Kyle Kloberdanz
Math 417

Exercise 3.3.1: Suppose $\phi : G \to H$ is a homomorphism, and $g \in G$. Prove that for all $n > 0$ we have $\phi(g^n) = \phi(g)^n$ by induction on n, thus completing the proof for Proposition 3.3.4

Proof. Base case, let $n = 1$

$$\phi(g^1) = \phi(g) = \phi(g)^1$$

Now, let n = 2

$$\phi(g^2) = \phi(g^{1+1}) = \phi(gg)$$

Because ϕ is a homomorphism

$$\phi(gg) = \phi(g)\phi(g) = \phi(g)^2$$

For $n = 3$

$$\phi(g^3) = \phi(g^{1+2}) = \phi(gg^2) = \phi(g)\phi(g^2)$$

But we have just seen that $\phi(g^2) = \phi(g)^2$, so

$$\phi(g)\phi(g^2) = \phi(g)\phi(g)^2 = \phi(g)\phi(g)\phi(g) = \phi(g)^3$$

By continuing this for any $n \in \mathbb{Z}_+$
$\phi(g^n) = \phi(g^{n-1}g) = \phi(g^{n-1})\phi(g) = \phi(g^{n-2}g)\phi(g) =$
$\phi(g^{n-2})\phi(g)\phi(g) = \phi(g)...$ n times $...\phi(g) = \phi(g)^n$

By continuing this for any $n \in \mathbb{Z}_-$
$\phi(g^n) = \phi(g^{n+1}g) = \phi(g^{n+1})\frac{1}{\phi(g)} = \phi(g^{n+2}g)\frac{1}{\phi(g)} =$
$\phi(g^{n+2})\frac{1}{\phi(g)}\frac{1}{\phi(g)} = \frac{1}{\phi(g)}...$ n times $...\frac{1}{\phi(g)} = \phi(g)^n$

And for $n = 0$, By proposition 3.3.4: $\phi(g^0) = \phi(e) = e = \phi(g)^0$.

Therefore $\phi(g^n) = \phi(g)^n$ □

Exercise 3.3.4: Prove that if G is an abelian group, then every subgroup of G is normal.

Proof. Let $N < G$
Recall, a normal group is a group where for all $g \in G$, $gNg^{-1} = N$.
Because N and G are abelian, $gNg^{-1} = Ngg^{-1} = Ne = N$
Therefore, if G is an abelian group, then every subgroup of G is normal. □

Exercise 3.3.6: Prove that for any subgroup $H < G$ and element $g \in G$, gHg^{-1} is also a subgroup of G, and that $c_g(h) = ghg^{-1}$ defines an isomorphism $c_g : H \to gHg^{-1}$. In particular, if $H \triangleleft G$, then conjugation in G defines an automorphism $c_g : H \to H$.

Proof. First we will show that gHg^{-1} is a subgroup of G. Recall that $gHg^{-1} = \{ghg^{-1}|h \in H\}$.

Because H is a subgroup of G, for all $h_1, h_2 \in H$ and $g_1, g_2 \in G$, $h_1h_2 \in H$ and $g_1g_2 \in G$. Because every $h \in H$ is also in G such that $h \in G$, then $gh \in G$ and $hg \in G$, hence every element in gHg^{-1} can also be found in G, hence $gHg^{-1} \subset G$.

We must show that for all $x, y \in gHg^{-1}$ that $xy \in gHg^{-1}$. Let $h_1, h_2, h_3 \in H$ such that $h_1h_2 = h_3$.

$$xy = (gh_1g^{-1})(gh_2g^{-1}) = gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} = gh_3g^{-1} \in gHg^{-1}$$

Hence, $xy \in gHg^{-1}$.

We must also show that the inverse x^{-1} exists such that $x \in gHg^{-1}$ and $x^{-1} \in gHg^{-1}$. We know that the identity e must be in gHg^{-1}, so we can find x^{-1} as follows.

Let $h \in H$

$$(ghg^{-1})(gh^{-1}g^{-1}) = ghh^{-1}g^{-1} = gg^{-1} = e$$

Hence the inverse x^{-1} exists such that $x \in gHg^{-1}$, and the inverse is $x^{-1} = gh^{-1}g^{-1}$.
Therefore gHg^{-1} is a subgroup of G.

