MODEL ANSWERS TO HWK #1

1. Suppose that a and b are elements of S. We have

$$\begin{aligned} a &= a * b && \text{by rule (1)} \\ &= b * a && \text{by rule (2)} \\ &= b && \text{by rule (1).} \end{aligned}$$

As a and b are arbitrary, S can have at most one element.
2. (a) Suppose that a and b are two integers and that $a * b = b * a$. Now $a * b = a - b$ and $b * a = b - a$ so that then $a - b = b - a$. Applying the standard rules of arithmetic, we get $2a = 2b$ and so $a = b$.
(b) Suppose that a, b and c are integers. Then

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

On the other hand

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

Thus equality holds iff $a + c - b = a - (b + c)$, that is, cancelling $c = -c$ so that $c = 0$. Thus $*$ is not associative. For example,

$$0 * (0 * 1) = 1$$

but

$$(0 * 0) * 1 = -1.$$

(c) Let a be an integer. Then

$$a * 0 = a - 0 = a.$$

(d) Let a be an integer. Then

$$a * a = a - a = 0.$$

3. Let R denote rotation through 90° degrees, clockwise. Then R^2 denotes rotation through 180° and R^3 rotation through 270°. Together with the identity these constitute all rotations. In addition there are four flips. Two side flips S_1 and S_2 and two diagonal flips D_1 and D_2. If the vertices are A, B, C and D, in clockwise order, then we may suppose that S_1 exchanges A and B, and C and D, S_2 exchanges A and D, and B and C, F_1 fixes A and C and exchanges B and D, whilst F_2 fixes B and D and exchanges A and C.
These are the only symmetries. There are 24 permutations of the letters $\{A, B, C, D\}$ but not all permutations can be realised as a symmetry of a square. Wherever one sends A, the images of the vertices B and D

are still adjacent to the image of A whilst the image of C is not. There are four places to send A, to any of $\{A, B, C, D\}$, but once we have decided where to send A there are only two more choices, where to send B (we cannot send it the vertex opposite the image of A); D has to be sent to the other vertex adjacent to the image of A and the image of C is to the vertex opposite the image of A. So the eight symmetries we have written down are the only symmetries.
We obviously get a group. Associativity follows as multiplication of symmetries corresponds to composition of functions. The identity symmetry acts as the identity and given any symmetry there is always a symmetry which undoes that symmetry. The inverse of I is I, the inverse of R is R^3, the inverse of R^2 is R^2 and the inverse of a flip is the same flip.
Here is the Cayley table:

$*$	I	R	R^2	R^3	S_1	S_2	D_1	D_2
I	I	R	R^2	R^3	S_1	S_2	D_1	D_2
R	R	R^2	R^3	I	D_2	D_1	S_1	S_2
R^2	R^2	R^3	I	R	S_2	S_1	D_2	D_1
R^3	R^3	I	R	R^2	D_1	D_2	S_2	S_1
S_1	S_1	D_1	S_2	D_2	I	R^2	R	R^3
S_2	S_2	D_2	S_1	D_1	R^2	I	R^3	R
D_1	D_1	S_2	D_2	S_1	R^3	R	I	R^2
D_2	D_2	S_1	D_1	S_2	R	R^3	R^2	I

To get the table, we need to compute $RS_1 = D_2$ the long way, use the obvious symmetry to conclude that $RS_2 = D_1$, and then use the fact that every row and column is a permutation of

$$\{\, I, R, R^2, R^3, S_1, S_2, D_1, D_2 \,\}$$

some easy manipulations and the fact that the inverse of a product is the product of the inverses in the reverse order, to fill in the rest.
4. Let

$$H = \{\, A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in M_{3,3}(\mathbb{R}) \,|\, x, y, z \in \mathbb{R} \,\}.$$

Note that if $A \in H$ then $\det A = 1$. Therefore H is a subset of $\mathrm{GL}_3(\mathbb{R})$ the invertible 3×3 matrices with real entries, which is a group under multiplication. It suffices to check that H is non-empty, closed under multiplication and taking inverses.

Note that $I_3 \in H$ so that H is certainly non-empty. If A and A' are two elements of H,

$$A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad A' = \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$AA' = \begin{pmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{pmatrix}$$

which is an element of H. Therefore H is closed under multiplication. On the other hand the inverse of A is

$$A^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix},$$

which is also an element of H. Therefore H is closed under inverses. It follows that H is a group.

5. Suppose not, suppose that G is not abelian. We will derive a contradiction.

We may suppose that the elements of G are $\{e, a, b, c, d\}$. As G is not abelian, possibly renaming, we must have $ab \neq ba$. Possibly renaming, we must have $ab = c$ and $ba = d$. Now $b \notin C_a$. As $aa^{-1} = a^{-1}a = e$ it follows that $a^{-1} \in C_a$. As $b = a^{-1}c$ and $a^{-1} \in C_a$ and C_a is a subgroup, so that it is closed under multiplication, $c \notin C_a$. Similarly $d \notin C_a$. Thus $C_a = \{e, a\}$.

