OPTIONAL PURE / GROUPS

Binary Operations and Group Axioms

Worked solutions 11 questions · 123 marks

EXAM BOARDS Edexcel FP2 9FM0/4A · OCR A Y545 · OCR MEI Extra Pure Y435

Questions

Question 1	*9 marks*	2
Question 2	*5 marks*	3
Question 3	*5 marks*	4
Question 4	*13 marks*	5
Question 5	*12 marks*	7
Question 6	*8 marks*	10
Question 7	*16 marks*	12
Question 8	*9 marks*	14
Question 9	*14 marks*	16
Question 10	*14 marks*	18
Question 11	*18 marks*	20

1. A binary operation $\circ$ is defined on the set $S = \{x \in \mathbb{R} \mid x \geq 4\}$ by

$$a \circ b = a + b - 4 \quad \text{for all } a, b \in S$$

(a) Prove that $\circ$ is associative on S. **[2]**

(b) Find the identity element e for $\circ$, and verify that $e \in S$. **[2]**

(c) Show that S is closed under $\circ$. **[2]**

(d) Find, in terms of a, the real number x such that $a \circ x = e$. Determine which elements of S have an inverse in S, and hence explain why S does **not** form a group under $\circ$. **[3]**

Solution

(a) Let $a, b, c \in S$. Working out each bracketing in turn:

$$(a \circ b) \circ c = (a + b - 4) \circ c = (a + b - 4) + c - 4 = a + b + c - 8$$

$$a \circ (b \circ c) = a \circ (b + c - 4) = a + (b + c - 4) - 4 = a + b + c - 8$$

These are equal for all $a, b, c \in S$, so $\circ$ is associative on S.

(b) The identity e must satisfy $a \circ e = a$ for every $a \in S$, which gives

$$a + e - 4 = a \quad \Longrightarrow \quad e = 4$$

Also $e \circ a = 4 + a - 4 = a$, so $e = 4$ works on both sides. Since $4 \geq 4$, $e \in S$.

(c) Let $a, b \in S$, so $a \geq 4$ and $b \geq 4$. Then $a + b - 4$ is a real number and

$$a \circ b = a + b - 4 \geq 4 + 4 - 4 = 4$$

so $a \circ b \in S$. Hence S is closed under $\circ$.

(d) Using $e = 4$ from part (b):

$$a + x - 4 = 4 \quad \Longrightarrow \quad x = 8 - a$$

Also $x \circ a = (8 - a) + a - 4 = 4 = e$, so $8 - a$ is the inverse of a. This lies in S only when

$$8 - a \geq 4 \quad \Longrightarrow \quad a \leq 4$$

Every element of S has $a \geq 4$, so the only element of S with an inverse in S is $a = 4$, which is its own inverse.

For example, $5 \in S$ but its inverse is $8 - 5 = 3$, and $3 \notin S$. So not every element of S has an inverse in S: the inverse axiom fails, and S does not form a group under $\circ$.

2. A binary operation $\circ$ is defined on the set of positive real numbers by

$$a \circ b = \frac{ab}{a+b}$$

Show that the set of positive real numbers is closed under $\circ$, and prove that $\circ$ is associative. **[5]**

Solution

Closure: let a and b be positive real numbers. Then $ab > 0$ and $a + b > 0$, so in particular $a + b \neq 0$ and $a \circ b$ is defined. It is the quotient of two positive real numbers, so

$$a \circ b = \frac{ab}{a+b} > 0$$

Hence $a \circ b$ is a positive real number, and the set of positive real numbers is closed under $\circ$.

Associativity: let a, b and c be positive real numbers. By closure, $a \circ b$ and $b \circ c$ are positive real numbers, so both bracketings below are defined. Multiplying the numerator and denominator by $a + b$ gives

$$\begin{aligned}(a \circ b) \circ c &= \frac{\left(\frac{ab}{a+b}\right)c}{\frac{ab}{a+b} + c} \\ &= \frac{abc}{ab + c(a+b)} \\ &= \frac{abc}{ab + bc + ca}\end{aligned}$$

Similarly, multiplying the numerator and denominator by $b + c$ gives

$$\begin{aligned}a \circ (b \circ c) &= \frac{a\left(\frac{bc}{b+c}\right)}{a + \frac{bc}{b+c}} \\ &= \frac{abc}{a(b+c) + bc} \\ &= \frac{abc}{ab + bc + ca}\end{aligned}$$

So $(a \circ b) \circ c = a \circ (b \circ c)$ for all positive real numbers a, b and c, and $\circ$ is associative.

3. Let G be a group under the binary operation $*$, with identity e. For $x \in G$, write x^{-1} for the inverse of x and x^2 for $x * x$.

