SOLUCIONES A LA TAREA 1

1. Sea $n \geq 2$ un natural. En este ejercicio consideramos a $\mathbb{Z}/n$ como anillo con la suma y producto de representantes.

(a) Sea M un grupo abeliano. Demuestra que M tiene una estructura de $\mathbb{Z}/n$–módulo izquierdo con la suma que ya tiene si y solo si $nm = 0$ para todo $m \in M$. Además, prueba que si M tiene tal estructura, entonces es única.

Solución:

Supongamos primero que M es un grupo abeliano que satisface $nm = 0$ para todo $m \in M$. Definimos

$$[k]_n \cdot m = km$$

Está bien definida pues si $[k]_n = [k']_n$, entonces $k - k' = rn$ y entonces

$$km = (k' + rn)m = k'm + rnm = k'm$$

pues $rnm = 0$. Notemos que el producto escalar por elementos de $\mathbb{Z}/n$ está definido mediante el producto escalar por elementos de $\mathbb{Z}$ que ya cumple los axiomas de módulo. Además el producto escalar por la suma de dos elementos de $\mathbb{Z}/n$ corresponde al producto escalar por la suma de los representantes, y lo mismo para el producto de elementos de $\mathbb{Z}/n$. Por último, el producto escalar por $[1]_n$ es el producto escalar por 1. Como los axiomas de módulo se cumplen para el producto escalar por elementos de $\mathbb{Z}$, también se cumplen para el producto escalar por elementos de $\mathbb{Z}/n$. Así que M es un $\mathbb{Z}/n$–módulo con la suma que ya tenía y este producto escalar que definimos.

Por otra parte, si M es un $\mathbb{Z}/n$–módulo izquierdo con la suma que ya tenía M, en particular es un grupo abeliano. Pero además

$$nm = m + \ldots + m = [1]_n m + \ldots + [1]_n m = ([1]_n + \ldots + [1]_n)m = [n]_n m = [0]_n m = 0$$

como queríamos probar.

Por último supongamos que M tiene dos estructuras de $\mathbb{Z}/n$–módulo izquierdo, pero con la misma suma, la que ya tenía M. Denotemos $[k]_n \cdot m$ y $[k]_n \star m$ a los dos productos escalares.

$$\begin{aligned}
[k]_n \cdot m &= ([1]_n + \ldots + [1]_n) \cdot m \\
&= [1]_n \cdot m + \ldots + [1]_n \cdot m \\
&= m + \ldots + m \\
&= [1]_n \star m + \ldots + [1]_n \star m \\
&= ([1]_n + \ldots + [1]_n) \star m \\
&= [k]_n \star m
\end{aligned}$$

Luego el producto escalar es único. Además notemos que en esta demostración se prueba que $[k]_n \cdot m = km$. □

(b) Enuncia y demuestra un teorema de clasificación de $\mathbb{Z}/n$–módulos finitamente generados.

Solución:

Sea M un $\mathbb{Z}/n$–módulo finitamente generado. Por el ejercicio anterior, es un grupo abeliano tal que $nm = 0$ para todo $m \in M$. Como M es finitamente generado como $\mathbb{Z}/n$–módulo, existe $X = \{m_1, \ldots, m_k\} \subseteq M$ tal que M está generado por X como $\mathbb{Z}/n$–módulo. Es decir, dado $m \in M$, existen $[r_1]_n, \ldots, [r_k]_n \in \mathbb{Z}/n$ tales que

$$m = [r_1]_n m_1 + \ldots + [r_k]_n m_k = r_1 m_1 + \ldots + r_k m_k$$

donde la segunda igualdad se cumple porque en la demostración de la parte (a) vimos que $[r]_n \cdot m = rm$. Pero esto muestra que M es finitamente generado como grupo abeliano. Así que podemos aplicar la clasificación de grupos abelianos finitamente generados de donde

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/s_1 \oplus \ldots \oplus \mathbb{Z}/s_j$$

para cierto $r \in \mathbb{N}$ y enteros $2 \leq s_1 \mid s_2 \mid \ldots \mid s_j$. Claro, esto es un isomorfismo de grupos abelianos nada más. Ahora $\mathbb{Z}^r$ no puede ser un $\mathbb{Z}/n$–módulo si $r > 0$, porque $n(1, \ldots, 1) = (n, \ldots, n) \neq (0, \ldots, 0)$. Por otra parte, si $\mathbb{Z}/s$ es un $\mathbb{Z}/n$–módulo, se debe cumplir

$$0 = n[1]_s = [n]_s$$

de donde s divide a n. Así que los s_i que aparecen en la descomposición deben dividir a n. Ahora podemos enunciar nuestro candidato a teorema de clasificación de $\mathbb{Z}/n$–módulos finitamente generados.

