Solutions to Homework

June 2, 2023

Contents

Chapter 1

Solutions to Homework9

Exercise. *For an ideal $I \subseteq R$, $r(I) = \{f \in R \mid f^n \in I$ for some $n \in \mathbb{Z}_{>0}\}$ is called its radical.*

1. *$r(I)$ is an ideal of R.*

2. *$r(I)$ is the intersection of all prime ideals of R containing I.*

3. *An ideal I is called radical if $r(I) = I$. Prove there is a one to one correspondence between the set of radical ideals and closed subets of $\operatorname{Spec} R$ by $I \mapsto Z(I)$, and this map reverses the inclusion relation.*

Proof. For (1). For $a, b \in I$, there exists $n \in \mathbb{Z}_{>0}$ such that $a^n \in I, b^n \in I$. Thus

$$(a+b)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} a^i b^{2n-i} \in I$$

and for all $c \in R$, $(ca)^n = c^n a^n \in I$. This shows $r(I)$ is an ideal.

For (2). It suffices to show the radical of zero ideal is the intersection of prime ideals by taking quotient. However, note that the radical of zero ideal is exactly nilradical.

For (3). For two ideals $I, J \subseteq R$, note that $Z(I) \subseteq Z(J)$ if and only if $r(I) \supseteq r(J)$. Then if $Z(I) = Z(J)$, then $I = r(I) = r(J) = J$ implies the correspondence is injective, and for arbitrary $Z(I)$, one has

$$Z(I) = Z(r(I))$$

which implies the correspondence is surjective. □

Exercise.

1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$

2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$

3. $r(\mathfrak{ab}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

4. $r(\mathfrak{a}) = (1) rightarrow \mathfrak{a} = (1)$

5. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

6. *if $\mathfrak{p}$ is prime, $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.*

Proof. (1) and (2) are almost obvious by definition. For (3). Note that

$$(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$$

Then by (2) we obtain

$$r(\mathfrak{a}\cap\mathfrak{b}) = r((\mathfrak{a}\cap\mathfrak{b})^2) \subseteq r(\mathfrak{a}\mathfrak{b}) \subseteq r(\mathfrak{a}\cap\mathfrak{b})$$

which implies $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a}\cap\mathfrak{b})$. For the half part. If $x \in \mathfrak{a}\cap\mathfrak{b}$, then there exists m, n such that $x^m \in \mathfrak{a}, x^n \in \mathfrak{b}$. Then $x^{\max\{m,n\}} \in \mathfrak{a}\cap\mathfrak{b}$, and converse is clear.

For (4). $r(\mathfrak{a}) = (1)$ is equivalent to for all $x \in (1)$, there exists n such that $x^n \in \mathfrak{a}$. Take $x = 1$ implies $1 \in \mathfrak{a}$, so we have $\mathfrak{a} = (1)$, and converse is clear.

For (5). Consider $m + n$, where $m \in r(\mathfrak{a}), n \in r(\mathfrak{b})$, then there exists a sufficiently large N such that $(m+n)^N \in \mathfrak{a}+\mathfrak{b}$, just by considering binomial expansion. So if there exists n such that $x^n \in r(\mathfrak{a}) + r(\mathfrak{b})$, then $x^{nN} \in \mathfrak{a}+\mathfrak{b}$, which implies $x \in r(\mathfrak{a}+\mathfrak{b})$, and converse is clear.

For (6). Just note that $x^n \in \mathfrak{p}$ is equivalent to $x \in \mathfrak{p}$ for a prime ideal $\mathfrak{p}$. □

Exercise. *The Jacobson radical ideal $\mathfrak{A}$ of a ring A is defined to be the intersection of all the maximal ideals of A. It can be characterized as follows: $x \in \mathfrak{R}$ if and only if $1 - xy$ is unit for all $y \in A$.*

Proof. If $1 - xy$ is not a unit, then there exists a maximal ideal $\mathfrak{m}$ containing $1 - xy$, but $x \in \mathfrak{R} \subseteq \mathfrak{m}$, which implies $1 \in \mathfrak{m}$, a contradiction. Conversely, suppose $x \notin \mathfrak{m}$ for some maximal ideal, then $\mathfrak{m}$ and x generates the unit ideal, so we have $u + xy = 1$ for some $u \in \mathfrak{m}, y \in A$, thus $1 - xy \in \mathfrak{m}$, and is therefore not a unit. □

