

ALGEBRA HW 1

CLAY SHONKWILER

1

Which of the following R -modules are finitely generated? Which are free? Which are R -algebras? Among the R -algebras, which are finitely generated as R -algebras?

(a): $R = \mathbb{Z}$, $M = \mathbb{Z}/5 \times \mathbb{Z}/7$

Answer: M is certainly finitely generated, as $(1, 1)$ generates all of $\mathbb{Z}/5 \times \mathbb{Z}/7$, since 5 and 7 are relatively prime. Note that $35(1, 1) = (0, 0)$ in M , and so M is not torsion-free and, therefore, not free.

M is an R -algebra under the usual multiplication in $\mathbb{Z}/5 \times \mathbb{Z}/7$, since, for $(a, b), (c, d) \in \mathbb{Z}/5 \times \mathbb{Z}/7$ and $r \in \mathbb{Z}$,

$$(a, b)(r(c, d)) = (a, b)(rc, rd) = (arc, brd) = r(ac, bd) = r(a, b)(c, d)$$

and

$$(r(a, b))(c, d) = (ra, rb)(c, d) = (rac, rbd) = r(ac, bd) = r(a, b)(c, d).$$

Since M is finitely generated as an R -module, it is certainly finitely generated as an R -algebra.



(b): $R = \mathbb{Z}$, $M = (5) =$ ideal generated by 5

Answer: If $a \in M$, then $a = 5b$ for some $b \in \mathbb{Z}$, so we see that $\{5\}$ is a generating set for M , and so M is finitely generated. Since 5 is torsion-free, we see that $\{5\}$ is a linearly independent set, and so M is free.

Also, M is an R -algebra under the usual multiplication in \mathbb{Z} , since, for any $a, b \in \mathbb{Z}$, $5a \cdot 5b = 25ab \in M$ and, for any $r \in \mathbb{Z}$,

$$5a(r \cdot 5b) = r(5a \cdot 5b) = (r \cdot 5a)5b$$

since \mathbb{Z} is a commutative ring. Finally, since M is finitely generated as an R -module, it is certainly finitely generated as an R -algebra.



(c): $R = \mathbb{Z}$, $M = \mathbb{Z}[\sqrt{3}]$

Answer: An element of M is of the form $a + b\sqrt{3}$, so we see that $\{1, \sqrt{3}\}$ is a generating set for M , so M is finitely generated as an R -module. Suppose $a, b \in \mathbb{Z}$ such that $a(1) + b\sqrt{3} = a + b\sqrt{3} = 0$.

Then $a = b = 0$, so $\{1, \sqrt{3}\}$ is linearly independent and so M is a free R -module.

Since M is a ring containing R , M is certainly an R -algebra. Since M is finitely generated as an R -module, it is finitely generated as an R -algebra.



(d): $R = \mathbb{Z}$, $M = \mathbb{Z}[\pi]$

Answer: Since π is transcendental, M is isomorphic to $\mathbb{Z}[x]$ which is not finitely generated. However, in consideration of this isomorphism, M is a free R -module with basis given by $\{1, \pi, \pi^2, \dots\}$.

Since M is a ring extension of R , M must be an R -algebra. Furthermore, M is finitely generated as an R -algebra with generating set $\{1, \pi\}$.



(e): $R = \mathbb{Z}$, $M = \mathbb{Z}[1/2, 1/3]$

Answer:



(f): $R = \mathbb{Z}$, $M = \mathbb{Q}$

Answer: Suppose M is finitely generated, with generating set $\left\{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\right\}$. Let a be relatively prime to q_1, \dots, q_n . Then, for any $c_1, \dots, c_n \in \mathbb{Z}$,

$$c_1 \frac{p_1}{q_1} + \dots + c_n \frac{p_n}{q_n} = \frac{\sum_{i=1}^n c_i p_i q_1 \cdots \widehat{q_i} \cdots q_n}{q_1 \cdots q_n} \neq \frac{1}{b},$$

since b is not a factor of $q_1 \cdots q_n$. Hence, M is not finitely generated.

Now, let $\left\{\frac{p}{q}, \frac{a}{b}\right\}$ be any two-element subset of M . Then

$$aq \frac{p}{q} - pb \frac{a}{b} = ap - ap = 0,$$

so this set is not linearly independent. Since a basis, if it exists, must be infinite, this proves that there can be no basis for M as an R -module and so M is not free.

Since M is a ring extension of R , M is necessarily an R -algebra. If M is finitely generated as an R -algebra, then there exists a generating set $\left\{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\right\}$; let b be relatively prime to q_1, \dots, q_n . Then, as we saw above, $\frac{1}{b}$ is not a linear combination of the $\frac{p_i}{q_i}$. Furthermore, for any $c_1, \dots, c_n \in \mathbb{Z}$,

$$\left(c_1 \frac{p_1}{q_1}\right) \cdots \left(c_n \frac{p_n}{q_n}\right) = \frac{c_1 p_1 \cdots c_n p_n}{q_1 \cdots q_n} \neq \frac{1}{b},$$

since b does not divide $q_1 \cdots q_n$. Thus, we conclude that M is not finitely generated as an R -algebra.



(g): $R = \mathbb{Z}$, $M = \frac{1}{2}\mathbb{Z} = \{\frac{n}{2} | n \in \mathbb{Z}\}$

Answer: Let $\frac{n}{2} \in \frac{1}{2}\mathbb{Z}$. Then

$$\frac{n}{2} = n \frac{1}{2},$$

so $\{\frac{1}{2}\}$ generates M as an R -module, and so M is finitely generated. Furthermore, since $n \frac{1}{2} = \frac{n}{2} \neq 0$ so long as $n \neq 0$, we see that $\frac{1}{2}$ is torsion-free, meaning $\{\frac{1}{2}\}$ is linearly independent, and so M is free.