(a) Prove that if $a * b = a * c$ for some $a, b, c \in G$, then $b = c$, stating which group axiom you use at each step. **[2]**

(b) Hence, or otherwise, prove that if $(a*b)^2 = a^2 * b^2$ for all $a, b \in G$, then G is abelian (commutative). **[3]**

Solution

(a) Every element of a group has an inverse, so $a^{-1} \in G$ exists. Combining both sides of $a * b = a * c$ on the left with a^{-1} gives

$$a^{-1} * (a * b) = a^{-1} * (a * c) \qquad \text{(inverse exists)}$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c \qquad \text{(associativity)}$$
$$e * b = e * c \qquad \text{(inverse)}$$
$$b = c \qquad \text{(identity)}$$

(b) Suppose $(a * b)^2 = a^2 * b^2$ for all $a, b \in G$. Writing out both squares:

$$(a * b) * (a * b) = (a * a) * (b * b)$$

By associativity, the brackets can be regrouped so that each side begins with a:

$$a * ((b * a) * b) = a * ((a * b) * b)$$

Hence, by part (a), cancelling a on the left gives

$$(b * a) * b = (a * b) * b$$

Now combine both sides on the right with b^{-1}, which exists since $b \in G$:

$$((b * a) * b) * b^{-1} = ((a * b) * b) * b^{-1}$$
$$(b * a) * (b * b^{-1}) = (a * b) * (b * b^{-1}) \qquad \text{(associativity)}$$
$$(b * a) * e = (a * b) * e \qquad \text{(inverse)}$$
$$b * a = a * b \qquad \text{(identity)}$$

This holds for all $a, b \in G$, so the operation $*$ is commutative and G is abelian.

4. The set S consists of the functions f_n, defined for all real x by $f_n(x) = 2^n x + 2^n - 1$, one for each integer n. The binary operation on S is composition of functions, where $f_m f_n$ denotes the composite function $f_m \circ f_n$, so that $f_m f_n(x) = f_m(f_n(x))$.

(a) Show that $f_m f_n = f_{m+n}$ for all integers m and n. **[2]**

(b) Hence show that the binary operation is associative on S. **[2]**

(c) Prove that S is a group under composition of functions. **[6]**

(d) The subset T of S consists of the functions f_n for which $n \geq 0$. Show that T is closed under composition of functions, but that T is not a subgroup of S. **[3]**

Solution

(a) Applying f_m to $f_n(x) = 2^n x + 2^n - 1$ gives

$$\begin{aligned} f_m f_n(x) &= f_m(2^n x + 2^n - 1) \\ &= 2^m(2^n x + 2^n - 1) + 2^m - 1 \\ &= 2^{m+n} x + 2^{m+n} - 2^m + 2^m - 1 \\ &= 2^{m+n} x + 2^{m+n} - 1 \\ &= f_{m+n}(x) \end{aligned}$$

This holds for all real x, so $f_m f_n = f_{m+n}$ for all integers m and n, as required.

(b) Let f_p, f_q, f_r be any elements of S. Using part (a) twice on each side:

$$(f_p f_q) f_r = f_{p+q} f_r = f_{(p+q)+r}$$
$$f_p (f_q f_r) = f_p f_{q+r} = f_{p+(q+r)}$$

Addition of integers is associative, so $(p+q)+r = p+(q+r)$, and hence $(f_p f_q) f_r = f_p(f_q f_r)$. The binary operation is associative on S.

(c) The four group axioms are checked in turn.

Closure: for $f_m, f_n \in S$, part (a) gives $f_m f_n = f_{m+n}$. Since $m+n$ is an integer, $f_{m+n} \in S$, so S is closed under composition.

Identity: 0 is an integer, so $f_0 \in S$, and

$$f_0(x) = 2^0 x + 2^0 - 1 = x$$

so f_0 is the identity function. By part (a), for every $f_n \in S$:

$$f_0 f_n = f_{0+n} = f_n \qquad \text{and} \qquad f_n f_0 = f_{n+0} = f_n$$

so f_0 is the identity element of S.

Inverses: for each integer n, $-n$ is also an integer, so $f_{-n} \in S$. By part (a):

$$f_n f_{-n} = f_{n+(-n)} = f_0 \qquad \text{and} \qquad f_{-n} f_n = f_{-n+n} = f_0$$

so every element f_n has inverse f_{-n} in S.

Associativity: this was shown in part (b).

All four group axioms hold, so S is a group under composition of functions.

(d) For $f_m, f_n \in T$, we have $m \geq 0$ and $n \geq 0$, so $m + n \geq 0$. By part (a), $f_m f_n = f_{m+n} \in T$, so T is closed under composition of functions.

The identity of S is f_0, from part (c). Now $f_1 \in T$, and for any $f_k \in T$, where $k \geq 0$, part (a) gives $f_1 f_k = f_{1+k}$, with

$$f_{1+k}(0) = 2^{1+k} - 1 \geq 2^1 - 1 = 1$$

whereas $f_0(0) = 0$. So $f_1 f_k \neq f_0$ for every $f_k \in T$: the element f_1 has no inverse in T. Hence T is not a group under composition of functions, and so T is not a subgroup of S.

5. The set C consists of all complex numbers excluding 0 and 1.
The binary operation $\oplus$ is defined on C by

$$a \oplus b = \frac{ab}{1 - a - b + 2ab}$$

where $a, b \in C$.