Exercise. *Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.*

Proof. If x is a nilpotent element, then $x \in \mathfrak{N} \subseteq \mathfrak{R}$. By exercise 3 we have $1 - xy$ is unit for any $y \in A$. Take $y = -1$ we obtain $1 + x$ is a unit. If y is unit, then we have $x + y = y(y^{-1}x + 1)$. Since $y^{-1}x$ is also nilpotent, we have $y^{-1}x + 1$ is unit, thus $x + y$ is unit. □

Exercise. *Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that*

1. *f is a unit in $A[x]$rightarrowa_0 is a unit in A and $a_1, \ldots, a_n$ are nilpotent.*
2. *f is nilpotent rightarrow$a_0, a_1, \ldots, a_n$ are nilpotent.*
3. *f is a zero-divisor rightarrow there exists $a \neq 0$ in A such that $af = 0$.*
4. *f is said to be primitive if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive rightarrow$f$ and g are primitive.*

Proof. For (1). Use $g = \sum_{i=0}^m b_ix^i$ to denote the inverse of f. Since $fg = 1$ and if we use c_k to denote $\sum_{m+n=k} a_mb_n$, then we have

$$\begin{cases} c_0 = 1 \\ c_k = 0, \quad k > 0 \end{cases}$$

But $c_0 = a_0b_0$, thus a_0 is unit. Now let's prove $a_n^{r+1}b_{m-r} = 0$ by induction on r: $r = 0$ is trivial, since $a_nb_m = c_{n+m} = 0$. If we have already proven this for $k < r$. Then consider c_{m+n-r}, we have

$$0 = c_{m+n-r} = a_nb_{m-r} + a_{n-1}b_{m-r+1} + \ldots$$

and multiply a_n^r we obtain

$$0 = a_n^{r+1}b_{m-r} + a_{n-1}\underbrace{a_n^rb_{m-r+1}}_{\text{by induction this term is } 0} + a_{n-2}a_n\underbrace{a_n^{r-1}b_{m-r+2}}_{\text{by induction this term is } 0} + \ldots$$

which completes the proof of claim. Take $r = m$, we obtain $a_n^{m+1} b_0 = 0$. But b_0 is unit, thus a_n is nilpotent and $a_n x^n$ is a nilpotent element in $A[x]$. By exercise 4, we know that $f - a_n x^n$ is unit, then we can prove a_{n-1}, a_{n-2} is also nilpotent by induction on degree of f; Conversely, if a_0 is unit and $a_1, \dots, a_n$ is nilpotent. We can imagine that if you power f enough times, then we will obtain unit. Or you can see $\sum_{i=1}^n a_i x^i$ is nilpotent, then unit plus nilpotent is also unit.

For (2)[1]. If $a_0, \dots, a_n$ are nilpotent, then clearly f is; Conversely, if f is nilpotent, then clearly a_n is nilpotent, and we have $f - a_n x^n$ is nilpotent, then by induction on degree of f to conclude.

For (3). $af = 0$ for $a \neq 0$ implies f is a zero-divisor is clear; Conversely choose a $g = \sum_{i=0}^m b_i x^i$ of least degree m such that $fg = 0$, then we have $a_n b_m = 0$, hence $a_n g = 0$, since $a_n g f = 0$ and has degree less than m. Then consider

$$0 = fg - a_n x^n g = (f - a_n x^n) g$$

Then $f - a_n x^n$ is a zero-divisor with degree $n-1$, so we can conclude by induction on degree of f.

