

(2) Find  $\{3,5\}$ .

$$[3,5] = \{(3,5), (1,3), (2,4)\}$$

(3) Compute  $A/R$ .

$$A/R = \{\{(5,1)\}, \{(4,2), (5,2)\}, \{(3,1), (4,2), (5,3)\}, \{(1,1), (2,2), (4,3), (5,4)\}, \{(1,2), (2,3), (3,4), (4,5)\}\}$$

4. [9 points] In the questions below find the matrix that represents the given relation. Use elements in the order given to determine rows and columns of the matrix.

a)  $R$  on  $\{-2, -1, 0, 1, 2\}$  where  $aRb$  means  $a^2 = b^2$ .

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

b)  $R^2$ , where  $R$  is the relation on  $\{1, 2, 3, 4\}$  such that  $aRb$  means  $|a - b| \leq 1$ .

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad M_{R^2} = M_R \otimes M_R = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

c)  $\bar{R}$ , where  $R$  is the relation on  $\{w, x, y, z\}$  such that

$$R = \{(w, w), (w, x), (x, w), (x, x), (x, y), (y, x), (z, z)\}.$$

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad M_{\bar{R}} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Page 3 of 10

5. [9 points] Let  $R$  be the relation on  $A = \{1, 2, 3, 4, 5\}$

$$\text{where } R = \{(1,1), (1,3), (1,4), (2,2), (2,1), (3,3), (3,4), (4,1), (4,3), (5,5)\}.$$

(1) Find the reflexive closure of  $R$ .

$$R = \{(1,1), (1,3), (1,4), (2,2), (2,1), (3,3), (3,4), (4,1), (4,3), (4,4), (5,5)\}$$

(2) Find the symmetric closure of  $R$ .

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (3,1), (3,3), (3,4), (4,1), (4,3), (4,4), (5,5)\}$$

(3) Use Warshall's algorithm to find the transitive closure of  $R$ .

$$M_R = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = W_0 \quad W_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = W_2 = W_3$$

$$W_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = W_4 \quad W_5 = W_4 \text{ is the transitive closure of } R$$

6. [4 points] Let  $(G, *)$  be a group with  $G = \{1, 2, 3, 4\}$ . Here is an incomplete operation table for  $*$ :

*	1	2	3	4
1	1	2	3	4
2	2	2	1	?
3	?	?	?	?
4	?	?	?	1

Redraw this table and fill the missing entries.

*	1	2	3	4
1	1	2	3	4
2	2	2	4	3
3	3	4	1	2
4	4	3	2	1

Page 4 of 10

7. [20 points] Let

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

be a parity check matrix.

(a) Determine the  $(3,6)$  group code  $e_H$ . (5 points)

$$e_H: \begin{aligned} e(000) &= 000000 \\ e(001) &= 001011 \\ e(010) &= 010110 \\ e(011) &= 011101 \\ e(100) &= 100100 \\ e(101) &= 101111 \\ e(110) &= 110010 \\ e(111) &= 111001 \end{aligned}$$

(b) Determine the number of errors that  $e_H$  will detect and its associated decoding function will correct. (2 points)

be the least weight of a nonzero code word is 2.  $e_H$  will detect 1 errors, its associated decoding function can not correct any error.

(c) Constructing a decoding table relative to a maximum likelihood decoding function associated with  $e_H$ . (5 points)

000000	001011	010110	011101	100100	101111	110010	111001
000001	000010	010111	011100	100101	101110	110001	111000
000010	000001	010100	011111	100110	101101	110000	111011
000011	000110	010000	011001	100010	101011	110011	111010
000100	000101	011110	010101	100111	101100	110000	111001
000101	000111	010001	011011	100011	101001	110011	111010
000110	000100	010011	011000	100001	101000	110000	111011
000111	000011	010000	011010	100000	101001	110001	111000
001000	001001	010010	011001	100011	101010	110000	111001
001001	001010	010001	011010	100000	101001	110001	111000
001010	001000	010011	011000	100010	101011	110000	111001
001011	001011	010000	011001	100001	101000	110001	111000
001100	001101	010001	011011	100011	101001	110000	111001
001101	001110	010010	011000	100010	101011	110001	111000
001110	001100	010011	011001	100001	101000	110001	111000
001111	001111	010000	011010	100000	101001	110001	111000

Page 5 of 10

(a) Decode the following words with the decoding table. (2 points)

$$\begin{aligned} a) & 011001 \rightarrow 011011 \\ b) & 101011 \rightarrow 101011 \\ c) & 100101 \rightarrow 100101 \\ d) & 011001 \rightarrow 011011 \\ e) & 101011 \rightarrow 101011 \\ f) & 100101 \rightarrow 100101 \end{aligned}$$

(c) Compute the syndrome for each coset leader found in (c). (3 points)

syndrome	coset leader
000	000000
001	000001
010	000010
100	000100
011	000101
101	000110
111	000111

(f) Decode the following words with the syndromes of coset leader. (3 points)

$$\begin{aligned} a) & \text{the syndrome of } 10101 \text{ is } 110, \text{ code word is } 111001 \\ b) & \text{the syndrome is } 101, \text{ code word is } 010110 \\ c) & \text{the syndrome is } 110, \text{ code word is } 100100 \end{aligned}$$

Page 6 of 10

130 points] Let  $N$  be a normal subgroup of a group, and let  $R$  be the following relation on  $G$ :

1)  $a \sim b$  if and only if  $a^{-1}b \in N$ .

