MA151 Algebra 1, Assignment 1

Dyson Dyson

Question 1

> In each case below determine whether the operation $\star$ defines a binary operation on the set S. Give reasons for your answers.

Q1 (i)

> $x \star y = x^2 + y^2, \ S = \mathbb{Z}$

This is a binary operation, since it takes two elements of S and always returns another element of S. An integer squared plus another integer squared will always be another integer.

Q1 (ii)

> $x \star y = x + 3, \ S = \mathbb{N}$

This is a binary operation, since it takes two elements of S and always returns another element of S. A natural number plus 3 is always another natural number.

Q1 (iii)

> $x \star y = \frac{x+y}{2}, \ S = \mathbb{Z}$

This is *not* a binary operation, since it takes two elements of S and but doesn't always return another element of S. The mean of two integers is not always an integer. Consider $2 \star 3$, for example. $2 \star 3 = \frac{2+3}{2} = \frac{5}{2} \notin \mathbb{Z}$.

Question 2

> Let S be a set and $\star$ a binary operation on S which is associative. Stating clearly how and when you use the associative property, show that if $a, b, c, d, e \in S$ then
>
> $$((a \star b) \star (c \star d)) \star e = a \star (((b \star c) \star d) \star e)$$

Associativity means that $(a \star b) \star c = a \star (b \star c)$. For the sake of explanation, I shall call the middle term the *pivot term*. So in the case of the example just given, the pivot term was b. In the case of $(f \circ (g \circ h)) \circ t = f \circ ((g \circ h) \circ t)$, the pivot term is $(g \circ h)$.

$$\begin{aligned}
((a \star b) \star (c \star d)) \star e &= (a \star b) \star ((c \star d) \star e) && \text{pivoting around } (c \star d) \\
&= a \star (b \star ((c \star d) \star e)) && \text{pivoting around } b \\
&= a \star ((b \star (c \star d)) \star e) && \text{pivoting around } (c \star d) \\
&= a \star (((b \star c) \star d) \star e) && \text{pivoting around } c
\end{aligned}$$

Question 3

> How many distinct commutative binary operations are there on the set $S = \{a, b, c, d\}$? Explain your answer carefully.

Call the binary operation $\oplus$. Since $\oplus$ is commutative over S, we know that $a \oplus b = b \oplus a$, $d \oplus b = b \oplus d$, etc. So we only need to consider half of the possible combinations. Specifically, we only need to define $a \oplus a$, $a \oplus b$, $a \oplus c$, $a \oplus d$, $b \oplus b$, $b \oplus c$, $b \oplus d$, $c \oplus c$, $c \oplus d$, and $d \oplus d$. Operations like $c \oplus a$ are necessarily given by $a \oplus c$, since $\oplus$ is commutative.

Thus, there are 10 operations to define. Each operation could output any of the 4 elements of S, so there are $4^{10} = 1,048,576$ distinct commutative binary operations over S.

Most of these operations will not be associative. For example, if $a \oplus b = c$, $b \oplus c = d$, $c \oplus c = a$, and $a \oplus d = b$, then $(a \oplus b) \oplus c = a$ but $a \oplus (b \oplus c) = b$. But the question didn't mention associativity, so this is not something we have to worry about.

Question 4

n each case below prove that the set together with the binary operation is a group. Justify your answers

Q4 (i)

$(\{3^n : n \in \mathbb{Z}\}, \times)$

1. A power of 3 multiplied by a power of 3 is always another power of 3, so the group is closed.
2. Multiplication of integers is associative.
3. The identity element is $3^0 = 1$.
4. For some element 3^n, its inverse is 3^{-n}, which is also in the set, so inverses exist.

Therefore this is a group.

