MODEL ANSWERS TO THE SECOND HOMEWORK

1. Label the vertices of the square A, B, C, D, where we start at the top left hand corner and we go around the square clockwise. In particular A is opposite to C and B is opposite to D.
There are three obvious types of symmetries. There are rotations. One obvious rotation R corresponds to rotation clockwise through $\pi/2$ radians. The others are R^2, R^3 and the identity I. They represent rotation through π and $3\pi/2$.
There are two sorts of flips. One set of flips are diagonal flips. The first D_1 fixes the diagonal AC and switches B and D. The other D_2 fixes the diagonal BD and switches A and C. The other possibility is to look at the flip F_1 which switches A and D and B and C and the flip F_2 which switches A and B and C and D.
I claim that this exhausts all possible symmetries. In fact any symmetry is determined by its action on the fours vertices A, B, C and D. Now there are $24 = 4!$ possible such permutations.
On the other hand any symmetry of a square must fix opposite corners. Thus once we have decided where to send A, for which there are four possibilities, the position of C is determined, it is opposite to A. There are then two possible positions for B. So there are at most eight symmetries and we have listed all of them.
We start looking for subgroups. Two trivial examples are D_4 and $\{I\}$. A non-trivial example is afforded by the set of all rotations $\{I, R, R^2, R^3\}$. Clearly closed under products and inverses. Note that rotation through π radians R^2 generates the subgroup $\{I, R^2\}$.
Simliarly, since any flip is its own inverse, the following are all subgroups, $\{I, F_1\}$, $\{I, F_2\}$, $\{I, D_1\}$ and $\{I, D_2\}$. Now try combining side flips and diagonal flips. Now $F_1D_1 = R^3$. So any subgroup that contains F_1 and D_1 must contain R^3 and hence all rotations. From there it is easy to see we will get the whole of G. So we cannot combine side flips with diagonal flips.
Now consider combining rotations and flips. Note that $F_1F_2 = R^2$ and $D_1D_2 = R^2$ by direct computation. We then try to see if

$$\{I, F_1, F_2, R^2\}$$

is a subgroup. As this is finite, it suffices to check that it is closed under products. We look at pairwise products. If one of the terms is I this is clear. We already checked F_1F_2. It remains to check F_1R^2 and F_2R^2.

Consider the equation $F_1F_2 = R^2$. Multiplying by F_1 on the left, and using the fact that it is its own inverse, we get $F_2 = F_1R^2$. Similarly all other products, of any two of F_1, F_2 and R^2, gives the third. Thus

$$\{I, F_1, F_2, R^2\}$$

is a subgroup.
Similarly

$$\{I, D_1, D_2, R^2\}$$

is a subgroup.
2. Chapter 2, Section 2: 1. This is a little tricky. The hard thing is to show that G contains an element e that acts as the identity.
Suppose that $b \in G$. Consider the equation

$$xb = b.$$

By assumption this has a solution, call it a. Then

$$ab = b.$$

Now suppose that $c \in G$. Consider the equation

$$bx = c.$$

Then this has a solution, say $x = d$, so that $bd = c$.
Start with the equation

$$\begin{aligned} ab &= b && \text{multiply both sides by } d \\ (ab)d &= bd && \text{now use associativity} \\ a(bd) &= c && \text{and the fact that } bd = c \\ ac &= c. \end{aligned}$$

So now we know that a is a left identity. As we can always solve the equation

$$xb = a,$$

for any $b \in G$, it follows that G has left inverses. But then by question 28, of the previous hwk, G is a group.
On the other hand, we can argue that there must be a right identity a', using the argument above. Now consider the product $a' * a$. As a is a right identity, this is equal to a'. But as a' is a left identity, this is equal to a'. Thus $a = a'$ and so a plays the role of an identity.
Now arguing as above, G must contain left and right inverses, for b. Again, it is not hard to prove that a right inverse of b is also a left inverse, given that b does have a left inverse. Thus G is a group.

2. Chapter 2, Section 2: 2. One way to do this is to appeal to the First Model Answers, qu 29. On the other hand, one can in fact reduce this problem to the previous question. Given $a \in G$ define a map

$$l \colon G \longrightarrow G$$

by the rule

$$l(g) = ag.$$

I claim that l is injective. Suppose that $l(g) = l(h)$. By definition this means $ag = ah$. But then $g = h$, by hypothesis. Thus f is injective.
As G is finite, it follows that f is surjective. But this means that for every y in G, there is an x such that $f(x) = y$. By definition this means $ax = y$.
Similarly we may define a map

$$r \colon G \longrightarrow G$$

by the rule

$$r(g) = ga.$$

By the same argument, using r instead of l, we can show that every equation of the form $xa = y$ has a solution in x, where $y \in G$.
Thus we have proved that the hypotheses of question 1 hold and we may apply question 1.
3. Chapter 2, Section 3: 1. Set $H = A \cap B$. We first check that H is non-empty.
But as A and B are subgroups, the identity is an element of both A and B. Thus H contains the identity. In particular it is not empty.
We have to check that H is closed under products and inverses.
Suppose that g and h are in H. Then g and h are in A and B. But then $gh \in A$ as A is closed under products. Similarly $gh \in B$ as B is closed under products. Thus $gh \in H$.
Now suppose that $g \in H$. Then $g \in A$ and $g \in B$. As A is closed under inverses, $g^{-1} \in A$. Similarly $g^{-1} \in B$. But then $g^{-1} \in H$. As g is arbitrary, H is indeed closed under taking inverses.
But then by (6.3), H is a subgroup of G.
3. Chapter 2, Section 3: 4. There are two ways to go about this. The first is to adapt the proof of the fact that the centraliser C_g of an element $g \in G$ is a subgroup of G. This is straightforward.
The second is a little smarter. Note that $Z(G)$ is, almost by definition, the intersection of the centraliser's C_g of all the elements of $g \in G$ (see question below). On the other hand it is proved in class, that the intersection of subgroups is a group.
Thus $Z(G)$ is indeed a subgroup.

