Universidade Federal de Santa Catarina

Departamento de Matemática

Curso de Licenciatura em Matemática

Um Tópico em Teoria de Módulos: Módulos Projetivos e Injetivos

por

Marcelo Rivadavia Troglia Peres

Florianópolis, março de 2007.

Esta Monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática – Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nª 26/CCM/07.

Profa. Carmen Suzane Comitre Gimenez

Professora da disciplina

Banca Examinadora:

Profa. Virgínia Silva Rodrigues

Orientador

Prof. Luiz Augusto Saeger

Profa. Giselle Spindler

Agradecimentos

Jesus Cristo seja Louvado pelos séculos e séculos. Amém.

Aos professores da banca que se disponibilizaram a ler este trabalho.

À professora Virgínia que aceitou orientar-me com muita dedicação e preocupação durante todo este trabalho. Atenção, dedicação, compromisso e conhecimento são qualidades que os professores que a possuem merecem distinção, a saber, você Professora Virgínia. Muito Obrigado.

Dedico ao Professor Paulo Henrique Viana de Barros este trabalho, pois mesmo não estando mais presente entre nós, os seus ensinamentos e sabedoria permanecem, é uma referência.

Agradeço humildemente a todas as pessoas que crêem em mim, a saber: Meu Pai, a ele dedico este trabalho como resultado da sua dedicação, do seu empenho em sempre me ajudar, nunca desamparou um filho seu. Como ele sei que não há. À minha mãe que nas suas possibilidades e mesmo estando distante, aposta em mim. À minha esposa Fabiana pelo apoio e compreensão, apesar de todas as adversidades, não perdeu a fé.

Aos meus irmãos Rodrigo, Gabriel, Cristina, Bruno e Emanuel, sempre torcendo por mim e eu por eles. Que sejamos unidos desde sempre.

E às minhas filhas Gabriela e Djéssica que amem a matemática tanto quanto eu.

Ofereço igualmente este trabalho ao Sr. Fritz Kröplin e à Sr. Isabel Kröplin, meus sogros, pelo anseio em ver esta obra finalizada.

Aos meus amigos Edson Ribeiro dos Santos, ao Leonardo Borges, ao Maicon Benvenutti e ao meu Amissíssimo Alexandre Costa da Silva que está ausente, mas presente diante de Deus, O Cristo.

E novamente este trabalho é de Nosso Senhor Jesus Cristo. A Ele toda a Glória.

Índice

Introdução

Nesse início, lembramos um "pouco" de álgebra linear. Dado um espaço vetorial V sobre um corpo K, estão definidas duas operações: uma operação soma $+$ que satisfaz quatro propriedades, (veja [3]) e também uma multiplicação por "escalar", isto é, uma multiplicação de elementos de K por elementos de V.

No entanto, se ao invés do corpo K supormos um anel R qualquer com unidade, e assim definirmos uma multiplicação de elementos de R por elementos de V, surge a definição do que vem a ser um módulo.

Nosso objetivo nessa monografia é desenvolver um pouco sobre a teoria de módulos detalhando alguns resultados que em muitos livros são deixados como exercício para o leitor. Além disso, dois tipos específicos de módulos nos interessam e efetivamente são estudados, a saber, módulos projetivos e injetivos.

No capítulo 1, definimos formalmente módulo e submódulo. Apresentamos uma série de exemplos a fim de familiarizar o leitor. De maneira análoga, como na teoria de anéis e na teoria de grupos, definimos módulos quocientes e homomorfismos de módulos, em especial provamos o teorema do homomorfismo para módulos.

No capítulo 2, estudamos e caracterizamos os módulos projetivos. Um fato sabido é que todo espaço vetorial sobre um corpo possui uma base, o que não é verdade para módulos; por exemplo, $\mathbb{Q}$ como um $\mathbb{Z}$-módulo não possui uma base, vamos provar o porquê disso oportunamente. No entanto, os chamados módulos livres possuem uma base e além disso, contribuem significativamente

para a caracterização dos módulos projetivos, por isso, dedicamos uma seção do capítulo 2 aos módulos livres

No capítulo 3, estudamos uma outra classe de módulos, os módulos injetivos, cujos estudo e caracterizações são feitos de maneira análoga ao que fizemos para os módulos projetivos. Em se tratando de uma definição dual da definição de módulo projetivo, invertemos o sentido das "flechas" trocando epimorfismos por monomorfismos.

Em todo trabalho, o anel R é um anel com unidade não necessariamente comutativo e todo módulo é definido sobre R.

Capítulo 1

Módulos

Nesse capítulo, definimos módulos e apresentamos uma série de exemplos a fim de familiarizar o leitor. Há uma semelhança interessante entre a teoria de módulos e a teoria de anéis (no sentido de que resultados provados para anéis com algumas "modificações" são provados para módulos), por exemplo, o teorema do homomorfismo para módulos é provado aqui. Outros assuntos são desenvolvidos a fim de auxiliar nos capítulos posteriores.

1.1 Resultados Básicos

Definição 1.1. *Seja M um conjunto não vazio munido de uma operação*

$$\begin{array}{rccc} + : & M \times M & \to & M \\ & (m, m_1) & \mapsto & m + m_1. \end{array}$$

M com a operação $+$ é dito um grupo se as seguintes propriedades são satisfeitas:

(i) *A operação $+$ é associativa, isto é, $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$, para quaisquer m_1, m_2, m_3 em M.*

(ii) *Existe um único elemento neutro, isto é, $\exists\ 0 \in M$ tal que $0 + m = m = m + 0$, para todo m em M.*

(iii) *Todo elemento em M possui um único elemento oposto em M, isto é, para todo m em M, existe um m' em M, tal que $m + m' = m' + m = 0$. Denotamos $m' = -m$.*

M é dito um grupo abeliano ou comutativo se:

(iv) *A operação $+$ é comutativa, isto é, $m_1 + m_2 = m_2 + m_1$, para quaisquer m_1, m_2 em M.*

Denotamos por $(M, +)$ o grupo M com a operação $+$, chamado grupo aditivo.

Exemplo 1.2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +)$ são grupos abelianos (aditivos).

Exemplo 1.3. Se p é primo, $(\mathbb{Z}_p - \{0\}, \cdot)$ é um grupo abeliano.

Definição 1.4. *Seja M um grupo. Um subconjunto não vazio N de M é um subgrupo de M (denotamos por $N < M$) quando, com a operação de M, o conjunto N é um grupo.*

Proposição 1.5. *Seja N um subconjunto não vazio do grupo aditivo M. Então N é um subgrupo de M se, e somente se, as seguintes condições são satisfeitas:*

(i)' *$n_1 + n_2 \in N$, para quaisquer n_1, n_2 em N.*

(ii)' *Para todo n em N, existe $-n \in N$ tal que $n + (-n) = (-n) + n = 0$.*

Demonstração: De fato, se N é um grupo, é claro que as condições (i)' e (ii)' são satisfeitas. Suponhamos que (i)' e (ii)' sejam satisfeitas. Claramente, $+$ é uma operação em N que é associativa. Por outro lado, dado $n \in N$, por (ii)' existe $-n \in N$ tal que $n + (-n) = (-n) + n = 0$. Por (i)', $0 \in N$. □

Na prática, verificamos as condições (i)' e (ii)' para mostrar que N é um subgrupo de um grupo M.

Definição 1.6. *Seja M um grupo abeliano. M é dito um módulo à esquerda sobre R (ou um R-módulo à esquerda) se a operação multiplicação de elementos de R por elementos de M definida abaixo satisfaz as propriedades* (i) − (iv)*:*

$$\begin{array}{rccc} \cdot : & R \times M & \to & M \\ & (r, m) & \mapsto & r \cdot m \end{array}$$

para quaisquer $r, r_1, r_2 \in R$ e para quaisquer $m, m_1, m_2 \in M$,

(i) $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$.
(ii) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$.
(iii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.
(iv) $1 \cdot m = m$.

Analogamente, definimos R-módulos à direita considerando a multiplicação à direita por elementos do anel R.

Se $r \in R$ e $m \in M$, escrevemos rm em todo o trabalho para denotar o elemento $r \cdot m$ (os elementos do anel R são chamados escalares).

Em todo o trabalho, M é um R-módulo à esquerda. Não havendo confusão quanto a isso, escreveremos sempre: M é um R-módulo. A notação ${}_R M$ é também usada para expressar que M é um R-módulo à esquerda.

Exemplo 1.7. O anel R tem a estrutura natural de R-módulo, isto é, R é um R-módulo sobre si mesmo tanto à direita quanto à esquerda. A estrutura de grupo abeliano é a do próprio anel R e a operação $\cdot$ é exatamente o produto do anel R.

Exemplo 1.8. Todo espaço vetorial sobre um corpo K é um K-módulo.

Exemplo 1.9. Todo grupo abeliano $(M, +)$ pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos inteiros definindo a multiplicação por

$$\begin{array}{rccl} \cdot : & \mathbb{Z} \times M & \to & M \\ & zg & \mapsto & \begin{cases} 0 \quad se \quad z = 0 \\ \underbrace{g + \cdots + g}_{z \quad vezes} \quad se \quad z > 0 \\ \underbrace{(-g) + \cdots + (-g)}_{-z \quad vezes} \quad se \quad z < 0 \end{cases} \end{array}$$

para todo $z \in \mathbb{Z}$ e para todo $g \in M$.

Exemplo 1.10. O grupo trivial 0 é um módulo sobre qualquer anel R.

Exemplo 1.11. Seja I um ideal à esquerda em um anel R. Então I admite um estrutura de R-módulo (à esquerda) com a soma induzida pela soma de R e a multiplicação definida pela multiplicação de R.

Definição 1.12. *Seja M um R-módulo. Um subconjunto $N \subset M$ diz-se um R-submódulo de M, ou simplesmente, um submódulo se:*
(i) *N é um subgrupo aditivo de M.*
(ii) *N é fechado em relação à operação $\cdot$, isto é, para todo $r \in R$ e para todo $n \in N$ tem-se que $rn \in N$.*

Proposição 1.13. *Seja M um R-módulo. Um subconjunto não vazio N de M é um submódulo de M se, e somente se, as seguintes condições são satisfeitas:*
(i)' *Para todo $n, n' \in N$. $n + n' \in N$.*
(ii)' *Para todo $r \in R$ e para todo $n \in N$, $rn \in N$.*

Demonstração: Se N é submódulo, então (i)' e (ii)' são satisfeitas. Reciprocamente, mostremos que N é um submódulo de M. De fato, claramente $+$ é uma operação em N, pois vale (i)', que é associativa e comutativa. Como N é não vazio, existe $n \in N$. Por (ii)' $0 = 0n \in N$. Agora, dado $n \in N$, temos que $-1 \in R$ (pois é o oposto da unidade 1), daí $-1n = -n \in N$. □

Exemplo 1.14. Dado um R-módulo M, temos que $\{0\}$ e M são submódulos de M, chamados submódulos triviais.

Exemplo 1.15. Seja M um grupo abeliano (M é visto como um $\mathbb{Z}$-módulo). Os subgrupos de M são os $\mathbb{Z}$-submódulos de M.

Exemplo 1.16. Se I é um ideal à esquerda de um anel R e se m é um elemento de um R-módulo M, então o conjunto $Im = \{\alpha m : \alpha \in I\}$ é um submódulo de M.

Exemplo 1.17. Os ideais de R são submódulos de R quando R é considerado como um R-módulo sobre si mesmo.

