Chapter 1 Module

1.3 Exercise

3.4 Prove that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ as $\mathbb{Z}$ modules iff $\gcd(m,n) = 1$.

Proof. "$\Rightarrow$" $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ as $\mathbb{Z}$ module means $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as Abelian group. Let the isomorphism be

$$\Psi: \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n .$$

Notice the order of $1_{\mathbb{Z}_{mn}}$ in $\mathbb{Z}_{mn}$ is mn. $\Psi(1_{\mathbb{Z}_{mn}}) = (1_{\mathbb{Z}_m}, 1_{\mathbb{Z}_n})$.

This isomorphism implies $\text{order}(\Psi(1_{\mathbb{Z}_{mn}})) = \text{order}(1_{\mathbb{Z}_{mn}}) = m \cdot n$.

But we know $\text{order}[(1_{\mathbb{Z}_m}, 1_{\mathbb{Z}_n})] = \text{lcm}(m,n)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. Using the formula $\text{lcm}(m,n) = m \cdot n / \gcd(m,n)$, we see $\gcd(m,n) = 1$.

"$\Leftarrow$". If $\gcd(m,n) = 1$. Define

$$f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$$
$$[a]_{\mathbb{Z}_{mn}} \mapsto ([a]_{\mathbb{Z}_m}, [a]_{\mathbb{Z}_n})$$

We need to show it's an isomorphism.

① f is well-defined. For $a - a' = k \cdot mn$, it's clear $[a]_{\mathbb{Z}_m} = [a']_{\mathbb{Z}_m}$ and $[a]_{\mathbb{Z}_n} = [a']_{\mathbb{Z}_n}$.

② f is $\mathbb{Z}$ module map.

③ f is surjective

④ $\text{Ker} f = 0$.

3.5. Let p be a prime number, prove that $\mathbb{Z}_{p^e}$ ($e \in \mathbb{Z}_{>0}$) can not be written as direct sum of two submodules (as $\mathbb{Z}$ module)

Proof. Suppose $\mathbb{Z}_{p^e} = \mathbb{Z}_m \oplus \mathbb{Z}_n$, then $\gcd(m,n) = 1$ and $m \cdot n = p^e$, which is impossible.