

Mathematics HL

Topic 8

Sets, Relations and Groups



ANSWERS

Györgyi Bruder
William Larson

ANSWERS

Chapter 1 – Sets

Exercise 1.1

a, b, c are true. d, e, f and g are false

Exercise 1.2

A, C, E are finite. $n(A) = 8$, $n(C) = 1$. B and D are infinite sets.

Exercise 1.3

a, b, d, f and g are true. (“{2}” is the set containing the number 2, which is not the same as “2”.)

Exercise 1.4

a. $A = \{-1, 0, 1, 2, 3, 4\}$, $B = \{\text{Thursday, Tuesday}\}$, $C = \{-1, 1\}$,

$D = \{\text{cube roots of unity}\} = \left\{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}$, $E = \emptyset$, the empty set,

Since F is an infinite set, its elements cannot be listed. $F = \{x \mid 1 \leq |x|\}$.

b. $2 \in A$, F , $2 \notin B, C, D, E$.

c. $n(A) = 6$, $n(B) = 2$, $n(C) = 2$, $n(D) = 0$, $n(E) = 3$.

Exercise 1.5

1. $\emptyset, \{a\}, \{b\}, \{a, b\}$.

2. $\emptyset, \{1\}, \{3\}, \{7\}, \{1, 3\}, \{1, 7\}, \{3, 7\}, \{1, 3, 7\}$.

3. $\emptyset, \{1\}, \{3\}, \{7\}, \{1, 3\}, \{1, 7\}, \{3, 7\}$.

Exercise 1.6

$A' = \{-7, 8, 11, 12\}$.

Exercise 1.7

1. Proof: $A \cup (B \cap A') = A \cup (B' \cup A) = A \cup B' \cup A = A \cup B'$

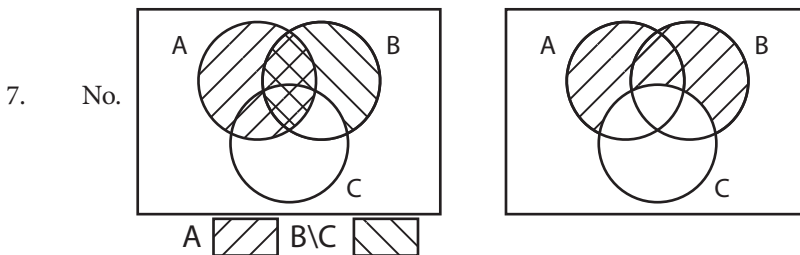
2. Proof: $((A \cap B)' \cup B)' = (A \cap B) \cap B' = (A \cap B) \cap B' = A \cap (B \cap B') = A \cap \emptyset = \emptyset$.

Exercise 1.8

$$\text{LHS} = (A \cup B) \setminus (A \cap B) = A \Delta B; \text{RHS} = (A \cap B') \cup A' \cap B = (A \setminus B) \cup (B \setminus A) = A \Delta B = \text{LHS: QED}$$

Exercise 1.9

1. a. $\{a, b\}$ b. $\{e\}$ c. 2
- d. 1 e. $\{a, b, e\}$ f. 3
- g. A h. $\{e, c, d\}$ i. $\{c, d\}$
- j. $\{e\}$
2. $\{1, 3, 4, 5\}$ has $2^4 = 16$ subsets. Adding "2" to each of these sets gives all of the subsets of A with "2" as an element, hence the answer is 16.
3. $A \cap (A \cup B)' \cap (B \cup A') = A \cap (B \cup A') = (A \cap B) \cup (A \cap A') = (A \cap B) \cup \emptyset = A \cap B.$
4. $[(A \cup B) \cap (A \cup B')] \cup [(A' \cup B) \cap (A' \cup B')]$
 $= [(A \cup (B \cap B'))] \cup [(A' \cup (B \cap B'))] = [(A \cup \emptyset) \cup [A' \cup \emptyset]] = A \cup A' = U.$
5. $[[A \cup (B \cap C')] \cap [B \cup (A \cap C)']]' = [A \cup (B \cap C')] \cup [B \cup (A \cap C)'] = [A' \cap (B' \cup C'')] \cup [B' \cap (A' \cup C'')]$
 $= [A' \cap (B' \cup C)] \cup [B' \cap (B' \cup A')] = [(A' \cap B') \cup (A' \cap C)] \cup [(B' \cap A') \cup (B' \cap C)]$
 $= (A' \cap B') \cup (A' \cap C) \cup (B' \cap A') \cup (B' \cap C) = (A' \cap B') \cup (A' \cap C) \cup (B' \cap C).$
6. $A \setminus (A \cap B) = A \cap (A \cap B)' = A \cap (A' \cup B') = (A \cap A') \cup (A \cap B') = \emptyset \cup (A \cap B') = A \cap B' = A \setminus B.$



Or use a counterexample. Let $A = \{a, b, c, d\}$, $B = \{c, d\}$, $C = \{c\}$

$$B \setminus C = \{d\} \quad A \cup (B \setminus C) = \{a, b, c, d\} \quad (A \cup B) \setminus C = \{a, d\}. \text{ So } A \cup (B \setminus C) \neq (A \cup B) \setminus C.$$

8. Venn diagrams suggest that this is true: $B \cap (A \setminus B) = B \cap (A \cap B') = (B \cap B') \cap A = \emptyset \cap A = \emptyset$

9. $(A \Delta B) \cup (A \cap B) = (A \setminus B) \cup (B \setminus A) \cup (A \cap B) = ((B \setminus A) \cup (A \cap B))$
 $= [(A \cup B) \cap (A \cup A') \cap (B' \cup B) \cap (B' \cup A')] \cup (A \cap B) = [(A \cup B) \cap \bar{A} \cap \bar{B} \cap (B' \cup A')] \cup (A \cap B)$
 $= [(A \cup B) \cap (B' \cup A')] \cup (A \cap B) = [(A \cup B) \cap (B \cap A)'] \cup (A \cap B) = \bar{A} \cup (A \cup B) = A \cup B.$
10. $A \Delta (A \setminus B) = A \Delta (A \cap B') = [A \setminus (A \cap B')] \cup [(A \cap B') \setminus A] = [A \cap (A \cap B')'] \cup [(A \cap B') \cap A']$
 $= [A \cap (A \cup B'')] \cup [(A \cap A') \cap B'] = [A \cap (A' \cup B)] \cup [\emptyset \cap B'] = [(A \cap A') \cup (A \cap B)] \cup \emptyset = \emptyset \cup (A \cap B)$
 $= A \cap B$
11. $A \Delta (A \cap B) = [A \cup (A \cap B)'] \setminus [A \cap (A \cap B)]$
 $[A \cup (A \cap B)] \cap [(A \cap A) \cap B]' = [A \cup (A \cap B)] \cap [A \cap B]' = A \cap [A \cap B]' = A \cap [A' \cup B']$
 $= (A \cap A') \cup (A \cap B') = \emptyset \cup [A \cap B'] = A \cap B' = A \setminus B.$

IB Exam Type Problems

1. We will show that $A \subseteq B$.

Let $x \in A$

$x \in A \cup B$ if x is in A , it must be in $A \cup$ anything

$x \in A \cap B$ given

$x \in B$ if x is in $A \cap B$, it must be in B

$A \subseteq B$

We will show that $B \subseteq A$.

Let $x \in B$

$x \in A \cup B$ if x is in B , it must be in $B \cup$ anything

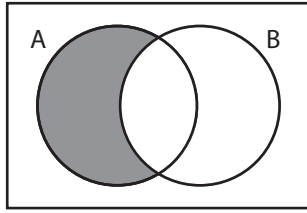
$x \in A \cap B$ given

$x \in A$ if x is in $A \cap B$, it must be in A

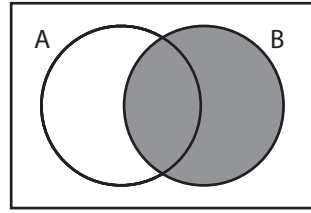
$B \subseteq A$

Since $A \subseteq B$ and $B \subseteq A$, $A = B$.

2. The Venn diagrams are



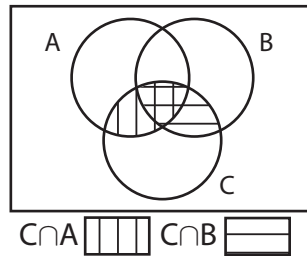
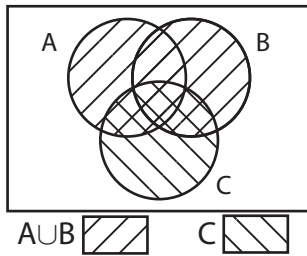
$A \setminus B$



$B \setminus A$

$B \cap (A \setminus B) = \emptyset$, but $B \cap (B \setminus A) = B \setminus A$, so they are not equal

3.



$C \cap (A \cup B)$ is the doubly shaded region. $(C \cap A) \cup (C \cap B)$ is region with any shading.

The two regions are the same.

4. a. $((X \cup Y) \cap (X' \cup Y'))' = (X \cup Y)' \cup (X' \cup Y')' = (X' \cap Y') \cup (X \cap Y)$

b. LHS = $A \cap (B \cup C)' = A \cap B' \cap C'$

RHS = $(A \setminus B) \cap (A \setminus C) = (A \cap B') \cap (A \cap C') = A \cap B' \cap C'$

LHS = RHS

c. LHS = $(A \cup B) \cap (A \cup B) = RHS$

d. LHS = $(A \cap B) \cap (A \cap C)' = (A \cap B) \cap (A' \cup C') = ((A \cap B) \cap A') \cup ((A \cap B) \cap C')$

$= (A \cap B \cap A') \cup (A \cap B \cap C') = \emptyset \cup (A \cap B \cap C') = A \cap B \cap C' = A \cap (B \setminus C) = RHS$

e. LHS = $((A \cup C) \cap (A \cup B))' \cup ((A \cup B) \cap (A \cup C))' = ((A \cup C) \cap (A' \cap B')) \cup ((A \cup B) \cap (A' \cap C'))$

$= [(A \cap (A' \cap B')) \cup (C \cap (A' \cap B'))] \cup [(A \cap (A' \cap C')) \cup (B \cap (A' \cap C'))]$

$= \emptyset \cup (C \cap (A' \cap B')) \cup \emptyset \cup (B \cap (A' \cap C')) = (A' \cap B' \cap C) \cup (A' \cap B \cap C') = RHS$

RHS = $C \cap (A \cup B)' \cup (B \cap (A \cup C))' = (C \cap (A' \cap B')) \cup (B \cap (A' \cap C')) = A' \cap B' \cap C \cup A' \cap B \cap C'$

Exercise 2.1

- a) $12R3$, b) $3R12$, c) $1R4$, $1R1$, $4R6$, $5R6$.
- a) $0R4$, b) $12R4$, c) $4R4$ and $4R-6$, $0R12$, $-1R12$.
- a) $(3, 4)R(0, 4)$, b) $(3, 4)R(3, 4)$, c) $R = \{((3, 4), (3, 4)), ((0, 4), (0, 4)), ((7, 23), (7, 23))\} (0, 4)R(7, 23), (0, 4)R(3, 4)$.
- a) $1R4$, b) $4R56$, c) $3R56$, $1R3$ and $4R3$; $8R56$, $8R4$.
- $1R3$, $4R6$ and $9R9$.
- $-1R0$, $\frac{1}{\sqrt{2}}R\frac{1}{\sqrt{2}}$, $\frac{3}{5}R\frac{4}{5}$ but $4R6$, $4R\frac{3}{5}$ and $\frac{1}{\sqrt{2}}R\frac{5}{\sqrt{3}}$.

Exercise 2.2

- It is not symmetric since many counter examples can be given. One of them is 12 and 1. 1 is a divisor of 12 but 12 is not a divisor of 1.
- It is symmetric since if $m + n < 10$ then $n + m < 10$ is also satisfied for every $n, m \in \mathbb{C}$.
- It is symmetric since if $d + a = c + b$ then $c + b = d + a$ for every $(a, b), (c, d) \in \mathbb{D}$.
- It is symmetric since if $\gcd(a, b) \neq 1$ then $\gcd(b, a) \neq 1$ for every $a, b \in \mathbb{E}$.

Exercise 2.3

- It is transitive since if a is the same age as b and b is the same age as c , then a and c must be of the same age.
- It is transitive since if a is at least as tall as b and b is at least as tall as c , then a is at least as tall as c .
- It is transitive since if a lives in the same city as b and b lives in the same city as c , then a and c also live in the same city for every $a, b, c \in \mathbb{H}$.
- It is transitive. If c is a factor of b and b is a factor of a , then c is a factor of a , for all $a, b, c \in \mathbb{B}$.
- It is not transitive. One counter example is $12R-6$ and $-6R4$, but $12R4$.
- It is transitive. This is a bit hard to see, so let's do algebra. Given $(a, b)R(c, d)$ and $(c, d)R(e, f)$, we must prove $(a, b)R(e, f)$ for all $(a, b), (c, d), (e, f) \in \mathbb{D}$. We are given that $d + a = b + c$ (1) and that $c + f = d + e$ (2).

We must prove that $a + f = b + e$ (3).

Adding (1) and (2) gives $a + d + c + f = b + c + d + e$.

Then subtracting $d + c$ from both sides gives (3).

7. It is not transitive. One counter example is $4R3$ and $3R56$, but $4\not R56$.

Exercise 2.4

1. a. It is reflexive since $1 + 1, 2 + 2, 3 + 3, 4 + 4$ are all even. Therefore $1R1, 2R2, 3R3$ and $4R4$. It is symmetric since if $x + y$ is even then $y + x$ is even, too. Hence if xRy then yRx for every $x, y \in A$. It is transitive since if $x + y$ is even and $y + z$ is even then $(x + y) + (y + z)$ and so $x + z$ are even as well. We can conclude that if xRy and yRz then xRz for every $x, y, z \in A$.

b. 1 is in relation with 3 and 2 is in relation with 4. Hence there are two equivalence classes: $\{1, 3\}$ and $\{2, 4\}$.

2. a) It is not an equivalence relation, because it is not symmetric, because it contains (b, a) but not (a, b) .

b. It is reflexive because $(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)$ are all in R .

It is symmetric because for all of the pairs $(1, 2), (2, 1), (1, 3), (3, 1),$ and $(2, 3), (3, 2)$, both members are in R .

It is transitive. Unfortunately checking transitivity can be laborious. Since $(1, 2)$ and $(2, 3)$ are in R then $(1, 3)$ must be too and it is. Also $(1, 3)$ and $(3, 1)$ requires $(1, 1)$, check. $(1, 3)$ and $(3, 2)$ requires $(1, 2)$, check, and so on. They are all there.

3. It is sufficient to show that one of the three properties does not hold. It is not reflexive: $3R3$ since $3 = 3$. (Symmetry is also ruled out because $4R3$ but $3\not R4$ and since $4 > 3$ but $3 > 4$. R is transitive.) Remark: If the inequality is changed to \geq then the relation is not an equivalence relation. It is reflexive and transitive but R is still not symmetric.

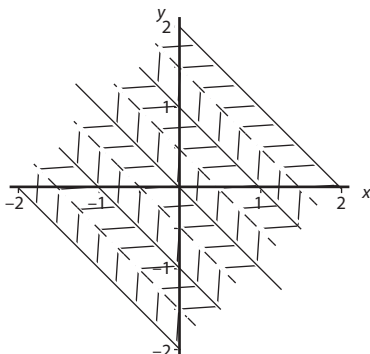
4. a. R is reflexive since $(x, y)R(x, y)$ holds for every $(x, y) \in \mathbb{R} \times \mathbb{R}$ since $[x + y] = [x + y]$. R is symmetric, since if $[x + y] = [a + b]$ then $[a + b] = [x + y]$. R is transitive. If $(x, y)R(a, b)$ and $(a, b)R(c, d)$ then $(x, y)R(c, d)$ as well for every $(x, y), (a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$, since if $[x + y] = [a + b]$ and $[a + b] = [c + d]$, then $[x + y] = [c + d]$. Therefore it is an equivalence relation.

b. Let us choose two pairs of numbers $(2.2, -1.6)$ and $(-2, 2.7)$. Are they in relation? $[2.2, -1.6] = 0$ and $[-2, 2.7] = 0$, so $(2.2, -1.6)R(-2, 2.7)$. Which $(x, y) \in \mathbb{R} \times \mathbb{R}$ are in relation with $(2.2, -1.6)$? We need (x, y) such that $[x + y] = 0$, that is $0 \leq x + y < 1$.

These are the points on the Cartesian plane which lie between the lines $x + y = 0$ (line included) and $x + y = 1$ (line excluded).

The points in the equivalence class with $(2.2, -0.6)$ are the points on the Cartesian plane which lie between the lines $x + y = 1$ (line included) and $x + y = 2$ (line excluded).

And so on. So the equivalence classes are the regions between adjacent parallel lines in the Cartesian coordinate system: $x + y = n$ (line included) and $x + y = n + 1$ (line excluded), $n \in \mathbb{Z}$. One can see that these sets fill up the plane, and no point lies in more than one of the sets.



The equivalence classes of $(x, y)R(a, b)$ if $[x + y] = [a + b]$ are diagonal bands.

5. We have to show that R is reflexive, symmetric and transitive. R is reflexive since $a - a = 0$ and 0 is divisible by 2 for every $a \in \mathbb{Z}$. R is symmetric since if $a - b$ is divisible by 2 then $b - a$ is divisible by 2, too. $b - a = -(a - b)$ for every $a, b \in \mathbb{Z}$. R is transitive since if aRb , that is $a - b = 2n$, $n \in \mathbb{Z}$ and bRc , that is $b - c = 2m$, $m \in \mathbb{Z}$, then $a - c = 2(n + m)$ where $n + m \in \mathbb{Z}$, therefore aRc for every $a, b, c \in \mathbb{Z}$. R partitions \mathbb{Z} into two equivalence classes: odd and even numbers.