Exemplo 1.18. Sejam N e K submódulos de M. Definimos $N + K = \{n + k : n \in N, k \in K\}$. Então $N + K$ é um submódulo de M. De fato, pois se $x, y \in N + K$ então $x = n + k$ e $y = n' + k'$ e para todo $r \in R$ segue que

$$\begin{aligned} x + y &= (n + n') + (k + k') \in N + K \text{ e} \\ rx &= r(n + k) = rn + rk \in N + K. \end{aligned}$$

As propriedades (i)' e (ii)' da Proposição 1.13 são facilmente verificadas.

Proposição 1.19. *Seja M um R-módulo. Então a interseção arbitrária de submódulos de M é um submódulo de M.*

Demonstração: Consideremos a família $\{M_i\}_{i\in I}$ onde I é um conjunto qualquer e M_i é um submódulo de M, para todo $i \in I$. Mostremos que $\bigcap_{i\in I} M_i$ é um submódulo de M. De fato, sejam $x, y \in \bigcap_{i\in I} M_i$. Então $x \in M_i$, para todo $i \in I$ e $y \in M_i$, para todo $i \in I$. Daí, $x + y \in M_i$, para todo $i \in I$ e isso implica que $x + y \in \bigcap_{i\in I} M_i$.

Sejam $r \in R$ e $x \in \bigcap_{i\in I} M_i$. Então $x \in M_i$, para todo $i \in I$ e portanto $rx \in M_i$, para todo $i \in I$. Logo, $rx \in \bigcap_{i\in I} M_i$. □

1.2 Módulos Quocientes

Sejam M um R-módulo e N um R-submódulo de M. Dados $m_1, m_2 \in M$, definimos a relação $m_1 \equiv m_2 \pmod N$ se, e somente se, $m_1 - m_2 \in N$.

É fácil verificar que $\equiv \pmod N$ é uma relação de equivalência.

Podemos escrever para $m \in M$ a sua respectiva classe de equivalência, que denotamos por $m + N$, mais explicitamente

$$\begin{aligned} m + N = \ & \{x \in M : x \equiv m \ (\mathrm{mod}\, N)\} \\ & \{x \in M : x - m \in N\} \\ & \{m + n : n \in N\}. \end{aligned}$$

Como M é um grupo abeliano, todo submódulo N de M é, na verdade, um subgrupo normal em N (isto é, $N + m = m + N, \forall\, m \in M$). Portanto, não escrevemos classe lateral à direita (à esquerda), pois ambas coincidem.

Proposição 1.20. *Dados $m_1, m_2 \in M$, então $m_1+N = m_2+N$ se, e somente se, $m_1 - m_2 \in N$, isto é, $m_1 \equiv m_2 \pmod N$.*

Demonstração: ($\Rightarrow$) Temos que $m_1 \in m_2 + N$, isto é, $m_1 = m_2 + n$ para algum $n \in N$. Daí, $m_1 + (-m_2) \in N$.

($\Leftarrow$) De fato, se $m_1 - m_2 \in N$, então $m_1 - m_2 = n$ para algum $n \in N$. Daí, $m_1 = m_2 + n$ e isso implica que $m_1 \in m_2 + N$. Analogamente, provamos que $m_2 \in m_1 + N$. Logo, $m_1 + N = m_2 + N$. □

Consideremos o conjunto quociente $M/N = \{m+N : m \in M\}$, o conjunto de todas as classes de equivalência. Definimos

$$\begin{array}{rccc} + : & M/N \times M/N & \to & M/N \\ & (m_1+N, m_2+N) & \mapsto & (m_1+N)+(m_2+N) = (m_1+m_2)+N. \end{array}$$

Primeiramente provemos que $+$ está bem definida. De fato, sejam m_1, m_2, $m_3, m_4 \in M$ tais que $(m_1+N, m_2+N) = (m_3+N, m_4+N)$. Então $m_1+N = m_3+N$ e $m_2+N = m_4+N$. Daí, $m_1 - m_3 \in N$ e $m_2 - m_4 \in N$. Logo, $(m_1-m_3)+(m_2-m_4) \in N$ e claramente, $(m_1+m_2)-(m_3+m_4) \in N$. Portanto, $(m_1+m_2)+N = (m_3+m_4)+N$.

Mostremos que M/N é um grupo abeliano. De fato, a operação $+$ é associativa, pois dados $m_1, m_2, m_3 \in M$, temos que

$$\begin{aligned} (m_1+N)+((m_2+N)+(m_3+N)) &= (m_1+N)+((m_2+m_3+N)) \\ &= (m_1+(m_2+m_3))+N \\ &= ((m_1+m_2)+m_3)+N \\ &= ((m_1+m_2)+N)+(m_3+N) \\ &= ((m_1+N)+(m_2+N))+(m_3+N). \end{aligned}$$

O elemento $0+N = N$ é o elemento neutro de M/N, pois para todo $m \in M$, vale que $(0+N)+(m+N) = (0+m)+N = m+N = (m+N)+(0+N)$.

O elemento oposto de $m+N$ é $(-m)+N$, pois $(m+N)+((-m)+N) = (m-m)+N = 0+N = N = ((-m)+N)+(m+N)$.

A operação $+$ é comutativa, pois $(m_1+N)+(m_2+N) = (m_1+m_2)+N = (m_2+m_1)+N = (m_2+N)+(m_1+N)$. Logo, $(M/N, +)$ é um grupo abeliano.

Agora, definimos

$$\begin{array}{rccc} \cdot : & R \times M/N & \to & M/N \\ & (r, m+N) & \mapsto & r \cdot (m+N) = rm+N. \end{array}$$

Escrevemos simplesmente $r(m+N)$ ao invés de $r \cdot (m+N)$. Vejamos que a operação $\cdot$ está bem definida. De fato, sejam $m_1, m_2 \in M$ e $r \in R$ tais que $(r, m_1+N) = (r, m_2+N)$, então $m_1+N = m_2+N$ e daí, $m_1 - m_2 \in N$. Logo, $r(m_1-m_2) = rm_1 - rm_2 \in N$, o que implica $rm_1+N = rm_2+N$.

Finalmente, sejam $r_1, r_2 \in R$ e $m+N, m_1+N, m_2+N \in M/N$. Então

$$\begin{aligned}
&\text{(i) } (r_1r_2)(m\ +\ N) &&= ((r_1r_2)m) + N = r_1(r_2m) + N = r_1(r_2m+N).\\
&\text{(ii) } (r_1\ +\ r_2)(m\ +\ N) &&= (r_1+r_2)m + N = (r_1m + r_2m) + N\\
& &&= (r_1m+N) + (r_2m+N).\\
&\text{(iii) } r((m_1\ +\ m_2)\ +\ N) &&= (r(m_1+m_2)) + N = (rm_1 + rm_2) + N\\
& &&= (rm_1+N) + (rm_2+N).\\
&\text{(iv) } 1(m\ +\ N) &&= 1m + N = m + N.
\end{aligned}$$

Exemplo 1.21. Se I é um ideal de um anel R, R/I tem estrutura de R-módulo. Os submódulos de R/I são precisamente os ideais de R/I.

Exemplo 1.22. Seja $\mathbb{Z}_6$ um $\mathbb{Z}$-módulo. Os subgrupos de $\mathbb{Z}_6$, além dos triviais, são $N_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $N_2 = \{\overline{0}, \overline{3}\}$. Os módulos quocientes são dados por $\mathbb{Z}_6/N_1 = \{N_1, \overline{1} + N_1\}$ e $\mathbb{Z}_6/N_2 = \{N_2, \overline{1} + N_2, \overline{2} + N_2\}$.

1.3 Homomorfismos de Módulos

Sejam M e N R-módulos. Uma função f de M em N diz-se um *R-homomorfismo* ou *homomorfismo de R-módulos* se para quaisquer $m, m_1, m_2 \in M$ e qualquer $r \in R$ são verificadas as condições:

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$.

(ii) $f(rm) = rf(m)$.

Se f é um homomorfismo injetor, sobrejetor ou bijetor, então f é dito um *monomorfismo*, um *epimorfismo* ou um *isomorfismo*, respectivamente. Um homomorfismo $f : M \to M$ é dito um *endomorfismo* de M.

Proposição 1.23. *Sejam M e N R-módulos. Seja $f : M \to N$ um homomorfismo. Então as seguintes propriedades são satisfeitas:*

(i) $f(0) = 0_N$ *(0_N é o elemento neutro de N).*

(ii) *Para todo $m \in M$, $f(-m) = -f(m)$.*

Demonstração: (i) De fato, temos que $f(0) = f(0+0) = f(0) + f(0)$. Daí, $0_N = f(0)$.

(ii) De fato, temos que $0_N = f(0) = f(m+(-m)) = f(m)+f(-m)$. Daí, $0_N = f(m) + f(-m)$ e isso nos diz que $-f(m) = f(-m)$, ou seja, o oposto de $f(m)$ é $f(-m)$. □

Dado um R-homomorfismo $f : M \to N$, chamamos imagem de f $(Im(f))$ e núcleo de f $(Ker(f))$ respectivamente aos conjuntos:

$$Im(f) = \{f(m) : m \in M\}$$
$$Ker(f) = \{m \in M : f(m) = 0\}.$$

Proposição 1.24. *Seja $f : M \to N$ um R-homomorfismo. Então $Im(f)$ e $Ker(f)$ são submódulos de N e M, respectivamente.*

Demonstração: Mostremos que $Im(f)$ é submódulo de N. De fato, é imediato que $Im(f)$ é não vazio, pois $f(0) = 0_N$.

Sejam $x, y \in Im(f)$. Então $x = f(m_1)$ e $y = f(m_2)$ para alguns $m_1, m_2 \in M$. Daí, $x + y = f(m_1) + f(m_2) = f(m_1 + m_2) \in Im(f)$. Ainda temos que, para todo $r \in R$, $rx = rf(m_1) = f(rm_1) \in Im(f)$. Logo, $Im(f)$ é submódulo de N.

Mostremos que $Ker(f)$ é submódulo de M. De fato, $Ker(f)$ é não vazio, pois $0 \in Ker(f)$. Sejam $m_1, m_2 \in Ker(f)$, então $0_N = f(m_1) + f(m_2) = f(m_1 + m_2)$. Logo, $m_1 + m_2 \in Ker(f)$. Para quaisquer $r \in R$ e $m \in Ker(f)$, temos que $0_N = rf(m) = f(rm)$, isto é, $rm \in Ker(f)$. Logo, $Ker(f)$ é um submódulo de M. □

A partir de agora, se $f : M \to N$ é um R-homomorfismo, não faremos mais distinção entre os elementos neutros de M e N.

Proposição 1.25. *Seja $f : M \to N$ um homomorfismo de R-módulos. Então f é um homomorfismo injetor se, e somente se, $Ker(f) = 0$.*

Demonstração: ($\Rightarrow$) Suponhamos f injetor. Seja $x \in Ker(f)$. Então $f(x) = 0 = f(0)$. Logo, $x = 0$.
($\Leftarrow$) Sejam $m_1, m_2 \in M$ tais que $f(m_1) = f(m_2)$. Portanto, $f(m_1 - m_2) = 0$ e isso implica que $m_1 - m_2 \in Ker(f) = \{0\}$. Logo, $m_1 = m_2$. □

Proposição 1.26. *Sejam $f : M \to N$ e $g : N \to P$ homomorfismos de R-módulos. Então a função composta*

$$\begin{array}{rccc} g \circ f : & M & \to & P \\ & m & \mapsto & (g \circ f)(m) = g(f(m)) \end{array}$$

é um homomorfismo.

