Conteúdo página 203 - 7.3 Subgrupos

A) 1) Liste todos os subgrupos cíclicos de:

a) U_{15}. $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$

$U_N = (N, a) = 1$

$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

- $\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 0\rangle$
  $\langle 1 \rangle = \mathbb{Z}_{15}$, é gerador de $\mathbb{Z}_{15}$

- $\langle 2 \rangle = \{2, 4, 6, 8, 10, 12, 14, 1, 3, 5, 7, 9, 11, 13, 0\}$

$2^1 = 2$ $\quad 2^5 = 10$ $\quad 2^9 = 2^8 + 2 = 18 = 3 \pmod{15}$

$2^2 = 4$ $\quad 2^6 = 12$ $\quad 2^{11} = 18 + 2 = 20 = 5 \pmod{15}$

$2^3 = 6$ $\quad 2^7 = 14$ $\quad 2^{12} = 20 + 2 = 7 \pmod{15}$

$2^4 = 8$ $\quad 2^8 = 16 = 1 \pmod{15}$ $\quad 2^{13} = 22 + 2 = 24 = 9 \pmod{15}$

$2^{14} = 24 + 2 = 26 = 11 \pmod{15}$

$2^{15} = 28 = 13 \pmod{15}$

$2^{16} = 30 = 0 \pmod{15}$

$\langle 2 \rangle = \mathbb{Z}_{15}$

- $\langle 4 \rangle$: $4^1 = 4$ $\quad 4^6 = 34 = 4 \pmod{15}$

$4^2 = 8$

$4^3 = 12$ $\quad \langle 4 \rangle = \{4, 8, 12, 1, 5, 9, 13, 2, \}$

$4^4 = 1 \pmod{15}$

$4^5 = 5 \pmod{15}$ $\quad$ → Não é subgrupo.

$4^6 = 20 + 4 = 24 = 9 \pmod{15}$

$4^4 = 28 = 13 \pmod{15}$

$4^5 = 32 = 2 \pmod{15}$

$\cdot \langle 7 \rangle$, $7^1 = 7$

$7^2 = 14$

$7^3 = 21 = 6 \pmod{15}$

$7^4 = 28 = 13 \pmod{15}$

$7^5 = 35 = 5 \pmod{15}$

$7^6 = 42 = 7 \pmod{15}$

$\langle 7 \rangle = \{7, 14, 6, 13, 5\}$

↳ Não é subgrupo

$\cdot \langle 8 \rangle$, $8^1 = 8$

$8^2 = 16 = 1 \pmod{15}$

$8^3 = 8^2 + 8 = 24 = 9 \pmod{15}$

$8^4 = 8^3 + 8 = 32 = 2 \pmod{15}$

$8^5 = 8^4 + 8 = 40 = 10 \pmod{15}$

$8^6 = 8^5 + 8 = 48 = 3 \pmod{15}$

$8^7 = 8^6 + 8 = 56 = 11 \pmod{15}$

$8^8 = 8^7 + 8 = 56 + 8 = 64 = 4 \pmod{15}$

$8^9 = 8^8 + 8 = 64 + 8 = 72 = 12 \pmod{15}$

$8^{10} = 8^9 + 8 = 72 + 8 = 80 = 5 \pmod{15}$

$8^{11} = 8^{10} + 8 = 88 = 13 \pmod{15}$

$8^{12} = 8^{11} + 8 = 96 = 6 \pmod{15}$

$8^{13} = 8^{12} + 8 = 104 = 14 \pmod{15}$

$8^{14} = 8^{13} + 8 = 112 = 7 \pmod{15}$

$8^{15} = 8^{14} + 8 = 120 = 0 \pmod{15}$

$\langle 8 \rangle = \{8, 1, 9, 2, 10, 3, 11, 4, 12, 5, 13, 6, 14, 7, 0\}$

$\cdot \langle 11 \rangle$ $11^1 = 11$

$11^2 = 22 = 7 \pmod{15}$

$11^3 = 33 = 3 \pmod{15}$

$11^4 = 44 = 14 \pmod{15}$

$11^5 = 55 = 10 \pmod{15}$

$11^6 = 66 = 6 \pmod{15}$

$11^7 = 77 = 2 \pmod{15}$

$11^8 = 85 = 10 \pmod{15}$ Repete.