6. First we determine which numbers are in relation with 0; 3 is a factor of $x - 0$, $[0]$ are the multiples of 3. $x \in \{\dots -6, -3, 0, 3, 6, \dots\}$. in other words $\{x \mid x = 3k, k \in \mathbb{Z}\}$. Now we determine which numbers are in relation with 1. We need x such that 3 is a factor of $x - 1$. These are the integers which give a remainder 1 on division by 3. $x \in \{\dots -5, -2, 1, 4, 7, \dots\}$; $\{x \mid x = 3k + 1, k \in \mathbb{Z}\}$. Next we determine which numbers are in relation with 2. We need x such that 3 is a factor of $x - 2$. These are the integers which give a remainder 2 on division by 3. $x \in \{\dots -4, -1, 2, 5, 8, \dots\}$; $\{x \mid x = 3k + 2, k \in \mathbb{Z}\}$. Which integers are in relation with 3? These numbers are the same as the first set, because 3 is in the first set. So we can conclude that there are altogether three equivalent classes.

7. We have to show that it is reflexive, symmetric and transitive. R is reflexive since m is a divisor of $a - a = 0$ for every $a \in \mathbb{Z}$ and $m \in \mathbb{N}$, $2 \leq m$. R is symmetric since if $a - b = k \cdot m$ then $b - a = -(a - b) = -k \cdot m$ for every $a, b, k \in \mathbb{Z}$ and $m \in \mathbb{N}$, $-k \in \mathbb{Z}$, $2 \leq m$. R is transitive since if $a - b = k \cdot m$ and $b - c = j \cdot m$ then $a - b + b - c = a - c = (k + j) \cdot m$ for every $a, b, c \in \mathbb{Z}$, $k + j \in \mathbb{Z}$, and $m \in \mathbb{N}$, $2 \leq m$. If we take any positive integer and divide it by any positive integer m , the possible remainders are integers: 0, 1, 2, 3, 4, ..., $m - 1$. We could place in one set all those integers which give a remainder 0 on division by m , in another set all those integers with remainder 1, in another those with remainder 2 and so on. All these sets will be different, and every integer will be in only one set for a given m . It is a partition of \mathbb{Z} . This relation partitions \mathbb{Z} into m equivalence classes.

Exercise 2.5

1. aRb if $|a| = |b|$ where $a, b \in \mathbb{R}$.

	Answer	Reasoning
reflexive	Yes	$ a = a $ for every $a \in \mathbb{R}$.
symmetric	Yes	If $ a = b $ then $ b = a $ for every $a, b \in \mathbb{R}$.
transitive	Yes	If $ a = b $ and $ b = c $ then $ a = c $ for every $a, b, c \in \mathbb{R}$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. Equivalence classes are: $\{0\}$, $\{3, -3\}$, $\{1.5, -1.5\}$, etc.

2. mRn if and $m, n \in \mathbb{Z}^+$ and 3 is a factor of $m^2 - n^2$. Notation: $3|m^2 - n^2$.

	Answer	Reasoning
reflexive	Yes	$3 m^2 - m^2 = 0$ for every $m \in \mathbb{Z}^+$.
symmetric	Yes	If $3 m^2 - n^2$ then $3 -(m^2 - n^2) = n^2 - m^2$ for every $m, n \in \mathbb{Z}^+$.
transitive	Yes	If $3 m^2 - n^2$ and $3 n^2 - k^2$, then $3 m^2 - n^2 + n^2 - k^2 = m^2 - k^2$ for every $m, n, k \in \mathbb{Z}^+$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

To find the equivalence classes, we make a table

x	x^2	$x^2 \pmod{3}$
1	1	1
2	4	1
3	9	0
4	16	1
5	25	1
6	36	0
7	49	1
8	64	1
9	81	0
10	100	1
11	121	1
12	144	0

There are 2 equivalence classes: multiples of 3 and non-multiples of 3.

3. xRy if $x, y \in \mathbb{Z}$ and 2 is a factor of $x^2 + y^2$.

	Answer	Reasoning
reflexive	Yes	$2 x^2 + x^2 = 2x^2$ for every $x \in \mathbb{Z}$.
symmetric	Yes	If $2 x^2 + y^2$ then $2 y^2 + x^2$ for every $x, y \in \mathbb{Z}$.
transitive	Yes	If $2 y^2 + x^2$ and $2 x^2 + k^2$ then $2 y^2 + x^2 + x^2 + k^2 = y^2 + k^2 + 2x^2$. Therefore $2 y^2 + k^2$ for every $y, x, k \in \mathbb{Z}$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. The equivalence classes are the odd and even numbers.

4. mRn if $m, n \in \mathbb{N}^+$ and $m \times n$ is a perfect square.

	Answer	Reasoning
reflexive	Yes	$a \times a$ is a perfect square for every $a \in \mathbb{N}^+$.
symmetric	Yes	If $a \times b$ is a perfect square then $b \times a$ is a perfect square for every $a, b \in \mathbb{N}^+$.
transitive	Yes	If $a \cdot b = n^2$ and $b \cdot c = m^2$, then $a \cdot c \cdot b^2 = m^2 \times n^2$ and $a \cdot c = \left(\frac{mn}{b}\right)^2$. Since b is a factor of n and m as well, $\left(\frac{mn}{b}\right)$ is an integer.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. Equivalence classes are formed by those positive integers for which the product of their prime factorisation has primes with even exponents only.

5. aRb if a and b are co-primes (relative primes) $a, b \in \mathbb{N}^+$. (a and b are co-primes if their greatest common divisor is 1, $\gcd(a, b) = 1$.)

	Answer	Reasoning
reflexive	No	" a " and " a " are not co-primes since $\gcd(a, a) = a \neq 1$ (unless $a = 1$).
symmetric	Yes	If $\gcd(a, b) = 1$ then $\gcd(b, a) = 1$ for every $a, b \in \mathbb{N}^+$.
transitive	No	Counter example: $a = 12$ and $b = 35$ $c = 2$: $\gcd(12, 35) = 1$ and $\gcd(35, 2) = 1$ but $\gcd(12, 2) = 2$. Therefore $12R2$.

Since R is neither reflexive nor transitive (only one counter example is needed), it is not an equivalence relation.

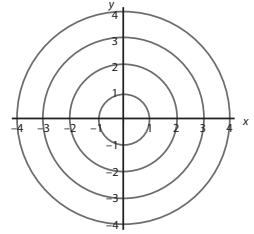
Mathematics HL Topic 8: Sets, Relations and Groups

6. $(x, y)R(a, b)$ if $x^2 + y^2 = a^2 + b^2$ $(a, b), (x, y) \in \mathbb{R} \times \mathbb{R}$.

	Answer	Reasoning
reflexive	Yes	$x^2 + y^2 = x^2 + y^2$ for every $(x, y) \in \mathbb{R} \times \mathbb{R}$.
symmetric	Yes	If $x^2 + y^2 = a^2 + b^2$ then $a^2 + b^2 = x^2 + y^2$ for every $(a, b), (x, y) \in \mathbb{R} \times \mathbb{R}$.
transitive	Yes	If $x^2 + y^2 = a^2 + b^2$ and $a^2 + b^2 = c^2 + d^2$ then $x^2 + y^2 = c^2 + d^2$ for every $(a, b), (x, y), (c, d) \in \mathbb{R} \times \mathbb{R}$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

Equivalence classes: We will try to find one example. We will find all of the points such that $(0, 1)R(x, y)$ that is where $x^2 + y^2 = 0^2 + 1^2$. Thus we need points for which $x^2 + y^2 = 1^2$. This determines a circle with the centre being the origin and the radius being equal to 1. This is one equivalence class. Thus R partitions $\mathbb{R} \times \mathbb{R}$ into equivalence classes consisting of circles centred at the origin, for example $\{(x, y) \mid x^2 + y^2 = 1\}$, $\{(x, y) \mid x^2 + y^2 = 2\}$, etc. The origin is in an equivalence class by itself.



7. aRb if $|a| - |b|$ is even where $a, b \in \mathbb{R}$.

	Answer	Reasoning
reflexive	Yes	$ a - a = 0$ which is even for every real number.
symmetric	Yes	If $ a - b $ is even then $ b - a = -(a - b)$ is even, too.
transitive	Yes	If $ a - b $ is even and $ b - c $ is even then their sum $ a - c $ is even, too.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. Those numbers are in the same equivalence class which are at the distance of 2 units from each other on the number line.

8. $(x, y)R(a, b)$ if $x, y, a, b \in \mathbb{R}$ and $x + y = a + b$.

	Answer	Reasoning
reflexive	Yes	$a + b = a + b$ for every $(a, b) \in \mathbb{R} \times \mathbb{R}$.
symmetric	Yes	If $(a, b)R(c, d)$ then $(c, d)R(a, b)$ that is if $a + b = c + d$ then $c + d = a + b$ for every $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$.
transitive	Yes	If $(a, b)R(c, d)$ and $(c, d)R(e, f)$ then $(a, b)R(e, f)$: If $a + b = c + d$ and $c + d = e + f$ then $a + b = e + f$ for every $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

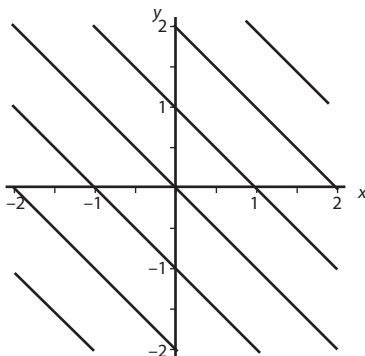
Equivalence classes: We will try to find one example. We will find all of the points such that $(0, 1)R(x, y)$ that is where $x + y = 0 + 1$. Thus we need points for which $x + y = 1$. This

determines a line $y = 1 - x$. This is one equivalence class.

Then we will find all of the points such that $(-2, 3.4)R(x, y)$ that is where $x + y = -2+3.4$. Thus we need points for which $x + y = 1.4$. This determines a line $y = 1.4 - x$. This is another equivalence class.

Other equivalence classes are lines with equation $y = c - x$ where $c \in \mathbb{R}$.

The equivalence classes consist of all lines with slope = -1.



The equivalence classes for $x + y = a + b$

9. $(a, b)R(c, d)$ if $|a| + |b| = |c| + |d|$, where $(a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$.

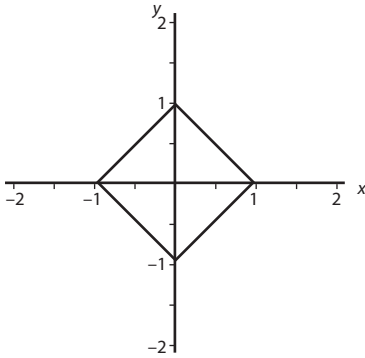
	Answer	Reasoning
reflexive	Yes	It is reflexive since $ a + b = a + b $ for every $(a, b) \in \mathbb{R}^2 \setminus (0, 0)$.
symmetric	Yes	If $(a, b) R(c, d)$ then $ a + b = c + d $. This implies that $(c, d)R(a, b)$ by using $ c + d = a + b $ where $(a, b), (c, d) \in \mathbb{R}^2 \setminus (0, 0)$.
transitive	Yes	If $(a, b)R(c, d)$ and $(c, d)R(e, f)$ then $ a + b = c + d $ and $ c + d = e + f $. Therefore $ a + b = e + f $ holds. This means that $(a, b) R(e, f)$ for every $(a, b), (c, d), (e, f) \in \mathbb{R}^2 \setminus (0, 0)$.

Since R is reflexive symmetric and transitive, it is an equivalence relation.

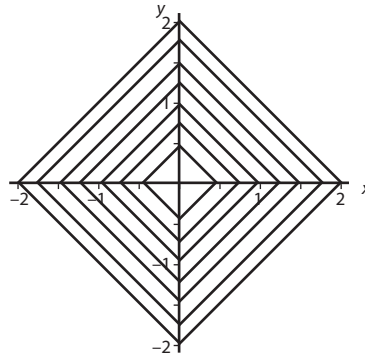
To find the equivalence classes we first try to find the equivalence classes for all points such that $(0, 1)R(x, y)$ where $|0| + |1| = 1$. We need points which satisfy $|x| + |y| = 1$. If we investigate points in the first quadrant then we need points such that $x + y = 1$ holds.

So $y = 1 - x$. This means a segment with endpoints $(0, 1)$ and $(1, 0)$. If we investigate points in the second quadrant then we need points when $-x + y = 1$.

So $y = 1 + x$. This means a segment with endpoints $(0, 1)$ and $(-1, 0)$. After drawing the other two segments in the third and fourth quadrant we have the locus which is a square with vertices $(0, 1), (0, -1), (1, 0)$ and $(-1, 0)$.



The equivalence class for (0,1)



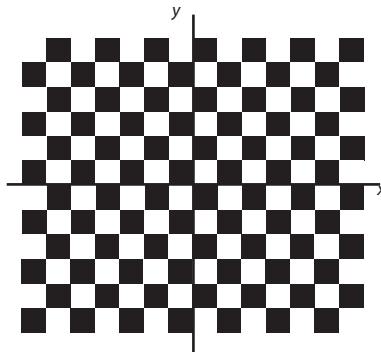
More equivalence classes

The other equivalence classes are all other squares with the centre of origin and vertices on the axes. If origin is included then one more class is the origin alone.

10. $(x, y)R(a, b)$ if $x, y, a, b \in \mathbb{R}$ and $[a] = [x], [b] = [y]$, where $[z]$, the floor function, means the greatest integer less than or equal to z . Notations: $\text{int}(x)$ or $[x]$. It is called the integral or integer part of a number.

reflexive	Yes	$(a, b)R(a, b)$ since $[a] = [a]$ and $[b] = [b]$ for every $(a, b) \in \mathbb{R} \times \mathbb{R}$.
symmetric	Yes	If $(a, b)R(c, d)$ then $(c, d)R(a, b)$. If $[a] = [c]$ and $[b] = [d]$ then $[c] = [a]$ and $[d] = [b]$ for every $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$.
transitive	Yes	If $[a] = [c], [b] = [d]$ and $[c] = [e], [d] = [f]$ then $[a] = [e]$ and $[b] = [f]$ for every $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. Equivalence classes: All of the points in each 1×1 square is an equivalence class. The upper right edges of each square are excluded from the class and the lower left edges of each square are included in the class.



The equivalence classes for $[a] = [x], [b] = [y]$

IB Exam Type Problems

1. i. R is reflexive because aRa since $a^2 \equiv a^2 \pmod{n}$ for every $a \in$ the set.
 R is symmetric since if $a^2 \equiv b^2 \pmod{n}$, then $b^2 \equiv a^2 \pmod{n}$ for every $a, b \in$ the set.
 Let aRb and bRc , then $a^2 - b^2 = nm$ and $b^2 - c^2 = nk$ where m, k are integers.
- ii. Adding gives $a^2 - c^2 = n(m + k)$, where $m + k \in \mathbb{Z}$, so aRc is transitive.

x	x^2	$x^2 \pmod{6}$
1	1	1
2	4	4
3	9	3
4	16	4
5	25	1
6	36	0
7	49	1
8	64	4
9	81	3
10	100	4
11	121	1
12	144	0
13	169	1
14	196	4

The equivalence classes are: $\{1, 5, 7, 11, 13\}$, $\{2, 4, 8, 10, 14\}$, $\{3, 9\}$ and $\{6, 12\}$.

2. i. Reflexive: $(a, b)R(a, b)$ because $ab = ba$ for every $(a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$.
 Symmetric: If $(a, b)R(c, d)$, then $ad = bc$, then $cb = da$, so $(c, d)R(a, b)$ for every $(a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$, so symmetric.
 Transitive: $(a, b)R(c, d)$ and $(c, d)R(e, f)$, then $ad = bc$ and $cf = de$, so $\frac{ad}{de} = \frac{bc}{cf}$, so $af = be$, so $(a, b)R(e, f)$ for every $(a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$, so transitive.
- ii. If $(a, b)R(x, y)$, then $ay = bx$ or $y = \frac{b}{a}x$. So the equivalence classes are points in the first quadrant on straight lines through the origin with slope $\frac{b}{a}$.
3. $1R2$, but $2R1$, so R is not symmetric, so R is not an equivalence relation.
4. i. Reflexive: $x^2 - 4x = x^2 - 4x$, for every $x \in \mathbb{R}$ so reflexive.
 Symmetric: if $x^2 - 4x = y^2 - 4y$, then $y^2 - 4y = x^2 - 4x$ for every $x, y \in \mathbb{R}$, so symmetric.
 Transitive: if $x^2 - 4x = y^2 - 4y$ and $y^2 - 4y = z^2 - 4z$, then $x^2 - 4x = z^2 - 4z$ for every $x, y, z \in \mathbb{R}$, so transitive.

So R is an equivalence relation.

Mathematics HL Topic 8: Sets, Relations and Groups

ii. If $y^2 - 4y = x^2 - 4x$, then $0 = x^2 - y^2 - (4x - 4y)$, so $(x - y)(x + y) - 4(x - y) = 0$, so $(x - y)(x + y - 4) = 0$, so either $x = y$ (which unhelpfully means that every number is in an equivalence class with itself) or $x + y = 4$ (which means equivalence classes are ..., $\{2, 2\}$, $\{3, 1\}$, $\{4, 0\}$, $\{5, -1\}$, $\{6, -2\}$, $\{7, -3\}$, $\{0.2, 3.8\}$, $\{-3.9, 7.9\}$, $\{6.4, -2.4\}$...

iii. $\{2\}$

4. i. Reflexive: $2^x \equiv 2^x \pmod{10}$ for every $x \in \mathbb{Z}^+$, so R is reflexive.

