Primeira Prova de CTC-20 – Estruturas Discretas
24/09/2009
Prof. Carlos Henrique Q. Forster

Nome: GABARITO

1. (4.0 pontos) Considere $Z_n = \{0,1,....,n-1\}$.
a) Mostre que $(Z_2, \oplus)$ é um grupo, onde $\oplus$ é a operação "ou-exclusivo".
b) Mostre que a operação ou-exclusivo bit-a-bit em palavras de 3 bits forma um grupo.
c) O grupo do item (b) é cíclico?
d) O grupo do item (b) é abeliano?

a)

i) associativa
Verificando-se exaustivamente os resultados de $a \oplus (b \oplus c)$ e de $(a \oplus b) \oplus c$ para todas possíveis triplas de valores (a,b,c) conclui-se que $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.

ii) elemento neutro
Verifica-se adotando o elemento 0 como identidade:
$a \oplus 0 = 0 \oplus a = a$

iii) elemento inverso
O inverso de 0 é 0 e o inverso de 1 é 1

b)

Trata-se do produto direto de grupos e portanto é um grupo, como pode-se verificar:

i) associativa
$[(a,b,c) \oplus (d,e,f)] \oplus (g,h,i) = ([a \oplus d] \oplus g, [b \oplus e] \oplus h, [c \oplus f] \oplus i) =$
$= (a \oplus [d \oplus g], b \oplus [e \oplus f], c \oplus [f \oplus i]) = (a,b,c) \oplus [(d,e,f) \oplus (g,h,i)]$

ii) elemento neutro (0,0,0)
$(a,b,c) \oplus (0,0,0) = (a \oplus 0, b \oplus 0, c \oplus 0) = (0 \oplus a, 0 \oplus b, 0 \oplus c) = (0,0,0) \oplus (a,b,c) = (a,b,c)$

iii) elemento inverso
O elemento inverso de (a,b,c) é o próprio (a,b,c) para todas possíveis triplas.
$(a,b,c) \oplus (a,b,c) = (a \oplus a, b \oplus b, c \oplus c) = (0,0,0)$

c)

Não é cíclico.

O ciclo gerado pelo elemento neutro (0,0,0) contém apenas o próprio.
Os demais ciclos, gerados por (a,b,c) diferente da identidade contem a identidade e o próprio elemento (a,b,c).
Dessa forma, não é possível encontrar um elemento gerador de todos elementos do conjunto.

d)

Sim, é abeliano.

Verifica-se que $a \oplus b = b \oplus a$.
De forma que

$$(a,b,c) \oplus (d,e,f) = (a \oplus d, b \oplus e, c \oplus f) = (d \oplus a, e \oplus b, f \oplus c)$$
$$= (d,e,f) \oplus (a,b,c)$$

2. (3.0 pontos) Quanto ao isomorfismo de grupos.
a) Mostre que dois grupos finitos isomorfos têm a mesma ordem.
b) Mostre que se G_1 e G_2 são grupos isomorfos, então dado $H_1 \leq G_1$ existe $H_2 \leq G_2$ isomorfo a H_1.
c) Responda justificando, considerando a operação "soma módulo n": o grupo formado por Z_8 e o grupo formado por $Z_2 \times Z_4$ são isomorfos? (Dica: o que acontece com $(0,3)+(0,1)$)

a)
Por definição, existe uma bijeção f entre grupos isomorfos A e B. Por ser função, cada elemento de A está associado a um elemento de B. Por ser sobrejetora, não há elementos de B que não estejam relacionados a um de A de forma que $|A| \geq |B|$. Por ser injetora, cada elemento de A está relacionado a um elemento de B distinto de forma que $|B| \geq |A|$.
Assim: $|f| = |A| = |B|$
(No caso de conjuntos infinitos, a igualdade das cardinalidades de dois conjuntos é por definição a existência de uma bijeção entre eles.)