Demonstração: De fato, sejam $m, m_1, m_2 \in M$. Então $(g \circ f)(m_1 + m_2) = g(f(m_1 + m_2)) = g(f(m_1) + f(m_2)) = g(f(m_1)) + g(f(m_2)) = (g \circ f)(m_1) + (g \circ f)(m_2)$.

Para todo $r \in R$, temos que $(g \circ f)(rm) = g(f(rm)) = g(rf(m)) = rg(f(m)) = r(g \circ f)(m)$. □

Teorema 1.27. *(Teorema do homomorfismo para módulos) Sejam $f : M \to N$ um homomorfismo de R-módulos e K o seu núcleo. Então os módulos M/K e $Im(f)$ são isomorfos.*

Demonstração: Definimos

$$\begin{array}{rccc} \overline{f} : & M/K & \to & Im(f) \\ & m + K & \mapsto & \overline{f}(m + K) = f(m). \end{array}$$

Mostremos que $\overline{f}$ está bem definida. Sejam $m_1 + K, m_2 + K$ tais que $m_1 + K = m_2 + K$. Então $m_1 - m_2 \in K$ e portanto, $0 = f(m_1 - m_2) = f(m_1) - f(m_2)$. Daí, $f(m_1) = f(m_2)$.

Suponhamos que $\overline{f}(m_1 + K) = \overline{f}(m_2 + K)$ para $m_1, m_2 \in M$. Então $f(m_1) = f(m_2)$ e daí, $f(m_1 - m_2) = 0$, ou seja, $m_1 - m_2 \in K$. Logo, $m_1 + K = m_2 + K$. Assim, $\overline{f}$ é injetor.

Temos que $Im(\overline{f}) = \{\overline{f}(m + K) : m \in M\} = \{f(m) : m \in M\} = Im(f)$ e isso nos diz que $\overline{f}$ é sobrejetor.

Agora, mostremos que $\overline{f}$ é um homomorfismo de R-módulos. Sejam $m_1 + K, m_2 + K, m_3 + K \in M/K$ e $r \in R$. Então

$$\begin{aligned} \overline{f}((m_1 + K) + (m_2 + K)) &= \overline{f}((m_1 + m_2) + K) \\ &= f(m_1 + m_2) = f(m_1) + f(m_2) \\ &= \overline{f}(m_1 + K) + \overline{f}(m_2 + K) \text{ e} \\ \overline{f}(r(m + K)) = f(rm) = rf(m) &= r\overline{f}(m + K). \end{aligned}$$

Logo, M/K e $Im(f)$ são isomorfos. □

Nota: Usamos a notação $\simeq$ para dizer que dois módulos são isomorfos.

Exemplo 1.28. Sejam M e N R-módulos. Então a função $0 : M \to N$ definida por $0(m) = 0$ para todo $m \in M$ é um homomorfismo, chamado *homomorfismo nulo.*

Exemplo 1.29. Se $\mathbb{K}$ é um corpo, os homomorfismos de $\mathbb{K}$-módulos ($\mathbb{K}$-espaços vetoriais) são precisamente as transformações lineares.

Exemplo 1.30. A função identidade $1_M : M \to M$ é um homomorfismo de R-módulos, na verdade, é um automorfismo, isto é, um endomorfismo bijetor.

Exemplo 1.31. Seja N um submódulo de um R-módulo M. Então a função inclusão

$$\begin{array}{rccc} i: & N & \hookrightarrow & M \\ & n & \mapsto & n \end{array}$$

é um monomorfismo.

Exemplo 1.32. Seja N um submódulo de um R-módulo M. A seguinte função é chamada projeção canônica

$$\begin{array}{rccc} \pi: & M & \to & M/N \\ & m & \mapsto & m+N. \end{array}$$

Claramente, π é sobrejetor. Sejam $m, m_1, m_2 \in M$ e $r \in R$. Então

$$\begin{aligned} \pi(m_1 + m_2) &= (m_1 + m_2) + N = (m_1 + N) + (m_2 + N) \\ &= \pi(m_1) + \pi(m_2) \text{ e} \\ \pi(rm) &= (rm + N) = r(m + N) = r\pi(m). \end{aligned}$$

Logo, π é um epimorfismo.

1.4 Produto Direto

Sejam I um conjunto não vazio qualquer e $\{M_i\}_{i\in I}$ uma família de R-módulos. Consideremos $M = \prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i\}$, onde $(m_i)_{i\in I}$ é uma família de elementos em M. É possível introduzir em M uma estrutura de R-módulo definindo as operações por

$$\begin{aligned}(m_i)_{i\in I} + (m_i')_{i\in I} &= (m_i + m_i')_{i\in I},\ m_i, m_i' \in M_i, \text{ para todo } i \in I.\\ r(m_i)_{i\in I} &= (rm_i)_{i\in I}, \text{ para todo } r \in R.\end{aligned}$$

O R-módulo obtido acima diz-se *produto direto* da família $\{M_i\}_{i\in I}$. Se I for um conjunto finito, digamos $I = \{1, 2, \cdots, n\}$, denotamos o produto direto por $M = M_1 \times M_2 \times \cdots \times M_n$.

As funções definidas abaixo são monomorfismos que são chamados de *inclusões naturais*, isto é, cada módulo $M_i, i \in I$, pode ser canonicamente imerso no produto direto M, assim

$$\begin{aligned} i_k : \ M_k &\to M \\ m_k &\mapsto (m_i)_{i\in I}, \ \text{ tal que } m_i = 0 \text{ se } i \neq k.\end{aligned}$$

Definimos as *projeções sobre as componentes* associando cada elemento $(m_i)_{i\in I}$ à k-ésima componente $m_k \in M_k$. As funções assim definidas são epimorfismos dados por

$$\begin{aligned} p_k : \ M &\to M_k \\ (m_i)_{i\in I} &\mapsto m_k.\end{aligned}$$

Não é difícil ver que:
(i) $p_k \circ i_k = 1_{M_k}, \forall\ k \in I$.
(ii) $p_k \circ i_h = 0, \forall\ h, k \in I$ tais que $h \neq k$.

Sejam I um conjunto qualquer, $\{M_i\}_{i\in I}$ uma família de R-módulos e $M = \prod_{i\in I} M_i$. Uma família $(m_i)_{i\in I} \in M$ diz-se uma *família quase-nula* se $m_i = 0$, exceto para um número finito de índices.

No conjunto das famílias quase-nulas de M podemos introduzir uma estrutura de R-módulo, por restrição das operações de M.

Definição 1.33. *Seja $\{M_i\}_{i\in I}$ uma família de R-módulos. O conjunto de todas as famílias quase-nulas de $M = \prod_{i\in I} M_i$ com a estrutura de R-módulo definida por restrição das operações de M chama-se a soma direta externa da família e é denotada por $\bigoplus_{i\in I}^{\bullet} M_i$.*

Se o conjunto de índices for finito, isto é, $I = \{1, 2, \cdots, n\}$ então

$$\dot{\bigoplus_{i\in I}} M_i = M_1 \dot{\bigoplus} M_2 \dot{\bigoplus} \cdots \dot{\bigoplus} M_n.$$

A soma direta externa de uma família de R-módulos é claramente um submódulo do produto direto e $\dot{\bigoplus_{i\in I}} M_i = \prod_{i\in I} M_i$ se, e somente se, o conjunto de índices I é finito.

Como um caso particular do produto direto, definimos as *inclusões naturais* e as projeções sobre as componentes de maneira análoga ao caso anterior.

As inclusões são monomorfismos e as projeções são epimorfismos e
(i) $p_k \circ i_k = 1_{M_k}, \forall\ k \in I$
(ii) $p_k \circ i_h = 0, \forall\ h, k \in I$ tais que $h \neq k$.

1.5 Soma Direta Interna

Nessa seção, estudamos um submódulo especial do produto direto, a soma direta interna. A diferença desse caso para os anteriores é que a família $\{M_i\}_{i\in I}$ é uma família de submódulos de um dado módulo M. A soma direta é de grande importância para os resultados que provaremos nos capítulos posteriores. A partir de agora não faremos mais distinção entre soma direta e soma direta interna.

Teorema 1.34. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. As seguintes afirmações são equivalentes:*
(i) *Todo elemento $m \in M$ se escreve de forma única como $m = \sum_{i\in I} m_i$, tal que $m_i \in M_i$, $\forall\ i \in I$ e a família $(m_i)_{i\in I}$ é quase nula.*
(ii) $M = \sum_{i\in I} M_i$ *e se* $\sum_{i\in I} m_i = 0$ *com* $m_i \in M_i$, *então* $m_i = 0$, $\forall\ i \in I$.
(iii) $M = \sum_{i\in I} M_i$ *e* $M_j \cap (\sum_{i\neq j} M_i) = \{0\}$, $\forall\ j \in I$.

Demonstração: (i) $\Rightarrow$ (ii) Suponhamos que $m = \sum_{i\in I} m_i = 0$, com $m_i \in M_i$. Mas por (i), todo elemento de M se escreve de modo único. Logo, $m_i = 0$, para todo $i \in I$.

(ii) $\Rightarrow$ (iii) Seja $m \in M_j \cap (\sum_{i\neq j} M_i)$. Então $m \in M_j$ e se escreve como $m = \sum_{i\neq j} m_i$, com $m_i \in M_i, i \in I$. Portanto, $\sum_{i\neq j} m_i - m = 0$ e por (ii) todos os somandos devem ser nulos. Em particular, $m = 0$.

(iii) $\Rightarrow$ (i) Do fato que $M = \sum_{i\in I} M_i$, temos que $m = \sum_{i\in I} m_i$ com $m_i \in M_i$. Mostremos que a decomposição de m é única.

Suponhamos que existam duas decomposições para m, isto é, $\sum_{i\in I} m_i = \sum_{i\in I} m'_i$. Para cada $j \in I$ temos que $m_j - m'_j = \sum_{i\neq j} m'_i - \sum_{i\neq j} m_i = \sum_{i\neq j}(m'_i - m_i)$ e portanto, $m_j - m'_j \in M_j \cap (\sum_{i\neq j} M_i) \overset{\text{(iii)}}{=} \{0\}$. Logo, $m_j = m'_j$. □

Definição 1.35. *O R-módulo M diz-se soma direta interna de uma família $\{M_i\}_{i\in I}$ de submódulos de M se é verificada uma (e portanto todas) as afirmações equivalentes do teorema acima.*

Para indicar que M é a soma direta interna dos submódulos $\{M_i\}_{i\in I}$ escrevemos $M = \bigoplus_{i\in I} M_i$ e se $I = \{1, 2, \cdots, n\}, M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Proposição 1.36. *Sejam M um R-módulo, N_1 e N_2 submódulos tais que $M = N_1 \oplus N_2$. Então o quociente M/N_1 é isomorfo a N_2.*

Demonstração: Sendo $M = N_1 \oplus N_2$, temos que para todo $m \in M$, m se escreve de modo único como $m = n_1 + n_2$, onde $n_1 \in N_1$ e $n_2 \in N2$. Tomemos

$$\begin{array}{rccl} p_2: & M & \to & N_2 \\ & m & \mapsto & n_2, \quad \text{onde } m = n_1 + n_2. \end{array}$$

Como p_2 é sobrejetor e $Ker(p_2) = N_1$, segue pelo Teorema 1.27 que $M/N_1 \simeq N_2$. □

Definição 1.37. *Seja N um submódulo de um R-módulo M. N é dito um somando direto de M se existe um submódulo N_1 de M tal que $M = N \oplus N_1$.*

Observe que na proposição anterior N_1 e N_2 são somandos diretos de M.

