Solution for Homework 7

Xiangcan Li

March 22, 2021

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 of Proposition 3.3.4.

For the base case $n = 1$, we have $\phi(g^1) = \phi(g^0 * g) = \phi(e * g) = \phi(g) = \phi(g)^1$.
Next, we assume that $\phi(g^k) = \phi(g)^k$ for $k = n - 1 > 0$, and prove that this also holds for $k = n$.
We have

$$\begin{aligned}
\phi(g^n) &= \phi(g^{n-1}g) \\
&= \phi(g^{n-1})\phi(g) && \phi \text{ is a homomorphism} \\
&= \phi(g)^{n-1}\phi(g) && \text{by inductive hypothesis} \\
&= \phi(g)^n
\end{aligned}$$

We conclude for all $n > 0$ we have $\phi(g^n) = \phi(g)^n$, thus completing the proof of Proposition 3.3.4.

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

Let N be an arbitrary subgroup of G. Since G is an abelian group, the operation is commutative. Then the operation restricted to N is also commutative.

Hence, for all $g \in G$, we have $gNg^{-1} = gg^{-1}N = eN$. Since $e \in G$ and $N \subset G$, $eN = N$. Then for all $g \in G$, we have $gNg^{-1} = N$.

We conclude G is a normal group.

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 $c_g : H \to H$.

Note that $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

Let m, n be arbitrary two elements in H. Then for some $g \in G$, $gmg^{-1}, gng^{-1} \in gHg^{-1}$. Note that $m, n \in G$ since $H \subset G$.

Then we have

$$\begin{aligned}
gmg^{-1}gng^{-1} &= gm(g^{-1}g)ng^{-1} && \text{by associativity} \\
&= gmeng^{-1} && \text{by the property of the inverse} \\
&= gm(eng^{-1}) && \text{by associativity} \\
&= gm(ng^{-1}) && \text{by the property of the identity} \\
&= g(mn)g^{-1} && \text{by associativity}
\end{aligned}$$

Since $m, n \in H$ and H is a subgroup, $mn \in H$. Hence, $gmng^{-1} \in gHg^{-1}$.

Since H is a subgroup, there exists an inverse $m^{-1} \in H$, with the property that $mm^{-1} = m^{-1}m = e$. Therefore, $gm^{-1}g^{-1} \in gHg^{-1}$.

Then we have

$$\begin{aligned}
(gmg^{-1})(gm^{-1}g^{-1}) &= gm(g^{-1}g)m^{-1}g^{-1} && \text{by associativity} \\
&= gmem^{-1}g^{-1} && \text{by the property of the inverse} \\
&= gm(em^{-1}g^{-1}) && \text{by associativity} \\
&= gm(m^{-1}g^{-1}) && \text{by the property of the identity} \\
&= g(mm^{-1})g^{-1} && \text{by associativity} \\
&= geg^{-1} && \text{by the property of the inverse} \\
&= gg^{-1} && \text{by the property of the identity} \\
&= e && \text{by the property of the identity}
\end{aligned}$$

Similarly,

$$\begin{aligned}
(gm^{-1}g^{-1})(gmg^{-1}) &= gm^{-1}(g^{-1}g)mg^{-1} && \text{by associativity} \\
&= gm^{-1}emg^{-1} && \text{by the property of the inverse} \\
&= gm^{-1}(emg^{-1}) && \text{by associativity} \\
&= gm^{-1}(mg^{-1}) && \text{by the property of the identity} \\
&= g(m^{-1}m)g^{-1} && \text{by associativity} \\
&= geg^{-1} && \text{by the property of the inverse} \\
&= gg^{-1} && \text{by the property of the identity} \\
&= e && \text{by the property of the identity}
\end{aligned}$$

Hence, for $gmg^{-1} \in gHg^{-1}$, there exists an inverse $gm^{-1}g^{-1} \in gHg^{-1}$.

Since m, n are arbitrary, gmg^{-1} and gng^{-1} are also arbitrary elements in gHg^{-1}. We conclude gHg^{-1} is a subgroup.

Let $gmg^{-1} = gng^{-1}$. Then we have

$$\begin{aligned}
gmg^{-1} = gng^{-1} &\implies g^{-1}(gmg^{-1})g = g^{-1}(gng^{-1})g \\
&\implies (g^{-1}g)m(g^{-1}g) = (g^{-1}g)n(g^{-1}g) && \text{by associativity} \\
&\implies eme = ene && \text{by the property of the inverse} \\
&\implies m = n && \text{by the property of the identity}
\end{aligned}$$

Hence, c_g is injective.

By the definition of c_g, for all $ghg^{-1} \in gHg^{-1}$, there exists $h \in H$ such that $ghg^{-1} \in gHg^{-1}$. Hence, c_g is surjective.

We conclude c_g is a bijective homomorphism, i.e. isomorphism.

Hence, 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 $c_g : H \to gHg^{-1}$.

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

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

is a subgroup containing H, and that $H \triangleleft N(H)$.

Let g, h be arbitrary elements in $N(H)$, then $g, h \in G$ and $gHg^{-1} = H, hHh^{-1} = H$. Hence, $gh \in G$ since G is a group. Then gh has an inverse $(gh)^{-1}$.