Symmetric: If $2^x \equiv 2^y \pmod{10}$, then $2^x - 2^y = 10n$, $n \in \mathbb{Z}$, so $2^y - 2^x = -10n$, so $2^y \equiv 2^x \pmod{10}$ for every $x, y \in \mathbb{Z}^+$, so R is symmetric.

Transitive: If $2^x \equiv 2^y \pmod{10}$ and $2^y \equiv 2^z \pmod{10}$, then $2^x - 2^y = 10n$ and $2^y - 2^z = 10m$, $n, m \in \mathbb{Z}$; adding gives, $2^x - 2^z = 10(n + m)$, so $2^x \equiv 2^z \pmod{10}$ for every $x, y, z \in \mathbb{Z}^+$, so transitive.

x	2^x	$2^x \pmod{10}$
1	2	2
2	4	4
3	8	8
4	16	6
5	32	2
6	64	4
7	128	8
8	256	6
9	512	2
10	1024	4
11	2048	8
12	4096	6

ii. The equivalence classes are $\{1, 5, 9, \dots\}$, $\{2, 6, 10, \dots\}$, $\{3, 7, 11, \dots\}$, $\{4, 8, 12, \dots\}$; that is the equivalence classes are $4k, 4k + 1, 4k + 2, 4k + 3, k \in \mathbb{Z}$.

6. i. Reflexive: Since $x^2 - y^2 = x^2 - y^2$, $(x, y)R(x, y)$ for every $(x, y) \in \mathbb{R}^+ \times \mathbb{R}^+$, so reflexive.

Symmetric: If $x^2 - y^2 = a^2 - b^2$, then $a^2 - b^2 = x^2 - y^2$ for every $(x, y), (a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$, so symmetric.

Transitive: If $x^2 - y^2 = a^2 - b^2$ and $a^2 - b^2 = c^2 - d^2$, then $x^2 - y^2 = c^2 - d^2$ for every $(x, y), (a, b), (c, d) \in \mathbb{R}^+ \times \mathbb{R}^+$, so transitive.

ii. If $(x, y) R (0, 0)$ then $x^2 - y^2 = 0^2 - 0^2$, so $x^2 - y^2 = 0$, so $(x - y)(x + y) = 0$, so $y = x$ or $y = -x$. Only $y = x$ is in the first quadrant, so the equivalence class of $(0, 0)$ is the part of the line $y = x$ in the first quadrant.

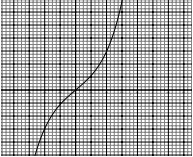
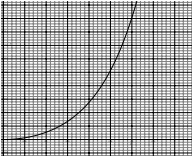
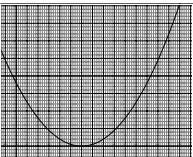
7. i. R_1 is not an equivalence relation, because cRc , so R_1 is not reflexive.

R_2 is not an equivalence relation, because dRf , but fRd , so R_2 is not symmetric.

R_3 is reflexive because gRg , hRh , iRi ; symmetric because gRi and iRg ; and transitive. So R_3 is an equivalence relation.

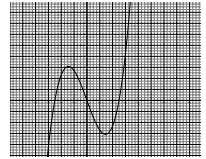
ii. For R_3 the equivalence classes are $\{h\}$ and $\{g, i\}$.

Exercise 3.1

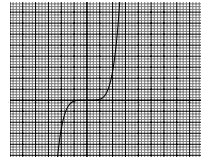
1. $f(x) = 2e^x$ range = \mathbb{R}^+ ; $f(x) = \arctan x$, range = $(-\frac{\pi}{2}, \frac{\pi}{2})$; $f(x) = \frac{1}{x}$, range = $\mathbb{R} \setminus \{0\}$. They are not surjections because their range is not \mathbb{R} , codomain. They are injections because they pass the HLT.
2. $f(x) = x^3 - x$. It is not an injection because $f(0) = f(1)$. It is a surjection because its range is \mathbb{R} , codomain.
3. a. Injective because it passes the HLT; surjective because the range = $\{a, b\}$ is codomain.
- b. Injective because it passes the HLT; not surjective since range = $\{a, b, c\} \neq B$.
- c. Injective because it passes the HLT; not surjective since range = $\mathbb{R}^+ \neq \mathbb{R}$.
- d. Injective because it passes the HLT, surjective because the range = \mathbb{R}^+ is codomain.
- e. Injective because it passes the HLT;
surjective since range = \mathbb{R} is the codomain. 
- f. Injective because it passes the HLT;
not surjective since range = $\mathbb{R}^+ \neq \mathbb{R} = \text{codomain}$. 
- g. Not injective because it fails the HLT;
surjective since range = $\mathbb{R}^+ \cup \{0\} = \text{codomain}$. 
- h. Injective, since if $f(a) = f(b)$, then $a - 2 = b - 2$, then $a = b$; surjective, since range = $\mathbb{Z} = \text{codomain}$.
- i. $f(-1) = f(1)$, so not injective; $x = \pm\sqrt{y+2}$ if $y \geq -2$, so for $y = 0$, $\pm\sqrt{2} \notin \mathbb{Z}$, so not surjective. Or if $y = 0$, $x^2 - 2 = 0$, so $x^2 = 2$, which has no integer solution.
- j. Injective, since if $f(a) = f(b)$, then $3a - 2 = 3b - 2$, then $a = b$; $x = \frac{y+2}{3}$, so for $y = 0$, $x \notin \mathbb{Z}$, so not surjective. Or for $y = 0$, $0 = 3x - 2$, which has no integer solution.
- k. Injective, since if $f(a) = f(b)$, then $\sqrt{a-2} = \sqrt{b-2}$ then $a - 2 = b - 2$, then $a = b$; surjective, since range = $\mathbb{R}^+ \cup \{0\} = \text{codomain}$.
- l. $f(1, 2) = f(2, 1)$ so not injective. For $f(x, y) = (1, 1)$, $xy = 1$, $x + y = 1$, we get $x^2 - x + 1 = 0$, which has no real solutions, so not surjective.
- m. Fails HLT so not injective, range is $[-1, 1]$ so not surjective.

Mathematics HL Topic 8: Sets, Relations and Groups

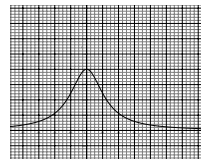
- n. Fails HLT so not injective, range is $[-1, 1]$ so surjective.
- o. Fails HLT so not injective, range is $[-1, 1]$ so surjective.
- p. Passes HLT so injective, range is $[-1, 1]$ so surjective.
- q. Injective, surjective.
- r. Fails HLT so not injective, surjective, since range $= \mathbb{R} =$ codomain.



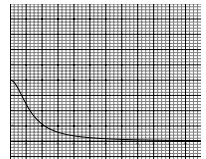
- s. Passes HLT so injective], surjective,
since range $= \mathbb{R} =$ codomain.



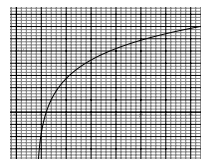
- t. Fails HLT, so not injective;
not surjective, since range $=]0, 1] \neq \mathbb{R} =$ codomain.



- u. Passes HLT so injective;
surjective, since range $=]0, 1] =$ codomain.



- v. Passes HLT so injective, surjective, since range $= \mathbb{R} =$ codomain.



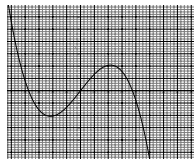
- w. $f(0.1) = f(0.2) = 0$, so not injective; range is $\mathbb{Z} \neq \mathbb{R} =$ codomain, so not surjective.

4.

- a. Fails HLT, so not injective, surjective, since range $=]0, 1] =$ codomain.
- b. Fails HLT, so not injective, not surjective, since range $=]0, 1] \neq \mathbb{R} =$ codomain.
- c. Passes HLT so injective, not surjective, since range $=]-1, 1[\neq \mathbb{R} =$ codomain.
- d. Passes HLT so injective, surjective, since range $=]-1, 1[=$ codomain.

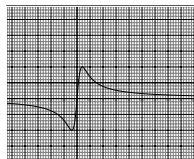
5. Since it is an odd polynomial, range = \mathbb{R} = codomain,

so surjective; $f(0) = f(3) = 0$, so not injective.



6. $f'(x) = \frac{2 - 2x^2}{(x^2 + 1)^2}$ $f'(x) = 0$ when $x = \pm 1$; f' changes sign at $x = \pm 1$,

so f is not an injection; $f(-1) = -1, f(1) = 1$, so surjection.



7. $f'(x) = \frac{1}{2\sqrt{x}} > 0$ for $x > 0$, so injection; range $y > 0$ which is not the codomain, so not a surjection.

8. $f'(x) = \sec^2 x > 0$ for all x and the domain includes only one period of $\tan(x)$, so $f(x)$ is injective. Range of $\tan x = \mathbb{R}$, so a surjection.

IB Exam Type Problems

1. Since $f(3) = f(-2) = 0$, it is not an injection.

Solving for x gives

$$f(x) = \begin{cases} \frac{x+2}{2} & \text{if } x \text{ is even} \\ \frac{x-3}{2} & \text{if } x \text{ is odd} \end{cases}$$

For all $y \in \mathbb{Z}$ there is an $x \in \mathbb{Z}$, since $2y - 2$ is even and $2y + 3$ is odd, so $f(x)$ is surjective.

2. We must show that $f(x)$ is injective and surjective.

$f'(x) = 2x + 2$, which is positive for all $x > -1$, so $f(x)$ is injective.

Starting with $y = x^2 + 2x - 15$, completing the square and solving for x gives $x = -1 \pm \sqrt{y + 16}$ which is real for $y \geq -16$; so $f(x)$ is surjective. So $f(x)$ is bijective. So $f(x)$ has an inverse, $f^{-1}(x) = -1 + \sqrt{x + 16}$, where from \pm the $+$ is selected to correspond to the domain of $f(x)$.

3. We must show that $f(x)$ is injective and surjective. So we must show that if $f(a, b) = f(c, d)$, then $a = c$ and $b = d$. So $a - b = c - d$ and $a + b = c + d$, adding the equations gives, $2a = 2c$, so $a = c$, subtracting the two equations gives $b = d$, so $f(x)$ is injective.

Letting $f(x, y) = (U, V)$ gives $U = x - y, V = x + y$.

Solving for x and y gives $x = \frac{U+V}{2}, y = \frac{-U+V}{2}$;

if $U, V \in \mathbb{R}$, then $x, y \in \mathbb{R}$, so $f(x)$ is surjective. So $f(x)$ is bijective.

So $f(x)$ has an inverse, $f^{-1}(x, y) = \left(\frac{x+y}{2}, \frac{-x+y}{2}\right)$

4. We must show that $f(x)$ is injective and surjective. So we must show that if $f(a, b) = f(c, d)$, then $a = c$ and $b = d$. So $3a - 2b = 3c - 2d$ and $-a + 2b = -c + 2d$. Adding the equations gives $2a = 2c$, so $a = c$; subtracting gives $c = d$, so $f(x)$ is injective.

Letting $f(x, y) = (U, V)$ gives $U = 3x - 2y$, $V = -x + 2y$.

Solving for x and y gives $x = \frac{U + V}{2}$, $y = \frac{U + 3V}{4}$

If $U, V \in \mathbb{R}$, then $x, y \in \mathbb{R}$, so $f(x)$ is surjective.

So $f(x)$ is bijective. So $f(x)$ has an inverse, $f^{-1}(x, y) = \left(\frac{x + y}{2}, \frac{x + 3y}{4}\right)$.

Exercises 4.1

1. a.

i. $2 * 3 = 2 + 3 - 2 \cdot 3 = -1$

ii. $-3 * 0 = -3 + 0 - (-3) \cdot 0 = -3$

iii. $6 \bullet 2 = 2 - 6 = -4$

iv. $(3 * 2) \bullet 4 = 4 - (3 + 2 - 3 \cdot 2) = 4 - (-1) = 5$

v. $(-2 \bullet 6) * 1 = [6 - (-2)] * 1 = 8 * 1 = 8 + 1 - 8 \cdot 1 = 1$.

b)

i. $2 * x = 3$ means $2 + x - 2x = 3$ which gives $x = -1$

ii. $x * 4 = 11$ means $x + 4 - x \cdot 4 = 11$ which gives $x = -\frac{7}{3}$

iii. $-3 \bullet x = 5$ means $x - (-3) = 5$ which gives $x = 2$.

2. Let $a * b = a^2b$, $a, b \in \mathbb{Z}$.

a)

i. $3 * 2 = 9 \cdot 2 = 18$

ii. $2 * 3 = 4 \cdot 3 = 12$

iii. $3 * 3 = 9 \cdot 3 = 27$

iv. $0 * -2 = 0 \cdot (-2) = 0$

v. $3 * 4 = 9 \cdot 4 = 36$

vi. $2 * 2 = 4 \cdot 2 = 8$

vii. $2 * (3 * 4) = 2 * (9 \cdot 4) = 2 * 36 = 4 \cdot 36 = 144$

viii. $(2 * 3) * 4 = (4 \cdot 3) * 4 = 12 * 4 = 144 \cdot 4 = 566.$

- b. For $a = b$ or either a or b is zero.
- c. No, counter-examples are given in part vii and viii.

Exercise 4.2

- a. It is not a binary operation since 0^0 is not defined.
- b. Not a binary operation, for example because $3 * -1$ is undefined.
- c. A binary operation since any two positive integers have a gcd. The greatest common divisor of two positive integers is a positive integer. So the binary operation is closed.
- d. Not a binary operation, for example because $1 * 1$ is undefined.
- e. A binary operation. As addition, subtraction and multiplication of real numbers are closed, $2a - 3c$ and $2b + d$ are real, so $(2a - 3c, 2b + d) \in \mathbb{R}^2$. So the binary operation is closed.
- f. A binary operation since you can form a fraction with a non-zero denominator. Any non-zero real number divided by another non-zero real number is a non-zero real number. So the binary operation is closed.
- g. A binary operation since you can calculate the result for any two integers a and b . As addition, subtraction and multiplication of integers is closed, $a + b - 2ab \in \mathbb{Z}$. So the binary operation is closed.
- h. It is a binary operation since the product is defined for all possible values of a and b . Not closed since $(3+2i)(4+6i) = 12 + 18i + 8i - 12 = 0$ which is not a member of the original set.
- i. It is a binary operation since the product is defined for all possible values of a and b . It is closed since $(a+bi)(c+di) = (ac - bd) + (ad + bc)i$ and if a and b are not both equal to zero and c and d are not both equal to zero, then at least one of ac , bd , ad or bc must also not equal zero.
- j. It is a binary operation, but not closed, since 3 divided by 4 is not a positive integer.
- k. It is a binary operation and it is closed since the product of any two positive odd integers is a positive odd integer as well.
- l. It is a binary operation. It is not closed since the sum of two odd numbers is even.

Exercise 4.3

1. $a * e = a$ for every integer.

$$a + e - 2ae = a$$

$$e = 2ae$$

$$e = 0$$

$a * a = a$ also gives $e = 0$, so $a * b$ has identity element $e = 0$.

2. $e * a = \frac{e}{a} = a$ gives $e = a^2$

$$a * e = \frac{a}{e} = a \text{ gives } e = 1.$$

$e * a \neq a * e$ so $a * b$ has no identity element.

3. $a * e = a$ and $e * a = a$ means $2ae = a$ and $2ea = a$. Therefore $e = \frac{1}{2}$ which is a real number.

4. $e * a = 2e + a = a$ means $e = 0$.

$a * e = 2a + e = a$ means $e = -a$ for every real number. There is no identity element.

5. $a * e = a + 3e = a$ means $e = 0$ for every real number.

$e * a = e + 3a = a$ means $e = -2a$. There is no identity element.

6. $e * a = a$ should hold if e is an identity. $e * a = e$ by the definition of the operation. This way e and a should be equal. There is no identity element.

7. The universal set is the identity element. $A \cap U = U \cap A = A$ for every $A \subseteq U$ and $U \subseteq U$ so it is from the set.

8. The empty set is the identity element $A \cup \emptyset = \emptyset \cup A = A$ for every $A \subseteq U$ and $\emptyset \subseteq U$ so it is from the set.

Exercise 4.4

1. We already know that $e = 0$.

$$a * a^{-1} = a + a^{-1} - 2aa^{-1} = e = 0$$

$$a + a^{-1} - 2aa^{-1} = 0$$

$$a = a^{-1}(1 - 2a) = 0$$

$$a^{-1} = \frac{1}{2a - 1} \in \mathbb{R}, \text{ for all elements } a \text{ other than } \frac{1}{2}.$$

2. We already know that $\frac{1}{2}$ is the identity element. $a * a^{-1} = 2aa^{-1} = \frac{1}{2}$ therefore $a^{-1} = \frac{1}{4a}$. But 0 has no inverse.

3. We already know that the identity is 1. $a \times \frac{1}{a} = 1$. If $a \in \mathbb{Q}$, $\frac{1}{a} \in \mathbb{Q}$ unless $a = 0$. Therefore $\frac{1}{a}$ is the inverse of a , except that 0 has no inverse.

4. We already know that the identity is 0. If $a \in \mathbb{Q}$ then $-a \in \mathbb{Q}$ and $a + (-a) = (-a) + a = 0$. Therefore $-a$ is the inverse of a .