Q4 (ii)

$\left(\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \text{ and } ac \neq 0\right\}, \times\right)$

1. Some matrix $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ multiplied by another matrix $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ equals $\begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}$. We note that $ac \neq 0$ and $xz \neq 0$, so $acxz \neq 0$, so this result is in the set and the group is closed under matrix multiplication.
2. Matrix multiplication is associative.
3. The identity element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is definitely in the set, since $1 \times 1 \neq 0$.
4. The inverse of an element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ is $\frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$. Since $ac \neq 0$, this inverse is well-defined and in the set, so inverses exists in the group.

Therefore this is a group.

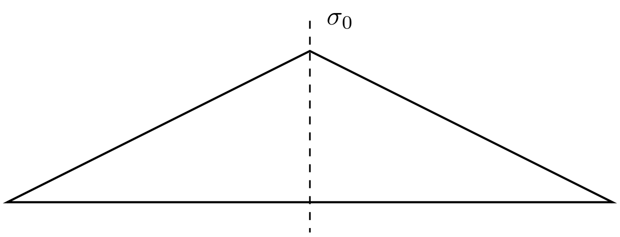
Question 5

> In both cases below, draw diagrams to show the symmetries of the object X. Give your symmetries letter names and then draw up a table to show the effect of any symmetry followed by any other symmetry (like you have seen in lectures for an equilateral triangle and a square).

Q5 (i)

> X is an isosceles triangle which is not equilateral.

For the non-equilateral isosceles triangle, the only symmetries are the 0° rotation (the identity), called ρ_0, and the reflection in the vertical line, called σ_0.



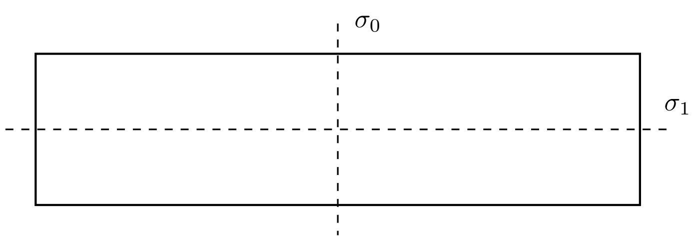
And here's the table:

	ρ_0	σ_0
ρ_0	ρ_0	σ_0
σ_0	σ_0	ρ_0

Q5 (ii)

> X is a rectangle which is not a square.

For the non-square rectangle, the only symmetries are the 0° rotation (the identity), called ρ_0, the 180° rotation, called ρ_1, the reflection in the vertical line, called σ_0, and the reflection in the horizontal line, called σ_1.



And here's the table:

	ρ_0	ρ_1	σ_0	σ_1
ρ_0	ρ_0	ρ_1	σ_0	σ_1
ρ_1	ρ_1	ρ_0	σ_1	σ_0
σ_0	σ_0	σ_1	ρ_0	ρ_1
σ_1	σ_1	σ_0	ρ_1	ρ_0

Question 6

Let G be a group and let $h \in G$.

Q6 (i)

Let $g_1, g_2 \in G$. Prove that $hg_1 = hg_2$ if and only if $g_1 = g_2$.

If $hg_1 = hg_2$, then we can left-multiply by h^{-1} on both sides to get $h^{-1}hg_1 = h^{-1}hg_2 \implies 1g_1 = 1g_2 \implies g_1g_2$. We know that h^{-1} must exist since $h \in G$ and G is a group.

Conversely, if $g_1 = g_2$, then we can left-multiply by h on both sides and get $hg_1 = hg_2$.

Q6 (ii)

Let $S = \{hg : g \in G\}$. Prove that $S = G$.

Suppose that $S \neq G$. That means there is some element $a \in G$ which is not in S, or there is some element $b \in S$ that was never in G.

For the first case, let $a \in G$. Then $h^{-1}a$ is another element of G. Thus, $h\left(h^{-1}a\right) = a$, so a must be in S. Therefore all elements in G must be in S.

For the second case, we know that groups are closed under their binary operation, so hg could never generate a new $b \notin G$. Therefore all elements in S must be in G.

Since $G \subset S$ and $S \subset G$, we must conclude that $S = G$.