For (4). Note that $(a_0, \dots, a_n) = 1$ is equivalent to there is no maximal ideal $\mathfrak{m}$ contains $a_0, \dots, a_n$, it's an equivalent description for primitive polynomials. For $f \in A[x]$, f is primitive if and only if for all maximal ideal $\mathfrak{m}$, we have $f \notin \mathfrak{m}[x]$. Note that we have the following isomorphism

$$A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$$

Indeed, consider the following homomorphism

$$\begin{aligned} \varphi\colon A[x] &\to (A/\mathfrak{m})[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n (a_i + \mathfrak{m}) x^i \end{aligned}$$

Clearly $\ker \varphi = \mathfrak{m}[x]$ and use the first isomorphism theorem. So in other words, $f \in A[x]$ is primitive if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x]$ for any maximal ideal $\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, then $(A/\mathfrak{m})[x]$ is an integral domain by (3), so $\overline{fg} \neq 0 \in (A/\mathfrak{m})[x]$ if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x], \overline{g} \neq 0 \in (A/\mathfrak{m})[x]$. This completes the proof. □

Exercise. *In the ring $A[x]$, the Jacobson radical is equal to the nilradical*

Proof. Since we already have $\mathfrak{N} \subseteq \mathfrak{R}$, it suffices to show for any $f \in \mathfrak{R}$, it's nilpotent. Note that by exercise 3, we have $1 - fg$ is unit for any $g \in A[x]$. Choose g to be x, then by (1) of exercise 5 we know that all coefficients of f is nilpotent in A, and by (2) of exercise 5, f is nilpotent. This completes the proof. □

Exercise. *Prove that* $\operatorname{Spec} R$ *is quasi-compact*[2] *under Zariski topology.*

Proof. It suffices to show every open covering taking the form $\{U_{f_i}\}$ has a finite subcovering, since U_f forms a basis of Zariski topology. We can translate $X = \bigcup_{i \in I} U_{f_i}$ as $(f_i)_{i \in I} = (1)$. Indeed,

$$(f_i)_{i \in I} = (1) \iff \bigcap_{i \in I} V(f_i) = V((f_i)_{i \in I}) = \varnothing \iff \bigcup_{i \in I} U_{f_i} = X$$

[1] An alternative proof of (2). Note that

$$\mathfrak{N}(A[x]) = \bigcap \mathfrak{p}[x] = (\bigcap \mathfrak{p})[x] = \mathfrak{N}(A)[x]$$

[2] Here X is called quasi-compact if every open covering of X has a finite subcovering, and a topological space is called compact, if it's both Hausdorff and quasi-compact.

So if $\{f_i\}_{i\in I}$ generates (1), then there is a finite expression such that

$$\sum_{i=1}^{n} a_i f_i = 1, \quad a_i \in A$$

So we can cover X just using $U_{f_1}, \dots, U_{f_n}$. $\square$

Exercise. *Let $X = \operatorname{Spec} R$ and $f \in R$. Denote by $U_f = X - Z(f)$. Let $S = R[x]/(xf-1)$. Prove that $\operatorname{Spec} S$ is homeomorphic to U_f induced by the natural ring homomorphism $R \to S$.*

Proof. If f is nilpotent, then $Z(f) = X$, that is $U_f = \varnothing$. In this case, unit equals to nilpotent element in S, since $1 + (xf-1) = xf + (xf-1)$. This shows S is a zero ring, which implies $\operatorname{Spec} S = \varnothing$.

If f is not nilpotent, then the localization of R with respect to $\{1, f, f^2, \dots\}$, denoted by R_f is isomorphic to $R[x]/(xf-1)$. Indeed, consider

$$\begin{aligned} \varphi\colon R[x] &\to R_f = \{\frac{r}{f^n} \mid r \in R, n \in \mathbb{Z}_{\geq 0}\} \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} \frac{a_i}{f^i} \end{aligned}$$

which is a surjective ring homomorphism with kernel $(xf-1)$. Now it suffices to show U_f is homeomorphic to $\operatorname{Spec} R_f$, which is a well-known result. $\square$

Exercise. *Let $A = \prod_{i=1}^{n} A_i$ be the direct product of rings A_{i}. Show that $\operatorname{Spec} A$ is the disjoint union of open (and closed) subspaces X_i, where X_i is canonically homeomorphic with $\operatorname{Spec} A_i$.*

Proof. For each i consider the projection $p_i\colon \prod A_i \to A_i$. It's a surjective, and thus there is a homeomorphism $X_i = V(\ker p_i) \cong \operatorname{Spec}(A_i)$. We claim $\{X_i\}$ covers A and $X_i \cap X_j = \varnothing$ for distinct i, j. Note that we can write X_i explictly as $V(\prod_{i\neq j} A_j)$. Then

$$\bigcup V(\prod_{i\neq j} A_j) = V(\bigcap \prod_{i\neq j} A_j) = V((0)) = X$$

And

$$X_i \cap X_j = V(\prod_{i\neq j} A_j + \prod_{i\neq j} A_i) = V((1)) = \varnothing$$