Exemplo 1.38. Para qualquer R-módulo M, tem-se que $M = M \oplus \{0\}$. Os submódulos M e $\{0\}$ dizem-se os somandos diretos triviais.

Exemplo 1.39. Consideremos o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Observe que os conjuntos $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $H_2 = \{\overline{0}, \overline{3}\}$ são submódulos tais que $H_1 \cap H_2 = \{0\}$. Logo, $\mathbb{Z}_6 = H_1 \oplus H_2$.

Exemplo 1.40. O $\mathbb{Z}$-módulo $\mathbb{Z}$ não possui somandos diretos não triviais. De fato, se $n\mathbb{Z}$ fosse um somando direto de $\mathbb{Z}$, então $\mathbb{Z} = n\mathbb{Z} \oplus m\mathbb{Z}$, para algum $m\mathbb{Z}$. Isso é um absurdo, pois estaríamos dizendo que todo número primo $p \in n\mathbb{Z} + m\mathbb{Z}$.

1.6 Seqüências Exatas

Sejam $\{\cdots, M_{i-1}, M_i, M_{i+1}, \cdots\}$ e $\{\cdots, f_i : M_i \to M_{i+1}, \cdots\}$ famílias de R-módulos e de R-homomorfismos, ambas eventualmente infinitas indexadas num conjunto não vazio I. Dizemos que o diagrama:

$$\longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}}$$

é uma seqüência exata, se é exata em M_i, para todo $i \in I$, isto é, se $Im(f_{i-1}) = Ker(f_i)$, para todo $i \in I$.

Definição 1.41. *Sejam E, F e G R-módulos. Uma seqüência exata da forma $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ é dita ser uma seqüência exata curta.*

Proposição 1.42. *Dada uma seqüência exata de R-módulos $K \xrightarrow{f} L \xrightarrow{g} M$, então $g \circ f = 0$.*

Demonstração: De fato, seja $x \in K$. Então $(g \circ f)(x) = g(f(x))$. Como $f(x) \in Im(f) = Ker(g)$, segue que $(g \circ f)(x) = 0$, isto é, $g \circ f = 0$. □

Consideremos o seguinte diagrama onde E, F e G são R-módulos

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & F \\ & \searrow^{\theta} & \downarrow{\scriptstyle \psi} \\ & & G \end{array}$$

o mesmo diz-se comutativo se $\theta = \psi \circ \varphi$.

Exemplo 1.43. A seqüência $0 \xrightarrow{f_0} E \xrightarrow{f} F$ é exata, se e somente se, f é um monomorfismo.

Se f é um monomorfismo então $Ker(f) = 0$ e como f_0 é o homomorfismo nulo, segue imediatamente que $Ker(f) = Im(f_0)$. Por outro lado, se a seqüência é exata temos que $0 = Im(f_0) = Ker(f)$. Logo, f é um monomorfismo.

Exemplo 1.44. A seqüência $E \xrightarrow{f} F \xrightarrow{f_0} 0$ é exata, se e somente se, f é um epimorfismo. A prova desse fato é análoga à anterior.

Exemplo 1.45. Dos exemplos citados acima segue imediatamente que a seqüência $0 \to E \xrightarrow{f} F \to 0$ é exata, se e somente se, f é um isomorfismo.

Exemplo 1.46. Seja $n \in \mathbb{Z}, n \geq 2$. A seqüência $0 \to n\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \to 0$ é exata, onde $i: \ n\mathbb{Z} \to \mathbb{Z}$ é a inclusão e $\pi : \mathbb{Z} \to \mathbb{Z}_n$ é a projeção canônica.

Exemplo 1.47. Mais geralmente, se E é um submódulo de F então a seqüência $0 \to E \xrightarrow{i} F \xrightarrow{\pi} F/E \to 0$ é exata, onde i é a inclusão e π é a projeção canônica.

Exemplo 1.48. Seja $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ uma seqüência exata curta de R-módulos. Então $G \simeq F/Im(f)$.

Definição 1.49. *Uma seqüência exata curta de R-módulos*

$$0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$$

cinde se $Im(f)$ é um somando direto de F.

Proposição 1.50. *Seja $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ uma seqüência exata curta de R-módulos. Então as seguintes afirmações são equivalentes:*
(i) *A seqüência cinde.*
(ii) *Existe um R-homomorfismo $\psi : F \to E$ tal que $\psi \circ f = 1_E$.*
(iii) *Existe um R-homomorfismo $\varphi : G \to F$ tal que $g \circ \varphi = 1_G$.*

Demonstração: (i) $\Rightarrow$ (ii) Temos que $Im(f)$ é um somando direto de F, isto é, existe um submódulo H de F tal que $F = Im(f) \oplus H$. Logo, todo elemento $x \in F$ é expresso de forma única como $x = y + h$, onde $y \in Im(f)$ e $h \in H$.

Como $y \in Im(f)$, temos que $y = f(z)$ para algum $z \in E$. Sendo f injetor, temos que z é único.

Agora, definimos $\psi : F \to E$ por $\psi(x) = z$ (onde $x = y + h$ com $y = f(z)$ para um único z e $h \in H$). Mostremos que ψ é um R-homomorfismo.

Sejam $x, x' \in F$. Então $x = y + h$ e $x' = y' + h'$ tais que $y, y' \in Im(f)$ e $h, h' \in H$. Então $y = f(z)$ e $y' = f(z')$ para alguns $z, z' \in E$. Temos que

$$\begin{aligned}
\psi(x + x') &= \psi((y + y') + (h + h')) = \psi(f(z + z') + (h + h')) \\
&= z + z' = \psi(x) + \psi(x') \quad \text{e} \\
\psi(rx) &= \psi(r(y + h)) = \psi(ry + rh) = \psi(rf(z) + rh) \\
&= \psi(f(rz) + rh) = rz = r\psi(x), \text{ para todo } r \in R.
\end{aligned}$$

Agora, provemos que $\psi \circ f = 1_E$. Então para todo $e \in E$, $(\psi \circ f)(e) = \psi(f(e)) = e$. Logo, $\psi \circ f = 1_E$.

(ii) $\Rightarrow$ (i) Mostremos que $F = Im(f) \oplus Ker(\psi)$. Seja $x \in F$. Chamemos $f(\psi(x)) = y$ e $z = x - y$. Então $x = y + z$ e claramente $y \in Im(f)$. É suficiente mostrar que $z \in Ker(\psi)$. De fato,

$$\begin{aligned} \psi(z) &= \psi(x-y) = \psi(x) - \psi(y) = \psi(x) - \psi(f(\psi(x))) \\ &= \psi(x) - (\psi \circ f)(\psi(x)) \overset{\text{(ii)}}{=} \psi(x) - \psi(x) = 0. \end{aligned}$$

Resta mostrarmos que $Im(f) \cap Ker(\psi) = \{0\}$. Seja $y \in Im(f) \cap Ker(\psi)$. Então $y \in Im(f)$, isto é, $y = f(x)$ para algum $x \in E$ e também $\psi(y) = 0$. Portanto, $0 = \psi(y) = \psi(f(x)) = (\psi \circ f)(x) = x$. Logo, $y = f(x) = f(0) = 0$.

(i) $\Rightarrow$ (iii) Temos que existe um submódulo H de F tal que $F = Im(f) \oplus H$.

Seja $y \in G$. Então existe $x \in F$ tal que $g(x) = y$. Mas $x = z + h$ onde $z \in Im(f)$ e $h \in H$. Temos que $g(x) = g(z) + g(h) = g(h)$, pois $z \in Im(f) = Ker(g)$. Logo, $g(h) = y$.

Mostremos que h com essa propriedade é único. Suponhamos que exista $h' \in H$ tal que $g(h') = y$. Então $g(h) = y = g(h')$ e isso implica que $g(h - h') = 0$. Portanto, $h - h' \in Ker(g) \cap H = Im(f) \cap H = \{0\}$. Assim, $h = h'$.

Agora, definimos $\varphi : G \to F$ por $\varphi(y) = h$ onde h é tal que $g(y) = h$. Mostremos que φ é um R-homomorfismo. Sejam $y, y' \in G$. Então $y = g(x)$ e $y' = g(x')$ para alguns $x, x' \in F$. Mas $F = Im(f) \oplus H$ e isso implica que $x = z + h$ e $x' = z' + h'$ com $z, z' \in Im(f)$ e $h, h' \in H$. Logo,

$$\begin{aligned} \varphi(y + y') &= \varphi(g(z+h) + g(z'+h')) = \varphi(g(z + z' + h + h')) \\ &= \varphi(g(z+z') + g(h+h')) \overset{(*)}{=} \varphi(g(h+h')) = h + h' \\ &= \varphi(y) + \varphi(y'). \end{aligned}$$

Para todo $r \in R$, segue que

$$\begin{aligned} \varphi(ry) &= \varphi(rg(z+h)) = \varphi(g(r(z+h))) = \varphi(g(rz + rh)) \\ &\overset{(*)}{=} \varphi(g(rh)) = rh = r\varphi(y), \end{aligned}$$

onde a igualdade $(*)$ é devida ao fato que $z + z'$ e rz estão ambos em $Ker(g)$. Além disso, $(g \circ \varphi)(y) = g(h) = y$, $\forall y \in G$. Logo, $g \circ \varphi = 1_G$.

(iii) $\Rightarrow$ (i) Mostremos que $F = Im(f) \oplus H$, onde $H = Im(\varphi)$. Se $x \in Im(f) \cap H$ existem elementos $z \in E$ e $y \in G$ tais que $x = f(z) = \varphi(y)$. Mas $g(x) = 0$, daí resulta que, $0 = g(f(z)) = g(\varphi(y)) = (g \circ \varphi)(y) = y$. Logo, $x = 0$ e assim $Im(f) \cap H = 0$.

Agora, seja $x \in F$. Então é claro que $x - \varphi(g(x)) \in Ker(g) = Im(f)$. Chamemos $v = x - \varphi(g(x))$ e daí, $x = v + \varphi(g(x)) \in Im(f) + Im(\varphi)$. Assim, $F = Im(f) \oplus H$ e a condição (i) é satisfeita. □

Corolário 1.51. *Se a seqüência exata curta* $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ *cinde então* $F \simeq E \oplus G$.

Demonstração: Como a seqüência cinde, então $F = Im(f) \oplus Im(\varphi)$, segundo (iii)$\Rightarrow$(i) da demonstração acima. Além disso, φ é injetor (pois $g \circ \varphi = 1_G$, isto é, φ tem inversa à esquerda) daí, $G \simeq Im(\varphi)$. Por ser f injetor, $Im(f) \simeq E$. Logo, $F = Im(f) \oplus Im(\varphi) \simeq E \oplus G$. □

Capítulo 2

Módulos Projetivos

Nesse capítulo, definimos os módulos projetivos e apresentamos algumas definições equivalentes via seqüências exatas. Mostramos também que todo módulo projetivo é um somando direto de um módulo livre. Por isso, estudamos um pouco sobre módulos livres na segunda seção do presente capítulo.

2.1 O Grupo de Homomorfismos

Sejam M e N R-módulos. Denotamos o conjunto de todos os R-homomorfismos de M em N por $Hom_R(M,N)$. Definimos a soma de dois elementos $f, g \in Hom_R(M,N)$ por $(f+g)(x) = f(x) + g(x)$, para todo $x \in M$. Vamos mostrar que este conjunto com a operação acima definida é um grupo abeliano.

