MODEL ANSWERS TO HWK #2

1. (i) If $h \in Z(G)$ if and only if $gh = hg$ for all $g \in H$. But $gh = gh$ if and only if $h \in C_g$. Hence

$$Z(G) = \bigcap_{g \in G} C_g.$$

(ii) We already proved that each C_g is a subgroup of G and the intersection of subgroups is a subgroup so $Z(G)$ is a subgroup.
2. As $|a| = |a|$, $a \sim a$ and $\sim$ is reflexive. If $a \sim b$ then $|a| = |b|$. But then $|b| = |a|$ and $b \sim a$. So $\sim$ is symmetric. Finally, if $a \sim b$ and $b \sim c$ then $|a| = |b|$ and $|b| = |c|$. It follows that $|a| = |c|$ so that $a \sim c$.
The equivalence classes are the circles centred at the origin.
3. 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.

4. First we write down the elements of U_{18}. These will be the left cosets, generated by integers coprime to 18. Of the integers between 1 and 17, those that are coprime are 1, 3, 5, 7, 11, 13 and 17.
Thus the elements of U_{18} are [1], [3], [5], [7], [11], [13] and [17]. We calculate the order of these elements.
[1] is the identity, it has order one.
Consider [5].
$$[5]^2 = [5^2] = [25] = [7],$$
as $25 = 7 \mod 18$. In this case
$$[5^3] = [5][5^2] = [5][7] = [35] = [17],$$
as $35 = 17 \mod 18$.
We could keep computing. But at this point, we can be a little more sly. By Lagrange the order of $g = [5]$ divides the order of G. As G has order 6, the order of [5] is one of 1, 2, 3, or 6. As we have already seen that the order is not 1, 2 or 3, by a process of elimination, we know that [5] has order 6. (Or we could use the fact that $[17] = [-1]$.)
As $[17] = [5]^3$, $[17]^2 = [5]^6 = [1]$. So [17] has order 2. Similarly, as $[7] = [5]^2$, $[7]^3 = [5]^6 = [1]$. So the order of [7] divides 3. But then the order of [7] is three.
It remains to compute the order of [11] and [13]. Now one of these is the inverse of [5]. It must then have order six. The other would then be $[5]^4$ and so this element would have order dividing 3, and so its order would be 3. Let us see which is which.
$$[5][11] = [55] = [1]$$
Thus [11] is the inverse of [5] and so it has order 6. Thus $[11] = [5]^5$. It follows that $[13] = [5]^4$ and so [13] has order 3.
Note that U_{18} is cyclic. In fact either [5] or [11] is a generator.
5. First we write down the elements of U_{20}. Arguing as before, we get [1], [3], [7], [9], [11], [13], [17] and [19].
We compute the order of [3].
$$[3]^2 = [9].$$
$$[3]^3 = [27] = [7].$$
$$[3^4] = [3][3^3] = [3][7] = [21] = [1].$$
So [3] and [7] are elements of order 4 and [9] is an element of order 2. Now note that the other elements are the additive inverses of the elements we just wrote down. Thus for example
$$[17]^2 = [-3]^2 = [3]^2 = [9].$$

So [17] and [13] have order 4 and [11] and $[19] = [-1]$ have order 2. Thus U_{20} is not cyclic.

6. The elements of D_4 are $\{ I, R, R^2, R^3, S_1, S_2, D_1, D_2 \}$, where R is rotation through $90°$ degrees, clockwise, S_1 and S_2 are the two side flips and D_1, D_2 are the two diagonal flips.

The order of any subgroup divides 8 by Lagrange. The divisors of 8 are 1, 2, 4 and 8. Two extreme cases are 1 and 8, in which case we get the trivial subgroup $\{I\}$ and the whole group D_4.

A subgroup of order 2 is generated by an element of order 2. The elements of order 2 are R^2, S_1, S_2, D_1 and D_2. Accordingly there are five subgroups of order 2, $\{ I, R^2 \}$, $\{ I, S_1 \}$, $\{ I, S_2 \}$, $\{ I, D_1 \}$ and $\{ I, D_2 \}$.