Teorema: Sea M un $\mathbb{Z}/n$–módulo finitamente generado. Entonces existen enteros $2 \leq s_1 \mid s_2 \mid \ldots \mid s_j \mid n$ tales que

$$M \cong \mathbb{Z}/s_1 \oplus \ldots \oplus \mathbb{Z}/s_j$$

Además esta descomposición es única.

Demostración: Por el argumento del párrafo anterior, existen enteros $2 \leq s_1 \mid s_2 \mid \ldots \mid s_j \mid n$ tales que

$$M \cong \mathbb{Z}/s_1 \oplus \ldots \oplus \mathbb{Z}/s_j$$

como grupos. Pero de hecho, si f es un isomorfismo de grupos entre dos $\mathbb{Z}/n$–módulos, se cumple

$$f([k]_n m) = f(km) = kf(m) = [k]_n f(m)$$

así que es un isomorfismo de $\mathbb{Z}/n$–módulos. Para la unicidad, si $\mathbb{Z}/s_1 \oplus \ldots \oplus \mathbb{Z}/s_j \cong \mathbb{Z}/r_1 \oplus \ldots \oplus \mathbb{Z}/r_i$ como $\mathbb{Z}/n$–módulos para otros enteros $2 \leq r_1 \mid \ldots \mid r_i \mid n$, en particular son isomorfos como grupos abelianos. Por la unicidad en el teorema de clasificación de grupos abelianos finitamente generados, obtenemos $j = i$ y $s_k = r_k$ para todo k. $\square$

2. Calcula los grupos de homología del complejo de grupos abelianos

$$\ldots \longrightarrow 0 \longrightarrow \mathbb{Z}^3 \xrightarrow{\partial_2} \mathbb{Z}^4 \xrightarrow{\partial_1} \mathbb{Z}^2 \longrightarrow 0 \longrightarrow \ldots$$

donde $\partial_2(x, y, z) = (x - y, 4x + 3y - z, 9y + 3z, 3x + 13y + 2z)$ y $\partial_1(x, y, z, w) = (y + z - x - w, -2x + 2y + 2z - 2w)$.

Solución:

Llamémosle C_* a este complejo. Puesto que hay ceros en esas posiciones, obtenemos $H_n(C_*) = 0$ si $n < 0$ ó $n > 2$. Vemos que

$$\partial_1(1, 0, 0, 0) = \partial_1(0, 0, 0, 1) = (-1, -2) \qquad \partial_1(0, 1, 0, 0) = \partial_1(0, 0, 1, 0) = (1, 2)$$

así que

$$H_0(C_*) = \frac{\mathbb{Z}^2}{\mathbb{Z}(1, 2)} = \frac{\mathbb{Z}(0, 1) \oplus \mathbb{Z}(1, 2)}{\mathbb{Z}(1, 2)} \cong \mathbb{Z}$$

Ahora vamos a calcular $H_1(C_*)$. Por otra parte, (x, y, z, w) está en $\mathrm{Ker}(\partial_1)$ si y solo si

$$y + z - x - w = 0 \qquad -2x - 2y + 2z - 2w = 0$$

y esto se cumple si y solo si $w = y + z - x$. Por lo tanto

$$(x, y, z, w) = (x, y, z, y + z - x) = x(1, 0, 0, -1) + y(0, 1, 0, 1) + z(0, 0, 1, 1)$$

Por otra parte, la imagen de ∂_2 está generada por las imágenes de $(1, 0, 0)$, $(0, 1, 0)$ y $(0, 0, 1)$, que son

$$(1, 4, 0, 3), (-1, 3, 9, 13), (0, -1, 3, 2)$$

Sean $v_1 = (1, 0, 0, -1)$, $v_2 = (0, 1, 0, 1)$ y $v_3 = (0, 0, 1, 1)$. Usaremos esta base para $\mathrm{Ker}(\partial_1)$. Además se tiene

$$\begin{aligned} (1, 4, 0, 3) &= v_1 + 4v_2 \\ (-1, 3, 9, 13) &= -v_1 + 3v_2 + 9v_3 \\ (0, -1, 3, 2) &= -v_2 + 3v_3 \end{aligned}$$