Next, we will show that $c_g(h) = ghg^{-1}$ defines an isomorphism $c_g : H \to gHg^{-1}$.

We will first show that c_g is a homomorphism.

$$c_g(h_1)c_g(h_2) = (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} = c_g(h_1h_2)$$

where $h_1, h_2 \in H$.

Next we will show that ϕ is a bijection.
For injectivity, $c_g(h_1) = c_g(h_2)$ implies that $gh_1g^{-1} = gh_2g^{-1}$. Hence:

$$\begin{aligned} g^{-1}gh_1g^{-1} &= g^{-1}gh_2g^{-1} \\ h_1g^{-1} &= h_2g^{-1} \\ h_1g^{-1}g &= h_2g^{-1}g \\ h_1 &= h_2 \end{aligned}$$

Thus c_g is injective.

Next we must demonstrate surjectivity. Because $gHg^{-1} = \{ghg^{-1}|h \in H\}$, we can see that for every $h \in H$ that $c_g(h)$ is represented in $\{ghg^{-1}|h \in H\}$, and hence in gHg^{-1}, so therefore c_g is surjective.

Because c_g is both surjective and injective, it is bijective. Because c_g is a bijective homomorphism, it is therefore an isomorphism.

By the definition of a normal subgroup, for $g \in G$, $gHg^{-1} = H \iff H \triangleleft G$, therefore, if $H \triangleleft G$ then $H = gHg^{-1}$ thus $c_g : H \to gHg^{-1} = c_g : H \to H$ which is an automorphism.

□

Exercise 3.3.8: Let G be a group and $H < G$ a subgroup. Prove that the set

$$N(H) = \{g \in G | gHg^{-1} = H\} \subset G$$

is a subgroup containing H, and that $H \triangleleft N(H)$.
The subgroup N(H) from Exercise 3.3.8 is called the ***normalizer of H****, and it is (by definition) the largest subgroup of G containing H in which H is normal.*

Proof. In order to show that $N(H)$ is a subgroup of G, we must show that $N(H) \subset G$. Because $N(H)$ is defined by only elements that are also in G, we see that for every $g \in G$ that $g \in N(H)$, thus $N(H) \subset G$

Next we must show that for every $g \in N(H)$ that $g^{-1} \in N(H)$. This can be seen from the definition of $N(H)$, that it is only constructed from g such that $gHg^{-1} = H$, therefore by the definition, for all $g \in N(H)$ $\exists$ $g^{-1} \in N(H)$

Now we must show that for all $x, y \in N(H)$ that $xy \in N(H)$. Let's start by assuming that xy is indeed in $N(H)$. If the property $xyH(xy)^{-1} = H$ holds, then $xy \in N(H)$

$$xyH(xy)^{-1} = xyHy^{-1}x^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$$

Finally, recall Lemma 3.3.12, if $H < N(H)$ then $H \triangleleft N(H) \iff \forall g \in N(H)$, $gHg^{-1} \subset H$. By the definition of $N(H)$, every element $g \in N(H)$ is such that $gHg^{-1} = H$. Because containment allows equality, we can see that $gHg^{-1} \subset H$, therefore by the lemma, $H \triangleleft N(H)$ □

Exercise 3.3.10: Prove that if $gcd(n, m) = 1$, then $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ (recall that in $\mathbb{Z}_n^\times$, the operation is multiplication of congruence classes). *Hint: Theorem 1.5.8 and the discussion there.*

Proof. In order to demonstrate that $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$, we must show that there exists a $\phi : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ such that ϕ is a bijection and $\phi(xy) = \phi(x)\phi(y)$ where $x, y \in \mathbb{Z}_{nm}$

Recall the Chinese Remainder Theorem which states that if $a = cb$ and cb are relatively prime then the function $F : \mathbb{Z}_a = \mathbb{Z}_b \times \mathbb{Z}_c$ is a bijection.

