که مجموعه گروه کوچکتر جزء مجموعه گروه بزرگتر باشد، بلکه می‌خواهیم عمل گروه روی هر دو مجموعه کوچک و بزرگ به طور یکسان عمل کند. حال به تعریف دقیق این مفاهیم می‌پردازیم.

www.mathematic87.blogfa.com

تعریف ۱-۱۱

فرض کنید G یک گروه و $H \neq \varnothing, H \subseteq G$. گوییم H یک **زیر گروه** G است اگر H همراه با عمل دوتایی G یک گروه باشد. در چنین حالتی می‌نویسیم $H \leq G$. خود G و زیر گروه $\{e\}$ مرکب از عنصر همانی زیرگروه‌های G هستند که **زیر گروه‌های بدیهی** G نامیده می‌شوند. اگر H زیرگروهی از G باشد و $H \neq G$ آنگاه H را یک **زیر گروه سره (حقیقی)** G می‌نامیم و می‌نویسیم $H < G$.

مثال ۲۳ : $H = \{1, -1, i, -i\}$ یک زیر گروه از $\mathbb{C}^*$ است. یادآوری می‌کنیم که $\mathbb{C}^*$ گروه ضربی اعداد مختلط ناصفر است.

■

مثال۲۴ : $\mathrm{SL}_2(\mathbb{R})$ یک زیرگروه از $\mathrm{GL}_2(\mathbb{R})$ است.

■

▼ **یادداشت:** یکی از روش‌های بررسی این که آیا دو گروه یکسان هستند یا خیر، بررسی زیر گروه‌های آنها می‌باشد. برای روشن شدن مطلب به مثال زیر توجه کنید:

مثال۲۵ : فرض کنید $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(a,b) | a,b \in \mathbb{Z}_2\}$ عمل دوتایی روی G را به صورت جمع مؤلفه‌وار تعریف می‌کنیم، یعنی $(a,b) + (c,d) = (a+c, b+d)$.
به آسانی می‌توان ملاحظه نمود که زیر گروه‌های غیر بدیهی G عبارتند از:

$$H_1 = \{(0,0),(0,1)\}, H_2 = \{(0,0),(1,0)\}, H_3 = \{(0,0),(1,1)\}$$

با توجه به این که $H = \{0,2\}$ تنها زیر گروه غیر بدیهی $\mathbb{Z}_4$ است، لذا $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4$ دو گروه متفاوت چهار عنصری‌اند. این که آیا دو گروه از نظر ساختاری مانند هم هستند یا خیر به مفهوم یکریختی منجر می‌شود که در فصل‌های بعدی مورد بحث قرار می‌گیرد.

■

هرگاه G یک گروه و $H \subseteq G$ داده شده باشد مناسب است آزمون ساده‌ای برای تعیین این که آیا H زیر گروهی از G هست یا نه داشته باشیم. اما چون G یک گروه است لازم

www.mathematic87.blogfa.com

نیست تمام شرایط مربوط به گروه را در مورد H بررسی کنیم. مثلاً قانون شرکت‌پذیری در مورد هر سه عنصر G برقرار است و لذا برای هر سه عنصر H نیز برقرار است در زیر شرط لازم و کافی برای این که H زیر گروهی از G باشد آورده می‌شود.

قضیه ۱-۷ (آزمون اول زیرگروه)

زیر مجموعه H از گروه G یک زیرگروه G است اگر و فقط اگر احکام زیر برقرار باشند.

(۱) عنصر همانی e از G به H تعلق داشته باشد،

(۲) H تحت عمل G بسته باشد،

(۳) برای هر $h \in H$ داشته باشیم $h^{-1} \in H$.

اثبات: فرض کنید H یک زیر گروه G باشد. فرض کنید e_H عنصر همانی گروه H باشد. داریم $ee_H = e_H = e_H e_H$ و طبق قانون حذف از راست (در G) خواهیم داشت $e = e_H$. بنابراین شرط (۱) برقرار می‌باشد. در ضمن شرایط (۲) و (۳) طبق تعریف برقرارند. برعکس، اگر H در سه شرط داده شده صدق کند، به وضوح H یک زیر گروه G می‌باشد.

■■■

نتیجه۱-۱

مجموعه حرکت‌های یک شکل هندسی که دارای n رأس می‌باشد، زیرگروهی از S_n است.

اثبات: اگر τ, δ دو حرکت از یک شکل باشند، $\delta\tau$ نیز حرکتی است که با اعمال τ سپس δ به دست می‌آید. همچنین δ^{-1} عکس حرکت δ است. سرانجام، جایگشت همانی id نیز یک حرکت (حاصل از ثابت ماندن رئوس) است.

■■■

آزمون فوق را می‌توان به صورت فشرده‌تر به صورت زیر مطرح ساخت.

www.mathematic87.blogfa.com

قضیه ۱-۸ (آزمون دوم زیرگروه)

فرض کنید H زیر مجموعه‌ای ناتهی در گروه G باشد. در این صورت H یک زیر گروه G است اگر و فقط اگر به ازای هر $h_1, h_2 \in H$ داشته باشیم $h_1 h_2^{-1} \in H$.

اثبات: فرض کنیم $H \leq G$. در این حالت اگر $h_1, h_2 \in H$، آنگاه $h_2^{-1} \in H$ و لذا $h_1 h_2^{-1} \in H$.

برعکس، چون $H \neq \phi$ پس $h \in H$ ای موجود است و از این رو $e = hh^{-1} \in H$، پس شرط (۱) در قضیه فوق برقرار است. حال فرض کنید $h \in H$، در این صورت با توجه به این که $e \in H$ خواهیم داشت $eh^{-1} = h^{-1} \in H$ یعنی شرط(۳) قضیه فوق برقرار است. حال فرض کنید $h_1, h_2 \in H$ پس $h_2^{-1} \in H$ و بنابراین $h_1 \left(h_2^{-1}\right)^{-1} \in H$. به عبارت دیگر $h_1 h_2 \in H$، یعنی شرط(۲) قضیه فوق نیز برقرار است.

■■■

توضیح تاریخی

هر چند که اولین تعریف گروه، به وسیله اصول موضوعه، درسال 1981توسط وبرا مطرح گردید، اما روش‌های نظریهٔ- گروه‌ها خیلی پیشتر برای بسط بسیاری از شاخه‌های ریاضیات از قبیل هندسه و نظریه معادلات جبری به کار گرفته شده بود.

لاگرانژ برای حل معادلات چند جمله‌ای، در سال 1771 – 1770 از روش‌های نظریهٔ- گروه‌ها استفاده کرده بعد از آن گالوا تشخیص داد که چه نوعی از معادلات چند جمله‌ای برحسب ضرایب قابل حل‌اند. لازم به ذکر است که ابزار اصلی گالوا نظریهٔ- گروه‌ها بوده است.

در سال 1872 کلاین با طرح این مطلب که، برای مطالعه فضاهای هندسی باید خواصی که تحت تبدیلاتی از فضا پایا هستند، مورد بررسی قرار گیرد، انقلابی در هندسه به پا کرد (تبدیلات تشکیل گروه می‌دهند). لی معاصر کلاین نیز در مطالعه معادلات دیفرانسیل با مشتقات جزیی از نظریهٔ- گروه‌ها استفاده کرده است. به عنوان اولین

www.mathematic87.blogfa.com

مرجع کاملی که به بررسی مدرن نظریهٔ- گروه‌ها پرداخته می‌توان به کتاب برنساید (مرجع زیر) اشاره داشت، اولین چاپ این کتاب در سال 1897 می‌باشد.

Burnside, W. *Theory of Groups of Finite Order*. 2 nd ed. Cambridge University Press, Cambridge, 1911 ; Dover, New York. A Classic. 1953.

تمرینها

۱. کدامیک از مجموعه‌های زیر همراه با عمل مشخص شده یک نیم‌گروه، تکوار یا گروه است، دلیل بیاورید.

(a) عمل * در $G = \mathbb{N} - \{1,2\}$ با تعریف $x * y = 2x + y - xy$،

(b) عمل * در $G = \{a \in \mathbb{R} | -1 < a < 1\}$ با تعریف $x * y = (x + y)/(1 + xy)$،

(c) عمل * در $G = \mathbb{Q} - \{-1\}$ با تعریف $x * y = x + y + xy$،

(d) مجموعهٔ ماتریسهای بالا مثلثی که روی قطر آنها صفر است و عمل ضرب ماتریسها.

۲. کدامیک از جدول ضربهای زیر روی مجموعهٔ $G = \{a,b,c,d\}$ تشکیل یک گروه می دهند، دلیل بیاورید.

(a)

$*$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

www.mathematic87.blogfa.com

(c)

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

۳. مطلوب است جدول کیلی $(\mathbb{Z}_4,+)$ و گروه حرکت‌های مستطیل. آیا این دو گروه یکی اند.

۴. جدول کیلی گروه حرکت‌های مربع را بنویسید. این گروه را با D_4 نشان می‌دهند. مطلوب است تمام زیر گروه‌های D_4.

۵. مطلوب است جدول کیلی گروه $U(12)$.

۶. ثابت یا رد کنید: هرگروه شش عنصری آبلی است.

۷. مطلوب است ارائه سه گروه آبلی متفاوت از مرتبه هشت. چرا این سه گروه متفاوتند.

۸. (a) فرض کنید $\mathbb{Z}_m \times \mathbb{Z}_n = \{(a,b))|a \in \mathbb{Z}_m, b \in \mathbb{Z}_n\}$. عمل دوتایی روی $\mathbb{Z}_m \times \mathbb{Z}_n$ به صورت زیر تعریف می کنیم.

$$(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$$

نشان دهید که $\mathbb{Z}_m \times \mathbb{Z}_n$ با این عمل یک گروه آبلی است.

www.mathematic87.blogfa.com

(b) فرض کنید $\mathbb{Z}_n^d = \{(a_1,a_2,...,a_d)|a_i \in \mathbb{Z}_n\}$. عمل دوتایی روی $\mathbb{Z}_n^d$ به صورت زیر تعریف
می کنیم.

$$(a_1,a_2,...,a_d)+(b_1,b_2,...,b_d)=(a_1+b_1,a_2+b_2,...,a_d+b_d)$$

نشان دهید که $\mathbb{Z}_n^d$ با این عمل یک گروه آبلی است. گروه $\mathbb{Z}_2^d$ در نظریه کدگذاری دارای اهمیت زیادی است.

۹. با پیدا کردن تمام زیرگروه‌های $\mathbb{Z}_3 \times \mathbb{Z}_3$ و $\mathbb{Z}_9$، نشان دهید $\mathbb{Z}_3 \times \mathbb{Z}_3$ و $\mathbb{Z}_9$ یکی نیستند.

۱۰. فرض کنید $U(n)$ گروه یکال‌های $\mathbb{Z}_n$ باشد. اگر $n>2$، ثابت کنید عنصر $k \in U(n)$ چنان موجود است که $k^2=1$ و $k \neq 1$.

۱۱. فرض کنید G گروهی از مرتبه زوج باشد. نشان دهید $a \in G$ چنان موجود است که $a \neq e$ و $a^2=e$.

۱۲. فرض کنید $n \in \mathbb{Z}, n\mathbb{Z}=\{nx|x \in \mathbb{Z}\}$. نشان دهید که $n\mathbb{Z}$ زیر گروهی از $\mathbb{Z}$ است. همچنین نشان دهید که زیر گروه های $\mathbb{Z}$ فقط این‌ها هستند.

۱۳. فرض کنید a,b عناصری از گروه G باشند. اگر $ab=ba^{-1}$ و $ba=ab^{-1}$، آنگاه $a^4=b^4=e$.

۱۴. اگر $a^2=e$ برای هر $a \in G$، آنگاه G باید آبلی باشد.

۱۵. نشان دهید که اگر G در یکی از خواص زیر صادق باشد آنگاه G آبلی است.

(a) برای هر $a,b \in G$ داشته باشیم $(ab)^2=ab$،

(b) برای هر $a,b \in G$ داشته باشیم $(ab)^2=a^2b^2$،

(c) برای هر $a,b \in G$ داشته باشیم $(ab)^{-1}=a^{-1}b^{-1}$.

۱۶. (a) مثالی از یک گروه نامتناهی ارایه دهید که هر زیر گروه غیر بدیهی آن نامتناهی باشد،

(b) مثالی از یک گروه نامتناهی ارایه دهید که هر زیر گروه حقیقی (سره) آن متناهی باشد.

۱۷. گزاره‌های زیر را ثابت یا رد کنید.

www.mathematic87.blogfa.com

(a) $\mathrm{SL}_2(\mathbb{Z})$، مجموعه ماتریس‌های 2×2 با درایه‌های صحیح که دترمینان آنها 1 است، یک زیر گروه از $\mathrm{SL}_2(\mathbb{R})$ است،

(b) اگر K,H زیر گروه‌های از گروه G باشند، آنگاه $H\cap K, H\cup K$ زیر گروه‌هایی از G می باشند،

(c) اگر K,H زیر گروه‌هایی از G باشند، آنگاه $HK=\{hk|h\in H,k\in K\}$ زیر گروه G است. اگر G آبلی باشد چطور؟

۱۸. فرض کنید H و K دو زیرگروه متناهی از گروه G باشند.

(a) ثابت کنید HK زیرگروهی از G است اگر و فقط اگر $HK=KH$،

(b) نشان دهید: $|HK|=(|H||K|)/|H\cap K|$.

۱۹. فرض کنید G یک گروه باشد نشان دهید:

$$C(G)=\{x\in G|xg=gx,\ g\in G \text{ برای هر }\}$$

یک زیر گروه از G است. این زیر گروه را **مرکز** G می نامیم.

۲۰. فرض کنید H زیرگروه از G باشد و $a\in G$ قرار می‌دهیم:

$$aHa^{-1}=\{aha^{-1}\mid h\in H\},$$
$$N_G(H)=\{g\in G\,|\,gHg^{-1}=H\},$$
$$C_G(H)=\{g\in G\,|\,ghg^{-1}=h\ ,\ \forall h\in H\}.$$

(a) نشان دهید aHa^{-1} یک زیرگروه G است. زیرگروه aHa^{-1} را یک **مزدوج** H (در G) می نامیم،

(b) نشان دهید $C_G(H)\le N_G(H)\le G$. زیرگروه‌های $C_G(H), N_G(H)$ را بترتیب **نرمال‌ساز** و**مرکز ساز** H در G می نامیم،

(c) نشان دهید $N_G(aHa^{-1})=aN_G(H)a^{-1}$.

۲۱. فرض کنید G یک گروه $a,b\in G$ نشان دهید برای تمام $n\in\mathbb{N}$،

(a) $(aba^{-1})^n=ab^na^{-1}$،

(b) اگر $aba^{-1}=b^m, m\in\mathbb{N}$، آنگاه $a^nba^{-n}=b^{m^n}$.

۲۲. فرض کنید X یک زیر مجموعهٔ ناتهی از گروه Gباشد.اگر $XgX=Xg$ برای هر $g\in G$، آنگاه $gX=Xg$ برای هر $g\in G$.

www.mathematic87.blogfa.com

مسائل مبارزه طلب

۱. فرض کنید $(S,*)$ یک نیم گروه باشد. نشان دهید $(S,*)$ گروه است اگر و فقط اگر برای هر $a \in S$ عنصر منحصر بفرد $b \in S$ چنان موجود باشد که $a*b*a=a$.

۲. فرض کنید G یک گروه و $a,b \in G$. اگر برای یک عدد طبیعی n داشته باشیم $ab^n = b^{n+1}a$ و $ba^n = a^{n+1}b$، آنگاه $a=b=e$.

۳. فرض کنید G یک گروه و $a,b \in G$. اگر رابطهٔ $(ab)^n = a^n b^n$ برای سه عدد متوالی n برقرار باشد، آنگاه $ab=ba$.

۴. فرض کنید p یک عدد اول باشد. نشان دهید:

$$|\mathrm{GL}_2(\mathbb{Z}_p)| = p(p+1)(p-1)^2,$$

$$|\mathrm{SL}_2(\mathbb{Z}_p)| = p(p^2-1).$$

۵. فرض کنید G یک گروه و $H,K \leq G$. ثابت کنید هرگاه $|H|+|K|>|G|$، آنگاه $G=HK$.

منابعی برای مطالعهٔ بیشتر

1. Baker, R. *Linear Algebra*. Rinton Press, 2001.
2. Fraleigh, J. B. *A First Course in Abstract Algebra*. Addison-Wesley, 1999.
3. Judson, T. W. *Abstract Algebra*. PWS Publishing Company, Boston, 1993.
4. Lang, S. *Introduction to Linear Algebra*. Springer-Verlag, New York, 1986.
5. Shores, T. S. *Applied Linear Algebra and Matrix Analysis*. Springer-Verlag, New York, 2007.

www.mathematic87.blogfa.com

فصل ۲

گروه‌های دوری

در این فصل می‌خوانید:

۲-۱ زیرگروه‌های دوری
۲-۲ زیر گروه‌های یک گروه دوری
۲-۳ گروه دایره و ریشه‌های واحد
۲-۴ گروه‌های متناهی مولد

مقدمه

$\mathbb{Z}$ و $\mathbb{Z}_n$ که از بین گروه‌هایی که تاکنون شناخته‌اید دارای ساختاری قابل فهم‌تر می‌باشند، مثال‌هایی از گروه‌های دوری‌اند. در این فصل به مطالعه خواص گروه‌های دوری که نقش قابل ملاحظه‌ای در رده‌بندی گروه‌های آبلی دارند، می‌پردازیم.

www.mathematic87.blogfa.com

۲-۱ زیرگروه‌های دوری

در بیشتر مواقع ساختار یک زیر گروه به یک عنصر از گروه بستگی پیدا می‌کند، یعنی با داشتن یک عنصر بخصوص می‌توان سایر اعضای زیرگروه را به دست آورد.

مثال۱: فرض کنید $3 \in \mathbb{Z}$. مجموعه تمامی مضارب (مثبت و منفی) 3 را در نظر بگیرید.

$$3\mathbb{Z} = \{3k | k \in \mathbb{Z}\} = \{\ldots -6, -3, 0, 3, 6, \ldots\}.$$

همان‌طور که می‌دانید $3\mathbb{Z}$ یک زیر گروه از $\mathbb{Z}$ است. این زیر گروه بستگی کامل به 3 دارد. چرا که هر عنصر این زیرگروه یک مضربی از 3 است. به عبارت دیگر این زیرگروه توسط 3 مشخص می‌شود.

■

مثال۲: فرض کنید $H = \{2^n | n \in \mathbb{Z}\}$. اگر $a = 2^m, b = 2^n$ عناصر یاز H باشند، آنگاه $ab^{-1} = 2^{m-n} \in H$. بنابراین H یک زیر گروه از $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ می‌باشد. این زیر گروه به طور کامل توسط 2 مشخص می‌شود.

■

قضیه ۲-۱

فرض کنید G یک گروه باشد و $a \in G$. در این صورت

$$< a >= \{a^k | k \in \mathbb{Z}\}$$

زیرگروهی از G است و کوچکترین زیرگروه G شامل a است.

اثبات: چون $a \in < a >$ پس $< a >$ غیر تهی است. حال فرض کنید $m, n \in \mathbb{Z}$ و $g = a^m$ و $h = a^n$ دو عنصر از G باشند. در این صورت $gh^{-1} = a^{m-n} \in < a >$، بنابراین طبق آزمون دوم زیرگروه، $< a >$ یک زیرگروه از G است. از طرفی اگر H یک زیر گروه دلخواه از G که شامل a است باشد، آنگاه H لزوماً باید شامل $\{a^k | k \in \mathbb{Z}\}$ نیز باشد، یعنی $< a > \subseteq H$.

■■■

www.mathematic87.blogfa.com

تعریف ۲-۱ (زیر گروه دوری)

فرض کنید a عنصری از گروه G باشد. زیر گروه $< a >$ از G را **زیرگروه دوری** تولید شده توسط a گوییم.

تعریف ۲-۲ (گروه دوری)

اگر $a \in G$ چنان موجود باشد که $G =< a >$، آنگاه G را یک **گروه دوری** و a را یک مولد G گوییم.

حال مرتبهٔ عناصر یک گروه را تعریف می‌کنیم. این تعریف، تعریفی کاملاً متفاوت با تعریف مرتبه یک گروه است، هر چند خواهیم دید که این تعریف ها رابطه نزدیکی با هم دارند.

تعریف ۲-۳ (مرتبه یک عنصر)

فرض کنید a عنصری از گروه G باشد. کوچکترین عدد طبیعی n (در صورت وجود) که $a^n = e$ را **مرتبه** a گوییم و با $\circ(a) = n$ نشان می‌دهیم. اگر چنین عدد طبیعی موجود نباشد، گوییم a یک عنصر از مرتبه نامتناهی است و می‌نویسیم $\circ(a) = \infty$.

قضیه ۲-۲

فرض کنید G یک گروه و $a \in G$ در این صورت مرتبه زیر گروه $< a >$ با مرتبه a برابر است. به عبارت دیگر

$$\circ(a) = |< a >|.$$

اثبات: ابتدا فرض کنید a دارای مرتبه نامتناهی باشد. اگر $m > n$ و $a^m = a^n$، آنگاه $a^{m-n} = e$ که متناقض با نامتناهی بودن مرتبه a است. لذا عناصر $< a >$ متمایزند. به عبارت دیگر $|< a >|$ نامتناهی است. اکنون فرض کنید $\circ(a) = n$. اگر k یک عدد صحیح دلخواهی باشد، طبق الگوریتم تقسیم خواهیم داشت $k = nq + r$ که $0 \leq r \leq n$، پس $a^k = a^{nq+r} = \left(a^n\right)^q a^r = a^r$.

یعنی $< a >= \{a^0, a^1, ..., a^{n-1}\}$ از طرفی چون عناصر $a^0, a^1, ..., a^{n-1}$ متمایزاند، لذا $|< a >| = n$.

■■■

مثال۳: توجه داشته باشید که یک گروه دوری می‌تواند بیش از یک مولد داشته باشد. به عنوان مثال عناصر 1 و 5 مولدهایی برای $\mathbb{Z}_6$ اند.

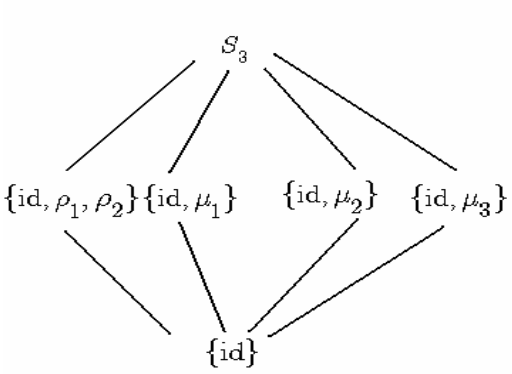
■

مثال۴: گروه $U(9)$ دوری است. در حقیقت $U(9) = \{1,2,4,5,7,8\}$ و 2 مولدی برای این گروه است، زیرا

$$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 8$$
$$2^4 = 7 \quad 2^5 = 5 \quad 2^6 = 1$$

■

مثال۵: این طور نیست که همه گروه‌ها دوری باشند، به عنوان مثال گروه حرکت‌های مثلث متساوی الاضلاع، S_3، دوری نیست، به عبارت دیگر S_3 دارای هیچ مولدی نیست. در صورتی که تمام زیرگروه‌های S_3 دوری‌اند.
در زیر نمودار زیر گروه‌های S_3 رسم شده است. **(نمودار لاتیس)**



■

قضیه زیر در مورد شناسایی گروه دوری کمک زیادی می‌کند.

قضیه ۲-۳

فرض کنید $|G| = n$. در این صورت G دوری است اگر و فقط اگر دارای عنصری از مرتبه n باشد.

اثبات: فرض کنید $a \in G$ از مرتبه n باشد. در این صورت طبق قضیه قبل $|< a >|= n$ و در نتیجه $G =< a >$. به عکس، اگر G یک گروه دوری از مرتبه n باشد، خواهیم داشت $G =< a >$ و $|< a >|= n$. بنابراین با استفاده مجدد از قضیه قبل خواهیم داشت $\circ(a) = n$.

■■■

قضیه۲-۴

هر گروه دوری آبلی است.

اثبات: فرض کنید G یک گروه دوری و a مولدی از آن باشد. اگر $h = a^m, g = a^n$ دو عنصر دلخواه از G باشند، آنگاه

$$gh = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = hg$$

و بنابراین G آبلی است.

■■■

❖ **تذکر :** از قضیه فوق نیز می‌توان نتیجه گرفت که S_3 دوری نیست.

۲-۱ زیر گروه‌های یک گروه دوری

حال به بررسی زیر گروه‌های یک گروه دوری می‌پردازیم.

www.mathematic87.blogfa.com

قضیه۲-۵

هر زیر گروه یک گروه دوری، خود دوری است.

اثبات: ابزارهای اصلی برای اثبات این قضیه الگوریتم تقسیم و اصل خوش ترتیبی می‌باشند. فرض کنید H یک زیر گروه از گروه دوری $G=<a>$ باشد. اگر $H=\{e\}$، به وضوح H دوری است. حال فرض کنید $H\neq\{e\}$، فرض کنید m کوچکترین عدد طبیعی باشد که $a^m\in H$ (بنا به اصل خوش ترتیبی چنین mای موجود است). ادعا می‌کنیم $H=<a^m>$. واضح است که $<a^m>\subseteq H$. حال نشان می‌دهیم $H\subseteq<a^m>$ برای این منظور فرض کنید $h=a^k\in H$، جایی که $k\in\mathbb{Z}$. طبق الگوریتم تقسیم اعداد r,q چنان موجوند که $k=mq+r$، جایی که $0\leq r<m$. بنابراین

$$a^k=a^{mq+r}=\left(a^m\right)^q a^r$$

و در نتیجه $a^r=a^k a^{-mq}\in H$. اما با توجه به خاصیت m باید $r=0$ و در نتیجه $k=mq$ یعنی

$$a^k=a^{mq}=\left(a^m\right)^q.$$

بنابراین $H=<a^m>$.

■■■

قبل از بیان نتیجه زیر متذکر می‌شویم که اگر از نماد جمعی استفاده کنیم زیر گروه تولید شده توسط a عبارت است از

$$<a>=\{na|n\in\mathbb{Z}\}.$$

نتیجه۲-۱

همه زیرگروه‌های $\mathbb{Z}$ عبارتند از $n\mathbb{Z}$ که $n=0,1,2,...$.

اثبات: به وضوح از قضیه قبل نتیجه می‌شود.

■■■

گزاره۲-۱

فرض کنید G یک گروه دوری از مرتبه n و $a \in G$ مولد برای آن باشد. در این صورت

$$a^k = e \Leftrightarrow n|k.$$

اثبات: $(\Rightarrow)$: فرض کنید $a^k = e$. با استفاده از الگوریتم تقسیم داریم $k = nq + r$ که $0 \le r < n$، بنابراین

$$e = a^k = a^{nq+r} = a^{nq}a^r = ea^r = a^r$$

و با توجه به تعریف مرتبه خواهیم داشت $r = 0$، یعنی $n|k$.

$(\Leftarrow)$: فرض کنید برای یک عدد صحیح s داشته باشیم $k = ns$ در این صورت

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$

■■■

حال قضیه اساسی مربوط به مولدهای زیرگروه‌های یک گروه دوری متناهی را بیان می‌کنیم.

قضیه۲-۶

فرض کنید $G =< a >$ یک گروه دوری از مرتبه n باشد. در این صورت

$$\circ(a^k) = n/(n,k).$$

اثبات: قرار می‌دهیم $d = (n,k)$. بایستی نشان داد که n/d کوچکترین عدد طبیعی است که $(a^k)^{n/d} = e$. داریم $(a^k)^{n/d} = (a^n)^{k/d} = e^{k/d} = e$. اگر عدد طبیعی m چنان موجود باشد که $(a^k)^m = e$، آنگاه طبق گزاره قبل داریم $n|km$ و در نتیجه $(n/d)|(k/d)m$ از طرفی چون $(n/d, k/d) = 1$ پس $(n/d)|m$. به عبارت دیگر $(n/d) \le m$. یعنی نشان داده ایم که

$$\circ(a^k) = n/d.$$

■■■

از قضیه فوق بلافاصله نتیجه زیر به دست می‌آید.

نتیجه۲-۲

فرض کنید $G =< a >$ یک گروه دوری از مرتبه n باشد. در این صورت a^k مولدی برای G است اگر و فقط اگر $(k,n)=1$.

مثال۶: مجموعه مولدهای $\mathbb{Z}_n$ عبارت است از $\{r|0 \le r < n,(r,n)=1\}$.

■

نتیجه۲-۳

فرض کنید G یک گروهی باشد بطوریکه دارای هیچ زیرگروه غیر بدیهی نیست (تعریف۶-۴ ملاحظه شود) . در این‌صورت G دوری واز مرتبهٔ عددی اول است.

اثبات: فرض کنید $e \neq a \in G$. در این‌صورت چون G دارای زیرگروه غیر بدیهی نیست، خواهیم داشت $G =< a >$. حال دو حالت در نظر می‌گیریم:

حالت (۱): $a^2 = e$. در این حالت $\circ(a) = 2$ و در نتیجه $|G| = 2$ و حکم بوضوح برقرار است.

حالت (۲): $a^2 \neq e$. در این حالت، با توجه به اینکه G دارای زیرگروه غیر بدیهی نیست، خواهیم داشت $< a >=< a^2 >$. بنابراین $k \in \mathbb{Z}$ بگونه‌ای موجود است که $a = a^{2k}$، یعنی $a^{2k-1} = e$. از این‌رو مرتبهٔ G متناهی است. فرض کنید $|G| = n$. نشان می‌دهیم n عددی اول است. (برهان خلف) فرض کنید n اول نباشد و $n = kt$، که $1 < k,t < n$. با توجه به قضیه۲، داریم، $\circ(a^k) = n/(n,k) = t$، یعنی G دارای زیرگروه غیر بدیهی ، $< a^k >$، می‌باشد، که تناقض است.

■■■

۲-۳ گروه دایره و ریشه‌های

تعریف ۲-۴

زیرگروه $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ از گروه ضربی اعداد مختلط، $\mathbb{C}^*$، **گروه دایره** نامیده می‌شود.

www.mathematic87.blogfa.com

اگرچه $\mathbb{T}$ یک گروه نامتناهی است، اما دارای زیر گروه‌های متناهی جالبی می‌باشد. بعنوان مثال $H=\{\pm 1,\pm i\}$ یک زیرگروه دوری متناهی از $\mathbb{T}$ است. توجه داشته باشیم که اعضای H دقیقاً ریشه‌های معادله $z^4=1$ می‌باشند.

تعریف ۲-۵

ریشه‌های معادله $z^n=1$ را **ریشه‌های n ام واحد** گوییم.

در حال کلی می‌توان گفت که مجموعه ریشه‌های nام واحد یعنی $U_n=\{z\in\mathbb{C}\mid z^n=1\}$ همراه با عمل ضرب یک گروه دوری مرتبه n از $\mathbb{T}$ است. در حقیقت به سادگی می‌توان نشان داد که

$$U_n=\left\{e^{\frac{2k\pi i}{n}}\,|0\le k\le n-1\right\}.$$

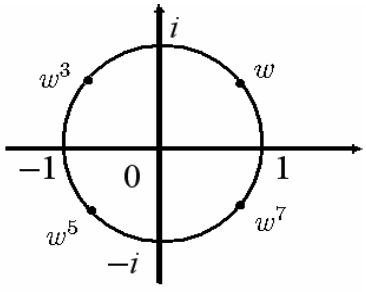
به عبارت دیگر $U_n=<w>=\{1,w,...,w^{n-1}\}$، جایی که $w=e^{\frac{2k\pi i}{n}}$. از نظر هندسی ریشه‌های nام واحد به فاصله‌های مساوی بردایره یکه واقع‌اند.

تعریف ۲-۶

مولدهای گروه U_n را **ریشه‌های nام واحد اولیه** گوییم.

مثال۷: ریشه‌های 8 ام واحد را می‌توان به عنوان به صورت 8 نقطه که به فاصله‌های مساوی روی دایره یکه قرار دارند نمایش داد (شکل زیر). در اینجا ریشه‌های 8 ام واحد اولیه عبارتند از:

$$w=(\sqrt{2}/2)+(\sqrt{2}/2)i,\ w^3=(-\sqrt{2}/2)+(\sqrt{2}/2)i,$$
$$w^5=(-\sqrt{2}/2)+(-\sqrt{2}/2)i,\ w^7=(\sqrt{2}/2)+(-\sqrt{2}/2)i.$$



■

۲-۴ گروه‌های متناهی مولد

این بخش به گروه‌های متناهی مولد که تعمیمی از گروه‌های دوری می‌باشند اختصاص دارد.

قضیه ۲-۷

اگر $\{H_\lambda | \lambda \in \Lambda\}$ خانواده‌ای از زیر گروه‌های گروه G باشد، آنگاه $\bigcap_{\lambda\in\Lambda} H_\lambda$ زیر گروه G است.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضیه فوق این امکان را به ما می‌دهد که زیر گروه تولید شده به وسیله مجموعه‌ای از عناصر مفروض را تعریف کنیم:

تعریف ۲-۷

(۱) فرض کنید G یک گروه و X زیر مجموعه‌ای از G باشد. اشتراک تمام زیرگروه‌های G که شامل X باشند را **زیرگروه تولید شده توسط** X گوییم و آنرا با $< X >$ نمایش می‌دهیم، به عبارت دیگر

$$< X >= \bigcap_{X\subseteq H\leq G} H.$$

X را مجموعه **مولدهای** این زیرگروه (یعنی $< X >$) گوییم. اگر $X = \{x_1, x_2, ..., x_n\}$ متناهی باشد، زیرگروه $< X >$ را با نماد $< x_1, x_2, ..., x_n >$ نمایش می‌دهیم.

(۲) زیرگروه H از G را یک **زیرگروه متناهی مولد** گوییم، اگر عناصر $x_1, x_2, ..., x_n \in G$ بگونه‌ای موجود باشند که $H =< x_1, x_2, ..., x_n >$.

(۳) G را یک **گروه متناهی مولد** گوییم، اگر بعنوان یک زیرگروه خودش متناهی مولد باشد.

▼ **یاد داشت:** فرض کنید G یک گروه و X زیر مجموعه‌ای از G باشد.

(۱) $< X >$ کوچکترین زیر گروه شامل X است.

www.mathematic87.blogfa.com

(۲) در صورتی که $X=\{a\}$ تک عنصری باشد، $< X >=< a >$ همان زیرگروه تولید شده توسط a می‌باشد.

قضیهٔ زیر مشخص کنندهٔ فرم کلی عناصر زیر گروه $< X >$ می‌باشد.

قضیه۲-۸

فرض کنید X زیرمجموعه‌ای از گروه G باشد. در این‌صورت:

$$< X >= \{x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n} \mid x_i \in X,\ \alpha_i = \pm 1\}.$$

اثبات: فرض کنید K مجموعهٔ تمام حاصل‌ضرب‌های متناهی بصورت بالا باشد. بوضوح K زیرگروهی از G شامل X می‌باشد. ازاین‌رو $< X >\subseteq K$. همچنین به آسانی می‌توان مشاهده نمود که هر زیرگروهی از G شامل X، شامل K نیز می‌باشد. در نتیجه

$$K \subseteq \bigcap_{X\subseteq H\leq G} H =< X > .$$

بنابراین $K =< X >$ و قضیه ثابت است.

■■■

مثال۸: فرض کنید $G=(\mathbb{Z},+)$. در این‌صورت:

$$G =< 1 >,$$
$$G =< 2,3 >,$$
$$G =< 6,10,15 > .$$

آیا می‌توانید مولدی با ۴ عنصر برای G بیابید بطوریکه هر زیر مجموعهٔ ۳ عنصری آن مولدی برای G نباشد (به تمرین ۲۲ مراجعه شود).

■

مثال۹:

$$\begin{aligned} S_3 &=< \rho_1,\mu_1 >=< \rho_2,\mu_1 > \\ &=< \rho_1,\mu_2 >=< \rho_2,\mu_2 > \\ &=< \rho_1,\mu_3 >=< \rho_2,\mu_3 > . \end{aligned}$$

■

❖ **تذکر (۱)** : ملا حظه می‌شود که یک گروه G می‌تواند مجموعه‌های مولد مختلفی داشته باشد.

www.mathematic87.blogfa.com

(۲) : هر گروه G حداقل دارای یک مجموعه مولد، یعنی خود مجموعهٔ G می‌باشد. هر چند که این مجموعه مولد از اهمیت خاصی برخوردار نیست.

تمرینها

۱. گزاره‌های زیر را ثابت یا رد کنید.

(a) $U(8)$ دوری است،

(b) همه مولدهای $\mathbb{Z}_{60}$ اول هستند،

(c) $\mathbb{Q}$ دوری است،

(d) اگر هر زیر گروه G دوری باشد، آنگاه G دوری است،

۲. اعضای هر یک از زیر گروه‌های زیر را بنویسید.

(a) زیر گروه تولید شده توسط 7 در $\mathbb{Z}$،

(b) زیرگروه تولید شده توسط 15 در $\mathbb{Z}_{24}$،

(c) تمام زیرگروه‌های $\mathbb{Z}_{60}$،

(d) زیرگروه تولید شده توسط 3 در $U(20)$،

(e) زیر گروه تولید شده توسط i در $\mathbb{C}^*$،

(f) زیرگروه تولید شده توسط $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$.

۳. مرتبه همه عناصر $\mathbb{Z}_{18}$ و D_4 را مشخص کنید.

۴. مطلوب است همه عناصر مرتبهٔ متناهی در گروه‌های $\mathbb{Z}, \mathbb{Q}^*, \mathbb{R}^*$.

۵. اگر $a^{24} = e$، آنگاه مرتبه a چه اعدادی می‌تواند باشد.

۶. برای $n \leq 20$، کدامیک از $U(n)$ ها دوری‌اند.

۷. یک گروه دوری با دقیقاً یک مولد بیابید. آیا می‌توانید یک گروه دوری با دقیقاً دو مولد بیابید. در مورد n مولد چطور؟

۸ . ریشه‌های۵ ام واحد را محاسبه و رسم کنید (روی دایره یکه). ریشه‌های ۵ ام واحد اولیه کدامند.

۹. فرض کنید $a, b \in G$ ثابت کنید.

www.mathematic87.blogfa.com

(a) $\circ(a^{-1}) = \circ(a)$،

(b) $\circ(a) = \circ(gag^{-1})$ برای هر $g \in G$،

(c) $\circ(ab) = \circ(ba)$.

۱۰. فرض کنید G یک گروه باشد و $n \in \mathbb{N}$. اگر $a \in G$ تنها عنصری باشد که زیر گروهی دوری از مرتبهٔ n تولید می‌کند، آنگاه $a \in C(G)$.

۱۱. فرض کنید q, p دو عدد اول متمایز و n یک عدد طبیعی باشد. مطلوب است تعداد مولدهای $\mathbb{Z}_{p^n}, \mathbb{Z}_{pq}$.

۱۲. فرض کنید G یک دوری از مرتبهٔ n باشد. دراین‌صورت:

(a) هر زیر گروه H از G بصورت $< a^m >$ است، که در آن عدد طبیعی m مقسوم علیهی از n است،

(b) برای هر زیر گروه H از G داریم $|H| \mid n$،

(c) اگر $m \mid n$، آنگاه G زیرگروه منحصربفردی از مرتبهٔ m دارد.

۱۳. اگر h, g عناصری ازگروه G با مرتبه‌های 15 و 16 باشند، مرتبه $< g > \cap < h >$ چیست.

۱۴. نشان دهید تعداد مولدهای $\mathbb{Z}_n (n > 2)$ عددی زوج می‌باشد.

۱۵. فرض کنید b, a عناصری از گروه G باشند. اگر $\circ(a) = m, \circ(b) = n$ و $(m, n) = 1$ آنگاه $< a > \cap < b >= \{e\}$.

۱۶. فرض کنید G یک گروه آبلی باشد. نشان دهید مجموعه همه عناصر مرتبه متناهی، یک زیر گروه از G است. این زیرگروه را **زیرگروه تابی** G گوییم.

۱۷. فرض کنید G یک گروه آبلی باشد. اگر G دارای دو زیر گروه از مرتبه 2 باشد، آنگاه G باید دارای زیر گروهی از مرتبه 4 باشد. آیا لزوماً این زیرگروه دوری است.

۱۸. فرض کنید G یک گروه و $a, b \in G$ و $\circ(a) = m, \circ(b) = n$ و $ab = ba$. نشان دهید:

(a) اگر $(m, n) = 1$، آنگاه $\circ(ab) = mn$،

(b) در حالت کلی: اگر $< a > \cap < b >= \{e\}$، آنگاه $\circ(ab) = [m, n]$.

۱۹. نشان دهید یک گروه با تعداد متناهی زیر گروه، متناهی است.

www.mathematic87.blogfa.com

۲۰. اگر $G=<a>$ یک گروه دوری نامتناهی باشد، نشان دهید a^{-1},a تنها مولدهای G هستند.

۲۱. زیر گروه سرهٔ M از گروه G را **ماکزیمال** گوییم اگر برای هر زیر گروه N که $M\leq N\leq G$، داشته باشیم $N=M$ یا $N=G$.
نشان دهید در گروه متناهی مولد G، هر زیرگروه سره در یک زیر گروه ماکزیمال قرار دارد.

۲۲. به ازای هر عدد طبیعی n، n عدد طبیعی پیدا کنید که $(\mathbb{Z},+)$ را تولید کند ولی هر زیرمجموعهٔ $n-1$ عنصری از آن، $(\mathbb{Z},+)$ را تولید نکند.

مسائل مبارزه طلب

۱. گروهی مثال بزنیدکه دارای دو عنصر a و b باشد، بطوریکه a و b از مرتبهٔ متناهی ولی ab از مرتبهٔ نامتناهی باشد.

۲. گروهی نامتناهی مثال بزنید که هر زیر گروه سرهٔ آن دوری و متناهی باشد.

۳.گروهی مانند $G\neq<e>$مثال بزنید که دارای زیرگروه ماکزیمال نباشد.

۴. فرض کنید G یک گروه متناهی باشد. اگر برای هر عدد طبیعی n، معادلهٔ $x^n=1$ حداکثر n ریشه در G داشته باشد، آنگاه G دوری است.

۵. مطلوب است کلیهٔ مقادیر n که به ازای آنها $U(n)$ یک گروه دوری باشد.

منابعی برای مطالعهٔ بیشتر

۱. محمدی حسن آبادی، علی اکبر. **جبر**. انتشارات دانشگاه اصفهان (۱۳۷۲).

2. Bhattacharya, P.B., Jain, S. K., Nagpaul, S. R. *Basic Abstract Algebra*. Cambridge University Press, 1994.

3. Gallian, J. *Contemporary Abstract Algebra*. Houghton Mifflin Co., Boston, 1998.

4. Nickelson, W. K. *Introduction to Abstract Algebra*. Wiley-Interscience seience (John-Wiley & Sons) Hoboken, 2007.

www.mathematic87.blogfa.com

فصل ۳

گروه‌های جایگشتی

در این فصل می‌خوانید:

۳-۱ نمایش دو سطری
۳-۲ نمایش دوری
۳-۳ حاصل ضرب دورها
۳-۴ تجزیه به دورها
۳-۵ تقارن‌ها

مقدمه

هر زیر گروه از S_n یک گروه **جایگشتی** نامیده می‌شود. گروه‌های جایگشتی در مطالعه تقارن‌های هندسی، نظریه گالوا و مطالعه معادلات چند جمله‌ای نقش بنیادی دارد. در این فصل به طور مفصل به بررسی گروه متقارن درجه n، S_n، و بعضی از زیرگروه‌های آن خواهیم پرداخت.

۳-۱ نمایش دو سطری

همان‌طور که قبلاً (در فصل ۱) گفته شده برای راحتی هر جایگشت $\sigma \in S_n$ را به صورت زیر نمایش می‌دهیم:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

این نمایش به **نمایش دو سطری** معروف است. این نمایش به ما کمک می‌کند که بتوانیم تعداد جایگشت‌ها را معین کنیم.

قضیه ۳-۱

به ازای هر عدد طبیعی n، $|S_n| = n!$.

اثبات: تصویر 1، یعنی $\sigma(1)$ هر یک از n عنصر $\{1,2,...,n\}$ می‌تواند باشد. هنگامی که $\sigma(1)$ نوشته شد، $\sigma(2)$ هر یک از $n-1$ عنصر دیگر (غیر از $\sigma(1)$) می‌تواند باشد،...، برای $\sigma(n-1)$، 2 انتخاب و برای $\sigma(n)$، 1 انتخاب خواهیم داشت، پس $|S_n| = n!$.

■■■

با به‌کارگیری نمایش دو سطری، محاسبه حاصل ضرب (ترکیب) جایگشت‌ها آسان می‌شود، فرض کنید:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \quad \text{و} \quad \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$$

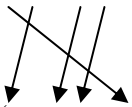
برای یافتن $\tau\sigma$ باید به ازای هر $i \in \{1,2,...,n\}$، $\tau\sigma(i) = \tau(\sigma(i))$ را پیدا کنیم. یعنی اول $\sigma(i)$ را از روی نمایش σ و سپس $\tau(\sigma(i))$ را از روی نمایش τ به دست می‌آوریم.

به عنوان مثال فرض کنید:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \text{و} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

www.mathematic87.blogfa.com

$$\sigma=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$



$$\tau=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$\Rightarrow \tau\sigma=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}.$$

جهت پیکان‌های بالا، $\tau\sigma(i)$، که $i\in\{1,2,3,4\}$، را نشان می‌دهد.

همین‌طور می‌توان نشان داد که

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

توجه داشته باشید که $\sigma\tau\neq\tau\sigma$. از روی نمایش دو سطری می‌توان وارون هر جایگشت را به آسانی پیدا کرد. به عنوان مثال، فرض کنید می‌خواهیم وارون σ را پیدا کنیم. طبق تعریف می‌دانیم که اگر σ عنصر i را به j ببرد، آنگاه وارون σ عنصر j را به i می‌برد.

پس مطابق شکل زیر وارون σ به دست می‌آید.

$$\sigma=\begin{pmatrix}1&2&3&4\\\uparrow\downarrow&\uparrow\downarrow&\uparrow\downarrow&\uparrow\downarrow\\4&1&2&3\end{pmatrix}\Rightarrow\sigma^{-1}=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}.$$

مثال۱: زیر گروه G از S_5 متشکل از id و جایگشت‌های زیر را در نظر بگیرید.

$$\sigma=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix},\ \tau=\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix},\ \mu=\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}.$$

جدول زیر قانون ترکیب (حاصل ضرب) عناصر گروه جایگشتی G را نشان می‌دهد.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

■

www.mathematic87.blogfa.com

❖ **تذکر :** بعضی از کتب، تصویر x تحت جایگشت (تابع) σ را بـه جـای ایـن کـه با $\sigma(x)$ نمایش دهند با $x\sigma$ نمایش می‌دهند. اگر σ_1 و σ_2 دو جایگشت (تـابع) باشند، با این قرار داد جدید $\sigma_1.\sigma_2$ جایگشتی (تـابعی) اسـت کـه بـر x چنـین تعریف می‌شود:

$$x(\sigma_1.\sigma_2) = (x\sigma_1)\sigma_2$$

یعنی اول σ_1 و بعد σ_2 اثر می‌کند. در حقیقت دلیل چنین قرار دادی این است که جایگشت‌ها (توابع) در $\sigma_1.\sigma_2$ به همان ترتیبی که نوشته می‌شوند اثر کنند.

۳-۲ نمایش دوری

نمایشی که تاکنون برای جایگشت‌ها به کار می‌بریم (نمایش دو سطری) تا حدودی پر زحمت است. یک روش کارآمد، استادانه و فشرده‌تر برای نمایش جایگشت‌ها، نمایش دوری می‌باشد، که در این بخش به آن می‌پردازیم.

تعریف ۳-۱

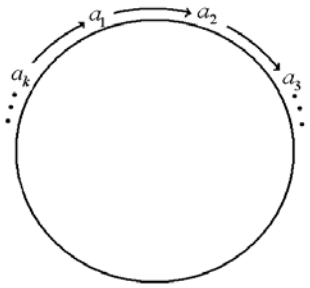
جایگشت $\sigma \in S_X$ را یک **دور** به‌طـول k گـوییم اگـر عناصـر $a_1, a_2, ..., a_k \in X$ موجـود باشند که

$$\sigma(a_1) = a_2$$
$$\sigma(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_k) = a_1$$

و بـــرای عناصـــر دیگـــر $x \in X$ داشـــته باشـــیم $\sigma(x) = x$. در ایـــن صـــورت مـی‌نویـسیم $\sigma = (a_1\ a_2\ \dots\ a_k)$. وقتـی کـه از نمـایش دوری اسـتفاده مـی‌کنـیم بایـد مجموعـه X از مـضمون واضـح باشـد. بـه عبـارت دیگـر، دور $\sigma = (a_1\ a_2\ \dots\ a_k)$ هـر عنصر $a_1, a_2, ..., a_k$ را یک قدم در دایره ترسیم شده زیر حرکـت داده و بقیـه عناصـر را

www.mathematic87.blogfa.com

حرکت نمی‌دهد. (اگر $\sigma(x)=x$ گوییم σ عنصر x را حرکت نمی‌دهد).



مثال۲: جایگشت

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\6&3&5&1&4&2&7\end{pmatrix}=\begin{pmatrix}1&6&2&3&5&4\end{pmatrix}$$

یک دور به‌طول ۶ و جایگشت

$$\tau=\begin{pmatrix}1&2&3&4&5&6\\1&4&2&3&5&6\end{pmatrix}=(2\ 4\ 3)$$

یک دور به‌طول ۳ است.

■

قرارداد: توافق می‌کنیم که هر دور به‌طول ۱، نشان دهندهٔ جایگشت همانی باشد.

مثال۳: گروه S_3 را در نظر بگیرید. همان‌طور که از قبل (فصل ۱) می‌دانید عناصر این گروه عبارتند از:

$$\mathrm{id}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\text{و}\rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\text{و}\ \rho_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\mu_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\text{و}\mu_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\text{و}\ \mu_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

نمایش دوری عناصر S_3 عبارتند از:

$$\mathrm{id}=(1)\ \text{و}\ \ \rho_1=(1\ 2\ 3)\ \text{و}\ \rho_2=(1\ 3\ 2)$$

$$\mu_1=(2\ 3)\ \ \text{و}\ \ \mu_2=(1\ 3)\ \ \text{و}\ \ \mu_3=\begin{pmatrix}1&2\end{pmatrix}$$

■

www.mathematic87.blogfa.com

۳-۳ حاصل ضرب

چون دورها نوعی خاص از جایگشت‌ها هستند، هر دو دور را مانند دو جایگشت می‌توان در هم ضرب کرد.

البته، باید توجه داشت که حاصل ضرب دو دور لزومی ندارد که خود یک دور باشد.

به عنوان مثال فرض کنید $\sigma = (1\ 3\ 2)$ و $\tau = (2\ 4\ 5)$. برای محاسبه $\sigma\tau = (1\ 3\ 2)(2\ 4\ 5)$ به طریقهٔ زیر عمل می‌کنیم:

$$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 3 \qquad 1 \xrightarrow{\sigma\tau} 3$$
$$2 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 4 \qquad 2 \xrightarrow{\sigma\tau} 4$$
$$3 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 2 \qquad 3 \xrightarrow{\sigma\tau} 2$$
$$4 \xrightarrow{\tau} 5 \xrightarrow{\sigma} 5 \qquad 4 \xrightarrow{\sigma\tau} 5$$
$$5 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 1 \qquad 5 \xrightarrow{\sigma\tau} 1$$

بنابراین

$$\sigma\tau = (1\ 3\ 2)(2\ 4\ 5) = (1\ 3\ 2\ 4\ 5).$$

حال اگر $(1\ 5\ 2)$ و $(1\ 4\ 5\ 6)$ دورهایی از S_6 باشند، آنگاه هیچ یک از دو جایگشت زیردور نیست.

$$(1\ 5\ 2)(1\ 4\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix},$$
$$(1\ 4\ 5\ 6)(1\ 5\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

تعریف ۳-۲

جایگشت‌های $\tau, \sigma \in S_X$ را **مجزا** گوییم، اگر $x \in X$ توسط یکی از آنها حرکت داده شود، آنگاه توسط دیگری ثابت نگه‌داشته شود. به عبارت معادل، برای هر $x \in X$ گزاره‌های زیر برقرار باشند.

$$\sigma(x) \neq x \Rightarrow \tau(x) = x,$$

$$\tau(x) \neq x \Rightarrow \sigma(x) = x.$$

www.mathematic87.blogfa.com

از تعریف فوق می‌توان نتیجه گرفت که دو دور $\sigma = (a_1\ a_2\ \dots\ a_k)$ و $\tau = (b_1\ b_2\ \dots\ b_l)$ از S_X مجزا هستند اگر برای هر i و j داشته باشیم $a_i \neq b_j$.

لم ۳-۱

فرض کنید $\tau, \sigma \in S_X$ دو جایگشت مجزا باشند. در این‌صورت $\sigma\tau = \tau\sigma$.

اثبات: عنصر دلخواه $x \in X$ را نظر بگیرید. اگر x توسط هر دو جایگشت σ و τ ثابت نگه داشته شود، به وضوح $\sigma\tau(x) = \tau\sigma(x)$. حال فرض کنید که x حداقل توسط یکی از جایگشت‌های σ یا τ حرکت داده شود. فرض کنید $\sigma(x) \neq x$. با توجه به یک به یک بودن σ، خواهیم داشت $\sigma(\sigma(x)) \neq \sigma(x)$. چون τ و σ مجزا می‌باشند پس $\tau(x) = x$ و $\tau(\sigma(x)) = \sigma(x)$ و در نتیجه

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = \tau(\sigma(x)) = \tau\sigma(x)$$

و لذا حکم ثابت است.

■■■

۳-۴ تجزیه به دورها

همان‌طور که ملاحظه کردید حاصل ضرب دورها، جایگشت می‌باشد. حال عکس این مطلب را نشان می‌دهیم، یعنی ثابت می‌کنیم که هر جایگشت، حاصل ضرب دورهاست.

مثال۴: فرض کنید

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 5 & 7 & 6 \end{pmatrix}.$$

چون $\sigma(1) = 4$، $\sigma(2) = 3$، $\sigma(3) = 1$، $\sigma(4) = 2$، لذا قسمتی از این جایگشت دور $(1\ 4\ 2\ 3)$ می باشد. $\sigma(6) = 7$ و $\sigma(7) = 6$ که منجر به دور $(6\ 7)$ می‌شود. در نتیجه $\sigma = (1\ 4\ 2\ 3)(6\ 7)$ و در حالت کلی قضیه زیر را خواهیم داشت (این قضیه نشان دهنده اهمیت دورها است).

■

www.mathematic87.blogfa.com

قضیه۳-۲

هر جایگشت $\sigma \in S_n$ حاصل ضربی از دورهای مجزا است.

اثبات: فرض کنید $X = \{1,2,...,n\}$. قرار می‌دهیم $X_1 = \{1, \sigma(1), \sigma^2(1), ...\}$. چون X متناهی است، عناصر X_1 همگی متمایز نیستند. فرض کنید ℓ کوچکترین عدد طبیعی باشد که به ازای tای $(0 \le t < \ell)$، $\sigma^\ell(1) = \sigma^t(1)$. دراین‌صورت $\sigma^\ell(1) = 1$. (چون، $\sigma^{\ell-t}(1) = 1$، $0 < \ell - t \le \ell$، و در نتیجه $t = 0$، $\sigma^\ell(1) = 1$) . ازاین‌رو، دور زیر را خواهیم داشت.

$$\sigma_1 = (1\ \sigma(1)\ \sigma^2(1)\ ...\sigma^{\ell-1}(1)).$$

فرض کنید i کوچکترین عنصری از X باشد که در X_1 نیست. قرار می‌دهیم $X_2 = \{i, \sigma(i), \sigma^2(i), ...\}$ و با تکرار آنچه گفته شد به دور σ_2 خواهیم رسید. حال نشان می‌دهیم $X_1 \cap X_2 = \varnothing$. (برهان خلف) فرض کنید اعداد صحیح نامنفی r, sچنان موجود باشند که $\sigma^r(1) = \sigma^s(i)$. اگر عدد طبیعی ℓ به‌گونه‌ای باشد که $r - s + n\ell \ge 0$، آنگاه

$$i = \sigma^{r-s}(1) = \sigma^{r-s}(\sigma^{n\ell}(1)) = \sigma^{r-s+n\ell}(1) \in X_1,$$

که تناقض است. بنابراین $X_1 \cap X_2 = \varnothing$. کار را ادامه می‌دهیم، کوچکترین عنصر X را که در $X_1 \cup X_2$ نباشد را انتخاب می‌کنیم و از اینجا به دور σ_3 می‌رسیم. چون X متناهی است این روند در جایی متوقف می‌شود. ازاین‌رو به مجموعه‌های دوبه دو مجزای $X_1, X_2, ... X_m$، که $X = X_1 \cup X_2 \cup ... \cup X_m$ و دورهای $\sigma_1, \sigma_2, ..., \sigma_m$ خواهیم رسید. مجزا بودن σ_iها از مجزا بودن X_iها نتیجه می‌شود. از طرفی اگر $x \in X$، آنگاه عدد $1 \le i \le m$ چنان موجود است که $x \in X_i$. دراین‌صورت اثر σ بر x همان اثر σ_i بر x خواهد بود و درنتیجه

$$\sigma = \sigma_1 \sigma_2 ... \sigma_m.$$

بدین ترتیب اثبات قضیه کامل است.

■■■

خواننده می‌تواند نشان دهد که نمایش یک جایگشت به حاصل ضرب دورهای مجزا، قطع نظر از وجود دورهای به‌طول ۱ و ترتیب دورها، منحصر به فرد است.

www.mathematic87.blogfa.com

تعریف ۳-۳

هر دور به‌طول ۲ را یک **ترانهش** می‌گوییم.

یعنی یک ترانهش، تمام عناصر مجموعه به جز دو عنصر را ثابت نگه می‌دارد و هر یک از این دو عنصر را به دیگری می‌نگارد.

نتیجه زیر با توجه به قضیه فوق و این مطلب که

$$(a_1\ a_2\ \dots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_3)(a_1\ a_2)$$

به دست می‌آید.

نتیجه ۳-۱

هر جایگشت $\sigma \in S_n$ حاصل ضربی از ترانهش‌ها است.

مثال ۵:

$$(1\ 6)(2\ 5\ 3) = (1\ 6)(2\ 3)(2\ 5) = (1\ 6)(4\ 5)(2\ 3)(4\ 5)(2\ 5),$$
$$\mathrm{id} = (1\ 2)(1\ 2) = (1\ 3)(2\ 4)(1\ 3)(2\ 4).$$

■

با توجه به مثال قبل ملاحظه می‌شود که در نمایش یک جایگشت به صورت ترانهش‌ها، اولاً نمایش مذکور منحصر به فرد نیست، ثانیاً، ترانهش‌ها می‌توانند مجزا نباشند. اما این واقعیت همیشه هست که تعداد ترانهش‌های به کار رفته برای جایگشتی مفروض باید یا همواره زوج باشد یا همواره فرد. برای اثبات این مطلب احتیاج به لم زیر(حالت خاص مطلب) داریم.

لم ۳-۲

اگر جایگشت همانی به صورت حاصل ضرب n ترانهش نوشته شود،

$$\mathrm{id} = \tau_1\tau_2\dots\tau_{n-1}\tau_n, \qquad (*)$$

آنگاه n باید عددی زوج باشد.

اثبات: فرض کنید عدد m در ترانهش، τ_n ظاهر شده باشد. در این صورت $\tau_{n-1}\tau_n$ ناچار باید به شکل طرف چپ یکی از تساوی‌های زیر باشد.

www.mathematic87.blogfa.com

$$(m\ a)(m\ a) = \mathrm{id},$$
$$(m\ y)(m\ a) = (m\ a)(a\ y),$$
$$(b\ c)(m\ a) = (m\ a)(b\ c),$$
$$(a\ b)(m\ a) = (m\ b)(a\ b).$$

اگر $\tau_{n-1}\tau_n$ به شکل طرف چپ تساوی اول باشد، قرار می دهیم $\tau_{n-1}\tau_n = \mathrm{id}$. به عبارت دیگر از تساوی $(*)$ دو ترانهش حذف می‌شود. اگر $\tau_{n-1}\tau_n$ به شکل طرف چپ تساویهای بعدی باشد، به جای $\tau_{n-1}\tau_n$ طرف راست تساوی‌های مربوطه را قرار می‌دهیم. بنابراین وقوع m یک مرحله به سمت چپ حرکت داده می‌شود. با تکرار این عمل، m از تساوی $(*)$ حذف می‌شود و تساوی $(*)$ به صورت id=idid...id تبدیل شود (البته باید توجه داشت که به حالتی نخواهیم رسید که m فقط در τ_1 باشد). با توجه به این که تعداد ترانهش‌های جایگزین شده در هر جانشینی یا تغییر نمی‌کند یا 2 تا کم می‌شود، ملاحظه می‌کنیم که n باید زوج باشد.

■■■

قضیه۳-۳

هیچ جایگشتی از یک مجموعه متناهی نمی‌تواند هم به صورت حاصل ضرب از تعداد زوجی ترانهش و هم به صورت حاصل ضربی از تعداد فردی ترانهش نوشته شود.

اثبات: فرض کنید

$$\sigma = \sigma_1\sigma_2...\sigma_r = \tau_1\tau_2...\tau_s$$

چون هر ترانهش معکوش خودش است، خواهیم داشت:

$$\mathrm{id} = \sigma\sigma^{-1} = \sigma_1...\sigma_r\left(\tau_1...\tau_s\right)^{-1} = \sigma_1...\sigma_r\tau_s...\tau_1$$

با توجه به لم قبل $r+s$ باید عددی زوج باشد. بنابراین r و s یا هر دو زوج‌اند یا هر دو فرد.

■■■

تعریف ۳-۴

یک جایگشت از یک مجموعه متناهی **زوج** یا **فرد** است برحسب اینکه تعداد ترانهش‌های هر تجزیه آن به حاصل ضرب ترانهش‌ها به ترتیب زوج یا فرد باشد. فرض کنید A_n مجموعهٔ جایگشتهای زوج S_n باشد. به آسانی میتوان بررسی کرد که A_n زیرگروهی از مرتبهٔ $n!/2$ از S_n است (تمرین۴(a)). A_n را **گروه متناوب از درجه** n می‌نامند.

مثال۶:

$$A_4 = \{(1),\ (2\ 4\ 3),\ (2\ 3\ 4),\ (1\ 4\ 3),(1\ 3\ 4),\ (1\ 4\ 2),\ (1\ 2\ 4),\ (1\ 3\ 2),\ (1\ 2\ 3),$$
$$(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

■

۳-۵ تقارن‌ها

منظور از یک **تقارن** از یک شکل هندسی که دارای n رأس بوده (رأسهای آن با اعداد $1,2,\ldots,n$ شماره گذاری شده‌اند)، جایگشتی از رئوس مانند $\sigma \in S_n$ است، به‌نحوی که فاصلهٔ بین هر دو رأس حفظ شود، یعنی برای هر $k, m \in \{1,2,\ldots,n\}$ داشته باشیم:

$$d(k,m) = d(\sigma(k), \sigma(m)),$$

که در اینجا $d(x,y)$ نشان دهندهٔ فاصلهٔ نقاط x, y در فضا می‌باشد.

قضیه۳-۴

مجموعه همه تقارن‌های هر شکل هندسی که n رأس داشته باشد، زیرگروهی از S_n است.

اثبات: جایگشت همانی به وضوح یک تقارن است. اگر τ, δ دو تقارن باشند، آنگاه به ازای هر دو رأس m, k داریم:

www.mathematic87.blogfa.com

$$d\big((\delta\tau)(k),(\delta\tau)(m)\big)=d\big(\delta(\tau k),\delta(\tau m)\big)=d(\tau k,\tau m)=d(k,m),$$
$$d\big(\delta^{-1}k,\delta^{-1}m\big)=d\big(\delta\delta^{-1}k,\delta\delta^{-1}m\big)=d(k,m).$$

بنابراین $\delta\tau$ و δ^{-1} نیز یک تقارن می‌باشند.

■■■

بدیهی است که هر حرکت ازیک شکل هندسی یک تقارن است. در حالیکه عکس آن درست نیست. اینک مثالی ارایه می‌دهیم که نشان دهد هر تقارن لزوماً یک حرکت نیست.

مثال۷: گروه حرکت‌های یک چهار وجهی منظم A_4 می‌باشد.

مجموعه حرکت‌های چهاروجهی منظم به صورت‌های زیر می‌باشد:

(۱): حرکت (جایگشت) همانی id.

(۲): دوران به اندازه 120° یا 240° حول محوری که از یک رأس و مرکز وجه مقابل می‌گذرد:

$$(1\ 2\ 3),(1\ 3\ 2),(1\ 2\ 4),(1\ 4\ 2),(1\ 3\ 4),(1\ 4\ 3),(2\ 3\ 4)\text{و}(2\ 4\ 3)$$

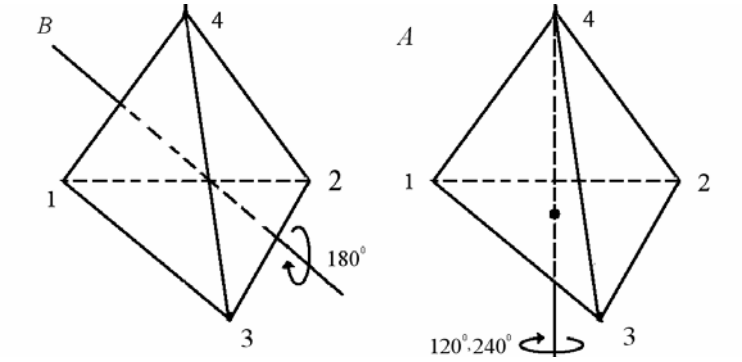
بعنوان مثال، همان طوری که در شکل زیر (قسمت A) نشان داده شده، دورهای $(1\ 2\ 3)$و $(1\ 3\ 2)$ نمایانگر حرکت‌هایی از چهار وجهی است که آن را به اندازه 120° و 240° حول محوری که از رأس و مرکز وجه مقابل آن می‌گذرد، می‌چرخاند.

(۳): دوران‌های 180° حول محورهای گذرنده بر وسط‌های دو یال مقابل:

$$(1\ 2)(3\ 4)\text{ و }(1\ 3)(2\ 4),(1\ 4)(2\ 3)$$

بعنوان مثال شکل زیر (قسمت B) جایگشت $(1\ 4)(2\ 3)$ را به دست می‌دهد.

www.mathematic87.blogfa.com



اگر گروه حرکتهای چهار وجهی را G بنامیم، با توجه به توضیحات فوق $A_4 \subseteq G$ از طرفی اگر $\delta \in G$ جایگشت فردی باشد آنگاه $\tau = (1\ 2)\delta$ جایگشتی زوج می‌شود و بنابراین $(1\ 2) = \tau\delta^{-1} \in G$، که این غیر ممکن است چون که هیچ حرکتی از این چهار وجهی وجود ندارد که فقط جای 1و 2 را عوض کند بدون آن که تغییری در $3,4$ به وجود آورد. بنابراین $G = A_4$.

■

❖ **تذکر:** هر حرکت از یک شکل هندسی یک تقارن است ولی عکس این مطلب درست نیست. به عنوان مثال $(1\ 2)$ یک تقارن از چهار وجهی است در صورتی که حرکت نیست.

قضیه ۳-۵

گروه تقارن‌های چهار وجهی منظم S_4 می‌باشد.

اثبات: فرض کنید G گروه تقارن‌های چهار وجهی منظم باشد. در این صورت $A_4 \subseteq G \subseteq S_4$ از طرفی چون $(1\ 2) \in G$، لذا $G \neq A_4$. با توجه به اینکه $A_4 \cap (1,2)A_4 = \varnothing$، داریم

$$|G| \geq |A_4 \cup (1,2)A_4| = |A_4| + |(1,2)A_4| = 4!/2 + 4!/2 = 4!.$$

بنابراین $G = S_4$.

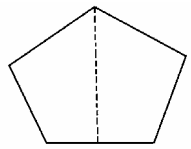
■■■

این بخش را با بررسی گروه حرکت n-**ضلعی منظم** به پایان می‌رسانیم. مجموعهٔ عناصر این گروه عبارتند از:

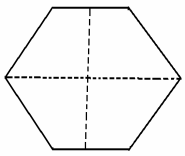
www.mathematic87.blogfa.com

(۱): دوران به اندازه $2\pi/n$ رادیان حول مرکز شکل.

(۲) (a): برای nهای فرد، دوران به اندازه π رادیان حول محوری که یک رأس را به نقطه وسط ضلعی که دقیقاً روبروی آن است وصل می‌کند (شکل زیر ملاحظه شود).



(b): برای n های زوج، دو نوع دوران (انعکاس) داریم یکی دوران به اندازه π رادیان حول محوری که دو رأس روبرو را به هم وصل می‌کند و دیگری دوران به اندازه π رادیان حول محوری که نقاط وسط دو ضلع روبرو را به هم وصل می‌کند (شکل زیر ملاحظه شود).



بنابراین با توجه به این که دقیقاً n حرکت از نوع (۱) و دقیقاً n حرکت از نوع (۲) داریم، پس گروه همه حرکت‌های یک $n-$ضلعی منظم از مرتبه $2n$ است این گروه را **گروه دو وجهی از مرتبهٔ** $2n$ نامیده و با D_n نمایش می‌دهیم (بعضی از کتب این گروه را با D_{2n} نیز نمایش می‌دهند).

فرض کنید $\delta = (1\ 2\ 3\ \ldots\ n)$ دورانی به اندازه $2\pi/n$ رادیان حول مرکز شکل و $\tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n-1 & n-2 & \ldots & 1 & n \end{pmatrix}$ دورانی به اندازه π رادیان حول محوری که از رأس n ام و مرکز شکل می‌گذرد باشند، با توجه به این که $\circ(\delta) = n$ و $\circ(\tau) = 2$ خواهیم داشت:

$$D_n = \left\{\mathrm{id}, \delta, \delta^2, \ldots, \delta^{n-1}, \tau, \tau\delta, \tau\delta^2, \ldots, \tau\delta^{n-1}\right\}$$

www.mathematic87.blogfa.com

از طرفی

$$\begin{aligned}
&1 \xrightarrow{\delta} 2 \xrightarrow{\tau} n-2 \xrightarrow{\delta} n-1,\\
&2 \xrightarrow{\delta} 3 \xrightarrow{\tau} n-3 \xrightarrow{\delta} n-2,\\
&\quad\vdots \qquad\quad \vdots \qquad\quad \vdots\\
&n-1 \xrightarrow{\delta} n \xrightarrow{\tau} n \xrightarrow{\delta} 1,\\
&n \xrightarrow{\delta} 1 \xrightarrow{\tau} n-1 \xrightarrow{\delta} n.
\end{aligned}$$

بنابراین در یک جمع بندی قضیه زیر را خواهیم داشت.

قضیه۳-۶

برای $n \geq 3$، گروه حرکت‌های $n-$ضلعی منظم برابر است با

$$D_n = \left\{\mathrm{id}, \delta, \delta^2, ..., \delta^{n-1}, \tau, \tau\delta, \tau\delta^2, ..., \tau\delta^{n-1}\right\},$$

که در آن $\circ(\delta) = n$، $\circ(\tau) = 2$ و $\delta\tau\delta = \tau$.

در تمرینها از خواننده خواسته شده که نشان دهد گروه حرکت وتقارن هر $n-$ضلعی منظم یکسانند(تمرین۲۰).

❖ **تذکر:** در واقع اگر شکل هندسی مورد نظر مسطح باشد آنگاه، طبق قضیه‌ای در هندسهٔ مسطحه، گروه حرکت و تقارن آن یکسانند.

تمرینها

۱. هر یک از جایگشت‌های زیر را به صورت حاصل ضرب دورهای مجزا بنویسید.

(a) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&7&9&8&2&1&6&3&5\end{pmatrix}$، (b) $\begin{pmatrix}1&2&3&4&5&6&7\\6&3&1&7&5&2&4\end{pmatrix}$.

۲. زوج و فرد بودن جایگشت‌های زیر را مشخص کنید.

(a) $(1\ 4\ 3\ 5\ 6)$، (b)

$(1\ 4\ 2\ 6)(1\ 4\ 2)$،

(c) $\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&1&6&7&5\end{pmatrix}$.

www.mathematic87.blogfa.com

۳. وارون دور $(a_1\ a_2\ \dots\ a_n)$ به‌طول n را بیابید.

۴.(a) ثابت کنید A_n زیرگروهی از مرتبهٔ $n!/2$ از S_n است،

(b) ثابت کنید در S_n تعداد $\frac{1}{r}\frac{n!}{(n-r)!}$ دور متمایز از طول r موجود است.

۵. مطلوب است تمام زیر گروه‌های A_4.

۶. عناصر S_5, S_4 از چه مرتبه‌هایی می‌توانند باشند.

۷ . نشان دهید A_{10} دارای عنصری از مرتبه 15 است.

۸ . مطلوب است بزرگترین عنصر از لحاظ مرتبه در S_n برای $n = 3,\dots,10$.

۹ . اگر τ, δ دو جایگشت مجزا باشند، آنگاه $\circ(\tau\delta) = [\circ(\tau), \circ(\delta)]$.

۱۰.(a) فرض کنید $\delta \in S_n$. نشان دهید δ را می‌توان به صورت حاصل ضرب حداکثر $n-1$ ترانهش نوشت،

(b) ثابت کنید دور $(a_1\ a_2\ \dots\ a_n)$ را نمی‌توان به‌صورت حاصل‌ضرب تعدادی کمتر از $n-1$ ترانهش نوشت.

۱۱ . فرض کنید $\delta \in S_n$. اگر δ دور نباشد، نشان دهید δ را می‌توان به صورت حاصل ضرب حداکثر $n-2$ ترانهش نوشت.

۱۲ . فرض کنید δ دوری به‌طول فرد باشد. ثابت کنید δ^2 نیز یک دور است.

۱۳. A_n برای $n \geq 3$ با دورهای به‌طول 3 تولید می‌شود.

۱۴. نشان دهید:

(a) اگر n فرد باشد، آنگاه $A_n = <(1\ 2\ 3), (1\ 2\ \dots\ n)>$،

(b) اگر n زوج باشد، آنگاه $A_n = <(1\ 2\ 3), (2\ 3\ \dots\ n)>$.

۱۵. نشان دهید S_n با هر یک از مجموعه‌های زیر تولید می‌شود.

(a) $\{(1\ 2), (2\ 3), \dots, (n-1\ n)\}$, (b) $\{(1\ 2), (1\ 2\ \dots\ n)\}$.

۱۶. مرکز D_8 و D_{10} را بیابید (تمرین ۱۹ فصل ۱ ملاحظه شود). نشان دهید:

$$C(D_n) = \begin{cases} \mathrm{id} & 2 \nmid n \\ <\delta^{n/2}> & 2 \mid n \end{cases}$$

۱۷. نشان دهید:

www.mathematic87.blogfa.com

(a) اگر $n \geq 3$، آنگاه $C(S_n) = \{\mathrm{id}\}$ (b) اگر $n \geq 4$، آنگاه $C(A_n) = \{\mathrm{id}\}$.

۱۸. فرض کنید p یک عدد اول باشد. ثابت کنید $S_p =< \sigma, \tau >$، که در آن σ یک ترانهش و τ یک دور به‌طول p است. اگر p اول نباشد چه می‌توان گفت؟

۱۹. ثابت کنید هر عنصر از مرتبهٔ 2 در A_n مربع عنصری از مرتبهٔ 4 در S_n است.

۲۰. نشان دهید گروه حرکت و تقارن هر $n-$ضلعی منظم یکسانند.

مسائل مبارزه طلب

۱. فرض کنید δ دوری به‌طول n باشد . نشان دهید δ^k یک دور است اگر و فقط اگر $(n,k) = 1$.

۲. فرض کنید p عددی اول باشد. نشان دهید در S_p تعداد $(p-1)!+1$ عنصر هست که در معادلهٔ $x^p = e$ صدق می‌کنند.

۳. فرض کنید $n > m > 1$ و $G =< (1\ 2\ \ldots\ m), (1\ 2\ \ldots\ n) >$. ثابت کنید G شامل یک دور به‌طول 3 است.

۴. نشان دهید $H =< (1\ 2\ 3\ 4\ 5\ 6\ 7), (2\ 6)(3\ 4) >$ یک زیرگروه 168 عنصری از S_7 است.

۵. مطلوب است گروه حرکت و گروه تقارن یک مکعب.

منابعی برای مطالعهٔ بیشتر

۱. درفشه، محمدرضا. **مقدمه‌ای بر نظریهٔ گروه‌ها**. نشر علوم پایه، چاپ اول (۱۳۶۹).

2. Fraleigh, J. B. *A First Course in Abstract Algebra*. Addison-Wesley, 1999.

3. Herstein, I. N. *Topics in Algebra*. New York , Blaisdell, 1984.

www.mathematic87.blogfa.com

فصل ۴

هم دسته‌ها و قضیه لاگرانژ

در این فصل می‌خوانید:

۴-۱ هم‌دسته‌ها
۴-۲ قضیه لاگرانژ
۴-۳ عکس قضیه لاگرانژ
۴-۴ قضیه اویلر و قضیه فرما

مقدمه

قضیه لاگرانژ، یکی از مهم‌ترین نتایج نظریه گروه‌های متناهی است. این قضیه بیان می‌کند که مرتبه هر زیر گروه مرتبه گروه را عاد می‌کند. این قضیه ابزاری بسیار قوی در آنالیز گروه‌های متناهی است، که به ما می‌گوید یک گروه چه نوع زیرگروه‌هایی می‌تواند داشته باشد. مبحث هم‌دسته‌ها برای فهم قضیه لاگرانژ نیازی اساسی است.

۴-۱ هم‌دسته‌ها

تعریف ۴-۱

فرض کنید G یک گروه و $H \leq G$. اگر $g \in G$، آنگاه مجموعه $Hg = \{hg | h \in H\}$ را یک **هم‌دسته راست** H در G و مجموعه $gH = \{gh | h \in H\}$ را یک **هم‌دسته چپ** H در G می‌نامند.

مثال۱: فرض کنید $G = \mathbb{Z}_6$، $H = \{0,3\}$. در این صورت

$$H + 0 = H + 3 = \{0,3\},$$
$$H + 1 = H + 4 = \{1,4\},$$
$$H + 2 = H + 5 = \{2,5\}.$$

■

❖ **تذکر:** در گروه‌های آبلی (مانند مثال بالا) هم‌دسته‌های راست و چپ یکی‌اند.

مثال۲ : فرض کنید $G = S_3$، $H = \{(1), (1\ 2)\} \leq G$ در این صورت هم‌دسته‌های راست H در G عبارتند از:

$$H(1) = H(1\ 2) = H,$$
$$H(1\ 3) = H(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\},$$
$$H(2\ 3) = H(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}.$$

و هم‌دسته‌های چپ عبارتند از

$$(1)H = (1\ 2)H = H,$$
$$(1\ 3)H = (1\ 2\ 3)H = \{(1\ 3), (1\ 2\ 3)\},$$
$$(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}.$$

همان طوری که مشاهده می‌شود هم‌دسته‌های راست و چپ H در G لزوماً یکی نیستند.

■

www.mathematic87.blogfa.com

قضیه ۴-۱

فرض کنید H یک زیر گروه از G باشد. در این صورت

(۱) اگر $g \in G$، آنگاه $g \in H \Leftrightarrow Hg = H$ و $g \in H \Leftrightarrow gH = H$.

(۲) برای هر $g_1, g_2 \in H$،

$g_1 H = g_2 H \Leftrightarrow g_1^{-1} g_2 \in H$ و $Hg_1 = Hg_2 \Leftrightarrow g_2 g_1^{-1} \in H$.

(۳) اگر $g \in G$، آنگاه $|H| = |Hg| = |gH|$.

(۴) برای هر $g_1, g_2 \in H$،

$g_1 H = g_2 H$ یا $g_1 H \cap g_2 H = \varnothing$ و $Hg_1 = Hg_2$ یا $Hg_1 \cap Hg_2 = \varnothing$.

(۵) مجموعه همدسته‌های راست (چپ) H در G یک افراز برای G است.

(۶) اگر $\mathscr{R}_H$، $\mathscr{L}_H$ به ترتیب مجموعه تمام همدسته‌های راست و چپ H در G باشند، آنگاه $|\mathscr{R}_H| = |\mathscr{L}_H|$.

اثبات: به دلیل تشابه، قضیه را فقط در مورد همدسته‌های راست ثابت می‌کنیم.

(۱) $(\Leftarrow)$: فرض کنید $Hg = H$. چون $e \in H$ پس $g = eg \in Hg = H$.

$(\Rightarrow)$: چون H زیر گروهی از G است، پس $Hg \subseteq H$ و $Hg^{-1} \subseteq H$. بنابراین

$$H = (Hg^{-1})g \subseteq Hg \subseteq H.$$

از اینرو $Hg = H$.

(۲): به آسانی از قسمت (۱) به دست می‌آید.

(۳): به آسانی می‌توان نشان داد که تابع $Hg \to H$ با ضابطه $hg \mapsto h$ دو سویی است.

(۴): فرض کنید $Hg_1 \cap Hg_2 \neq \varnothing$. بنابراین عناصر $h_1, h_2 \in H$ چنان موجودند که $a = h_1 g_1 = h_2 g_2$ و از اینجا، $g_2 g_1^{-1} = h_2^{-1} h_1 \in H$ و طبق قسمت (۲)، $Hg_1 = Hg_2$.

(۵): از قسمت (۴) و این واقعیت که $G = \bigcup_{g \in G} Hg$ بدست می‌آید.

(۶): تعریف می‌کنیم:

$$\varphi : \mathscr{R}_H \to \mathscr{L}_H$$
$$\varphi(Hg) = g^{-1}H$$

ابتدا نشان می‌دهیم که φ خوش تعریف است. اگر $Hg_1 = Hg_2$، آنگاه $g_2g_1^{-1} \in H$ و در نتیجه $g_1^{-1}H = g_2^{-1}H$.

حال ثابت می‌کنیم که φ دو سویی است. اگر $\varphi(Hg_1) = \varphi(Hg_2)$، آنگاه $g_1^{-1}H = g_2^{-1}H$. بنابراین $g_2g_1^{-1} \in H$ و در نتیجه $Hg_1 = Hg_2$. یعنی φ یک به یک است. بالاخره برای هر $gH \in \mathscr{L}_H$ داریم:

$$\varphi(Hg^{-1}) = (g^{-1})^{-1}H = gH,$$

یعنی φ پوشا است.

■■■

با توجه به قسمت (۶) قضیه قبل، تعریف زیر را خواهیم داشت:

تعریف۴-۲

فرض کنید G یک گروه و $H \leq G$. تعداد هم‌دسته‌های راست یا چپ (متناهی یا نامتناهی) H در G را **اندیس** H در G نامیده وبا $[G : H]$ نمایش می‌دهیم.

مثال۳ : فرض کنید $G = \mathbb{Z}_6$، $H = \{0,3\}$. در این صورت $[G : H] = 3$.

■

مثال۴: فرض کنید $G = S_3$، $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. در این صورت $[G : H] = 2$.

■

در مورد اندیس زیر گروه‌های یک گروه، **قضیه اساسی** زیر را داریم.

www.mathematic87.blogfa.com

قضیه ۴-۲

فرض کنید H، K زیر گروه‌هایی از گروه G باشند به طوری که $K \leq H \leq G$. در این صورت

$$[G:K]=[G:H][H:K].$$

اثبات: با توجه به قسمت (۴) و (۵) قضیه قبل خواهیم داشت، $G=\bigcup_{i\in I} Ha_i$ که $a_i \in G$ و Ha_i ها مجزا و $|I|=[G:H]$. به طور مشابه $H=\bigcup_{j\in J} Kb_j$ که $b_j \in H$ و Kb_j ها مجزا و $|J|=[H:K]$. بنابراین:

$$G=\bigcup_{i\in I} Ha_i=\bigcup_{i\in I}(\bigcup_{j\in J} Kb_j)a_i=\bigcup_{(i,j)\in I\times J} Kb_ja_i.$$

اگر نشان دهیم Kb_ja_i مجزایند، آنگاه

$$[G:K]=|I\times J|=|I||J|=[G:H][H:K],$$

و قضیه اثبات است. اگر $Kb_ja_i \cap Kb_ta_s \neq \varnothing$، آنگاه طبق قسمت (۴) قضیه قبل $Kb_ja_i=Kb_ta_s$ و در نتیجه $k\in K$ چنان موجود است که $b_ja_i=kb_ta_s$. با توجه به این که $k\in H$، b_j، b_t داریم:

$$Ha_i=Ha_s.$$

در نتیجه $i=s$ و لذا $b_j=kb_t$. بنابراین $Kb_j=Kb_t$ و در نتیجه $j=t$. یعنی نشان داده‌ایم که Kb_ja_i ها مجزایند.

■■■

www.mathematic87.blogfa.com

قضیه ۴-۳ (قضیه لاگرانژ)

فرض کنید G یک گروه $H \leq G$. در این صورت

$$|G| = [G : H]|H|.$$

اثبات: در قضیه قبل قرار دهید $K = \{e\}$.

■■■

نتیجه۴-۱

فرض کنید G یک گروه متناهی باشد. در این صورت

(۱) اگر $H \leq G$، آنگاه $|H| \| |G|$ (مرتبه H مرتبه G را عاد می‌کند)،

(۲) اگر $g \in G$، آنگاه $\circ(g) \| |G|$ (مرتبه g مرتبه G را عاد می‌کند)،

(۳) اگر $g \in G$، آنگاه $g^{|G|} = e$.

اثبات (۱): نتیجه مستقیم قضیه لاگرانژ است.

(۲): چون $\circ(g) = |\langle g \rangle|$، لذا طبق قسمت (۱) خواهیم داشت $\circ(g) \| |G|$.

(۳): از قسمت (۲) بدست می‌آید.

■■■

نتیجه۴-۲

فرض کنید G گروهی از مرتبه عددی اول باشد. در این صورت G دوری بوده و دارای زیر گروه غیر بدیهی نمی‌باشد.

اثبات: فرض کنید $|G| = p$ عددی اول و $g \in G$ عنصر غیر همانی باشد. با توجه به این که $\circ(g) \| |G|$ داریم $\circ(g) = p$ و در نتیجه $G = \langle g \rangle$ و دوری است. به علاوه چون $|G| = p$، بنابر قضیه لاگرانژ به سادگی دیده می‌شود که G زیر گروهی جز $\{e\}$ و G ندارد.

■■■

اگر H و K زیرمجموعه‌های غیر تهی از یک گروه G باشند، آنگاه **حاصل ضرب** HK به صورت زیر تعریف می‌شود:

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

درحالت کلی اطلاعات زیادی در مورد HK نداریم. حتی اگر H، K هر دو زیر گروه‌هایی از یک گروه G باشند، باز هم ممکن است HK زیر گروه G نباشد (تمرین ۱۷ و۱۸ فصل۱ ملاحظه شود). اما در مورد تعداد عناصر HK داریم:

قضیه۴-۴

فرض کنید H، K زیر گروه‌های متناهی از یک گروه G باشند. در این صورت

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

اثبات: فرض کنید:

$$n = [K : H \cap K] = \frac{|K|}{|H \cap K|}.$$

از این‌رو

$$K = (H \cap K)k_1 \cup (H \cap K)k_2 \cup ... \cup (H \cap K)k_n,$$

که $k_i \in K$ و $(H \cap K)k_i$ ها مجزایند. با توجه به این که $H(H \cap K) = H$ داریم:

$$HK = Hk_1 \cup Hk_2 \cup ... \cup Hk_n.$$

حال فرض کنید $i \neq j$ و $Hk_i \cap Hk_j \neq \varnothing$. در این‌صورت عناصر $h' \in H$، h وجود دارند به قسمی که $hk_i = h'k_j$، از این‌رو $k_i k_j^{-1} = h^{-1}h'$ و لذا:

$$k_i k_j^{-1} \in H \cap K.$$

ازاین‌رو $(H \cap K)k_i = (H \cap K)k_j$، که تناقض است. در نتیجه به ازای هر i، j که $i \neq j$، $Hk_i \cap Hk_j = \varnothing$. بنابراین

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

■■■

www.mathematic87.blogfa.com

نتیجه۴-۳

اگر H، K زیر گروه‌هایی از یک گروه متناهی G باشند به طوری که $|H|>\sqrt{|G|}$، $|K|>\sqrt{|G|}$ آنگاه $H\cap K\neq\{e\}$.

