Universidade Federal do Amazonas

Pró-reitoria de Pesquisa e Pós-graduação

Departamento de Apoio à Pesquisa

Programa de Bolsas de Iniciação Científica

Relatório Final

PIB-E-0082/2010-2011

Rigor Científico em Álgebra Pura – Módulos e Domínios Euclidianos

Miqueias de Melo Lobo, CNPq

Orientador: Prof. Dr. Claudenir Freire Rodrigues

MANAUS-2011

Sumário

Introdução

Nosso objetivo nesse trabalho é desenvolver um pouco sobre a teoria dos módulos detalhando alguns resultados que em muitos livros são deixados como exercício para o leitor. Logo no início definimos formalmente módulo e submódulo. Apresentamos uma série de exemplo a fim de familiarizar quem está lendo. 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.

Objetivos

Geral:

O projeto *Rigor Científico em Álgebra Pura – Módulos e Domínios Euclidianos* tem como finalidade, antes mesmo de estudar o tema citado, abordar assuntos básicos de interesse geral na formação de estudantes que visam se especializar em algum ramo da Álgebra.

Específico:

O Objetivo específico deste projeto não difere muito de sua proposta geral, obviamente. A preocupação está em conceder ao aluno maior fluência em álgebra e torná-lo preparado para expor tais assuntos, seja como docente ou como palestrante. Ao tratar de módulos e domínios euclidianos e suas aplicações, o aluno verá a relação entre, pelo menos, três estruturas algébricas diferentes. São elas: Espaços Vetoriais (caso particular de módulo), Anéis e Grupos.

Metodologia

A metodologia utilizada neste projeto consistiu basicamente em pesquisa bibliográfica. O conhecimento adquirido foi assimilado através de discussões periódicas com o orientador, exposições para o comitê, estudos individuais e resolução de exercícios. Parte do conteúdo aqui exposto, deve-se à aulas oferecidas pelo departamento de matemática da Universidade Federal do Amazonas.

1 MÓDULOS

1.1 Noções Básicas

De início, estaremos supondo que algumas definições são conhecidas (como, por exemplo, a noção de Anéis e Espaços Vetoriais). A definição de Grupo, embora muito conhecida, será ainda apresentada e somente depois daremos a definição e muitos exemplos de Módulos.

Definição 1: *Seja M um conjunto não-vazio no qual está definida uma operação entre seus pares de elementos, denotada por:*

$$\begin{array}{rcccc} + & : & M \times M & \to & M \\ & & (a,b) & \rightsquigarrow & a+b \end{array}$$

Se $+$ cumpre as propriedades **(i)**, **(ii)** *e* **(iii)** *abaixo, então $(M,+)$ é dito um grupo.*

(i) *A operação $+$ é associativa, isto é, $u+(v+w)=(u+v)+w$ para quaisquer u,v,w em M*

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

(iii) *Todo elemento de M possui um elemento oposto em M, ou seja, para todo u em M, existe um v em M tal que $u+v=v+u=0$. Denotamos v por $-u$.*

Se em $(M,+)$ verifica-se a propriedade:

(iv) *$a+b=b+a$, para quisquer a,b em M,*

dizemos que $(M,+)$ é um grupo abeliano ou comutativo.

Exemplo 1: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ são grupos abelianos aditivos.

Exemplo 2: Seja $d \in \mathbb{Z}$. O conjunto de todos os múltiplos de d (denotaremos: $d \cdot \mathbb{Z}$) é um grupo com a operação usual de soma.

(i) Sejam a,b e $c \in d \cdot \mathbb{Z}$, $a=d \cdot x_1, b=d \cdot x_2$ e $c=d \cdot x_3$. A soma é claramente associativa para a,b e $c \in d \cdot \mathbb{Z}$, pois isso vale para todos os elementos de $\mathbb{Z}$.

(ii) Existe um elemento neutro e este é 0, pois $0=d \cdot 0 \in d \cdot \mathbb{Z}$.

(iii) Para todo $a \in d \cdot \mathbb{Z}$, $-a = d \cdot (-x_1)$ é o seu inverso.

É de fácil verificação que o conjunto $d \cdot \mathbb{Z}$ é um grupo abeliano.

