

Solution for Homework 11

Xiangcan Li

January 17, 2021

Exercise 3.7.7 In this exercise you will identify $\text{Aut}(\mathbb{Z}_n)$.

1. Prove that for any $[a] \in \mathbb{Z}_n^\times$ multiplication by $[a]$ defines an automorphism $\alpha_{[a]} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, given by $\alpha_{[a]}([k]) = [ak]$.

Note that \mathbb{Z}_n is an additive group. For arbitrary $[k_1], [k_2] \in \mathbb{Z}_n$, we have

$$\alpha_{[a]}([k_1] + [k_2]) = [a][k_1 + k_2] = [a(k_1 + k_2)] = [ak_1 + ak_2] = [ak_1] + [ak_2] = \alpha_{[a]}([k_1]) + \alpha_{[a]}([k_2]).$$

For some $[k] \in \mathbb{Z}_n$, let $\alpha_{[a]}([k]) = [0]$, the identity in \mathbb{Z}_n . Then $[ak] = [0]$. Then for some $m = ak + nj \in [ak]$, $j \in \mathbb{Z}$, $m \in [0]$. Then $m = 0 + nl = nl$, $l \in \mathbb{Z}$. Hence, $ak + nj = nl$. Then $ak = n(l - j)$, $l - j \in \mathbb{Z}$. Hence, $n \mid ak$.

Note that $[a] \in \mathbb{Z}_n^\times$, then $\gcd(a, n) = 1$, which means $n \nmid a$. Then we have $n \mid k$. Hence, $[k] = [0]$, the identity in \mathbb{Z}_n .

Hence, $\ker(\alpha_{[a]}) = [0]$. By Proposition 3.3.9, $\alpha_{[a]}$ is injective.

We conclude $\alpha_{[a]} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is an automorphism.

2. Prove that $\alpha : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$ defines an injective homomorphism.

Consider $\alpha : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$ be $\alpha([a]) = \alpha_{[a]}$ for $[a] \in \mathbb{Z}_n^\times$.

For some $[a], [b] \in \mathbb{Z}_n^\times$, then $\alpha([ab]) = \alpha_{[ab]}$.

Note that $\alpha_{[ab]}([k]) = [ab][k] = [a][b][k] = [a]\alpha_{[b]}([k]) = \alpha_{[a]}(\alpha_{[b]}([k])) = (\alpha_{[a]} \circ \alpha_{[b]})([k])$ for some $[k] \in \mathbb{Z}_n$.

Hence, we have $\alpha([ab]) = \alpha_{[a]} \circ \alpha_{[b]} = \alpha([a])\alpha([b])$.

Let $\alpha([a]) = \text{id}_{\mathbb{Z}_n}$, then $\alpha_{[a]} = \text{id}_{\mathbb{Z}_n}$. Hence, $\alpha_{[a]}([k]) = [k]$ for all $[k] \in \mathbb{Z}_n$. Then $[ak] = [k]$. Hence, $[a] = [1]$, the identity in \mathbb{Z}_n^\times .

Hence, $\ker(\alpha) = [1]$. By Proposition 3.3.9, α is injective.

We conclude α is an injective homomorphism.

3. Prove that any automorphism $\phi \in \text{Aut}(\mathbb{Z}_n)$ is determined by $\phi([1])$, and that $\phi([1])$ must be a generator of \mathbb{Z}_n .

Since $\phi \in \text{Aut}(\mathbb{Z}_n)$, we have $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$. Let $\text{Im}(\phi)$ denote the image of ϕ .

For some $[k] \in \mathbb{Z}_n$, we have

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

Hence, for all $a \in \text{Im}(\phi)$, $a = m\phi([1])$ for some $m \in \mathbb{Z}$. Then $a \in \langle \phi([1]) \rangle$. For all $a \in \langle \phi([1]) \rangle$, $a = x\phi([1])$ for some $x \in \mathbb{Z}$. Then $x \in \text{Im}(\phi)$. Hence, $\text{Im}(\phi) = \langle \phi([1]) \rangle$.

We have $\text{Im}(\phi) = \mathbb{Z}_n$. Hence, $\langle \phi([1]) \rangle = \mathbb{Z}_n$. We conclude $\phi([1])$ is must be a generator of \mathbb{Z}_n .

4. Prove that $\alpha : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$ is an isomorphism.

Note that $\langle \phi([1]) \rangle = \mathbb{Z}_n$. Then we have $|\langle \phi([1]) \rangle| = |\mathbb{Z}_n|$. By definition, $|\phi([1])| = |\mathbb{Z}_n| = n$.