اثبات: با توجه به این که $HK\subseteq G$، داریم:

$$|G|\geq|HK|=\frac{|H|.|K|}{|H\cap K|}>\frac{\sqrt{|G|}\sqrt{|G|}}{|H\cap K|}=\frac{|G|}{|H\cap K|},$$

و لذا $|H\cap K|>1$.

■■■

قضیه۴-۵

اگر H و K زیر گروه‌هایی از گروه G باشند، آنگاه

$$[K:H\cap K]\leq[G:H]$$

و اگر $[G:H]$ متناهی باشد، آنگاه

$$[K:H\cap K]=[G:H]\Leftrightarrow G=HK.$$

اثبات: فرض کنید A مجموعه همه هم‌دسته‌های راست $H\cap K$ در K و B مجموعه همه هم‌دسته‌های راست H در G باشد. تعریف می‌کنیم:

$$\varphi: A \to B$$
$$(H\cap K)k\mapsto Hk$$

بوضح φ تابعی یک به یک است. بنابراین

$$[K:H\cap K]=|A|\leq|B|=[G:H].$$

اگر $[G:H]$ متناهی باشد، آنگاه $[K:H\cap K]=[G:H]$ اگر و فقط اگر φ پوشا باشد. از طرف دیگر φ پوشا است اگر و فقط اگر $G=HK$.

■■■

نتیجه۴-۴

فرض کنید H، K دو زیر گروه با اندیس متناهی از گروه G باشند. در این صورت $[G : H \cap K]$ متناهی است و

$$[G : H \cap K] \leq [G : H][G : K].$$

علاوه بر این

$$[G : H \cap K] = [G : H][G : K] \Leftrightarrow G = HK.$$

اثبات: به آسانی از قضیه قبل نتیجه می‌شود.

■■■

۴-۳ عکس قضیه لاگرانژ

قضیه لاگرانژ بیان می‌کند که اگر H زیرگروهی از گروه متناهی G باشد، آنگاه $d = |H|$ مقسوم علیهی از $|G|$ است. اکنون این سؤال مطرح می‌شود که آیا عکس این قضیه درست است؟ یعنی اگر G یک گروه متناهی باشد و d مقسوم علیهی از $|G|$، آیا G دارای زیر گروهی از مرتبه d هست؟

این مطلب در مورد گروه‌های آبلی درست است (تمرین (a)۹ از فصل۷)، ولی در حالت کلی جواب منفی است.

تعریف۴-۳

فرض کنید G یک گروه باشد. اگر $a, b \in G$، گوییم a **مزدوج** b است اگر عنصری مانند $g \in G$ وجود داشته باشد به طوری که $gag^{-1} = b$.

قضیه۴-۶

فرض کنید α، β دو دور در S_n باشند. دراین صورت:

α، β دارای طول یکسانی باشند $\Leftrightarrow$ α مزدوج β است.

اثبات ($\Rightarrow$): فرض کنید $\alpha = (a_1\ a_2\ \dots\ a_k)$، $\sigma \in S_n$ چنان باشد که $\beta = \sigma\alpha\sigma^{-1}$. در این صورت

$$\beta = \sigma\alpha\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \dots\ \sigma(a_k)),$$

یعنی α، β دارای طول یکسانند.

($\Leftarrow$): فرض کنید $\alpha = (a_1\ a_2\ \dots\ a_k)$، $\beta = (b_1\ b_2\ \dots\ b_k)$. قرار می‌دهیم:

$$\{x_1, x_2, \dots, x_{n-k}\} = \{1,2,\dots,n\} - \{a_1, a_2, \dots, a_k\},$$
$$\{y_1, y_2, \dots, y_{n-k}\} = \{1,2,\dots,n\} - \{b_1, b_2, \dots, b_k\}.$$

جایگشت $\sigma \in S_n$ را به‌صورت زیر تعریف می‌کنیم:

$$\sigma(x) = \begin{cases} b_i & x = a_i \\ y_i & x = x_i \end{cases}$$

در این صورت $\sigma\alpha\sigma^{-1} = \beta$، یعنی α مزدوج β است.

■■■

نتیجه۴-۵

A_4 دارای زیرگروهی از مرتبه 6 نیست.

اثبات: فرض کنید H زیرگروهی از A_4 با مرتبه 6 باشد. ابتدا نشان می‌دهیم که برای هر $\sigma \in A_4$، $\sigma H = H\sigma$ (به تمرین ۹ مراجعه شود). اگر $\sigma \in H$، مطلب واضح است. اگر $\sigma \notin H$ در این صورت چون $[G : H] = 2$ خواهیم داشت که،

$$\mathcal{L}_H = \{H, \sigma H\} \text{ و } \mathcal{R}_H = \{H, H\sigma\}$$

چون مجموعه هم‌دسته‌های راست وچپ H در G افرازهایی برای Gمی‌باشند، پس $\sigma H = H\sigma$.

چون A_4 دارای 8 هشت دور به‌طول 3 و H زیرگروهی از مرتبه 6 است، پس H باید شامل دوری به‌طول 3 مانند $(a\ b\ c)$ باشد. حال فرض کنید $(u\ v\ w)$دور دلخواهی به‌طول 3 از A_4 باشد. در این‌صورت با توجه به قضیه فبل، $\sigma \in A_4$ چنان موجود است که

www.mathematic87.blogfa.com

$$(u\ v\ w) = \sigma(a\ b\ c)\sigma^{-1} \in \sigma H\sigma^{-1} = H.$$

ازاین‌رو H شامل تمامی دورهای به‌طول 3 خواهد بود، که تناقض است.

■■■

۴-۴ قضیه اویلر و قضیه فرما

با استفاده از قضیه لاگرانژ بعضی از نتایج مهم نظریه اعداد را می‌توان به آسانی اثبات کرد.

تعریف۴-۴

تابع ϕ - اویلر یک تابع با دامنه $\mathbb{N}$ است که برای هر $n \geq 1$ به صورت زیر تعریف می‌شود:

$\phi(n) =$ تعداد اعداد طبیعی $1 \leq m < n$، که نسبت به n اول‌اند.

قضیه۴-۷ (قضیه اویلر)

فرض کنید n، a دو عدد صحیح که $n > 0$ و $(a,n) = 1$. در این صورت $a^{\phi(n)} \overset{n}{\equiv} 1$.

اثبات: فرض کنید $U(n)$ گروه یکه‌های $\mathbb{Z}_n$ باشد. دراین صورت با توجه به این که

$$|U(n)| = \phi(n) \text{ و } \overline{a} \in U(n)$$

داریم $\overline{a}^{\phi(n)} = \overline{1}$ ولذا $a^{\phi(n)} \overset{n}{\equiv} 1$.

■■■

حالت خاص قضیه اویلر (عددی اول $= n$)، منسوب به فرما می‌باشد.

قضیه ۴-۸ (قضیه کوچک فرما)

فرض کنید a یک عدد صحیح و p عدد اولی باشد که $p \nmid a$. در این صورت:

$$a^{p-1} \overset{p}{\equiv} 1.$$

علاوه بر این برای هر عدد صحیح b داریم:

$$b^p \overset{p}{\equiv} b.$$

www.mathematic87.blogfa.com

توضیح تاریخی

جاسب- لوئیس لاگرانژ $(1736-1813)$ متولد تورین ایتالیا دارای اجدادی ایتالیایی و فرانسوی است. استعداد ریاضیات وی در سنین کم ظهور پیدا کرد. لئونارد اویلر قدرت و توانایی لاگرانژ را در سن۱۹ سالگی موقعی که با وی روی حساب تغییرات کار می‌کرد، کشف کرد. در آن سال او استاد مدرسه رویال آدتیلری در تورین شد. در سن۲۳ سالگی به آکادمی برلین پیوست. کارهای او در نظریه اعداد، نظریه گروه‌ها، فیزیک، مکانیک، حساب تغییرات، نظریه معادلات و معادلات دیفرانسیل می باشد. او را می‌توان همراه با لاپلاس و لاوازییر به عنوان طراحان سیستم‌های متری نام برد.

تمرینها

۱. فرض کنید G یک گروه متناهی باشد. اگر G دارای زیر گروه‌هایی از مرتبه 7، 5 باشد، آنگاه $|G| \geq 35$.

۲. فرض کنید G یک گروه از مرتبه 60 باشد. مرتبه عناصر G چه اعدادی می‌توانند باشند.

۳. نشان دهید هر گروه از مرتبهٔ 10دارای زیرگروهی از مرتبهٔ 5است.

۴. مطلوب است مجموعهٔ هم‌دسته‌های چپ و راست زیر گروه‌های داده شده زیر:

(a) $\langle 8 \rangle$ در $\mathbb{Z}_{24}$،

(b) $3\mathbb{Z}$ در $\mathbb{Z}$،

(c) A_n در S_n،

(d) $\mathbb{T}$ در $\mathbb{C}^*$،

www.mathematic87.blogfa.com

(e) $H=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$ در S_4.

۵. ثابت کنید A_5 دارای زیرگروهی با اندیس $3,2$ و 4 نیست. زیرگروهی با اندیس 5 در A_5 بیابید.

۶. نشان دهید تعداد عناصر از مرتبهٔ عدد اول p در گروه متناهی G مضربی از $p-1$ است.

۷. نشان دهید رابطه مزدوج بودن در گروه G یک رابطه هم‌ارزی است.

۸. فرض کنید $|G|=2n$. نشان دهید G دارای عنصری از مرتبهٔ 2 است. اگر n فرد و G آبلی باشد، نشان دهید G فقط یک عنصر از مرتبهٔ 2 دارد.

۹. زیر گروه H از G را یک **زیرگروه نرمال** گوییم و با نماد $H\trianglelefteq G$ نمایش می‌دهیم، اگر $gH=Hg$ برای هر $g\in G$ (فصل ۶ ملاحظه شود).

فرض کنید $[G:H]=2$. در این‌صورت:

(a) اگر a، b در H نباشد، آنگاه $ab\in H$،

(b) $H\trianglelefteq G$.

۱۰. فرض کنید H و K دو زیر گروه از G و $g\in G$. نشان دهید $gH\cap gK$ یک هم‌دسته از $H\cap K$ در G است.

۱۱. فرض کنید H و K دو زیر گروه از G و $a,b\in G$. نشان دهید:

(a) اگر $aH=bK$، آنگاه $H=K$،

(b) اگر $aH\cap bK\neq\varnothing$، آنگاه $c\in G$ چنان موجود است که $c(H\cap K)=aH\cap bK$.

۱۲. فرض کنید H و K دو زیر گروه از G باشند و $[G:H]=m$، $[G:K]=n$. در این‌صورت اگر $(m,n)=1$ آنگاه $[G:H\cap K]=mn$.

۱۳. فرض کنید H زیرگروهی از G باشد بطوریکه $[G:H]=2$. اگر H و gH دو هم‌دسته چپ مجزای H در G باشند، نشان دهید $g^2\in H$.

۱۴. فرض کنید $|G|=2n$. اگر نصف عناصر G از مرتبهٔ 2 و نصف عناصر دیگر تشکیل گروهی مانند H از مرتبهٔ n بدهند . نشان دهید H از مرتبهٔ فرد و زیرگروهی آبلی از G است.

www.mathematic87.blogfa.com

۱۵. (a) فرض کنید H، K زیرگروه‌هایی از G باشند، رابطه $\sim$ روی G را به صورت زیر تعریف می‌کنیم:

$x \sim y$ اگر عناصر $h \in H$ و $k \in K$ بگونه‌ای موجود باشند که $y = hxk$.

نشان دهید که این رابطه یک رابطه هم‌ارزی روی G است،

(b) فرض کنید H و K دو زیر گروه متناهی از G باشند. در این‌صورت برای هر $x \in G$ داریم:

$$| HxK | = \frac{| H || K |}{| H \cap xKx^{-1} |}.$$

(c) فرض کنید H، K زیرگروه‌هایی از G باشند. فرض کنید:

$$N_K(H) = \{k \in K \mid kHk^{-1} = H\}.$$

$N_K(H)$ را **نرمال‌ساز** H در K گوییم. نشان دهید $N_K(H)$ زیر گروهی از G است. در حقیقت:

$$N_K(H) = N_G(H) \cap K.$$

(d) نشان دهید تعداد مزدوج‌های H القاء شده بوسیلهٔ عناصر K، یعنی $\left|\{kHk^{-1} \mid k \in K\}\right|$، برابر است با $[K : N_K(H)]$.

۱۶. فرض کنید p عددی اول و G گروهی از مرتبه p^n باشد. نشان دهید که G باید حاوی زیر گروهی از مرتبه p باشد. اگر $n \geq 3$ آیا G دارای زیرگروهی از مرتبه p^2 است؟

۱۷. فرض کنید G یک گروه دوری از مرتبه n باشد. نشان دهید G دارای $\phi(n)$ مولد است.

۱۸. برای عدد صحیح مثبت n نشان دهید:

$$n = \sum_{d|n} \phi(d).$$

۱۹. فرض کنید G یک گروه متناهی از مرتبهٔ n باشد. نشان دهید G دوری است اگر وفقط اگر برای هر مقسوم علیه d از n، زیر گروه منحصربفردی از مرتبهٔ d داشته باشیم.

۲۰. **(قضیهٔ ویلسون)** اگر p عددی اول باشد، آنگاه $(p-1)! \overset{p}{\equiv} -1$.

www.mathematic87.blogfa.com

مسائل مبارزه طلب

۱. فرض کنید G یک گروه متناهی مولد باشد و $H \leq G$. اگر $[G : H] < \infty$، آنگاه H متناهی مولد است.

۲. فرض کنید H ، K و L سه زیر گروه سره از Gباشند و $G = H \cup K \cup L$ ثابت کنید:

$$[G : H] = [G : K] = [G : L] = 2.$$

۳. فرض کنید Gگروهی متناهی باشد که به ازای هر $x \in G$ داشته باشیم $x^2 = e$. نشان دهید که $|G|$باید توانی از 2 باشد.

۴. فرض کنید $|G| = pq$،که pو qدو عدد اول می‌باشند و $p > q$. ثابت کنید Gحداکثر یک زیر گروه از مرتبهٔ p دارد.

۵. فرض کنید $m > 1$یک عدد طبیعی باشد. ثابت کنید $n \mid \phi(m^n - 1)$.

منابعی برای مطالعهٔ بیشتر

1. Cohn, P. M. *Algebra I,II*. John Wily, New York, 1974, 1977.
2. Herstein, I. N. *Abstract Algebra*. Macmillan, New York, 1986.
3. Lang, S. *Algebraic Number Theory*. Addison-Wesley, 1970.

www.mathematic87.blogfa.com

فصل ۵

یکریختی

در این فصل می‌خوانید:

۵-۱ یکریختی
۵-۲ قضیه کیلی
۵-۳ خودریختی‌ها
۵-۴ حاصل ضرب‌های مستقیم

مقدمه

همان طوری که می‌دانید گروه دوری $\mathbb{Z}_4$ با گروه چهار عنصری کلاین متفاوت است. مفهوم یکریختی برای نشان دادن تفاوت بین گروه‌های مختلف به وجود آمده است. تا کنون این احساس در شما به وجود آمده که دو گروه G و H دارای ساختار یکسانی (یکریخت) هستند، اگر قطع نظر از نام هر عنصر و نام عمل دو تایی مربوط کاملاً مثل هم باشند. هم اکنون مفهوم یکسان بودن ساختار یا یکریختی دو گروه G و H را به صورت دقیق ریاضی بیان می‌کنیم.

۵-۱ یکریختی

تعریف ۵-۱

فرض کنید G و H دو گروه باشند. تابع $\varphi: G \to H$ یک **یکریختی (ایزومورفیسم)** نامیده می‌شود اگر

(۱) ϕ یک به یک و پوشا باشد،

(۲) برای هر a,b در G، $\varphi(ab) = \varphi(a)\varphi(b)$.

وقتی از G به H یک یکریختی موجود باشد، می‌گوییم G با H **یکریخت (ایزومورف)** است و می‌نویسیم:

$$G \cong H.$$

اگر G با H یکریخت نباشد می‌نویسیم $G \ncong H$.

تذکر: توجه داشته باشید که در رابطهٔ $\varphi(ab) = \varphi(a)\varphi(b)$، ضرب ab در G بوده در حالی که ضرب $\varphi(a)\varphi(b)$ در H است.

مثال۱: نشان می‌دهیم $\mathbb{Z}_4 \cong \langle i \rangle$.

تابع $\phi: \mathbb{Z}_4 \to \langle i \rangle$ را با ضابطه $\varphi(n) = i^n$ تعریف می‌کنیم. به‌وضوح φ یک به یک و پوشا است و

$$\varphi(m+n) = i^{m+n} = i^m i^n = \varphi(m)\varphi(n).$$

■

مثال۲: نشان می‌دهیم $\mathbb{R}$ تحت عمل جمع با $\mathbb{R}^+$ تحت عمل ضرب یکریخت است. به‌وضوح تابع $\varphi: \mathbb{R} \to \mathbb{R}^+$ با ضابطه $\varphi(x) = e^x$ یک به یک و پوشا است و همچنین

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

■

برای این که نشان دهیم دو گروه G و H یکریخت نیستند باید نشان دهیم که هیچ یکریختی از G به H موجود نیست. به مثال‌های زیر توجه کنید.

مثال ۳: گروه S_3 با $\mathbb{Z}_4$ یکریخت نیست. هیچ تابع یک به یک و پوشایی از S_3 به $\mathbb{Z}_4$ وجود ندارد.

■

مثال۴: گروه جمعی $\mathbb{Z}$ با گروه جمعی $\mathbb{R}$ یکریخت نیست. (برهان خلف) فرض کنید $\varphi : \mathbb{Z} \to \mathbb{R}$ یک یکریختی باشد. دراین‌صورت $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$و در نتیجه $\varphi(0) = 0$. ازاین‌رو برای هر $n \in \mathbb{Z}$ داریم $0 = \varphi(n + (-n)) = \varphi(n) + \varphi(-n)$، یعنی $\varphi(-n) = -\varphi(n)$. حال فرض کنید $\varphi(1) = a$. چون φ پوشاست، پس $m \in \mathbb{Z}$ چنان موجود است که $\varphi(m) = a/2$. چون φ یک به یک است، پس $a \neq 0$ و درنتیجه $m \neq 0$. اگر $m > 0$، آنگاه

$$a/2 = \varphi(m) = \varphi(\underbrace{1+1+\cdots+1}_{m \text{ بار}}) = m\varphi(1) = ma.$$

درنتیجه $m = 1/2$، که تناقض است. اگر $m < 0$، آنگاه

$$-a/2 = -\varphi(m) = \varphi(-m) = \varphi(\underbrace{1+1+\cdots+1}_{-m \text{ بار}}) = -m\varphi(1) = -ma.$$

درنتیجه $m = 1/2$، که دوباره تناقض است. بنابراین گروه جمعی $\mathbb{Z}$ با گروه جمعی $\mathbb{R}$ یکریخت نیست.

- **تذکر:** این مثال را همچنین می‌توان با استفاده از نظریهٔ مجموعه‌ها بررسی کرد. در حقیقت، چون اعداد اصلی $\mathbb{Z}$و $\mathbb{R}$ متفاوتند، هیچ تابع یک به یک و پوشایی از $\mathbb{Z}$ به $\mathbb{R}$ موجود نیست و در نتیجه گروه جمعی $\mathbb{Z}$ با گروه جمعی $\mathbb{R}$ یکریخت نیست.

www.mathematic87.blogfa.com

خواننده برای اطلاع بیشتر در این مورد می‌تواند به کتب نظریه مجموعه‌ها (مبانی ریاضیات) رجوع کند.

■

مثال ۵: نشان می‌دهیم گروه جمعی $\mathbb{Q}$ با گروه ضربی $\mathbb{Q}^*$ یکریخت نیست.
فرض کنید $\varphi : \mathbb{Q} \to \mathbb{Q}^*$ یک یکریختی باشد. با توجه به پوشا بودن φ، عنصر $q \in \mathbb{Q}$ چنان موجود است که $\varphi(q) = 2$. داریم

$$2 = \varphi(q) = \varphi(q/2 + q/2) = \varphi(q/2)\varphi(q/2) = \varphi(q/2)^2,$$

که با گویا بودن $\varphi(q/2)$ در تناقض است. بنابراین هیچ یکریختی از $\mathbb{Q}$ به $\mathbb{Q}^*$ وجود ندارد.

■

قضیه زیر نشان می‌دهد که یک یکریختی علاوه بر حفظ عمل دوتایی، عنصر همانی، معکوس، توان و بالاخره مرتبه هر عنصر را نیز حفظ می‌کند.

قضیه ۵-۱

فرض کنید $\varphi : G \to H$ یک یکریختی باشد.
(۱) اگر e عنصر همانی G باشد، آنگاه $\varphi(e)$ عنصر همانی H است،
(۲) برای هر $g \in G$، $\varphi(g^{-1}) = \varphi(g)^{-1}$،
(۳) برای هر $g \in G$ و هر $n \in \mathbb{Z}$، $\varphi(g^n) = \varphi(g)^n$،
(۴) برای هر $g \in G$، $\circ(g) = \circ(\varphi(g))$.

اثبات (۱): داریم $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$، لذا طبق قانون حذف در H، $\varphi(e)$ عنصر همانی H می‌باشد.
(۲): این گزاره با توجه به مطلب زیر به دست می‌آید.

$$\varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

(۳): این گزاره به آسانی با استقرای ریاضی به دست می‌آید.

www.mathematic87.blogfa.com

(۴): فرض کنید $o(g)=\infty$. نشان می‌دهیم $o(\varphi(g))=\infty$. اگر $o(\varphi(g))=n$ متناهی باشد، آنگاه $\varphi(g^n)=\varphi(g)^n=e_H=\varphi(e)$ و در نتیجه با توجه به یک به یک بودن φ خواهیم داشت $g^n=e$، که تناقض است. حال فرض کنید $o(g)=n$. در این‌صورت $\varphi(g)^n=\varphi(g^n)=\varphi(e)=e_H$ و لذا $m=o(\varphi(g))\mid n$. از طرف دیگر چون $\varphi(g^m)=\varphi(g)^m=e_H=\varphi(e)$ و با توجه به یک به یک بودن φ خواهیم داشت $g^m=e$ پس $n\mid m$. بنابراین $n=m$ و قضیه ثابت است.

■■■

- **تذکر:** دیده می‌شود که در اثبات قسمت‌های (۱)، (۲) و (۳) از قضیه فوق تنها از خاصیت $\varphi(ab)=\varphi(a)\varphi(b)$ استفاده شده است، یعنی تنها خاصیتی که مورد استفاده قرار گرفته، حفظ عمل دوتایی است. هر تابعی که فقط دارای این خاصیت باشد یک همریختی نامیده می‌شود. همریختی‌ها نقش مهمی در نظریه گروه‌ها ایفا می‌کنند که به طور مفصل در فصل بعدی مورد بررسی قرار می‌گیرند.

قضیه ۵-۲

فرض کنید $\varphi: G\to H$ یک یکریختی باشد. در این صورت:

(۱) $|G|=|H|$،

(۲) $\varphi^{-1}: H\to G$ یک یکریختی است،

(۳) اگر G یک گروه آبلی باشد، آنگاه H نیز آبلی است،

(۴) اگر G یک گروه دوری باشد، آنگاه H نیز دوری است،

(۵) اگر G دارای عنصری از مرتبه n باشد، آنگاه H نیز دارای عنصری از مرتبه n است،

(۶) اگر G دارای زیرگروهی از مرتبه n باشد، آنگاه H نیز دارای زیرگروهی از مرتبه n است.

اثبات (۱): از یک به یک و پوشا بودن φ به دست می‌آید.

www.mathematic87.blogfa.com

(۲): به وضوح $\varphi^{-1}: H \to G$ تابعی یک به یک و پوشا است. فرض کنید $h,k \in H$. چون φ پوشاست عناصری چون $a,b \in G$ موجودند بطوریکه $\varphi(a)=h$ و $\varphi(b)=k$. بنابراین

$$\varphi^{-1}(hk)=\varphi^{-1}(\varphi(a)\varphi(b))=\varphi^{-1}(\varphi(ab))=ab=\varphi^{-1}(h)\varphi^{-1}(k),$$

یعنی $\varphi^{-1}: H \to G$ یک یکریختی است.

(۳): فرض کنید $h,k \in H$. چون φ پوشاست، عناصری چون $a,b \in G$ موجودندکه $\varphi(a)=h$ و $\varphi(b)=k$. بنابراین

$$hk=\varphi(a)\varphi(b)=\varphi(ab)=\varphi(ba)=\varphi(b)\varphi(a)=kh,$$

یعنی H آبلی است.

(۴): فرض کنید $G=<a>$ در این صورت واضح است که $H=\varphi(G)=<\varphi(a)>$.

(۵): از قسمت(۴) قضیهٔ ۱ بدست می‌آید.

(۶): افرض کنید $G_1 \le G$. در این‌صورت $H_1=\varphi(G_1) \le H$ و به‌وضوح $\varphi|_{G_1}: G_1 \to H_1$ یک یکریختی است. در نتیجه $|G_1|=|H_1|$.

■■■

تعریف ۵-۲

خواص ساختاری گروه، خواصی است که تحت یکریختی حفظ شود.

خواص زیر مثال‌هایی از خواص ساختاری گروه اند.

(۱) مرتبهٔ عناصر گروه،

(۲) آبلی بودن گروه،

(۳) دوری بودن گروه،

(۴) گروه دقیقاً m عنصر از مرتبه n دارد،

(۵) معادله $x^n=a$ برای هر a در گروه جواب دارد.

www.mathematic87.blogfa.com

اینک چند مثال غیر ساختاری ارائه می‌دهیم.

(۱) تمام عناصر گروه ماتریس هستند،

(۲) تمام عناصر گروه جایگشت هستند،

(۳) عمل گروه ترکیب است،

(۴) گروه حاوی عدد مختلط است،

(۵) تمام عناصر گروه عدد هستند.

اینک در موقعیتی هستیم که بتوانیم گروه‌های دوری را طبقه بندی کنیم.

قضیه ۵-۳

فرض کنید $G =< g >$ یک گروه دوری باشد. در این صورت:

(۱) اگر $|G| = n$ آنگاه $G \cong \mathbb{Z}_n$،

(۲) اگر $|G| = \infty$ آنگاه $G \cong \mathbb{Z}$.

اثبات (۱): تعریف می‌کنیم:

$$\varphi : \mathbb{Z}_n \to G$$
$$\overline{m} \mapsto g^m$$

با توجه به این که

$$\overline{m}_1 = \overline{m}_2 \Leftrightarrow n \mid m_1 - m_2 \Leftrightarrow g^{m_1} = g^{m_2}$$

φ یک به یک و خوش تعریف است. همچنین

$$\varphi(\overline{m}_1 + \overline{m}_2) = \varphi\left(\overline{m_1 + m_2}\right) = g^{m_1+m_2} = g^{m_1} g^{m_2} = \varphi(\overline{m}_1)\varphi(\overline{m}_2).$$

به‌وضوح φ پوشا ست و درنتیجه φ یک یکریختی است.

(۲): تابع $\varphi : \mathbb{Z} \to G$ با ضابطه $\varphi(m) = g^m$ به وضوح پوشا است و

$$\varphi(m_1 + m_2) = g^{m_1+m_2} = g^{m_1} g^{m_2} = \varphi(m_1)\varphi(m_2).$$

www.mathematic87.blogfa.com

بنابراین کافی است نشان دهیم φ یک به یک است. فرض کنید $\varphi(m_1)=\varphi(m_2)$. بدون این که از کلیت کاسته شود می‌توان فرض کرد $m_1 \geq m_2$. از این‌رو $g^{m_1-m_2}=e$ و در نتیجه $m_1=m_2$.

■■■

۵- ۲ قضیه کیلی

قضیه کیلی نشان می‌دهد که هر گروه با گروهی از جایگشت‌ها یکریخت است. در مورد گروه‌های متناهی قضیه کیلی نشان می‌دهد که هر گروه n عنصری با زیر گروهی از S_n یکریخت است. این قضیه بسیار مفید است، چرا که در S_n، با جایگشت‌ها، دورها و تجزیهٔ جایگشت‌ها به حاصل ضرب دورها آشنا هستیم در صورتی که در مورد گروه‌های مجرد هیچ گونه شناختی نداریم.

قضیه ۵-۴ (قضیه کیلی)

هر گروه با گروهی از جایگشت‌ها یکریخت است. بعبارت دیگر، هر گروه G با زیرگروهی از S_G یکریخت است.

اثبات: فرض کنید G گروه مفروضی باشد. کافی است یک زیر گروه G_1 از S_G ویک یکریختی $\theta : G \to G_1$ را مشخص کنیم. برای هر $g \in G$ تعریف می‌کنیم:

$$\tau_g : G \to G$$
$$x \mapsto gx$$

چون τ_g هم یک به یک و هم پوشا است. پس τ_g جایگشتی از G است $(\tau_g \in S_G)$. اکنون فرض می‌کنیم:

$$G_1 = \{\tau_g \,|\, g \in G\}.$$

www.mathematic87.blogfa.com

برای هر $g,h \in G$ داریم $\tau_g\tau_h = \tau_{gh}$، $(\tau_g)^{-1} = \tau_{g^{-1}}$ و به علاوه اگر e عنصر همانی G باشد آنگاه τ_e همان جایگشت همانی id از S_G است (یعنی G_1 زیرگروهی از S_Gاست).

تعریف می‌کنیم:

$$\theta : G \to G_1$$
$$g \mapsto \tau_g$$

اگر $\tau_g = \tau_h$ آنگاه $g = h$، یعنی θ یک به یک است. پوشا بودن θ بدیهی است و سرانجام $\tau_{gh} = \tau_g\tau_h$، یکریختی بودن θ را نتیجه می‌دهد.

■■■

قضیه ۵-۵

فرض کنید X,Y دو مجموعه غیر تهی باشند. در این‌صورت:

(۱) اگر $|X| = |Y|$، آنگاه $S_X \cong S_Y$،

(۲) اگر $|X| = n$، آنگاه $S_X \cong S_n$.

اثبات (۱): فرض کنید $f : X \to Y$ یک دوسویی باشد و $\delta \in S_X$. همان طوری که در نمودار زیر دیده می‌شود:

$$Y \xrightarrow{f^{-1}} X \xrightarrow{\delta} X \xrightarrow{f} Y$$

$f\delta f^{-1} \in S_Y$. به سادگی مشاهده می‌شود که تابع $\varphi : S_X \to S_Y$ با ضابطه $\varphi(\delta) = f\delta f^{-1}$ یک یکریختی است.

(۲): قرار می‌دهیم $Y = \{1,2,...,n\}$. در این صورت با توجه به قسمت (۱) داریم $S_X \cong S_Y = S_n$.

■■■

از ترکیب قضیه کیلی و قضیه فوق به آسانی نتیجه زیر به دست می‌آید.

نتیجه ۵-۱

هر گروه n عنصری با زیر گروهی از S_n یکریخت است.

www.mathematic87.blogfa.com

۵-۳ خودریختی‌ها

تعریف ۵-۳

فرض کنید G یک گروه باشد. هر یکریختی $\varphi : G \to G$ یک **خودریختی (اتومورفیسم)** از G نامیده می‌شود. مجموعهٔ همهٔ خودریختی‌های G را با $\mathrm{Aut}(G)$ نمایش می‌دهیم.

مثال۶: فرض کنید G یک گروه باشد. تابع همانی $\mathrm{id} : G \to G$، که $\mathrm{id}(x) = x$ یک خودریختی از Gاست.

■

مثال۷: تابع $\varphi : \mathbb{Z} \to \mathbb{Z}$ با ضابطهٔ $\varphi(x) = -x$ یک خودریختی از $\mathbb{Z}$است.

■

◆ **تذکر:** در حالت کلی $\varphi : G \to G$ با ضابطهٔ $\varphi(x) = x^{-1}$ یک خودریختی از Gاست اگر و فقط اگر G آبلی باشد.

قضیه ۵-۶

اگر G یک گروه باشد، آنگاه $\mathrm{Aut}(G)$ نسبت به عمل ترکیب توابع یک گروه است. در واقع

$$\mathrm{Aut}(G) \leq S_G.$$

اثبات: چون $\mathrm{id} \in \mathrm{Aut}(G)$ پس $\mathrm{Aut}(G) \neq \varnothing$. حال فرض کنید $f, g \in \mathrm{Aut}(G)$ با توجه به اینکه $f, g \in S_G$ و S_G یک گروه است، پس $fg^{-1} \in S_G$ و لذا fg^{-1} یک به یک و پوشاست. از طرف دیگر با توجه به قسمت (۲) قضیه ۵-۲ خواهیم داشت:

$$fg^{-1}(ab) = f(g^{-1}(a)g^{-1}(b)) = fg^{-1}(a)fg^{-1}(b).$$

بنابراین $fg^{-1} \in \mathrm{Aut}(G)$. یعنی $\mathrm{Aut}(G)$ یک زیر گروه S_G است.

■■■

تعریف ۵-۴

$\mathrm{Aut}(G)$ را **گروه خودریختی‌های** G می‌نامیم.

قضیه ۵-۷

فرض کنید G یک گروه و $g \in G$. در این‌صورت تابع

$$\tau_g : G \to G$$
$$x \mapsto gxg^{-1}$$

یک خودریختی G است.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۵-۵

فرض کنید G یک گروه باشد. هر خودریختی $\tau_g : G \to G$ یک **خودریختی داخلی** از G نامیده می‌شود. مجموعهٔ همهٔ خودریختی‌های داخلی G، یعنی $\{\tau_g \mid g \in G\}$، را با $\mathrm{Inn}(G)$ نمایش می‌دهیم.

قضیه ۵-۸

فرض کنید G یک گروه باشد. در این‌صورت:

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq S_G.$$

اثبات: چون $\tau_e = \mathrm{id} \in \mathrm{Inn}(G)$ پس $\mathrm{Inn}(G) \neq \varnothing$. حال فرض کنید $g,h \in G$. برای هر $x \in G$ داریم:

$$\tau_g\tau_h(x) = \tau_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \tau_{gh}(x).$$

www.mathematic87.blogfa.com

بنابراین $\tau_g\tau_h = \tau_{gh}$ و با قرار دادن $h = g^{-1}$ خواهیم داشت

$$(\tau_g)^{-1} = \tau_{g^{-1}},$$

یعنی $\mathrm{Inn}(G)$ یک گروه است.

■■■

تعریف ۵-۶

$\mathrm{Inn}(G)$ را **گروه خودریختی‌های داخلی** G می‌نامیم. هر عنصر $\varphi \in \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$ را **خودریختی‌های خارجی** G نامیده ومجموعهٔ همهٔ خودریختی‌های خارجی G را با $\mathrm{Out}(G)$ نمایش می‌دهیم.

۵- ۴ حاصل ضرب‌های مستقیم

فرض کنید دو گروه G, H داده شده باشند. می‌خواهیم گروه جدید بزرگتری با استفاده از حاصل ضرب دکارتی $G \times H$ بسازیم. بر عکس اگر گروه بزرگ G داده شده باشد. می‌خواهیم ببینیم که آیا می‌توان G رابا حاصل ضرب مستقیم گروه‌های کوچکتری یکریخت ساخت. در صورت اخیر مطالعه گروه G منجر به مطالعهٔ گروه‌های کوچکتر می‌شود که کار را نسبتاً آسان می‌کند.

فرض کنید $G_1, G_2, \ldots, G_n$ گروه باشند. حاصل ضرب دکارتی $\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$ با عمل دوتایی ضرب مولفه ای ساختار گروهی دارد. عمل ضرب مولفه ای چنین است که اگر $(g_1, g_2, \ldots, g_n)$ و $(h_1, h_2, \ldots, h_n)$ دو عنصر $\prod_{i=1}^{n} G_i$ باشند، آنگاه

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n).$$

www.mathematic87.blogfa.com

قضیه۵-۹

فرض کنید $G_1, G_2, \ldots, G_n$ گروه باشند. حاصل ضرب دکارتی $\prod_{i=1}^{n} G_i$ با عمل دوتایی ضرب مولفه ای یک گروه است و **حاصل ضرب مستقیم خارجی** گروه‌های G_i نامیده می‌شود.

اثبات: به وضوح $\prod_{i=1}^{n} G_i$ نسبت به عمل دوتایی ضرب مولفه ای بسته است. اگر e_i عنصر همانی G_i باشد، آنگاه $(e_1, e_2, \ldots, e_n)$ عنصر همانی $\prod_{i=1}^{n} G_i$ خواهد بود. معکوس $(g_1, g_2, \ldots, g_n)$ عنصر $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$ است. بالاخره شرکت پذیر بودن این عمل دوتایی به راحتی از شرکت پذیر بودن اعمال دوتایی G_iها نتیجه می‌شود.

■■■

قضیه۵-۱۰

فرض کنید $x = (g_1, g_2, \ldots, g_n) \in \prod_{i=1}^{n} G_i$. دراین‌صورت مرتبه x در $\prod_{i=1}^{n} G_i$ برابر است با کوچکترین مضرب مشترک $\circ(g_i)$ها. بعبارت دیگر

$$\circ(x) = [\circ(g_1), \circ(g_2), \ldots, \circ(g_n)].$$

اثبات: فرض کنید $M = [\circ(g_1), \circ(g_2), \ldots, \circ(g_n)]$ و $m = \circ(x)$. در این صورت:

$$(g_1, g_2, \ldots, g_n)^M = (g_1{}^M, g_2{}^M, \ldots, g_n{}^M) = (e_1, e_2, \ldots, e_n)$$

$$(g_1{}^m, g_2{}^m, \ldots, g_n{}^m) = (g_1, g_2, \ldots, g_n)^m = (e_1, e_2, \ldots, e_n)$$

که در این جا e_i عنصر همانی G_i است. از رابطه اول خواهیم داشت که $m \mid M$. از رابطه دوم داریم $\circ(g_i) \mid m$ و بنابراین طبق تعریف $M \mid m$ ودر نتیجه $M = m$.

■■■

www.mathematic87.blogfa.com

مثال۸: مرتبه $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ برابر 6 است. پس $(1,1)$ مولدی برای $\mathbb{Z}_2 \times \mathbb{Z}_3$ است. چون در حد یکریختی دقیقاً یک گروه دوری وجود دارد. بنابراین $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. در حالت کلی قضیه زیر را داریم.

■

قضیه۵-۱۱

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ اگر و فقط اگر $(m,n)=1$.

اثبات ($\Leftarrow$): فرض کنید $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. اگر $(m,n)=d>1$ در این صورت برای هر $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ داریم :

$$\underbrace{(a,b)+(a,b)+\cdots+(a,b)}_{\text{مرتبه } [m,n]} = (0,0),$$

که در اینجا $[m,n] = (mn)/d < mn$ بنابراین هیچ عنصری چون (a,b) نمی‌تواند $\mathbb{Z}_m \times \mathbb{Z}_n$ را تولید کند که این تناقض است پس $(m,n)=1$.

($\Rightarrow$): فرض کنید $x=(1,1)$. از قضیه قبل داریم ، $o(x)=[m,n]=mn$. بنابراین $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

■■■

با استدلال استقرایی، دو نتیجه زیر را خواهیم داشت.

نتیجه۵-۲

اگر $n_1, n_2, \ldots, n_k$ اعداد صحیح مثبتی باشند آنگاه

$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 \ldots n_k} \Leftrightarrow n_i$ ها دو به دو نسبت به هم اول باشند.

نتیجه۵-۳

فرض کنید n را به صورت حاصل ضربی از توان‌های اعداد اول متمایز، به صورت $n = p_1^{n_1}...p_k^{n_k}$ بنویسیم. در این صورت:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

تذکر: در فصل۷ نشان می‌دهیم که هر گروه آبلی متناهی با حاصل ضرب مستقیمی به شکل زیر یکریخت است:

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}},$$

که در آن p_i ها اعدادی اول (نه لزوماً متمایز) هستند.

فرض کنید گروه مفروض G داده شده باشد. در این بخش نشان می‌دهیم که چه وقت G با حاصل ضرب مستقیم خارجی زیر گروه‌هایش یکریخت است.

تعریف ۵-۷

فرض کنید G یک گروه و $\{H_i\}_{i=1}^{n}$ خانواده ای از زیر گروه‌های G باشد. Gرا **حاصل ضرب مستقیم داخلی** H_i ها می‌نامیم هر گاه:

(۱) $gH_i = H_ig$ برای هر $1 \le i \le n$ و هر $g \in G$،

(۲) هر عنصر $g \in G$ را بتوان به طور منحصر به فردی به شکل $g = h_1h_2...h_n$ نوشت، که $h_i \in H_i$.

تذکر: شرط (۱) در تعریف فوق شرط نرمال بودن H_iاست، یعنی $H_i \trianglelefteq G$، که در فصل بعدی مورد بررسی قرار می‌گیرد.

لم ۵-۱

فرض کنید H و K زیر گروه‌های از گروه G باشند به قسمی که

(۱) $gH = Hg$ و $gK = Kg$ برای هر $g \in G$،

(۲) $H \cap K = \{e\}$.

دراین صورت به ازای هر $h \in H$ و $k \in K$ داریم $hk = kh$.

اثبات: عنصر $h^{-1}k^{-1}hk$ را در نظر بگیرید. با توجه به فرض (۱)، $h^{-1}k^{-1}hk \in H \cap K$. بنابراین $h^{-1}k^{-1}hk = e$ و در نتیجه $hk = kh$.

■■■

قضیه۵-۱۲

فرض کنید G حاصل ضرب مستقیم داخلی خانواده $\{H_i\}_{i=1}^{n}$ از زیر گروه‌هایش باشد. دراین صورت G حاصل ضرب مستقیم خارجی H_i ها است. یعنی

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

اثبات: تعریف می‌کنیم:

$$\varphi : \prod_{i=1}^{n} H_i \to G$$
$$\varphi\left(h_1, h_2, \ldots, h_n\right) = h_1 h_2 \ldots h_n$$

تعریف می‌کنیم. به‌وضوح φ خوش تعریف و یک به یک است. چون هرعنصر $g \in G$ به طور منحصر به فرد به شکل $g = h_1 h_2 \ldots h_n$ نوشته می‌شود، پس φ دوسویی است. حال فرض کنید $i \neq j$ و $x \in H_i \cap H_j$. در این صورت

$$x = e \ldots \overset{\text{مکان } i}{\overset{\uparrow}{x}} \ldots e = e \ldots \overset{\text{مکان } j}{\overset{\uparrow}{x}} \ldots e.$$

www.mathematic87.blogfa.com

با توجه به این که $i \neq j$، داریم $x = e$. نشان داده ایم که برای هر $i \neq j$ داریم $H_i \cap H_j =< e >$.

بنابراین طبق لم قبل برای هر $i \neq j$ عناصر H_i و H_j با هم جابجا می‌شوند. ازاین‌رو

$$\varphi\Big(\big(h_1,...,h_n\big)\big(h_1',...,h_n'\big)\Big) = \varphi\big(h_1h_1',...,h_nh_n'\big) = h_1h_1'...h_nh_n'$$
$$= (h_1...h_n)(h_1'...h_n') = \varphi\big(h_1,...,h_n\big)\varphi\big(h_1',...,h_n'\big),$$

لذا $G \cong H_1 \times H_2 \times \cdots \times H_n$.

■■■

قضیه۵-۱۳

فرض کنید $\{H_i\}_{i=1}^{n}$ خانواده ای از زیر گروه‌های G باشد. اگر داشته باشیم:

(۱) $gH_i = H_ig$ برای هر $1 \leq i \leq n$ و هر $g \in G$،

(۲) $H_i \cap H_1...H_{i-1} = \{e\}$، برای هر $2 \leq i \leq n$،

(۳) $G = H_1...H_n$،

آنگاه G حاصل ضرب مستقیم داخلی H_i ها است.

اثبات: ابتدا نشان می‌دهیم که اگر $i \neq j$، آنگاه عناصر H_i و H_j با هم جابجا می‌شوند. طبق لم قبل کافی است نشان دهیم $H_i \cap H_j = \{e\}$. فرض کنید $i > j$، یعنی $i - 1 \geq j$. در این صورت

$$H_i \cap H_j \subseteq H_i \cap H_1H_2...H_{i-1} = \{e\}.$$

در نتیجه $H_i \cap H_j = \{e\}$. حال فرض کنید

$$g = h_1h_2...h_n = h_1'h_2'...h_n'$$

که $h_i, h_i' \in H_i$. با توجه به این که برای $i \neq j$، عناصر H_i و H_j با هم جابجا می‌شوند، خواهیم داشت:

$$h_nh_n'^{-1} = h_1^{-1}h_1'...h_{n-1}^{-1}h_{n-1}' \in H_n \cap H_1H_2...H_{n-1} = \{e\}.$$

www.mathematic87.blogfa.com

ازاین‌رو $h_n' = h_n$ و در نتیجه

$$h_1h_2...h_{n-1} = h_1'h_2'...h_{n-1}'.$$

با ادامهٔ این روند خواهیم داشت، $h_i = h_i'$، $1 \le i \le n$.

بنابراین هر $g \in G$ به طور منحصر به فردی به صورت $g = h_1h_2...h_n$، $h_i \in H_i$، نوشته می‌شود.

■■■

با توجه به قضیهٔ فوق به آسانی نتیجهٔ مهم زیر حاصل می‌شود.

نتیجه۵-۴

فرض کنید $\{H_i\}_{i=1}^{n}$ خانواده ای از زیر گروه‌های G باشد. اگر داشته باشیم:

(۱) $gH_i = H_ig$ برای هر $1 \le i \le n$ و هر $g \in G$،

(۲) $H_i \cap H_1...H_{i-1}H_{i+1}...H_n =< e >$، برای هر $2 \le i \le n$،

(۳) $G = H_1...H_n$،

آنگاه G حاصل ضرب مستقیم داخلی H_i ها است.

توضیح تاریخی

آرتور کیلی در سال 1821در انگلستان متولد شد. در سن 17 سالگی پدر تاجر او علی رغم میل باطنی اش وی را به دانشگاه کمبریج فرستاد. کیلی اولین جایزهٔ اسمیت در ریاضیات را به خود اختصاص داد. در سن۲۵ سالگی به مطالعه حقوق پرداخت و بعد از سه سال کرسی وکالت در دادگاه را به دست آورد اما بیشتر وقت آزاد خود را به مطالعه و تحقیق در ریاضیات اختصاص می‌داد. درسال 1863 با کناره گیری از وکالت، سمت استادی در دانشگاه کمبریج را در بدست آورد. کیلی بیش از ۹۰۰ مقاله در زمینه‌های نظریه میدان، نظریه گروه‌ها،

هندسه و جبر خطی به چاپ رسانده است. در ضمن از کیلی می‌توان به عنوان اولین کسی که مفهوم گروه‌های مجرد را معرفی کرد یاد برد.

تمرینها

۱. ثابت کنید $\mathbb{Z} \cong n\mathbb{Z}$، برای هر $n \neq 0$.

۲. نشان دهید رابطه یکریخت بودن بین گروه‌ها یک رابطه هم ارزی است.

۳. نشان دهید $\mathbb{C}^*$ یکریخت است با زیر گروهی از $\mathrm{GL}_2(\mathbb{R})$ متشکل از ماتریس‌های به شکل:

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

۴. ثابت کنید یا رد کنید:

(a) $\mathrm{K}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$،

(b) $D_3 \cong S_3$،

(c) $U(8) \cong \mathbb{Z}_4$،

(d) $\mathbb{Q} \cong \mathbb{Z}$،

(e) $\mathbb{Q} \cong \mathbb{R}$،

(f) $(\mathbb{Q}^+,.) \cong (\mathbb{Z}[x],+)$.

(توجه داشته باشید که $(\mathbb{Z}[x],+)$ گروه جمعی تمام چندجمله‌ها با مجهول x و ضرایب صحیح می‌باشد و $(\mathbb{Q}^+,.)$ گروه اعداد گویای مثبت نسبت به ضرب است) .

۵. ثابت کنید $U(8)$ یکریخت است با گروه ماتریس‌های زیر

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

www.mathematic87.blogfa.com

۶. نشان دهید:

(a) $U(5)$با $U(10)$ یکریخت است ولی با $U(12)$ یکریخت نیست ،

(b) گروه ریشه‌های n ام واحد با $\mathbb{Z}_n$ یکریخت است،

(c) S_4 با D_{12} یکریخت نیست.

۷. فرض کنید $w = e^{2\pi i/n}$ یک ریشه nام اولیه واحد باشد و

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ و } B = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}$$

نشان دهید گروه ضربی تولید شده توسط ماتریس‌های A, B با D_n یکریخت است.

۸. نشان دهید که مجموعه همه ماتریس‌های به شکل $\begin{pmatrix} \pm 1 & m \\ 0 & 1 \end{pmatrix}$ که $m \in \mathbb{Z}_n$ با گروه D_n یکریخت است.

۹. (a) اگر G یک گروه از مرتبهٔ 4 باشد، ثابت کنید $G \cong \mathbb{Z}_4$ یا $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$،

(b) اگر G یک گروه از مرتبهٔ 6 باشد، ثابت کنید $G \cong \mathbb{Z}_6$ یا $G \cong S_3$.

۱۰. (a) ثابت کنید $U(5) \cong \mathbb{Z}_4$. آیا در حالت کلی می‌توان گفت $U(p) \cong \mathbb{Z}_{p-1}$؟

(b) نشان دهید $S_3 \times \mathbb{Z}_2 \cong D_6$. در حالت کلی چه می‌توان گفت؟

۱۱. گزاره‌های زیر را ثابت کنید:

(a) اگر $H \cong H_1$ و $K \cong K_1$ آنگاه $H \times K \cong H_1 \times K_1$،

(b) $H \times K \cong K \times H$،

(c) $C(H \times K) = C(H) \times C(K)$،

(d) $H \times K$ آبلی است اگر وفقط اگر K, H آبلی باشند.

۱۲. نشان دهید:

(a) هریک از گروه‌های D_4, S_3 و $\mathbb{Z}_{p^n}$ (p اول) را نمی‌توان به صورت حاصل ضرب مستقیم داخلی دو زیر گروه سره نوشت.

www.mathematic87.blogfa.com

(b) هریک از گروه‌های $\mathbb{Q},\mathbb{Z}$ را نمی‌توان به صورت حاصل ضرب مستقیم داخلی دو زیر گروه غیر بدیهی نوشت.

۱۳. فرض کنید $H_1 \le G_1$ و $H_2 \le G_2$ نشان دهید $H_1 \times H_2 \le G_1 \times G_2$. آیا عکس این مطلب درست است، یعنی آیا هر زیر گروه $G_1 \times G_2$ به شکل $H_1 \times H_2$ است ، که $H_1 \le G_1$ و $H_2 \le G_2$.

۱۴. فرض کنید G یک گروه آبلی و متناهی و $3 \| |G|$. نشان دهید G باید زیرگروهی از مرتبه 3 داشته باشد.

۱۵. فرض کنید G,H گروه‌های دوری متناهی باشند. نشان دهید $G \times H$ دوری است اگر و فقط اگر $(|G|,|H|)=1$.

۱۶. گزاره‌های زیر را ثابت یا رد کنید:

(a) فرض کنید K,H,G گروه باشند. اگر $G \times K \cong H \times K$، آنگاه $G \cong H$،

(b) گروهی آبلی و غیر دوری از مرتبه 52 موجود است.

۱۷. نشان دهید S_n با زیر گروهی از A_{n+2} یکریخت است.

۱۸. (a) تابع $a+bi \to a-bi$ یک خودریختی از $\mathbb{C}^*$ است،

(b) تابع $A \to BAB^{-1}$ برای هر $B \in \mathrm{GL}_2(\mathbb{R})$ یک خودریختی از $\mathrm{SL}_2(\mathbb{R})$ است،

(c) مطلوب است $\mathrm{Aut}(\mathbb{Z}_6)$ و $\mathrm{Aut}(\mathbb{Z})$،

(d) دو گروه غیر یکریخت H,G پیدا کنید که $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$،

(e) مطلوب است $\mathrm{Inn}(Q)$.

۱۹. ثابت کنید:

(a) $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$،

(b) $\mathrm{Aut}(\mathbb{Z}_n \times \mathbb{Z}_n) \cong \mathrm{GL}_2(\mathbb{Z}_n)$،

(c) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

۲۰. فرض کنید K,H دو زیرگروه نرمال G و $G \cong H \times K$. در این‌صورت:

(a) $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ با زیرگروهی از $\mathrm{Aut}(G)$ یکریخت است،

www.mathematic87.blogfa.com

(b) اگر G گروهی متناهی و $(|H|,|K|)=1$، آنگاه $\mathrm{Aut}(H)\times\mathrm{Aut}(K)\cong\mathrm{Aut}(G)$،

(c) فرض کنید $n=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ که p_i اعداد اول دو به دو متمایز و k_i اعداد طبیعی‌اند. نشان دهید:

$$\mathrm{Aut}(\mathbb{Z}_n)\cong\mathrm{Aut}(\mathbb{Z}_{p_1^{k_1}})\times\cdots\times\mathrm{Aut}(\mathbb{Z}_{p_t^{k_t}}).$$

مسائل مبارزه طلب

۱. (a) اگر $p>2$ یک عدد اول باشد، آنگاه به ازای هر عدد طبیعی m،

$$U(p^m)\cong\mathbb{Z}_{(p-1)p^{m-1}},$$

(b) برای هر عدد طبیعی $m>2$،

$$U(2^m)\cong\mathbb{Z}_2\times\mathbb{Z}_{2^{m-2}},$$

(c) $|U(2)|=1$ و $|U(4)|=2$.

۲. ثابت کنید که $\mathrm{Aut}(D_4)\cong D_4$ و $\mathrm{Aut}(S_4)\cong S_4$.

۳. فرض کنید G یک گروه متناهی باشد بطوریکه $|G|>2$. ثابت کنید $|\mathrm{Aut}(G)|>1$. (در واقع $|\mathrm{Aut}(G)|$ عددی زوج است).

۴. نشان دهید که:

(a) $\mathrm{Aut}(\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n\text{ بار}})\cong\mathrm{GL}_n(\mathbb{Z})$،

(b) $\mathrm{Aut}(\underbrace{\mathbb{Z}_{p^m}\times\cdots\times\mathbb{Z}_{p^m}}_{n\text{ بار}})\cong\mathrm{GL}_n(\mathbb{Z}_{p^m})$.

۵. فرض کنید n یک عدد طبیعی و $m=\mathrm{Log}_2 n$. نشان دهید تعداد گروه‌های غیر یکریخت از مرتبهٔ n از عدد n^m کمتر است.

www.mathematic87.blogfa.com

منابعی برای مطالعهٔ بیشتر

1. Cameron, P. J. *Introduction to Algebra*. Cambridge University Press, 1998.
2. Lang, S. *Algebra*. Addison-Wesley, 1993.
3. Macdonald. I. D. *The Thoery of Groups*. Oxford University Press, 1968.
4. Rose. J. S. *A Course on Group Theory*. Cambridge University Press, 1978.

www.mathematic87.blogfa.com

فصل ۶

زیر گروه‌های نرمال و همریختی‌ها

در این فصل می‌خوانید:

۶-۱ زیرگروه‌های نرمال
۶-۲ همریختی‌ها
۶-۳ قضایای یکریختی
۶-۴ ساده بودن $A_n (n \geq 5)$

مقدمه

فرض کنید H زیرگروهی از گروه دلخواه G باشد. می‌دانیم که به ازای هر $g \in G$ لزوماً تساوی $gH = Hg$ برقرار نیست. زیر گروه‌هایی که به ازای هر $g \in G$ هم‌دسته‌های چپ وراست آنها یکسان هستند، نقشی اساسی در نظریه گروه‌ها دارند (یادآوری: بخش ۳ از فصل ۵ ملاحظه شود). چنین زیرگروه‌هایی این اجازه را به ما می‌دهند که رده جدیدی از گروه‌های خارج قسمتی بسازیم. گروه‌های خارج‌قسمتی را همچنین می‌توان از طریق همریختی‌ها که تعمیم یکریختی‌ها هستند نیز مورد مطالعه قرار داد.

www.mathematic87.blogfa.com

۶-۱زیرگروه‌های نرمال

تعریف ۶-۱

زیر گروه H از گروه G را یک **زیر گروه نرمال** نامیده و با نماد $H \trianglelefteq G$ نمایش می‌دهیم، هرگاه برای هر $g \in G$، تساوی $gH = Hg$ برقرار باشد.

مثال۱: هر زیرگروه از یک گروه آبلی، یک زیر گروه نرمال است.

■

مثال۲: اگر G یک گروه باشد، زیر گروه‌های بدیهی $G, \{e\}$ زیر گروه‌های نرمال در G می‌باشند.

■

مثال۳: گروه $N = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ یک زیر گروه نرمال از S_3 است. چرا که هم دسته‌های N عبارتند از:

$$(1\ 2)N = N(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\},$$
$$(1\ 3)N = N(1\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\},$$
$$(2\ 3)N = N(2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\},$$
$$(1)N = N(1) = (1\ 2\ 3)N = N(1\ 2\ 3) = (1\ 3\ 2)N = N(1\ 3\ 2) = N.$$

■

مثال۴: اگر G یک گروه و N زیر گروهی از $C(G)$ باشد آنگاه N زیر گروه نرمالی از G است.

■

www.mathematic87.blogfa.com

قضیه۶-۱ (آزمون نرمال بودن)

گزاره‌های زیر در مورد زیر گروه H از گروه G معادلند:

(۱) H در G نرمال است،

(۲) به ازای هر $g \in G$، $gHg^{-1} = H$،

(۳) به ازای هر $g \in G$، $gHg^{-1} \subseteq H$.

اثبات: **(۱)** $\Leftrightarrow$ **(۲)** و **(۲)** $\Leftarrow$ **(۳)** واضح می‌باشند.

(۲) $\Rightarrow$ **(۳)**: اگر در رابطه (۳) به جای عنصر g قرار دهیم، داریم $g^{-1}Hg \subseteq H$ و لذا

$$H = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1},$$

یعنی رابطه (۲) برقرار است.

■■■

نتیجه ۶-۱

فرض کنید G یک گروه باشد. در این‌صورت $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

اثبات: اگر $f \in \mathrm{Aut}(G)$ و $g \in G$، به‌وضوح $f\tau_g f^{-1} = \tau_{f(g)} \in \mathrm{Inn}(G)$ ولذا طبق آزمون فوق $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

■■■

بار دیگر ساختار $\mathbb{Z}_n$ را مورد مطالعه قرار می‌دهیم. همان طوری که می دانید $\mathbb{Z}_n$ متشکل از همه هم‌دسته‌های $a + n\mathbb{Z}$ است، که در آن $a \in \mathbb{Z}$. جمع دو هم دسته به صورت زیر تعریف می‌شود:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

از این رو ایده‌ای برای تعریف حالت کلی به دست می‌آوریم، اگر H زیر گروهی از گروه G باشد، می‌توان ضرب زیر را روی هم دسته‌های چپ آن تعریف کرد:

برای هر $a,b \in G$ ، $aHbH = abH$

البته ممکن است این ضرب خوش تعریف نباشد، زیرا هم دسته‌ها را می‌توان به صورت‌های گوناگونی نمایش داد. به مثال زیر توجه کنید.

■

مثال۵: زیر گروه $H = \{(1),(1\ 2)\}$ در S_3 و هم‌دسته‌های زیر را در نظر بگیرید.

$$(2\ 3)H = (1\ 3\ 2)H \quad \text{و} \quad (1\ 3)H = (1\ 2\ 3)H$$

اگر قرار دهیم $X = (1\ 3)H$ و $Y = (2\ 3)H$، آنگاه

$$XY = (1\ 3)H(2\ 3)H = (1\ 3\ 2)H.$$

در حالی که اگر $X = (1\ 2\ 3)H$ و $Y = (1\ 3\ 2)H$، آنگاه

$$XY = (1\ 2\ 3)H(1\ 3\ 2)H = (1)H = H.$$

چون $H \neq (1\ 3\ 2)H$، لذا این ضرب خوش تعریف نیست.

■

بنابراین لازم است خاصیتی روی H گذاشته شود که برطرف کنندهٔ مشکل مثال۵ باشد.
به عبارت دیگر، اگر $aH = a_1H$ و $bH = b_1H$، می‌خواهیم مطمئن شویم که $abH = a_1b_1H$.
به زودی مشخص می‌شود که خاصیت مطلوب همان نرمال بودن H است.

قضیه ۶-۲

فرض کنید H زیرگروهی از گروه G باشد. در این صورت گزاره‌های زیر معادلند.

(۱) H در G نرمال است،

(۲) $(aH)(bH) = abH$ ضرب خوش تعریفی از هم‌دسته‌های چپ H در G است.

اثبات (۱)⇐(۲): فرض کنید $aH = a_1H$ و $bH = b_1H$. نشان دهیم $abH = a_1b_1H$. با استفاده مکرر از نرمال بودن H خواهیم داشت:

$$abH = a(bH) = a(b_1H) = a(Hb_1)$$
$$= (aH)b_1 = (a_1H)b_1 = (Ha_1)b_1$$

$$= Ha_1b_1 = a_1b_1H.$$

(۲) ⇐ (۱): فرض کنید g عنصر دلخواهی از G و h عنصر دلخواهی از H باشد. با توجه به خاصیت (۲) داریم:

$$(ghg^{-1})H = (gh)Hg^{-1}H = gHg^{-1}H = (gg^{-1})H = eH = H.$$

ازاین‌رو $gHg^{-1} \subseteq H$ و در نتیجه H در G نرمال است.

■■■

قضیه ۶-۳

فرض کنید N زیر گروه نرمالی از گروه G باشد. مجموعه تمام هم‌دسته‌های (چپ یا راست) N را با $G/N = \{gN \mid g \in G\}$ نمایش می‌دهیم. در این صورت

(۱) G/N تحت عمل $(aN)(bN) = abN$ یک گروه با مرتبه $[G:N]$ است،

(۲) اگر G آبلی باشد ، آنگاه G/N نیز آبلی است،

(۳) اگر $G =< g >$ دوری باشد، آنگاه G/N هم دوری است، در واقع $G/N =< gN >$.

اثبات (۱): قبلاً نشان دادیم که عمل مذکور روی G/N خوش تعریف است. این عمل دوتایی شرکت پذیر است، زیرا

$$aN(bNcN) = aN(bc)N = a(bc)N = (ab)cN = (ab)NcN = (aNbN)cN.$$

از آن جا که به ازای هر aN،

$$aNeN = (ae)N = aN = eNaN,$$

لذا هم‌دسته $eN = N$ عنصر همانی G/N است. بالاخره برای هر aN در G/N داریم:

$$aNa^{-1}N = (aa^{-1})N = N = (a^{-1}a)N = a^{-1}NaN$$

لذا $(aN)^{-1} = a^{-1}N$ و بنابراین G/N یک گروه است. به‌وضوح تعداد عناصر این گروه عبارت است ازتعداد هم دسته‌های N در G، یعنی $|G/N| = [G:N]$.

(۲): اگر G آبلی باشد، G/N نیز هست زیرا به ازای هر aN و bN در G/N داریم:

$$aNbN = abN = baN = bNaN.$$

(۳): نشان می‌دهیم $G/N =< gN >$. چون هر هم‌دسته در G/N به صورت $g^m N$ است. لذا کافی است نشان دهیم که به ازای هر عدد صحیح m، $g^m N = (gN)^m$.
برای $m \geq 0$، این تساوی با روش استقرا به سادگی اثبات می‌شود. برای $m < 0$، کافی است قرار دهیم $n = -m$، زیرا در این صورت $n > 0$ و داریم:

$$g^m N = \left(g^n\right)^{-1} N = \left(g^n N\right)^{-1} = \left[(gN)^n\right]^{-1} = (gN)^m .$$

■■■

تعریف ۶-۲

اگر N زیر گروه نرمالی از G باشد آنگاه گروه G/N متشکل از همه هم‌دسته‌های N در G **گروه خارج قسمت** G بر N نامیده می‌شود.

❖ **تذکر:** تمام مطالبی را که تا کنون در مورد گروه‌ها آموخته‌ایم، در مورد گروه‌های خارج قسمتی نیز می‌توان به کار برد، فقط باید توجه داشت که عناصر گروه خارج قسمتی هم‌دسته هستند.

مثال ۶ : فرض کنید $\mathbb{C}$ گروه اعداد مختلط و $\mathbb{R}$ گروه اعدادحقیقی باشد. در این صورت

$$\mathbb{C}/\mathbb{R} = \{(a+bi)+\mathbb{R} \,|\, a,b \in \mathbb{R}\} = \{bi+\mathbb{R} \,|\, b \in \mathbb{R}\}.$$

■

مثال۷: فرض کنید $K = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$. نشان می‌دهیم $K \trianglelefteq A_4$ وسپس جدول کیلی A_4/K را رسم می‌کنیم.

حـــل: هم دسته‌های A_4/K عبارتند از:

$$(1)K = K(1) = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\},$$
$$(1\ 2\ 3)K = K(1\ 2\ 3) = \{(1\ 2\ 3),(2\ 4\ 3),(1\ 4\ 2),(1\ 3\ 4)\},$$
$$(1\ 3\ 2)K = K(1\ 3\ 2) = \{(1\ 3\ 2),(1\ 4\ 3),(2\ 3\ 4),(1\ 2\ 4)\}.$$

بنابراین K زیر گروه نرمالی از A_4 است و جدول کیلی A_4/K به صورت زیر است:

www.mathematic87.blogfa.com

$\circ$	K	$(1\,2\,3)K$	$(1\,3\,2)K$
K	K	$(1\,2\,3)K$	$(1\,3\,2)K$
$(1\,2\,3)K$	$(1\,2\,3)K$	$(1\,3\,2)K$	K
$(1\,3\,2)K$	$(1\,3\,2)K$	K	$(1\,2\,3)K$

در ضمن با توجه به این که $|A_4 / K| = 3$، گروه A_4 / K یک گروه دوری است.

■

قضیه زیر محک مفیدی برای آبلی بودن یک گروه در اختیار ما قرار می‌دهد.

قضیه ۶-۴

فرض کنید G گروه و N یک زیر گروهی از $C(G)$ باشد. اگر G / N دوری باشد آنگاه G آبلی است.

اثبات: فرض کنید $G / N =< gN >$. برای هر دو عنصر $a,b \in G$ عناصر aN و bN به شکل $aN = g^m N$ و $bN = g^n N$ می‌باشند. بنابراین برای n_1, n_2 ای در N داریم $a = g^m n_1$ و $b = g^n n_2$. لذا با توجه به این که $N \subseteq C(G)$ خواهیم داشت:

$$ab = g^m n_1 g^n n_2 = g^{n+m} n_1 n_2 = g^n n_2 g^m n_1 = ba,$$

یعنی G آبلی است.

■■■

فرض کنید N زیر گروه نرمالی از G باشد. محک مفیدی برای آبلی بودن G / N موجود است. برای دستیابی به این محک توجه کنید که برای هر دو هم دسته aN و bN از G / N داریم:

$$aNbN = bNaN \Leftrightarrow abN = baN \Leftrightarrow (ba)^{-1} ab \in N \Leftrightarrow a^{-1}b^{-1}ab \in N.$$

این مشاهدات انگیزه‌ای است برای ارائه تعریف زیر:

تعریف ۶-۳ (جابه‌جاگر)

هر عنصری از گروه G به شکل $a^{-1}b^{-1}ab$ را یک **جابه‌جاگر** (یا برگردان) نامیم و با نماد $[a,b]$ نمایش می‌دهیم. مجموعه G' متشکل از حاصل ضرب‌های جابه‌جاگرها را زیر گروه جابه‌جاگر یا **زیر گروه مشتق** در G می‌نامند. در حالت کلی برای هر $n\in\mathbb{N}$ **مشتق nام**، $G^{(n)}$، بطور استقرایی به‌صورت زیر تعریف می‌شود:

$$G^{(1)}=G',\quad G^{(n)}=(G^{(n-1)})',\quad n\geq 2$$

قضیه ۶-۵

فرض کنید N زیر گروه نرمال از گروه G باشد. در این‌صورت:

(۱) G' زیر گروهی نرمال از G است،

(۲) G/N آبلی است اگر وفقط اگر $G'\leq N$.

اثبات (۱): ابتدا نشان می‌دهیم G' یک زیر گروه G است. داریم $e=[e,e]\in G'$. حال فرض کنید $x=[a_1,b_1]...[a_n,b_n]$ و $y=[c_1,d_1]...[c_m,d_m]$ عناصر دلخواهی از G' باشند. با توجه به این که $[a,b]^{-1}=[b,a]$ ، داریم:

$$xy^{-1}=([a_1,b_1]...[a_n,b_n])([c_1,d_1]...[c_m,d_m])^{-1}=[a_1,b_1]...[a_n,b_n][d_m,c_m]...[d_1,c_1].$$

بنابراین طبق آزمون دوم زیر گروه بودن، G' زیر گروهی از G است.

حال نشان می‌دهیم G' یک زیر گروه نرمالی از G است. برای این منظور فرض کنید $x=[a_1,b_1][a_2,b_2]...[a_n,b_n]\in G'$ و $g\in G$. با قرار دادن $gg^{-1}=e$ بین جابه‌جاگرها خواهیم داشت:

$$gxg^{-1}=g[a_1,b_1]g^{-1}.g[a_2,b_2]g^{-1}...g[a_n,b_n]g^{-1}.$$

با توجه به

$$g[a,b]g^{-1}=[gag^{-1},gbg^{-1}],$$

www.mathematic87.blogfa.com

داریم

$$gxg^{-1} = \left[ga_1g^{-1}, gb_1g^{-1}\right]\left[ga_2g^{-1}, gb_2g^{-1}\right]...\left[ga_ng^{-1}, gb_ng^{-1}\right].$$

بنابراین gxg^{-1} نیز برابر حاصل ضربی از جابجاگرها بوده و در نتیجه $gxg^{-1} \in G'$، یعنی $G' \trianglelefteq G$.

(۲): ابتدا فرض کنید $G' \leq N$ و $a,b \in G$. در این صورت داریم $a^{-1}b^{-1}ab \in G'$ و در نتیجه $a^{-1}b^{-1}ab \in N$. پس $abN = baN$، که از این نتیجه می‌شود $aNbN = bNaN$. بنابراین G/N آبلی است، برعکس، اگر G/N آبلی باشد، آنگاه برای تمام $aN, bN \in G/N$ داریم

$$aNbN = bNaN \Rightarrow abN = baN \Rightarrow a^{-1}b^{-1}ab \in N$$

ولذا طبق تعریف $G' \leq N$.

■■■

نتیجه ۶-۲

فرض کنید یک گروه باشد. دراین‌صورت

(۱) G آبلی است اگر وفقط اگر $G' = \{e\}$،

(۲) G/G' آبلی است.

اثبات (۱): در قسمت (۲) قضیه قبل قرار دهید $N = \{e\}$.

(۲): در قسمت (۲) قضیه قبل قرار دهید $N = G'$.

■■■

معمولاً برای مطالعه ساختار گروه G، ساختار G/N $(N \trianglelefteq G)$ را که از بعضی لحاظ ساده تر است مورد بررسی قرار می‌دهیم. البته استفاده از این روش در صورتی دارای اهمیت است که بتوانیم از اطلاعات به دست آمده درباره G/N به اطلاعاتی در مورد G دست یابیم. بعنوان مثال می‌توان به گزارهٔ مهم زیر اشاره داشت:

www.mathematic87.blogfa.com

«اگر به ازای زیرگروهی چون N از $C(G)$، G/N دوری باشد آنگاه G آبلی است».
قضیه زیر ارتباط بین زیر گروه‌های G/N و زیر گروه‌های G را نشان می‌دهد.

قضیه ۶-۶ (قضیه تناظر)

فرض کنید N زیر گروهی نرمال از G باشد.

(۱) اگر $N \subseteq H \leq G$، آنگاه $H/N = \{hN \,|\, h \in H\}$ زیر گروهی از G/N است

(۲) اگر L زیرگروهی از G/N باشد، آنگاه زیر گروهی چون H از G موجود است به طوری که $N \subseteq H$ و داریم $L = H/N$. در واقع $H = \{g \in G \,|\, gN \in L\}$،

(۳) تناظر زیر یک دوسویی بین زیر گروه‌های G/N و زیر گروه‌هایی از G که شامل N باشند برقرار می‌کند.

$$H \leftrightarrow H/N,$$

(۴) تناظر (۳) حافظ شمول است: $H_1/N \subseteq H_2/N \Leftrightarrow H_1 \subseteq H_2$،

(۵) تناظر (۳) حافظ نرمال بودن است: $H/N \trianglelefteq G/N \Leftrightarrow H \trianglelefteq G$.

اثبات (۱): چون $N \trianglelefteq G$ لذا $N \trianglelefteq H$ ودر نتیجه گروه خارج قسمت H/N قابل تعریف است. به‌وضوح گروه خارج قسمتی H/N زیر گروهی از G/N است.

(۲): ابتدا نشان می‌دهیم مجموعه H تعریف شده در (۲) یک گروه است. چون $eN = N \in L$، لذا $e \in H$. اگر g, g_1 عناصری از H باشند، آنگاه $gg_1N = gN.g_1N \in L$ و $g^{-1}N = (gN)^{-1} \in L$. بنابراین gg_1 و g^{-1} متعلق به H هستند. لذا H زیر گروهی از G است. واضح است که $N \leq H$ و با توجه به نرمال بودن N در G خواهیم داشت که $N \trianglelefteq H$، لذا گروه خارج قسمت H/N قابل تعریف است. حال نشان می‌دهیم $L = H/N$. واضح است که $L \subseteq H/N$. برعکس، اگر hN، که $h \in H$، عنصر دلخواهی از H/N باشد، آنگاه طبق تعریف $hN \in L$ ودرنتیجه $H/N \subseteq L$.

(۳): طبق (۲) تابع $H \to H/N$ پوشا است. برای اثبات یک به یک بودن فرض کنید $H/N = H_1/N$ آنگاه در صورتی که (۴) ثابت شود، به آسانی نتیجه می‌شود که $H = H_1$.

www.mathematic87.blogfa.com

(۴) $(\Leftarrow)$: به‌وضوح بر قرار است.

$(\Rightarrow)$: فرض کنید $H_1/N \subseteq H_2/N$. اگر $h_1 \in H_1$ آنگاه $h_1N \in H_2/N$. بنابراین $h_2 \in H_2$ چنان موجود است که $h_1N = h_2N$ وبا توجه به این که $N \subseteq H_2$، داریم $h_1 \in h_2N \subseteq H_2$.

(۵) $(\Leftarrow)$: فرض کنید $H \trianglelefteq G$ و $h \in H$ و $g \in G$. با توجه به این که $ghg^{-1} \in H$ داریم:

$$gNhNg^{-1}N = ghg^{-1}N \in H/N$$

$(\Rightarrow)$: فرض کنید $H/N \trianglelefteq G/N$. اگر $h \in H$ و $g \in G$ آنگاه

$$\left(ghg^{-1}\right)N = gNhNg^{-1}N \in gN(H/N)(gN)^{-1} = H/N.$$

لذا عنصر $h_1 \in H$ چنان موجود است که $ghg^{-1}N = h_1N$ و ازاین‌رو $ghg^{-1} \in HN \subseteq H$ (چون $N \subseteq H$)، یعنی $H \trianglelefteq G$.

■■■

تعریف ۶-۴

گروه $G \neq \{e\}$ را **ساده** گوییم اگر و تنها اگر زیر گروه‌های نرمال آن $\{e\}$ و G باشند.

تعریف ۶-۵

زیر گروه سرهٔ M از گروه G را **نرمال ماکزیمال** گوییم اگر M یک زیر گروه نرمال G و برای هر زیر گروه N که $M \leq N \trianglelefteq G$، داشته باشیم $N = M$ یا $N = G$.

قضیه ۶-۷

(۱) فرض کنید $G \neq \{e\}$ یک گروه متناهی مولد و H یک زیرگروه نرمال وسره از G باشد.

دراین‌صورت H در یک زیر گروه نرمال ماکزیمال قرار دارد،

(۲) زیرگروه نرمال M از گروه G یک زیرگروه نرمال ماکزیمال است اگر وفقط اگر G/M ساده باشد.

اثبات (۱): فرض کنید $G = < x_1, x_2, ..., x_n >$. قرار می‌دهیم:

$\Omega = \{K \mid H \subseteq K, \text{ است } G \text{ از } K \text{ زیرگروه نرمال سره‌ای}\}$.

به‌وضوح Ω غیر تهی است، زیرا $H \in \Omega$. حال زنجیر صعودی $K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$ از عناصر Ω را در نظر می‌گیریم. نشان می‌دهیم $K = \bigcup_{i=1}^{\infty} K_i \in \Omega$. برای این منظور فرض کنید $x, y \in K$. در این صورت اندیس‌های i و j و $(i \geq j)$ چنان موجودند که $x \in K_i$, $y \in K_j$ و لذا $xy^{-1} \in K_i \subseteq K$، در نتیجه K یک زیرگروه G است. حال باید نشان دهیم که K زیرگروه سره‌ای از G است. (برهان خلف)، فرض کنیم $K = G$. در این صورت برای هر $1 \leq i \leq n$ ایده‌ال K_{ℓ_i} از زنجیر فوق‌الذکر موجود است که $x_i \in K_{\ell_i}$. فرض کنید $\ell = \max\{\ell_i\}_{i=1}^{n}$. در این صورت $G =< x_1, x_2, ..., x_n > \subseteq K_\ell$، که تناقض است. بالاخره توجه می‌کنیم که $H \subseteq K \trianglelefteq G$. بنابراین $K \in \Omega$ یک کران بالا از زنجیر بالا است. بنابراین طبق لم زرن، Ω دارای عنصر ماکزیمال M است. به‌وضوح عنصر ماکزیمال Ω (یعنی M) همان زیرگروه نرمال ماکزیمال مطلوب است.

(۲): قضیه تناظر، زیر گروه‌های نرمال H از G که شامل M نیز باشند را با زیر گروه‌های نرمال H/M از G/M نظیرمی‌کند. بنابراین مجموعه اول فقط شامل M و G است اگر وفقط اگر مجموعه دوم فقط شامل $M/M = \{M\}$ و G/M باشد. ازاین‌رو اثبات تمام است.

■■■

۶-۲ همریختی‌ها

یک یکریختی ازگروه G به گروه H تابعی یک به یک و پوشایی چون φ از G به H بود که برای هر $a, b \in G$، $\varphi(ab) = \varphi(a)\varphi(b)$. اگر شرط یک به یک و پوشا بودن φ برداشته شود، φ یک همریختی نامیده می‌شود. به عبارت دیگر یک همریختی از G به H تابعی است که حافظ عمل دو تایی باشد. خواهیم دیدکه همریختی‌ها با گروه‌های خارج قسمتی ارتباط نزدیکی دارند.

www.mathematic87.blogfa.com

تعریف ۶-۶

تابع φ از گروه G به گروه H را یک **همریختی (هوموورفیسم)** گوییم اگر برای هر a,b از G داشته باشیم:

$$\varphi(ab)=\varphi(a)\varphi(b).$$

هرهمریختی $\varphi: G\to G$ یک **درون‌ریختی (اندوموورفیسم)** از G نامیده می‌شود. مجموعهٔ همهٔ درون‌ریختی‌های G را با $\mathrm{End}(G)$ نمایش می‌دهیم.

▼ **یادداشت:** همریختی یک به یک $\varphi: G\to H$ را **تکریختی (مونوموورفیسم)** و همریختی پوشا $\varphi: G\to H$ را **برووریختی (اپی‌موورفیسم)** می‌نامیم.

مثال ۸: بین هر دو گروه دلخواه G,H، همیشه همریختی زیر موسوم **همریختی بدیهی** موجود است.

$$\varphi: G\to H$$
$$g\mapsto e_H$$

■

مثال ۹: فرض کنید G یک گروه و $g\in G$. تابع $\varphi: \mathbb{Z}\to G$ با ضابطه $\varphi(n)=g^n$ یک همریختی است، زیرا

$$\varphi(m+n)=g^{m+n}=g^m g^n=\varphi(m)\varphi(n).$$

■

مثال ۱۰: تابع $\varphi: \mathrm{GL}_n(\mathbb{R})\to \mathbb{R}^*$ با ضابطه $\varphi(A)=\det A$ یک برووریختی است.

■

مثال ۱۱: فرض کنید N زیر گروهی نرمال از گروه G باشد. تعریف می‌کنیم:

$$\gamma : G \to G/N$$
$$g \mapsto gN$$

به‌وضوح γ یک همریختی پوشا (برووریختی) است. این همریختی را **همریختی طبیعی (کانونی)** می‌نامند. در ادامه، این همریختی به‌کرات مورد استفاده قرار خواهد گرفت.

■

مثال ۱۲: فرض کنید $G = G_1 \times ... \times G_n$ حاصل‌ضربی از گروه‌ها باشد. برای هر $1 \le i \le n$ تعریف می‌کنیم:

$$\pi_i : G \to G_i \qquad \text{و} \qquad \delta_i : G \to G_i$$
$$(g_1,...,g_n) \mapsto g_i \qquad g \mapsto (e,...,g,...,e)$$

(g در مکان i ام)

π_i یک برووریختی (موسوم به i-امین تصویر)، δ_i یک تکریختی (موسوم به i-امین انژکسیون) می‌باشد.

■

قضیه ۶-۸

فرض کنید $\varphi : G \to H$ یک همریختی باشد. دراین‌صورت :

(۱) $\varphi(e_G) = e_H$ (φ همانی را حفظ می‌کند) ،

(۲) به ازای هر $g \in G$، $\varphi(g^{-1}) = \varphi(g)^{-1}$ (φ عنصر معکوس را حفظ می‌کند)،

(۳) به ازای هر $g \in G$، هر $n \in \mathbb{Z}$، $\varphi(g^n) = \varphi(g)^n$ (φ توان را حفظ می‌کند).

اثبات: همان استدلالی که قبلاً برای قضیه ۵-۱ در مورد یکریختی‌ها ارائه شد، این جا نیز کار می‌کند.

■■■

www.mathematic87.blogfa.com

قبلاً دیدیم که هر یکریختی حافظ مرتبه است. به عبـارت دیگـر اگـر $\varphi : G \to H$ یـک یکریختـی باشـد، آنگـاه بـرای هـر $g \in G$، $\circ(\varphi(g)) = \circ(g)$. ایـن مطلـب در مـورد همریختی‌ها درست نیست. اما نتیجه زیر در هر حال برقرار است.

نتیجه ۶-۳

فرض کنید $\varphi : G \to H$ یک همریختی باشد. اگر $g \in G$ از مرتبه متناهی باشد، آنگاه $\varphi(g)$ نیز از مرتبه متناهی است و مرتبه $\varphi(g)$، مرتبه g را عاد می‌کند.

اثبات: اگر $\circ(g) = n$، آنگاه $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$. بنابراین $\circ(\varphi(g))$ عدد n را عاد می‌کند.

■■■

در مطالعه همریختی‌ها دو زیر گروه از اهمیت خاصی برخوردار است یکی تصویر و دیگری هسته همریختی.

تعریف ۶-۷

فرض کنید $\varphi : G \to H$ یک همریختی باشد. **تصویر و هسته** φ به ترتیب عبارت اند از:

$$\text{تصویر } \varphi = \mathrm{Im}\varphi = \varphi(G) = \{\varphi(g) | g \in G\},$$

$$\text{هسته } \varphi = \mathrm{Ker}\varphi = \{g \in G | \varphi(g) = e\}.$$

قضیه ۶-۹

فرض کنید $\varphi : G \to H$ یک همریختی باشد. در این صورت

(۱) $\varphi(G)$ یک زیرگروه H است،

(۲) $\mathrm{Ker}\varphi$ زیر گروه نرمالی از G است.

اثبات (۱): واضح است که $e = \varphi(e) \in \varphi(G)$. حال فرض کنید $h = \varphi(g) \in \varphi(G)$ و $h_1 = \varphi(g_1) \in \varphi(G)$. دراین‌صورت :

$$hh_1^{-1} = \varphi(g)\varphi(g_1)^{-1} = \varphi(g)\varphi(g_1^{-1}) = \varphi(gg_1^{-1}) \in \varphi(G).$$

بنابراین طبق آزمون دوم زیر گروه بودن، $\varphi(G)$ زیر گروهی از H است.

(۲): چون $\varphi(e)=e$ لذا $e\in \mathrm{Ker}\,\varphi$. حال اگر k_1,k دو عنصر $\mathrm{Ker}\,\varphi$ باشند، با توجه به این که:

$$\varphi(kk_1^{-1})=\varphi(k)\varphi(k_1^{-1})=\varphi(k)\varphi(k_1)^{-1}=ee=e,$$

خواهیم داشت، $kk_1^{-1}\in \mathrm{Ker}\,\varphi$. بنابراین $\mathrm{Ker}\,\varphi$ زیر گروهی از G است. کافی است نشان دهیم که برای هر $k\in \mathrm{Ker}\,\varphi$ و $g\in G$ داریم $gkg^{-1}\in \mathrm{Ker}\,\varphi$.

$$\varphi(gkg^{-1})=\varphi(g)\varphi(k)\varphi(g^{-1})=\phi(g)e\phi(g^{-1})=\varphi(g)\varphi(g)^{-1}=e.$$

یعنی

$$gkg^{-1}\in \mathrm{Ker}\,\varphi.$$

■■■

مثال ۱۳: تابع قدرمطلق $\varphi:\mathbb{C}^*\to\mathbb{R}^*$ که به ازای هر $z\in\mathbb{C}^*$ به صورت $\varphi(z)=|z|$ تعریف می‌شود، به‌وضوح یک همریختی است هسته φ عبارت است از

$$\mathrm{Ker}\,\varphi=\mathbb{T}=\text{گروه دایره}=\{z\in\mathbb{C}^*\ :\ |z|=1\}$$

■

مثال ۱۴: هسته تابع دترمینان $\mathrm{GL}_n(\mathbb{R})\to\mathbb{R}^*$ گروه خطی خاص $\mathrm{SL}_n(\mathbb{R})$ می‌باشد.

■

هرگاه $\varphi:G\to H$ یک همریختی باشد، φ پوشا ست اگر وفقط اگر $\varphi(G)=H$ یعنی تصویر φ تا حد امکان بزرگ باشد. قضیه زیر نشان می‌دهد که φ یک به یک است اگر وفقط اگر هسته φ تا حد امکان کوچک باشد.

قضیه ۶-۱۰

همریختی φ از گروه G به H یک به یک است اگر وفقط اگر $\mathrm{Ker}\,\varphi=\{e\}$.

اثبات: اگر φ یک به یک باشد، به‌وضوح $\mathrm{Ker}\varphi=\{e\}$. برعکس، فرض کنید که $\mathrm{Ker}\,\varphi=\{e\}$. اگر $\varphi(a)=\varphi(b)$، آنگاه

www.mathematic87.blogfa.com

$$e = \varphi(e) = \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b),$$

و بنابراین $a^{-1}b \in \mathrm{Ker}\,\varphi$. ازاین‌رو $a^{-1}b = e$، یعنی $a = b$.

■■■

تذکر: از قضیه فوق اغلب برای اثبات یک به یک بودن همریختی‌ها استفاده می‌شود.

۶-۳ قضایای یکریختی

قضایای زیر، که به قضایای یکریختی معروف می‌باشند، ارتباط بین همریختی‌ها، زیرگروه‌های نرمال وگروه‌های خارج قسمتی را توصیف می‌کنند.

قضیه ۶-۱۱ (قضیه اول یکریختی)

فرض کنید $\varphi : G \to H$ یک همریختی باشد. در این‌صورت

$$G/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\varphi,$$

و در حالت خاص اگر φ پوشا باشد آنگاه $G/\mathrm{Ker}\,\varphi \cong H$.

