NATIONAL UNIVERSITY OF SINGAPORE

CS1231 - DISCRETE STRUCTURES

(Semester 1: AY2017/18)

Time Allowed: 2 Hours

INSTRUCTIONS TO CANDIDATES

1. This assessment paper contains **EIGHTEEN (18)** questions in **TWO (2)** parts and comprises **THIRTEEN (13)** printed pages, including this page.
2. Answer **ALL** questions.
3. This is an **OPEN BOOK** assessment.
4. You are allowed to use **NUS APPROVED CALCULATORS**.
5. You are to submit two documents: The **OCR form** and the **Answer Sheet**. You may keep this question paper.
6. **Shade** and **write** your **Student Number** completely and accurately on the OCR form.
7. You must use 2B pencil for the OCR form.
8. **Write** your **Student Number** on the Answer Sheet. **Do not write your name.**
9. You may use pen or pencil to write your answers, but please erase cleanly, and write legibly. Marks may be deducted for illegible handwriting.

Part A: (30 marks) MCQ. Answer on the OCR form.

For each multiple choice question, choose the best answer and **shade** the corresponding choice on the OCR form. Remember to **shade** and **write** your **Student Number** (check that it is correct!) on the OCR form. Each multiple choice question is worth 2 marks. No mark is deducted for wrong answers. You should use a **2B pencil**.

Q1. Given four words "eye", "can", "zoo" and "eat", in how many ways can you arrange these words and the letters within each word?

A. $4! \times 3^2 \times 6^2$
B. $4! \times 6^4$
C. $4 \times 3^2 \times 6^2$
D. $4! \times 3!$
E. $12!$

Q2. In how many ways can you pair up 8 boys and 8 girls?
(A pair consists of a boy and a girl.)

A. 8^2
B. $8!$
C. $4! + 4!$
D. $8! + 8!$
E. $16!$

Q3. Given the predicates below:

$$M(x) = (\ x \text{ is a male student }).$$
$$F(x) = (\ x \text{ is a female student }).$$
$$CM(x,y) = (\ x \text{ and } y \text{ take a common module }).$$

Which of the following quantified statements means "Every female student takes some common module with every male student"? (The domain is the set of all students and is omitted in the quantified statements below.)

(I). $\forall x \forall y\ (\ M(x)\ \wedge\ F(y)\ \rightarrow\ CM(x,y)\ )$.
(II). $\forall x\ (\ F(x)\ \rightarrow\ \forall y\ (\ M(y)\ \wedge\ CM(x,y)\ )\ )$.
(III). $\forall x\ (\ F(x)\ \rightarrow\ \forall y\ (\ M(y)\ \rightarrow\ CM(x,y)\ )\ )$.
(IV). $\forall x \forall y\ (\ M(x)\ \wedge\ F(y)\ \wedge\ CM(x,y)\ )$.

A. (I) only.
B. (IV) only.
C. (I) and (III) only.
D. (II) and (IV) only.
E. None of A, B, C, or D.

Q4. Given the following three pairs of graphs:

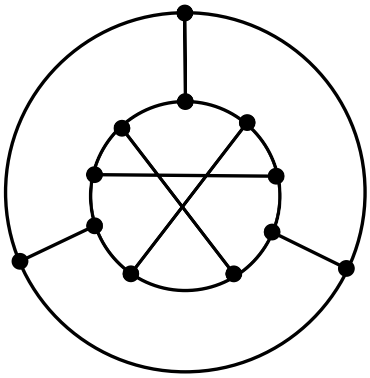


Figure 1A

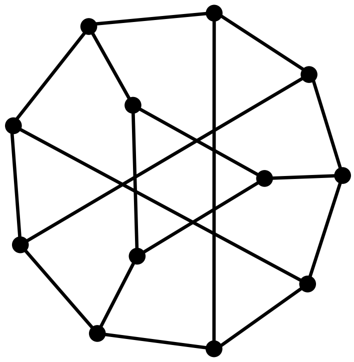


Figure 1B

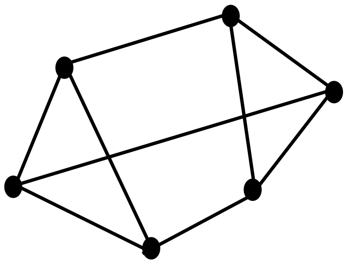


Figure 2A

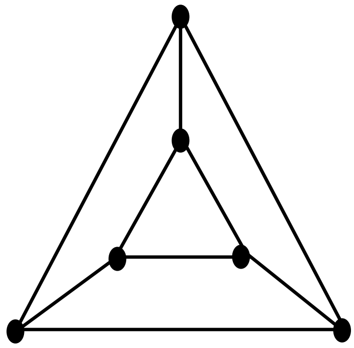


Figure 2B

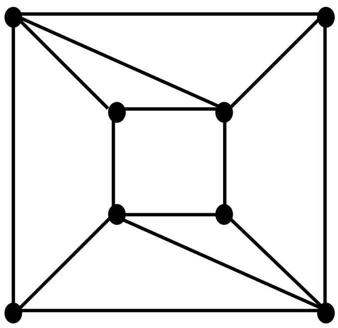


Figure 3A

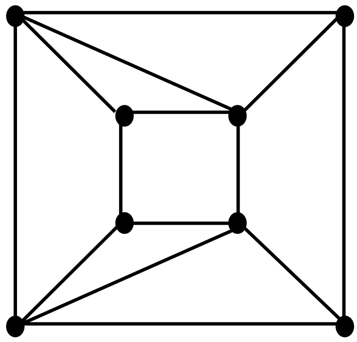


Figure 3B

Which of the following statements are TRUE?

(I). The graphs in Figures 1A and 1B are isomorphic.

(II). The graphs in Figures 2A and 2B are isomorphic.

(III). The graphs in Figures 3A and 3B are isomorphic.

A. (I) only.

B. (II) only.

C. (I) and (II) only.

D. (II) and (III) only.

E. All of (I), (II) and (III).

Q5. Which of the following statements are TRUE?

(I). The Tietze's graph shown in Figure 1A in Q4 is an Eulerian graph.
(II). The number of edges in a complete graph K_n is $n^2/2$.
(III). If a simple connected graph on n vertices does not contain a cycle, then it must have exactly $n-1$ edges.

A. (I) only.
B. (II) only.
C. (III) only.
D. All of (I), (II) and (III).
E. None of (I), (II) and (III).

Q6. In a game of chance, you are required to draw one ball from a bag containing 4 red balls, 7 green balls, and 9 blue balls. You win \$20 if you draw a red ball, \$15 if you draw a green ball, or nothing if you draw a blue ball. You pay \$10 for each game. After each game, the ball drawn is returned to the bag.

If Aiken plays this game 100 times, how much would you expect her to lose?

A. \$9.25.
B. \$75.
C. \$92.50.
D. \$100.
E. None of the above.

Q7. Figure 4 below shows a graph on three vertices. Define $W3(v_i)$ to be the number of walks of length 3 from vertex v_i to itself.

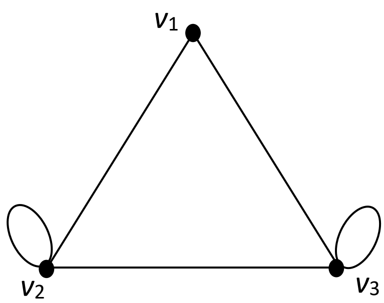


Figure 4

Which of the following is TRUE?

A. $W3(v_1) = 2; W3(v_2) = 2; W3(v_3) = 2$.
B. $W3(v_1) = 4; W3(v_2) = 6; W3(v_3) = 6$.
C. $W3(v_1) = 4; W3(v_2) = 6; W3(v_3) = 8$.
D. $W3(v_1) = 4; W3(v_2) = 8; W3(v_3) = 8$.
E. None of the above.

Q8. Let X, Y be two finite sets with m and n elements, respectively. Which of the following statements is FALSE?

(I). For $m = n$, there are $n!$ different bijective functions from X to Y.

(II). For $m = 6, n = 3$, there are 120 different one-to-one functions from X to Y.

