Complemento de Álgebra Homológica

Edmundo Martins

20 de abril de 2023

Este documento contém algumas anotações adicionais referentes à disciplina *Tópicos de Álgebra* ministrada pelo professor Eduardo do Nascimento Marcos durante o primeiro semestre de 2023 como parte do Programa de Pós-Graduação em Matemática do IME-USP. O documento em questão não tem a proposta de servir como notas de aula para o curso, mas apenas como um conjunto de notas adicionais destrinchando algumas coisas que foram discutidas durante as aulas.

1 Módulos

Nessa subseção relembramos brevemente o significado de módulo sobre um anel. Suponha que A seja um anel não necessariamente comutativo, mas contendo uma unidade 1_A. Intuitivamente, um A-módulo à esquerda é um grupo abeliano juntamente com uma ação de A sobre esse grupo abeliano.

1.1 Definição. Um A-módulo à esquerda é um conjunto M munido de duas operações $+ : M \times M \to M$ e $\cdot : A \times M \to M$ sujeitas às seguintes condições:

1. M é um grupo abeliano com relação à operação $+$;
2. $a \cdot (m + n) = a \cdot m + a \cdot n$ para quaisquer $a \in A$ e $m, n \in M$;
3. $(a + b) \cdot m = a \cdot m + b \cdot m$ para quaisquer $a, b \in A$ e $m \in M$;
4. $a \cdot (b \cdot m) = (ab) \cdot m$ para quaisquer $a, b \in A$ e $m \in M$;
5. $1_A \cdot m = m$ para qualquer $m \in M$.

Por vezes, alguns autores consideram módulos sobre anéis sem unidade, de forma que a última condição deve ser omitida. Nesse contexto, os A-módulos que satisfazem a última propriedade são ditos *unitários*.

A definição acima pode ser facilmente alterada para obtermos a noção de um A-módulo *à direita*, ou seja, com os escalares de A agindo da forma $m \cdot a$ ao invés de $a \cdot m$. Vamos ver agora que, embora os conceitos de módulos à esquerda e à direita não sejam exatamente iguais, existe uma relação próxima entre os dois.

Dado um anel A qualquer, podemos considerar um outro anel A^{op} cuja operação de soma é a mesma, mas cuja operação de multiplicação é a oposta, ou seja, definimos $a \cdot_{\mathrm{op}} b := ba$, onde a justaposição indica a multiplicação já existente em A. O fato de A já ser um anel garante que essa multiplicação oposta também faça de A^{op} um anel.

Suponha agora que M seja um A-módulo à esquerda. Podemos obter um A^{op}-módulo *à direita* M^{op} considerando a mesma operação de soma, e definido o produto por escalares $\cdot : M \times A^{\mathrm{op}} \to M$ por meio da fórmula $m \cdot a := a \cdot m$ para todo $a \in A^{\mathrm{op}}$ e $m \in M$. A verifcação de que isso define de fato uma estrutura de A^{op}-módulo à direita é tranquila. A parte mais interessante é verificar a "associatividade" do produto por escalares. Dados a, $b \in A^{\mathrm{op}}$ e $m \in M$, temos

$$(m \cdot a) \cdot b = b \cdot (m \cdot a) = b \cdot (a \cdot m) = (ba) \cdot m = (a \cdot_{\mathrm{op}} b) \cdot m = m \cdot (a \cdot_{\mathrm{op}} b).$$

Analogamente, todo A-módulo à direita dá origem a um A^{op}-módulo à esquerda. Combinando essas duas construções, e o fato que $(A^{\mathrm{op}})^{\mathrm{op}} = A$, obtemos a equivalência abaixo.

1.2 Proposição. *Existe um isomorfismo de categorias $A - \mathsf{Mod} \cong \mathsf{Mod} - A^{\mathrm{op}}$.*

Em particular, se A é comutativo, então $A^{\mathrm{op}} = A$, e o resultado acima implica o seguinte:

1.3 Corolário. *Se A é um anel comutativo, existe um isomorfismo de categorias $A - \mathsf{Mod} \cong \mathsf{Mod} - A$.*

Isso explica porque no caso comutativo é comum ignorarmos a distinção entre módulos à esquerda e à direita.

1.1 Módulos como ações de um anel

No início da parte anterior mencionamos que, intuitivamente, um módulo sobre um anel é dado pela ação de um anel sobre um grupo abeliano. Note que a operação de produto por escalares $\cdot : A \times M \to M$ é análoga à operação $G \times X \to X$ usada para definir a ação de um grupo G sobre um conjunto X.

Na Teoria de Grupos, um fato interessante é que uma ação de grupo pode ser definida também em termos de um morfismo de grupos $G \to \mathrm{Sym}(X)$, onde $\mathrm{Sym}(X)$ denota o grupo simétrico de X, ou seja, o grupo formado por todas as bijeções $X \to X$. Nosso objetivo nessa parte é mostrar que um módulo também pode ser pensado como uma família de transformações de um objeto parametrizada pelos elementos do anel em questão.