اثبات: قرار می‌دهیم $K = \mathrm{Ker}\,\varphi$. تابع $\overline{\varphi}$ را به صورت زیر تعریف می‌کنیم:

$$\overline{\varphi} : G/K \to \mathrm{Im}\varphi$$
$$\overline{\varphi}(gK) = \varphi(g)$$

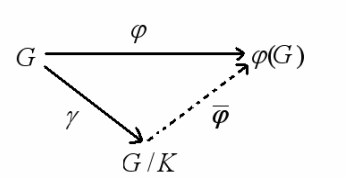
فرض کنید $g_1, g_2 \in G$. در این صورت

$$g_1K = g_2K \Leftrightarrow g_1^{-1}g_2 \in K \Leftrightarrow \varphi(g_1^{-1}g_2) = e \Leftrightarrow \varphi(g_1) = \varphi(g_2) \Leftrightarrow \overline{\varphi}(g_1K) = \overline{\varphi}(g_2K).$$

بنابراین φ خوش‌تعریف و یک به یک است. با توجه به این که پوشا بودن $\overline{\varphi}$ واضح است، $\overline{\varphi}$ یک یکریختی است.

■■■

نمودار زیر قضیه فوق را توضیح می‌دهد. در این جا $\gamma : G \to G/K$ همریختی طبیعی است.



توجه کنیدکه $\varphi = \overline{\varphi}\gamma$ تجزیه‌ای از همریختی φاست به صورت ترکیب یک برووریختی γو یک تکریختی $\overline{\varphi}$. به علاوه $\overline{\varphi}$ تنها همریختی از G/K به H است که در شرط $\varphi = \overline{\varphi}\gamma$ صدق می‌کند. در واقع، وقتی این تساوی برقرار است، داریم

$$\overline{\varphi}(gK) = \overline{\varphi}\big(\gamma(g)\big) = \overline{\varphi}\gamma(g) = \varphi(g)$$

یعنی مقدار $\overline{\varphi}(gK)$ برای هر $gK \in G/K$ مشخص است.

◆ **تذکر:** در نمودارفوق عبارت $\varphi = \overline{\varphi}\gamma$ معمولاً بدین صورت بیان می‌شود:

«که نمودار **تعویض پذیر** است».

▼ **یادداشت:** راه استفاده ازقضیه اول یکریختی به این شرح است:

«برای نشان دادن $G/K \cong H$، باید یک برووریختی $G \to H$ با هسته K تعیین نمود».

در اینجا، بدون احتیاج به هیچ استدلال، می‌دانیم که K در G نرمال است زیرا هستهٔ یک همریختی است.

به مثال‌های زیر توجه کنید.

مثال ۱۵: اگر G یک گروه دوری باشد، آنگاه $G \cong \mathbb{Z}_n$ یا $G \cong \mathbb{Z}$.

حل: فرض کنید $G = \langle g \rangle$. تابع $\varphi : \mathbb{Z} \to G$ را با ضابطه $\varphi(n) = g^n$ به ازای هر $n \in \mathbb{Z}$ تعریف می‌کنیم. به‌وضوح ϕ پوشا است و $\mathrm{Ker}\varphi = \{n | g^n = e\}$، اگر $\circ(g) = n$ متناهی باشد آنگاه $\mathrm{Ker}\varphi = n\mathbb{Z}$ و در نتیجه $G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ و اگر $\circ(g) = \infty$ آنگاه $\mathrm{Ker}\varphi = \{0\}$ و

www.mathematic87.blogfa.com

لذا $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

■

قبلاً این نتیجه را مستقیماً با ساختن یک یکریختی نشان داده‌ایم. در صورتی که تنها چیزی که در این جا لازم داریم یک همریختی است و بقیه کارها را قضیه اول یکریختی انجام می‌دهد.

مثال ۱۶: نشان می‌دهیم $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$، که در این جا $\mathbb{T} = \{z \in \mathbb{C} : |z|=1\}$ همان گروه دایره‌ای است.

حـــل: تابع $\varphi : \mathbb{R} \to \mathbb{T}$ با ضابطه $\varphi(x) = e^{2\pi xi}$ یک همریختی است. زیرا:

$$\varphi(x+y) = e^{2\pi(x+y)i} = e^{2\pi xi}e^{2\pi yi} = \varphi(x)\varphi(y)$$

به علاوه φ پوشاست و همچنین $\mathrm{Ker}\varphi = \mathbb{Z}$. حال نتیجه مطلوب با استفاده از قضیه اول یکریختی به آسانی به دست می‌آید.

■

مثال ۱۷: اگر $K_1 \trianglelefteq G_1$ و $K_2 \trianglelefteq G_2$، آنگاه $(G_1 \times G_2)/(K_1 \times K_2) \cong G_1/K_1 \times G_2/K_2$.

حـــل: تابع $\varphi : G_1 \times G_2 \to G_1/K_1 \times G_2/K_2$ با ضابطه $\varphi(g_1, g_2) = (g_1K_1, g_2K_2)$ یک بروریختی است و $\mathrm{Ker}\varphi = K_1 \times K_2$، لذا طبق قضیه اول یکریختی نتیجه مطلوب حاصل می‌شود.

■

قضیه ۶-۱۲

فرض کنید G یک گروه متناهی و $H \leq G$ و $H \neq G$.

(۱) اگر $|G| \nmid [G:H]!$، آنگاه G ساده نیست. به عبارت دیگر، H باید حاوی یکی از زیرگروه‌های نرمال غیر بدیهی G باشد،

(۲) اگر $[G:H] = p$ و p کوچکترین عدد اولی باشد که $|G|$ را عاد می‌کند، آنگاه $H \trianglelefteq G$.

www.mathematic87.blogfa.com

اثبات: فرض کنید X مجموعه همه هم‌دسته‌های چپ H در G باشد. همریختی زیر را داریم.

$$\varphi : G \to S_X$$
$$g \mapsto \varphi_g$$

جاییکه φ_g به‌صورت زیر تعریف می‌شود:

$$\varphi_g : X \to X$$
$$xH \mapsto gxH$$

فرض کنید $K = \mathrm{Ker}\varphi$. به‌وضوح $K \le H$ (در واقع $K = \bigcap_{x\in G} xHx^{-1}$). از طرفی طبق قضیه اول یکریختی $G/K \cong \mathrm{Im}\varphi \le S_X$ و لذا $|G/K| \mid [G:H]!$.

اثبات (۱): چون $|G| \nmid [G:H]!$، پس $K \neq \{e\}$. از طرفی چون $K \le H < G$، پس H حاوی زیرگروه نرمال غیر بدیهی K از G می‌باشد.

(۲): چون $|G/K| \mid |G|$ و $|G/K| \mid p!$، لذا $|G/K| = 1$ یا $|G/K| = p$. اگر $|G/K| = 1$، آنگاه $K = H = G$، که تناقض است. بنابراین $|G/K| = p$ و درنتیجه

$$p = |G/K| = [G:K] = [G:H][H:K] = p[H:K].$$

ازاین‌رو $[H:K] = 1$، یعنی $H = K$، پس H زیرگروه نرمالی از G است.

■■■

❖ **تذکر:** در قضیهٔ فوق زیرگروه $K = \bigcap_{x\in G} xHx^{-1}$ را **زیر گروه مغز (کر)** H در G نامیده و با علامت $\mathrm{Core}_G(H)$ نمایش می‌دهیم.

▼ **یادداشت:** گروه H را **تصویر همریخت** گروه G نامیم هرگاه به ازای یک همریختی $\varphi : G \to H$ داشته باشیم $\varphi(G) = H$. به‌وضوح هر گروه خارج

www.mathematic87.blogfa.com

قسمتی G/K یک تصویر همریخت از G است (تحت همریختی طبیعی $G \to G/K$). همچنین طبق قضیه اول یکریختی هر تصویر همریخت از G نیز با یک گروه خارج قسمتی از آن یکریخت است.

لم ۶-۱

فرض کنید G یک گروه $H \leq G$ و $N \trianglelefteq G$. دراین‌صورت

(۱) $HN = NH \leq G$،

(۲) $H \cap N \trianglelefteq H$،

(۳) به علاوه اگر $H \trianglelefteq G$ آنگاه $HN \trianglelefteq G$.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضیه ۶-۱۳ (قضیه دوم یکریختی)

اگر G یک گروه و $H \leq G$ و $N \trianglelefteq G$ آنگاه

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

اثبات: با توجه به قسمت (۱) لم قبل، HN یک گروه است. تعریف می‌کنیم:

$$\varphi : H \to HN/N$$
$$h \mapsto hN$$

به‌وضوح φ خوش تعریف است. φ یک همریختی است زیرا برای هر h_1 ، $h_2 \in H$ داریم:

$$\varphi(h_1h_2) = h_1h_2N = h_1Nh_2N = \varphi(h_1)\varphi(h_2).$$

با توجه به این که

$$HN/N = \{hnN \,|\, h \in H, n \in N\} = \{hN \,|\, h \in H\},$$

پوشا بودن φ حاصل می‌شود. همچنین داریم:

$$\mathrm{Ker}\varphi = \{h \in H \,|\varphi(h) = N\} = \{h \in H \,|hN = N\} = \{h \in H \,|h \in N\} = H \cap N.$$

بنابراین طبق قضیه اول یکریختی حکم به دست می‌آید.

■■■

قضیه ۶-۱۴ (قضیه سوم یکریختی)

فرض کنید H و K زیرگروه‌های نرمالی از G باشند و $H \leq K$. در این‌صورت

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

اثبات: تعریف می‌کنیم:

$$\varphi : G/H \to G/K$$
$$gH \mapsto gK$$

به‌وضوح φ یک همریختی خوش تعریف و پوشا است. حال هسته φ را به دست می‌آوریم.

$$\mathrm{Ker}\varphi = \{gH \,|\varphi(gH) = K\} = \{gH \,|gK = K\} = \{gH \,|g \in K\} = K/H,$$

و بدین ترتیب طبق قضیه اول یکریختی حکم ثابت می‌شود.

■■■

قضیه ۶-۱۵(قضیه تناظر)

فرض کنید $\varphi : G \to G_1$ یک همریختی باشد و $K = \mathrm{Ker}\varphi$.

(۱) اگر H زیرگروهی از G شامل K باشد، آنگاه $\varphi(H) = \{\varphi(h) | h \in H\}$ زیرگروهی از $\varphi(G)$ است.

(۲) اگر L زیرگروه $\varphi(G)$ باشد، آنگاه $L = \varphi(H)$، جایی که H زیرگروهی از G شامل K به صورت زیر است:

$$H = \{g \in G | \varphi(g) \in L\}$$

(۳) تناظر زیر یک دو سویی بین زیرگروه‌های H شامل K از G و زیرگروه‌های $\varphi(H)$

www.mathematic87.blogfa.com

از $\varphi(G)$ برقرار می‌سازد:

$$\varphi(H) \leftrightarrow H$$

(۴) تناظر (۳) حافظ رابطه مشمول است:

$$\varphi(H) \subseteq \varphi(H_1) \Leftrightarrow H \subseteq H_1$$

۵) تناظر (۳) حافظ نرمال بودن است:

$$\varphi(H) \trianglelefteq \varphi(G) \Leftrightarrow H \trianglelefteq G.$$

اثبات: اثبات این قضیه کاملاً شبیه به قضیه ۶ است و به خواننده واگذار می‌گردد.

■■■

۶-۴ ساده بودن $A_n (n \geq 5)$

ثابت می‌کنیم A_n برای $n \geq 5$ ساده است. برای اثبات این مطلب احتیاج به لم‌های جالب زیر داریم.

لم ۶-۲

برای $n \geq 3$ ، A_n توسط دورهای به طول 3 تولید می‌شود.

اثبات: با توجه به این که هر دور به طول 3 در A_n است، کافی است نشان دهیم که هر جایگشت از A_n را می‌توان به صورت حاصل ضربی از دورهای به طول 3 نوشت. اما هر عنصر A_n حاصل ضرب تعداد زوجی از ترانهش هاست پس وجود تساوی‌های زیر اثبات را کامل می‌کند.

$$(a\ b)(a\ b) = (1),$$
$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d),$$
$$(a\ b)(a\ c) = (a\ c\ b).$$

■■■

لم ۶-۳

فرض کنید $n \geq 5$. اگر $H \trianglelefteq A_n$ و H شامل یک دور به طول 3 باشد، آنگاه $H = A_n$.

اثبات: فرض کنید $(a\ b\ c) \in H$ یک دور به طول 3 باشد. اگر $(u\ v\ w)$ یک دور دلخواهی به طول 3 باشد، آنگاه با توجه به قضیه۴-۶ عنصر $\delta \in S_n$ چنان موجود است که $\delta(a\ b\ c)\delta^{-1} = (u\ v\ w)$. حال دو حالت در نظر می‌گیریم:

حالت (۱): $\delta \in A_n$. در این‌صورت $(u\ v\ w) \in H$.

حالت (۲): $\delta \notin A_n$. در این‌صورت δ یک جایگشت فرد است. چون $n \geq 5$ فرض کنید $d, e \in \{1,2,\ldots,n\}$ و $d, e \notin \{a,b,c\}$. دراین‌صورت:

$$(u\ v\ w) = \delta(a\ b\ c)\delta^{-1} = \delta(a\ b\ c)(d\ e)(d\ e)\delta^{-1} = \delta(d\ e)(a\ b\ c)(d\ e)\delta^{-1}$$
$$= (\delta(d\ e))(a\ b\ c)\big(\delta(d\ e)\big)^{-1},$$

و در نتیجه $(u\ v\ w) \in H$. بنابراین H شامل تمام دورهای به طول 3 می‌باشد. بنابراین طبق لم قبل $H = A_n$.

■■■

قضیه ۶-۱۶

گروه متناوب A_n به ازای $n \geq 5$ ساده است.

اثبات: فرض کنید $H \neq \{e\}$ یک زیرگروه نرمال از A_n باشد. فرض کنید δ یک جایگشت غیر همانی H باشد، به طوری که کمترین تعداد عناصر، مثلاً m عنصر، را حرکت دهد. مسلماً $m \geq 3$ اگر $m = 3$ آنگاه δ دوری به طول 3 بوده و با توجه به لم قبل اثبات کامل

www.mathematic87.blogfa.com

است. نشان می‌دهیم که فرض $m \geq 4$ به تناقض منجر می‌شود. فرض کنید $\delta = \delta_1\delta_2...\delta_k$ تجزیه δ به حاصل ضرب دورهای مجزا باشد. دو حالت زیر ممکن است:

حالت (۱): تمامی δ_i ها ترانهش هستند. در این صورت δ باید حداقل حاصل ضربی از دو ترانهش مجزا باشد، یعنی

$$\delta = (a\ b)(c\ d)\delta_3...\delta_k$$

فرض کنید $e \notin \{a,b,c,d\}$ قرار می‌دهیم $\beta = (c\ d\ e)$ و $\delta' = \delta^{-1}\beta\delta\beta^{-1}$ به آسانی ملاحظه می‌شود که $\delta'(a) = a$ و $\delta'(b) = b$ و $\delta'(e) \neq e$ و اگر $u \notin \{a,b,c,d,e\}$ و $\delta(u) = u$ آنگاه $\delta'(u) = u$. یعنی δ' تعداد کمتری عنصر را نسبت به δ حرکت می‌دهد، که این با انتخاب δ در تناقض است.

حالت (۲): حداقل یکی از δ_i ها ترانهش نیست. چون دورهای مجزا جابجا می‌شوند، می‌توان فرض کرد $\delta_1 = (a\ b\ c...)$، یعنی:

$$\delta = (a\ b\ c...)\delta_2...\delta_k$$

اگر $m = 4$ آنگاه δ دوری به طول 4 خواهد بود که جایگشت فردی است. پس فرض کنید $m \geq 5$. یعنی فرض کنید δ دو عنصر دیگر مثلاً e,f را نیز کنار c,b,a حرکت دهد. مانند حالت (۱) قرار می‌دهیم $\beta = (c\ d\ e)$ و $\delta' = \delta^{-1}\beta\delta\beta^{-1}$. به آسانی مشاهده می‌شود که $\delta'(a) = a$ و $\delta'(b) \neq b$ و برای هر $u \notin \{a,b,c,d,e\}$ اگر $\delta(u) = u$ آنگاه $\delta'(u) = u$. بنابراین مانند حالت (۱) تناقض مطلوب به دست می‌آید.

■■■

توضیح تاریخی

نشان داده می‌شود که هر گروه متناهی نوعی تجزیه به گروه‌های ساده دارد که عوامل، قطع نظر از ترتیب یکتا هستند. این وضعیت مانند تجزیه اعداد طبیعی به اعداد اول است. بنابراین گروه‌های ساده متناهی بلوک‌های ساختمانی گروه‌های متناهی‌اند.

www.mathematic87.blogfa.com

اولین گروه‌های غیر آبلی ساده گروه‌های متناوب هستند. گالوا اولین کسی بود که نشان داد A_5 ساده است. تعیین و رده‌بندی تمام گروه‌های متناهی ساده در سال 1981 تکمیل شد. در سه دهه گذشته بیش از صدها ریاضیدان روی این موضوع کار می‌کردند. به جرأت می‌توان گفت که این کار یکی از بزرگترین دستاوردهای ریاضی در قرن بیستم است.

یکی از کارهای عمده‌ای که در این راستا انجام شد. پاسخ به حدس برنساید بود که مدت‌ها بدون جواب مانده بود. تامپسون وفایت در سال 1963 حدس قدیمی برنساید مبنی بر این که هر گروه ساده ناآبلی متناهی از مرتبه زوج است را ثابت کردند. این مطلب در مجله "Pacific Journal of Mathematics" به چاپ رسید و حدود ۲۵۰ صفحه اثبات دارد.

شایان ذکر است که گروه‌های ناآبلی ساده از سه نوع‌اند:

(۱) A_n ها برای $n \geq 5$،

(۲) گروه‌های ماتریسی روی میدان‌های متناهی،

(۳) گروه‌های که به گروه‌های **پراکنده** موسوم‌اند و تعداد آنها۲۶ است و هر یک از آنها باید جداگانه بررسی شود. گریس با ساختن گروهی از نوع (۳)، موسوم به **"غول"** با حدود 10^{54} عنصر کار رده‌بندی را کامل ساخت. در خاتمه اشباخر شرح نهایی رده‌بندی را در اوت 1980 ارائه داد.

تمرینها

۱. در هر یک از حالات زیر مشخص کنید آیا H زیرگروه نرمال G هست یا خیر. اگر H یک زیرگروه نرمال باشد، جدول کیلی G/H را تشکیل دهید.

(a) $G = S_4$ ، $H = A_4$،

(b) $G = Q$ ، $H = \{\pm 1, \pm I\}$،

(c) $G = S_4$ ، $H = D_4$.

www.mathematic87.blogfa.com

۲. مطلوب است تمام زیرگروه‌های نرمال گروه‌های S_3 ، D_4، D_6 و Q.

۳. کدامیک از توابع زیر همریختی‌اند. اگر تابع همریختی باشد، هسته آن چیست.

(a) تابع $\varphi : \mathbb{R}^* \to \mathrm{GL}_2(\mathbb{R})$ با ضابطه:

$$\varphi(a) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$$

(b) تابع $\varphi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}$ با ضابطه:

$$\varphi(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = ad - bc$$

(c) تابع $\varphi : \mathrm{M}_2(\mathbb{R}) \to \mathbb{R}$ با ضابطه:

$$\varphi(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = b$$

۴. فرض کنید:

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} | a,b,c \in \mathbb{R} \right\}$$

نشان دهید که:

(a) G زیرگروهی از $\mathrm{SL}_3(\mathbb{R})$ و $C(G) \cong \mathbb{R}$،

(b) $G/C(G) \cong \mathbb{R} \times \mathbb{R}$.

۵. (a) نشان دهید تابع $\varphi : \mathbb{Z} \to \mathbb{Z}$ با ضابطه $\varphi(n) = 7n$ یک همریختی است. تصویر و هسته φ چیست،

(b) فرض کنید G یک گروه آبلی باشد. اگر $n \in \mathbb{Z}$ آنگاه تابع $\varphi : G \to G$ با ضابطه $\varphi(x) = nx$ یک همریختی است،

(c) فرض کنید A یک ماتریس $m \times n$ با درایه‌های حقیقی باشد. نشان دهید که ضرب ماتریسی $X \to AX$ یک همریختی از $\mathbb{R}^n$ به $\mathbb{R}^m$ تعریف می‌کند.

۶. همریختی نابدیهی $\mathbb{Q} \to S_3$ موجود نیست.

۷. فرض کنید G به وسیله مجموعه $X=\{x_i \mid i\in I\}$ تولید شده باشد، که در آن I مجموعه‌ای اندیسگذار است. فرض کنید $\varphi: G\to H$ یک همریختی باشد. نشان دهید که مقدار φ در هر عنصر G با مقدارهای $\varphi(x_i)$ کاملاً مشخص می‌شود. در حالت خاص، هر همریختی یک گروه دوری با مقدار آن در یکی از مولدهای گروه کاملاً مشخص می‌شود.

۸. (a) مطلوب است تمام همریختی‌های از $\mathbb{Z}$ به $\mathbb{Z}_3$،

(b) همهٔ همریختی‌های گروهی $\mathbb{Z}\to\mathbb{Z}$ را توصیف کنید،

(c) فرض کنید G یک گروه متناهی مولد باشد. نشان دهید به ازای هر عدد طبیعی n، G دارای تعداد متناهی زیرگروه با اندیس n است.

۹. فرض کنید G و H دو گروه جمعی آبلی باشند. مجموعه همه همریختی‌های گروهی $\alpha: G\to H$ را با $\mathrm{Hom}(G,H)$ نمایش می‌دهیم. هر گاه $\alpha,\beta\in \mathrm{Hom}(G,H)$ جمع آنها را به صورت $\alpha+\beta: G\to H$ با ضابطه $(\alpha+\beta)(g)=\alpha(g)+\beta(g)$ تعریف می‌کنیم. نشان دهید:

(a) $\mathrm{Hom}(G,H)$ تحت این عمل جمع یک گروه آبلی است،

(b) به ازای هر گروه جمعی آبلی H، $\mathrm{Hom}(\mathbb{Z},H)\cong H$،

(c) اگر $d=(m,n)$ آنگاه $\mathrm{Hom}(\mathbb{Z}_m,\mathbb{Z}_n)\cong\mathbb{Z}_d$.

۱۰. فرض کنید $N\trianglelefteq G$. نشان دهید که اگر N و G/N هر دو خاصیتهای مفروض زیر را داشته باشند، G هم داراست.

(a) مرکز بدیهی است ،

(b) هر عنصر از مرتبهٔ توانی از عدد اول p است،

(c) هر عنصر از مرتبه متناهی،

(d) بطور متناهی تولید شدن.

۱۱. (a) فرض کنید $[G:H]=2$. نشان دهید H یک زیرگروه نرمال G است،

(b) A_n تنها زیرگروه S_n با اندیس 2 است.

۱۲. فرض کنید G یک گروه باشد.

www.mathematic87.blogfa.com

(a) اگر $H \trianglelefteq G$ و $K \leq G$، آنگاه $(HK)' \leq HK'$ و $(G/H)' = (G'H)/H$،

(b) فرض کنید $H \trianglelefteq G$ و $K \trianglelefteq G$، نشان دهید:

$$H/(H \cap K) \times K/(H \cap K) \cong HK/(H \cap K).$$

(c) فرض کنید $H \leq G$، $K \leq G$ و $G = H \times K$. نشان دهید $G/K \cong H$ و $G/H \cong K$.

۱۳. (a) فرض کنید $\varphi : G \to H$ یک تکریختی باشد و $N \trianglelefteq G$. نشان دهید که $\varphi(N) \trianglelefteq \varphi(G)$ و $\varphi(G)/\varphi(N) \cong G/N$،

(b) فرض کنید $\varphi : G \to H$ یک برووریختی و $K \trianglelefteq H$. نشان دهید $\varphi^{-1}(K) \trianglelefteq G$ و $G/\varphi^{-1}(K) \cong H/K$.

۱۴. (a) مرکز ساز $g \in G$ به صورت زیر تعریف می‌شود:

$$C(g) = \{x \in G | xg = gx\}.$$

نشان دهید که $C(g)$ یک زیرگروه G است. اگر $\langle g \rangle \trianglelefteq G$ آنگاه $C(g) \trianglelefteq G$،

(b) فرض کنید H یک زیرگروه دوری از G باشد. اگر $H \trianglelefteq G$، آنگاه هر زیرگروه H در G نرمال است.

۱۵. (a) نشان دهید $G/C(G) \cong \mathrm{Inn}(G)$،

(b) نشان دهید $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$.

۱۶. اگر $N \trianglelefteq G$، $|N|$متناهی، $H \leq G$، $[G:H]$ متناهی و $(|N|,[G:H]) = 1$، آنگاه $N \leq H$.

۱۷. اگر $N \trianglelefteq G$، $[G:N]$ متناهی، $H \leq G$، $|H|$ متناهی و $(|H|,[G:N]) = 1$، آنگاه $H \leq N$.

۱۸. نشان دهید:

(a) $H \trianglelefteq N_G(H)$،

(b) اگر $H \trianglelefteq K$ آنگاه $K \subseteq N_G(H)$ (یعنی $N_G(H)$ بزرگترین زیرگروه G است که در آن H نرمال است)،

(c) $H \trianglelefteq G$ اگر و فقط اگر $N_G(H) = G$،

www.mathematic87.blogfa.com

(d) $C_G(H) \trianglelefteq N_G(H)$،

(e) $N_G(H)/C_G(H)$ با زیر گروهی از $\mathrm{Aut}(G)$ یکریخت است.

۱۹. با یک مثال نشان دهید اگر H زیر گروه نرمالی از گروه G و K زیرگروه نرمالی از H باشد، آنگاه الزاماً K زیرگروه نرمالی از G نخواهد بود.

۲۰ . فرض کنید G یک گروه و $H \leq G$. در این صورت H را یک **زیر گروه مشخصه** G می‌نامیم، هرگاه به ازای تمام خودریختی‌های φ از G داشته باشیم $\varphi(H) \leq H$. نشان دهید:

(a) اگر H زیرگروه مشخصه از G باشد، آنگاه به ازای تمام خودریختی‌های φ از G داریم $\varphi(H) = H$،

(b) اگر H زیرگروه مشخصه از G باشد، آنگاه $H \trianglelefteq G$،

(c) فرض کنید G یک گروه و $K \leq H \trianglelefteq G$. اگر K زیرگروه مشخصه H باشد، آنگاه $K \trianglelefteq G$،

(b) فرض کنید G یک گروه باشد. نشان دهید $C(G)$ و G' زیرگروه‌های مشخصه G می‌باشند.

۲۱ .(a) فرض کنید G زیرگروهی از S_n باشد. اگر G شامل جایگشتی فرد باشد، آنگاه درست نیمی از عناصر G جایگشت زوج ونیم دیگرجایگشت فردند. نتیجه بگیرید G زیرگروهی از اندیس 2 دارد،

(b) فرض کنید G یک گروه ساده و H زیرگروه سره‌ای از آن باشد بطوریکه $[G : H] = n$. نشان دهید G با زیرگروهی از A_n یکریخت است،

(c) هرگاه گروه متناهی G زیرگروه سره‌ای از اندیس n داشته باشد بطوریکه $|G| \nmid n!/2$، آنگاه G ساده نیست.

۲۲ .(a) فرض کنید H یک زیرگروه سره از گروه G باشد. نشان دهید $\bigcup_{g \in G} gHg^{-1} \neq G$،

(b) فرض کنید G یک گروه متناهی غیر آبلی باشد. اگر هر زیر گروه سره G آبلی باشد، ثابت کنید G ساده نیست.

www.mathematic87.blogfa.com

مسائل مبارزه طلب

۱. فرض کنید G یک گروه متناهی غیرآبلی باشد. اگر هر زیر گروه سرهٔ G آبلی باشد، آنگاه ساده نیست.

۲. فرض کنید m عددی فرد و G گروهی از مرتبهٔ $2m$ باشد. نشان دهید G زیرگروهی از اندیس 2 دارد.

۳. گروهی متناهی مانند G مثال بزنید که زیرگروهی نرمال چون H داشته باشد که $|\mathrm{Aut(H)}| < |\mathrm{Aut(G)}|$.

۴. فرض کنید G گروهی از مرتبهٔ n باشد. اگر $(n, \phi(n)) = 1$، آنگاه G آبلی است.

۵. گروهی مانند G موجود نیست بطوریکه $G' \cong S_4$.

منابعی برای مطالعهٔ بیشتر

1. Fraleigh, J. B. *A First Course in Abstract Algebra*. Addison-Wesley, 1999.

2. Malik, D. S., Mordeson John M., Sen, M. K. *Fundamentals of Abstract Algebra*. McGraw-Hill Companies, Inc., 1996.

3. Nickelson, W. K. *Introduction to Abstract Algebra*. Wiley-Interscience seience (John-Wiley & Sons) Hoboken, 2007.

www.mathematic87.blogfa.com

فصل ۷

گروه‌های آبلی متناهی مولد

در این فصل می‌خوانید:

۷-۱ قضیهٔ اساسی گروه‌های آبلی متناهی مولد
۷-۲ مثال‌ها و کاربردها
۷-۳ اثبات قضیهٔ اساسی گروه‌های آبلی متناهی مولد

مقدمه

قبلاً نشان دادیم که هر گروه دوری در صورت متناهی بودن با یک $\mathbb{Z}_n$ و در صورت نامتناهی بودن با $\mathbb{Z}$ یکریخت است. به عبارت دیگر گروه‌های دوری را رده‌بندی کرده‌ایم. در این فصل در حالت کلی به رده‌بندی گروه‌های آبلی متناهی مولد می‌پردازیم. نشان می‌دهیم که هر گروه آبلی متناهی مولد را می‌توان به یک و تنها یک صورت به حاصل ضرب مستقیم تعدادی از زیرگروه‌های دوری غیربدیهی‌اش تجزیه کرد. بنابراین خواص ساختاری گروه آبلی متناهی مولد به وسیله چنین زیرگروه‌های دوری کاملاً مشخص می‌شود.

۷-۱ قضیه اساسی گروه‌های آبلی متناهی مولد

ابتدا به بیان صورت قضیهٔ اساسی گروه‌های آبلی متناهی مولد می‌پردازیم. سپس چند مثال و کاربرد از این قضیه را ارایه می‌دهیم و در نهایت با اثبات (نسبتاً طولانی) این قضیه، فصل را به پایان می‌رسانیم.

قضیه۷-۱ (صورت اول قضیهٔ اساسی گروه‌های آبلی متناهی مولد)

هر گروه آبلی متناهی مولد G یکریخت است با حاصل‌ضرب مستقیمی از گروه‌های دوری به صورت

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{s \text{ بار}}$$

که در آن هر عدد m_i عدد m_{i+1} را عاد می‌کند. همچنین عدد s (**عدد بتی** G) و **ضرایب تاب** m_i یکتا می‌باشند.

قضیه۷-۲ (صورت دوم قضیهٔ اساسی گروه‌های آبلی متناهی مولد)

هر گروه آبلی متناهی مولد یکریخت است با حاصل‌ضرب مستقیمی از گروه‌های دوری به صورت

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{n_\ell}} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{t \text{ بار}},$$

که در این جا نیز عدد r و توان‌های اول $p_i^{n_i}$ یکتا می‌باشند. ($p_i^{n_i}$ ها لزوماً متمایز نیستند).

▼ **یادداشت:** اصطلاحات عدد بتی و ضرایب تاب از توپولوژی جبری می‌آیند.

از دو قضیه فوق به آسانی نتیجه مهم زیر به دست خواهد آمد.

قضیه۷-۳ (قضیهٔ اساسی گروه‌های آبلی متناهی)

هر گروه آبلی متناهی به دو صورت مختلف با حاصل‌ضرب مستقیم گروه‌های دوری یکریخت است.

(۱) با حاصل‌ضرب مستقیمی به صورت

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r},$$

که در آن هر عدد m_i عدد m_{i+1} را عاد می‌کند،

(۲) با حاصل‌ضرب مستقیمی به صورت

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{n_\ell}},$$

که در آن p_i ها اعدادی اول (نه لزوماً متمایز) هستند.

در هر دو حالت حاصل‌ضرب مستقیم منحصر به فرد است مگر احیاناً با تغییر ترتیب عوامل، یعنی ضرایب تاب m_i منحصر به فرد هستند و توان‌های اول $p_i^{n_i}$ نیز منحصر به فردند.

۷-۲ مثال‌ها و کاربردها

با استفاده از یک تابع حسابی و قضیه فوق می‌توانیم تعداد گروه‌های آبلی از مرتبه n را تعیین کنیم.

تعریف ۷-۱

فرض کنید G گروهی آبلی و $|G| = p^n$ که p عددی است اول و $G \cong \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$ به طوری که $e_1 \geq \ldots \geq e_k \geq 1$. در این صورت اعداد $p^{e_k}, \ldots, p^{e_1}$ را **پایاهای** G می‌نامند.

نتیجه۷-۱

هر دو گروه از مرتبه p^n یکریخت‌اند اگر و تنها اگر پایاهای آنها یکسان باشند.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۷-۲

فرض کنید $e_1,\dots,e_k$، n اعدادی طبیعی باشند، $e_1 \geq \dots \geq e_k$. در این صورت مجموعه $\{e_1,\dots,e_k\}$ را یک **افراز** n خوانیم هر گاه $n = e_1 + \dots + e_k$.

قضیه۷-۴

تعداد گروه‌های آبلی غیر یکریخت مرتبه p^n برابر است با تعداد افرازهای n.

اثبات: فرض کنید $\mathscr{P}_A(n)$ گردایه همه گروه‌های آبلی دو به دو غیر یکریخت از مرتبه p^n، $\mathscr{P}(n)$ مجموعه همه افرازهای n باشد. فرض کنید $G \in \mathscr{P}_A(n)$ ، $p^{e_k},\dots,p^{e_1}$ پایاهای G باشند. تابع $\theta : \mathscr{P}_A(n) \to \mathscr{P}(n)$ با ضابطه $G \mapsto \{e_1,\dots,e_k\}$ طبق نتیجه فوق دو سویی است.

■■■

با توجه به قضیهٔ اساسی گروه‌های آبلی متناهی و قضیه فوق خواهیم داشت.

نتیجه۷-۲

فرض کنید $n = p_1^{n_1} \dots p_k^{n_k}$ که p_i ها اعداد اول متمایز هستند. در این صورت تعداد گروه‌های آبلی غیر یکریخت از مرتبه n برابر است با

$$\left|\mathscr{P}(n_1)\right| \times \dots \times \left|\mathscr{P}(n_k)\right|.$$

مثال۱: می‌خواهیم گروه‌های آبلی مرتبه 2^5 را با تقریب یکریختی پیدا کنیم. ابتدا توجه داریم که افرازهای عدد 5 عبارتند از:

$$\begin{aligned} 5 &= 1+1+1+1+1 \\ &= 2+1+1+1 \\ &= 2+2+1 \\ &= 3+1+1 \\ &= 3+2 \\ &= 4+1 \\ &= 5 \end{aligned}$$

بنابراین 7 گروه آبلی غیر یکریخت از مرتبه 2^5 وجود دارد که عبارتند از:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$$
$$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\mathbb{Z}_8 \times \mathbb{Z}_4$$
$$\mathbb{Z}_{16} \times \mathbb{Z}_2$$
$$\mathbb{Z}_{32}.$$

■

مثال۲: تعداد گروه‌های آبلی از مرتبه $360 = 2^3 \times 3^2 \times 5$ برابر است با $|\mathscr{P}(1)|.|\mathscr{P}(2)|.|\mathscr{P}(3)| = 1.2.3 = 6$. تمامی این گروه‌ها را بر اساس قسمت (۱) و (۲) قضیهٔ اساسی به صورت زیر فهرست می‌کنیم:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{60}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{180}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{120}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{360}.$$

■

www.mathematic87.blogfa.com

تعریف ۷-۳

فرض کنید p عددی اول باشد. گروه G را یک p-**گروه** گوییم اگر مرتبهٔ هر عنصر آن توانی از p باشد.

گزاره ۷-۱

اگر G یک p-گروه آبلی متناهی مولد باشد، آنگاه $|G| = p^n$.

اثبات: با توجه به صورت دوم قضیهٔ اساسی گروه‌های آبلی متناهی مولد خواهیم داشت:

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{n_\ell}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{t \text{ بار}}$$

اگر $t \neq 0$، آنگاه G دارای عنصری از مرتبه نامتناهی خواهد بود. پس $t = 0$، یعنی

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{n_\ell}}.$$

چون مرتبه هر عنصر G توانی از عدد اول p است، پس $p_1 = p_2 = \ldots = p_\ell = p$ یعنی،

$G \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_\ell}}$ پس $|G| = p^n$، جاییکه $n = n_1 + \cdots + n_\ell$.

■■■

۷-۳ اثبات قضیه اساسی گروه‌های آبلی متناهی مولد

در این بخش مفهوم گروه آبلی آزاد را معرفی و احکامی درباره آن ثابت می‌کنیم و با ارایه اثباتی از قضیهٔ اساسی گروه‌های آبلی متناهی مولد بخش را به اتمام می‌رسانیم.

تعریف ۷-۴

فرض کنید G یک گروه آبلی و X یک زیر مجموعه ناتهی از G باشد. گوییم X یک **پایه** برای G است اگر $G=\langle X\rangle$ و X مستقل خطی باشد، یعنی برای هر $n_i\in\mathbb{Z}$، $x_i\in X$، $1\le i\le k$،

$$n_1x_1+n_2x_2+\cdots+n_kx_k=0\Rightarrow n_1=n_2=\cdots=n_k=0.$$

قضیه ۷-۵

شرایط زیر در مورد گروه آبلی G معادلند:

(۱) G دارای یک پایه (متناهی) است.

(۲) عدد طبیعی k چنان موجود است که

$$G\cong\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{k\text{ بار}}.$$

اثبات (۲)⇒(۱): فرض کنید $X=\{x_1,\ldots,x_k\}$ یک پایه برای G باشد. تعریف می‌کنیم:

$$\theta:G\to\overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{k\text{ بار}}$$

$$\theta(n_1x_1+\cdots+n_kx_k)=(n_1,\ldots,n_k)$$

به راحتی می‌توان مشاهده نمودکه θ یک یکریختی است.

(۱)⇒(۲): فرض کنید

$$\theta:G\to\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{k\text{ بار}},$$

یک یکریختی باشد. فرض کنید

$$u_i=(0,\ldots,0,\overset{\text{مکان } i\text{ ام}}{\overset{\uparrow}{1}},0,\ldots,0)\in\mathbb{Z}\times\cdots\times\mathbb{Z}$$

با توجه به پوشا بودن θ عناصر $x_i \in G\,(1 \le i \le k)$ چنان موجودند که $\theta(x_i) = u_i$. به آسانی می‌توان نشان داد که $X = \{x_1,\ldots,x_k\}$ یک پایه برای G است.

■■■

تعریف ۷-۵

گروه آبلی صادق در قضیه فوق را یک گروه **آبلی آزاد متناهی مولد** گوییم.

لم۷-۱

فرض کنید G یک گروه آبلی آزاد متناهی مولد و $X = \{x_1,\ldots,x_k\}$ پایه‌ای برای آن باشد. در این‌صورت:

$$|G/2G| = 2^k.$$

اثبات: از قضیهٔ قبل خواهیم داشت $G \cong \underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{k\,\text{بار}}$. بنابراین به آسانی میتوان مشاهده نمود که

$$\frac{G}{2G} \cong \frac{\mathbb{Z}\times\cdots\times\mathbb{Z}}{2(\mathbb{Z}\times\cdots\times\mathbb{Z})} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}\times\cdots\times\frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2\times\cdots\times\mathbb{Z}_2.$$

درنتیجه $|G/2G| = 2^k$.

■■■

قضیه۷-۶

فرض کنید G یک گروه آبلی آزاد متناهی مولد باشد. در این صورت تعداد عناصر هر دو پایه از G برابر است.

اثبات: با توجه به لم قبل کافی است نشان دهیم که Gدارای پایهٔ نامتناهی نیست. (برهان خلف) فرض کنید Y یک پایهٔ نامتناهی برای G باشد. چون G یک گروه آبلی آزاد متناهی

مولد است، لذا دارای یک پایه مانند $X=\{x_1,\dots,x_k\}$ می باشد. فرض کنید $r>k$. زیر مجموعهٔ $Y_1=\{y_1,\dots,y_r\}$ از عناصر متمایز Y را در نظر بگیرید. اگر H زیرگروه تولید شده بوسیله Y_1 و K زیرگروه تولید شده بوسیلهٔ عناصر $Y-Y_1$ باشد، آنگاه به‌آسانی می‌توان مشاهده نمود که

$$G/2G\cong(H\times K)/2(H\times K)\cong(H/2H)\times(K/2K),$$

لذا با توجه به لم قبل داریم $2^k=|G/2G|\geq|H/2H|=2^r$. یعنی $k\geq r$، که تناقض است.

■■■

تعریف ۷-۶

تعداد عناصر هر پایه از گروه آبلی آزاد متناهی مولد G را **رتبه** G نامیده و با $\operatorname{rank}G$ نمایش می‌دهیم.

قضیه۷-۷

هر گروه آبلی متناهی مولد تصویر همریخت یک گروه آبلی آزاد متناهی مولد است.

اثبات: فرض کنید $X=\{x_1,\dots,x_k\}$ مولدی برای گروه آبلی دلخواه G باشد. تعریف می‌کنیم:

$$\theta:\mathbb{Z}\overbrace{\times\cdots\times}^{k\text{بار}}\mathbb{Z}\to G$$
$$(n_1,\dots,n_k)\mapsto n_1x_1+\cdots+n_kx_k$$

به آسانی مشاهده می‌شود که θ یک بروریختی است. بنابراین G تصویر همریخت $\mathbb{Z}\times\cdots\times\mathbb{Z}$ می‌باشد.

■■■

اثبات لم زیر آسان و به خواننده محول می‌شود.

لم۷-۲

فرض کنید $X=\{x_1,\dots,x_k\}$ پایه‌ای برای گروه آبلی آزاد G باشد، $n\in\mathbb{Z}$ در این صورت برای هر $i\neq j$ مجموعه $Y=\{x_1,\dots,x_{j-1},x_j+nx_i,x_{j+1},\dots,x_k\}$ نیز یک پایه برای G است.

قضیه۷-۸

فرض کنید G یک گروه آبلی آزاد از رتبهٔ k باشد و H نیز گروه ناصفری از Gباشد. در این صورت پایه‌ای مانند $\{x_1,\dots,x_k\}$ از G، عدد صحیحی مانند $r\,(1\leq r\leq k)$ و اعداد صحیح مثبتی مانند $m_r,\dots,m_1$ وجود دارد به طوری که $m_{i-1}|m_i$ ، $2\leq i\leq r$ و $\{m_1x_1,\dots,m_rx_r\}$ پایه‌ای برای H است.

اثبات: اگر $k=1$، آنگاه $G=<x_1>$. چون هر زیر گروه یک گروه دوری، دوری است. بنابراین H دوری است و به‌وضوح $m_1>0$ چنان موجود است که $H=<m_1x_1>$. حال فرض کنید قضیه برای همه گروه‌های آبلی آزاد از رتبهٔ کوچکتر از k برقرار باشد. فرض کنید S زیر مجموعه‌ای از اعداد طبیعی متشکل از $m\in\mathbb{N}$ به قسمی که پایه‌ای مانند $\{y_1,\dots,y_k\}$ از G و عنصری از H به شکل $h=my_1+n_2y_2+\cdots+n_ky_k$,$n_i\in\mathbb{Z}$ موجود باشد.

چون $H\neq\{0\}$، پس $S\neq\varnothing$. فرض کنید m_1 کوچکترین عنصر S باشد، یعنی $(2\leq i\leq k)\,n_i\in\mathbb{Z}$ و پایه $\{y_1,\dots,y_k\}$ از G چنان موجود است که

$$h=m_1y_1+n_2y_2+\cdots+n_ky_k\in H.$$

با توجه به الگوریتم تقسیم $r_i\in\mathbb{Z}$ ، q_i موجودند که

$$n_i=q_im_1+r_i,\ 0\leq r_i\leq m,\ \ i=2,3,\dots,k.$$

پس $h=m_1\left(y_1+q_2y_2+\cdots+q_ky_k\right)+r_2y_2+\cdots+r_ky_k$. با توجه به مینیمال بودن m_1 و پایه بودن $\{y_1+q_2y_2+\cdots+q_ky_k,y_2,\dots,y_k\}$ برای G، خواهیم داشت $r_i=0$، $2\leq i\leq k$.

www.mathematic87.blogfa.com

در نتیجه $h = m_1 x_1 \in H$، جاییکه $x_1 = y_1 + q_2 y_2 + \cdots + q_k y_k$. قرار می‌دهیم $K =< y_2,\ldots,y_k >$. بنابراین K یک گروه آبلی آزاد از رتبه $k-1$ است.

ادعا می‌کنیم $H =< m_1 x_1 > + H \cap K$. فرض کنید $a \in H$. دراین‌صورت $1 \le i \le k,\ t_i \in \mathbb{Z}$ چنان موجودند که $a = t_1 x_1 + t_2 y_2 + \cdots + t_k y_k$. بنا به الگوریتم تقسیم $q_1, r_1 \in \mathbb{Z}$، چنان موجودند که $t_1 = q_1 m_1 + r_1$، $0 \le r_1 < m_1$. پس

$$r_1 x_1 + t_2 y_2 + \cdots + t_k y_k = a - q_1 m_1 x_1 \in H.$$

با توجه به مینیمال بودن m_1 داریم $r_1 = 0$ و در نتیجه

$$a = q_1 \left(m_1 x_1\right) + t_2 y_2 + \cdots + t_k y_k \in < m_1 x_1 > + H \cap K,$$

یعنی نشان دادیم که $H =< m_1 x_1 > + H \cap K$. اگر $H \cap K = \{0\}$، آنگاه $H =< m_1 x_1 >$ و به وضوح قضیه درست است. اگر $H \cap K \neq \{0\}$، آنگاه طبق فرض استقرا پایه $\left\{x_2,\ldots,x_k\right\}$ از K و عدد صحیحی مانند $(2 \le r \le k)r$ و اعداد صحیح مثبتی مانند $m_r,\ldots,m_2$ وجود دارد به طوری که $m_{i-1} | m_i$ ، $3 \le i \le r$ و $\left\{m_2 x_2,\ldots,m_r x_r\right\}$ پایه‌ای برای $H \cap K$ است. به‌وضوح $\left\{x_1,\ldots,x_k\right\}$ یک پایه برای G و $\left\{m_1 x_1, m_2 x_2,\ldots,m_r x_r\right\}$ یک پایه برای H است. تنها باقی می‌ماند که نشان دهیم $m_1 | m_2$. با توجه به الگوریتم تقسیم عناصر $q, r \in \mathbb{Z}$ موجودند که $m_2 = q m_1 + r$ ، $0 \le r < m_1$. مجموعه $\left\{x_2, x_1 + q x_2, x_3,\ldots,x_k\right\}$ یک پایه G است و

$$r x_2 + m_1 \left(x_1 + q x_2\right) = m_1 x_1 + m_2 x_2 + 0 m_3 x_3 + \cdots + 0 m_k x_k \in H.$$

بنابراین با توجه به مینیمال بودن m_1، خواهیم داشت $r = 0$، یعنی $m_1 | m_2$.

■■■

■ اثبات وجود تجزیه در صورت اول قضیهٔ اساسی گروه‌های آبلی متناهی مولد

فرض کنید G توسط k عنصر تولید شود. در این‌صورت اگر $F = \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{k\text{ بار}}$، آنگاه همریختی پوشای $\theta : F \to G$ را خواهیم داشت (اثبات قضیه ۷ ملاحظه شود)،

www.mathematic87.blogfa.com

لـــذا $F/\mathrm{Ker}\theta \cong G$. فـــرض کنیـــد $\{x_1,\ldots,x_k\}$ پایـــه‌ای بـــرای F باشـــد بطوریکـــه $\{m_1x_1,\ldots,m_rx_r\}$ پایـــه‌ای بـــرای $\mathrm{Ker}\theta$ کـــه در آن $(1\le r\le k)$ و $m_{i-1}|m_i$ ، $2\le i\le r$.
اکنون داریم:

$$F \cong < x_1 > \times\cdots\times < x_k >,$$
$$\mathrm{Ker}\theta \cong < m_1x_1 > \times\cdots\times < m_rx_r > .$$

بنابر این

$$G \cong F/\mathrm{Ker}\theta \cong \frac{< x_1 >}{< m_1x_1 >}\times\cdots\times\frac{< x_r >}{< m_rx_r >}\times < x_{r+1} > \times\cdots\times < x_k >$$
$$\cong \mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_r}\times\mathbb{Z}\times\cdots\times\mathbb{Z}.$$

■■■

■ **اثبات وجود تجزیه در صورت دوم قضیهٔ اساسی گروه‌های آبلی متناهی مولد**

اثبات وجود تجزیه، در صورت دوم قضیهٔ اساسی گروه‌های آبلی متنـاهی مولـد بـه وضـوح از مطلب فوق و نتیجه ۵-۳ بدست می‌آید.

■■■

■ **اثبات یکتایی صورت دوم قضیهٔ اساسی گروه‌های آبلی متناهی مولد**

قبل از ارائهٔ اثبات لم و تعریف زیر را بیان می‌کنیم.

لم۷-۳

فرض کنید G گروهی آبلی، m عددی صحیح و p عددی اول باشد. در این صورت هر یک از مجموعه‌های زیر، زیرگروهی از G است:

(۱) $mG = \{mg|g\in G\}$،

(۲) $G[m] = \{g\in G|mg=0\}$،

www.mathematic87.blogfa.com

(۳) $G(p)=\left\{g\in G\;\middle|\;\circ(g)=p^n, n\geq 0\right\}$ به ازای یک،

(۴) $T(G)=\left\{g\in G\;\middle|\;\circ(g)<\infty\right\}$.

یکریختی‌های زیر موجودند.

(۵) $p^m\mathbb{Z}_{p^n}\cong\mathbb{Z}_{p^{n-m}}\ (m<n)$،

(۶) $\mathbb{Z}_{p^n}[p]\cong\mathbb{Z}_p\ (n\geq 1)$،

(۷) فرض کنید G و $G_i\ (i=1,2,\ldots,n)$ گروه‌های آبلی باشند. اگر $G\cong\prod_{i=1}^{n}G_i$، آنگاه

$mG\cong\prod_{i=1}^{n}mG_i$ و $G[m]\cong\prod_{i=1}^{n}G_i[m]$.

(۸) فرض کنید G و H دو گروه آبلی باشند. اگر $G\cong H$، آنگاه $T(G)\cong T(H)$ و $G(p)\cong H(p)$.

اثبات: به عنوان تمرین به عهده خواننده واگذار می‌شود.

■■■

تعریف ۷-۷

هر گاه G گروهی آبلی باشد، آنگاه زیر گروه $T(G)$ تعریف شده در لم قبل، **زیر گروه تابی** G نام دارد. هر گاه $T(G)=G$ آنگاه گوییم G یک **گروه تابی** است. هر گاه $T(G)=\{0\}$، آنگاه گوییم G **فارغ از تاب** است.

فرض کنید G دو تجزیه داشته باشد، مثلاً

$$\mathbb{Z}_{p_1^{n_1}}\times\cdots\times\mathbb{Z}_{p_\ell^{n_\ell}}\times\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{t\text{ بار}}\cong G\cong\mathbb{Z}_{q_1^{m_1}}\times\cdots\times\mathbb{Z}_{q_k^{m_k}}\times\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{s\text{ بار}}.$$

با توجه به دو تجزیهٔ فوق خواهیم داشت:

$$\mathbb{Z}_{p_1^{n_1}}\times\cdots\times\mathbb{Z}_{p_\ell^{n_\ell}}\cong T(G)\cong\mathbb{Z}_{q_1^{m_1}}\times\cdots\times\mathbb{Z}_{q_k^{m_k}},$$

و لذا

$$\frac{G}{T(G)} \cong \underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{t\text{ بار}} \text{ ، } \frac{G}{T(G)} \cong \underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{s\text{ بار}}.$$

بنابراین $t = s$. از این‌رو کافی است فرض شود $G = T(G)$، یعنی

$$\mathbb{Z}_{p_1^{n_1}} \times\cdots\times \mathbb{Z}_{p_\ell^{n_\ell}} \cong G \cong \mathbb{Z}_{q_1^{m_1}} \times\cdots\times \mathbb{Z}_{q_k^{m_k}}.$$

حال باید نشان داد $\ell = k$ و (پس از ترتیب مجدد)، به ازای هر i، $p_i^{n_i} = q_i^{m_i}$.

فرض کنید p عددی اول باشد. به وضوح $(\prod p_i^{n_i})(p)$ یکریخت با مجموع مستقیم آن $\mathbb{Z}_{p_i^{n_i}}$ هایی است که $p_i = p$ باشد و به همین نحو در مورد تجزیه سمت راست G. چون طبق لم قبل $(\prod p_i^{n_i})(p) \cong (\prod q_i^{m_i})(p)$، لذا کافی است که p_i, q_i ها را عدد اول ثابت p در نظر گرفت. از این‌رو داریم.

$$\prod_{i=1}^{\ell} \mathbb{Z}_{p^{a_i}} \cong G \cong \prod_{j=1}^{k} \mathbb{Z}_{p^{b_j}},$$

که در این جا $1 \le a_1 \le a_2 \le \ldots \le a_\ell$ و $1 \le b_1 \le b_2 \le \ldots \le b_k$. ابتدا نشان می‌دهیم که $\ell = k$. لم قبل و تجزیه سمت چپ G نشان می‌دهند که

$$G[p] \cong \prod_{i=1}^{\ell} \mathbb{Z}_{p^{a_i}}[p] \cong \underbrace{\mathbb{Z}_p \times\cdots\times \mathbb{Z}_p}_{\ell\text{ بار}},$$

که از آن جا $|G[p]| = p^\ell$. استدلالی مشابه با تجزیه سمت راست G نشان می‌دهد که $|G[p]| = p^k$. بنابراین، $p^\ell = p^k$ و در نتیجه $\ell = k$. فرض کنید $u\,(1 \le u \le l)$ اولین عدد صحیحی باشد که به ازای هر $i < u$ ، $a_i = b_i$ و $a_u \ne b_u$. می‌توان فرض کرد $a_u < b_u$. چون به ازای $a_i \le a_u$، $p^{a_u}\mathbb{Z}_{p^{a_i}} = 0$، تجزیه سمت چپ G و لم قبل ایجاب می‌کنند که:

$$p^{a_u}G \cong \prod_{i=1}^{\ell} p^{a_u}\mathbb{Z}_{p^{a_i}} \cong \prod_{i=u+1}^{\ell} \mathbb{Z}_{p^{a_i-a_u}}.$$

بطو مشابه از تجزیهٔ سمت راست G داریم:

$$p^{a_u}G \cong \prod_{i=u}^{\ell} \mathbb{Z}_{p^{b_i-a_u}},$$

www.mathematic87.blogfa.com

یعنی دو تجزیه با تعداد مؤلفه‌های مختلف برای $p^{a_u}G$ داریم، که تناقض است. در نتیجه برای هر i، $a_i = b_i$.

■■■

■ یکتایی صورت اول قضیهٔ اساسی گروه‌های آبلی متناهی مولد

فرض کنید

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{s\,\text{بار}} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{t\,\text{بار}},$$

که در اینجا $m_1 > 1$ و $n_1 > 1$ و $m_1 \mid m_2 \mid \ldots \mid m_r$ و $n_1 \mid n_2 \mid \ldots \mid n_\ell$. با توجه به استدلال یکتایی صورت دوم، $s = t$. حال فرض کنید

$$m_i = {p_1}^{a_{i1}} {p_2}^{a_{i2}} \cdots {p_d}^{a_{id}},$$
$$n_i = {p_1}^{b_{i1}} {p_2}^{b_{i2}} \cdots {p_d}^{b_{id}}.$$

تجزیه‌های m_i, n_i به حاصل‌ضرب توانهای اعداد اول متمایز باشد. با توجه به نتیجه ۵-۳ داریم:

$$\prod_{i,j} \mathbb{Z}_{{p^{a_{ij}}}} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \cong T(G) \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_\ell} \cong \prod_{i,j} \mathbb{Z}_{{p^{a_{ij}}}},$$

و لذا برای هر $j = 1,2,\ldots,d$، داریم:

$$\prod_{i=1}^{r} \mathbb{Z}_{{p_j}^{a_{ij}}} \cong G(p_j) \cong \prod_{i=1}^{\ell} \mathbb{Z}_{{p_j}^{b_{ij}}},$$

و لذا با استفادهٔ مجدد از یکتایی صورت دوم، $r = \ell$ و برای هر i, j، $a_{ij} = b_{ij}$. در نتیجه برای هر i، $m_i = n_i$.

■■■

www.mathematic87.blogfa.com

توضیح تاریخی

یکی از مسائل مهم توپولوژی تشخیص یکسان نبودن دو فضای توپولوژیک است. بعنوان مثال نوار مستطیل شکلی را در نظر بگیرید. با روشهای زیر دو شکل می‌سازیم:

(۱) استوانه: دو سر نوار را بهم می‌چسبانیم تا یک استوانه حاصل شود.

(۲) نوار موبیوس: ابتدا دو سر نوار را به اندازهٔ ۱۸۰ درجه چرخانده سپس دو سر نوار را بهم می‌چسبانیم.

توپولوژی دانها به هر فضای توپولوژیک یک گروه نسبت می‌دهند، که اگر دو فضای توپولوژیک یکسان باشند، آنگاه گروه‌های وابسته به آنها نیز یکسان هستند. این گروه‌ها را گروه‌های بنیادین می‌نامیم. بنابراین اگر گروه‌های بنیادین دو فضای توپولوژیک یکسان نباشند، آنگاه این دو فضای توپولوژیک یکسان نیستند.

وجود عناصر از مرتبهٔ متناهی در گروه بنیادین دلالت بر چرخش فضاست (مثل نوار موبیوس). از این‌رو اصطلاح عناصر تابدار در مورد عناصری از مرتبهٔ متناهی در یک گروه آبلی مورد استفاده قرار می‌گیرد.

تمرینها

۱. در حد یکریختی، مطلوب است تعیین تمام گروه‌های آبلی از مرتبهٔ کوچکتر از 30.

۲. (a) فرض کنید p عددی اول باشد. نشان دهیدکه گروه $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (با n مولفه) دارای $(p^n-1)/(p-1)$ زیر گروه از مرتبهٔ p است،

(b) تعداد زیرگروه‌های مرتبهٔ p^2 در گروه آبلی $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3}$ چیست؟

۳. نشان دهید $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ دارای p^2-1 عنصر از مرتبهٔ p است.

۴. فرض کنید $G = \{(x,y) \mid x,y \in \mathbb{Z},\ x \overset{10}{\equiv} y\}$.

(a) نشان دهید G یک گروه بدون تاب از $\mathbb{Z} \times \mathbb{Z}$ است،

www.mathematic87.blogfa.com

(b) نشان دهید G متناهی مولد است.

۵. فرض کنید G یک گروه آبلی متناهی باشد. اگر مرتبهٔ هر عنصر G عدد اول p باشد، آنگاه $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

۶. فرض کنید H, G و K گروه های آبلی متناهی مولد باشند.

(a) اگر $G \times G \cong H \times H$، آنگاه $G \cong H$،

(b) اگر $G \times H \cong G \times K$، آنگاه $H \cong K$،

(c) فرض کنید $\mathbb{Z}[x]$ گروه جمعی تمام چندجمله‌ها از x با ضرایب صحیح باشد. نشان دهید $\mathbb{Z}[x] \times \mathbb{Z} \cong \mathbb{Z}[x] \times \mathbb{Z} \times \mathbb{Z}$ اما $\mathbb{Z} \ncong \mathbb{Z} \times \mathbb{Z}$.

۷. ثابت کنید که گروه آبلی متناهی G دوری است اگر و تنها اگر به ازای هرعدد اولی چون p، گروه G زیرگروهی یکریخت با $\mathbb{Z}_p \times \mathbb{Z}_p$ نداشته باشد.

۸. (a) فرض کنید G گروهی آبلی و $|G| = p^n$،که p عددی اول است. اگر به ازای هر مقسوم‌علیه d از $|G|$ گروه G حداکثر دارای یک زیرگروه از مرتبهٔ d، آنگاه G دوری است،

(b) فرض کنید G گروهی آبلی و متناهی باشد بطوریکه به ازای هر عدد طبیعی n معادلهٔ $nx = 0$ حداکثر n ریشه در G داشته باشد. در این‌صورت G دوری است.

۹. (a) فرض کنید G یک گروه آبلی متناهی از مرتبهٔ n باشد. نشان دهید به ازای هر $d \mid n$، زیرگروهی از G با مرتبهٔ d وجود دارد. همچنین نشان دهید G یک گروه خارج قسمتی از مرتبهٔ d دارد.

(b) فرض کنید G یک گروه آبلی متناهی باشد. اگر برای هر عدد طبیعی n، معادلهٔ $x^n = e$ (با نماد جمعی، $nx = 0$) حداکثر n ریشه در G داشته باشد، آنگاه G دوری است.

۱۰. گزاره‌های زیر را ثابت یا رد کنید.

(a) اگر G گروهی آبلی آزاد با رتبهٔ n باشد، آنگاه هر زیر مجموعهٔ مستقل خطی با n عنصر یک پایه برای G است،

(b) اگر G گروهی آبلی آزاد متناهی مولد باشد، آنگاه هر مجموعهٔ مولد G شامل پایه‌ای از G است،

www.mathematic87.blogfa.com

(c) فرض کنید G یک گروه آبلی متناهی مولد باشد که در آن هیچ عنصری (جز 0) مرتبهٔ متناهی ندارد. دراین‌صورت G یک گروه آبلی آزاد متناهی مولد است،

(d) اگر G گروهی متناهی مولد باشد، آنگاه هر زیرگروه G نیز متناهی مولد است.

۱۱. فرض کنید H,G دو گروه آبلی متناهی باشند. اگر به ازای هر عدد طبیعی n، تعداد عناصر از مرتبهٔ n این دو گروه برابر باشند، آنگاه $G \cong H$.

۱۲. فرض کنید G یک گروه آبلی متناهی و p عددی اول باشد. نشان دهید که تعداد زیرگروه‌های از مرتبهٔ p با زیرگروه‌های از اندیس p برابر است.

۱۳. (a) نشان دهید $(\mathbb{Q},+)$ متناهی مولد نیست،

(b) نشان دهید هر زیرگروه متناهی از $\mathbb{Q}/\mathbb{Z}$ دوری است.

۱۴. فرض کنید H زیرگروهی از گروه آبلی متناهی G باشد. نشان دهید G دارای زیرگروهی یکریخت با G/H است.

۱۵. یک p-گروه آبلی متناهی با عناصر مرتبهٔ ماکزیمال خود تولید می‌شود.

۱۶. فرض کنید G گروهی آبلی متناهی مولد باشد. نشان دهید تعداد زیرگروه‌های دو به دو غیر یکریخت G متناهی است.

۱۷. فرض کنید G یک گروه متناهی مولد باشد. در این‌صورت کوچکترین عدد طبیعی مانند n را که G با n عنصر خود تولید می‌شود را با $\mu(G)$ نمایش می‌دهیم.

(a) فرض کنید $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{s \text{ بار}}$. نشان دهید $\mu(G) = r + s$،

(b) فرض کنید H,G دو گروه آبلی متناهی‌مولد و H فارغ از تاب باشد. نشان دهید $\mu(G \times H) = \mu(G) + \mu(H)$.

۱۸. فرض کنید $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (با n مولفه). نشان دهید $\mathrm{Aut(G)} \cong \mathrm{GL}_n(\mathbb{Z}_p)$.

۱۹. فرض کنید G یک p-گروه آبلی متناهی باشد. اگر $p^2 \mid\mid |G|$ نشان دهید $p \mid\mid \mathrm{Aut}(G)|$.

۲۰. فرض کنید $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (با n مولفه). نشان دهید $2^n - 1 \mid\mid \mathrm{Aut}(G)|$.

www.mathematic87.blogfa.com

مسائل مبارزه طلب

۱. فرض کنید G گروهی آبلی متناهی مولد و $f : G \to G$ یک بروریختی باشد، ثابت کنید f یکریختی است.

۲. اگر G یک گروه آبلی و هر خانواده از زیرگروه‌های G دارای عنصر مینیمال باشد، آنگاه هر تکریختی $\varphi : G \to G$ یک یکریختی است.

۳. اگر G یک گروه آبلی متناهی غیر دوری باشد، آنگاه $\mathrm{Aut}(G)$ آبلی نیست.

۴. فرض کنید G یک گروه متناهی و $|G| \geq 3$. نشان دهید مرتبهٔ $\mathrm{Aut}(G)$ نمی‌تواند عددی فرد باشد.

۵. فرض کنید G یک p-گروه غیر دوری متناهی باشد. ثابت کنید G یک زیر گروه نرمال مانند N دارد بطوریکه $G/N \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

۶. گروهی آبلی مانند G مثال بزنید که $G \cong G \times G \times G$ اما $G \ncong G \times G$.

منابعی برای مطالعهٔ بیشتر

1. Hungerford, T. W. *Algebra*. Springer-Verlag, New York, 1974.
2. Jacobson, N. *Basic Algebra I, II*. W. H. Freeman, San Francisco, 1974, 1980.
3. Lang, S. *Algebra*. Addison-Wesley, 1993.
4. Malik, D. S., Mordeson John M., Sen, M. K. *Fundamentals of Abstract Algebra*. McGraw-Hill Companies, Inc., 1996.

www.mathematic87.blogfa.com

فصل۸

عمل گروه‌ها و قضایای سیلو

در این فصل می‌خوانید:

۸-۱ عمل گروه‌ها

۸-۲ معادله رده‌ای

۸-۳ قضایای سیلو

۸-۴ کاربردهایی از قضایای سیلو

۸-۵ شمارش مدارها

مقدمه

در این فصل به معرفی عمل یک گروه روی یک مجموعه خواهیم پرداخت. سپس بعنوان نتیجه به اثبات قضایای سیلو که در رده بندی گروه‌ها از اهمیت زیادی برخوردارند می‌پردازیم. در نهایت بعنوان یک نتیجهٔ کاربردی به اثبات قضیهٔ برنساید که کاربرد زیادی در مسائل ترکیبیاتی دارد خواهیم پرداخت.

www.mathematic87.blogfa.com

۸-۱ عمل گروهها

عمل گروه‌ها تعمیمی از ضرب گروه است. اگر G یک گروه و X یک مجموعه دلخواه غیر تهی باشد منظور از **عمل** (چپ) G بر X، نگاشت $G \times X \to X$ داده شده توسط $(g,x) \mapsto gx$ می‌باشد به‌طوریکه

(۱) $ex = x$ برای هر $x \in X$،

(۲) $(g_1 g_2)x = g_1(g_2 x)$ برای هر $x \in X$ و هر $g_1, g_2 \in G$.

مثال۱: فرض کنید $G = \mathrm{GL}_2(\mathbb{R})$ و $X = \mathbb{R}^2$. در این صورت G با عمل ضرب از چپ بر X عمل می‌کند. اگر $x \in \mathbb{R}^2$ و I ماتریس همانی باشد، در این صورت $Ix = x$. اگر A و B دو ماتریس معکوس پذیر 2×2 باشند، در این صورت با توجه به خاصیت شرکت‌پذیری ضرب ماتریسها خواهیم داشت $(AB)x = A(Bx)$.

■

مثال۲: فرض کنید X یک مجموعه دلخواه غیر تهی باشد. در این صورت S_X روی X به‌صورت زیر عمل می‌کند.

$$S_X \times X \to X$$
$$(\sigma, x) \mapsto \sigma(x).$$

شرط (۱) از تعریف جایگشت همانی و شرط (۲) نتیجهٔ تعریف ضرب جایگشتی به عنوان ترکیب توابع است.

■

مثال۳: اگر G یک گروه آنگاه G روی خودش مطابق قانون زیر (ضرب از چپ) عمل می‌کند.

$$G \times G \to G$$
$$(g, x) \mapsto gx.$$

■

www.mathematic87.blogfa.com

مثال۴: فرض کنید H زیر گروهی از گروه G باشد. در این صورت H با **عمل تزویج** روی X عمل می‌کند:

$$H \times G \to G$$
$$(h, g) \mapsto hgh^{-1}.$$

■

مثال۵: فرض کنید H زیر گروهی از G و $\mathscr{L}_H$ مجموعه هم‌دسته‌های چپ H در G باشد در این صورت G با **عمل انتقال چپ** روی $\mathscr{L}_H$ عمل می‌کند:

$$G \times \mathscr{L}_H \to \mathscr{L}_H$$
$$(g, xH) \mapsto gxH.$$

■

قضیه۸-۱

فرض کنید G بر مجموعه X عمل کند. برای هر $x, y \in X$ قرار می‌دهیم $x \sim y$ اگر و فقط اگر عنصری چون $g \in G$ موجود باشد به طوریکه $gx = y$. نشان دهید $\sim$ یک رابطه هم ارزی بر X است.

اثبات: برای هر $x \in X$ داریم $ex = x$، از این رو $x \sim x$. پس $\sim$ انعکاسی است. فرض کنید $x \sim y$ لذا به ازای عنصری چون $g \in G$، $gx = y$، پس

$$g^{-1}y = g^{-1}(gx) = \left(g^{-1}g\right)x = ex = x.$$

از این‌رو $y \sim x$، لذا $\sim$ متقارن است. سر انجام اگر $y \sim z, x \sim y$ ، آنگاه به ازای g و h - ای از G و $gx = y$ و $hy = z$ پس $(hg)x = h(gx) = hy = z$ از این رو $x \sim z$ و $\sim$ متعدی است.

■■■

نمادگذاری: فرض کنید G بر X عمل کند و $g \in G$ و $x \in X$ قرار می‌دهیم:

$$X_g = \{x \in X \,|\, gx = x\},$$
$$G_x = \{g \in G \,|\, gx = x\}.$$

قضیه۸-۲

فرض کنید G بر X عمل کند و $x \in X$. در این صورت G_x یک زیر گروه G است.

اثبات: فرض کنید $x \in X$ و $h \in G_x$ و g. بنابراین $gx = hx = x$ و در نتیجه $(gh)x = g(hx) = gx = x$. از این رو $gh \in G_x$ و G_x تحت عمل دوتایی G بسته است. $ex = x$ و از این رو $e \in G_x$. اگر $g \in G_x$، آنگاه $gx = x$ پس $x = xe = x(g^{-1}g) = (xg)g^{-1} = xg^{-1}$ و در نتیجه $g^{-1} \in G_x$. بنابراین G_x زیر گروهی از G است.

■■■

تعریف ۸-۱

X_g را مجموعه نقاط ثابت g از X و G_x را گروه **ثابت ساز** یا گروه **ایزوتروپی** از x گوییم.

تعریف ۸-۲

فرض کنید G بر X عمل کند. هر قطعه در افراز با نسبت هم ارزی بیان شده یک **مدار** در X تحت G می‌نامیم. اگر $x \in X$ قطعه شامل x را مدار x می‌نامیم و با $\overline{x}$ نمایش می‌دهیم.

❖ **تذکر:** به آسانی ملاحظه می‌شود که $\overline{x} = Gx = \{gx \mid g \in G\}$.

قضیه۸-۳

فرض کنید G بر X عمل کند و $x \in X$. در این‌صورت $|\overline{x}| = [G : G_x]$.

اثبات: فرض کنید $h \in G$ و g. خواهیم داشت:

$$gx = hx \Leftrightarrow g^{-1}hx = x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow hG_x = gG_x.$$

بنابراین نگاشت $gG_x \mapsto gx$ یک نگاشت دوسویی است بنابراین $|\overline{x}| = [G : G_x]$.

■■■

۸-۲ معادله رده‌ای

فرض کنید G بر X عمل کند. قرار می‌دهیم

$$X_0 = \{x \in X \,|\, gx = x \ , g \in G \quad \text{برای هر} \ \}.$$

ملاحظه می‌شود که برای هر $x \in X$، مجموعه $\overline{x}$ تک عنصری است اگر و فقط اگر $x \in X_0$.
بنابراین X را می‌توان به صورت مجموعه‌های مجزا به شکل زیر افزار کرد:

$$X = X_0 \cup \overline{x}_1 \cup \overline{x}_2 \cup \ldots \cup \overline{x}_n,$$

که در آن $|\overline{x}_i| > 1$. بنابراین

$$|X| = |X_0| + \sum_{i=1}^{n} [G : G_{x_i}] \qquad (*)$$

معادله $(*)$را **معادلهٔ رده‌ای** گوییم.

www.mathematic87.blogfa.com

قضیه۸-۴

برای هر گروه متناهی G داریم

$$|G| = |C(G)| + \sum_{i=1}^{n} [G : C(x_i)],$$

که در آن $x_i \in G - C(G)$.

اثبات: فرض کنید G با عمل تزویج روی خودش عمل کند، یعنی $(g,x) \mapsto gxg^{-1}$. در این صورت

$$C(G) = X_0 = \{x \in G \,|\, gx = xg, \forall g \in G\}$$

$$G_x = \{g \in G \,|\, gxg^{-1} = x\} = C(x)$$

و بنابراین قضیه با توجه به معادلهٔ ردهای اثبات می‌گردد.

■■■

قضیه۸-۵

فرض کنید G یک گروه از مرتبه p^n باشد(p عددی اول است). در این صورت مرکز G غیر بدیهی است.

اثبات: با توجه به قضیه قبل خواهیم داشت:

$$p^n = |G| = |C(G)| + \sum_{i=1}^{n} [G : G_{x_i}],$$

که در آن $p \mid [G : G_{x_i}]$. بنابراین $p \mid |C(G)|$، یعنی $|C(G)| \geq p$.

■■■

۸-۳ قضایای سیلو

قضیه اساسی گروه‌های آبلی متناهی اطلاعات کاملی در مورد گروه‌های آبلی متناهی به ما می‌دهد. مطالعه گروه‌های ناآبلی متناهی به مراتب پیچیده‌تر است. قضایای سیلو اطلاعات مهمی درباره آنها به ما می‌دهند. طبق قضیه لاگرانژ می‌دانیم که مرتبه هر زیر گروه از یک گروه متناهی مرتبه آن گروه را عاد می‌کند. اینک این سوال را مطرح می‌کنیم که آیا عکس این قضیه درست است. یعنی اگر G یک گروه متناهی و $d\|G|$ آیا G دارای زیر گروهی از مرتبه d است. در حالتهای خاص این مطلب درست است. مثلا" اگر G گروهی دوری باشد به ازای هر مقسوم علیه d از $|G|$، زیر گروهی از G با مرتبه d وجود دارد. اما در حالت کلی عکس قضیه لاگرانژ صحت ندارد، چرا که A_4 زیر گروهی از مرتبه 6 ندارد. با وجود این که عکس قضیه لاگرانژ در حالت کلی درست نیست. اما با محدودیتهایی روی مقسوم علیه‌های $|G|$ صحت پیدا می‌کند. قضایای سیلو تایید می‌کنند که برای هر عدد اول p و عدد طبیعی n، اگر $p^n\|G|$ آنگاه G زیر گروهی از مرتبه p^n دارد.
به عنوان اولین قدم ، قضیه‌کشی را ثابت می‌کنیم.

قضیه۸-۶ (قضیه‌کشی)

فرض کنید G یک گروه متناهی و p عدد اولی باشد که $|G|$ را عادی کند. در این‌صورت G دارای عنصری از مرتبهٔ p است.

اثبات: فرض کنید

$$X=\{(a_1,\ldots,a_p)\big|a_i\in G, a_1a_2\ldots a_p=e\}.$$

چون a_p به طور یکتا به صورت $\left(a_1a_2\ldots a_p\right)^{-1}$ معین می‌شود، خواهیم داشت که $|X|=n^{p-1}$ که در آن $n=|G|$. فرض کنید گروه $H=(\mathbb{Z}_p,+)$ روی X به صورت زیر عمل کند

$$H \times X \to X$$
$$\big(k,(a_1,a_2,\dots,a_p)\big) \mapsto (a_{h+1},a_{h+2},\dots,a_p,a_1,\dots,a_h)$$

با توجه به اینکه در یک گروه اگر $ab=e$ آنگاه $ba=(a^{-1}a)(ba)=a^{-1}(ab)a=e$ به آسانی ملاحظه می‌شود که

$$(a_{h+1},a_{h+2},\dots,a_p,a_1,\dots,a_h)\in X.$$

از طرفی برای هر $h,h'\in H$ و $x\in X$ داریم:

$$0x=x\ ,\quad (h+h')x=h(h'x),$$

یعنی H روی X عمل می‌کند. داریم

$$X_0=\{(a_1,\dots,a_p)\mid h(a_1,\dots,a_p)=(a_1,\dots,a_p),\ \forall h\in H\}$$
$$=\{(a,\dots,a)\mid a^p=e\}.$$

بنابراین $(e,e,\dots,e)\in X_0$ و لذا $|X_0|\neq 0$. با توجه به معادلهٔ رده‌ای داریم $|X|=|X_0|+\sum_{i=1}^{n}[H:H_{x_i}]$، که در آن $[H:H_{x_i}]>1$. از طرفی چون $p\mid [H:H_{x_i}]$، لذا $[H:H_{x_i}]=p$ و درنتیجه $|X|=|X_0|+pn$. از این‌رو $p\mid\mid X_0$ و با توجه به ناصفر بودن $|X_0|$ خواهیم داشت $|X_0|\geq p$. در نتیجه $a\neq e$ در G چنان موجود است که $(a,a,\dots,a)\in X_0$ و لذا $a^p=e$ و چون p عددی اول است پس $\circ(a)=p$.

■■■

تذکر: خواننده می‌تواند قضیه‌کشی را بدون استفاده از عمل گروه‌ها و با استفاده از استقرای ریاضی و به کارگیری معادله رده‌ای اثبات نماید.

یادآوری: فرض کنید p عددی اول باشد. گروه G را یک $p-$گروه گوییم اگر مرتبهٔ تمام عناصر آن توانی از p باشد (تعریف۷-۳ ملاحظه شود).

www.mathematic87.blogfa.com

گزاره ۸-۱

گروه متناهی G یک $p-$گروه است اگر و فقط اگر $|G|$ توانی از عدد اول p باشد.

اثبات: فرض کنید G یک $p-$گروه باشد و q عددی اول باشد که $q\|G|$. در این صورت طبق قضیه‌کشی G دارای عنصری از مرتبه q می‌شود و با توجه به فرض عدد طبیعی n چنان موجود است که $q = p^n$ و لذا $p = q$. به عکس اگر $|G| = p^n$ آنگاه بنابر قضیه لاگرانژ مرتبه هر عنصر G توانی از عدد اول p خواهد بود.

■■■

تعریف ۸-۳

فرض کنید H زیر گروهی از گروه G باشد. اگر H یک $p-$گروه باشد، آنگاه H را یک $p-$ **زیر گروه** G گوییم.

لم ۸-۱

فرض کنید H یک $p-$گروه متناهی G باشد. اگر H روی X عمل کند، آنگاه

$$|X_0| \overset{p}{\equiv} |X|.$$

اثبات: در معادلهٔ رده‌ای، $|X| = |X_0| + \sum_{i=1}^{n} \left[H : H_{x_i}\right]$، داریم $p \mid [G : G_{x_i}]$ و لذا $|X_0| \overset{p}{\equiv} |X|$.

■■■

نتیجه ۸-۱

فرض کنید H یک $p-$زیر گروه از گروه متناهی G باشد. در این صورت

$$\left[N_G(H) : H\right] \overset{p}{\equiv} [G : H].$$

اثبات: فرض کنید X مجموعه همه هم‌دسته‌های چپ H در G باشد. H با انتقال چپ روی X عمل می‌کند و داریم

$$X_0 = \{xH \mid hxH = xH \ , \forall h \in H\} = \{xH \mid x^{-1}hxH = H, \forall h \in H\}$$
$$= \{xH \mid x^{-1}Hx = H\} = \{xH \mid xHx^{-1} = H\}$$
$$= \{xH \mid x \in N_G(H)\}.$$

بنابراین $|X_0|$ برابر با تعداد هم‌دسته‌های H در $N_G(H)$ است، یعنی $[N_G(H) : H]$ و $|X_0| =$ لذا

$$[N_G(H) : H] = |X_0| \overset{p}{\equiv} |X| = [G : H].$$

■■■

نتیجه۸-۲

فرض کنید H یک $p-$زیر گروه از گروه متناهی G باشد و $p \nmid [G : H]$، در این صورت $N_G(H) \neq H$.

اثبات: با توجه به اینکه

$$0 \overset{p}{\equiv} [G : H] \overset{p}{\equiv} [N_G(H) : H],$$

داریم $p \nmid [N_G(H) : H]$. از طرفی چون $[N_G(H) : H] \geq 1$، لذا $N_G(H) \neq H$.

■■■

قضیه ۸-۷ (قضیه اول سیلو)

فرض کنید G یک گروه با مرتبه $p^n m$ باشد که در آن $n \geq 1$، p عددی اول و $(p, m) = 1$. در این صورت به ازای هر i، $1 \leq i \leq n$، G شامل زیر گروهی از مرتبه p^i است. بـه عـلاوه هر زیر گروه از G با مرتبه p^i $(1 \leq i < n)$ در یک زیر گروه با مرتبه p^{i+1} نرمال است.

اثبات: مطلب را با استقرا روی i ثابت می‌کنیم. چون $p\|G|$، طبق قضیه کشی، G شامل عنصری از مرتبه p و لذا شامل زیر گروهی از مرتبه p است. پس قضیه برای $i=1$ برقرار است حال فرض کنید G شامل زیر گروه H با مرتبه $p^i\,(1\le i<n)$ باشد. در این صورت $p\|[G:H]$ و با توجه نتیجه۱ و ۲ داریم:

$$\big[N_G(H):H\big]\overset{p}{\equiv}[G:H]\overset{p}{\equiv}0,$$
$$\big[N_G(H):H\big]>1,$$

و

$$1<\big|N_G(H)/H\big|=\big[N_G(H):H\big]\overset{p}{\equiv}[G:H]\overset{p}{\equiv}0.$$

بنابراین $p\big\|N_G(H)/H\big|$ و دوباره بنابر قضیه کشی $N_G(H)/H$ شامل زیر گروهی از مرتبه p است. فرض کنید این زیر گروه به شکل H_1/H باشد که در آن $H\le H_1\le N_G(H)$. حال چون $H\trianglelefteq N_G(H)$، لذا $H\trianglelefteq H_1$. بالاخره $\big|H_1\big|=|H|\big|H_1/H\big|=p^ip=p^{i+1}$.

■■■

تعریف ۸-۴

زیر گروه P از گروه G را $p-$**زیر گروه سیلو** از G گوییم اگر P یک $p-$زیر گروه ماکزیمال از G باشد (یعنی، اگر $P\le H\le G$، که H یک $p-$زیر گروه از G باشد، آنگاه $H=P$ یا $H=G$)

تذکر: قضیه اول سیلو نشان می‌دهد که اگر $|G|=p^nm$ و $(p,m)=1$، آنگاه $p-$زیر گروه‌های سیلوی G دقیقا" همان زیرگروه‌های از مرتبه p^n هستند.

مثال۶: گروه متناوب A_4 را در نظر بگیرید. چون $\big|A_4\big|=2^2.3$، لذا $2-$ زیر گروه سیلوهای A_4 از مرتبه 4 و $3-$ زیر گروه سیلوهای A_4 از مرتبه 3 می‌باشند. بنابراین

www.mathematic87.blogfa.com

$P=\{\mathrm{id},(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$ یک $2-$ زیر گروه سیلو از A_4 و $Q_1=\{\mathrm{id},(1\ 2\ 3),(1\ 3\ 2)\}$، $Q_2=\{\mathrm{id},(1\ 2\ 4),(1\ 4\ 2)\}$ دو $3-$ زیر گروه سیلو A_4 می‌باشند.

■

مثال۷: فرض کنید p عددی اول باشد. قرار می‌دهیم:

$$G=\left\{\begin{bmatrix}a & b\\ 0 & a^{-1}\end{bmatrix}\mid a,b\in\mathbb{Z}_p, a\neq 0\right\}.$$

به آسانی مشاهده می‌شود که $|G|=p(p-1)$. فرض کنید:

$$P=\left\{\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix}\mid b\in\mathbb{Z}_p\right\}.$$

در این‌صورت $|P|=p$. از طرفی چون $(p,p-1)=1$، لذا P یک $p-$زیر گروه سیلو از Gاست.

■

اگر P یک $p-$ زیر گروه سیلو باشد، هر مزدوج xPx^{-1} از P هم یک $p-$ زیر گروه سیلو است. قضیه دوم سیلو حاکی این است که هر $p-$زیر گروه سیلو را می‌توان از P بدست آورد، یعنی هر دو $p-$زیر گروه سیلو مزدوج هستند.

قضیه۸- ۸ (قضیه دوم سیلو)

اگر H یک $p-$زیرگروه از گروه متناهی G و P هر $p-$زیر گروه سیلو از G باشد آنگاه عنصر $x\in G$ چنان موجود است که $H\leq xPx^{-1}$. بویژه هر دو $p-$زیر گروه سیلوی G مزدوجند.

اثبات: فرض کنید $X=\{xP\mid x\in G\}$. در این صورت H روی X با انتقال چپ عمل می‌کند و بنابر لم ۱،

www.mathematic87.blogfa.com

$$\left|X_0\right| \overset{p}{\equiv} |X| = [G : P].$$

اما $p \nmid [G : P]$ ، بنابراین $|X_0| \neq 0$ و لذا عنصری مانند $xP \in X_0$ موجود است. اما

$$xP \in X_0 \Leftrightarrow hxP = xP \ ,\forall h \in H \Leftrightarrow x^{-1}hxP = P \ ,\forall h \in H$$

$$\Leftrightarrow x^{-1}Hx \leq P \Leftrightarrow H \leq xPx^{-1}$$

اگر H نیز یک $p-$ زیر گروه سیلو باشد، آنگاه $|H| = |P| = \left|xPx^{-1}\right|$ و لذا $H = xPx^{-1}$.

■■■

قضیه سوم سیلو اطلاعاتی در مورد تعداد $p-$زیرگروه‌های سیلو به ما می‌دهد. این قضیه در رده‌بندی گروه‌های متناهی از اهمیت زیادی برخوردار است.

نمادگذاری: فرض کنید G یک گروه متناهی و p عددی اول باشد. تعداد $p-$زیرگروه سیلوهای G را با n_p نمایش می‌دهیم.

قضیه۸-۹ (قضیه سوم سیلو)

فرض کنید G یک گروه متناهی باشد. دراین صورت $n_p \overset{p}{\equiv} 1$ و $n_p \| |G|$.

اثبات: طبق قضیه دوم سیلو تعداد $p-$زیرگروه‌های سیلو G عبارت است از تعداد مزدوج‌های یکی از آنها مثلا P اما این عدد برابر $\left[G : N_G(P)\right]$ است، که الزاما $|G|$ را عاد می‌کند. حال فرض کنید X مجموعه همه $p-$زیرگروه‌های سیلو G باشد. در این صورت P با عمل تزویج روی X عمل می‌کند. داریم:

$$Q \in X_0 \Leftrightarrow xQx^{-1} = Q \ (\forall x \in P) \Leftrightarrow P \leq N_G(Q)$$

اما P و Q هر دو $p-$زیرگروه‌های سیلوی G اند و لذا $p-$زیر گروه‌های سیلوی $N_G(Q)$ می‌باشند و بنابرقضیه دوم سیلو در $N_G(Q)$ مزدوج اند. اما چون $Q \trianglelefteq N_G(Q)$، نتیجه می‌شود که $P = Q$، یعنی $X_0 = \{P\}$ و لذا طبق لم۱ خواهیم داشت:

$$n_p = |X| \overset{p}{\equiv} \left|X_0\right| = 1,$$

و بنابراین اثبات کامل است.

■■■

۸- ۴کاربردهایی از قضایای سیلو

در این بخش به ارائه کاربردهایی از قضایای سیلو خواهیم پرداخت. به‌عنوان مثال اگر مرتبه گروه فقط چند عامل داشته باشد قضایای سیلو برای تعیین ساختار گروه می‌توانند ثمر بخش باشند. یکی دیگر از کاربردهای قضایای سیلو پاسخ به سؤال زیر می‌باشد.

« آیا از مرتبه‌های معینی گروهی ساده موجود است ».