Definição 2: *Seja M um grupo. Um subconjunto não-vazio N de M é um subgrupo de M (denotamos por $N \leq M$) quando, com a operação de M, o conjunto N é um grupo.*

Proposição 1: *Seja N um subconjunto não-vazio do grupo M. Então N é dito um subgrupo de M se, e somente se, as seguintes condições são satisfeitas:*

(i) *$a + b \in N$, para quaisquer $a, b \in N$.*

(ii) *Para todo $a \in N$, existe $-a \in N$ tal que $a + (-a) = (-a) + a = 0$*

Demonstração: Se N é grupo, as condições são satisfeitas. Agora, suponhamos que valham (i) e (ii). Claramente, $+$ é uma operação em N que é associativa. Por outro lado, dado $a \in N$, por (ii) existe $-a$ em N tal que $a + (-a) = (-a) + a = 0$. Por (i), $0 \in N$.

Definição 3: *Seja M um grupo abeliano. M é dito um módulo à esquerda sobre R (ou um R-módulo à esquerda) se a operação de multiplicação de um elemento de R por outros de M definida abaixo satisfaz as propriedades de (i) à (iv):*

$$\begin{array}{cccc} \cdot \; : & R \times M & \to & M \\ & (r, m) & \rightsquigarrow & r \cdot m \end{array}$$

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

(i) $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$.

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

Exemplo 3: 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 o produto do anel R.

Exemplo 4: Todo espaço vetorial sobre um corpo K é um K-módulo.

Exemplo 5: Todo grupo abeliano $(M, +)$ pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos inteiros definindo o produto por:

$$\cdot : \mathbb{Z} \times M \to M$$

$$n \cdot g = \begin{cases} 0 \ , & \text{se} \quad n = 0 \\ \underbrace{g + g + \cdots + g}_{n-vezes}, & \text{se} \quad n > 0 \\ \underbrace{(-g) + (-g) + \cdots + (-g)}_{n-vezes}, & \text{se} \quad n < 0 \end{cases}$$

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

Exemplo 6: O grupo trivial $\{0\}$ é um módulo sobre qualquer anel R.

Exemplo 7: Todo ideal em um anel R é um R-módulo com a soma induzida pela soma de R e a multiplicação definida pela multiplicação de R.

Definição 4: *Seja M um R-módulo. Um subconjunto $N \subset M$ é um R-submódulo de M ou, simplesmente, um submódulo se:*

(i) *N é um subgrupo abeliano aditivo de M.*

(ii) *N é fechado em relação ao produdo por elementos do anel, isto é, para todo $r \in R$ e todo $n \in N$ tem-se que $rn \in N$.*

Proposição 2: *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 todos $n_1, n_2 \in N$, $n_1 + n_2 \in N$.*

(ii) *Para todo $r \in R$ e para todo $n \in N$, $rn \in N$.*

Demonstração: Se N é um submódulo, então (i) e (ii) são satisfeitos. Reciprocamente, é claro que $+$ é uma operação em N, pois vale (i) que é associativa e comutativa. Como N é não-vazio, existe $n \in N$. Por (ii), $0 = 0 \cdot n \in N$. Agora, dado $n \in N$, temos que $-1 \in R$ (pois é o oposto da unidade 1). Daí, $-n = -1 \cdot n \in N$.

Exemplo 8: Dado um R-módulo M, temos que $\{0\}$ e M são submódulos de M, chamados submódulos triviais.

Exemplo 9: 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 10: 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 $I \cdot m = \{a \cdot m \mid a \in I\}$ é um submódulo de M.

Exemplo 11: Os ideais de R são submódulos de R quando R é considerado como um R-módulo sobre si mesmo.

Exemplo 12: 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

$$x + y = (n + n') + (k + k') \in N + K$$

e

$$rx = r(n + k) = rn + rk \in N + K$$

As propriedades da **Proposição 2** são facilmente verificadas.

Proposição 3: *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 de e M_i é um submódulo de M, para todo $i \in I$. Mostraremos 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 $m_1 \equiv m_2(\text{mod}N)$ se, e somente se, $m_1 - m_2 \in N$.É fácil verificar que $\equiv(\text{mod}N)$ é uma relação de equivalência.