Se M é um grupo abeliano qualquer, lembre-se que um *endomorfismo* de M é simplesmente um morfismo de grupos $f : M \to M$ do grupo para si mesmo. O conjunto de todos esses endomorfismos é denotado por $\mathrm{End}(M)$. A operação de soma em M pode ser estendida pontualmente para uma operação análoga em $\mathrm{End}(M)$: dados f, $g \in \mathrm{End}(M)$, definimos $f + g : M \to M$ pela fórmula

$$(f + g)(m) \coloneqq f(m) + g(m) \quad \forall\, m \in M.$$

Uma verificação rotineira mostra que $f + g$ define realmente um endormofismo do grupo M, portanto temos de fato uma operação binária $+ : \mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M)$. As propriedades algébricas da adição em M garantem que essa operação defina uma estrutura de grupo em $\mathrm{End}(M)$, na qual o elemento neutro é dado pelo endormofismo constante $\mathrm{ct}_{M,0} : M \to M$, e na qual o inverso $-f$ de um endomorfismo f é definido pela fórmula

$$(-f)(m) \coloneqq -f(m) \quad \forall\, m \in M.$$

O mais interessante é que o conjunto $\mathrm{End}(M)$ possui *outra* operação binária advinda da composição de funções. É fácil mmostrar que, dados endomorfismos f, $g \in \mathrm{End}(M)$, sua composição $g \circ f : M \to M$ define um outro endomorfismo, o que nos permite então definir uma operação binária $\circ : \mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M)$. Fazendo alguns cálculos diretos podemos mostrar que essa operação goza das seguintes propriedades:

1. $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$ para quaisquer f_1, f_2, $g \in \mathrm{End}(M)$;

2. $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$ para quaisquer f, g_1, $g_2 \in \mathrm{End}(M)$;

3. $h \circ (g \circ f) = (h \circ g) \circ f$ para quaisquer $f, g, h \in \operatorname{End}(M)$;

4. $\mathrm{id}_M \circ f = f \circ \mathrm{id}_M = f$ para qualquer $f \in \operatorname{End}(M)$.

Em outras palavras, as operações $+$ e $\circ$ juntas definem uma estrutura de *anel* no conjunto de endomorfismos $\operatorname{End}(M)$. Esse é o ingrediente necessário para definirmos uma ação de um anel sobre um grupo abeliano.

1.4 Definição. Uma **ação** de um anel A sobre um grupo abeliano M é um morfismo de anéis $\varphi : A \to \operatorname{End}(M)$.

Assim, uma ação de A sobre M define, para cada $a \in A$, um endomorfismo $\varphi_a \coloneqq \varphi(a) \in \operatorname{End}(M)$, e essa coleção parametrizada de endormofismos satisfaz as seguintes propriedades:

1. $\varphi_a + \varphi_b = \varphi_{a+b}$ para quaisquer $a, b \in A$;

2. $\varphi_b \circ \varphi_a = \varphi_{ba}$ para quaisquer $a, b \in A$;

3. $\varphi_{1_A} = \mathrm{id}_M$.

Suponha agora que M seja um A-módulo à esquerda. Dado $a \in A$ qualquer, definimos um mapa $\ell_a : M \to M$ pela fórmula

$$\ell_a(m) \coloneqq a \cdot m \quad \forall\, m \in M.$$

Esse mapa ℓ_a define na verdade um endomorfismo de M, pois por hipótese o produto por escalares distribui sobre a soma em M, de forma que obtemos um elemento $\ell_a \in \operatorname{End}(M)$.

Variando o elemento $a \in A$ em questão define então um mapa $\ell : A \to \operatorname{End}(M)$ dado pela regra $a \mapsto \ell_a$. As propriedades da operação de produtos por escalares garantem que esse mapa seja um morfismo de anéis:

- a igualdade $(a + b) \cdot m$ implica a igualdade $\ell_{a+b} = \ell_a + \ell_b$;
- a igualadade $(ab) \cdot m = a \cdot (b \cdot m)$ implica a igualdade $\ell_{ab} = \ell_a \circ \ell_b$;
- a igualdade $1_A \cdot m = m$ implica a igualdade $\ell_{1_A} = \mathrm{id}_M$.

Assim, a estrutura de A-módulo em M induz uma ação de A sobre M por meio do morfismo $\ell : A \to \operatorname{End}(M)$. Em certo sentido, esse morfismo é análogo ao morfismo $G \to \operatorname{Sym}(G)$ que aparece na demonstração do Teorema de Cayley.

Existe também uma construção inversa. Dada uma ação $\varphi : A \to \operatorname{End}(M)$ do anel A sobre o grupo abeliano M, considere o produto por escalares $\cdot_\varphi : A \times M \to M$ definido pela fórmula

$$a \cdot_\varphi m \coloneqq \varphi_a(m) \quad \forall\, a \in A,\ \forall\, m \in M.$$

O fato de φ ser um morfismo de anéis garante que esse produto $\cdot_\varphi$ defina juntamente com a soma $+$ uma estrutura de A-módulo à esquerda em M:

- a igualdade $\varphi_{a+b} = \varphi_a + \varphi_b$ implica a igualdade $(a + b) \cdot_\varphi m = a \cdot_\varphi m + b \cdot_\varphi m$;
- o fato de φ_a ser um endomorfismo implica a igualdade $a \cdot_\varphi (m + n) = a \cdot_\varphi m + b \cdot_\varphi n$;
- a igualdade $\varphi_{ab} = \varphi_a \circ \varphi_b$ implica a igualdade $(ab) \cdot_\varphi m = a \cdot_\varphi (b \cdot_\varphi m)$;
- a igualdade $\varphi_{1_A} = \mathrm{id}_M$ implica a igualdade $1_A \cdot_\varphi m = m$.

É possível mostrar que essas duas construções são inversas uma da outra, o que nos leva ao resultado abaixo.

1.5 Teorema. *A noção de A-módulo à esquerda é equivalente à noção de ação de um anel sobre um grupo abeliano.*

Essa equivalência provavelmente pode ser formulada em termos categóricos, mas eu não sei ao certo como fazer isso. É claro que temos a categoria de A-módulos à esquerda $A - \mathsf{Mod}$, mas como interpretar morfismos de anéis do tipo $A \to \mathrm{End}(M)$ como objetos de alguma categoria?

2 Álgebras sobre anéis

Nessa subseção, consideramos outra estrutura algébrica mais rica do que a de módulo sobre um anel. Intuitivamente, uma álgebra sobre um anel consiste de um módulo sobre o anel em questão equipado com uma operação adicional de multiplicação que é compatível com as operações de soma produto por escalares já existentes. As condições exatas de compatibilidade estão formuladas na definição abaixo.