به کمک قضیه سوم سیلو می‌توان به آسانی یکی از قضیه‌های مهم نظریهٔ اعداد را اثبات نمود:

قضیه۸-۱۰ (قضیه ویلسون)

فرض کنید p یک گروه متناهی باشد. دراین صورت:
$(p-1)!\overset{p}{\equiv}-1.$

اثبات: به آسانی می‌توان بررسی کرد که:

« P یک $p-$زیر گروه سیلو از S_p است اگر و فقط اگر دوری بطول p مانند $\sigma \in S_p$ چنان باشد که $P =< \sigma >$ ».

ازطرفی چون $(p-1)!$دور بطول p در S_pداریم، پس

تعداد $p-$زیر گروه‌های سیلو $S_p = n_p = (p-1)!/(p-1) = (p-2)!.$

بنابراین طبق قضیه سوم سیلو $(p-2)!\overset{p}{\equiv}1$و در نتیجه $(p-1)!\overset{p}{\equiv}-1$.

■■■

قضیه۸-۱۱

به ازای هر عدد اول p، هر گروه G از مرتبه p^2 آبلی است.

اثبات: با توجه به قضیه ۵، $C(G) \neq \{e\}$. بنابراین دو حالت ممکن است: یا $|C(G)| = p$ یا $|C(G)| = p^2$. اگر $|C(G)| = p^2$، آنگاه G آبلی است و اگر $|C(G)| = p$، آنگاه $|G/C(G)| = p$ و بنابراین $G/C(G)$ یک گروه دوری است و لذا G آبلی است.

■■■

حال به شناسایی برخی از گروه‌های غیر ساده خواهیم پرداخت. یادآوری می‌کنیم که گروه G را ساده گوییم اگردارای هیچ زیر گروه نرمال غیر بدیهی نباشد.

قضیه۸-۱۲

فرض کنید p و q دو عدد اول متمایزی باشند که $p > q$ و G گروهی از مرتبهٔ pq باشد. دراین‌صورت:

(۱) G ساده نیست،

اثبات (۱): چون $n_p = 1 + kp \,|\, pq$، لذا $n_p \,|\, q$ و با توجه به اینکه $p > q$، خواهیم داشت $n_p = 1$. پس تنها یک $p-$زیر گروه سیلو خواهیم داشت(مثلا P). چون این زیر گروه $p-$سیلو یکتا است با توجه به قضیه دوم سیلو در G نرمال خواهد بود.

(۲): حال اگر $p \not\equiv 1 \pmod{q}$ آنگاه با توجه به $n_q = 1 + kq \,|\, p$ خواهیم داشت $n_q = 1$ و لذا طبق بحث قبلی G دارای یک $q-$زیرگروه سیلوی نرمال (مثلا Q) می‌باشد، لذا $G \cong P \times Q$ و در واقع $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$، یعنی G دوری است.

■■■

مثال۸: هیچ گروهی از مرتبه 15 ساده نیست. در حالت کلی هرگروه از مرتبهٔ pq، جاییکه p, q دو عدد اول (نه لزوماً متمایز) باشند، ساده نیست.

■

قضیه۸-۱۳

اگر p و q دوعدد اول متمایز باشند، آنگاه هر گروه G از مرتبه p^2q ساده نیست.

اثبات: برهان خلف، فرض کنید $n_p>1$ و $n_q>1$. با توجه به $n_p=1+kp|q$ خواهیم داشت $1+kp=q$، لذا $p<q$. از طرف دیگر $n_q=p$ یا $n_q=p^2$. اگر $n_q=p$ آنگاه $q<p$ که تناقض است. بنابراین $n_q=p^2$. چون هر دو زیرگروه متمایز از مرتبه q تنها در عنصر همانی مشترک می‌باشند، لذا G شامل $n_q(q-1)$ عنصر متمایز از مرتبه q می‌باشد. بنابراین G دارای $p^2q-p^2(q-1)=p^2$ عنصر می‌باشد که از مرتبه q نیستند. اما در این صورت، چون هر $-p$ زیر گروه سیلو عنصری از مرتبه q ندارد، لذا G باید تنها یک $-p$ زیر گروه سیلو از p^2 مرتبه داشته باشد که تناقض است.

■■■

قضیه۸-۱۴

اگر p و q و r سه عدد اول متمایز باشند، آنگاه هر گروه G از مرتبه pqr ساده نیست.

اثبات: بدون اینکه از کلیت کاسته شود فرض کنید $p>q>r$. فرض کنید (برهان خلف) $n_p>1$ و $n_q>1$ و $n_r>1$. چون $n_p|qr$ و $p>q>r$ لذا $n_p=qr$. همینطور $n_q|pr$. چون $q>r$، لذا $n_q\geq p$. بالاخره چون $n_r|pq$، لذا $n_r\geq q$. با توجه به اینکه G شامل $n_p(p-1)$ عنصر متمایز از مرتبه p و $n_q(q-1)$ عنصر متمایز ازمرتبه q و $n_r(r-1)$ عنصر متمایز از مرتبه r خواهد بود، لذا

$$\begin{aligned}|G|=pqr&\geq 1+n_p(p-1)+n_q(q-1)+n_r(r-1)\\&\geq 1+qr(p-1)+p(q-1)+q(r-1).\end{aligned}$$

از این‌رو $0\geq(p-1)(q-1)$، که تناقض است.

■■■

www.mathematic87.blogfa.com

مثال۹: هیچ گروهی از مرتبه 48 ساده نیست.

حل: واضح هست که $n_2 = 1$ یا $n_2 = 3$. اگر $n_2 = 1$، که مسئله حل است. د رغیر این‌صورت G دارای سه زیر گروه از مرتبه 16 خواهد بود. فرض کنید H و K دو تا از آنها باشند. در این‌صورت $|H \cap K| = 8$ ، چرا که اگر $|H \cap K| \leq 4$ آنگاه $|HK| \geq 64$ که غیر ممکن است. از طرفی $H \cap K$ در H و K نرمال است (بخاطر داشتن اندیس 2) و بنابراین $H \cup K \subseteq N_G(H \cap K)$ و لذا مرتبه $N_G(H \cap K)$ بزرگتر اکید از 16 و مقسوم علیه 48 می‌باشد. بنابراین $G = N_G(H \cap K)$، یعنی $H \cap K$ در G نرمال است.

■

در نهایت این بخش را با حدس مشهور برنساید که در مقاله‌ای طولانی و سخت توسط فیت و تامپسون در سال 1963 اثبات گردید به پایان می‌رسانیم.

قضیه۸-۱۵(قضیه مرتبه فرد)

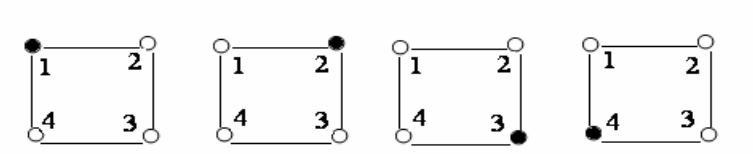
هر گروه ساده متناهی از مرتبه غیر اول بایستی از مرتبه زوج باشد.

۸-۵ شمارش مدارها

فرض کنید که بخواهیم رئوس یک مربع را با دو رنگ سفید و سیاه رنگ آمیزی کنیم. بدیهی است که جمعا $2^4 = 16$ صورت برای رنگ آمیزی رئوس وجود دارد. زیرا که هر رأس می‌تواند به هر یک ازدو رنگ باشد. اما بعضی از این رنگ آمیزی‌ها یکسان می‌باشند. مثلا مربعی که در آن رأس اول سیاه و رئوس باقیمانده سفید با مربعی که رأس دوم آن سیاه و

www.mathematic87.blogfa.com

بقیهٔ رئوس آن سفید است، دارای رنگ آمیزی یکسانی می‌باشند. شکل زیر چهار رنگ آمیزی یکسان از مربع را نشان می‌دهد.



توجه داشته باشید که با حرکت صلب مربع، رنگ آمیزی جدیدی بدست نمی‌آید. فرض کنید $G = D_4$ گروه حرکت مربع و X مجموعه 2^4 رنگ آمیزی مختلف مربع باشد فرض کنید G بطور طبیعی روی X عمل کند. در این‌صورت دو رنگ آمیزی یکسانند اگر و فقط اگر در یک مدار قرار داشته باشند. به‌عبارت دیگر هر مدار X تحت G متناظر با یک رنگ آمیزی است و مدارهای متفاوت رنگ آمیزی‌های متفاوت را نشان می‌دهند. قضیه زیر (قضیه برنساید) ابزاری برای تعیین مدارهای عمل یک گروه بر یک مجموعه می‌باشد که دارای کاربردهایی در ترکیبیات است.

قضیه۸-۱۶ (قضیه برنساید)

فرض کنید گروه متناهی G بر مجموعه X عمل کند. اگر t تعداد مدارهای متمایز عمل باشد آنگاه:

$$t = \frac{1}{|G|}\sum_{g\in G}|X_g|$$

اثبات: فرض کنید $N = \{(g,x)|g \in G, x \in X, gx = x\}$. برای هر $g \in G$، $|X_g|$ زوج با مولفه اول g وجود دارد. بنابراین

$$|N| = \sum_{g\in G}|X_g|.$$

از طرف دیگر برای هر $x \in X$، $|G_x|$ زوج با مولفه دوم x وجود دارد، پس

$$|N| = \sum_{x \in X} |G_x|.$$

بنابراین

$$|N| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\overline{x}|} = |G| \sum_{x \in X} \frac{1}{|\overline{x}|}.$$

اما $\frac{1}{|\overline{x}|}$ برای تمام xهایی که در یک مدار قرار دارند مقدار ثابتی است. ازاین‌رو اگر O یک مدار باشد داریم $\sum_{x \in O} \frac{1}{|\overline{x}|} = 1$. بنابراین $t = \sum_{x \in X} \frac{1}{|\overline{x}|}$، پس $|N| = |G|\, t$، یعنی

$$\text{تعداد مدارهای } G = t = \frac{|N|}{|G|} = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

■■■

مثال‌های زیر نشان می‌دهند که چگونه می‌توان قضیه برنساید را در حل مسائل مربوط به شمردن بکار برد.

مثال۱۰: به مثال مطرح شده در ابتدای بخش برمی‌گردیم. می‌خواهیم ببینیم که به چند طریق می‌توان رئوس یک مربع را با دو رنگ سفید و سیاه رنگ آمیزی کرد، با این شرط که یک رنگ را بتوان برای اضلاع مختلف بکار برد.

حل: فرض کنید $G = D_4$ گروه حرکت مربع باشد. یادآوری می‌کنیم که

$$D_4 = \{(1), (1\ 3), (2\ 4), (1\ 4\ 3\ 2), (1\ 2\ 3\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$$

Gبطور طبیعی روی رئوس مربع (یعنی مجموعه $\{1,2,3,4\}$) عمل می‌کند. فرض کنید X مجموعه همه مربع‌های رنگ آمیزی شده بدون توجه به تمایز آنها باشد. تعداد رنگ آمیزی های متمایز با تعداد مدارهای عمل G روی X برابر می‌شد. اکنون قضیهٔ برنساید را برای یافتن تعداد این مدارها بکار می‌بریم:

$|X_g|$ را برای تمامی $g \in G$ محاسبه می‌کنیم:

www.mathematic87.blogfa.com

(۱) ($\left|X_{(1)}\right| = |X| = 16$) ، چرا که جایگشت همانی رنگ آمیزی‌ها را تغییر نمی‌دهد.

(۲) $\left|X_{(1\ 2\ 3\ 4)}\right| = 2$، چرا که جایگشت $(1\ 2\ 3\ 4)$ دو رنگ آمیزی را ثابت نگه می‌دارد، یکی اینکه همه رئوس سفید و دیگر اینکه همه رئوس سیاه باشند.

$$\left|X_{(1\ 2\ 3\ 4)}\right| = 2 \qquad \textbf{(۳)}$$

(۴) $\left|X_{(1\ 3)(2\ 4)}\right| = 2^2 = 4$، چرا که رئوس 1 و 3 وهمچنین 2 و 4 باید هم رنگ باشند.

$$\left|X_{(1\ 2)(3\ 4)}\right| = 4 \qquad \textbf{(۵)}$$

$$\left|X_{(1\ 4)(2\ 3)}\right| = 4 \qquad \textbf{(۶)}$$

(۷) $\left|X_{(1\ 3)}\right| = 2^3 = 8$، چرا که رئوس 1 و 3 باید همرنگ باشند و دو رأس دیگر هر رنگی می‌توانند باشند.

$$\left|X_{(2\ 4)}\right| = 8 \qquad \textbf{(۸)}$$

و طبق قضیه برنساید داریم:

$$\text{تعداد مدارها} = t = \frac{1}{8}\left(2^4 + 2^1 + 2^2 + 2^2 + 2^2 + 2^2 + 2^3 + 2^3\right) = 6,$$

یعنی 6 رنگ آمیزی متمایز خواهیم داشت.

■

مثال۱۱: به چند طریق می‌توان اضلاع یک مثلث متساوی الاضلاع را با چهار رنگ، رنگ آمیزی کرد، با این شرط که یک رنگ را بتوان برای اضلاع مختلف بکار برد.

حل: به‌وضوح $2^4 = 64$ رنگ آمیزی وجود دارد، زیرا هر یک از ضلع‌ها را می‌توان با چهاررنگ، رنگ آمیزی کرد. فرض کنید X مجموعه این 64 رنگ آمیزی باشد. فرض کنید $G = S_3$ گروه حرکت مثلث باشد، که بطور طبیعی روی مجموعه رئوس مثلث (مجموعه $\{1,2,3\}$) عمل می‌کند.

به آسانی می‌توان ملاحظه نمود که $|X_{(1)}| = 64$، $|X_{(1\ 2\ 3)}| = |X_{(1\ 2\ 3)}| = 4$ و $|X_{(1\ 2)}| = |X_{(1\ 3)}| = |X_{(2\ 3)}| = 16$. ازاین‌رو

$$\text{تعداد مدارها} = \frac{1}{6}(64 + 4 + 4 + 16 + 16 + 16) = 20.$$

بنابراین 20 مثلث رنگ آمیزی شده متمایز داریم.

■

توضیح تاریخی

سیلو (Peter Ludvig Mejdell Sylow) در دسامبر 1832 در کریستیانای نروژ متولد شد. وی بلافاصله بعد از فارغ التحصیلی از دانشگاه کریستیانا، شروع به تدریس در دبیرستان کریستیانا نمود. سیلو در سال 1862 به عنوان کادر موقت به دانشگاه کریستیانا راه یافت. سیلو همراه با سوفزلی ویرایشی جدید از کارهای آبل ارائه داد. همچنین در سال 1902 به کمک الینگ هلست تناظرهای آبل را به چاپ رساند. سیلو بخاطر کارهایش در نظریهٔ گروه‌ها شناخته شده است: در سال 1845 کشی نشان داد که هر گروه متناهی دارای زیرگروهی از مرتبه عددی اول است که مرتبه گروه را عاد می‌کند. سیلو در سال 1872 در یک مقاله ۱۰ صفحه‌ای این مطلب را تعمیم داد. این مطالب که به نام قضایای سیلو معروف می‌باشند کاربردهایی بسیار اساسی در ساختار گروه‌های متناهی دارند. سیلو در سپتامبر 1918 در گذشت.

www.mathematic87.blogfa.com

تمرینها

۱. مطلوب است X_g و G_x برای هر یک از حالات زیر:

(a) $X = \{1,2,3\}$، $G = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

(b) $X = \{1,2,3,4,4,5,6\}$،

$G = \{\mathrm{id}, (1\ 2), (3\ 4\ 5), (3\ 5\ 4), (1\ 2)(3\ 4\ 5), (1\ 2)(3\ 5\ 4)\}$

۲. فرض کنید $G = A_4$ و فرض کنید G با عمل تزویج روی خودش عمل کند، یعنی $(g,h) \mapsto ghg^{-1}$.

(a) کلاس هم ارزی هر عنصر G را مشخص کنید،

(b) گروه ثابت ساز هر عنصر G را بیابید.

۳. رده‌های تزویج و معادله رده‌ای هر یک ازگروه‌های زیر را بیابید.

(a) S_4 (b) D_4 (c) $\mathbb{Z}_9$ (d) Q

۴. نشان دهید هر گروه از مرتبهٔ 12، 28 ، 56، 96، 160، 200 ساده نیست.

۵. فرض کنید G گروهی متناهی باشد که در آن هر زیزگروه سیلو نرمال است. دراین‌صورت G حاصل‌ضرب مستقیم زیرگروه‌های سیلویش می‌باشد.

۶. نشان دهید هر گروه از مرتبهٔ 77، 255 ، 455و 665 دوری است.

۷. (a) فرض کنید G گروهی از مرتبه p^2q^2 باشد که در آن p و q دو عدد اول متمایز و $q \nmid p^2-1$ و $p \nmid q^2-1$. نشان دهید G آبلی است. سه جفت از اعداد اولی که دارای چنین خاصیتی باشند مثال بزنید.

(b) فرض کنید G گروهی از مرتبه p^2q باشد که در آن p و q دو عدد اول متمایز و $q \nmid p^2-1$ و $p \nmid q-1$. نشان دهید G آبلی است.

www.mathematic87.blogfa.com

۸. (a) هر گروه از مرتبهٔ p^2q^2 که در آن p,q دو عدد اولند، ساده نیست،
(b) هر گروه از مرتبهٔ p^nq که در آن p,q دو عدد اولند و $n \geq 1$، ساده نیست.

۹. فرض کنید G گروهی متناهی باشد که هر $p-$زیرگروه سیلوی آن نرمال باشد. اگر P یک $p-$زیرگروه سیلوی G باشد، آنگاه $C(P) \leq C(G)$.

۱۰. (a) فرض کنید G روی مجموعهٔ غیرتهی X عمل کند. نشان دهید این عمل یک همریختی $\varphi: G \to S_X$ را القاء خواهد کرد،

(b) اگر گروه G دارای زیر گروه سره‌ای با اندیس متناهی باشد، آنگاه G شامل یک زیر گروه نرمال سره‌ای با اندیس متناهی است.

۱۱. فرض کنید p عددی اول و $|G| = p(p+1)$. ثابت کنید G دارای زیرگروه نرمالی از مرتبهٔ p یا $p+1$ است.

۱۲. فرض کنید G یک گروه متناهی و p عدد اولی است که $p \mid |G|$ و $H \trianglelefteq G$. نشان دهید:

(a) برای هر $p-$زیرگروه سیلوی P از G، $P \cap H$ یک $p-$زیرگروه سیلوی H است. برعکس، اگر P_0 یک $p-$زیرگروه سیلوی از H باشد، آنگاه $p-$زیرگروه سیلوی P از G چنان موجود است که $P_0 = P \cap H$.

(b) برای هر $p-$زیرگروه سیلوی P از G، PH/H یک $p-$زیرگروه سیلوی G/H است. برعکس، هر $p-$زیرگروه سیلو از G/H به‌صورت PH/H است، که در اینجا P یک $p-$زیرگروه سیلوی G است.

۱۳. تمام $3-$زیر گروه سیلوهای S_4 را بیابید و نشان دهید که همه آنها مزدوج‌اند.

۱۴. (a) فرض کنید $n \neq 4$. نشان دهید A_n تنها زیرگروه نرمال غیر بدیهی S_n است،

(b) نشان دهید $S_4' = A_4$ و $A_4' = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ و اگر $n \geq 5$، آنگاه $S_n' = A_n$ و $A_n' = A_n$،

(c) نشان دهید هر خودریختی S_4 یک خودریختی داخلی است،

www.mathematic87.blogfa.com

(d) گروهی مانند G وجود ندارد بطوریکه $G' \cong S_3$ یا $G' \cong S_4$.

۱۵. فرض کنید G متناهی ساده غیر آبلی و p بزرگترین عدد اولی باشد که $p \| G|$.

(a) اگر $H < G$، آنگاه $[G : H] \geq p$.

(b) اگر X یک رده تزویجی از G باشد که $|X| > 1$، آنگاه $|X| \geq p$.

۱۶. اگر G یک $p-$گروه متناهی باشد، $H \trianglelefteq G$ و $H \neq \{e\}$، آنگاه $H \bigcap C(G) \neq \{e\}$.

۱۷. فرض کنید G یک گروه متناهی باشد و p کوچکترین عدد اولی باشد که $p \| G|$. اگر $N \trianglelefteq G$ و $|N| = p$، ثابت کنید $N \leq C(G)$.

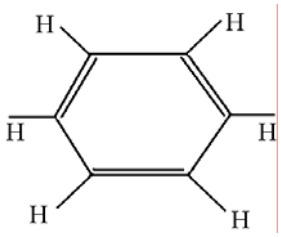
۱۸. به چند طریق متمایز می‌توان شش وجه یک مکعب را از یک تا شش نقطه، نقطه گذاری کرد تا یک تاس بدست آید.

۱۹. برای ساختن اسباب بازی، وجوه مکعب‌های چوبی هم اندازه را باید با رنگ‌های متفاوت رنگ آمیزی کنیم. اگر 8 رنگ در اختیارمان باشد، چند مکعب متمایز می‌توانیم بسازیم.

۲۰. یک ملکول بنزن از شش اتم کربن و شش اتم هیدروژن مطابق شکل زیر تشکیل می‌شود.

(a) از تعویض یک یا چند اتم هیدروژن با یک اتم کلر در ملکول بنزن، چند ترکیب شیمیایی متمایز به وجود می‌آید،

(b) از تعویض سه اتم هیدروژن با ترکیب CH_3 در ملکول بنزن، چند ترکیب شیمیایی متمایز به دست می‌آید.



www.mathematic87.blogfa.com

مسائل مبارزه طلب

۱. فرض کنید G گروهی از مرتبهٔ $2^m n$ باشد که n عددی فرد و $m \geq 1$. اگر G دارای عنصری از مرتبهٔ 2^m باشد، آنگاه G دارای زیرگروه نرمالی از مرتبهٔ n است.

۲. فرض کنید G گروهی از مرتبهٔ $2^m n$ باشد که n عددی فرد است. هرگاه 2- زیر گروه سیلوی G دوری باشد، آنگاه G دارای زیرگروه مشخصه از مرتبهٔ nاست.

۳. فرض کنید G یک گروه متناهی باشد بطوریکه برای هر عدد طبیعی n، Gدارای حداکثر n عنصر از مرتبهٔ n باشد. ثابت کنید G دوری است.

۴. (a) فرض کنید $n > 2$ یک عدد طبیعی باشد. در این‌صورت هر زیرگروه با اندیس n در A_n، با A_{n-1} یکریخت است،

(b) فرض کنید G گروهی متناهی، ساده وغیر آبلی باشد که $|G| \leq 160$. نشان دهید $G \cong A_5$.

۵. اگر G یک گروه متناهی و $H \trianglelefteq G$ و P یک $p-$زیرگروه سیلو از G باشد، نشان دهید $G = HN_G(P)$.

منابعی برای مطالعهٔ بیشتر

1. Aschbacher, A. *Finite Group Theory*. Cambridge University Press, 2000.
2. Burnside, W. *Theory of Groups of Finite Order*. Dover Publications, Inc., New York, 1955.
3. Herstein, I. N. *Topics in Algebra*. Blaisdell International Textbook Series, 1964.
4. Hungerford, T. W. *Algebra*. Springer-Verlag, New York, 1974.

www.mathematic87.blogfa.com

۹ فصل

حلقه‌ها

در این فصل می‌خوانید:

۹-۱ تعریف‌ها و خواص اساسی
۹-۲ ایده‌آل‌ها و حلقه‌های خارج قسمتی
۹-۳ همریختی‌های حلقه

مقدمه

تا اینجا با مجموعه‌هایی سر و کار داشتیم که در آنها یک عمل دوتایی تعریف شده بود. مثال‌هایی مشهود مجموعه‌های $\mathbb{Z}$، $\mathbb{R}$، $\mathbb{Q}$ و $\mathbb{C}$ نشان می‌دهند که باید مطالعه مجموعه‌هایی که در آنها دو عمل دوتایی تعریف شده است از اهمیت زیادی برخوردار باشد. فصل حاضر به مطالعه حلقه‌ها، دستگاه‌های مجردی که در آنها دو عمل دوتایی وجود دارد، اختصاص دارد.

۹-۱ تعریف‌ها و خواص اساسی

تعریف ۹-۱

مجموعه ناتهی R همراه با دو عمل دوتایی (که به صورت جمع و ضرب نوشته می‌شوند) یک **حلقه** است اگر شرایط زیر برقرار باشند.

(۱) $(R,+)$ یک گروه آبلی باشد،

(۲) (قانون **شرکت‌پذیری**): به ازای هر $c \in R$ و b و a

$$(ab)c = a(bc),$$

(۳) (قانون **توزیع‌پذیری**): به ازای هر $c \in R$ و b و a

$$a(b+c) = ab + ac, \quad \text{(توزیع‌پذیری چپ)}$$

$$(a+b)c = ac + bc. \quad \text{(توزیع‌پذیری راست)}$$

تعریف ۹-۲

حلقه R را **جابجایی** گوییم اگر برای هر $b \in R$ و a داشته باشیم:

$$ab = ba.$$

اگر R جابجایی نباشد آنرا **ناجابجایی** گوییم.

تعریف ۹-۳

حلقه R را **یکدار** گوییم اگر عنصر $1_R \in R$ چنان موجود باشد که برای هر $a \in R$،

$$1_R a = a 1_R = a.$$

مثال ۱: هر یک از $\mathbb{Z}$، $\mathbb{Q}$ ، $\mathbb{R}$ و $\mathbb{C}$ همراه با جمع و ضرب معمولی اعداد حلقه‌هایی جابجایی و یکدار می‌باشند.

■

مثال ۲: برای هر عدد طبیعی n، $\mathbb{Z}_n$ حلقه‌ای جابجایی و یکدار است.

■

مثال ۳ (حلقه چندجمله‌ای‌ها): یک **چندجمله‌ای** بر حسب متغیر(مجهول) x روی حلقه R عبارتی به صورت جمع صوری زیر است:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

که در آن $n \geq 0$ و a_i، $0 \leq i \leq n$، عناصری از R موسوم به **ضرایب** $f(x)$ می‌باشند. مجموعه همه چندجمله‌ای‌ها روی R را با $R[x]$ نشان می‌دهیم، به عبارت دیگر

$$R[x] = \left\{a_0 + a_1x + \cdots + a_nx^n \,\middle|\, n \in \mathbb{N} \cup \{0\}, a_i \in R\right\}.$$

اگر $g(x) = b_0 + b_1x + \cdots + b_mx^m$ نیز یک چندجمله‌ای از متغیر x روی R باشد، آنگاه گوییم $f(x)$ و $g(x)$ مساویند و می‌نویسیم $f(x) = g(x)$ اگر ضرایب آنها نظیر به نظیر مساوی باشند، به عبارت دیگر

$$m = n \Leftrightarrow f(x) = g(x) \quad \text{و برای هر} \quad 0 \leq i \leq n \quad a_i = b_i,$$

جمع و ضرب چندجمله‌ای‌ها مطابق قوانین معمولی به صورت زیر تعریف می‌شوند:
اگر $f(x)$ و $g(x)$ دو چندجمله‌ای فوق‌الذکر باشند،

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots,$$

$$f(x)\,g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots = \sum_{k=1}^{n+m} c_kx^k,$$

جاییکه $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$. از این تعاریف می‌توان استفاده کرد و نشان داد که $R[x]$ یک حلقه است که جابجایی و یکدار بودن آن مشروط به جابجایی و یکدار بودن R است.

■

مثال ۴ (حلقه‌های ماتریسی): فرض کنید R یک حلقه باشد. مجموعه ماتریس‌های $n \times n$ روی حلقه R، یعنی $\mathrm{M}_n(R)$ همراه با جمع و ضرب ماتریس‌های

www.mathematic87.blogfa.com

$n \times n$ یک حلقه است. اگر R حلقه‌ای یکدار باشد $\mathrm{M}_n(R)$ نیز چنین است. اگر $R \neq \{0\}$ آنگاه برای $n \geq 2$ حلقه $\mathrm{M}_n(R)$ حلقه‌ای ناجابجایی است.

■

مثال ۵ : هرگاه $R_n, \ldots, R_2, R_1$ حلقه باشند، با تعریف عمل‌های مولفه‌ای روی حاصل‌ضرب دکارتی آنها، یعنی $R_1 \times R_2 \times \cdots \times R_n$، به‌صورت:

$$(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n),$$
$$(r_1, r_2, \ldots, r_n).(s_1, s_2, \ldots, s_n) = (r_1 s_1, r_2 s_2, \ldots, r_n s_n).$$

حلقه‌ای به دست می‌آید که **حاصل‌ضرب مستقیم حلقه‌های** $R_n, \ldots, R_2, R_1$ نامیده می‌شود. این حلقه جابجایی است اگر و فقط اگر هر R_i جابجایی باشد، و این حلقه یکدار است اگر و فقط اگر هر R_i یکدار باشد و یک آن $(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})$ می‌باشد.

■

مثال ۶: فرض کنید X یک مجموعه غیرتهی باشد. روی $R = \mathrm{Map}(X, \mathbb{R})$ اعمال جمع و ضرب را چنین تعریف می‌کنیم:

به ازای هر $f, g \in R$ و به ازای هر $x \in X$

$$(f + g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x)\, g(x).$$

به راحتی مشاهده می‌شود که R حلقه‌ای جابجایی است. صفر این حلقه تابع صفر، θ، است که به ازای هر $x \in X$ به صورت $\theta(x) = 0$ تعریف می‌شود و به ازای هر $f \in R$، معکوس f نسبت به عمل جمع (قرینه f) تابع $(-f)$ می‌باشد که به ازای هر $x \in X$ به صورت $(-f)(x) = -(f(x))$ تعریف می‌شود.

■

مثال ۷ (حلقه صفر): فرض کنید $(G, +)$ یک گروه آبلی باشد. یک عمل ضرب روی G به‌صورت زیر تعریف می‌کنیم:

به ازای هر $a,b \in G$، $ab = 0$. در این صورت G یک حلقه است. حلقه‌هایی که این‌گونه ساخته می‌شوند **حلقه صفر** نامیده می‌شود. چنین حلقه‌هایی همیشه موجودند اما چندان جالب نمی‌باشند.

■

مثال ۸ : فرض کنید $\mathbb{H}(\mathbb{R}) = \mathbb{H} = \left\{a_0 + a_1 i + a_2 j + a_3 k \middle| a_i \in \mathbb{R}\right\}$

در این مجموعه دو عنصر $a_0 + a_1 i + a_2 j + a_3 k$ و $b_0 + b_1 i + b_2 j + b_3 k$ را مساوی گوییم اگر و فقط اگر $a_i = b_i$ برای $i = 0,1,2,3$. جمع و ضرب روی $\mathbb{H}(\mathbb{R})$ را چنین تعریف می‌کنیم:

$$\begin{aligned}&\left(a_0 + a_1 i + a_2 j + a_3 k\right) + \left(b_0 + b_1 i + b_2 j + b_3 k\right) = \\ &\left(a_0 + b_0\right) + \left(a_1 + b_1\right) i + \left(a_2 + b_2\right) j + \left(a_3 + b_3\right) k,\end{aligned}$$

و

$$\begin{aligned}&\left(a_0 + a_1 i + a_2 j + a_3 k\right)\left(b_0 + b_1 i + b_2 j + b_3 k\right) = \\ &\left(a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3\right) + \left(a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2\right) i + \\ &\left(a_0 b_2 + a_2 b_0 + a_3 b_1 - a_1 b_3\right) j + \left(a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1\right) k.\end{aligned}$$

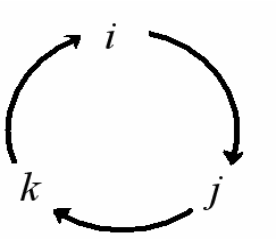
در این صورت $\mathbb{H}(\mathbb{R})$ همراه با جمع و ضرب فوق یک حلقه است. این حلقه را حلقه **چهارگانی حقیقی** می‌نامند. به راحتی می‌توان بررسی کرد که فرمول‌های زیر برقرارند.

$$i^2 = j^2 = k^2 = ijk = -1$$

$$ki = j = -ik \quad , \quad jk = i = -kj \quad , \quad ij = k = -ji$$

به سادگی می‌توان این فرمول‌ها را به خاطر سپرد. حاصل‌ضرب هر دو عنصر متوالی در جهت عقربه‌های ساعت عنصر بعدی آنها است، و حاصل‌ضرب هر دو عنصر متوالی در جهت خلاف عقربه‌های ساعت منفی عنصر بعدی است. (شکل زیر ملاحظه شود).

www.mathematic87.blogfa.com



■

از این پس همواره 0 را عنصر همانی جمعی یک حلقه می‌گیریم و اگر R حلقه‌ای یکدار باشد در صورتی‌که جای هیچ ابهامی نباشد، برای راحتی به جای نماد 1_R از 1 استفاده می‌کنیم، معکوس جمعی عنصر a را با $-a$ و همچنین $a+(-b)$ را با $a-b$ نمایش می‌دهیم. برای هر عدد طبیعی n قرار می‌دهیم

$$na = a + a + \cdots + a \quad (n\text{بار})$$

$$(-n)\,a = (-a) + (-a) + \cdots + (-a) \quad (n\text{بار})$$

و سرانجام تعریف می‌کنیم $0a = 0$.

قضیه ۹-۱

فرض کنید R یک حلقه باشد. در این صورت

(۱) $0a = a0 = 0$ برای هر $a \in R$،

(۲) $a(-b) = (-a)b = -(ab)$ برای هر $a,b \in R$،

(۳) $(-a)(-b) = ab$ برای هر $a,b \in R$،

(۴) $(na)b = a(nb) = n(ab)$ برای هر $n \in \mathbb{Z}$ و هر $a,b \in R$.

اثبات (۱): چون $0a = (0+0)\,a = 0a + 0a$، لذا طبق قانون حذف در گروه $(R,+)$ داریم $0a = 0$. به دلیل مشابه $a0 = 0$.

www.mathematic87.blogfa.com

(۲): با توجه به(۱) داریم $0a = a(0) = a\big(b + (-b)\big) = ab + a(-b)$ و لذا $a(-b) = -(ab)$. به دلیل مشابه $(-a)b = -(ab)$.

(۳): با توجه به(۲) داریم $(-a)(-b) = -(-(a)b) = ab$.

(۴): اگر $n = 0$، بنابر (۱) نتیجه حاصل است. فرض کنید $k(ab) = (ka)b$ که $k > 0$ در این صورت

$$(k+1)(ab) = k(ab) + ab = (ka)b + ab = (ka + a)b = \big[(k+1)a\big]b$$

و لذا طبق استقرا به ازای هر $n > 0$ مطلب ثابت شده است.

حال اگر $n < 0$، آنگاه $(na)b = -n(ab)$ و لذا $-\big((na)b\big) = (-na)b = -n(ab)$. بقیه اثبات مشابه می‌باشد.

■■■

تعریف ۹-۴

فرض کنید R یک حلقه باشد. **مشخصهٔ** حلقه R به‌صورت زیر تعریف می‌شود:

$$\mathrm{Char}R = \mathrm{Min}\{n \in \mathbb{N} \mid nR = 0\},$$

و اگر برای هر $n \in \mathbb{N}$ داشته باشیم $nR \neq 0$، قرار می‌دهیم $\mathrm{Char}R = 0$.

قضیه۹-۲

فرض کنید R یک حلقهٔ یکدار باشد و $\mathrm{Char}R = n > 0$. در این‌صورت:

$$\mathrm{Char}R = \mathrm{Min}\{n \in \mathbb{N} \mid n1_R = 0\}.$$

اثبات: فرض کنید $n = \mathrm{Char}R$ و $m = \mathrm{Min}\{n \in \mathbb{N} \mid n1_R = 0\}$. در این‌صورت:

$$m1_R = 0 \Rightarrow ma = m(1_R a) = (m1_R)a = 0 \text{ ،} a \in R \text{ برای هر} \Rightarrow mR = 0 \Rightarrow n \leq m$$
$$nR = 0 \Rightarrow n1_R = 0 \Rightarrow m \leq n.$$

بنابراین $n = m$.

■■■

www.mathematic87.blogfa.com

مثال ۹ : حلقه $\mathbb{Z}_n$ دارای مشخصه n و حلقه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ دارای مشخصه 0 هستند.
■

تعریف ۹-۵

زیر مجموعه S از حلقه R یک **زیر حلقه** از R نامیده می‌شود، اگر با اعمال تعریف شده در R ، خود یک حلقه باشد.

قضیه۹-۳ (آزمون اول زیر حلقه بودن)

زیر مجموعه ناتهی S از حلقه R یک زیر حلقه است، هرگاه به ازای هر $a,b \in S$ داشته باشیم:

$$a+b,\ ab,\ -a \in S$$

اثبات: با توجه به شرایط داده شده S نسبت به هر دو عمل جمع و ضرب بسته است. کافی است نشان دهیم $0 \in S$. چون S ناتهی است پس عنصری مانند a در Sموجود است. بنابراین طبق فرض $-a$ نیز در S است و لذا $0 = a + (-a) \in S$.

■■■

قضیه۹-۴ (آزمون دوم زیر حلقه بودن)

زیر مجموعه ناتهی S از حلقه R یک زیر حلقه است، هرگاه به ازای هر $a,b \in S$ داشته باشیم:

$$a-b,\ ab \in S$$

اثبات: فرض کنید $a \in S$ پس $0 = a - a \in S$ ولذا $0 - a = -a \in S$. اکنون فرض کنید $a,b \in S$ پس $-b \in S$ ولذا $a-(-b) = a+b \in S$. بنابراین طبق آزمون اول S یک زیرحلقه است.

■■■

مثال ۱۰: فرض کنید $\mathbb{Z}(i)=\{a+bi|a,b\in\mathbb{Z}\}$. در این‌صورت $\mathbb{Z}(i)$ زیر حلقه‌ای از $\mathbb{C}$ موسوم به حلقه **اعداد صحیح گاوسی** است.

■

مثال ۱۱ (حلقه ماتریس‌های بالا مثلثی): برای حلقه R مجموعه زیر

$$\begin{bmatrix} R & R \\ 0 & R \end{bmatrix}=\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}|a,b,c\in R\},$$

یک زیر حلقه از $\mathrm{M}_2(R)$ است که به حلقه ماتریس‌های بالا مثلثی روی R موسوم است. حلقه ماتریس‌های پایین مثلثی نیز به طریق مشابه تعریف می‌شود.

■

مثال ۱۲: مجموعه تمام توابع پیوسته $\mathbb{R}\to\mathbb{R}$ یک زیر حلقه از $\mathrm{Map}(\mathbb{R},\mathbb{R})$ است.

■

مثال ۱۳: هرگاه R یک حلقه باشد، **مرکز** آن $C(R)$ که به‌صورت زیر تعریف می‌شود:

$$C(R)=\{a\in R\mid ar=ra\ ،\quad r\in R \text{ به ازای هر}\}$$

یک زیر حلقه جابجایی از R است.

■

تعریف ۹-۶

فرض کنید R حلقه‌ای یکدار باشد. گوییم عنصر $a\in R$ **معکوس چپ** دارد، اگر $b\in R$ چنان موجود باشد که $ba=1$. همین‌طور، گوییم عنصر $a\in R$ **معکوس راست** دارد، اگر $c\in R$ چنان موجود باشد که $ac=1$. عنصر $a\in R$ **معکوس‌پذیر (یکال)** گوییم اگر معکوس راست وچپ داشته باشد. مجموعه همه یکال‌های R که با R^* (یا $U(R)$) نمایش داده می‌شود تحت عمل ضرب تشکیل یک گروه می‌دهد که موسوم به **گروه یکال‌های** R است.

www.mathematic87.blogfa.com

❖ **تذکر:** اگر عنصر $a \in R$ معکوس‌پذیر باشد، آنگاه به آسانی می‌توان نشان داد که معکوس چپ و معکوس راست a با هم برابر است. بنابراین می‌توان گفت که عنصر $a \in R$ معکوس‌پذیر است اگر وفقط اگر عنصر $a^{-1} \in R$ چنان موجود باشد که $aa^{-1} = a^{-1}a = 1$. در این حالت عنصر a^{-1} را **معکوس** a گوییم.

مثال ۱۴: $\mathbb{Z}^* = \{-1,1\}$، $\mathbb{Z}_n^* = \{\overline{m} \in \mathbb{Z}_n \,|\, (m,n) = 1\}$.

■

مثال ۱۵: نشان دهید اگر $\mathbb{Z}(i) = \{a + bi \,|\, a,b \in \mathbb{Z}\}$ حلقه اعداد صحیح گاوسی باشد، آنگاه $\mathbb{Z}(i)^* = \{\pm 1, \pm i\}$.

حل: فرض کنید $u = a + bi$ یکالی از $\mathbb{Z}(i)$ باشد، چون $uu^{-1} = 1$، لذا

$$|u|^2 \left|u^{-1}\right|^2 = \left|uu^{-1}\right|^2 = 1^2 = 1$$

اما $|u|^2 = a^2 + b^2$ یک عدد طبیعی است، پس $|u|^2 = a^2 + b^2 = 1$. با توجه به اینکه a و b اعداد صحیح هستند، تنها جواب‌های ممکن عبارتند از $(a,b) = (\pm 1, 0)$ یا $(a,b) = (0, \pm 1)$. بنابراین $\mathbb{Z}(i)^* = \{\pm 1, \pm i\}$.

■

تعریف ۹-۷

فرض کنید R حلقه‌ای یکدار باشد که $1_R \neq 0$. در این‌صورت حلقه R را یک **حلقه بخشی (تقسیم)** گوییم هرگاه $R^* = R - \{0\}$. به‌عبارت دیگر هر عنصر غیر صفرش معکوس‌پذیر باشد. حلقه بخشی جابجایی را **میدان** گوییم.

مثال ۱۶: $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$ و $\mathbb{Z}_p$ (p عددی اول) میدان هستند.

■

مثال ۱۷: حلقه چهارگانی حقیقی، $\mathbb{H}(\mathbb{R})$، یک حلقه بخشی است.

www.mathematic87.blogfa.com

حل: فرض کنید $X = a_0 + a_1 i + a_2 j + a_3 k$ عنصر ناصفری از $\mathbb{H}(\mathbb{R})$ باشد. قرار می‌دهیم $b = a_0^2 + a_1^2 + a_2^2 + a_3^2$ و

$$Y = (a_0 / b) - (a_1 / b)i - (a_2 / b)j - (a_3 / b)k \in \mathbb{H}(\mathbb{R})$$

به آسانی می‌توان ملاحظه نمود که $XY = 1 = YX$ و لذا $\mathbb{H}(\mathbb{R})$ یک حلقه بخشی است.

■

تعریف ۹-۸

عنصر e از حلقه R را **خودتوان** گوییم اگر $e^2 = e$.

مثال ۱۸: فرض کنید R حلقه‌ای یکدار باشد. در این‌صورت عناصر 0 و 1 مثال‌هایی ازعناصر خودتوان هستند. عناصر

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

در حلقه $\mathrm{M}_2(R)$ و $(1,0)$، $(0,1)$ در حلقه $R \times R$ خودتوانند. همچنین $4, 3$ در $\mathbb{Z}_6$ مثال‌های دیگری از عناصر خودتوانند.

■

تعریف ۹-۹

عنصر a از حلقه R را **پوچ‌توان** گوییم اگر به ازای یک $n \geq 1$، داشته باشیم $a^n = 0$.

مثال ۱۹: عنصر 0 در هر حلقه‌ای پوچ‌توان است. در حلقه $\mathrm{M}_2(R)$ عناصر

$$\begin{bmatrix} 0 & 0 \\ r & 0 \end{bmatrix}, \begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix}$$

www.mathematic87.blogfa.com

پوچ‌توانند. عنصر 2 در $\mathbb{Z}_4$ و $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$ در $\mathrm{M}_2(\mathbb{Z}_2)$ مثال‌های دیگری از پوچ‌توان‌ها هستند.

■

تعریف ۹-۱۰

فرض کنید R یک حلقه باشد عنصر $a \in R$ را یک **مقسوم‌علیه صفر چپ** گوییم اگر عنصر $0 \neq b \in R$ موجود باشد به طوریکه $ab = 0$. همین‌طور، عنصر $a \in R$ را یک **مقسوم‌علیه صفر راست** گوییم اگر عنصر $0 \neq b \in R$ موجود باشد که $ba = 0$. یک **مقسوم‌علیه صفر** عنصری است که هم یک مقسوم‌علیه صفر راست و هم یک مقسوم‌علیه صفر چپ باشد.

نمادگذاری: مجموعه عناصر مقسوم‌علیه صفر، مقسوم‌علیه صفر راست و مقسوم‌علیه چپ حلقه R به ترتیب با $Z(R)$, $Z_r(R)$ و $Z_\ell(R)$ نشان داده می‌شوند.

اگر R یک حلقه دلخواه باشد واضح است که $Z(R) = Z_r(R) \cap Z_\ell(R)$ و اگر R حلقه‌ای جابجایی باشد، $Z(R) = Z_r(R) = Z_\ell(R)$.

مثال ۲۰: فرض کنید $R \neq \{0\}$ یک حلقه باشد. هر عنصر پوچ‌توان $a \in R$ یک مقسوم‌علیه صفر است، زیرا اگر $a = 0$، به‌وضوح مسئله حل است، در غیر این‌صورت به ازای یک $n \geq 2$ خواهیم داشت $a^n = 0$ و $a^{n-1} \neq 0$ و لذا $aa^{n-1} = a^{n-1}a = 0$، یعنی a یک مقسوم علیه صفر است.

■

مثال ۲۱: در حلقهٔ یکدار R هر عنصر خودتوان $1_R \neq e \neq 0$، یک مقسوم‌علیه صفر است، زیرا

$$e(1_R - e) = 0 = (1_R - e)e.$$

■

مثال ۲۲: $Z(\mathbb{Z}) = Z(\mathbb{H}(\mathbb{R}))=\{0\}$ و $Z(\mathbb{Z}_6) = \{0,2,3,4\}$.

■

تعریف ۹-۱۱

فرض کنید R حلقه‌ای یکدار باشد که $1_R \neq 0$. در این‌صورت

(۱) R را **حوزه** گوییم اگر $Z(R) = \{0\}$،

(۲) هر حوزهٔ جابجایی را یک **حوزه صحیح** نامیم.

قضیه ۹-۵

فرض کنید R حلقه جابجایی و یکدار باشد که $1_R \neq 0$. در این‌صورت R یک حوزهٔ صحیح است اگر و فقط اگر برای هر $a,b \in R$،

$$ab = 0 \Rightarrow a = 0 \text{ یا } b = 0.$$

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

مثال ۲۳: $\mathbb{Z}$ یک حوزه صحیح است. هر حلقه بخشی یک حوزه و هر میدان یک حوزه صحیح است.

■

تعریف ۹-۱۲

دو حلقه R و S را **یکریخت (ایزومورف)** گوییم (و می‌نویسیم $R \cong S$)، هرگاه تابعی یک به یک و پوشا چون $\varphi : R \to S$ موجود باشد که در شرایط زیر صدق کند:

(۱) $\varphi(a+b) = \varphi(a) + \varphi(b)$ برای هر $a,b \in R$،

(۲) $\varphi(ab) = \varphi(a)\varphi(b)$ برای هر $a,b \in R$.

تابع φ را **یکریختی (ایزومورفیسم) حلقه‌ای** می‌نامیم.

مثال ۲۴: نشان دهید که

$$R=\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}|a,b\in\mathbb{R}\}$$

حلقه‌ای است که با $\mathbb{C}$ یکریخت است.

حل: تابع $\varphi:R\to\mathbb{C}$ را با ضابطه $\varphi\begin{bmatrix} a & b \\ -b & a \end{bmatrix}=a+bi$ تعریف می‌کنیم. به آسانی می‌توان مشاهده نمود که φ یک به یک وپوشا و حافظ عمل جمع است و

$$\begin{aligned}\varphi(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix})&=\varphi(\begin{bmatrix} aa'-bb' & ab'+ba' \\ -ba'-ab' & aa'-bb' \end{bmatrix})\\ &=\big(aa'-bb'\big)+\big(ab'+ba'\big)i\\ &=(a+bi)\big(a'+b'i\big)\\ &=\varphi(\begin{bmatrix} a & b \\ -b & a \end{bmatrix})\varphi(\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}),\end{aligned}$$

نشان می‌دهد که φ حافظ ضرب نیز هست. بنابراین φ یک یکریختی است.

■

یکی از مهم‌ترین نتایج قضیه لاگرانژ آن است که هر گروه با مرتبه اول دوری است. این بخش را با نتیجه‌ای مشابه در مورد حلقه‌ها به پایان می‌رسانیم.

قضیه ۹-۶

فرض کنید R حلقه‌ای یکدار و p عدد اولی باشد که $|R|=p$. دراین‌صورت $R\cong\mathbb{Z}_p$.

اثبات: طبق قضیه لاگرانژ در گروه $(R,+)$، داریم $R=<1_R>$ (در حقیقت هر عنصر غیر صفر می‌تواند مولد باشد). اکنون تابع φ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned}\varphi:\mathbb{Z}_p&\to R\\ \overline{m}&\mapsto m1_R\end{aligned}$$

www.mathematic87.blogfa.com

خواهیم داشت:

$$\varphi(\overline{m}_1)=\varphi(\overline{m}_2)\Leftrightarrow R \text{ در } m_1 1_R = m_2 1_R \Leftrightarrow p \mid m_1-m_2 \Leftrightarrow \mathbb{Z}_p \text{ در } \overline{m}_1=\overline{m}_2$$

بنابراین φ تابعی خوش تعریف و یک به یک است. خواننده به آسانی می‌تواند اثبات یکریختی حلقه‌ای بودن φ را کامل کند.

■■■

❖ **تذکر:** در قضیهٔ بالا شرط یکدار بودن حلقه لازم است. برای مثال فرض کنید G یک گروه آبلی از مرتبهٔ عدد اول p باشد. در این‌صورت G یک حلقهٔ صفر از مرتبهٔ p بوده که با حلقهٔ $\mathbb{Z}_p$ یکریخت نیست. (مثال ۷ ملاحظه شود).

۹-۲ ایده‌آل‌ها و حلقه‌های خارج قسمتی

ایده‌آل‌ها، تقریباً همان نقشی که زیر گروه‌های نرمال در نظریه گروه‌ها بر عهده دارند، در نظریه حلقه‌ها ایفا می‌کنند. هر یک از اینها موجب پیدایش ساختارهای خارج قسمتی روی هم‌دسته‌ها می‌شوند.

تعریف ۹-۱۳

فرض کنید I یک زیر حلقه از R باشد.

(۱) I یک **ایده‌آل چپ** Rاست اگر برای هر $r\in R$ وهر $a\in I$ داشته باشیم $ra\in I$،

(۲) I یک **ایده‌آل راست** R است اگر برای هر $r\in R$ وهر $a\in I$ داشته باشیم $ar\in I$،

(۳) I یک **ایده‌آل (دوطرفه)** R است اگر هم یک ایده‌آل چپ و هم ایده‌آل راست باشد.

ایده‌آل (چپ یا راست) I از حلقهٔ R را **سره (حقیقی)** نامیم، اگر $I\neq R$.

مثال ۲۵: در حلقه R، $\{0\}$ و خود R ایده‌آل‌هایی از R هستند. ایده‌آل $\{0\}$ را **ایده‌آل صفر** یا **ایده‌آل بدیهی** نامند.

www.mathematic87.blogfa.com

■

مثال ۲۶: به ازای هر $n \in \mathbb{Z}$، $n\mathbb{Z}$ یک ایده‌آل $\mathbb{Z}$ است.

■

مثال ۲۷: فرض کنید R حلقه‌ای یکدار باشد که $1 \neq 0$. فرض کنید C_k مجموعه عناصر $\mathrm{M}_n(R)$ باشد که درایه‌های غیر صفر تنها در ستون k-ام قرار دارند. در این صورت C_k یک ایده‌آل چپ $\mathrm{M}_n(R)$ است ولی یک ایده‌آل راست نیست. همین‌طور اگر R_k مجموعه عناصر $\mathrm{M}_n(R)$ باشد که درایه‌های غیر صفر تنها روی سطر k-ام قرار دارند. در این صورت R_k یک ایده‌آل راست $\mathrm{M}_n(R)$ است ولی ایده‌آل چپ نیست.

■

قضیه ۹-۷

فرض کنید R یک حلقه باشد.

(۱) اگر $\{S_\lambda \,|\lambda \in \Lambda\}$ خانواده‌ای از زیر حلقه‌های R باشد، آنگاه $\bigcap_{\lambda\in\Lambda} S_\lambda$ زیر حلقه R است،

(۲) اگر $\{I_\lambda \,|\lambda \in \Lambda\}$ خانواده‌ای از ایده‌آل‌های R باشد، آنگاه $\bigcap_{\lambda\in\Lambda} I_\lambda$ یک ایده‌آل R است.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضیه فوق این امکان را به ما می‌دهد که زیر حلقه و ایده‌آل تولید شده به وسیله مجموعه‌ای از عناصر مفروض را تعریف کنیم:

تعریف ۹-۱۴

فرض کنید X زیر مجموعه‌ای از حلقه R باشد. در این صورت اشتراک تمام زیر حلقه‌های R که شامل X باشند را **زیرحلقه تولید شده** توسط X نامیده و آن را با $< X >$ نمایش می‌دهیم.

گزاره ۹-۱

فرض کنید R یک حلقه و $X \subseteq R$. در این صورت زیر حلقه تولید شده به وسیله X برابر است با مجموعه همهٔ حاصل‌جمع‌های متناهی عناصر

$$\pm x_1 x_2 \dots x_n$$

که در آن $x_i \in X, n \in \mathbb{N}$.

اثبات: مجموعه همهٔ حاصل‌جمع‌های متناهی عناصر $\pm x_1 x_2 \dots x_n$ را با A نمایش می‌دهیم. چون $\langle X \rangle$ زیر حلقه‌ای شامل X است لذا $A \subseteq \langle X \rangle$. از طرفی به آسانی می‌توان نشان داد که A حلقه‌ای شامل X است. بنابراین $\langle X \rangle \subseteq A$ و در نتیجه $\langle X \rangle = A$.

■■■

تعریف ۹-۱۵

فرض کنید X زیر مجموعه‌ای از حلقه R باشد. در این صورت اشتراک تمام ایده‌آل‌های حلقه R که شامل X باشند را **ایده‌آل تولید شده** توسط X نامیده و آن را با (X) نمایش می‌دهیم. عناصر X را **مولدهای** ایده‌آل (X) نامیم. اگر $X = \{x_1, \dots, x_n\}$، آنگاه (X) را با $(x_1, \dots, x_n)$ نمایش داده و آنرا **ایده‌آل متناهی مولد** می‌نامیم. ایده‌آل (X) تولید شده توسط عنصر $X = \{x\}$ را **ایده‌آل اصلی** تولید شده توسط x می‌نامیم. حلقه R را **حلقه ایده‌آل اصلی** (به اختصار PIR) نامیم اگر هر ایده‌آل آن اصلی باشد و حلقه‌ای مانند R را **حوزه ایده‌آل اصلی** (به اختصار PID) نامیم اگر R یک حوزه صحیح و حلقه ایده‌آل اصلی باشد.

❖ **تذکر:** حلقه R را متناهی مولد گوییم اگر R به عنوان یک ایده‌آل متناهی مولد باشد.

غالباً مفید است که توصیفی درونی از ایده‌آل تولید شده توسط مجموعه مفروض X داشته باشیم. اکنون چنین توصیفی را ارائه می‌دهیم.

قضیه ۹-۸

فرض کنید R یک حلقه و $x \in R$ و $X \subseteq R$. در این صورت

(۱) $(x) = \{rx + xs + nx + \sum_{i=1}^{m} r_i x s_i \,|\, r, s, r_i, s_i \in R, m \in \mathbb{N}, n \in \mathbb{Z}\}$،

(۲) اگر R یکدار باشد، آنگاه $(x) = \{\sum_{i=1}^{m} r_i x s_i \,|\, r_i, s_i \in R, m \in \mathbb{N}\}$،

(۳) اگر $x \in C(R)$، آنگاه $(x) = \{rx + nx | r \in R, n \in \mathbb{Z}\}$،

(۴) $Rx = \{rx | r \in R\}$ و $xR = \{xr | r \in R\}$ به ترتیب ایده‌آل چپ و راست R می‌باشند (که ممکن است شامل x نباشند). اگر R حلقه‌ای یکدار باشد، آنگاه $x \in Rx$، $x \in xR$

(۵) اگر R حلقه‌ای یکدار و $x \in C(R)$، آنگاه $(x) = xR = Rx$،

(۶) اگر R حلقه‌ای یکدار و $X \subseteq C(R)$، آنگاه

$$(X) = \{\sum_{i=1}^{m} r_i x_i \,|\, r_i \in R, x_i \in X, m \in \mathbb{N}\}.$$

اثبات (۱): نشان دهید که

$$I = \{rx + xs + nx + \sum_{i=1}^{m} r_i x s_i \,|\, r, s, r_i, s_i \in R, m \in \mathbb{N}, n \in \mathbb{Z}\}$$

ایده‌آلی از R است که $x \in I$. به علاوه هر ایده‌آل دیگر R که شامل x باشد، شامل I خواهد بود و لذا $I = (x)$.

(۲): به آسانی از مطالب زیر نتیجه می‌شود

www.mathematic87.blogfa.com

$$rx = rx1_R,$$
$$xs = 1_R xs,$$
$$nx = n\left(1_R x\right) = (n1_R)x.$$

بقیه اثبات به عنوان تمرین به خواننده واگذار می‌شود.

■■■

فرض کنید $I_n,\dots,I_2,I_1$ زیر مجموعه‌های غیر تهی از حلقه R باشند. تعریف می‌کنیم:

$$I_1 + I_2 + \cdots + I_n = \left\{a_1 + a_2 + \cdots + a_n \,\middle|\, a_i \in I\right\}.$$

اگر I و J دو زیر مجموعه غیر تهی از R باشند، تعریف می‌کنیم:

$$IJ = \left\{a_1b_1 + \cdots + a_nb_n \,\middle|\, a_i \in I, b_i \in J, n \in \mathbb{N}\right\}.$$

اگر $I = \{a\}$ به جای IJ می‌نویسیم aJ. همین‌طور اگر $J = \{b\}$ به جای IJ می‌نویسیم Ib. توجه داشته باشیم که اگر J (یا I) نسبت به عمل جمع بسته باشد آنگاه

$$\left(Ib = \{ab|a \in I\}\right) \quad aJ = \{ab|b \in J\}.$$

در حالت کلی $I_1I_2\dots I_n$ را مجموعه تمام حاصل‌جمع‌های متناهی به صورت $a_1a_2\dots a_n$، $a_i \in I, n \in \mathbb{N}$، تعریف می‌کنیم. در حالت خاص که به ازای هر i، $1 \le i \le n$، $I_i = I$، $I_1I_2\dots I_n$ را با I^n نمایش می‌دهیم.

قضیه ۹-۹

فرض کنید $K,J,I_n,\dots,I_2,I_1,I$ ایده‌آل‌هایی از حلقه R باشند. در این صورت

(۱) $I_1 + I_2 + \cdots + I_n$ ، $I_1I_2\dots I_n$ ایده‌آل‌هایی از R می‌باشند،

(۲) $(I + J) + K = I + (J + K)$ ، $(IJ)K = I(JK)$،

(۳) $J\left(I_1 + I_2 + \cdots + I_n\right) = JI_1 + JI_2 + \cdots + JI_n$،

$$\left(I_1 + I_2 + \cdots + I_n\right)K = I_1K + I_2K + \cdots + I_nK.$$

www.mathematic87.blogfa.com

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

اینک مفهوم گروه‌های خارج قسمتی را به حلقه‌های خارج قسمتی تعمیم می‌دهیم.

لم ۹-۱

فرض کنید I یک زیر گروه جمعی حلقه R باشد. در این صورت شرایط زیر معادلند.
(۱) عمل ضرب $(a+I)(b+I)=ab+I$ روی R/I خوش تعریف است،
(۲) I ایده‌آلی از حلقه R است.

اثبات (۱) $\Leftarrow$ **(۲)**: فرض کنید $r\in R$ و $a\in I$. در این صورت با توجه به (۱) داریم

$$(ra+I)=(r+I)(a+I)=(r+I)(0+I)=r0+I=0+I=I.$$

این نتیجه می‌دهد که $ra\subseteq I$، پس $rI\subseteq I$. به طور مشابه، $Ir\subseteq I$.

(۲) $\Leftarrow$ **(۱)**:فرض کنید $a+I=a'+I$ و $b+I=b'+I$. در این صورت عناصر $x,y\in I$ چنان موجودند که $a=a'+x$ و $b=b'+y$. در نتیجه

$$ab=(a'+x)(b'+y)=a'b'+a'y+xb'+xy.$$

بنابراین $ab-a'b'\in I$ و لذا $ab+I=a'b'+I$. بدین ترتیب قسمت (۱) بدست می‌آید.

■■■

قضیه ۹-۱۰

فرض کنید I ایده‌آلی از حلقه R باشد. دراین‌صورت گروه خارج قسمتی جمعی R/I همراه با عمل ضرب $(a+I)(b+I)=ab+I$ یک حلقه است. اگر R جابجایی یا یکدار باشد، R/I نیز چنین است.

اثبات: با توجه به لم قبل، عمل ضرب خوش تعریف است. در مورد قانون شرکت‌پذیری داریم:

www.mathematic87.blogfa.com

$$\begin{aligned}\big((a+I)(b+I)\big)(c+I) &= (ab+I)(c+I)\\ &= (ab)\,c+I\\ &= a\,(bc)+I\\ &= (a+I)(bc+I)\\ &= (a+I)\big((b+I)(c+I)\big).\end{aligned}$$

اثبات قانون توزیع‌پذیری را به خواننده واگذار می‌کنیم. اگر R حلقه‌ای جابجایی باشد به‌وضوح R/I نیز جابجایی است و اگر R حلقه‌ای یکدار باشد، آنگاه R/I نیز یکدار است و یک آن 1_R+I می‌باشد.

■■■

تعریف ۹-۱۶

ایده‌آل سرهٔ P از حلقه R را **اول** گوییم اگر و فقط اگر برای هر $a,b\in R$،

$$aRb\subseteq P \Rightarrow a\in P \text{ یا } b\in P.$$

مجموعهٔ ایده‌آل‌های اول حلقهٔ R را با نماد $\mathrm{Spect}(R)$ نمایش می‌دهیم.

نتیجه ۹-۱

فرض کنید R یک حلقه جابجایی و یکدار باشد. ایده‌آل سرهٔ P از R اول است اگر و فقط اگر برای هر $a,b\in R$،

$$ab\in P \Rightarrow a\in P \text{ یا } b\in P.$$

در نظریه حلقه‌های جابجایی ایده‌آل‌های اول به صورت زیر شناسایی می‌شوند.

قضیه ۹-۱۱

ایده‌آل P از حلقه جابجایی و یکدار R اول است و اگر و فقط اگر R/P یک حوزه

اثبات: فرض کنید P ایده‌آل اولی از حلقه R باشد. چون $P\neq R$، $1+P\neq 0+P$. فرض کنید $(a+P)(b+P)=P$. بنابراین $ab+P=P$ و لذا $ab\in P$. چون P ایده‌آل

www.mathematic87.blogfa.com

اولی در حلقه جابجایی R می‌باشد، بنابرنتیجه فوق $a \in P$ یا $b \in P$. یعنی $a+P=P$ یا $b+P=P$. بنابراین R/P یک حوزه صحیح می‌باشد. به عکس، اگر R/P یک حوزه صحیح باشد، آنگاه $1+P \neq 0+P$ و لذا $P \neq R$. حال اگر $ab \in P$ آنگاه $ab+P=P$ و لذا $(a+P)(b+P)=P$. ازاین‌رو $a+P=P$ یا $b+P=P$. در نتیجه $a \in P$ یا $b \in P$ و بنابر نتیجه فوق P اول است.

■■■

تعریف ۹-۱۷

ایده‌آل سرهٔ M از حلقه R را یک **ایده‌آل ماکزیمال** گوییم هرگاه به ازای هر ایده‌آل I از R که $M \subseteq I \subseteq R$، داشته باشیم $I=R$. مجموعهٔ ایده‌آل‌های ماکزیمال حلقهٔ R را با نماد $\mathrm{Max}(R)$ نمایش می‌دهیم.

اکنون شرطی لازم و کافی برای ماکزیمال بودن یک ایده‌آل در یک حلقه جابجایی و یکدار ارائه می‌دهیم.

قضیه ۹-۱۲

فرض کنید R یک حلقه جابجایی و یکدار و M ایده‌آلی از R باشد. در این صورت M ماکزیمال است اگر و فقط اگر R/M یک میدان باشد.

اثبات: فرض کنید M یک ایده‌آل ماکزیمال از حلقهٔ R باشد. در
این‌صورت $1+M \neq 0+M$. فرض کنید $a+M$ عنصر غیر صفری از R/M باشد.
دراین‌صورت $a \notin M$ و با توجه به ماکزیمال بودن M داریم $Ra+M=R$.
ازاین‌رو $1=ra+m$ که در آن $m \in M, r \in R$. حال داریم:

$$1+M=ra+m+M=ra+M=(r+M)(a+M),$$

یعنی $r+M$ معکوس $a+M$ می‌باشد و در نتیجه R/M یک میدان است.
برعکس، فرض کنید R/M یک میدان باشد. در این‌صورت $1+M \neq 0+M$ و لذا $M \neq R$. حال فرض کنید I ایده‌آلی از R باشد که $M \subsetneq I \subseteq R$. بنابراین

$a \in I$ چنان موجود است که $a \notin M$. چون $a+M$ عنصر غیر صفری از حلقهٔ R/M است، پس عنصر $b+M \in R/M$ چنان موجود است که $(a+M)(b+M) = 1+M$. ازاین‌رو عنصری مانند $m \in M$ به‌گونه‌ای موجود است که $1 = ab+m$. در نتیجه $1 \in I$، یعنی $I = R$.

■■■

مثال ۲۸: ایده‌آل (3) در حلقه $\mathbb{Z}$ ماکزیمال است، ولی ایده‌آل (4) ماکزیمال نیست زیرا $\mathbb{Z} \subseteq (2) \subseteq (4)$.

■

نتیجهٔ زیر به‌آسانی از قضیه ۱۲ و۱۳ بدست می‌آید.

نتیجه ۹-۲

فرض کنید R یک حلقه جابجایی و یکدار باشد. در این‌صورت

$$\mathrm{Max}(R) \subseteq \mathrm{Spect}(R).$$

❖ **تذکر (۱)** : عکس قضیه فوق برقرار نمی‌باشد، زیرا که $\{0\}$ یک ایده‌آل اول حلقه $\mathbb{Z}$ است در صورتیکه ماکزیمال نیست.

(۲) برای حالت کلیتر نتیجه بالا تمرین ۱۴ را ملاحظه کنید.

قضیه زیر مبین وجود ایده‌آل‌های ماکزیمال می‌باشد.

قضیه ۹-۱۳

اگر R یک حلقه متناهی مولد باشد، آنگاه هر ایده‌آل سره از R در یک ایده‌آل ماکزیمال قرار دارد.

اثبات: فرض کنید $R =< a_1, ..., a_n >$ و I ایده‌آل سره‌ای از R باشد. قرار می‌دهیم.

$$\Omega = \{J \,|\, I \subseteq J, \text{ است } R \text{ ایده‌آل سره‌ای از } J\}$$

www.mathematic87.blogfa.com

به‌وضوح Ω غیر تهی است، زیرا $I \in \Omega$. حال زنجیر صعودی $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ از عناصر Ω را در نظر می‌گیریم. نشان می‌دهیم $J = \bigcup_{i=1}^{\infty} J_i \in \Omega$. برای این منظور فرض کنید $a,b \in J$ و $r \in R$. در این صورت اندیس‌های i و j، که $i \geq j$، چنان موجودند که $a \in J_i$, $b \in J_j$ و لذا $a-b \in J_i \subseteq J$ همچنین $ar,\ ra \in J_i \subseteq J$. در نتیجه J یک ایده‌آل R است. حال باید نشان دهیم که J ایده‌آل سره‌ای از R است. برعکس، فرض کنیم $J = R$. در این صورت برای هر $1 \leq k \leq n$ ایده‌آل J_{ℓ_k} از زنجیر فوق‌الذکر موجود است که $a_k \in J_{\ell_k}$. اگر $\ell = \max\left\{\ell_k\right\}_{k=1}^{n}$، آنگاه $R =< a_1,...,a_n > \subseteq J_\ell$، که تناقض است. بالاخره توجه می‌کنیم که $I \subseteq J$. بنابراین J یک کران بالا از زنجیر است. ازاین‌رو طبق لم زرن، Ω دارای عنصر ماکزیمال M است. به‌وضوح عنصر ماکزیمال Ω (یعنی M) همان ایده‌آل ماکزیمال مطلوب است.

■■■

این بخش را با معرفی حلقه‌های ساده به پایان می‌بریم.

تعریف ۹-۱۸

حلقه یکدار R را **ساده** گوییم اگر $R \neq 0$ و تنها ایده‌آل‌های R برابر باشند با $\{0\}$ و R.

مثال ۲۹: هر حلقه بخشی یک حلقه ساده است.

■

قضیه ۹-۱۴

حلقه جابجایی و یکدار R ساده است اگر و فقط اگر یک میدان باشد.

اثبات: واضح است که هر میدان یک حلقه ساده است. برعکس، اگر R یک حلقه جابجایی و یکدار ساده باشد و $0 \neq a \in R$ آنگاه $Ra \neq 0$ (زیرا $a \in Ra$) و لذا از ساده بودن R نتیجه می‌شود $Ra = R$. بنابراین $1 \in Ra$ و در نتیجه a در R یکال است. لذا R یک میدان است.

■■■

۹-۳ همریختی‌های حلقه

در مطالعه نظریه گروه‌ها، یک همریختی تابعی است بین دو گروه که حافظ عمل گروه باشد. به طور مشابه، یک همریختی بین دو حلقه تابعی است که حافظ عمل جمع و ضرب باشد. بحث در مورد همریختی‌های حلقه‌ها را به موازات مطالب فصل ۶ در مورد همریختی‌های گروه‌ها پیش می‌بریم.

تعریف ۹-۱۹

فرض کنید R و S دو حلقه باشند.

تابع $\varphi : R \to S$ را یک **همریختی** (هوموморفیسم) حلقه‌ای نامیم اگر برای هر a و b در R:

(۱) $\varphi(a+b) = \varphi(a) + \varphi(b)$،

(۲) $\varphi(ab) = \varphi(a)\varphi(b)$.

همریختی $\varphi : R \to S$ را **تکریختی** (مونومورفیسم) حلقه‌ای گوییم، اگر φ یک به یک باشد.

همریختی $\varphi : R \to S$ را **برووریختی** (اپی‌مورفیسم) حلقه‌ای گوییم، اگر φ پوشا باشد.

گوییم R در S **قابل نشاندن** است (و یا R در S می‌نشیند)، اگر یک تکریختی $\varphi : R \to S$ موجود باشد. به عبارت دیگر R با زیرحلقه‌ای از S یکریخت باشد.

یادآوری: همریختی $\varphi : R \to S$ یک یکریختی (ایزومورفیسم) است، اگر φ یک به یک و پوشا باشد.

مثال ۳۰ : اگر I ایده‌آلی از حلقه R باشد، نگاشت طبیعی $\gamma : R \to R/I$ که با ضابطه $\gamma(a) = a + I$ تعریف می‌شود، یک برووریختی حلقه‌ای است.

■

مثال ۳۱: فرض کنید n یک عدد طبیعی باشد، نگاشت $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ که با ضابطه $\varphi(a) = \overline{a}$ تعریف می‌شود، یک برووریختی حلقه‌ای است.

■

مثال ۳۲: تابع $\varphi : \mathbb{C} \to \mathrm{M}_2(\mathbb{R})$ با تعریف زیر یک تکریختی است.

$$\varphi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

■

مثال ۳۳: هرگاه $R_n, \ldots, R_2, R_1$ حلقه باشند، توابع تصویری زیر برووریختی می‌باشند.

$$\pi_i : R_1 \times R_2 \times \ldots \times R_n \to R_i$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_i$$

■

قضیه ۹-۱۵

فرض کنید $\varphi : R \to S$ یک همریختی حلقه‌ای باشد و $a \in R$.

(۱) $\varphi(0) = 0$ (φ، عنصر همانی جمع را حفظ می‌کند)،

(۲) $\varphi(-a) = -\varphi(a)$ (φ، قرینه را حفظ می‌کند)،

(۳) $\varphi(na) = n\varphi(a)$ برای هر $n \in \mathbb{Z}$،

(۴) $\varphi(a^n) = \varphi(a)^n$ برای هر $n \in \mathbb{N} \cup \{0\}$،

(۵) اگر $a \in R^*$، $\varphi(a^n) = \varphi(a)^n$ برای هر $n \in \mathbb{Z}$.

اثبات: با توجه به اینکه همریختی‌های حلقه‌ای، همریختی‌هایی از گروه‌های جمعی آبلی هستند، سه خاصیت حفظ کنندگی اول واضح هستند. اثبات دو قسمت آخر به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضیه ۹-۱۸

فرض کنید $\varphi : R \to S$ یک بروریختی حلقه‌ای باشد. نشان دهید $\varphi(1_R) = 1_S$.

اثبات: فرض کنید $\varphi(1_R) = e$. اگر $s \in S$ عنصر دلخواهی باشد، آنگاه به ازای یک $r \in R$، داریم $\varphi(r) = s$ (چون φ پوشا است). از این‌رو

$$se = \varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r) = s$$

به همین ترتیب $es = s$. بنابراین $e = 1_S$.

■■■

مثال‌های زیر نشان می‌دهند که شرط پوشا بودن در قضیه فوق الزامی است.

مثال ۳۴: اگر $\varphi : R \to S$ چنین تعریف شود: به ازای هر $r \in R$، $\varphi(r) = 0$، آنگاه φ یک همریختی حلقه‌ای است. این همریختی را همریختی صفر می‌نامیم. φ عنصر همانی ضربی را حفظ نمی‌کند.

■

مثال ۳۵: تابع $\varphi : R \to R \times R$ با ضابطه $\varphi(r) = (r, 0)$ یک تکریختی است که اگر $R \neq 0$، φ عنصر همانی ضربی را حفظ نمی‌کند.

■

تعریف ۹-۲۰

فرض کنید $\varphi : R \to S$ یک همریختی حلقه‌ای باشد. در این صورت **تصویر و هسته** φ عبارتند از:

$$\text{تصویر } \varphi = \operatorname{Im}\varphi = \varphi(R) = \{\varphi(a) | a \in R\},$$

$$\text{هسته } \varphi = \operatorname{Ker}\varphi = \{a \in R | \varphi(a) = 0\}.$$

www.mathematic87.blogfa.com

قضیه ۹-۱۷

اگر $\varphi : R \to S$ یک همریختی حلقه‌ای باشد، آنگاه

(۱) $\mathrm{Im}\,\varphi$ زیر حلقه‌ای از S است،

(۲) $\mathrm{Ker}\,\varphi$ ایده‌آلی از R است.

اثبات (۱): هر همریختی حلقه‌ای $\varphi : R \to S$، یک همریختی جمعی نیز هست. بنابراین تصویر و هسته φ به ترتیب زیر گروه‌هایی از R و S هستند. به علاوه، تساوی $\varphi(ab) = \varphi(a)\varphi(b)$ نشان می‌دهد که $\mathrm{Im}\,\varphi$ تحت عمل ضرب نیز بسته است.

(۲): اگر $a \in R$ و $k \in \mathrm{Ker}\,\varphi$، آنگاه $\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)0 = 0$ و در نتیجه $ak \in \mathrm{Ker}\,\varphi$. به طور مشابه می‌توان نشان داد که $ka \in \mathrm{Ker}\,\varphi$. بنابراین $\mathrm{Ker}\,\varphi$ ایده‌آلی از R است.

■■■

لم ۹-۲

همریختی حلقه‌ای $\varphi : R \to S$ یک به یک است اگر و فقط اگر $\mathrm{Ker}\,\varphi = \{0\}$.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

اینک، مهم‌ترین قضایای این بخش، یعنی قضایای یکریختی حلقه‌ها را مطرح می‌کنیم. با توجه به اینکه اثبات این قضایا مشابه قضایای یکریختی گروه‌ها است، اثبات این قضایا را به خواننده واگذار می‌کنیم.

قضیه۹-۱۸ (قضیه اول یکریختی)

فرض کنید $\varphi : R \to S$ یک همریختی حلقه‌ای باشد. اگر $K = \mathrm{Ker}\varphi$، آنگاه φ یکریختی حلقه‌ای زیر را القاء می‌کند:

$$\overline{\varphi} : R/K \to \mathrm{Im}\,\varphi$$
$$a + K \mapsto \varphi(a)$$

قضیه۹-۱۹(قضیه دوم یکریختی)

فرض کنید I و J در ایده‌آل از حلقه R باشند. در این صورت

$$\frac{J}{I \cap J} \cong \frac{(I+J)}{I}.$$

قضیه۹-۲۰ (قضیه سوم یریختی)

فرض کنید I و J دو ایده‌آل از حلقه R باشند، به قسمی که $I \subseteq J$. در این صورت J/I ایده‌آلی از R/I می‌باشد و

$$\frac{R/I}{J/I} \cong \frac{R}{J}.$$

قضیه۹-۲۳ (قضیه تناظر)

فرض کنید I ایده‌آلی از حلقه R باشد. در این صورت یک دوسویی بین ایده‌آل‌های R که شامل I هستند و مجموعه ایده‌آل‌های R/I، به صورت $J \leftrightarrow J/I$، وجود دارد. از این رو هر ایده‌آل در R/I به صورت J/Iمی‌باشد، که در آن J ایده‌آلی از R است به قسمی که $I \subseteq J$.

مثال ۳۶: فرض کنید R یک حلقه باشد. نشان دهید $R[x]/<x> \cong R$.

حل: تابع $\varphi : R[x] \to R$ با ضابطه $\varphi\left(a_0 + a_1x + \ldots + a_nx^n\right) = a_0$ مسلماً یک بروریختی است. چون $\text{Ker}\varphi = <x>$، پس طبق قضیه اول یکریختی $R[x]/<x> \cong R$.

■

مثال ۳۷: فرض کنید R یک حلقه باشد. نشان دهید $R/<0> \cong R$.

حل: تابع $\varphi : R \to R$ با ضابطه $\varphi(a) = a$ (همریختی همانی) یک به یک و پوشا است. ازاین‌رو طبق قضیه اول $R/<0> \cong R$.

■

www.mathematic87.blogfa.com

مثال ۳۸: فرض کنید I ایده‌آلی از حلقه R باشد. نشان دهید.

$$\mathrm{M}_n(R)/\mathrm{M}_n(I) \cong \mathrm{M}_n(R/I).$$

حل: همریختی طبیعی $\gamma : R \to R/I$، همریختی زیر را القاء می‌کند:

$$\overline{\gamma} : \mathrm{M}_n(R) \to \mathrm{M}_n(R/I)$$
$$\overline{\gamma}\left(\left[a_{ij}\right]\right) = \left[\lambda(a_{ij})\right] = \left[a_{ij} + I\right]$$

بدیهی است که $\overline{\gamma}$ پوشا بوده و $\mathrm{Ker}\,\overline{\gamma} = \mathrm{M}_n(I)$. بنابراین طبق قضیه اول یکریختی نتیجه مطلوب برقرار است.

■

مثال ۳۹: فرض کنید I ایده‌آلی از حلقه R باشد. در این‌صورت:

$$R[x]/I[x] \cong (R/I)[x]$$

حل: این مطلب از آنجا نتیجه می‌شود که هر همریختی حلقه‌ای $R \to S$ یک همریختی حلقه‌ای $R[x] \to S[x]$ را القاء می‌کند.

■

قضیه ۹-۲۲

ایده‌آل M از حلقه R ماکزیمال است اگر و فقط اگر حلقه خارج قسمتی R/M ساده

اثبات: ایده‌آل M ماکزیمال است اگر و فقط اگر حلقه خارج قسمتی R/M تنها دارای دو ایده‌آل 0 و R/M باشد (طبق قضیه تناظر). چون برقراری این شرط به معنی ساده بودن حلقه R/M است، لذا اثبات قضیه کامل است.

■■■

گزاره ۹-۲

فرض کنید R و S دو حلقه غیر صفر باشند. در این‌صورت

(۱) K ایده‌آلی از $R\times S$ است اگر و فقط اگر $K=I\times J$، که I و J به ترتیب ایده‌آل‌هایی از R و S هستند،

(۲) ایده‌آل‌های ماکزیمال M در $R\times S$ به یکی از دو شکل زیر می‌باشند:

(الف) $M=I\times S$، که I ایده‌آل ماکزیمالی از R است،

(ب) $M=R\times J$، که J ایده‌آل ماکزیمالی از S است.

اثبات (۱): فرض کنید I و J به ترتیب ایده‌آل‌هایی از R و S باشند. در این‌صورت به وضوح $I\times J$ ایده‌آلی از $R\times S$ است. برعکس، فرض کنید K یک ایده‌آل از $R\times S$ باشد. تعریف می‌کنیم:

$$I=\{a\in R\,|\,(a,0)\in K\},\quad J=\{b\in S\,|\,(0,b)\in K\}$$

به آسانی می‌توان مشاهده نمود که I ایده‌آلی از R و J ایده‌آلی از S است. کافی است نشان دهیم $K=I\times J$ اگر $(r,s)\in K$، آنگاه $(r,0)=(r,s)(1,0)\in K$ و $(0,s)=(r,s)(0,1)\in K$. ازاین‌رو $r\in I$ و $s\in J$ و در نتیجه $(r,s)\in I\times J$. یعنی $K\subseteq I\times J$. از طرف دیگر، اگر $(a,b)\in I\times J$ آنگاه $(a,b)=(a,0)+(0,b)\in K+K\subseteq K$. بنابراین $K=I\times J$.

(۲): فرض کنید M ایده‌آل ماکزیمالی از حلقه $R\times S$ باشد، طبق (۱)، $M=I\times J$، که I و J به ترتیب ایده‌آل‌هایی از R و S می‌باشند. اما تابع

$$\varphi: R\times S\to R/I\times S/J$$
$$(r,s)\mapsto(r+I,s+J)$$

یک برورختی با $\mathrm{Ker}\,\varphi=I\times J=M$ می‌باشد. با توجه به قضیه تناظر، ایده‌آل M در $R\times S$ ماکزیمال است اگر و فقط اگر $\varphi(R\times S)=R/I\times S/J$ ساده باشد. اما حاصل‌ضرب دو حلقه فقط و فقط در صورتی ساده است که یکی از آنها صفر و دیگری ساده

باشد. بنابراین حلقه $R/I\times S/J$ ساده است اگر و فقط اگر $J=S$ و I در R ماکزیمال باشد و یا $I=R$ و J در S ماکزیمال باشد. بدین ترتیب قسمت (۲) اثبات می‌شود.

■■■

❖ **تذکر:** بطریق مشابه میتوان نشان داد که ایده‌آل اول P از $R\times S$ به یکی از دو شکل زیر است:

(۱) $P=I\times S$، که I ایده‌آل اولی از R است،

(۲) $P=R\times J$، که J ایده‌آل اولی از S است.

تعریف ۹-۲۱

فرض کنید I ایده‌آلی از حلقه R و $a,b\in R$. گوییم a و b به پیمانه I همنشت اند (و می‌نویسیم $a\overset{I}{\equiv}b$) اگر $a-b\in I$.

لم ۹-۳

فرض کنید $I_1,\ldots,I_n$ ایده‌آل‌هایی از حلقه R باشند که برای هر i، $R^2+I_i=R$ و برای هر $i\neq j$، $I_i+I_j=R$. در این‌صورت:

$$R=I_k+(\bigcap_{i\neq k}I_i)\ (k=1,2,\ldots,n)$$

اثبات: چون $I_1+I_2=R$ و $I_1+I_3=R$،

$$R^2=(I_1+I_2)(I_1+I_3)=I_1^2+I_1I_3+I_2I_1+I_2I_3\subseteq I_1+I_2I_3\subseteq I_1+(I_2\cap I_3)$$

با توجه به اینکه $R=I_1+R^2$،

$$R=I_1+R^2\subseteq I_1+(I_1+(I_2\cap I_3))=I_1+(I_2\cap I_3)\subseteq R$$

بنابراین $R=I_1+(I_2\cap I_3)$. به طور استقرایی فرض کنید

www.mathematic87.blogfa.com

$$R = I_1 + \big(I_2 \cap I_3 \cap \ldots \cap I_{k-1}\big).$$

در این‌صورت $R^2 = \big(I_1 + \big(I_2 \cap \ldots \cap I_{k-1}\big)\big)\big(I_1 + I_k\big) \subseteq I_1 + \big(I_2 \cap I_3 \cap \ldots \cap I_k\big)$

و در نتیجه $R = R^2 + I_1 \subseteq I_1 + \big(I_2 \cap \ldots \cap I_k\big)$. بنابراین $R = I_1 + (\bigcap_{i\neq 1} I_i)$. با استدلالی مشابه می‌توان نشان داد که

$$R = I_k + (\bigcap_{i\neq k} I_i) \ (k = 1,2,\ldots,n).$$

■■■

قضیه۹-۲۳ (قضیه باقیمانده چینی)

فرض کنید $I_1,\ldots,I_n$ ایده‌آل‌هایی از حلقه R باشند به طوریکه برای هر i، $R^2 + I_i = R$ و برای هر $i \neq j$، $I_i + I_j = R$. اگر $b_1,\ldots,b_n \in R$، آنگاه عنصر $r \in R$ چنان موجود است که

$$r \overset{I_i}{\equiv} b_i \quad (i = 1,2,\ldots,n)$$

اثبات: با توجه به لم فوق برای هر $1 \leq k \leq n$، عناصر $a_k \in I_k$ و $r_k \in \bigcap_{i\neq k} I_i$ چنان موجودند که $b_k = a_k + r_k$. ازاین‌رو

$$r_k \overset{I_k}{\equiv} b_k \,, r_k \overset{I_i}{\equiv} 0 \quad (i \neq k)$$

حال قرار می‌دهیم $r = r_1 + r_2 + \ldots + r_n$. در این صورت برای هر i، $b \overset{I_i}{\equiv} r_i \overset{I_i}{\equiv} b_i$. در نهایت اگر $s \in R$ و $s \overset{I_i}{\equiv} b_i$ (برای هر i)، آنگاه $r \overset{I_i}{\equiv} s$ و لذا $r - s \in I_i$ و در نتیجه $r - s \in \bigcap_{i=1}^{n} I_i$، یعنی r و s به پیمانه $\bigcap_{i=1}^{n} I_i$ همنهشت اند.

■■■

نتیجه۹-۳ (قضیه باقیمانده چینی در نظریه اعداد)

فرض $m_n,\ldots,m_1$ اعدادی طبیعی باشند که دو به دو نسبت به هم اولند. اگر $b_n,\ldots,b_1$ اعدادی صحیح باشند، آنگاه دستگاه

$$\begin{cases} x \overset{m_1}{\equiv} b_1 \\ x \overset{m_2}{\equiv} b_2 \\ \vdots \\ x \overset{m_n}{\equiv} b_n \end{cases}$$

دارای جواب است واین جواب به پیمانه $m = m_1 m_2 ... m_n$ یکتا است.

اثبات: اگر $I_i = (m_i)$، آنگاه $\bigcap_{i=1}^{n} I_i = (m)$. رابطه $(m_i, m_j) = 1$ ایجاب می‌کند $I_i + I_j = \mathbb{Z}$. حال مطلب با توجه به قضیه فوق به دست می‌آید.