Exercise 4.5

- $a * b$ is commutative, because the definition is symmetric with respect to a and b . Or explicitly: $a * b = a^2 + b^2 - 3(a + b)^2 = b * a = b^2 + a^2 - 3(b + a)^2$ for every $a, b \in \mathbb{R}$.
- $a * b$ is not commutative, because the definition is not symmetric with respect to a and b . Or one counterexample is $3 * 1 = 3^2 + 1^3 - 3(3 + 1)^2 = -38 \neq 1 * 3 = 1^2 + 3^3 - 3(3 + 1)^2 = -20$.
- $a * b = a + b - 2a - 2b = -a - b$; $b * a = b + a - 2b - 2a = -a - b$ for every $a, b \in \mathbb{R}$. So $a * b$ is commutative.

Exercise 4.6

- It is commutative since $a * b = (2^a)^b = 2^{ab} = b * a = (2^a)^b = 2^{ab}$ for every $a, b \in \mathbb{R}$.

It is not associative since $(2 * 3) * 1 = (2^2)^3 * 1 = 64 * 1 = 2^{64} \neq$

$$2 * (3 * 1) = 2 * [(2^3)^1] = 2 * 8 = (2^2)^8 = 2^{16}.$$

- It is commutative since $a * b = a + b + ab$ and $b * a = b + a + ba$ for every $a, b \in \mathbb{R}$.

It is associative since

$$(a * b) * c = (a + b + ab) * c = a + b + ab + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc$$

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc$$

which are equal.

- It is not commutative since $1 * 2 = 3 + 4 = 7 \neq 2 * 1 = 6 + 2 = 8$.

It is not associative since $(2 * 3) * 1 = (6 + 6) * 1 = 12 * 1 = 36 + 2 = 38 \neq$

$$2 * (3 * 1) = 2 * (9 + 2) = 2 * 11 = 6 + 22 = 28.$$

- It is not commutative since $1 * 2 = 1 \cdot 4 = 4 \neq 2 * 1 = 2 \cdot 1 = 2$.

It is not associative since $(2 * 3) * 2 = (2 \cdot 3^2) * 2 = 18 * 2 = 18 \cdot 2^2 = 72 \neq$

$$2 * (3 * 2) = 2 * (3 \cdot 2^2) = 2 * 12 = 2 \cdot 12^2 = 288.$$

- It is commutative since $a * b = (a \cdot b)^2 = b * a = (b \cdot a)^2$ for every $a, b \in \mathbb{R}$.

It is not associative since

$$(2 * 3) * 1 = 36 * 1 = 36^2 = 1296 \neq 2 * (3 * 1) = 2 * 9 = 18^2 = 324.$$

Mathematics HL Topic 8: Sets, Relations and Groups

6. It is commutative since $a * b = a^2 + b^2 = b * a = b^2 + a^2$ for every $a, b \in \mathbb{R}$.
It is not associative since $(2 * 3) * 1 = (2^2 + 3^2) * 1 = 13 * 1 = 13^2 + 1^2 = 169 + 1 = 170 \neq$
 $2 * (3 * 1) = 2 * (3^2 + 1^2) = 2 * 10 = 2^2 + 10^2 = 104$.
7. It is commutative since $a * b = |a - b| = b * a = |b - a|$ for every $a, b \in \mathbb{R}$.
It is not associative since $(5 * 3) * 1 = |5 - 3| * 1 = 2 * 1 = |2 - 1| = 1 \neq$
 $5 * (3 * 1) = 5 * |3 - 1| = 5 * 2 = |5 - 2| = 3$.
8. It is commutative since $a * b = b * a$ for every $a, b \in \mathbb{R}$, since the remainder of $a \cdot b$ is the same as the remainder of $b \cdot a$. It is associative, because the remainder of a product is equal to the remainder of the product of the remainders.
9. It is commutative since $a * b = b * a$ for every $a, b \in S$, because the remainder of $a + b$ on division by 4 is the same as the remainder of $b + a$ on division by 4.
It is associative since the remainder of a sum is equal to the remainder of the sum of the remainders.
10. It is neither commutative nor associative.
11. It is commutative since $a * b = b * a$ for every $a, b \in S$, because the remainder of $a + b$ on division by n is the same as the remainder of $b + a$ on division by n .
It is associative since the remainder of a sum is equal to the sum of the remainders.
12. It is commutative since $a * b = b * a$ for every $a, b \in \mathbb{R}$ since the remainder of $a \cdot b$ is the same as the remainder of $b \cdot a$. It is associative, because the remainder of a product is equal to the remainder of the product of the remainders.
13. i. a. $x = q$, b. $x = p$, c. $x = s$, d. $x = r$.
ii. a. No solution, b. $x = p$, c. $x = p, q$, d. $x = q$.

IB Exam Type Problems

1. a. It is closed. $a + b - 1 \in \mathbb{Z}^+$, for all $a, b \in \mathbb{Z}^+$.
b. $a * e = e * a = a + e - 1 = a$; therefore $e = 1 \in \mathbb{Z}$.
c. $a^{-1} * a^{-1} = a * a^{-1} = e = 1 = a + a^{-1} - 1$; so $a^{-1} = 2 - a$. Since a^{-1} must belong to \mathbb{Z}^+ , a^{-1} exists only for $a = 1$.
d. $a * b = a + b - 1$; $b * a = b + a - 1$, so it is commutative for every $a, b \in \mathbb{Z}^+$.
e. $(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$
 $a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$

for every $a, b, c \in \mathbb{Z}^+$. So it is associative.

2. (a) It is closed. $a + b + 2ab \in \mathbb{R}$ for all $a, b \in \mathbb{R}$.

b. $a * e = e * a = a + e + 2ae = a$; $e(1 + 2a) = 0$; therefore $e = 0 \in \mathbb{R}$.

$e * a = e + a + 2ea = a$ gives the same identity element.

c. $a^{-1} * a^{-1} = a * a^{-1} = a + a^{-1} - 2aa^{-1} = e = 0$; so $a = a^{-1}(2a - 1)$, so $a^{-1} = \frac{a}{2a - 1}$ a^{-1} exists for $a \neq \frac{1}{2}$

d. $a * b = a + b + 2ab = b * a = b + a + 2ba$ for all $a, b \in \mathbb{R}$, so it is commutative.

e. $(a * b) * c = (a + b + 2bc) * c = a + b + 2ab + c + 2(a + b + 2bc)c = a + b + 2ab + c + 2ac + bc + 4abc$.

$a * (b * c) = a * (b + c + 2bc) = a + b + c + 2bc + 2a(b + c + 2bc)$

$= a + b + c + 2bc + 2ab + 2ac + 4abc$. So it is associative.

3. a. It is not closed. $1 * 2 = \frac{2}{3} \notin \mathbb{Z}^+$

b. $a * e = e * a = \frac{ae}{a + e}$, so $ae = a^2 + ae$, which has no solutions for e , so there is no identity.

d. It is commutative.

e. It is associative because

$$(a * b) * c = \frac{ab}{a + b} * c = \frac{\frac{abc}{a + b}}{\frac{ab}{a + b} + c} = \frac{\frac{abc}{a + b}}{\frac{ab}{a + b} + c \frac{a + b}{a + b}} = \frac{\frac{abc}{a + b}}{\frac{ab + ca + cb}{a + b}} = \frac{abc}{ab + ac + bc}$$

$$a * (b * c) = a * \frac{bc}{b + c} = \frac{\frac{abc}{b + c}}{a + \frac{bc}{b + c}} = \frac{\frac{abc}{b + c}}{a \frac{b + c}{b + c} + \frac{bc}{b + c}} = \frac{abc}{ab + ac + bc} = (a * b) * c.$$

4. a.

\times	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

so closed.

b. Yes, 1.

c. 3, 5 and 7 are self inverses.

d. Yes, because $\text{Rem}(a \times b) = \text{Rem}(\text{Rem}(a) \times \text{Rem}(b))$.

5. a, Closed. b, No. c. None.
- d. Yes, because $\text{Rem}(a+b) = \text{Rem}(\text{Rem}(a)+\text{Rem}(b))$.
6. a. Yes, \mathbb{R} is closed under addition, subtraction and multiplication.
- b. $(a, b) * (e_1, e_2) = (a, b) = (ae_1 - be_2, ae_2 + be_1)$. So $a = ae_1 - be_2$, $b = ae_2 + be_1$. Solving simultaneously gives $(e_1, e_2) = (1, 0)$.

c. $(a, b) * (a^{-1}, b^{-1}) = (e_1, e_2) = (1, 0) = (a a^{-1} - b b^{-1}, a b^{-1} + b a^{-1})$.

Therefore $1 = a a^{-1} - b b^{-1}$, (1) $0 = a b^{-1} + b a^{-1}$. (2)

Therefore $b = a b a^{-1} - b^2 b^{-1}$, $b \times (1)$ $0 = a^2 b^{-1} + a b a^{-1}$. $a \times (2)$

Subtracting gives $b = -b^2 b^{-1} - a^2 b^{-1}$ so $-b = b^{-1} (a^2 + b^2)$

so $b^{-1} = \frac{-b}{a^2 + b^2}$.

Substituting this into (2) gives $0 = a \frac{-b}{a^2 + b^2} + b a^{-1}$

so $a^{-1} = \frac{a}{a^2 + b^2}$.

And finally $(a^{-1}, b^{-1}) = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$

- d. Yes.

Exercise 5.1

1. Closure: It is closed. The sum of two even numbers is even.

Identity element: $e = 0$ since, $0 + a = a + 0 = a$ for every an even number. 0 is even.

Inverses: If $a = 2n$, where $n \in \mathbb{Z}$, then $a - 1 = -2n$ since $2n - 2n = 0$ and $-2n$ is even as well.

Associativity: $(2n + 2m) + 2k = 2n + (2m + 2k)$ for every $n, m, k \in \mathbb{Z}$.

So it is a group.

2. 3 has no inverse. $3 \times a = 1$ has solution, $a = \frac{1}{3}$ but it is not an integer. So it is not a group.

3. 0 has no inverse. So it is not a group.

4. Closure: It is not closed: $\frac{1}{3} \times \frac{1}{2} = \frac{1}{6} \notin A$ So it is not a group.

5. Identity element: $e = S$ since $S \cap A = A \cap S = A$ for every subset A of S. $S \subseteq S$.

But only S has an inverse, itself. So it is not a group.

6. Not associative, for example $a = 4, b = 1, c = 2$. $(a * b) * c = 1$ and $a * (b * c) = 3$.

So it is not a group.

7. There is no identity element. $\frac{ae}{a+e} \rightarrow ae = a^2 + ae \rightarrow a^2 = 0 \rightarrow a = 0 \notin \mathbb{R}^+$.

So it is not a group.

Exercise 5.2

1. It is not a group, because not closed $s * s = t$.
2. It is not a group, because there is no identity element.
3. r is the identity element. It is not a group, because q has no inverse.
4. It is a group. s is the identity element. $r^{-1} = r$, $s^{-1} = s$, $p^{-1} = q$, $q^{-1} = p$.

Exercise 5.3

1.
 - a. For all $a, b \in S$, $a * b \in S$.
 - b. The identity element is a , because $a * b = b$ and $b * a = b$ for all $b \in S$ and $a \in S$.
 - c. For all $b \in S$, $b * b = a$ so each element is self inverse.
 - d. $b * (c * d) = c$, but $(b * c) * d = a$.
2.
 - a. There is no identity element since $a * e = a$ and $e * a = e$ for every $a \in \mathbb{Z}$. So it is not a group.
 - b. $1 * 1 = \sqrt{1^2 + 1^2} = \sqrt{2} \notin \mathbb{Q}$, so it is not closed. So it is not a group.
 - c. There is no identity element, since $a \circ e = a$ gives $2(a + e) = a$, so $e = -\frac{a}{2}$. So there is no identity element. So it is not a group.
 - d. $(a, b) * (e_1, e_2) = (ae_1 - be_2, ae_1 + be_2) = (a, b)$ $ae_1 - be_2 = a$ and $ae_1 + be_2 = b$ gives $(e_1, e_2) = \left(\frac{b+a}{2a}, \frac{b-a}{2b}\right)$.
The identity element must be independent of a and b , so the identity element does not exist. So $(S, *)$ is not a group.
 - e. It is not a group, since for $a = 1$ and $b = -1$ $a * b$ cannot be calculated. It is not a binary operation.
 - f. There is no identity element, e , such that $\min(a, e) = \min(e, a) = a$, so it is not a group.
 - g. 0^0 cannot be evaluated, so it is not a group.

- h. There is no identity element, so it is not a group.
- i. It is not closed. The scalar product is a real number not a vector.
- j. It is closed. The vector product of two vectors is a vector as well. There is no identity element, so it is not a group.

Exercise 5.4

1. $a * x = a * y$ Given.
- $a^{-1} * (a * x) = a^{-1} * (a * y)$ Since it is a group every element has an inverse a^{-1} .
- $(a^{-1} * a) * x = (a^{-1} * a) * y$ Applying associativity.
- $e * x = e * y$ Applying the inverse property.
- $x = y$. Applying the identity property

2. Step 1:

- $y * a = b$ Given
- $(y * a) * a^{-1} = b * a^{-1}$ Since $\{S, *\}$ is a group, a has an inverse a^{-1} . Right multiply by a^{-1}
- $y * (a * a^{-1}) = b * a^{-1}$ Using associativity.
- $y * e = b * a^{-1}$ Applying inverse property.
- $y = b * a^{-1}$ Applying identity property. From closure, y exists.

Step 2:

Let us assume that there are two **different** values of y , y_1 and y_2 for which $y * a = b$ with $y_1 \neq y_2$. Since they both equal b , $y_1 * a = y_2 * a$ now applying the right cancellation law, $y_1 = y_2$ which is a contradiction. So y is unique.

Exercise 5.5

1. $3 * 3 = 9$; so we need $a = 9$;

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

With $a = 9$, S is closed.

1 is the identity element.

$3^{-1} = 7, 7^{-1} = 3, 9$ is self inverse

9 is order 2, since it is self inverse. $3^2 = 9, 3^3 = 7, 3^4 = 1$ and $7^2 = 9, 7^3 = 3, 7^4 = 1$, so 3 and 7 are order 4.

Yes, since it is symmetric about the main diagonal, it is Abelian.

2. If $a * c = c * b = e$ then right multiplying by c^{-1} and using associativity,
 $a * (c * c^{-1}) = c * b * c^{-1}$. Hence $a * e = c * b * c^{-1}$ and $a = c * b * c^{-1}$.
3. $\frac{1}{2}(1 + i\sqrt{3}) = \text{cis } \frac{\pi}{3} \cdot \left(\text{cis } \frac{\pi}{3}\right)^n$, for $n = 2, 3, 4, 5$ and 6 gives
 $\frac{1}{2}(1 + i\sqrt{3}), -1, \frac{1}{2}(-1 - i\sqrt{3}), \frac{1}{2}(1 - i\sqrt{3}), 1$.
4. Both are equal to a^{-2} .
- 5) a. Not a group since $1 * 7 = 7$ and $3 * 7 = 7$, so it does not have the Latin Square Property.

b.

Closure	*	2	4	8	10	14	16
	2	4	8	16	2	10	14
	4	8	16	14	4	2	10
	8	16	14	10	8	4	2
	10	2	4	8	10	14	16
	14	10	2	4	14	16	8
	16	14	10	2	16	8	4
	It is closed.						

Identity element	$e = 10$
Inverses	$2^{-1} = 14, 14^{-1} = 2, 4^{-1} = 16, 16^{-1} = 4, 8^{-1} = 8, 10^{-1} = 10.$
Associativity	Holds

So it is a group.

c.

Closure	*	0	2	3	4	5	6
	0	0	2	3	4	5	6
	2	2	0	6	5	4	3
	3	3	6	4	2	0	5
	4	4	5	2	6	3	0
	5	5	4	0	3	6	2
	6	6	3	5	0	2	4
	It is closed.						
Identity element	$e = 0$						
Inverses	$2^{-1} = 2, 5^{-1} = 3, 3^{-1} = 5, 4^{-1} = 6, 6^{-1} = 4.$						
Associativity	Holds						

So it is a group.

d.

Closure	<p>It is closed.</p> <p>If $0 \leq x, y < 1$ then $\frac{x+y}{1+xy} < 1$ since</p> $1 - \frac{x+y}{1+xy} = \frac{1+xy-x-y}{1+xy} = \frac{(y-1)(x-1)}{1+xy} > 0,$ <p>and $x * y = \frac{x+y}{1+xy} > 0.$</p>
Identity element	$\frac{x+e}{1+xe} = x = \frac{e+x}{ex+1}$ <p>so $x+e = x+x^2e$, so $e = x^2e$, so $e = 0$ for every x and 0 is in the given interval.</p> <p>Check: $x = \frac{0+x}{0 \cdot x + 1} = x = \frac{x+0}{x \cdot 0 + 1}$</p>

Inverses	$\frac{x + x^{-1}}{1 + x \cdot x^{-1}} = 0$, where $0 \leq x < 1$.
	$x + x^{-1} = 0$ $x^{-1} = -x$, $-1 < -x \leq 0$, so there is no inverse.

So it is not a group.

e)

Closure	<p>It is closed.</p> <p>If x and y are non-zero real numbers then their product is non-zero as well.</p>
Identity element	$x \bullet e = 2xe = x$ and $e \bullet x = 2ex = x$ for every $x \in \mathbb{R} \setminus \{0\}$. $e = \frac{1}{2}$ which is non-zero.
Inverses	$x \bullet x^{-1} = 2 \times x \times x^{-1} = \frac{1}{2} = x^{-1} \bullet x$ for every $x \in \mathbb{R} \setminus \{0\}$. $x^{-1} = \frac{1}{4x}$ which is non-zero.
Associativity	Multiplication on real numbers is associative.

So it is a group.

6.