As $a^{-1} \in C_a$ and $a^{-1} \neq e$, we must have $a^{-1} = a$. As a only commutes with e and a, by the same argument, we must also have $b^{-1} = b$ and $c^{-1} = c$. But then

$$\begin{aligned} c &= c^{-1} \\ &= b^{-1}a^{-1} \\ &= ba \\ &= d, \end{aligned}$$

a contradiction. Therefore G is abelian.

6. As $y \in G$ there is an element $z \in G$ such that $z * y = e$. Multiplying both sides on the right by x we get

$$\begin{aligned} x &= e * x \qquad \text{by rule (2)} \\ &= (z * y) * x \\ &= z * (y * x) \qquad \text{by associativity} \\ &= z * e \qquad \text{by rule (3).} \end{aligned}$$

It follows that

$$\begin{aligned} x * e &= (z * e) * e \\ &= z * (e * e) \qquad \text{by associativity} \\ &= z * e \qquad \text{by rule (2)} \\ &= x. \end{aligned}$$

As x is arbitrary and $e * x = x = x * e$ it follows that e acts as the identity. But then

$$\begin{aligned} x &= z * e \\ &= z. \end{aligned}$$

As $y * x = e = x * y$ it follows that y is the inverse of x. x is arbitrary every element has an inverse and so G is a group.

7. Consider the function

$$\phi\colon G \longrightarrow G \qquad \text{given by} \qquad \phi(b) = a * b.$$

By assumption ϕ is injective. As G is finite it follows that ϕ is bijective. Similarly the function

$$\psi\colon G \longrightarrow G \qquad \text{given by} \qquad \psi(b) = b * a,$$

is bijective. Given a, as ϕ is surjective we may find $e \in G$ such that

$$\phi(e) = a \qquad \text{so that} \qquad a * e = a.$$

Now suppose that $b \in G$. By a similar argument we may find $f \in G$ such that $f * b = b$. Now

$$\begin{aligned} (a * f) * b &= a * (f * b) \\ &= a * b. \end{aligned}$$

As

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

we have

$$a * f = a,$$

by rule (3). As

$$a * f = a = a * e,$$

we must have $e = f$ by rule (2). As a and b are arbitrary, it follows that $e * g = g * e$ for any $g \in G$. Thus e plays the role of the identity. As ψ is surjective we may find an element $b \in G$ such that $b * a = e$. At this point we are done by question 6 but here is a much easier argument:

$$\begin{aligned}(a * b) * a &= a * (b * a) \qquad \text{by associativity}\\ &= a * e\\ &= a\\ &= e * a.\end{aligned}$$

As

$$(a * b) * a = e * a,$$

we must have $a * b = e$ by rule (3). Thus b is the inverse of a and G is a group.

8. Let $G = \mathbb{N}$ and let $*$ be ordinary addition. If a, b and c are three natural numbers such that

$$a + b = a + c$$

then adding the integer $-a$ to both sides we see that $b = c$. Similarly, if a, b and c are three natural numbers such that

$$b + a = c + a,$$

then adding the integer $-a$ to both sides we see that $b = c$. On the other hand, $\mathbb{N}$ is not a group (it is a subset of $\mathbb{N}$ which is not closed under taking inverses).

9. (a) Let f be the function $f(x) = \log x$ (we will adopt the convention that $\log -x = \log x$). Then

$$f(a*b) = f(ab) = \log(ab) = \log(a)+\log(b) = f(a)+f(b) = f(a)\#f(b),$$

by the usual rules for logs. Given $y > 0$ let $x = 10^y$. Then $\log x = y$, so that f is surjective.

(b) Let f be any such function. We check that $f(1) = f(-1) = 0$. We have

$$f(1) = f(1 \cdot 1) = f(1) + f(1).$$

Hence $f(1) = 0$. On the other hand,

$$0 = f(1) = f(-1 \cdot -1) = f(-1) + f(-1),$$

so that $f(-1) = 0$ as well. But then f is not injective.

10. Since $a^3 = e$ we have

$$\begin{aligned} ba &= a^4 b \\ &= a^3(ab) \qquad \text{by associativity} \\ &= e(ab) \\ &= ab. \end{aligned}$$

11. Let $G = \mathbb{Z}$ be the integers under addition. If $H \subset \mathbb{Z}$ is a non-trivial subgroup then H contains a non-zero integer n. But then H must contain

$$2n \qquad 3n \qquad 4n \ldots,$$

all multiples of n, as H is closed under addition. But then H is infinite. As H is arbitrary, every non-trivial subgroup of G is infinite.