2.1 Definição. Seja A um anel qualquer com unidade. Uma **A-álgebra** consiste de um conjunto M juntamente com três operações $+ : M \times M \to M$, $\cdot : A \times M \to M$ e $* : M \times M \to M$ sujeitas às seguintes condições:

1. M é um grupo abeliano com relação à operação de soma $+$;
2. as operações $+$ e $\cdot$ juntas fazem de M um A-módulo à esquerda;
3. a operação $*$ é A-bilinear.

A operação A-bilinear $*$ é comumante chamada de *multiplicação*, e é mais comum denotar seus valores por justaposição, ou seja, escrevemos mn no lugar de $m * n$. Levando em conta essa notação, a condição de A-bilinearidade da multiplicação pode ser descrita mais explicitamente em termos das seguintes igualdades:

(i) $(m_1 + m_2)n = m_1n + m_2n$ para quaisquer m_1, m_2, $n \in M$;

(ii) $m(n_1 + n_2) = mn_1 + mn_2$ para quaisquer m, n_1, $n_2 \in M$;

(iii) $(a \cdot m)n = a \cdot (mn)$ para quaisquer $a \in A$ e m, $n \in M$;

(iv) $m(a \cdot n) = a \cdot (mn)$ para quaisquer $a \in A$ e m, $n \in M$.

As duas primeiras propriedades mostram que a multiplicação distribui sobre a soma em ambos os lados, enquanto as duas últimas mostram que a multiplicação é em algum sentido compatível com o produto por escalares, os quais "transitam livremente por dentro da multiplicação". Veremos logo mais que existem diferentes "sabores" de A-álgebras caracterizados por propriedades adicionais impostas sobre a operação de multiplicação.

Existe uma definição natural de transformação entre duas álgebras. Formalmente, dadas duas A-álgebras M e N, uma função $f : M \to N$ é um *morfismo de A-álgebras* se satisfaz as seguintes condições:

1. $f(m + n) = f(m) + f(n)$ para todos m, $n \in M$;
2. $f(a \cdot m) = a \cdot f(m)$ para todo $m \in M$ e $a \in A$;
3. $f(mn) = f(m)f(n)$ para todo m, $n \in M$.

As duas primeiras condições dizem que f é um morfismo de A-módulos, enquanto a terceira diz que f é compatível com as operações de multiplicação existentes em M e N.

É tranquilo mostrar que dois morfismos de A-álgebras podem ser compostos para definir um novo morfismo de A-álgebras, e também que o mapa idêntico $\mathrm{id}_M : M \to M$ define um morfismo de A-álgebras. Podemos então definir uma categoria $A - \mathsf{Alg}$ cujos objetos são A-álgebras e cujos morfismos são morfismos de A-álgebras.

Agora introduzimos algumas propriedades adicionais que uma álgebra pode ou não satisfazer.

2.2 Definição. Uma A-álgebra M é dita

- **unitária** se existe um elemento $1_M \in M$ tal que as igualdades $1_M m = m = m 1_M$ valham para todo $m \in M$;
- **comutativa** se a igualdade $mn = nm$ é válida para quaisquer m, $n \in M$;
- **associativa** se a igualdade $(m_1 m_2) m_3 = m_1 (m_2 m_3)$ é válida para quaisquer m_1, m_2, $m_3 \in M$.

Vejamos alguns exemplos interessantes relacionados às propriedades acima.

2.3 Exemplo. Dado um anel com unidade qualquer A, podemos considerar a A-álgebra $M_n(A)$ de matrizes $n \times n$ com entradas em A. Essa é uma A-álgebra associativa e unitária, sendo a unidade dada pela matriz identidade, mas ela só é comutativa quando A é comutativo e n é igual a 1.

2.4 Exemplo. Seja M um A-módulo à esquerda sobre um anel *comutativo* e com unidade. Um endomorfismo de A-módulos de M é por definição um morfismo de A-módulo do tipo $M \to M$. Considere o conjunto $\mathrm{End}_A(M)$ formado por todos os endomorfismos do A-módulo M. Note que temos uma inclusão de conjuntos $\mathrm{End}_A(M) \subseteq \mathrm{End}(M)$, a qual é em geral estrita, já que um endormofismo de grupos abelianos $M \to M$ não precisa ser compatível com a operação de produto por escalares.

Assim como no caso em que M é apenas um grupo abeliano, a operação de soma em $+$ pode ser estendida para uma operação de soma $+ : \mathrm{End}_A(M) \times \mathrm{End}_A(M) \to \mathrm{End}_A(M)$ no conjunto de endomorfismos de A-módulos.

$$(S + T)(m) \coloneqq S(m) + T(m) \quad \forall\, m \in M.$$

No contexto atual, podemos também estender a operação de produtos por escalares para o conjunto de endomorfismos. Formalmente, dados $a \in A$ e $T \in \mathrm{End}_A(M)$, definimos um novo mapa $a \cdot T : M \to M$ pela fórmula

$$(a \cdot T)(m) \coloneqq a \cdot T(m) \quad \forall\, m \in M.$$

Vejamos que $a \cdot T$ define de fato um endomorfismos de M. Primeiramente, dados m, $m' \in M$, temos

$$(a \cdot T)(m + m') = a \cdot T(m + m') = a \cdot (T(m) + T(m')) = a \cdot T(m) + a \cdot T(m') = (a \cdot T)(m) + (a \cdot T)(m'),$$

portanto $a \cdot T$ é compatível com a operação de soma em M. Agora, dados $a' \in A$ e $m \in M$, por um lado temos

$$(a \cdot T)(a' \cdot m) = a \cdot T(a' \cdot m) = a \cdot (a' \cdot T(m)) = (aa') \cdot T(m),$$

enquanto por outro

$$a' \cdot ((a \cdot T)(m)) = a' \cdot (a \cdot T(m)) = (a'a) \cdot T(m).$$

Como A foi suposto comutativo, vale a igualdade $aa' = a'a$, e comparando então as duas cadeias de igualdades anteriores vemos que

$$(a \cdot T)(a' \cdot m) = a' \cdot ((a \cdot T)(m));$$

mostrando que $a \cdot T$ também é compatível com a operação de produto por escalares em M.

