MODEL ANSWERS TO THE FIRST HOMEWORK

1. Chapter 1, §1: 1. Suppose that a and b are elements of S. By rule (1)

$$a * b = a.$$

But by rule (2),

$$a * b = b * a.$$

Applying rule (1) we get $a * b = b * a = b$.
Thus $a = a * b = b$. As a and b are arbitrary, S can have at most one element.
1. Chapter 1 §1: 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 if and only if $a+c-b = a-(b+c)$, 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

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

2. Chapter 2, §1: (a). No, by the question above, this rule of multiplication is not associative.

(b) No this is not a group. We consider the three axioms. Suppose that a, b and c are three integers. Then

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc. \end{aligned}$$

Similarly

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + c + ab + bc + ac + ac + abc. \end{aligned}$$

Since we get the same answer however we bracket the triple product, this is an associative rule of multiplication.
I claim that zero acts as an identity. Let a be an integer. Then

$$a * 0 = a + 0 + a0 = a,$$

and

$$0 * a = 0 + a + 0a = a.$$

Thus 0 is an identity for $*$. By a result in class, this is the only possible choice of identity.
Now suppose that a is an integer. An inverse of a would be an integer x such that $a * x = 0$. In other words x would be a solution to the equation

$$a + x + ax = 0.$$

Solving for x gives

$$x = -\frac{a}{a+1}.$$

The only problem is if $a = -1$. In other words if b is an inverse of -1 then $-1 + b - b = 0$, which is absurd. Thus we don't have a group as -1 is an element without an inverse.
(c). No, this is not a group. Addition of numbers is associative and zero is the unique identity element. However the number one has no inverse. Indeed if b is the inverse of 1, then

$$b + 1 = 0.$$

In this case $b = -1$. But -1 is not a non-negative integer.
(d) We first have to check a slightly subtle thing. We need to check that $a * b$ is never equal to -1. In other words we have to check that we really have a well-defined rule of multiplication. Suppose that a and b are rational numbers and that

$$a + b + ab = -1.$$

Then

$$1 + a + b + ab = 0.$$

But

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

so that either $1 + a = 0$ or $1 + b = 0$. In other words either $a = -1$ or $b = -1$. Thus we have a well-defined multiplication rule.
We proved in (b) that this rule of multiplication is associative and that zero is an identity element. Clearly

$$a * b = b * a.$$

Let a be a rational number, not equal to -1. Let

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

Note that we are allowed to divide through by $1 + a$ as $a \neq -1$.
Then

$$a * b = a + b + ab = a - \frac{a}{a + 1} - a\frac{a}{a + 1} = a - a = 0.$$

Since $b * a = a * b$, $b * a = 0$ as well. But then b acts as an inverse for a. As a is arbitrary, every element has an inverse. Hence the rational numbers excluding -1 form a group, with this law of multiplication.
(e) The set G consists of all rational numbers of the form $a/5b$ where 5 does not divide a. Note that we don't get a well-defined law of multiplication. For example, $x = 1/5 \in G$ and $y = 4/5 \in G$. But

$$x * y = \frac{1}{5} + \frac{4}{5} = 1,$$

which is not an element of G.
(f) This is not a group. There cannot be an identity element. Suppose not, suppose that e is an identity element and let a be an element of G that is not equal to e. Then

$$e * a = e \neq a,$$

which contradicts the basic property of an identity.
2. Chapter 2, §1, 2. The main thing to prove is that H is closed under multiplication and taking inverses. Suppose that U and V are in H. Then $U = T_{a,b}$ and $V = T_{c,d}$, where a and b are equal to ± 1. Now

$$\begin{aligned} U * V &= T_{a,b} * T_{c,d} \\ &= T_{ac,ad+b}. \end{aligned}$$

Now if $a = \pm 1$ and $c = \pm 1$ then clearly $ac = \pm 1$. Thus the product $U * V$ is in H and H is closed under multiplication. On the other hand the inverse of $U = T_{a,b}$ is $T_{a^{-1},-a^{-1}b}$. If $a = \pm 1$ then so is a^{-1}. Thus H is closed under taking inverses.

At this point we could of course invoke the Proposition proved in class to conclude that H is a subgroup and so a group.

On the other hand we can argue as follows. This product is clearly associative in H, since it is associative in G (or indeed since composition of functions is associative).

The identity $I = T_{1,0}$ is in H and is an identity in H. We already checked that H contains inverses.

2. Chapter 2, §1: 5. The inverse of g is clearly rotation clockwise through 90°. This is represented by $h(x, y) = (y, -x) = g^3(x, y)$. We check that h is an inverse of g formally:

$$\begin{aligned}(h * g)(x, y) &= h(g(x, y)) \\ &= h(-y, x) \\ &= (x, y)\end{aligned}$$

and

$$\begin{aligned}(g * h)(x, y) &= g(h(x, y)) \\ &= g(y, -x) \\ &= (x, y).\end{aligned}$$

Thus h is the inverse of g. We now check that $g * f = f * h$. We have

$$\begin{aligned}(g * f)(x, y) &= g(f(x, y)) \\ &= g(-x, y) \\ &= (-y, -x).\end{aligned}$$

On the other hand,

$$\begin{aligned}f * h(x, y) &= f(h(x, y)) \\ &= f(y, -x) \\ &= (-y, -x).\end{aligned}$$

Therefore $g * f = f * h = f * g^{-1} = f * g^3$. It follows that

$$g * f^s = f^s * g^{s'}$$

where s' is 1 if $s = 0$ and $s' = 3$ if $s = 1$. Therefore

$$g^j * f^s = f^s * g^{j'}$$

where $j' = j$ if $s = 0$ and $j' = -j$ if $s = 1$. Putting all of this together we get

$$(f^i g^j) * (f^s g^t) = f^{i+s} g^{j'+t}.$$

where $j' = j$ if $s = 0$ and $j' = -j$ if $s = 1$.

