Groups 2A

1 a Consider two elements of S, $z_1 = x_1 + y_1\sqrt{3}$ and $z_2 = x_2 + y_2\sqrt{3}$

Then $z_1 - z_2 = x_1 - x_2 + (y_1 - y_2)\sqrt{3}$

Since integers are closed under subtraction, $x_1 - x_2 \in \mathbb{Z}$ and $y_1 - y_2 \in \mathbb{Z}$

So $x_1 - x_2 + (y_1 - y_2)\sqrt{3} \in S$

Hence subtraction is a binary operation on S.

b Consider two elements of S, $z_1 = x_1 + y_1\sqrt{3}$ and $z_2 = x_2 + y_2\sqrt{3}$

Then $z_1z_2 = (x_1 + y_1\sqrt{3})(x_2 + y_2\sqrt{3}) = x_1x_2 + x_1y_2\sqrt{3} + x_2y_1\sqrt{3} + 3y_1y_2$

$= x_1x_2 + 3y_1y_2 + (x_1y_2 + x_2y_1)\sqrt{3}$

Integers are closed under multiplication (and obviously 3 is an integer), so

$x_1x_2 + 3y_1y_2 + (x_1y_2 + x_2y_1)\sqrt{3} \in S$

Hence multiplication is a binary operation on S.

c Consider two elements of S, $z_1 = x_1 + y_1\sqrt{3}$ and $z_2 = x_2 + y_2\sqrt{3}$

Then $\dfrac{z_1}{z_2} = \dfrac{x_1 + y_1\sqrt{3}}{x_2 + y_2\sqrt{3}} = \dfrac{x_1 + y_1\sqrt{3}}{x_2 + y_2\sqrt{3}} \times \dfrac{x_2 - y_2\sqrt{3}}{x_2 - y_2\sqrt{3}} = \dfrac{(x_1 + y_1\sqrt{3})(x_2 - y_2\sqrt{3})}{x_2^2 - 3y_2^2}$

$= \dfrac{x_1x_2 - 3y_1y_2}{x_2^2 - 3y_2^2} + \dfrac{y_1x_2 - x_1y_2}{x_2^2 - 3y_2^2}\sqrt{3}$

Putting $y_1 = y_2 = 0$, $x_1 = 3$ and $x_2 = 2$, gives $\dfrac{z_1}{z_2} = \dfrac{6}{4} + 0\sqrt{3}$

As $\dfrac{6}{4} \notin \mathbb{Z}$, in this case $\dfrac{z_1}{z_2} \notin S$

Hence division is not a binary operation on S.

2 a For any two positive integers x and y:

$x * y = \dfrac{x!y!}{xy} = \dfrac{\left(x \times (x-1) \times \ldots \times 2 \times 1\right)\left(y \times (y-1) \times \ldots \times 2 \times 1\right)}{xy}$

$= \left((x-1) \times \ldots \times 2 \times 1\right)\left((y-1) \times \ldots \times 2 \times 1\right) =$

$= (x-1)!(y-1)!$

Since the factorial of a non-negative integer is always a positive integer, this is a positive integer.
So the set of positive integers is closed under the operation *.

b If $x = -1$ and $y = 0$, then $x * y = \sqrt{-1} \notin \mathbb{R}$.
So the set of real numbers is not closed under the operation *.

c A number is odd if and only if 2 is not one of its prime factors.
The prime factors of the product of two numbers are exactly the prime factors of the two numbers; therefore, if 2 is not a factor of x then it is not a factor of x^2; and if it is not a factor of both y and x^2 then it can't be a factor of x^2y.
Therefore the set of odd numbers is closed under the operation *.

2 d The modulus of a complex number is a real number.
The sum of two real numbers is a real number; and every real number is a complex number.
Therefore, the set of complex numbers is closed under the operation $*$.