$11^9 = 93 = 3 \pmod{15}$

$\langle 11 \rangle = \{11, 7, 3, 14, 10, 6, 2,\}$

↳ Não é subgrupo

$\cdot \langle 13 \rangle \quad 13^1 = 13$

$13^2 = 26 = 11 \pmod{15}$

$13^3 = 39 = 9 \pmod{15}$

$13^4 = 42 = 12 \pmod{15}$

$13^5 = 55 = 10 \pmod{15}$

$13^6 = 58 = 13 \pmod{15}$

$13^7 = 71 = 11 \pmod{15}$ Repete.

$13^8 = 84 = 9 \pmod{15}$

$\langle 13 \rangle = \{13, 11, 9, 12, 10, \}$

↳ Não é subgrupo

$\cdot \langle 14 \rangle$

$14^1 = 14$

$14^2 = 28 = 3 \pmod{15}$

$14^3 = 42 = 12 \pmod{15}$

$14^4 = 56 = 11 \pmod{15}$

$14^5 = 70 = 10 \pmod{15}$

$14^6 = 84 = 9 \pmod{15}$

$14^7 = 98 = 8 \pmod{15}$

$14^8 = 112 = 7 \pmod{15}$

$14^9 = 126 = 6 \pmod{15}$

$14^{10} = 140 = 5 \pmod{15}$

$14^{11} = 154 = 4 \pmod{15}$

$14^{12} = 168 = 2 \pmod{15}$

$14^{13} = 182 = 2 \pmod{15}$

Repete

$\langle 14 \rangle = \{14, 3, 12, 11, 10, 9, 8, 7, 6, 5, 4, 2\}$

↳ Não é subgrupo

Somente $\langle 1 \rangle$ e $\langle 8 \rangle$ possui o elemento neutro, mas também não é subgrupo de U_{15}.

2) a) Liste todos os subgrupos cíclicos do D_4.

$D_4 = \{r_0, r_1, r_2, r_3, h, v, d, t\}$

?

4| $\langle 2 \rangle$ na adição $\mathbb{Z}_{12}$. $\langle 2 \rangle$.

$\mathbb{Z}_{12}$: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$2^1 = 2$, $2^2 = 4$, $2^3 = 6$, $2^4 = 8$, $2^5 = 10$
$2^6 = 12 \equiv 0 \pmod{12}$, $2^7 = 14 \equiv 2 \pmod{12}$.

$\langle 2 \rangle = \{\underline{2}, \underline{4}, \underline{6}, \underline{8}, \underline{10}, \underline{0}\}$

$\langle 2 \rangle \subseteq \mathbb{Z}_{12}$. e $\langle 2 \rangle$ é cíclico.

5| $\langle 2 \rangle$ é um grupo aditivo em $\mathbb{Z}$.

$\mathbb{Z}$: $\{\ldots, -1, 0, 1, \ldots\}$

$\langle 2 \rangle = \{2, 4, 6, 8, 10, \ldots\}$ é o conjunto dos números inteiros par.

6| $\langle 2 \rangle$ no grupo multiplicativo de elementos diferentes de zero de $\mathbb{Z}_{11}$.

$\mathbb{Z}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\langle 2 \rangle$: $2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16 = 5 \pmod{11}$
$2^5 = 32 = 10 \pmod{11}$
$2^6 = 64 = 9 \pmod{11}$
$2^7 = 128 = 7 \pmod{11}$
$2^8 = 256 = 3 \pmod{11}$

$\langle 2 \rangle = \{2, 4, 8, 5, 9, 7, 3, 6, 1\}$

$2^9 = 512 = 6 \pmod{11}$
$2^{10} = 1024 = 1 \pmod{11}$
$2^{11} = 2048 = 2 \pmod{11}$
↳ repete

7. $\langle 2 \rangle$ no grupo multiplicativo $\mathbb{Q}^*$ dos números racionais diferentes de zero.

$(\mathbb{Q}^*, \cdot)$ é um grupo infinito

$\langle 2 \rangle$ é um gerador infinito.

8) $\langle 3 \rangle$ no grupo multiplicativo de elementos diferentes de zero em $\mathbb{Z}_{11}$.

$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\langle 3 \rangle = 3^1 = 3$

$3^2 = 9$

$3^3 = 27 = 5 \pmod{11}$

$3^4 = 81 = 4 \pmod{11}$

$3^5 = 243 = 1 \pmod{11}$

$3^6 = 729 = 3 \pmod{11}$

16.807 ⌊15

18   1120

307

7

$\langle 3 \rangle = \{3, 9, 5, 4, 1\}$

9) Mostre que U_{15} é gerado pelo conjunto $\{2, 13\}$

$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\langle 7 \rangle = 7^1 = 7$

$7^2 = 49 = 4 \pmod{15}$

$7^3 = 343 = 13 \pmod{15}$

$7^4 = 1 = \pmod{15}$

$7^5 = 7 = \pmod{15}$

↳ repete.