O raciocínio acima mostra que temos uma operação bem-definida de produto por escalares $\cdot : A \times \mathrm{End}_A(M) \to \mathrm{End}_A(M)$ Veja que essa operação goza das seguintes propriedades:

1. $a \cdot (S + T) = a \cdot S + a \cdot T$, pois em M vale que $a \cdot (m + n) = a \cdot m + a \cdot n$;
2. $(a + b) \cdot T = a \cdot T + b \cdot T$, pois em M vale que $(a + b) \cdot m = a \cdot m + b \cdot m$;
3. $a \cdot (b \cdot T) = (ab) \cdot T$, pois em M vale que $a \cdot (b \cdot m) = (ab) \cdot m$;
4. $1_A \cdot T = T$, pois em M vale que $1_A \cdot m = m$.

Em resumo, as operações $+$ e $\cdot$ juntas definem uma estrutura de A-módulo à esquerda em $\mathrm{End}_A(M)$. Lembrando que a operação de produto por escalares só ficou bem-definida porque o anel A foi suposto comutativo.

Quando estudamos o conjunto de endomorfismos de um grupo abeliano M, vimos que, além da operação de soma, tínhamos também a operação de composição, e que as duas operações interagiam corretamente de forma a definir uma estrutura de anel no conjunto de endomorfismos. Essa operação também faz sentido no contexto atual de endomorfismos de A-módulos. Dados dois endomorfismos $S, T : M \to M$, é fácil verificar que sua composição $T \circ S : M \to M$ resulta ainda em um endomorfismo de A-módulos, de forma que podemos definir uma operação binária $\circ : \mathrm{End}_A(M) \times \mathrm{End}_A(M) \to \mathrm{End}_A(M)$. Assim como no caso de endomorfismos de um grupo abeliano, é possível mostrarmos que essa operação interage bem com a soma, ou seja, para quaisquer endomorfismos R, S, $T : M \to M$ valem as igualdades

$$(T + S) \circ R = T \circ R + S \circ R \quad \text{e} \quad T \circ (S + R) = T \circ S + T \circ R.$$

Felizmente, essa operação de composição também interage bem com o produto por escalares em ambas variáveis. De fato, dados $a \in A$, S, $T \in \mathrm{End}_A(M)$ e $m \in M$ quaisquer, por um lado temos

$$[(a \cdot T) \circ S](m) = (a \cdot T)(S(m)) = a \cdot T(S(m)) = a \cdot (T \circ S)(m) = [a \cdot (T \circ S)](m),$$

mostrando a igualdade $(a \cdot T) \circ S = a \cdot (T \circ S)$; e por outro temos

$$[T \circ (a \cdot S)](m) = T((a \cdot S)(m)) = T(a \cdot S(m)) = a \cdot T(S(m)) = a \cdot (T \circ S)(m) = [a \cdot (T \circ S)](m),$$

mostrando a igualdade $T \circ (a \cdot S) = a \cdot (T \circ S)$.

As discussões dos dois últimos parágrafos mostram que a composição define uma operação A-bilinear no A-módulo $\mathrm{End}_A(M)$. Combinando tudo que foi discutido neste exemplo até o momento, concluímos que $\mathrm{End}_A(M)$ possui a estrutura de uma *A-álgebra*!

Sendo a operação de multiplicação em $\mathrm{End}_A(M)$ definida em termos da composição de funções, a qual é uma operação sabidamente associativa, $\mathrm{End}_A(M)$ é um exemplo de A-álgebra *associativa*. Além disso, o mapa idêntico $\mathrm{id}_M : M \to M$ pertence certamente ao conjunto dos endomorfismos de A-módulos e satisfaz as igualdades $\mathrm{id}_M \circ T = T \circ \mathrm{id}_M = T$ para qualquer outro endomorfismo T, o que mostra que $\mathrm{End}_A(M)$ é também uma A-álgebra *unitária*. Por fim, dados dois endomorfismos S, $T \in \mathrm{End}_A(M)$, não existe é perfeitamente possível que as composições $T \circ S$ e $S \circ T$ sejam distintas, portanto $\mathrm{End}_A(M)$ define em geral uma A-álgebra *não-comutativa*.

Um comentário final é que a álgebra de matrizes do Exemplo 2.3 pode em certos casos ser vista como um caso particular da álgebra de endomorfismos construída no exemplo em questão. Mais precisamente, dado um anel comutativo e com unidade A, podemos considerar a estrutura de A-módulo à esquerda usual no produto A^n para algum inteiro $n \geq 1$. Seguindo a construção do exemplo atual, obtemos a partir disso a A-álgebra de endomorfismos $\mathrm{End}_A(A^n)$. Escolhendo uma base para o A-módulo A^n, podemos associar a cada endomorfismo $T : A^n \to A^n$ uma matriz $[A] \in M_n(A)$. Fazendo algumas contas simples porém tediosas podemos mostrar que a associação $T \mapsto [T]$ define um isomorfismo de A-álgebras $\mathrm{End}_A(A^n) \cong M_n(A)$.

2.5 Observação. Veremos mais tarde que existem outras maneiras de obtermos estruturas de álgebras em conjutnos de morfismos usando estrutura mais gerais conhecidas como *bimódulos*. Em particular, poderemos então obter estruturas de álgebras em conjuntos de morfismos mesmo sem supor a comutatividade do anel de escalares.