Primeiramente, devemos mostrar que $f+g \in Hom_R(M,N)$. De fato, dados $x, x_1, x_2 \in M$ e $r \in R$, temos que

$$\begin{aligned}(f+g)(x_1+x_2) &\overset{\text{def}}{=} f(x_1+x_2) + g(x_1+x_2)\\ &\overset{(1)}{=} f(x_1) + f(x_2) + g(x_1) + g(x_2)\\ &\overset{(2)}{=} (f(x_1) + g(x_1)) + (f(x_2) + g(x_2))\\ &\overset{\text{def}}{=} (f+g)(x_1) + (f+g)(x_2) \quad \text{e}\end{aligned}$$

$$\begin{aligned}(f+g)(rx) &\overset{\text{def}}{=} f(rx) + g(rx) \overset{(1)}{=} rf(x) + rg(x)\\ &\overset{(2)}{=} r(f(x) + g(x)) \overset{\text{def}}{=} r((f+g)(x)),\end{aligned}$$

onde nas igualdades (1) usamos que f e g são R-homomorfismos e em (2) usamos que N é um R-módulo.

Provemos que $Hom_R(M, N)$ é um grupo abeliano.

(i) A operação $+$ é claramente associativa.

(ii) Claramente, o homomorfismo nulo é o elemento neutro para a operação $+$, isto é, $f + 0 = 0 + f = f$, onde $0(x) = 0$, para todo $x \in M$.

(iii) Para todo $f \in Hom_R(M, N)$, existe $g \in Hom_R(M, N)$ definido por $g(x) = -f(x)$, para todo $x \in M$. É claro que $f + g = g + f = 0$.

(iv) Sejam $f, g \in Hom_R(M, N)$. Para todo $x \in M$, temos que $(f + g)(x) = f(x) + g(x) \overset{(*)}{=} g(x) + f(x) = (g + f)(x)$, a igualdade $(*)$ segue do fato de que N é um R-módulo. Portanto, $f + g = g + f$.

Aqui, vale acrescentar que nem sempre $Hom_R(M, N)$ possui uma estrutura de R-módulo, a menos que o anel R seja comutativo. Para maiores detalhes, veja [6].

2.2 Módulos Livres

Dado um anel R, notamos por $R^{(I)}$ o conjunto de todas as famílias quase-nulas $(\lambda_i)_{i \in I}$ em que $\lambda_i \in R$, para todo $i \in I$, sendo esse um conjunto não vazio qualquer. Notemos que $R^{(I)}$ é uma soma direta $\bigoplus_{i \in I} R_i$ onde cada somando é igual a R.

Seja M um R-módulo. Uma família $(x_i)_{i \in I}$ de elementos em M, indexada por um conjunto não vazio I qualquer, diz-se *linearmente independente* ou *livre*, se para toda família $(\lambda_i)_{i \in I} \in R^{(I)}$ tal que $\sum_{i \in I} \lambda_i x_i = 0$ tivermos que $\lambda_i = 0$, para todo $i \in I$. Caso contrário, a família $(x_i)_{i \in I}$ em M diz-se linearmente dependente.

Um elemento $x \in M$ é uma *combinação linear* dos elementos da família $(x_i)_{i \in I}$ em M, se existe $(\lambda_i)_{i \in I} \in R^{(I)}$ tal que $x = \sum_{i \in I} \lambda_i x_i$.

A soma acima está bem definida, pois apenas um número finito de somandos é diferente de zero.

É fácil verificar que dado um subconjunto K de M, o submódulo gerado

por K é o conjunto de todas as combinações lineares de elementos de K. Assim, podemos definir "base"de um R-módulo M.

Definição 2.1. *Uma família $(x_i)_{i\in I}$ de elementos em M diz-se uma base de M se é uma família linearmente independente e se gera M.*

Definição 2.2. *Um R-módulo M é dito livre se M possui uma base, isto é, M possui uma família linearmente independente que o gera.*

Exemplo 2.3. Todo espaço vetorial sobre um corpo K é um K-módulo livre.

Exemplo 2.4. Se R é um anel com unidade e n é um inteiro ≥ 1 então o produto cartesiano R^n é um R-módulo livre. Uma base é dada por $e_1 = (1, 0, 0, \cdots, 0)$, $\cdots$, $e_n = (0, 0, 0, \cdots, 1)$.

De fato, se $a_1e_1 + \cdots + a_ne_n = (0, \cdots, 0)$ então $(a_1, \cdots, a_n) = (0, \cdots, 0)$ e portanto, $a_1 = \cdots = a_n = 0$. Por outro lado, dado $(a_1, \cdots, a_n) \in R^n$ temos que $(a_1, \cdots, a_n) = a_1e_1 + \cdots + a_ne_n$. A base $e_1, e_2, \cdots, e_n$ é chamada a *base canônica* de R^n. Em particular, R é um R-módulo livre com base $\{1\}$.

Mais geralmente, dado um anel R, consideremos a soma direta $R^{(I)}$. Indicamos por e_k o elemento $e_k = (x_i)_{i\in I}$, tal que $x_k = 1$ e $x_i = 0$ se $i \neq k$. A família $E = (e_k)_{k\in I}$ é uma base de $R^{(I)}$, chamada *base canônica*. Logo, $R^{(I)}$ é um R-módulo livre.

Exemplo 2.5. Seja R um anel comutativo com unidade. Então qualquer subconjunto de R com mais de um elemento não pode ser linearmente independente. Consideremos $X \subset R$ com mais de um elemento. Sejam $a, b \in X$. Então a combinação linear $ba + (-a)b = 0$, pois R é comutativo e $-a$ e b em R não são ambos nulos.

Resulta então que as bases do R-módulo R são conjuntos unitários. Além disso, não é difícil ver que $\{u\}$ é uma base de R se, e somente se, u é um elemento invertível em R. Concluímos que as únicas bases do $\mathbb{Z}$-módulo $\mathbb{Z}$ são $\{1\}$ e $\{-1\}$.

Exemplo 2.6. O corpo $\mathbb{Q}$ dos números racionais, considerado como um $\mathbb{Z}$-módulo, não é livre. Observamos primeiramente que dois elementos quaisquer em $\mathbb{Q}$ são linearmente dependentes. De fato, sejam $r = \frac{a}{b}$ e $s = \frac{c}{d}$ em $\mathbb{Q}$. Se

$r = 0$ então $1r + 0s = 0$. Se $r \neq 0$ então $(bc)r - (ad)s = 0$ e é claro que $ad \neq 0$. Em ambos os casos, concluímos que r e s são linearmente dependentes.

Suponhamos que $\mathbb{Q}$ seja um $\mathbb{Z}-$módulo livre, então sua base possui apenas um elemento, digamos $\frac{a}{b}$, com $a \neq 0$. Tomemos um número primo p que não divide b; é claro que não existe $n \in \mathbb{Z}$ tal que $\frac{1}{p} = n\frac{a}{b}$.

Exemplo 2.7. Nem sempre um submódulo de um módulo livre é livre. Consideremos o anel $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Como um módulo sobre si mesmo, $\mathbb{Z}_6$ é livre, mas o $\mathbb{Z}_6$-submódulo $H = \{\overline{0}, \overline{2}, \overline{4}\}$ não o é, pois todo subconjunto unitário de H é linearmente dependente.

Podemos ser levados a pensar que os módulos livres comportam-se de forma análoga aos espaços vetoriais, o que nem sempre é verdade, por isso apresentamos abaixo alguns contra-exemplos.

Contra-exemplo 1: Não é verdade que todo subconjunto linearmente independente de um módulo livre pode ser ampliado a uma base. De fato, o conjunto $\{2\}$ em $\mathbb{Z}$ é linearmente independente. No entanto, não é uma base (não é invertível em $\mathbb{Z}$) e nem pode ser ampliado a uma, pois pelo Exemplo 2.5, todo conjunto com dois ou mais elementos, é linearmente dependente.

Contra-exemplo 2: É falso que todo conjunto gerador contém uma base. O conjunto $\{2, 3\}$ é um conjunto gerador de $\mathbb{Z}$, porém não contém 1 e nem -1.

Contra-exemplo 3: Se numa família de elementos $(x_i)_{i\in I}$ de um R-módulo M, um deles é combinação linear dos outros, a família não é uma base. Para espaços vetoriais a recíproca é verdadeira, mas é falsa para módulos.

Basta considerarmos novamente a família $\{2, 3\}$ em $\mathbb{Z}$ que não é uma base e nenhum dos dois elementos é múltiplo inteiro do outro.

Proposição 2.8. *Sejam M e N R-módulos tal que M seja um módulo livre e X uma base de M. Dada uma função $f : X \to N$ é possível estendê-la a um R-homomorfismo $\overline{f} : M \to N$, isto é, construir um R-homomorfismo $\overline{f} : M \to N$ tal que $\overline{f}$ restrito a X coincida com f. Tal homomorfismo é único.*

Demonstração: Seja $X = (x_i)_{i\in I}$ uma base de M. Então todo elemento $m \in M$ pode ser escrito de modo único como $m = \sum_{i\in I} \lambda_i x_i$ com $(\lambda_i)_{i\in I} \in R^{(I)}$.

Assim, podemos definir $\overline{f}(m) = \sum_{i\in I}\lambda_i f(x_i)$. Verifiquemos que $\overline{f}$ é um R-homomorfismo. Sejam $m_1, m_2 \in M$. Então $m_1 = \sum_{i\in I}\lambda_i x_i$ e $m_2 = \sum_{i\in I}\alpha_i x_i$. Daí,

$$\begin{aligned}
\overline{f}(m_1+m_2) &= \overline{f}(\sum_{i\in I}(\lambda_i+\alpha_i)x_i) = \sum_{i\in I}(\lambda_i+\alpha_i)f(x_i) \\
&= \sum_{i\in I}\lambda_i f(x_i) + \sum_{i\in I}\alpha_i f(x_i) = \overline{f}(m_1)+\overline{f}(m_2) \text{ e} \\
\overline{f}(rm) &= \overline{f}(r\sum_{i\in I}\lambda_i x_i) = \overline{f}(\sum_{i\in I}(r\lambda_i)x_i) \\
&= \sum_{i\in I} r(\lambda_i f(x_i)) = r\sum_{i\in I}\lambda_i f(x_i) \\
&= r\overline{f}(m).
\end{aligned}$$

A unicidade é facilmente verificada. □

Corolário 2.9. *Se M é um R-módulo livre com base $X = (x_i)_{i\in I}$ então M é isomorfo a $R^{(I)}$.*

Demonstração: Basta definirmos $f : X \to R^{(I)}$ por $f(x_i) = e_i$ para todo $i \in I$ (onde $(e_i)_{i\in I}$ é a base canônica de $R^{(I)}$, veja Exemplo 2.4). Considerando a única extensão $\overline{f} : M \to R^{(I)}$ obtida na proposição anterior, segue que $\overline{f}$ é um R-isomorfismo. De fato, seja $x \in Ker(\overline{f})$. Então $\overline{f}(x) = 0$. Como $x = \sum_{i\in I}\lambda_i x_i$, então $\overline{f}(x) = \sum_{i\in I}\lambda_i f(x_i) = \sum_{i\in I}\lambda_i e_i = 0$. Logo, $\lambda_i = 0$ para todo $i \in I$. Portanto, $\overline{f}$ é injetor.