Note that

$$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin M$$

so M is not an R -algebra. ♣

(h): $R = \mathbb{Z}[\sqrt{-5}]$, $M = (2, 1 + \sqrt{-5}) \subset R$

Answer: Clearly, $\{2, 1 + \sqrt{-5}\}$ generates M as an R -module, so M is finitely generated. Since 2 and $1 + \sqrt{-5}$ are prime in R , any generating set for M must contain both of these elements. However,

$$3(2) - (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6 - 6 = 0$$

is a linear combination of 2 and $1 + \sqrt{-5}$ with coefficients in R , so we see that M is not free.

Now, since M is an ideal of R , M is closed under multiplication and, since R is a commutative ring, the multiplication in M respects the module structure, so M is an R -algebra. Since M is finitely generated as an R -module, M is also finitely generated as an R -algebra. ♣

(i): $R = \mathbb{R}[x]$, $M = \mathbb{R}[x, y]$

Answer: Since $\mathbb{R}[x, y]$ is isomorphic to $\mathbb{R}[x][y] = R[y]$ which we know is not finitely generated over R , we see that M is not finitely generated. However, the set $\{1, y, y^2, \dots\}$ does generate M as an R -module and, if $g_1, g_2, \dots \in R$ such that at least one but no more than finitely many are non-zero, then

$$\sum_{i=0}^{\infty} g_i(x)y^i \neq 0,$$

so $\{1, y, y^2, \dots\}$ is linearly independent. Hence, M is free as an R -module.

Since M is a ring extension of R , it is necessarily an R -algebra. Furthermore, the set $\{1, y\}$ generates M as an algebra over R , so M is finitely generated as an R -algebra. ♣

(j): $R = \mathbb{R}[x]$, $M = \mathbb{R}[x, y]/(y^2 - x)$

Answer: Note that, since $y^2 = x$ in M , we can re-write any element of M as a polynomial with highest y -degree at most 1. Hence, $\{1, y\}$ generate M as an R -module, so M is finitely generated. Furthermore, if $g(x) \in R$ is non-zero, then the degree of $g(x)y$ is at least 1, and so, for any $g_1, g_2 \in R$,

$$g_1(x) + g_2(x)y \neq 0,$$

so $\{1, y\}$ is a basis for M , and so M is free.

Since M is a ring extension of R it is certainly an R -algebra. Furthermore, since M is finitely generated as an R -module, it must also be finitely generated as an R -algebra.



(k): $R = \mathbb{R}[x, y]$, $M = (x, y) \subset R$

Answer: It's clear that $\{x, y\}$ generates M as an R -module, so M is finitely generated. Now, let $f, g \in I$ be any two elements of I . Since f and g are also in R , $fg - gf = 0$ is a linear combination of f and g with coefficients in R , so we see that any two elements of I are linearly dependent. Furthermore, since R is dimension 2 and (x, y) is a maximal ideal (since $R/(x, y) \simeq \mathbb{R}$), (x, y) cannot be principal, so any possible basis of M must contain at least two elements. Therefore, M is not free.

Since M is an ideal in R , it is certainly closed under multiplication and the multiplication inherited from R is distributive and preserves the module structure, so M is an R -module. Furthermore, since M is finitely generated as an R -module, it is certainly finitely generated as an R -algebra.



2

Let M be a module over R , and let $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$ be an exact sequence of R -modules. Show by example that the induced sequences

$$(1) \quad 0 \rightarrow \text{Hom}(M, N') \rightarrow \text{Hom}(M, N) \rightarrow \text{Hom}(M, N'') \rightarrow 0$$

$$(2) \quad 0 \rightarrow \text{Hom}(N'', M) \rightarrow \text{Hom}(N, M) \rightarrow \text{Hom}(N', M) \rightarrow 0$$

$$(3) \quad 0 \rightarrow M \otimes N' \rightarrow M \otimes N \rightarrow M \otimes N'' \rightarrow 0$$

are *not* necessarily exact, unlike the case of vector spaces over a field.

Proof. Consider the \mathbb{Z} -modules $\mathbb{Z}/2$ and $\mathbb{Z}/4$. Define the map $f : \mathbb{Z}/2 \rightarrow \mathbb{Z}/4$ by

$$a \mapsto 2a.$$

Then $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$, so f is a homomorphism. Define $g : \mathbb{Z}/4 \rightarrow \mathbb{Z}/2$ by

$$a \mapsto a \pmod{2}.$$

Then $g(a + b) = a + b \pmod{2} = a \pmod{2} + b \pmod{2} = g(a) + g(b)$, so g is also a homomorphism. Note that $\ker g = \{0, 2\} = \{f(0), f(1)\} = \text{im } f$. Also, f is injective and g is surjective, so

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/4 \rightarrow \mathbb{Z}/2 \rightarrow 0$$

is an exact sequence of \mathbb{Z} -modules. Now, let $M = \mathbb{Z}/2$. Suppose $f \in \text{Hom}(\mathbb{Z}/2, \mathbb{Z}/2)$. Then either $f(1) = 0$ or $f(1) = 1$. In the first case, f is the trivial homomorphism and, in the second, it is the identity homomorphism. Since these are the only possible such homomorphisms, we see that $\text{Hom}(\mathbb{Z}/2, M) = \text{Hom}(M, \mathbb{Z}/2) \simeq \mathbb{Z}/2$. If $f \in \text{Hom}(\mathbb{Z}/2, \mathbb{Z}/4)$, then $f(1)$ must have order 1 or 2; since the only such elements of $\mathbb{Z}/4$ are 0 and 2 and $f(1) = 0$ and $f(1) = 2$ define different homomorphisms, we see that $\text{Hom}(M, \mathbb{Z}/4) \simeq \mathbb{Z}/2$. On the other hand, if $f \in \text{Hom}(\mathbb{Z}/4, \mathbb{Z}/2)$, then either $f(1) = 0$ or $f(1) = 1$. The first possibility is the trivial homomorphism and the second is just the g we defined above, which we already know is a non-trivial homomorphism, so we see that $\text{Hom}(\mathbb{Z}/4, M) \simeq \mathbb{Z}/2$.