■■■

نتیجه۹-۴

فرض کنید $I_n,\ldots,I_1$ ایده‌آل‌هایی از حلقه R باشند در این صورت تکریختی زیر موجود است

$$\varphi : R/(I_1 \cap \ldots \cap I_n) \to R/I_1 \times \cdots \times R/I_n.$$

اثبات: فرض کنید $I = \bigcap_{i=1}^{n} I_i$ تابع φ را چنین تعریف می‌کنیم:

$$\varphi : R/I \to R/I_1 \times \cdots \times R/I_n$$
$$r + I \mapsto \left(r + I_1, \ldots, r + I_n\right)$$

به وضوح φ یک تکریختی است. حال با استفاده از شرایط داده شده نشان می‌دهیم φ پوشا است. فرض کنید $\left(b_1+I_1,\ldots,b_n+I_n\right)\in R/I_1\times\cdots\times R/I_n$. با توجه به قضیه باقیمانده چینی عنصری مانند $r\in R$ چنان است که برای هر i، $r\overset{I_i}{\equiv}b_i$ ، لذا

$$\varphi(r+I)=\left(r+I_1,\ldots,r+I_n\right)=\left(b_1+I_1,\ldots,b_n+I_n\right).$$

بنابراین φ پوشا است.

■■■

توضیح تاریخی

منابع اولیه نظریه حلقه را می‌توان در دو شاخه زیر جستجو کرد:

(۱) نظریه اعداد: تلاش برای تعمیم قضیه تجزیه اعداد صحیح به عوامل اول (قضیه اساسی حساب)، موجب پیدایش مجموعه اعداد صحیح گاوسی شده که خود تحت عمل‌های جمع و ضرب بسته است.

(۲) هندسه: مطالعه سطوح فضایی که توسط چندجمله‌ای‌ها تعیین می‌شوند ما را با جمع و ضرب چندجمله‌ای‌های چند متغیره درگیر می‌سازند.

د رهر دو حالت ما با ضرب‌هایی سرو کار داریم که خاصیت جابجایی دارند. دیوید هیلبرت ($1862-1943$) حلقه را ابداع نمود و ریچارد ددکیند ($1831-1916$) مطالعه تجریدی این سیستم را آغاز کرد. ددکیند با تمرکز روی ایده‌آل‌ها به مطالعه حوزه‌های صحیح خاصی پرداخت (موسوم به حوزه‌های ددکیند) که در آنها هر ایده‌آلی به صورت یکتا به حاصل‌ضربی از ایده‌آل‌های اول تجزیه می‌شود. ددکیند کارهای بسیار ارزنده‌ای در نظریه حلقه‌ها، گروه‌ها، و میدان‌ها انجام داده است. موریس کلاین ددکیند را کاشف **" جبر مجرد"** نامیده است.

لازم به ذکر است که سال‌ها قبل، در سال 1843، ویلیام رون هامیلتون ($1805-1865$) کواترنیون‌های خود را معرفی نمود، یعنی مجموعه‌ای شامل اعداد مختلط که خود یک حلقه

www.mathematic87.blogfa.com

ناجابجایی است. وی با گسترش حسابان به کواترنیون‌ها امیدوار بود بتواند از آنها در فیزیک استفاده کند.

تمرینها

۱. فرض کنید R حلقه‌ای یکدار باشد. نشان دهید که $a+b=b+a$ از اصل‌های دیگر حلقه به دست می‌آید.

۲. (a) حلقه R را **بولی** گوییم اگر برای هر $x\in R$ داشته باشیم $x^2=x$. نشان دهید که هر حلقه بولی یک حلقه جابجایی است،

(b) فرض کنید R حلقه‌ای یکدار باشد. ثابت کنید اگر به ازای هر $x,y\in R$ داشته باشیم $(xy)^2=x^2y^2$، آنگاه R جابجایی است. با ارائهٔ مثالی نشان دهید که شرط یکدار بودن لازم است،

(c) فرض کنید R حلقه‌ای یکدار باشد بطوریکه برای هر $x,y\in R$ داریم $(xy)^2=(yx)^2$. اگر در R از رابطهٔ $2x=0$ نتیجه شود $x=0$، آنگاه R جابجایی است .

۳. فرض کنید R حلقه‌ای یکدار باشد و $a,b\in R$. نشان دهید که اگر $ab+ba=1$ و $a^3=a$، آنگاه $a^2=1$.

۴. فرض کنید R حلقه‌ای یکدار باشد و $a,b\in R$. نشان دهید $1+ab$ یکال است اگر و فقط اگر $1+ba$ یکال باشد.

۵. ثابت کنید مشخصه یک حوزه صحیح یا صفر است یا عددی اول .

۶. فرض کنید R حلقه‌ای یکدار و $\varphi : R\to S$ یک همریختی حلقه‌ای غیر صفر باشد. اگر $Z(S)=\{0\}$، آنگاه $\varphi(1_R)$ یک حلقهٔ S است.

۷. فرض کنید F یک میدان و $A,B\in \mathrm{M}_n(F)$. اگر $A+B=AB$، آنگاه $AB=BA$.

www.mathematic87.blogfa.com

۸. فرض کنید $R \neq \{0\}$ یک حلقه متناهی و جابجایی باشد که $Z(R) = \{0\}$. نشان دهید R یک میدان است.

۹. فرض کنید R یک حلقه یکدار و $a \in R$ عنصری با بیش از یک معکوس راست باشد. نشان دهید a دارای بینهایت معکوس راست است.

۱۰. فرض کنید p عددی اول باشد.

(a) نشان دهید هر حلقه یکدار از مرتبه p^2 جابجایی است،

(b) حلقه‌هایی ناجابجایی از مرتبه‌های p^2 و p^3 مثال بزنید.

۱۱. $e \in R$ را همانی چپ (راست) گوییم اگر برای هر $a \in R$ داشته باشیم $ea = a$ $(ae = a)$. نشان دهید:

(a) یک همانی چپ ممکن است همانی راست نباشد،

(b) اگر R دارای عنصر همانی چپ یکتای باشد، آنگاه e همانی راست نیز هست.

۱۲. (a) فرض کنید R یک حلقه یکدار باشد. نشان دهید R یک حلقه بخشی است اگر و فقط اگر R دارای ایده‌آل سره چپ نباشد،

(b) اگر R حلقه‌ای باشد که دارای ایده‌آل سره چپ نیست ، نشان دهید یا $R^2 = 0$ یا R یک حلقه بخشی است.

۱۳. کدامیک از حلقه‌های زیر PID می‌باشند.

(a) $\mathbb{Z}$،

(b) $\mathbb{Z}[x]$.

۱۴. فرض کنید R حلقه‌ای جابجایی باشد که $R^2 = R$ (درحالت خاص، R یکدار باشد) . نشان دهید

$$\mathrm{Max}(R) \subseteq \mathrm{Spect}(R).$$

۱۵ فرض کنید P ایده‌آل سره‌ای از حلقه R باشد. نشان دهید شرایط زیر معادلند:

(a) P یک ایده‌آل اول حلقه R است،

www.mathematic87.blogfa.com

(b) برای هردو ایده‌آل B, A از R، اگر $AB \subseteq P$ آنگاه $A \subseteq P$ یا $B \subseteq P$.

۱۶. فرض کنید P ایده‌آل سره‌ای از حلقه یکدار R باشد. نشان دهید شرایط زیر معادلند:

(a) P یک ایده‌آل اول حلقه Rاست،

(b) برای هر $a, b \in R$، اگر $(a)(b) \subseteq P$ آنگاه $a \in P$ یا $b \in P$،

(c) برای هر $a, b \in R$، اگر $aRb \subseteq P$ آنگاه $a \in P$ یا $b \in P$،

(d) برای هردو ایده‌آل چپ B, A از R، اگر $AB \subseteq P$ آنگاه $A \subseteq P$ یا $B \subseteq P$،

(e) برای هردو ایده‌آل راست B, A از R، اگر $AB \subseteq P$ آنگاه $A \subseteq P$ یا $B \subseteq P$.

۱۷. فرض کنید I یک ایده‌آل دلخواه و $P_n, \ldots, P_2, P_1$ ایده‌آل‌های اولی از حلقه جابجایی R باشند. اگر $I \subseteq \bigcup_{i=1}^{n} P_i$، نشان دهید به ازای یک i، $1 \leq i \leq n$، $I \subseteq P_i$.

۱۸.فرض کنید $F \subseteq R$ که F یک میدان نامتناهی و R یک حلقه جابجایی و یکداراست. فرض کنید $I_n, \ldots, I_1, I$ ایده‌آل‌هایی از Rباشد که $I \subseteq \bigcup_{i=1}^{n} I_i$. نشان دهید $1 \leq j \leq n$چنان موجود است $I \subseteq I_j$.

۱۹. فرض کنید R یک حلقه یکدار باشد. نشان دهید هر ایده‌آل $\mathrm{M}_n(R)$ به شکل $\mathrm{M}_n(I)$ است که در آن I یک ایده‌آل حلقه است. در حالت خاص اگر R حلقه‌ای ساده باشد، $\mathrm{M}_n(R)$ نیز ساده است.

۲۰. (a) فرض کنید R یک حلقه جابجایی و یکدار باشد.

اگر $f(x) = \sum_{i=0}^{n} a_i x^i \in Z(R[x])$، ثابت کنید که یک عنصر $b \in R$ چنان موجود است که $ba_0 = ba_1 = \cdots = ba_n = 0$،

(b) نشان دهید که اگر R یک حوزه باشد، حلقه چندجمله‌ای‌ها $R[x]$ نیز یک حوزه است.

۲۱. فرض کنید R یک حلقه جابجایی و یکدار باشد.

www.mathematic87.blogfa.com

(a) اگر $a \in R$ پوچ‌توان باشد، آنگاه $1+a$ معکوس‌پذیر است. از اینجا نتیجه بگیرید که اگر $a \in R$ پوچ‌توان و $u \in R$ معکوس‌پذیر باشد، آنگاه $u+a$ معکوس‌پذیر است،

(b) عنصر $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ معکوس‌پذیر است اگر و فقط اگر a_0 در R معکوس‌پذیر و $a_n, \ldots, a_2, a_1$ عناصر پوچ‌توان R باشند.

۲۲. فرض کنید R یک حلقه باشد. قرار می‌دهیم:

$$R[[x]] = \left\{ a_0, a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots \middle| a_i \in R \right\}.$$

(a) نشان دهید $R[[x]]$ نسبت به اعمال زیر یک حلقه است.

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

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

جاییکه $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

(b) اگر R یک حوزه صحیح باشد، آنگاه $R[[x]]$ نیز حوزه صحیح است،

(c) $f(x) = \sum_{i=0}^{\infty} a_i x^i$ در $R[[x]]$ معکوس‌پذیر است اگر و فقط اگر a_0 در R معکوس‌پذیر باشد.

۲۳. (a) نشان دهید در حلقه بولی یکدار هر ایده‌آل اول ماکزیمال است،

(b) فرض کنید R حلقه‌ای جابجایی و یکدار باشد به طوریکه برای هر $x \in R$، عدد طبیعی $n(x) > 1$ چنان موجود باشد که $x^{n(x)} = x$. نشان دهید هر ایده‌آل اول R یک ایده‌آل ماکزیمال است.

۲۴. مفهوم **زیر میدان** مشابه با مفهوم زیرحلقه قابل تعریف است. میدان F را یک **میدان اول** گوییم اگر دارای تنها یک زیر میدان یعنی F، باشد. زیر میدان F' از F را یک **زیرمیدان اول** گوییم اگر F' یک میدان اول باشد.

www.mathematic87.blogfa.com

(a) اگر F یک میدان و $\{F_\alpha \mid \varphi \in \Lambda\}$ خانواده‌ای از زیر میدان‌های F باشد ، آنگاه $\bigcap_{\alpha\in\Lambda} F_\alpha$ نیز زیر میدانی از F است،

(b) هر میدان F شامل زیر میدان اول یکتایی می‌باشد،

(c) اگر $\mathrm{Char}F = 0$، آنگاه زیر میدان اول F با $\mathbb{Q}$ یکریخت است،

(d) اگر p عددی است اول و $\mathrm{Char}F = p$، آنگاه زیر میدان اول F با $\mathbb{Z}_p$ یکریخت است.

مسائل مبارزه طلب

۱. فرض کنید $R = C[0,1]$ حلقهٔ توابع پیوسته روی بازهٔ $[0,1]$ باشد. نشان دهید ایده‌آل M از R ماکزیمال است اگر وفقط اگر $a \in [0,1]$ چنان موجود باشد که $M = \{f \in R \mid f(a) = 0\}$.

۲. فرض کنید E مجموعهٔ عناصر خودتوان حلقه یکدار R باشد. اگر $e \in R$ و $eE \subseteq E$ و $Ee \subseteq E$، آنگاه $e \in C(R)$.

۳. فرض کنید I ایده‌آلی چپ مینیمالی ازحلقهٔ یکدار R باشد. نشان دهید یا $I^2 = 0$ یا $I = Re$، که $e^2 = e$.

۴. فرض کنید R یک حلقه باشد.

(a) اگر برای هر $a \in R$، $a^3 = a$، آنگاه R حلقه‌ای جابجایی است،

(b) اگر برای هر $a \in R$، $a^4 = a$، آنگاه R حلقه‌ای جابجایی است،

(c) فرض کنید $n \geq 2$. اگر برای هر $a \in R$، $a^n = a$، آنگاه R حلقه‌ای جابجایی است.

۵. حلقهٔ R را **فون نیومن منظم** گوییم اگر برای هر $a \in R$ داشته باشیم $a \in aRa$. نشان دهید R فون نیومن منظم است اگر وفقط اگر $\mathrm{M}_n(R)$ فون نیومن منظم باشد.

www.mathematic87.blogfa.com

منابعی برای مطالعهٔ بیشتر

1. Chatters, A. W., Hajarnavis, C. R. *An Introductory Course in Commutative Algebra*. Oxford University Press, 1998.
2. Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, 1996.
3. Kaplansky, I. *Commutative Rings*. Boston: Allyn and Bacon, Inc., 1970.
4. Lam, T. Y. *A first Course in Noncommutative Rings*. Springer-Verlag, New York, 1991.
5. Lam, T. Y. *Exercises in Module and Rings*. Springer-Verlag, New York, 2007.
6. Lambek, J. *Lectures on Rings and Modules*. Blaisdell,Waltham, 1966.
7. Rotman, J. *Galois Theory*. Springer-Verlag, 1998.

www.mathematic87.blogfa.com

فصل ۱۰

تجزیه در حلقه‌ها

در این فصل می‌خوانید:

۱۰-۱ حلقه چند جمله‌ای‌ها
۱۰-۲ حوزه‌های اقلیدسی
۱۰-۳ میدان کسرها
۱۰-۴ حوزهٔ تجزیهٔ یکتا
۱۰-۵ آزمون‌های تحویل‌ناپذیری

مقدمه

در این فصل به تجزیهٔ عناصر یک حلقهٔ جابجایی و یکدار به عامل‌های تحویل‌ناپذیر (تجزیه‌ناپذیر) می‌پردازیم، همچنین حلقه‌هایی را که در آنها، قضیه‌ای مانند قضیهٔ اساسی حساب برقرار است، مورد مطالعه قرار می‌دهیم.

www.mathematic87.blogfa.com

۱۰-۱ حلقه چند جمله‌ای ها

در سراسر این فصل R نمایانگر یک حلقهٔ جابجایی و یکدار می‌باشد.

در این بخش به تعریف دقیق حلقهٔ چند جمله‌ای‌ها می‌پردازیم وسپس خـواص اساسـی ایـن حلقه را مورد بررسی قرار می‌دهیم.

قضیه۱۰-۱

قرار می دهیم

$P(R) = \{(a_0, a_1, a_2, \ldots) \mid a_n \in R$، فقط تعداد متناهی از a_nها غیر صفر باشند$\}$.

در این‌صورت گزاره‌های زیر برقرارند.

(۱) $P(R)$ همراه با اعمال زیر یک حلقه است.

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$
$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).$$

(۲) نگاشت زیر یک تکریختی است.

$$\varphi : R \to P(R)$$
$$a_0 \mapsto (a_0, 0, 0, \ldots)$$

(۳) اگر $x := (0,1,0,\ldots)$ و حلقهٔ R را با تصویر یکریخت آن یعنی $\varphi(R)$ یکی بگیریم، آنگاه

$$P(R) = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \geq 0\}.$$

اثبات: به‌عنوان تمرین به‌عهدهٔ خواننده واگذار می‌شود.

■■■

www.mathematic87.blogfa.com

تعریف ۱۰-۱

حلقهٔ $P(R)$ را **حلقهٔ چند جمله‌ای ها** روی R گوییم و با نماد $R[x]$ نمایش می‌دهیم.
فرض کنید

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x].$$

اگر $a_n \neq 0$، a_n را **ضریب پیشروی** $f(x)$ می‌خوانیم و گوییم $f(x)$ از **درجه** n است و می‌نویسیم $\deg f(x) = n.$
اگر $a_n = 1$، آنگاه $f(x)$ را یک چند جمله‌ای **تکین** می‌نامیم.

برای راحتی درجهٔ چند جمله‌ای صفر را $-\infty$ تعریف می‌کنیم.

قضیه۱۰-۲

فرض کنید R یک حوزهٔ صحیح باشد. اگر $f(x),\ g(x) \in R[x]$، آنگاه

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

اثبات: اگر $f(x)$ یا $g(x)$ چند جمله‌ای صفر باشند، حکم به‌وضوح برقرار است. حال فرض کنید

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m,$$

که در آن $a_n \neq 0$ و $a_m \neq 0$. دراین‌صورت

$$f(x)\,g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + a_nb_mx^{n+m}.$$

چون R حوزهٔ صحیح است، پس $a_nb_m \neq 0$ و در نتیجه

$$\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x).$$

■■■

www.mathematic87.blogfa.com

نتیجه ۱۰-۱

فرض کنید R یک حوزهٔ صحیح باشد. دراین‌صورت $R[x]$ نیز یک حوزهٔ صحیح است.

اثبات: فرض کنید $f(x),\ g(x) \in R[x]$ و $f(x)g(x) = 0$. در این‌صورت $\deg f(x)g(x) = -\infty$ و در نتیجه $\deg f(x) + \deg g(x) = -\infty$. ازاین‌رو $f(x) = 0$ یا $g(x) = 0$. بنابراین $R[x]$ یک حوزهٔ صحیح است.

■■■

قضیه۱۰-۳ (الگوریتم تقسیم)

فرض کنید $f(x),\ g(x) \in R[x]$، که ضریب پیشروی $g(x)$ یکال است. در این صورت چند جمله‌ای‌های یکتای $q(x),\ r(x) \in R[x]$ وجود دارند که

$$f(x) = g(x)q(x) + r(x) \quad \text{و} \quad \deg r(x) < \deg g(x)$$

اثبات (وجود): فرض کنید

$$S = \{f(x) - g(x)h(x) \mid h(x) \in R[x]\}.$$

به‌وضوح $S \neq \varnothing$، زیرا $f(x) \in S$. اگر $0 \in S$، آنگاه چند جمله‌ای $h(x) \in R(x)$ وجود دارد بطوریکه

$$f(x) - g(x)h(x) = 0$$

و لذا $f(x) = g(x)h(x)$. در نتیجه $q(x) = h(x)$ و $r(x) = 0$ در شرایط قضیه صدق می‌کند. حال فرض کنید $0 \notin S$. در این صورت عناصر S از درجهٔ نامنفی بوده و لذا طبق اصل خوش ترتیبی S دارای عنصری با کوچکترین درجه مانند $r(x)$ خواهد بود. بنابراین $q(x) \in R[x]$ چنان موجود است که

$$r(x) = f(x) - g(x)q(x),$$

حال فرض کنید (فرض خلف) $\deg r(x) \geq \deg g(x)$. اگر

$$g(x) = a_0 + a_1x + \cdots + a_nx^n,$$
$$r(x) = b_0 + b_1x + \cdots + b_mx^m,$$

که در آن $a_n \neq 0,\ b_m \neq 0$، آنگاه با توجه به اینکه $m \geq n$ خواهیم داشت:

$$\alpha(x) := r(x) - (b_m / a_n)x^{m-n}g(x) = f(x) - g(x)h(x) - (b_m / a_n)x^{m-n}g(x)$$
$$= f(x) - g(x)(h(x) - (b_m / a_n)x^{m-n}) \in S.$$

اما $\deg \alpha(x) < \deg r(x)$، که متناقض با انتخاب $r(x)$ است. ازاین‌رو $\deg r(x) < \deg g(x)$، همانگونه که لازم بود.

(یکتایی): فرض کنید

$$f(x) = g(x)q(x) + r(x)\text{، } \deg r(x) < \deg g(x)$$

$$f(x) = g(x)q_1(x) + r_1(x) \text{ ،} \deg r_1(x) < \deg g(x)$$

در این صورت $r(x) - r_1(x) = g(x)(q_1(x) - q(x))$. چون ضریب پیشروی $g(x)$ یکال است، داریم

$$\deg(q_1(x) - q(x)) = \deg(r(x) - r_1(x)) - \deg g(x) < 0.$$

ازاین‌رو $\deg(q_1(x) - q(x)) = -\infty$ و لذا $q_1(x) - q(x) = 0$ و در نتیجه $r_1(x) - r(x) = 0$. بدین ترتیب $q_1(x) = q(x)$ و $r_1(x) = r(x)$.

■■■

تعریف ۱۰-۲

فرض کنید R زیرحلقه‌ای از حلقهٔ جابجایی و یکدار S باشد. فرض کنید $f(x) \in R[x]$. عنصر $u \in S$ را یک **ریشه** از چند جمله‌ای $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ گوییم، اگر

$$f(u) := a_0 + a_1u + \cdots + a_nu^n = 0.$$

www.mathematic87.blogfa.com

نتیجه ۱۰-۲

فرض کنید R یک حوزهٔ صحیح $f(x) \in R[x]$ و $a \in R$. در این‌صورت

$$f(a) = 0 \quad \Leftrightarrow \quad (x-a) \text{ عاملی از } f(x) \text{ باشد.}$$

اثبات ($\Leftarrow$): فرض کنید $f(a) = 0$. طبق قضیه قبل (الگوریتم تقسیم) چند جمله‌ای‌های $q(x), r(x) \in R[x]$ به‌گونه‌ای موجوداند که $f(x) = (x-a)q(x) + r(x)$ و $\deg r(x) = 0$. بنابراین $r(x) = b \in R$. از طرفی چون $r(a) = 0$، پس $b = 0$. در نتیجه $f(x) = (x-a)q(x)$.

($\Rightarrow$): حال فرض کنید $(x-a)$ عاملی از $f(x)$ باشد. در این‌صورت چند جمله‌ای $q(x)$ چنان موجود است که $f(x) = (x-a)q(x)$. بنابراین $f(a) = 0$.

■■■

نتیجه ۱۰-۳

فرض کنید R یک حوزهٔ صحیح $f(x) \in R[x]$ و $\deg f(x) = n \geq 0$. در این‌صورت $f(x)$ دارای حداکثر n ریشهٔ متمایز در R است.

اثبات: استقرا روی n به‌کار می‌بریم. اگر $n = 0$، آنگاه $f(x) = c \neq 0$ و لذا $f(x)$ ریشه‌ای در R ندارد. حال فرض کنید $n > 0$. اگر $f(x)$ هیچ ریشه‌ای در R نداشته باشد، مطلب اثبات شده است. پس فرض کنید $f(x)$ دارای ریشه‌ای مانند a در R باشد. با توجه به نتیجهٔ قبل چند جمله‌ای $q(x) \in R[x]$ به‌گونه‌ای موجود است که $f(x) = (x-a)q(x)$. اگر $b \in R$ ریشه‌ای از $f(x)$ بجز a باشد، آنگاه

$$f(b) = (b-a)q(b) = 0.$$

www.mathematic87.blogfa.com

بنابراین با توجه به اینکه $b-a\neq 0$، خواهیم داشت $q(b)=0$، یعنی b ریشه‌ای از $q(x)$ می‌باشد. از طرفی بنابر فرض استقرا $q(x)$ دارای حداکثر $n-1$ ریشهٔ متمایز در R است. بنابراین نتیجه می‌شود که $f(x)$ دارای حداکثر n ریشهٔ متمایز در R است.

■■■

یکی از مهمترین ویژگی‌های $\mathbb{C}$، میدان اعداد مختلط، که آنرا بدون اثبات بیان خواهیم کرد، برقراری قضیهٔ زیر است.

قضیه۱۰-۴ (قضیهٔ اساسی جبر)

هر چندجمله‌ای ناثابت از $\mathbb{C}[x]$ دارای ریشه‌ای در $\mathbb{C}$ است.

اثبات این قضیه، برخلاف نامش، جبری نیست. همهٔ اثبات‌های معروف درگیر تکنیک‌های آنالیزی یا توپولوژیکی می‌باشند. برای دیدن اثباتی از این قضیه می‌توان صفحهٔ ۲۲۲ منبع زیر را ملاحظه نمود.

رودین، والتر. **اصول آنالیز ریاضی**. ترجمهٔ عالم زاده، علی اکبر. انتشارات علمی و فنی (۱۳۶۲).

این بخش را با معرفی حلقهٔ چند جمله‌ای‌های n متغیره (مجهول) روی حلقهٔ R به پایان می‌رسانیم.

تعریف ۱۰-۳

حلقهٔ چندجمله‌ای‌های n متغیره روی R به استقرا به صورت زیر تعریف می‌شود.

$$R[x_1,\ldots,x_n]=(R[x_1,\ldots,x_{n-1}])[x_n].$$

۱۰-۲ حوزه‌های اقلیدسی

در این فصل حلقه‌هایی را که در آنها الگوریتم تقسیم برقرار است، مورد مطالعهٔ قرار می‌دهیم.

www.mathematic87.blogfa.com

تعریف ۱۰-۴

فرض کنید R یک حلقه باشند و $\mathbb{N}_0$ مجموعهٔ اعداد صحیح نامنفی باشد. R را یک **حلقهٔ اقلیدسی** (به اختصار ER) نامیم اگر تابعی مانند $\upsilon : R-\{0\} \to \mathbb{N}_0$ چنان موجود باشد که

(۱) به ازای هر $a,b \in R$، به‌قسمی که $ab \neq 0$، $\upsilon(a) \leq \upsilon(ab)$،

(۲) به ازای هر $a,b \in R$، به‌قسمی که $b \neq 0$ ، عناصر $q,r \in R$، وجود داشته باشند به‌طوری‌که، $a = bq + r$، که در این تساوی $r = 0$ یا $\upsilon(r) < \upsilon(b)$.

تابع υ را تابع **اقلیدسی** در R می‌نامند. یک حلقهٔ اقلیدسی که یک حوزهٔ صحیح باشد را یک **حوزهٔ اقلیدسی**(به اختصار ED) نامیم.

دلیل نام‌گذاری این حلقه‌ها به حلقه‌های اقلیدسی، کارآمد بودن الگوریتم اقلیدس، برای یافتن بزرگترین مقسوم‌علیه مشترک دو عنصر، می‌باشد(تمرین۱۳).

مثال ۱: میدان F با $\upsilon(x) = 1$ یک حوزهٔ اقلیدسی است.

■

مثال ۲: حلقهٔ $\mathbb{Z}$ با $\upsilon(n) = |n|$ یک حوزهٔ اقلیدسی است.

■

مثال ۳: فرض کنید F یک میدان باشد. دراین‌صورت $F[x]$ با $\upsilon(f(x)) = \deg f(x)$ یک حوزهٔ اقلیدسی است.

■

مثال ۴: حلقهٔ اعداد صحیح گاوسی، $\mathbb{Z}[i]$، یک حوزهٔ اقلیدسی است.

حل: تعریف می‌کنیم:

$$\upsilon : \mathbb{Z}[i] - \{0\} \to \mathbb{N}_0$$
$$\upsilon(a+bi) = \mid a+bi \mid^2 = a^2 + b^2.$$

فرض کنید $z = a+bi$، $w = c+di$، که $w \neq 0$، عناصری از $\mathbb{Z}[i]$ باشند. دراین‌صورت $\upsilon(w) \geq 1$ و در نتیجه

$$\upsilon(z) \leq \upsilon(z)\upsilon(w) = \mid z \mid^2 \mid w \mid^2 = \mid zw \mid^2 = \upsilon(zw).$$

z و w را به‌عنوان عناصری از $\mathbb{Q}(i) = \{p+qi \mid p,q \in \mathbb{Q}\}$ در نظر می‌گیریم. مشاهده می‌کنیم که

$$zw^{-1} = (a+bi)\frac{c-di}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bd-ad}{c^2+d^2}$$
$$= (m_1+s) + (m_2+t)i = (m_1+m_2i) + (s+ti),$$

که در این‌جا اعداد صحیح m_1, m_2 و اعداد گویای s,t به‌گونه‌ای انتخاب می‌شوند که $|s| \leq 1/2, \quad |t| \leq 1/2$. بنابراین

$$z = zw^{-1}w = (m_1+m_2i)w + (s+ti)w = qw + r,$$

جاییکه $q = m_1 + m_2i$ و $r = (s+ti)w$. چون z و qw در $\mathbb{Z}[i]$ قرار دارند، پس r نیز در $\mathbb{Z}[i]$ است. اگر $r \neq 0$ باشد، آنگاه

$$\upsilon(r) = \upsilon(w)\upsilon(s+ti) \leq \upsilon(w)(s^2+t^2) \leq \upsilon(w)(1/4+1/4) = (1/2)\upsilon(w) < \upsilon(w).$$

بدین ترتیب نشان داده‌ایم که $\mathbb{Z}[i]$ یک حوزهٔ اقلیدسی است.

■

قضیه ۱۰-۵

(۱) هرحلقهٔ اقلیدسی یک حلقهٔ ایده‌آل اصلی است. به‌عبارت دیگر $ER \Rightarrow PIR$،

(۲) هر حوزهٔ اقلیدسی یک حوزهٔ ایده‌آل اصلی است. به‌عبارت دیگر $ED \Rightarrow PID$.

www.mathematic87.blogfa.com

اثبات (۱): فرض کنید I ناصفری از حلقهٔ R باشد. نشان می‌دهیم I یک ایده‌آل اصلی است. قرار می‌دهیم:

$$S = \{\upsilon(x) \mid x \neq 0, x \in I\}.$$

فرض کنید $\upsilon(a)$ عنصر مینیمال باشد. ادعا می‌کنیم $I = (a)$. به‌وضوح $(a) \subseteq I$. حال فرض کنید $0 \neq b \in I$. در این صورت عناصر $q, r \in R$ چنان موجودند که $b = aq + r$ و در این تساوی $r = 0$ یا $\upsilon(r) < \upsilon(a)$. با توجه به مینیمال بودن $\upsilon(a)$ و اینکه $r = b - aq \in I$، رابطهٔ $\upsilon(r) < \upsilon(a)$ برقرار نمی باشد ولذا $r = 0$ و $b = aq \in (a)$. یعنی $I = (a)$، همانگونه که خواسته شده بود.

(۲): به آسانی از (۱) نتیجه می‌شود.

■■■

۱۰-۳ میدان کسرها

در این بخش، طرز ساخت اعداد گویا از طریق اعداد صحیح را تعمیم خواهیم داد.

قضیه ۱۰-۶

فرض کنید R یک حوزهٔ صحیح باشد و $S = R \setminus \{0\}$. در این صورت رابطه زیر یک رابطه هم ارزی روی $R \times S$ است

$$(r, s) \sim (r', s') \Leftrightarrow rs' = sr'.$$

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

نمادگذاری: فرض کنید R یک حوزهٔ صحیح باشد. کلاس هم ارزی $(r, s) \in R \times S$ را با r / s نمایش داده و قرار می‌دهیم:

$$F = \{r / s | r \in R, s \in S\}.$$

www.mathematic87.blogfa.com

قضیه۱۰-۷

فرض کنید R یک حوزهٔ صحیح باشد و $S = R \setminus \{0\}$. در این صورت F همراه با اعمال جمع و ضرب زیر یک میدان است.

$$r/s + r'/s' = (rs' + sr')/ss',$$
$$(r/s)(r'/s') = (rr'/ss').$$

اثبات: نشان می‌دهیم که عمل جمع خوش تعریف است. فرض کنید $r/s = r_1/s_1$ و $r'/s' = r_1'/s_1'$. دراین‌صورت

$$rs_1 = sr_1,$$
$$r's_1' = s'r_1'.$$

با ضرب معادله اول در $s's_1'$ و معادله دوم در ss_1 و جمع آنها داریم:

$$(rs' + sr')s_1s_1' = (r_1s_1' + s_1r_1')ss'.$$

بنابراین $(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s'$. یعنی عمل جمع خوش تعریف است. به طریق مشابه می‌توان دید که عمل ضرب نیز خوش تعریف است. برای هر $s \in S$ عنصر $0/s = 0/1$ عنصر همانی جمعی F و $s/s = 1/1$ عنصر همانی عمل ضرب F است. جابجایی بودن F به‌وضوح از جابجایی بودن R نتیجه می‌شود. فرض کنید r/s عنصر غیر صفری از F باشد، در این صورت $r \neq 0$، لذا $r \in S$. بنابراین $s/r \in F$ و $(r/s)(s/r) = 1$. یعنی r/s معکوس‌پذیر است. تکمیل بقیهٔ اثبات بعنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱۰-۵

اگر R یک حوزهٔ صحیح باشد و $S = R \setminus \{0\}$، F را **میدان کسرهای** R می‌نامند.

www.mathematic87.blogfa.com

مثال۵: میدان کسرهای حلقهٔ اعداد صحیح $\mathbb{Z}$، دقیقاً میدان اعداد گویای $\mathbb{Q}$ است.

■

مثال۶: فرض کنید R یک حوزهٔ صحیح باشد. میدان کسرهای حلقهٔ چند جمله‌ای‌های $R[x]$ را با $R(x)$ نمایش داده و آنرا میدان **توابع گویا** از متغیر (مجهول) x روی حلقهٔ R نامیم. در حقیقت

$$R(x)=\{f(x)/g(x)\mid f(x),g(x)\in R[x],g\neq 0\}.$$

در حالت کلی میدان کسرهای حلقهٔ چند جمله‌ای‌های $R[x_1,\ldots,x_n]$ را با $R(x_1,\ldots,x_n)$ نمایش داده و آنرا میدان **توابع گویا** ازمتغیرهای (مجهول‌های) $x_1,\ldots,x_n$ روی حلقهٔ R نامیم. در حقیقت

$$R(x_1,\ldots,x_n)=\{f(x_1,\ldots,x_n)/g(x_1,\ldots,x_n)\mid f(x),g(x)\in R[x_1,\ldots,x_n],g\neq 0\}.$$

■

قضیه۱۰-۸

فرض کنید R یک حوزهٔ صحیح باشد و $S=R\setminus\{0\}$. در این‌صورت نگاشت $\varphi:R\to F$ با ضابطه $\varphi(r)=r/1$ یک تکریختی است. به عبارت دیگر هر حوزهٔ صحیح قابل نشاندن در میدان کسرهای خود است.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

۱۰-۴ حوزهٔ تجزیهٔ یکتا

www.mathematic87.blogfa.com

قضیهٔ اساسی حساب بیان می‌کند که هر عدد طبیعی $n > 1$ را می‌توان به‌صورت یکتایی به حاصل‌ضرب اعداد اول تجزیه کرد. مشابهٔ این قضیه را به آسانی می‌توان برای حلقهٔ اعداد صحیح، $\mathbb{Z}$، تعمیم داد. در این بخش حلقه‌هایی را بررسی می‌کنیم که قضیه‌ای مشابه با قضیهٔ اساسی حساب در آنها برقرار است.

تعریف ۱۰-۶

(۱) فرض کنید $a,b \in R$. اگر $x \in R$ وجود داشته باشد به‌طوریکه $ax = b$، گوییم a **عاد می‌کند** b و می‌نویسیم $a \mid b$،

(۲) عنصر غیر یکال و غیر صفر $c \in R$ را **تحویل‌ناپذیر** (تجزیه‌ناپذیر) گوییم، اگر

$$c = ab \Rightarrow \text{ یکال } a \text{ یا } b \text{ یکال}$$

(۳) عنصر غیر یکال و غیر صفر $p \in R$ را **اول** گوییم، اگر

$$p \mid ab \Rightarrow \ p \mid b \text{ یا } p \mid a$$

(۴) دوعنصر a و b از حلقهٔ R را **شریک** (وابسته) گوییم و با نماد $a \sim b$ نمایش می‌دهیم، اگر عنصر یکال $u \in R$ چنان باشد که $a = bu$.

تذکر: تعریف تحویل‌ناپذیر مشابه با تعریف عدد اول برای اعداد صحیح می‌باشد. اما مرسوم است که نام تحویل‌ناپذیر (تجزیه ناپذیر)، برای این مفهوم در نظر گرفته شود.

گزاره ۱۰-۱

(۱) رابطهٔ شریک بودن یک رابطهٔ هم ارزی است،

(۲) اگر $a,b \in R$ شریک باشند، آنگاه $(a) = (b)$. هرگاه R یک حوزهٔ صحیح باشد، وارون این مطلب نیز درست است.

اثبات: به‌عنوان تمرین به عهدهٔ خواننده واگذار می‌شود.

■■■

گزاره ۱۰-۲

فرض کنید R یک حوزهٔ صحیح باشد. در این‌صورت

(۱) هر عنصر اول R تحویل‌ناپذیر است،

(۲) هرگاه R یک حوزهٔ ایده‌آل اصلی باشد و $p \in R$، آنگاه p اول است اگر و فقط اگر p تحویل‌ناپذیر باشد.

اثبات: به‌عنوان تمرین به عهدهٔ خواننده واگذار می‌شود.

■■■

تذکر: عکس قسمت (۱) گزارهٔ بالا برقرار نمی باشد. یعنی یک عنصر تحویل‌ناپذیر لزوماً اول نمی‌باشد (تمرین۹ ملاحظه شود).

تعریف ۱۰-۷

حوزهٔ صحیح R را یک **حوزهٔ تجزیهٔ یکتا** (به اختصار UFD) نامیم هرگاه

(۱) (وجود تجزیه) هر عنصر غیر صفر و غیر یکال $a \in R$ را بتوان به‌صورت $a = a_1 a_2 \dots a_n$ نوشت که در آن a_iها عناصر تحویل‌ناپذیری از R می‌باشند. به‌عبارت دیگر $a \in R$ را بتوان به‌صورت حاصل‌ضربی از عوامل تحویل‌ناپذیر تجزیه کرد.

(۲) (یکتایی تجزیه) اگر $a = b_1 b_2 \dots b_n = c_1 c_2 \dots c_m$، که b_iها و c_iها تحویل‌ناپذیرند، آنگاه $n = m$ و c_i را بتوان طوری تجدید شماره‌گذاری کرد که هر b_i و c_i شریک باشند.

تعریف ۱۰-۸

گوییم حلقهٔ R در شرط ACC **(شرط زنجیر صعودی)** روی ایده‌آل‌هایش صدق می‌کند. اگر هر زنجیر صعودی از ایده‌آل‌هایش ایستا باشد. به عبارت دیگر اگر $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ یک زنجیر صعودی از ایده‌آل‌های R باشد، آنگاه $k \in \mathbb{N}$ چنان موجود باشد که $I_k = I_{k+1} = I_{k+2} = \dots$.

قضیه۱۰-۹

شرایط زیر روی حلقهٔ R معادلند.

(۱) R در شرط ACC روی ایده‌آل‌هایش صدق می‌کند،

(۲) هر خانواده غیر تهی از ایده‌آل‌های R دارای عنصر ماکزیمال است،

(۳) هر ایده‌آل R متناهی مولد است.

اثبات (۲) $\Rightarrow$**(۱)**: فرض کنید Ω یک خانواده غیر تهی از ایده‌آل‌های R باشد که دارای عنصر ماکزیمال نیست. اگر $I_1 \in \Omega$، آنگاه چون Ω دارای عنصر ماکزیمال نیست، پس $I_2 \in \Omega$ چنان موجود است که $I_1 \subsetneq I_2$. دوباره چون Ω دارای عنصر ماکزیمال نیست، پس $I_3 \in \Omega$ چنان موجود است که $I_1 \subsetneq I_2 \subsetneq I_3$. با ادامه این روند زنجیر صعودی ناایستای زیر را خواهیم داشت.

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_t \subsetneq \cdots.$$

(۳) $\Rightarrow$**(۲)**: فرض کنید I ایده‌آلی از R باشد و

$$\Omega = \{J \mid J \subseteq I \text{ و } J \text{ یک ایده‌آل متناهی مولد حلقهٔ } R\}.$$

چون $(0) \in \Omega$، لذا $\Omega \neq \varnothing$. بنابراین طبق فرض Ω دارای عنصر ماکزیمال است. فرض کنید J عنصر ماکزیمال Ω باشد. اگر $x \in I$، آنگاه $J + (x) \in \Omega$ و لذا با توجه به ماکزیمال بودن J خواهیم داشت $J + (x) = J$. بنابراین $x \in J$ و در نتیجه $J = I$. ازاین‌رو I متناهی مولد است.

(۱) $\Rightarrow$**(۳)**: فرض کنید $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ یک زنجیر صعودی از ایده‌آل‌های R باشد. قرار می‌دهیم $I = \bigcup_{k=1}^{\infty} I_k$. به‌وضوح I یک ایده‌آل R است. چون I متناهی مولد است لذا عناصر $x_i \in I_{k_i}\ (1 \leq i \leq n)$ به‌گونه‌ای موجودند که $I = (x_1, x_2, \ldots, x_n)$. فرض کنید

www.mathematic87.blogfa.com

$(1 \le i \le n)\, x_i \in I_{k_i}$. اگر $k = \max\{k_i\}_{i=1}^{n}$، آنگاه با توجه به صعودی بودن زنجیر خواهیم داشت، $I \subseteq I_k$ و لذا

$$I = I_k = I_{k+1} = I_{k+2} = \cdots.$$

■■■

قضیه۱۰-۱۰

هر حوزهٔ ایده‌آل اصلی یک حوزهٔ تجزیهٔ یکتاست. به‌عبارت دیگر $PID \Rightarrow UFD$.

اثبات: فرض کنید R یک حوزهٔ ایده‌آل اصلی باشد.

(وجود تجزیه): فرض کنید S مجموعهٔ عناصر غیر صفر و غیر یکال از R باشد که نتوان آنها را به‌صورت حاصل‌ضرب تعداد متناهی از عناصر تحویل‌ناپذیر نوشت. اگر $S = \varnothing$، مسئله حل است. حال فرض کنید $S \neq \varnothing$. قرار می‌دهیم:

$$\Omega = \{(x) \mid x \in S\}.$$

$\Omega \neq \varnothing$، چون $S \neq \varnothing$. بنابراین طبق قضیهٔ قبل Ω دارای عنصر ماکزیمالی مانند (a) خواهد بود. چون $a \in S$، لذا a تحویل‌ناپذیر نبوده و ازاین‌رو $a = bc$، که در اینجا b, c غیر یکال می‌باشند. اگر $(a) = (b)$، آنگاه عنصر یکال $u \in R$ چنان موجود است که $a = bu$. ازاین‌رو $bc = bu$ و در نتیجه $c = u$، که تناقض است. بنابراین $(b) \subsetneq (a)$. به‌طریق مشابه می‌توان نشان داد که $(a) \subsetneq (c)$. درنتیجه با توجه به ماکزیمال بودن $a \in S$، داریم $b, c \notin S$. لذا عناصر تحویل‌ناپذیر $b_1, b_2, \ldots, b_m$ و $c_1, c_2, \ldots, c_m$ چنان موجودند که $b = b_1 b_2 \ldots b_m$ و $c = c_1 c_2 \ldots c_n$. بنابراین

$$a = bc = b_1 b_2 \ldots b_m c_1 c_2 \ldots c_n.$$

یعنی a را می‌توان به‌صورت حاصل‌ضرب تعداد متناهی از عناصر تحویل‌ناپذیر نوشت، که متناقض با انتخاب a است. ازاین‌رو $S = \varnothing$ و بدین ترتیب وجود تجزیه اثبات شده است.

(یکتایی تجزیه): حال فرض کنید $a = b_1 b_2 \ldots b_n = c_1 c_2 \ldots c_m$، که b_iها و c_iها تحویل‌ناپذیرند. دراین‌صورت $b_1 \mid c_1 c_2 \ldots c_m$. با شماره‌گذاری مجدد c_iها (در صورت لزوم)،

www.mathematic87.blogfa.com

می‌توان فرض کرد $b_1 \mid c_1$. از آنجا که b_1 و c_1 تحویل‌ناپذیر هستند، b_1 و c_1 باید شریک باشند، یعنی $c_1 = b_1u_1$ که u_1 یکالی از R است. بنابراین با توجه به ناصفر بودن b_1 خواهیم داشت

$$b_2b_3 \dots b_n = (u_1c_2)c_3 \dots c_m.$$

با ادامهٔ این روند به تساوی زیر می‌رسیم

$$1 = u_1 \dots u_nc_{n+1} \dots c_m.$$

چون c_iها تحویل‌ناپذیرند، نتیجه می‌شود که $m = n$ و با شماره‌گذاری مجدد (در صورت لزوم) برای هر i، b_i شریک c_i است. بدین ترتیب یکتایی تجزیه اثبات شده است.

■■■

قضیه‌های ۵ و ۱۰ را می‌توان به‌صورت زیر، که بخاطر سپردن آن آسان است، خلاصه شود.

$$ED \Rightarrow PID \Rightarrow UFD.$$

تعریف ۱۰-۹

فرض کنید $a_1, a_2, \dots, a_n \in R$. عنصر $d \in R$ را **بزرگترین مقسوم‌علیه مشترک** عناصر $a_1, a_2, \dots, a_n$ گوییم و با نماد $d = (a_1, a_2, \dots, a_n)$ نمایش می‌دهیم، اگر

(۱) به ازای هر i، $d \mid a_i$،

(۲) به ازای هر i نتیجه دهد $c \mid d$ $c \mid a_i$.

تعریف ۱۰-۱۰

عناصر $a_1, a_2, \dots, a_n$ از حلقهٔ R را **نسبت به هم اول** گوییم اگر 1 بزرگترین مقسوم‌علیه مشترک عناصر $a_1, a_2, \dots, a_n$ باشد.

www.mathematic87.blogfa.com

- **تذکر:** بزرگترین مقسوم‌علیه مشترک همیشه موجود نیست. همچنین بزرگترین مقسوم‌علیه مشترک ممکن است یکتا نباشد. اما می‌توان نشان داد که مقسوم‌علیه مشترک در حد شریک بودن یکتاست (تمرین ۱۲).

گزارهٔ زیر نشان می‌دهد که در یک حلقهٔ ایده‌آل اصلی بزرگترین مقسوم‌علیه مشترک موجود است. در تمرین ۸ از خواننده خواسته شده که نشان دهد در یک حلقهٔ حوزهٔ تجزیهٔ یکتا نیز بزرگترین مقسوم‌علیه مشترک موجود است.

گزاره ۱۰-۳

فرض کنید $a_1,\dots,a_n \in R$.

(۱) اگر $r_1,\dots,r_n \in R$ و $d = r_1a_1 + \cdots + r_na_n$، آنگاه

$$(a) = (a_1) + \cdots + (a_n) \Leftrightarrow d = (a_1,\dots,a_n).$$

(۲) اگر R یک حلقهٔ ایده‌آل اصلی باشد، آنگاه بزرگترین مقسوم علیه مشترک عناصر $a_1, a_2,\dots,a_n$ موجود بوده و به‌صورت $d = r_1a_1 + \cdots + r_na_n$، که $r_i \in R$،

اثبات (۱) $(\Leftarrow)$: به‌وضوح $(a_1) + \cdots + (a_n) \subseteq (d)$. حال فرض کنید $s_1a_1 + \cdots + s_na_n$ عنصر دلخواهی از $(a_1) + \cdots + (a_n)$باشد. در این‌صورت با توجه به‌اینکه $d \mid a_i$، خواهیم داشت $d \mid s_1a_1 + \cdots s_na_n$ و لذا $s_1a_1 + \cdots + s_na_n \in (d)$.

$(\Rightarrow)$: به‌وضوح $d \mid a_i$، به ازای هر i. حال فرض کنید $c \mid a_i$ به ازای هر i. در این‌صورت با توجه به اینکه $d = r_1a_1 + \cdots + r_na_n$، داریم $c \mid d$. بنابراین طبق تعریف $d = (a_1,\dots,a_n)$.

(۲): چون R یک حلقهٔ ایده‌آل اصلی باشد، پس عنصر $d \in R$ به‌گونه‌ای موجود است که $(d) = (a_1) + \cdots + (a_n)$. از این‌روطبق قسمت (۱)، $d = (a_1,\dots,a_n)$.

■■■

www.mathematic87.blogfa.com

تعریف ۱۰-۱۱

فرض کنید $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. **محتوای** f که با $C(f)$ نمایش داده می‌شود، بزرگترین مقسوم‌علیه مشترک ضرایب $a_1,a_2,\ldots,a_n$ تعریف می‌شود. به‌عبارت دیگر $C(f)\sim(a_1,a_2,\ldots,a_n)$. چند جمله‌ای f را **اولیه** گوییم اگر $C(f)\sim 1$.

لازم به ذکر است که $C(f)$ یکتا نیست، زیرا بزرگترین مقسوم‌علیه مشترک یکتا نمی‌باشد. ولی هر دو بزرگترین مقسوم‌علیه مشترک الزاماً شریک‌اند و هر شریک از یک محتوای f خود یک محتوا برای f است. پس $C(f)$ در حد یکال یکتا است.

گزاره ۱۰-۴

فرض کنید $f(x)\in R[x]$ و $a\in R$. در این‌صورت

(۱) چند جمله‌ای f را می‌توان به‌صورت $f=C(f)f_1$ نوشت که f_1 یک چند جمله‌ای اولیه است.

(۲) $C(af)\sim aC(f)$.

اثبات: به‌عنوان تمرین به عهدهٔ خواننده واگذار می‌شود

■■■

لم ۱۰-۱۲ (لم گاوس)

فرض کنید R یک حوزهٔ تجزیهٔ یکتا باشد و $f,g\in R[x]$.
دراین‌صورت $C(fg)\sim C(f)C(g)$. بخصوص، اگر f,g دو چند جمله‌ای اولیه باشند، آنگاه fg نیز یک چندجمله‌ای اولیه است.

اثبات: فرض کنید $f=C(f)f_1$ و $g=C(g)g_1$ ، که f_1 و g_1 اولیه‌اند. در این‌صورت

www.mathematic87.blogfa.com

$$C(fg) = C(C(f)f_1C(g)g_1) \sim C(f)C(g)C(f_1g_1)$$

ازاین‌رو کافی است ثابت شود که f_1g_1 اولیه است. اگر $f_1 = \sum_{i=0}^{m} a_i x^i$ و $g_1 = \sum_{i=0}^{n} b_j x^j$، آنگاه $f_1g_1 = \sum_{k=0}^{m+n} c_k x^k$، که $c_k = \sum_{i+j=k} a_i b_j$. هرگاه f_1g_1 اولیه نباشد، آنگاه یک عنصر تحویل‌ناپذیر مانند $p \in R$ هست بطوریکه $p \mid c_k$ به ازای هر k. چون $C(f_1)$ یک یکال است، $p \nmid C(f_1)$، در نتیجه، کوچکترین عدد صحیح مانند s هست بطوریکه $p \mid a_i$ به ازای هر i، $i < s$ و $p \nmid a_s$. همین‌طور، کوچکترین عدد صحیح t موجود است بطوریکه $p \mid b_j$ برای هر j ، $j < t$ و $p \nmid b_t$. از طرفی

$$p \mid c_{s+t} = a_0b_{s+t} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0.$$

از این‌رو $p \mid a_sb_t$. چون هر عنصر تحویل‌ناپذیر در R اول است، $p \mid a_s$ یا $p \mid b_t$،که یک تناقض است. بنابراین f_1g_1 اولیه است.

■■■

لم ۱۰-۲

فرض کنید R یک حوزهٔ تجزیهٔ یکتا با میدان کسرهای F بوده و f و g چندجمله‌ای‌های اولیه در $R[x]$ باشند. در این‌صورت

f و g در $R[x]$ شریک‌اند $\Leftrightarrow$ f و g در $F[x]$ شریک باشند.

اثبات ($\Leftarrow$) : به‌وضوح برقرار است.

($\Rightarrow$) : فرض کنید f و g در $F[x]$ شریک باشند. در این‌صورت عنصر یکال $u \in F[x]$ چنان موجود است که $f = gu$. اما u باید یک یکال از F باشد ولذا $u = a/b$ که $a, b \in R$ و $b \neq 0$. بنابراین $bf = ag$ و در نتیجه با توجه به یکال بودن $C(f)$ و $C(g)$ در R، خواهیم داشت.

www.mathematic87.blogfa.com

$$b \sim bC(f) \sim C(bf) = C(ag) \sim aC(g) \sim a.$$

بنابراین، به ازای یکالی چون $v \in R$ ، $a = bv$ و لذا $bf = ag = bvg$. در نتیجه $f = vg$ و لذا f و g در $R[x]$ شریک‌اند.

■■■

لم ۱۰-۳

فرض کنید R یک حوزهٔ تجزیهٔ یکتا با میدان کسرهای F بوده و f یک چندجمله‌ای غیر ثابت در $R[x]$ باشد. در این‌صورت

f در $R[x]$ تحویل‌ناپذیر است $\Leftrightarrow$ f در $F[x]$ تحویل‌ناپذیر و در $R[x]$ اولیه باشد

اثبات ($\Rightarrow$): اگر $f = gh$ ، که در آن $g,h \in R[x]$، آنگاه چون f در $F[x]$ تحویل‌ناپذیر است، یکی از g یا h (مثلاً g) باید در $F[x]$ یکال باشد. ازاین‌رو $g(x)$ باید یک چندجمله‌ای ثابت باشد و لذا $g \in R$. چون f اولیه است و $C(f) = C(gh) \sim gC(h)$، پس g باید در R و در نتیجه در $R[x]$ یکال باشد. بنابراین f در $R[x]$ تحویل‌ناپذیر است.

($\Leftarrow$): فرض کنید f در $R[x]$ تحویل‌ناپذیر است. چون $f = C(f)f_1$ که f_1 اولیه است، $C(f)$ باید در $R[x]$ و در نتیجه در R یکال باشد. بنابراین f اولیه است. حال فرض کنید (فرض خلف) که f در $F[x]$ تحویل‌ناپذیر نباشد. ازاین‌رو $f = gh$ که $g,h \in F[x]$ و $\deg f \geq 1$ ، $\deg g \geq 1$. فرض کنید $g = (a/b)g_1$ و $h = (c/d)h_1$ ، که $g_1, h_1 \in R[x]$ اولیه‌اند و $a,b,c,d \in R$. در این‌صورت $gh = (ac/bd)g_1h_1$ و در نتیجه $bdgh = acg_1h_1$. با توجه به اولیه بودن g_1h_1 ، داریم

$$bd \sim bdC(f) \sim C(bdf) = C(bdgh) = C(acg_1h_1) \sim acC(g_1h_1) \sim ac.$$

www.mathematic87.blogfa.com

ازاین‌رو bd و ac در R شریک‌اند، که نتیجه می‌دهد f و $g_1 h_1$ در $R[x]$ شریک می‌باشند. در نتیجه f در $R[x]$ تحویل‌ناپذیرنیست، که تناقض می‌باشد. بنابراین f در $F[x]$ تحویل‌ناپذیر است.

■■■

اینک برای اثبات قضیهٔ اصلی این بخش آماده هستیم.

قضیه ۱۰-۱۱

اگر R یک حوزهٔ تجزیهٔ یکتا باشد، آنگاه $R[x]$ نیز یک حوزهٔ تجزیهٔ یکتااست.

اثبات (وجود تجزیه): فرض کنید $f(x)$ یک عنصر غیر صفر وغیر یکال از $R[x]$ باشد. اگر $\deg f(x) = 0$، مسئله حل است، زیرا R حوزهٔ تجزیهٔ یکتا است. فرض کنید $\deg f(x) > 0$ و F میدان کسرهای حلقهٔ R باشد. چند جمله‌ای $f(x)$ را به‌عنوان عنصری از $F[x]$ در نظر بگیرید. چون $F[x]$ حوزهٔ تجزیهٔ یکتا است، می‌توان فرض کرد $f(x) = p_1(x)\dots p_m(x)$، که p_i ها در $F[x]$ تحویل‌ناپذیرند. فرض کنید $f(x) = C(f)f'(x)$ و $p_i(x) = (a_i / b_i)q_i(x)$، که $a_i, b_i \in R$ و چند جمله‌ای‌های $q_i(x) \in R[x]$ و $f'(x) \in R[x]$ اولیه‌اند. دراین‌صورت

$$C(f)f'(x) = (a / b)q_1(x)\dots q_m(x),$$

جاییکه $a = a_1 \dots a_m$ و $b = b_1 \dots b_m$. بنابراین طبق لم ۱ و گزاره ۴، عنصر یکال $u \in R$ چنان موجود است که $bC(f)u = a$. از این‌رو

$$bf(x) = aq_1(x)\dots q_m(x) = bC(f)uq_1(x)\dots q_m(x),$$

و در نتیجه

$$f(x) = (C(f)u)q_1(x)\dots q_m(x).$$

www.mathematic87.blogfa.com

چون هر $p_i(x)$ در $F[x]$ تحویل‌ناپذیر است، لذا $q_i(x)$، که عبارت است از حاصل‌ضرب $p_i(x)$ در یکالی از F، نیز در $F[x]$ تحویل‌ناپذیر است. چون $q_i(x)$ در $R[x]$ اولیه است، لذا طبق لم۳ ، $q_i(x)$ در $R[x]$ تحویل‌ناپذیرمی‌باشد. از طرفی چون $C(f)u$ یا یک یکال از R است یا می‌توان آنرا به حاصل‌ضربی از تحویل ناپذیرهایی R تجزیه کرد، لذا نشان داده‌ایم که $f(x)$ را می‌توان به صورت حاصل‌ضربی ازتحویل‌ناپذیرها در $R[x]$ نوشت.

اثبات (یکتایی تجزیه): فرض کنید

$$f(x) = a_1 \dots a_m p_1(x) \dots p_n(x) = b_1 \dots b_r q_1(x) \dots q_s(x),$$

جاییکه a_i, b_i عناصری تحویل‌ناپذیر از R و $p_i(x), q_i(x)$ عناصری تحویل‌ناپذیر از درجهٔ مثبت از $R[x]$ می‌باشند.

با توجه به اولیه بودن $p_i(x), q_i(x)$ (طبق لم۳) و حوزه تجزیهٔ یکتا بودن $F[x]$، $n = s$ و بعد از شماره گذاری مجدد (در صورت لزوم) هر $p_i(x)$ یک شریک $q_i(x)$ در $F[x]$ می‌باشد. از این‌رو لم ۲ ایجاب می‌کند که هر $p_i(x)$ یک شریک $q_i(x)$ در $R[x]$ است. بنابراین عنصر یکال $u_i \in R$ چنان موجود است که $q_i(x) = u_i p_i(x)$. بنابراین خواهیم داشت:

$$a_1 a_2 \dots a_m = (u_1 \dots u_n b_1) b_2 \dots b_r$$

چون R یک حوزهٔ تجزیهٔ یکتا است، پس $m = r$ و بعد از شماره گذاری مجدد (در صورت لزوم) هر a_i یک شریک b_i در R (ودر نتیجه در $R[x]$) می‌باشد. بدین ترتیب اثبات قضیه کامل است.

■■■

www.mathematic87.blogfa.com

در این بخش سه محک مهم در مورد تحویل ناپذیر بودن عناصر $\mathbb{Q}[x]$ مطرح می‌شود.

قضیه۱۰-۱۲ (محک آیزنشتاین)

فرض کنید P یک ایده‌آل اول از حوزهٔ صحیح R باشد. فرض کنید $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$ (در اینجا $n\geq 1$). اگر $a_0,a_1,\ldots,a_{n-1}\in P$ و $a_n\notin P$ و $a_0\notin P^2$، آنگاه $f(x)$ در $R[x]$ تحویل‌ناپذیر است.

اثبات: (برهان خلف) فرض کنید f تحویل‌پذیر باشد. در این‌صورت

$$f(x)=(b_0+b_1x+\cdots+b_mx^m)(c_0+c_1x+\cdots+c_kx^k),$$

که $b_i,c_i\in R$ و $m,k\geq 1$. چون $b_0c_0=a_0\in P$، $a_0\notin P^2$، پس P فقط شامل یکی از عناصر b_0,c_0 می‌باشد. فرض کنید $b_0\in P$ و $c_0\notin P$. چون $a_n=b_mc_k$ و $a_n\notin P$، پس $b_m\notin P$. فرض کنید i کوچکترین عدد صحیح مثبتی باشد که $b_i\notin P$. در این‌صورت $i\leq m<n$ و

$$a_i=b_ic_0+(b_{i-1}c_1+\cdots+b_0c_i).$$

اما $a_i\in P$، $b_{i-1}c_1+\cdots+b_0c_i\in P$ ، پس $b_ic_0\in P$. چون P یک ایده‌آل اول است، لذا $b_i\in P$ یا $c_0\in P$، که تناقض است. بنابراین نتیجه می‌گیریم که f در $R[x]$ تحویل‌ناپذیر است.

■■■

نتیجهٔ زیر به آسانی از محک آیزنشتاین بدست می‌آید.

نتیجه۱۰-۴(محک آیزنشتاین برای $\mathbb{Z}[x]$)

فرض کنید $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$. فرض کنید p یک عدد اولی باشد که $p\mid a_i$ برای هر $0\leq i\leq n-1$ و $p^2\nmid a_0$ و $p\nmid a_n$. در این‌صورت f در $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

www.mathematic87.blogfa.com

مثال۷: $f(x)=x^3-2$ در $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

■

قضیه۱۰-۱۳

فرض کنید R یک حوزهٔ تجزیهٔ یکتا و F میدان کسرهای R باشد. فرض کنید $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. اگر $r/s\in F$ ریشه‌ای از f باشد که در آن r و s نسبت بهم اولند، آنگاه $r\mid a_0$ و $s\mid a_n$.

اثبات: داریم $f(r/s)=a_0+a_1(r/s)+\cdots+a_n(r/s)^n=0$. با ضرب در s^n خواهیم داشت:

$$a_0s^n+a_1rs^{n-1}+\cdots+a_{n-1}r^{n-1}s+a_nr^n=0.$$

بنابراین $a_nr^n=s(-a_0s^{n-1}-\cdots-a_{n-1}r^{n-1})$. از این‌رو $s\mid a_nr^n$. چون $(r,s)=1$، پس $s\mid a_n$. به‌همین ترتیب، $a_0s^n=r(-a_1s^{n-1}-\cdots-a_nr^{n-1})$ و درنتیجه $r\mid a_0$.

■■■

مثال۸: فرض کنید $f(x)=8x^3-6x-1$. در این مورد نمی‌توان از محک آیزنشتاین برای تحویل‌ناپذیر بودن $f(x)$ روی $\mathbb{Q}[x]$ استفاده کرد. به‌هرحال اگر $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌پذیر باشد، آنگاه $f(x)$ باید دارای یک عامل درجهٔ یک و در نتیجه دارای یک ریشه در $\mathbb{Q}[x]$ باشد. با توجه به قضیهٔ قبل این ریشه باید عنصری از مجموعهٔ $A=\{\pm1,\pm(1/2),\pm(1/4),\pm(1/8)\}$ باشد، که یک تناقض است، چون‌که هیچ یک از عناصر A ریشهٔ $f(x)$ نیست. بنابراین $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

■

قضیه زیر محک دیگری برای تحویل‌ناپذیری یک چند جمله‌ای در $\mathbb{Z}[x]$ ارائه می‌دهد.

www.mathematic87.blogfa.com

قضیه ۱۰-۱۴

فرض کنید $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$ و p عدد اول اولی باشد که $p\nmid a_n$. فرض کنید $\overline{f}(x)=\overline{a}_0+\overline{a}_1x+\cdots+\overline{a}_nx^n\in\mathbb{Z}_p[x]$، که در آن $\overline{a}_i$ تصویر a_i تحت همریختی طبیعی $\mathbb{Z}\to\mathbb{Z}_p$ می‌باشد. در این‌صورت اگر f در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر باشد، آنگاه f در $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ نیز تحویل‌ناپذیر است.

اثبات: با توجه لم ۳، کافی است ثابت کنیم که f در $\mathbb{Z}[x]$ تحویل ناپذیر است. فرض کنید f در $\mathbb{Z}[x]$ تحویل ناپذیر نباشد. در این‌صورت چندجمله‌ای‌های $g(x),\ h(x)\in\mathbb{Z}[x]$ به‌گونه‌ای موجودند که $f(x)=g(x)h(x)$ و $\deg g(x)<\deg f(x)$ و $\deg h(x)<\deg f(x)$. به آسانی ملاحظه می‌شود که $\overline{f}(x)=\overline{g}(x)\overline{h}(x)$ و $\deg f(x)=\deg\overline{f}(x)$. حال داریم

$$\deg\overline{g}(x)\le\deg g(x)<\deg f(x)=\deg\overline{f}(x),$$
$$\deg\overline{h}(x)\le\deg h(x)<\deg f(x)=\deg\overline{f}(x),$$

که تناقض با تحویل‌ناپذیر بودن $\overline{f}$ در $\mathbb{Z}_p[x]$ است.

■■■

مثال ۹: فرض کنید $f(x)=x^5+x^2+1\in\mathbb{Z}[x]$. در این مورد نمی‌توان از دو محک قبل برای تحویل‌ناپذیر بودن $f(x)$ روی $\mathbb{Q}[x]$ استفاده کرد. فرض کنید $\overline{f}(x)=\bar{1}x^5+\bar{1}x^2+\bar{1}\in\mathbb{Z}_2[x]$. در این‌صورت

(۱) چون $\overline{f}(0)\neq 0$ و $\overline{f}(1)\neq 0$، پس $f(x)$ دارای عامل درجهٔ یک در $\mathbb{Z}_2[x]$ نیست،

(۲) چندجمله‌ای‌های درجهٔ دو در $\mathbb{Z}_2[x]$ عبارتند از: $\bar{1}x^2+\bar{1}$، $\bar{1}x^2$، $\bar{1}x^2+\bar{1}x$ و $\bar{1}x^2+\bar{1}x+\bar{1}$. با توجه به قسمت (۱) چندجمله‌ای‌های $\bar{1}x^2+\bar{1}$، $\bar{1}x^2$، $\bar{1}x^2+\bar{1}x$ هیچ‌کدام عاملی از $f(x)$ در $\mathbb{Z}_2[x]$ نمی باشند و همچنین با انجام عملیات تقسیم می‌توان نشان داد که $\bar{1}x^2+\bar{1}x+\bar{1}$ نیز عاملی از $f(x)$ در $\mathbb{Z}_2[x]$ نمی باشد.

www.mathematic87.blogfa.com

بنابراین $f(x)$ در $\mathbb{Z}_2[x]$ تحویل‌ناپذیر است. پس نتیجه می‌گیریم $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

■

توضیح تاریخی

کارل فریدریش گاوس در 30آوریل 1777در برنسویک آلمان بدنیا آمد. ایشان به‌عنوان بزرگترین ریاضی‌دانی که تاکنون پا به عرصهٔ هستی گذاشته است، معروف است. در سن سه سالگی وی قادر به یافتن اشتباهاتی از کتاب‌های تجارت پدرش شد. گاوس در سن پانزده سالگی وارد کالج شد و قبل از سن بیست سالگی قادر به ترسیم ۱۷-ضلعی منتظم بوسیلهٔ خط‌کش و پرگار شد. گاوس در سال 1799موفق به کسب مدرک Ph. Dاز دانشگاه هلمستد شد. وی در پایان‌نامهٔ دکترای خود برای اولین بار اثبات کاملی از قضیهٔ اساسی جبر، که بیان می‌کند که هر چندجمله‌ای با ضرایب حقیقی به حاصل‌ضرب عوامل خطی روی اعداد مختلط تجزیه می‌شود، ارائه داد. ایشان برای اولین بار از نماد iبجای $\sqrt{-1}$ استفاده نمود. گاوس سپس توجه خود را معطوف نظریهٔ اعداد نمود و در این زمینه درسال 1801 کتاب معروفش تحت عنوان Disquisitioncs Arithmeticaeرا به چاپ رساند. سخن مشهور زیر از ایشان است:

«ریاضیات ملکهٔ علوم است و نظریهٔ اعداد ملکهٔ ریاضیات»

گاوس شاگردان زیادی به جامعهٔ ریاضی تحویل داده که از آن‌جمله‌اند: آیزنشتاین، ریمان، کومر، دیریکله و ددکیند. سرانجام گاوس در 23 فوریهٔ 1855در سن ۷۸ سالگی در گوتینگن درگذشت.

www.mathematic87.blogfa.com

تمرینها

۱. فرض کنید R یک حوزهٔ صحیح باشد. ثابت کنید $(R[x])^* = R^*$. به عبارت دیگر عناصر معکوس‌پذیر(یکال) حلقه‌های $R[x]$ و R برابرند.

۲. (a) ثابت کنید $\mathbb{Z}[x]$ یک حوزهٔ ایده‌آل اصلی نیست،

(b) فرض کنید R حوزهٔ صحیحی باشد که دارای یک عنصر تحویل‌ناپذیر مانند c است. ثابت کنید $R[x]$ یک حوزهٔ ایده‌آل اصلی نیست.

۳. (a) اگر R یک حوزهٔ صحیح باشد، ثابت کنید $R[x,y]$ یک حوزهٔ ایده‌آل اصلی نیست،

(b) حلقه‌ای مانند R مثال بزنید که حوزهٔ تجزیهٔ یکتا بوده ولی حوزهٔ ایده‌آل اصلی نباشد.

۴. فرض کنید R یک حلقهٔ جابجایی و یکدار باشد. نشان دهید $(R[x])[y] \cong (R[y])[x]$. به‌عبارت دیگر $R[x,y] \cong R[y,x]$.

۵. فرض کنید R یک حلقهٔ جابجایی باشد. نشان دهید R را می‌توان در یک حلقهٔ جابجایی ویکدار نشاند.

۶. فرض کنید F یک میدان باشد. نشان دهید میدان کسرهای F یکریخت با F است.

۷. دو حوزهٔ صحیح غیر یکریخت مثال بزنید که میدان کسرهایشان یکریخت باشند.

۸. (a) فرض کنید R یک حوزهٔ تجزیهٔ یکتا و $a_1, a_2 \in R$. فرض کنید $a_1 = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ و $a_2 = p_1^{\beta_1} \cdots p_n^{\beta_n}$، که در آن p_iها تحویل‌ناپذیرند. نشان دهید بزرگترین مقسوم‌علیه مشترک a_1 و a_2 برابر است با

$$p_1^{\min\{\alpha_1,\beta_1\}} \dots p_n^{\min\{\alpha_n,\beta_n\}}.$$

www.mathematic87.blogfa.com

(b) قسمت (a) را برای n عنصر بیان واثبات کنید.

۹. اگر $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$، آنگاه $2 \in \mathbb{Z}[\sqrt{-3}]$ تحویل‌ناپذیر بوده ولی اول نمی‌باشد.

۱۰. (a) فرض کنید p عنصر ناصفری از حوزهٔ صحیح R باشد. نشان دهید p یک عنصر اول است اگر و فقط اگر (p) یک ایده‌آل اول باشد،

(b) فرض کنید a عنصر ناصفری از حوزهٔ صحیح R باشد. نشان دهید a یک عنصر تحویل ناپذیر است اگر و فقط اگر (a) در مجموعهٔ همهٔ ایده‌آل‌های اصلی سرهٔ R ماکزیمال باشد،

(c) فرض کنید F یک میدان و $f(x) \in F[x]$. نشان دهید $(f(x))$ یک ایده‌آل ماکزیمال ازحلقهٔ $F[x]$ است اگر و فقط اگر $f(x)$ یک عنصر تحویل‌ناپذیر باشد.

۱۱. فرض کنید R یک حوزهٔ تجزیهٔ یکتا و a عنصر غیر صفری از R باشد. نشان دهید تنها تعداد متناهی ایده‌آل اصلی شامل (a) موجود است.

۱۲. (a) فرض کنید R یک حلقه و $d \in R$ بزرگترین مقسوم علیه مشترک عناصر $a_1, a_2, \ldots, a_n \in R$ باشد. اگر $d_1 \in R$ شریک dباشد، آنگاه نشان دهید d_1 نیز بزرگترین مقسوم علیه مشترک عناصر $a_1, a_2, \ldots, a_n$ می‌باشد،

(b) فرض کنید R یک حوزهٔ صحیح باشد. نشان دهید هر دو بزرگترین مقسوم علیه مشترک عناصر $a_1, a_2, \ldots, a_n \in R$ شریک می‌باشند،

(c) فرض کنید $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ و $a = 4$ و $b = 2 + 2\sqrt{-3}$. نشان دهید بزرگترین مقسوم علیه مشترک عناصر a, bموجود نمی‌باشد.

۱۳. (الگوریتم اقلیدس) فرض کنید R یک حلقهٔ اقلیدسی با تابع اقلیدسی $\upsilon : R - \{0\} \to \mathbb{N}_0$ باشد. اگر $a, b \in R$ و $b \neq 0$، نشان دهید روش زیر بزرگترین مقسوم علیه مشترک a و b را بدست می‌آورد. فرض کنید

www.mathematic87.blogfa.com

$$a = bq_0 + r_1 \text{، که در آن } r_1 = 0 \text{ یا } \upsilon(r_1) < \upsilon(b)\text{،}$$

$$b = r_1q_1 + r_2 \text{، که در آن } r_2 = 0 \text{ یا } \upsilon(r_2) < \upsilon(r_1)\text{،}$$

$$r_1 = r_2q_2 + r_3 \text{، که در آن } r_3 = 0 \text{ یا } \upsilon(r_3) < \upsilon(r_2)\text{،}$$

$$\vdots$$

$$r_m = r_{m+1}q_{m+1} + r_{m+2} \text{، که در آن } r_{m+2} = 0 \text{ یا } \upsilon(r_{m+2}) < \upsilon(r_{m+1}).$$

اگر $r_0 = b$ و n کوچکترین عدد صحیحی باشد که $r_{n+1} = 0$، آنگاه r_n بزرگترین مقسوم علیه مشترک a و b است.

۱۴. فرض کنید R یک حوزهٔ صحیح باشد. نشان دهید R یک حوزهٔ تجزیهٔ یکتاست اگر وفقط اگر

(۱) هر عنصر غیر صفر وغیر یکال به‌صورت حاصل‌ضربی از تحویل‌ناپذیرها نوشته شود،

(۲) هر تحویل‌ناپذیری اول باشد.

۱۵. فرض کنید P, Q دو ایده‌آل اول از حوزهٔ صحیح R باشند به‌طوریکه $P \subseteq Q$. نشان دهید $P = Q$.

۱۶. نشان دهید چند جمله‌ای‌های زیر روی $\mathbb{Z}[x]$ تحویل‌ناپذیرند.

(۱) $f(x) = 2x^6 - 6x^5 + 9x + 15$ (۲) $f(x) = 2x^5 - 10x + 5$

(۳) $f(x) = x^4 + 4x^2 + 2$ (۴) $f(x) = x^3 + x^2 - 2x - 1$

(۵) $f(x) = 5x^5 + 2x^4 + x^2 + 5$ (۶) $f(x) = x^3 - 3x + 1$.

۱۷. نشان دهید چند جمله‌ای $f(x) = x^4 - 2x^3 + x + 1$ روی $\mathbb{Z}[x]$ تحویل‌ناپذیر است.

www.mathematic87.blogfa.com

۱۸. (a) فرض کنید c عنصری از میدان F بوده و $f(x) \in F[x]$. نشان دهید $f(x)$ در $F[x]$ تحویل‌ناپذیراست اگر و فقط اگر $f(x+c)$ در $F[x]$ تحویل‌ناپذیر باشد،

(b) نشان دهید چند جمله‌ای $f(x) = x^4 + 4x^3 + 6x^2 + 4x + 4$ روی $\mathbb{Z}[x]$ تحویل‌ناپذیر است.

۱۹. اگر $n \in \mathbb{N}$ و $f(x) = (x-1)(x-2)\cdots(x-n) - 1$، ثابت کنید $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۲۰. فرض کنید $n \in \mathbb{N}$ و $f(x) = 1 + x + \cdots + x^{n-1}$، ثابت کنید $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و فقط اگر n اول باشد.

مسائل مبارزه طلب

۱. فرض کنید F یک میدان باشد. نشان دهید

$$\mathrm{Max} F[x_1,\ldots,x_n] = \{(x_1 - a_1,\ldots,x_n - a_n) \mid a_i \in F\}.$$

۲. یک زیر حلقهٔ سره از میدان اعداد حقیقی $\mathbb{R}$ بیابید که میدان کسرهایش برابر $\mathbb{R}$ باشد.

۳. حوزهٔ صحیح R حوزهٔ تجزیهٔ یکتاست اگر وفقط اگر هر ایده‌آل اول ناصفر در R شامل ایده‌آل اصلی ناصفری است که اول می‌باشد.

۴. حلقهٔ R یک حوزهٔ ایده‌ال اصلی است اگر وفقط اگر R یک حوزهٔ تجزیهٔ یکتا بوده و هرایده‌ال اول ناصفرش ماکزیمال است.

۵. فرض کنید R زیر حلقهٔ $\{a + b(1+\sqrt{19}i)/2 \mid a,b \in \mathbb{Z}\}$ از اعداد مختلط باشد. نشان دهید R یک حوزهٔ ایده‌آل اصلی است ولی یک حوزهٔ اقلیدسی نیست.

www.mathematic87.blogfa.com

منابعی برای مطالعهٔ بیشتر

۱. طائری، بیژن. **مبانی جبرمجرد**. انتشارات دانشگاه صنعتی اصفهان (۱۳۸۲).

۲. هانگرفورد، تی. دبلیو. **مقدمه‌ای بر جبر مجرد**. ترجمه اعظم، سعید و انشائی، رضا. انتشارات دانشگاه اصفهان (۱۳۸۱).

3. Judson, T. W. *Abstract Algebra*. PWS Publishing Company, Boston, 1993.
4. Rotman, J. *Galois Theory*. Springer-Verlag, 1998.

www.mathematic87.blogfa.com

فصل۱۱

مباحثی پیشرفته‌تر در نظریه حلقه‌ها

در این فصل می‌خوانید:

۱۱-۱ مجموعه‌های بسته ضربی
۱۱-۲ حلقه کسرها
۱۱-۳ رادیکال‌ها
۱۱-۴ مدول ها

مقدمه

در این فصل حلقه‌ها را به طور عمیق‌تر مورد مطالعه قرار می‌دهیم. در بخش اول به مجموعه‌های بسته ضربی، که نقش بسیار مهمی در حلقه‌ها مخصوصاً حلقه‌های جابجایی دارد، می‌پردازیم. در بخش دوم به مطالعهٔ حلقه کسرها، که تعمیم میدان کسرها است، خواهیم پرداخت. در بخش سوم به بررسی رادیکال‌ها می‌پردازیم. در بخش آخر مروری اجمالی بر نظریه مدول‌ها خواهیم داشت. اثبات اینکه هر حلقه آرتینی یک حلقه نوتری است از نتایج مهم بخش آخر است.

www.mathematic87.blogfa.com

۱۱-۱ مجموعه‌های بسته ضربی

تعریف ۱۱-۱

فرض کنید R یک حلقه و S یک زیر مجموعه ناتهی از R باشد.

(۱) S را **بسته ضربی** گوییم، اگر

$$a,\ b \in S \Rightarrow ab \in S.$$

(۲) S را **بسته ضربی تعمیم یافته** گوییم، اگر

به ازای یک $r \in R$، $a,\ b \in S \Rightarrow arb \in S$.

❖ **تذکر (۱):** اگر R یک حلقه یکدار باشد، آنگاه هر زیرمجموعهٔ بستهٔ ضربی، یک زیرمجموعهٔ بستهٔ ضربی تعمیم یافته است.

(۲): زیر مجموعه‌های بستهٔ ضربی در حلقه‌های جابجایی و زیر مجموعه‌های بستهٔ ضربی تعمیم یافته در حلقه‌های ناجابجایی حائز اهمیت می‌باشند.

مثال ۱: فرض کنید R یک حلقه و $a \in R$. در این صورت $S = \{a^1, a^2, a^3, \ldots\}$ یک زیر مجموعه بسته ضربی (تعمیم یافته) از R است.

■

مثال ۲ (۱): اگر I یک ایده‌آل چپ (راست) از حلقه R باشد، آنگاه I یک زیر مجموعه بسته ضربی (تعمیم یافته) از R است.

(۲): اگر R' زیر حلقه‌ای از حلقهٔ R باشد، آنگاه R' یک زیر مجموعه بسته ضربی (تعمیم یافته) از R است.

(۳): اگر R' زیر حلقه‌ای از حلقهٔ یکدار R باشد، آنگاه $1 + R'$ یک زیر مجموعه بسته ضربی (تعمیم یافته) از R است.

■

مثال ۳: فرض کنید P ایده‌آل اولی از حلقه R باشد. در این صورت $S = P^c = R - P$ یک زیر مجموعه بسته ضربی تعمیم یافته از R است.

www.mathematic87.blogfa.com

■

مثال ۴: فرض کنید R حلقه‌ای جابجایی باشد. در این صورت $S = Z(R)^c = R - Z(R)$ یک زیر مجموعه بسته ضربی از R است.

■

قضیه۱۱-۱

فرض کنید R یک حلقه و S یک مجموعه بسته ضربی از R و I ایده‌آلی از R باشد. اگر $I \cap S = \varnothing$، آنگاه ایده‌آلی اولی مانند P چنان موجود است که $I \subseteq P$ و $P \cap S = \varnothing$.

اثبات: قرار می‌دهیم:

$$\Omega = \{J | I \subseteq J \subseteq R,\ J \cap S = \varnothing,\ R \text{ ایده‌آلی از } J\}.$$

به‌وضوح $\Omega \neq \varnothing$ در شرایط لم زرن صدق می‌کند. فرض کنید P عنصر ماکزیمال Ω باشد. کافی است نشان دهیم P یک ایده‌آل اول است. برای این منظور فرض کنید $(a)(b) \subseteq P$، $a \notin P$ و $b \notin P$. چون P عنصر ماکزیمال Ωاست لذا $P + (a) \notin \Omega$و $P + (b) \notin \Omega$. در نتیجه $(P + (a)) \cap S \neq \varnothing$ و $(P + (b)) \cap S \neq \varnothing$. بنابراین عناصر $p_1, p_2 \in P$ و $a_1 \in (a)$ و $b_1 \in (a)$چنان موجودند که $p_1 + a_1 = s_1$ و $p_2 + b_1 = s_2$. بنابراین

$$s = s_1 s_2 = (p_1 + a_1)(p_2 + b_1) = p_1 p_2 + p_1 b_1 + a_1 p_2 + a_1 b_1 \in P,$$

یعنی $s \in P \cap S$، که تناقض است، لذا P ایده‌آل اولی از R است.

■■■

❖ **تذکر:** با استدلالی مشابه، میتوان نشان داد که قضیهٔ فوق برای زیر مجموعه‌های بستهٔ ضربی تعمیم یافته نیز صادق است.

حال تمام حلقه‌های جابجایی را که در آنها مجموعه ایده‌آل‌های اول و ماکزیمال برابرند، به طور کامل مشخص می‌کنیم.

www.mathematic87.blogfa.com

تعریف ۱۱-۲

حلقه جابجایی و یکدار R را **منظم** $-\pi$ گوییم، اگر برای هر $x \in R$ عدد صحیح $n \geq 0$ چنان موجود باشد که $x^n \in Rx^{n+1}$.

قضیه۱۱-۲

فرض کنید R حلقه‌ای جابجایی و یکدار باشد. نشان دهید:

R یک حلقه π - منظم است $\Leftrightarrow$ هر ایده‌آل اول R ماکزیمال باشد.

اثبات ($\Leftarrow$): فرض کنید P ایده‌آل اولی از حلقه R باشد و J ایده‌آلی از R باشد که $P \subsetneq J \subseteq R$. بنابراین $x \in J$ چنان موجود است که $x \notin P$. با توجه به فرض عدد صحیح $n \geq 0$, $r \in R$ چنان موجود است که $x^n = rx^{n+1}$. لذا $0 = x^n(1-rx) \in P$ و چون $x \notin P$ پس $1 - rx \in P \subseteq J$، یعنی $1 \in J$ یا $J = R$.

($\Rightarrow$): فرض کنید $x \in R$. قرار می‌دهیم:

$$S = \left\{x^n - rx^{n+1} \,|n \in \mathbb{N} \cup \{0\},\ r \in R\right\}.$$

به وضوح S یک زیر مجموعه بسته ضربی از R است. اگر $0 \in S$ که مسئله حل است. بنابراین فرض کنید $0 \notin S$. قرار می‌دهیم $I = \{0\}$. در این صورت طبق قضیه ۱ ایده‌آل اول (در حقیقت ایده‌آل ماکزیمال) P چنان موجود است که $P \cap S = \varnothing$. چون $x \in S$، پس $P + Rx = R$. بنابراین عناصر $r \in R$ و $p_1 \in P$ موجودند که $p_1 + rx = 1$ لذا $p_1 = 1 - rx \in P \cap S$ که تناقض است.

■■■

www.mathematic87.blogfa.com

این بخش به تعمیم مطالب بخش ۱۰-۳ (میدان کسرها) اختصاص دارد. در سراسر این بخش R نشان دهندهٔ یک حلقهٔ جابجایی و یکدار و S یک زیرمجموعهٔ بستهٔ ضربی از R است بطوریکه $1 \in S$.

قضیه ۱۱-۳

فرض کنید S یک زیر مجموعه بسته ضربی از R باشد. در این صورت رابطه زیر یک رابطه هم ارزی روی $R \times S$ است:

$$(r,s) \sim (r',s') \Leftrightarrow s_1(s'r - sr') = 0,\ s_1 \in S$$ به ازای یک

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

نمادگذاری: فرض کنید S یک زیر مجموعه بسته ضربی از R باشد. کلاس هم ارزی $(r,s) \in R \times S$ را با r/s نمایش داده و قرار می‌دهیم:

$$S^{-1}R = \{r/s \,|\, r \in R, s \in S\}.$$

قضیه ۱۱-۴

فرض کنید S یک زیر مجموعه بسته ضربی از R باشد.

(۱) $S^{-1}R$ همراه با اعمال جمع و ضرب زیر یک حلقه جابجایی و یکدار است،

$$r/s + r'/s' = (s'r + sr')/ss',\ (r/s)(r'/s') = (rr'/ss')$$

(۲) اگر R یک حوزه صحیح و $0 \notin S$، آنگاه $S^{-1}R$ نیز یک حوزه صحیح است.

اثبات (۱): ابتدا نشان می‌دهیم که عمل جمع خوش تعریف است. فرض کنید $r/s = r_1/s_1$ و $r'/s' = r'/s_1'$. طبق فرض عناصر $s_2, s_3 \in S$ چنان موجودند که

$$s_2(s_1r - sr_1) = 0,$$
$$s_3(s'r_1' - s'r_1') = 0.$$

با ضرب معادله اول در $s_3s's_1'$ و معادله دوم در s_2ss_1 و جمع آنها داریم:

www.mathematic87.blogfa.com

$$s_2 s_3 \left[\left(s'r + sr' \right) s_1 s_1' - \left(s_1' r_1 + s_1 r_1' \right) ss' \right] = 0$$

بنابراین $(rs' + r's)/ss' = (r_1 s_1' + r_1' s_1)/s_1 s'$. یعنی عمل جمع خوش تعریف است. به طریق مشابه می‌توان دید که عمل ضرب نیز خوش تعریف است. برای هر $s, s' \in S$ عنصر $0/s = 0/s'$ عنصر همانی جمعی $S^{-1}R$ و $1/1 = s/s = s'/s'$ عنصر همانی عمل ضرب $S^{-1}R$ است. جابجایی بودن $S^{-1}R$ به‌وضوح از جابجایی بودن R نتیجه می‌شود. تکمیل بقیهٔ اثبات به‌عنوان تمرین به خواننده واگذار می‌شود.

(۲): چون R یک حوزه صحیح و $0 \notin S$، لذا

$$(r/s)(r'/s') = 0 \Leftrightarrow rr' = 0 \Leftrightarrow r = 0 \text{ یا } r' = 0 \Leftrightarrow r/s = 0 \text{ یا } r'/s' = 0$$

■■■

تعریف ۱۱-۳

اگر S یک زیر مجموعه بسته ضربی از R باشد، $S^{-1}R$ را **حلقه کسرهای** R روی S می‌نامند.

تذکر: اگر R حوزه صحیح باشد، آنگاه به‌وضوح $S = R - \{0\}$ یک زیر مجموعهٔ بسته ضربی است و $F = S^{-1}R$ همان میدان کسرهای R خواهد بود (بخش ۱۰-۳ ملاحظه شود).