b)
G_1, G_2 isomorfos $\Rightarrow \exists f: G_1 \to G_2 \mid f(a,b) = f(a)f(b),\ f$ injetora e sobrejetora
H_1 subgrupo de G_1
$\forall h \in H_1,\ f(h) \in H_2 \Rightarrow H_2$ é a imagem de f com domínio H_1.
Por construção de H_2, f é sobrejetora de H_1 para H_2.
Por hipótese, f é injetora $f(a) \neq f(b) \Leftrightarrow a \neq b$
H_2 é fechada com a operação do grupo de G_2 pois:
$\forall h_1, h_2 \in H_1 \Rightarrow f(h_1), f(h_2) \in H_2$
$h_1 h_2 \in H_1 \Rightarrow f(h_1 h_2) \in H_2$
$f(h_1 h_2) = f(h_1) f(h_2) \in H_2$
Verificando as propriedades de grupo
i) associativa
$f(a)[f(b)f(c)] = f(a)f(bc) = f(a(bc)) = f((ab)c) = f(ab)f(c) = [f(a)f(b)]f(c)$

ii) elemento neutro
$f(e)f(h) = f(eh) = f(he) = f(h)f(e) = f(h)$

iii) elemento inverso
$f(h)f(h^{-1}) = f(hh^{-1}) = f(h^{-1}h) = f(h^{-1})f(h) = f(e)$

c)
Há várias possíveis respostas, porém basta notar que em ambos os grupos qualquer elemento elevado a oito resulta na identidade e apenas para o segundo grupo qualquer elemento elevado a quatro resulta na identidade. Dessa forma, é impossível encontrar uma associação no segundo conjunto para o número 1, pois $1^4 = 4 \neq 0$

3. (2.0 pontos) Seja $(G,\cdot)$ um grupo finito e $(H,\cdot)$ um subgrupo de G. Definimos em $G \times G$ a relação ~ tal que $x \sim y$ se $x \cdot y^{-1} \in H$.

a) Mostre que ~ é uma relação de equivalência.

b) Determine em quantas classes de equivalência G é particionado e o tamanho de cada classe.

a)

i) reflexiva

$x \sim x \Leftrightarrow xx^{-1} = e \in H$, verdade porque H é grupo.

ii) simétrica

$x \sim y \Rightarrow xy^{-1} \in H$

$(xy^{-1})^{-1} \in H$ (existência do inverso)

$(xy^{-1})^{-1} = yx^{-1} \in H \Rightarrow y \sim x$

iii) transitiva

$x \sim y \Rightarrow xy^{-1} \in H$

$y \sim z \Rightarrow yz^{-1} \in H$

$(xy^{-1})(yz^{-1}) \in H \Rightarrow x(y^{-1}y)z^{-1} = xz^{-1} \in H \Rightarrow z \in H$

b)

sendo ~ uma relação de equivalência, é induzida uma partição em G em N conjuntos distintos e com intersecção nula:

$$| G | = \sum_{i=1}^{N} | G_i |$$

Dado um elemento x em G e o sub-grupo H,

Para cada elemento $h \in H$, existe um único y tal que $xy^{-1} = h$.

$x = hy \rightarrow y = h^{-1}x$

Esse y é único para cada h, pois

$y = h_1^{-1}x = h_2^{-1}x \Rightarrow h_1 = h_2$

Logo cada classe G_i possui exatos $| H |$ elementos

$$| G | = \sum_{i=1}^{N} | G_i | = N | H | \quad \rightarrow \quad N = \frac{| G |}{| H |}$$

4. (1.0 ponto) Seja τ_{ij} a permutação que faz apenas a troca da posição i com a posição j de forma que τ_{ii} é a identidade e $i, j \geq 1$.
Mostre por indução finita em N que a função $f_N : Z_2 \times Z_3 \times \cdots \times Z_N \to S_N$, definida por $f_N(i, j, k, ..., z) = \tau_{2(i+1)}\tau_{3(j+1)}\tau_{4(k+1)} \ldots \tau_{N(z+1)}$, é bijetora, onde S_N é o conjunto das permutações de N elementos.

Para **N=2**

$f_2 : Z_2 \to S_2$

$$f(0) = \tau_{21} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$f(1) = \tau_{22} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Esgotadas as possibilidades, a função é bijetora.

Supondo f_N bijetora, mostrar que f_{N+1} é bijetora.

$f_N(i, j, k, ..., z) = \tau_{2(i+1)}\tau_{3(j+1)}\tau_{4(k+1)} \ldots \tau_{N(z+1)}$ corresponde a todas permutações em S_N.

$f_{N+1}(i, j, k, ..., z, w) = f_N(i, j, k, ..., z)\tau_{(N+1)(w+1)}$ corresponde a trocar o elemento de índice N+1 de cada uma das permutações em S_N por um dos elementos de 1 até N definido por w+1 ou manter o N+1 sem trocar se w=N. Dessa forma, todas permutações em S_{N+1} podem ser construídas (já que inserimos um novo elemento de toda forma possível) e todas permutações construídas com índices distintos são distintas (verdadeiro por hipótese para os índices i...z e verdadeiro para w porque cada w gera uma permutação diferente das anteriores).