Seja $y \in R^{(I)}$. Então $y = \sum_{i\in I}\lambda_i e_i = \sum_{i\in I}\lambda_i f(x_i) = \overline{f}(\sum_{i\in I}\lambda_i x_i) = \overline{f}(x) = y$. Logo, $\overline{f}$ é sobrejetor. □

Corolário 2.10. *Todo R-módulo M é uma imagem epimórfica de um módulo livre.*

Demonstração: Seja $X = (x_i)_{i\in I}$ uma família de geradores de M (sempre é possível determinar tal conjunto de geradores de M; o próprio M o é).

Definimos $f : E \to M$ por $f(e_i) = x_i$, $\forall i \in I$, onde E é a base do Exemplo 2.4. Pela Proposição 2.8, estendemos f unicamente ao R-homomorfismo $\overline{f} : R^{(I)} \to M$ que é dado por $\overline{f}(\lambda) = \sum_{i\in I}\lambda_i f(e_i) = \sum_{i\in I}\lambda_i x_i$, onde $\lambda = \sum_{i\in I}\lambda_i e_i$ e $(\lambda_i)_{i\in I} \in R^{(I)}$.

Pelo fato de que $(x_i)_{i\in I}$ é uma família de geradores de M segue que $\overline{f}$ é sobrejetor. Portanto, M é uma imagem epimórfica do R-módulo livre $R^{(I)}$. □

2.3 Módulos Projetivos

Definição 2.11. *Sejam U e M R-módulos. O módulo M é dito U-projetivo se para qualquer R-módulo N, $f \in Hom_R(M,N)$ e $\pi \in Hom_R(U,N)$ um epimorfismo, existe $h \in Hom_R(M,U)$ tal que $\pi \circ h = f$. O diagrama abaixo ilustra essa situação*

$$\begin{array}{ccccc} & & M & & \\ & \swarrow^{h} & \downarrow{\scriptstyle f} & & \\ U & \xrightarrow[\pi]{} & N & \longrightarrow & 0. \end{array}$$

O módulo M é dito *projetivo* se M é P-projetivo para todo R-módulo P.

Proposição 2.12. *Todo módulo livre é projetivo.*

Demonstração: Seja M um R-módulo livre. Sejam U e N R-módulos, $f : M \to N$ um homomorfismo e $\pi : U \to N$ um epimorfismo. Mostremos que existe $h \in Hom_R(M,U)$ tal que $\pi \circ h = f$ tal como ilustra o diagrama

$$\begin{array}{ccccc} & & M & & \\ & \swarrow^{h} & \downarrow{\scriptstyle f} & & \\ U & \xrightarrow[\pi]{} & N & \longrightarrow & 0. \end{array}$$

Seja $(x_i)_{i\in I}$ uma base de M. Chamemos $y_i = f(x_i)$, para todo $i \in I$. Como π é um epimorfismo, existem $u_i \in U$ tal que $\pi(u_i) = y_i$, para todo $i \in I$. Definimos $h'(x_i) = u_i$, para todo $i \in I$ e como qualquer $m \in M$ é escrito unicamente como $m = \sum_{i\in I} \lambda_i m_i$, segue pela Proposição 2.8 que h' pode estender-se a uma função $h : M \to U$ definindo $h(m) = \sum_{i\in I} \lambda_i h'(x_i) = \sum_{i\in I} \lambda_i u_i$ para todo $m \in M$. Ainda pela proposição citada, segue que h é um R-

homomorfismo. Notemos que para todo $m \in M$

$$\begin{aligned}(\pi \circ h)(m) &= \pi(\sum_{i\in I} \lambda_i u_i) = \sum_{i\in I} \lambda_i \pi(u_i) \\ &= \sum_{i\in I} \lambda_i y_i = \sum_{i\in I} \lambda_i f(x_i) = \sum_{i\in I} f(\lambda_i x_i) \\ &= f(\sum_{i\in I} \lambda_i x_i) = f(m).\end{aligned}$$

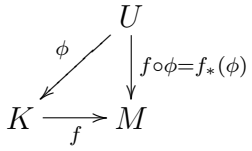
Logo, M é um R-módulo projetivo. □

Corolário 2.13. *Todo anel com unidade visto como um módulo sobre si mesmo é um módulo projetivo.*

Seja U um R-módulo. A todo R-homomorfismo $f : K \to M$, associamos uma função f_* do seguinte modo

$$\begin{aligned}f_* : \ Hom_R(U,K) &\to Hom_R(U,M) \\ \phi &\mapsto f_*(\phi) = f \circ \phi.\end{aligned}$$

O diagrama abaixo ilustra tal situação



Mostremos que f_* é um homomorfismo de grupos (abelianos). De fato, $\phi_1, \phi_2 \in Hom_R(U,K)$. Então, para todo $x \in U$, temos que

$$\begin{aligned}(f_*(\phi_1 + \phi_2))(x) &= (f \circ (\phi_1 + \phi_2))(x) = f((\phi_1 + \phi_2)(x)) \\ &= f(\phi_1(x) + \phi_2(x)) = f(\phi_1(x)) + f(\phi_2(x)) \\ &= (f \circ \phi_1)(x) + (f \circ \phi_2)(x) \\ &= ((f \circ \phi_1) + (f \circ \phi_2))(x).\end{aligned}$$

Logo, $f_*(\phi_1 + \phi_2) = f_*(\phi_1) + f_*(\phi_2)$.

Teorema 2.14. *Seja* $0 \to K \xrightarrow{f} M \xrightarrow{g} N \to 0$ *uma seqüência exata curta de* R*-módulos. Então a seqüência induzida de grupos abelianos, como segue,* $0 \to Hom_R(U,K) \xrightarrow{f_*} Hom_R(U,M) \xrightarrow{g_*} Hom_R(U,N)$ *é exata.*

Demonstração: Primeiro provemos que $Ker(f_*) = 0$. Seja $\phi \in Ker(f_*)$. Então $f_*(\phi) = 0$ e isso implica que $f \circ \phi = 0$. Como f é injetor e $f(\phi(x)) = 0$, para todo $x \in U$; segue que $\phi(x) = 0$, para todo $x \in U$. Logo, ϕ é o homomorfismo nulo e portanto, f_* é um homomorfismo injetor de grupos abelianos.

Provemos que $Im(f_*) = Ker(g_*)$. Seja $\beta \in Im(f_*)$. Então existe $\phi \in Hom_R(U, K)$ tal que $f_*(\phi) = \beta$. Aplicando g_* em β, segue que $g_*(\beta) = g_*(f_*(\phi)) = g_*(f \circ \phi) = g \circ (f \circ \phi)$. Mas $g \circ f = 0$ pela Proposição 1.42. Portanto, $g_*(\beta) = 0$ e assim, $Im(f_*) \subset Ker(g_*)$.

Agora provemos que $Ker(g_*) \subset Im(f_*)$. Seja $\beta \in Ker(g_*)$. Para todo $z \in U$, temos que $0 = (g_*(\beta))(z) = (g \circ \beta)(z) = g(\beta(z))$ e isso implica que $\beta(z) \in Ker(g) = Im(f)$.

Assim, para cada $z \in U$, existe $x \in K$ tal que $\beta(z) = f(x)$ e x é único, pois f é injetor. Portanto, podemos definir $\psi : U \to K$ tal que $\psi(z) = x$, onde $\beta(z) = f(x)$. Para todo $z \in U$, $(f \circ \psi)(z) = f(\psi(z)) = f(x) = \beta(z)$ e portanto, $\beta = f \circ \psi = f_*(\psi)$. Só resta provarmos que ψ é um R-homomorfismo. Sejam $z_1, z_2 \in U$. Então

$$\begin{aligned} f(\psi(z_1 + z_2)) &= \beta(z_1 + z_2) \overset{(*)}{=} \beta(z_1) + \beta(z_2) \\ &= (f \circ \psi)(z_1) + (f \circ \psi)(z_2) \\ &= f(\psi(z_1) + \psi(z_2)) \end{aligned}$$

e pela injetividade de f, segue que $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$.

Dados $r \in R$ e $z \in U$, segue que

$$\begin{aligned} f(\psi(rz)) &= \beta(rz) \overset{(*)}{=} r\beta(z) \\ &= r(f(\psi(z))) = f(r\psi(z)) \end{aligned}$$

e novamente pela injetividade de f vem que $\psi(rz) = r\psi(z)$.

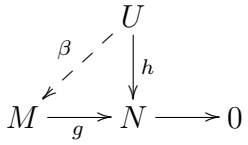
A igualdade $(*)$ em ambos os casos é devido ao fato de que β é um R-homomorfismo. □

Teorema 2.15. *Sejam M e U R-módulos. São equivalentes:*

(i) *U é M-projetivo.*

(ii) *Para toda seqüência exata curta de R-módulos* $0 \to K \xrightarrow{f} M \xrightarrow{g} N \to 0$*, a seqüência induzida de grupos abelianos* $0 \to Hom_R(U,K) \xrightarrow{f_*} Hom_R(U,M) \xrightarrow{g_*} Hom_R(U,N) \to 0$ *é também exata.*

Demonstração: (i)⇒(ii) Devido ao Teorema 2.14, é suficiente provarmos que g_* é sobrejetor. Seja $h \in Hom_R(U,N)$. Temos o seguinte diagrama



e por ser U um módulo M-projetivo, existe $\beta \in Hom_R(U,M)$ tal que $g \circ \beta = h$, isto é, $g_*(\beta) = h$. Portanto, g_* é sobrejetor.

(ii)⇒(i) Sejam N um R-módulo, $g \in Hom_R(M,N)$ um epimorfismo e $h \in Hom_R(U,N)$.

Consideremos a seqüência exata curta $0 \to Ker(g) \xrightarrow{i} M \xrightarrow{g} N \to 0$, onde i é a inclusão, temos por hipótese que a seqüência induzida de grupos abelianos $0 \to Hom_R(U,Ker(g)) \xrightarrow{i_*} Hom_R(U,M) \xrightarrow{g_*} Hom_R(U,N) \to 0$ é exata e daí, g_* é sobrejetor.

Logo, existe $\beta \in Hom_R(U,M)$ tal que $g_*(\beta) = h$, ou seja, $g \circ \beta = h$. Portanto, U é M-projetivo. □

Teorema 2.16. *Seja M um R-módulo. Então as seguintes condições são equivalentes:*

(i) *M é projetivo.*

(ii) *Para toda seqüência exata de R-módulos $K \xrightarrow{f} L \xrightarrow{g} N$, a seqüência induzida de grupos abelianos $Hom_R(M,K) \xrightarrow{f_*} Hom_R(M,L) \xrightarrow{g_*} Hom_R(M,N)$ é também exata.*

(iii) *M é um somando direto de todo módulo do qual ele é uma imagem epimórfica.*

(iv) *M é um somando direto de um módulo livre.*

Demonstração: (i)⇒(ii) Basta mostrarmos que $Im(f_*) = Ker(g_*)$. Seja $\phi \in Im(f_*)$. Então $\phi = f_*(\varphi)$ para algum $\varphi \in Hom_R(M,K)$. Mas $g_*(\phi) = g_*(f_*(\varphi)) = g_*(f \circ \varphi) = g \circ f \circ \varphi = 0$, pois $g \circ f = 0$ pela Proposição 1.42. Logo, $Im(f_*) \subset Ker(g_*)$.