Closure	<p>It is closed. If $a, b \in S$ then $a \times b - a - b + 2 = a(b - 1) - (b - 1) + 1$ $= (a - 1)(b - 1) + 1 \neq 1$.</p>
Identity element	$e = 2$ since $(e - 1)(a - 1) + 1 = a \Rightarrow (e - 1)(a - 1) = a - 1$, where $a \neq 1$ $\Rightarrow e - 1 = 1 \Rightarrow e = 2 \neq 1$
Inverses	$a^{-1} = \frac{a}{a - 1}$ since $a * a^{-1} = a \times a^{-1} - a - a^{-1} + 2 = 2 = a^{-1} \bullet a - a^{-1} - a + 2$, $a^{-1}(a - 1) = a$, If $a \neq 1$ then $a^{-1} = \frac{a}{a - 1}$ and $\frac{a}{a - 1} \neq 1$. Unless 1 is excluded a^{-1} is not defined for all a .

Associativity	<p>Show that $(a * b) * c = a * (b * c)$ for every $a, b, c \in \mathbb{R} \setminus \{1\}$.</p> $(a * b) * c = (ab - a - b + 2)c - ab + a + b - c - 2 + 2$ $= abc - ac - bc + 2c - ab + a + b - c$ $= abc - ac - bc - ab + a + b + c$ $a * (b * c) = a(bc - b - c + 2) - a - bc + b + c - 2 + 2$ $= (abc - ab - ac + 2a) - a - bc + b + c - 2 + 2$ $= abc - ab - ac - bc + a + b + c.$
Abelian	<p>Show that $a * b = b * a$ for every $a, b, c \in \mathbb{R} \setminus \{1\}$.</p> $a * b = a \times b - a - b + 2 =$ $b * a = b a - b - a + 2. \text{ So it is Abelian.}$

7.

Closure	$\frac{1+2m}{1+2n} \cdot \frac{1+2k}{1+2s} = \frac{1+2(k+m+2km)}{1+2(n+s+2ns)}$ <p>If $m, n, k, s \in \mathbb{Z}$ then $k + m + 2km, 1 + 2(n + s + 2nl) \in \mathbb{Z}$.</p> <p>Can $n + s + 2ns = -\frac{1}{2}$? No, because if we let $n + s + 2ns = -\frac{1}{2}$, solving for n (or s) gives $n(1 + 2s) = -\frac{1}{2} - s = -\frac{1}{2}(1 + 2s)$ which gives $n = -\frac{1}{2}$. So, it is closed.</p>
Identity element	<p>$e = 1$, where $0 \in \mathbb{Z}$ and $0 \neq -\frac{1}{2}$.</p> <p>$\frac{1+2\bullet 0}{1+2\bullet 0}$ where $0 \in \mathbb{Z}$ and $0 \neq -\frac{1}{2}$.</p>
Inverses	<p>If $\frac{1+2m}{1+2n}, X = 1, m, n \in \mathbb{Z}$, then $X = \frac{1+2n}{1+2m} \in S$.</p>

So it is a group.

8.

Closure	It is closed. If $a, c \neq 0$ then $ac \neq 0$.
---------	---

Identity element	$(a, b) * (c, d) = (ac, bc + d) = (a, b) = (c, d) * (a, b).$ $a = ac$ and $b = bc + d$ $c = 1, b = b + d$ $c = 1, d = 0.$ So $e = (1, 0) \in S.$
Inverses	$(x, y) * (a, b) = (a, b) * (x, y) = (1, 0),$ where $a \neq 0,$ therefore $a \times x = 1$ and $b \times x + y = 0.$ Hence $b \times \frac{1}{a} + y = 0.$ $x = \frac{1}{a}, y = -\frac{b}{a}.$ $(a, b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right) \in S$ since $= \frac{1}{a} \neq 0.$
Associativity	$[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f) = (ace, bce + de + f)$ $(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, de + f) = (ace, bce + de + f)$ for every $(a, b), (c, d), (e, f) \in S.$

Not Abelian. Counter example:

$$(1, 2) * (3, 4) = (3, 2 \times 3 + 4) = (3, 10) \text{ but}$$

$$(3, 4) * (1, 2) = (3, 4 \times 1 + 2) = (3, 6)$$

9. a.

*	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

It is closed, $e = I, C^{-1} = A, A^{-1} = C, B^{-1} = B, I^{-1} = I.$ Associativity is known.

b. i. $B * (C * A) = B * I = B,$

ii. $(A * B) * (B * C) = C * A = I.$

IB Exam Type Problems

1. a. $P_1: (b^{-1}ab)^1 = b^{-1}a^1b$, so P_1 is true

Assume $P_k: (b^{-1}ab)^k = b^{-1}a^k b$

Therefore $(b^{-1}ab)^{k+1}$

$$= (b^{-1}ab)^k (b^{-1}ab)$$

$$= (b^{-1}a^k b)(b^{-1}ab) \quad \text{Using the assumption}$$

$$= b^{-1}a^k e ab \quad \text{Using associativity and the inverse property}$$

$$= b^{-1}a^k ab \quad \text{Using the identity property}$$

$$= b^{-1}a^{k+1} b$$

So $P_k \Rightarrow P_{k+1}$ and P_1 is true. So P_n is true for every $n \in \mathbb{Z}^+$ by mathematical induction.

b, EITHER

By the definition of the inverse $h^{-1}h = e$; so we must show $(b^{-1}ab)(b^{-1}a^{-1}b) = e$

$$(b^{-1}ab)(b^{-1}a^{-1}b)$$

$$= b^{-1}a(bb^{-1})a^{-1}b \quad \text{Using associativity}$$

$$= b^{-1}aea^{-1}b$$

$$= b^{-1}aa^{-1}b$$

$$= b^{-1}eb$$

$$= b^{-1}b$$

$$= e.$$

OR

$$(b^{-1}ab)^{-1}$$

$$= (ab)^{-1}(b^{-1})^{-1} \quad \text{Using the reversal rule}$$

$$= b^{-1}a^{-1}(b^{-1})^{-1} \quad \text{Using the reversal rule}$$

$$= b^{-1}a^{-1}b.$$

c Let $n = -m$, where $m \in \mathbb{Z}^+$.

$$\text{So } (b^{-1}ab)^n = (b^{-1}ab)^{-m} = (b^{-1}ab)^{-1m} = ((b^{-1}ab)^{-1})^m$$

$$= (b^{-1}a^{-1}b)^m \quad \text{Using part b}$$

$$= (b^{-1}(a^{-1})^m b) \quad \text{Using part a}$$

$$= b^{-1}a^{-1m}b$$

$$= b^{-1}a^n b$$

for all negative integers n .

2. a. $b * a = b + a - 1 = a * b$, for all $a, b \in \mathbb{R}$, so yes, commutative.

b. Closure: \mathbb{R} is closed under addition and subtraction so closed.

Associativity: $(a * b) * c = (a + b - 1) * c = a + b - 1 + c - 1 = a + b + c - 2$

$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2.$

So associative, for all $a, b \in \mathbb{R}$.

Identity: $e * a = a * e = a + e - 1 = a$, so $e = 1 \in \mathbb{R}$, so an identity element exists

Inverse: $a * a^{-1} = e$ so

$$a + a^{-1} - 1 = 1 \quad \text{so}$$

$a^{-1} = 2 - a \in \mathbb{R}$, so each element has an inverse element.

The 4 conditions for a group are met, so $\{\mathbb{R}, *\}$ is a group.

3. a. Closure: $(a + b\sqrt{5}) \times (c + d\sqrt{5}) = ac + 5bd + (bc + ad)\sqrt{5}$ where $a, b, c, d \in \mathbb{Q}$ and

$$a^2 + b^2 \neq 0 \text{ and } c^2 + d^2 \neq 0$$

$ac + 5bd \in \mathbb{Q}, bc + ad \in \mathbb{Q}$. From $a^2 + b^2 \neq 0$ a and b cannot both be zero, equally c and d cannot both be zero therefore $ac + 5bd$ and $bc + ad$ cannot both be zero, so $(ac + 5bd)^2 + (bc + ad)^2 \neq 0$. So it is closed.

The identity is $1 \in S$. $1 = 1 + 0\sqrt{5}$ and $1^2 + 0^2 \neq 0$.

Inverse: $\frac{a + b\sqrt{5}}{a + b\sqrt{5}} = 1$ so $a + b\sqrt{5} = \frac{1}{a + b\sqrt{5}} \in S$ since

$$\frac{1}{a + b\sqrt{5}} \frac{(a - b\sqrt{5})}{(a - b\sqrt{5})} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2} \sqrt{5} = \frac{a}{a^2 - 5b^2} \in \mathbb{Q}$$

$$\frac{-b}{a^2 - 5b^2} \in \mathbb{Q} \text{ if } a, b \in \mathbb{Q}. \left(\frac{a}{a^2 - 5b^2}\right)^2 + \left(\frac{-b}{a^2 - 5b^2}\right)^2 \neq 0 \text{ since } a, b \neq 0.$$

Since a and b cannot both be zero $a^2 - 5b^2 \neq 0$, unless $\frac{a}{b} = \sqrt{5}$, which is not possible since $a, b \in \mathbb{Q}$. So the inverse exists.

Associative: multiplication on \mathbb{R} is associative.

The 4 conditions for a group are met, so it is a group.

(b) if $x, y \in \mathbb{R}$ then $\frac{x}{y} = \sqrt{5}$, would be possible, so an inverse element would not exist.

4. If the order of an element is 1, it is e . Since $ee = ee$, e commutes.

If the order of elements a and b is 2, $a^2 = b^2 = (ab)^2 = e$.

So a, b and ab are all self inverses; i.e. $a = a^{-1}$, etc.

$$(ab)^2 = e$$

$$ab ab = e$$

$$a (abab) b = aeb \quad \text{left multiplying by } a \text{ and right multiplying by } b$$

$$eba e = ab$$

$$ba = ab.$$

OR

$$ab = (ab)^{-1}$$

$$ab = b^{-1}a^{-1} \quad \text{using the reversal rule}$$

$$ab = ba.$$

5. Closure: for $a, b \in \mathbb{R} \setminus \{0\}$, $\frac{a}{b} \in \mathbb{R} \setminus \{0\}$, so closed.

Associativity: $\frac{(\frac{1}{2})}{3} = \frac{1}{6} \neq \frac{1}{(\frac{2}{3})} = \frac{3}{2}$, so not associative.

There is no identity, because $\frac{a}{1} = a$ but $\frac{1}{a} \neq a$, for all $a \in \mathbb{R} \setminus \{0\}$.

Inverse: Since there is no identity, there cannot be an inverse.

6. Given $a \times a = a$. Since it is a group a^{-1} must exist. So multiply both sides by a^{-1} , giving $a^{-1} \times a \times a = a^{-1} \times a$ so $e \times a = e$ so $a = e$.

7. $a * b$ cannot be a , since that would mean $b = e$, which is not true. Similarly $a * b$ cannot be b . So $a * b =$ either e or c .

If $a * b = e$, $a = b^{-1}$ and $b = a^{-1}$. So $b * a * b * a = b * e * a$, which gives

$$e = b * a. \text{ So } b * a = b * a.$$

If $a * b = c$, then by the reasoning above $b * a = c$ also, so $b * a = b * a$.

8. a. $x * y = y * x^2$, given

$$x * y * y = y * x^2 * y, \quad \text{right multiplying by } y$$

$$x * e = y * x^2 * y, \quad \text{using } y^2 = e \text{ and associativity}$$

$$x = y * (x^2 * y). \quad \text{using associativity}$$

- b. $x * y = y * x^2$ given

$$x^2 * x * y * x = x^2 * y * x^2 * x, \text{ left multiplying by } x^2 \text{ and right multiplying by } x$$

$$y * x = x^2 * y. \quad \text{using } x^3 = e$$

c. $(x*y)^2$
 $= x*(y*x)*y$
 $= x*(x^2*y)*y$
 $= x^3*y^2$ using $y*x = x^2*y$
 $= e*e = e.$

Exercise 6.1

1. i.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

ii.

\times_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- ii. a. $x + 2 = 1$, add $2^{-1} = 3$, giving $x = 4$.
- b. $4x = 3$, $x = 2$. By trial and error. Note that the cancellation law (multiplying both sides by the “inverse”) does not always work because $\{\mathbb{Z}_5, \times_5\}$ is not a group.
- c. $3x + 4 = 2$. Add $4^{-1} = 1$, $3x = 3$, $x = 1$.
- d. $4x + 3 = 0$. Add $3^{-1} = 2$, $4x = 2$, $x = 3$.
- e. $3(x + 1) = 0$, $x + 1 = 0$. Add $1^{-1} = 4$, $x = 4$.

f. $4x = 2x + 1$. Add $3x$, $2x = 1$, $x = 3$.

2. i. $\{\mathbb{Z}_p \setminus \{0\}, \times_p\}$, where p is a prime forms a group. 7 is prime.

$\{\mathbb{Z}_n, +_n\}$ forms a group for $n \in \mathbb{N}$, $n \geq 2$. The cancellation laws hold for all groups.

ii, For $\{\mathbb{Z}_7, +_7\}$ $0^{-1} = 0$, otherwise $a^{-1} = 7 - a$.

For $\{\mathbb{Z}_7 \setminus \{0\}, \times_7\}$ $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$.

iii.

a. $x + 4 = 3$, add $4^{-1} = 3$, $x = 6$.

b. $2x = 5$, multiply by $2^{-1} = 4$, $x = 6$

c. $3x + 2 = 3$, add $2^{-1} = 5$, $3x = 1$, multiply by $3^{-1} = 5$, $x = 5$.

d. $5x + 6 = 0$, add $6^{-1} = 1$, $5x = 1$, multiply by $5^{-1} = 3$, $x = 3$.

e. $6x + 3 = 5$, add $3^{-1} = 4$, $6x = 2$, multiply by $6^{-1} = 6$, $x = 5$.

f. $4x + 1 = 2x$, add $5x$, since $2^{-1} = 5$, $2x + 1 = 0$, add $1^{-1} = 6$, $2x = 6$, multiply by $2^{-1} = 4$, $x = 3$.

3. a. The Cayley table is:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

So it is closed. The identity element, $I = 0$, inverses: $0^{-1} = 0$, $1^{-1} = 2$, $2^{-1} = 1$, it is associative, because $\text{Rem}(a + b) = \text{Rem}(\text{Rem}(a) + \text{Rem}(b))$.

b. $0 +_3 1 = 0$ and $0 +_3 2 = 0$, so it does not have the Latin Square Property, so it is not a group.

c. $0 +_3 1 = 0$ and $0 +_3 2 = 0$, so it does not have the Latin Square Property, so it is not a group.

So it is closed, identity element: $I = 1$, inverses: $1^{-1} = 1$, $2^{-1} = 2$.

Associativity: Yes. So it is a group.

d. It is not closed: $2 \times_4 2 = 0$, so it is not a group.

e. The Cayley table is:

\times_{10}	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

It is closed, identity element: $I = 6$, inverses: $2^{-1} = 8$, $8^{-1} = 2$, $6^{-1} = 6$, $4^{-1} = 4$. Associativity: Yes, it holds, so it is a group.

f. The Cayley table is:

\times_{12}	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

It is closed, identity element: $I = 1$, inverses: $1^{-1} = 1$, $5^{-1} = 5$, $7^{-1} = 7$, $11^{-1} = 11$. Associativity: Yes, it holds. So it is a group.

g. The Cayley table is:

\times_{15}	1	2	4	8
1	1	2	4	8
2	2	4	8	1
4	4	8	1	2
8	8	1	2	4

It is closed, identity element: $I = 1$, inverses: $1^{-1} = 1$, $2^{-1} = 8$, $8^{-1} = 2$, $4^{-1} = 4$. Associativity: Yes, it holds. So it is a group.

h. The Cayley table is:

\times_{15}	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

It is closed. Identity element: $I = 6$. Inverses: $3^{-1} = 12$, $12^{-1} = 3$, $6^{-1} = 6$, $9^{-1} = 9$. Associativity: Yes, it holds. So it is a group.

i. The Cayley table is:

\times_{11}	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

It is closed. Identity element: $I = 1$. Inverses: $3^{-1} = 4$, $4^{-1} = 3$, $5^{-1} = 9$, $9^{-1} = 5$. Associativity: Yes, it holds. So it is a group.

j. The Cayley table is:

\times_{14}	2	4	6	8	10	12
2	4	8	12	2	6	10
4	8	2	10	4	12	6
6	12	10	8	6	4	2
8	2	4	6	8	10	12
10	6	12	4	10	2	8
12	10	6	2	12	8	4

It is closed. Identity element: $I = 8$. Inverses: $2^{-1} = 4$, $4^{-1} = 2$, $6^{-1} = 6$, $8^{-1} = 8$, $10^{-1} = 12$, $12^{-1} = 10$. Associativity: Yes, it holds. So it is a group.

k. The Cayley table is:

\times_{14}	1	3	5	7	9	11	13
1	1	3	5	7	9	11	13
3	3	9	1	7	13	5	11
5	5	1	11	7	3	13	9
7	7	7	7	7	7	7	7
9	9	13	3	7	11	1	5
11	11	5	13	7	1	9	3
13	13	11	9	7	5	3	1

From the 7 row and column, it is not a group.

l. The Cayley table is:

\times_{14}	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

It is closed. Identity element: $I = 1$. Inverses: $3^{-1} = 5$, $5^{-1} = 3$, $9^{-1} = 11$, $11^{-1} = 9$, $13^{-1} = 13$. Associativity: Yes, it holds. So it is a group.

m. There is no identity element, so it is not a group.

n. $\{\mathbb{Z}_n, +_n\}$ forms an Abelian group for $n \in \mathbb{N}$, $n \geq 2$. So it is a group.

o. The Cayley table is:

\times_9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

It is closed. Identity element: $I = 1$. Inverses: $2^{-1} = 5$, $5^{-1} = 2$, $4^{-1} = 7$, $7^{-1} = 4$, 8 is self inverse. Associativity: Yes, it holds. So it is a group.

