

26

0.25a7

$G = \langle a \rangle$ مثال ۲۶
 فرض کنید G دو مولفه‌ای هیچ از آن، مولفه دیگری a می‌باشد و a بر این مولفه a مرتبه n دارد.
 H یک مولفه G دو مولفه‌ای می‌باشد که a بر این مولفه a مرتبه n دارد.
 نسبت به عمل ضرب در G است.

تذکر: فرض کنیم $G = \langle a \rangle$ یک مولفه G دو مولفه‌ای باشد، در این صورت اگر H یک مولفه G دو مولفه‌ای باشد، از G باشد H یک مولفه G دو مولفه‌ای می‌باشد.

قضیه: زیرگروهها گروه جفتی $\mathbb{Z}$ دقیقاً n گانه باشد به عبارتی $n \in \mathbb{N}$

قضیه: فرم کنیم $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ یک گروه دایره ای باشد و $n = |G|$ در این صورت هر عنصر a^d به n گانه در G یک زیرگروه H از G تولید میکند بطوریکه $|H| = n/d$ که در آن d بزرگترین مقسوم علیه مشترک n و d می باشد.

ثبات: $a^m = (a^d)^{m/d}$ چون $a^d = e$ ، $a^m = e$ اگرچه m بر d بخش پذیر نیست. $a^m = e$ پس m بر d بخش پذیر است. d بر m بخش پذیر است. d بر m بخش پذیر است. d بر m بخش پذیر است.

حال $d \mid d$ ، هیچ عاملی از d نمی تواند d را تقسیم کند زیرا که d بزرگترین عامل مشترک n ، $d \mid n$ پس $m \mid d \mid n$ ، m کوچکترین عدد صحیح مثبتی است که $m \mid n$ ، بنابراین $m = \frac{n}{d}$

نتیجه: فرض کنیم $\langle a \rangle = G$ گروه ادری ساده باشد و $|G| = n$ را نسبت
مولد a را در صورت a^r است که در آن $0 \leq r < n$ و نسبت به n
ادر می باشد.

$$|\langle a^r \rangle| = \frac{n}{1} = n \Rightarrow \langle a^r \rangle = G$$

یعنی اگر a و b هر دو در G باشند، پس a^m و b^m در G هستند.
 در این صورت $a^m = (a^m)^m = e$

(27)

مثال ۱) اگر $\mathbb{Z}_{12}$ را بنظر گیریم
 عناصر مرتبه مولد باشند نسبت به $n=12$ اول باشند
 همه زیرگروهها $\mathbb{Z}_{12}$:

$$\langle 0 \rangle = \{0\}$$

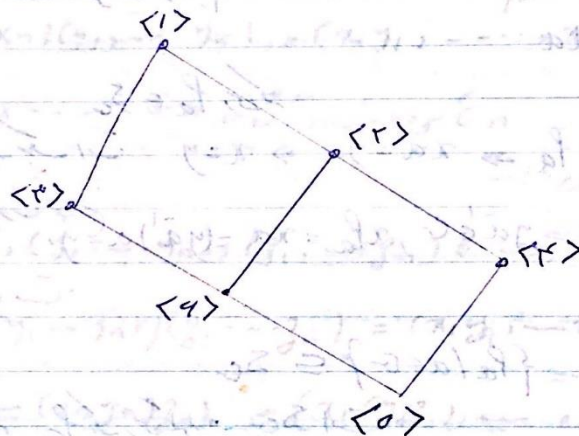
$$\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} \quad |\langle 2 \rangle| = \frac{12}{\gcd(2, 12)} = \frac{12}{2} = 6$$

$$\langle 4 \rangle = \{0, 4, 8\} \quad \langle 3 \rangle = \{0, 3, 6, 9\}$$

$$\langle 6 \rangle = \{0, 6\}$$

نمودار لائس $\mathbb{Z}_{12}$ به صورت زیر می باشد



مثال ۲) گروه $\mathbb{Z}_{18}$ را در نظر بگیریم
 مولدها $m \times 1 = (m, 18)$ و $m=1, 5, 7, 11, 13, 17$ و $m=9$ و $m=18$

$$\langle 0 \rangle = \{0\}, \quad \mathbb{Z}_{18} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle$$

$$(2, 9) = 1 \times 2 : 2 = 1, 2, 4, 5, 7, 8$$

مولدها $\langle 2 \rangle$:

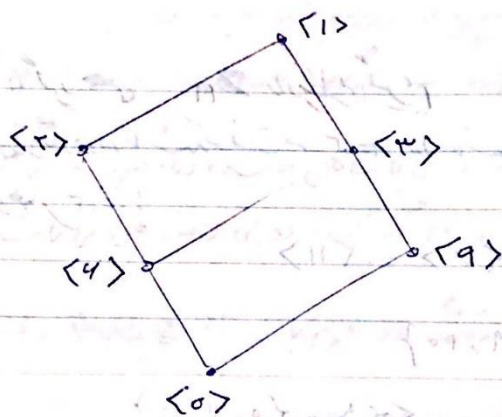
$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} = \langle 4 \rangle = \langle 1 \rangle = \langle 10 \rangle = \langle 14 \rangle$$

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\} = \langle 15 \rangle \quad \langle 6 \rangle = \{0, 6, 12\} = \langle 12 \rangle$$

$$\langle 9 \rangle = \{0, 9\}$$

$$\langle 18 \rangle = \{0, 18\}$$

(25)



نمودار لائین Z_{11} :

تصمیم خیلی: هرگز هم با گروهی از جا نیست دیگر نیست است.

آیات: فرض کنیم $\alpha \in G$ تعریف کنیم
 $f_\alpha: G \rightarrow G$
 $\alpha f_\alpha = \alpha a$

$$\alpha f_\alpha = \alpha a$$

در این صورت $f_\alpha \in S_G$ زیرا که:

$$\alpha f_\alpha = \gamma f_\alpha \Rightarrow \alpha a = \gamma a \Rightarrow \alpha = \gamma$$

$$\gamma \in G \Rightarrow \alpha = \gamma \alpha^{-1} \in G, \alpha f_\alpha = \alpha a = (\gamma \alpha^{-1}) a = \gamma$$

بن f_α یوش است.

$$f_G = \{f_\alpha / \alpha \in G\} \subseteq S_G$$

فرض کنیم f_α یک زیر گروه S_G است.

$$\forall \alpha \in G, (\alpha f_e = \alpha e = \alpha), f_e \in f_G$$

$$f_a, f_b \in f_G \Rightarrow f_a f_b = f_{ab}$$

$$\alpha \in G, \alpha(f_a f_b) = (\alpha f_a) f_b = (\alpha a) f_b = (\alpha a) b = \alpha(ab) = \alpha f_{ab}$$

$$f_a \in f_G \Rightarrow (f_a)^{-1} = f_{a^{-1}}$$

$$(f_a)(f_{a^{-1}}) = f_{aa^{-1}} = f_e, f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$$

بن $(f_a)^{-1} \in f_G$

ارائه اثبات:

نشان بدهیم که $G \cong f_G$

$$\varphi: G \rightarrow f_G$$

$$a\varphi = f_a$$

درین است که φ یک تابع پوشش است

$$a, b \in G, (ab)\varphi = f_{ab} = f_a f_b = (a\varphi)(b\varphi)$$

$$a\varphi = b\varphi \Rightarrow f_a = f_b \Rightarrow f_a = f_b \Rightarrow e f_a = e f_b \Rightarrow e a = e b \Rightarrow a = b$$

پس φ یک هم‌توپی است، زیرا $G \cong f_G$

فصل هشتم: حاصل ضرب مستقیم گروه‌ها

تعریف: فرض کنیم $G_1, \dots, G_n$ گروه باشند، $G = G_1 \times \dots \times G_n$ حاصل ضرب مستقیم آنها را بصورت زیر تعریف می‌کنیم

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$$

قضیه: اگر $G_1, \dots, G_n$ گروه باشند، آنگاه $G = G_1 \times \dots \times G_n$ یک گروه است.