As desired. $\square$

Exercise. *A topological space X is called noetherian if it satisfies the descending chain condition for closed subets.*

1. *A topological space X is noetherian if and only if every collection of closed subsets of X has a minimal element under inclusion.*

2. *A topological space X is noetherian if and only if every open subset of X is compact.*

3. *Every closed subset of noetherian space X is a finite union of irreducible subsets.*

4. *If R is a noetherian ring, then $\operatorname{Spec} R$ is noetherian.*

Proof. For (1). Let $\{Y_i\}_{i\in I}$ be a collection of closed subsets of X. If there is no minimal element in this collection under inclusion, then there exists a descending chain of closed subsets which is not stable, a contradiction. Conversely, suppose $Y_1 \supseteq Y_2 \supseteq \dots$ is a chain of closed subsets. Then there exists a minimal element under inclusion, denoted by Y_m, which implies $Y_m = Y_{m+1} = \dots$.

For (2). It's clear to see X is noetherian if and only if it satisfies the increasing chain condition for open subsets. For open subset $U \subseteq X$ with open covering $\{U_i\}_{i\in I}$. If there is no finite subcovering, then there exists an increasing chain of open subsets which is not stable, a contradiction. Conversely, if $U_1 \subseteq U_2 \subseteq \dots$ is an increasing chain of open subsets, then consider open subset $U = \bigcup_{i=1}^{\infty} U_i$ which is compact by hypothesis. Then open covering $\{U_i\}_{i=1}^{\infty}$ of U admits a finite subcovering, which implies this chain is stable.

For (3). Let $\mathcal{A}$ be the set of nonempty closed subsets of X which cannot be written as a finite union of irreducible closed subsets. If $\mathcal{A}$ is nonempty, then since X is noetherian, it must contain a minimal element, say Y. Then Y is not irreducible, by definition there exists proper closed subsets Y' and Y'' of Y such that $Y = Y' \cup Y''$. By minimality of Y, each of Y' and Y'' can be expressed as a finite union of closed irreducible subsets, hence Y also, which is a contradiction.

For (4). Let $Z(I_1) \supseteq Z(I_2) \supseteq \dots$ be a chain of closed subsets in $\operatorname{Spec} R$, and without lose of generality we may assume I_i are radical ideals, since $Z(I) = Z(r(I))$. By exercise 1 this corresponds to an increasing chain of ideals in R, that is

$$I_1 \subseteq I_2 \subseteq \dots$$

Since R is noetherian, there exists $m \in \mathbb{Z}_{>0}$ such that $I_m = I_{m+1} = \dots$, which implies $Z(I_m) = Z(I_{m+1}) = \dots$. This completes the proof. □

Exercise. *Describe points and closed subets of* $\operatorname{Spec} \mathbb{C}[x,y]/(x^2+y^2)$ *and* $\operatorname{Spec} \mathbb{R}[x,y]/(x^2+y^2)$.

Proof. Note that $\operatorname{Spec} \mathbb{C}[x,y]/(x^2+y^2)$ is homeomorphic to $Z(x^2+y^2) = Z(x+\sqrt{-1}y) \cup Z(x-\sqrt{-1}y)$. Note that

$$\mathbb{C}[x,y]/(x-\sqrt{-1}y) \cong \mathbb{C}[y]$$

This shows

$$Z(x-\sqrt{-1}y) = \{(x-\sqrt{-1}y), (x-\sqrt{-1}y, y-\alpha) \mid \alpha \in \mathbb{C}\}$$

The same argument shows

$$Z(x+\sqrt{-1}y) = \{(x+\sqrt{-1}y), (x+\sqrt{-1}y, y-\beta) \mid \beta \in \mathbb{C}\}$$

This gives all points of $\operatorname{Spec} \mathbb{C}[x,y]/(x^2+y^2)$. To see all its closed subsets, it suffices to find all its irreducible closed subsets, since $\operatorname{Spec} \mathbb{C}[x,y]/(x^2+y^2)$ is noetherian. However, every irreducible closed subsets of prime spectral turns out to be the closure of some point, so it suffices to consider closure of all points. By Hilbert's Nullstellensatz $(x-\sqrt{-1}y, y-\alpha)$ and $(x+\sqrt{-1}y, y-\beta)$ are maximal ideals for arbitrary $\alpha, \beta \in \mathbb{C}$, so they're closed points. $(x-\sqrt{-1}y)$ and $(x+\sqrt{-1}y)$ are not closed points, and their closures are $Z(x-\sqrt{-1}y)$ and $Z(x-\sqrt{-1}y)$ respectively.

