CTC – 20
Estruturas Discretas para Computação

Prof. Armando Gouveia

Grupos cíclicos

Questão:

Dado um grupo G, encontrar alguns subgrupos.

Primeira tentativa:

$e \in H$

se $a \in H$ então $a^{-1} \in H$

$a * a \in H$

$a^{-1} * a^{-1} \in H$

$a * a * a \in H$ etc...

Definição

$$a^n = \begin{cases} e & , \text{se } n = 0 \\ a^{n-1} * a & , \text{se } n > 0 \\ (a^{-1})^{|n|} & , \text{se } n < 0 \end{cases}$$

Propriedades

(1) $a^r * a^s = a^{r+s}$

(2) $(a^n)^{-1} = a^{-n}$

(3) $(a^r)^s = a^{r \cdot s}$

Demonstração

Exercício.

Usar definição.

Exemplo

$(Z, +)$

Quanto valem 5^3 e 5^{-1} ?

$5^3 = 5 + 5 + 5 = 15$

$5^{-1} = -5$

$5^3 * 5^{-1} = 15 - 5 = 10 = 5^2$

Definição

Dado um grupo G e um elemento a em G, define-se

$$< a > \; = \; \{\ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\}$$

= subgrupo cíclico de G gerado por a.

Demonstração

Devemos provar que $< a >$ é subgrupo.

- Fechado: Sejam $x, y \in < a >$

$$\left.\begin{array}{l} x \in < a > \Rightarrow \exists r \mid x = a^r \\ y \in < a > \Rightarrow \exists s \mid y = a^s \end{array}\right\} \Rightarrow x * y = a^r * a^s = a^{r+s} \in < a >$$

- Elem. neutro: $e \in < a >$ por definição
- Inversas: Seja $x \in < a >$ então $\exists r \mid x = a^r$

logo $x^{-1} = (a^r)^{-1} = a^{-r} \Rightarrow x^{-1} \in < a >$ [CQD]

Definição

a é chamado "gerador" de $< a >$

Observação

Posso ter $a \neq b$ mas $< a > = < b >$?

Sim. Exemplo: $G = (Z, +)$

$$< 5 > = < -5 > = \{ \ldots , -10, -5, 0, 5, 10, 15, \ldots \}$$

Observação 2

Se $H < G$ e $a \in H$ então $< a > \leq H$

Definição

Se ocorrer que $< a >$ é o próprio G

então G é chamado grupo cíclico

isto é, gerado por algum dos seus elementos.

Exemplo

$(Z, +)$ é grupo cíclico, pois $Z = < 1 > \ = \ < -1 >$

Observação

Z é gerado apenas por esses dois elementos.

Exemplo

Um grupo cíclico finito?

Já visto:

$*_2$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Qual o gerador? a (ou c).

Grupo Z_n

Seja o conjunto $Z_n = \{ 0, 1, 2, ..., n-1 \}$.

Seja $\oplus$ a soma módulo n.

Exemplo: $Z_5 = \{ 0, 1, 2, 3, 4 \}$

$$3 \oplus 4 = 2$$

pois $3 + 4 = 7 \equiv 2 \pmod 5$

Observações

Para todo n,

Z_n é um grupo

Z_n é cíclico, pois $Z_n = < 1 >$

Z_n é abeliano, pois $a \oplus b = b \oplus a$

(mesmo "resto" na divisão por n).

Teorema

Todo grupo cíclico é abeliano.

Demonstração

$G = < a >$

$$\left.\begin{array}{l} x \in G \\ y \in G \end{array}\right\} \Rightarrow \left.\begin{array}{l} \exists r \mid x = a^r \\ \exists s \mid y = a^s \end{array}\right\} \Rightarrow x * y = a^r * a^s = a^{r+s} = a^{s+r}$$

$$= a^s * a^r = y * x \qquad \text{[CQD]}$$

Algoritmo da Divisão

Teorema

Dados $m, n \in Z,$ com $m > 0$

$$\text{Existem} \quad \left.\begin{array}{l} q, r \in Z \\ q, r \ \text{únicos} \end{array}\right\} \text{ tais que } \begin{cases} n = m \cdot q + r \\ 0 \le r < m \end{cases}$$

Teorema

Todo subgrupo de um grupo cíclico é também cíclico.

Demonstração

Temos $H \leq G = < a >$

Caso 1: Se $H = \{ e \}$, ok.

Caso 2: Se $| H | \geq 2$,

consideremos o menor inteiro positivo m tal que $a^m \in H$. (*)

Seja $c = a^m$.

Provaremos que $H = < c >$.

Seja um elemento genérico $a^n \in H$.