Vemos que $\mathrm{Im}(\partial_2) + \langle v_3 \rangle = \mathrm{Ker}(\partial_1)$, pues $v_2 = 3v_3 - (0, -1, 3, 2)$ y

$$v_1 = (1, 4, 0, 3) - 4v_2 = (1, 4, 0, 3) - 12v_3 + 4(0, -1, 3, 2)$$

Sea $A = \mathrm{Im}(\partial_2)$ y $B = \langle v_3 \rangle$. Entonces por el segundo teorema de isomorfismo

$$H_1(C_*) = \frac{\mathrm{Ker}(\partial_1)}{\mathrm{Im}(\partial_2)} = \frac{A + B}{A} \cong \frac{B}{A \cap B}$$

Si $x \in A \cap B$, se tiene

$$x = \lambda v_3 = a(v_1 + 4v_2) + b(-v_1 + 3v_2 + 9v_3) + c(-v_2 + 3v_3)$$

de donde

$$\begin{aligned} a - b &= 0 \\ 4a + 3b - c &= 0 \\ \lambda &= 9b + 3c \end{aligned}$$

Despejando, tenemos $a = b$, luego $c = 7b$ y entonces $\lambda = 30b$. Es decir, $x = 30bv_3 \in 30\mathbb{Z}v_3$ por lo tanto $A \cap B \subseteq 30\mathbb{Z}v_3$. Por otra parte, se tiene claramente que $30v_3 \in B$ y

$$30v_3 = (v_1 + 4v_2) + (-v_1 + 3v_2 + 9v_3) + 7(-v_2 + 3v_3) \in \mathrm{Im}(\partial_2) = A$$

así que $A \cap B = 30\mathbb{Z}v_3$. Por lo tanto

$$H_1(C_*) \cong \frac{B}{A \cap B} = \frac{\mathbb{Z}v_3}{30\mathbb{Z}v_3} \cong \mathbb{Z}/30$$

Por último debemos calcular

$$H_2(C_*) = \mathrm{Ker}(\partial_2)$$

El elemento (x, y, z) está en el núcleo de ∂_2 si y solo si

$$\begin{aligned} x - y &= 0 \\ 4x + 3y - z &= 0 \\ 9y + 3z &= 0 \\ 3x + 13y + 2z &= 0 \end{aligned}$$

de donde obtenemos $x = y$ de la primera ecuación, después $z = 7x$ de la segunda y $z = -3y$ de la tercera. Igualando obtenemos

$$7x = -3y = -3x \Rightarrow 10x = 0 \Rightarrow x = 0$$

así que el núcleo de ∂_2 es trivial. Para resumir

$$H_n(C_*) \cong \begin{cases} 0 & \text{si } n < 0 \text{ ó } n \geq 2 \\ \mathbb{Z} & \text{si } n = 0 \\ \mathbb{Z}/30 & \text{si } n = 1 \end{cases}$$

y con esto concluimos el ejercicio. □

También podríamos haber calculado $H_1(C_*)$ usando el algoritmo de Smith, ya que lo que queremos calcular

$$\frac{\mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \mathbb{Z}v_3}{\mathbb{Z}(v_1 + 4v_2) + \mathbb{Z}(-v_1 + 3v_2 + 9v_3) + \mathbb{Z}(-v_2 + 3v_3)}$$

coincide con el conúcleo del homomorfismo $f\colon \mathbb{Z}^3 \to \mathbb{Z}^3$ que está únicamente determinado por

$$\begin{aligned} f(1, 0, 0) &= (1, 4, 0) \\ f(0, 1, 0) &= (-1, 3, 9) \\ f(0, 0, 1) &= (0, -1, 3) \end{aligned}$$

es decir, $f(n, m, k) = (n - m, 4n + 3m - k, 9m + 3k)$. Aplicamos ahora el algoritmo

$$\begin{pmatrix} 1 & -1 & 0 \\ 4 & 3 & -1 \\ 0 & 9 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 & 0 \\ 0 & 7 & -1 \\ 0 & 9 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & -1 \\ 0 & 9 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & -1 \\ 0 & 30 & 0 \end{pmatrix} \mapsto$$

$$\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 30 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 30 \end{pmatrix}$$

