**Exercise**. Let $(G, *)$ is an abelian group with identity $e$. Given an element $g$ in $G$ and a positive integer $n$, we write $ng$ to mean $g * \cdots * g$, where $g$ is repeated $n$ times, for brevity. Show that the set $R = \mathbb{Z} \times G$ of ordered pairs $(n, g)$ of elements $n$ in $\mathbb{Z}$ and $g$ in $G$ is a commutative ring with identity $(1, e)$ under the addition

$$(n, g) \boxplus (n', g') = (n + n', g * g')$$

and multiplication

$$(n, g) \boxtimes (n', g') = (nn', ng * n'g).$$

The units of $(R, \boxplus, \boxtimes)$ are $\{\pm 1\} \times G$.

**Solution**.

• (R+0) Since $n + n' \in \mathbb{Z}$ and $g * g' \in G$, we have $(n, g) \boxplus (n', g') = (n + n', g * g) \in \mathbb{Z} \times G$.

• (R+1) On one hand,

$$(n, g) \boxplus ((n', g') \boxplus (n'', g'')) = (n, g) \boxplus (n' + n'', g' * g'') = (n + (n' + n''), g * (g' * g'')).$$

On the other hand,

$$((n, g) \boxplus (n', g')) \boxplus (n'', g'') = (n + n', g * g') \boxplus (n'', g'') = ((n + n') + n'', (g * g') * g'').$$

By (R+1) for $(\mathbb{Z}, +, \times)$, $n + (n' + n'') = (n + n') + n''$ while it follows from (G1) for $(G, *)$ that $g * (g' * g'') = (g * g') * g''$. Therefore

$$(n, g) \boxplus ((n', g') \boxplus (n'', g'')) = ((n, g) \boxplus (n', g')) \boxplus (n'', g'')$$

holds.

• (R+2) The element $(0, e)$ is the (additive) identity element with respect to $\boxplus$. Indeed,

$$(n, g) \boxplus (0, e) = (n + 0, g * e) = (n, g)$$

since $n + 0 = n$ by (R+2) for $(\mathbb{Z}, +, \times)$ and $g * e = g$ by (G2) for $(G, *)$.

Similarly,

$$(0, e) \boxplus (n, g) = (0 + n, e * g) = (n, g).$$

• (R+3) The inverse of $(n, g)$ is $(-n, -g)$ where $-g$ denotes the inverse of $g$, i.e., (unique) element of $G$ satisfying $g * (-g) = (-g) * g = e$ as prescribed by (G3). Indeed,

$$(n, g) \boxplus (-n, -g) = (n + (-n), g * (-g)) = (0, e)$$

since $-n$ is the (additive) inverse of $n$ by (R+2) for $(\mathbb{Z}, +, \times)$ and $g * (-g) = e$ by (G3).

Similarly,

$$(-n, -g) \boxplus (n, g) = ((-n) + n, (-g) * g) = (0, e).$$

• (R+4)

$$(n, g) \boxplus (n', g') = (n + n', g * g') = (n' + n, g' * g) = (n', g') \boxplus (n, g)$$

since $n + n' = n' + n$ by (R+4) for $(\mathbb{Z}, +, \times)$ and $g * g' = g' * g$ by (G4) for $(G, *)$.

• (R×0) Since $nn' \in \mathbb{Z}$ by (R×0) and $ng' * n'g \in G$ by (G0), we have $(n,g) \boxtimes (n',g') \in \mathbb{Z} \times G = R$.

• (R×1) On one hand,

$$(n,g) \boxtimes ((n',g') \boxtimes (n'',g'')) = (n,g) \boxtimes (n'n'', n'g'' * n''g') = (n(n'n''), n(n'g'' * n''g') * n'n''g)$$

Since $(G, *)$ is abelian, this equals

$$(nn'n'', (nn'g'' * nn''g') * (n'n''g))$$

On the other hand,

$$((n,g) \boxtimes (n',g')) \boxtimes (n'',g'') = (nn', ng' * n'g) \boxtimes (n'',g'') = ((nn')n'', nn'g'' * n''(ng' * n'g))$$

Since $(G, *)$ is abelian, this equals

$$(nn'n'', nn'g'' * (nn''g' * n'n''g))$$

By (G1) for $(G, *)$,

$$(n,g) \boxtimes ((n',g') \boxtimes (n'',g''')) = ((n,g) \boxtimes (n',g')) \boxtimes (n'',g'')$$

holds.

• (R+×) On one hand,

$$(n,g) \boxtimes ((n',g') \boxplus (n'',g'')) = (n,g) \boxtimes (n' + n'', g' * g'') = (n(n' + n''), n(g' * g'') * (n' + n'')g).$$

Since $(G, *)$ is abelian, this equals

$$(n(n' + n''), (ng' * ng'') * (n' + n'')g).$$

On the other hand,

$$((n,g) \boxtimes (n',g')) \boxplus ((n,g) \boxtimes (n'',g'')) = (nn', ng' * n'g) \boxplus (nn'', ng'' * n''g) = (nn' + nn'', (ng' * n'g) * (ng'' * n''g)).$$

Since $(G, *)$ is abelian, this equals

$$(nn' + nn'', (n' + n'')g * ng' * ng'').$$

By (R×+) for $(\mathbb{Z}, +, \times)$,

$$(n,g) \boxtimes ((n',g') \boxplus (n'',g'')) = ((n,g) \boxtimes (n',g')) \boxplus ((n,g) \boxtimes (n'',g''))$$

holds.

• (R+×) On one hand,

$$((n',g') \boxplus (n'',g'')) \boxtimes (n,g) = (n' + n'', g' * g'') \boxtimes (n,g) = ((n' + n'')n, (n' + n'')g * n(g' * g'')).$$

Since $(G, *)$ is abelian, this equals

$$((n' + n'')n, (n' + n'')g * ng' * ng'').$$

On the other hand,

$$((n', g') \boxtimes (n, g)) \boxplus ((n'', g'') \boxtimes (n, g)) = (n'n, n'g * ng') \boxplus (n''n, n''g * ng'') = (n'n + n''n, (n'g * ng') * (n''g * ng'')).$$

Since $(G, *)$ is abelian, this equals

$$(n'n + n''n, (n' + n'')g * ng' * ng'').$$

By (R$\times$+) for $(\mathbb{Z}, +, \times)$,

$$((n', g') \boxplus (n'', g'')) \boxtimes (n, g) = ((n', g') \boxtimes (n, g)) \boxplus ((n'', g'') \boxtimes (n, g))$$

holds.

- $(R, \boxplus, \boxtimes)$ is commutative. On one hand,

$$(n, g) \boxtimes (n', g') = (nn', ng' * n'g).$$

On the other hand,

$$(n', g') \boxtimes (n, g) = (n'n, n'g * ng').$$

Since $(R, +, \times)$ is abelian $nn' = n'n$. Since $(G, *)$ is abelian, $ng' * n'g = n'g * ng'$. It therefore follows that

$$(n, g) \boxtimes (n', g') = (n', g') \boxtimes (n, g).$$

- The multiplicative identity is $(1, e)$. Indeed,

$$(n, g) \boxtimes (1, e) = (n \times 1, ne * g) = (n, e * g) = (n, g)$$

since $ne = e * \cdots * e (n \text{ times}) = e$ by (G2).

Similarly,

$$(1, e) \boxtimes (n, g) = (1 \times n, g * ne) = (n, g * e) = (n, g).$$

- The units of $(R, \boxplus, \boxtimes)$ are $\{\pm 1\} \times G$, since the units of $\mathbb{Z}$ are $\{\pm 1\}$.