(a) Find the identity element of C under $\oplus$. **[2]**

(b) Show that every element x of C has an inverse in C under $\oplus$, giving this inverse in terms of x. **[2]**

(c) Show that $\oplus$ is associative on C. **[3]**

(d) Explain why $(C, \oplus)$ is not a group. **[1]**

(e) The set D is defined by $D = \{x \in \mathbb{R} \mid 0 < x < 1\}$.
Show that $(D, \oplus)$ is a group. **[4]**

Solution

(a) Let e be the identity element. Then $a \oplus e = a$ for every $a \in C$, so

$$\frac{ae}{1 - a - e + 2ae} = a$$

Since $a \neq 0$, dividing both sides by a and multiplying by the denominator gives

$$e = 1 - a - e + 2ae$$

$$2e - 2ae = 1 - a$$

$$2e(1 - a) = 1 - a$$

Since $a \neq 1$, $1 - a \neq 0$, so

$$e = \frac{1}{2}$$

The formula for $a \oplus b$ is unchanged when a and b are swapped, so $\oplus$ is commutative and $\frac{1}{2} \oplus a = a$ as well. Since $\frac{1}{2} \in C$, the identity element of C under $\oplus$ is $\frac{1}{2}$.

(b) Let y be the inverse of x. Then $x \oplus y = \frac{1}{2}$, so

$$\frac{xy}{1 - x - y + 2xy} = \frac{1}{2}$$

Multiplying both sides by $2(1 - x - y + 2xy)$:

$$2xy = 1 - x - y + 2xy$$

$$y = 1 - x$$

For this y, the denominator is $1 - x - (1 - x) + 2x(1 - x) = 2x(1 - x)$, which is non-zero because $x \neq 0$ and $x \neq 1$. Also $1 - x \neq 1$ and $1 - x \neq 0$, so $1 - x \in C$. Since $\oplus$ is commutative, $(1 - x) \oplus x = \frac{1}{2}$ too, so every element x of C has inverse $1 - x$ in C.

(c) Let $a, b, c \in C$. Then

$$(a \oplus b) \oplus c = \frac{\left(\dfrac{ab}{1-a-b+2ab}\right)c}{1 - \dfrac{ab}{1-a-b+2ab} - c + \dfrac{2abc}{1-a-b+2ab}}$$

Multiplying the numerator and denominator by $1 - a - b + 2ab$:

$$\begin{aligned}(a \oplus b) \oplus c &= \frac{abc}{(1-a-b+2ab)(1-c) - ab + 2abc} \\ &= \frac{abc}{1-a-b+2ab-c+ac+bc-2abc-ab+2abc} \\ &= \frac{abc}{1-a-b-c+ab+bc+ca}\end{aligned}$$

Working in the same way:

$$a \oplus (b \oplus c) = \frac{a\left(\dfrac{bc}{1-b-c+2bc}\right)}{1 - a - \dfrac{bc}{1-b-c+2bc} + \dfrac{2abc}{1-b-c+2bc}}$$

Multiplying the numerator and denominator by $1 - b - c + 2bc$:

$$\begin{aligned}a \oplus (b \oplus c) &= \frac{abc}{(1-b-c+2bc)(1-a) - bc + 2abc} \\ &= \frac{abc}{1-b-c+2bc-a+ab+ac-2abc-bc+2abc} \\ &= \frac{abc}{1-a-b-c+ab+bc+ca}\end{aligned}$$

Hence $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for all $a, b, c \in C$, so $\oplus$ is associative on C.

(d) C is not closed under $\oplus$. For example, $2 \in C$ and $\frac{1}{3} \in C$, but the denominator of $2 \oplus \frac{1}{3}$ is

$$1 - 2 - \frac{1}{3} + 2 \times 2 \times \frac{1}{3} = 0$$

so $2 \oplus \frac{1}{3}$ is undefined, and $(C, \oplus)$ is not a group.

(e) Every element of D is a complex number other than 0 and 1, so D is contained in C.

Closure: let $a, b \in D$. The denominator of $a \oplus b$ can be written as

$$1 - a - b + 2ab = (1-a)(1-b) + ab$$

Since $0 < a < 1$ and $0 < b < 1$, both $(1-a)(1-b) > 0$ and $ab > 0$, so the denominator is positive and greater than the numerator ab. Hence

$$0 < \frac{ab}{(1-a)(1-b)+ab} < 1$$

so $a \oplus b \in D$.

Identity: by part (a), $a \oplus \frac{1}{2} = \frac{1}{2} \oplus a = a$ for every $a \in C$, and so for every $a \in D$. Since $0 < \frac{1}{2} < 1$, the identity $\frac{1}{2}$ is in D.

Inverses: by part (b), each $x \in D$ has inverse $1 - x$. Since $0 < x < 1$, it follows that $0 < 1 - x < 1$, so $1 - x \in D$.

Associativity: since D is contained in C, $\oplus$ is associative on D by part (c).

All four group axioms hold, so $(D, \oplus)$ is a group.

6. The elements x and y belong to a group G, whose binary operation is written as multiplication and whose identity is e.
The inverse of an element g of G is written g^{-1}.