Exercise 6.2

1.

\circ	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

It is closed.

From the Cayley table e is the identity element.

Inverses: $e^{-1} = e$, $f^{-1} = f$, $h^{-1} = h$, $g^{-1} = g$.

Composition of functions is associative, therefore it holds for a subset as well.

The Cayley table is symmetric about the main diagonal, so it is an Abelian group.

2.

\circ	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	f	e
h	h	g	e	f

It is closed.

From the Cayley table e is the identity element.

Inverses: $e^{-1} = e, f^{-1} = f, h^{-1} = g, g^{-1} = h$.

Composition of functions is associative, therefore it holds for a subset as well.

The Cayley table is symmetric about the main diagonal, so it is an Abelian group.

3. It is not closed, because $p \circ f = \frac{x}{x-1}$. So it is not a group.

4.

\circ	f	g	h
f	f	g	h
g	g	h	f
h	h	f	g

It is closed.

From the Cayley table f is the identity element.

Inverses: $f^{-1} = f, g^{-1} = h, h^{-1} = g$.

Composition of functions is associative, therefore it holds for a subset as well.

The Cayley table is symmetric about the main diagonal.

So it is an Abelian group.

5.

\circ	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

It is closed.

From the Cayley table b is the identity element.

Inverses: $a^{-1} = a, b^{-1} = b, c^{-1} = c, d^{-1} = d$.

Composition of functions is associative therefore it holds for a subset as well.

Mathematics HL Topic 8: Sets, Relations and Groups

The Cayley table is symmetric about the main diagonal, so it is an Abelian group.

6. It is not closed, because $f \circ g = \frac{1-x}{x+1}$. So it is not a group.

7.

\circ	e	n	g	k	m	h
e	e	n	g	k	m	h
n	n	e	k	g	h	m
g	g	m	e	h	n	k
k	k	h	n	m	e	g
m	m	g	h	e	k	n
h	h	k	m	n	g	e

It is closed.

From the Cayley table e is the identity element.

Inverses: $e^{-1} = e$, $n^{-1} = n$, $g^{-1} = g$, $k^{-1} = m$, $m^{-1} = k$, $h^{-1} = h$.

Composition of functions is associative therefore it holds for a subset as well.

So it is a group.

$h \circ k = g \neq k \circ h = n$. So it is not Abelian.

Exercise 6.3

1.

a. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

b. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

c. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

d. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

2.

a. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

b. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

c. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$,

d. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

3. a. i.

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$q^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$q^{-1}p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$pq = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$(pq)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Indeed, both equal: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

ii. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Indeed, both equal: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

b.

i. $x = qp^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

ii. $x = pq^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

iii. $x = p^{-1}q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

iv. $x = q^{-1}p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

4. a. Make a Cayley table:

	W	X	Y	Z
W	W	X	Y	Z
X	X	W	Z	Y
Y	Y	Z	W	X
Z	Z	Y	X	W

Closure: Yes.

Associative: Composition of permutations is associative.

Identity: W.

Inverse: X, Y and Z are self inverse.

It is a group because it satisfies the four group properties.

It is Abelian because it is symmetric about the main axis.

X , Y and Z are of order 2, W is of order 1.

b. Make a Cayley table:

	W	X	Y	Z
W	W	X	Y	Z
X	X	Y	Z	W
Y	Y	Z	W	X
Z	Z	W	X	Y

Closure: Yes.

Associative: Composition of permutations is associative.

Identity: W .

Inverse: $X^{-1} = Z$, $Z^{-1} = X$, Y is self inverse.

It is a group because it satisfies the four group properties.

It is Abelian, because it is symmetric about the main axis.

X and Z are of order 4, Y is of order 2.

5. a. i. x ii. y iii. e iv. x v. y vi. x vii. e viii. s

b. i. $a = er^{-1} = s$ ii. $a = s^{-1}r = s$ iii. $a = ys^{-1} = z$ iv. $a = zy^{-1} = s$

Exercise 6.4

1. a. $(1\ 5)(2\ 3)$ b. $(1\ 2\ 3\ 4\ 5)$ c. $(1\ 5)(2\ 3\ 4)$

2. a. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ b. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ c. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$ d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 5 & 1 \end{pmatrix}$

e. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

3. $p = (476)(235)$. For p^2 each number is moved by two positions in the cycle for p , so $p^2 = (467)(253)$. For p^{-1} each cycle in p must be reversed, so $p^{-1} = (467)(253)$.

4. $p^2 = (1\ 3\ 2)$, $p^3 = (1)(2)(3) = Id$, $p^k = (1)(2)(3) \dots (k) = Id$

5. $pq = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $qp = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$. Yes.

6. $pq = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 4 & 6 & 1 \end{pmatrix} qp = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 4 & 6 & 3 \end{pmatrix}$. No.
7. a. (1 3 5), b. (1 2) (4 5), c. (1 2 3 4 5), d. (1 2 3 4 5), e. (1 4).
8. a. $3! = 6$ b. (1), (12), (13), (23), (123), (132)

c. Let's do a few (working right to left)

(12)(13): $1 \rightarrow 3, 2 \rightarrow 1, 3 \rightarrow 1 \rightarrow 2$ so (12)(13) = (132)

(123) (23): $1 \rightarrow 2, 2 \rightarrow 3 \rightarrow 1, 3 \rightarrow 2 \rightarrow 3$, so (123) (23) = (12)(3) = (12)

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Exercise 6.5

1. a. $a (b c) = a r_1 = b$
 b. $a r_1 (b r_2) = a (r_1 a) = a c = r_2$
 c. $(r_1)^2 r_2 = r_1 (r_1 r_2) = r_1 r_0 = r_1$
 d. $r_1^{-1} (r_2^{-1})^2 = r_2 r_1^2 = r_2 r_2 = r_1$
 e. $a r_2 a^{-1} = a r_2 a = a b = r_1$
2. a. $y = r_1^{-1} c = r_2 c = a$
 b. $y = r_1 r_2^{-1} = r_1 r_1 = r_2$
 c. $y = a^{-1} r_2 c^{-1} = a r_2 c = a a = r_0$
3. a. $a (b d) = a r_A = c$
 b. $(a r_1) (b r_2) = c a = r_3$
 c. $(r_1)^2 r_2 = r_2 r_2 = r_0$
 d. $r_1^{-1} (r_2^{-1})^2 = r_3 r_2^2 = r_3 r_0 = r_3$

e. $(dr_2)a^{-1} = ca = r_3$

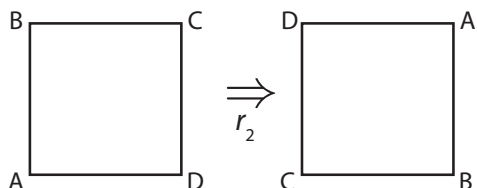
4. a. $y = r_1^{-1}c = b$

b. $y = r_1r_2^{-1} = r_1r_2 = r_3$

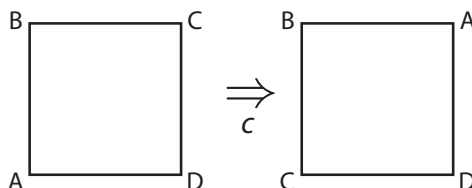
c. $y = a^{-1}r_3d^{-1} = ar_3d = r_0$

5. a.

i.



ii.



so i. r_2 ii) c

b. There are $4! = 24$ permutations, but only 8 symmetries so no.

For example $\begin{pmatrix} A & B & C & D \\ A & B & D & C \end{pmatrix}$ is not possible.

6.

notation symmetry

r_0 rotation about O through 0° – do nothing

r_1 rotation about O through 120° anti-clockwise

r_2 rotation about O through 240° anti-clockwise

*	r_0	r_1	r_2
r_0	r_0	r_1	r_2
r_1	r_1	r_2	r_0
r_2	r_2	r_0	r_1

It is closed. r_0 is the identity element. $r_0^{-1} = r_0$, $r_1^{-1} = r_2$, $r_2^{-1} = r_1$. It is commutative. So it is a group. It is an Abelian group since the Cayley table has a line of symmetry along the leading diagonal.

7.

notation symmetry

r_0 rotation about O through 0° – do nothing

r_1 rotation about O through 90° anti-clockwise

r_2 rotation about O through 180° anti-clockwise

r_3 rotation about O through 270° anti-clockwise

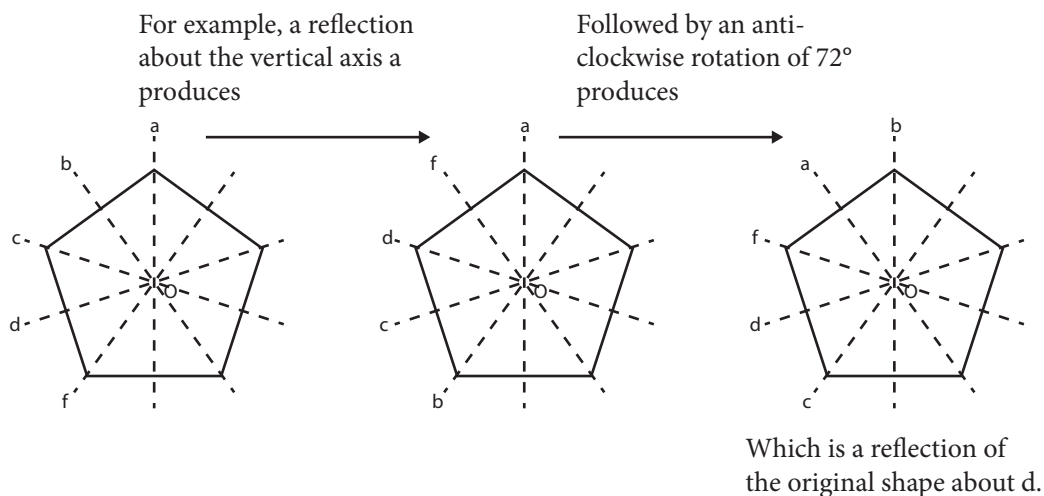
*	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

It is closed. r_0 is the identity element. $r_1^{-1} = r_3, r_3^{-1} = r_1$. The operations r_2 and r_0 are self inverse. So it is a group. It is an Abelian group since the Cayley table has a line of symmetry along the leading diagonal, that is, it is commutative. .

8. The operation is composition of symmetries. Because there are 10 symmetries, it is too tiresome to construct a Cayley table.

First we check closure. The composition of two rotations is one of the rotations r_0 to r_4 .

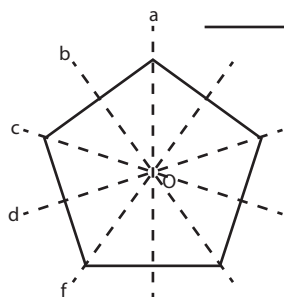
The composition of a reflection and a rotation is one of the reflections a to f . We check one example.



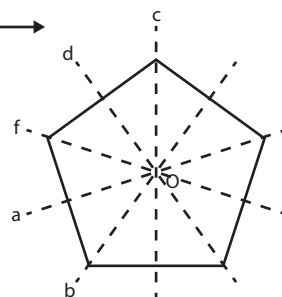
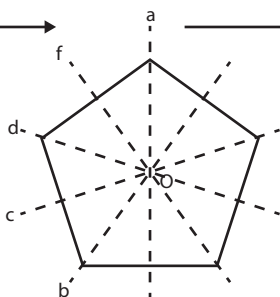
You may use the fact that every rotation is a composition of two reflections with lines of symmetry intersecting at the centre of rotation. The angle enclosed by the lines must be half the angle of rotation.

The composition of two of the reflections a to f is one of the rotations r_0 to r_4 .

For example a reflection of the original state about the vertical axis a produces



Then a reflection about b produces



Which is an anti-clockwise rotation of $4 \times 72^\circ$ of the original

You may use the fact that the composition of two reflections with intersecting lines of symmetry is a rotation centred on the intersection of the lines. The angle of rotation is double the angle between the lines.

We certainly do not want to check associativity case by case for the 1000 cases. Fortunately this is another example of composition of functions which is associative.

The identity element is r_0 a rotation of 0° .

Reflections are self inverses. r_1 and r_4 are inverses. r_2 and r_3 are inverses.

9. The set is the set of all rotations of Rubik's Cube. The group operation is function composition, that is, chaining rotations. The identity operation is doing nothing. For any rotation the inverse is rotating it backwards.
10. b. We can rotate 120° or 240° about a line running from each vertex to the centre of the opposite face for 8 rotations. We can rotate about a line through the midpoint of an edge and its opposite vertex for 3 rotations and we can do nothing for a total of 12 rotations.¹ There are also reflections in a plane through one edge and the opposite midpoint.

Exercise 7.1

1. a. The Cayley table is:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

0 is the identity element. 0 cannot be the generator since it has an order equal to 1.

¹ Symmetries in 3D objects is not in the IB syllabus.

$1^1 = 1, 1^2 = 2, 1^3 = 0, 2^1 = 2, 2^2 = 1, 2^3 = 0$. Therefore 1 and 2 have order 3 and are generators.

It is cyclic, since it has generators.

Alternately since it is a group of prime order, it must be cyclic.

b. The Cayley table is:

$+_6$	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

0 cannot be the generator since it has an order equal to 1.

$$1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 4, 1^5 = 5, 1^6 = 0,$$

$$2^1 = 2, 2^2 = 4, 2^3 = 0,$$

$$3^1 = 3, 3^2 = 0,$$

$$4^1 = 4, 4^2 = 2, 4^3 = 0,$$

$$5^1 = 5, 5^2 = 4, 5^3 = 3, 5^4 = 2, 5^5 = 1, 5^6 = 0.$$

2 and 4 are order 3. 3 is order 2. 1 and 5 are order 6 and so are generators. It is cyclic since it has a generator.

Alternatively, since 1 does not have order 1, 2 or 3, by Lagrange's theorem it must have order 6 and be a generator. Since $5 = 1^{-1}$, it must be a generator too.

c. The Cayley table is:

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1 cannot be the generator since it has an order equal to 1.

$$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1,$$

$$3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1,$$

$$4^1 = 4, 4^2 = 1.$$

4 has order 2. 2 and 3 have order 4 and are generators. It is cyclic, since it has generators.

Alternatively, since 2 and 3 do not have order 1 or 2, by Lagrange's theorem they must have order 4 and be generators.

d. The Cayley table is:

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1 cannot be the generator since it has an order equal to 1.

$$2^2 = 4, 2^3 = 1,$$

$$3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1,$$

$$4^2 = 2, 4^3 = 1,$$

$$5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3, 5^6 = 1.$$

$$6^2 = 1.$$

2 and 4 are order 3. 6 is order 2.

3 and 5 are order 6 and so generators. It is cyclic, since it has generators.

Alternatively, since 3 does not have order 1, 2 or 3, by Lagrange's theorem it must have order 6 and be a generator. Since $5 = 3^{-1}$, it must be a generator too.

e. The Cayley table is

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

2 and 6 have order 4. 4 has order 2. 1, 3, 5, and 7 have order 8 and so are generators. It is cyclic, since it has generators.

Alternatively, since 1 and 3 do not have order 1, 2 or 4, by Lagrange's theorem it must have order 8 and be a generator. Since $5 = 3^{-1}$, and $7 = 1^{-1}$, they must be a generator too.

Note that since $1^2 = 2 \neq 0$, it's not order 2. From Lagrange's theorem elements must be order 1, 2, 4 or 8. So check $1^4 = (1^2)^2 = 2^2 = 4 \neq 0$. So from Lagrange's theorem 1 is order 8.

f. The Cayley table is:

\times_{14}	2	4	6	8	10	12
2	4	8	12	2	6	10
4	8	2	10	4	12	6
6	12	10	8	6	4	2
8	2	4	6	8	10	12
10	6	12	4	10	2	8
12	10	6	2	12	8	4

8 is the identity element. 8 cannot be the generator since it has an order equal to 1.

$$2^2 = 4, 2^3 = 8,$$

$$4^2 = 2, 4^3 = 8,$$

$$6^2 = 8,$$

$$10^2 = 2, 10^3 = 6, 10^4 = 4, 10^5 = 12, 10^6 = 8,$$

$$12^2 = 4, 12^3 = 6, 12^4 = 2, 12^5 = 10, 12^6 = 8.$$

2 and 4 are order 3. 6 is order 2, 10 and 12 are order 6 and so generators. It is cyclic, since it has generators.

Alternatively, since 10 does not have order 1, 2 or 3, by Lagrange's theorem it must have order 6 and be a generator. Since $12 = 10^{-1}$, it must be a generator too.

g. The Cayley table is:

\times_{15}	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

6 is the identity element. 6 cannot be the generator since it has an order equal to 1.

$$3^2 = 9, 3^3 = 12, 3^4 = 6,$$

$$9^2 = 6,$$

$$12^2 = 9, 12^3 = 3, 12^4 = 6.$$

9 is order 2, 3 and 12 are order 4 and so generators. It is cyclic, since it has generators.

h. The Cayley table is:

\times_{10}	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

6 is the identity element. 6 cannot be the generator since it has an order equal to 1.

$$2^2 = 4, 2^3 = 8, 2^4 = 6,$$

$$4^2 = 6,$$

$$8^2 = 4, 8^3 = 2, 8^4 = 6.$$

4 is order 2, 2 and 8 are order 4 and so generators. It is cyclic, since it has generators.

i. The Cayley table is:

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

1 is the identity element. 1 cannot be the generator since it has an order equal to 1. 9 has order 2. 3 and 7 have order 4 and so are generators. It is cyclic, since it has generators.

j. The Cayley table is:

\times_8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

1 is the identity element. 1 cannot be the generator since it has an order equal to 1.