2.6 Exemplo. Seja A um anel com unidade. Dado um conjunto não-vazio qualquer X, seja $F(X, A)$ o conjunto de todas as funções de tipo $X \to A$. As operações existentes em A podem ser estendidas pontualmente para $F(X, A)$:

- dados $f, g \in F(X, A)$, definimos $f + g : X \to A$ por $(f + g)(x) := f(x) + g(x)$ para todo $x \in X$;
- dados $f \in F(X, A)$ e $a \in A$, definimos $a \cdot f : X \to A$ por $(a \cdot f)(x) := af(x)$ para todo $x \in X$;
- dados $f, g \in F(X, A)$, definimos $fg : X \to A$ pela fórmula $(fg)(x) := f(x)g(x)$ para todo $x \in X$.

Novamente, contas rotineiras usando as propriedades algébricas das operações em A nos permitem mostrar que as operações definidas acima munem $F(X, A)$ de uma estrutura de A-álgebra. Como a multiplicação em $F(X, A)$ é definida em termos da multiplicação em A, a qual é associativa, $F(X, A)$ é também uma álgebra associativa. Além disso, a função $\mathrm{ct}_{X,1_A} : X \to A$ que é constante e igual a 1_A é uma unidade bilateral para a operação de multiplicação em $F(X, A)$, portanto temos uma A-álgebra unitária. Note por fim que $F(X, A)$ é comutativa se, e somente se, o anel A é comutativo. Por um lado, se A é comutativo, então para quaisquer duas funções $f, g : X \to A$ vale que

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$$

para todo $x \in X$, de forma que $fg = gf$. Por outro lado, dados dois elementos $a, b \in A$, podemos considerar as funções constantes $\mathrm{ct}_{X,a}, \mathrm{ct}_{X,b} \in F(X, A)$, as quais por hipótese satisfazem a igualdade $\mathrm{ct}_{X,a}\mathrm{ct}_{X,b} = \mathrm{ct}_{X,b}\mathrm{ct}_{X,a}$; mas aplicando essas duas funções a qualquer elemento de X concluímos que $ba = ab$.

2.1 Álgebras via anéis e vice-versa

Nessa subseção vamos discutir como certos tipos de álgebras podem ser definidas em termos de anéis e vice-versa. Se quisermos mais precisos, vamos mostrar que existe uma correspondência entre certas A-álgebras e morfismos de anéis cujo domínio é A. Durante esta subseção, consideraremos apenas anéis comutativos com unidade, e os morfismos de anéis serão unitários, ou seja, mapearão a unidade de um anel para a unidade de outro.

Suponha que M seja uma A-álgebra unitária e associativa. Deixando de lado momentaneamente a operação de produto por escalares, as operações de soma e multiplicação juntas definem uma estrutura de anel em M. Veja que as hipóteses de que M seja uma A-álgebra unitária e associativa são essenciais para que tenhamos realmente uma estrutura de anel.

E qual é a relação da operação de produtos por escalares de A para essa estrutura de anel subjacente em M? Usando tal operação podemos definir uma função $\varphi_M : A \to M$ dada por $\varphi_M(a) \coloneqq a \cdot 1_M$. Usando as propriedades algébricas da estrutura de A-álgebra em M vemos que valem as seguintes igualdades:

- $\varphi_M(1_A) = 1_A \cdot 1_M = 1_M$;
- $\varphi_M(a + b) = (a + b) \cdot 1_M = a \cdot 1_M + b \cdot 1_M = \varphi_M(a) + \varphi_M(b)$ para quaisquer a, $b \in A$;
- $\varphi_M(ab) = (ab) \cdot 1_M = (a \cdot 1_M)(b \cdot 1_M) = \varphi_M(a)\varphi_M(b)$ para quaisquer a, $b \in A$.

Assim, a aplicação $\varphi_M : A \to M$ define um *morfismo de anéis* o qual é chamado de **morfismo estrutural de** M. Esse morfismo possui uma propriedade importante decorrente da A-bilinearidade da multiplicação em M: dado $a \in A$ e $m \in M$ quaisquer, por um lado temos

$$\varphi_M(a)m = (a \cdot 1_M)m = a \cdot (1_M m) = a \cdot m,$$

enquanto por outro temos

$$m\varphi_M(a) = m(a \cdot 1_M) = a \cdot (m1_M) = a \cdot m.$$

As igualdades acima mostram que os elementos pertencentes à imagem do morfismo estrutural φ_M comutam com todos os elementos de M, ou seja, existe vale a inclusão $\varphi_M(A) \subseteq Z(M)$, onde $Z(M)$ denota o *centro* do anel subjacente a M.

Isso sugere a seguinte construção: considere a categoria $A\backslash\mathsf{Ring}_Z$ cujos objetos são pares (B, φ), onde B é um anel, e $\varphi : A \to B$ é um morfismo de anéis satisfazendo a condição $f(A) \subseteq Z(B)$. Um morfismo do tipo $(B_1, \varphi_1) \to (B_2, \varphi_2)$ nessa categoria é dado por um morfismo de anéis $f : B_1 \to B_2$ satisfazendo a igualdade $f \circ \varphi_1 = \varphi_2$, como mostrado no diagrama comutativo abaixo.

$$\begin{tikzcd}
 & B_1 \arrow[dd, dashed, "f"] \\
A \arrow[ur, "\varphi_1"] \arrow[dr, "\varphi_2"'] & \\
 & B_2
\end{tikzcd}$$

Vimos acima que, dada uma A-álgebra associativa e unitária M, considerando a estrutura de anel subjacente em M, usando o produto por escalares definimos o morfismo de anéis estrutural $\varphi_M : A \to M$ o qual satisfaz a condição $\varphi_M(A) \subseteq Z(M)$. Em outras palavras, o par (M, φ_M) define um objeto da categoria $A\backslash\mathsf{Ring}_Z$ que acabamos de introduzir.