A subgroup of order 4 can come in two possible flavours. If the subgroup is cyclic it must be generated by an element of four. D_4 contains only two elements of order 4, R and R^3 and they both generate the same subgroup, $\{ I, R, R^2, R^3 \}$. The final possibility is a subgroup of order four that contains three elements of order 2.

We need to combine to consider the subgroup generated by two elements of order 2.

We first try to combine a side flip with a diagonal flip. By symmetry we can consider S_1 and D_1. As $S_1 D_1 = R$, the group generated by S_1 and D_1 must contain R, so that it must be the whole of D_4.

Now consider combining rotations and flips. Note that $F_1 F_2 = R^2$ and $D_1 D_2 = R^2$ 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 $F_1 F_2$. It remains to check $F_1 R^2$ and $F_2 R^2$. Consider the equation $F_1 F_2 = R^2$. Multiplying by F_1 on the left, and using the fact that it is its own inverse, we get $F_2 = F_1 R^2$. 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.

7. For every i, there is a unique b_i which is the inverse of a_i. Thus the elements of G are both $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$. Now

$$\begin{aligned} x^2 &= (a_1a_2\dots a_n)(a_1a_2\dots a_n) \\ &= (a_1a_2\dots a_n)(b_1b_2\dots b_n) \\ &= (a_1b_1)(a_2b_2)(a_3b_3)\cdots(a_nb_n) = e^n = e, \end{aligned}$$

where we used the fact that G is abelian to rearrange these products.
8. Suppose not, that is, suppose that there is a number a such that $a^2 = -1 \mod p$. Let $g = [a] \in U_p$. What is the order of g?
Well

$$g^2 = [a]^2 = [a^2] = [-1] \neq [1],$$

and so

$$g^4 = (g^2)^2 = [-1]^2 = [1].$$

Thus g has order 4. But the order of any element divides the order of the group, in this case $p-1 = 4n+2$. But 4 does not divide $4n+2$, a contradiction.
9. Define

$$f\colon T \longrightarrow S$$

by the rule

$$f(Ha) = a^{-1}H.$$

The key point is to check that f is well-defined. The problem is that if $b \in Ha$ then $Ha = Hb$ and we have to check that $a^{-1}H = b^{-1}H$.
As $b \in Ha$, we have $b = ha$. But then $b^{-1} = a^{-1}h^{-1}$. As H is a subgroup $h^{-1} \in H$. But then $b^{-1} \in a^{-1}H$ so that $a^{-1}H = b^{-1}H$ and f is well-defined.
To show that f is a bijection, we will show that it has an inverse. Define

$$g\colon S \longrightarrow T$$

by the rule

$$g(aH) = Ha^{-1}.$$

We have to show that g is well-defined. This follows similarly to the proof that f is well-defined.
We now that g is the inverse of f.

$$\begin{aligned} (g\circ f)(Ha) &= g(f(Ha)) \\ &= g(a^{-1}H) \\ &= H(a^{-1})^{-1} \\ &= Ha. \end{aligned}$$

Therefore $g\circ f$ is the identity. Similarly $f\circ g$ is the identity. It follows that f is a bijection.

10. Let $[a]_L$ denote the left-coset generated by a and let $[a]_R$ denote the right-coset generated by a. Suppose that $b \in [a]_L$. Then $[a]_L = [b]_L$ and so $aH = bH$. By assumption $Ha = Hb$. But then $[a]_R = [b]_R$ and so $b \in [a]_R$.
As b is an arbitrary element of $[a]_L$, it follows that $[a]_L \subset [a]_R$. In other words $aH \subset Ha$. Multiplying both sets on the right by a^{-1} we get the inclusion

$$aHa^{-1} \subset H(aa^{-1}) = H.$$

Now this is valid for any $a \in G$, so that

$$bHb^{-1} \subset H.$$

for all $b \in G$. Take $b = a^{-1}$. Then

$$a^{-1}Ha \subset H,$$

so that multipying on the left by a, we get

$$Ha \subset aH.$$

Thus $Ha = aH$ and $aHa^{-1} = H$.
11. Let $m = a^n - 1$. Then $\phi(m)$ is the order of the group generated by $G = U_m$. It suffices to exhibit an element g of G of order n.
Set $g = [a]$. Now

