Álgebra II Práctica (clase 11)

Guido Arnone

Universidad de Buenos Aires

2 de Junio de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta la Sección 3.3.

Módulos

Recordemos que un dado un anillo A, un A-módulo M es un grupo abeliano junto con un morfismo de anillos $\rho : A \to \mathrm{End}_{\mathbb{Z}}(M)$.

Módulos

Recordemos que un dado un anillo A, un A-módulo M es un grupo abeliano junto con un morfismo de anillos $\rho : A \to \mathrm{End}_{\mathbb{Z}}(M)$.

Esto es lo mismo que definir una operación $\cdot : A \times M \to M$ que satisface

- $a \cdot (m + m') = a \cdot m + a \cdot m'$
- $(a + a') \cdot m = a \cdot m + a' \cdot m$
- $(aa') \cdot m = a \cdot (a' \cdot m)$
- $1 \cdot m = m$

para cada $a, a' \in A$ y $m, m' \in M$.

Dado un morfismo ρ podemos definir $a \cdot m := \rho(a)(m)$, y dada una operación $\cdot$ como la anterior definimos $\rho(a)(m) := a \cdot m$.

Módulos - Ejemplos

Veamos algunos ejemplos de módulos:

Cuando k es un cuerpo, un k-módulo es un k-espacio vectorial: los axiomas que satisface $\cdot$ son precisamente los del producto escalar.

Módulos - Ejemplos

Veamos algunos ejemplos de módulos:

Cuando k es un cuerpo, un k-módulo es un k-espacio vectorial: los axiomas que satisface $\cdot$ son precisamente los del producto escalar.

Un $\mathbb{Z}$-módulo es lo mismo que un grupo abeliano. Una forma de ver esto es que hay un único morfismo $\mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$. Otra forma es notar que las condiciones $1 \cdot m = m$ y $(s + t) \cdot m = s \cdot m + t \cdot m$ determinan completamente a la operación.

Módulos - Ejemplos

Veamos algunos ejemplos de módulos:

Cuando k es un cuerpo, un k-módulo es un k-espacio vectorial: los axiomas que satisface $\cdot$ son precisamente los del producto escalar.

Un $\mathbb{Z}$-módulo es lo mismo que un grupo abeliano. Una forma de ver esto es que hay un único morfismo $\mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$. Otra forma es notar que las condiciones $1 \cdot m = m$ y $(s + t) \cdot m = s \cdot m + t \cdot m$ determinan completamente a la operación.

Si A es un anillo, un ideal I a izquierda es un A-módulo donde la operación es la multiplicación del anillo $a \cdot x := ax$ para cada $a \in A$ y $x \in I$.

Módulos - Ejemplos (cont.)

Dar una estructura de $k[X]$-módulo consiste en dar un espacio vectorial V junto con un endomorfismo k-lineal $T : V \to V$. Veámoslo:

Módulos - Ejemplos (cont.)

Dar una estructura de $k[X]$-módulo consiste en dar un espacio vectorial V junto con un endomorfismo k-lineal $T : V \to V$. Veámoslo:

- Dado un k-e.v. V y un endomorfismo T, la operación definida por $(a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot v := a_0 \cdot v + a_1 \cdot T(v) + \cdots + a_r \cdot T^r(v)$ hace de V un $k[X]$-módulo.

Módulos - Ejemplos (cont.)

Dar una estructura de $k[X]$-módulo consiste en dar un espacio vectorial V junto con un endomorfismo k-lineal $T : V \to V$. Veámoslo:

- Dado un k-e.v. V y un endomorfismo T, la operación definida por $(a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot v := a_0 \cdot v + a_1 \cdot T(v) + \cdots + a_r \cdot T^r(v)$ hace de V un $k[X]$-módulo.
- Si V es un $k[X]$-módulo, entonces viendo a un elemento de k como polinomio constante, tenemos una multiplicación por escalares en V que hace de este un k-e.v. Además, la multiplicación por X define un endomorfismo k-lineal de V.

Módulos - Ejemplos (cont.)

Dar una estructura de $k[X]$-módulo consiste en dar un espacio vectorial V junto con un endomorfismo k-lineal $T : V \to V$. Veámoslo:

- Dado un k-e.v. V y un endomorfismo T, la operación definida por $(a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot v := a_0 \cdot v + a_1 \cdot T(v) + \cdots + a_r \cdot T^r(v)$ hace de V un $k[X]$-módulo.
- Si V es un $k[X]$-módulo, entonces viendo a un elemento de k como polinomio constante, tenemos una multiplicación por escalares en V que hace de este un k-e.v. Además, la multiplicación por X define un endomorfismo k-lineal de V.

Ambas construcciones son inversas.

Módulos - Ejemplos (cont.)

Ejemplo

Tenemos una estructura de $\mathbb{R}[X]$*-módulo en* $\mathscr{C}^\infty(0,1)$ *via*

$$T : f \in \mathscr{C}^\infty(0,1) \longmapsto f' \in \mathscr{C}^\infty(0,1).$$

Así, es por ejemplo $(X^2 + \sqrt{2}X + 4) \cdot f = f'' + \sqrt{2}f' + 4f$.