Con lo cual

$$H_1(C_*) \cong \frac{\mathbb{Z}w_1 \oplus \mathbb{Z}w_2 \oplus \mathbb{Z}w_3}{\mathbb{Z}w_1 \oplus \mathbb{Z}(-w_2) \oplus \mathbb{Z}(30w_3)} \cong \mathbb{Z}/30$$

3. Sea $R = \mathbb{Z}[X]$. Podemos ver a $\mathbb{Z}/2$ como R–módulo mediante la operación $p(x)\cdot[n]_2 = [p(0)n]_2$. Calcula la homología del complejo de R–módulos

$$\dots \longrightarrow 0 \longrightarrow \mathbb{Z}[X] \xrightarrow{\partial_3} \mathbb{Z}[X]^2 \xrightarrow{\partial_2} \mathbb{Z}[X] \xrightarrow{\partial_1} \mathbb{Z}/2 \longrightarrow 0 \longrightarrow \dots$$

donde $\partial_3(p(x)) = (xp(x), 2p(x))$, $\partial_2(p(x), q(x)) = 2p(x) - xq(x)$ y $\partial_1(p(x)) = [p(0)]_2$.

Solución:

Sea C_* este complejo. Puesto que $C_n = 0$ si $n < 0$ ó $n > 3$, tenemos que $H_n(C_*) = 0$ si $n < 0$ ó $n > 3$. Vemos que ∂_1 es sobreyectivo, pues

$$\partial_1(0) = [0]_2 \qquad \partial_1(1) = [1]_2$$

así que

$$H_0(C_*) = \frac{\mathbb{Z}/2}{\mathrm{Im}(\partial_1)} = 0$$

Ahora calculemos en dimensión uno. Por una parte, $p(x) \in \mathrm{Ker}(\partial_1)$ si y solo si $p(0)$ es par. Entonces

$$p(x) = xq(x) + 2m$$

donde $q(x) \in \mathbb{Z}[X]$ y $m \in \mathbb{Z}$. Luego $\mathrm{Ker}(\partial_1) \subseteq \langle x, 2\rangle$. Pero también x y 2 están en el núcleo de ∂_1, luego $\mathrm{Ker}(\partial_1) = \langle x, 2\rangle$. Por otra parte

$$\partial_2(p(x), q(x)) = 2p(x) - xq(x) \in \langle 2, x\rangle$$

es decir, $\mathrm{Im}(\partial_2) \subseteq \langle 2, x\rangle$. También se tiene $2 = \partial_2(1, 0)$ y $x = \partial_2(0, -1)$, luego $\mathrm{Im}(\partial_2) = \langle 2, x\rangle$. Por lo tanto

$$H_1(C_*) = 0$$

Pasemos a dimensión dos. El elemento $(p(x), q(x))$ está en el núcleo de ∂_2 si y solo si $2p(x) = xq(x)$. Como $2p(0) = 0q(0) = 0$, el coeficiente de x^0 en $p(x)$ es 0 y por lo tanto

$p(x) = xr(x)$ para algún $r(x) \in \mathbb{Z}[X]$. También de esa igualdad vemos que todos los coeficientes de $q(x)$ son pares, es decir, $q(x) = 2s(x)$ para algún $s(x) \in \mathbb{Z}[X]$. Entonces

$$2xr(x) = 2xs(x)$$

Como $\mathbb{Z}[X]$ es un dominio y $2x \neq 0$, se tiene $r(x) = s(x)$, es decir,

$$(p(x), q(x)) = (xr(x), 2r(x)) = \partial_3(r(x))$$

Esto prueba que $\operatorname{Ker}(\partial_2) \subseteq \operatorname{Im}(\partial_3)$. Puesto que C_* es un complejo, la otra inclusión se cumple automáticamente y entonces tenemos

$$H_2(C_*) = 0$$

Por último, tenemos que $p(x)$ está en el núcleo de ∂_3 si y solo si $xp(x) = 0$ y $2p(x) = 0$. Como $\mathbb{Z}[X]$ es un dominio y $2 \neq 0$, de la segunda igualdad, obtenemos $p(x) = 0$ y por lo tanto $H_3(C_*) = 0$. Para resumir hemos probado que

$$H_n(C_*) = 0$$

para todo $n \in \mathbb{Z}$. □

4. Sea R un anillo conmutativo con unidad que no sea el anillo cero y sean I, J conjuntos. Demuestra que $RI \cong RJ$ si y solo si existe una biyección entre I y J. **Pista:** Se cumple si R es un campo.