$$g^n = [a]^n = [a^n] = [m + 1] = [1].$$

So the order of g divides n. On the other hand $a^i < m$, for any $i < n$ so that

$$g^i = [a^i] \neq [1].$$

Thus the order of g is n and so n divides m by Lagrange.
12. Let G be a cyclic group of order n, and let $g \in G$ be a generator of G. Suppose $h \in G$. Then $h = g^i$, for some i.
I claim that h has order m iff $i = kj$, where $k = n/m$ and j is coprime to m.
Suppose that $i = kj$. Then

$$h^m = (g^i)^m = g^{kjm} = g^{jn} = e.$$

Now suppose that $a < m$ and consider $h^a = g^{akj}$. This is equal to the identity iff akj is divisible by n. Dividing by k, this is the same as saying that aj is divisible by m. As j is coprime to m, this would mean that m divides a, impossible.
This establishes the claim. The number of integers of the form kj, where j is coprime to m, is equal to the number of integers j coprime to m (and less than m) which is $\phi(m)$.

13. Let G be a cyclic group of order n. Partition the elements of G into subsets A_m, where A_m consists of all elements of order m. Then

$$\begin{aligned} n &= |G| \\ &= |\bigcup_{m|n} A_m| \\ &= \sum_{m|n} |A_m| = \sum_{m|n} \phi(m). \end{aligned}$$

14. Let G be the set of all complex numbers of the form

$$\exp\left(\frac{a}{2^m}\right),$$

where a is an integer, $m \in \mathbb{N}$ is a natural number and

$$\exp(x) = e^{2\pi i x}.$$

We first check that G is a group under multiplication of complex numbers. As G is a subset of the group $\mathbb{C}^*$, it suffices to check that G is non-empty, and closed under multiplication and inverses. It is clearly non-empty, for example,

$$1 = \exp(0) \in G.$$

If

$$\exp\left(\frac{a}{2^m}\right) \qquad \text{and} \qquad \exp\left(\frac{b}{2^n}\right),$$

then first note we may assume that $m = n$ (multiply a and b by appropriate powers of 2). In this case the product

$$\exp\left(\frac{a}{2^n}\right)\exp\left(\frac{b}{2^n}\right) = \exp\left(\frac{a+b}{2^n}\right) \in G.$$

Therefore G is closed under multiplication. Similarly the inverse of

$$\exp\left(\frac{a}{2^m}\right) \qquad \text{is} \qquad \exp\left(\frac{-a}{2^m}\right) \in G,$$

and so G is closed under inverses. Thus G is a group.
Suppose that H is a subgroup of G which contains

$$g = \exp\left(\frac{a}{2^m}\right)$$

where a is odd. As a and 2^m are coprime, we may find integers p and q such that

$$pa + q2^m = 1.$$

As H is closed under multiplication and inverses, H must contain

$$g^p = \exp\left(\frac{pa}{2^m}\right) = \exp\left(\frac{pa + q2^m}{2^m}\right) = \exp\left(\frac{1}{2^m}\right).$$

But then H must contain the finite set

$$H_m = \{\, \exp\left(\frac{i}{2^m}\right) \,|\, 0 \leq i \leq 2^m - 1 \,\},$$

(which one may check is in fact a subgroup).
Note that if $m \leq l$ then $H_m \subset H_l$. Furthermore,

$$G = \bigcup_{m \in \mathbb{N}} H_m.$$

Now suppose that H is infinite. If m is a natural number then H is not contained in H_m, since H_m is finite. But then H contains an element $g \in H_l$ not in H_m. Let l be the smallest integer such that $g \in H_l$. Then

$$g = \exp\left(\frac{a}{2^l}\right),$$

where a is odd. But then H contains H_l so that it contains H_m. As m is arbitrary $H = G$.
So G contains no proper infinite subgroups.