(III). For $m = 5, n = 2$, there are 30 different surjective functions from X to Y.

(IV). For $m = 4, n = 5$, there are 120 different injective functions from X to Y.

A. (I) only.

B. (II) only.

C. (I) and (II) only.

D. (II), (III) and (IV) only.

E. All of (I), (II), (III) and (IV) are FALSE.

The next 7 questions (Q9 to Q15) refer to the following definitions.

Definition 1. *A **Group**, denoted $(G, *)$, is a set G along with a binary operator $*$ that satisfies these four axioms:*

(A1)	*Closure:*	$\forall a, b \in G,\ a * b \in G.$
(A2)	*Associativity:*	$\forall a, b, c \in G,\ (a * b) * c = a * (b * c).$
(A3)	*Identity:*	$\exists e \in G$ *such that* $\forall a \in G,\ a * e = e * a = a.$
(A4)	*Inverse:*	$\forall a \in G,\ \exists b \in G$ *(called the **inverse** of a) such that* $a * b = b * a = e.$

Remarks:

1. It is usual to write ab to mean $a * b$.
2. Because of Associativity, there is no ambiguity in writing abc, since the result is the same whichever way it is evaluated.
3. The element $e \in G$ is called the **identity element**, or simply **identity**.
4. The inverse of a is usually denoted a^{-1}.

Definition 2. *If G is finite with $m \in \mathbb{Z}^+$ elements, then the **group order** of G is said to be m. For small m, it is often helpful to see the group as a **Cayley table**. Let $a_1, a_2, \ldots, a_m$ be the elements of G, then each entry, c_{ij} in the $m \times m$ Cayley table is defined as $c_{ij} = a_i a_j$, for $i, j = 1, 2, \ldots, m$ (see Table 1(a) on page 6.)*

An example of a group is $(\{\textbf{true}, \textbf{false}\}, \oplus)$. Its Cayley table is shown in Table 1(b). As you may recall, $\oplus$ is the logical *exclusive-OR* binary operator, which evaluates to **true** when both its inputs are different, and **false** otherwise.

To check whether this is a group, let's see if it satisfies the four axioms. Closure is obvious from the table, and Associativity is guaranteed by the $\oplus$ operator. From the table, the *identity* is **false**, because **true** $\oplus$ **false** $=$ **true** , and **false** $\oplus$ **false** $=$ **false**, thus satisfying Axiom (A3). The last equality also means that **false** is its own inverse; while **true** $\oplus$ **true** $=$ **false** means that **true** is its own inverse too. Thus, $(\{\textbf{true}, \textbf{false}\}, \oplus)$ is a group since it satisfies all 4 axioms.

$*$	a_1	$\dots$	a_j	$\dots$	a_m
a_1					
$\vdots$			$\vdots$		
a_i		$\dots$	c_{ij}	$\dots$	
$\vdots$			$\vdots$		
a_m					

(a) General Cayley table

$\oplus$	**true**	**false**
true	**false**	**true**
false	**true**	**false**

(b) Cayley table for $(\{\mathbf{true}, \mathbf{false}\}, \oplus)$

Table 1: Cayley tables.

Another example of a group is the familiar $(\mathbb{Z}, +)$, that is, the set of integers with the usual addition operator. Closure and Associativity are true for integers under addition, and thus axioms (A1) and (A2) are satisfied. The *identity* is 0, since $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$. Finally, for each $a \in \mathbb{Z}$, its inverse is $-a$, since $a + (-a) = (-a) + a = 0$. Thus, $(\mathbb{Z}, +)$ is a group. But since $\mathbb{Z}$ is infinite, it is not possible to draw its Cayley table.

Q9. Which of the following is a group?