Solución:

Supongamos primero que hay una biyección $f\colon I \to J$. Consideremos $\iota_J f\colon I \to RJ$. Por la propiedad universal del R–módulo libre, existe un único homomorfismo $F\colon RI \to RJ$ tal que $F\iota_I = \iota_J f$ y de hecho en la demostración de esta propiedad universal vimos su fórmula explícita:

$$F\left(\sum_{i\in I} r_i i\right) = \sum_{i\in I} r_i f(i)$$

Si hacemos lo mismo con $f^{-1}\colon J \to I$, obtenemos un homomorfismo $G\colon RJ \to RI$ que está dado por

$$G\left(\sum_{i\in I} r_i i\right) = \sum_{i\in I} r_i f^{-1}(i)$$

Ahora notemos que

$$FG\left(\sum_{i\in I} r_i i\right) = F\left(\sum_{i\in I} r_i f^{-1}(i)\right) = \sum_{i\in I} r_i f f^{-1}(i) = \sum_{i\in I} r_i i$$

$$GF\left(\sum_{i\in I} r_i i\right) = G\left(\sum_{i\in I} r_i f(i)\right) = \sum_{i\in I} r_i f^{-1} f(i) = \sum_{i\in I} r_i i$$

Luego $RI \cong RJ$.

Ahora supongamos $RI \cong RJ$ y sea $f\colon RI \to RJ$ un tal isomorfismo de R–módulos. Como R es un anillo conmutativo con unidad que no es el anillo cero, tiene al menos un ideal maximal $\mathfrak{m}$. Recordemos que $R/\mathfrak{m}$ es un campo que denotaremos k. Consideramos los submódulos $\mathfrak{m}RI$ y $\mathfrak{m}RJ$ de RI y RJ, respectivamente. La composición de f con el cociente $\pi\colon RJ \to RJ/\mathfrak{m}RJ$ cumple que si $a_s \in \mathfrak{m}$ y $x_s \in RI$, entonces

$$\pi f\left(\sum_{s=1}^{t} a_s x_s\right) = \pi\left(\sum_{s=1}^{t} a_s f(x_s)\right) = \mathfrak{m}RJ$$

porque $\sum_{s=1}^{t} a_s f(x_s) \in \mathfrak{m}RJ$. Por la propiedad universal del cociente, existe un único homomorfismo de R–módulos $F\colon RI/\mathfrak{m}RI \to RJ/\mathfrak{m}RJ$ que al componer con el cociente $RI \to RI/\mathfrak{m}RI$ nos da πf. De hecho en la demostración vimos que $F(x + \mathfrak{m}RI) = \pi f(x) = f(x) + \mathfrak{m}RJ$. El mismo argumento con f^{-1} nos daría un homomorfismo de R–módulos $G\colon RJ/\mathfrak{m}RJ \to RI/\mathfrak{m}RI$ que estaría dado por $G(y + \mathfrak{m}RJ) = f^{-1}(y) + \mathfrak{m}RI$. Claramente G es la inversa de F, así que $RJ/\mathfrak{m}RJ \cong RI/\mathfrak{m}RI$ como R–módulos.

Por otra parte consideremos la función $\iota_J^k\colon J \to kJ$ y veamos a kJ como un R–módulo con la multiplicación escalar

$$r \star \left(\sum (r_j + \mathfrak{m})j\right) = \sum (r r_j + \mathfrak{m})j$$

Por la propiedad universal del R–módulo libre, existe un único homomorfismo de R–módulos $h\colon RJ \to kJ$ tal que $h\iota_J^R = \iota_J^k$. Es decir

$$h\left(\sum_j r_j j\right) = \sum_j r_j \star j = \sum_j r_j \star (1 + \mathfrak{m})j = \sum_j (r_j + \mathfrak{m})j$$