Thus, we can reduce diagram (1):

$$0 \rightarrow \text{Hom}(M, \mathbb{Z}/2) \rightarrow \text{Hom}(M, \mathbb{Z}/4) \rightarrow \text{Hom}(M, \mathbb{Z}/2) \rightarrow 0$$

to

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow 0.$$

Now, this diagram cannot be exact. To see why, simply note that exactness would imply that the first $\mathbb{Z}/2 \rightarrow \mathbb{Z}/2$ is injective which means, since these groups are finite with the same cardinality, that it is also surjective, and so, to maintain exactness, the rightmost $\mathbb{Z}/2$ should be a 0.

Similarly, using the above information, we can reduce diagram (2):

$$0 \rightarrow \text{Hom}(\mathbb{Z}/2, M) \rightarrow \text{Hom}(\mathbb{Z}/4, M) \rightarrow \text{Hom}(\mathbb{Z}/2, M) \rightarrow 0$$

to

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow 0$$

which, as we've just seen, cannot be exact.

Now, consider $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/2$. Define $\phi : \mathbb{Z}/2 \times \mathbb{Z}/2 \rightarrow \mathbb{Z}/2$ by

$$(a, b) \mapsto ab.$$

Then, for $a_1, a_2, b_1, b_2 \in \mathbb{Z}/2$ and $c_1, c_2 \in \mathbb{Z}$,

$$\begin{aligned} \phi((c_1 a_1, b_1) + (c_2 a_2, b_1)) &= \phi(c_1 a_1 + c_2 a_2, b_1) = (c_1 a_1 + c_2 a_2) b_1 &= c_1 a_1 b_1 + c_2 a_2 b_1 \\ &= c_1 \phi(a_1, b_1) + c_2 \phi(a_2, b_1) \end{aligned}$$

and

$$\begin{aligned} \phi((a_1, c_1 b_1) + (a_1, c_2 b_2)) &= \phi(a_1, c_1 b_1 + c_2 b_2) = a_1 (c_1 b_1 + c_2 b_2) &= c_1 a_1 b_1 + c_2 a_1 b_2 \\ &= c_1 \phi(a_1, b_1) + c_2 \phi(a_1, b_2), \end{aligned}$$

so ϕ is bilinear and, hence, induces a homomorphism $\Phi : \mathbb{Z}/2 \otimes \mathbb{Z}/2 \rightarrow \mathbb{Z}/2$. Furthermore, if we define $\Psi : \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \otimes \mathbb{Z}/2$ by

$$a \mapsto 1 \otimes a,$$

then, for $a_1, a_2 \in \mathbb{Z}/2$,

$$\Psi(a_1 + a_2) = 1 \otimes (a_1 + a_2) = 1 \otimes a_1 + 1 \otimes a_2 = \Psi(a_1) + \Psi(a_2),$$

so Ψ is a homomorphism. Finally, for $a, b \in \mathbb{Z}/2$,

$$\Psi \circ \Phi(a \otimes b) = \Psi(ab) = 1 \otimes ab = a \otimes b$$

and

$$\Phi \circ \Psi(a) = \Phi(1 \otimes a) = a,$$

so we see that $\Phi \circ \Psi = Id$ and $\Psi \circ \Phi = Id$, so Φ is an isomorphism. Hence, $M \otimes \mathbb{Z}/2 \simeq \mathbb{Z}/2$.

Now, if we consider $\mathbb{Z}/2 \otimes \mathbb{Z}/4$, define $\phi : \mathbb{Z}/2 \times \mathbb{Z}/4 \rightarrow \mathbb{Z}/2$ by

$$(a, b) \mapsto ab.$$

Then, for $a_1, a_2 \in \mathbb{Z}/2$, $b_1, b_2 \in \mathbb{Z}/4$

$$\phi((a_1, b_1) + (a_2, b_1)) = \phi(a_1 + a_2, b_1) = (a_1 + a_2)b_1 = a_1b_1 + a_2b_1 = \phi(a_1, b_1) + \phi(a_2, b_1)$$

and

$$\phi((a_1, b_1) + (a_1, b_2)) = \phi(a_1, b_1 + b_2) = a_1(b_1 + b_2) = a_1b_1 + a_1b_2 = \phi(a_1, b_1) + \phi(a_1, b_2),$$

so ϕ is bilinear and so induces a homomorphism $\Phi : \mathbb{Z}/2 \otimes \mathbb{Z}/4 \rightarrow \mathbb{Z}/2$. Now, define $\Psi : \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \otimes \mathbb{Z}/4$ by

$$a \mapsto a \otimes 1.$$

Then, for $a_1, a_2 \in \mathbb{Z}/2$,

$$\Psi(a_1 + a_2) = (a_1 + a_2) \otimes 1 = a_1 \otimes 1 + a_2 \otimes 1 = \Psi(a_1) + \Psi(a_2)$$

so Ψ is a homomorphism. Furthermore, for $a \in \mathbb{Z}/2$, $b \in \mathbb{Z}/4$,

$$\Psi \circ \Phi(a \otimes b) = \Psi(ab) = ab \otimes 1 = a \otimes b$$

and

$$\Phi \circ \Psi(a) = \Phi(a \otimes 1) = a,$$

so $\Phi \circ \Psi = Id$ and $\Psi \circ \Phi = Id$, and so $\Phi : \mathbb{Z}/2 \otimes \mathbb{Z}/4 \rightarrow \mathbb{Z}/2$ is an isomorphism, from which we can conclude that $M \otimes \mathbb{Z}/4 \simeq \mathbb{Z}/2$. With these results in hand, then, we can reduce diagram (3):

$$0 \rightarrow M \otimes \mathbb{Z}/2 \rightarrow M \otimes \mathbb{Z}/4 \rightarrow M \otimes \mathbb{Z}/2 \rightarrow 0$$

to

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \rightarrow 0,$$

which we've seen is not exact.