3 a The identity element is 1, since for any complex number z, $z \times 1 = 1 \times z = z$.

b $\frac{1}{1+i} = \frac{1}{1+i} \times \frac{1-i}{1-i} = \frac{1-i}{1+1} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i$

4 a The identity matrix is $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, since for any matrix $\mathbf{A}$, $\mathbf{AI} = \mathbf{IA} = \mathbf{A}$.

b The inverse of this matrix $\mathbf{A} = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$ is $\frac{1}{\det \mathbf{A}} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & 0 \\ 0 & 1 \end{pmatrix}$

5 a For three real numbers x, y and z:
$x * (y * z) = x * (yz^2) = xy^2z^4$
$(x * y) * z = xy^2 * z = xy^2z^2$
For $z \notin \{0,1\}$ and $x, y \neq 0$, $xy^2z^2 \neq xy^2z^4$, so the operation is not associative.

b For three real numbers x, y and z:
$x * (y * z) = x * 3^{yz} = 3^{x3^{yz}}$
$(x * y) * z = 3^{xy} * z = 3^{3^{xy}z}$
Clearly if $x \neq z$ then $3^{x3^{yz}} \neq 3^{3^{xy}z}$ so the operation is not associative.

c For three real numbers x, y and z:
$$\begin{aligned} x * (y * z) &= x * (|y| + |z|) = |x| + |(|y| + |z|)| \\ &= |x| + |y| + |z| = |(|x| + |y|)| + |z| \\ &= (x * y) * z \end{aligned}$$
So the operation is associative.

d For three real numbers x, y and z:
$$\begin{aligned} x * (y * z) &= x * (yz + y + z) \\ &= xyz + xy + xz + x + yz + y + z \\ &= xyz + xz + yz + xy + x + y + z \\ &= (xy + x + y) * z \\ &= (x * y) * z \end{aligned}$$
So the operation is associative.

6 a The positive real numbers are closed under multiplication, as the sum of two positive real numbers is a positive real number.
For every real number x, $x \times 1 = 1 \times x = x$, so 1 is an identity element.
If x is positive then there exists an element $\frac{1}{x}$ such that $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$, so $\frac{1}{x}$ is the inverse of x.
The real numbers are associative under multiplication.
So all axioms hold, and therefore the set of positive real numbers under multiplication is a group.

6 b Division is not a binary operation on the set of integers (for example, $2 \div 3 \notin \mathbb{Z}$), so the first axiom (closure) does not hold. The set of integers under division is not a group.

c Addition is not a binary operation of the set of odd integers (for example, $1+1=2$ which is not an odd number), so the first axiom (closure) does not hold. The set of odd integers under addition is not a group.

d The multiplicative identity for the integers is 1, which is not a member of the set of even integers; therefore, the identity axiom does not hold. The set of even integers under multiplication is not a group.

e Subtraction is not associative on the set of real numbers, for example:
$(1-1)-1=0-1=-1$, while $1-(1-1)=1-0=1$
Therefore the set of real numbers under subtraction is not a group.

f This operation doesn't have an identity: while $x \div 1 = x$ for all x, if $x \neq 1$, but $1 \div x \neq x$. In addition, division is not associative on the set of positive rational numbers. Therefore the set of positive rational numbers under division is not a group.

7 a Consider two positive rational numbers $\frac{a}{b}$ and $\frac{c}{d}$, where $a, b, c, d \in \mathbb{N}$

Then $\frac{a}{b} * \frac{c}{d} = \frac{\frac{ac}{bd}}{\frac{a}{b}+\frac{c}{d}} = \frac{\frac{ac}{bd}}{\frac{ad+bc}{bd}} = \frac{ac}{ad+bc}$

Since natural numbers are closed under multiplication and addition, $ac,\ ad+bc \in \mathbb{N}$

Therefore $\frac{ac}{ad+bc}$ is a positive rational number.

Hence $\mathbb{Q}^+$ is closed under *.

b Suppose there is an identity element e, then $a * e = a$ for any $a \in \mathbb{Q}^+$

But $a * e = \frac{ae}{a+e}$, so $\frac{ae}{a+e} = a \Rightarrow ae = a^2 + ae \Rightarrow a^2 = 0$

This is a contradiction since a can be any element in $\mathbb{Q}^+$
So this binary operation does not have an identity element.