Es claramente sobreyectiva, así que por el primer teorema de isomorfismo hay un isomorfismo de R–módulos $RJ/\mathrm{Ker}(h) \cong kJ$. Pero vemos que $\sum_j r_j j$ está en el núcleo si y solo si $r_j \in \mathfrak{m}$

para todo j, luego $\operatorname{Ker}(h) \subseteq \mathfrak{m}RJ$. Por otra parte, si $a_s \in \mathfrak{m}$ y $x_s = \sum_j r_j^s j \in RJ$, se tiene

$$h\left(\sum_{s=1}^{t} a_s x_s\right) = \sum_{s=1}^{t} a_s \left(\sum_j r_j^s \star j\right) = \sum_{s=1}^{t} a_s \left(\sum_j (r_j^s + \mathfrak{m})j\right) = \sum_{s,j} (a_s r_j^s + \mathfrak{m})j = 0$$

pues $a_s r_j^s \in \mathfrak{m}$, así que $\operatorname{Ker}(h) = \mathfrak{m}RJ$. Hemos probado que $RJ/\mathfrak{m}RJ \cong kJ$ como R–módulos. Igualmente se tendría $RI/\mathfrak{m}RI \cong kI$ como R–módulos. Por lo tanto $kI \cong kJ$ como R–módulos. Pero por la manera que definimos su estructura de R–módulos, veremos que también es un isomorfismo de k–módulos. Para empezar notemos que si $r + \mathfrak{m} \in k$ se tiene

$$(r + \mathfrak{m}) \sum_i (r_i + \mathfrak{m})i = \sum_i (rr_i + \mathfrak{m})i = r \star \sum_i (r_i + \mathfrak{m})i$$

y lo mismo para kJ. Por lo que si $\varphi\colon kI \to kJ$ es un isomorfismo de R–módulos y $r + \mathfrak{m} \in k$, $x \in kI$ se tiene

$$\varphi((r + \mathfrak{m})x) = \varphi(r \star x) = r \star \varphi(x) = (r + \mathfrak{m})\varphi(x)$$

Así que φ es un isomorfismo de k–módulos, es decir, de espacios vectoriales sobre k. Entonces las bases I y J de kI y kJ deben tener la misma cardinalidad, es decir, existe una biyección entre I y J. $\square$

La primera implicación también se podría haber probado usando que la asignación $I \mapsto RI$ es parte de un funtor, y los funtores envían objetos isomorfos a objetos isomorfos.

5. Se dice que un R–módulo es **simple** si sus únicos submódulos son $\{0\}$ y M.

(a) Demuestra que todo R–módulo simple es cíclico, pero que existen R–módulos cíclicos que no son simples.

Solución:

Sea M un R–módulo simple. Si $M = \{0\}$, ciertamente está generado por 0, así que es cíclico. Supongamos que $M \neq \{0\}$. Entonces existe $m_0 \neq 0$ en M. El submódulo generado por m_0 debe ser entonces $\{0\}$ ó M, pero no puede ser $\{0\}$ porque contiene a $m_0 \neq 0$. Así que $M = \langle m_0 \rangle$, es decir, M es cíclico.

Sea $R = \mathbb{Z}$ y consideremos $M = \mathbb{Z}/6$. Es un $\mathbb{Z}$–módulo cíclico pues está generado por $[1]_6$, pero no es simple pues contiene al submódulo

$$L = \{[0]_6, [3]_6\} = \{[3m]_6 \mid m \in \mathbb{Z}\}$$

Es un submódulo pues es no vacío y

$$\begin{aligned}[3m]_6 + [3n]_6 &= [3(m+n)]_6 \\ -[3m]_6 &= [3(-m)]_6 \\ n[3m]_6 &= [3nm]_6\end{aligned}$$

pero no es M ni $\{0\}$. □

(b) Clasifica todos los R–módulos simples salvo isomorfismo, cuando R es un campo y cuando $R = \mathbb{Z}$.

Solución:

Recordemos que en general, si M es un R–módulo cíclico, existe un ideal izquierdo J de R tal que $M \cong R/J$ como R–módulos.

Cuando R es un campo, sus únicos ideales son $\{0\}$ y R, así que $M = R$ ó $M = \{0\}$. Claramente $\{0\}$ es simple. Los R–submódulos de R son sus ideales, así que solo son $\{0\}$ y R, es decir, R también es simple. Los campos son diferentes de $\{0\}$ por definición, así que todos los R–módulos simples salvo isomorfismo serían R y $\{0\}$.