Módulos - Ejemplos (cont.)

Ejemplo

Tenemos una estructura de $\mathbb{R}[X]$*-módulo en* $\mathscr{C}^\infty(0,1)$ *via*

$$T : f \in \mathscr{C}^\infty(0,1) \longmapsto f' \in \mathscr{C}^\infty(0,1).$$

Así, es por ejemplo $(X^2 + \sqrt{2}X + 4) \cdot f = f'' + \sqrt{2}f' + 4f$.

Ejemplo

La matriz $M = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *define un endomorfismo de* $V = (\mathbb{Z}_2)^3$*, cuya matriz en la base canónica* $B = \{e_1, e_2, e_3\}$ *es* M*. Por lo tanto, se tiene una estructura de* $\mathbb{Z}_2[X]$*-módulo en* V*. Por ejemplo,*

$$\begin{aligned}(1 + X^2) \cdot (1,0,1) &= 1 \cdot (1,0,1) + X^2 \cdot (1,0,1) \\ &= (1,0,1) + (0,0,1) \\ &= (1,0,0).\end{aligned}$$

Morfismos de Módulos

Sea A un anillo y M, N dos A-módulos. Un morfismo de A-módulos $f : M \to N$ es una función que es A-lineal, es decir, que satisface

- $f(m + m') = f(m) + f(m')$
- $f(a \cdot m) = a \cdot f(m)$

para cada $m, m' \in M$ y $a \in A$.

- Si k es un cuerpo, un morfismo de k-módulos es una transformación k-lineal.

Morfismos de Módulos

Sea A un anillo y M, N dos A-módulos. Un morfismo de A-módulos $f : M \to N$ es una función que es A-lineal, es decir, que satisface

- $f(m + m') = f(m) + f(m')$
- $f(a \cdot m) = a \cdot f(m)$

para cada $m, m' \in M$ y $a \in A$.

- Si k es un cuerpo, un morfismo de k-módulos es una transformación k-lineal.
- Un morfismo de $\mathbb{Z}$-módulos es un morfismo de grupos abelianos.

Morfismos de Módulos (cont.)

Fijemos ahora un cuerpo k y caracterizemos los morfismos entre dos $k[X]$-módulos M y N. Una función $f : M \to N$ será un morfismo si

$$f((a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot m) = (a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot f(m)$$

y $f(m + m') = f(m) + f(m')$ para cada $m, m' \in M$ y $a_0, \ldots, a_r \in k$.

Morfismos de Módulos (cont.)

Fijemos ahora un cuerpo k y caracterizemos los morfismos entre dos $k[X]$-módulos M y N. Una función $f : M \to N$ será un morfismo si

$$f((a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot m) = (a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot f(m)$$

y $f(m + m') = f(m) + f(m')$ para cada $m, m' \in M$ y $a_0, \ldots, a_r \in k$. Esto es equivalente a que f sea k-lineal y satisfaga $f(X \cdot m) = X \cdot f(m)$.

Morfismos de Módulos (cont.)

Fijemos ahora un cuerpo k y caracterizemos los morfismos entre dos $k[X]$-módulos M y N. Una función $f : M \to N$ será un morfismo si

$$f((a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot m) = (a_0 + a_1 \cdot X + \cdots + a_r \cdot X^r) \cdot f(m)$$

y $f(m + m') = f(m) + f(m')$ para cada $m, m' \in M$ y $a_0, \ldots, a_r \in k$. Esto es equivalente a que f sea k-lineal y satisfaga $f(X \cdot m) = X \cdot f(m)$.

Por lo tanto, si $T \in \mathrm{End}_k(M)$ y $S \in \mathrm{End}_k(N)$ son los endomorfismos que definen las estructuras de $k[X]$-módulo en M y N, dar un morfismo de $k[X]$-módulos $M \to N$ equivale a dar un morfismo k-lineal $f : M \to N$ tal que $S \circ f = f \circ T$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle S} \\ M & \xrightarrow{f} & N \end{array}$$

Morfismos de Módulos (cont.)

Por lo anterior, fijado M un $k[X]$-módulo sabemos que $\mathrm{End}_{k[X]}(M)$ consiste de los endomorfismos k-lineales de M que conmutan con T,

$$\mathrm{End}_{k[X]}(M) = \{f \in \mathrm{End}_k(M) : f \circ T = T \circ f\} = C_{\mathrm{End}_k(M)}(T).$$

Ejemplo

Consideremos $V = k^2$ como $k[X]$-módulo via $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, es decir, definiendo $X \cdot (x, y) = (y, x)$. Los endomorfismos de V se corresponden con matrices que conmutan con A. Estas son precisamente las matrices $B \in \mathrm{M}_2(k)$ tales que $B_{11} = B_{22}$ y $B_{21} = B_{12}$, pues

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}.$$

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

- Los submódulos de un $\mathbb{Z}$-módulo son sus subgrupos.