We refer reader to the proof of Exercise 3.2.2. We proved that $\gcd(a, n) = 1$ if and only if $|[a]| = n$. Hence, $\gcd(\phi([1]), n) = 1$. Then $\phi([1]) \in \mathbb{Z}_n^\times$.

Then for some $[k] \in \mathbb{Z}_n$ we have

$$\alpha(\phi([1])) = \alpha_{\phi([1])}$$

and

$$\alpha_{\phi([1])}([k]) = [k]\phi([1]) = \phi([1]) + \cdots + \phi([1]) = \phi([1] + \cdots + [1]) = \phi([k][1]) = \phi([k])$$

for any $\phi \in \text{Aut}(\mathbb{Z}_n)$.

Hence, for any $\phi \in \text{Aut}(\mathbb{Z}_n)$, there exists $\phi([1]) \in \mathbb{Z}_n^\times$ such that $\alpha(\phi([1])) = \phi$. We conclude α is surjective. Then $\alpha : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$ is an isomorphism.

Exercise 3.7.8 For every $n \geq 3$, construct a nonabelian group of order $n\phi(n)$, where $\phi(n)$ is the Euler phi function of n .

Consider $\alpha : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$ as $[a] \mapsto \alpha_{[a]}$, where $\alpha_{[a]}([x]) : [x] \mapsto [ax]$ for some $[a] \in \mathbb{Z}_n^\times$. Then by Exercise 3.7.7, α is an isomorphism. By Proposition 3.7.6, $\mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_n^\times$ is a group and $|\mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_n^\times| = n\phi(n)$.

Note that $[0], [1] \in \mathbb{Z}_n$ and $\phi(n) \geq 1$ for $n \geq 3$. Then there exists a $[b] \neq [1]$ and $[b] \in \mathbb{Z}_n^\times$.

By definition of semidirect product, we have

$$\begin{aligned} ([h], [k])([h'], [k']) &= ([h] + \alpha_{[a]}([h']), [k][k']) = ([h] + [a][h'], [k][k']) = ([h + ah'], [kk']) \\ ([h'], [k'])([h], [k]) &= ([h'] + \alpha_{[a]}([h]), [k'][k]) = ([h'] + [a][h], [k'][k]) = ([h' + ah], [k'k]) \end{aligned}$$

Let $[h] = [0], [k] = [1], [h'] = [1], [k] \neq [1]$, then

$$([h], [k])([h'], [k']) = ([a], [k'])$$

and

$$([h'], [k'])([h], [k]) = ([1], [k']).$$

Note that $[a]$ can be any element in \mathbb{Z}_n . When $[a] \neq [1]$, for example, $[a] = [0]$, $([h], [k])([h'], [k']) \neq ([h'], [k'])([h], [k])$. Hence, $\mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_n^\times$ is a nonabelian group.

We conclude $\mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_n^\times$ is a nonabelian group of order $n\phi(n)$, where $\phi(n)$ is the Euler phi function of n .

Exercise 4.1.1 Prove Proposition 4.1.5:

Suppose $G \times X \rightarrow X$ is an action. Then for all $x \in X$, $\text{stab}_G(x)$ is a subgroup of G and the kernel K of the action is the intersection of all stabilizers

$$K = \bigcap_{x \in X} \text{stab}_G(x)$$

The orbits $\mathcal{O}_G(X)$ form a partition of X , and the action of G on X is transitive if and only if $G \cdot x = X$ for some $x \in X$.

Note that $\text{stab}_G(x) = \{g \in G \mid g \cdot x = x\}$. Clearly, $\text{stab}_G(x) \subset G$.

By the property of the action, for all $g, h \in \text{stab}_G(x)$,

$$(g \cdot h) \cdot x = g \cdot (h \cdot x) = g \cdot x = x.$$

Hence, $g \cdot h \in \text{stab}_G(x)$.

For all $g \in G$, $g^{-1} \in G$. By the property of the action, $e \cdot g = (g^{-1} \cdot g)x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x = x$.

Hence, $\text{stab}_G(x)$ is a subgroup of G .

For all $g \in K$, we have $g \cdot x = x$ for all $x \in X$. Then $g \in \text{stab}_G(x)$ for all $x \in X$. Hence, $K \subset \text{stab}_G(x)$.

For all $g \in \bigcap_{x \in X} \text{stab}_G(x)$, $g \cdot x = x$ for all x .

Hence, $K = \bigcap_{x \in X} \text{stab}_G(x)$.

For any $x \in X$, $x = e \cdot x \in G \cdot x$. If $x \in G \cdot x_1 \cap G \cdot x_2$, then there exists some $g_1, g_2 \in G$ such that $g_1 \cdot x_1 = x_1$ and $g_2 \cdot x_2 = x_2$ and $x = g_1 \cdot x_1 = g_2 \cdot x_2$.