$\{7, 11\}$ é gerador de U_{15}.

$\langle 2 \rangle = 2^1 = 2$

$2^2 = 4$ $\qquad \langle 2 \rangle = \{2, 4, 8, 1\}$

$2^3 = 8$

$2^4 = 16 \equiv 1 \pmod{15}$

$2^5 = 32 \equiv 2 \pmod{15}$

$\Rightarrow$ repete.

$13^1 = 13$, $2 \cdot 13 = 26 \equiv 9 \pmod{15}$

$2^2 \cdot 13 = 4 \cdot 13 = 52 \equiv 7 \pmod{15}$

$2^3 \cdot 13 = 8 \cdot 13 = 104 \equiv 14 \pmod{15}$

$\{2, 13\} = \{2, 4, 8, 1, \cancel{2}, 13, \cancel{9}, 7, 14, 11\}$

$2^4 \cdot 13 = 32 \cdot 13 \equiv 11 \pmod{15}$

Temos que $\{2, 13\}$ é gerador de U_{15}.

10) Mostre que $(1,0)$ e $(0,2)$ são geradores aditivos em $\mathbb{Z} \times \mathbb{Z}_7$

(a,b) tal $a \in \mathbb{Z}$ e $b \in (0,6)$ esta em $\mathbb{Z} \times \mathbb{Z}_7$

$(1,0) \rightarrow (\mathbb{Z}, 0)$

$N(1,0) \rightarrow (\mathbb{Z}, 0)$, $N = -\infty$ a $+\infty$. $\Big\{$ a.

$(0,2)$, como $(2,7) = mdc = 1$.

$(0,2)^6 = (0,5)$

$(0,2)^7 = (0,0)$

$(0,2)^1 \rightarrow (0,2)$

$(0,2)^2 \rightarrow (0,2) + (0,2) = (0,4)$

$(0,2)^3 \rightarrow (0,2) + (0,2) + (0,2) = (0,6)$

$(0,2)^4 \rightarrow (0,2)^3 + (0,2) = (0,8) = (0,1) \pmod 7$

$(0,2)^5 \rightarrow (0,2)^4 + (0,2) = (0,10) = (0,3) \pmod 7$

Assim $(1,0)$ gera $(\mathbb{Z},0)$ ao aplicar n em adição:

$$(1+n,0) \rightarrow (\mathbb{Z},0)$$

e $(0,2)$ gera $(0,\mathbb{Z}_7)$, ao aplicar a operação sucessiva:

$$\langle(0,2)\rangle = \{(0,2),(0,4),(0,6),(0,1),(0,3),(0,5),(0,0)\}$$

Com isso $(1,0)$ e $(0,2)$ gera $\mathbb{Z}\times\mathbb{Z}_7$.

11) Mostre que o grupo aditivo $\mathbb{Z}_2\times\mathbb{Z}_3$ é cíclico.

$\mathbb{Z}_2=\{0,1\}$ e $\mathbb{Z}_3=\{0,1,2\}$ $\quad mdc(2,3)=1$

	$\mathbb{Z}_3$			
	+	0	1	2
$\mathbb{Z}_2$	0	0	1	2
	1	1	2	0

Definição: Temos G e H sendo grupos. O produto direto $G\times H$ de G e H é o conjunto de todos os pares ordenados:

$\{(g,h) \mid g\in G, h\in H\}$ com a operação:

$(g_1,h_1)\cdot(g_2,h_2)=(g_1g_2,h_1h_2)$, $Id=(1,1)$

$(g_1,h_1)+(g_2,h_2)=(g_1+g_2,h_1+h_2)$, $Id=(0,0)$

Inverso: $(g,h)^{-1}=(g^{-1},h^{-1})$

Inverso: $-(g,h)=(-g,-h)$

Temos que mostrar que $\mathbb{Z}_2 \times \mathbb{Z}_3$ é cíclico;

Temos que $\mathbb{Z}_2 = \{0,1\}$ e $\mathbb{Z}_3 = \{0,1,2\}$

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

Se tomarmos multiplicações sucessivas de $(1,1)$, do produto cartesiano aditivo teremos:

$$(1,1)+(0,0),\ (1,1)+(0,2),\ (1,1)+(1,0),\ (1,1)+(1,1),\ (1,1)+(1,2) =$$

$$(1,1),\ (1,0),\ (0,1),\ (0,2),\ (0,0) \Rightarrow$$

$3=0 \pmod 3$, $2=0 \pmod 2$, mod 2, mod 2

Começa a repetir a partir de $(1,1)$ novamente. Com isso temos que o produto cartesiano de $\mathbb{Z}_2 \times \mathbb{Z}_3$ de múltiplos de $(1,1)$ é cíclico e possui ordem 6, sendo igual a $\mathbb{Z}_6 = |\mathbb{Z}_6|$

$$|\mathbb{Z}_2| \cdot |\mathbb{Z}_3| = |\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_6|$$

---

12) Mostre que o grupo aditivo $\mathbb{Z}_2 \times \mathbb{Z}_4$ não é cíclico, mas é gerado por 2 elementos.