Thus, we conclude that exactness of the original sequence does not imply exactness of the induced sequences. \square

3

(a): If R is a commutative ring, find an isomorphism $R \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}] \xrightarrow{\sim} R[x]/(x^2 - 2)$.

Answer: Define the map $\phi : R \times \mathbb{Z}[\sqrt{2}] \rightarrow R[x]/(x^2 - 2)$ by letting

$$(r, a + b\sqrt{2}) = r(a + bx).$$

If $r_1, r_2 \in R$ and $a, b, c, d, z_1, z_2 \in \mathbb{Z}$, then

$$\begin{aligned} \phi((z_1 r_1, a + b\sqrt{2}) + (z_2 r_2, a + b\sqrt{2})) &= \phi(z_1 r_1 + z_2 r_2, a + b\sqrt{2}) \\ &= (z_1 r_1 + z_2 r_2)(a + bx) \\ &= z_1 r_1(a + bx) + z_2 r_2(a + bx) \\ &= z_1 \phi(r_1, a + b\sqrt{2}) + z_2 \phi(r_2, a + b\sqrt{2}) \end{aligned}$$

and

$$\begin{aligned} \phi((r_1, z_1(a + b\sqrt{2})) + (r_1, z_2(c + d\sqrt{2}))) &= \phi(r_1, z_1 a + z_2 c + (z_1 b + z_2 d)\sqrt{2}) \\ &= r_1(z_1 a + z_2 c + (z_1 b + z_2 d)x) \\ &= z_1 r_1(a + bx) + z_2 r_1(c + dx) \\ &= z_1 \phi(r_1, a + b\sqrt{2}) + z_2 \phi(r_1, c + d\sqrt{2}), \end{aligned}$$

so we see that ϕ is bilinear. Hence, by the universal property of the tensor product, ϕ induces a unique module homomorphism $\Phi : R \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}] \rightarrow R[x]/(x^2 - 2)$ such that

$$\phi = \Phi \circ \pi$$

where $\pi : R \times \mathbb{Z}[\sqrt{2}] \rightarrow R \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ is the standard projection.

Furthermore, if $r_1, r_2 \in R$ and $a, b, c, d \in \mathbb{Z}$, then

$$\begin{aligned} \Phi((r_1 \otimes (a + b\sqrt{2}))(r_2 \otimes (c + d\sqrt{2}))) &= \Phi(r_1 r_2 \otimes (a + b\sqrt{2})(c + d\sqrt{2})) \\ &= \Phi(r_1 r_2 \otimes (ac + 2bd + (ad + bc)\sqrt{2})) \\ &= r_1 r_2 (ac + 2bd + (ad + bc)x) \\ &= r_1 r_2 (ac + bdx^2 + (ad + bc)x) \\ &= r_1 r_2 (a + bx)(c + dx) \\ &= r_1 (a + bx) r_2 (c + dx) \\ &= \Phi(r_1 \otimes (a + b\sqrt{2})) \Phi(r_2 \otimes (c + d\sqrt{2})) \end{aligned}$$

since $2 = x^2$ in $R[x]/(x^2 - 2)$, so Φ preserves the multiplicative structure of $R \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ and hence is, in fact, a \mathbb{Z} -algebra homomorphism.

Now, suppose $\phi(r, a + b\sqrt{2}) = 0$. Then

$$0 = \phi(r, a + b\sqrt{2}) = r(a + bx) = ar + brx.$$

Hence either $a = b = 0$ or $r = 0$; either way, this implies that $\pi(r, a + b\sqrt{2}) = r \otimes (a + b\sqrt{2}) = 0$, so Φ is injective.

On the other hand, suppose $f \in R[x]/(x^2 - 2)$. Then, since $x^2 = 2$ in $R[x]/(x^2 - 2)$, meaning each coset in $R[x]/(x^2 - 2)$ has at least

one representative of degree no greater than 1 (except, of course the zero coset, which has representative 0), we can assume, without loss of generality, that $f(x) = r + sx$ for some $r, s \in R$. Now,

$$\Phi(r \otimes 1 + s \otimes \sqrt{2}) = \Phi(r \otimes 1) + \Phi(s \otimes \sqrt{2}) = \phi(r, 1) + \phi(s, \sqrt{2}) = r + sx,$$

so we see that Φ is surjective. Therefore, since Φ is a bijective \mathbb{Z} -algebra homomorphism, it is an isomorphism. ♣

(b): Determine whether $\mathbb{Z}[\sqrt{3}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ are integral domains.

Answer: By part (a) above, we know that $\mathbb{Z}[\sqrt{3}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ is isomorphic to $\mathbb{Z}[\sqrt{3}][x]/(x^2 - 2)$, which, in turn, is isomorphic to $\mathbb{Z}[\sqrt{3}, \sqrt{2}]$, which is an integral domain.

