MODEL ANSWERS TO HWK #4

1. (i) Yes. Given a and $b \in \mathbb{Z}$,

$$\begin{aligned}\varphi(ab) &= [ab] \\ &= [a][b] \\ &= \varphi(a)\varphi(b).\end{aligned}$$

This map is clearly surjective but not injective. Indeed the kernel is easily seen to be $n\mathbb{Z}$.
(ii) No. Suppose that G is not abelian and that x and y are two elements of G such that $xy \neq yx$. Then $x^{-1}y^{-1} \neq y^{-1}x^{-1}$. On the other hand

$$\begin{aligned}\varphi(xy) &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &\neq x^{-1}y^{-1} \\ &= \varphi(x)\varphi(y),\end{aligned}$$

and one wrong certainly does not make a right.
(iii) Yes. Suppose that x and y are in G. As G is abelian

$$\begin{aligned}\varphi(xy) &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &= x^{-1}y^{-1} \\ &= \varphi(x)\varphi(y).\end{aligned}$$

Thus φ is a homomorphism. φ is its own inverse, since $(a^{-1})^{-1} = a$ and φ is a bijection.
In particular the kernel of φ is trivial.
(iv) Yes. φ is a homomorphism as the product of two positive numbers is positive, the product of two negative numbers is positive and the product of a negative and a positive number is negative.
This map is clearly surjective. The kernel consists of all positive real numbers. Thus φ is far from injective.

(v) Yes. Suppose that x and y are in G. Then

$$\begin{aligned}\varphi(xy) &= (xy)^n \\ &= x^n y^n \\ &= \varphi(x)\varphi(y).\end{aligned}$$

In general this map is neither injective nor surjective. For example, if $G = \mathbb{Z}$ and $n = 2$ then the image of φ is $2\mathbb{Z}$, and for example 1 is not in the image.
Now suppose that $G = \mathbb{Z}_4$ and $n = 2$. Then $2[2] = [4] = [0]$, so that $[2]$ is in the kernel. In general the kernel of φ is

$$\operatorname{Ker}\varphi = \{\, g \in G \,|\, g^n = e \,\}.$$

2. We need to check that $aHa^{-1} = H$ for all

$$a \in G = \{\, I, R, R^2, R^3, S_1, S_2, D_1, D_2 \,\}.$$

Since H is generated by R,

$$H = \langle R \rangle = \{\, I, R, R^2, R^3 \,\},$$

it suffices to check that $aRa^{-1} \in H$. If we pick $a \in H$ there is nothing to prove. By symmetry we only need to worry about $a = S_1$ and $a = D_1$.

$$S_1RS_1^{-1} = S_1RS_1 = D_1S_1 = R^3 \qquad \text{and} \qquad D_1RD_1^{-1} = D_1RD_1 = S_2D_1 = R^3,$$

which is in H. Thus $H \lhd G$.
3. Let $g \in G$. We want to show that $gZg^{-1} \subset Z$. Pick $z \in Z$. Then z commutes with g, so that $gzg^{-1} = zgg^{-1} = z \in Z$. Thus Z is normal in G.
4. Let $g \in G$. We want to show that $g(H \cap K)g^{-1} \subset H \cap K$. Pick $l \in H \cap K$. Then $l \in H$ and $l \in K$. It follows that $glg^{-1} \in H$ and $glg^{-1} \in K$, as both H and K are normal in G. But then $glg^{-1} \in H \cap K$ and so $H \cap K$ is normal.
5. $H = \{e, (1,2)\}$. Then the left cosets of H are
(i)

$$\begin{aligned} H &= \{e, (1,2)\} \\ (1,3)H &= \{(1,3), (1,2,3)\} \\ (2,3)H &= \{(2,3), (1,3,2)\} \end{aligned}$$

and the right cosets are

(ii)

$$\begin{aligned} H &= \{e, (1,2)\} \\ H(1,3) &= \{(1,3), (1,3,2)\} \\ H(2,3) &= \{(2,3), (1,2,3)\}. \end{aligned}$$

(iii) Clearly not every left coset is a right coset. For example $\{(1,3),(1,2,3)\}$ is a left coset, but not a right coset.
6. (i) Suppose that a and $b \in G$. Let $c = ab$ and $\sigma = \sigma_a = \psi(a)$, $\tau = \sigma_b = \psi(b)$ and $\rho = \sigma_c = \psi(c)$. We want to check that

$$\rho = \sigma\tau.$$

Since both sides are permutations of G, it suffices to check that both sides have the same effect on an arbitrary element $g \in G$.