Agora mostremos que $Ker(g_*) \subset Im(f_*)$. Seja $\varphi \in Ker(g_*)$. Então $g_*(\varphi) = 0$ e portanto, $g \circ \varphi = 0$, isto é, $g(\varphi(x)) = 0, \forall x \in M$. Logo, $Im(\varphi) \subset Ker(g) = Im(f)$. Podemos considerar o diagrama

$$\begin{array}{ccccc} & & & & M \\ & & & \swarrow^{\psi} & \downarrow{\scriptstyle \varphi} \\ K & \xrightarrow[f]{} & Im(f) & \longrightarrow & 0. \end{array}$$

Como M é projetivo, segue que existe $\psi \in Hom_R(M, K)$ tal que $\varphi = f \circ \psi$. Logo, $\varphi = f_*(\psi)$, isto é, $Ker(g_*) \subset Im(f_*)$. Concluímos então que $Ker(g_*) = Im(f_*)$.

(ii)⇒(i) Sejam T e P R-módulos, $g : T \to P$ um epimorfismo e $\varphi : M \to P$ um homomorfismo. Queremos mostrar que existe $\psi : M \to T$ tal que $g \circ \psi = \varphi$.

Consideremos a seqüência exata $T \xrightarrow{g} P \to 0$. Por hipótese, a seqüência induzida de grupos abelianos $Hom_R(M, T) \xrightarrow{g_*} Hom_R(M, P) \to 0$ é exata e portanto, g_* é sobrejetor. Como $\varphi \in Hom_R(M, P)$, existe $\psi \in Hom_R(M, T)$ tal que $g_*(\psi) = g \circ \psi = \varphi$ e isso nos diz que M é projetivo.

(i)⇒(iii) Seja $\varphi : N \to M$ um epimorfismo. Consideremos 1_M, o homomorfismo identidade. Sendo M projetivo, então existe $\psi : M \to N$, tal que $\varphi \circ \psi = 1_M$. Pela Proposição 1.50, a seqüência exata $(*)$ cinde e pelo Corolário 1.51, M é um somando direto de N.

$$\begin{array}{ccccccccc} & & & & & & M & & \\ & & & & & \swarrow^{\psi} & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & Ker(\varphi) & \xrightarrow{i} & N & \xrightarrow{\varphi} & M & \longrightarrow & 0 \qquad (*). \end{array}$$

(iii)⇒(iv) Pelo Corolário 2.10, todo módulo é uma imagem epimórfica de um módulo livre, então existe um módulo livre N e um epimorfismo $\varphi : N \to M$. Por (iii), M é um somando direto de N.

(iv)⇒(i) Seja L um módulo livre tal que $L = M \oplus S$ para algum R-módulo S. Sejam P e N R-módulos, $f : P \to N$ um epimorfismo e $g : M \to N$ um homomorfismo. Provemos que existe $\psi : M \to P$ tal que $f \circ \psi = g$.

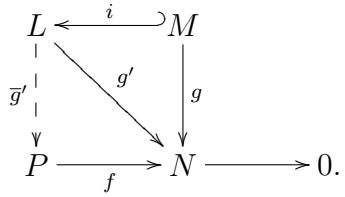
Como $L = M \oplus S$, todo elemento $x \in L$ é escrito de modo único como $x = x_1 + x_2$, com $x_1 \in M$ e $x_2 \in S$. Podemos estender a função $g : M \to N$

a um homomorfismo $g' : L \to N$, pois L é livre, tal que $g'(x) = g'(x_1 + x_2) = g(x_1)$. Mostremos que g' é realmente um R-homomorfismo.

Sejam $x, y \in L$ e $r \in R$. Então $x = x_1 + x_2$ e $y = y_1 + y_2$ com $x_1, y_1 \in M$ e $x_2, y_2 \in S$. Portanto,

$$\begin{aligned} g'(x+y) &= g'(x_1 + y_1 + x_2 + y_2) = g(x_1 + y_1) \\ &= g(x_1) + g(y_1) = g'(x) + g'(y) \text{ e} \\ g'(rx) &= g'(r(x_1 + x_2)) = g'(rx_1 + rx_2) \\ &= g(rx_1) = rg(x_1) = rg'(x). \end{aligned}$$

Mas L é projetivo, pois L é livre. Daí existe $\overline{g}' : L \to P$ tal que $f \circ \overline{g}' = g'$. O diagrama abaixo ilustra essa situação



Tomando $\psi = \overline{g}' \circ i$, temos que $(f \circ \psi)(m) = (f \circ \overline{g}' \circ i)(m) = (g' \circ i)(m) = g'(i(m)) = g'(m) = g(m)$, para todo $m \in M$. Logo, M é projetivo. □

Exemplo 2.17. $\{0\}$ é trivialmente um R-módulo projetivo para qualquer anel R.

Exemplo 2.18. Todo espaço vetorial V sobre um corpo K é um K-módulo projetivo, assim como todos os seus subespaços vetoriais, basta lembrarmos que todo subespaço vetorial de V é um somando direto do mesmo.

Exemplo 2.19. Sejam A um anel e $R = M_2(A)$ o anel das matrizes de ordem 2 sobre A. É fácil verificar que os conjuntos

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in A \right\} \quad e \quad J = \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} : c, d \in A \right\}$$

são ideais à esquerda de R, isto é, submódulos de ${}_RR$ e que ${}_RR = I \oplus J$. Como ${}_RR$ é um módulo livre, segue que I e J são R-módulos projetivos.

Na verdade, esse exemplo pode ser generalizado se tomarmos $R = M_n(A)$ o anel das matrizes de ordem n sobre o anel A e para todo $k \in \{1, 2, \cdots, n\}$,

$I_k = (a_{ij})$ tal que $a_{ij} \in A$ para $i, j \in \{1, \cdots, n\}$ e $a_{ij} = 0$ se $j \neq k$. Não é difícil ver que I_k é um ideal à esquerda de R, para todo $k \in \{1, 2, \cdots, n\}$ e é claro que ${}_RR = \bigoplus_{k=1}^{n} I_k$ e, portanto, cada I_k é um R-módulo projetivo.

Capítulo 3

Módulos Injetivos

Nesse capítulo, definimos os módulos injetivos. Na verdade, esses são uma dualização dos projetivos, pois invertemos o sentido das "flechas", isto é, trocamos epimorfismos por monomorfismos. Apresentamos algumas definições equivalentes via seqüências exatas.

Definição 3.1. *Sejam U, M e K R-módulos. Então M é dito U-injetivo se dados $f \in Hom_R(K, M)$ e $\rho \in Hom_R(K, U)$ um monomorfismo, existe $h \in Hom_R(U, M)$ tal que $h \circ \rho = f$. Ilustramos essa situação através do diagrama*

$$\begin{array}{ccccc} & & M & & \\ & & \uparrow{\scriptstyle f} & \nwarrow^{h} \searrow & \\ 0 & \longrightarrow & K & \xrightarrow[\rho]{} & U. \end{array}$$

O módulo M é dito *injetivo* se M é P-injetivo para todo R-módulo P.

Seja U um R-módulo. A todo R-homomorfismo $f : K \to M$, associamos uma função f^* do seguinte modo:

$$\begin{array}{rccl} f^* : & Hom_R(M, U) & \to & Hom_R(K, U) \\ & \phi & \mapsto & f^*(\phi) = \phi \circ f. \end{array}$$

O diagrama abaixo ilustra tal situação:

$$\begin{array}{ccccc} & & U & & \\ & & \uparrow{\scriptstyle f^*(\phi)=\phi\circ f} & \nwarrow^{\phi} \searrow & \\ K & & \xrightarrow[f]{} & & M \end{array}$$

Mostremos que f^* é um homomorfismo de grupos (abelianos). De fato, sejam $\phi_1, \phi_2 \in Hom_R(M,U)$. Então, para todo $x \in K$, temos que

$$\begin{aligned}(f^*(\phi_1+\phi_2))(x) &= ((\phi_1+\phi_2)\circ f)(x) = (\phi_1+\phi_2)(f(x)) \\ &= \phi_1(f(x)) + \phi_2(f(x)) = (\phi_1\circ f)(x) + (\phi_2\circ f)(x) \\ &= (f^*(\phi_1))(x) + (f^*(\phi_2))(x) \\ &= ((f^*(\phi_1) + f^*(\phi_2))(x).\end{aligned}$$

Logo, $f^*(\phi_1+\phi_2) = f^*(\phi_1) + f^*(\phi_2)$.

Teorema 3.2. *Seja* $0 \to K \xrightarrow{f} M \xrightarrow{g} N \to 0$ *uma seqüência exata curta de R-módulos. Então a seqüência induzida de grupos abelianos, como segue,* $0 \to Hom_R(N,U) \xrightarrow{g^*} Hom_R(M,U) \xrightarrow{f^*} Hom_R(K,U)$ *é também exata.*

Demonstração: Primeiramente provemos que $Ker(g^*) = 0$. Seja $\varphi \in Ker(g^*)$. Então $g^*(\varphi) = 0$ e daí, $\varphi \circ g = 0$. Como g é sobrejetor, segue que para todo $n \in N$, existe $m \in M$ tal que $g(m) = n$. Daí, $\varphi(n) = \varphi(g(m)) = (\varphi\circ g)(m) = 0$. Portanto, $\varphi(n) = 0$, para todo $n \in N$ e φ é o homomorfismo nulo. Logo, g^* é o homomorfismo injetor de grupos abelianos.

Mostremos que $Im(g^*) = Ker(f^*)$. Seja $\beta \in Im(g^*)$. Então $\beta = g^*(\phi)$ para algum $\phi \in Hom_R(N,U)$. Aplicando f^* a β, segue que $f^*(\beta) = f^*(g^*(\phi)) = g^*(\phi)\circ f = (\phi\circ g)\circ f$. Mas $g\circ f = 0$ pela Proposição 1.42. Portanto, $f^*(\beta) = 0$ e assim, $Im(g^*) \subset Ker(f^*)$.

Agora mostremos que $Ker(g^*) \subset Im(f^*)$. Seja $\beta \in Ker(f^*)$. Então $f^*(\beta) = 0$, isto é, $\beta \circ f = 0$. Sendo g sobrejetor, temos que para todo $n \in N$, existe $m \in M$ tal que $g(m) = n$. Definimos a função

$$\begin{array}{rccl}\psi: & N & \to & U \\ & n & \mapsto & \psi(n) = \beta(m), \quad \text{onde } m \text{ é tal que } g(m) = n.\end{array}$$

É necessário mostrarmos que ψ está bem definida. De fato, suponhamos que $\psi(n) = \beta(m_1)$ tal que $g(m_1) = n$ e que $\psi(n) = \beta(m_2)$ tal que $g(m_2) = n$. Assim, $g(m_1) = g(m_2)$ e isso implica que $g(m_1 - m_2) = 0$. Logo, $m_1 - m_2 \in Ker(g) = Im(f)$. Então $f(k) = m_1 - m_2$, para algum $k \in K$. Portanto, $\beta(m_1 - m_2) = \beta(f(k)) = (\beta\circ f)(k) = 0$ e, como β é um homomorfismo, segue que $\beta(m_1) = \beta(m_2)$.

Por outro lado, para todo $m \in M$ temos que $(\psi \circ g)(m) = \psi(g(m)) = \psi(n) \stackrel{\text{def}}{=} \beta(m)$, onde $n = g(m)$, e isso nos diz que $\beta = \psi \circ g = g^*(\psi)$, isto é, $\beta \in Im(g^*)$.