On the other hand, again by part (a), we know that $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ is isomorphic to $\mathbb{Z}[\sqrt{2}][x]/(x^2 - 2)$. Now, $x + \sqrt{2}, x - \sqrt{2} \in \mathbb{Z}[\sqrt{2}][x]/(x^2 - 2)$ and

$$(x + \sqrt{2})(x - \sqrt{2}) = x^2 - 2 = 0$$

in $\mathbb{Z}[\sqrt{2}][x]/(x^2 - 2)$. Hence, $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ is not an integral domain. ♣

(c): Simplify each of the following \mathbb{Z} -modules (up to isomorphism): $\text{Hom}(\mathbb{Z}/10, \mathbb{Z})$, $\text{Hom}(\mathbb{Z}, \mathbb{Z}/10)$, $\text{Hom}(\mathbb{Z}/10, \mathbb{Z}/6)$, $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/10$, $\mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Z}/6$, $\mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Answer: $\text{Hom}(\mathbb{Z}/10, \mathbb{Z})$: Suppose $f : \mathbb{Z}/10 \rightarrow \mathbb{Z}$ is a \mathbb{Z} -module homomorphism (i.e. an abelian group homomorphism). Then $f(1)$ must have order dividing 10, since 1 has order 10 in $\mathbb{Z}/10$. The only element of \mathbb{Z} having finite order is 0, so we see that $f(1) = 0$ and so f must be the zero map. Hence, $\text{Hom}(\mathbb{Z}/10, \mathbb{Z}) \simeq 0$.

$\text{Hom}(\mathbb{Z}, \mathbb{Z}/10)$: Suppose $f : \mathbb{Z} \rightarrow \mathbb{Z}/10$ is a homomorphism. Then, since 1 generates \mathbb{Z} , f is completely determined by $f(1)$. Furthermore, since \mathbb{Z} has no torsion, there are no restrictions on $f(1)$, so $f(1)$ can be any element of $\mathbb{Z}/10$. Hence, $\text{Hom}(\mathbb{Z}, \mathbb{Z}/10) \simeq \mathbb{Z}/10$.

$\text{Hom}(\mathbb{Z}/10, \mathbb{Z}/6)$: Suppose $f : \mathbb{Z}/10 \rightarrow \mathbb{Z}/6$ is a homomorphism. Then, since 1 has order 10 in $\mathbb{Z}/10$, $f(1)$ must have order dividing 10 in $\mathbb{Z}/6$. The possible orders of elements of $\mathbb{Z}/6$ are 1, 2, 3, 6, so either $f(1) = 0$ or $f(1)$ has order 2. If $f(1) = 0$, then f is the zero map. Now, there are two elements of $\mathbb{Z}/6$ of order 2, 2 and 4. Clearly, $f(1) = 2$ and $f(1) = 4$ determine different non-zero homomorphisms, so we see that $\text{Hom}(\mathbb{Z}/10, \mathbb{Z}/6)$ has exactly 3 elements. The only \mathbb{Z} -module (abelian group) with three elements is isomorphic to $\mathbb{Z}/3$, so we see that $\text{Hom}(\mathbb{Z}/10, \mathbb{Z}/6) \simeq \mathbb{Z}/3$.

$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/10$: Define $\phi : \mathbb{Z} \times \mathbb{Z}/10 \rightarrow \mathbb{Z}/10$ by

$$(a, b) \mapsto ab.$$

Then, if $a_1, a_2, c_1, c_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}/10$,

$$\begin{aligned}\phi((c_1a_1, b_1) + (c_2a_2, b_1)) &= \phi(c_1a_1 + c_2a_2, b_1) = (c_1a_1 + c_2a_2)b_1 \\ &= c_1a_1b_1 + c_2a_2b_1 \\ &= c_1\phi(a_1, b_1) + c_2\phi(a_2, b_1)\end{aligned}$$

and

$$\begin{aligned}\phi((a_1, c_1b_1) + (a_1, c_2b_2)) &= \phi(a_1, c_1b_1 + c_2b_2) \\ &= a_1(c_1b_1 + c_2b_2) \\ &= c_1a_1b_1 + c_2a_1b_2 \\ &= c_1\phi(a_1, b_1) + c_2\phi(a_1, b_2),\end{aligned}$$

so ϕ is bilinear and so induces a homomorphism $\Phi : \mathbb{Z} \otimes \mathbb{Z}/10 \rightarrow \mathbb{Z}/10$.

Now, define $\Psi : \mathbb{Z}/10 \rightarrow \mathbb{Z} \otimes \mathbb{Z}/10$ by

$$b \mapsto 1 \otimes b.$$

Then, if $c_1, c_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}/10$,

$$\Psi(c_1b_1 + c_2b_2) = 1 \otimes (c_1b_1 + c_2b_2) = 1 \otimes c_1b_1 + 1 \otimes c_2b_2 = c_1(1 \otimes b_1) + c_2(1 \otimes b_2) = c_1\Psi(b_1) + c_2\Psi(b_2),$$

so Ψ is a homomorphism. Now, if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}/10$, then

$$\Psi \circ \Phi(a \otimes b) = \Psi(ab) = 1 \otimes ab = a \otimes b$$

and

$$\Phi \circ \Psi(b) = \Phi(1 \otimes b) = b,$$

so $\Psi \circ \Phi = id$ and $\Phi \circ \Psi = id$, so Φ is an isomorphism. Thus, we conclude that $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/10 \simeq \mathbb{Z}/10$.