(a) Prove that $(xy)^{-1} = y^{-1}x^{-1}$. **[2]**

(b) Given that $g^2 = e$ for every element g of G, use part (a) to prove that G is abelian (commutative). **[3]**

(c) Suppose instead only that $x^2 = e$ and $y^2 = e$. Does it follow that $xy = yx$? Justify your answer by considering the group of non-singular 2×2 matrices with real entries under matrix multiplication. **[3]**

Solution

(a) Let $z = (xy)^{-1}$, so that

$$(xy)z = e$$

Using associativity, this is $x(yz) = e$. Premultiplying both sides by x^{-1}:

$$x^{-1}\big(x(yz)\big) = x^{-1}e$$
$$(x^{-1}x)(yz) = x^{-1}$$
$$yz = x^{-1}$$

Premultiplying both sides by y^{-1} in the same way:

$$(y^{-1}y)z = y^{-1}x^{-1}$$
$$z = y^{-1}x^{-1}$$

So $(xy)^{-1} = y^{-1}x^{-1}$, as required.

(b) For every element g of G, $gg = g^2 = e$, so g is its own inverse:

$$g^{-1} = g \quad \text{for every } g \in G$$

Now xy is an element of G by closure, so it is also its own inverse. Using part (a):

$$xy = (xy)^{-1}$$
$$= y^{-1}x^{-1}$$
$$= yx$$

using $y^{-1} = y$ and $x^{-1} = x$ in the last line. Since x and y can be any elements of G, every pair of elements commutes, so G is abelian.

(c) No, it does not follow. In the group of non-singular 2×2 real matrices under matrix multiplication, the identity is $\mathbf{I}$. Take

$$x = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

Then $\det(x) = -1$ and $\det(y) = -1$, so both are non-singular and belong to the group. Squaring each:

$$x^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$$

$$y^2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$$

so $x^2 = e$ and $y^2 = e$. However, the products in the two orders are

$$xy = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

$$yx = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

The top-right entries differ, so $xy \neq yx$. Hence $x^2 = e$ and $y^2 = e$ do not imply that $xy = yx$.

7. The set G is given by

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{R},\ b \in \mathbb{R},\ a \neq 0 \right\}$$

(a) Show that G forms a group under matrix multiplication, $\times$. You may assume that matrix multiplication is associative. **[5]**

(b) The set S is defined by

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \{-1, 1\},\ b \in \mathbb{Z} \right\}$$

(i) Determine whether S is closed under $\times$. **[2]**

(ii) Determine whether S is a subgroup of $(G, \times)$, justifying your answer. **[2]**

(c) (i) By giving a suitable example, show that $\times$ is not commutative on G. **[2]**

(ii) Show that the identity matrix is the only element of G that commutes with every element of G. **[3]**

(d) With the help of an example, explain why G does **not** form a group under matrix addition. **[2]**

Solution

(a) Let $\mathbf{X} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\mathbf{Y} = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ be elements of G, so $a \neq 0$ and $c \neq 0$.

Closure: multiplying gives

$$\mathbf{XY} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}$$

The entries ac and $ad + b$ are real, the bottom row is $0 \quad 1$, and $ac \neq 0$ since $a \neq 0$ and $c \neq 0$. So $\mathbf{XY} \in G$, and G is closed under $\times$.

Identity: taking $a = 1$ and $b = 0$ gives $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$, and $\mathbf{IX} = \mathbf{XI} = \mathbf{X}$ for every $\mathbf{X} \in G$.

Inverses: $\det(\mathbf{X}) = a \times 1 - b \times 0 = a \neq 0$, so $\mathbf{X}$ has an inverse. For a 2×2 matrix with $ps - qr \neq 0$, the inverse is

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1} = \frac{1}{ps - qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$$

so

$$\mathbf{X}^{-1} = \frac{1}{a} \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$$

Its entries are real, its bottom row is $0 \quad 1$, and $\frac{1}{a} \neq 0$, so $\mathbf{X}^{-1} \in G$.

Associativity: matrix multiplication is associative.

All four group axioms hold, so G forms a group under matrix multiplication.

(b) (i) Let $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ be elements of S, so $a, c \in \{-1, 1\}$ and $b, d \in \mathbb{Z}$. By part (a), their product is

$$\begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}$$

Since $a, c \in \{-1, 1\}$, the product ac is 1 or -1, and since a, b, d are integers, $ad + b \in \mathbb{Z}$. So the product lies in S, and S is closed under $\times$.

(ii) Every element of S has $a = \pm 1 \neq 0$ and $b \in \mathbb{R}$, so S is a subset of G.

By part (b)(i), S is closed under $\times$.

Taking $a = 1$ and $b = 0$ shows that $\mathbf{I} \in S$.

By part (a), the inverse of $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$. For $a = \pm 1$, $\frac{1}{a} = a$, so

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & -ab \\ 0 & 1 \end{pmatrix}$$

Here $a \in \{-1, 1\}$ and $-ab \in \mathbb{Z}$, so the inverse lies in S.

Associativity holds in S because it holds for matrix multiplication. Hence S is a subgroup of $(G, \times)$.

(c) (i) Take $\mathbf{A} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, both in G. Then

$$\mathbf{AB} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{BA} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

So $\mathbf{AB} \neq \mathbf{BA}$, and $\times$ is not commutative on G.

(ii) The identity matrix commutes with every element of G, since $\mathbf{IY} = \mathbf{Y} = \mathbf{YI}$.