Suponha agora que N seja uma outra A-álgebra unitária e associativa, e considere um morfismo *unitário* de A-álgebras $f : M \to N$, ou seja, f é compatível com as operações de soma, multiplicação, produto por escalares, e também preserva unidades, portanto a igualdade $f(1_M) = 1_N$ é válida. Note que para todo $a \in A$ vale que

$$f(\varphi_M(a)) = f(a \cdot 1_M) = a \cdot f(1_M) = a \cdot 1_N = \varphi_N(a).$$

Suponha então que N seja uma outra A-álgbera unitária e associativa e, e considere um morfismo *unitário* de A-álgebras $f : M \to N$, ou seja, f é compatível com as operação de soma, multiplicação, produto por escalares, e preserva unidades, de forma que vale a igualdade $f(1_M) = 1_N$. Isso significa que, esquecendo por um momento da operação de produto por escalares, podemos encarar f como um morfismo de anéis $A \to M$. Note então que, para todo $a \in A$, vale que

$$f(\varphi_M(a)) = f(a \cdot 1_M) = a \cdot f(1_M) = a \cdot 1_N = \varphi_N(a),$$

portanto f faz comutar o diagrama abaixo.

$$\begin{tikzcd} & M \arrow[dd, dashed, "f"] \\ A \arrow[ur, "\varphi_M"] \arrow[dr, "\varphi_N"'] & \\ & N \end{tikzcd}$$

Podemos então considerar f como um morfismo do tipo $(M, \varphi_M) \to (N, \varphi_N)$ na categoria $A\backslash\mathsf{Ring}_Z$. Se $A - \mathsf{Alg}_{\mathsf{ua}}$ denota a categoria cujos objetos são as A-álgebras unitárias e associativas e cujos morfismos são os morfismos unitários de A-álgebras, a construção acima nos permite definir um funtor $E : A - \mathsf{Alg}_{\mathsf{ua}} \to A\backslash\mathsf{Ring}_Z$[1] que associa a uma A-álgebra unitária e associativa M o par (M, φ_M), sendo φ_M seu morfismo estrutural, e que associa a um morfismo unitário de A-álgebras $f : M \to N$ ele mesmo visto agora como morfismo do tipo $f : (M, \varphi_M) \to (N, \varphi_N)$ em $A\backslash\mathsf{Ring}_Z$. Como essa construção não faz esencialmente nada com os morfismos, é claro que ela preserva composições e identidades, definido de fato um funtor.

Vamos mostrar agora que é possível também definir um funtor no sentido contrário. Dado um morfismo de anéis $\varphi : A \to B$ tal que $\varphi(A) \subseteq Z(B)$, o conjunto B já possui operações compatíveis de soma e multiplicação, então se quisermos obter uma estrutura de A-álgebra, precisamos antes definir uma operação de produto por escalares de A. Dados $a \in A$ e $b \in B$, definimos então $a \cdot_\varphi b := \varphi(a)b$. Veja que essa operação goza das seguintes propriedades:

- $a \cdot_\varphi (b_1 + b_2) = \varphi(a)(b_1 + b_2) = \varphi(a)b_1 + \varphi(a)b_2 = a \cdot_\varphi b_1 + a \cdot_\varphi b_2$ para quaisquer $a \in A$ e b_1, $b_2 \in B$.
- $(a_1 + a_2) \cdot_\varphi b = \varphi(a_1 + a_2)b = (\varphi(a_1) + \varphi(a_2))b = \varphi(a_1)b + \varphi(a_2)b = a_1 \cdot_\varphi b + a_2 \cdot_\varphi b$ para quaisquer a_1, $a_2 \in A$ e $b \in B$.
- $a_1 \cdot_\varphi (a_2 \cdot_\varphi b) = \varphi(a_1)(\varphi(a_2)b) = (\varphi(a_1)\varphi(a_2))b = \varphi(a_1 a_2)b = (a_1 a_2) \cdot_\varphi b$ para quaisquer a_1, $a_2 \in A$ e $b \in B$.
- $1_A \cdot_\varphi b = \varphi(1_A)b = 1_B b = b$ para qualquer $b \in B$.

Em outras palavras as operações $+$ e $\cdot_\varphi$ juntas fazem de B um A-módulo. Além disso, as igualdades abaixo mostram que essa ooperação de produto por escalares de A interage bem com a multiplicação já existente em B:

- $(a \cdot_\varphi b_1)b_2 = (\varphi(a)b_1)b_2 = \varphi(a)(b_1 b_2) = a \cdot_\varphi (b_1 b_2)$ para quaisquer $a \in A$ e b_1, $b_2 \in B$.
- $b_1(a \cdot_\varphi b_2) = b_1(\varphi(a)b_2) = (b_1 f(a))b_2 = (\varphi(a)b_1)b_2 = \varphi(a)(b_1 b_2) = a \cdot_\varphi (b_1 b_2)$ para quaisquer $a \in A$ e b_1, $b_2 \in B$.

Note que na segunda cadeia de igualdades a condição $\varphi(A) \subseteq Z(B)$ foi essencial para podermos comutar os termos $\varphi(a)$ e b_1.

Em resumo, a discussão dos dois parágrafos anteriores mostra que as operação de soma e multiplicação do anel B juntamente com o produto por escalares $\cdot_\varphi$ fazem de B uma A-álgebra, a qual denotaremos por B^φ daqui para frente. Como um anel possui uma unidade multiplicativa, e sua multiplicação é associativa por hipótese, B^φ é uma A-álgebra unitária e associativa.