$\mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Z}/6$: Define $\phi : \mathbb{Z}/10 \times \mathbb{Z}/6 \rightarrow \mathbb{Z}/2$ by

$$(a, b) \mapsto ab.$$

Then, if $a_1, a_2 \in \mathbb{Z}/10$, $b_1, b_2 \in \mathbb{Z}/6$ and $c_1, c_2 \in \mathbb{Z}$,

$$\begin{aligned}\phi((c_1a_1, b_1) + (c_2a_2, b_1)) &= \phi(c_1a_1 + c_2a_2, b_1) = (c_1a_1 + c_2a_2)b_1 \\ &= c_1a_1b_1 + c_2a_2b_1 \\ &= c_1\phi(a_1, b_1) + c_2\phi(a_2, b_1)\end{aligned}$$

and

$$\begin{aligned}\phi((a_1, c_1b_1) + (a_1, c_2b_2)) &= \phi(a_1, c_1b_1 + c_2b_2) = a_1(c_1b_1 + c_2b_2) \\ &= c_1a_1b_1 + c_2a_1b_2 \\ &= c_1\phi(a_1, b_1) + c_2\phi(a_1, b_2),\end{aligned}$$

so ϕ is bilinear and so induces a homomorphism $\Phi : \mathbb{Z}/10 \otimes \mathbb{Z}/6 \rightarrow \mathbb{Z}/2$. Now, define $\Psi : \mathbb{Z}/2 \rightarrow \mathbb{Z}/10 \otimes \mathbb{Z}/6$ by

$$a \mapsto 1 \otimes a.$$

Then, if $a, b \in \mathbb{Z}/2$, $c_1, c_2 \in \mathbb{Z}$,

$$\Psi(c_1a + c_2b) = 1 \otimes (c_1a + c_2b) = 1 \otimes c_1a + 1 \otimes c_2b = c_1\Psi(a) + c_2\Psi(b),$$

so Ψ is a homomorphism. Note that $a \otimes b = 1 \otimes ab$ and that

$$\begin{aligned} 1 \otimes 0 &= 0 \\ 1 \otimes 1 &= 1 \otimes 1 \\ 1 \otimes 2 &= 1 \otimes 20 = 20 \otimes 1 = 0 \otimes 1 = 0 \\ 1 \otimes 3 &= 1 \otimes 21 = 21 \otimes 1 = 1 \otimes 1 \\ 1 \otimes 4 &= 1 \otimes 10 = 10 \otimes 1 = 0 \otimes 1 = 0 \\ 1 \otimes 5 &= 1 \otimes 11 = 11 \otimes 1 = 1 \otimes 1. \end{aligned}$$

so we see that either $a \otimes b = 0$ or $a \otimes b = 1 \otimes 1$.

Then

$$\Phi \circ \Psi(a) = \Phi(a \otimes a) = a^2 = a$$

since $0^2 = 0$ and $1^2 = 1$ and

$$\Psi \circ \Phi(a \otimes b) = \Psi(ab) = 1 \otimes a = a \otimes b$$

by the argument given above, so Ψ and Φ are inverses and so $\Phi : \mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Z}/6 \rightarrow \mathbb{Z}/2$ is an isomorphism

$\mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Q}$: Suppose $a \otimes \frac{p}{q} \in \mathbb{Z}/10 \otimes \mathbb{Q}$. Then $\frac{p}{q} = \frac{10p}{10q}$, so

$$a \otimes \frac{p}{q} = a \otimes \frac{10p}{10q} = 10a \otimes \frac{p}{10q} = 0 \otimes \frac{p}{10q} = 0,$$

so $\mathbb{Z}/10 \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$: Suppose $\frac{a}{b} \otimes \frac{p}{q} \in \mathbb{Q} \otimes \mathbb{Q}$. Then

$$\frac{a}{b} \otimes \frac{p}{q} = \frac{aq}{bp} \otimes \frac{p}{q} = \frac{p}{bpq} \otimes ap = \frac{ap^2}{bpq} \otimes 1 = \frac{ap}{bq} \otimes 1.$$

Define $\phi : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ by

$$\left(\frac{a}{b}, \frac{p}{q} \right) \mapsto \frac{ap}{bq}.$$

Then, if $a_1, a_2, b_1, b_2, c_1, c_2, p_1, p_2, q_1, q_2 \in \mathbb{Z}$,

$$\begin{aligned} \phi \left(\left(c_1 \frac{a_1}{b_1}, \frac{p_1}{q_1} \right) + \left(c_2 \frac{a_2}{b_2}, \frac{p_2}{q_2} \right) \right) &= \phi \left(\frac{c_1 a_1}{b_1} + \frac{c_2 a_2}{b_2}, \frac{p_1}{q_1} \right) = \left(\frac{c_1 a_1}{b_1} + \frac{c_2 a_2}{b_2} \right) \frac{p_1}{q_1} \\ &= c_1 \frac{a_1 p_1}{b_1 q_1} + c_2 \frac{a_2 p_1}{b_2 q_1} \\ &= c_1 \phi \left(\frac{a_1}{b_1}, \frac{p_1}{q_1} \right) + c_2 \phi \left(\frac{a_2}{b_2}, \frac{p_1}{q_1} \right) \end{aligned}$$

and similarly for the other term, so we see that ϕ is bilinear and, hence, induces a homomorphism $\Phi : \mathbb{Q} \otimes \mathbb{Q} \rightarrow \mathbb{Q}$. Now, define $\Psi : \mathbb{Q} \rightarrow \mathbb{Q} \otimes \mathbb{Q}$ by

$$\frac{a}{b} \mapsto \frac{a}{b} \otimes 1.$$

Then, for $a, b, p, q, c_1, c_2 \in \mathbb{Z}$,

$$\Psi \left(c_1 \frac{a}{b} + c_2 \frac{p}{q} \right) = \left(c_1 \frac{a}{b} + c_2 \frac{p}{q} \right) \otimes 1 = c_1 \frac{a}{b} \otimes 1 + c_2 \frac{p}{q} \otimes 1 = c_1 \Psi \left(\frac{a}{b} \right) + c_2 \Psi \left(\frac{p}{q} \right),$$

so Ψ is a homomorphism. Now, for $a, b, p, q \in \mathbb{Z}$,

$$\Psi \circ \Phi \left(\frac{a}{b} \otimes \frac{p}{q} \right) = \Psi \left(\frac{ap}{bq} \right) = \frac{ap}{bq} \otimes 1 = \frac{ap^2}{bpq} \otimes 1 = \frac{p}{bpq} \otimes ap = \frac{p}{bpq} \otimes aq \frac{p}{q} = \frac{aq p}{bp q} \otimes \frac{p}{q} = \frac{a}{b} \otimes \frac{p}{q}$$

and

$$\Phi \circ \Psi \left(\frac{a}{b} \right) = \Phi \left(\frac{a}{b} \otimes 1 \right) = \frac{a}{b}.$$

Hence, Φ and Ψ are inverses, and so $\Phi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{Q}$ is an isomorphism.