Como M é um grupo abeliano, todo submódulo N de M é, na verdade, um subgrupo normal de N (isto é, $N + m = m + N$ para todo $m \in M$). portanto, não escrevemos classe lateral à direita ou à esquerda, pois ambas coincidem.
Podemos escrever para m sua respectiva classe de equivalência, que denotamos por $m + N$, ou mais explicitamente

$$\begin{array}{rcl} m + N & = & \{x \in M \ : \ x \equiv m(modN)\} \\ & & \{x \in M \ : \ x - m \in N\} \\ & & \{m + n \ : \ n \in N\} \end{array}$$

Proposição 4: *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 $m - 1 \equiv m_2(modN)$.*

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 isto implica que $m_1 \in m_2 + N$. Analogamente se prova 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

$$\begin{array}{rcccc} + & : & M/N \times M/N & \longrightarrow & M/N \\ & & (m_1 + N, m_2 + N) & \rightsquigarrow & (m_1 + m_2) + N \end{array}$$

Primeiramente provaremos 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, portanto, $(m_1 + m_2) - (m_3 + m_4) \in N$.

Mostraremos 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 $(0+N)+(m+N)=(0+m)+N=m+N$.

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

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

$$\begin{array}{rcccc}
+ & : & R\times M/N & \longrightarrow & M/N\\
 & & (r,m+N) & \longmapsto & r\cdot m+N
\end{array}$$

Escrevemos simplesmente $rm+N$ ao invés de $r\cdot m+N$. Vejamos que a operação $\cdot$ está bem dedefinida. 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

(i) $(r_1r_2)(m+N)=((r_1r_2)m)+N=r_1(r_2m)+N=r_1(r_2m+N)$.

(ii) $(r_1+r_2)(m+N)=(r_1+r_2)m+N=(r_1m+r_2m)+N=(r_1m+N)+(r_2m+N)$.

(iii) $r((m_1+m_2)+N)=(r(m_1+m_2))+N=(rm_1+rm_2)+N=(rm_1+N)+(rm_2+N)$.

(iv) $1(m+N)=1m+N=m+N$.

Exemplo 13: 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 14: 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 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, epimorfismo* ou um *isomorfismo*, respectivamente. Um homomorfismo $f : M \to M$ é dito um *endomorfismo* de M.

Proposição 5: *Sejam M e N R-módulos. Seja $f : M \to N$ um homomorfismo. Então as seguintes propriedades são satisfeitas:*

(i) $f(0) = 0_N$.

(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, $f(0) = 0_N$
(ii) De fato, temos que $0_N = f(0) = f(m + (-m)) = f(m) + f(-m)$. Daí, $-f(m) = f(-m)$, ou seja, o posto de $f(m)$ é $f(-m)$.

Dado um R-homomorfismo $f : M \to N$. A imagem da f e o núcleo da f são, respectivamente, os conjuntos:

$$\mathrm{Im} f = \{f(m) \ : \ m \in M\}$$

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

Proposição 6: *Seja $f : M \to N$ um R-homomorfismo. Então Imf e Kerf são submódulos de N e M, respectivamente.*

Demonstração: Mostremos que Imf é um submódulo de N. De fato, é imediato que Imf é não-vazio, pois $f(0) = 0$. Sejam $x, y \in Imf$. Então, $x = f(m_1)$ e $y = f(m_2)$ para $m_1, m_2 \in M$. Daí, $x + y = f(m_1) + f(m_2) = f(m_1 + m_2) \in Imf$. Por outro lado, para todo $r \in R$, $rx = rf(m_1) = f(rm_1) \in Imf$. Logo, Imf é um submódulo de N.

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

Proposição 6: *Seja $f : M \to N$ um R-homomorfismo. Então f é um homomorfismo injetor se, e somente se, $Kerf = 0$.*

Demonstração: Suponhamos que f seja injetor. Dado $x \in Kerf$, então $f(x) = 0 = f(0)$. Logo, $x = 0$. Reciprocamente, sejam $m_1, m_2 \in M$ tais que $f(m_1) = f(m_2)$. Daí, $f(m_1 - m_2) = f(m_1) - f(m_2) = 0$. Portanto, $m_1 - m_2 \in Kerf = \{0\}$. Logo, $m_1 = m_2$.

Proposição 7: *Seja $f : M \to N$ e $g : N \to P$ homomorfismos de R-módulos. Então a função composta*

$$\begin{array}{cccc} g \circ f & : & M & \longrightarrow & P \\ & & m & \longmapsto & (g \circ f)(m) = g(f(m)) \end{array}$$

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: *(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 Imf são isomorfos.*

Demonstração: Definimos

$$\begin{array}{ccccc} \overline{f} & : & M/K & \longrightarrow & Imf \\ & & m + K & \longmapsto & \overline{f}(m + K) = f(m) \end{array}$$

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 $Im\overline{f} = \{\overline{f}(m + K) \ : \ m \in M\} = \{f(m) \ : \ m \in M\} = Imf$ 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

$$\begin{aligned}
\overline{f}(m_1 + K) + (m_2 + K) &= \overline{f}((m_1 + m_2) + K) \\
&= f(m_1 + m_2) \\
&= f(m_1) + f(m_2) \\
&= \overline{f}(m_1 + K) + \overline{f}(m_2 + K)
\end{aligned}$$

e

$$\overline{f}(r(m + K)) = f(rm) = rf(m) = r\overline{f}(m + K)$$

Logo, M/K e Imf são isomorfos.