A. $(R, \circ)$, where $R = \{R_{120}, R_{240}, R_{360}\}$, and R_θ means "rotate an equilateral triangle[1] θ degrees clockwise around its center O" (see Figure 5), and $\circ$ means function composition, ie. $R_{\theta_2} \circ R_{\theta_1}$ means "rotate clockwise by θ_1, followed by θ_2". Its Cayley table is shown below:

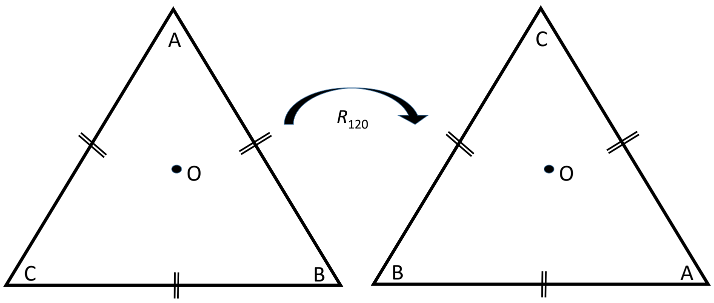


Figure 5: Rotation of an equilateral triangle by R_{120}.

$\circ$	R_{120}	R_{240}	R_{360}
R_{120}	R_{240}	R_{360}	R_{120}
R_{240}	R_{360}	R_{120}	R_{240}
R_{360}	R_{120}	R_{240}	R_{360}

B. $(\mathbb{Z}, \times)$, that is, the set of integers with the multiplication operator.

C. $(\{\mathbf{true}, \mathbf{false}\}, \vee)$, whose Cayley table is:

$\vee$	**true**	**false**
true	**true**	**true**
false	**true**	**false**

D. All of the above.

E. None of the above.

[1]An equilateral triangle is a triangle in which all 3 sides have equal length, and all 3 angles are $60°$.

Q10. Define three functions as follows:

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \quad \forall x \in \mathbb{R}, \quad f(x) = x + 1.$$
$$g : \mathbb{R} \longrightarrow \mathbb{R}, \quad \forall x \in \mathbb{R}, \quad g(x) = x - 1.$$
$$h : \mathbb{R} \longrightarrow \mathbb{R}, \quad \forall x \in \mathbb{R}, \quad h(x) = x.$$

Let $F = \{f, g, h\}$, and let $\circ$ denote function composition, ie. $(f \circ g)(x) = f(g(x))$.

Then, $(F, \circ)$ is *not* a group because:

(I) The Closure property is not satisfied. (II) $\circ$ is not associative.
(III) There is no identity element in F. (IV) Not every element in F has an inverse.

A. (I) only.
B. (IV) only.
C. (I) and (IV) only.
D. (II), (III) and (IV) only.
E. None of A, B, C or D.

Q11. Given a group $(G, *)$, and from the 4 group axioms (A1) to (A4) alone, it is possible to deduce that all the following statements are true, EXCEPT:

A. (Left cancellation law:) $\forall a, b, c \in G,\ (ab = ac) \rightarrow (b = c)$.
B. (Uniqueness of inverse:) $\forall a, b, b' \in G,\ ((ab = ba = e) \wedge (ab' = b'a = e)) \rightarrow (b = b')$.
C. $\forall a, b \in G$, it is always possible to solve for $x \in G$ in $ax = b$.
D. In each row of the Cayley table of G, every $x \in G$ appears *exactly* once.
E. (Commutative law:) $\forall a, b \in G,\ ab = ba$.

Definition 3. *Given a group $(G, *)$, and any $x \in G$, define* ***powers*** *of x recursively as follows:*

$$x^n = \begin{cases} e \text{ (identity)}, & \text{if } n = 0, \\ x * x^{n-1}, & \text{if integer } n > 0, \\ x^{-1} * x^{n+1}, & \text{if integer } n < 0. \end{cases}$$

This means the usual power law holds: $x^{m+n} = x^m * x^n$ and $(x^m)^n = x^{mn}$, $\forall m, n \in \mathbb{Z}$.

Definition 4. *For any $x \in G$, let k be the smallest positive integer, if such a k exists, such that $x^k = e$, then the* ***element order*** *of x is said to be k.*

Define $G_1 = \{1, 2, 3, 4\}$ and define $*$ so that $a * b = a \times b \ mod\ 5$, for all $a, b \in G_1$. In other words, $a * b$ computes the remainder of $a \times b$ when divided by 5. Consider the group $(G_1, *)$, whose Cayley table is shown in Table 2.

