Practice Midterm Solutions

Robert Kropholler

October 28, 2018

1. Bookwork.

2. (a) Let $g \in I_G$, i.e. $g^2 = e$. We have the sequence of equalities $\phi(g)^2 = \phi(g^2) = \phi(e) = e$. Thus $\phi(g) \in I_H$.

   (b) Suppose that ϕ is an isomorphism. Let $h \in I_H$. There is a $g \in G$ such that $h = \phi(g)$. Since $\phi(g)^2 = h^2 = e$ and ϕ is an isomorphism we can see that $g^2 = e$ and $g \in I_G$. Thus we have a surjection from I_G to I_H. This is also injective, since ϕ is injective.

   (c)

   (d)

   (e) We can see that the only elements in Q_8 which satisfy $g^2 = e$ are ± 1. For D_4 there are 4 elements satisfying this equality. Thus, we cannot have an isomorphism between these groups by part b).

3. (a) We have the following chain of equalities.

$$\phi([k]) = \phi([1] + [1] + \cdots + [1]) = \phi([1]) + \phi([1]) + \cdots + \phi([1]).$$

   Thus once we know $\phi([1])$ we know $\phi([k])$ for all k.

   (b) Since $\phi([1]) = [k]$ for some k. We see that $\phi([a]) = [ka]$ by part a). Thus, all homomorphisms must be of this form.

   (c) To find the order of $[k]$ we must consider when does $[k]^l = [kl] = [0]$. This is the case if and only if n divides ka. We can see that this first occurs at $\frac{n}{\gcd(k,n)}$.

   (d) If the map is an isomorphism then $o(\phi([1])) = o([1]) = n$. Assume that the automorphism send $[1]$ to $[k]$. We must have that $\frac{n}{\gcd(k,n)} = n$. To have this equality we need that $\gcd(k,n) = 1$.

   Suppose that $\gcd(k,n) = 1$. Then we can define a homomorphism by $\phi([1]) = [k]$. This is an isomorphism since $o([k]) = n$ by part b).

   (e) We now have a bijection from the group $Aut(\mathbb{Z}/n\mathbb{Z}) = \{\phi \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \mid \phi \text{ is an isomorphism } \}$ to the set $(\mathbb{Z}/n\mathbb{Z})^\times$. We can also see that this map defines an isomorphism.

$\cdot$	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1