4

Let R be the ring of real polynomial functions on the circle $x^2 + y^2 = 25$. Let P be the point $(3, 4)$, and let I be the ideal of functions in R vanishing at P .

(a): Show that I is generated by the elements $x - 3, y - 4$.

Proof. Note that $R = \mathbb{R}[x, y]/(x^2 + y^2 - 25)$. Let $f \in I$. Then we can view f as an element of $\mathbb{R}[x, y] = \mathbb{R}[x][y]$. Hence, since f vanishes at $(3, 4)$, there exist $p, r \in \mathbb{R}[x][y]$ such that

$$f(x, y) = f(x)(y) = (y - 4)q(x)(y) + r(x)(y)$$

such that the degree of r as a polynomial in y is less than $1 = \deg(y - 4)$; that is, $r(x)(y)$ is a polynomial purely in x , so we can simply notate it as $r(x)$. Now,

$$0 = f(3, 4) = (4 - 4)q(3, 4) + r(3) = r(3),$$

so $x = 3$ is a zero of r , and so

$$r(x) = (x - 3)p(x) + \tilde{r}(x),$$

where $\deg(\tilde{r}(x)) < \deg(x - 3) = 1$, so \tilde{r} is a constant, which we denote simply by c . Furthermore, since

$$0 = r(3) = (3 - 3)p(3) + c = c,$$

we see that, in fact,

$$f(x, y) = (y - 4)q(x, y) + (x - 3)r(x).$$

Since our choice of $f \in I$ was arbitrary, we conclude that $x - 3$ and $y - 4$ generate I . \square

(b): Show that if $I = (f)$ where $f \in R$, then f divides $x - 3$ and $y - 4$ in R . Deduce that f cannot vanish at any point of the circle except for P . Also, deduce that f cannot vanish to order ≥ 2 at P , as a function on the circle.

Proof. If $I = (f)$ for some $f \in R$, then, for all $g \in I$, $g(x, y) = f(x, y)h(x, y)$ for some $h \in R$. Hence, since $x - 3, y - 4 \in I$, certainly it must be the case that f divides both $x - 3$ and $y - 4$.

Now, $x - 3$ vanishes only for those (x, y) on the circle such that $x = 3$. Since the circle is defined by the equation $x^2 + y^2 = 25$, we see that the only such points on the circle occur when

$$y = \pm\sqrt{25 - 3^2} = \pm\sqrt{16} = \pm 4,$$

so the only points on the circle where $x - 3$ vanishes are $(3, \pm 4)$. Similarly, $y - 4$ vanishes only when

$$x = \pm\sqrt{25 - 4^2} = \pm\sqrt{9} = \pm 3;$$

that is, the points $(\pm 3, 4)$. Now, since f divides both $x - 3$ and $y - 4$, both these functions must vanish at all the points that f does. Hence, f can vanish only at points in the intersection

$$\{(3, 4), (3, -4)\} \cap \{(3, 4), (-3, 4)\} = \{(3, 4)\}$$

so $(3, 4)$ is the only point on the circle at which f can vanish (and, of course, to be in I it must vanish at this point).

Similarly, if f vanishes at $(3, 4)$ to order ≥ 2 , then all multiples of f must vanish to order ≥ 2 as well. However, since $x - 3$ and $y - 4$ vanish only to order 1, we see that f cannot vanish to order ≥ 2 at P as a function on the circle. \square

(c): Deduce that I cannot be principal.

Proof. Suppose $I = (f)$ and let $F(x, y) \in \mathbb{R}[x, y]$ represent f . Consider the zero locus of F ; i.e., the graph of $F(x, y) = 0$. This will be some curve in the plane; since f vanishes at P , it must be the case that F does as well, so the graph of $F(x, y) = 0$ must intersect the circle in at least one point, namely P . This curve can then either be transversal to P or tangent to P . If it is transversal to P , then the curve must enter the circle and must, therefore, exit the circle at some point. If it exits the circle at some point other than P , then F vanishes at that other point, and so f must as well. However, as we argued in (b) above, f cannot vanish at any point of the circle other than P , so this is impossible. If the curve exits the circle at the same point P that it entered, then this means that F , and hence f , must vanish to order ≥ 2 at P . However, we demonstrated in (b) that this is also impossible.

Hence, we see that the curve that is the graph of $F(x, y) = 0$ must be tangent to the circle at P . \square

(d): Show that no two elements in I are linearly independent over the ring R .

Proof. Suppose $f, g \in I$. Then, since f and g are also, thereby, elements of R , we simply note that

$$fg - gf = 0,$$

is a linear combination of f and g with coefficients in R . Therefore, since our choice of f and g was arbitrary, we conclude that no two elements of I are linearly independent. \square

(e): Using (c) and (d), conclude that I is not a free R -module.