شماره زیر را یک گروه است: $\{e_1, \dots, e_n\}$

اثبات: اثبات می‌کنیم $(x_1, \dots, x_n), (y_1, \dots, y_n), (z_1, \dots, z_n) \in G$

$$((x_1, \dots, x_n)(y_1, \dots, y_n))(z_1, \dots, z_n) = (x_1 y_1, \dots, x_n y_n)(z_1, \dots, z_n)$$

$$= ((x_1 y_1) z_1, \dots, (x_n y_n) z_n) = (x_1 (y_1 z_1), \dots, x_n (y_n z_n))$$

$$= (x_1, \dots, x_n)(y_1 z_1, \dots, y_n z_n) = (x_1, \dots, x_n)(y_1, \dots, y_n)(z_1, \dots, z_n)$$

پس $e = (e_1, \dots, e_n)$ عنصر هائی که G باشد، هر $1 \leq i \leq n$

عنصر هائی که G است زیرا که $(x_1, \dots, x_n) \in G$ داریم:

$$(x_1, \dots, x_n)(e_1, \dots, e_n) = (x_1 e_1, \dots, x_n e_n) = (x_1, \dots, x_n)$$

$$(e_1, \dots, e_n)(x_1, \dots, x_n) = (e_1 x_1, \dots, e_n x_n) = (x_1, \dots, x_n)$$

پس $(x_1, \dots, x_n)$ یک عضو خنثی است و G را بصورت

$$(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1}) \in G$$

$$(x_1, \dots, x_n)(x_1^{-1}, \dots, x_n^{-1}) = (x_1 x_1^{-1}, \dots, x_n x_n^{-1}) = (e_1, \dots, e_n)$$

$$(\pi_1' - \pi_n')(\alpha_1 - \alpha_n) = (\pi_1' \alpha_1 - \pi_n' \alpha_n) = (e_1 - e_n)$$

پس یک گروه است.

تمرین: نشان دهید که اگر $\alpha_1, \dots, \alpha_n$ گروهی را بسازند که یک گروه باشد، آنگاه $\alpha_1 \dots \alpha_n$ نیز آن گروه است. (برای $n=2$ به سادگی می توان دید)

$$(\alpha_1 - \alpha_n)(\beta_1 - \beta_n) = (\alpha_1 \beta_1 - \alpha_n \beta_n) = (\beta_1 \alpha_1 - \beta_n \alpha_n)$$

تعریف: اگر $\alpha_1, \dots, \alpha_n$ گروهی را بسازند که یک گروه باشد، آنگاه $\alpha_1 \dots \alpha_n$ نیز آن گروه است.

خارجی $\alpha_1, \dots, \alpha_n$ نامیده می شود.

$$\mathbb{Z} \times \{0\} \leq \mathbb{Z} \times \mathbb{Z}$$

مثال: گروه جعبه $\mathbb{Z} \times \mathbb{Z}$ را در نظر بگیرید.

$$\mathbb{Z} \times \mathbb{Z} = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{Z}\}$$

در این صورت $\mathbb{Z} \times \mathbb{Z}$ توسط عنصر $(1, 0)$ و $(0, 1)$ تولید می شود.

$$\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1) \rangle$$

تمرین: فرض کنید S یک مجموعه باشد، $S \subseteq \mathbb{Z}$ را در این صورت نشان دهید که زیرگروه تولید شده توسط S ادا است.