Só resta mostrarmos que ψ é um R-homomorfismo. Sejam $n_1, n_2 \in N$ e $r \in R$. Então $n_1 = g(m_1)$ e $n_2 = g(m_2)$ para alguns $m_1, m_2 \in M$. Portanto,

$$\begin{aligned}
\psi(n_1 + n_2) &= \psi(g(m_1) + g(m_2)) = \psi(g(m_1 + m_2)) = (\psi \circ g)(m_1 + m_2) \\
&= \beta(m_1 + m_2) \stackrel{(*)}{=} \beta(m_1) + \beta(m_2) = \psi(n_1) + \psi(n_2) \text{ e} \\
\psi(rn_1) &= \psi(rg(m_1)) = \psi(g(rm_1)) = (\psi \circ g)(rm_1) \\
&= \beta(rm_1) = r\beta(m_1) = r\psi(n_1).
\end{aligned}$$

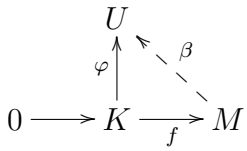
A igualdade $(*)$ é devido ao fato de que β é um R-homomorfismo. □

Teorema 3.3. *Sejam M e U R-módulos. São equivalentes:*

(i) *U é M-injetivo.*

(ii) *Para toda seqüência exata curta de R-módulos $0 \to K \stackrel{f}{\to} M \stackrel{g}{\to} N \to 0$, a seqüência induzida de grupos abelianos $0 \to Hom_R(N, U) \stackrel{g^*}{\to} Hom_R(M, U) \stackrel{f^*}{\to} Hom_R(K, U) \to 0$ é também exata.*

Demonstração: (i)⇒ (ii) Devido ao Teorema 3.2, só resta provarmos que f^* é sobrejetor. Seja $\varphi \in Hom_R(K, U)$. Temos o seguinte diagrama



e por ser U um módulo M-injetivo, existe $\beta \in Hom_R(M, U)$ tal que $\beta \circ f = \varphi$, isto é, $f^*(\beta) = \varphi$. Portanto, f^* é sobrejetor.

(ii)⇒ (i) Sejam K um R-módulo, $f \in Hom_R(K, M)$ um monomorfismo e $h \in Hom_R(K, U)$.

Consideremos a seqüência exata curta $0 \to K \stackrel{f}{\to} M \stackrel{\pi}{\to} M/K \to 0$, onde π é a projeção canônica. Temos por hipótese que a seqüência induzida de grupos abelianos $0 \to Hom_R(M/K, U) \stackrel{\pi^*}{\to} Hom_R(M, U) \stackrel{f^*}{\to} Hom_R(K, U) \to 0$ é exata. Logo, f^* é sobrejetor e daí, existe $\beta \in Hom_R(M, U)$ tal que $f^*(\beta) = h$, ou seja, $\beta \circ f = h$. Logo, U é M-injetivo. □

Enunciamos agora, sem demonstrar, um resultado necessário para a demonstração do Teorema 3.5, o leitor pode consultar ([5], Proposition 5 - Corollary, pg 90).

Teorema 3.4. *Todo módulo é isomorfo a um submódulo de um módulo injetivo.*

Teorema 3.5. *Seja M um R-módulo. Então são equivalentes:*
(i) *M é injetivo.*
(ii) *Para toda seqüência exata de R-módulos $K \xrightarrow{f} L \xrightarrow{g} N$, seqüência induzida de grupos abelianos $Hom_R(N,M) \xrightarrow{g^*} Hom_R(L,M) \xrightarrow{f^*} Hom_R(K,M)$ é também exata.*
(iii) *M é um somando direto de todo módulo do qual ele é um submódulo.*

Demonstração: (i)⇒ (ii) Basta mostrarmos que $Im(g^*) = Ker(f^*)$. Seja $\phi \in Im(g^*)$. Então $\phi = g^*(\varphi)$ para algum $\varphi \in Hom_R(N,M)$. Mas $f^*(\phi) = f^*(g^*(\varphi)) = g^*(\varphi) \circ f = \varphi \circ g \circ f = 0$, pois $g \circ f = 0$, veja Proposição 1.42. Logo, $Im(g^*) \subset Ker(f^*)$.

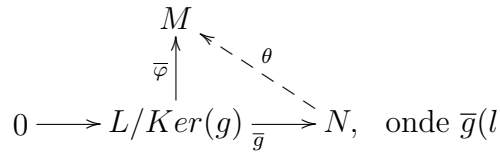
Agora a inclusão contrária. Seja $\varphi \in Ker(f^*)$. Então $f^*(\varphi) = 0$, isto é, $\varphi \circ f = 0$. Seja $y \in Ker(g)$. Então $y = f(x)$ para algum $x \in K$, pois $Ker(g) = Im(f)$. Assim, $\varphi(y) = \varphi(f(x)) = (\varphi \circ f)(x) = 0$. Logo, $Ker(g) \subset Ker(\varphi)$. Definimos a função

$$\begin{array}{rccc} \overline{\varphi}: & L/Ker(g) & \to & M \\ & l + Ker(g) & \mapsto & \varphi(l). \end{array}$$

Claramente que $\overline{\varphi}$ está bem definida, pois $Ker(g) \subset Ker(\varphi)$. Mostremos que $\overline{\varphi}$ é um R-homomorfismo. Sejam $l_1, l_2 \in L$ e $r \in R$.

$$\begin{array}{rcl} \overline{\varphi}((l_1 + Ker(g)) + (l_2 + Ker(g))) & = & \overline{\varphi}(l_1 + l_2 + Ker(g)) = \varphi(l_1 + l_2) \\ & = & \varphi(l_1) + \varphi(l_2) \\ & = & \overline{\varphi}(l_1 + Ker(g)) + \overline{\varphi}(l_2 + Ker(g)) \text{ e} \\ \overline{\varphi}(r(l_1 + Ker(g))) & = & \overline{\varphi}(rl_1 + Ker(g)) = \varphi(rl_1) = r\varphi(l_1) \\ & = & r\overline{\varphi}(l_1 + Ker(g)). \end{array}$$

Pelo teorema do homomorfismo, temos que $L/Ker(g) \simeq Im(g) \subset N$. Assim, a função $\overline{g} : L/Ker(g) \to N$ é um monomorfismo. Observemos o diagrama abaixo

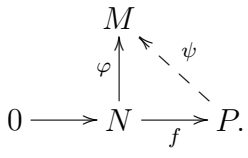


onde $\overline{g}(l + Ker(g)) = g(l)$, $\forall\, l \in L$.

Por ser M um módulo injetivo, existe $\theta \in Hom_R(N, M)$ tal que $\theta \circ \overline{g} = \overline{\varphi}$.

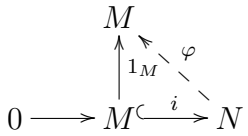
Além disso, para todo $l \in L$, temos que $\varphi(l) = \overline{\varphi}(l + Ker(g)) = = (\theta \circ \overline{g})(l + Ker(g)) = \theta(g(l)) = (\theta \circ g)(l)$. Portanto, $\varphi = \theta \circ g = g^*(\theta)$ e isso nos diz que $\varphi \in Im(g^*)$.

(ii)$\Rightarrow$ (i) Sejam P e N R-módulos, $f : N \to P$ um monomorfismo e $\varphi : N \to M$ um homomorfismo. Mostremos que existe $\psi : P \to M$ tal que $\psi \circ f = \varphi$, como ilustra o diagrama



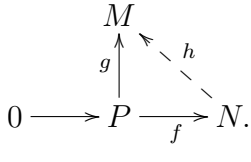
Por hipótese, a exatidão da seqüência $0 \to N \xrightarrow{f} P$ implica que a seqüência induzida de grupos abelianos $Hom_R(P, M) \xrightarrow{f^*} Hom_R(N, M) \to 0$ seja exata. Assim, f^* é sobrejetor, isto é, dado existe $\psi \in Hom_R(P, M)$ tal que $f^*(\psi) = \psi \circ f = \varphi$. Portanto, M é injetivo.

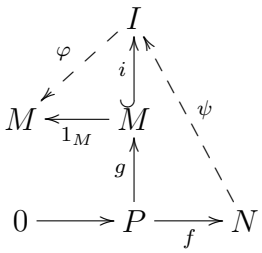
(i)$\Rightarrow$ (iii) Seja N um R-módulo. Suponhamos que M seja um submódulo de N. Como M é injetivo, existe $\varphi : N \to M$ tal que o diagrama abaixo comuta



ou seja , $\varphi \circ i = 1_M$. Pela Proposição 1.50, M é um somando direto de N.

(iii)$\Rightarrow$ (i) Sejam P e N R-módulos, $f : P \to N$ um monomorfismo e $g : P \to M$ um homomorfismo. Pelo Teorema 3.4, M é um submódulo de um módulo injetivo I. Vamos mostrar que existe $h : N \to M$ tal que $h \circ f = g$, como ilustra o diagrama abaixo





Observemos o diagrama acima. Como I é injetivo existe $\psi : N \to I$ tal que $\psi \circ f = i \circ g$. A seqüência exata curta $0 \to M \xrightarrow{i} I \xrightarrow{\pi} I/M \to 0$ cinde, pois M é um somando direto de I. Assim, existe $\varphi : I \to M$ tal que $\varphi \circ i = 1_M$, . Portanto, $\varphi \circ (\psi \circ f) = (\varphi \circ i) \circ g = 1_M \circ g = g$. Tomando h como $h = \varphi \circ \psi$, segue que M é injetivo. □

Exemplo 3.6. $\{0\}$ é trivialmente um R-módulo injetivo para qualquer anel R.

Exemplo 3.7. Seja V um K-espaço vetorial. Então todo subespaço vetorial de V é um K-módulo injetivo. Em particular, seja $V = \mathbb{R}^3$ o espaço vetorial sobre $\mathbb{R}$. Então os subespaços vetoriais de dimensão 0, 1 e 2, respectivamente, a origem, as retas (que contêm a origem) e os planos (que contêm a origem) são $\mathbb{R}$-módulos injetivos.

Conclusão

Por meio desse trabalho, a pesquisa e a forma de pensar em Matemática, mais especificamente em Álgebra, foram aperfeiçoados e certamente reorientados.

Estudar módulos foi importante para aumentar os horizontes e perceber as suas utilidades em diversos ramos, pois durante a pesquisa, embora tenhamos abordado um único tópico, estudar os módulos injetivos e projetivos, esses assuntos estudados estão em conectividade com outras áreas, por isso a sua importância para a iniciação a Álgebra.

O estudo do teorema do homomorfismo para módulos, a soma direta interna e as seqüências exatas, são a pedra angular do estudo da projetividade e injetividade de módulos. Os exemplos citados permitem perceber e entender com mais profundidade os resultados dos teoremas.

Certamente um trabalho proveitoso e por que não dizer de uma beleza matemática ímpar?

Finalmente, desejamos que esse trabalho possa ser útil a estudantes ou professores como um material de estudo e/ou consulta.

Referências Bibliográficas

[1] Azevedo, Alberto. *"Módulos Sobre Domínios Principais"*. In: 8ª Colóquio Brasileiro de Matemática, Impa, Rio de Janeiro, 1971.

[2] Hungerford, T.W., *"Algebra"*. Springer Verlag, 1974.

[3] Kunze, R., *"Álgebra Linear"*. LTC, 2ª ed., São Paulo, 1979.

[4] Lam, T.Y., *"A First Course in Noncommutative Rings"*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1991.

[5] Lambek, J., *"Rings and Modules "*, New York, 1986.

[6] Milies, F.P., *"Anéis e Módulos"*. Publicações do IME-USP, São Paulo, 1972.

[7] Raftery, J.G., *"On Strongly Prime Rings and Modules"*, Durban, 1986.