$3^2 = 1, 5^2 = 1, 7^2 = 1$, so 3, 5 and 7 have order 2.

It is not cyclic, since it has no generator, that is, it has no element of order 4.

k. The Cayley table is:

\times_{12}	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

1 is the identity element. 1 cannot be the generator since it has an order equal to 1.

5, 7 and 11 are all order 2. So there are no generators. It is not cyclic, since it has no generators.

l. The Cayley table is:

\times_{15}	1	2	4	8
1	1	2	4	8
2	2	4	8	1
4	4	8	1	2
8	8	1	2	4

1 is the identity element. 1 cannot be the generator since it has an order equal to 1.

4 is order 2.

2 and 8 are order 4 and so generators. It is cyclic, since it has generators.

m. The Cayley table is:

\times_{11}	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

1 is the identity element. 1 cannot be the generator since it has an order equal to 1. 3, 4, 5 and 9 are all order 5, so generators. It is cyclic, since it has generators.

Alternately since it is a group of prime order, it must be cyclic.

n. $\{1, 2, 4, 5, 7, 8\}$ under \cdot_9 :

The Cayley table is:

\times_9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

1 is order 1. 8 is order 2. 4, 7 are order 3.

2 and 5 are order 6 and so are generators. It is cyclic, since it has generators.

Alternatively, since 2 does not have order 1, 2 or 3, by Lagrange's theorem it must have order 6 and be a generator. Since $5 = 2^{-1}$, it must be a generator too.

- o. e is order 1. a, b and c are order 2. There are no elements of order 4, so it is not cyclic.
- p. Each element is order 2, except r_0 (order 2). There are no elements of order 4, so it is not cyclic.
- q. r_0 is order 1. r_2, a, b, c and d are order 2. r_3 and r_1 are order 4. There are no elements of order 8, so it is not cyclic.
- r. The Cayley table is:

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

1 is the identity element. 1 cannot be the generator since it has an order equal to 1.

$(-1)^2 = 1$. -1 is not a generator.

$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$. $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$. Therefore i and $-i$ are generators. It is cyclic, since it has generators.

- s. The Cayley table is:

\circ	e	n	g	k	m	h
e	e	n	g	k	m	h
n	n	e	m	h	g	k
g	g	k	e	n	h	m
k	k	g	h	m	e	n
m	m	h	n	e	k	g
h	h	m	k	g	n	e

n, g and h have order 2, m and k have order 3.

It is not cyclic, since it has no generator, that is, it has no element of order 6.

- t. Call a rotation about the centre of $n \times 60^\circ$ r_n , where $n = 0, 1, 2, 3, 4, 5$.

r_0 cannot be the generator since it has an order equal to 1.

$$r_1^2 = r_2, r_1^3 = r_3, r_1^4 = r_4, r_1^5 = r_5, r_1^6 = r_0,$$

$$r_2^2 = r_4, r_2^3 = r_0,$$

$$r_3^2 = r_0,$$

$$r_4^2 = r_2, r_4^3 = r_0,$$

$$r_5^2 = r_4, r_5^3 = r_3, r_5^4 = r_2, r_5^5 = r_1, r_5^6 = r_0.$$

Therefore r_1 and r_5 are the generators. It is cyclic, since it has generators.

2. e has order 1. Since the group is cyclic with order 8, $x^k = x^{k \bmod 8}$ and $x^8 = x^0 = e$.

Since 3, 5 and 7 have no common factor > 1 with 8 are not factors of 8, the lowest power of x^3, x^5, x^7 that equals x^0 is the 8th power. Therefore x, x^3, x^5, x^7 generate the group.

Since $2 \times 4 \pmod{8} = 0$ and $6 \times 4 \pmod{8} = 0$, x^2 and x^6 have order 4.

Since $4 \times 2 \pmod{8} = 0$, x^4 has order 2.

3. e has order 1. The group is cyclic with order 7. Since 7 is prime, the lowest power of $a, a^2, a^3, a^4, a^5, a^6$ that equals $a^0 = e$ is the 7th power, so they all generate the group.

4. a. i. $(ab)^2 = b^4$ gives $abab = bbbb$. The right cancellation law gives $aba = b^3$.

ii. $a^2 = (ab)^2$ gives $aa = abab$. The left cancellation law gives $a = bab$.

b. i. $a^3b \neq e$, because if it did, then $a^4b = ae$, so $b = a$, which is not true. So a^3b is not order 1.

ii. $(a^3b)^2 = (a^3b)(a^3b) = a^2(aba)a^2b = b^4(b^3)b^4b = b^4b^4b^4 = a^2a^2a^2 = e$ $a^2 = a^2 \neq e$. So a^3b is not order 2.

$(a^3b)^3 = (a^3b)^2(a^3b) = a^2a^3b = eab = ab \neq e$, because if it did, then $(ab)^2 = e$, so $abab = e$, so $b^4 = e$, so $a^2 = e$ which is false. So a^3b is not order 3.

$(a^3b)^4 = a^2a^2 = a^4 = e$. So a^3b is order 4.

ii. Similarly b^3a is of order 4.

5. The elements of C are all of the form x^p , where p is a positive integer. Since x is of order n , $x^n = e$, where e is the identity. There must be integers q and r such that $p = nq + r$, where $q \geq 0$, $0 \leq r \leq n-1$.

If $r = 0$, $x^p = (x^n)^q = e^q = e$.

If $r \neq 0$, $x^p = x^{nq+r} = (x^n)^q x^r = e^q x^r = x^r$.

Thus, for all values of p , x^p is an element of the set $\{e, x, x^2, x^3, \dots, x^{n-1}\}$.

Now we must show that they are all distinct. We assume that there are at least two elements that are not distinct. If $x^s = x^t$, where $0 < t < s \leq n$, then $x^{s-t} = e$. Therefore $s - t$ is a multiple of n , but this is impossible if s and r are both less than or equal to n , so they are all distinct.

6. a. The solutions of $z^4 = 1$ are $1, -1, i, -i$. But 1 is the identity and -1 has order 2. i and $-i$ have order 4.

b. The solutions of $z^3 = 1$ are $1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

But 1 is the identity. $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$ have order 3.

Exercise 7.2

1. The Cayley table is

Δ	X	Y	Z	\emptyset
X	\emptyset	Z	Y	X
Y	Z	\emptyset	X	Y
Z	Y	X	\emptyset	Z
\emptyset	X	Y	Z	\emptyset

It is closed. The identity element, $e = \emptyset$. Each element is a self inverse.

Δ is associative on sets therefore it is associative on a subset as well.

The subgroups are $\{\emptyset\}, \{\emptyset, X\}, \{\emptyset, Y\}, \{\emptyset, Z\}$, since they are closed.

2. The Cayley table is

\times_{18}	2	4	8	10	14	16
2	4	8	16	2	10	14
4	8	16	14	4	2	10
8	16	14	10	8	4	2
10	2	4	8	10	14	16
14	10	2	4	14	16	8
16	14	10	2	16	8	4

It is closed. The identity element, $e = 10$.

Inverses: $2^{-1} = 14, 14^{-1} = 2, 4^{-1} = 16, 16^{-1} = 4, 8^{-1} = 8,$

Associativity: Yes.

So it is a group.

Proper subgroups are $\{10, 8\}$, $\{10, 4, 16\}$.

Exercise 7.3

$$1. \quad 0H = \{m \mid m = 4k, k \in \mathbb{Z}\} = H. \qquad 1H = \{m \mid m = 4k + 1, k \in \mathbb{Z}\}.$$

$$2H = \{m \mid m = 4k + 2, k \in \mathbb{Z}\}. \qquad 3H = \{m \mid m = 4k + 3, k \in \mathbb{Z}\}.$$

$4H = 0H$, $5H = 1H$, etc. When taking negative integers you get the cosets above: $-1H = 3H$, $-2H = 2H$, etc.

Therefore we have 4 cosets: $\{m \mid m = 4k, k \in \mathbb{Z}\}$, $\{m \mid m = 4k + 1, k \in \mathbb{Z}\}$, $\{m \mid m = 4k + 2, k \in \mathbb{Z}\}$, $\{m \mid m = 4k + 3, k \in \mathbb{Z}\}$. Notice that the 4 sets are disjoint and their union is the whole group. Therefore the 4 cosets form a partition of \mathbb{Z} .

2. Take one element from the group and add it to all elements of the subgroup $\{0, 4, 8\}$.

Adding 0 to H gives $0H = \{0, 4, 8\}$.

Adding 1 to H gives $1H = \{1, 5, 9\}$.

Adding 2 gives $2H = \{2, 4, 6\}$. Adding 3 to H gives $3H = \{3, 9, 11\}$.

You can see that $4H = 0H$, $5H = 1H$, etc. Therefore there are no new cosets formed when the rest of the elements of the group are used.

We have 4 cosets which form a partition of \mathbb{Z}_{12} .

3. It is false. In D_4 $r_1H = \{r_1r_0, r_1d\} = \{r_1, a\} = aH = \{ar_0, ad\} = \{a, r_1\}$.

But $Hr_1 = \{r_0r_1, dr_1\} = \{r_1, b\} \neq Ha = \{r_0a, da\} = \{a, r_3\}$.

4. $Hb = \{hb \mid h \in H\}$. $b = eb \in Hb$, since $e \in H$. Since $Ha = Hb$, $b \in Ha$.

$$5. \quad 1H = \left\{1, \operatorname{cis} \frac{2\pi}{3}, \operatorname{cis} \frac{4\pi}{3}\right\} \qquad \operatorname{cis} \frac{\pi}{3} H = \left\{\operatorname{cis} \frac{\pi}{3}, -1, \operatorname{cis} \frac{5\pi}{3}\right\}$$

$$\operatorname{cis} \frac{2\pi}{3} H = \left\{\operatorname{cis} \frac{2\pi}{3}, \operatorname{cis} \frac{4\pi}{3}, 1\right\} \qquad -1 H = \left\{-1, \operatorname{cis} \frac{5\pi}{3}, \operatorname{cis} \frac{\pi}{3}\right\}$$

$$\operatorname{cis} \frac{4\pi}{3} H = \operatorname{cis} \frac{\pi}{3} \left\{\operatorname{cis} \frac{4\pi}{3}, 1, \operatorname{cis} \frac{2\pi}{3}\right\} \qquad \operatorname{cis} \frac{5\pi}{3} H = \left\{\operatorname{cis} \frac{5\pi}{3}, \operatorname{cis} \frac{\pi}{3}, -1\right\}$$

$$6. \quad aH = \{ar_0, aa\} = \{a, r_0\} \qquad bH = \{br_0, ba\} = \{b, r_1\}$$

$$r_1H = \{r_1r_0, r_1a\} = \{r_1, b\} \qquad r_0H = \{r_0r_0, r_0a\} = \{r_0, a\}$$

Exercise 7.4

1. a. $\{r_3\}, \{r_1, r_2, r_3\}, \{r_3, a\}, \{r_3, b\}, \{r_3, c\}$
 b. $\{\}, \{1, -1\}, \{1, -1, i, -i\}$ c. $\{\}, \{1, 6\}, \{1, 2, 4\}$ d. $\{6\}, \{6, 9\}$
2. a. Yes. It is closed; the sum of two even integers is even. 0 is included. Every element has its inverse.
 b. No, since it is not closed; the sum of two odd integers is even.
 c. No, since no element but zero has an inverse.
 d. Yes, since it is closed, the sum of two integers divisible by 3 is divisible by 3. 0 is included. Every element has its inverse.

3. a. No, because only 1 has an inverse. b. Yes, because it has the 4 properties.
 c. No, because only 1 has an inverse.

4. a. e is order 1, x, y and z are order 2, r and s are order 3.
 b. $z \circ s = y, s \circ z = x$ c. $\{e, r, s\}$
 d. r and s are both generators. e. $\{e, x\}, \{e, y\}, \{e, z\}$ and S itself.

5. a. $(ab)(ab) = e$
 $a(ab)(ab)b = aeb$ left multiplying by a and right multiplying by b
 $(aa)ba(bb) = aeb$ using associativity
 $ba = ab$ using $g^2 = e$ and the identity property

b. From the given information the Cayley table must be:

*	e	a	b
e	e	a	b
a	a	e	
b	b		e

c. Yes as below

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

6. $\{e\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e, a, b, c\}$.

IB Exam Type Problems

- Since S is cyclic, there is an $a \in S$ such that a generates S . We will do a proof by contradiction. We assume that (finite) S is **not** of prime order; we assume $|S| = m \times n$, $m, n \in \mathbb{Z}$, $m, n \neq 1$. If so, a^m generates a subgroup of order n , but this is a contradiction, since G has no non-trivial proper subgroups, so S must be of prime order. Now suppose S is an infinite cyclic group. If so, a^2 (along with e) will generate an infinite proper subgroup, but this is a contradiction, since G has no non-trivial proper subgroups, so S must be of finite order.
- Find the identity element, e . $x * e = x = x + e + a x e$, which gives $e = 0$. Find an element b which is self-inverse. $b * b = e = 0 = b + b + abb$, which gives $0 = (2 + ab) b$. Since b is not the identity, element $b = -2/a$. So the subgroup is $\{0, -2/a\}$.
- $(S, *)$ must contain an element, a , which is different from e , its identity element. The order of element a is equal to the order n of the subgroup it generates. By Lagrange's theorem n must be a factor of p . Since p is prime, either $n = 1$ or $n = p$. Since $a \neq e$, $n \neq 1$ and therefore $n = p$. Since the order of a is p , a generates $(S, *)$, which is therefore cyclic.
- A cyclic group has a generator, a such that all elements of the group $= a^n$, for some $n \in \mathbb{Z}$.
- Since S is cyclic, it has at least one generator, a . That is $a^m = e$. Multiplying both sides of this equation by $(a^{-1})^m$ gives $a^m \circ (a^{-1})^m = e \circ (a^{-1})^m$, which gives $e = (a^{-1})^m$. Therefore a^{-1} is also order m , so it too is a generator. But what if a is self-inverse? Then $m = 2$ and S is order 2, which is a contradiction. So S must have more than one generator.
- The sixth roots are $z_0 = 1, z_1 = \text{cis } \frac{\pi}{3}, z_2 = \text{cis } \frac{2\pi}{3}, z_3 = -1, z_4 = \text{cis } \frac{4\pi}{3}, z_5 = \text{cis } \frac{5\pi}{3}$. The Cayley table is:

\times	z_0	z_1	z_2	z_3	z_4	z_5
z_0	z_0	z_1	z_2	z_3	z_4	z_5
z_1	z_1	z_2	z_3	z_4	z_5	z_0
z_2	z_2	z_3	z_4	z_5	z_0	z_1
z_3	z_3	z_4	z_5	z_0	z_1	z_2
z_4	z_4	z_5	z_0	z_1	z_2	z_3
z_5	z_5	z_0	z_1	z_2	z_3	z_4

Closure: From the table S is closed.

Associativity: Multiplication of complex numbers is associative.

Identity: z_0 .

Inverses: $z_1^{-1} = z_5, z_2^{-1} = z_4, z_4^{-1} = z_2, z_3^{-1} = z_3$

$\text{cis } \frac{\pi}{3}$ and $\text{cis } \frac{5\pi}{3}$ are generators. Therefore S is cyclic.

7. a. i. a is order 2, b is order 2, c is order 2, e is order 1.
 ii. a is order 4, b is order 4, c is order 2, e is order 1.
 b. i. $\{e, a\}$, $\{e, b\}$, $\{e, c\}$. ii. $\{e, c\}$.

Exercise 8.1

1. $\{\mathbb{Z}_4, +_4\}$ is a group. \mathbb{Z}_4 under subtraction modulo 4 is not a group, for example it's not closed, so it cannot be isomorphic to $\{\mathbb{Z}_4, +_4\}$.
 2. Determine which of the following groups of order four are isomorphic.
- a. The operation table is.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- b. The operation table is.

\circ	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	f	e
h	h	g	e	f

- c. The operation table is.

$*$	r_0	a	b	r_1
r_0	r_0	a	b	r_1
a	a	r_0	r_1	b
b	b	r_1	r_0	a
r_1	r_1	b	a	r_0

d. The operation table is.

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

e. The operation table is.

\circ	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

All elements of groups c and e except the identity element have order 2, groups c and e are isomorphic. $f: r_1 \rightarrow d, r_0 \rightarrow b, a \rightarrow a, b \rightarrow c$.

Groups a, b and d have the identity element, one element of order 2 and 2 elements of order 4, so groups a, b and d are isomorphic.

Possible bijections are: $k(0) = e, k(2) = f, k(1) = g, k(3) = h$

and $l(e) = l, l(f) = g, l(g) = 3, l(h) = 7$.

Remember that once we saw that an element was not of order 1 or 2 (in a group of order 4) it must be of order 4, because 3 is not a factor of 4 and because the Latin Square property requires every element to have an order less than or equal to the order of the group.

3. The operation table for S is:

$*$	a	b	r_1	r_0
a	r_0	r_1	b	a
b	r_1	r_0	a	b
r_1	b	a	r_0	r_1
r_0	a	b	r_1	r_0

The operation table for T is:

\times_8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

All elements of groups S and T except the identity element have order 2.

The isomorphism $f: S \rightarrow T$ is $r_0 \mapsto 1, r_1 \mapsto 3, a \mapsto 5, b \mapsto 7$. (Except that it must be $r_0 \mapsto 1$, all other possible mappings are also correct.) So groups S and T are isomorphic.

4. The Cayley table for T is.

$+_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The identity element is 1. 4 has order 2. 2 and 3 have order 4.

The Cayley table for H is:

\times_{10}	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

The identity element is 6. 4 has order 2. 2 and 8 have order 4.