Now suppose $\mathbf{X} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ commutes with every $\mathbf{Y} = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ in G. From part (a):

$$\mathbf{XY} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{YX} = \begin{pmatrix} ca & cb + d \\ 0 & 1 \end{pmatrix}$$

These are equal exactly when $ad + b = bc + d$, that is, when

$$d(a - 1) = b(c - 1)$$

This must hold for every $c \neq 0$ and every real d. Taking $c = 1$ and $d = 1$ gives $a - 1 = 0$, so $a = 1$. The condition then becomes $0 = b(c - 1)$, and taking $c = 2$ gives $b = 0$.

So $\mathbf{X} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$, and the identity matrix is the only element of G that commutes with every element of G.

(d) Take $\mathbf{I} \in G$. Then

$$\mathbf{I} + \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Its bottom-right entry is 2, not 1, so $\mathbf{I} + \mathbf{I} \notin G$. Hence G is not closed under matrix addition, and so does not form a group under addition.

8. Let M be the set of all 2×2 matrices whose entries are integers. Matrix multiplication is a binary operation on M.
The matrices $\mathbf{A}$ and $\mathbf{B}$ in M are given by

$$\mathbf{A} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

(a) Find $\mathbf{A}^{-1}$ and $\mathbf{B}^{-1}$, and hence show that M does not form a group under matrix multiplication. **[3]**

(b) State the largest subset of M which forms a group under matrix multiplication, and show that it is a group. **[6]**

Solution

(a) For a 2×2 matrix with $ps - qr \neq 0$, the inverse is

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1} = \frac{1}{ps - qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$$

For $\mathbf{A}$, $\det(\mathbf{A}) = 3 \times 3 - 2 \times 4 = 1$, so

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

For $\mathbf{B}$, $\det(\mathbf{B}) = 3 \times 2 - 1 \times 4 = 2$, so

$$\mathbf{B}^{-1} = \frac{1}{2} \begin{pmatrix} 2 & -1 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & \frac{3}{2} \end{pmatrix}$$

The identity for matrix multiplication is $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is in M. The only matrix $\mathbf{X}$ with $\mathbf{BX} = \mathbf{XB} = \mathbf{I}$ is $\mathbf{B}^{-1}$, and $\mathbf{B}^{-1}$ has entries $-\frac{1}{2}$ and $\frac{3}{2}$, which are not integers, so $\mathbf{B}^{-1} \notin M$. Hence $\mathbf{B} \in M$ has no inverse in M, the inverse axiom fails, and M does not form a group under matrix multiplication.

(b) The largest such subset is

$$G = \{\mathbf{X} \in M \mid \det(\mathbf{X}) = 1 \text{ or } \det(\mathbf{X}) = -1\}$$

It is the largest because if $\mathbf{X}$ and $\mathbf{X}^{-1}$ both have integer entries, then $\det(\mathbf{X})$ and $\det(\mathbf{X}^{-1})$ are integers with $\det(\mathbf{X})\det(\mathbf{X}^{-1}) = \det(\mathbf{I}) = 1$, so $\det(\mathbf{X}) = \pm 1$.

Closure: let $\mathbf{X}, \mathbf{Y} \in G$. The entries of $\mathbf{XY}$ are sums of products of integers, so they are integers, and

$$\det(\mathbf{XY}) = \det(\mathbf{X})\det(\mathbf{Y}) = (\pm 1) \times (\pm 1) = \pm 1$$

so $\mathbf{XY} \in G$.

Identity: $\mathbf{I}$ has integer entries and $\det(\mathbf{I}) = 1$, so $\mathbf{I} \in G$, and $\mathbf{IX} = \mathbf{XI} = \mathbf{X}$ for every $\mathbf{X} \in G$.

Inverses: let $\mathbf{X} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in G$, so $ps - qr = \pm 1$. Then

$$\mathbf{X}^{-1} = \frac{1}{\pm 1} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} = \pm \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$$

which has integer entries, and $\det(\mathbf{X}^{-1}) = \frac{1}{\det(\mathbf{X})} = \pm 1$, so $\mathbf{X}^{-1} \in G$.

Associativity: matrix multiplication is associative.

All four group axioms hold, so G is a group under matrix multiplication.

9. The binary operation $*$ is defined on the set of ordered pairs (x, y), where $x, y \in \mathbb{R}$, by

$$(a, b) * (c, d) = \left(ac,\ ad + bc^3\right)$$

(a) Prove that $*$ is associative. **[3]**

(b) Find the identity element for $*$, showing that it is an identity on both sides. **[2]**

(c) Find all the elements which commute with $(-1, 1)$. **[3]**

(d) It is given that the particular element (m, n) has an inverse. Find this inverse in terms of m and n. **[2]**

(e) Find all self-inverse elements. **[3]**

(f) Give a reason why the set of ordered pairs (x, y), under the operation $*$, does not form a group. **[1]**

Solution

(a) Let (a, b), (c, d) and (e, f) be any three elements. Bracketing the first two together:

$$\begin{aligned}\big((a, b) * (c, d)\big) * (e, f) &= \left(ac,\ ad + bc^3\right) * (e, f) \\ &= \left(ace,\ acf + (ad + bc^3)e^3\right) \\ &= \left(ace,\ acf + ade^3 + bc^3e^3\right)\end{aligned}$$

Bracketing the last two together:

$$\begin{aligned}(a, b) * \big((c, d) * (e, f)\big) &= (a, b) * \left(ce,\ cf + de^3\right) \\ &= \left(ace,\ a(cf + de^3) + b(ce)^3\right) \\ &= \left(ace,\ acf + ade^3 + bc^3e^3\right)\end{aligned}$$

The two results are equal for all real a, b, c, d, e, f, so $*$ is associative.