2) Prove that  $R$  is a congruence relation on  $G$  and  $N$  is the equivalence class  $[e]$  relative to  $R$ .

3) Prove  $R$  is a congruence relation: 1)  $\forall x \in N, x^{-1} \in N$  because  $N$  is subgroup. 2)  $\forall x \in [e], x \in N$  because  $x = x \cdot e$  and  $e \in N$ .

4)  $a \sim b \iff a^{-1}b \in N$ . 5)  $a \sim b \iff a^{-1}b \in N$ . 6)  $a \sim b \iff a^{-1}b \in N$ . 7)  $a \sim b \iff a^{-1}b \in N$ . 8)  $a \sim b \iff a^{-1}b \in N$ . 9)  $a \sim b \iff a^{-1}b \in N$ . 10)  $a \sim b \iff a^{-1}b \in N$ .

11. (10 points) Consider a group  $Z_6$ , the operation table shown in following figure.

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

a) Find all of the normal subgroups of  $Z_6$  (4 points)

because  $Z_6$  is abelian group. all subgroups of  $Z_6$  are normal subgroups of  $Z_6$ .

$\{[0]\}$ ,  $\{[0], [3]\}$ ,  $\{[0], [2], [4]\}$ ,  $\{[0], [1], [2], [3], [4], [5]\}$  are normal subgroups of  $Z_6$ .

1) closed:  $\forall (a_1, b_1), (a_2, b_2) \in (ZXZ, \times)$   
 $(a_1, b_1) \times (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$   
 $a_1 + a_2 \in ZX$  and  $b_1 + b_2 \in Z$  so  $(a_1 + a_2, b_1 + b_2) \in (ZXZ, \times)$

2) commutative:  $\forall (a_1, b_1), (a_2, b_2) \in (ZXZ, \times)$   
 $(a_1, b_1) \times (a_2, b_2) = (a_1 + a_2, b_1 + b_2) = (a_2 + a_1, b_2 + b_1) = (a_2, b_2) \times (a_1, b_1)$

3)  $(0, 0)$  is the identity element

4)  $\forall (a_1, b_1) \in (ZXZ, \times)$   $(-a_1, -b_1) \in (ZXZ, \times)$   
 $(a_1, b_1) \times (-a_1, -b_1) = (a_1 - a_1, b_1 - b_1) = (0, 0)$

5)  $\forall (a_1, b_1), (a_2, b_2) \in (ZXZ, \times)$   
 $(a_1, b_1) \times (a_2, b_2) = (a_1 + a_2, b_1 + b_2) = (a_2 + a_1, b_2 + b_1) = (a_2, b_2) \times (a_1, b_1)$

so  $(ZXZ, \times)$  is an abelian group

b) Describe a congruence relation  $R$  on  $Z_6$  and find a corresponding normal subgroup from (a). (3 points)

$a \sim b$  if and only if the remainder of  $a$  divides six is the same as the remainder of  $b$  divides six.

$\forall [a], [b] \in Z_6, [a] \sim [b] \iff a \equiv b \pmod{3}$

c) For this congruence relation  $R$  in (b), Write the operation table of quotient group  $Z_6/R$ . (3 points)

$Z_6/R = \{[0], [1], [2]\}$

$A = \{[0], [1], [2]\}$

$Z_6/R = \{[0], [1], [2]\}$

$\oplus$	$\{[0]\}$	$\{[1]\}$	$\{[2]\}$	$\{[3]\}$	$\{[4]\}$	$\{[5]\}$
$\{[0]\}$	$\{[0]\}$	$\{[1]\}$	$\{[2]\}$	$\{[3]\}$	$\{[4]\}$	$\{[5]\}$
$\{[1]\}$	$\{[1]\}$	$\{[2]\}$	$\{[3]\}$	$\{[4]\}$	$\{[5]\}$	$\{[0]\}$
$\{[2]\}$	$\{[2]\}$	$\{[3]\}$	$\{[4]\}$	$\{[5]\}$	$\{[0]\}$	$\{[1]\}$
$\{[3]\}$	$\{[3]\}$	$\{[4]\}$	$\{[5]\}$	$\{[0]\}$	$\{[1]\}$	$\{[2]\}$
$\{[4]\}$	$\{[4]\}$	$\{[5]\}$	$\{[0]\}$	$\{[1]\}$	$\{[2]\}$	$\{[3]\}$
$\{[5]\}$	$\{[5]\}$	$\{[0]\}$	$\{[1]\}$	$\{[2]\}$	$\{[3]\}$	$\{[4]\}$

isomorphism to  $Z_3$