Temos que $\mathbb{Z}_2 = \{0,1\}$ e $\mathbb{Z}_4 = \{0,1,2,3\}$, então:

$$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$$

Temos que: $(1,0) \in \mathbb{Z}_2$ e $(0,1) \in \mathbb{Z}_4 \longrightarrow x(1,0) + y(0,1)$

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

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

Portanto $\mathbb{Z}_2 \times \mathbb{Z}_4$ não é cíclico e deveria ter ordem:

$$|\mathbb{Z}_2 \times \mathbb{Z}_4| = |\mathbb{Z}_2| \times |\mathbb{Z}_4| = |\mathbb{Z}_8| = 8.$$

Temos que $\langle 1,0 \rangle$ e $\langle 0,1 \rangle$ são cíclicos, mas o produto cartesiano não é.

$\langle 1,0 \rangle \times \langle 0,1 \rangle = \{(1,1), (1,2), (1,3), (1,0), (0,1), (0,2), (0,3), (0,0)\}$

Mas $|\mathbb{Z}_2 \times \mathbb{Z}_4| = \langle 1,0 \rangle \times \langle 0,1 \rangle$ não é cíclico.

4

13) Temos H sendo um subgrupo de um grupo G. Se e_G é a identidade (elemento) de G e e_H é o elemento identidade de H. Prove que $e_G = e_H$.

Temos que $H \subseteq G$, sendo $H < G$ ou $H \leq G$.

Tomamos $a \in H$ e como $H \subseteq G$, temos que $a \in G$. Se a for elemento identidade de H então a é único por definição das propriedades de grupo, seja um grupo aditivo e/ou multiplicativo.

Como todo subgrupo é diferente de vazio e deve possuir elemento identidade, temos que e_H é identidade em H. Mas $H \subseteq G$, então $e_H \in G$ e portanto e_H também é elemento identidade de G. Portanto: $e_H = e_G$.

14) Temos H e K sejam subgrupos de um grupo G.

a) Mostre por exemplo que $H \cup K$ pode não ser um subgrupo de G.

i) H, K $\neq$ vazio
ii) $*$ associativo
iii) $*$ admite elemento neutro
iv) admite simetrico
v) $*$ é fechado

Considere o grupo $\mathbb{Z}^2$, e tomamos:

$H = \{(x,0) ; x \in \mathbb{Z}\}$ e $K = \{(0,x) ; x \in \mathbb{Z}\}$

Note que H e K são subgrupos de $\mathbb{Z}^2$. Assim, se pegarmos $(1,0) \in H$ e $(0,1) \in K$, encontraremos $(1,1)$ que não pertence a $H \cup K$.

Então, $H \cup K$ é um subgrupo.

b) Prove que $H \cup K$ é um subgrupo de G se e somente se $H \subseteq K$ ou $K \subseteq H$.

i) Suponha $H \subseteq K$ ou $K \subseteq H$, então $H \cup K = K$ ou $H \cup K = H$. Como $H \cup K \subseteq G$, então $H \cup K < G$ ou $H \cup K \leq G$ e $H, K \leq G$.

ii) Suponha que $H \cup K \leq G$, para mostrar que $H \subseteq K$ ou $K \subseteq H$, precisamos mostrar que $H \nsubseteq K \Rightarrow K \subseteq H$.

Dadas as duas condições (i) e (ii), supomos $H \not\subseteq K$. Então existe um $h \in H$ sendo que $h \notin K$. Temos que $k \in K$.

Então $h, k \in H \cup K$, que significa que $hk \in H \cup K$ desde que $H \cup K \leq G$.

Se $hk \in K$ então $h = he = h(kk^{-1}) = (hk)k^{-1} \in K$, uma contradição.

Entretanto se $hk \in H$, isto significa que $k = ek = (h^{-1}h)k = h^{-1}(hk) \in H$.

Com isso temos que $K \subseteq H$.