Vamos mostrar que essa construção se comporta de forma funtorial. Considere dois objetos (B, φ) e (C, ψ) na categoria $A\backslash\mathsf{Ring}_Z$, e considere também um morfismo $\theta : (B, \varphi) \to (C, \psi)$

[1] A letra E remete à palavra *estrutural*, já que é justamente a construção do morfismo estrutural a parte importante da definição desse funtor.

entre eles. Lembre-se que isso significa que $\theta : B \to C$ é um morfismo de anéis satisfazendo a igualdade $\theta \circ \varphi = \psi$. Como as operações de soma e multiplicação nas álgebras B^φ e C^ψ são aquelas herdadas dos anéis B e C, respectivamente, e θ é um morfismo de anéis, fica claro que θ é compatível com essas duas operações. Segue disso também que θ preserva as unidades das álgebras B^φ e C^ψ.

Note, além disso, que θ também é compatível com os produtos por escalares nas duas A-álgebras, pois dados $a \in A$ e $b \in B$, vale que

$$\theta(a \cdot_\varphi b) = \theta(\varphi(a)b) = \theta(\varphi(a))\theta(b) = \psi(a)\theta(b) = a \cdot_\psi \theta(b).$$

Concluímos assim que θ também pode ser visto como um morfismo de A-álgebras do tipo $B^\varphi \to C^\psi$.

Associando a cada objeto $(B, \varphi) \in A\backslash\mathsf{Ring}_Z$ a A-álgebra B^φ, e associando a um morfismo $\theta : (B, \varphi) \to (C, \psi)$ ele mesmo visto como morfismo de A-álgebras $\theta : B^\varphi \to C^\psi$ obtemos um funtor $F : A\backslash\mathsf{Ring}_Z \to A - \mathsf{Alg}_{ua}$.

Associando então a cada par $(B, \varphi) \in A\backslash\mathsf{Ring}_Z$ a A-álgebra unitária e associativa B^φ, e associando a um morfismo $\theta : (B, \varphi) \to (C, \psi)$ ele mesmo visto agora como um morfismo de A-álgebras $\theta : B^\varphi \to C^\psi$ obtemos um funtor $F : A\backslash\mathsf{Ring}_Z \to A - \mathsf{Alg}_{\mathsf{ua}}$.

2.7 Teorema. *Os funtores E e F definidos acima são inversos e definem, portanto, um isomorfismo de categorias $A - \mathsf{Alg}_{\mathsf{ua}} \cong A\backslash\mathsf{Ring}_Z$.*

Demonstração. Dada uma A-álgebra unitária e associativa B, temos que mostrar que $B^{\varphi_B} = B$, onde $\varphi_B : A \to B$ é o morfismo estrutural da álgebra. Lembre-se que as operações de soma e multiplicação de B^φ são as operações correspondentes do anel subjacente a B, e essas são exatamente as operações correspondentes da A-álgebra B inicial; ou seja, as operações de soma e multiplicação das A-álgebras B e B^{φ_B} são iguais. O mesmo raciocínio mostra que o mesmo é verdade para as unidades multiplicativas. Resta apenas mostrar que as operações de produto por escalares também são iguais. De fato, dados $a \in A$ e $b \in B$, pelas definições temos

$$a \cdot_{\varphi_B} b = \varphi_B(a)b = (a \cdot 1_B)b = a \cdot (1_B b) = a \cdot b.$$

Concluímos então que $F \circ E$ é igual ao funtor identidade da categoria $A - \mathsf{Alg}_{\mathsf{ua}}$.

Vamos agora analisar a composição $E \circ F$. Dado um objeto $(B, \varphi) \in A\backslash\mathsf{Ring}_Z$, queremos mostrar a igualdade $(B^\varphi, \varphi_{B^\varphi})$, onde $\varphi_{B^\varphi} : A \to B^\varphi$ é o morfismo estrutural da A-álgebra induzida B^φ. Lembre-se que o anel subjacente à A-álgebra B^φ é exatamente o anel B, portanto a igualdade desejada se reduz essencialmente à igualdade dos morfismos de anéis φ e φ_{B^φ}. Essa igualdade é válida pois, dado $a \in A$, por definição temos

$$\varphi_{B^\varphi}(a) = a \cdot_\varphi 1_{B^\varphi} = \varphi(a)1_B = \varphi(a)\varphi(1_A) = \varphi(a).$$

Isso mostra que $\varphi = \varphi_{B^\varphi}$, portanto $(B, \varphi) = (B^\varphi, \varphi_{B^\varphi})$, e disso concluímos que $E \circ F$ é igual ao funtor idêntico da categoria $A\backslash\mathsf{Ring}_Z$. ∎

2.8 Observação (O caso comutativo)**.** A discussão anterior e o **??** ficam um pouco mais simples se trabalharmos apenas com álgebras comutativas. Se B é uma A-álgebra unitária, associativa e também comutativa, então o anel subjacente a B é também comutativo. Veja então que a condição $\varphi(A) \subseteq Z(B)$ sobre o morfismo estrutural é trivial nesse caso, pois a comutatividade de B implica $Z(B) = B$.

Essa trivialidade se reflete na construção inversa também. Nesse caso, se B é um anel comutativo, e $f : A \to B$ é um morfismo (unitário) de anéis, então o produto por escalares $a \cdot_f b \coloneqq f(a)b$ é sempre compatível com as operações do anel e define, portanto, uma estrutura de A-álgebra no conjunto B.

Podemos então resumir esse caso mais simples no resultado abaixo.

2.9 Teorema. *Existe um isomorfismo entre a categoria $A - \mathsf{Alg}_{\mathsf{uac}}$ das A-álgebras unitárias, associativas e comutativas e a categoria $A\backslash\mathsf{CRing}$*[2] *cujos objetos são morfismos de anéis do tipo $A \to B$, sendo B comutativo.*

3 Equivalências entre categorias

Nessa seção introduzimos a noção de equivalência entre duas categorias, apresentamos uma formulação alternativa em termos de propriedades "conjuntistas" de um funtor, e então usamos essa outra formulação para exibir algumas equivalências surpreendentes entre categorias de módulos.