قضیه۱۱-۵

فرض کنید S یک زیر مجموعه بسته ضربی از R باشد.

(۱) نگاشت $\varphi : R \to S^{-1}R$ با ضابطه $\varphi(r) = r/1$ یک همریختی حلقه‌ای است،

(۲) اگر $S \cap Z(R) = \varnothing$، آنگاه همریختی مطرح شده در قسمت (۱)، یک به یک است،

(۳) هر حوزهٔ صحیح قابل نشاندن در میدان کسرهای خود است.

www.mathematic87.blogfa.com

اثبات: به عنوان تمرین به خواننده واگذار می‌شود(قضیه ۱۰-۸ ملاحظه شود).

■■■

قضیه زیر ایده‌آل‌های اول $S^{-1}R$ را بر حسب ایده‌آل‌های اول R به طور کامل مشخص می‌کند.

قضیه۱۱-۶

فرض کنید S یک زیر مجموعه بسته ضربی از R باشد.

(۱) اگر I ایده‌آلی از R باشد، آنگاه $S^{-1}I = \{a/s | a \in I, s \in S\}$ ایده‌آلی از $S^{-1}R$ است،

(۲) اگر I ایده‌آلی از R باشد، آنگاه $S^{-1}I \neq S^{-1}R$ اگر و فقط اگر $S \cap I \neq \varnothing$،

(۳) اگر J ایده‌آلی از $S^{-1}R$ باشد، آنگاه $J = S^{-1}\varphi^{-1}(J)$. (توجه داشته باشد که φ همان همریختی قضیه ۵ است).

(۴) اگر $Q \in \operatorname{Spect}(S^{-1}R)$، آنگاه $\varphi^{-1}(Q) \in \operatorname{Spect}(R)$، $\varphi^{-1}(Q) \cap S = Q$ و $S^{-1}\varphi^{-1}(Q) = Q$.

(۵) $\operatorname{Spect}(S^{-1}R) = \{S^{-1}P | P \in \operatorname{Spect}(R), P \cap S = \varnothing\}$.

اثبات: (۱) و **(۲)** بدیهی‌اند.

(۳): بدیهی است که $S^{-1}\varphi^{-1}(J) \subseteq J$. بنابراین کافی است ثابت کنیم $J \subseteq S^{-1}\varphi^{-1}(J)$. برای این منظور فرض کنید $\lambda \in J$. در این صورت عناصر $a \in R$ و $s \in S$ چنان موجودند که $\lambda = a/s$. داریم

$$\varphi(a) = a/1 = (s/1)(a/s) \in J.$$

ازاین‌رو $a \in \varphi^{-1}(J)$ و $\lambda = a/s = (1/s)\varphi(a) \in S^{-1}\varphi^{-1}(J)$.

(۴): با توجه به (۲) و (۳) خواهیم داشت $\varphi^{-1}(Q) \cap S = \varnothing$ و $S^{-1}\varphi^{-1}(Q) = Q$. بنابراین کافی است ثابت کنیم $\varphi^{-1}(Q) \in \operatorname{Spect}(R)$. برای این منظور فرض کنید $ab \in \varphi^{-1}(Q)$،

www.mathematic87.blogfa.com

لذا $ab/1=(a/1)(b/1)\in Q$ چون Q اول است لذا $a/1\in Q$ یا $b/1\in Q$.
بنابراین $a\in\varphi^{-1}(Q)$ یا $b\in\varphi^{-1}(Q)$.

(۵): فرض کنید $Q\in \mathrm{Spect}(S^{-1}R)$. قرارمی‌دهیم $P=\varphi^{-1}(Q)$. در این صورت طبق (۴) خواهیم داشت $P\in \mathrm{Spect}(R)$، $Q=S^{-1}P$ و $P\cap S=\varnothing$. حال فرض کنید P ایده‌آل اولی از R باشد که $P\cap S=\varnothing$. نشان می‌دهیم $S^{-1}P$ ایده‌آل اولی از $S^{-1}R$ است. طبق (۲) $S^{-1}P\neq S^{-1}R$. حال فرض کنید $(a/s)(b/t)\in S^{-1}P$ لذا $p_1\in P$ و $s_1\in S$ چنان موجود است که $ab/st=p_1/s_1$ و در نتیجه $s'\in S$ چنان موجود است که $s'(abs_1-p_1st)=0$ و لذا $abs's_1\in P$ چون P یک ایده‌آل اول R ، $P\cap S=\varnothing$. در نتیجه $ab\in P$ که از آنجا $a\in P$ یا $b\in P$. پس $a/s\in S^{-1}P$ یا $b/t\in S^{-1}P$.

■■■

نمادگذاری: فرض کنید P یک ایده‌آل اول از R باشد. اگر $S=R-P$، آنگاه حلقه $S^{-1}R$ را با R_P نمایش می‌دهیم.

تعریف ۱۱-۴

حلقه R را **موضعی** گوییم اگر تنها دارای یک ایده‌آل ماکزیمال باشد.

قضیه۱۱-۷

فرض کنید P ایده‌آل اولی از R باشد. در این‌صورت R_P یک حلقه موضعی است.

اثبات: ادعا می‌کنیم که $S^{-1}P=\{a/s \mid a\in P\ ,s\in S\}$ تنها ایده‌آل ماکزیمال R_P است. فرض کنید $b/t\in R_P-S^{-1}P$. در این‌صورت $b\notin P$ و لذا $b\in S=R-P$ و $(b/t)(t/b)=1$، یعنی هر عنصر خارج از $S^{-1}P$ معکوس‌پذیر است، و لذا $S^{-1}P$ تنها ایده‌آل ماکزیمال R_P است.

■■■

www.mathematic87.blogfa.com

۱۱-۳ رادیکال‌ها

دراین بخش به معرفی رادیکال‌ها که نقش بسیار مهمی در نظریه حلقه‌ها دارند می‌پردازیم.

تعریف ۱۱-۵

فرض کنید I ایده‌آل سره‌ای از حلقهٔ یکدار R باشد. در این صورت، **رادیکال اول** I (رادیکال پوچ I)، که آنرا با $\sqrt{I}$ نشان می‌دهیم عبارت است از

$$\sqrt{I} = \bigcap_{\substack{P\in \mathrm{Spect}(R)\\ I\subseteq P}} P.$$

قرار داد: برای حلقهٔ یکدار R قرار می‌دهیم $\sqrt{R} = R$.

قضیه۱۱-۸

فرض کنید I ایده‌آلی از حلقه جابجایی و یکدار R باشد. در این صورت:

$$\sqrt{I} = \{x \in R \,|\, x^n \in I \ \ , n \geq 0 \ \text{به ازای یک}\}.$$

اثبات: اگر $I = R$، به وضوح حکم برقرار است. حال فرض کنید I ایده‌آل سره‌ای از R باشد. فرض کنید عدد صحیح $n \geq 0$ چنان باشد که $x^n \in I$ و P ایده‌آل اولی از R باشد که $I \subseteq P$. در این صورت $x^n \in I \subseteq P$ و لذا $x \in P$، یعنی

$$\{x \in R \,|\, x^n \in I\,,\ n \geq 0 \ \text{برای یک}\} \subseteq \sqrt{I}.$$

حال فرض کنید $x \in R$ و برای هر عدد صحیح $n \geq 0$، $x^n \notin I$. در این صورت مجموعه $S = \{x^n \,|n \geq 0\}$ یک زیر مجموعه بسته ضربی از R است که $I \cap S = \varnothing$. ازاین‌رو ایده‌آل اول P چنان موجود است که $I \subseteq P$ و $I \cap S = \varnothing$، ازاین‌رو $x \notin P$ و در نتیجه $x \notin \sqrt{I}$. یعنی

$$\sqrt{I} \subseteq \{x \in R \,|\, x^n \in I\,,\ n \geq 0 \ \text{برای یک}\}.$$

■■■

نتیجه ۱۱-۱

فرض کنید R یک حلقه جابجایی و یکدار باشد. در این صورت

$$\Big\{x \in R \big| x^n = 0,\ n \geq 0\Big\} = \text{عناصر پوچ توان} = \bigcap_{P \in \mathrm{Spect}(R)} P.$$

اثبات : در قضیه فوق قرار دهید $I = (0)$.

■■■

قضیه ۱۱-۹

فرض I و J ایده‌آل‌هایی از حلقه جابجایی و یکدار R باشند. در این صورت

(۱) $I \subseteq \sqrt{I} = \sqrt{\sqrt{I}}$،

(۲) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$،

(۳) $\sqrt{I} = R \Leftrightarrow I = R$،

(۴) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$،

(۵) اگر I یک ایده‌آل و n یک عدد طبیعی باشد، آنگاه $\sqrt{I^n} = \sqrt{I}$،

(۶) اگر P یک ایده‌آل اول و n یک عدد طبیعی باشد، آنگاه $\sqrt{P^n} = P$.

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱۱-۶

ایده‌آل I از حلقه یکدار R را **نیم اول** گوییم اگر برای هر $a \in R$

$$aRa \subseteq I \Rightarrow a \in I.$$

قضیه ۱۱-۱۰

فرض کنید I ایده‌آلی از حلقه یکدار R باشد. در این صورت:
$\sqrt{I} = I \Leftrightarrow I$ یک ایده‌آل نیم اول است

اثبات ($\Rightarrow$): اگر

$$aRa \subseteq I = \sqrt{I} = \bigcap_{\substack{P \in \mathrm{Spect}(R) \\ I \subseteq P}} P,$$

آنگاه $a \in \bigcap_{\substack{P \in \mathrm{Spect}(R) \\ I \subseteq P}} P$ و لذا $a \in I$.

($\Leftarrow$): (برهان خلف) فرض کنید $\sqrt{I} \neq I$ و $a \in \sqrt{I} - I$. قرار می‌دهیم $a_1 = a$. چون I یک ایده‌آل نیم اول است، لذا $r_1 \in R$ چنان موجود است که $a_2 = a_1 r_1 a_1 \in R - I$. به همین ترتیب $r_2 \in R$ چنان موجود است که $a_3 = a_2 r_2 a_2 \in R - I$. با ادامهٔ این روند به مجموعهٔ $S = \{a_1, a_2, a_3, \ldots\}$ خواهیم رسید. به‌وضوح S یک زیرمجموعهٔ بسته ضربی تعمیم یافته از R است که $I \cap S = \varnothing$ و $a \in S$. بنابراین ایده‌آل اول P چنان موجود است که $I \subseteq P$ و $P \cap S = \varnothing$. ازاین‌رو $a \notin P$ و در نتیجه $a \notin \sqrt{I}$، که تناقض است.

■■■

نمادگذاری: فرض کنید R حلقه‌ای یکدار باشد. مجموعه ایده‌آل‌های ماکزیمال چپ حلقه R را با $\mathfrak{L}_R$ و مجموعه ایده‌آل‌های ماکزیمال راست حلقه R را با $\mathfrak{R}_R$ نمایش داده، قرار می‌دهیم:

$$J_r(R) = \bigcap_{\mathfrak{m} \in \mathfrak{R}_R} \mathfrak{m} \quad \text{و} \quad J_\ell(R) = \bigcap_{\mathfrak{m} \in \mathfrak{L}_R} \mathfrak{m}$$

www.mathematic87.blogfa.com

قضیه۱۱-۱۱

فرض کنید R حلقه‌ای یکدار باشد. دراین صورت گزاره‌های زیر معادلند.

(۱) $x \in J_\ell(R)$،

(۲) $1-ax$ برای هر $a \in R$ معکوس‌پذیر چپ است،

(۳) $xR \subseteq J_\ell(R)$،

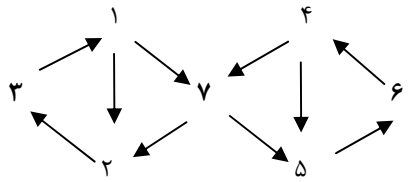
(۴) $x \in J_r(R)$،

(۵) $1-xb$ برای هر $b \in R$ معکوس‌پذیر راست است،

(۶) $Rx \subseteq J_r(R)$،

(۷) $1-axb$ برای هر $a,b \in R$ معکوس‌پذیر است.

اثبات: قضیه را مطابق نمودار زیر اثبات می‌کنیم.



(۲)$\Rightarrow$(۱): فرض کنید $x \in J_\ell(R)$. اگر $1-ax$ معکوس‌پذیر چپ نباشد، آنگاه ایده‌آل $\mathfrak{m} \in \mathfrak{L}_R$ چنان موجود است که $1-ax \subseteq \mathfrak{m}$. از طرفی $x \in \mathfrak{m}$، لذا $1 \in \mathfrak{m}$ که تناقض است.

(۳)$\Rightarrow$(۲): فرض کنید $a \in R$ چنان باشد که $xa \notin J_\ell(R)$. دراین‌صورت ایده‌آل $\mathfrak{m} \in \mathfrak{L}_R$ چنان موجود است که $xa \notin \mathfrak{m}$. بنابراین $Rxa + \mathfrak{m} = R$. ازاین‌رو

www.mathematic87.blogfa.com

عناصر $r \in R$ و $m \in \mathfrak{m}$ چنان موجودند که $rxa + m = a$. بعبارت دیگر $(1-rx)a = m$. اگر u معکوس چپ $1-rx$ باشد، آنگاه $a = um \in \mathfrak{m}$. یعنی $xa \in \mathfrak{m}$، که تناقض است.

(۱) $\Rightarrow$ **(۳)**: بدیهی است.

با استدلالی مشابه بالا داریم (۴) $\Rightarrow$ (۶) $\Rightarrow$ (۵) $\Rightarrow$ (۴).

(۲) $\Rightarrow$ **(۷)**: کافی است قرار دهیم $b = 1$.

(۵) $\Rightarrow$ **(۷)**: کافی است قرار دهیم $a = 1$.

(۷) $\Rightarrow$ **(۱)**: فرض کنید $a,b \in R$. دراین‌صورت $xb \in J_\ell(R)$ و لذا $1-a(xb)$ معکوس‌پذیر چپ است. فرض کنید $u(1-axb) = 1$. بنابراین $u = 1 - uaxb$. در نتیجه u معکوس چپ دارد. از اینرو $1-axb$ معکوس‌پذیر است.

(۴) $\Rightarrow$ **(۷)**: با استدلال(۷) $\Rightarrow$ (۱) مشابه است.

■■■

تعریف ۱۱- ۷ (رادیکال جیکوبسن)

فرض کنید R حلقه‌ای یکدار باشد. دراین صورت، رادیکال جیکوبسن R، که آنرا با $J(R)$ نشان می‌دهیم عبارت است از

$$J(R) = J_\ell(R) = J_r(R).$$

۱۱-۴ مدول‌ها

مدول‌ها تعمیمی از فضای برداری می‌باشند. در این بخش به طور مختصر مروری بر نظریه مدول‌ها خواهیم داشت. در سراسر این فصل R نشان دهندهٔ یک حلقهٔ دلخواه است.

www.mathematic87.blogfa.com

تعریف ۱۱-۸

گروه آبلی جمعی M همراه با ضرب (ضرب اسکالر)

$$R \times M \to M$$
$$(r, x) \mapsto rx$$

یک R-**مدول (چپ)** نامیده می‌شود اگر برای هر $x, y \in M$ و هر $r, s \in R$ داشته باشیم:

(۱) $r(x+y) = rx + ry$،

(۲) $(r+s)x = rx + sx$،

(۳) $r(sx) = (rs)x$.

اگر R یکدار و برای هر $x \in M$ داشته باشیم $1x = x$، M یک R- مدول چپ **یکانی** نامیده می‌شود.

❖ **تذکر:** R-مدول راست نیز به طریق مشابه تعریف می‌شود.

نمادگذاری: R- مدول چپ (راست) M را با نماد $(M_R)_R M$ نمایش می‌دهیم.

اگر R حلقه‌ای جابجایی باشد هر R- مدول چپ M با تعریف ضرب زیر یک R- مدول راست نیز هست.

$$M \times R \to M$$
$$(x, r) \mapsto rx$$

اگر R یک حلقه جابجایی باشد تمایز بین R- مدول چپ و راست ضروری نیست در چنین حالتی به طور ساده می‌گوییم R- مدول، بدون اینکه چیزی در مورد چپ یا راست بودن آن بیان کنیم.

مثال۵: هر فضای برداری روی میدان F، یک F- مدول است. به عبارت دیگر مدول‌ها

www.mathematic87.blogfa.com

تعمیمی از فضای برداری‌اند.

■

مثال ۶: حلقه R یک R - مدول (چپ و راست) است.

■

مثال ۷ : هر گروه آبلی G یک $\mathbb{Z}$–مدول یکانی است که در آن ضرب اسکالر به صورت زیر تعریف می‌شود.

$$\mathbb{Z} \times G \to G$$
$$(n, g) \mapsto ng.$$

■

مثال ۸: اگر I ایده‌آل چپی از حلقه R باشد، آنگاه گروه جمعی R/I با ضرب اسکالر زیر یک R -مدول چپ است.

$$R \times R/I \to R/I$$
$$(r, x + I) \mapsto rx + I.$$

■

مثال ۹: فرض کنید $\varphi : R \to S$ یک همریختی حلقه‌ای باشد. اگر M یک S - مدول چپ باشد. آنگاه M با ضرب اسکالر زیر یک R - مدول چپ نیز هست:

$$R \times M \to M$$
$$(r, x) \mapsto \varphi(r)\, x.$$

■

مثال ۱۰: فرض کنید $M_1, M_2, \ldots, M_n$، R - مدول‌هایی چپ باشند. در این صورت گروه آبلی $M_1 \times M_2 \times \ldots \times M_n$ همراه با ضرب اسکالر زیر R - مدول چپ است.

$$r\left(x_1, x_2, \ldots, x_n\right) = \left(rx_1, rx_2, \ldots, rx_n\right).$$

■

www.mathematic87.blogfa.com

تعریف ۱۱-۹

فرض کنید M یک R- مدول چپ باشد. زیر مجموعه ناتهی N از M یک **زیر مدول** نامیده می‌شود اگر N همراه با اعمال تعریف شده در M، یک R- مدول چپ باشد.

قضیه۱۱-۱۲(آزمون زیر مدول بودن)

فرض کنید N زیر مجموعه‌ای غیر تهی از ${}_RM$ باشد. N یک زیر مدول ${}_RM$ است اگر و فقط اگر N نسبت به تفاضل و ضرب اسکالر بسته باشد.

اثبات: اگر N یک زیر مدول باشد، آنگاه N بایستی تحت اعمال جمع و ضرب اسکالر بسته باشد. بر عکس، فرض کنید N نسبت به تفاضل و ضرب اسکالر بسته باشد. در این صورت N یک زیرگروه، گروه آبلی M است و سایر قوانین به طور خود به خود برقرار می‌باشند.

■■■

مثال ۱۱: اگر I ایده‌آل چپی از R باشد، آنگاه IM که به صورت زیر تعریف می‌شود یک زیر مدولی از M است.

$$IM = \{\sum_{i=1}^{n} r_i x_i \,\big|\, r_i \in I,\ x_i \in M,\ n \in \mathbb{N}\}.$$

■

مثال۱۲ (اشتراک زیرمدول‌ها) : فرض کنید $\{N_\alpha \,|\alpha \in \Lambda\}$ خانواده‌ای از زیر مدول‌های ${}_RM$ باشد. در این صورت $\bigcap_{\alpha\in\Lambda} N_\alpha$ زیر مدولی از ${}_RM$ است.

■

مثال۱۳ (مجموع زیرمدول‌ها) : فرض کنید $\{N_i\}_{i=1}^{n}$ خانواده‌ای از زیرمدول‌های ${}_RM$ باشد. تعریف می‌کنیم:

$$N_1 + N_2 + \cdots + N_n = \{x_1 + x_2 + \cdots + x_n \mid x_i \in N_i\}.$$

به‌وضوح $N_1 + N_2 + \cdots + N_n$ زیرمدولی از ${}_RM$ است. در حالت کلی، اگر $\{N_\alpha \,|\alpha \in \Lambda\}$ خانواده‌ای از زیر مدول‌های ${}_RM$ باشد، تعریف می‌کنیم:

$\sum_{\alpha\in\Lambda} N_\alpha = \{\sum_{\alpha\in\Lambda'} x_\alpha \mid x_\alpha \in N_\alpha, \Lambda$ باشد یک زیر مجموعهٔ متناهی از $\Lambda'\}$.

خواننده به آسانی می‌تواند نشان دهد که $\sum_{\alpha\in\Lambda} N_\alpha$ نیز زیرمدولی از $_RM$ است.

■

تعریف ۱۱-

فرض کنید X زیر مجموعه‌ای از $_RM$ باشد. اشتراک تمام زیر مدول‌های شامل X را **زیر مدول تولید شده** توسط X نامیده و آنرا با $< X >$ نمایش می‌دهیم. عناصر X را **مولدهای** زیر مدول $< X >$ می‌نامند. اگر $X = \{x_1, x_2, \ldots, x_n\}$، آنگاه زیر مدول $< X >$ را با $< x_1, x_2, \ldots, x_n >$ نمایش داده و آنرا **متناهی مولد** می‌گوییم. زیر مدول $< x >$ تولید شده توسط عنصر $x \in M$ را **زیر مدول دوری** تولید شده توسط x می‌نامیم.

▼ **یادداشت:** $_RM$ را متناهی مولد گوییم اگر $_RM$ به عنوان یک زیر مدول خودش متناهی مولد باشد.

قضیه ۱۱-۱۳

اگر $X \subseteq {}_RM$، $x \in M$ و $Rx = \{rx \mid r \in R\}$، آنگاه

(۱) Rx یک زیر مدول $_RM$ است،

(۲) $< x >= Rx$، و اگر $_RM$ یکانی باشد، $< x >= \{rx + nx \mid r \in R,\ n \in \mathbb{Z}\}$،

(۳) $< X >= \{\sum_{i=1}^{s} r_i x_i + \sum_{j=1}^{t} n_j y_j \mid s,t \in \mathbb{N}, x_i, y_j \in X, r_i \in R, n_j \in \mathbb{Z}\}$.

اگر $_RM$ یکانی باشد، آنگاه $< X >= RX = \{\sum_{i=1}^{s} r_i x_i \mid s \in \mathbb{N}, x_i \in X, r_i \in R\}$.

(۴) اگر $\{N_\alpha \mid \alpha \in \Lambda\}$ خانواده‌ای از زیر مدول‌های $_RM$ باشد، آنگاه $\sum_{\alpha\in\Lambda} N_\alpha = < \bigcup_{\alpha\in\Lambda} N_\alpha >$.

www.mathematic87.blogfa.com

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضیه۱۱-۱۴ (مدول‌های خارج قسمتی)

فرض کنید N زیر مدولی از ${}_RM$ باشد. در این صورت گروه آبلی M/N همراه با ضرب اسکالر زیر یک R- مدول چپ است

$$R\times M/N \to M/N$$
$$(r, x+N) = rx+N.$$

M/N را **مدول خارج قسمتی** M بر N می‌نامیم.

اثبات: نشان می‌دهیم که ضرب فوق خوش تعریف است. فرض کنید $(r_1, x_1+N) = (r_2, x_2+N)$. بنابراین $r = r_1 = r_2$ و $x_1 - x_2 \in N$. لذا $r_1(x_1-x_2) \in N$ پس $rx_1 + N = rx_2 + N$ و یا $r_1x_1 + N = r_2x_2 + N$. یعنی عمل ضرب خوش تعریف است. بقیه اثبات را به عهده خواننده واگذار می‌کنیم.

■■■

تعریف ۱۱-۱۱

تابع ${}_RM \to {}_RN$: φ را یک **همریختی** (هوموورفیسم) $R-$مدولی گوییم هرگاه φ حافظ اعمال جمع و ضرب اسکالر باشد. به عبارت دیگر برای هر $r \in R$ و هر $x, y \in M$ داشته باشیم :

(۱) $\varphi(x+y) = \varphi(x) + \varphi(y)$،

(۲) $\varphi(rx) = r\varphi(x)$.

تعریف ۱۱-۱۲

فرض کنید ${}_RM \to {}_RN$: φ یک همریختی R- مدولی باشد. **تصویر و هسته** φ را به صورت زیر تعریف می‌کنیم:

$$\varphi \text{ تصویر} = \operatorname{Im}\varphi = \varphi(M) = \{\varphi(x) | x \in M\},$$
$$\varphi \text{ هسته} = \operatorname{Ker}\varphi = \{x \in M | \varphi(x) = 0\}.$$

به آسانی می‌توان تحقیق نمود که $\operatorname{Ker}\varphi$ زیر مدولی از ${}_RM$ و $\operatorname{Im}\varphi$ زیر مدولی از ${}_RN$ می‌باشد.

تعریف ۱۱-۱۳

همریختی R- مدولی ${}_RM \to {}_RN : \varphi$ را یک **یکریختی** (ایزومورفیسم) R- مدولی گوییم، اگر φ یک به یک و پوشا باشد. وقتی R- یکریختی ${}_RM \to {}_RN : \varphi$ باشد، گوییم ${}_RM$ با ${}_RN$ یکریخت است و می‌نویسیم ${}_RM \cong {}_RN$.

همریختی ${}_RM \to {}_RN : \varphi$ را **تکریختی** (مونومورفیسم) $R-$مدولی گوییم، اگر φ یک به یک باشد.

همریختی ${}_RM \to {}_RN : \varphi$ را **برووریختی** (اپی‌مورفیسم) $R-$مدولی گوییم، اگر φ پوشا باشد.

در نظریهٔ مدول‌ها نیز قضایایی مشابه با قضایای یکریختی و قضیه تناظر در نظریه گروه‌ها و حلقه ها خواهیم داشت که به علت مشابه بودن استدلالها از اثبات آنها صرف‌نظر می کنیم:

قضیه۱۱-۱۵ (قضیه اول یریختی)

اگر ${}_RM \to {}_RN : \varphi$ یک همریختی R- مدولی باشد، آنگاه φ یکریختی R- مدولی زیر را القاء می‌کند

$$M / \operatorname{Ker}\varphi \cong \operatorname{Im}\varphi.$$

قضیه۱۱-۱۶ (قضیه دوم و سوم یکریختی)

فرض کنید K, N زیر مدول‌هایی از ${}_RM$ باشند.

(۱) $N/(N \cap K) \cong (N+K)/K$،

(۲) اگر K زیر مدولی از N باشد، آنگاه N/K زیر مدولی از M/K است و

$$\frac{M/K}{N/K} \cong \frac{M}{N}.$$

قضیه۱۱-۱۷ (قضیه تناظر)

فرض کنید N زیر مدولی از ${}_RM$ باشد. تناظر، $K \leftrightarrow K/N$، یک دوسویی بین زیر مدول‌های ${}_RM$ که شامل N هستند و زیر مدول‌های M/N برقرار می‌سازد. از این روهر زیر مدول در M/N، به صورت K/N می‌باشد که در آن K زیر مدولی از ${}_RM$ است به قسمی که $N \subseteq K$.

تعریف ۱۱-۱۴

گوییم ${}_RM$ در شرط ACC **(شرط زنجیر صعودی)** روی زیر مدول‌هایش صدق می‌کند. اگر هر زنجیر صعودی از زیر مدول‌هایش ایستا باشد. به عبارت دیگر اگر $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ یک زنجیر صعودی از زیر مدول‌های ${}_RM$ باشد، آنگاه $k \in \mathbb{N}$ موجود باشد که $N_k = N_{k+1} = N_{k+2} = \ldots$.

تعریف ۱۱-۱۵

گوییم ${}_RM$ در شرط DCC **(شرط زنجیر نزولی)** روی زیر مدول‌هایش صدق می‌کند اگر هر زنجیر نزولی از زیر مدول‌هایش ایستا باشد. به عبارت دیگر اگر $N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$ یک زنجیر نزولی از زیر مدول‌های ${}_RM$ باشد، آنگاه $k \in \mathbb{N}$ موجود باشد که $N_k = N_{k+1} = N_{k+2} = \ldots$

قضیه۱۱-۱۸

شرایط زیر روی ${}_RM$ معادلند.

(۱) ${}_RM$ در شرط ACC روی زیر مدول‌هایش صدق می‌کند،

(۲) هر خانواده غیر تهی از زیر مدول‌های ${}_RM$ دارای عنصر ماکزیمال است،

(۳) هر زیر مدول ${}_RM$ متناهی مولد است.

اثبات (۲) $\Rightarrow$**(۱)**: فرض کنید Ω یک خانواده غیر تهی از زیر مدول‌های M باشد که دارای عنصر ماکزیمال نیست. فرض کنید $N_1 \in \Omega$، چون Ω دارای عنصر ماکزیمال نیست، لذا $N_2 \in \Omega$ چنان موجود است که $N_1 \subsetneq N_2$. دوباره چون Ω دارای عنصر ماکزیمال نیست لذا $N_3 \in \Omega$ چنان موجود است که $N_1 \subsetneq N_2 \subsetneq N_3$. با ادامه این روند زنجیر صعودی ناایستای زیر خواهیم داشت.

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots \subsetneq N_t \subsetneq \cdots.$$

(۳) $\Rightarrow$**(۲)**: فرض کنید N زیر مدولی از ${}_R M$ باشد. فرض کنید Ω خانوادهٔ همه زیرمدول‌های متناهی مولد N باشد. چون $(0) \in \Omega$، لذا $\Omega \neq \varnothing$. بنابراین طبق فرض Ω دارای عنصر ماکزیمال است. فرض کنید N_0 عنصر ماکزیمال Ω باشد. اگر $x \in N$، آنگاه $N_0 + < x > \in \Omega$ یک مدول متناهی مولد از N است و لذا با توجه به ماکزیمال بودن N_0 خواهیم داشت $N_0 + < x >= N$. بنابراین $x \in N_0$ ودر نتیجه $N_0 = N$. ازاین‌رو N متناهی مولد است.

(۱) $\Rightarrow$**(۳)**: فرض کنید $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ یک زنجیر صعودی از زیر مدول‌های ${}_R M$ باشد. قرار می‌دهیم $N = \bigcup_{k=1}^{\infty} N_k$. به‌وضوح N یک زیر مدول ${}_R M$ است. چون N متناهی مولد است لذا $N =< x_1, x_2, \ldots, x_n >$. فرض کنید $(1 \leq i \leq n)\, x_i \in N_{k_i}$. اگر $k = \max\{k_i\}_{i=1}^{n}$، آنگاه با توجه به صعودی بودن زنجیر خواهیم داشت، $N \subseteq N_k$ و لذا

$$N = N_k = N_{k+1} = N_{k+2} = \cdots.$$

■■■

به آسانی می‌توان بررسی کرد که ${}_R M$ متناهی مولد است اگر وفقط اگر برای هر خانواده، $\{N_\alpha\}_{\alpha \in \Lambda}$، از زیرمدول‌های ${}_R M$ داشته باشیم:

$$M = \sum_{\alpha \in \Lambda} N_\alpha \Rightarrow M = \sum_{\alpha \in \Lambda'} N_\alpha,$$

www.mathematic87.blogfa.com

که Λ' یک زیرمجموعه متناهی از Λ است. با توجه به مطلب اخیر، می‌توان دوگان مفهوم متناهی مولد را مطرح ساخت:

تعریف ۱۱-۱۶

$_RM$ را **متناهی هم-مولد** گوییم. اگر برای هر خانواده، $\{N_\alpha\}_{\alpha\in\Lambda}$، از زیرمدول‌های $_RM$ داشته باشیم

$$\bigcap_{\alpha\in\Lambda} N_\alpha = (0) \Rightarrow \bigcap_{\alpha\in\Lambda'} N_\alpha = (0),$$

که در اینجا Λ' یک زیرمجموعه متناهی از Λ است.

قضیه۱۱-۱۹

شرایط زیر روی $_RM$ معادلند.

(۱) $_RM$ در شرط DCC روی زیر مدول‌هایش صدق می‌کند،

(۲) هر خانواده غیر تهی از زیر مدول‌های $_RM$ دارای عنصر مینیمال است،

(۳) هر خارج قسمت $_RM$ متناهی هم- مولد است.

اثبات (۲) $\Rightarrow$**(۱)**: (فرض خلف) فرض کنید Ω یک خانواده غیر تهی از زیر مدول‌های M باشد که دارای عنصر مینیمال نیست. فرض کنید $N_1 \in \Omega$، چون Ω دارای عنصر مینیمال نیست، لذا $N_2 \in \Omega$ چنان موجود است که $N_1 \supsetneq N_2$. دوباره چون Ω دارای عنصر مینیمال نیست لذا $N_3 \in \Omega$ چنان موجود است که $N_1 \supsetneq N_2 \supsetneq N_3$. با ادامه این روند زنجیر نزولی ناایستای زیر را خواهیم داشت.

$$N_1 \supsetneq N_2 \supsetneq N_3 \supsetneq \cdots \supsetneq N_t \supsetneq \cdots,$$

که با فرض در تناقض است.

(۳) $\Rightarrow$**(۲)**: فرض کنید M/N یک خارج قسمت از M باشد و $\bigcap_{\alpha\in\Lambda}(M_\alpha/N) = (0)$. در اینصورت $\bigcap_{\alpha\in\Lambda} M_\alpha = N$. قرار می‌دهیم:

$$\Omega = \{\bigcap_{\alpha\in\Lambda'} M_\alpha \mid \Lambda' \subseteq \Lambda,\ \left|\Lambda'\right| < \infty\}.$$

www.mathematic87.blogfa.com

با توجه به فرض Ω دارای عنصر مینیمال است. فرض کنید $\bigcap_{\alpha\in\Lambda'} M_\alpha$ عنصر مینیمال Ωباشد. در این‌صورت به آسانی می‌توان نشان داد که $\bigcap_{\alpha\in\Lambda'} M_\alpha = N$. در نتیجه $\bigcap_{\alpha\in\Lambda'} (M_\alpha / N) = (0)$.

(۱) ⇒(۳): فرض کنید $N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$ یک زنجیر نزولی از زیر مدول‌های ${}_RM$ باشد. قرار می‌دهیم $N = \bigcap_{k=1}^{\infty} N_k$. در این‌صورت $\bigcap_{k=1}^{\infty} (N_k / N) = (0)$. درنتیجه طبق فرض زیرمجموعهٔ متناهی $A \subseteq \mathbb{N}$ به‌گونه‌ای موجود است که $N = \bigcap_{k\in A} N_k$. حال اگر kعنصر ماکزیمال A باشد، خواهیم داشت:

$$N = N_k = N_{k+1} = N_{k+2} = \ldots.$$

■■■

تعریف ۱۱-۱۷

${}_RM$ را **نوتری (آرتینی)** گوییم اگر در شرایط معادل قضیه ۱۸ (۱۹) صدق کند.

قضیهٔ معروفی بنام قضیهٔ کوهن، شرط ضعیفی برای نوتری بودن یک مدول ارایه می‌دهد. دراینجا اثباتی ساده از منبع زیر برای قضیهٔ کوهن می آوریم.

Naghipour, A. R. *A Simple Proof of Cohen's Theorem*, Amer. Math. Monthly. 112(9), 825-826 (2005).

نماد گذاری: فرض کنید ${}_RM$ یک مدول باشد و X یک زیر مجموعهٔ ناتهی از Mباشد. قرار می‌دهیم:

$$\mathrm{Ann}(X) := \{r \in R \mid rX = 0\}.$$

www.mathematic87.blogfa.com

$\mathrm{Ann}(X)$ یک ایده‌آل چپ از حلقهٔ R بوده که **پوچ‌ساز** زیر مجموعهٔ X از ${}_RM$ نامیده می‌شود.

قضیه ۱۱-۲۰ (قضیه کوهن)

فرض کنید M یک مدول متناهی مولد روی حلقهٔ جابجایی و یکدار R باشد. در این‌صورت:
برای هر $\mathfrak{p} \in \mathrm{Spec}(R)$، زیر مدول $\mathfrak{p}M$ متناهی مولد است $\Leftrightarrow$ M نوتری است

اثبات : کافی است قسمت $(\Leftarrow)$ ثابت شود. (برهان خلف) فرض کنید M نوتری نباشد. با توجه به لم زرن، فرض کنید N زیر مدولی از M باشد که در بین زیر مدول‌های غیر متناهی مولد ماکزیمال باشد. نشان می‌دهیم $\mathfrak{p} := \mathrm{Ann}(M/N)$ یک ایده‌آل اول است. فرض کنید $ab \in \mathfrak{p}$ و $a \notin \mathfrak{p}$ و $b \notin \mathfrak{p}$. در این‌صورت $N + aM$ یک زیرمدول متناهی مولد می‌باشد. فرض کنید $\{n_i + am_i\}_{i=1}^{\ell}$ مولدی برای $N + aM$ باشد. قرار می‌دهیم $L := \{m \in M \mid am \in N\}$ به آسانی می‌توان مشاهده نمود که L زیرمدولی از M و شامل N و bM می‌باشد. از این‌رو با توجه به ماکزیمال بودن N، L یک زیرگروه متناهی مولد است. نشان می‌دهیم $N = \sum_{i=1}^{\ell} Rn_i + aL$. فرض کنید $y \in N$. دراین‌صورت $y \in N + aM$ و در نتیجه عناصر $b_1,\ldots,b_\ell \in R$ چنان موجودند که

$$y = \sum_{i=1}^{\ell} b_i(n_i + am_i) = \sum_{i=1}^{\ell} b_i n_i + a\sum_{i=1}^{\ell} b_i m_i.$$

بنابراین $a\sum_{i=1}^{\ell} b_i m_i \in N$ و لذا $y \in \sum_{i=1}^{\ell} Rn_i + aL$. چون طرف دیگر شمول بدیهی است، پس $N = \sum_{i=1}^{\ell} Rn_i + aL$. از اینجا N متناهی مولد می‌شود، که تناقض است، پس $\mathfrak{p}$ یک ایده‌آل اول است. فرض کنید $M/N = R(x_1 + N) + \cdots + R(x_t + N)$، که $x_i \in M$. داریم $\mathfrak{p} = \bigcap_{i=1}^{t} \mathrm{Ann}(Rx_i + N)$ و با توجه به اول بودن $\mathfrak{p}$، $1 \le j \le t$ چنان موجود است

www.mathematic87.blogfa.com

که $\mathfrak{p} = \mathrm{Ann}(Rx_j + N)$. فرض کنید $\{y_i + r_i x_j\}_{i=1}^{k}$ مولدی برای $N + Rx_j$ باشد. با استدلالی مشابه قبل، خواهیم داشت $N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j$. با توجه به $\mathfrak{p}M \subseteq N$، داریم:

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j \subseteq \sum_{i=1}^{k} Ry_i + \mathfrak{p}M \subseteq \sum_{i=1}^{k} Ry_i + N \subseteq N.$$

از این‌رو $N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}M$ یک زیر مدول متناهی مولد از M بوده که تناقض است. بنابراین M نوتری است.

■■■

تعریف ۱۱-۱۸

حلقه R را **نوتری (آرتینی) چپ** گوییم اگر ${}_R R$ نوتری (آرتینی) باشد. همچنین R را **نوتری (آرتینی) راست** گوییم اگر R_R نوتری (آرتینی) باشد. حلقه R را **نوتری (آرتینی)** گوییم اگر هم نوتری (آرتینی) چپ و هم نوتری (آرتینی) راست باشد.

مثال ۱۴: چون $\mathbb{Z}$ یک PID است لذا $\mathbb{Z}$ یک حلقه نوتری است. از طرفی $\mathbb{Z}$ آرتینی نیست، زیرا که داریم

$$< 2 > \supsetneq < 2^2 > \supsetneq < 2^3 > \supsetneq \cdots.$$

■

مثال ۱۵: فرض کنید p عددی اول باشد. قرار می‌دهیم:

$$\mathbb{Z}(p^\infty) = \{a / p^n + \mathbb{Z} | a \in \mathbb{Z} \ , \ n = 0,1,2,\ldots\}.$$

$\mathbb{Z}(p^\infty)$ زیر گروهی از $\mathbb{Q} / \mathbb{Z}$ است.

برای $\ell = 0,1,2,\ldots$ قرار می دهیم:

$$G_\ell = < 1 / p^\ell + \mathbb{Z} > = \{a / p^\ell + \mathbb{Z} | a \in \mathbb{Z}\}.$$

نشان می دهیم که هر زیر گروه سره $\mathbb{Z}(p^\infty)$ به‌شکل G_ℓ ها می باشند.

www.mathematic87.blogfa.com

فرض کنید H یک زیر گروه سره‌ای از $\mathbb{Z}(p^\infty)$ باشد. فرض کنید n بزرگترین عددی صحیح مثبتی باشد که $1/p^n+\mathbb{Z}\in H$ و $1/p^{n+1}+\mathbb{Z}\notin H$، ادعا می‌کنیم $H=G_n$. واضح است $G_n\subseteq H$. فرض کنید $h\in H-G_n$. بنابراین عناصر $a\in\mathbb{Z}$ و $i\in\mathbb{N}$ چنان موجودند که $h=a/p^{n+i}+\mathbb{Z}$ و $(a,p)=1$. چون $(a,p)=1$ لذا $(a,p^{n+i})=1$ و در نتیجه عناصر $x,y\in\mathbb{Z}$ چنان موجودند که $ax+p^{n+i}y=1$. پس

$$1/p^{n+i}+\mathbb{Z}=(ax+p^{n+i}y)/p^{n+i}+\mathbb{Z}=(ax)/p^{n+i}+\mathbb{Z}\in H$$

و در نتیجه $1/p^{n+1}+\mathbb{Z}\in H$، که تناقض است. با توجه به زنجیر صعودی

$$G_0\subsetneq G_1\subsetneq G_2\subsetneq\cdots,$$

$\mathbb{Z}(p^\infty)$ یک $\mathbb{Z}$- مدول نوتری نیست. اما با توجه به متناهی بودن G_ℓ ها، $\mathbb{Z}(p^\infty)$ یک $\mathbb{Z}$- مدول آرتینی است.

■

▼ **یادداشت:** مثال فوق نشان می‌دهد که یک مدول نوتری لزوماً آرتینی نیست. ولی در مورد حلقه‌های جابجایی ثابت خواهیم کرد که هر حلقه آرتینی یک حلقه نوتری است.

قضیه۱۱-۲۱

فرض کنید V یک فضای برداری روی میدان F باشد. در این صورت شرایط زیر معادلند.

(۱) $\dim_F V<\infty$،

(۲) V به عنوان F- مدول نوتری است،

(۳) V به عنوان F مدول آرتینی است.

اثبات: **(۲)** $\Rightarrow$ **(۱)** و **(۳)** $\Rightarrow$ **(۱)** بدیهی‌اند.

(۱) $\Rightarrow$ **(۲)** و **(۱)** $\Rightarrow$ **(۳)**: فرض کنید $\dim_F V=\infty$. فرض کنید B پایه‌ای برای V باشد و $\{x_i\}_{i=1}^{\infty}\subseteq B$. در این صورت زنجیرهای زیر را خواهیم داشت:

www.mathematic87.blogfa.com

$$< x_1 > \subsetneq < x_1, x_2 > \subsetneq < x_1, x_2, x_3 > \subsetneq \dots,$$
$$< x_1, x_2, x_3, \dots > \supsetneq < x_2, x_3, \dots > \supsetneq < x_3, x_4, \dots > \supsetneq \dots,$$

که با فرض در تناقض می‌باشند.

■■■

قضیه۱۱-۲۲

فرض کنید N زیر مدولی از ${}_RM$ باشد. در این صورت

$M/N,\ N$ نوتری (آرتینی)باشند $\Leftrightarrow$ M نوتری (آرتینی) است

اثبات: مطلب را در مورد نوتری ثابت می‌کنیم در مورد آرتینی اثبات مشابه است.

$(\Rightarrow)$: چون هر زیر مدول N یک زیرمدول ${}_RM$ است، لذا هر زنجیر صعودی از زیرمدول‌های N ایستاست. یعنی N نوتری است. حال فرض کنید

$$M_1/N \subseteq M_2/N \subseteq M_3/N \subseteq \dots,$$

یک زنجیر صعودی از زیرمدول‌های M/N باشد. در این‌صورت

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots,$$

یک زنجیر صعودی از زیرمدول‌های M است. بنابراین طبق فرض $k \in \mathbb{N}$ موجود است که $M_k = M_{k+1} = M_{k+2} = \dots$. ازاین‌رو $M_k/N = M_{k+1}/N = M_{k+2}/N = \dots$، یعنی M/N نوتری است.

$(\Leftarrow)$: فرض کنید $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ یک زنجیر صعودی از زیر مدول‌های M باشد. داریم:

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \cdots,$$
$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq (M_3 + N)/N \subseteq \cdots.$$

www.mathematic87.blogfa.com

با توجه به فرض عدد طبیعی k چنان موجود است که برای هر $i = 1,2,\ldots$، $M_k \cap N = M_{k+i} \cap N$ و $M_k + N = M_{k+i} + N$. ادعا می‌کنیم $M_k = M_{k+i}$. فرض کنید $x \in M_{k+i}$. در این صورت

$$x \in M_{k+i} + N = M_k + N \Rightarrow$$
$$x = a + b,\ \ a \in M_k, b \in N \Rightarrow x - a = b \in N \Rightarrow$$
$$x - a \in M_{k+i} \cap N = M_k \cap N \Rightarrow x - a \in M_k \Rightarrow x \in M_k.$$

یعنی M نوتری است.

■■■

❖ **تذکر:** توجه داشته باشید که زیر حلقهٔ یک حلقه آرتینی (نوتری) لزوماً نوتری نیست. به‌عنوان مثال،

$\mathbb{Q}$ یک حلقهٔ آرتینی است ولی همان‌طوری که می‌دانیم $\mathbb{Z}$ به‌عنوان یک زیر حلقهٔ $\mathbb{Q}$ آرتینی نیست. برای مثالی در حالت نوتری به تمرین ۲۲ مراجعه نمایید.

لم۱۱-۱

فرض کنید I ایده‌آلی از حلقه R و ${}_RM$ مدولی باشد که $IM = 0$ (یعنی $I \subseteq \mathrm{Ann}(M)$). در این صورت

(۱) M ساختار R/I−مدول چپ دارد،

(۲) اگر N یک زیرمجموعه از M باشد، آنگاه

N یک زیر مدول ${}_RM$ است $\Leftrightarrow$ N یک زیر مدول ${}_{R/I}M$ باشد.

(۳) ${}_RM$ نوتری (آرتینی) است اگر و فقط اگر ${}_{R/I}M$ نوتری (آرتینی) باشد.

اثبات (۱): تعریف می‌کنیم:

$$R/I \times M \to M$$
$$(r + I, x) = rx$$

www.mathematic87.blogfa.com

نشان می‌دهیم که این ضرب اسکالر خوش تعریف است. فرض کنید $(r_1+I,x_1)=(r_2+I,x_2)$ بنابراین $r_1-r_2\in I, x_1=x_2$ لذا $(r_1-r_2)x_1=0$ یعنی $r_1x_1=r_2x_1=r_2x_2$. بررسی بقیه خواص به خواننده واگذار می‌شود.

(۲): با توجه به قسمت (۱)، داریم $rx\in N\Leftrightarrow (r+I)x\in N$. از طرف دیگر اعمال جمع در ${}_RM$ و ${}_{R/I}M$ یکسانند، لذا حکم با توجه به آزمون زیر مدول بودن به دست می‌آید

(۳): به آسانی از قسمت (۲) نتیجه می‌شود.

■■■

لم ۱۱-۲ (لم ناکایاما)

فرض کنید M یک مدول متناهی مولد روی حلقه جابجایی و یکدار R و I ایده‌آلی از R باشد که $IM=M$. در این صورت $a\in I$ چنان موجود است که $(1-a)M=0$.

اثبات: فرض کنید $M=<x_1,x_2,\ldots,x_n>$. دراین‌صورت

$$\begin{aligned}
x_1\in IM &\Rightarrow\ x_1=a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\\
x_2\in IM &\Rightarrow\ x_2=a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\\
&\ \ \vdots\\
x_n\in IM &\Rightarrow\ x_n=a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n
\end{aligned}$$

که در اینجا $a_{ij}\in I$. حال

$$\begin{cases}
(1-a_{11})x_1-a_{12}x_2-\cdots-a_{1n}x_n=0\\
-a_{21}x_1+(1-a_{22})x_2-\cdots-a_{2n}x_n=0\\
\qquad\qquad\vdots\\
-a_{n1}x_1-a_{n2}x_2-\cdots+(1-a_{nn})x_n=0
\end{cases}$$

و در نتیجه

$$\Rightarrow \begin{bmatrix} 1-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & 1-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ -a_{n1} & -a_{n1} & \cdots & 1-a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

اگر $A = \left[a_{ij}\right]_{n\times n}$ و $B = I - A$ و $X = \left[x_i\right]_{n\times 1}$ و $\overline{0} = [0]_{n\times 1}$، آنگاه

$$BX = \overline{0} \;\Rightarrow \operatorname{adj}(B)\,BX = \overline{0} \;\Rightarrow (\det B)\,X = \overline{0} \;\Rightarrow (\det B)\,M = 0$$

از طرفی با توجه به بسط دترمینان B خواهیم داشت که $\det B = 1 - a$، که $a \in I$.

■■■

نتیجه زیر به آسانی از لم ناکایاما و قضیه ۱۱ بدست می‌آید.

نتیجه۱۱-۲

فرض کنید M یک مدول متناهی مولد روی حلقه جابجایی و یکدار R و I ایده‌آلی از R باشد که $I \subseteq J(R)$ و $IM = M$. در این صورت $M = 0$.

قضیه۱۱-۲۳

فرض کنید R حلقه‌ای جابجایی و یکدار و آرتینی باشد.

(۱) R دارای تعداد متناهی ایده‌آل ماکزیمال است،

(۲) $J = J(R)$ یک ایده‌آل پوچ توان است (یعنی عدد طبیعی n چنان هست که $J^n = 0$).

اثبات (۱): فرض کنید تعداد ایده‌آل‌های ماکزیمال R نامتناهی باشد و $\left\{\mathfrak{m}_i\right\}_{i=1}^{\infty}$ یک خانواده از ایده‌آل‌های ماکزیمال (متمایز) R باشد. زنجیر نزولی زیر را در نظر بگیرید.

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supseteq \cdots.$$

ادعا می‌کنیم که این زنجیر اکید می‌باشد. فرض کنید $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k\mathfrak{m}_{k+1}$ در این صورت

www.mathematic87.blogfa.com

$$\mathfrak{m}_{k+1} \supseteq \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k\mathfrak{m}_{k+1} = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$$

لذا $1 \le i \le k$ موجود است که $\mathfrak{m}_{k+1} \supseteq \mathfrak{m}_i$، یعنی $\mathfrak{m}_{k+1} = \mathfrak{m}_i$، که تناقض می‌باشد. لذا زنجیر اکید می‌باشد، که متناقض با آرتینی بودن حلقه است. بنابراین تعداد ایده‌آل‌های ماکزیمال R باید متناهی باشد.

(۲): زنجیر زیر را در نظر می‌گیریم.

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots.$$

باتوجه به آرتینی بودن R، عدد $n \in \mathbb{N}$ به‌گونه‌ای موجود است که $J^n = J^{n+1}$. فرض کنید $I = J^n$. اگر $I = 0$ باشد، قضیه اثبات است. در غیر این‌صورت قرار می‌دهیم:

$$\Omega = \{K \mid R \text{ یک ایده‌ال سره } K,\ IK \neq 0\}.$$

باتوجه به اینکه $I^2 = I$، خواهیم داشت $I \in \Omega$، لذا $\Omega \neq \varnothing$. فرض کنید K عنصر مینیمال Ω باشد. چون $IK \neq 0$، لذا $k \in K$ چنان موجود است که $I < k >= Ik \neq 0$. با توجه به مینیمال بودن K خواهیم داشت $K =< k >$. از طرفی $IJk = Ik \neq 0$، لذا $J < k >= K =< k >$ و بنابر نتیجه ۲، خواهیم داشت $k = 0$، که تناقض است.

■■■

قضیه ۱۱-۲۴

فرض کنید R یک حلقه جابجایی و یکدار و M یک R- مدول باشد. اگر ایده‌آل‌های ماکزیمال $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ چنان موجود باشند که $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n M = 0$، آنگاه
M آرتینی است $\Leftrightarrow$ M نوتری است

اثبات: مطلب را با استقرا روی n ثابت می‌کنیم. فرض کنید $n = 1$ در این صورت $\mathfrak{m}_1 M = 0$ و لذا M یک فضای برداری روی میدان $R/\mathfrak{m}_1$ می‌باشد و لذا طبق قضیه ۲۱ و لم۱ حکم برقرار است. حال فرض کنید ایده‌آل‌های ماکزیمال $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ چنان موجود باشد که $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n M = 0$ قرار می‌دهیم $N = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{n-1}M$. در این صورت $\mathfrak{m}_n N = 0$, $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{n-1}(M/N) = 0$. حال اگر M نوتری (آرتینی) باشد

www.mathematic87.blogfa.com

آنگاه طبق قضیه ۲۲، مدولی‌های N و M/N نوتری (آرتینی) می‌باشند و لذا طبق فرض استقرا N و M/N مدول‌هایی آرتینی (نوتری) می‌باشند و با استفاده مجدد از قضیه ۲۲، M مدولی آرتینی (نوتری) می‌شود.

■■■

نتیجه ۱۱-۳

هر حلقه جابجایی و یکدار آرتینی R، نوتری است.

اثبات: با توجه به قضیه ۲۳ ایده‌آل‌های ماکزیمال $\mathfrak{m}_1,\dots,\mathfrak{m}_n$ (نه لزوماً متمایز) از R چنان موجودند که $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n=0$ و لذا $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_nR=0$. بنابراین طبق قضیه ۲۴، R حلقه‌ای نوتری است.

■■■

تمرینها

۱. فرض کنید R حلقه‌ای جابجایی و یکدار باشد. ثابت کنید ایده‌آل اول $P\in \operatorname{Spect}(R)$ چنان موجود است که $P\subseteq Z(R)$.

۲. فرض کنید $P_1,P_2,\dots,P_n$ ایده‌آل‌های اولی از حلقه جابجایی و یکدار R باشند. اگر $S=\bigcap_{i=1}^{n}\left(R-P_i\right)$، آنگاه حلقه $S^{-1}R$ دارای تعداد متناهی ایده‌آل ماکزیمال است.

۳. فرض کنید R حلقه‌ای جابجایی و یکدار و S یک زیر مجموعه بسته ضربی از R باشد. اگر R یک PID باشد، آنگاه $S^{-1}R$ نیز یک PID است.

www.mathematic87.blogfa.com

۴. (یادآوری) حلقه جابجایی و یکدار R را فون نیومن منظم گوییم اگر برای هر $a \in R$ داشته باشیم $a \in aRa$. نشان دهید شرایط زیر معادلند:

(a) R یک حلقه فون نیومن منظم است،

(b) برای هر $\mathfrak{m} \in \mathrm{Max}(R)$ $R_{\mathfrak{m}}$ یک میدان است،

(c) هر ایده‌آل اول حلقه R ماکزیمال است و از $a^2 = 0$ خواهیم داشت $a = 0$.

۵. فرض کنید R یک حوزه صحیح باشد. برای هر ایده‌آل ماکزیمال $\mathfrak{m}$، $R_{\mathfrak{m}}$ را به عنوان زیر حلقه‌ای از میدان کسرهای R در نظر بگیرید. ثابت کنید:

$$\bigcap_{\mathfrak{m} \in \mathrm{Max}(R)} R_{\mathfrak{m}} = R.$$

۶. فرض کنید I ایده‌آلی از حلقه R باشد. ایده‌آل اول P از R را یک ایده‌آل اول مینیمال از I گوییم اگر $I \subseteq P$ و ایده‌آل اولی مانند P' از R موجود نباشند به طوریکه $I \subseteq P' \subsetneq P$. ایده‌آل اول مینیمال ایده‌آل $\{0\}$ را ایده‌آل اول مینیمال حلقه R گوییم. نشان دهید:

(a) اگر I و P ایده‌آل‌هایی از حلقه R باشند به طوریکه P اول و $I \subseteq P$، آنگاه P شامل یک ایده‌آل اول مینیمال از I می‌باشد،

(b) هر ایده‌آل سره از حلقه جابجایی و یکدار R حداقل یک ایده‌آل اول مینیمال دارد.

۷. فرض کنید C ایده‌آلی از حلقه یکدار R باشد. نشان دهید شرایط زیر معادلند:

(a) C یک ایده‌آل نیم اول است،

(b) برای هر $a \in R$، اگر $(a)^2 \subseteq C$ آنگاه $a \in C$،

(c) برای هر $a \in R$ ، اگر $aRa \subseteq C$ آنگاه $a \in C$،

(d) برای هر ایده‌آل چپ A از R ، اگر $A^2 \subseteq C$ آنگاه $A \subseteq C$،

www.mathematic87.blogfa.com

(e) برای هر ایده‌آل راست A از R ، اگر $A^2 \subseteq C$ آنگاه $A \subseteq C$.

۸. فرض S یک زیر مجموعه بسته ضربی از حلقه جابجایی و یکدار R باشد. اگر I ایده‌آلی از R باشد، آنگاه $S^{-1}(\sqrt{I}) = \sqrt{S^{-1}I}$.

۹. فرض کنید R و S دو حلقهٔ جابجایی و یکدار و $\varphi : R \to S$ یک همریختی حلقه‌ای باشد. ثابت کنید:

(a) اگر I ایده‌آلی از R باشد، آنگاه $< \varphi(\sqrt{I}) > \subseteq \sqrt{< \varphi(I) >}$. تحت چه شرایطی تساوی رخ می‌دهد،

(b) اگر J ایده‌آلی از S باشد، آنگاه $\sqrt{\varphi^{-1}(J)} = \varphi^{-1}(\sqrt{J})$.

۱۰. حلقه یکدار R (نه لزوماً جابجایی) را **موضعی** گوییم اگر تنها دارای یک ایده‌آل ماکزیمال چپ باشد. نشان دهید در حلقه یکدار R شرایط زیر معادلند:

(a) R دارای تنها یک ایده‌آل چپ ماکزیمال است،

(b) R دارای تنها یک ایده‌آل راست ماکزیمال است،

(c) $R/J(R)$ یک حلقه بخشی است،

(d) $R \setminus R^*$ یک ایده‌آل R است،

(e) $R \setminus R^*$ تحت عمل جمع یک گروه است،

(f) برای هر n اگر $a_1 + a_2 + \cdots + a_n \in R^*$، آنگاه برای یک i، $a_i \in R^*$،

(g) اگر $a + b \in R^*$ آنگاه $a \in R^*$ یا $b \in R^*$.

۱۱. فرض کنید R حلقه‌ای یکدار باشد.

(a) اگر هر عنصر $R \setminus R^*$ پوچ توان باشد آنگاه R حلقه‌ای موضعی است،

www.mathematic87.blogfa.com

(b) فرض کنید D یک حلقه بخشی باشد که $R \subseteq D$. اگر برای هر $d \in D^*$ داشته باشیم $d \in R$ یا $d^{-1} \in R$ آنگاه R یک حلقه موضعی است.

۱۲. فرض کنید R حلقه‌ای یکدار باشد. نشان دهید:

$$(R/J(R))^* = \{a + J(R) | a \in R^*\}.$$

۱۳. فرض کنید $R_n, \ldots, R_2, R_1$ حلقه‌هایی یکدار باشند. نشان دهید

$$J(\prod_{i=1}^{n} R_i) = \prod_{i=1}^{n} J(R_i).$$

۱۴. فرض کنید R حلقه‌ای یکدار باشد. نشان دهید

(a) $J(\mathrm{M}_n(R)) = \mathrm{M}_n(J(R))$،

(b) اگر e عنصر خودتوانی از R باشد، آنگاه $J(e\,\mathrm{Re}) = eJ(R)e$،

(c) اگر I ایده‌آلی از حلقه R باشد، آنگاه $(J(R)+I)/I \subseteq J(R/I)$ و تساوی فقط و فقط وقتی رخ می‌دهد که $I \subseteq J(R)$.

۱۵. (a) اگر M یک R-مدول متناهی مولد باشد، نشان دهید هر زیرمدول سره در یک زیر مدول ماکزیمال قرار دارد،

(b) اگر R یک حلقهٔ متناهی مولد باشد، نشان دهید هر ایده‌آل سره چپ در یک ایده‌آل ماکزیمال چپ قرار دارد.

۱۶. فرض کنید R یک حلقه جابجایی و M و N دو R- مدول باشند. قرار دهیم:

$$\mathrm{Hom}_R(M,N) = \{\varphi | \varphi : M \to N \text{ همریختی } R\text{- مدولی باشد}\},$$

$$\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M).$$

(a) نشان دهید $\mathrm{Hom}_R(M,N)$ ساختار R- مدولی دارد و $\mathrm{End}_R(M)$ حلقه‌ای یکدار است،

www.mathematic87.blogfa.com

(b) اگر M_1, M_2, N_1 و N_2 چهار R-مدول باشند، نشان دهید:

$$\mathrm{Hom}_R\left(M_1 \times M_2, N\right) \cong \mathrm{Hom}_R\left(M_1, N\right) \times \mathrm{Hom}_R\left(M_2, N\right),$$
$$\mathrm{Hom}_R\left(M, N_1 \times N_2\right) \cong \mathrm{Hom}_R\left(M, N_1\right) \times \mathrm{Hom}_R\left(M, N_2\right).$$

۱۷. فرض کنید $\varphi : {}_RM \to {}_RM$ یک همریختی مدولی باشد.

(a) فرض کنید ${}_RM$ نوتری باشد. اگر φ پوشا باشد، آنگاه φ یک به یک است،

(b) فرض کنید ${}_RM$ آرتینی باشد. اگر φ یک به یک باشد، آنگاه φ پوشا است.

۱۸. (a) فرض کنید R حلقه‌ای نوتری باشد. نشان دهید ایده‌آل صفر، (0)، حاصل‌ضربی از ایده‌آلهای اول است،

(b) فرض کنید R حلقه‌ای بولی و نوتری باشد. نشان دهید $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (با n مولفه).

۱۹. فرض کنید R حلقه‌ای جابجایی و یکدار و I ایده‌آل متناهی مولدی از R باشد که $I^n = I$ $(n \geq 2)$، نشان دهید عنصر خودتوان $e \in I$ چنان موجود است که $I = eR$.

۲۰. فرض کنید M یک مدول متناهی مولد روی حلقه جابجایی یکدار و نوتری R باشد.

(a) نشان دهید M خارج قسمت (تصویر همریخت) R-مدولی بشکل $R \times R \times \cdots \times R$ می‌باشد،

(b) اگر R حلقه‌ای نوتری (آرتینی) باشد، آنگاه M نیز یک R-مدول نوتری (آرتینی) است. آیا شرط جابجایی و یکدار بودن لازم است؟

۲۱. فرض کنید R یک حلقهٔ یکدار نوتری چپ و $a, b \in R$. نشان دهید:

$$ab = 1 \Leftrightarrow ba = 1.$$

۲۲. فرض کنید

$$R = M_2(\mathbb{R}) = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ \mathbb{R} & \mathbb{R} \end{bmatrix}, \quad R_1 = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix} \text{ و } R_2 = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{bmatrix}$$

www.mathematic87.blogfa.com

(a) نشان دهید R یک حلقهٔ نوتری است،

(b) R_1 یک حلقهٔ نوتری (آرتینی) چپ است در صورتیکه، نوتری (آرتینی) راست نمی‌باشد،

(c) R_2 یک حلقهٔ نوتری چپ است در صورتیکه نوتری راست نمی‌باشد،

(d) R_2 یک حلقهٔ آرتینی چپ (راست) نمی‌باشد.

مسائل مبارزه طلب

۱. فرض کنید P ایده‌آل اول مینیمالی از حلقه جابجایی و یکدار R باشد. نشان دهید $P \subseteq Z(R)$.

۲. فرض کنید R زیر حلقه‌ای از حلقهٔ جابجایی و یکدار S. اگر P ایده‌آل اول مینیمالی از R باشد، آنگاه ایده‌آل اول Q از S چنان موجود است که $Q \cap R = P$.

۳. فرض کنید R یک حلقه جابجایی یکدار باشد. در این‌صورت

$$R \text{ آرتینی است } \Leftrightarrow R \text{ نوتری و } \operatorname{Spect}(R) = \operatorname{Max}(R).$$

۴. فرض کنید M یک مدول متناهی مولد روی حلقه جابجایی و یکدار R باشد. اگر $\varphi : M \to M$ یک بروریختی R-مدولی باشد، آنگاه φ یک یکریختی است.

۵. فرض کنید R حلقه‌ای یکدار باشد.

(a) اگر R آرتینی چپ (راست) باشد، آنگاه R نوتری چپ (راست) است،

(b) اگر R نوتری چپ (راست) باشد، آنگاه $R[x]$ نیز نوتری چپ (راست) است،

(c) اگر R نوتری (آرتینی) باشد، آنگاه $M_n(R)$ نیز، برای هر $n \geq 1$، نوتری (آرتینی) است.

www.mathematic87.blogfa.com

۶. فرض کنید $M_1, M_2, \ldots, M_n$، R - مدول‌هایی چپ باشند و $M = M_1 \times M_2 \times \cdots \times M_n$. یکریختی حلقه‌ای زیر را ثابت کنید.

$$\mathrm{End}_R(M) \cong \begin{bmatrix} \mathrm{Hom}_R(M_1, M_1) & \mathrm{Hom}_R(M_2, M_1) & \cdots & \mathrm{Hom}_R(M_n, M_1) \\ \mathrm{Hom}_R(M_1, M_2) & \mathrm{Hom}_R(M_2, M_2) & \cdots & \mathrm{Hom}_R(M_n, M_2) \\ \vdots & \vdots & & \vdots \\ \mathrm{Hom}_R(M_1, M_n) & \mathrm{Hom}_R(M_2, M_n) & \cdots & \mathrm{Hom}_R(M_n, M_n) \end{bmatrix}.$$

منابعی برای مطالعهٔ بیشتر

1. Anderson, F. W., Fuller, K. R. *Rings and Categories of Modules*. Springer-Verlag, Berlin, 1974.
2. Bhattacharya, P.B., Jain, S. K., Nagpaul, S. R. *Basic Abstract Algebra*. Cambridge University Press, 1994.
3. Faith, C. *Algebra: Categories, Ring and Modules*. Springer-Verlag, Berlin, 1973.
4. Howie, J. M. *Fields and Galoies Theory*. Springer-Verlag, London , 2006.
5. Mutsumura, H. *Commutative Algebra*. Benjamin, New York, 1970.
6. Passman, D. S. *A Course in Ring Theory*. Wadsworth & Brooks/Cole, Pasific Grove, California, 1991.
7. Reid, M. *Undergraduate Algebraic Geometry*. Cambridge University Press, 1988.
8. Reid, M. *Undergraduate Commutative Algebra*. Cambridge University Press, 1995.
9. Rowen, L. *Ring Theory*. Academic Press, Boston, 1988.
10. Sharp, R. *Steps in Commutative Algebra*. Cambridge University Press, 2000.
11. Zariski, O., Samuel, P. *Commutative Algebra I, II*. Van Nostran, 1958, 1960.

www.mathematic87.blogfa.com

فصل ۱۲

مباحثی پیشرفته‌تر در نظریه گروه‌ها

در این فصل می‌خوانید:

۱۲-۱ سری گروه‌ها
۱۲-۲ گروه‌های حل‌پذیر
۱۲-۳ گروه‌های پوچ‌توان
۱۲-۴ نمایش آزاد گروه‌ها
۱۲-۵ برخی رده‌بندی‌ها

مقدمه

در این بخش مفهوم سری گروه‌ها که شناخت کاملی در مورد ساختار گروه به ما می‌دهند ارایه خواهد شد. از اهداف اصلی این بخش اثبات قضیه ژردان- هولدر است. این قضیه بیان می‌کند که هر گروه متناهی را می‌توان با استفاده از گرادایه یکتایی از گروه‌های ساده به دست آورد. به عبارت دیگر مطالعه گروه‌های متناهی به مطالعه گروه‌های ساده منجر می‌شود. در ادامه این بخش به بررسی گروه‌های حل‌پذیر خواهیم پرداخت. علت نام‌گذاری این گروه‌ها به گروه‌های حل‌پذیر به درس جبر۲ (نظریه گالوا) بر می‌گردد، که به طور خلاصه می‌توان به ارتباط بین این گروه‌ها و

معادلات چندجمله‌ای که توسط رادیکال‌ها حل‌پذیر می‌باشند اشاره داشت. در ادامه به بررسی گروه‌های پوچ‌توان، که عکس قضیه لاگرانژ در مورد آنها درست است، خواهیم پرداخت. در نهایت به بحث نمایش آزاد گروه‌ها و به دنبال آن به برخی رده‌بندی‌ها اشاره خواهیم داشت.

۱۲-۱سری گروه‌ها

تعریف ۱۲-۱

فرض کنید G یک گروه و $G_0 = G$ و $G_n,...,G_1$ زیر گروه‌هایی از G باشند. اگر به ازای هر i، $0 \le i \le n-1$ ، $G_{i+1} \le G_i$، آنگاه زنجیر

$$G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

را یک **سری** از زیر گروه‌های G می‌نامند.

(۱) اگر برای هر i، $0 \le i \le n-1$، $G_{i+1} \trianglelefteq G_i$ آنگاه سری

$$G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

را یک **سری زیر نرمال** برای G گوییم.

(۲) اگر برای هر i، $0 \le i \le n-1$، $G_i \trianglelefteq G$، آنگاه سری

$$G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

را یک **سری نرمال** برای G گوییم.

تعریف ۱۲-۲

اگر $G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$ یک سری زیر نرمال برای G باشد، آنگاه G_i / G_{i+1} $(0 \le i \le n-1)$ را یک **عامل** این سری و تعداد عامل‌های غیر بدیهی این سری را **طول** این سری نامیم.

تعریف ۱۲-۳

فرض کنید G یک گروه باشد. سری زیر نرمال زیر نظر را در نظر بگیرید.

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

(۱) سری فوق را یک سری **حل‌پذیر(آبلی)** برای G گوییم اگر عوامل G_i / G_{i+1} آبلی باشند.

(۲) سری فوق را یک سری **ترکیبی** برای G گوییم اگر عوامل G_i / G_{i+1} ساده باشند.

(۳) سری فوق را یک سری **مرکزی** برای G گوییم اگر این سری نرمال بوده و G_i / G_{i+1} در مرکز G_i / G_{i+1} باشد.

یادآوری (۱): زیر گروه سرهٔ M از گروه G را نرمال ماکزیمال گوییم اگر M یک زیر گروه نرمال G و برای هر زیر گروه N که $M \leq N \trianglelefteq G$، داشته باشیم $N = M$ یا $N = G$.

(۲): M یک زیر گروه نرمال ماکزیمال G است اگر و فقط اگر G / M ساده باشد.

قضیه ۱۲-۱

هر گروه متناهی $G \neq \{e\}$ دارای یک سری ترکیبی است.

اثبات: قضیه را با استقرا روی $|G|$ ثابت می‌کنیم. مسئله برای $|G| = 2$ واضح است. حال فرض کنید $|G| > 2$ و G_1 یک زیر گروه نرمال ماکزیمال از $G_0 = G$ باشد. اگر $G_1 = \{e\}$، آنگاه $\{e\} = G_1 \leq G_0 = G$ سری ترکیبی مورد نظر است. حال فرض کنید $G_1 \neq \{e\}$. چون $|G_1| < |G_0|$، لذا طبق فرض استقرا G_1 دارای سری ترکیبی زیر است.

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_2 \leq G_1.$$

با اضافه کردن G_0 به این سری ، یک سری ترکیبی برای G خواهیم داشت.

■■■

قضیه ۱۲-۲

فرض کنید G گروهی باشد که دارای یک سری ترکیبی (بطول n) باشد و H زیر گروه نرمال غیر بدیهی از G باشد. در این صورت H دارای سری ترکیبی (بطول کمتر از n) می‌باشد.

اثبات: فرض کنید $\{e\} = G_n \leq G_{n-1} \leq \ldots \leq G_1 \leq G_0 = G$ یک سری ترکیبی به طول n برای G باشد. قرار می‌دهیم $H_i = G_i \cap H$. در این صورت

$$\{e\} = H_n \leq H_{n-1} \leq \ldots \leq H_1 \leq H_0 = H,$$

یک سری زیر نرمال برای H است. تعریف می‌کنیم:

$$\mu : H_i / H_{i+1} \to G_i / G_{i+1}$$
$$hH_{i+1} \mapsto hG_{i+1}$$

به وضوح μ یک تکریختی است. با توجه به ساده بودن G_i / G_{i+1} و اینکه $\mu(H_i / H_{i+1}) \trianglelefteq G_i / G_{i+1}$، داریم:

$$\mu(H_i / H_{i+1}) = \{e\} \text{ یا } \mu(H_i / H_{i+1}) = G_i / G_{i+1}.$$

از این‌رو $H_i / H_{i+1} = \{e\}$ یا $H_i / H_{i+1} \cong G_i / G_{i+1}$. بنابراین با حذف بعضی جملات سری زیر نرمال H می‌توان به یک سری ترکیبی، با طول حداکثر n، برای H رسید. حال فرض کنید طول این سری ترکیبی دقیقاً n باشد. دراین‌صورت چون G_{n-1} و H_{n-1} گروه‌های ساده‌ای بوده، لذا $H_{n-1} = G_{n-1}$. از طرف دیگر

$$H_{n-2} / H_{n-1} = H_{n-2} / G_{n-1} \leq G_{n-2} / G_{n-1}.$$

بنابراین با توجه به ساده بودن G_{n-1} / G_n و نا صفر بودن H_{n-2} / H_{n-1}، خواهیم داشت $H_{n-2} = G_{n-2}$. با ادامه این روند داریم، $H = H_0 = G_0 = G$، که تناقض است. از این‌رو H دارای سری ترکیبی بطول کمتر از n می‌باشد.

■■■

www.mathematic87.blogfa.com

لم ۱۲-۱

فرض کنید G یک گروه و N و N' دو زیر گروه نرمال G باشند که $N \neq N'$. اگر G/N و G/N' ساده باشند. در این‌صورت

$$G/N \cong N'/(N \cap N'),\ G/N' \cong N/(N \cap N')$$

اثبات: ابتدا نشان می‌دهیم $N \neq NN'$. اگر $N = NN'$، آنگاه $N' \leq NN' = N \leq G$ و این متناقض با ساده بودن G/N' است. بنابراین

$$N \subsetneq NN' \subseteq G.$$

با توجه به ساده بودن G/N داریم $G = NN'$. طبق قضیه دوم یکریختی

$$G/N = (NN')/N \cong N'/(N \cap N').$$

قسمت دیگر لم نیز به طور مشابه اثبات می‌شود.

■■■

تعریف ۱۲-۴

فرض کنید G یک گروه و

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G,$$

$$\{e\} = N_m \leq N_{m-1} \leq \cdots \leq N_1 \leq N_0 = G,$$

دو سری زیر نرمال برای G باشند، دو سری فوق را **هم ارز** نامیم اگر $m = n$ و تناظری دوسوئی بین عامل‌های دو سری برقرار بوده، بطوریکه عامل‌های متناظر یکریخت باشند.

قضیه ژردان- هولدر بیان می‌کند که لیست عوامل ترکیبی هر دو سری ترکیبی با هم برابر است (به عبارت دیگر، هر عامل و تعداد تکرارهای آن همواره در هر سری ترکیبی ظاهر می‌شود).

www.mathematic87.blogfa.com

قضیه ۱۲-۳ (قضیه ژردان – هولدر)

فرض کنید

$$\{e\} = G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G, \qquad \textbf{(۱)}$$

$$\{e\} = N_m \le N_{m-1} \le \cdots \le N_1 \le N_0 = G, \qquad \textbf{(۲)}$$

دو سری ترکیبی برای گروه غیر بدیهی G باشند. در این صورت این دو سری هم ارزند.

اثبات: قضیه را با استقرا روی n ثابت می‌کنیم. مطلب برای $n = 1$ بدیهی است. فرض کنید $n > 1$ و حکم برای مقادیر کوچکتر از n برقرار باشد. اگر $G_1 = N_1$، آنگاه به‌وضوح طبق فرض استقرا حکم برقرار است. حال فرض کنید $G_1 \neq N_1$. قرار می‌دهیم $H = G_1 \cap N_1$. اگر $H = \{e\}$، آنگاه طبق لم قبل

$$G_0 / G_1 \cong N_1 / H \cong N_1 \ , N_0 / N_1 \cong G_1 / H \cong G_1.$$

از این‌رو $G_1,\ N_1$ زیرگروه‌های سادهٔ G می‌باشند. بنابراین حالت $n = 2$ اتفاق افتاده و حکم به آسانی بدست می‌آید. حال فرض کنید $H \neq \{e\}$ و

$$\{e\} = H_\ell \le H_{\ell-1} \le \cdots \le H_0 = H,$$

یک سری ترکیبی برای H باشد (قضیه ۲ ملاحظه شود). با توجه به لم قبل، سریهای ترکیبی زیر برای G موجود است.

$$\{e\} = H_\ell \le H_{\ell-1} \le \cdots \le H_0 = H \le G_1 \le G_0 = G, \qquad \textbf{(۳)}$$

$$\{e\} = H_\ell \le H_{\ell-1} \le \cdots \le H_0 = H \le N_1 \le N_0 = G. \qquad \textbf{(۴)}$$

سری‌ها (۱) و (۳) طبق فرض استقرا هم ارزند. از این‌رو $n = \ell + 2$ و در نتیجه سری‌های (۲) و (۴) نیز طبق فرض استقرا هم ارزند. از طرفی سری‌های (۳) و (۴) طبق لم قبل هم ارزند. بنابراین سری‌های (۱) و (۲) هم ارزند.

■■■

www.mathematic87.blogfa.com

با توجه به قضیه فوق، تعریف زیر را خواهیم داشت.

تعریف ۱۲-۵

طول گروه G را با $\ell(G)$ نمایش داده و به صورت زیر تعریف می‌کنیم:

$$\ell(G)=\begin{cases}0 & \text{اگر } G=\{e\}\\ n & \text{اگر } G \text{ دارای یک سری ترکیبی به طول } n \text{ باشد}\\ \infty & \text{اگر } G \text{ دارای سری ترکیبی نباشد}\end{cases}$$

۱۲-۲ گروه‌های حل‌پذیر

تعریف ۱۲-۶

گروه G را **حل‌پذیر** گوییم اگر دارای یک سری حل‌پذیر (آبلی) باشد.

قضیه۱۲-۴

فرض کنید G یک گروه متناهی باشد. در این صورت گزاره‌های زیر معادلند.

(۱) G حل‌پذیر است،

(۲) عدد صحیح مثبت n چنان موجود است که $G^{(n)}=\{e\}$،

(۳) G دارای یک سری ترکیبی است که عامل‌ها آن گروه‌هایی دوری از مرتبه عددی اولند.

www.mathematic87.blogfa.com

اثبات (۲) ⇒ (۱): فرض کنید G یک گروه حل‌پذیر و $\{e\} = G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$ یک سری حل‌پذیر (آبلی) برای G باشد. دراین صورت با استقرا روی i ثابت می‌کنیم که به ازای هر i، $G^{(i)} \le G_i$ و لذا $G^{(n)} \le G_n = \{e\}$ ، که نتیجه حاصل است. به ازای $i = 0$، $G^{(0)} = G \le G = G_0$. فرض کنید $G^{(k)} \le G_k$. در این صورت بنابر فرض استقرا

$$G^{(k+1)} = \left(G^{(k)}\right)' \le G_k' \le G_{k+1},$$

زیرا بنابر فرض G_k / G_{k+1} آبلی است. در نتیجه بنابر استقرا به ازای هر i، $G^{(i)} \le G_i$.

(۱) ⇒ (۲): سری زیر یک سری حل‌پذیر برای G است.

$$\{e\} = G^{(n)} \le G^{(n-1)} \le \cdots \le G^{(0)} = G.$$

(۱) ⇒ (۳): بدیهی است.

(۳) ⇒ (۱): فرض کنید $\{e\} = G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$ یک سری حل‌پذیر (آبلی) برای G باشد. با توجه به قضیه ۲ و نتیجه ۳-۲، سری ترکیبی زیر، که در آن عامل‌ها از مرتبهٔ عددی اولند، برای G_i / G_{i+1} موجود است.

$$G_{i+1} / G_{i+1} \le H_{in_i} / G_{i+1} \le \cdots \le H_{i1} / G_{i+1} \le G_i / G_{i+1}.$$

با اضافه کردن $H_{in_i} \le \cdots \le H_{i1}$ بین $G_{i+1} \le G_i$، می‌توانیم به یک سری ترکیبی برای G برسیم که در آن عامل‌ها گروه‌هایی دوری از مرتبه عددی اولند.

■■■

❖ **تذکر:** توجه داشته باشید که در گروه‌های نامتناهی تنها گزاره‌های (۱) و (۲) از قضیه فوق معادلند (با بررسی اثبات قضیه، این مطلب را تحقیق کنید).

مثال۱: اگر G گروهی آبلی باشد، آنگاه چون $G' = \{e\}$، لذا G گروهی حل‌پذیر است.

■

اینک خواص دیگری از گروه‌های حل‌پذیر را مطرح می‌کنیم:

www.mathematic87.blogfa.com

قضیه ۱۲-۵

(۱) هر زیر گروه و هر تصویر همریخت از یک گروه حل‌پذیر، حل‌پذیر است،

(۲) اگر N یک زیر گروه نرمال از یک گروه G باشد به طوریکه N و G/N حل‌پذیر باشند، آنگاه G حل‌پذیر است،

(۳) حاصل‌ضرب مستقیم هر تعداد متناهی از گروه‌های حل‌پذیر، حل‌پذیر است.

اثبات (۱): فرض کنید H زیر گروهی از گروه حل‌پذیر G باشد. در این صورت n ای موجود است که $G^{(n)}=\{e\}$ چون $H^{(n)}\subseteq G^{(n)}$، لذا $H^{(n)}=\{e\}$ یعنی H حل‌پذیر است. برای تصویر همریخت، فرض کنید $\varphi: G\to H$ یک برووریختی باشد (H تصویر همریخت گروه G است). در این صورت به آسانی می‌توان نشان داد که برای هر i، $\varphi(G^{(i)})=H^{(i)}$. حال چون G حل‌پذیر است، لذا n ای موجود است که $G^{(n)}=\{e\}$. در این صورت

$$\{e\}=\varphi\left(G^{(n)}\right)=H^{(n)},$$

یعنی H حل‌پذیر است.

(۲): فرض کنید $\gamma: G\to G/N$ همریختی طبیعی باشد. چون G/N حل‌پذیر است، لذا n ای موجود است که

$$\gamma(G^{(n)})=(G/N)^{(n)}=\{N\}.$$

از این رو $G^{(n)}\leq \operatorname{Ker}\gamma=N$. چون N حل‌پذیر است. طبق قسمت (۱) عدد k چنان موجود است که $(N)^{(k)}=\{e\}$ و لذا $G^{(n+k)}=\left(G^{(n)}\right)^{(k)}\subseteq (N)^{(k)}=\{e\}$. بنابراین G حل‌پذیر است.

(۳): فرض کنید $G=H\times K$ که H و K حل‌پذیراند. به‌وضوح $H\times\{e\}\trianglelefteq H\times K=G$ و $G/(H\times\{e\})=(H\times K)/(H\times\{e\})\cong K$. بنابراین $G/(H\times\{e\})$ حل‌پذیر است. از طرفی چون $H\times\{e\}\cong H$، لذا $H\times\{e\}$ نیزحل‌پذیر بوده و درنتیجه طبق قسمت (۲)، G حل‌پذیر خواهد بود. حالت کلی به آسانی با استقرای ریاضی بدست می آید.

■■■

www.mathematic87.blogfa.com

نتیجه زیر در درس جبر ۲ (نظریه گالوا) نقشی بسیار اساسی دارد.

نتیجه ۱۲-۱

برای $n \geq 5$، گروه S_n حل‌پذیر نیست.

اثبات: اگر نشان دهیم A_n برای $n \geq 5$ حل‌پذیر نیست، آنگاه طبق قضیه قبل S_n نیز برای $n \geq 5$ حل‌پذیر نخواهد بود. چون A_n آبلی نیست ، پس $A_n' \neq \{e\}$. از طرفی با توجه به اینکه $A_n' \trianglelefteq A_n$ و A_n ساده است (البته $n \geq 5$)، باید داشته باشیم $A_n' = A_n$. بنابراین برای هر $i \geq 1$, $A_n^{(i)} = A_n \neq \{e\}$ و لذا A_n حل‌پذیر نیست.

■■■

قضیه ۱۲-۶

هر p - گروه متناهی، گروهی حل‌پذیر است.

اثبات: فرض کنید G یک p - گروه متناهی باشد. قضیه را با استقرا روی $|G|$ ثابت می‌کنیم. مسئله برای $|G| = 1$واضح است. حال فرض کنید $|G| \neq 1$. $C(G)$ آبلی و در نتیجه حل‌پذیر است. از طرفی $|G/C(G)| < |G|$ وطبق فرض استقرا $G/C(G)$ نیزحل‌پذیر است، لذا طبق قسمت (۲) قضیهٔ ۵ ، G گروهی حل‌پذیر است.

■■■

قضیه ۱۲-۷

فرض کنید G یک گروه و $|G| = pq$ که p و q اعدادی اولند. در این صورت G حل‌پذیر

اثبات: اگر $p = q$، آنگاه G یک p -گروه است و لذا طبق قضیه قبل حل‌پذیر است. حال فرض کنید $q < p$. در این‌صورت طبق قضیهٔ سوم سیلو Gدارای تنها یک زیر گروه p -سیلو می‌باشند. فرض کنید P این زیر گروه باشد. چون $P \trianglelefteq G$، پس $|G/P| = q$. از طرفی P و G/P گروه‌های دوری و در نتیجه آبلی‌اند ، لذا هر دو حل‌پذیر بوده و در نتیجه G حل‌پذیر می‌باشد.

■■■

هال کارهایی بسیار مهمی در نظریه گروه‌های حل‌پذیر انجام داده است. قضیه زیر که تعمیم قضیه سیلو برای گروه‌های حل‌پذیر متناهی است، منسوب به وی می‌باشد. به علت طولانی بودن اثبات از آوردن اثبات صرف‌نظر کرده و خواننده را به کتابهای زیر رجوع می‌دهیم.

۱. محمدی حسن آبادی، علی اکبر. **جبر**. انتشارات دانشگاه اصفهان (۱۳۷۲).

2. Hungerford, T. W. *Algebra*. Springer-Verlag, New York, 1974.

قضیه۱۲-۸ (قضیه پ.هال)

فرض کنید G یک گروه حل‌پذیر از مرتبه mn باشد به طوریکه $(m,n)=1$. در این صورت

(۱) G شامل یک زیر گروه با مرتبه m است،

(۲) هر دو زیر گروه از G با مرتبه m مزدوجند،

(۳) هر زیر گروه از G با مرتبه k، که $k \mid m$، در یک زیر گروه از G با مرتبه m قرار دارد.

بحث گروه‌های حل‌پذیر را با ذکر حدس طولانی مدت بر نساید، که هر گروه متناهی با مرتبه فرد حل‌پذیر است به پایان می‌بریم. این نتیجه که اثبات آن با اطلاعات کتاب حاضر میسر نیست اولین بار در سال ۱۹۶۳ توسط فایت-تامسون به اثبات رسید.

قضیه ۱۲-۹ (قضیه فایت-تامسون)

هر گروه متناهی از مرتبهٔ فرد، حل‌پذیر است.

۱۲-۳ گروه‌های پوچ‌توان

www.mathematic87.blogfa.com

تعریف ۱۲-۷

گروه G را **پوچ‌توان** گوییم اگر دارای سری مرکزی باشد.

مثال۲: هر گروه آبلی، پوچ‌توان است.

■

مثال ۳: هر p-گروه متناهی، پوچ‌توان است.

حل: با استقرا روی مرتبه گروه فرض کنید G یک گروه متناهی باشد. اگر $G = C(G)$، حکم واضح است. در غیر این صورت $G/C(G)$ یک p-گروه است که مرتبه آن از مرتبه G کوچکتر است. بنابراین دارای سری مرکزی زیر است.

$$C(G) = G_n / C(G) \leq G_{n-1} / C(G) \leq \cdots \leq G_1 / C(G) \leq G_0 / C(G) = G / C(G)$$

است. به آسانی مشاهده می‌شود که

$$\{e\} \subseteq C(G) = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

یک سری مرکزی برای G است.