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

Table 2: Cayley table for $(G_1, *)$.

It is easy to verify that $(G_1, *)$ is indeed a group. Note that $4^3 = 4 * 4 * 4 = 1 * 4 = 4$. Note also that the element order of 2 is 4, since $2^4 = 2 * 2 * 2 * 2 = 4 * 4 = 1$, and 4 is the smallest positive integer such that $2^4 = 1$.

Q12. Using the Cayley table for $(G_1, *)$, what is 2^{-1} ?

A. $\frac{1}{2}$

B. 1

C. 2

D. 3

E. 4

Q13. Using the Cayley table for $(G_1, *)$, what is the element order of 4?

A. 1

B. 2

C. 3

D. 4

E. None of the above.

Q14. Using the Cayley table for $(G_1, *)$, solve $3x^2 = 1$.

A. $1/\sqrt{3}$

B. 1

C. 2

D. $\sqrt{2}$

E. There is no solution.

Q15. Using the Cayley table for $(G_1, *)$, determine $3^{4^{5^{6^7}}}$.
(Note that powers are right-associative: a^{b^c} means $a^{(b^c)}$.)

A. 1

B. 2

C. 3

D. 4

E. There is no solution.

Part B: (40 marks) Structured questions. Write your answer in the Answer Sheet. Marks may be deducted for illegible handwriting and unnecessary statements in proofs.

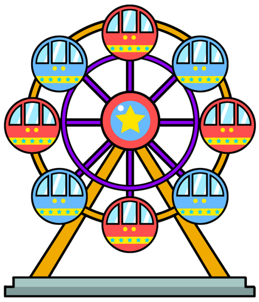
Q16. (14 marks) **Counting and Probability.**

(a) (7 marks) Answer the following parts. Working is not required.

i. (2 marks) How many integer solutions are there for the following equation, where each $x_i \geq 1$?

$$x_1 + x_2 + x_3 = 10$$

ii. (2 marks) Assume that each cabin on a ferris wheel can carry only one person. In how many ways can you arrange 30 people on a ferris wheel with 30 cabins? In how many ways can you arrange 29 people on a ferris wheel with 30 cabins?



iii. (3 marks) Dueet is known to speak the truth two out of three times. He throws a fair, six-sided die and reports that it shows a 6. What is the probability that the number shown on the die is really 6? (Write your answer as a simple fraction.)

(b) (3 marks) Prove that two consecutive positive integers are co-prime, that is, $\forall x \in \mathbb{Z}^+$, x and $x + 1$ are co-prime.

(c) (4 marks) Using the Pigeonhole Principle (other proofs will not be accepted), prove that if we take $n + 1$ numbers from the set $\{1, 2, 3, ..., 2n\}$, then some pair of numbers will be co-prime.

Q17. (14 marks) **Trees and Graphs.**

(a) (3 marks) Based on the postorder traversal and inorder traversal of a binary tree with vertices A, B, C, D, E, F, G and H as given below, draw the binary tree.

Postorder:	F	C	E	H	D	A	B	G
Inorder:	C	F	G	E	D	H	B	A

(b) (6 marks) The Dijkstra's Shortest Path Algorithm is shown below. G, shown below, is a connected simple graph with a positive weight for every edge, a is the starting vertex and z the ending vertex. The function $w(u, v)$ denotes the weight for the edge connecting vertices u, v. The notation "$x := y$" means assign the value of y to variable x.