(b) Let the identity be (u, v). For every element (x, y), it must satisfy

$$(x, y) * (u, v) = \left(xu,\ xv + yu^3\right) = (x, y)$$

Equating first components, $xu = x$ for all x, so $u = 1$. Then $xv + y = y$ for all x, so $v = 0$.
Checking $(1, 0)$ on both sides:

$$\begin{aligned}(x, y) * (1, 0) &= \left(x \times 1,\ x \times 0 + y \times 1^3\right) = (x, y) \\ (1, 0) * (x, y) &= \left(1 \times x,\ 1 \times y + 0 \times x^3\right) = (x, y)\end{aligned}$$

So the identity element is $(1, 0)$.

(c) Let (x, y) be any element. Then

$$\begin{aligned}(x, y) * (-1, 1) &= \left(-x,\ x \times 1 + y(-1)^3\right) = (-x,\ x - y) \\ (-1, 1) * (x, y) &= \left(-x,\ -1 \times y + 1 \times x^3\right) = (-x,\ x^3 - y)\end{aligned}$$

The first components always agree, so the elements commute exactly when

$$x - y = x^3 - y \quad \Longrightarrow \quad x^3 - x = 0 \quad \Longrightarrow \quad x(x-1)(x+1) = 0$$

so $x = 0$, $x = 1$ or $x = -1$, with y unrestricted. The elements which commute with $(-1, 1)$ are $(0, y)$, $(1, y)$ and $(-1, y)$ for any $y \in \mathbb{R}$.

(d) Let the inverse be (p, q). Then

$$(m, n) * (p, q) = \big(mp,\ mq + np^3\big) = (1, 0)$$

so $mp = 1$, which needs $m \neq 0$ and gives $p = \frac{1}{m}$. Then

$$mq + \frac{n}{m^3} = 0 \quad \Longrightarrow \quad q = -\frac{n}{m^4}$$

Checking on the other side:

$$\left(\frac{1}{m},\ -\frac{n}{m^4}\right) * (m, n) = \left(1,\ \frac{n}{m} - \frac{n}{m^4} \times m^3\right) = (1, 0)$$

so the inverse of (m, n) is $\big(\frac{1}{m},\ -\frac{n}{m^4}\big)$.

(e) An element (x, y) is self-inverse when $(x, y) * (x, y)$ is the identity $(1, 0)$:

$$(x, y) * (x, y) = \big(x^2,\ xy + yx^3\big) = (1, 0)$$

Equating first components, $x^2 = 1$, so $x = \pm 1$. Equating second components gives

$$y\big(x + x^3\big) = 0$$

When $x = 1$, $x + x^3 = 2$, and when $x = -1$, $x + x^3 = -2$. In both cases $x + x^3 \neq 0$, so $y = 0$.

The self-inverse elements are $(1, 0)$ and $(-1, 0)$.

(f) Any element $(0, y)$ has no inverse: for every (p, q), $(0, y) * (p, q) = \big(0,\ yp^3\big)$, whose first component is 0, never 1. So the inverse axiom fails and the set does not form a group under $*$.

10. For rational numbers a and b, the matrix $M(a,b)$ is defined by

$$M(a,b) = \begin{pmatrix} a & 2b \\ b & a+2b \end{pmatrix}$$

(a) Given that $\sqrt{3}$ is an irrational number, prove that $\det M(a,b) \neq 0$ for all $a, b \in \mathbb{Q}$ where a and b are not both 0. **[3]**

A set G is defined by $G = \{M(a,b) \mid a, b \in \mathbb{Q},\ a \text{ and } b \text{ not both } 0\}$.

(b) Prove that G is a group under matrix multiplication. You may assume that matrix multiplication is associative. **[7]**

(c) A subset H of G is defined by $H = \{M(a,b) \mid a, b \in \mathbb{Z},\ a \text{ and } b \text{ not both } 0\}$. Determine whether or not H is a subgroup of $(G, \times)$, where $\times$ denotes matrix multiplication. **[2]**

(d) Using $(G, \times)$, prove by counter-example that the statement "Every subgroup of an infinite group, other than the subgroup containing only the identity, is itself infinite" is false. **[2]**

Solution

(a) The determinant is

$$\begin{aligned} \det M(a,b) &= a(a+2b) - 2b \times b \\ &= a^2 + 2ab - 2b^2 \\ &= (a+b)^2 - 3b^2 \end{aligned}$$

Suppose, for contradiction, that $\det M(a,b) = 0$ for some $a, b \in \mathbb{Q}$, not both 0. Then

$$(a+b)^2 = 3b^2$$

If $b = 0$, this gives $a^2 = 0$, so $a = 0$, but a and b are not both 0. So $b \neq 0$, and dividing by b^2:

$$\left(\frac{a+b}{b}\right)^2 = 3 \quad \Longrightarrow \quad \sqrt{3} = \pm\frac{a+b}{b}$$

Since a and b are rational and $b \neq 0$, $\frac{a+b}{b}$ is rational, so $\sqrt{3}$ would be rational. This contradicts $\sqrt{3}$ being irrational, so $\det M(a,b) \neq 0$ for all $a, b \in \mathbb{Q}$ where a and b are not both 0.