$$\begin{aligned} (\sigma \circ \tau)(g) &= \sigma(\tau(g)) \\ &= \sigma(bgb^{-1}) \\ &= a(bgb^{-1})a^{-1} \\ &= (ab)g(ab)^{-1} \\ &= cgc^{-1} \\ &= \rho(g). \end{aligned}$$

Thus ψ is a group homomorphism.
(ii) Suppose that $z \in Z(G)$. Let $\sigma = \sigma_z = \psi(z)$. Then

$$\sigma(g) = zgz^{-1} = gzz^{-1} = g.$$

Thus σ is the identity permutation and $z \in \operatorname{Ker}\psi$. Thus

$$Z(G) \subset \operatorname{Ker}\psi.$$

Now suppose $a \in \operatorname{Ker}\psi$. Let $\sigma = \sigma_a = \psi(a)$. Then σ is the identity permutation, so that

$$g = \sigma(g) = aga^{-1},$$

for any $g \in G$. But then $ga = ag$ for all $g \in G$ so that $a \in Z(G)$. Thus

$$\operatorname{Ker}\psi \subset Z(G),$$

so that $\operatorname{Ker}\psi = Z(G)$.
7. Let $g \in G$. We have to show that $g\theta(N)g^{-1} \subset \theta(N)$. Now as θ is surjective, we may write $g = \theta(h)$, for some $h \in G$. Pick $m \in \theta(N)$. Then $m = \theta(n)$, for some $n \in N$. We have

$$\begin{aligned} gmg^{-1} &= \theta(h)\theta(n)\theta(h)^{-1} \\ &= \theta(hnh^{-1}). \end{aligned}$$

Now $hnh^{-1} \in N$ as N is normal. So $gmg^{-1} \in \theta(N)$ and $\theta(N)$ is normal in G.

8. Note that S_3 is the group of permutations of three objects. So we want to find three things on which G acts. Pick any element h of G. Then the order of h divides the order of G. As the order of G is six, it follows that the order of h is one, two, three, or six. It cannot be six, as then G would be cyclic, whence abelian, and it can only be one if h is the identity.

We first try to prove that G contains an element of order 2. Suppose not. Let a be an element of G, not the identity. Then $H_1 = \langle a \rangle = \{ e, a, a^2 \}$ contains three elements. Pick an element b of G not an element of H_1. Then $H_2 = \langle b \rangle = \{ e, b, b^2 \}$ contains three elements, two of which, b and b^2, are not elements of H_1. Thus $H_1 \cup H_2$ has five elements. The last element c of G must have order two, a contradiction. Thus G contains an element of order 2.

Suppose that a has order two. Let $H = \langle a \rangle = \{ e, a \}$, a subgroup of G of order two. Pick an element b which does no belong to H. Consider the group generated by a and b, $K = \langle a, b \rangle$. This has at least three elements, e, a and b. The order of K divides G, so that K has order 3 or 6, by Lagrange. K contains H, so that the order of K is even. It follows that K has order 6, so that $G = \langle a, b \rangle$. As G is not abelian, a and b don't commute, $ab \neq ba$.

The number of left cosets of H in G (the index of H in G) is equal to three, by Lagrange. Let S be the set of left cosets. Define a map from G to $A(S)$ as follows,

$$\phi\colon G \longrightarrow A(S)$$

by sending g to $\sigma = \phi(g)$, where σ is the map,

$$\sigma\colon S \longrightarrow S$$

$\sigma(xH) = gxH$, that is, σ acts on the left cosets by left multiplication by g. Suppose that $xH = yH$, then $y = xh$ and $(gy) = (gx)h$ so that $(gx)H = (gy)H$ and ϕ is well-defined. σ is a bijection, as its inverse τ is given by left multiplication by g^{-1}. Now we check that ϕ is a homomorphism. Suppose that g_1 and g_2 are two elements of G. Set $\sigma_i = \phi(g_i)$ and let $\tau = \phi(g_1 g_2)$. We need to check that $\tau = \sigma_1\sigma_2$. Pick a left coset xH. Then

$$\begin{aligned} \sigma_1\sigma_2(xH) &= \sigma_1(g_2 xH) \\ &= g_1 g_2 xH \\ &= \tau(xH). \end{aligned}$$