Pelo Algoritmo da Divisão, $\exists q, r \in Z$ tais que $n = m \cdot q + r$

com $0 \leq r < m$ (**)

Então $a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$

Logo $a^r = \underbrace{a^n}_{\in H} * \underbrace{(a^m)^{-q}}_{\in H} \Rightarrow a^r \in H$

Mas (*) e (**) implicam que
se $a^r \in H$ então $r = 0$.

Temos $a^n = a^{mq+0} = a^{mq} = (a^m)^q = c^q$

Ou seja, dado um elemento genérico $a^n \in H$

provamos que ele é da forma c^q.

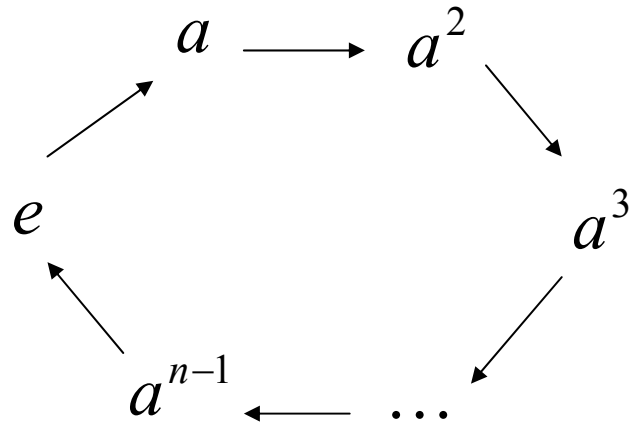
Portanto $H = < c > = < a^m >$

e, assim, H é cíclico.

[CQD]

Observação

Por que o nome “cíclico”?



Isso “sugere” que existe um inteiro n tal que $a^n = e$.

Mas isso não ocorre se o grupo cíclico for infinito.

Por exemplo, $(Z, +)$.

Questão

Seja G um grupo cíclico com n elementos.

$G = \{ e, a, \ldots , a^{n-1} \}$

$a^n = e$

Quantos elementos tem o subgrupo $< a^k >$?

Exemplo

$| G | = 12$

$G = \{ e, a, a^2, \ldots , a^{11} \}$

$< a^6 > = \{ e, a^6 \}$; tamanho 2.

$< a^5 > = \{ e, a^5, a^{10}, a^3, a^8, a, a^6, a^{11}, a^4, a^9, a^2, a^7 \} = G$

$< a^4 > = \{ e, a^4, a^8 \}$; tamanho 3

$< a^8 > = \{ e, a^8, a^4 \} = < a^4 >$

Teorema

Grupo cíclico $G = \{ e, a, \ldots , a^{n-1} \}$

$a^n = e$

Então o subgrupo $< a^k >$ tem $\dfrac{n}{\text{mdc}(n,k)}$ elementos.

Ordem de um elemento

Em um grupo $(G, *)$

para cada elemento $a \in G$

definimos $o(a) =$ ordem do elemento a

$=$ menor $k > 0$ tal que $a^k = e$.

Exemplo

$| G | = 12$

$G = \{ e, a, a^2, \ldots , a^{11} \}$

$o(a) = 12,$ pois $\begin{cases} a^n \neq e, \text{ para } 1 \leq n \leq 11 \\ a^{12} = e \end{cases}$

$o(a^4) = 3$

$o(a^5) = 12$

Exemplo

Grupo de Klein

$o(e) = 1$

$o(a) = o(b) = o(c) = 2$

Exemplo

$(Q^*, \cdot)$

$o\,(1) = 1$

$o\,(2) = \text{infinito}$

$o\,(456) = \text{infinito}$

$o\,(-1) = 2$

Exemplo

$Z_8 = \{\, 0, 1, 2, 3, 4, 5, 6, 7 \,\}$

$o\,(0) = 1$

$o\,(1) = 8$

$o\,(4) = 2$

Observação

Em um grupo cíclico infinito $G = < a >$

pode ocorrer $a^r = a^s$ com $r \neq s$?

Resposta: não.

Demonstração

Supor $a^r = a^s$ com $r \neq s$.

Sem perda de generalidade, $r > s$.

Então $a^{r-s} = e$.

Considere o menor natural $n \neq 0$ tal que $a^n = e$.

Tal n existe, pois $n \leq r - s$.

Então $G = < a > = \{e, a, a^2, \ldots, a^{n-1}\}$ seria finito. [Contradição]

pois $\begin{cases} a^{n+1} = a^n * a = e * a = a \\ a^{n+k} = a^n * a^k = e * a^k = a^k \end{cases}$