(b) **Closure:** let $M(a,b)$ and $M(c,d)$ be in G. Then

$$\begin{aligned} M(a,b)M(c,d) &= \begin{pmatrix} a & 2b \\ b & a+2b \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c+2d \end{pmatrix} \\ &= \begin{pmatrix} ac+2bd & 2ad+2bc+4bd \\ ad+bc+2bd & ac+2ad+2bc+6bd \end{pmatrix} \\ &= \begin{pmatrix} ac+2bd & 2(ad+bc+2bd) \\ ad+bc+2bd & (ac+2bd)+2(ad+bc+2bd) \end{pmatrix} \\ &= M(p,q) \end{aligned}$$

where $p = ac+2bd$ and $q = ad+bc+2bd$. Since a, b, c, d are rational, so are p and q. Using part (a):

$$\det M(p,q) = \det M(a,b) \times \det M(c,d) \neq 0$$

and $M(0,0)$ is the zero matrix, whose determinant is 0, so p and q are not both 0. Hence $M(a,b)M(c,d) \in G$, and G is closed under matrix multiplication.

Identity: taking $a = 1$ and $b = 0$:

$$M(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$$

Since 1 and 0 are rational and not both 0, $\mathbf{I} \in G$, and $\mathbf{I}M(a,b) = M(a,b)\mathbf{I} = M(a,b)$ for every $M(a,b) \in G$, so $\mathbf{I}$ is the identity.

Inverses: let $M(a,b) \in G$ and let $D = \det M(a,b) = a^2 + 2ab - 2b^2$. By part (a), $D \neq 0$, and D is rational. For a 2×2 matrix with $\alpha\delta - \beta\gamma \neq 0$, the inverse is

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

so

$$M(a,b)^{-1} = \frac{1}{D} \begin{pmatrix} a+2b & -2b \\ -b & a \end{pmatrix}$$

This is $M(x,y)$ with $x = \frac{a+2b}{D}$ and $y = -\frac{b}{D}$, since then $2y = -\frac{2b}{D}$ and $x + 2y = \frac{a}{D}$. Both x and y are rational, and $\det M(x,y) = \frac{1}{D} \neq 0$, so x and y are not both 0. Hence $M(a,b)^{-1} \in G$.

Associativity: matrix multiplication is associative.

All four group axioms hold, so G is a group under matrix multiplication.

(c) $M(2,0) = 2\mathbf{I}$ is in H, since 2 and 0 are integers and not both 0. Its inverse is

$$M(2,0)^{-1} = \frac{1}{2}\mathbf{I} = M\left(\frac{1}{2}, 0\right)$$

and $\frac{1}{2} \notin \mathbb{Z}$, so $M(2,0)^{-1} \notin H$. Hence H does not contain the inverse of each of its elements, and H is not a subgroup of $(G, \times)$.

(d) G is infinite, since $M(n,0) = n\mathbf{I}$ is in G for every positive integer n, and these matrices are all different. Consider the subset $\{\mathbf{I}, -\mathbf{I}\}$ of G, where $-\mathbf{I} = M(-1,0)$. Its products are

$$\mathbf{I}\mathbf{I} = \mathbf{I}, \qquad \mathbf{I}(-\mathbf{I}) = (-\mathbf{I})\mathbf{I} = -\mathbf{I}, \qquad (-\mathbf{I})(-\mathbf{I}) = \mathbf{I}$$

so it is closed, it contains the identity $\mathbf{I}$, each element is its own inverse, and associativity holds as in G. So $\{\mathbf{I}, -\mathbf{I}\}$ is a subgroup of the infinite group G that is not $\{\mathbf{I}\}$ but has only 2 elements, and the statement is false.

11. A binary operation, $\circ$, is defined on a set of numbers, A, in terms of constants k_1, k_2, k_3 and k_4 (which are not necessarily in A) by

$$a \circ b = k_1ab + k_2a + k_3b + k_4, \qquad \text{for } a, b \in A$$

Addition, subtraction and multiplication of numbers have their usual notation and meaning.
You are initially given the following information about $\circ$ and A.

- $A = \{x \in \mathbb{R} \mid x \neq 2\}$
- $0 \circ 0 = 10$ and $1 \circ 0 = 6$
- An identity element, e, exists for $\circ$ in A

(a) Show that $a \circ b = 2ab - 4a - 4b + 10$. **[6]**

(b) State the value of e. **[1]**

(c) Explain whether $\circ$ is commutative over A. **[1]**

(d) Determine whether or not $(A, \circ)$ is a group. **[7]**

(e) Explain whether your answer to part (d) would change in each of the following cases, giving details of any change.