Thus ϕ is a homomorphism. We check that ϕ is injective. It suffices to prove that the kernel of ϕ is trivial. Pick $g \in \operatorname{Ker} \phi$. Then $\sigma = \phi(g)$ is the identity permutation, so that for every left coset xH,

$$gxH = xH.$$

Consider the left coset H. Then $gH = H$. It follows that $g \in H$, so that either $g = e$ or $g = a$. If $g = a$, then consider the left coset bH. We would then have $abH = bH$, so that $ab = bh'$, where $h' \in H$. So $h' = e$ or $h' = a$. If $h' = e$, then $ab = b$, and $a = e$, a contradiction. Otherwise $ab = ba$, a contradiction. Thus $g = e$, the kernel of ϕ is trivial and ϕ is injective.
As both G and $A(S)$ have order six and ϕ is injective, it follows that ϕ is a bijection. Hence G is isomorphic to S_3.
9. Let G be a group of order nine. Let $g \in G$ be an element of G. Then the order of g divides the order of G. Thus the order of g is 1, 3 or 9. If G is cyclic then G is certainly abelian. Thus we may assume that there is no element of order nine. On the other hand the order of g is one iff $g = e$.
Thus we may assume that every element of G, other than the identity, has order three. Let $a \in G$ be an element of G, other than the identity. Let $H = \langle a \rangle$. Then H has order three. Let S be the set of left cosets of H in G. By Lagrange S has three elements. Let

$$\phi \colon G \longrightarrow A(S) \simeq S_3$$

be the map given by left multiplication. As in question 8, ϕ is a group homomorphism. Let G' be the order of the image. Then G' divides the order of G, by Lagrange and it also divides the order of S_3. Thus G' must have order three. It follows that the kernel of ϕ has order three. Thus the kernel of ϕ is H and H is a normal subgroup of G.
Let $b \in G$ be any element of G. Then bab^{-1} must be an element of H, as H is normal in G. It is clear that $bab^{-1} \neq e$. If $bab^{-1} = a$ then $ba = ab$, so that a and b commute. If $bab^{-1} = a^2$ then

$$\begin{aligned} b^{-1}ab &= b^2ab^{-2} \\ &= b(bab^{-1})b^{-1} \\ &= ba^2b^{-1} \\ &= (bab^{-1})(bab^{-1}) \\ &= a, \end{aligned}$$

and so $ab = ba$. Therefore G is abelian.
10. Let S be the set of left cosets of H in G. Define a map

$$\phi \colon G \longrightarrow A(S)$$

by sending $g \in G$ to the permutation $\sigma \in A(S)$, a map

$$S \longrightarrow S$$

defined by the rule $\sigma(aH) = gaH$. As in question 8, ϕ is a homomorphism.

Let N be the kernel of ϕ. Then N is normal in G. Suppose that $n \in N$ and let $\sigma = \phi(n)$. Then σ is the identity permutation of S. In particular $\sigma(H) = H$, so that $nH = H$. Thus $n \in H$ and so $N \subset H$. Let n be the index of H, so that the image of G has at most $n!$ elements. In this case there are at most $n!$ left cosets of N in G, since each left coset of N in G is mapped to a different element of $A(S)$.

11. Let A be the set of elements such that $\phi(a) = a^{-1}$. Pick an element $g \in G$ and let $B = g^{-1}A$. Then

$$\begin{aligned}
|A \cap B| &= |A| + |B| - |A \cup B| \\
&> (3/4)|G| + (3/4)|G| - |G| \\
&= (1/2)|G|.
\end{aligned}$$

Now suppose that $g \in A$. If $h \in A \cap B$ then $gh \in A$. It follows that

$$\begin{aligned}
h^{-1}g^{-1} &= (gh)^{-1} \\
&= \phi(gh) \\
&= \phi(g)\phi(h) \\
&= g^{-1}h^{-1}.
\end{aligned}$$

Taking inverses, we see that g and h must commute. Let C be the centraliser of g. Then $A \cap B \subset C$, so that C contains more than half the elements of G. On the other hand, C is a subgroup of G. By Lagrange the order of C divides the order of G. Thus $C = G$. Hence g is in the centre Z of G and so the centre Z of G contains at least $3/4$ of the elements of G. But then the centre of G must also equal G, as it is also a subgroup of G. Thus G is abelian.