For $\operatorname{Spec} \mathbb{R}[x,y]/(x^2+y^2)$, it's homeomorphic to $Z(x^2+y^2)$, and thus all points are prime ideals of $\mathbb{R}[x,y]$ containing (x^2+y^2). Let R be a PID. Then all prime ideals in $R[y]$ are listed as follows.

1. (0).
2. $(f(y))$, where $f(y)$ is irreducible in $R[y]$
3. $(p, f(y))$, where $p \in R$ is prime and $f(y)$ is irreducible in $(R/p)[y]$.

Thus all prime ideals of $\mathbb{R}[x,y]$ containing (x^2+y^2) are $(x^2+y^2), (x,y), (x-a, y^2+a^2), (y-a, x^2+a^2), (x+cy+d, x^2+y^2), (y+cx+d, x^2+y^2)$, where $a, c, d \in \mathbb{R}$. Note that

$$\mathbb{R}[x,y]/(x-a, y^2+a^2) \cong \mathbb{C}$$

Thus $(x-a, y^2+a^2)$ is a closed points, and the same argument yields both $(y-a, x^2+a^2), (x+cy+d, x^2+y^2), (y+cx+d, x^2+y^2)$ and (x,y) are closed points. Thus all irreducible closed subsets of $\operatorname{Spec} \mathbb{R}[x,y]/(x^2+y^2)$ are $Z(x^2+y^2)$ and points except (x^2+y^2). □

Chapter 2

Solutions to Homework11

Exercise. *Calculate* $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ *for positive integers* m *and* n.

Proof. Now we're going to prove the following isomorphism

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m,n)\mathbb{Z}$$

Consider the following mapping

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/\gcd(m,n)\mathbb{Z} \\ (x+m\mathbb{Z}, y+n\mathbb{Z}) &\mapsto xy+\gcd(m,n)\mathbb{Z} \end{aligned}$$

It's well-defined and bilinear, and thus it induces a linear map $f\colon \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\gcd(m,n)\mathbb{Z}$ such that

$$f(x+m\mathbb{Z} \otimes y+n\mathbb{Z}) = xy+\gcd(m,n)\mathbb{Z}$$

Consider the following map

$$\begin{aligned} g\colon \mathbb{Z}/\gcd(m,n)\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \\ z+\gcd(m,n)\mathbb{Z} &\mapsto (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) \end{aligned}$$

It's well-defined. Indeed, if we let $z' = z + k\gcd(m,n)$, then Bezout theorem implies that there exists $a, b \in \mathbb{Z}$ such that $am + bn = \gcd(m,n)$. Thus

$$\begin{aligned} (z'+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) &= (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) + (k(am+bn)+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) \\ &= (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) + (n(kb+m\mathbb{Z})) \otimes (1+n\mathbb{Z}) \\ &= (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) + (kb+m\mathbb{Z}) \otimes (n+n\mathbb{Z}) \\ &= (z+m\mathbb{Z}) \otimes (1+n\mathbb{Z}) \end{aligned}$$

It's clear $f \circ g = 1, g \circ f = 1$, so we have desired isomorphism. □

Exercise. *Let* V *be a free* R*-module with basis* $x, x \in X$ *and* W *a free* R*-module with basis* $y, y \in Y$. *Show that the tensor product of* V *and* W *is free with basis* $x \otimes y$.