By the problem statement m and n are relatively prime. Let $\phi = F$, $m = c$, $n = b$, hence $mn = a$, hence we can apply the Chinese Remainder Theorem,

therefore ϕ is bijective.

Next, we must demonstrate that ϕ is a homomorphism. Recall, the group operator for $\mathbb{Z}_k$ where $k \in \mathbb{Z}$ is addition.

By the direct product rule on groups (Proposition 3.1.7 and example 3.1.6), we can see that

$$\phi(x)\phi(y) = (([x]_n, [x]_m), ([y]_n, [y]_m)) = (([x]_n + [y]_n), ([x]_m + [y]_m)) = ([x+y]_n, [x+y]_m) = \phi(x+y).$$

Hence ϕ is indeed a homomorphism.

We have shown that ϕ is a homomorphism and ϕ is also a bijection, hence ϕ is isomorphic and therfore $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ □

Exercise 3.3.13: An **ideal** (or sometimes called a **two-sided ideal**) is a subring $\mathcal{J} \subset R$ with the property that for all $r \in R$ and $a \in \mathcal{J}$, we have $ar, ra \in \mathcal{J}$. Prove that the kernel of a ring homomorphism $\phi : R \to S$ is an ideal.

Proof. Recall, a kernel of ϕ is defined as:

$$ker(\phi) = \{g \in G | \phi(g) = e\}$$

Hence, the kernel of ϕ is:

$$ker(\phi) = \{r \in R | \phi(r) = 0\}$$

Let $r \in R$ and $a \in ker(\phi)$. We can see that $\phi(a) = 0$

$$\phi(r \times a) = \phi(r) \times \phi(a) = \phi(r) \times 0 = 0$$
$$\phi(a \times r) = \phi(a) \times \phi(r) = 0 \times \phi(r) = 0$$

Because $\mathcal{J}$ is a ring, $0 \in \mathcal{J}$, hence $ar, ra \in \mathcal{J}$, therefore $\phi : R \to S$ is an ideal. □

Exercise 3.3.16: Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be given by $\phi(k) = 2k$. Prove that although ϕ is a homomorphism of additive groups, it is *not* a ring homomorphism.

Proof. First, we will demonstrate that ϕ is indeed a group homomorphism.

Let $x, y \in \mathbb{Z}$ and let $k = a + b$

$$\phi(k) = \phi(a + b) = \phi(a) + \phi(b) = 2 \times a + 2 \times b = 2(a + b) = 2k$$

We can see that ϕ is indeed a group homomorphism.

Recall, a ring homomorphism requires that both addition and multiplication are preserved.

We will demonstrate a counter example in which addition is preserved, but multiplication is not. Given that integers form a group under addition, and as we

have shown above, $\phi : \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism, we know that addition will be preserved.

Let $k = 10$.

$$\phi(10) = 2 \times 10 = 20$$

$$\phi(10) = \phi(2 + 8) = \phi(2) + \phi(8) = 2 \times 2 + 2 \times 8 = 4 + 16 = 20$$

So far so good. While this doesn't prove anything in itself, we have now seen an example of ϕ preserving addition.

Now let's try multiplication.

$$\phi(10) = 2 \times 10 = 20$$

Let's see what happens when we substitute 10 for 2×5 and assume that ϕ will form a homomorphism under multiplication.

$$10 = 2 \times 5$$

$$\phi(2 \times 5) = \phi(2) \times \phi(5) = 2 \times 2 \times 2 \times 5 = 40$$

$$20 \neq 40$$

Because the homomorphism is not preserved under multiplication, this therefore demonstrates a counterexample that ϕ is not a ring homomorphism.
A more general way to demonstrate this is as follows, assume that ϕ forms a homomorphism under multiplication.

Let $x, y \in \mathbb{Z}$ and $k = x \times y$.

$$\phi(k) = \phi(x \times y) = \phi(x) \times \phi(y) = 2x \times 2y = 4(x \times y) = 2 \times 2(x \times y) = 2 \times 2k \neq 2k$$

We can see that while $\phi : \mathbb{Z} \to \mathbb{Z}$ forms a group homomorphism under addition, it does not preserve multiplication, and is therefore not a ring homomorphism. □