8 a i Let a = 1 and b = 1, then $a * b = 1 * 1 = 1 + 1 - 2 = 0$, which is not a positive integer.
So the operation is not closed.

ii Suppose a, b and c are three positive integers.

$$\begin{aligned}\text{Then } a*(b*c) &= a*(b+c-2)\\ &= a+b+c-2-2\\ &= a+b-2+c-2\\ &= (a+b-2)*c\\ &= (a*b)*c\end{aligned}$$

So $*$ is associative.

b i Clearly, $a*2 = a+2-2 = a$ and $2*a = 2+a-2 = a$, so 2 is an identity for $*$.

8 b ii Suppose there exist $a, b \in \mathbb{Z}^+$ such that $a * b = 2$, the identity element.
Then $a+b-2=2 \Rightarrow b=4-a$, so if $a=5$, then $b=-1 \notin \mathbb{Z}^+$
So $a = 5$ (in fact any $a > 4$) does not have an inverse.
Hence the inverse axiom does not hold, so $\mathbb{Z}^+$ does not form a group under *.

9 Suppose e is an identity for $*$.
Then $a * e = ae + a = a \Rightarrow e = 0$
But $e * a = ae + e = 0 \neq a$ for any $a \neq 0$
So e cannot be an identity element, hence the identity axiom does not hold.

Alternatively, it can be shown that the operation is not associative.
$a*(b*c) = a*(bc+b) = abc + ab + a$
$(a*b)*c = (ab+a)*c = abc + ac + ab + a$
Hence $a*(b*c) \neq (a*b)*c$

So $\mathbb{R}$ does not form a group under *.

10 Closure: Let $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$ then
$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1+b_1 & a_2+b_2 \\ a_3+b_3 & a_4+b_4 \end{pmatrix}$$
As addition on the set of integers is a binary operation, then $a_1+b_1, a_2+b_2, a_3+b_3, a_4+b_4 \in \mathbb{Z}$

Identity: The identity element is the zero matrix $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

For any integer-valued 2×2 matrix $\mathbf{A}$, $\mathbf{0} + \mathbf{A} = \mathbf{A} + \mathbf{0} = \mathbf{A}$

Inverse: for matrix $\mathbf{A} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, the matrix $\mathbf{A}^{-1} \begin{pmatrix} -a_1 & -a_2 \\ -a_3 & -a_4 \end{pmatrix}$ is its inverse as $\mathbf{A}^{-1} + \mathbf{A} = \mathbf{A} + \mathbf{A}^{-1} = \mathbf{0}$

Associativity: as the addition of integers is associative, it follows that the addition of integer-valued 2×2 matrices is associative.

All four axioms hold, so the set of integer-valued 2×2 matrices forms a group under addition.

11 Closure: Let $\lambda, \delta \in \mathbb{R}$ and $\lambda, \delta \neq 0$ then
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \lambda\delta & 0 \\ 0 & \lambda\delta \end{pmatrix}$$
As multiplication on the set of real numbers is a binary operation, then $\lambda\delta \in \mathbb{R}$ and $\lambda\delta \neq 0$

Identity: The identity element is the matrix $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

For any 2×2 matrix $\mathbf{A}$, $\mathbf{IA} = \mathbf{AI} = \mathbf{A}$

Inverse: for matrix $\mathbf{A} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ the matrix $\mathbf{A}^{-1} \begin{pmatrix} \frac{1}{\lambda} & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}$ is its inverse as $\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$

Associativity: Matrix multiplication is associative in general. So the associative axiom holds.

All four axioms hold, so the set of diagonal 2×2 matrices with $\lambda \neq 0$ forms a group under matrix multiplication.