3.1 Definição. Um funtor $F : \mathsf{C} \to \mathsf{D}$ é dito uma **equivalência de categorias** se existe um funtor $G : \mathsf{D} \to \mathsf{C}$ tal que $G \circ F \simeq \mathrm{id}_{\mathsf{C}}$ e $F \circ G \simeq \mathrm{id}_{\mathsf{C}}$. Nesse caso, o funtor G é chamado de um **quase-inverso** de F.

O principal resultado é que a propriedade de um funtor $F : \mathsf{C} \to \mathsf{D}$ ser uma equivalência de categorias pode ser descrita inteiramente em termos de propriedades do funtor F sem a necessidade de falar de um funtor do tipo $\mathsf{D} \to \mathsf{C}$. Isso é análogo ao fato de uma bijeção pode ser descrita como uma injeção e uma sobrejeção.

Antes de enunciarmos e provarmos o resultado de fato, precisamos de algumas definições auxiliares.

3.2 Definição. Dizemos que um funtor $F : \mathsf{C} \to \mathsf{D}$ é

(a) **denso** se, para todo $d \in \mathsf{D}$, existe algum $c \in \mathsf{C}$ tal que $d \cong F(c)$;[3]

(b) **fiel** se, para quaisquer dois objetos $a, b \in \mathsf{C}$, a função $F_{a,b} : \mathsf{C}(a,b) \to \mathsf{D}(F(a), F(b))$ for injetiva;

(c) **pleno** se, para quaisquer dois objetos $a, b \in \mathsf{C}$, a função $F_{a,b} : \mathsf{C}(a,b) \to \mathsf{D}(F(a), F(b))$ for sobrejetiva.

Agora temos os ingredientes para enunciar e demonstrar o resultado desejado.

3.3 Teorema. *Dado um funtor $F : \mathsf{C} \to \mathsf{D}$, as seguintes afirmações são equivalentes:*

(a) F é uma equivalência de categorias;

(b) F é denso, fiel e pleno.

Demonstração. Suponha primeiro que F seja uma equivlência, e considere então um funtor quase-inverso $G : \mathsf{D} \to \mathsf{C}$. Existe então um isomorfismo natural $\theta : F \circ G \Rightarrow \mathrm{id}_{\mathsf{D}}$. Assim, dado $d \in \mathsf{D}$, temos um isomorfismo $\theta_d : F(G(d)) \to d$, logo, se definirmos $c := G(d)$, vale que $F(c) \cong d$; mostrando a densidade do funtor F.

Suponha agora que tenhamos dois morfismos $f, g : a \to b$ em C tais que $F(f) = F(g)$. Se $\psi : G \circ F \Rightarrow \mathrm{id}_{\mathsf{C}}$ denota um isomorfismo natural, então por naturalidade temos os diagramas comutativos abaixo.

$$\begin{tikzcd} G(F(a)) \arrow[r, "G(F(f))"] \arrow[d, "\psi_a"'] & G(F(b)) \arrow[d, "\psi_b"] \\ a \arrow[r, "f"'] & b \end{tikzcd} \qquad \begin{tikzcd} G(F(a)) \arrow[r, "G(F(g))"] \arrow[d, "\psi_a"'] & G(F(b)) \arrow[d, "\psi_b"] \\ a \arrow[r, "g"'] & b \end{tikzcd}$$

[2] Embora tenhamos usado a notação de categorias co-slice, cabe apontar que $A\backslash\mathsf{CRing}$ como definida *não* é uma categoria co-slice, já que a princípio podemos ter $A \notin \mathsf{CRing}$.

[3] Por vezes, um funtor denso também é dito **essencialmente sobrejetivo**.

Levando em conta que ψ_a e ψ_b são isomorfismos, os diagramas acima nos permitem escrever

$$f = \psi_b \circ G(F(f)) \circ \psi_a^{-1} \quad \text{e} \quad g = \psi_b \circ G(F(g)) \circ \psi_a^{-1},$$

mas como $F(f) = F(g)$, também vale que $G(F(f)) = G(F(g))$, portanto segue diretamente das duas igualdades acima que $f = g$.

Considere agora dois objetos $a, b \in \mathsf{C}$, e um morfismo $h : F(a) \to F(b)$. Queremos mostrar a existência de um morfismo $f : a \to b$ tal que $h = F(f)$. Lembre-se que temos isomorfismos $\psi_a : G(F(a)) \to a$ e $\psi_b : G(F(b)) \to b$, portanto faz sentido considerarmos o morfismo $f : a \to b$ definido pela composição $f \coloneqq \psi_b \circ G(h) \circ \psi_a^{-1}$, conforme mostrado no diagrama abaixo.

$$\begin{tikzcd}
G(F(a)) \arrow[r, "G(h)"] & G(F(b)) \arrow[d, "\psi_b"] \\
a \arrow[u, "\psi_a^{-1}"] \arrow[r, dashed, "f"'] & b
\end{tikzcd}$$

A naturalidade do isomorfismo garante que temos o diagrama comtuativo abaixo,

$$\begin{tikzcd}
G(F(a)) \arrow[r, "G(F(f))"] \arrow[d, "\psi_a"'] & G(F(b)) \arrow[d, "\psi_b"] \\
a \arrow[r, "f"'] & b
\end{tikzcd}$$

portanto podemos escrever $f = \psi_b \circ G(F(f)) \circ \psi_a^{-1}$. Comparando as duas expressões para f vemos que

$$\psi_b \circ G(h) \circ \psi_a^{-1} = \psi_b \circ G(F(f)) \circ \psi_a^{-1},$$

e cancelando os isomorfismos ψ_b e ψ_a^{-1} de ambos os lados concluímos que $G(h) = G(F(f))$. Ora, como G também é uma equivalência, segue do que já provamos que G é fiel, portanto a última igualdade implica $h = F(f)$ conforme desejado. ■