■

با توجه به حل‌پذیر بودن یک سری مرکزی، قضیهٔ زیر را خواهیم داشت.

قضیه۱۲-۱۰

هر گروه پوچ‌توان، حل‌پذیر است.

تعریف ۱۲-۸

فرض کنید H و K زیر گروه‌هایی از گروه G باشند. زیر گروه $< [h,k] \mid h \in H,\ k \in K >$ از G را **زیر گروه جابجاگر** H و K می‌نامیم و آنرا با $[H,K]$ نمایش می‌دهیم.

اثبات لم زیر آسان و به عهده خواننده واگذار می‌شود.

لم ۱۲-۲

فرض کنید H و K زیر گروه‌هایی از گروه G باشند. در این صورت:

(۱) $[H,K]=[K,H]$،

(۲) اگر $H_1 \le H$ و $K_1 \le K$ آنگاه $[H_1,K_1] \le [H,K]$،

(۳) اگر $H \trianglelefteq G$ آنگاه $[H,K] \le H$،

(۴) اگر $H \trianglelefteq G$ و $K \trianglelefteq G$ آنگاه $[H,K] \trianglelefteq G$،

(۵) $[H,K] \le H$ اگر و تنها اگر $K \le N_G(H)$،

(۶) اگر $H \le K$ و $H \trianglelefteq G$، آنگاه

$$K/H \le C(G/H) \Leftrightarrow [G,K] \le H,$$

(۷) اگر φ یک همریختی گروه G باشد آنگاه $[\varphi(H),\varphi(K)]=\varphi[H,K]$،

(۸) اگر $H \le K$ و A گروهی دلخواه و $B \le A$، آنگاه $[K \times A, H \times B]=[K,H]\times[A,B]$.

از قسمت (۶) لم فوق، نتیجه زیر به آسانی حاصل می‌شود.

نتیجه ۱۲-۲

گروه G پوچ‌توان است اگر و تنها اگر سری نرمالی مانند

$$\{e\}=G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

داشته باشیم به طوریکه به ازای هر $0 \le i \le n-1$، $[G,G_i] \le G_{i+1}$.

قضیه ۱۲-۱۱

(۱) هر زیر گروه و هر تصویر همریخت از یک گروه پوچ‌توان، پوچ‌توان است،

(۲) حاصل‌ضرب مستقیم هر تعداد متناهی از گروه‌های پوچ‌توان، پوچ‌توان است.

اثبات (۱): فرض کنید $H \leq G$. چون G پوچ‌توان است. G دارای یک سری مرکزی مانند

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G \qquad (*)$$

می‌باشد. قرار می‌دهیم $H_i = G_i \cap H$. کافی است نشان دهیم سری

$$\{e\} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = H$$

یک سری مرکزی برای H است. نشان می‌دهیم $[H, H_i] \leq H_{i+1}$، که در آن $0 \leq i \leq n-1$. با توجه به پوچ‌توان بودن G داریم $[H, H_i] \leq [G, G_i] \leq G_{i+1}$. از طرفی $[H, H_i] \leq H$ بنابراین

$$\left[H, H_i\right] \leq G_{i+1} \cap H = H_{i+1},$$

پس H پوچ‌توان است.

برای تصویر همریخت، فرض کنید $\varphi : G \to H$ یک برووریختی باشد. با در نظر گرفتن سری مرکزی $(*)$ خواهیم داشت که سری

$$\{e\} = \varphi(G_n) \leq \varphi\left(G_{n-1}\right) \leq \cdots \leq \varphi\left(G_1\right) \leq \varphi\left(G_0\right) = H,$$

یک سری نرمال برای H است. از طرفی $[H, \varphi\left(G_i\right)] = \varphi[G, G_i] \leq \varphi\left(G_{i+1}\right)$. یعنی یک سری مرکزی برای H داریم، لذا H پوچ‌توان است.

(۲): حکم را در مورد حاصل‌ضرب مستقیم دو گروه پوچ‌توان ثابت می‌کنیم، حالت کلی با استقرا به دست می‌آید. فرض کنید H و K دو گروه پوچ‌توان با سری‌های مرکزی زیر باشند (توجه داشته باشید که با درج زیر گروه‌های مکرر می‌توان طول دو سری را یکسان گرفت):

$$\{e\} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = H,$$
$$\{e\} = K_n \leq K_{n-1} \leq \cdots \leq K_1 \leq K_0 = K.$$

با توجه به قسمت (۸) لم قبل خواهیم داشت که سری

$$\{e\} \times \{e\} = H_n \times K_n \leq H_{n-1} \times K_{n-1} \leq \cdots \leq H_1 \times K_1 \leq H_0 \times K_0 = H \times K$$

یک سری مرکزی برای $H \times K$ می‌باشد.

■■■

www.mathematic87.blogfa.com

❖ **تذکر:** قسمت (۲) از قضیهٔ ۵ در مورد گروه‌های پوچ‌توان درست نمی‌باشد.(تمرین۱۵ ملاحظه شود).

قضیه۱۲-۱۲

فرض کنید H زیر گروه سره‌ای از گروه پوچ‌توان G باشد. در این صورت

$$N_G(H) \neq H.$$

اثبات: فرض کنید

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

یک سری مرکزی برای G باشد. فرض کنید $1 \leq \ell \leq n$ کوچکترین عددی باشد که $G_\ell \leq H (G_{\ell-1} \not\leq H)$. مشاهده می‌کنیم که

$$\left[H, G_{\ell-1}\right] \leq \left[G, G_{\ell-1}\right] \leq G_\ell \leq H.$$

طبق قسمت (۵) لم قبل $G_{\ell-1} \leq N_G(H)$، در نتیجه $N_G(H) \neq H$.

■■■

لم۱۲-۳

فرض کنید H یک زیر گروه و P یک p - زیر گروه سیلو ازگروه متناهی G باشد که $N_G(P) \leq H$. در این‌صورت

$$N_G(H) = H.$$

اثبات: فرض کنید $g \in N_G(H)$. چون $P \leq N_G(P) \leq H$، $gPg^{-1} \leq gHg^{-1} = H$. لذا P و gPg^{-1} هر دو زیر گروه‌های p - سیلوی H می‌باشند. لذا طبق قضیه دوم سیلو P و gPg^{-1} در H مزدوج‌اند. بنابراین $h \in H$ چنان موجود است که $hgPg^{-1}h^{-1} = P$. در نتیجه $hg \in N_G(P) \leq H$، پس $g \in H$.

■■■

قضیه ۱۲-۱۳

فرض کنید G یک گروه نابدیهی متناهی باشد. در این صورت گزاره‌های زیر معادلند.

(۱) G پوچ‌توان است،

(۲) همه زیر گروه‌های ماکزیمال G نرمال‌اند،

(۳) هر زیر گروه سیلوی G نرمال است،

(۴) G حاصل‌ضرب مستقیم زیر گروه‌های سیلوی خود است.

اثبات (۲) $\Rightarrow$ **(۱):** فرض کنید G پوچ‌توان و M یک زیر گروه ماکزیمال از G باشد. در این صورت طبق قضیه قبل $M < N_G(M) \leq G$، بنابر ماکزیمال بودن M داریم $G = N_G(M)$ که نتیجه می‌دهد $M \trianglelefteq G$.

(۳) $\Rightarrow$ **(۲):** فرض کنید P یک p-زیر گروه سیلو از G و $N_G(P) < G$ (فرض خلف). بنابراین زیر گروه ماکزیمال M از G چنان موجود است که $N_G(P) \leq M < G$. با توجه به قضیه قبل داریم $N_G(M) = M$ که تناقض با نرمال بودن M است.

(۴) $\Rightarrow$ **(۳):** تمرین ۵ از فصل ۸ ملاحظه شود.

(۱) $\Rightarrow$ **(۴):** از مثال ۳ و قضیه ۱۱ نتیجه می‌شود.

■■■

❖ **تذکر:** قضیه بالا ساختار گروه‌های پوچ‌توان متناهی را مشخص می‌کند.

۱۲-۴ نمایش آزاد گروه‌ها

در این بخش به توصیف گروه‌های آزاد خواهیم پرداخت. گروه‌های آزاد فاقد هر گونه روابط غیر بدیهی بین عناصرشان می‌باشند. از طرف دیگر اهمییت گروه‌های آزاد در نظریهٔ گروه‌ها بدین دلیل است که هر گروه دلخواه را می‌توان به‌صورت خارج قسمت یک گروه آزاد نمایش داد. بنابراین

www.mathematic87.blogfa.com

مطالعهٔ خارج قسمت گروه‌های آزاد همان مطالعهٔ نظریهٔ گروه‌ها بطور عام است. لازم به ذکر است که این نوع نمایش گروه‌ها نه تنها در جبر، بلکه در توپولوژی نیز بسیار مورد توجه است.

فرض کنید X یک مجموعه غیر تهی باشد. قرار می‌دهیم:

$$X^{-1}=\{x^{-1}|x\in X\}.$$

توجه داشته باشید که x^{-1} معکوس x نیست. در اینجا x^{-1} صرفاً یک نماد است، زیرا هیچ نوع عمل دوتایی روی X تعریف نشده است (برای مثال $X^{-1}=\{(x,2)|x\in X\}$). عنصری که آنرا با 1 نمایش می‌دهیم در نظر می‌گیریم که در $X\cup X^{-1}$ نباشد. یک **کلمه** بر X دنباله‌ای است نامتناهی مانند $(x_1,x_2,...)$ با $x_i\in X\cup X^{-1}\cup\{1\}$ بطوریکه $n\in\mathbb{N}$ چنان موجود باشدکه برای هر $k\geq n$، $x_k=1$. دنباله ثابت $(1,1,...)$ را **کلمهٔ تهی** گوییم و با 1 نمایش می‌دهیم.

تعریف۱۲-۹

کلمه $(x_1,x_2,...)$ را یک کلمه **کاهش یافته** گوییم اگر برای هر $x\in X$، عناصر x و x^{-1} مجاور نباشد، یعنی برای هر i داشته باشیم:

(۱)
$$\begin{cases}x_i=x\Rightarrow x_{i+1}\neq x^{-1}\\ x_i=x^{-1}\Rightarrow x_{i+1}\neq x\end{cases}$$

(۲) $x_k=1$ ایجاب کند که $x_i=1$ برای هر $i\geq k$.

هر کلمه کاهش یافته به فرم $(x_1^{\alpha_1},x_2^{\alpha_2},...,x_n^{\alpha_n},1,1,...)$ می‌باشد که $\alpha_i=\pm1$ و $x_i\in X$. (توجه کنید که x_i^{+1} به معنی x_i است). در ضمن برای ما مناسب است که پرانتزها را برداشته وکلمه اخیر را به صورت $x_1^{\alpha_1}...x_n^{\alpha_n}$ بنویسیم. فرض کنید $F(X)$ مجموعه تمام کلمه‌های کاهش یافته از X باشد. به طریق طبیعی ، $F(X)$ یک گروه است: به ازای هر دو کلمه y,x از $F(X)$ کلمه xy را کلمه کاهش یافته از توالی xy از دو کلمه تعریف می‌کنیم. واضح است که کلمه تهی 1 به عنوان عنصر همانی عمل می‌کند. برای هر کلمه کاهش یافته $x=x_1^{\alpha_1}...x_n^{\alpha_n}$، کلمه $x^{-1}=x_n^{-\alpha_n}...x_1^{-\alpha_1}$ معکوس کلمه x است. به این ترتیب نشان داده‌ایم که $F(X)$ یک گروه است.

www.mathematic87.blogfa.com

تعریف ۱۲-۱۰

$F(X)$ را **گروه آزاد** تولید شده توسط X می‌نامیم (اگر $X=\varnothing$ قرار می‌دهیم $F(X)=<e>$).

قضیه ۱۲-۱۴

هر گروه تصویر همریخت یک گروه آزاد است. یعنی برای هر گروه G، گروه آزاد F و زیر گروه نرمال $R \trianglelefteq F$ چنان موجود اند که $G \cong F/R$.

اثبات: فرض کنید $G=<X>$. قرار می‌دهیم $F=F(X)$. تابع φ را به صورت زیر تعریف می‌کنیم:

$$\varphi : F(X) \to G$$

$$x_1^{\alpha_1}...x_n^{\alpha_n} \mapsto x_1^{\alpha_1}...x_n^{\alpha_n}$$

به وضوح φ یک بروریختی است و لذا $F/R \cong G$، که در اینجا $R=\mathrm{Ker}\varphi$.

■■■

تعریف ۱۲-۱۱

فرض کنید گروه G توسط $X=\{x_i\}$ تولید شود. طبق قضیه قبل $G \cong F(X)/R = F/R$. عناصر $X=\{x_i\}$ را مولد وهر عنصر $R=\{r_i\}$ یک رابطهٔ G نامیده و گروه $G \cong F/R$ را به‌صورت $G=<x_i|r_i>$ نمایش داده و آن را یک **نمایش آزاد گروه** G می‌نامیم.

❖ **تذکر (۱):** توجه داشته باشیم که بجز روابط موجود در R، هیچ رابطهٔ دیگری بین مولدهای x_i موجود نیست.

(۲): چون $r_i \in R$ (یعنی $r_i=1$)، مناسب است بجای نماد $G=\langle x_1,x_2,...,x_n | r_1,r_2,...,r_m \rangle$، از نماد زیر استفاده شود.

www.mathematic87.blogfa.com

$$G =< x_1, x_2, \ldots, x_n \mid r_1 = r_2 = \ldots = r_m = 1 > .$$

مثال۴: فرض کنید $G =< x, y \mid x^2 = y^3 = x^{-1}y^{-1}xy = 1 >$ یک نمایش برای گروه G باشد. از رابطه $x^{-1}y^{-1}xy = 1$ خواهیم داشت $xy = yx$. چون هر عنصر G ترکیبی از عناصر x و y است. پس G گروهی آبلی است. هر عنصر G را می‌توان به صورت $x^i y^j$ ، $1 \leq i \leq 2$ ، $1 \leq j \leq 3$ نوشت. لذا $|G| = 6$. حال اگر قرار دهیم $a = xy$، آنگاه $\circ(a) = 6$ و در نتیجه $G = \langle a \rangle$ گروهی دوری است. در این مثال مشاهده می‌شود که G دارای نمایش $G =< a \mid a^6 = 1 >$ نیز هست.

■

مثال۵: فرض کنید $G =< x, y \mid y^2x = y, yx^2y = x >$ نمایش برای گروه G باشد از $y^2x = y$ با ضرب از چپ در y^{-1}، $yx = 1$ را به دست می‌آوریم. با قرار دادن $yx = 1$ در $yx^2y = x$ یعنی $(yx)(xy) = x$ نتیجه می‌گیریم $xy = x$. سپس با ضرب از چپ در x^{-1} خواهیم داشت $y = 1$. با جایگزینی در $yx = 1$ به دست می‌آوریم $x = 1$. به این ترتیب نشان داده‌ایم که G گروهی بدیهی است.

■

مثال‌های قبل نشان می‌دهند که یک گروه ممکن است نمایش‌های متفاوتی داشته باشد. مسئلهٔ یکسان بودن دو نمایش ممکن است خیلی مشکل باشد، حتی نشان داده شده که تعدادی از این مسائل در ارتباط با این نظریه قابل حل نیستند، یعنی روش عادی و خوش‌تعریف برای کشف یک راه حل در تمام حالات وجود ندارد. این مسائل حل ناپذیر مشتملند بر

(۱): مسأله تشخیص اینکه آیا دو نمایش یکریخت هستند،

(۲): آیا گروه عرضه شده با یک نمایش، آبلی یا بدیهی است ،

(۳): مسأله مشهور **مسأله کلمه** برای تعیین اینکه آیا یک کلمهٔ مفروض w حاصلی از مجموعه مفروض کلماتی چون $\{w_i\}$ هست یا نه.

مثال۶ (نمایش گروه دو جهی D_n): گروه D_n دارای نمایش زیر است.

$$< x, y \mid x^n = y^2 = (xy)^2 = 1 > .$$

حل: فرض کنید $G =< x,y|x^n = y^2 = (xy)^2 = 1 >$. تابع $\varphi : G \to D_n$ با ضابطهٔ $x \to \delta$ و $y \to \tau$، که بوسیلهٔ همریختی روی تمام G توسعه می‌یابد، یک برووریختی است. از اینکه مرتبهٔ هر دوی D_n و G برابر $2n$ است، φ یک یکریختی بوده و در نتیجه $G \cong D_n$.

■

این بخش را با تعریف زیر به پایان می‌بریم.

تعریف۱۲-۱۲

به ازای هر عدد طبیعی $n \geq 2$. گروه **کواترنیون‌های تعمیم یافته از مرتبهٔ** $4n$ که آنرا با Q_{4n} نشان می‌دهیم زیر گروهی از $\mathrm{GL}_2(\mathbb{C})$است که با دو ماتریس زیر تولید می‌شود.

$$\begin{bmatrix} e^{\frac{i\pi}{n}} & 0 \\ 0 & e^{-\frac{i\pi}{n}} \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

به آسانی ملاحظه می‌شود که Q_{4n} دارای نمایش زیر است.

$$< x,y|x^n = y^2, y^{-1}xy = x^{-1} > .$$

◆ **تذکر:** گروه کواترنیون از مرتبهٔ 8، $Q = \{\pm 1, \pm I, \pm J, \pm K\}$، با گروه Q_8 یکریخت است. (تمرین۱۹ ملاحظه شود).

۱۲-۵ برخی رده‌بندی‌ها

در این بخش به کمک نتایجی که در بخش قبل ذکر شده، به این سوال پاسخ می‌دهیم که گروه‌های مرتبه n با تقریب یکریخت چه هستند. جواب دادن به این سوال، در حالت کلی مشکل است. در این بخش گروه‌های متناهی که مرتبه‌شان کوچکتر یا مساوی۱۵ است را با تقریب یکریختی معین می‌کنیم. این گروه‌ها را به وسیله مولدها و روابط بین آنها (نمایش آزاد) عرضه می‌کنیم.

www.mathematic87.blogfa.com

قضیه ۱۲-۱۵

فرض کنید G یک گروه از مرتبه pq باشد که در آن p و q دو عدد اول هستند به طوریکه $p > q$. در این صورت یا $G \cong \mathbb{Z}_{pq}$ یا

$$G =< a,b | a^p = b^q = 1,\ \ bab^{-1} = a^r >,$$

دراینجا $1 < r < p$ عددی طبیعی است که $r^q \overset{p}{\equiv} 1$.

اثبات: طبق قضیه کشی عناصر $a,b \in G$ چنان موجودند که $\circ(a) = p$ و $\circ(b) = q$. زیر گروه $A = \langle a \rangle$ یک p - زیر گروه سیلو از G است. اگر n_p تعداد p - زیر گروه‌های سیلوی G باشد، آنگاه بنابر قضیه سوم سیلو $n_p \mid pq$ و $n_p \overset{p}{\equiv} 1$ لذا $n_p \in \{1,p,q,pq\}$ که چون $p > q$ باید $n_p = 1$ ، یعنی $A \trianglelefteq G$. حال چون $|G/A| = q$ یک عدد اول است ، $G/A = \langle bA \rangle$ دوری است. بنابراین هر عنصر G به صورت $a^i b^j$ می‌باشد، لذا $G = \langle a,b \rangle$. اگر n_q تعداد $q-$زیر گروه‌های سیلوی Gباشد، آنگاه $n_q \mid pq$ ، $n_q \overset{q}{\equiv} 1$ و $n_q \in \{1,p,q,pq\}$ که نتیجه می‌شود $n_q = 1$ یا $n_q = p$.

حالت (۱): اگر $n_q = 1$ آنگاه $B = \langle b \rangle \trianglelefteq G$. از طرفی طبق قضیه لاگرانژ، $A \cap B = \{e\}$. از این‌رو

$$G \cong A \times B \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

حالت (۲): حال فرض کنید $n_q = p$. چون $A \trianglelefteq G$، پس $bab^{-1} = a^r \in A$، که در اینجا r یک عدد صحیح مثبتی است که $1 < r < p$. (اگر $r = 1$ ، آنگاه G آبلی و در نتیجه $n_q = 1$ که تناقض است. اگر $r = p$ آنگاه $a = e$ و در نتیجه $p = 1$ که باز هم تناقض است). از طرفی $a = b^q ab^{-q} = a^{r^q}$ و از این‌رو $r^q \overset{p}{\equiv} 1$. بنابراین $G =< a,b | a^p = b^q = 1,\ \ bab^{-1} = a^r >$، که در آن $1 < r < p$ عددی طبیعی است که $r^q \overset{p}{\equiv} 1$.

■■■

نتیجه ۱۲-۳

فرض کنید p یک عدد اول فرد و G یک گروه از مرتبه $2p$ باشد. در این صورت

$$G \cong \mathbb{Z}_{2p} \text{ یا } G \cong D_p$$

www.mathematic87.blogfa.com

اثبات: به عنوان تمرین به خواننده واگذار می‌شود.

■■■

قضایای زیر، گروه‌های مرتبه 8 و 12 را رده بندی می‌کنند.

قضیه ۱۲-۱۶

پنج گروه (در حد یکریختی) از مرتبه 8 موجود است: $\mathbb{Z}_8$ ، $\mathbb{Z}_4\times\mathbb{Z}_2$ و $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ که آبلی‌اند و D_4 و $Q_8 =< a,b|a^4=1,\ a^2=b^2,\ bab^{-1}=a^{-1}>$،گروه کواترنیون‌ها از مرتبه 8، که غیر آبلی می‌باشند.

اثبات (الف): اگر G آبلی باشد، در این صورت با توجه به قضیه اساسی گروه‌های آبلی G به صورت یکی از گروه‌های زیر است.

$$\mathbb{Z}_8,\ \mathbb{Z}_4\times\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$

(ب): فرض کنید G گروهی ناآبلی از مرتبه 8 باشد. G نمی‌تواند عنصری از مرتبه 8 داشته باشد و یا اینکه مرتبه هر عنصر آن 2 باشد. از این‌رو G باید دارای عنصری از مرتبه 4 باشد. فرض کنید $a\in G$ و $\circ(a)=4$ چون $[G:\langle a\rangle]=2$ لذا $\langle a\rangle \trianglelefteq G$ و در نتیجه $|G/\langle a\rangle|=2$. بنابراین عنصری مانند $b\in G\setminus\langle a\rangle$ چنان موجود است که $b^2\in\langle a\rangle$. اگر $b^2=a$، از آنجا که $\circ(a)=4$ خواهیم داشت $\circ(b)=8$، که تناقض است. به دلیل مشابه $b^2\neq a^3$. در نتیجه دو حالت زیر اتفاق می‌افتد:

حالت (۱): $b^2=1$، **حالت (۲):** $b^2=a^2$.

چون $\langle a\rangle \trianglelefteq G$، پس $bab^{-1}\in\langle a\rangle$ و تنها امکان این است که $bab^{-1}=a^3=a^{-1}$، لذا

در حالت (۱) $G =< a,b|a^4=b^2=1\ ,\ bab^{-1}=a^{-1}>\cong D_4$

در حالت (۲) $G =< a,b|a^4=b^4=1\ ,\ a^2=b^2\ ,\ bab^{-1}=a^{-1}>\cong Q_8$.

■■■

www.mathematic87.blogfa.com

قضیه ۱۲-۱۷

قضیه پنج گروه (در حد یکریختی) از مرتبه 12 وجود دارد: $\mathbb{Z}_{12}$ و $\mathbb{Z}_6 \times \mathbb{Z}_2$ که آبلی‌اند و A_4، D_6 و $T =< a,b \mid a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} >$.

اثبات (الف): اگر G آبلی باشد در این صورت طبق قضیه اساسی گروه‌های آبلی G با یکی از گروه‌های $\mathbb{Z}_{12}$ یا $\mathbb{Z}_6 \times \mathbb{Z}_2$ یکریخت است.

(ب): حال فرض کنید G آبلی نباشد. فرض کنید P یک زیر گروه سیلو از G باشد. در این صورت $|P| = 3$ و $[G : P] = 4$. همریختی $\varphi : G \to S_4$ چنان موجود است که $K = \mathrm{Ker}\,\varphi \leq P$. چون $|P| = 3$، خواهیم داشت $K = \{e\}$ یا $K = P$. اگر $K = \{e\}$، آنگاه G با زیر گروهی از S_4 از مرتبه 12 که A_4 می‌باشد یکریخت است (چرا؟). اگر $K = P$، آنگاه $P \trianglelefteq G$ و P تنها 3 - زیر گروه سیلوی G می‌باشد. بنابراین G شامل دقیقاً دو عنصر از مرتبه 3 است. اگر c یکی از این دو عنصر باشد، آنگاه $\left[G : C_G(c)\right]$ که تعداد مزدوج‌های c می‌باشد، برابر 1 یا 2 است. در نتیجه $C_G(c)$ زیر گروهی از G با مرتبه 6 یا 12می‌باشد. در هر دو حالت، بنابر قضیه کشی عنصری مانند $d \in C_G(c)$ از مرتبه 2موجود است و لذا $\circ(cd) = \circ(c) \circ (d) = 3 \times 2 = 6$. فرض کنید $a = cd$. در این صورت $[G : \langle a \rangle] = 2$ و لذا $\langle a \rangle \trianglelefteq G$ و

$$G / \langle a \rangle = \langle b \langle a \rangle \rangle,\ b^2 \in \langle a \rangle,\ b \neq \langle a \rangle$$

از آنجا که $bab^{-1} \in \langle a \rangle$ و G ناآبلی و $\circ(a) = 6$، خواهیم داشت $bab^{-1} = a^5 = a^{-1}$ برای $b^2 \in \langle a \rangle$، شش امکان موجود است. $b^2 = a$ و $b^2 = a^2$ و $b^2 = a^4$ به تناقض می‌رسند. $b^2 = a^5$ و $b^2 = a^3$ یا $b^2 = e$ نتیجه می‌دهند که $\circ(b) = 12$، یعنی G آبلی است. بنابراین و لذا

$$G =< a,b \mid a^6 = b^2 = 1\ ,\ bab^{-1} = a^{-1} > \cong D_6$$

یا

$$G =< a,b \mid a^6 = 1\ ,\ b^2 = a^3\ ,\ bab^{-1} = a^{-1} >= T.$$

■■■

www.mathematic87.blogfa.com

در جدول زیر نمایش گروه‌های ناآبلی از مرتبه کوچکتر از ۳۰ آورده شده است.

مرتبه	مولدها	روابط	ساختار
6	a,b	$a^2=b^3=(ab)^2=1$	$S_3\cong D_3$
8	a,b	$a^4=b^2=(ab)^2=1$	D_4
	a,b	$a^4=1,a^2=b^2,bab^{-1}=a^{-1}$	Q_8
10	a,b	$a^2=b^5=(ab)^2=1$	D_5
12	a,b	$a^2=b^3=(ab)^3=1$	A_4
	a,b	$a^6=b^2=(ab)^2=1$	$D_6=\mathbb{Z}_2\times D_3$
	a,b	$a^6=1,b^2=a^3,bab^{-1}=a^{-1}$	T
14	a,b	$a^7=b^2=(ab)^2=1$	D_7
16	a,b,c	$a^2=b^2=c^2=(ab)^2=(ac)^2=(bc)^4=1$	$\mathbb{Z}_2\times D_4$
	a,b,c	$a^2=b^2=(ab)^2,c^2=1,ac=ca,bc=cb$	$\mathbb{Z}_2\times Q_8$
	a,b	$a^8=b^2=(ab)^2=1$	D_8
	a,b	$a^2=1\ ,\ aba=b^3$	
	a,b	$a^2=1\ ,\ aba=b^{-3}$	
	a,b	$a^4=b^4=1\ ,\ b^{-1}ab=a^{-1}$	
	a,b	$a^4=b^4=(ab)^4=\left(a^{-1}b\right)^2=1$	
	a,b,c	$a^2=b^2=c^2=1,abc=bca=cab$	
	a,b,c	$a^4=b^2=(ab)^2$	
18	a,b	$a^2=b^2=1\ ,\ (ab)^2=(ba)^2$	$\mathbb{Z}_3\times D_3$
	a,b	$a^2=b^9=(ab)^2=1$	
	a,b,c	$a^2=b^2=c^2=(abc)^2=(ab)^3=(ac)^3=1$	
20	a,b	$a^{10}=b^2=(ab)^2=1$	$D_{10}\cong\mathbb{Z}_2\times D_5$
	a,b	$a^2baba^{-1}=b^2=1$	

www.mathematic87.blogfa.com

	a,b	$a^5=b^2=(ab)^2$	
21	a,b	$a^3=1\ ,\ a^{-1}ba=b^2$	
22	a,b	$a^{11}=b^2=(ab)^2=1$	D_{11}
24	a,b	$a^3=b^2=\left(a^{-1}bab\right)^2=1$	$\mathbb{Z}_2\times A_4$
	a,b	$a^2=b^2=c^2=(bc)^6=(ca)^2=(ab)^2=1$	$\mathbb{Z}_2\times D_6$
	a,b	$a^2=b^{12}=1\ ,\ aba=b^{-5}$	$\mathbb{Z}_3\times D_4$
	a,b	$a^{12}=1\ ,\ b^2=a^6\ ,\ b^{-1}ab=a^7$	$\mathbb{Z}_3\times Q_8$
	a,b	$a^2=b^{12}=1\ ,\ aba=b^5$	$\mathbb{Z}_4\times D_3$
	a,b	$a^4=b^6=1\ ,\ a^{-1}ba=b^{-1}$	$\mathbb{Z}_2\times T$
	a,b	$a^{12}=b^2=(ab)^2=1$	D_{12}
	a,b	$a^2=b^4=(ab)^3=1$	S_4
	a,b	$a^3=b^3=(ab)^2$	
	a,b	$a^4=b^6=(ab)^2=\left(a^{-1}b\right)^2=1$	
	a,b	$a^2=b^2=(ab)^3$	
	a,b	$a^2=b^6=(ab)^2$	
	a,b		
26	a,b	$a^{13}=b^2=(ab)^2=1$	D_{13}
27	a,b	$a^3=b^3=(ab)^3=\left(a^{-1}b\right)^3=1$	
	a,b	$a^3=1, a^{-1}ba=b^{-2}$	
28	a,b	$a^2=b^{14}=(ab)^2=1$	D_{14}
	a,b	$a^2=b^7=(ab)^2$	
30	a,b	$a^2=1, aba=b^4$	$\mathbb{Z}_3\times D_5$
	a,b	$a^2=1, aba=b^{-4}$	$\mathbb{Z}_5\times D_3$
	a,b	$a^{15}=b^2=(ab)^2=1$	D_{15}

www.mathematic87.blogfa.com

تمرینها

۱. تمام سری‌های ترکیبی $A_4, S_3 \times \mathbb{Z}_3$ و S_4 را بنویسید.

۲. ثابت کنید هر گروه با مرتبهٔ کوچکتر از 60 گروهی حل‌پذیر است.

۳. با استفاده از قضیه ژردان-هولدر قضیهٔ اساسی حساب را ثابت کنید.

۴. فرض کنید p، q و r اعداد اول و n یک عدد طبیعی باشد. نشان دهید

(a) هر گروه از مرتبهٔ pqr حل‌پذیر است،

(b) هر گروه از مرتبهٔ p^2q^2 حل‌پذیر است،

(c) هر گروه از مرتبهٔ p^nq حل‌پذیر است.

۵. با یک مثال نقض نشان دهید که هر گروه نامتناهی الزاماً دارای یک سری ترکیبی نیست.

۶. ثابت کنید گروه آبلی G دارای سری ترکیبی است اگر و فقط اگر G متناهی باشد.

۷. (a) اگر G یک گروه حل‌پذیر متناهی باشد، ثابت کنید هر زیر گروه نرمال مینیمال G یک p-گروه آبلی است،

(b) اگر N یک زیرگروه نرمال غیر بدیهی از گروه پوچتوان G باشد، نشان دهید $N \cap C(G) \neq < e >$.

(c) فرض کنید G یک گروه پوچتوان متناهی باشد. ثابت کنید که هر زیر گروه نرمال مینیمال غیر بدیهی از G در $C(G)$ قرار دارد و دارای مرتبه اول است.

۸. اگر M یک زیر گروه ماکزیمال سره‌ای از گروه حل‌پذیر متناهی G باشد، ثابت کنید $[G : M]$ توانی از یک عدد اول است.

۹. اگر G یک گروه متناهی غیر ساده باشد بطوریکه همهٔ زیرگروه‌های سرهٔ آن آبلی باشند، ثابت کنید G حل‌پذیر است.

۱۰. فرض کنید G یک گروه متناهی باشد. نشان دهید شرایط زیر معادلند:

(a) G یک گروه پوچتوان است،

www.mathematic87.blogfa.com

(b) برای هر دوعنصر $x,y \in G$ که مرتبهٔ آنها نسبت بهم اول است، $xy = yx$.

۱۱. (a) نشان دهید S_3 و S_4 پوچ‌توان نیستند، در صورتیکه حل‌پذیرند،

(b) نشان دهید $\mathrm{GL}_n(\mathbb{R})$ پوچ‌توان نیست.

۱۲. فرض کنید G یک گروه باشد. اشتراک همهٔ زیرگروه‌های ماکزیمال G را **زیرگروه فراتینی** G نامند و با علامت $\Phi(G)$ نمایش می‌دهند. هرگاه G دارای زیرگروه ماکزیمال نباشد، بر طبق قرارداد $\Phi(G) = G$.

(a) فرض کنید G یک گروه متناهی باشد. نشان دهید $\Phi(G)$ پوچ‌توان است.

(b) فرض کنید G یک گروه متناهی باشد. ثابت کنید G پوچ‌توان است اگر و فقط اگر $G' \leq \Phi(G)$.

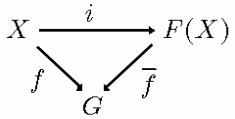
۱۳. فرض کنید G یک گروه پوچ‌توان متناهی باشد. ثابت کنید که اگر p عدد اولی باشد که $p \mid\mid G \mid$، آنگاه $p \mid\mid C(G) \mid$.

۱۴. فرض کنید G یک گروه متناهی باشد. ثابت کنید که اگر $\mathrm{Aut}(G)$ پوچ‌توان باشد، آنگاه G پوچ‌توان است.

۱۵. (a) نشان دهید گزارهٔ (۲) از قضیه ۶ در مورد گروه‌های پوچ‌توان درست نیست،

(b) فرض کنید G یک گروه و $H \leq C(G)$. اگر H و G/H پوچ‌توان باشند، ثابت کنید G نیز پوچ‌توان است.

۱۶. فرض کنید $F(X)$ گروه آزاد تولید شده توسط مجموعه غیر تهی X و $i : X \to F(X)$ تابع شمول باشد. اگر G یک گروه و $f : X \to G$ یک تابع باشد، نشان دهید همریختی یکتایی مانند $\overline{f} : F(X) \to G$ چنان موجود است که $f = \overline{f}i$. به‌عبارت دیگر، نمودار زیر تعویض‌پذیر است.



۱۷. ثابت کنید $< x,y \mid x^2 = 1,\ xy = yx > \cong \mathbb{Z}_2 \times \mathbb{Z}$،

۱۸. (a) اگر $n \in \mathbb{Z}$، ثابت کنید $< x,y \mid y^{-1}x^n y = x^{n+1}, x^{-1}y^n x = y^{n+1} >$ یک گروه بدیهی است،

(b) اگر $G =< x,y \mid x^2 = y^3 = (xy)^7 = 1 >$، ثابت کنید $G' = G$.

www.mathematic87.blogfa.com

۱۹. نشان دهید $Q=\{\pm 1,\pm I,\pm J,\pm K\}$، گروه کواترنیون از مرتبهٔ 8، با گروه Q_8 یکریخت است.

۲۰. تمام گروه‌های با مرتبه 18 و 20 و 30 را رده‌بندی کنید.

مسائل مبارزه طلب

۱. فرض کنید G گروهی حل ناپذیر باشد بطوریکه $|G|\leq 120$. ثابت کنید $G\cong A_5$.

۲. اگر اندیس هر زیرگروه ماکزیمال گروه متناهی G عددی اول یا مربع عددی اول باشد، نشان دهید G حل‌پذیر است.

۳. اگر G یک گروه پوچ‌توان متناهی مولد باشد، نشان دهید هر زیرگروه G نیز متناهی مولد است.

۴. گروه‌های مرتبهٔ p^3 (p عددی اول) را رده بندی کنید.

۵. همهٔ گروه‌های مرتبهٔ ۲۴ را رده بندی کنید.

منابعی برای مطالعهٔ بیشتر

۱. جمالی، علیرضا. **نظریهٔ گروه‌ها**. انتشارات مبتکران (۱۳۸۰).

2. Dixon, J. D. *Problems in Group Theory*. Dover Publishing Inc., New York, 1973.
3. Robinson, D. J. S. *A Course in the Theory of Groups*. Springer-Verlag, 1996.
4. Rotman, J. J. *The Theory of Groups*. Allyn and Bacon Inc., Boston, 1973.
5. Suzuki, M. *Group Theory I, II*. Springer-Verlag, Berlin, 1982, 1986.

www.mathematic87.blogfa.com

حل تمرینهای فرد

(لطفاً از سعی و تلاش خود برای حل هر تمرین قبل از نگاه به جواب مطمئن شوید)

فصل ۱

۱. (a): G دارای خاصیت شرکت‌پذیری نیست.

(b): G یک گروه است. در این گروه $e = 0$ و $x^{-1} = x$.

(c): G یک گروه است. در این گروه $e = 0$ و $x^{-1} = (-x)/(1+x)$.

(d): G یک نیم گروه است.

۳.

جدول $(\mathbb{Z}_4, +)$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

جدول گروه حرکت‌های مستطیل

$\circ$	id	ρ	μ_1	μ_2
id	id	ρ	μ_1	μ_2
ρ	ρ	id	μ_2	μ_1
μ_1	μ_1	μ_2	id	ρ
μ_2	μ_2	μ_1	ρ	id

www.mathematic87.blogfa.com

زیرگروه‌های غیر بدیهی گروه حرکت‌های مستطیل عبارتند از: $\{\mathrm{id},\rho\}$، $\{\mathrm{id},\mu_1\}$ و $\{\mathrm{id},\mu_2\}$. درحالی $\{\bar{0},\bar{2}\}$ تنها زیر گروه غیر بدیهی $(\mathbb{Z}_4,+)$ می‌باشد. از این‌رو این دو گروه متفاوتند.

۵. $U(12)=\{1,5,7,11\}$ و جدول کیلی آن:

•	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

۷. $\mathbb{Z}_8$ و $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ و $\mathbb{Z}_4\times\mathbb{Z}_2$. تعداد زیرگروه‌های این گروه‌ها متفاوت اند.

۹. تعداد زیرگروه‌های $\mathbb{Z}_3\times\mathbb{Z}_3$ برابر 6 در حالی که $\mathbb{Z}_9$ دارای 3 زیرگروه است.

۱۱. (فرض خلف) فرض کنید $e\neq x\in G$. چون $x^2\neq e$، لذا $x\neq x^{-1}$. قرار می‌دهیم $S_1=G-\{x,x^{-1},e\}$. به‌وضوح $S_1=\varnothing$، یک تناقض است، از این‌رو فرض کنید $y\in S_1$، $y^2\neq e$. قرار می‌دهیم $S_2=G-\{x,x^{-1},y,y^{-1},e\}$. چون G متناهی است این روند در جایی متوقف می‌شود، یعنی nای موجود است که $S_n=\varnothing$. بنابراین $|G|=2n+1$، که تناقض است.

۱۳. داریم $ba=ab^{-1}=(ba^{-1}b^{-1})b^{-1}=ba^{-1}b^{-2}$. با ضرب طرفین تساوی اخیر در b^{-1} خواهیم داشت $a=a^{-1}b^{-2}$ و لذا $a^2=b^{-2}$. در نتیجه

$$a^4=a^2a^2=a^2b^{-2}=a(ab^{-1})b^{-1}=a(ba)b^{-1}=(ab)(ab^{-1})=(ba^{-1})(ab^{-1})=e.$$

بنابراین $b^4=a^{-4}=e$.

۱۵. (a): با قرار دادن $b=e$ در رابطهٔ $(ab)^2=ab$ خواهیم داشت $a^2=a$، درنتیجه $a=e$، یعنی $G=\{e\}$.

(b): چون $(ab)^2=a^2b^2$، لذا $abab=aabb$. با حذف a,b خواهیم داشت $ab=ba$.

www.mathematic87.blogfa.com

(c):داریم $ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = ba$.

۱۷.(a): فرض کنید $A, B \in \mathrm{SL}_2(\mathbb{Z})$. به‌وضوح درایه‌های AB, A^{-1} صحیح می‌باشند.

(b): $H \cap K$ همواره زیر گروه G است ولی $H \cup K$ در حالت کلی زیرگروهی از G نیست. بعنوان مثال فرض کنید $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ و $H = \{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$ و $K = \{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}$. به‌وضوح $H \cup K$ زیرگروه نیست.

(c): اگر G آبلی باشد HK زیرگروهی از G است. اما در حالت کلی این مطلب درست نیست. بعنوان مثال فرض کنید $G = S_3$ و $H = \{\mathrm{id}, \mu_1\}$ و $K = \{\mathrm{id}, \mu_2\}$. در این‌صورت $HK = \{\mathrm{id}, \mu_1, \mu_2, \rho_1\}$، که زیرگروهی از S_3 نیست.

۱۹. فرض کنید $x, y \in C(G)$. در این‌صورت برای هر $g \in G$ داریم:

$$(xy^{-1})g = (xy^{-1})(g^{-1})^{-1} = x(g^{-1}y)^{-1} = x(yg^{-1})^{-1}$$
$$= x(gy^{-1}) = (xg)y^{-1} = g(xy^{-1}),$$

و لذا $xy^{-1} \in C(G)$.

۲۱.(a): (استقرا روی n) $(aba^{-1})^{n+1} = (aba^{-1})^n(aba^{-1}) = (ab^n a^{-1})(aba^{-1}) = ab^{n+1}a^{-1}$.

(b): (استقرا n)

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

فصل ۲

۱. (a): **نادرست.** $U(8) = \{1,3,5,7\}$ دوری نیست. زیرا $<3> = \{1,3\}$، $<5> = \{1,5\}$ و $<7> = \{1,7\}$.

(b): **نادرست.** زیرا $(49,60) = 1$ و لذا $<49> = \mathbb{Z}_{60}$.

(c): **نادرست.** اگر $\mathbb{Q} = <m/n>$، که $(m,n) = 1$. دراین‌صورت $1/(n+1) \in <m/n>$ ولذا $k \in \mathbb{Z}$ چنان موجود است که $(km)/n = 1/(n+1)$. بنابراین $km(n+1) = n$، که تناقض است.

www.mathematic87.blogfa.com

(d): **نادرست.** $G=\mathbb{Z}_2\times\mathbb{Z}_2$ را در نظر بگیرید.

۳. در $\mathbb{Z}_{18}$ مرتبهٔ عناصر $\bar{1},\bar{5},\bar{7},\overline{11},\overline{13},\overline{17}$ برابر 18، مرتبهٔ عناصر $\bar{2},\bar{4},\bar{8},\overline{10},\overline{14},\overline{16}$ برابر 9، مرتبهٔ عناصر $\bar{3},\overline{15}$ برابر 6، مرتبهٔ عناصر $\bar{6},\overline{13}$ برابر 3 و در نهایت $\circ(\bar{9})=2$ و $\circ(\bar{0})=1$.

در D_4، $\circ(\mathrm{id})=1$، مرتبهٔ عناصر ρ_2 برابر $\mu_1,\mu_2,\delta_1,\delta_2$ ومرتبهٔ عناصر ρ_1,ρ_3 برابر 4 می‌باشد، که در اینجا

$$\mathrm{id}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \rho_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\ \rho_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ \rho_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$

$$\mu_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ \mu_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\ \delta_1=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\text{و}\ \delta_2=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

۵. $\circ(a)\in\{1,2,3,6,8,12,24\}$ ولذا $|\,24\circ(a)$.

۷. $\mathbb{Z}_2$ دارای دقیقاً یک مولد و $\mathbb{Z}_3$ دارای دقیقاً دو مولد می‌باشد. اگر mای باشد که $n=\varphi(m)$، آنگاه $\mathbb{Z}_m$ دقیقاً دارای n مولد است.

۹ (a) : فرض کنید $\circ(a)=d$. در این‌صورت $(a^{-1})^d=(a^d)^{-1}=e$. حال اگر عدد طبیعی m چنان باشد که $(a^{-1})^m=e$، آنگاه $a^{-m}=(a^{-1})^m=e$ و لذا $d\mid -m$ و در نتیجه $d\le m$، یعنی $\circ(a^{-1})=d$.

(b): فرض کنید $\circ(a)=d$. در این‌صورت $(gag^{-1})^d=ga^dg^{-1}=e$. حال اگر عدد طبیعی m چنان باشد که $(gag^{-1})^m=e$، آنگاه $(gag^{-1})^m=ga^mg^{-1}=e$ و لذا $a^m=e$، در نتیجه $d\le m$، یعنی $\circ(gag^{-1})=d$.

(c): طبق قسمت (b) خواهیم داشت: $\circ(ba)=\circ(a(ba)a^{-1})=\circ(ab)$.

۱۱. تعداد مولدهای $\mathbb{Z}_{pq}$ برابر $\phi(pq)=(p-1)(q-1)$و تعداد مولدهای $\mathbb{Z}_{pq}$ برابر $\phi(p^n)=p^n(1-1/p)=p^n-p^{n-1}$، که در اینجا ϕ تابع اویلراست.

۱۳. اگر $H=<g>\cap<h>$، آنگاه $|\,H\,|\circ(g)=15$ و $|\,H\,|\circ(h)=16$. بنابراین $|\,H\,|=1$.

www.mathematic87.blogfa.com

۱۵. چون $(m,n)=1$، لذا اعداد صحیح r,s چنان موجودند که $mr+ns=1$. اگر $x\in<a>\cap<b>$، آنگاه $x^m=x^n=e$ ولذا $x=x^1=x^{mr+ns}=(x^m)^r(x^n)^s=e$.

۱۷. فرض کنید $H=\{e,a\}$ و $K=\{e,b\}$ دو گروه متمایز از مرتبهٔ 2 باشند. دراین‌صورت $HK=\{e,a,b,ab\}$ یک زیرگروه مرتبهٔ 4 از G است. این زیر گروه لزوماً دوری نیست، بعنوان مثال $G=\mathbb{Z}_2\times\mathbb{Z}_2$ را ملاحظه نمایید.

۱۹. داریم $G=\bigcup_{g\in G}<g>$. چون G دارای تعداد متناهی زیرگروه است، خواهیم داشت $G=\bigcup_{i=1}^{n}<g_i>$. برای هر $1\le i\le n$، $<g_i>$ باید یک گروه دوری متناهی باشد، زیرا در غیر این‌صورت $<g_i>$ ودر نتیجه G دارای تعداد نامتناهی زیر گروه خواهد بود. بنابراین $|G|\le\sum_{i=1}^{n}\circ(g_i)<\infty$.

۲۱. فرض کنید H یک زیرگروه سرهٔ $G=<x_1,\ldots,x_n>$ باشد. قرار می‌دهیم: $\Omega=\{K\le G\mid H\le K<G\}$. چون $H\in\Omega$، لذا $\Omega\neq\varnothing$. فرض کنید $K=\bigcup_{i=1}^{\infty}K_i$. به $K_1\subseteq K_2\subseteq K_3\subseteq\cdots$ یک زنجیر صعودی از Ω باشد. قرار می‌دهیم وضوح K یک زیرگروه G است. حال فرض کنید $K=G$. دراین‌صورت $x_i\in K_{\ell_i}$، که $1\le i\le n$. اگر $\ell=\max\{\ell_i\}_{i=1}^{n}$، آنگاه $K_\ell=G$، که تناقض است. یعنی $K\in\Omega$. به عبارت دیگر Ω در شرایط لم زرن صدق می‌کند. بنابراین Ω دارای عنصر ماکزیمال است یا به‌طور معادل H در یک زیرگروه ماکزیمال قرار دارد.

فصل ۳

۱. (a): (1 4 8 3 9 5 2 7 6). (b): (4 7)(1 6 2 3).

۳. $(a_n\ a_{n-1}\ \ldots\ a_2\ a_1)$.

www.mathematic87.blogfa.com

۵. زیرگروه‌های A_4 عبارتند از:

$\{\mathrm{id}\}$، A_4، $\{\mathrm{id},(1\ 2)(3\ 4)\}$، H_1، $\{\mathrm{id},(1\ 3)(2\ 4)\}$ و H_2، $\{\mathrm{id},(1\ 4)(2\ 3)\}$ و H_3،

$\{\mathrm{id},(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$ و H، $\{\mathrm{id},(1\ 2\ 3),(1\ 3\ 2)\}$ و K_1،

$\{\mathrm{id},(1\ 2\ 4),(1\ 4\ 2)\}$ و K_2، $\{\mathrm{id},(2\ 3\ 4),(2\ 4\ 3)\}$ و K_3، $\{\mathrm{id},(1\ 4\ 2),(1\ 2\ 4)\}$ و K_4.

توجه داشته باشید که A_4 زیر گروه مرتبهٔ 6 ندارد.

۷. فرض کنید $\sigma = (1\ 2\ 3\ 4\ 5)$ و $\tau = (6\ 7\ 8)$. دراین‌صورت $\circ(\sigma\tau) = 15$.

۹. نتیجهٔ مستقیم تمرین۱۸ فصل۲.

۱۱. فرض کنید $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ تجزیهٔ σ به حاصل‌ضرب دورهای مجزا باشد $(\sigma_i \neq id, k \geq 2)$. در این‌صورت $\circ(\sigma_1) + \circ(\sigma_2) + \cdots + \circ(\sigma_k) \leq n$. چون σ_i دوری به طول $\circ(\sigma_i)$ است، لذا می‌توان آنرا به حاصل‌ضرب حداکثر $\circ(\sigma_i) - 1$ ترانهش نوشت. از این‌رو σ را می‌توان به حاصل‌ضرب حداکثر t ترانهش نوشت که

$$t = (\circ(\sigma_1) - 1) + (\circ(\sigma_2) - 1) + \cdots + (\circ(\sigma_k) - 1) = (\sigma_1) + \circ(\sigma_2) + \cdots + \circ(\sigma_k) - k$$

از طرفی چون $k \geq 2$، خواهیم داشت $t \leq n - 2$.

۱۳. با توجه به اینکه $(i\ j) = (1\ i)(1\ j)(1\ i)$، لذا S_n را می‌توان با ترانهش‌های $(1, i)$, $2 \leq i \leq n$ تولید کرد، از طرفی چون $(1\ i\ j) = (1\ j)(1\ i)$، لذا A_n را می‌توان با دورهای $(1\ i\ j)$, $2 \leq i, j \leq n$, $i \neq j$ تولید کرد.

۱۵. (a): فرض کنید $H = <(1\ 2),(2\ 3),\ldots,(n-1\ n)>$ کافی است با استقرا نشان دهیم که $(1\ k) \in H$, $2 \leq k \leq n$. داریم $(1, 2) \in H$. حال فرض کنید $(1\ k) \in H$, $1 \leq k < n$. در این‌صورت

$$(1\ k+1) = (k\ \ k+1)(1\ k)(k\ \ k+1) \in H$$

(b): فرض کنید $\sigma = (1\ 2)$ و $\tau = (1\ 2\ \ldots\ n)$. به آسانی می‌توان ملاحظه نمود که $\tau^i\sigma\tau^{-i} = (i+1\ \ i+2)$ و لذا طبق قسمت قبل مسئله حل است.

www.mathematic87.blogfa.com

۱۷. (a): (برهان خلف) فرض کنید $\sigma \in C(S_n)$ و $\sigma \neq \mathrm{id}$. بنابراین $x \in \{1,2,\ldots,n\}$ چنان موجود است که $y = \sigma(x) \neq x$. حال اگر $z \notin \{x,y\}$، آنگاه $\sigma(y\ z) \neq \sigma(y\ z)$، که تناقض است.

(b): (برهان خلف) فرض کنید $\sigma \in C(A_n)$ و $\sigma \neq \mathrm{id}$. دراین‌صورت $x \in \{1,2,\ldots,n\}$ چنان موجود است که $y = \sigma(x) \neq x$. حال اگر $z \notin \{x,y,\sigma(y)\}$، آنگاه $\sigma(x\ y\ z) \neq \sigma(x\ y\ z)$، که تناقض است.

۱۹. فرض کنید $\mathrm{id} \neq \sigma \in A_n$. فرض کنید $\sigma = \sigma_1\sigma_2\ldots\sigma_k$ تجزیهٔ σ به دورهای مجزا باشد $(\sigma_i \neq \mathrm{id})$. با توجه به اینکه $\circ(\sigma) = [\circ(\sigma_1), \circ(\sigma_2), \ldots, \circ(\sigma_k)] = 2$، خواهیم داشت $\circ(\sigma_i) = 2$، یعنی هر σ_i یک ترانهش است. چون σ زوج است، لذا σ را می‌توان به‌صورت زیر نوشت:

$$\begin{aligned}\sigma &= (x_1\ y_1)(z_1\ w_1)(x_2\ y_2)(z_2\ w_2)\cdots(x_t\ y_t)(z_t\ w_t)\\ &= (x_1\ z_1\ y_1\ w_1)^2(x_2\ z_2\ y_2\ w_2)^2\cdots(x_t\ z_t\ y_t\ w_t)^2\\ &= ((x_1\ z_1\ y_1\ w_1)(x_2\ z_2\ y_2\ w_2)\cdots(x_t\ z_t\ y_t\ w_t))^2.\end{aligned}$$

فصل ۴

۱. فرض کنید H, K زیرگروه‌هایی از مرتبهٔ $5,7$ باشند. دراین‌صورت با توجه به قضیه لاگرانژ $5\|G|$ و $7\|G|$. بنابراین $35\|G|$ و در نتیجه $|G| \geq 35$.

۳. اگر G عنصری از مرتبهٔ 10 داشته باشد، آنگاه G دوری است و عنصری (زیرگروهی) از مرتبهٔ 5 خواهیم داشت. (برهان خلف) حال فرض کنید G عنصری از مرتبه‌های $10,5$ نداشته باشد. در این‌صورت مرتبهٔ هر عنصر G برابر 2 بوده و در نتیجه G آبلی است. اگر $a,b \in G$ دو عنصر متمایز از مرتبهٔ 2 باشند، قرار می‌دهیم $H = <a>$ و $K = <b>$. دراین‌صورت $|HK| = (|H||K|)/|H \cap K| = 4$. چون HK یک زیرگروه G است، لذا $4\|G|$، که تناقض است.

۵. عناصر غیر بدیهی A_5 از سه نوع زیر می‌باشند:

www.mathematic87.blogfa.com

(الف): $(a\ b\ c\ d\ e)$: تعداد $5\times4\times3\times2\times1/5=24$ عنصر از این نوع (دورهای بطول 5) وجود دارد.

(ب): $(a\ b\ c)$: تعداد $5\times4\times3/3=20$ عنصر از این نوع (دورهای بطول 3) وجود دارد.

(ج): $(a\ b)\ (c\ d)$: تعداد $(5\times4\times3\times2)/(2\times2\times2)=15$ عنصر از این نوع (حاصلضرب دودور مجزا بطول 2) وجود دارد.

فرض کنید H گروهی باشد که $[G:H]\le4$. دراینصورت $|H|\ge15$. با توجه به توضیحات فوق، دوری مانند $x=(a\ b\ c\ d\ e)$ چنان موجود است که $x\notin H$ (در حقیقت با حاصلضرب دورهای بطول 5 می‌توان همه دورهای بطول 3 را تولید کرد: $(a\ b\ c)=(a\ c\ b\ d\ e)\ (c\ b\ a\ e\ d)$). اگر $K=<x>$، آنگاه $H\cap K=\{e\}$ و لذا $|G|\ge|HK|=|H||K|/|H\cap K|=|H||K|=75$، که تناقض است.

اگر A_4, A_5 بصورت دوری نمایش داده شود، آنگاه $A_4\le A_5$ و $[A_5:A_4]=5$. توجه داشته باشید که این مطلب در حالت کلی درست است. یعنی برای هر عدد طبیعی n بزرگتر از 2، A_n دارای زیر گروهی از اندیس n است. در ضمن هر زیرگروه با اندیس n در A_n با A_{n-1} یکریخت است (تمرین ۴ از مسائل مبارزه طلب فصل ۸ ملاحظه شود).

۷. چون $a=eae^{-1}$، لذا a و a مزدوج می‌باشند. اگر a و b مزدوج باشند، آنگاه $a=gbg^{-1}$ و لذا $b=g^{-1}a(g^{-1})^{-1}$، یعنی b و a مزدوج اند. حال فرض کنید $a=gbg^{-1}$ و $b=hch^{-1}$. دراینصورت $a=gbg^{-1}=g(hch^{-1})g^{-1}=(gh)c(gh)^{-1}$. یعنی a و c مزدوج اند.

۹. (a): چون $a\notin H$، لذا $a^{-1}\notin H$. باتوجه به اینکه $[G:H]=2$، خواهیم داشت $G=H\cup a^{-1}H$ و $G=H\cup bH$. با توجه به مجزا بودن $a^{-1}H$ با H و bH با H، داریم $a^{-1}H=bH$. درنتیجه $ab\in H$.

(b): اگر $g\in H$، آنگاه بوضوح $gH=Hg=H$. حال فرض کنید $g\notin H$. در اینصورت $G=H\cup gH$ و $G=H\cup Hg$ و با توجه به $H\cap Hg=\{e\}$ و $H\cap Hg=H$، داریم $gH=Hg$.

www.mathematic87.blogfa.com

۱۱. (a): چون $aH = bK$، لذا عنصر $k \in K$ چنان موجود است که $a = bk$. حال داریم $bkH = bK$. با ضرب چپ در b^{-1}، داریم $kH = K$ و در نتیجه $H = k^{-1}K = K$.

(b): فرض کنید $c \in aH \cap bK$. دراین‌صورت عناصر $h \in H$ و $k \in K$ چنان موجودند که $c = ah = bk$. بنابراین $c(H \cap K) = cH \cap cK = ahH \cap bkK = aH \cap bK$.

۱۳. (برهان خلف) فرض کنید $g^2 \notin H$. در این‌صورت $g^2 \in gH$. ازاین‌رو $g \in H$، که تناقض می‌باشد.

۱۵. (a): به‌وضوح $x \sim x$. حال اگر $x \sim y$، آنگاه عناصر $h \in H$ و $k \in K$ چنان موجودند که $hxk = y$. از اینجا خواهیم داشت $x = h^{-1}yxk^{-1}$، یعنی $y \sim x$. حال اگر $x \sim y$ و $y \sim z$، آنگاه عناصر $h_1, h_2 \in H$ و $k_1, k_2 \in K$ چنان موجودند که $h_1xk_1 = y$ و $h_2yk_2 = z$. از اینجا $z = h_2yk_2 = h_2(h_1xk_1)k_2 = (h_2h_1)x(k_1k_2)$، یعنی $x \sim z$.

(b):

$$\begin{aligned} |HxK| &= |HxKx^{-1}| \\ &= (|H||xKx^{-1}|)/(|H \cap xKx^{-1}|) \\ &= (|H||K|)/(|H \cap xKx^{-1}|). \end{aligned}$$

(c): واضح است.

(d): فرض کنید $\Lambda = \{kHk^{-1} \mid k \in K\}$ و $\Gamma = \{aN_K(H) \mid a \in K\}$. تعریف می‌کنیم: $f : \Lambda \to \Gamma$ با ضابطهٔ $f(aHa^{-1}) = aN_K(H)$. اگر $k_1, k_2 \in K$، آنگاه خواهیم داشت:

$$\begin{aligned} k_1Hk_1^{-1} = k_2Hk_2^{-1} &\Leftrightarrow H = k_1^{-1}k_2H(k_1^{-1}k_2)^{-1} \\ &\Leftrightarrow k_1^{-1}k_2 \in N_K(H) \Leftrightarrow k_1N_K(H) = k_2N_K(H). \end{aligned}$$

این نشان می‌دهد که f خوش‌تعریف و یک به یک است. به‌وضوح f پوشاست و لذا $|\Lambda| = |\Gamma| = [K : N_K(H)]$.

۱۷. فرض کنید $G = \langle a \rangle$ یک گروه دوری از مرتبه n باشد. در این‌صورت a^k یک مولد است اگر و فقط اگر $(n,k) = 1$، لذا تعداد مولدهای G برابر $\phi(n)$ می‌باشد.

www.mathematic87.blogfa.com

۱۹. فرض کنید d یک مقسوم علیه دلخواه n باشد. تعداد عناصر G که مرتبهٔ آنها d است را با $\omega(d)$ نشان می‌دهیم. (در نظر داشته باشید که در حالت کلی ممکن است $\omega(d)=0$). به آسانی دیده می‌شود که $n=\sum_{d|n}\omega(d)$. اینک فرض کنید $a\in G$ عنصری از مرتبهٔ d باشد. قرار می‌دهیم $H=<a>=\{e,a,\ldots,a^{d-1}\}$ با توجه به اینکه H تنها زیرگروه مرتبهٔ d می‌باشد، لذا تعداد عناصر مرتبهٔ d برابر $\phi(d)$است(یعنی $\omega(d)=\phi(d)$). بنابراین

$$\omega(d)=\begin{cases}\phi(d) & \text{اگر } G \text{ عنصری از مرتبهٔ } d \text{ داشته باشد}\\ 0 & \text{در غیر این‌صورت}\end{cases}$$

با توجه به اینکه $\phi(n)=\sum_{d|n}\phi(d)$، به سادگی معلوم می‌شود که G باید عنصری از مرتبهٔ d داشته باشد. زیرا در غیراین‌صورت $\omega(d)=0$ و در نتیجه $n=\sum_{d|n}\omega(d)<\sum_{d|n}\phi(d)=n$، که تناقض است. حال چون d مقسوم علیه دلخواهی از n بود، لذا با انتخاب $d=n$ نتیجه می‌گیریم که G باید عنصری از مرتبهٔ n داشته باشد، یعنی G دوری است.

فصل ۵

۱. تابع $\varphi:\mathbb{Z}\to n\mathbb{Z}$ با ضابطهٔ $\varphi(m)=nm$ یک یکریختی است.

۳. فرض کنید $H=\left\{\begin{bmatrix}a & b\\ -b & a\end{bmatrix}|a,b\in\mathbb{R}\right\}$. در این‌صورت زیر گروهی از $\mathrm{GL}_2(\mathbb{R})$ بوده و تابع $\varphi:\mathbb{C}^*\to H$ با ضابطهٔ $\varphi(a+bi)=\begin{bmatrix}a & b\\ -b & a\end{bmatrix}$ یک یکریختی است.

www.mathematic87.blogfa.com

۵. تابع $\varphi: U(8) \to G$ با ضابطهٔ $\varphi(1)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$، $\varphi(3)=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$، $\varphi(5)=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$ و $\varphi(7)=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ یک یکریختی است.

۷. فرض کنید $G =< A,B >$. چون $A^2 = B^n = I$ و $BAB = A$، پس

$$G = \{A^i B^j \mid 0 \le i \le 1, 0 \le j \le n-1\}.$$

به آسانی می‌توان دید که تابع $\varphi: D_n \to G$ با ضابطهٔ $\varphi(\tau^i \delta^j) = A^i B^j$ یک یکریختی است.

۹.(a): اگر G دوری باشد، آنگاه $G \cong \mathbb{Z}_4$. حال فرض کنید G دوری نباشد. چون فقط e دارای مرتبهٔ 1 است. لذا سه عنصر باقیمانده باید دارای مرتبهٔ 2 باشند. فرض کنید $G = \{e,a,b,c\}$، که $a^2 = b^2 = c^2 = e$. به آسانی می‌توان ملاحظه نمود که $ab = ba = c$، $ac = ca = b$ و $bc = cb = a$. تعریف می‌کنیم: $\varphi: G \to \mathbb{Z}_2 \times \mathbb{Z}_2$، $\varphi(e) = (0,0)$، $\varphi(a) = (1,0)$، $\varphi(b) = (0,1)$ و $\varphi(c) = (1,1)$. به وضوح φ یک دوسوئی است. از طرفی $\varphi(ab) = \varphi(c) = (1,1) = (1,0) + (0,1) = \varphi(a) + \varphi(b)$. حالات دیگر را نیز می‌توان به آسانی بررسی کرد.

(b): فرض کنید G دوری نباشد. نشان می‌دهیم $G \cong S_3$. برای این منظور دو ادعای زیر را ثابت می‌کنیم.

• **ادعای۱:** G باید عنصری از مرتبهٔ 3 داشته باشد، زیرا در غیر این‌صورت برای هر $x \in G$ داریم $x^2 = e$ و به آسانی مشاهده می‌شود که G آبلی است. حال اگر e,a,b سه عنصر متمایز از G باشند، آنگاه $H = \{e,a,b,ab\}$ یک زیرگروه مرتبهٔ 4 است که با قضیهٔ لاگرانژ در تناقض است.

بنابراین فرض کنید $a \in G$ عنصری از مرتبهٔ 3 باشد وقرار می‌دهیم $K =< a >= \{e,a,a^2\}$.

• **ادعای۲:** اگر $x \in G - K$، آنگاه $\circ(x) = 2$. داریم $G = K \cup Kx$. چون $x^2 \notin Kx$ پس $x^2 \in K$. حال اگر $\circ(x) = 3$، آنگاه $x = x^4 = (x^2)^2 \in K$، که متناقض با انتخاب x است. حال فرض کنید $b \notin K$. دراین‌صورت $G = K \cup Kb$ اجتماعی از مجموعه‌های مجزاست و

www.mathematic87.blogfa.com

لذا $G=\{e,a,a^2,b,ba,ba^2\}$. با توجه به اینکه $ba\notin K$ خواهیم داشت $(ba)^2=1$، یعنی $baba=1$. پس $bab=b^{-1}=b$. به این ترتیب به آسانی مشاهده می‌شود که $G\cong S_3$.

۱۱.(a): فرض کنید $\varphi:H\to H_1$ و $\psi:K\to K_1$ یکریختی‌های مربوطه باشند. تابع $\theta:H\times K\to H_1\times K_1$ با ضابطهٔ $\theta(h,k)=(\varphi(h),\psi(k))$ یک یکریختی است.

(b): تابع $\theta:H\times K\to K\times H$ با ضابطهٔ $\theta(h,k)=(k,h)$ یک یکریختی است.

(c): فرض کنید $(x,y)\in C(H\times K)$. در این‌صورت برای هر $(h,k)\in H\times K$ داریم $(x,y)(h,k)=(h,k)(x,y)$. پس $xh=hx, yk=ky$ ولذا $(x,y)\in C(H)\times C(K)$. برعکس، اگر $(x,y)\in C(H)\times C(K)$، آنگاه برای هر $h\in H$ و $k\in K$ داریم $xh=hx$، $yk=ky$ و لذا $(x,y)(h,k)=(h,k)(x,y)$، یعنی $(x,y)\in C(H\times K)$.

(d): به آسانی از قسمت(c) بدست می‌آید.

۱۳. چون $(e,e)\in H_1\times H_2$، لذا $H_1\times H_2\neq\varnothing$. حال فرض کنید $(a_1,a_2)\in H_1\times H_2$ و $(b_1,b_2)\in H_1\times H_2$. در این‌صورت

$$(a_1,a_2)(b_1,b_2)^{-1}=(a_1,b_1)(b_1^{-1},b_2^{-1})=(a_1b_1^{-1},a_2b_2^{-1})\in H_1\times H_2$$

بنابراین $H_1\times H_2$ یک زیرگروه است. برای قسمت دوم، فرض کنید $G_1=G_2=\mathbb{Z}_p$، که p عددی اول باشد. دراین‌صورت $K=\{(x,x)\,|\,x\in\mathbb{Z}_p\}$ زیرگروهی از $\mathbb{Z}_p\times\mathbb{Z}_p$ است، که به‌صورت $H_1\times H_2$ نمی‌باشد.

۱۵. ابتدا مسئلهٔ زیر را مطرح می‌کنیم:

فرض کنید G و H دو گروه و $a\in G$ و $b\in H$ عناصری از مرتبهٔ متناهی باشند. دراین‌صورت

$$\circ(a,b)=[\circ(a),\circ(b)].$$

حل: فرض کنید $\circ(a)=m$ و $\circ(b)=n$. دراین‌صورت $(a,b)^{[m,n]}=(a^{[m,n]},b^{[m,n]})=(e,e)$. حال اگر $(a,b)^d=(e,e)$ آنگاه $a^d=b^d=e$ و لذا $m\mid d$ ، $n\mid d$ و درنتیجه $[m,n]\mid d$، یعنی $\circ(a,b)=[m,n]$.

حال به حل مسئله اصلی می‌پردازیم.

www.mathematic87.blogfa.com

فرض کنید G,H دوری و $G=<a>$ و $H=<b>$ و $(\circ(a),\circ(b))=1$. در این‌صورت با توجه به مسئلهٔ اخیر، $\circ(a,b)=[\circ(a),\circ(b)]=\circ(a)\circ(b)=|G\times H|$، یعنی $G\times H$ دوری است.
برعکس، فرض کنید $G\times H$ دوری باشد. (برهان خلف) اگر $(|G|,|H|)=d>1$، آنگاه برای هر عنصر $(g,h)\in G\times H$ خواهیم داشت $(g,h)^{|G||H|/d}=((g^{|G|})^{|H|/d},(h^{|H|})^{|G|/d})=(e,e)$. در نتیجه $G\times H$ عنصری از مرتبهٔ $|G||H|$ نخواهد داشت، که تناقض با دوری بودن $G\times H$ می‌باشد.

۱۷. تابع $\varphi:S_n\to A_{n+1}$ با ضابطهٔ زیر، یک تکریختی است. بنابراین

$$\varphi(\sigma)=\begin{cases}\sigma & \text{اگر } \sigma \text{ جایگشتی زوج باشد}\\ (n+1\ n+2)\sigma & \text{در غیر این‌صورت}\end{cases}$$

و در نتیجه $S_n\cong\varphi(S_n)\le A_{n+2}$.

۱۹.(a): تابع $\varphi:\mathrm{Aut}(\mathbb{Z}_n)\to U(n)$ با ضابطهٔ $\varphi(\sigma)=\sigma(1)$، را در نظر می‌گیریم. چون σ یک یکریختی است لذا $\sigma(1)$ مولدی برای $\mathbb{Z}_n$ است، یعنی σ خوش‌تعریف است.
اگر $\tau\in\mathrm{Aut}(\mathbb{Z}_n)$ و $\tau(1)=k$، آنگاه

$$\varphi(\sigma\tau)=\sigma\tau(1)=\sigma(k)=k\,\sigma(1)=\sigma(1)(k)=\sigma(1)\tau(1)=\varphi(\sigma)\varphi(\tau).$$

یک به یک بودن φ بدیهی است برای اثبات پوشا بودن، فرض کنید $m\in U(n)$. تابع $\tau_m\in\mathbb{Z}_n\to\mathbb{Z}_n$ با ضابطهٔ $\tau_m(1)=m$ به‌وضوح خودریختی است و $\varphi(\tau_m)=\tau_m(1)=m$. از این‌رو φ یک یکریختی است.

(b): تابع $\varphi:\mathrm{Aut}(\mathbb{Z}_n\times\mathbb{Z}_n)\to\mathrm{GL}_2(\mathbb{Z}_n)$ با ضابطهٔ $\varphi(\sigma)=\begin{bmatrix}a & c\\ b & d\end{bmatrix}$، که در آن $\sigma(1,0)=(a,b)$ و $\sigma(0,1)=(c,d)$ یک یکریختی است.

(c): با توجه به قسمت(b) داریم $|\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2)|=|\mathrm{GL}_2(\mathbb{Z}_2)|=6$. چون $\mathrm{GL}_2(\mathbb{Z}_2)$ یک گروه ناآبلی است، لذا $\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2)\cong\mathrm{GL}_2(\mathbb{Z}_2)\cong S_3$.

www.mathematic87.blogfa.com

فصل ۶

۱.(a): چون $[S_4 : A_4] = 2$، پس $A_4 \trianglelefteq S_4$. درضمن $S_4 / A_4 = \{A_4, (1\ 2)A_4\}$ و جدول S_4 / A_4

$\cdot$	A_4	$(1\ 2)A_4$
A_4	A_4	$(1\ 2)A_4$
$(1\ 2)A_4$	$(1\ 2)A_4$	A_4

(b): مشابه قسمت(a) می‌باشد.

(c): داریم:

$$D_4 = \{\mathrm{id}, (1\ 3), (2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$$

چون $(2\ 3)(1\ 3)(2\ 3)^{-1} = (1\ 2) \notin D_4$، لذا D_4 زیرگروه نرمالی از A_4 نیست.

۳.(a): φ یک همریختی است. زیرا:

$$\varphi(ab) = \begin{bmatrix} 1 & 0 \\ 0 & ab \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} = \varphi(a)\varphi(b)$$ و

$$\mathrm{Ker}\varphi = \left\{ a \in \mathbb{R}^* \mid \varphi(a) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} = \{1\}.$$

(b): φ همریختی نیست، زیرا:

$$1 = \varphi\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) \neq \varphi\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 2$$

(c): φ یک همریختی است، زیرا:

$$\varphi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}\right) = b_1 + b_2 = \varphi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right)$$

$$\mathrm{Ker}\varphi = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};\ a,d,c \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \mid a,d,c \in \mathbb{R} \right\}.$$

۵. (a): φ یک همریختی است، زیرا: $\varphi(n+m) = 7(n+m) = 7n + 7m = \varphi(n) + \varphi(m)$

و $\mathrm{Ker}\varphi = \{0\}$ و $\mathrm{Im}\varphi = 7\mathbb{Z}$.

(b): φ یک همریختی است، زیرا: $\varphi(a+b)=n(a+b)=na+nb=\varphi(a)+\varphi(b)$.

(c): این ضرب ماتریسی را می‌توان به‌صورت تابع $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ با ضابطهٔ $\varphi(X)=AX$ در نظر گرفت. φ همریختی است. زیرا: $\varphi(X+Y)=A(X+Y)=AX+AY=\varphi(X)+\varphi(Y)$.

۷. هر $x\in G$ را می‌توان به‌صورت $x_{i_1}^{\alpha_1}\dots x_{i_k}^{\alpha_k}$ نوشت، که در اینجا $i_j\in I$ و $\alpha_j\in\{\pm1\}$. حال خواهیم داشت:

$$\varphi(x)=\varphi(x_{i_1}^{\alpha_1}\dots x_{i_k}^{\alpha_k})=\varphi(x_{i_1}^{\alpha_1})\dots\varphi(x_{i_k}^{\alpha_k})=\varphi(x_{i_1})^{\alpha_1}\dots\varphi(x_{i_k})^{\alpha_k}.$$

یعنی مقدار $\varphi(x)$ با مقدارهای $\varphi(x_i)$ کاملاً مشخص می‌شود.

۹. (a): به‌وضوح $\mathrm{Hom}(G,H)$ تحت این عمل جمع بسته است. همریختی بدیهی $o:G\to H$ با ضابطهٔ $o(g)=e$ عنصر همانی این عمل می‌باشد. عنصر معکوس $\alpha\in\mathrm{Hom}(G,H)$ همریختی $(-\alpha):G\to H$ با ضابطهٔ $(-\alpha)(g)=-\alpha(g)$ می‌باشد.

(b): برای هر $h\in H$ تابع $\sigma_h:\mathbb{Z}\to H$ با ضابطهٔ $\sigma_h(1)=h$ یک همریختی است. به‌راحتی می‌توان نشان داد که $\varphi:H\to\mathrm{Hom}(\mathbb{Z},H)$ با ضابطهٔ $\varphi(g)=\sigma_h$ یک یکریختی است.

(c): برای هر $k\in\mathbb{Z}_d$ تابع $\alpha_k:\mathbb{Z}_m\to\mathbb{Z}_n$ با ضابطهٔ $\alpha_k(x)=(k\frac{n}{d})x$ یک همریختی است. به راحتی می‌توان نشان داد که $\varphi:\mathbb{Z}_d\to\mathrm{Hom}(\mathbb{Z}_m,\mathbb{Z}_n)$ با ضابطهٔ $\varphi(k)=\alpha_k$ یک یکریختی است.

۱۱. (a): به آسانی از قضیهٔ ۶-۱۲ بدست می‌آید (تمرین ۹ فصل ۴ ملاحظه شود).

(b): فرض کنید H زیرگروهی از اندیس 2 در S_n باشد. با توجه به (a)، $H\trianglelefteq S_n$. فرض کنید $\sigma=(a\ b\ c)$ دوری بطول 3 از S_n باشد. چون $(\sigma H)^2=H$، لذا $\sigma^2\in H$ و در نتیجه $\sigma=\sigma\sigma^3=(\sigma^2)^2\in H$. یعنی H شامل تمام دورهای بطول 3 است. بنابراین $A_n\subseteq H$. از طرفی $2=[S_n:A_n]=[S_n:H][H:A_n]=2[H:A_n]$، پس $H=A_n$.

۱۳. (a): چون $\varphi(g)\varphi(n)\varphi(g)^{-1}=\varphi(gng^{-1})\in\varphi(N)$، پس $\varphi(N)\trianglelefteq\varphi(G)$. به آسانی می‌توان دید که تابع $\theta:G/N\to\varphi(G)/\varphi(N)$ با ضابطهٔ $\theta(gN)=\varphi(g)\varphi(N)$ یک یکریختی است.

www.mathematic87.blogfa.com

(b): فرض کنید $x \in \varphi^{-1}(K)$ و $g \in G$. در این‌صورت برای عنصری مانند $k \in K$ داریم $\varphi(x) = k$ و در نتیجه $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)k\,\varphi(g)^{-1} \in K$. بنابراین $gxg^{-1} \in \varphi^{-1}(K)$، یعنی $\varphi^{-1}(K) \trianglelefteq G$. به آسانی می‌توان نشان داد که تابع $\theta : G/\varphi^{-1}(K) \to H/K$ با ضابطهٔ $\theta(g\varphi^{-1}(K)) = \varphi(g)K$ یک یکریختی است.

۱۵. (a): برای هر $g \in G$ تابع $\tau_g : G \to G$ با ضابطهٔ $\tau_g(x) = gxg^{-1}$ یک خودریختی است. به راحتی می‌توان نشان داد که $\varphi : G \to \mathrm{Aut}(G)$ با ضابطهٔ $\varphi(g) = \tau_g$ یک همریختی است. در ضمن

$$\mathrm{Ker}\varphi = \{g \in G \mid \tau_g = id\} = \{g \in G \mid gxg^{-1} = x \ ; \ \forall x \in G\} = C(G).$$

اکنون با استفاده از قضیهٔ اول یکریختی نتیجهٔ مطلوب حاصل می‌شود.

(b): چون $C(S_3) = \{\mathrm{id}\}$، لذا $\mathrm{Inn}(S_3) \cong S_3$. کافی است نشان دهیم $|\mathrm{Aut}(S_3)| \le 6$. داریم $S_3 = <(1\ 2), (1\ 2\ 3)>$. بنابراین هر خودریختی، $\varphi \in \mathrm{Aut}(S_3)$، توسط $\varphi(1\ 2)$ و $\varphi(1\ 2\ 3)$ تعیین می‌شود. اما $2 = o(\varphi(1\ 2)) \mid o(\varphi(1\ 2\ 3)) = 3$. پس برای $\varphi(1\ 2)$ سه انتخاب $(1\ 2)$، $(1\ 3)$، $(2\ 3)$ و برای $\varphi(1\ 2)$ دو انتخاب $(1\ 2\ 3)$ و $(1\ 3\ 2)$ وجود دارد. پس حداکثر $3.2 = 6$ انتخاب برای φ وجود دارد.

۱۷. فرض کنید $h \in H$. چون $1 = (|H|, [G : N])$، لذا اعداد صحیح $m, n \in \mathbb{Z}$ چنان موجودند که $m|H| + n[G : N] = 1$. حال داریم

$$hN = (hN)^{m|H|+n[G:N]} = (hN)^{m|H|}(hN)^{n[G:N]} = (x^{|H|}N)^m((hN)^{[G:N]})^n = NN = N$$

و در نتیجه $h \in N$، یعنی $H \le N$.

۱۹. فرض کنید

$$G = D_4 = \{\mathrm{id}, (1\ 3), (2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$$

و $H = \{\mathrm{id}, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$ و $K = \{\mathrm{id}, (1\ 4)(2\ 3)\}$. دراین‌صورت چون $[G : H] = 2$ و $[H : K] = 2$، لذا $H \trianglelefteq G$ و $K \trianglelefteq H$. اکنون نشان می‌دهیم که K زیرگروه نرمال G نیست. برای $(2\ 4) \in G$ داریم $(2\ 4)^{-1}(1\ 4)(2\ 3)(2\ 4) = (1\ 2)(3\ 4) \notin K$ و در نتیجه K زیرگروه نرمال G نیست.

www.mathematic87.blogfa.com

۲۱. (a): فرض کنید $\sigma \in G$ یک جایگشت فرد و A مجموعهٔ همهٔ جایگشتهای زوج G باشد. نشان می‌دهیم $G = A \cup \sigma^{-1}A$. واضح است که $A \cup \sigma^{-1}A \subseteq G$. حال فرض کنید $\delta \in G$. اگر δ زوج باشد، آنگاه $\delta \in A$. اگر $\delta \in G$ فرد باشد، آنگاه $\sigma\delta \in A$ و در نتیجه $\delta \in \sigma^{-1}A$. بنابراین $G = A \cup \sigma^{-1}A$. چون $|G| = |A \cup \sigma^{-1}A| = |A| + |\sigma^{-1}A| = 2|A|$، داریم $[G : A] = 2$، یعنی G زیرگروهی از اندیس 2 دارد.

(b): با توجه به اثبات قضیهٔ ۶-۱۲ داریم $G / \mathrm{Ker}\varphi \cong \varphi(G) \leq S_n$. چون G ساده است لذا $\mathrm{Ker}\varphi = <e>$. به عبارت دیگر داریم $G \cong \varphi(G) \leq S_n$. ادعا می‌کنیم که $\varphi(G) \leq A_n$. زیرا هرگاه $\varphi(G)$ شامل یک جایگشت فرد باشد، آنگاه طبق قسمت(a) ، G دارای زیرگروه نرمالی از اندیس 2 است، که با سادگی G در تناقض است.

(c): (برهان خلف) فرض کنید G ساده نباشد. در این‌صورت با توجه به قسمت(b)، G با زیرگروهی از A_n یکریخت است. در نتیجه $|G| \,|\, |A_n| = n!/2$، که تناقض است.

فصل ۷

۱. برای هر عدد اول p ، تنهاگروه از مرتبهٔ p، گروه دوری $\mathbb{Z}_p$ می‌باشد. برای اعدادی به‌صورت $n = pq$، که p,q اعداد اول متمایز می‌باشند، تنهاگروه آبلی از مرتبهٔ n، گروه دوری $\mathbb{Z}_n$ می‌باشد. حال به بررسی بقیهٔ اعداد می‌پردازیم:

مرتبهٔ 4: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$.

مرتبهٔ 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

مرتبهٔ 9: $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$.

مرتبهٔ 12: $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

مرتبهٔ 16: $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

مرتبهٔ 18: $\mathbb{Z}_{18}$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

مرتبهٔ 20: $\mathbb{Z}_{20}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.

www.mathematic87.blogfa.com

مرتبهٔ 24: $\mathbb{Z}_{24}$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3$, $\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_3$.

مرتبهٔ 25: $\mathbb{Z}_{25}$, $\mathbb{Z}_5\times\mathbb{Z}_5$.

مرتبهٔ 27: $\mathbb{Z}_{27}$, $\mathbb{Z}_9\times\mathbb{Z}_3$, $\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$.

مرتبهٔ 28: $\mathbb{Z}_{28}$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_7$.

۳. فرض کنید $(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_{p^2}$ از مرتبهٔ عدد اول p باشد. دراین‌صورت $pa=pb=0$. بنابراین $a\in A=\{0,1,2,\ldots,p-1\}$ و $b\in B=\{0,p,2p,\ldots,(p-1)p\}$. با توجه به اینکه هر عنصر $A\times B$ بجز $(0,0)$ از مرتبهٔ p است، لذا تعداد عناصر از مرتبهٔ p عبارت است از $|A\times B|-1=p^2-1$.

۵. با توجه به قضیه اساسی گروه‌های آبلی متناهی مولد، خواهیم داشت:

$$G\cong\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_t}\times\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{r\text{ بار}}$$

اگر $r\neq 0$، آنگاه G دارای عنصری از مرتبه نامتناهی خواهد بود. پس $r=0$، یعنی $G\cong\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_t}$. چون مرتبه هر عنصر G عدد اول p است، پس $m_1=\cdots=m_t=p$ و در نتیجه $G\cong\mathbb{Z}_p\times\cdots\times\mathbb{Z}_p$.

۷. فرض کنید G دوری باشد. دراین‌صورت هر زیرگروه G دوری است ولذا G دارای زیر گروهی به‌شکل $\mathbb{Z}_p\times\mathbb{Z}_p$ نمی‌باشد.

برعکس، با توجه به قضیه اساسی $G\cong\mathbb{Z}_{p_1^{n_1}}\times\mathbb{Z}_{p_2^{n_2}}\times\cdots\times\mathbb{Z}_{p_k^{n_k}}$. چون G دوری نیست لذا اعداد اول p^{n_i} نمی‌توانند همگی متمایز باشند. بدون اینکه از کلیت کاسته شود می‌توان فرض کرد $p_1=p_2=p$. ازاین‌رو $G\cong\mathbb{Z}_{p^{n_1}}\times\mathbb{Z}_{p^{n_2}}\times\mathbb{Z}_{p_3^{n_3}}\times\cdots\times\mathbb{Z}_{p_k^{n_k}}$. فرض کنید $H=\mathbb{Z}_p\times\mathbb{Z}_p\times<0>\times\cdots\times<0>$. چون $H\cong\mathbb{Z}_p\times\mathbb{Z}_p$، لذا G دارای زیرگروهی به‌شکل $\mathbb{Z}_p\times\mathbb{Z}_p$ می‌باشد.

۹.(a): اگر $n=1$، آنگاه $d=1$ و $<0>$ زیرگروهی از مرتبهٔ d است. حال فرض کنید $n>1$. در این‌صورت اعداد اول $p_1,p_2,\ldots,p_k$ و اعداد صحیح مثبت $n_1,n_2,\ldots,n_k$ چنان موجودند

www.mathematic87.blogfa.com

که $G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$. بنابراین $n = p_1^{n_1} \ldots p_k^{n_k}$. چون $d \mid n$ ، لذا اعداد $0 \le d_i \le n_i$ چنان موجودند که $d = p_1^{d_1} \ldots p_k^{d_k}$. فرض کنید H_i زیرگروهی از مرتبهٔ $p_i^{d_i}$ از گروه دوری $\mathbb{Z}_{p_i^{n_i}}$ باشد. در این‌صورت $H = H_1 \times \cdots \times H_k$ زیرگروهی از مرتبهٔ d از G است.

برای قسمت دوم، فرض کنید H زیرگروهی از G از مرتبهٔ n/d باشد. در این‌صورت $|G/H| = d$.