(i) $A = \{x \in \mathbb{R} \mid x > 2\}$ **[1]**

(ii) $A = \{n \in \mathbb{Z} \mid n \neq 2\}$ **[1]**

(iii) $A = \{x \in \mathbb{R} \mid x < 2\}$ **[1]**

Solution

(a) Using $0 \circ 0 = 10$:

$$k_1 \times 0 \times 0 + k_2 \times 0 + k_3 \times 0 + k_4 = 10 \implies k_4 = 10$$

Using $1 \circ 0 = 6$:

$$k_2 + k_4 = 6 \implies k_2 = -4$$

So $a \circ b = k_1ab - 4a + k_3b + 10$. The identity e satisfies $e \circ a = a$ for every $a \in A$, so

$$k_1ea - 4e + k_3a + 10 = a$$

$$(k_1e + k_3)a + (10 - 4e) = a$$

This holds for every $a \in A$, so equating coefficients of a and equating constant terms:

$$k_1e + k_3 = 1, \qquad 10 - 4e = 0$$

The second equation gives $e = \frac{5}{2}$. The identity also satisfies $a \circ e = a$ for every $a \in A$, so

$$k_1ae - 4a + k_3e + 10 = a$$

$$(k_1e - 4)a + (k_3e + 10) = a$$

Equating coefficients of a, with $e = \frac{5}{2}$:

$$\tfrac{5}{2}k_1 - 4 = 1 \implies k_1 = 2$$

Then $k_1 e + k_3 = 1$ gives

$$5 + k_3 = 1 \quad \Longrightarrow \quad k_3 = -4$$

Hence $a \circ b = 2ab - 4a - 4b + 10$, as required.

(b) From part (a), $10 - 4e = 0$, so $e = \frac{5}{2}$.

(c) Swapping a and b:

$$b \circ a = 2ba - 4b - 4a + 10 = 2ab - 4a - 4b + 10 = a \circ b$$

This holds for all $a, b \in A$, so $\circ$ is commutative over A.

(d) First write the operation in factorised form:

$$\begin{aligned} a \circ b &= 2ab - 4a - 4b + 10 \\ &= 2(ab - 2a - 2b + 4) + 2 \\ &= 2(a-2)(b-2) + 2 \end{aligned}$$

Closure: for $a, b \in A$, $a \circ b$ is real, and $a - 2 \neq 0$ and $b - 2 \neq 0$, so

$$a \circ b - 2 = 2(a-2)(b-2) \neq 0$$

Hence $a \circ b \neq 2$, so $a \circ b \in A$ and A is closed under $\circ$.

Identity: $e = \frac{5}{2} \in A$, since $\frac{5}{2} \neq 2$, and for every $a \in A$

$$\frac{5}{2} \circ a = 2 \times \frac{1}{2}(a-2) + 2 = a$$

Since $\circ$ is commutative, $a \circ \frac{5}{2} = a$ too, so $\frac{5}{2}$ is the identity.

Inverses: for $a \in A$, look for b with $a \circ b = \frac{5}{2}$:

$$\begin{aligned} 2(a-2)(b-2) + 2 &= \frac{5}{2} \\ (a-2)(b-2) &= \frac{1}{4} \\ b &= 2 + \frac{1}{4(a-2)} \end{aligned}$$

This is a real number, defined since $a \neq 2$, and $b \neq 2$ since $\frac{1}{4(a-2)} \neq 0$, so $b \in A$. By commutativity $b \circ a = \frac{5}{2}$ as well, so every $a \in A$ has inverse $2 + \frac{1}{4(a-2)}$ in A.

Associativity: for $a, b, c \in A$, using $a \circ b - 2 = 2(a-2)(b-2)$:

$$\begin{aligned} (a \circ b) \circ c &= 2((a \circ b) - 2)(c-2) + 2 \\ &= 2 \times 2(a-2)(b-2)(c-2) + 2 \\ &= 4(a-2)(b-2)(c-2) + 2 \\ a \circ (b \circ c) &= 2(a-2)((b \circ c) - 2) + 2 \\ &= 2(a-2) \times 2(b-2)(c-2) + 2 \\ &= 4(a-2)(b-2)(c-2) + 2 \end{aligned}$$

These are equal, so $\circ$ is associative.

All four group axioms hold, so $(A, \circ)$ is a group.

(e) (i) For $a, b > 2$, $(a-2)(b-2) > 0$, so $a \circ b = 2(a-2)(b-2) + 2 > 2$ and A is closed. The identity $e = \frac{5}{2} > 2$ is in A, for $a > 2$ the inverse $2 + \frac{1}{4(a-2)} > 2$ is in A, and associativity still holds. So $(A, \circ)$ is still a group: the answer does not change.

(ii) An identity e would satisfy $e \circ a = a$, that is $(2e-4)a + 10 - 4e = a$, for every $a \in A$, so $10 - 4e = 0$ and $e = \frac{5}{2}$, which is not an integer. There is no identity in A, so $(A, \circ)$ is not a group: the answer changes.

(iii) For $a, b < 2$, $a-2 < 0$ and $b-2 < 0$, so $(a-2)(b-2) > 0$ and $a \circ b > 2$; for example $0 \circ 0 = 10 \notin A$. So A is not closed under $\circ$ and $(A, \circ)$ is not a group: the answer changes.