Let m be an arbitrary element in H. We have

$$\begin{aligned}(gh)m(gh)^{-1} &= (gh)m(h^{-1}g^{-1}) && \text{by } \textbf{Corollary 3.1.2}\\ &= g(hmh^{-1})g^{-1} && \text{by associativity}\\ &= gmg^{-1} && \text{by the definition of } N(H)\\ &= m && \text{by the definition of } N(H)\end{aligned}$$

Since m is arbitrary, $(gh)n(gh)^{-1} = n$ for all $n \in H$. Then $(gh)H(gh)^{-1} = H$. We conclude $gh \in N(H)$.
Since $g \in G$ and G is a group, there exists an inverse $g^{-1} \in G$ such that $g^{-1}g = gg^{-1} = e$.
Then we have

$$\begin{aligned}g^{-1}m(g^{-1})^{-1} &= g^{-1}mg && \text{by } \textbf{Corollary 3.1.2}\\ &= g^{-1}(gmg^{-1})g && \text{by the definition of } N(H)\\ &= (g^{-1}g)m(g^{-1}g) && \text{by associativity}\\ &= eme && \text{by the property of the inverse}\\ &= m && \text{by the property of the identity}\end{aligned}$$

Since m is arbitrary, $g^{-1}n(g^{-1})^{-1} = n$ for all $n \in H$. Then $g^{-1}H(g^{-1})^{-1} = H$. We conclude $g^{-1} \in N(H)$.
Since g, h are arbitrary, we conclude for all $g, h \in N(H)$, $gh \in N(H)$ and $g^{-1} \in N(H)$. Hence, $N(H)$ is a subgroup.
For an arbitrary $h \in H$, we have $h \in G$ and $hhh^{-1} = h(hh^{-1}) = he = h$. Then $hHh^{-1} = H$. Hence, $h \in N(H)$. We conclude $N(H)$ contains H.
Hence, $N(H) = \{g \in G \mid gHg^{-1} = H\} \subset G$ is a subgroup containing H.

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

Since $\gcd(n, m) = 1$, n, m are relatively prime. By **Theorem 1.5.8**, there exists a function $F : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ given by $F([a]_{nm}) = (\pi_{n.nm}([a]_{nm}), \pi_{m,nm}([a]_{nm}))$.
Then we have

$$\begin{aligned}F([a]_{nm} + [b]_{nm}) &= (\pi_{n.nm}([a]_{nm} + [b]_{nm}), \pi_{m,nm}([a]_{nm} + [b]_{nm}))\\ &= (\pi_{n.nm}([a]_{nm}) + \pi_{m,nm}([b]_{nm}), \pi_{m,nm}([a]_{nm}) + \pi_{m,nm}([b]_{nm}))\\ &= (\pi_{n.nm}([a]_{nm}), \pi_{m,nm}([a]_{nm})) + (\pi_{n.nm}([b]_{nm}), \pi_{m,nm}(b]_{nm}))\\ &= F([a]_{nm}) + F([b]_{nm})\end{aligned}$$

We conclude $F : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ is a bijective homomorphism. Hence, $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.
By **Proposition 1.5.9**, $F(\mathbb{Z}_{nm}^\times) = \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$.
We have

$$\begin{aligned}F([a]_{nm}[b]_{nm}) &= F([ab]_{nm})\\ &= ([ab]_n, [ab]_m)\\ &= ([a]_n[b]_n, [a]_m[b]_m)\\ &= ([a]_n, [a]_m)([b]_n[b]_m)\\ &= F([a]_n)F([b]_m)\end{aligned}$$

We conclude $F : \mathbb{Z}_{nm}^\times \to \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ is a bijective homomorphism. Hence, $\mathbb{Z}_{nm}^\times \cong \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$.

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.

Since R is a ring, the additive identity is 0. Then we have $\ker(\phi) = \{r \in R \mid \phi(r) = e\} == \{r \in R \mid \phi(r) = 0\}$.

Then for all $r, s \in \ker(\phi)$, $r + s \in R$ and $\phi(s + r) = \phi(s) + \phi(r) = 0 + 0 = 0$. Hence, $r + s \in \ker(\phi)$. Also, $\phi(sr) = \phi(s)\phi(r) = 0 * 0 = 0$. Note that $r \in \ker(\phi)$ implies $r \in R$, we conclude $\ker(\phi) \subset R$ is a substring.

For all $r \in R$ and $a \in \ker(\phi) \subset R$, we have $ar, ra \in R$ and $\phi(a) = 0$. Then $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$ and $\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$. Hence, $ar, ra \in \ker(\phi)$. We conclude $\ker(\phi)$ 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.

Note that $\mathbb{Z}$ is a group. For all $w, v \in \mathbb{Z}$, $\phi(w + v) = \phi(w) + \phi(v) = 2w + 2v = 2(w + v) = \phi(w + v)$. Hence, ϕ is a homomorphism of additive groups.

However, $\phi(wv) = 2wv \neq 4wv = (2w)(2v) = \phi(w)\phi(v)$. Hence, ϕ is not a ring homomorphism

We conclude although ϕ is a homomorphism of additive groups, it is not a ring homomorphism.