(b): ابتدا فرض کنید $|G| = p^n$. فرض کنید $x \in G$ عنصری با بزرگترین مرتبه باشد. فرار می‌دهیم ، $H = \langle x \rangle = \{e, x, x^2, \ldots, x^{p^m - 1}\}$ که در آن $\circ(x) = p^m$. با توجه به اینکه تمامی عناصر G در معادلهٔ $x^{p^m} = e$ صدق می‌کند ، لذا طبق فرض عناصر H تنها ریشه‌های این معادله می‌باشند. حال فرض کنید $a \in G$. در این‌صورت $\circ(a) = p^k \le p^m$. در نتیجه $a^{p^m} = e$ و لذا $a \in H$. چون $a \in G$ عنصر دلخواهی بود ، پس $G = H$.(حالت کلی) حال فرض کنید $|G| = n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ ، که اعداد اول متمایز می‌باشند. با توجه به قسمت (a) ، فرض کنید H_i زیرگروهی از G از مرتبهٔ $p_i^{n_i}$ باشد. چون H_i در فرض قسمت (a) صادق است ، لذا H_i دوری است و ازاین‌رو

$$G \cong H_1 \times H_2 \times \cdots \times H_k \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \cong \mathbb{Z}_n .$$

۱۱. فرض کنید $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ و $H \cong \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_\ell} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$ که دراینجا $m_{i-1} \mid m_i$ و $n_{i-1} \mid n_i$، برای هر $1 \le i \le t$ و $k_\ell \mid n_1$. فرض کنید $m_t \ne n_t$. بدون اینکه از کلیت کاسته شود می‌توان فرض کرد $m_t > n_t$. در این‌صورت G دارای زیرگروهی از مرتبهٔ m_t است درصورتیکه H عنصری از مرتبهٔ m_t نمی‌باشد، که تناقض می‌باشد. بنابراین $m_t = n_t$. حال فرض کنید $m_{t-1} \ne n_{t-1}$. بدون اینکه از کلیت کاسته شود می‌توان فرض کرد $m_{t-1} > n_{t-1}$. در این‌صورت تعداد عناصر G از مرتبهٔ m_{t-1}از تعداد عناصر H از مرتبهٔ m_{t-1}بیشتر است، که تناقض می‌باشد، لذا $m_{t-1} = n_{t-1}$. با ادامهٔ این روند برای هر $1 \le i \le t$ داریم $m_i = n_i$. حال اگر $k_\ell > 1$، آنگاه تعداد عناصر H از مرتبهٔ k_ℓ از تعداد

www.mathematic87.blogfa.com

عناصر G از مرتبهٔ k_ℓ بیشتر است، که تناقض می‌باشد. بنابراین $k_\ell = 1$ و در نتیجه $\mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_\ell} \cong < 0 > \times \cdots \times < 0 > \cong < 0 >$، یعنی $G \cong H$.

۱۳.(a): (برهان خلف) فرض کنید $\mathbb{Q} = < a_1/b_1, a_2/b_2, \ldots, a_n/b_n >$. فرض کنید p عدد اولی باشد که هیچ یک از اعداد $b_1, b_2, \ldots, b_n$ را عاد نکند. داریم:

$$1/p = r_1(a_1/b_1) + r_2(a_2/b_2) + \cdots + r_n(a_n/b_n) = a/(b_1 b_2 \cdots b_n),$$

جاییکه $a, r_i \in \mathbb{Z}$. در نتیجه $p \mid b_1 b_2 \cdots b_n$، که تناقض است.

(b): فرض کنید H یک زیرگروه متناهی از $\mathbb{Q}/\mathbb{Z}$. برای هر $n \in \mathbb{N}$ داریم:

$$\{x + \mathbb{Z} \mid n(x + \mathbb{Z}) = \mathbb{Z}\} = \{x + \mathbb{Z} \mid nx \in \mathbb{Z}\}$$
$$= \{x + \mathbb{Z} \mid x = m/n, m \in \mathbb{Z}\} \subseteq \{1/n + \mathbb{Z}, 2/n + \mathbb{Z}, \ldots, n/n + \mathbb{Z}\}$$

یعنی معادلهٔ $n(x + \mathbb{Z}) = \mathbb{Z}$ در $\mathbb{Q}/\mathbb{Z}$ و در نتیجه در H حداکثر دارای n ریشه است و لذا با توجه به تمرین۸ قسمت(b) H دوری است.

۱۵. فرض کنید $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$، جاییکه $m_{i-1} \mid m_i$، $2 \le i \le t$. قرار می‌دهیم:

$$x_1 = (0, 0, \ldots, 0, 0, 1)$$
$$x_2 = (0, 0, \ldots, 0, 1, 1)$$
$$x_3 = (0, 0, \ldots, 1, 0, 1)$$
$$\vdots$$
$$x_t = (1, 0, \ldots, 0, 0, 1)$$

دراین‌صورت $\circ(x_i) = m_t$. یعنی عناصر x_i در گروه G از مرتبهٔ ماکزیمال می‌باشند. از طرفی $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} = < x_1, x_2, \ldots, x_t >$، زیرا برای هر $x \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ داریم:

$$x = (a_1, a_2, \ldots, a_t) = a_t(x_1) + a_{t-1}(x_2 - x_1) + \cdots + a_1(x_t - x_1)$$

اگر $\varphi : \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} \to G$ یکریختی مربوطه باشد، آنگاه به‌وضوح $\varphi(x_i)$ها عناصری با مرتبهٔ ماکزیمال از G بوده و $G = < \varphi(x_1), \varphi(x_2), \ldots, \varphi(x_t) >$.

۱۷. (a): فرض کنید $t + s = n$. در این‌صورت مجموعهٔ $\{e_1, e_2, \ldots, e_n\}$، که در

www.mathematic87.blogfa.com

آن $e_i=(0,0,\ldots 0,1,0,\ldots,0)$ (1 در مکان i ام قرار دارد). یک مولد برای G می‌باشد. ادعا می‌کنیم $\mu(G)=t+s$. (برهان خلف) فرض کنید $m=\mu(G)<t+s$ و $X=\{x_1,\ldots,x_m\}$ مولدی برای G باشد. تعریف می‌کنیم:

$$\theta: F=\overbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}^{m\text{ بار}}\to G$$
$$(r_1,\ldots,r_m)\mapsto r_1x_1+\cdots+r_mx_m.$$

به آسانی مشاهده می‌شود که θ یک برووریختی است. ازاین‌رو $F/\mathrm{Ker}\theta\cong G$. بنابراین عدد صحیحی مانند $r\,(1\le r\le m)$ و اعداد صحیح مثبتی مانند $n_r,\ldots,n_1$ وجود دارد به طوری که $2\le i\le r$ ، $n_{i-1}\big|n_i$

$$G\cong F/\mathrm{Ker}\theta\cong\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_r}\times\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{\ell\text{ بار}},$$

که دراینجا $r+\ell=m$. چون $r+\ell=m<n=s+t$، لذا دو تجزیهٔ متمایز برای G خواهیم داشت که تناقض است.

(b): به آسانی ازقسمت(a) نتیجه می‌شود.

۱۹. فرض کنید $G\cong\mathbb{Z}_{p^{n_1}}\times\mathbb{Z}_{p^{n_2}}\times\cdots\times\mathbb{Z}_{p^{n_k}}$. دو حالت در نظر می‌گیریم:

حالت (۱): $G\cong\mathbb{Z}_p\times\mathbb{Z}_p\times\cdots\times\mathbb{Z}_p$ (با n مولفه). در این حالت با توجه به تمرین ۱۸، داریم $\mathrm{Aut}(G)\cong\mathrm{GL}_n(\mathbb{Z}_p)$. بنابراین کافی است ثابت کنیم $p\big|\mathrm{GL}_n(\mathbb{Z}_p)$. برای این منظور عنصر زیر از $\mathrm{GL}_n(\mathbb{Z}_p)$ را در نظر می‌گیریم:

$$A=\begin{bmatrix}1&1&\cdots&1\\0&1&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&1\end{bmatrix}$$

به آسانی مشاهده می‌شود که $\circ(A)=p$ و لذا $p\big|\mathrm{GL}_n(\mathbb{Z}_p)$.

www.mathematic87.blogfa.com

حالت (۲): اگر G به‌شکل حالت(۱) نباشد، آنگاه بدون اینکه از کلیت کاسته شود می‌توان فرض کرد $G \cong H \times K$، جاییکه $H = \mathbb{Z}_{p^{n_1}}$، $n_1 \geq 2$ و $K = \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$. با توجه به تمرین ۲۰ فصل۵، $\mathrm{Aut}(H)$ با زیرگروهی از $\mathrm{Aut}(G)$ یکریخت خواهد بود و لذا $p \mid |\mathrm{Aut}(G)|$، یعنی $|\mathrm{Aut}(H)| = |U(p^{n_1})| = p^{n_1}(1-\frac{1}{p}) \mid |\mathrm{Aut}(G)|$.

فصل۸

۱. $G_1 = \{\mathrm{id}, (2\ 3)\}$، $G_2 = \{\mathrm{id}, (1\ 3)\}$، $G_3 = \{\mathrm{id}, (1\ 2)\}$.

(b): $X_{\mathrm{id}} = \{1,2,3,4,5,6\}$، $X_{(12)} = \{3,4,5,6\}$، $X_{(3\ 4\ 5)} = X_{(3\ 5\ 4)} = \{1,2,6\}$ و $X_{(1\ 2)(3\ 4\ 5)} = X_{(1\ 2)(3\ 5\ 4)} = \{6\}$.

$G_1 = G_2 = \{\mathrm{id}, (3\ 4\ 5), (3\ 5\ 4)\}$ و $G_3 = G_4 = G_5 = \{id, (1\ 2)\}$ و $G_6 = G$.

۳.(a): $\overline{\mathrm{id}} = \{\mathrm{id}\}$ ، $\overline{(1\ 2)} = \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}$،

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

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

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

$$|S_4| = |C(S_4)| + [S_4 : C((1\ 2))] + [S_4 : C((1\ 2)(3\ 4))] + [S_4 : C((1\ 2\ 3))] + [S_4 : C((1\ 2\ 3\ 4))]$$
$$24 \quad = 1 \quad + 6 \quad + 3 \quad + 8 \quad + 6$$

(b): $\overline{\mathrm{id}} = \{\mathrm{id}\}$ ، $\overline{(1\ 3)} = \{(1\ 3), (2\ 4)\}$،

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

$$|D_4| = |C(D_4)| + [D_4 : C((1\ 3))] + [D_4 : C((1\ 2)(3\ 4))] + [D_4 : C((1\ 2\ 3\ 4))]$$
$$8 \quad = 2 \quad + 2 \quad + 2 \quad + 2$$

(c): $\overline{0} = \{0\}$، $\overline{1} = \{1\}$، ...، $\overline{8} = \{8\}$ و معادلهٔ رده‌ای عبارت است از $|\mathbb{Z}_9| = |C(\mathbb{Z}_9)| = 9$.

(d): $\overline{1} = \{1\}$ ، $\overline{-1} = \{-1\}$، $\overline{I} = \{\pm I\}$، $\overline{J} = \{\pm J\}$، $\overline{K} = \{\pm K\}$

$$|Q| = |C(Q)| + [Q : C(I)] + [Q : C(J)] + [Q : C(K)]$$
$$8 \quad = 2 \quad + 2 \quad + 2 \quad + 2$$

۵. فرض کنید $|G| = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ که در آن $p_i^{\alpha_i}$ اعداد اول متمایزی هستند. فرض کنید P_iها زیرگروه‌های سیلوی G باشند که $|P_i| = p_i^{\alpha_i}$. چون $P_i \trianglelefteq G$ و $P_i \cap P_j = \{e\}$، لذا برای هر $x_i \in P_i$ و هر $x_j \in P_j$ داریم $x_i x_j = x_j x_i$. حال اگر $x \in P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_n \cap P_i$، آنگاه $x = x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$ و در نتیجه $\circ(x) \mid p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_n^{\alpha_n}$. از طرفی چون $\circ(x) \mid p_i^{\alpha_i}$، لذا $\circ(x) = 1$، یعنی $x = e$. چون $|G| = |P_1 P_2 \dots P_n|$، پس $G = P_1 P_2 \dots P_n$ و لذا $G \cong P_1 \times P_2 \times \dots \times P_n$.

۷.(a): چون $p^2 q^2 \mid n_p = 1 + kp$، لذا $n_p \in \{1, q, q^2\}$. اگر $n_p = q$ یا $n_p = q^2$، آنگاه $p \mid q^2 - 1$، که تناقض است. بنابراین تنها یک $p-$زیر گروه سیلوخواهیم داشت (مثلاً P). به همین ترتیب تنها یک $q-$زیر گروه سیلوخواهیم داشت(مثلاً Q).

چون این زیر گروه‌های سیلو یکتا هستند با توجه به قضیه دوم سیلو در G نرمال خواهد بود. ولذا $G \cong P \times Q$. چون P, Q آبلی‌اند، لذا G نیز آبلی خواهد بود. سه مثال از چنین اعداد اولی عبارتند از: $(11,17), (7,17), (5,13)$.

(b): با استدلالی مشابه باقسمت(a) خواهیم داشت $n_p = n_q = 1$. اگر P, Q به ترتیب $p-$زیر گروه سیلو و $q-$زیر گروه سیلوباشند، آنگاه $G \cong P \times Q$ ولذا G آبلی خواهد بود.

۹. فرض کنید G حاصلضرب مستقیم $p-$سیلو زیرگروه‌هایش باشد. به عبارت دیگر $G = P_1 P_2 \dots P_n$، که در اینجا P_iها زیرگروه‌های سیلومی‌باشند. نشان می‌دهیم $C(P_i) \subseteq C(G)$، $1 \le i \le n$. برای این منظور فرض کنید $y \in C(P_i)$ و $x = x_1 x_2 \dots x_n \in G$ ($x_j \in P_j$). با توجه به اینکه برای هر $j \neq i$ عناصر P_j, P_iبا هم جابجا می‌شوند، خواهیم داشت:

$$yx = y(x_1 x_2 \dots x_{i-1} x_i x_{i+1} \dots x_n) = x_1 x_2 \dots x_{i-1} (y x_i) x_{i+1} \dots x_n$$
$$= x_1 x_2 \dots x_{i-1} (x_i y) x_{i+1} \dots x_n = xy.$$

ازاین‌رو $y \in C(G)$، یعنی $C(P_i) \subseteq C(G)$.

۱۱. اگر $p = 2$ ، آنگاه $G \cong \mathbb{Z}_6$ یا $G \cong S_3$ و لذا حکم به‌وضوح برقرار است . حال فرض کنید $p > 2$. طبق قضیهٔ سوم سیلو $n_p = 1 + kp \mid p(p+1)$ و لذا $n_p = 1$ یا $n_p = p + 1$.

www.mathematic87.blogfa.com

اگر $n_p = 1$، آنگاه حکم به‌وضوح برقرار است. حال فرض کنید $n_p = p+1$ و $P = <a> = \{e, a, a^2, \ldots, a^{p-1}\}$ یک $p-$سیلو زیرگروه از G باشد. در این‌صورت

$$p+1 = n_p = [G : N_G(P)] = |G|/|N_G(P)| = p(p+1)/|N_G(P)|.$$

از این‌رو $|N_G(P)| = p$ و در نتیجه $N_G(P) = P$. چون $p \neq 2$، لذا G دارای عنصری مانند x از مرتبهٔ 2 است. قرار می‌دهیم:

$$S = \{a^i x a^{-i} \mid 0 \leq i \leq p-1\}.$$

براحتی می‌توان نشان داد که مرتبهٔ کلیهٔ عناصر S برابر 2 است. اینک ثابت می‌کنیم عناصر S متمایزند. (برهان خلف) فرض کنید $i \neq j$ و $a^i x a^{-i} = a^j x a^{-j}$. در این‌صورت $x^{-1}a^{i-j}x = a^{i-j}$ ولذا برای هر $t \in \mathbb{Z}$، $x^{-1}a^{t(i-j)}x = a^{t(i-j)}$. از این‌رو خواهیم داشت $x \in N_G(P) = P$ و درنتیجه $x^{-1}Px \subseteq P$. بنابراین $\circ(x) = 1$ یا $\circ(x) = p$ ، که تناقض است . با توجه به اینکه هر دو زیرگروه از مرتبهٔ p از G تنها عنصر همانی را در اشتراک دارند ، لذا G دارای $n_p(p-1) = (p+1)(p-1)$ عنصر از مرتبهٔ p خواهد بود و چون $|S| = p$، پس خواهیم داشت:

$$|G| = p \text{ تعداد عناصر از مرتبهٔ } + |S| + 1,$$

یعنی هر عنصر غیر همانی G یا از مرتبهٔ 2 است یا از مرتبهٔ p و لذا $|G| = 2^m p$. حال با توجه به قضیهٔ اول سیلو، G دارای زیرگروهی مانند H از مرتبهٔ 2^m می‌باشد. چون اشتراک H با هر زیرگروه $p-$ سیلو برابر عنصر همانی است، لذا عناصر غیرهمانی H لزوماً در S می‌باشند. بنابراین $H = S \cup \{e\}$ و در نتیجه H تنها زیرگروه G از مرتبهٔ 2^m است. از این‌رو $H \trianglelefteq G$، یعنی G زیرگروه نرمالی از مرتبهٔ $p+1$ دارد.

۱۳. تمام $3-$زیر گروه سیلوهای S_4 عبارتند از: $P_1 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$،

$P_2 = \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$، $P_3 = \{\mathrm{id}, (1\ 2\ 5), (1\ 5\ 2)\}$، $P_4 = \{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$،

$P_5 = \{\mathrm{id}, (1\ 3\ 5), (1\ 5\ 3)\}$، $P_6 = \{\mathrm{id}, (1\ 4\ 5), (1\ 5\ 4)\}$، $P_7 = \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}$،

$P_8 = \{\mathrm{id}, (2\ 3\ 5), (2\ 5\ 3)\}$، $P_9 = \{\mathrm{id}, (2\ 4\ 5), (2\ 5\ 4)\}$، $P_{10} = \{\mathrm{id}, (3\ 4\ 5), (3\ 5\ 4)\}$. این زیرگروه‌ها مزدوجند

www.mathematic87.blogfa.com

زیرا $P_1=(3\ 4)$، $P_2=(3\ 4)P_1(3\ 4)$، $P_3=(4\ 5)P_2(4\ 5)$، $P_4=(2\ 3)(4\ 5)P_3(2\ 3)(4\ 5)$، $P_5=(4\ 5)P_4(4\ 5)$، $P_6=(3\ 4)P_5(3\ 4)$، $P_7=\begin{pmatrix}1&4&5\\2&3&4\end{pmatrix}P_6\begin{pmatrix}1&4&5\\2&3&4\end{pmatrix}^{-1}$، $P_8=(4\ 5)P_7(4\ 5)$، $P_9=(3\ 4)P_8(3\ 4)$ و $P_{10}=(2\ 3)P_9(2\ 3)$.

۱۵. (a): فرض کنید $[G:H]<p$. در این‌صورت $|G|\nmid[G:H]!$ و در نتیجه G ساده نمی‌باشد، که تناقض با فرض است.

(b): فرض کنید X یک رده تزویجی از G باشد که $|X|>1$. (با توجه به غیرآبلی بودن G چنین فرضی ممکن است). در این‌صورت $x\in G$ چنان موجود است که $X=\overline{x}$. ازاین‌رو $|X|=|\overline{x}|=[G:C(x)]>1$ و لذا $C(x)<G$ بنابراین طبق قسمت(a) داریم $|X|=[G:C(x)]\geq p$.

۱۷. فرض کنید G روی N با تزویج عمل کند. اگر $\overline{x}_1$، $\overline{x}_2$، ...، $\overline{x}_n$ تمام مدارها باشند، آنگاه معادلهٔ رده‌ای به‌صورت زیرخواهد بود:

$$|N|=\sum_{i=1}^{n}\overline{x}_i=\sum_{i=1}^{n}[G:C(x_i)]$$

با توجه به اینکه $[G:C(x_i)]=1\Leftrightarrow G=C(x_i)\Leftrightarrow x_i\in N\cap C(G)$، خواهیم داشت:

$$p=|N|=|N\cap C(G)|+\sum_{x_i\notin C(G)}[G:C(x_i)]$$

چون $p\geq[G:C(x_i)]$، جاییکه $x_i\notin C(G)$ و $|N\cap C(G)|\geq 1$، لذا $\sum_{x_i\notin C(G)}[G:C(x_i)]=0$، پس $(C(G))^c\cap N=\varnothing$، یعنی $N\leq C(G)$.

۱۹. یک مکعب را می‌توان 20160 طرق مختلف رنگ‌آمیزی کرد. فرض کنید X مجموعهٔ این 20160 مکعب رنگ‌آمیزی شده باشد. اگر G گروه حرکت مکعب باشد(توجه داشته باشید که $|G|=24$)، آنگاه $|X_e|=20160$ و برای هر $e\neq g\in G$، $|X_g|=0$، زیرا هرحرکت غیرهمانی هریک از 20160 مکعب رنگ‌آمیزی شده را به دیگری تبدیل می‌کند. بنابراین طبق قضیهٔ برنساید داریم:

www.mathematic87.blogfa.com

تعداد مدارها=تعدادمکعبهای رنگ‌آمیزی شده $= t = 20160/24 = 840.$

فصل۹

۱. عبارت $(a+1)(b+1)$ را به دو طریق حساب می‌کنیم:

$$(a+1)(b+1) = a(b+1)+1(b+1) = ab+a+b+1,$$
$$(a+1)(b+1) = (a+1)b+(a+1)1 = ab+b+a+1.$$

از مقایسهٔ دو عبارت فوق خواهیم داشت $a+b=b+a$.

۳. داریم $a^2b = aab = a(1-ab) = a-aba = (1-ab)a = baa = ba^2$ و لـذا $a^3b = aba^2$. از این‌رو $a^2 = ab+ba = 1$ در نتیجه $ab = aba = (1-ba)a^2 = a^2-ba^3 = a^2-ba$.

۵. فرض کنید D یک حوزهٔ صحیح و $\mathrm{Char}D = n \neq 0$. باید نشان دهیم n عددی اول است. (فرض خلف) فرض کنید $n = n_1n_2$، که $1 < n_1, n_2 < n$. چون D یک حوزهٔ صحیح است و $n1 = (n_1n_2)1 = (n_11)(n_21) = 0$، لذا $n_11 = 0$ یا $n_21 = 0$، که تناقض است.

۷. از جبر خطی مقدماتی می‌دانیم که اگر $X, Y \in \mathrm{M}_n(F)$ و $XY = I$، آنگاه $YX = I$. حال داریم

$$A+B = AB \Rightarrow (A-I)(B-I) = I \Rightarrow (B-I)(A-I) = I \Rightarrow A+B = BA.$$

بنابراین $AB = BA$.

۹. فرض کنید $A = \{x \in R \mid ax = 1\}$ و $x_0 \in A$. قرارمی‌دهیم:

$$B = \{xa-1+x_0 \mid x \in A\}.$$

چون $a(xa-1+x_0) = axa-a+ax_0 = a-a+ax_0 = 1$ ، لذا $A \subseteq B$. تابع $f : A \to B$ با ضابطهٔ $f(x) = xa-1+x_0$ به‌وضوح پوشاست. همچنین f یک به یک است، زیرا

$$f(x) = f(y) \Rightarrow xa-1+x_0 = ya-1+x_0 \Rightarrow xa = ya \Rightarrow (xa)x = (ya)x \Rightarrow x = y$$

www.mathematic87.blogfa.com

حال اگر A یک مجموعهٔ متناهی باشد (فرض خلف)، آنگاه $A=B$ ولذا $x_0 \in B$ و در نتیجه $x \in A$ چنان موجود است که $x_0 = xa - 1 + x_0$، یعنی $xa = 1$. از این‌رو a معکوس‌پذیر است، که تناقض است.

۱۱. (a): فرض کنید $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | a,b \in \mathbb{R} \right\}$. در این‌صورت $e = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ یک همانی چپ است که همانی راست نیست.

(b): اگر $e \in R$ یک همانی چپ یکتا باشد، آنگاه برای هر دو عنصر دلخواه $x, y \in R$ داریم $(e + xe - x)y = ey + xey - xy = y + xy - xy = y$. یعنی $e + xe - x$ یک همانی چپ است. در نتیجه $e + xe - x = e$ ولذا $xe = x$، یعنی e یک همانی راست نیز می‌باشد.

۱۳. (a): اگر I ایده‌آل دلخواهی از $\mathbb{Z}$ باشد، آنگاه چون I زیرگروهی از گروه آبلی $\mathbb{Z}$ است، لذا $n \in \mathbb{Z}$ چنان موجود است که $I = n\mathbb{Z}$. یعنی I یک ایده‌آل اصلی است.

(b): نشان می‌دهیم ایده‌آل $I = (x, x+1)$ اصلی نیست. برهان خلف، فرض کنید $f(x) \in \mathbb{Z}[x]$ چنان باشد که $(x, x+1) = (f(x))$. بنابراین عناصر $g(x), h(x) \in \mathbb{Z}[x]$ موجود می‌باشند بقسمی که $x = f(x)g(x)$ و $x + 1 = f(x)h(x)$. ازاین‌رو $f(x)(h(x) - g(x)) = 1$. در نتیجه $f(x) = \pm 1$، که به‌وضوح یک تناقض است.

۱۵. (a) $\Leftarrow$ (b): فرض کنید A و B دو ایده‌آل از R باشند. که $AB \subseteq P$. اگر $A \nsubseteq P$ آنگاه عنصر $a \in A$ چنان موجود است که $a \notin P$. فرض کنید $b \in B$ عنصر دلخواهی باشد. دراین‌صورت داریم $aRb = (aR)b \subseteq AB \subseteq P$. چون $a \notin P$ پس $b \in P$ و لذا $B \subseteq P$.

(b) $\Leftarrow$ (a): فرض کنید $aRb \subseteq P$، که $a, b \in R$. فرض کنید $A = RaR$ و $B = RbR$. در این صورت A و B ایده‌آل‌هایی از R می‌باشند. همچنین

$$AB = (RaR)(RbR) \subseteq R(aRb)R \subseteq RPR \subseteq P.$$

بنابراین $A \subseteq P$ یا $B \subseteq P$. فرض کنید $A \subseteq P$. داریم $(a)^3 \subseteq RaR = A \subseteq P$. از این‌رو $(a) \subseteq P$ و در نتیجه $a \in P$. به طور مشابه اگر $B \subseteq P$، آنگاه $b \in P$. بنابراین یا $a \in P$ یا $b \in P$.

www.mathematic87.blogfa.com

۱۷. مسئله را با استقرا ثابت می‌کنیم. حالت $n=1$ بدیهی است. فرض کنید $I \subseteq \cup_{i=1}^{n} P_i$. اکنون دو حالت در نظر می‌گیریم:

حالت(۱): فرض کنید $1 \le k \le n$ چنان باشد که $I \subseteq \cup_{i \neq k} P_i$. در این حالت طبق فرض استقرا مسئله حل است.

حالت(۲): فرض کنید برای هر $1 \le k \le n$، داشته باشیم $I \not\subseteq \cup_{i \neq k} P_i$. نشان می‌دهیم این حالت به تناقض منجر می‌شود. ابتدا ثابت می‌کنیم $I \cap (\cap_{j \neq k} P_j) \subseteq P_k$. برای این منظور فرض کنید $x \in I \cap (\cap_{j \neq k} P_j)$. چون $I \not\subseteq \cup_{i \neq k} P_i$، لذا $y \in I$ چنان موجود است که $y \notin \cup_{i \neq k} P_i$ (در حقیقت $y \in P_k$). از طرفی $x + y \in I \subseteq \cup_{i=1}^{n} P_i$، لذا دو حالت خواهیم داشت.

حالت(A): $x + y \in \cup_{i \neq k} P_i$. در این حالت چون $x \in I \cap (\cap_{j \neq k} P_j)$ ، لذا $y \in \cup_{i \neq k} P_i$، که تناقض است.

حالت(B): $x + y \in P_k$. در این حالت چون $y \in P_k$، لذا $x \in P_k$.

یعنی نشان داده‌ایم $I \cap (\cap_{j \neq k} P_j) \subseteq P_k$. که با توجه به اول بودن P_k خواهیم داشت $I \subseteq P_k$ (که تناقض است) یا $\cap_{j \neq k} P_j \subseteq P_k$ که از اینجا $j \neq k$ چنان موجود است که $P_j \subseteq P_k$(که باز هم تناقض است).

۱۹. فرض کنید K ایده‌آلی از $\mathrm{M}_n(R)$ باشد. قرار می‌دهیم $I = \{a_{11} \mid [a_{ij}] \in K\}$. به آسانی دیده می‌شود که I ایده‌آلی از R است کافی است نشان دهیم $K=\mathrm{M}_n(I)$. فرض کنید $M = [m_{ij}]$ یک ماتریس دلخواه باشد. در این‌صورت خواهیم داشت:

$$E_{ij} M E_{k\ell} = m_{jk} E_{i\ell}$$

که در اینجا $\{E_{ij}\}$ ماتریس‌های یکانی می‌باشند. (درایهٔ (i,j)ام E_{ij} برابر 1 و بقیهٔ درایه‌ها صفر است). حال فرض کنید $M \in K$. با قرار دادن $i = \ell = 1$ در رابطهٔ فوق خواهیم داشت $m_{jk} E_{11} \in K$ و بنابراین $m_{jk} \in I$ یعنی داریم $K \subseteq \mathrm{M}_n(I)$. برعکس، فرض کنید $[a_{ij}] \in \mathrm{M}_n(I)$. برای هر i, ℓ ماتریس $M = [m_{ij}] \in K$ چنان موجود است که $a_{i\ell} = m_{11}$.

www.mathematic87.blogfa.com

با استفادهٔ مجدد از رابطهٔ فوق داریم $a_{i\ell}E_{i\ell} = m_{11}E_{i\ell} = E_{i1}ME_{1\ell} \in K$ و ازاین‌رو $[a_{ij}] = \sum_{i,\ell} a_{i\ell}E_{i\ell} \in K$.

۲۱.(a): اگر $a^n = 0$، آنگاه $(1+a)(1-a+\cdots+(-1)^{n-1}a^{n-1}) = 1$. یعنی $(1+a)$ معکوس‌پذیر است. برای قسمت دوم داریم $(u+a) = u(1+u^{-1}a)$. چون $u^{-1}a$ پوچ‌توان است، لذا $a+u$ حاصل‌ضرب دو عنصرمعکوس‌پذیر است. بنابراین $a+u$ معکوس‌پذیر است.

(b): فرض کنید a_0 معکوس‌پذیر و $a_n,\ldots,a_2,a_1$ پوچ‌توان باشند. براحتی می‌توان نشان داد که $a_1x^1+a_2x^2+\cdots+a_nx^n$ عنصری پوچ‌توان از $R[x]$ است. بنابراین طبق قسمت(a) $a_0+a_1x^1+a_2x^2+\cdots+a_nx^n$ معکوس‌پذیر است. برعکس، فرض کنید $f(x) = a_0+a_1x^1+a_2x^2+\cdots+a_nx^n$ عنصری معکوس‌پذیر از $R[x]$ باشد. بنابراین $g(x) = b_0+b_1x^1+b_2x^2+\cdots+b_mx^m \in R[x]$ چنان موجود است که $f(x)g(x) = 1$. بنابراین $a_0b_0 = 1$، یعنی a_0 معکوس‌پذیر است. با استقرا روی t می‌توان نشان داد که $a_n^{t+1}b_{m-t} = 0$، و در نتیجه a_n پوچ‌توان است. با توجه به قسمت(a) عنصر $a_0+a_1x^1+a_2x^2+\cdots+a_{n-1}x^{n-1} = f(x)-a_nx^n$ معکوس‌پذیر است. با استدلال اخیر می‌توان دید که a_{n-1} نیز پوچ‌توان است و لذا استقرا روی n نشان می‌دهد که $a_n,\ldots,a_2,a_1$ پوچ‌توان می‌باشند.

۲۳.(a) : از(b) بدست می‌آید.

(b): فرض کنید P یک ایده‌آل اول باشد. نشان می‌دهیم P یک ایده‌آل ماکزیمال است. برای این منظور فرض کنید J ایده‌آلی از حلقهٔ R باشد که $P \subseteq J \subseteq R$. فرض کنید $J \neq P$ و $x \in J-P$. با توجه به فرض عدد طبیعی $n(x) > 1$ چنان موجود است که $x^{n(x)} = x$. بنابراین $x(x^{n(x)-1}-1) = x^{n(x)}-x = 0 \in P$ با توجه به اول بودن P و اینکه $x \notin P$، خواهیم داشت $x^{n(x)-1}-1 \in P$ و لذا $1 = x^{n(x)-1}-(x^{n(x)-1}-1) \in J$، یعنی $J = R$.

www.mathematic87.blogfa.com

۱. به‌وضوح $R^* \subseteq (R[x])^*$. حال فرض کنید $f(x) \in (R[x])^*$. در این‌صورت چند جمله‌ای $g(x) \in R[x]$ چنان موجود است که $f(x)g(x) = 1$. با توجه به اینکه $\deg f(x) + \deg g(x) = 0$، خواهیم داشت $f(x) = a \in R$ و $g(x) = b \in R$. بنابراین $f(x) \in R^*$. در نتیجه $(R[x])^* = R^*$.

۳. (a): نشان می‌دهیم $I = (x, y)$ یک ایده‌آل اصلی نیست. (برهان خلف) فرض کنید $f(x, y) \in R[x, y]$ به‌گونه‌ای باشد که $I = (f(x, y))$. چون $x, y \in I$، لذا عناصر $g(x, y), h(x, y) \in R[x, y]$ موجودند که $x = f(x, y)g(x, y)$ و $y = f(x, y)h(x, y)$. بنابراین $f(x, y) \in R[x]$ و $f(x, y) \in R[y]$. ازاین‌رو $f(x, y) = a \in R$ و درنتیجه $I = (a) \subseteq R$، که تناقض است.

(b): فرض کنید F یک میدان باشد. در این‌صورت $F[x, y]$ حوزهٔ تجزیهٔ یکتا بوده ولی حوزهٔ ایده‌آل اصلی نیست.

۵. فرض کنید R یک حلقهٔ جابجایی ویکدار باشد. قرار می‌دهیم $S = \mathbb{Z} \times R$. به‌آسانی می‌توان نشان داد که S با اعمال جمع و ضرب زیر یک حلقه است.

$$(m, a) + (n, b) = (m + n, a + b),$$
$$(m, a)(n, b) = (mn, mb + na).$$

در ضمن $(1, 0)$ عنصر همانی ضربی این حلقه است. به‌عبارت دیگر $1_S = (1, 0)$. همچنین تابع

$$\varphi : R \to S$$
$$a \mapsto (0, a).$$

یک تکریختی است. بنابراین R را می‌توان در حلقهٔ یکدار S نشاند.

۷. فرض کنید $R_1 = \mathbb{Z}$ و $R_2 = \mathbb{Q}$. در این‌صورت $R_1 \not\cong R_2$ ولی میدان کسرهای R_1 و R_2 برابر $\mathbb{Q}$ است.

۹. فرض کنید $2 = (a + bi\sqrt{3})(c + id\sqrt{3})$. در این‌صورت با مزدوج گیری خواهیم داشت $2 = (a - bi\sqrt{3})(c - id\sqrt{3})$. بنابراین $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. در رابطهٔ اخیر هر عامل سمت راست باید مقسوم علیهی از 4 باشد، اما چون $a^2 + 3b^2 \neq 2$، پس عاملهای سمت راست باید 1 و 4 باشند. اگر $a^2 + 3b^2 = 1$، آنگاه $a = \pm 1$ و $b = 0$، که نشان می‌دهد که یکی از

www.mathematic87.blogfa.com

عامل‌های 2 باید یکال باشد. بطور مشابه $c^2+3d^2=1$ نتیجه می‌دهد که یکی از عامل‌های 2 باید یکال باشد. بنابراین 2 عنصری تحویل‌ناپذیر است. از طرفی $2=(1+i\sqrt{3})(1-i\sqrt{3})$ و 2 هیچ یک از عامل‌های سمت راست را عاد نمی‌کند. بنابراین 2 اول نیست.

۱۱. اگر a یکال باشد، آنگاه به‌وضوح حکم برقرار است. حال فرض کنید a عنصری غیر یکال (و غیر صفر) از R باشد. در این‌صورت $a=a_1a_2\dots a_n$، که a_iها عناصری تحویل‌ناپذیر از R می‌باشند. فرض کنید (c) یک ایده‌آل اصلی سرهٔ شامل (a) باشد. در این‌صورت $c=c_1c_2\dots c_m$، که c_iها عناصری تحویل‌ناپذیر از R می‌باشند. چون $(a)\subseteq(c)$، پس بنابراین عنصر $d\in R$ چنان موجود است که $a=cd$. بنابراین

$$a_1a_2\dots a_n=c_1c_2\dots c_md.$$

با توجه به یکتایی تجزیه در R و بدون کاستن از کلیت می‌توان فرض کرد که $c_m,\dots,c_2,c_1$ به‌ترتیب با $a_m,\dots,a_2,a_1$ شریک‌اند. از این‌رو

$$(c)=(c_1c_2\dots c_m)=(c_1)(c_2)\dots(c_m)=(a_1)(a_2)\dots(a_m).$$

بنابراین تعداد متناهی ایده‌آل اصلی شامل (a) موجود است.

۱۳. فرض کنید $r_0=b$. روابط زیر را در نظر بگیرید.

$$a=bq_0+r_1 \quad (۱)$$
که در آن $r_1\neq 0$ و $\upsilon(r_1)<\upsilon(b)$،

$$b=r_1q_1+r_2 \quad (۲)$$
که در آن $r_2\neq 0$ و $\upsilon(r_2)<\upsilon(r_1)$،

$$r_1=r_2q_2+r_3 \quad (۳)$$
که در آن $r_3\neq 0$ و $\upsilon(r_3)<\upsilon(r_2)$،

$$\vdots$$

$$r_{n-2}=r_{n-1}q_{n-1}+r_n \quad (n)$$
که در آن $r_n\neq 0$ و $\upsilon(r_n)<\upsilon(r_{n-1})$،

$$r_{n-1}=r_nq_n \quad (n+1)$$
.

www.mathematic87.blogfa.com

نشان می‌دهیم $(a,b)=r_n$. از رابطهٔ $(n+1)$ام داریم $r_n \mid r_{n-1}$. از این‌جا با توجه به رابطهٔ (n)ام خواهیم داشت $r_n \mid r_{n-2}$. با ادامهٔ این روند و استفاده از روابط $(n-1)$،...، (۲) و (۱) خواهیم داشت $r_n \mid a$ و $r_n \mid b$.

حال فرض کنید $c \mid a$ و $c \mid b$. از رابطهٔ (۱)ام داریم $c \mid r_1$. از این‌جا با توجه به رابطهٔ(۲) ام خواهیم داشت $c \mid r_2$. با ادامهٔ این روند و استفاده از روابط (۳)، ...، (n)خواهیم داشت $c \mid r_n$. بدین ترتیب نشان داده‌ایم که $(a,b)=r_n$.

۱۵. فرض کنید $P=(p)$ و $Q=(q)$. چون $P \subseteq Q$، لذا عنصر $a \in R$ چنان موجود است که $p=aq$. ازاین‌رو $aq \in P$ ودر نتیجه $a \in P$ یا $q \in P$. اگر $a \in P$، آنگاه عنصر $b \in R$ به‌گونه‌ای موجود است $a=bp$. بنابراین $p=aq=bpq$ ودر نتیجه $bq=1$، که متناقض با اول بودن Qاست. ازاین‌رو باید داشته باشیم $q \in P$،که از این‌جا خواهیم داشت $(q) \subseteq P$ و لذا $P=Q$.

۱۷. فرض کنید $f(x)$دارای یک عامل درجهٔ اول باشد. در این‌صورت این ریشه عبارت است از ± 1، اما $f(1)=1$ و $f(-1)=3$. بنابراین نتیجه خواهیم گرفت که $f(x)$دارای یک عامل درجهٔ اول نیست. حال فرض کنید $f(x)$به حاصل‌ضرب دو عامل درجهٔ دوم در $\mathbb{Q}[x]$ تجزیه شده باشد. در این‌صورت $f(x)$ را می‌توان به حاصل‌ضرب دو عامل درجهٔ دوم در $\mathbb{Z}[x]$ نیز تجزیه کرد. یعنی

$$\begin{aligned} f(x) &= (x^2+ax+b)(x^2+cx+d) \\ &= x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd \end{aligned}$$

جائیکه $a,b,c,d \in \mathbb{Z}$. در نتیجه

$$\begin{aligned} a+c &= -2 \\ ac+b+d &= 0 \\ ad+bc &= 1 \\ bd &= 1 \end{aligned}$$

www.mathematic87.blogfa.com

چون $bd=1$، یا $b=d=1$ یا $b=d=-1$. در هر دو حالت $b=d$ و در نتیجه $ad+bc=b(a+c)=1$. چون $a+c=-2$، باید داشته باشیم $-2b=1$، که یک تناقض است. بنابراین $f(x)$ روی تحویل‌ناپذیر $\mathbb{Q}[x]$ است.

۱۹. برهان خلف، فرض کنید $f(x)=g(x)h(x)$. چون $g(i)h(i)=-1$، برای هر $1\le i\le n$، خواهیم داشت $g(x)+h(x)=0$ و در نتیجه $f(x)=g(x)h(x)=-[g(x)]^2$، که یک تناقض است، زیرا ضریب بزرگترین جمله‌ای $f(x)$ مثبت ولی ضریب بزرگترین جمله‌ای $-[g(x)]^2$ عددی منفی است.

فصل ۱۱

۱. مجموعهٔ $S=R-Z(R)$ بستهٔ ضربی است و $0\notin S$. بنابراین ایده‌آل اول P از R چنان موجود است که $\{0\}\subseteq P$ و $P\cap S=\varnothing$. ازاین‌رو $P\subseteq Z(R)$.

۳. می‌دانیم که اگر R حوزهٔ صحیح باشد، آنگاه $S^{-1}R$ نیز چنین است. بنابراین کافی است ثابت کنیم $S^{-1}R$ یک حلقهٔ ایده‌آل اصلی است. برای این منظور نگاشت $\varphi: R\to S^{-1}R$ با ضابطه $\varphi(r)=r/1$ را در نظر بگیرید. اگر J ایده‌آلی از $S^{-1}R$ باشد، آنگاه $J=S^{-1}\varphi^{-1}(J)$. اما $\varphi^{-1}(J)$ یک ایده‌آل R است از این‌رو $a\in R$ چنان موجود است که $\varphi^{-1}(J)=<a>$ و لذا

$$S^{-1}\varphi^{-1}(J)=S^{-1}(Ra)=\{ra/s\,|\,r\in R,s\in S\}$$
$$=\{(r/s)(a/1)\,|\,r\in R,s\in S\}=<a/1>.$$

۵. تذکر: فرض کنید F میدان کسرهای R باشد با یکسان گرفتن r و $r/1$ می‌توان R را بعنوان زیرحلقه‌ای از F و $R_{\mathfrak{m}}$ در نظر گرفت.

با توجه به تذکر فوق برای هر $\mathfrak{m}\in \mathrm{Max}(R)$ داریم $R\subseteq R_{\mathfrak{m}}$. حال فرض کنید $x\in \bigcap_{\mathfrak{m}\in \mathrm{Max}(R)} R_{\mathfrak{m}}$. قرار می‌دهیم $A=\{a\in R\,|\,ax\in R\}$. براحتی می‌توان نشان داد که A یک ایده‌آل از R است. چون $x\in R_{\mathfrak{m}}$، لذا $x=r/s$، که در اینجا $r\in R$

www.mathematic87.blogfa.com

و $s \in R - \mathfrak{m}$. داریم $sx \in R$، لذا $s \in A$. یعنی نشان داده‌ایم $A \not\subset \mathfrak{m}$. چون $\mathfrak{m}$ یک ایده‌آل ماکزیمال دلخواه بود، لذا باید داشته باشیم $A = R$. از این‌رو $1 \in A$ ودر نتیجه $x \in R$.

۷. (a)$\Rightarrow$(b): بدیهی.

(b)$\Rightarrow$(c): فرض کنید $aRa \subseteq A$.

دراین‌صورت $(a)(b) = (RaR)(RaR) = RaRaR \subseteq A$. از این‌رو $a \in A$.

(c)$\Rightarrow$ (d): فرض کنید $a \in A$. در این‌صورت $Ra \subseteq A$ و در نتیجه $aRa \subseteq A$ و لذا $a \in C$.

(c)$\Rightarrow$ (e): فرض کنید $a \in A$. در این‌صورت $aR \subseteq A$ و در نتیجه $aRa \subseteq A$ و لذا $a \in C$.

(d)$\Rightarrow$(a) و (e)$\Rightarrow$ (a): بدیهی.

۹.(a): فرض کنید $x \in \varphi(\sqrt{I})$. در این‌صورت $r \in R$ چنان موجود است که $r^n \in I$ و $x \in \varphi(r)$. داریم

$$x^n = \varphi(r^n) \in \varphi(I) \Rightarrow x^n \in <\varphi(I)> \Rightarrow x \in \sqrt{<\varphi(I)>}.$$

بنابراین $\varphi(\sqrt{I}) \subseteq \sqrt{<\varphi(I)>}$ و در نتیجه $<\varphi(\sqrt{I})> \subseteq \sqrt{<\varphi(I)>}$. تساوی برقرار است که φ پوشا بوده و $\mathrm{Ker}\varphi \subseteq I$.

(b): فرض کنید $x \in \sqrt{\varphi^{-1}(J)}$. در این‌صورت عدد صحیح مثبت n چنان موجود است که $x^n \in \varphi^{-1}(J)$. ازاین‌رو $\varphi(x)^n = \varphi(x^n) \in J$ و در نتیجه $\varphi(x) \in \sqrt{J}$، یعنی $x \in \varphi^{-1}(\sqrt{J})$. برعکس، فرض کنید $x \in \varphi^{-1}(\sqrt{J})$. در این‌صورت $\varphi(x) \in \sqrt{J}$ ودر نتیجه عدد صحیح مثبت n چنان موجود است که $\varphi(x^n) = \varphi(x)^n \in J$ ولذا $x^n \in \varphi^{-1}(J)$. یعنی $x \in \sqrt{\varphi^{-1}(J)}$.

۱۱.(a): کافی است نشان دهیم $R - R^* = J(R)$. بدیهی است که $J(R) \subseteq R - R^*$. حال فرض کنید $x \in R - R^*$ و فرض کنید n کوچکترین عدد طبیعی باشد که $x^n = 0$. در این‌صورت $Rx \subseteq R - R^*$، زیرا اگر $rx \in R^*$، آنگاه $(rx)x^{n-1} = 0$ ودر نتیجه $x^{n-1} = 0$، که تناقض است. از این‌رو rx پوچ‌توان بوده و لذا $1 - rx \in R^*$، یعنی $x \in J(R)$.

(b): فرض کنید $a, b \in R$ و $a + b = u \in R^*$. خواهیم داشت $u^{-1}a + u^{-1}b = 1$. برای راحتی کار قرار می‌دهیم $a_1 = u^{-1}a$ و $b_1 = u^{-1}b$. فرض کنید $c = a_1^{-1}b_1$. دو حالت زیر اتفاق می‌افتد:

www.mathematic87.blogfa.com

حالت(۱): $c \in R$. در این حالت $a_1^{-1} = a_1^{-1}(a_1 + b_1) = 1 + c \in R$ و در نتیجه $a^{-1} \in R$.

حالت(۲): $c \notin R$. در این حالت $c^{-1} = b_1^{-1}a_1 \in R$ و داریم $b_1^{-1} = b_1^{-1}(a_1 + b_1) = c + 1 \in R$ و در نتیجه $b^{-1} \in R$.

۱۳. اگر $x = (x_1, \ldots, x_n) \in J(\prod_{i=1}^{n} R_i)$، آنگاه برای هر $a = (a_1, \ldots, a_n) \in \prod_{i=1}^{n} R_i$، عنصر $1 - ax = (1 - a_1x_1, \ldots, 1 - a_nx_n)$ معکوس‌پذیر چپ است. بنابراین برای هر $1 \le i \le n$، $1 - a_ix_i$ معکوس‌پذیر چپ است و لذا $x_i \in J(R_i)$ و در نتیجه $x \in \prod_{i=1}^{n} J(R_i)$. برعکس، اگر $x = (x_1, \ldots, x_n) \in \prod_{i=1}^{n} J(R_i)$، آنگاه برای هر $1 \le i \le n$ و هر $a_i \in R_i$، عنصر $1 - a_ix_i$ معکوس‌پذیر چپ است و لذ اگر $a = (a_1, \ldots, a_n)$، آنگاه $1 - ax = (1 - a_1x_1, \ldots, 1 - a_nx_n)$ معکوس‌پذیر چپ است. از این‌رو $x = (x_1, \ldots, x_n) \in J(\prod_{i=1}^{n} R_i)$.

۱۵.(a): فرض کنید N یک زیرمدول سرهٔ M باشد. قرار می‌دهیم: $\Omega = \{K \le M \mid N \le K\}$. چون $N \in \Omega$، لذا $\Omega \neq \varnothing$. فرض کنید $K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$ یک زنجیر صعودی از Ω باشد. قرار می‌دهیم $K = \bigcup_{i=1}^{\infty} K_i$. به وضوح K یک زیر مدول M است. حال فرض کنید $K = M =< x_1, \ldots, x_n >$. فرض کنید $(1 \le i \le n)\, x_i \in K_{\ell_i}$. اگر $\ell = \max\{\ell_i\}_{i=1}^{n}$، آنگاه $K_\ell = M$، که تناقض است. یعنی $K \in \Omega$. به عبارت دیگر Ω در شرایط لم زرن صدق می‌کند. بنابراین Ω دارای عنصر ماکزیمال است یا به‌طور معادل N در یک زیرمدول ماکزیمال قرار دارد.

(b): چون ایده‌آل‌های چپ حلقه R و زیرمدول‌های ${}_RR$ یکی هستند، لذا حکم با توجه به قسمت(a) بدست می‌آید.

۱۷.(a): زنجیر صعودی زیر از زیرمدول‌های M را در نظر می‌گیریم:

$$\mathrm{Ker}\varphi \subseteq \mathrm{Ker}\varphi^2 \subseteq \mathrm{Ker}\varphi^3 \subseteq \cdots.$$

www.mathematic87.blogfa.com

با توجه به نوتری بودن M زنجیر فوق ایستاست. از این‌رو عدد طبیعی n چنان موجود است که $\operatorname{Ker}\varphi^n = \operatorname{Ker}\varphi^{n+1} = \cdots$. اکنون فرض کنید $\varphi(x) = 0$. چون φ و در نتیجه φ^n پوشاست، لذا $y \in M$ چنان موجود است که $\varphi^n(y) = x$. داریم:

$$\varphi(x) = 0 \Rightarrow \varphi(\varphi^n(y)) = \varphi^{n+1}(y) = 0 \Rightarrow y \in \operatorname{Ker}\varphi^{n+1} = \operatorname{Ker}\varphi^n \Rightarrow \varphi^n(y) = 0 \Rightarrow x = 0.$$

(b): زنجیر نزولی زیر از زیرمدول‌های M را در نظر می‌گیریم:

$$\operatorname{Im}\varphi \supseteq \operatorname{Im}\varphi^2 \supseteq \operatorname{Im}\varphi^3 \supseteq \cdots.$$

با توجه به آرتینی بودن M زنجیر فوق ایستاست. از این‌رو عدد طبیعی n چنان موجود است که

$$\operatorname{Im}\varphi^n = \operatorname{Im}\varphi^{n+1} = \cdots.$$

حال فرض کنید $x \in M$. در این‌صورت.

$$\varphi^n(x) \in \operatorname{Im}\varphi^n = \operatorname{Im}\varphi^{n+1} \Rightarrow \exists y \in M \ \text{ s.t } \varphi^n(x) = \varphi^{n+1}(y) \Rightarrow \varphi^n(\varphi(y) - x) = 0$$

چون φ و در نتیجه φ^n یک به یک است، لذا $x = \varphi(y)$.

۱۹. داریم $I^{n-1}I = I$. بنابراین $e \in I^{n-1}$ چنان موجود است که $(1-e)I = 0$. چون $e \in I^{n-1} \subseteq I$، لذا $e^2 = e$. حال فرض کنید $x \in I$. در این‌صورت $(1-e)x = 0$ و در نتیجه $x = ex$. یعنی $I \subseteq eI$. بنابراین $I \subseteq eI \subseteq eR \subseteq I$ و لذا $I = eR$.

۲۱. ($\Leftarrow$): تعریف می‌کنیم: $\varphi : {}_RR \to {}_RR$, $x \mapsto xa$. به‌وضوح φ یک همریختی است. از طرفی چون $\varphi(b) = ba = 1$ لذا φ پوشا و در نتیجه طبق تمرین ۱۷ یک به یک است. با توجه به $\varphi(ab) = aba = a = \varphi(1)$ و یک به یک بودن φ خواهیم داشت $ab = 1$. قسمت ($\Rightarrow$): بطور مشابه ثابت می‌شود.

فصل ۱۲

۱. (a): با توجه به اینکه تنها زیرگروه نرمال S_3، $H = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ می‌باشد لذا سریهای ترکیبی $S_3 \times \mathbb{Z}_3$ عبارتند از

www.mathematic87.blogfa.com

$\{\mathrm{id}\}\times<0>\trianglelefteq\{\mathrm{id}\}\times\mathbb{Z}_3\trianglelefteq H\times\mathbb{Z}_3\trianglelefteq S_3\times\mathbb{Z}_3$ و $\{\mathrm{id}\}\times<0>\trianglelefteq H\times<0>\trianglelefteq H\times\mathbb{Z}_3\trianglelefteq S_3\times\mathbb{Z}_3$.

(b): تنها زیرگروه نرمال A_4 عبارت است از $H=A_4'=\{\mathrm{id},(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$. این گروه دارای سه زیر گروه نرمال می‌باشد که عبارتند از: $H_1=\{\mathrm{id},(1\,2)(3\,4)\}$ و $H_2=\{\mathrm{id},(1\,3)(2\,4)\}$ و $H_3=\{\mathrm{id},(1\,4)(2\,3)\}$. از این‌رو A_4 دارای سه سری ترکیبی است که عبارتند از $\{e\}\trianglelefteq H_i\trianglelefteq H\trianglelefteq A_4$، $1\le i\le 3$.

(c): فرض کنید $\{\mathrm{id}\}=G_m\le G_{m-1}\le\cdots\le G_1\le G_0=S_4$ یک سری ترکیبی برای S_4 باشد. در این‌صورت S_4/G_1 یک گروه ساده بوده و $|S_4/G_1|\le 12$. ازاین‌رو S_4/G_1 باید آبلی باشد و در نتیجه $S_4'=A_4\le G_1$. چون تنها زیر گروه نرمال S_4 از مرتبهٔ بزرگتر از 12، A_4' می‌باشد لذا با توجه به قسمت(b) سریهای ترکیبی S_4 عبارتند از $\{e\}\trianglelefteq H_i\trianglelefteq H\trianglelefteq A_4\trianglelefteq S_4$، $1\le i\le 3$.

۳. قضیهٔ اساسی حساب: هر عدد طبیعی $n>1$ را می‌توان بطور یکتایی به شکل $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\ell^{\alpha_\ell}$ نوشت، که $p_1<p_2<\dots<p_\ell$ و $\alpha_i\ge 1$.

وجود: فرض کنید $\mathbb{Z}_n=G_0\ge G_1\ge\cdots\ge G_m=<0>$ یک سری ترکیبی با عاملهای از مرتبهٔ عددی اول باشند. فرض کنید $|G_i/G_{i+1}|=q_i$، $0\le i\le m-1$. داریم:

$$n=|\mathbb{Z}_n|=|G_0|=|G_m||G_{m-1}/G_m||G_{m-2}/G_{m-1}|\cdots|G_0/G_1|=\prod_{i=0}^{m-1}q_i,$$

که در اینجا اعداد اول q_i ها الزاماً متمایز نیستند. لذا می‌توان فرض کرد $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\ell^{\alpha_\ell}$ که $p_i\in\{q_0,q_1,\dots,q_{m-1}\}$، $p_1<p_2<\dots<p_\ell$ و $\alpha_i\ge 1$.

یکتایی: فرض کنید $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\ell^{\alpha_\ell}=q_1^{\beta_1}p_2^{\beta_2}\dots q_t^{\beta_t}$. چون $\mathbb{Z}_n$ آبلی است، لذا از مرتبهٔ هر مقسوم‌علیه n زیرگروه داریم. ازاین‌رو دو سری ترکیبی زیر را برای $\mathbb{Z}_n$ خواهیم داشت.

$$\{0\}=H_0\le H_1\le H_2\le\cdots\le H_{\alpha_1+\cdots+\alpha_\ell}=\mathbb{Z}_n,$$
$$\{0\}=K_0\le K_1\le K_2\le\cdots\le K_{\beta_1+\cdots+\beta_t}=\mathbb{Z}_n,$$

www.mathematic87.blogfa.com

که $|H_1|=p_1$، $|H_2|=p_1^2$، ...، $|H_{\alpha_1}|=p_1^{\alpha_1}$، ...، $|H_{\alpha_1+\cdots+\alpha_\ell}|=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\ell^{\alpha_\ell}$ و $|K_1|=q_1$، $|K_2|=q_1^2$، ...، $|K_{\beta_1}|=p_1^{\beta_1}$، ...، $|K_{\beta_1+\cdots+\beta_t}|=q_1^{\beta_1}p_2^{\beta_2}\dots q_t^{\beta_t}$. با توجه به قضیهٔ ژردان- هولدر دو سری فوق هم‌ارز است، که از اینجا یکتایی تجزیه ثابت می‌شود.

۵. در حقیقت هر گروه آبلی نامتناهی دارای سری ترکیبی نیست (تمرین۶). نشان می‌دهیم $\mathbb{Z}(p^\infty)$ دارای سری ترکیبی نیست. (فرض خلف) فرض کنید

$$<0>=G_m\le G_{m-1}\le\cdots\le G_1\le G_0=\mathbb{Z}(p^\infty)$$

یک سری ترکیبی برای $\mathbb{Z}(p^\infty)$ باشد. چون هر زیرگروه $\mathbb{Z}(p^\infty)$ دوری و متناهی است لذا می‌توان فرض کنید $G_1=<1/p^n+\mathbb{Z}>$. اما G/G_1 نمی‌تواند ساده باشد (زیرا که $G_1=<1/p^n+\mathbb{Z}>\subsetneq<1/p^{n+1}+\mathbb{Z}>\subsetneq G$)، که تناقض است.

۷.(a): فرض کنید N یک زیرگروه نرمال مینیمال G باشد. با توجه به اینکه $N'\trianglelefteq N\trianglelefteq G$ و N' یک زیرگروه مشخصهٔ N است، خواهیم داشت $N'\trianglelefteq G$. با توجه به مینیمال بودن N و اینکه $\{e\}\le N'\le N$، دو حالت ممکن است. $N'=\{e\}$ یا $N'=N$. حالت $N'=N$ ممکن نیست، زیرا در این صورت N حل‌پذیر نمی‌باشد که با حل‌پذیر بودن G در تناقض است. بنابراین $N'=\{e\}$، یعنی N آبلی است. فرض کنید $p\,||N|$ (که p عددی اول است) و P یک زیر گروه p-سیلو از N باشد. با توجه به اینکه N یک گروه آبلی است، لذا P یک زیرگروه مشخصهٔ از N است و در نتیجه $P\trianglelefteq G$ و با توجه به مینیمال بودن N باید داشته باشیم $P=N$، یعنی N یک p-گروه آبلی است.

(b): فرض کنید G پوچ‌توان بوده و $\{e\}=G_m\le G_{m-1}\le\cdots\le G_1\le G_0=G$ یک سری مرکزی برای G باشد. قرار می‌دهیم $A=\{\ell\,|\,\ell\ge 0, N\cap G_\ell\neq\{e\}\}$. واضح است که $0\in A$. فرض کنید n عنصر ماکزیمال A باشد. داریم $N\cap G_{n+1}=\{e\}$ اینک ملاحظه می‌کنیم که $[G,N\cap G_n]\le[G,G_n]\le G_{n+1}$. از طرفی چون $N\cap G_n$ در G نرمال است، $[G,N\cap G_n]\le N\cap G_n\le N$. بنابراین $[G,N\cap G_n]\le N\cap G_{n+1}=\{e\}$. از اینجا معلوم می‌شود که $N\cap G_n\le C(G)\cap N$. حال چون $N\cap G_n\neq\{e\}$، حکم ثابت می‌شود.

www.mathematic87.blogfa.com

(c): فرض کنید N یک زیرگروه مینیمال از G باشد. با توجه به قسمت(a) و اینکه هر گروه پوچ‌توان، حل‌پذیر است، N یک p-گروه آبلی خواهد بود. با توجه به قسمت(b)، $\{e\} \neq N \cap C(G) \trianglelefteq G$. ازاین‌رو با توجه به مینیمال بودن N باید $N = N \cap C(G)$ و در نتیجه $N \subseteq C(G)$. حال فرض کنید $H \leq N$ یک زیرگروه از مرتبهٔ p باشد. چون $H \subseteq N \subseteq C(G)$، لذا $H \trianglelefteq G$ و با توجه به مینیمال بودن N باید $H = N$ و لذا N یک گروه از مرتبهٔ p است.

۹. کافی است نشان دهیم G زیرگروه نرمالی از اندیس یک عدد اول دارد. این مطلب را با استقرا روی $|G|$ ثابت می‌کنیم. اگر $|G| = 6$، آنگاه $G \cong \mathbb{Z}_6$ یا $G \cong S_3$ که به‌وضوح حکم برقرار است. حال فرض کنید $|G| > 6$. چون G ساده نیست لذا زیر گروه نرمالی غیر بدیهی چون N دارد. اگر G/N آبلی باشد، آنگاه به‌وضوح هر زیرگروه ماکزیمال آن مانند M/N زیرگروهی نرمال از اندیس یک عدد اول است. در نتیجه $M \trianglelefteq G$ و $[G : M]$ اول است و حکم ثابت می‌شود. حال اگر G/N آبلی نباشد، آنگاه توجه به تمرین ۲۲ فصل ۶، G/N ساده نیست. بنابراین طبق فرض استقرا G/N زیرگروه نرمالی مانند H/N از اندیس یک عدد اول دارد. بنابراین $H \trianglelefteq G$ و $[G : H]$ اول است وحکم ثابت است.

۱۱.(a): فرض کنید S_3 (S_4) پوچ‌توان باشد و $\{\mathrm{id}\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G$، که $G_{m-1} \neq \{\mathrm{id}\}$ یک سری مرکزی برای $G = S_3$ ($G = S_4$) باشد. طبق تعریف داریم $G_{m-1}/\{\mathrm{id}\} \subseteq C(G/\{\mathrm{id}\})$ و لذا $G_{m-1} \subseteq C(G) = \{\mathrm{id}\}$، که تناقض است. حال نشان می‌دهیم S_3 و S_4 حل‌پذیرند. چون $S_3' = A_3$ و $A_3' = \{\mathrm{id}\}$، لذا $S_3'' = \{\mathrm{id}\}$، یعنی S_3 حل‌پذیر است. چون $S_4' = A_4$ و $A_4' = H = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ و $H' = \{\mathrm{id}\}$، لذا $S_4''' = \{\mathrm{id}\}$، یعنی S_4 حل‌پذیر است.

(b): فرض کنید $\{E_{ij}\}$ ماتریس‌های یکانی باشند. در این‌صورت برای هر $i \neq j \neq k$ داریم

$$(I + E_{ik})(I + E_{kj})(I + E_{ik})^{-1}(I + E_{kj})^{-1} =$$
$$(I + E_{ik})(I + E_{kj})(I - E_{ik})(I - E_{kj}) = (I + E_{ij}).$$

www.mathematic87.blogfa.com

حال فرض کنید $H =< (I + E_{ij}) \mid i \neq j >$. در این‌صورت با توجه به رابطهٔ بالا $H' = H$. بنابراین $\mathrm{GL}_n(\mathbb{R})$ نمی‌تواند حل‌پذیر باشد.

۱۳. چون G پوچ‌توان است لذا حاصل ضرب زیرگروه‌های سیلویش می‌باشد. فرض کنید $G = P_1 \times \cdots \times P_n$. چون $p \mid \mid G \mid$، لذا $1 \leq i \leq n$ موجود است که $p \mid \mid P_i \mid$. چون P_i یک p-سیلو زیرگروه است، $C(P_i) \neq \{e\}$ و لذا $p \mid \mid C(P_i) \mid$. پس $p \mid \mid C(P_1) \times \cdots \times C(P_i) \times \cdots \times C(P_n) \mid = \mid C(G) \mid$.

۱۵.(a): فرض کنید $G = S_3$ و $N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. در این‌صورت G/N و N بدلیل آبلی بودن پوچ‌توان هستند، در صورتیکه G پوچ‌توان نمی‌باشد.

(b): فرض کنید

$$H/H = G_m/H \leq G_{m-1}/H \leq \cdots \leq G_1/H \leq G_0/H = G/H$$

یک سری مرکزی برای G/H باشد. در این‌صورت با توجه به قضیهٔ سوم یکریختی خواهیم داشت $G_i/G_{i+1} \subseteq C(G/G_{i+1})$، $0 \leq i \leq m-1$. حال سری

$$< e > \leq H = G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G_0 = G$$

با توجه به اینکه $H \subseteq C(G)$، یک سری مرکزی برای G بوده و لذا G پوچ‌توان است.

۱۷. فرض کنید $G =< x, y \mid x^2 = 1,\ xy = yx >$. تابع $\varphi : G \to \mathbb{Z}_2 \times \mathbb{Z}$ با ضابطهٔ $x \to (1,0)$ و $y \to (0,1)$، که بوسیلهٔ همریختی روی تمام G توسعه می‌یابد، یک برووریختی است. حال نشان می‌دهیم φ یک به یک است. فرض کنید $\varphi(x^n y^m) = (0,0)$، که در اینجا $0 \leq n \leq 1$ و $m \in \mathbb{Z}$. داریم $\varphi(x^n y^m) = (n,m) = (0,0)$ و در نتیجه $x^n y^m = x^0 y^0 = 1$، یعنی φ یک به یک است. بنابراین φ یک یکریختی بوده و در نتیجه $G \cong \mathbb{Z}_2 \times \mathbb{Z}$.

۱۹. داریم $Q_8 =< x, y \mid x^2 = y^2, y^{-1}xy = x^{-1} >$. تابع $\varphi : Q_8 \to Q$ با ضابطهٔ $x \to I$ و $y \to J$، که بوسیلهٔ همریختی روی تمام Q_8 توسعه می‌یابد، یک برووریختی است. از اینکه مرتبهٔ هر دوی Q_8 و Q برابر 8 است، لذا φ یک یکریختی بوده و در نتیجه $Q_8 \cong Q$.

www.mathematic87.blogfa.com

فهرست نمادها

نماد	مفهوم	اولین صفحهٔ مراجعه
$\mathbb{Z}$	مجموعه اعداد صحیح	۱
$\mathbb{Z}_n$	مجموعه $\{0,1,\ldots,n-1\}$ با همنهشتی به پیمانه n	۲
S_X	مجموعهٔ جایگشت‌های مجموعهٔ X	۴
S_n	مجموعهٔ جایگشت‌های یک مجموعهٔ n عنصری	۴
$\begin{pmatrix} x_1 & \cdots & x_n \\ \delta(x_1) & \cdots & \delta(x_n) \end{pmatrix}$	جایگشت δ از مجموعه $\{x_1,\ldots,x_n\}$	۵
K_4	مجموعهٔ حرکتهای مستطیل (چهارتایی کلاین)	۵
$\mathbb{R}$	مجموعهٔ اعداد حقیقی	۹
$A\Delta B$	تفاضل متقارن مجموعه‌های A و B	۹
$P(X)$	مجموعهٔ زیر مجموعه‌های X	۹
e	عنصر همانی یک تکوار	۱۰
$\lvert G\rvert$	عدد اصلی گروه G	۱۱
$\mathbb{C},\mathbb{Q},\mathbb{N}$	مجموعهٔ اعداد طبیعی، گویا و مختلط	۱۱
$\mathrm{Map}(X,X)$	مجموعهٔ همهٔ توابع از X به X	۱۲
$\mathbb{C}^*,\mathbb{R}^*,\mathbb{Q}^*,\mathbb{Z}^*$	مجموعهٔ اعداد صحیح، گویا، حقیقی و مختلط ناصفر	۱۲
S_n	گروه متقارن درجه n	۱۳

www.mathematic87.blogfa.com

$U(n)$	گروه یکال‌های $\mathbb{Z}_n$	۱۳
$\mathrm{M}_n(R)$	مجموعهٔ ماتریسهای $n\times n$ با درایه‌های از R	۱۴
$\mathrm{GL}_n(R)$	گروه خطی عمومی از درجه n روی R	۱۴
$\mathrm{SL}_n(R)$	گروه خطی ویژه از درجه n روی R	۱۴
Q	گروه کواترنیون از مرتبهٔ ۸	۱۵
x^{-1}	معکوس عنصر x در یک گروه	۱۶
$< e >$	زیرگروه $\{e\}$ از گروه G	۲۰
$H \leq G$	H یک زیرگروه از گروه G است	۲۰
$H < G$	H یک زیرگروه سره از گروه G است	۲۰
D_4	گروه تقارن های مربع	۲۴
HK	$\{hk \mid h \in H, k \in K\}$	۲۶، ۶۷
$C(G)$	مرکز G	۲۶
$C_G(H)$	مرکز ساز زیرگروه H در گروه G	۲۶
$N_G(H)$	نرمال ساز زیرگروه H در گروه G	۲۶
$< a >$	گروه دوری تولید شده توسط a	۳۱
$\circ(a)$	مرتبهٔ عنصر a از یک گروه	۳۱
$\mathbb{T}$	گروه دایره	۳۶
U_n	گروه ریشه‌های nام واحد	۳۷
$< X >$	زیرگروه (مدول) تولید شده توسط X	۳۸،۲۶۹
$(a_1\ a_2\ \ldots\ a_k)$	دور بطول k	۴۶
A_n	گروه متناوب از درجه n	۵۳
D_n	گروه دو وجهی از مرتبه $2n$	۵۶
Hg, gH	هم‌دسته‌های چپ و راست	۶۲
$\mathscr{R}_H$ ، $\mathscr{L}_H$	مجموعه تمام هم‌دسته‌های چپ و راست H در G	۶۳

www.mathematic87.blogfa.com

$[G:H]$	اندیس H درگروه G	۶۴
ϕ	تابع فی اویلر	۷۱
$H \trianglelefteq G$	H یک زیرگروه نرمال از گروه G است	۷۳،۱۰۲
$N_K(H)$	نرمال ساز H در K	۷۴
$\cong$	یکریخت است با	۷۸ ،۱۹۱،۲۷۱
$\ncong$	یکریخت نیست با	۷۸
$\mathrm{Aut}(G)$	گروه خودریختی‌های گروه G	۸۶
$\mathrm{Inn}(G)$	گروه خودریختی‌های داخلی گروه G	۸۸
$\mathrm{Out}(G)$	مجموعهٔ همهٔخودریختی‌های خارجی گروه G	۸۸
$\prod_{i=1}^{n} G_i$	حاصل ضرب مستقیم خارجی گروه‌های G_i	۸۸
G/N	گروه خارج قسمت G بر N	۱۰۶
$[a,b]$	جابجاگر عناصر aو b از یک گروه	۱۰۸
G'	زیرگروه مشتق گروه G	۱۰۸
$G^{(n)}$	زیرگروه مشتق nام گروه G	۱۰۸
$\mathrm{Im}\varphi$	تصویر همریختی φ	۱۱۵، ۲۰۵ ،۲۷۱
$\mathrm{Ker}\varphi$	هسته همریختی φ	۱۱۵، ۲۰۵ ،۲۷۱
$\mathrm{Core}_G(H)$	زیرگروه مغز Hدر گروه G	۱۲۰
$\mathrm{Hom}(G,H)$	مجموعه تمام همریختی‌های گروهی $G \to H$	۱۲۸
$C(g)$	مرکز ساز عنصر g در گروه G	۱۲۹
$\mathscr{P}(n)$	مجموعه همه افرازهای n	۱۳۶
$\mathrm{rank}\,G$	رتبه G	۱۴۱
$G[m]$	$\{g \in G \mid mg = 0\}$	۱۴۴
$G(p)$	$\{g \in G \mid \circ(g) = p^n, n \geq 0$ به ازای یک $\}$	۱۴۴
$T(G)$	زیرگروه تابی G	۱۴۵

www.mathematic87.blogfa.com

$\mu(G)$	تعداد عناصرمجموعه مولد مینیمال گروه G	۱۵۰
X_g	مجموعه نقاط ثابت g	۱۵۶
G_x	گروه ثابت ساز g	۱۵۶
$\overline{x}$	مدار x	۱۵۶
n_p	تعداد $p-$زیرگروه سیلوهای G	۱۶۵
1_R	یک حلقه R	۱۸۰
$R[x]$	حلقه چند جمله‌ای ها	۱۸۱
$\mathrm{M}_n(R)$	مجموعهٔ ماتریسهای $n\times n$ روی حلقهٔ R	۱۸۱
$\mathbb{H}(\mathbb{R})$	حلقه چهارگانی حقیقی	۱۸۳
$\mathrm{Char}R$	مشخصهٔ حلقه R	۱۸۵
$U(R)$ یا R^*	گروه یکال‌های R	۱۸۷
$Z(R)$	مجموعه عناصر مقسوم‌علیه صفر حلقه R	۱۹۰
$Z_r(R)$	مجموعه عناصر مقسوم‌علیه صفر راست حلقه R	۱۹۰
$Z_\ell(R)$	مجموعه عناصر مقسوم‌علیه صفر چپ حلقه R	۱۹۰
$\langle X\rangle$	زیر حلقهٔ تولید شده توسط زیر مجموعه X از یک حلقه	۱۹۴
(X)	ایده‌ال تولید شده توسط زیر مجموعه X از یک حلقه	۱۹۵
PIR	حلقهٔ ایده‌ال اصلی	۱۹۵
PID	حوزهٔ ایده‌ال اصلی	۱۹۵
$\mathrm{Spect}(R)$	مجموعهٔ ایده‌ال‌های اول حلقهٔ R	۱۹۹
$\mathrm{Max}(R)$	مجموعهٔ ایده‌ال‌های ماکزیمال حلقهٔ R	۲۰۰
$a\overset{I}{\equiv}b$	$a-b\in I$	۲۱۰
$\deg f$	درجهٔ چند جمله‌ای f	۲۲۳
ER	حلقهٔ اقلیدسی	۲۲۸
ED	حوزهٔ اقلیدسی	۲۲۸

www.mathematic87.blogfa.com

$R(x)$	میدان توابع گویا از متغیر x	۲۳۲
$R(x_1,\ldots,x_n)$	میدان توابع گویا از متغیرهای $x_1,\ldots,x_n$	۲۳۲
UFD	حوزهٔ تجزیهٔ یکتا	۲۳۴
ACC	شرط زنجیر صعودی	۲۳۴، ۲۷۲
$(a_1,\ldots,a_n)$	بزرگترین مقسوم علیه مشترک عناصر $a_n,\ldots,a_1$	۲۳۷
$C(f)$	محتوای چند جمله‌ای f	۲۳۹
$S^{-1}R$	حلقهٔ کسرهای R بر S	۲۵۷
R_P	موضعی سازی R در P	۲۶۰
$\sqrt{I}$	رادیکال اول I	۲۶۱
$J(R)$	رادیکال جیکوبسن R	۲۶۵
$(M_R)_R M$	R - مدول چپ (راست)	۲۶۶
DCC	شرط زنجیر نزولی	۲۷۲
$\mathrm{Ann}(X)$	پوچ‌ساز زیر مجموعهٔ X از مدول M	۲۷۵
$\mathbb{Z}(p^\infty)$	$\{\frac{a}{p^n}+\mathbb{Z} \mid a\in\mathbb{Z}\ ,\ n=0,1,2,\ldots\}$	۲۷۷
$\mathrm{Hom}_R(M,N)$	مجموعه تمام همریختی‌های R-مدولی $M\to N$	۲۸۷
$\mathrm{End}_R(M)$	$\mathrm{Hom}_R(M,M)$	۲۸۷
$\ell(G)$	طول سری ترکیبی گروه G	۲۹۷
$[H,K]$	زیر گروه جابجاگر H و K	۳۰۲
$F(X)$	گروه آزاد تولید شده توسط X	۳۰۸
$< x_i \mid r_i >$	نمایش گروه با مجموعه مولد $\{x_i\}$ و مجموعهٔ روابط $\{r_i\}$	۳۰۸
Q_{4n}	کواترنیون‌های تعمیم یافته از مرتبهٔ $4n$	۳۱۰
T	$< a,b \mid a^6=1, b^2=a^3, bab^{-1}=a^{-1} >$	۳۱۳
$\Phi(G)$	زیرگروه فراتینی گروه G	۳۱۷

www.mathematic87.blogfa.com

واژه‌نامه فارسی به انگلیسی و فهرست راهنما

آ–ا

آبلی، ۱۰	Abelian
آرتینی، ۲۷۵، ۲۷۷	Artinian
-چپ، ۲۷۷	left-
-راست، ۲۷۷	right-
اپی‌مورفیسم، ۱۱۳	epimorphism
اتومورفیسم، ۸۶	automorphism
افراز، ۱۳۶	partition
اندومورفیسم، ۱۱۳	endomorphism
اندیس، ۶۴	index
ایده‌ال، ۱۹۳	ideal
-اصلی، ۱۹۵	principle-
-اول، ۱۹۹	prime-
-تولید شده توسط مجموعه X، ۱۹۵	-generated by the set X
-چپ، ۱۹۳	left-
-راست، ۱۹۳	right-
-سره، ۱۹۳	proper-

www.mathematic87.blogfa.com

maximal-	-ماکزیمال، ۲۰۰
semiprime-	-نیم اول، ۲۶۲
isomorphism	ایزومورفیسم، ۷۸، ۲۰۳، ۲۷۱

ب-پ-ت

commutator	برگردان، ۱۰۸
epimorphism	بروریختی، ۱۱۳، ۲۰۳، ۲۷۱
closed set	بسته ضربی، ۲۵۴
generalized-	-تعمیم یافته، ۲۵۴
invariant	پایاها، ۱۳۵
base	پایه، ۱۳۹
nilpotent	پوچ‌توان، ۱۸۹
annihilator	پوچ‌ساز، ۲۷۶
p -group	p -گروه، ۱۳۸
p -subgroup	p - زیر گروه، ۱۶۱
Sylow p -subgroup	p -زیر گروه سیلو، ۱۶۳
π -regular	π -منظم، ۲۵۶
transposition	ترانهش، ۵۱
image	تصویر، ۱۱۵، ۲۰۵، ۲۷۰
homomorphism-	-همریخت، ۱۲۰
symmetric difference	تفاضل متقارن، ۹
symmetric	تقارن، ۵۳
monomorphism	تکریختی، ۱۱۳، ۲۰۳، ۲۷۱
monoid	تکوار، ۱۰
distributive	توزیع‌پذیری، ۱۸۰

www.mathematic87.blogfa.com

ج-چ

جابجا گر (برگردان)،۱۰۸ commutator
جابجایی،۱۰،۱۸۰ commutative
جایگشت،۴ permutation
-زوج،۵۳ even-
-فرد،۵۳ odd-
-مجزا،۴۸ disjoint-
جدول کیلی،۱۳ Cayley table
چند جمله‌ای،۱۸۱ polynomial
-اولیه،۲۳۹ primitive-
-تکین،۲۲۳ monic-

ح-خ

حاصل‌ضرب،۹ multiplication
حاصل‌ضرب- -product
مستقیم خارجی،۸۹ external direct
مستقیم داخلی،۹۱ internal direct
حرکت،۵ motion
حلقه،۱۸۰ ring
-اقلیدسی،۲۲۸ Euclidean-
-ایده‌ال اصلی،۱۹۵ principal ideal (PIR)-
-بخشی (تقسیم)،۱۸۸ division-
-بولی،۲۱۴ Boolean-
-جابجایی،۱۸۰ commutative-
-چند جمله‌ای،۱۸۱ polynomial-

www.mathematic87.blogfa.com

-چهارگانی حقیقی،۱۸۳ real quaternion-

-ساده،۲۰۲ simple-

-صفر،۱۸۲ zero-

-کسرها،۲۵۸ -of quotients

-ماتریسی،۱۸۱ matrix-

-ماتریس‌های بالا مثلثی، ۱۸۷ upper triangular matrix-

-موضعی،۲۶۰،۲۸۶ local-

-یکدار،۱۸۰ -with identity

حوزه،۱۹۱ domain

-اقلیدسی،۲۲۸ Euclidean-

-تجزیهٔ یکتا،۲۳۴ unique factorization-

-صحیح،۱۹۱ integral-

حوزهٔ ایده‌ال اصلی،۱۹۵ principal ideal domain (PID)

خواص ساختاری،۸۲ structure property

خودتوان،۱۸۹ idempotent

خودریختی،۸۶ automorphism

-داخلی (خارجی)،۸۷(۸۸) inner-

د-ر-ز

درجه،۲۲۳ degree

درون‌ریختی،۱۱۳ endomorphism

دور،۴۶ cycle

رادیکال- -radical

اول،۲۶۱ prime

جیکوبسن،۲۶۵ Jacobson

www.mathematic87.blogfa.com

rank	رتبه،۱۴۱
nth root of unity	ریشهٔ n ام واحد،۳۷
primitive nth root of unity	ریشهٔ nام واحد اولیه،۳۷
subring	زیر حلقه،۱۸۶
-generated by X	-تولید شده توسط X ،۱۹۴
subgroup	زیرگروه،۲۰
trivial-	-بدیهی،۲۰
torsion-	-تابی،۴۱،۱۴۵
-generated by X	-تولید شده توسط X ،۳۸
commutator	-جابجاگر،۳۰۲
cyclic-	-دوری،۳۱
proper-	-سره(حقیقی)،۲۰
Ferattini-	-فراتینی،۳۱۷
maximal-	-ماکزیمال،۴۲
derived-	-مشتق،۱۰۸
nth derived	-مشتق nام،۱۰۸
characteristic-	-مشخصه،۱۳۰
core-	-مغز(کر)،۱۲۰
normal-	-نرمال،۷۳،۱۰۲
maximal normal -	-نرمال ماکزیمال،۱۱۱
submodule	زیرمدول،۲۶۸
-generated by X	-تولید شده توسط X ،۲۶۹
prime subfield	زیر میدان ،۲۱۷
prime-	-اول،۲۱۷

www.mathematic87.blogfa.com

س–ش

سری،۲۹۲	series
-ترکیبی،۲۹۳	composition-
-حل‌پذیر،۲۹۳	solvable-
-زیرنرمال،۲۹۲	subnormal-
-نرمال،۲۹۲	normal-
شرط زنجیر صعودی۲۷۲،۲۳۴	ascending chain condition (ACC)
شرط زنجیر نزولی ،۲۷۲	descending chain condition (DCC)
شرکت‌پذیر،۱۰ ،۱۸۰	associative
شریک (وابسته)، ۲۳۳	associate
شکل هندسی،۵	geometric figure

ض

ضریب پیشرو،۲۲۳	leading coefficient
ضرایب تاب،۱۳۴	torsion coefficients
ضرایب چند جمله‌ای،۱۸۱	polynomial coefficients

ع

عدد بتی،۱۳۴	Betti number
عمل،۱۵۴	action
عمل دوتایی،۹	binary operation
عنصر-	-element
اول،۲۳۳	prime
تحویل‌ناپذیر،۲۳۳	irreducible

ف–ق

www.mathematic87.blogfa.com

فارغ از تاب،۱۴۵	torsion free
فون نیومن منظم،۲۱۸	von Neumann regular
قابل نشاندن،۲۰۳	embeddable
قضیهٔ اساسی گروههای آبلی متناهی مولد،۱۳۴	fundamental theorem of finitely generated abelian groups
قضیهٔ اساسی جبر،۲۲۷	fundamental theorem of algebra
قضیهٔ-	-Theorem
اول یکریختی،۱۱۷،۲۰۶،۲۷۱	First Isomorphism
اول سیلو،۱۶۲	First Sylow
اویلر،۷۱	Euler's
باقیمانده چینی،۲۱۱	Chinese Reminder
برنساید،۱۷۰	Burnside's
تناظر،۱۲۲،۲۰۷،۲۷۲	Correspondence
دوم یکریختی،۱۲۱،۲۰۷،۲۷۱	Second Isomorphism
دوم سیلو،۱۶۴	Second Sylow
ژردان-هولدر،۲۹۶	Jordan-Holder
سوم یکریختی،۱۲۲،۲۰۷،۲۷۱	Third Isomorphism
سوم سیلو،۱۶۵	Third Sylow
فایت-تامسون،۳۰۱	Feit-Thompson
کشی،۱۵۹	Cauchy's
کوچک فرما،۷۱	Fermat little
کیلی،۸۴	Cayley's
لاگرانژ ،۶۶	Lagrange's
مرتبه فرد،۱۶۹	Odd order

www.mathematic87.blogfa.com

ویلسون،۷۴، ۱۶۶ Wilson’s
هال،۳۰۱ Hall ‘s

ک–گ

کلمه، ۳۰۷ word
-تهی ،۳۰۷ empty-
-کاهش یافته،۳۰۷ reduced-
کواترنیون،۱۵ quaternion
-تعمیم یافته،۳۱۰ generalized-
گروه،۱۰ group
-آبلی آزاد متناهی مولد،۱۴۰ free abelian-
-آزاد،۳۰۸ free-
-ایزوتروپی،۱۵۶ isotropy-
-پوچتوان،۳۰۲ nilpotent-
-تابی،۱۴۵ torsion-
-ثابت ساز،۱۵۶ isotropy-
-چهارتایی کلاین،۱۲ Klein four-
-حل‌پذیر،۲۹۷ solvable-
-خارج قسمت،۱۰۶ factor-
-خطی عمومی،۱۴ general linear-
-خطی ویژه،۱۴ special linear-
-خودریختی،۸۷ automorphism-
-خودریختی داخلی (خارجی)،۸۸ inner automorphism-
-دایره،۳۶ circle-
-دوری،۳۱ cyclic-

www.mathematic87.blogfa.com

-دو وجهی،۵۶	dihedral-
-ساده،۱۱۱	simple-
-متقارن،۱۳	symmetric-
-متناوب،۵۳	alternating-
-متناهی مولد،۳۸	finitely generated-
-یکال‌ها،۱۳،۱۸۷	units-

ل-م

لم ناکایاما،۲۸۱	Nakayama's Lemma
محتوا،۲۳۹	content
مدار،۱۵۶	orbit
مدول-	-module
چپ،۲۶۶	left
دوری،۲۶۹	cyclic
راست،۲۶۶	right
متناهی مولد،۲۶۹	finitely generated
متناهی هم-مولد،۲۷۴	finitely cogenerated
یکانی،۲۶۶	unitary
مرتبه،۱۱،۳۱	order
مرکز،۲۶،۱۸۷	center
مرکز ساز،۲۶	centralizer
مزدوج،۲۶،۶۹	conjugate
مسأله کلمه،۳۰۹	word problem
مشخصه،۱۸۵	characteristic
معادله رده‌ای،۱۵۷	class equation

www.mathematic87.blogfa.com

معکوس،۱۶،۱۸۷	inverse
-چپ،۱۶،۱۸۷	left-
-راست،۱۶،۱۸۷	right-
معکوس‌پذیر،۱۶،۱۸۷	invertible
مقسوم علیه صفر،۱۹۰	zero divisor
-چپ،۱۹۰	left-
-راست،۱۹۰	right-
مولد،۳۸،۱۹۵،۲۶۹	generator
مونومورفیسم،۱۱۳،۲۳۰،۲۷۱	monomorphism
مونوئید،۱۰	monoid
میدان،۱۸۸	field
-اول،۲۱۷	prime-
-کسرها،۲۳۱	quotients-

ن

نرمال ساز،۲۶،۷۴	normalizer
نمایش آزاد گروه،۳۰۸	free representation of a group
نمایش دوری،۴۶	cycle representation
نمایش دو سطری،۴۴	two rows representation
نمودار	diagram
-تعویض‌پذیر،۱۱۸	commutative-
- لاتیس،۳۳	lattice-
نوتری،۲۷۵،۲۷۷	Noetherian
-چپ،۲۷۷	left-
-راست،۲۷۷	right-

www.mathematic87.blogfa.com

نیم گروه،۱۰	semigurop

ه–ی

هسته،۱۱۵،۲۰۵،۲۷۰	kernel
هم‌ارز،۲۹۵	equivalent
همانی،۱۰	identity
هم‌دسته-	-coset
چپ ،۶۲	left
راست،۶۲	right
همریختی،۱۱۳،۲۰۳،۲۷۰	homomorphism
هممورفیسم،۱۱۳،۲۰۳،۲۷۰۱	homomorphism
یکال،۱۸۷	unit
یکریختی،۷۸،۱۹۱،۲۷۱	isomorphism

www.mathematic87.blogfa.com