Cuando $R = \mathbb{Z}$, sus ideales son todos de la forma $n\mathbb{Z}$ para algún entero $n \geq 0$. Si $n = 1$, el cociente es $\{0\}$, que es simple. Si $n = 0$, el cociente es $\mathbb{Z}$ que no es simple pues contiene por ejemplo al submódulo $2\mathbb{Z}$ que no es $\{0\}$ ni $\mathbb{Z}$. Ahora estudiemos cuando $n \geq 2$, en cuyo caso el cociente es $\mathbb{Z}/n$. Si n no es primo y se rompe $n = p_1^{r_1} \dots p_k^{r_k}$ con $k \geq 2$ ó algún $r_i \geq 2$. Entonces por la clasificación de grupos abelianos finitamente generados

$$\mathbb{Z}/n \cong \bigoplus_{j=1}^{k} \mathbb{Z}/p_j^{r_j}$$

Si $k \geq 2$, entonces $\mathbb{Z}/p_1^{r_1}$ es un submódulo del lado derecho distinto de $\{0\}$ y del total. Si algún $r_i \geq 2$, entonces $\mathbb{Z}/p_i$ es un submódulo del lado derecho distinto de $\{0\}$ y del total. Como un isomorfismo envía submódulos distintos de $\{0\}$ y del total a submódulos distintos de $\{0\}$ y del total, obtenemos que $\mathbb{Z}/n$ no es simple.

Por lo tanto, se debe tener que $n = p$ es primo. Sabemos que los únicos subgrupos de $\mathbb{Z}/p$ son $\{0\}$ y $\mathbb{Z}/p$, así que es simple. Además, si p y q son primos, se tiene $\mathbb{Z}/p \cong \mathbb{Z}/q$ si y solo si $p = q$. Para concluir, los $\mathbb{Z}$–módulos simples salvo isomorfismo son $\{0\}$ y los $\mathbb{Z}/p$, para p primo. $\square$

6. Encuentra una familia $\{M_j\}_{j\in J}$ de R–módulos (para algún R) tal que la suma directa y el producto no son isomorfos.

Solución:

Sea $R = \mathbb{Z}$. Consideremos la familia $\{\mathbb{Z}\}_{j\in\mathbb{N}}$ de $\mathbb{Z}$–módulos. Por conveniencia no incluimos 0 en $\mathbb{N}$. Comencemos con

$$M = \prod_{j\in\mathbb{N}} \mathbb{Z}$$

y consideremos el subconjunto

$$X = \{(a_j)_j \in M \mid a_j \in \{0,1\}\}$$

Supongamos que X es numerable, es decir, existe una biyección $f\colon \mathbb{N} \to X$. Se tiene $f(n) = (a_j^n)_j$ para ciertos $a_j^n \in \{0,1\}$. Ojo, a_j^n no se refiere a la n-ésima potencia de a_j, la n de arriba es simplemente otro índice. Consideremos la tupla $(b_j)_j$ definida mediante

$$b_j = 1 - a_j^j$$

Ciertamente $(b_j)_j \in X$. Pero $(b_j)_j \neq (a_j^n)_j$ porque $b_n \neq a_n^n$. Esto contradice que f sea sobreyectiva. Por lo tanto X no es numerable y como $X \subseteq M$, tampoco M es numerable.

Por otra parte, consideremos

$$N = \bigoplus_{j\in\mathbb{N}} \mathbb{Z}$$

Para cada $r \geq 1$, definimos

$$N_r = \{(a_j)_j \in N \mid a_j = 0 \text{ si } j > r\}$$

La función $(a_j)_j \mapsto (a_j)_{j\leq r}$ define una biyección (de hecho un isomorfismo, pero esto no importará) entre N_r y $\mathbb{Z}^r$, luego N_r es numerable. Como

$$N = \bigcup_{r\in\mathbb{N}} N_r$$

es una unión numerable de conjuntos numerables, es numerable. Así que M no puede ser isomorfo a N, pues ni siquiera existe una biyección entre ellos. $\square$

Extra. Sea V la suma directa de la familia $\{\mathbb{C}\}_{n\in\mathbb{N}}$ de $\mathbb{C}$–espacios vectoriales y sea $R = \operatorname{End}_{\mathbb{C}}(V)$. Demuestra que $R \cong R^2$ como R–módulos. **Pista:** Construye un isomorfismo lineal $V \to V \oplus V$ y úsalo para obtener dos endomorfismos de V a partir de uno.