Proof. Suppose $X \otimes Y$ is the free module generated by basis $\{x \otimes y \mid x \in X, y \in Y\}$, and $\tau\colon V \times W \to X \otimes Y$ be the map given by $(x, y) \mapsto x \otimes y$. Now we're going to prove $X \otimes Y$ satisfies the universal property, and then the uniqueness shows $X \otimes Y \cong V \otimes W$. For arbitrary R-module P and a bilinear map $f\colon V \times W \to P$, it suffices to prove there exists a unique linear map $\widetilde{f}\colon X \otimes Y \to P$ such that the following diagram commute

$$\begin{tikzcd} V \times W \arrow[r, "f"] \arrow[d, "\tau"'] & P \\ X \otimes Y \arrow[ur, "\widetilde{f}"'] & \end{tikzcd}$$

Since $X \otimes Y$ is the free module generated by $\{x \otimes y \mid x \in X, y \in Y\}$, $\widetilde{f}$ is uniquely determined by its values on basis, and in order to let the diagram commute, we need to define

$$\widetilde{f}(x \otimes y) = f(x, y)$$

Note that $\widetilde{f}$ defined in this way is linear since f is. This shows the existence and uniqueness of $\widetilde{f}$, and thus $X \otimes Y \cong V \otimes W$. $\square$

Exercise. *Let M be a R-module. Prove that both $\operatorname{Hom}_R(-, M)$ and $\operatorname{Hom}_R(M, -)$ are left exact.*

Proof. Here we only prove $\operatorname{Hom}_R(-, M)$ is left exact. If

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is exact, we need to show the induced sequence

$$0 \to \operatorname{Hom}_R(C, M) \xrightarrow{g^*} \operatorname{Hom}_R(B, M) \xrightarrow{f^*} \operatorname{Hom}_R(A, M)$$

is exact, where $f^* = \operatorname{Hom}_R(f, M)$ and $g^* = \operatorname{Hom}_R(g, M)$. One inclusion, namely $\ker f^* \supseteq \operatorname{im} g^*$ is obvious, because $f^* \circ g^* = (g \circ f)^* = 0^* = 0$. Now let $h \in \ker f^*$, which means $f^*(h) = h \circ f = 0$. This is equivalent to $\operatorname{im} f \subseteq \ker h$ and, by exactness of the original sequence, $\ker g \subseteq \ker h$. By the homomorphism theorems, $h \colon B \to M$ induces a homomorphism $h \colon B/\ker g \to M$ such that $h = h \circ \pi$, where $\pi \colon B \to B/\ker g$ is the canonical map. By assumption g is surjective, g induces an isomorphism $g \colon B/\ker g \to C$ such that $g = g \circ \pi$. Consider $k = h \circ g^{-1} \colon C \to M$ and then

$$g^*(k) = k \circ g = h$$

which implies $h \in \operatorname{im} g^*$, and thus $\ker f^* = \operatorname{im} g^*$. For $h \in \ker g^*$, that is $h \circ g = 0$, one must have $h = 0$ since g is surjective. This completes the proof. $\square$

Exercise. *In general, tensor product does not commute with direct product.*

Proof. Now we're going to show $(\prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0$ and $\prod_{n \geq 1}(\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$, and thus tensor product doesn't commute with direct product in general. It's clear to see $\prod_{n \geq 1}(\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$, since $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ for any $n \in \mathbb{Z}_{\geq 1}$. Let $S = \mathbb{Z} \setminus \{0\}$. Then

$$(\prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong S^{-1}(\prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z})$$

Consider $\alpha = (1)_{n \geq 1} \in \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$, which is a non-torsion element. In particular, there is no element $N \in S$ such that $N\alpha = 0$, and thus its image in $S^{-1}(\prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z})$ is not zero. This completes the proof. $\square$

Exercise. *Let A and B be two R-algebras. Let $\pi_1 \colon A \to A \otimes_R B, a \mapsto a \otimes 1$ and $\pi_2 \colon B \to A \otimes_R B, b \mapsto 1 \otimes b$ be two homomorphisms of R-algebras. Show the universal property of $A \otimes_R B$. In other words, if there is a R-algebra C with $f_1 \colon A \to C$ and $f_2 \colon B \to C$, then there exists a unique homomorphism of R-algebra $f \colon A \otimes_R B \to C$ such that $f_i = f \circ \pi_i$.*

