

7. Proving the following two claims solves the question.

Claim 1: The R -module $K := \text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})$ is an injective R -module.

Let N and M be any R -modules with the injective R -homomorphism $i : N \rightarrow M$. Let $\beta : N \rightarrow K$ be an R -homomorphism. To prove the claim, we must show that β extends to M . There is a natural map of \mathbf{Z} -modules $\phi : K \rightarrow \mathbf{Q}/\mathbf{Z}$ such that $\phi(\varphi) = \varphi(1)$ for every $\varphi \in K$. Let $\beta' := \phi \circ \beta$. Since \mathbf{Q}/\mathbf{Z} is an injective \mathbf{Z} -module, there exists an extension γ' of β' to M as \mathbf{Z} -module homomorphism. Now, we define the desired homomorphism $\gamma : M \rightarrow K$ of R -modules by sending m to the map φ defined by $\varphi(1) = \gamma'(rm)$. It is easy to see that this is an R -homomorphism. We have $\phi \circ \beta = \gamma' \circ i$ and $\phi \circ \gamma = \gamma'$, which implies that $\phi \circ \beta = \phi \circ \gamma \circ i$. Now, to say that $\beta = \gamma \circ i$, we should show that for any R -module A and for every \mathbf{Z} -homomorphism $A \rightarrow \mathbf{Q}/\mathbf{Z}$, there exists a unique R -homomorphism $A \rightarrow K$. This is true because, consider the map

$$g : \text{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z}) \rightarrow \text{Hom}_R(A, \text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z}))$$

defined by $g(\varphi) = \delta_\varphi$ where δ_φ is defined on A as $\delta_\varphi(a) = \alpha_{(\varphi, a)}$ where the map $\alpha_{(\varphi, a)}$ is defined on R as $\alpha_{(\varphi, a)}(\lambda) = \varphi(\lambda a)$. The map g is an isomorphism. Hence, claim 1 follows.

Claim 2: The R -module K is isomorphic to R as R -modules.

Let $\{g_0, g_1, \dots, g_n\}$ be the elements of the group G . Every element r of R can be written uniquely in the form $r = a_0g_0 + a_1g_1 + \dots + a_ng_n$ where $a_i \in \mathbf{F}_p$. Consider the map

$$f : R \rightarrow K,$$

where for any $r = a_0g_0 + a_1g_1 + \dots + a_ng_n$ in R the map f is defined by $f(r) = \varphi_r$ where for any arbitrary element $r' = b_0g_0 + b_1g_1 + \dots + b_ng_n$ of R the map φ_r is defined on R by $\varphi_r(r') = \sum_{h=0}^n b_h a_{h-1} / p$. It is easy to see that the map is an \mathbf{F}_p -homomorphism. But we should also check that the actions of G on R and on K are compatible so that the map f is an R -homomorphism. We define the action of G on K for every $g \in G$ and every $\varphi \in K$ as,

$$g \cdot \varphi(x) = \varphi(gx)$$

for every $x \in R$. Thus, to prove the claim, you should prove that for every $g \in G$ and $r \in R$, we have $f(gr) = g \cdot f(r)$. Then, you should also check that f is both surjective and injective.

9. (\implies) Suppose $\text{Spec}(R)$ is disconnected. Then, there exists $A \subset \text{Spec}(R)$ which is clopen. This means that both A and $A^c := \text{Spec}(R) - A$ are closed subsets of $\text{Spec}(R)$. Then, there exist ideals I and J in R such that

$$\begin{aligned} A &= V(I) = \{P \in \text{Spec}(R) : I \subset P\}, \\ A^c &= V(J) = \{P \in \text{Spec}(R) : J \subset P\}. \end{aligned}$$

We have $V(I) \cup V(J) = \text{Spec}(R)$. This implies that $V(IJ) = \text{Spec}(R)$. This means that the ideal IJ is contained in every prime ideal of R and hence in the nilradical of R . We

also have $V(I) \cap V(J) = \emptyset$. This implies that $V(I + J) = \emptyset$. Since every ideal in R , which is not equal to R , is contained in a maximal ideal, we have $I + J = R$.

Then there exist $x \in I$ and $y \in J$ such that $x + y = 1$. Since xy is in the nilradical of R , there exists a positive integer n such that $(xy)^n = 0$. Let I' be the ideal generated by the element x^n and J' be the ideal generated by the element y^n . Then, we have $I' + J' = R$. This is because, $x + y = 1$ implies that $(x + y)^{2n} = 1$ and if we expand $(x + y)^{2n}$, we see that

$$\begin{aligned} (x + y)^{2n} &= x^{2n} + \binom{2n}{1} x^{2n-1} y + \dots + \binom{2n}{n} x^n y^n + \dots + \binom{2n}{2n-1} x y^{2n-1} + y^{2n} \\ &= x^n (x^n + \binom{2n}{1} x^{n-1} y + \dots + \binom{2n}{n} y^n) + \\ &\quad y^n (\binom{2n}{n+1} x^{n-1} y + \dots + \binom{2n}{2n-1} x y^{n-1} + y^n) \\ &= 1 \end{aligned}$$

This shows that $1 \in I' + J'$. Thus, $I' + J' = R$. We also have $I'J' = 0$ as $(xy)^n = 0$. Now, there exist $e \in I'$ and $e' \in J'$ such that $e + e' = 1$. Since $I'J' = 0$, we also have $ee' = 0$. Then, the equalities

$$e = e(e + e') = e^2 + ee' = e^2.$$

show that e is an idempotent element of R .

Claim: $R = eR \times (1 - e)R$.

Let $b \in eR \cap (1 - e)R$. Then, there exist $r \in R$ such that $b = er$ and $r' \in R$ such that $b = (1 - e)r'$. We have $er = (1 - e)r'$, we multiply both sides by e and we see that $b = er = 0$. For any $r \in R$, we can write $r = er + (1 - e)r$. Hence we proved the claim.

(\Leftarrow) Suppose R is isomorphic to the product $A \times B$. Any ideal E of $A \times B$ is a prime ideal if and only if $E = P \times \{0\}$ for a prime ideal P of A or $E = \{0\} \times Q$ for a prime ideal Q of B . Let $I = A \times \{0\}$ and $J = \{0\} \times B$. Then, $\text{Spec}(R)$ is the disjoint union of $V(I)$ and $V(J)$. Hence, $\text{Spec}(R)$ is disconnected.