The two possible isomorphisms are: $f: T \rightarrow H: 1 \mapsto 6, 4 \mapsto 4, 2 \mapsto 2, 3 \mapsto 8$ and $g: T \rightarrow H: 1 \mapsto 6, 4 \mapsto 4, 2 \mapsto 8, 3 \mapsto 2$.

5. The Cayley table for G_1 is:

$+_6$	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

The identity element is 0. 3 has order 2. 2 and 4 have order 3. 1 and 5 have order 6.

The Cayley table for G_2 is:

\times_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

The identity element is 1. 6 has order 2. 2 and 4 have order 3. 3 and 5 have order 6.

The Cayley table for G_3 is

\circ	r_0	r_1	r_2	a	b	c
r_0	r_0	r_1	r_2	a	b	c
r_1	r_1	r_2	r_0	c	a	b
r_2	r_2	r_0	r_1	b	c	a
a	a	b	c	r_0	r_1	r_2
b	b	c	a	r_2	r_0	r_1
c	c	a	b	r_1	r_2	r_0

The identity element is r_0 . a , b and c have order 2. r_1 and r_2 have order 3.

Since G_1 and G_2 have elements with the same orders they are isomorphic.

One possible bijection is: $f: G_1 \rightarrow G_2, 0 \rightarrow 1, 3 \rightarrow 6, 2 \rightarrow 2, 4 \rightarrow 4, 5 \rightarrow 5, 1 \rightarrow 3$.

But G_3 has elements with different orders, so it is not isomorphic to G_1 or G_2 .

6. a. Both are of infinite order.

b. $\ln(1) = 0$,

c. $\ln(1/a) = -\ln(a)$.

7. The Cayley table for the symmetry group of the equilateral triangle is

\circ	r_0	r_1	r_2	a	b	c
r_0	r_0	r_1	r_2	a	b	c
r_1	r_1	r_2	r_0	c	a	b
r_2	r_2	r_0	r_1	b	c	a
a	a	b	c	r_0	r_1	r_2
b	b	c	a	r_2	r_0	r_1
c	c	a	b	r_1	r_2	r_0

The identity element is r_0 . a , b and c have order 2. r_1 and r_2 have order 3.

The cyclic group of order 6 has elements e, a, a^2, a^3, a^4, a^5 , where $a^6 = e$. So a and its inverse a^5 have order 6 that is they are generators, a^2 and its inverse a^4 have order 3. a^3 has order 2.

Since symmetry group of the equilateral triangle has no generator and the cyclic group of order 6 does, they are not isomorphic.

8. The Cayley table for G , the cube roots of unity is

\times	1	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$
1	1	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$
$e^{\frac{2i\pi}{3}}$	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$	1
$e^{\frac{4i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$	1	$e^{\frac{2i\pi}{3}}$

1 is the identity, $e^{\frac{2i\pi}{3}}$ and $e^{\frac{4i\pi}{3}}$ are inverses and have order 3.

See answer for Q 9, 10.

The Cayley table for $H, \{1, 2, 4, \times_7\}$ is

\times_7	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

The isomorphism $f: G \rightarrow H$ is $1 \rightarrow 1, e^{\frac{2\pi}{3}} \rightarrow 2, e^{\frac{4\pi}{3}} \rightarrow 4$.

1 is the identity, 2 and 4 are inverses and have order 3.

9. The fifth roots of unity are $\omega_0 = 1, \omega_1 = e^{\frac{i2\pi}{5}}, \omega_2 = e^{\frac{i4\pi}{5}}, \omega_3 = e^{\frac{i6\pi}{5}}, \omega_4 = e^{\frac{i8\pi}{5}}$.

The Cayley table for G , the fifth roots of unity under multiplication is:

\times	1	ω_1	ω_2	ω_3	ω_4
1	1	ω_1	ω_2	ω_3	ω_4
ω_1	ω_1	ω_2	ω_3	ω_4	1
ω_2	ω_2	ω_3	ω_4	1	ω_1
ω_3	ω_3	ω_4	1	ω_1	ω_2
ω_4	ω_4	1	ω_1	ω_2	ω_3

1 is the identity. ω_1 and ω_4 are inverses and order 5, ω_2 and ω_3 are inverses and order 5. Since 5, the order of the group, is prime, elements must either be order 1 or 5.

The Cayley table for $\{\mathbb{Z}_5, +_5\}$ is:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

0 is the identity. 1 and 4 are inverses and order 5, 2 and 3 are inverses and order 5.

The isomorphism $f: \{\mathbb{Z}_5, +_5\} \rightarrow G$ is $a \mapsto \omega_a$.

We must show that $f(a +_5 b) = f(a) \times f(b)$.

LHS = $\omega_{a+_5 b}$.

RHS = $\omega_a \times \omega_b = \omega_{a+b}$, because $e^{i(2\pi k+\theta)} = e^{i\theta}$, $k \in \mathbb{Z}$.

10. The isomorphism is $f: \mathbb{Z} \rightarrow 2\mathbb{Z}$. Now we need to prove $f(a+b) = f(a) + f(b)$. LHS = $2(a+b)$. RHS = $2a + 2b$. LHS = RHS.

11. In both $\{\mathbb{R}\setminus\{0\}, \times\}$ and $\{\mathbb{C}\setminus\{0\}, \times\}$ the element 1 has order 1 and the element -1 has order 2. In $\{\mathbb{R}\setminus\{0\}, \times\}$ all other elements have infinite order, that is, there is no $m \in \mathbb{Z}$ such that $a^m = 1$. In $\{\mathbb{C}\setminus\{0\}, \times\}$ there are two elements, i and $-i$, which have order 4. Since $\{\mathbb{R}\setminus\{0\}, \times\}$ has no elements of order 4, it cannot be isomorphic to $\{\mathbb{C}\setminus\{0\}, \times\}$.

12. The mapping is given. We must prove $f(x \otimes y) = f(x) \circ f(y)$.

In this case $\otimes = \circ = *$.

$$\text{LHS} = b * (x * y) * b^{-1}.$$

$$\text{RHS} = (b * x * b^{-1}) * (b * y * b^{-1})$$

$$= b * x * b^{-1} * b * y * b^{-1}$$

$$= b * x * e * y * b^{-1}$$

$$= \text{LHS}.$$

13. The rhombus.

14. The Cayley table for the rotations and reflections of a square is:

*	r_0	r_1	r_2	r_3	a	b	c	d
r_0	r_0	r_1	r_2	r_3	a	b	c	d
r_1	r_1	r_2	r_3	r_0	c	d	b	a
r_2	r_2	r_3	r_0	r_1	b	a	d	c
r_3	r_3	r_0	r_1	r_2	d	c	a	b
a	a	d	b	c	r_0	r_2	r_3	r_1
b	b	c	a	d	r_2	r_0	r_1	r_3
c	c	a	d	b	r_1	r_3	r_0	r_2
d	d	b	c	a	r_3	r_1	r_2	r_0

The rotations alone form an isomorphic subgroup.

15. The operation table for the symmetry group of the square is:

*	r_0	r_1	r_2	r_3	a	b	c	d
r_0	r_0	r_1	r_2	r_3	a	b	c	d
r_1	r_1	r_2	r_3	r_0	c	d	b	a
r_2	r_2	r_3	r_0	r_1	b	a	d	c
r_3	r_3	r_0	r_1	r_2	d	c	a	b
a	a	d	b	c	r_0	r_2	r_3	r_1
b	b	c	a	d	r_2	r_0	r_1	r_3
c	c	a	d	b	r_1	r_3	r_0	r_2
d	d	b	c	a	r_3	r_1	r_2	r_0

One subgroup is $\{r_0, r_1, r_2, r_3\}$.

*	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

The other subgroups are $\{r_0, r_2, a, b\}$

*	r_0	r_2	a	b
r_0	r_0	r_2	a	b
r_2	r_2	r_0	b	a
a	a	b	r_0	r_2
b	b	a	r_2	r_0

and

*	r_0	r_2	c	d
r_0	r_0	r_2	c	d
r_2	r_2	r_0	d	c
c	c	d	r_0	r_2
d	d	c	r_2	r_0

They are subgroups because they are subsets, from the tables they are closed. r_0 is the identity and all elements are self-inverse except r_1 and r_3 , which are inverses. They have r_0 and r_2 in common. Because it is the identity r_0 commutes with all other elements of the whole group. By inspection of the table r_2 commutes with all other elements of the whole group.

IB Exam Type Problems

1. Two groups $\{G, *\}$ and $\{H, \bullet\}$ are isomorphic, if there exists a bijection $f: G \rightarrow H$ such that $f(a * b) = f(a) \bullet f(b)$ for all $a, b \in G$.
2. We must prove that $f: \{\mathbb{R}^+, \times\} \rightarrow \{\mathbb{R}, +\}$ is a bijection. Since $f(x)$ is monotonically increasing f is an injection. Since the range of $f(x)$ is \mathbb{R} , f is a surjection. Now we must prove $f(a * b) = f(a) \bullet f(b)$ for all $a, b \in \mathbb{R}^+$.

$$\text{LHS} = f(a \times b) = \ln(ab)$$

$$\text{RHS} = f(a) + f(b) = \ln(a) + \ln(b) = \ln(ab)$$

$$\text{LHS} = \text{RHS}.$$

3. a. The table for S is

*	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

The table for G is

•	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- b. For S and G all elements except the identity are order 2. For H 6 is the identity, 9 has order 2 and 3 and 12 have order 4.
- c. Since only H has elements of order 4 only H is cyclic. The generators are 3 and 12.
- d. Since H has two elements of order 4 but for S and G all elements (except the identity) are order 2, H cannot be isomorphic to either S or G. S and G are isomorphic with the mapping: $e \mapsto 1, f \mapsto 3, g \mapsto 5, h \mapsto 7$, since e and 1 are order 1 and the rest are order 2 and by inspection of the respective tables $f(a * b) = f(a) \bullet f(b)$ for all $a, b \in \mathbb{R}^+$.

4. a. The table for S is

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

The table for G is

$*$	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

with r_n being a rotation of $90^\circ \times n$ degrees anti-clockwise.

- b. For S, 1 is the identity, -1 has order 2 i and $-i$ have order 4. For G r_0 is the identity, r_2 has order 2, r_1 and r_3 have order 4. For H, 6 is the identity, 4 has order 2, 2 and 8 have order 4.

- c. S, G and H are all cyclic.

The generators are for S are i and $-i$, for G are r_1 and r_3 . For H are 2 and 8.

- d. $f: S \rightarrow G, 1 \rightarrow r_0, -1 \rightarrow r_2, i \rightarrow r_3, -i \rightarrow r_3$. and $g: G \rightarrow H, r_0 \rightarrow 6, r_2 \rightarrow 4, r_1 \rightarrow 2, r_3 \rightarrow 8$.

5. a.

Closure: $(3^a \times 5^b) \times (3^c \times 5^d) = 3^{a+c} \times 5^{b+d}$ with $a + c$ and $b + d \in \mathbb{Z}$, for all $a, b, c, d \in \mathbb{Z}$.

Associativity: multiplication of any subset of \mathbb{C} is associative.

Identity: 1 i.e. $a = b = 0$ is the identity.

Inverse: the inverse of $3^a \times 5^b$ is $3^{-a} \times 5^{-b}$

- b. The isomorphism is $f: (3^a \times 5^b) \rightarrow \begin{pmatrix} a \\ b \end{pmatrix}$. We must show that $f(x * y) = f(x) \bullet f(y)$ for all $a, b \in \mathbb{Z}$.

$$\text{LHS} = f((3^a \times 5^b) \times (3^c \times 5^d)) = f(3^{a+c} \times 5^{b+d}) = \begin{pmatrix} a+c \\ b+d \end{pmatrix}.$$

$$\text{RHS} = f(3^a \times 5^b) + f(3^c \times 5^d) = \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ b+d \end{pmatrix}.$$

LHS = RHS

6. We must prove that $f(e_s) \circ f(a) = f(a)$, for all $a \in H$.

From isomorphism $f(b) \circ f(a) = f(b * a)$, so $f(e_s) \circ f(a) = f(e_s * a)$.

Since e_s is the identity element in S , $e_s * a = a$, so $f(e_s * a) = f(a)$, so $f(e_s) \circ f(a) = f(a)$.

The proof of $f(a) \circ f(e_s) = f(a)$, is nearly identical, so is omitted.

7. i. G: 10 has order 1, 8 has order 2, 4 and 16 have order 3 and 2 and 14 have order 6.

H: 0 has order 1, 2 has order 2, 4 and 6 have order 3 and 3 and 5 have order 6.

I: 8 has order 1, 6 has order 2, 2 and 4 have order 3 and 10 and 12 have order 6.

J: e has order 1, n, g and h have order 2, k and m have order 3.

ii. G: {10, 8}, {10, 4, 16}

H: {0, 2}, {0, 4, 6}

I: {8, 6}, {8, 2, 4}

J: {e, n}, {e, g}, {e, h}, {e, k, m}

iii. G; H and I are isomorphic to each other. The identity elements map to each other. The elements with order 2 map to each other. The elements with order 3 map to each other. The elements with order 6 map to each other.

iv. G; H and I are cyclic. The generators are the elements with order 6: G: 2 and 14; H: 3 and 5, I: 10 and 1

Exercise 9.1

1. a. $\{+1, -1\}$ is a group under multiplication.

We need to show that $f(p * q) = f(p) \cdot f(q)$ for all $p, q \in G$. The product of two even permutations is even, the product of two odd permutations is even, and the product of an even and an odd is odd.

p	q	LHS	RHS
even	even	$f(\text{even}) = +1$	$+1 \times +1 = +1$
even	odd	$f(\text{odd}) = -1$	$+1 \times -1 = -1$
odd	even	$f(\text{odd}) = -1$	$-1 \times +1 = -1$
odd	odd	$f(\text{even}) = +1$	$-1 \times -1 = +1$

So LHS = RHS. Therefore it is a homomorphism,

- b. f is not injective. For example all even permutations, for example $(1\ 2)(2\ 1)$, map to 1.
- c. Since 1 is the identity element for $\{\{1, -1\}, \times\}$ and since all even permutations map to 1, the kernel is all even permutations.
2. a. Yes, it is the trivial homomorphism.
- b. No, it is not injective.
- c. All of $g \in G$.
3. a. Yes
- b. Yes
- c. $\{0\}$
4. a. No, it is not injective.
- b. Yes.
- c. $\{2\pi ki \text{ with } k \in \mathbb{Z}\}$.
5. a. $f(a + b) = (a + b) \pmod n = a \pmod n +_n b \pmod n = f(a) +_n f(b)$ so f is a homomorphism.
- b. No, because $f(n) = f(2n)$ so f is not injective, but it is surjective.
- c. All integers divisible by n .
6. a. $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$ so f is a homomorphism.
- b. But f is not surjective, since there is no integer n that satisfies $f(n) = 3$.
- However f is injective, since $f(n) = f(m)$ implies $2n = 2m$ which implies $n = m$. Not isomorphic.
- c. $\{0\}$

IB Type Problems

1. We must prove that if $f: G \rightarrow H$ is an injective homomorphism, the kernel is e_G .

$$f(e_G) = e_H \quad \text{A group isomorphism property.}$$

Assume the kernel includes another distinct element a .

$$\text{If so, } f(a) = f(e_G) \quad \text{They must both equal } e_H.$$

$$a = e_G \quad \text{If } f(x_1) = f(x_2), \text{ then } x_1 = x_2, \text{ because } f \text{ is injective}$$

So our assumption is wrong and the kernel only includes e_G .

2. We must prove that if for $f: G \rightarrow H$ the kernel is e_G , then f is an injective homomorphism.

So we must prove that if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Assume $f(x_1) = f(x_2)$.

$$f(x_1) * (f(x_2))^{-1} = f(x_2) * f(x_2)^{-1} \quad \text{Right multiplying by } f(x_2)^{-1}.$$

$$f(x_1) * (f(x_2))^{-1} = e_H \quad \text{The definition of the inverse.}$$

$$f(x_1) * f(x_2^{-1}) = e_H \quad f(a^{-1}) = f(a)^{-1}.$$

$$f(x_1 \circ x_2^{-1}) = e_H \quad f(x \otimes y) = f(x) * f(y).$$

$$x_1 \circ x_2^{-1} \in \ker f \quad \text{Definition of } \ker f.$$

$$x_1 \circ x_2^{-1} = e_G \quad \text{The kernel is trivial.}$$

$$x_1 = x_2 \quad \text{Definition of inverse.}$$

3. First we give the homomorphism:

$$f: G \rightarrow H: \{a, c\} \mapsto A \text{ and } \{b, d\} \mapsto B$$

Now we show $f(x \otimes y) = f(x) * f(y)$

There are 16 cases to show, so we need to find an economical way to write these.

The diagonal cases:

$$f(a \otimes a) = f(c \otimes c) = f(a) = A; \quad f(a) * f(a) = f(c) * f(c) = A * A = A$$

$$f(b \otimes b) = f(d \otimes d) = f(c) = A; \quad f(b) * f(b) = f(d) * f(d) = B * B = A.$$

Since \square is commutative, we only need to do half of the non-diagonal cases.

$$f(b \otimes a) = f(d \otimes c) = f(b) = B; \quad f(b) * f(a) = f(d) * f(c) = B * A = B.$$

$$f(c \otimes b) = f(d) = B; \quad f(c) * f(b) = A * B = B.$$

$$f(d \otimes a) = f(d) = B; \quad f(d) * f(a) = B * A = B.$$

$$f(c \otimes a) = f(c) = A; \quad f(c) * f(a) = A * A = A.$$

$$f(d \otimes b) = f(a) = A; \quad f(d) * f(b) = B * B = A.$$