Proof. Since A, B are R-modules we may form their tensor product $A \otimes_R B$, which is an R-module. To make it into an R-algebra, it suffices to define a multiplication on it. Consider the following linear map from $A \times B \times A \times B$ to $A \otimes_R B$ given by

$$(a, b, a', b') \mapsto aa' \otimes bb'$$

It induces an R-module homomorphism

$$(A \otimes_R B) \otimes_R (A \otimes_R B) \to A \otimes_R B$$

which gives the multiplication structure on $A \otimes_R B$. Suppose there is R-algebra C with $f_1 \colon A \to C$ and $f_2 \colon B \to C$, by universal property of tensor product, there exists a unique R-module homomorphism $f \colon A \otimes_R B \to C$ such that $f_i = f \circ \pi$, and by the construction of multiplication structure on $A \otimes_R B$, it's clear to see f is a R-algebra homomorphism. $\square$

Exercise. *Simplify* $\mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[t], \mathbb{C}[t] \otimes_{\mathbb{C}[t]} \mathbb{C}[t]$ *and* $\mathbb{C}[t,s] \otimes_{\mathbb{C}[t]} \mathbb{C}[t,s]$. *Here* $\mathbb{C}[t]$ *and* $\mathbb{C}[t,s]$ *are* $\mathbb{C}[t]$*-modules via the natural embedding.*

Proof. It's clear $\mathbb{C}[t] \otimes_{\mathbb{C}[t]} \mathbb{C}[t] \cong \mathbb{C}[t]$, and $\mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[t] \cong \mathbb{C}[x,y], \mathbb{C}[t,s] \otimes_{\mathbb{C}[t]} \mathbb{C}[t,s] \cong \mathbb{C}[x,y,z]$. The last two isomorphisms follows from the following claim: Let R be a ring. Then $R[x] \otimes_R R[y] \cong R[x,y]$, which can be directly proved by universal property of tensor product. $\square$

Exercise. *Let M and N be two R-modules and G be an abelian group. We call a map $f \colon M \times N \to G$ "R-balanced" if the map is $\mathbb{Z}$-bilinear and also satisfies $f(rm,n) = f(m,rn)$ for any $r \in R, m \in M$ and $n \in N$. The set of such maps is denoted by* $\mathrm{Hom}_{R-balance}(M \times N, G)$.

(1) *Show that there is a bijection between*

$$\mathrm{Hom}_{R-balance}(M \times N, G) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N,G))$$

Here the R-module structure on $\mathrm{Hom}_{\mathbb{Z}}(N,G)$ is given by $(r\phi)(n) = \phi(rn)$ for any $\phi \in \mathrm{Hom}_{\mathbb{Z}}(N,G)$.

(2) *Construct an abelian group $M \tilde{\otimes} N$ such that there is an natural bijection between*

$$\mathrm{Hom}_{\mathbb{Z}}(M \tilde{\otimes} N, G) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N,G)).$$

Try to write it as quotient group of free abelian group with basis $M \times N$ quotient by some relations. Denote by $m \tilde{\otimes} n$ for the image of $(m,n) \in M \times N$ in $M \tilde{\otimes} N$. State the universal property of $M \tilde{\otimes} N$.

(3) *Use the universal property to prove that $r \cdot m \tilde{\otimes} n = (rm) \tilde{\otimes} n$ gives a well defined R-module structure on $M \tilde{\otimes} N$. Prove that the natural map $M \otimes N \to M \tilde{\otimes} N$ is R-bilinear under this R-module structure.*

(4) *Show that $M \tilde{\otimes} N \cong M \otimes N$ as R-module.*

Proof. For (1). Let $f \in \mathrm{Hom}_{R-\mathrm{balance}}(M \times N, G)$ and $m \in M$, we define $g(m)$ be the map $n \mapsto f(m,n)$, where $n \in N$. Note that $n \mapsto f(m,n)$ lies in $\mathrm{Hom}_{\mathbb{Z}}(N,G)$, so if we want to show g gives an element in $\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N,G))$, it suffices to show g is a R-module homomorphism. For arbitrary $m_1, m_2 \in M$, one has

$$\begin{aligned} g(m_1 + m_2) &= \{n \mapsto f(m_1 + m_2, n)\} \\ &= \{n \mapsto f(m_1, n) + f(m_2, n)\} \\ &= \{n \mapsto f(m_1, n)\} + \{n \mapsto f(m_2, n)\} \\ &= g(m_1) + g(m_2) \end{aligned}$$

and for $r \in R, m \in M$, one has

$$\begin{aligned} g(rm) &= \{n \mapsto f(rm, n)\} \\ &= \{n \mapsto f(m, rn)\} \\ &= r\{n \mapsto f(m, n)\} \\ &= rg(m) \end{aligned}$$

If we use φ to denote this correspondence, we're going to show φ is a bijection. It's clear φ is injective, since if $\varphi(f_1) = \varphi(f_2)$, then for arbitrary $(m,n) \in M \times N$, one has $f_1(m,n) = f_2(m,n)$.