Solución:

Consideremos la función

$$\begin{aligned}\varphi\colon V &\to V^2\\ (a_j)_j &\mapsto ((a_{2j})_j, (a_{2j-1})_j)\end{aligned}$$

Cumple

$$\begin{aligned}\varphi((a_j)_j + (b_j)_j) &= \varphi((a_j + b_j)_j)\\ &= ((a_{2j} + b_{2j})_j, (a_{2j-1} + b_{2j-1})_j)\\ &= ((a_{2j})_j, (a_{2j-1})_j) + ((b_{2j})_j, (b_{2j-1})_j)\\ &= \varphi((a_j)_j) + \varphi((b_j)_j)\end{aligned}$$

$$\varphi(\lambda(a_j)_j) = \varphi((\lambda a_j)_j) = ((\lambda a_{2j})_j, (\lambda a_{2j-1})_j) = \lambda((a_{2j})_j, (a_{2j-1})_j) = \lambda\varphi((a_j)_j)$$

así que es una transformación $\mathbb{C}$–lineal. Si $\varphi((a_j)_j) = 0$, entonces todas las coordenadas pares e impares son cero, luego $(a_j)_j = (0)_j$, es decir, φ es inyectiva. Por otra parte, dada $((b_j)_j, (c_j)_j) \in V^2$ podemos definir

$$a_j = \begin{cases} b_{j/2} & \text{si } j \text{ es par}\\ c_{(j+1)/2} & \text{si } j \text{ es impar}\end{cases}$$

y vemos que $\varphi((a_j)_j) = ((b_j)_j, (c_j)_j)$, luego φ es un isomorfismo $\mathbb{C}$–lineal. Definimos ahora

$$\begin{aligned}f\colon R &\to R^2\\ h &\mapsto (h\varphi^{-1}\iota_1, h\varphi^{-1}\iota_2)\end{aligned}$$

donde $\iota_j\colon V \to V^2$ es la inclusión canónica en la j-ésima coordenada. También definimos

$$\begin{aligned}g\colon R^2 &\to R\\ (h_1, h_2) &\mapsto h_1 \operatorname{pr}_1 \varphi + h_2 \operatorname{pr}_2 \varphi\end{aligned}$$

donde $\operatorname{pr}_j\colon V^2 \to V$ es la proyección a la j-ésima coordenada. Ahora notemos que

$$gf(h) = g(h\varphi^{-1}\iota_1, h\varphi^{-1}\iota_2) = h\varphi^{-1}\iota_1 \operatorname{pr}_1 \varphi + h\varphi^{-1}\iota_2 \operatorname{pr}_2 \varphi = h\varphi^{-1}\varphi = h$$

donde la tercera igualdad se cumple porque

$$\iota_1 \operatorname{pr}_1(a,b) + \iota_2 \operatorname{pr}_2(a,b) = \iota_1(a) + \iota_2(b) = (a,0) + (0,b) = (a,b)$$

Por otra parte

$$\begin{aligned} fg(h_1,h_2) &= f(h_1 \operatorname{pr}_1 \varphi + h_2 \operatorname{pr}_2 \varphi) \\ &= ((h_1 \operatorname{pr}_1 \varphi + h_2 \operatorname{pr}_2 \varphi)\varphi^{-1}\iota_1, (h_1 \operatorname{pr}_1 \varphi + h_2 \operatorname{pr}_2 \varphi)\varphi^{-1}\iota_2) \\ &= (h_1 \operatorname{pr}_1 \iota_1 + h_2 \operatorname{pr}_2 \iota_1, h_1 \operatorname{pr}_1 \iota_2 + h_2 \operatorname{pr}_2 \iota_2) \\ &= (h_1, h_2) \end{aligned}$$

donde la última igualdad se cumple porque $\operatorname{pr}_i \iota_j = \delta_{ij} 1_V$. Esto muestra que f es una biyección. Veamos que es un morfismo de R–módulos.

$$f(h+k) = ((h+k)\varphi^{-1}\iota_1, (h+k)\varphi^{-1}\iota_2) = (h\varphi^{-1}\iota_1 + k\varphi^{-1}\iota_1, h\varphi^{-1}\iota_2 + k\varphi^{-1}\iota_2) = f(h) + f(k)$$

$$f(k \circ h) = (kh\varphi^{-1}\iota_1, kh\varphi^{-1}\iota_2) = k(h\varphi^{-1}\iota_1, h\varphi^{-1}\iota_2) = kf(h)$$

Por lo tanto, es un isomorfismo de R–módulos izquierdos. $\square$

Con otros homomorfismos entre R y R^2 se podría lograr probar que también son isomorfos como R–módulos derechos.