4. Chapter 2, Section 3: 5. Suppose that $h \in Z(G)$. Let $a \in G$. Then

$$ha = ah,$$

as $h \in Z(G)$. But then $h \in C_a$. As a is arbitrary,

$$h \in \bigcap_{a \in G} C_a.$$

Thus $Z(G) \subset \bigcap_{a \in G} C_a$.
Now suppose that $h \in \bigcap_{a \in G} C_a$. Then $h \in C_a$, for every $a \in G$. But then

$$ha = ah,$$

for all $a \in G$. By definition then $h \in Z(G)$. Thus $\bigcap_{a \in G} C_a \subset Z(G)$.
4. Chapter 2, Section 3: 12. Let G be a cyclic group. Then there is an element $a \in G$ such that $G = \langle a \rangle$. Suppose that g and $h \in G$. Then there are integers m and n such that $g = a^m$ and $h = a^n$. But then

$$\begin{aligned} gh &= a^m a^n \\ &= a^{m+n} \\ &= a^{n+m} \\ &= a^n a^m = hg \end{aligned}$$

Thus G is abelian.
4. Chapter 2, Section 3: 16. Let G be a group, with no proper subgroups. If G contains only one element, there is nothing to prove. Otherwise pick an element $a \in G$, not equal to the identity. Then $H = \langle a \rangle$ is a subgroup of G.
By assumption $H \neq \{e\}$. As G contains no proper subgroups, then $H = G$. Thus G is cyclic.
There are two cases. Suppose that G is infinite. Consider $b = a^2$. This generates a proper subgroup H of G. In fact the elements of H are all the elements of the form a^{2n}, $n \in \mathbb{Z}$. But then H is a proper subgroup of G, a contradiction.
Thus G must have finite order. Suppose that the order n of G is not prime. Then $n = xy$, where x and y are positive integers, and neither is equal to one.
Let $b = a^x$ and look at the subgroup H generated by b. Note that the elements of H are all of the form a^{ix}, where $i \in \mathbb{Z}$. Indeed this set is clearly closed under multiplication and taking inverses. Thus H is a proper subgroup, as $a \notin H$, for example. Again, this contradicts our hypotheses on G.
So the order of G must be a prime.

Here is another way to argue, if G is finite, of order n. Let i be any integer less than n. Consider the element $b = a^i$. Then $a^i \neq e$, so the subgroup it generates, must be the whole of G. In particular the element a must be power of b, so that $b^m = (a^i)^m = a$. Thus

$$im = 1 \mod n.$$

In this case i is coprime to n. As i was arbitrary, every integer less than n is coprime to n. But then n is prime.

5. **Challenge Problems** Chapter 2, Section 3: 25. Let $S = \mathbb{Z}$ and let $X = \mathbb{N}$. Consider the function

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Z},$$

which sends x to $x + 1$.

This is a bijection. Indeed, its inverse is the function

$$g\colon \mathbb{Z} \longrightarrow \mathbb{Z},$$

which sends x to $x - 1$. Thus $f \in A(S)$.

On the other hand f is clearly an element of $T(X)$, since if $x > 0$ then so is $x + 1$.

But g is not an element of $T(X)$. Indeed $g(1) = 0 \notin X$. Thus $T(X)$ is not closed under taking inverses.

5. **Challenge Problems** Chapter 2, Section 3: 26. The right cosets are precisely the equivalence classes of an appropriate relation (just as in class). It follows that they must be disjoint.

Here is a direct proof. Suppose that $g \in Ha \cap Hb$. Then $g = h_1 a = h_2 b$, for some h_1 and h_2. Thus $b = h_2^{-1} h_1 a$. Suppose that $k \in Hb$. Then $k = hb = (hh_2^{-1}h_1)a$. As H is a subgroup $hh_2^{-1}h_1 \in H$. Thus $k \in Ha$. Thus $Hb \subset Ha$. By symmetry $Ha \subset Ha$. Thus $Ha = Hb$.

5. **Challenge Problems** Chapter 2, Section 3: 27. $|Ha| = |H|$. This was proved in class.

Here is another proof. Suppose that the elements of $|H|$ are $h_1, h_2, \dots, h_k$, so that $k = |H|$. Then the elements of Ha are $h_1 a$, $h_2 a$, $\dots$, $h_k a$. It suffices to show that these elements are distinct. Suppose not. Then

$$h_i a = h_j a$$

for $i \neq j$. But since we have a group, we can cancel (that is multiply by a^{-1} on the right). Thus

$$h_i = h_j.$$