CTC – 20
Estruturas Discretas para Computação

Prof. Armando Gouveia

Classes laterais

Dados um grupo $(G, *)$

um subgrupo $H \leq G$

um elemento fixo $a \in G$

Definição

conjunto $aH = \{a * h \mid h \in H\}$ = classe lateral à esquerda

$Ha = \{h * a \mid h \in H\}$ = classe lateral à direita

Observação

Em inglês: coset

Exemplo

Grupo S_3

$H = \{\rho_0, \rho_1, \rho_2\}$

Calcular todas as classes laterais à esquerda.

$$\rho_0 H = \{\rho_0\rho_0, \rho_0\rho_1, \rho_0\rho_2\} = \{\rho_0, \rho_1, \rho_2\} = H$$

$$\rho_1 H = \{\rho_1\rho_0, \rho_1\rho_1, \rho_1\rho_2\} = \{\rho_1, \rho_2, \rho_0\} = H$$

$$\rho_2 H = = H$$

$$\mu_1 H = \{\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2\} = \{\mu_1, \mu_2, \mu_3\}$$

$$\mu_2 H = \{\mu_2\rho_0, \mu_2\rho_1, \mu_2\rho_2\} = \{\mu_2, \mu_3, \mu_1\}$$

$$\mu_3 H = \{\mu_3, \mu_1, \mu_2\}$$

Exemplo

Grupo S_3

$H = \{\mu_1\}$

Calcular todas as classes laterais à esquerda.

$\rho_0 H = \{\rho_0 \mu_1\} = \{\mu_1\}$?

$\mu_2 H = \{\mu_2 \mu_1\} = \{\rho_2\}$?

NÃO atende à definição!

Pois neste caso H não é subgrupo de S_3.

Outras observações

- De modo geral $aH \neq Ha$.
- G abeliano $\rightarrow aH = Ha$.
- $aH = Ha$ não implica H abeliano.

Questão

Como será o formato das classes laterais, em geral?

Proposição

Dados um grupo G e um subgrupo $H \leq G$,
as classes laterais à esquerda de H
determinam uma partição de G.

Demonstração

Quero provar que $P = \{aH \mid a \in G\}$ é partição.

(i) $\forall a \in G, aH \neq \emptyset$?

H subgrupo $\Rightarrow e \in H \Rightarrow ae \in aH \Rightarrow a \in aH \Rightarrow aH \neq \emptyset$

(iii) $\bigcup_{X \in P} X = G$?

Provar $\subseteq$ é trivial

pois G grupo $\rightarrow$ fechado $\rightarrow aH \subseteq G$.

Para $\supseteq$ temos :

$\forall a \in G, \exists X = aH \in P$ tal que $a \in X$.

(ii) $\forall a,b \in G$ vale $aH \cap bH = \varnothing$ ou $aH = bH$ (?)

Se $aH \cap bH = \varnothing$ então OK.

Caso contrário, seja $c \in aH \cap bH$

então $\exists h_1 \in H$ tq $ah_1 = c$

$\exists h_2 \in H$ tq $bh_2 = c$

Seja um elemento $d \in aH$ genérico

vale $\exists h \in H$ tq $d = ah$

então $d = ah = ah_1 h_1^{-1} h$

$= ch_1^{-1} h$

$= b\underbrace{h_2 h_1^{-1} h}_{\in H}$ logo $d \in bH$.

Conclusão: $\forall d \in aH$ vale $d \in bH$

Analogamente, $\forall d' \in bH$ vale $d' \in aH$

} então $aH = bH$.

[CQD]

Observação

Já provamos um teorema que nos diz que toda partição em um conjunto nos fornece uma relação de equivalência.

Definição

As classes laterais são chamadas "classes de equivalência".

Exemplo

Grupo $(Z, +)$

Subgrupo $(5Z, +) = \{ \ldots, -10, -5, 0, 5, 10, \ldots\}$

$\{ \ldots, -9, -4, 1, 6, 11, \ldots\}$

Quais são as classes laterais? $\{ \ldots, -8, -3, 2, 7, 12, \ldots\}$

$\{ \ldots, -7, -2, 3, 8, 13, \ldots\}$

$\{ \ldots, -6, -1, 4, 9, 14, \ldots\}$

$\{ \ldots, -5, 0, 5, 10, 15, \ldots\}$

Notação

Escolhemos um representante x de cada classe

para designar o conjunto, usando $\overline{x}$.

No exemplo, temos $\overline{0} = \{ \ldots, -10, -5, 0, 5, 10, \ldots\}$

$\overline{1} = \{ \ldots, -9, -4, 1, 6, 11, \ldots\}$

Dizemos $\overline{x} =$ classe de equivalência do elemento x.

Exemplo (novamente)

Grupo $(Z, +)$

Subgrupo $(5Z, +) = \{ \ldots, -10, -5, 0, 5, 10, \ldots \}$

Observação

Sabemos: partição $\leftrightarrow$ relação de equivalência.

Pergunta: com a partição acima, qual relação de equivalência obtemos?

Resposta: soma módulo 5.

Ou seja, $a \sim b$ sse $a \equiv b \pmod 5$

Importante

Recordação: $Z_n = \{ 0, 1, 2, 3, \ldots, n-1 \}$

com operação $a*b = (a+b) \bmod n$

No "conjunto" Z_n temos um representante de cada classe.

Questão

Analisar os tamanhos das classes

para $|G|$ finito e infinito.

Teorema

Seja G um grupo finito e H um subgrupo de G.

Então, para qualquer $a \in G$,

H e aH têm o mesmo número de elementos.

Demonstração

Basta mostrar uma bijeção entre H e aH.

$(\rightarrow)$

Basta mostrar uma bijeção entre H e aH.

Seja a função $f : H \to aH$

$$f(h) = a * h$$

Sobrejetora : óbvio.

Injetora : $f(h_1) = f(h_2) \Rightarrow$

$$a * h_1 = a * h_2 \underset{\text{Cancelamento}}{\Rightarrow} h_1 = h_2$$

[CQD]

Teorema de Lagrange

Seja G um grupo finito

e H um subgrupo de G.

Então $|H|$ é divisor de $|G|$.

Corolário

Dado G um grupo finito,

a ordem de qualquer elemento de G

é divisor da ordem de G.

Demonstração

(informal)

$a \in G \quad \Rightarrow \quad < a > \leq G$

mas $\text{o}(a) = |< a >|$ é divisor do $|G|$. [CQD]

Corolário

Todo grupo de ordem prima é cíclico.

Teorema

Para cada primo p,

Z_p é o "único" grupo de ordem p.

Observação

Acima, "único" significa que

qualquer outro de ordem p será isomorfo a ele.

Definição

Seja um grupo G e um subgrupo $H \leq G$.

O número de classes laterais determinadas por H

chama-se índice de H em G e é denotado $(G : H)$.

Obs.: $$|G| \text{ finito } \Rightarrow \ (G:H) = \frac{|G|}{|H|}$$