12 Closure: Let $a, b, c, d, e, f \in \mathbb{R}$ and $a, c, d, f \neq 0$ then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}$$

As addition and multiplication on the set of real numbers is a binary operation, then $ad, ae+bf, cf \in \mathbb{R}$ and $ad, cf \neq 0$

Identity: The identity element is the matrix $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

For any matrix, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$

Inverse: for matrix $\mathbf{A} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ the matrix $\mathbf{A}^{-1}$ $\begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$ is its inverse as $\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$

Associativity: Matrix multiplication is associative in general. So the associative axiom holds.

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

13 Closure: Let $f(x) = ax + b$ and $g(x) = cx + d$ for $a, b, c, d \in \mathbb{R}$ and $a, c \neq 0$ then $g(f(x)) = c(ax+b)+d = (ca)x+(cb+d)$ with $ca, cb+d \in \mathbb{R}$ and $ca \neq 0$, so closure holds.

Identity: Let $f(x) = x$, then $g(f(x)) = f(g(x)) = g(x)$ for all $g(x)$, so $f(x) = x$ is the identity element.

Inverse: Let $g(x) = \frac{1}{a}x - \frac{b}{a}$, then

$$f(g(x)) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x - b + b = x \text{ and } g(f(x)) = \frac{1}{a}(ax+b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x$$

So $f^{-1}(x) = g(x)$, and each element of the set has an inverse element that is a member of the set.

Associativity: This follows by the normal associativity of function composition, i.e. $fg(h(x)) = f(gh(x))$ for all functions $f(x)$, $g(x)$, $h(x)$.

All four axioms hold, so the set forms a group under function composition.

14 Suppose x is an element of a group, y and z are inverses of x and e is the identity.
Then:

$y = y * e = y * (x * z) = (y * x) * z = e * z = z$

$\Rightarrow y = z$

$\Rightarrow$ the inverse of any element is unique

So $y = z$.

15 a As $a * a^{-1} = a^{-1} * a = e$ and the inverse is unique (see question **14**), a is an inverse for a^{-1}, hence $(a^{-1})^{-1} = a$.

b By associativity: $a * b * (b^{-1} * a^{-1}) = (a * b * b^{-1}) * a^{-1} = a * a^{-1} = e$

Similarly, $(b^{-1} * a^{-1}) * (a * b) = e$

So, by uniqueness of the inverse, $(a * b)^{-1} = b^{-1} * a^{-1}$.

16 Since $(ab)^2 = abab$:

$a^2b^2 = abab$

$\Rightarrow a^{-1}a^2b^2b^{-1} = a^{-1}ababb^{-1}$

$\Rightarrow eabe = ebae$

$\Rightarrow ab = ba$

17 $a \circ b = b \circ a \Rightarrow a \circ a \circ b \circ b = a \circ b \circ a \circ b$

$\Rightarrow e \circ e = a \circ b \circ a \circ b$ as a and b are self-inverses

$\Rightarrow e = (a \circ b) \circ (a \circ b)$

$\Rightarrow a \circ b$ is a self-inverse

Challenge

a Suppose $\mathbb{N}^0$ contains n distinct elements for some finite number n.
Then apply the successor function to each of these n elements.
By the fourth Peano axiom, these n successor elements are all distinct and members of $\mathbb{N}^0$.
By the second Peano axiom, none of these elements is 0; so there are $n+1$ distinct elements of $\mathbb{N}^0$.
This is a contradiction. So $\mathbb{N}^0$ must contain an infinite number of elements.

b Use induction on c. First put $c = 0$; then $(a+b)+0 = a+b = a+(b+0)$, so the claim holds.
If the claim holds for c, then consider $\mathrm{S}(c)$ and apply the seventh Peano axiom:

$$\begin{aligned}(a+b)+\mathrm{S}(c) &= \mathrm{S}((a+b)+c)\\ &= \mathrm{S}(a+(b+c))\\ &= a+\mathrm{S}(b+c)\\ &= a+(b+\mathrm{S}(c))\end{aligned}$$