To see it's surjective, for arbitrary $g \in \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, G))$, we define $f(m, n) = g(m)(n)$, where $(m, n) \in M \times N$, a routine computation shows such f is R-balanced.

For (2). Suppose $F(M \times N)$ is the free abelian group with basis $M \times N$, and consider

$$M \widetilde{\otimes} N := F(M \times N)/N$$

where N is the subgroup generated by $\{(m_1+m_2, m)-(m_1, n)-(m_2, n), (m, n_1+n_2)-(m, n_1)-(m, n_2), (rm, n)-(m, rn) \mid m_1, m_2 \in M, n_1, n_2 \in N, r \in R\}$. By definition of $M\widetilde{\otimes}N$, it's clear there is a bijection between

$$\mathrm{Hom}_{R-\mathrm{balance}}(M \times N, G) \cong \mathrm{Hom}_{\mathbb{Z}}(M\widetilde{\otimes}N, G)$$

and thus $\mathrm{Hom}_{\mathbb{Z}}(M\widetilde{\otimes}N, G) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Hom}_{\mathbb{Z}}(N, G))$. There is a universal property of $M\widetilde{\otimes}N$: Let $\tau\colon M \times N \to M\widetilde{\otimes}N$ be the map $(m, n) \mapsto m\widetilde{\otimes}n$. For arbitrary abelian group G and R-balanced map $f\colon M \times N \to G$, there exists a unique group homomorphism $\widetilde{f}\colon M\widetilde{\otimes}N \to G$ such that the following diagram commutes

$$\begin{tikzcd}
M \times N \arrow[d, "\tau"'] \arrow[dr, "f"] & \\
M\widetilde{\otimes}N \arrow[r, "\widetilde{f}"'] & G
\end{tikzcd}$$

For (3). For $r \in R$, consider the following map

$$\begin{aligned} M \times N &\to M\widetilde{\otimes}N \\ (m, n) &\mapsto (rm)\widetilde{\otimes}n \end{aligned}$$

A direct computation shows it's R-balanced. By universal property, it induces a well-defined map

$$\begin{aligned} M\widetilde{\otimes}N &\to M\widetilde{\otimes}N \\ m\widetilde{\otimes}n &\mapsto (rm)\widetilde{\otimes}n \end{aligned}$$

which gives a R-module structure on $M\widetilde{\otimes}N$.

For (4). Consider the map $\tau\colon M \times N \to M\widetilde{\otimes}N$ given by $(m, n) \mapsto m\widetilde{\otimes}n$. Note that for $m \in M, n \in N, r \in R$, one has

$$\begin{aligned} \tau(rm, n) &= (rm)\widetilde{\otimes}n = r(m\widetilde{\otimes}n) = r\tau(m, n) \\ \tau(m, rn) &= m\widetilde{\otimes}(rn) = (rm)\widetilde{\otimes}n = r(m\widetilde{\otimes}n) = r\tau(m, n) \end{aligned}$$

Thus τ is a R-bilinear map, and thus it induces a R-module homomorphism $F\colon M \otimes N \to M\widetilde{\otimes}N$. Conversely, consider the map $\tau'\colon M \times N \to M \otimes N$ given by $(m, n) \mapsto m \otimes n$, which is R-bilinear. In particular it's R-balanced, so by universal property it induces a group homomorphism $G\colon M\widetilde{\otimes}N \to M \otimes N$, and it's also a R-module homomorphism if we consider R-module structure of $M\widetilde{\otimes}N$. A direct computation yields $F \circ G = \mathrm{id}$ and $G \circ F = \mathrm{id}$, so $M\widetilde{\otimes}N \cong M \otimes N$ as R-modules.

$\square$