Nota: Usaremos o símbolo $\simeq$ para dizer que dois módulos são isomorfos.

Exemplo 15: Sejam M e N R-módulos. Então a função $f : M \to N$ definida por $f(m) = 0$ para todo $m \in M$ é um homomorfismo, chamado *homomorfismo nulo.*

Exemplo 16: Se $\mathbb{K}$ é um corpo, os homomorfismos de $\mathbb{K}$-módulo são precisamente as tranformações lineares.

Exemplo 17: A função identidade $I : M \to M$ é um homomorfismo, na verdade é um automorfismo, isto é, um endomorfismo bijetor.

Exemplo 18: Seja N um submódulo de um R-módulo M. Então a função inclusão

$$\begin{aligned}
i : N &\longrightarrow M \\
n &\longmapsto n
\end{aligned}$$

é um monomorfismo.

Exemplo 19: Seja N um submódulo de um R-módulo M. A seguinte função é chamada projeção canônica

$$\begin{array}{rcl}\pi : M & \longrightarrow & M/N \\ m & \longmapsto & m+N\end{array}$$

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

$$\begin{array}{rcl}\pi(m_1+m_2) & = & (m_1+m_2)+N) \\ & = & (m_1+N)+(m_2+N) \\ & = & \pi(m_1)+\pi(m_2)\end{array}$$

e

$$\pi(rm) = (rm+N) = r(m+N) = r\pi(m)$$

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 de M. É possível introduzir em M uma estrutura de R-módulo definindo as operações por

$$(m_i)_{i \in I} + (m'_i)_{i \in I} = (m_i + m'_i)_{i \in I}, \ m_i, m'_i \in M, \text{ para todo } i \in I$$

$$r(m_i)_{i \in I} = (rm_i)_{i \in I}, \text{ para todo } r \in R$$

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,

$$\begin{array}{rcl}i_k : M_k & \longrightarrow & M \\ m_k & \longmapsto & (m_i)_{i \in I}\end{array}$$

tal que $m_i = 0$ se $i \neq k$.

Definimos as *projeções sobre os 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

$$\begin{array}{rccc} p_k: & M & \longrightarrow & M_k \\ & (m_i)_{i\in I} & \longmapsto & m_k \end{array}$$

Não é difícil ver que

(i) $p_k \circ i_k = 1_{M_k}$, para todo $k \in I$.

(ii) $p_k \circ i_h = 0$, para quaisquer $h, k \in I$ 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 5: *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 da família e é denotada por $\bigoplus_{i\in I} M_i$.*

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

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

A soma direta externa de uma família de R-módulos é claramente um submódulo do produto direto e $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ 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 inclusões são epimorfismos e

(i) $p_k \circ i_k = 1_{M_k}$, para todo $k \in I$.

(ii) $p_k \circ i_h = 0$, para quaisquer $h, k \in I$ tais que $h \neq k$.

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 suas utilidades.
Certamente um trabalho proveitoso e de uma beleza ímpar. Meus sinceros agradecimentos ao professor Dr. Claudenir Freire Rodrigues e a todos os demais professores do curso de matemática da Ufam.

Cronograma

O desenvolvimento do projeto obedece o seguinte cronograma:

Atividades	Fev - 2011	Mar	Abr	Mai	Jun	Jul
Grupos Abelianos Finitamente Gerados	X					
Teoria dos Módulos	X	X	X	X	X	X
Estudo dirigido pelo orientador	X	X	X	X	X	X
Elaboração do Relatório Final					X	X

Referências

[1] ATIYAH, M.F and MACDONALD, I. G. *Intoduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] GARCIA, A. *Elementos de Álgebra*. IMPA – Projeto Euclides, 2010

[3] HERNSTEIN, I.N. *Topics in Algebra*. Blaisdell.

[4] HUNGERFORD, T. W. *Algebra*. Springer-Verlag, 1974

[5] ROTMAN, Joseph J. *Advanced Modern Algebra*. Springer-Verlag