$$\langle S \rangle = \{d_1 \dots d_k \mid k \in \mathbb{N}, d_1, \dots, d_k \in \mathbb{Z}, d_1 \dots d_k \in S\} = T$$

$$S = \{d_1, \dots, d_n\} \text{ در } \langle d_1, \dots, d_n \rangle = \{d_1^{k_1} \dots d_n^{k_n} \mid k_1, \dots, k_n \in \mathbb{Z}\}$$

$$\langle (1, 0), (0, 1) \rangle = \{m(1, 0) + n(0, 1) \mid m, n \in \mathbb{Z}\} = \{(m, n) \mid m, n \in \mathbb{Z}\}$$

در حالت کلی اگر $\alpha_1, \dots, \alpha_n$ را در نظر بگیریم، آنگاه $\langle \alpha_1, \dots, \alpha_n \rangle$ یک گروه است.

$$\langle a \rangle = \alpha_1, \alpha_2 = \alpha_1^2, \alpha_3 = \alpha_1^3, \dots$$

$$\alpha_1 \times \alpha_2 = \langle (a, e_1), (e_1, b) \rangle = \{(a, e_1)^{k_1} (e_1, b)^{k_2} \mid k_1, k_2 \in \mathbb{Z}\}$$

مثال: گروه جعبه $\mathbb{Z}_2 \times \mathbb{Z}_2$ را در نظر بگیرید (هات هم).

$$\mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

$$\langle (1, 1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$$

مثال: $\mathbb{Z} \times \mathbb{Z}$ یک گروه است.

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

$$(1, 1)^k = (k, k) \text{ در } \mathbb{Z} \times \mathbb{Z}$$

مثال: گروه رجبی $\mathbb{Z}_2, \mathbb{Z}_4$ را در نظریه کریم
 $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), (0,2), (1,2), (0,4), (1,4), (1,1), (1,2)\}$
 یک گروه دوری نیست.

تئرم: فرض کنیم a یک گروه باشد، $a \in \langle a \rangle$ را بصورت مرتبه a کوکرتس
 عدد صحیح، نسبتی است مانند n طوری که $a^n = e$
 $|a| = |\langle a \rangle|$

نویسند: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_d \times \mathbb{Z}_k$ چنانچه d و k در $\mathbb{Z}_m \times \mathbb{Z}_n$ یک گروه دوری است.

تفسیر: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ اگر فقط اگر m, n نسبت هم اول باشند

اثبات: عنصر $(1,1)$ را در $\mathbb{Z}_m \times \mathbb{Z}_n$ را در نظریه کریم. فرض کنیم d بزرگترین مقسوم علیه
 مشترک m, n باشد. در این صورت m, n هر دو mn/d را تقسیم می کنند و
 به علاوه mn/d کوکرتس m, n است که m, n آن را تقسیم می کند. عبارت دیگر mn/d
 کوکرتس مضرب مشترک m, n می باشد. حال فرض کنیم mn/d کوکرتس
 عدد صحیح، نسبتی است که $(1,1)$ را از مرتبه d با هم جمع کنیم $(0,0)$ بدست
 می آید. عبارت دیگر مرتبه $(1,1)$ مساوی mn/d است. بنابراین mn/d کوکرتس
 $|\langle (1,1) \rangle| = mn/d$ پس یک شرط لازم برای $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ این است که
 این شرط کافی است. $d=1$ می باشد. بنابراین $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ اگر فقط اگر m, n نسبت
 هم اول باشند.

مثال: $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 \dots m_k}$ اگر فقط اگر m_i در m_j نسبت هم اول باشند
 (اثبات: شرط استقرای)

مثال: $n \in \mathbb{N}$ اگر $n = p_1^{k_1} \dots p_r^{k_r}$ آنگاه:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$$

(چون $p_i^{k_i}$ در $p_j^{k_j}$ نسبت هم اولند)

هر گروه دوری را به یک گروه حاصل ضرب
 p گروه دوری متناهی تجزیه کرد.