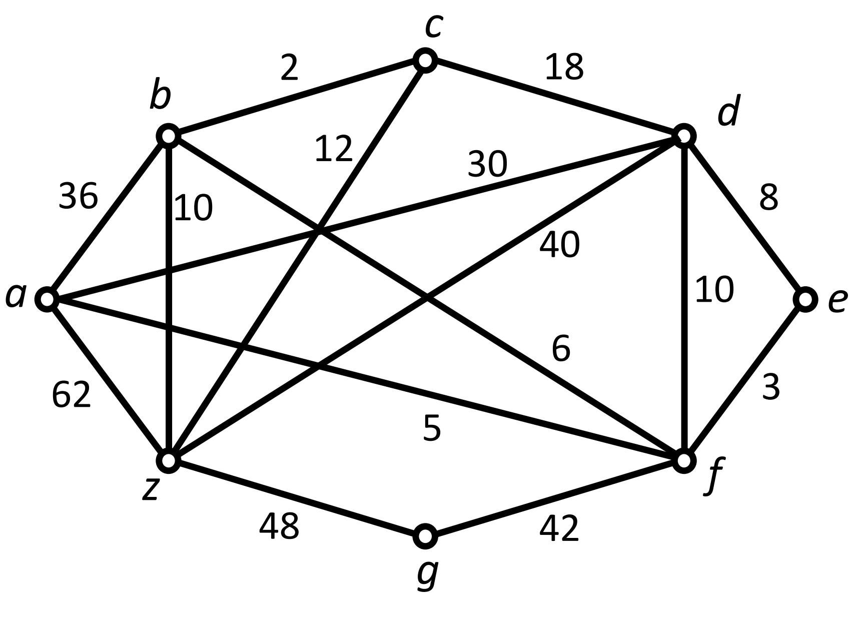
Dijkstra's Algorithm

Input: Graph G, with starting vertex a, ending vertex z.

Output: $L(z)$, the length of the shortest path from a to z.

1. Initialize T to be the graph with vertex a and no edges. Let $V(T)$ be the set of vertices in T, and let $E(T)$ be the set of edges of T.
2. Let $L(a) := 0$, and for all vertices x in G except a, let $L(x) := +\infty$. (The number $L(x)$ is called the label of x.)
3. Let $v := a$ and $F := \{a\}$.
4. **while** $(z \notin V(T))$
   - 4.1. $F := (F - \{v\}) \cup \{$vertices that are adjacent to v and are not in $V(T)\}$
   - 4.2. For each vertex u that is adjacent to v and is not in $V(T)$
     - 4.2.1. **if** $L(v) + w(v, u) < L(u)$ **then**
       - 4.2.1.1. $L(u) := L(v) + w(v, u)$
       - 4.2.1.2. $D(u) := v$
   - 4.3. Find a vertex x in F with the smallest label.
   - 4.4. Add vertex x to $V(T)$, and add edge $\{D(x), x\}$ to $E(T)$.
   - 4.5. $v := x$

end while



Run Dijkstra's algorithm on the graph shown above.

i. (2 marks) What is the shortest distance from a to z?

ii. (4 marks) Write out the final $V(T)$, with the vertices arranged in order of their addition into $V(T)$ according to the above algorithm. The first vertex and the last vertex are of course a and z, respectively.

(c) (5 marks) Suppose you are given a pile of n stones. At each step, you are allowed to separate a pile of k stones into two piles of k_1 and k_2 stones. Obviously, $k_1 + k_2 = k$. On doing this, you earn $k_1 \times k_2$ dollars.

What is the maximum amount of money you can earn starting with a pile of n stones? Explain your answer.

Q18. (12 marks) **Group Theory.** (Please refer to the Group Definitions 1 to 4 given on pages 5 and 7.) We make one more definition.

Definition 5. *Two groups, $(G, *)$ and $(H, \odot)$, are said to be* ***isomorphic****, if and only if, there exists a bijection $f : G \longrightarrow H$ such that:*

(Isomorphic property:) $\forall x, y \in G,\ f(x * y) = f(x) \odot f(y).$

Note that in the left hand side of the above equation, the binary operator is that of G, while the right hand side's binary operator is that of H. As long as we keep this in mind, we may re-write the property as:

(Isomorphic property:) $\forall x, y \in G,\ f(xy) = f(x)f(y).$

We write $G \cong H$ to denote the fact that groups $(G, *)$ and $(H, \odot)$ are isomorphic.

Isomorphic groups are, as you may have guessed, "equal" to each other, in the sense that one group $(H, \odot)$ may be obtained from the other group $(G, *)$ by:

(i) renaming the elements in G to those in H, and

(ii) renaming the binary operator $*$ to $\odot$,

in such a way that their Cayley tables agree. The bijection f, with the isomorphic property, captures this renaming mathematically.