Note that $G = Gg_1 = Gg_2$.

Hence, $Gx_1 = (Gg_1)x_1 = G(g_1x_1) = G(g_2x_2) = (Gg_2)x_2 = Gx_2$.

It follows that $\mathcal{O}_G(x)$ is a partition.

- \implies : Since the action is transitive, we have for all $x, y \in X$, there exists $g \in G$ so that $g \cdot x = y$. By the property of the action, $e \cdot x = (g^{-1} \cdot g) \cdot x = g^{-1} \cdot (g \cdot x) = x$. Hence, $g^{-1} \cdot y = x$. Note that $g^{-1} \in G$. Hence, $x, y \in X$, then $x \in G \cdot y$ and $y \in G \cdot x$. Then $X \subset G \cdot x$. By the definition of the orbit, $G \cdot x \subset X$. Hence, $G \cdot x = X$.
- \impliedby : Since $G \cdot x = X$ for some $x \in X$. Then for all $y, z \in X$, we have $y = g_1 \cdot x$ and $z = g_2 \cdot x$, where $g_1, g_2 \in G$. By the property of the action, $e \cdot x = (g_1^{-1} \cdot g_1) \cdot x = g_1^{-1} \cdot (g_1 \cdot x) = x$. Hence, $g_1^{-1} \cdot y = x$. Then $g_2 \cdot (g_1^{-1} \cdot y) = z$, i.e., $(g_2 \cdot g_1^{-1}) \cdot y = z$. Note that $g_2 \cdot g_1^{-1} \in G$. Hence, for all $y, z \in X$, there exists $g \in G$ so that $g \cdot y = z$. Then the action is transitive.

We conclude the action of G on X is transitive if and only if $G \cdot x = X$ for some $x \in X$.

Exercise 4.2.3 Edges e, e' of a tetrahedron T are said to be opposite if they are disjoint (that is, they do not share a vertex). The 6 edges can be partitioned into a set X of three pairs of opposite edges. Prove that G_3 , the group of symmetries of T , acts on X and the kernel $K < G_3$ is a normal subgroup of order 4.

Note that G_3 is a group and $X \neq \emptyset$, consider $G \times X \rightarrow X$ as $(g, x) \mapsto g \cdot x$.

- X is a set of three pairs of opposite edges. Note that the identity in G_3 fixes vertices and thus fixed the edges in X . Then we have $e \cdot x = x$.
- Consider G_3 as 24 symmetries of a regular tetrahedron, comprised of 12 rotational and 12 reflectional symmetries. Then any action preserves adjacent vertices and thus preserves opposite edges.

Let A, B, C denote three vertices on S , respectively, and D denotes the remaining vertex in the tetrahedron that is not on S . Without loss of generality, edge AB and CD are a pair of opposite edges (By the definition of the opposite edges, an edge connecting two vertices on S and an edge connecting the remaining vertex on S and D are a pair of opposite edges). Let g, h be arbitrary two elements in G_3 and S be an arbitrary face of tetrahedron. Then we have $g \cdot (h \cdot A) = (g \cdot h) \cdot A$. Hence, AB and CD must be preserved. Then the opposite edges are also be preserved. Hence, $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ for some $x \in X$.

We conclude G_3 acts on X .

If we flip two vertices on one edge, then a pair of opposite edges does not change. For all 3-cycles in G_3 , we observe that they do not preserve pairs of opposite edges. Let 1, 2, 3, 4 denote four vertices on T . Note that $e = (1\ 2)(2\ 1)$, which flips an edge twice. Then $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(3\ 2)\}$. Then the order of K is 4.

We have $A_n \cong \ker(\epsilon) \triangleleft S_n$, where ϵ is the sign homomorphism. Hence, we have $A_4 \triangleleft S_4$. We can enumerate all products of elements in K to observe that K is a subgroup of A_4 .

Since $K \subset A_4$, for all $k \in K$, $k \in A_4$, then $gkg^{-1} = k$ for all $g \in S_4$, which means for all $gkg^{-1} \in gKg^{-1}$, $gkg^{-1} \in K$. Then $gKg^{-1} \subset K$ for all $g \in S_4$. Hence, $K \triangleleft S_4$. By proposition 4.2.1, $G_3 \cong S_4$. Hence, $K \triangleleft G_3$.

We conclude the kernel $K < G_3$ is a normal subgroup of order 4.

Exercise 4.2.8 Draw the Cayley graph of D_4 with respect to the generating set j, r .

