$f(n+m) = n+m+p\mathbb{Z}$. $f(n)+f(m) = n+p\mathbb{Z}+m+p\mathbb{Z} = n+m+p\mathbb{Z}$.
$\therefore f(n+m) = f(n)+f(m)$. *Also* $f(n-m) = f(n) - f(m)$.

$f(nm) = nm + p\mathbb{Z}$.

$$\begin{aligned} f(n)f(m) &= (n+p\mathbb{Z})(m+p\mathbb{Z}) \\ &= nm + np\mathbb{Z} + mp\mathbb{Z} + p^2\mathbb{Z}\mathbb{Z} \\ &= nm + p(n\mathbb{Z} + mp\mathbb{Z} + p\mathbb{Z}) \\ &= nm + p\mathbb{Z} \end{aligned}$$

Thus $f(nm) = f(n)f(m)$ *and* f *is a ring homomorphism.*

$Ker(f) = \{n \in \mathbb{Z} \mid f(n) = 0\} = \{n \in \mathbb{Z} \mid n+p\mathbb{Z} = 0_{\mathbb{Z}_p} = 0+p\mathbb{Z}\} = \{np \mid n \in \mathbb{Z}\}$

Since $f(np) = np + p\mathbb{Z} = p(n+\mathbb{Z}) = p\mathbb{Z} = 0 + p\mathbb{Z} = 0$. *So* $f : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ *has kernal* $p\mathbb{Z}$.

Let $I \lhd R$. Then consider the set $R/I = \{I + r : r \in R\}$. Define

- addition by $(r+I)+(s+I) = (r+s)+I$.
- multiplication by $(r+I)(s+I) = (rs)+I$.

R/I is a ring (check i.e. $0_{R/I} = 0 + I$, $(r+I)+(-r+I) = 0+I = 0_{R/I}$, and so on).

Consider the ring homomorphism $f : R \longrightarrow R/I$ defined by $f(r) = r + I$. What is $Ker(f)$? $Ker(f) = \{r \in R : f(r) = 0\} = \{r \in R : f(r) = 0+I\} = I$ (Since if $i \in I$, we have $f(i) = i + I = I$).

Therefore given any ideal I of a ring R, we can come up with a ring homomorphism $f : R \longrightarrow R/I$ such that $I = Ker(f)$. Note that we often write $f(r) = r + I = \overline{r}$ (r mod I).

Example 1.48 $p\mathbb{Z} \lhd \mathbb{Z}$, $p\mathbb{Z}$ *is the kernal of the homomorphism* $f : \mathbb{Z} \longrightarrow \mathbb{Z}_p \cong \mathbb{Z}/\mathbb{Z}_p$.