Proof. By part (c), we know that I is not principal, and so, if it has a basis, the basis must have cardinality ≥ 2 . However, by part (d), we know that any set containing more than one element must be linearly dependent, and so we conclude that I has no basis and, hence, is not a free R -module. \square

5

In the notation of problem 4, let Q be the point $(-3, 4)$ and let J be the ideal of functions in R vanishing at Q . Consider the R -module $I \oplus J$.

(a): Show that every element $(i, j) \in I \oplus J$ can be uniquely expressed in the form

$$((x - 3)f + (y - 4)g, (x + 3)f + (y - 4)g),$$

for some $f, g \in R$.

Proof. Let $(i, j) \in I \oplus J$. Then, since $i \in I$, 4(a) above demonstrates that there exist $f, g \in R$ such that

$$i = (x - 3)f + (y - 4)g.$$

Now, we want to show that j can be uniquely expressed as $j = (x + 3)f + (y - 4)g$. Showing this is equivalent to showing that the system

$$\begin{aligned} (x - 3)f + (y - 4)g &= i \\ (x + 3)f + (y - 4)g &= j \end{aligned}$$

has a unique solution. Subtracting the two equations, we get

$$-6f = i - j,$$

or $f = \frac{j-i}{6}$, which is certainly in R since j and i are. Now, adding the equations in the above system yields

$$i + j = 2xf + 2(y - 4)g = 2x \left(\frac{j - i}{6} \right) + 2(y - 4)g,$$

so

$$2(y - 4)g = i + j - 2x \left(\frac{j - i}{6} \right) = \frac{6 + 2x}{6}i + \frac{6 - 2x}{6}j = \frac{3 + x}{3}i + \frac{3 - x}{3}j.$$

Now, *a priori*, it's not at all clear that we can divide both sides by $2(y-4)$ as we would like; to justify doing so, we need to demonstrate that $\frac{3+x}{y-4}i$ and $\frac{3-x}{y-4}j$ are in R . To that end:

$$\begin{aligned}
\frac{x+3}{y-4}i &= \frac{x+3}{y-4}((x-3)f + (y-4)g) \\
&= \frac{x^2-9}{y-4}f + \frac{(x+3)(y-4)}{y-4}g \\
&= \frac{16-y^2}{y-4}f + (x+3)g \\
&= \frac{-(y-4)(y+4)}{y-4}f + (x+3)g \\
&= -(y+4)f + (x+3)g,
\end{aligned}$$

which is indeed in R .

On the other hand, a similar argument to that given in 4(a) demonstrates that $x+3$ and $y-4$ generate J , so there exist $h, k \in R$ such that $j = (x+3)h + (y-4)k$. Hence

$$\begin{aligned}
\frac{3-x}{y-4}j &= \frac{3-x}{y-4}((x+3)h + (y-4)k) \\
&= \frac{9-x^2}{y-4}h + (3-x)k \\
&= \frac{y^2-16}{y-4}h + (3-x)k \\
&= (y+4)h + (3-x)k,
\end{aligned}$$

which is also in R . Hence, we see that dividing by $2(y-4)$ is indeed legitimate, so

$$g = \frac{3+x}{6(y-4)}i + \frac{3-x}{6(y-4)}j.$$

Now, note that, if we actually plug in these values of f and g ,

$$\begin{aligned}
(x-3)f + (y-4)g &= (x-3)\left(\frac{j-i}{6}\right) + (y-4)\left(\frac{3+x}{6(y-4)}i + \frac{3-x}{6(y-4)}j\right) \\
&= \frac{(x-3)(y-4)(j-i)}{6(y-4)} + \frac{(y-4)(x+3)i + (y-4)(3-x)j}{6(y-4)} \\
&= \frac{6i}{6} \\
&= i
\end{aligned}$$

and

$$\begin{aligned}
 (x+3)f + (y-4)g &= (x+3) \left(\frac{j-i}{6} \right) + (y-4) \left(\frac{3+x}{6(y-4)}i + \frac{3-x}{6(y-4)}j \right) \\
 &= \frac{(x+3)(y-4)(j-i)}{6(y-4)} + \frac{(y-4)(x+3)i + (y-4)(3-x)j}{6(y-4)} \\
 &= \frac{6j}{6} \\
 &= j,
 \end{aligned}$$

so (i, j) can indeed be expressed as

$$((x-3)f + (y-4)g, (x+3)f + (y-4)g).$$

Furthermore, since f and g were completely determined as solutions of the original system of equations, we see that this expression for (i, j) is unique. \square

(b): Show conversely that every element of $R \times R$ of the above form must lie in $I \oplus J$.

Proof. Suppose $(a, b) = ((x-3)f + (y-4)g, (x+3)f + (y-4)g) \in R \times R$ for some $f, g \in R$. Then a, b, f and g can be represented by $A(x, y), B(x, y), F(x, y), G(x, y) \in \mathbb{R}[x, y]$ and

$$A(3, 4) = (3-3)F(3, 4) + (4-4)G(3, 4) = 0,$$

$$B(-3, 4) = (-3+3)F(-3, 4) + (4-4)G(-3, 4) = 0,$$

so A vanishes at $(3, 4)$ and B vanishes at $(-3, 4)$ and, hence, $a \in I$ and $b \in J$. Hence, $(a, b) \in I \oplus J$. \square

(c): Deduce that $I \oplus J$ is a free R -module of rank 2, even though I is not free.

Proof. Parts (a) and (b) demonstrate that $I \oplus J$ consists precisely of elements of the form

$$((x-3)f + (y-4)g, (x+3)f + (y-4)g)$$

for some $f, g \in R$ and that each element of $I \oplus J$ can be uniquely expressed as such; hence, $(x-3, x+3)$ and $(y-4, y-4)$ form a basis for $I \oplus J$. Therefore, $I \oplus J$ is a free R -module of rank 2 even though I is not free. \square