MODEL ANSWERS TO THE FIFTH HOMEWORK

1. Chapter 3, Section 5: 1 (a) Yes. Given a and $b \in \mathbb{Z}$,

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

This map is clearly surjective but not injective. Indeed the kernel is easily seen to be $n\mathbb{Z}$.

(b) No. Suppose that G is not abelian and that $xy \neq yx$. Then $x^{-1}y^{-1} \neq y^{-1}x^{-1}$. On the other hand

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

and one wrong certainly does not make a right.

(c) Yes. Suppose that x and y are in G. As G is abelian

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

Thus ϕ is a homomorphism. Suppose that $a \in G$. Then a is the inverse of $b = a^{-1}$, so that $\phi(b) = a$. Thus ϕ is surjective. Suppose that a is in the kernel of ϕ. Then $a^{-1} = e$ and so $a = e$. Thus the kernel of ϕ is trivial and ϕ is injective.

(d) 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.

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

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

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.
10. We need to check that $aHa^{-1} = H$ for all $a \in G$. If we pick $a \in H$ there is nothing to prove. Now $a = f^i g^j$. Conjugation by a is the same as conjugation by g^j followed by conjugation by f^i. So we only need to worry about conjugation by f. Now $gf = fg^{-1}$ so that $fgf^{-1} = g^{-1}$. Thus conjugation by f leaves H fixed, as it sends a generator to a generator.
12. 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.
16. We need to show that MN is non-empty and closed under products and inverses. MN is non-empty as it contains $e = ee$.
Suppose that a_1 and a_2 belong to MN. Then we may find $m_i \in M$ and $n_i \in N$, such that $a_i = m_i n_i$, $i = 1$ and 2. As M is normal

$$m = n_1 m_2 n_1^{-1} \in M \qquad \text{so that} \qquad n_1 m_2 = m n_1.$$

In this case

$$\begin{aligned} a_1 a_2 &= (m_1 n_1)(m_2 n_2) \\ &= m_1 (n_1 m_2) n_2 \\ &= m_1 (m n_1) n_2 \\ &= (m_1 m)(n_1 n_2) \in MN \end{aligned}$$

as $m_1 m \in M$ and $n_1 n_2 \in N$. Thus MN is closed under products.
Now suppose that $a = mn \in MN$. As M is normal

$$l = n^{-1} m^{-1} n \in M \qquad \text{so that} \qquad n^{-1} m^{-1} = l n^{-1} \in MN.$$

Thus MN is closed under inverses.
It follows that MN is a subgroup of G.
Now suppose that $g \in G$ and $a = mn \in MN$. Then

$$\begin{aligned} gag^{-1} &= g(mn)g^{-1} \\ &= (gmg^{-1})(gng^{-1}) \in MN, \end{aligned}$$

as both M and N are normal. Thus MN is normal in G.
22. $H = \{e, (1, 2)\}$. Then the left cosets of H are

(a)

$$H = \{e, (1,2)\}$$
$$(1,3)H = \{(1,3), (1,2,3)\}$$
$$(2,3)H = \{(2,3), (1,3,2)\}$$

and the right cosets are
(b)

$$H = \{e, (1,2)\}$$
$$H(1,3) = \{(1,3), (1,3,2)\}$$
$$H(2,3) = \{(2,3), (1,2,3)\}.$$

(c) 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.
23. Let H be the subgroup generated by a. By assumption H is normal in G. It follows that $bab^{-1} \in H$. Thus

$$bab^{-1} = a^j,$$

some j. But then

$$ba = a^j b.$$

26. (a) Let a and $b \in G$. Let $\sigma = \sigma_a$, $\tau = \sigma_b$ and $\rho = \sigma_{ab}$. We want to check that $\rho = \sigma\tau$. Both sides of this equation are functions from G to G, so we just need to check that they have the same effect on an element $g \in G$:

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

Thus ϕ is a group homomorphism.
(b) Suppose that $a \in Z$ and let $\sigma = \sigma_a = \phi(a)$. If $g \in G$ then

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

Thus σ is the identity map and so $a \in \operatorname{Ker}\phi$.
Now suppose that $a \in \operatorname{Ker}\phi$. Then σ is the identity map and so

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

Multiplying on the right by a we get

$$ga = ag,$$

so that $a \in Z$. Thus $Z = \operatorname{Ker}\phi$.
28. $\operatorname{Aut}(G)$ is certainly non-empty, as it contains the identity. We check that $\operatorname{Aut}(G) \subset A(S)$ is closed under products and inverses.
Suppose that ϕ and $\psi \in \operatorname{Aut}(G)$. Let $\xi = \phi \circ \psi$. If g and $h \in G$ then

$$\begin{aligned}\xi(gh) &= (\phi \circ \psi)(gh) \\ &= \phi(\psi(gh)) \\ &= \phi(\psi(g)\psi(h)) \\ &= \phi(\psi(g))\phi(\psi(h)) \\ &= (\phi \circ \psi)(g)(\phi \circ \psi)(h) \\ &= \xi(g)\xi(h).\end{aligned}$$