Define two groups, $(G_2, \times)$, and $(G_3, \bullet)$ by their Cayley tables shown below:

$\times$	1	i	$-i$	-1
1	1	i	$-i$	-1
i	i	-1	1	$-i$
$-i$	$-i$	1	-1	i
-1	-1	$-i$	i	1

(a) $(G_2, \times)$, where $i = \sqrt{-1}$.

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(b) $(G_3, \bullet)$.

Table 3: Cayley tables.

(a) (2 marks) Compare groups $(G_1, *)$ (defined in Table 2, on page 8), and $(G_2, \times)$ above. It should be obvious that $G_1 \cong G_2$. Find the bijection $f : G_1 \longrightarrow G_2$ with the isomorphic property that establishes the isomorphism.

(b) (2 marks) Now compare $(G_2, \times)$ with $(G_3, \bullet)$. Explain why $G_2 \not\cong G_3$, ie. they are not isomorphic. (Do not say "because no bijection exists"; instead, explain using some property of the elements of the groups.)

(c) (4 marks) Let's show that $\cong$ is an equivalence relation on S, the set of groups. It is straightforward to prove reflexivity and transitivity:

Proof (Reflexivity).

1. Take any group $g \in S$.
2. The identity function $I_g : g \longrightarrow g$ such that $I_g(x) = x, \forall x \in g$, is a bijection, by Q3(a), Assignment #2.
3. Also, clearly, $\forall x, y \in g,\ I_g(xy) = xy = I_g(x)I_g(y)$, by definition of I_g.
4. Thus, I_g has the isomorphic property.
5. Hence $g \cong g$, and $\cong$ is reflexive. ■

Proof (Transitivity).

1. Take any three groups $g, h, i \in S$.
2. Suppose $g \cong h$ and $h \cong i$:
   - 2.1. Then $\exists r : g \longrightarrow h$ which is a bijection with the isomorphic property, by definition of isomorphism.
   - 2.2. Then $\exists s : h \longrightarrow i$ which is a bijection with the isomorphic property, by definition of isomorphism.
   - 2.3. Then $s \circ r : g \longrightarrow i$ is also a bijection, by Theorems 7.3.3, 7.3.4 (Epp).
   - 2.4. (To prove isomorphic property:) Take any $x, y \in g$.
   - 2.5. Then, $s \circ r(x)\, s \circ r(y) = s(r(x))s(r(y))$, by definition of $\circ$.
   - 2.6. $= s(r(x)r(y))$, by the isomorphic property of s.
   - 2.7. $= s(r(xy))$, by the isomorphic property of r.
   - 2.8. $= s \circ r(xy)$, by definition of $\circ$.
   - 2.9. Thus $s \circ r$ has the isomorphic property.
   - 2.10. Thus, $g \cong i$.
3. Hence $\cong$ is transitive. ■

Notice that in these proofs, we needed to (i) find the bijection, and (ii) prove that it possess the isomorphic property. Complete the proof below that $\cong$ on S is symmetric. Fill in the missing 3 (at most 4) steps from Lines 2.5. to 2.8. If you exceed 4 steps, 0 marks will be given. Be sure to justify each step.

Proof (Symmetry).

1. Take any two groups $g, h \in S$.
2. Suppose $g \cong h$:
   - 2.1. Then $\exists f : g \longrightarrow h$ which is a bijection with the isomorphic property, by definition of isomorphism.
   - 2.2. Then $f^{-1} : h \longrightarrow g$ is also a bijection, by Theorem 7.2.3 (Epp).
   - 2.3. (To prove that f^{-1} has the isomorphic property:)
   - 2.4. Take any $x, y \in h$.
   - 2.5.
   - 2.6.
   - 2.7.
   - 2.8. (Optional)
   - 2.9. Thus f^{-1} has the isomorphic property.
   - 2.10. Thus $h \cong g$.
3. Hence $\cong$ is symmetric. ■

(d) (4 marks) Prove that for any group $(G, *)$, with identity element e, if G is finite, then $\forall x \in G,\ \exists n \in \mathbb{Z}^+$ such that $x^n = e$.

END OF PAPER