We check the axioms for a group. By the formula above we have a well-defined product. Multiplication is associative as it is just composition of functions. The identity is f^0g^0. The inverse of f^ig^j is $f^{-i}g^{j'}$ where $j' = j$ if $i = 1$ and $j' = -j$ if $i = 0$. Thus we have a group of order 8 which is clearly not abelian.

21. Suppose the elements of G are $\{e, a, b, c, d\}$. e is the identity. If G is not abelian then we can find g and h such that $gh \neq hg$. If $g = e$ then $gh = h = hg$. Thus we may assume that $g \neq e$. By the same token we may assume that $h \neq e$. If $g = h$ then $gh = g^2 = hg$. Thus we may assume that $g \neq h$.

By symmetry we may therefore assume that $g = a$ and $h = b$. By assumption $ab \neq ba$. If $ab = e$ then a is the inverse of a and so $ba = e = ab$, a contradiction. If $ab = a$ then $b = e$, another contradiction. By the same token we may assume that the sets $\{ab, ba\}$ and $\{a, b\}$ don't intersect.

Thus by symmetry we may assume that $ab = c$. Since $ba \neq c$ we may assume that $ba = d$.

On the other hand a has an inverse. e is neither the inverse of a nor the inverse of b. a and b are not inverses of each other. Suppose that c is the inverse of a. Then

$$a^2b = a(ab) = aa^{-1} = e.$$

Thus a^2 is the inverse of b. It follows that

$$e = ba^2 = (ba)a \qquad \text{so that} \qquad ba = c,$$

a contradiction.

The only remaining possibility is that a is its own inverse,

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

In this case multiplying both sides by a we get

$$a^2 = aa^{-1} = e.$$

Consider the product aba. It is equal to an element of G.

We consider each cases, one by one.

Suppose it is equal to e. Then

$$aba = e.$$

Multiplying on the left by a we get

$$ba = a$$

Multiplying on the right by a we get

$$b = e,$$

a contradiction.

Suppose it is equal to a. Then

$$aba = a$$

Multiplying on the left by a we get

$$ba = e,$$

so that b is the inverse of a, which is nonsense.
Suppose it is equal to c. Then

$$ca = c,$$

so that $a = e$, a contradiction.
Suppose it is equal to d. Then

$$ad = d,$$

so that $a = e$, a contradiction.
Finally, suppose it is equal to b. Then

$$aba = b.$$

Multiplying both sides on the right by $a = a^{-1}$ we get

$$ab = ba,$$

so that a and b, a contradiction.
We have therefore shown that a does not have an inverse, a contradiction.
Therefore G is abelian.
23. We may find c and d such that $U = T_{c,d}$. We have

$$T_{ac,cb+d} = T_{c,d} * T_{a,b} = U * T_{a,b} = T_{a,b} * U = T_{a,b} * T_{c,d} = T_{ac,ad+b}.$$

In other words we must have

$$T_{ac,cb+d} = T_{ac,ad+b}.$$

Since $T_{\alpha,\beta}$ is uniquely determined by α and β, we have equality if and only if

$$bc + d = ad + b.$$

We view this as an equation for c and d, which is valid for any a and b. If we put $a = 1$ then we get

$$bc + d = d + b \qquad \text{so that} \qquad b = bc.$$

If we put $b = 1$ then we conclude that $c = 1$. The original equation now reduces to

$$b + d = ad + b \qquad \text{so that} \qquad d = ad.$$

If we put $a = 2$ then we see that $d = 0$.

Thus the only element of G which commutes with everything is the identity.
28. By assumption there is an element $z \in G$ such that $z * y = e$. We compute the product $z * y * x$ in two different ways (the product is unambiguous by associativity).
On the one hand

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

On the other hand

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

Thus $x = z * e$. Let's now compute $x * y$:

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

Finally

$$\begin{aligned} x * e &= x * (y * x) \\ &= (x * y) * x \\ &= e * x \\ &= x. \end{aligned}$$

Thus G is a group.
29. Define a function $l_a \colon G \longrightarrow G$ by the rule $l_a(g) = a * g$. Suppose that $l_a(b) = l_a(c)$. Then $a * b = a * c$ and so $b = c$. But then l_a is an injective function. As G is finite and l_a is injective it follows that l_a is surjective. Thus l_a is bijective. In particular we may find e such that $l_a(e) = a$. In this case $a * e = a$.
Similarly we may define a function $r_b \colon G \longrightarrow G$ by the rule $r_b(c) = c*b$. By symmetry r_b is bijective. Thus we may find f 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 r_a is surjective we may find an element $b \in G$ such that $b * a = e$. At this point we are done by question 28 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.

30. Let $G = \mathbb{N}$ and let $a * b = a + b$. Then $*$ is an associative binary operation. If $a * b = a * c$ then $a + b = a + c$ so that $b = c$. $a * b = a + b = b + a = b * a$. But G is not a group, since inverses don't exist.

31. (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.