Thus $\xi = \phi \circ \psi$ is a group homomorphism. Thus $\operatorname{Aut}(G)$ is closed under products.
Now let $\xi = \phi^{-1}$. If g and $h \in G$ then we can find g' and h' such that $g = \phi(g')$ and $h = \phi(h')$. It follows that

$$\begin{aligned}\xi(gh) &= \xi(\phi(g')\phi(h')) \\ &= \xi(\phi(g'h')) \\ &= g'h' \\ &= \xi(g)\xi(h).\end{aligned}$$

Thus $\xi = \phi^{-1}$ is a group homomorphism. Thus $\operatorname{Aut}(G)$ is closed under inverses.
37. 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.
Note that elements of order 3 come in pairs. If a is an element of order 3 then $a^2 = a^{-1}$ also has order three and they are the two elements of $\langle a \rangle$ not equal to the identity. So the number of elements of order 3 is even. As there are five elements of G which don't have order one, it follows that at least one element a of G has order 2. If $H = \langle a \rangle$ then H is a subgroup of G of order two.
Let b be any other element of G. Consider the subgroup $K = \langle a, b \rangle$ of G generated by a and b. Then K has at least three elements, e, a and b and on the other hand the order of K is even by Lagrange as H is a subgroup of order 2. Thus K has at least four elements. As the order of K divides the order of G the order of K is six, so that $G = \langle a, b \rangle$ is generated by a and b.

If $ab = ba$ it is not hard to check that G is abelian. As G is not abelian we must have $ab \neq ba$.
As H is a subgroup of G of order two, 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 $A(S)$,

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

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. If $xH = yH$ so that $y = xh$ for some $h \in H$ then

$$gy = g(xh) = (gx)h,$$

so that $(gy)H = (gx)H$ and σ 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

$$\begin{aligned}\sigma_1\sigma_2(xH) &= \sigma_1(g_2xH)\\ &= g_1g_2xH\\ &= \tau(xH).\end{aligned}$$

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 $A(S)$ has order six and ϕ is injective, it follows that ϕ is a bijection.
Thus G is isomorphic to S_3.
1. Chapter 3, Section 6: 1 There are two cosets. The first coset is $[1] = N$, the second is the coset containing -1, which is the set of all negative real numbers.
$[1] \cdot [1] = [1]$, $[1] \cdot [-1] = [-1] \cdot [1] = [-1]$ and $[-1] \cdot [-1] = [1]$.

Chapter 3, Section 6: 2. Let $a \in \mathbb{R}$. Then $[a] = \{a, -a\}$. Thus any coset contains two elements, exactly one of which is a positive real number. Given a and b positive, $[a][b] = [ab]$. Define a homomorphism

$$\phi\colon G \longrightarrow \mathbb{R}^+,$$

by sending a to $|a|$. The kernel is $N = \{1, -1\}$. By the first Isomorphism Theorem, $G/N \simeq \mathbb{R}^+$.
Chapter 3, Section 6: 3. Consider the canonical homomorphism

$$u\colon G \longrightarrow G/N.$$

Then $M = u^{-1}(\bar{M})$. As the kernel of u is N, it follows that M contains N, as $\bar{M}$ contains the identity of G/N.
To show that M is a subgroup of G, it suffices to prove that it is closed under products and inverses. Suppose that a and b are in M. Then $u(a)$ and $u(b)$ are in $\bar{M}$. Then $u(ab) = u(a)u(b) \in \bar{M}$ as $\bar{M}$ is closed under products.
Thus $ab \in M$ and M is closed under products.
Similarly $u(a^{-1}) = u(a)^{-1} \in \bar{M}$ as $\bar{M}$ is closed under inverses. Thus $a^{-1} \in M$ and M is closed under inverses.
Thus M is a subgroup of G.
Chapter 3, Section 6: 4. Suppose that $\bar{M}$ is normal in G/N.
Pick $g \in G$. We want to prove $gMg^{-1} \subset M$. Pick $a \in M$. Then

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1}.$$

As $\bar{M}$ is normal in G/N, it follows that $\phi(g)\phi(a)\phi(g)^{-1} \in \bar{M}$. But then $gag^{-1} \in M$.
Challenge Problems (Just for fun)
43. 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 if and only if $g = e$.
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 corresponding homomorphism. Let G' be the order of the image. Then the order of G' is the number of left cosets of the kernel, which divides G by Lagrange. On the other hand the order of G' divides the order of $A(S)$, again by Lagrange.

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 that does not commute with a. Then bab^{-1} must be an element of H, as H is normal in G, and so $bab^{-1} = a^2$. It follows that $ba = a^2b^2$. In this case

$$\begin{aligned}(ba)^2 &= baba \\ &= a^2b^2ba \\ &= a^2a \\ &= e.\end{aligned}$$

Thus ba is an element of order 2, which is impossible as G has order 9.
49. 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

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

defined by the rule $\sigma(aH) = gaH$. Note that τ, which acts by multiplication on the left by g^{-1} is the inverse of σ, so that σ is indeed a permutation of S. It is easy to check, as before, that ϕ is a homomorphism.
Let N be the kernel of ϕ. Then N is normal in G. Suppose that $a \in N$ and let $\sigma = \phi(a)$. Then σ is the identity permutation of S. In particular $\sigma(H) = H$, so that $aH = H$. Thus $a \in H$ 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 $A(S)$. Thus the index of N is at most $n!$.
52. 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 pick $h \in A \cap B$ and suppose that $g \in A$. 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 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.