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

- Los submódulos de un $\mathbb{Z}$-módulo son sus subgrupos.
- Si V es un k-módulo (es decir un k-e.v.), sus submódulos son los subespacios vectoriales de V.

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

- Los submódulos de un $\mathbb{Z}$-módulo son sus subgrupos.
- Si V es un k-módulo (es decir un k-e.v.), sus submódulos son los subespacios vectoriales de V.
- Si A es un anillo, podemos verlo como un módulo a izquierda sobre sí mismo. Sus submódulos son exactamente sus ideales a izquierda.

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

- Los submódulos de un $\mathbb{Z}$-módulo son sus subgrupos.
- Si V es un k-módulo (es decir un k-e.v.), sus submódulos son los subespacios vectoriales de V.
- Si A es un anillo, podemos verlo como un módulo a izquierda sobre sí mismo. Sus submódulos son exactamente sus ideales a izquierda.
- Sea M un $k[X]$-módulo. Un subconjunto $S \subset M$ es un submódulo si $S + S \subset S$ y $p \cdot S \subset S$ para cada $p \in k[X]$. Asumiendo la primera condición eso es equivalente a que $k \cdot S \subset S$ y $X \cdot S \subset S$.

Submódulos

Recordemos que un submódulo de un A-módulo M es un subconjunto $S \subset M$ tal que $S + S \subset S$ y $a \cdot S \subset S$ para todo $a \in A$.

- Los submódulos de un $\mathbb{Z}$-módulo son sus subgrupos.
- Si V es un k-módulo (es decir un k-e.v.), sus submódulos son los subespacios vectoriales de V.
- Si A es un anillo, podemos verlo como un módulo a izquierda sobre sí mismo. Sus submódulos son exactamente sus ideales a izquierda.
- Sea M un $k[X]$-módulo. Un subconjunto $S \subset M$ es un submódulo si $S + S \subset S$ y $p \cdot S \subset S$ para cada $p \in k[X]$. Asumiendo la primera condición eso es equivalente a que $k \cdot S \subset S$ y $X \cdot S \subset S$.

  Si $T \in \mathrm{End}_k(M)$ define la multiplicación por X, los submódulos de M son sus subespacios T-invariantes.

Cocientes

Sea M un A-módulo. Un submódulo $S \subset M$ es en particular un subgrupo de M, así que tiene sentido considerar el cociente M/S.

Cocientes

Sea M un A-módulo. Un submódulo $S \subset M$ es en particular un subgrupo de M, así que tiene sentido considerar el cociente M/S. Allí existe una única estructura de A-módulo que hace de $\pi : M \to M/S$ un morfismo. Concretamente, es

$$a \cdot [m] := [a \cdot m].$$

Cocientes

Sea M un A-módulo. Un submódulo $S \subset M$ es en particular un subgrupo de M, así que tiene sentido considerar el cociente M/S. Allí existe una única estructura de A-módulo que hace de $\pi : M \to M/S$ un morfismo. Concretamente, es

$$a \cdot [m] := [a \cdot m].$$

Como para grupos y anillos, si $f : M \to N$ es una función A-lineal y $S \subset \ker f$ un submódulo de M entonces tenemos un morfismo inducido en el cociente,

$$\overline{f} : [m] \in M/S \mapsto f(m) \in N.$$

Cuando $S = \ker f$ se tiene un isomorfismo

$$M/\ker f \simeq \mathrm{im} f.$$

Cocientes (cont.)

Proposición

Sea V un k-espacio vectorial de dimensión $n \in \mathbb{N}$ y $S \leq V$ un subespacio de dimensión d. Entonces $\dim_k V/S = n - d$.

Cocientes (cont.)

Proposición

Sea V un k-espacio vectorial de dimensión $n \in \mathbb{N}$ y $S \leq V$ un subespacio de dimensión d. Entonces $\dim_k V/S = n - d$.

Demostración.

Sea $B = \{s_1, \ldots, s_d\}$ una base de S.

Cocientes (cont.)

Proposición

Sea V un k-espacio vectorial de dimensión $n \in \mathbb{N}$ y $S \leq V$ un subespacio de dimensión d. Entonces $\dim_k V/S = n - d$.

Demostración.

Sea $B = \{s_1, \ldots, s_d\}$ una base de S. Podemos extender B a una base $B' = \{s_1, \ldots, s_d, x_1, \ldots, x_{n-d}\}$ de V, veamos ahora que $B'' = \{[x_1], \ldots, [x_{n-d}]\}$ es una base de V/S.

Cocientes (cont.)

Proposición

Sea V un k-espacio vectorial de dimensión $n \in \mathbb{N}$ y $S \leq V$ un subespacio de dimensión d. Entonces $\dim_k V/S = n - d$.

Demostración.

Sea $B = \{s_1, \ldots, s_d\}$ una base de S. Podemos extender B a una base $B' = \{s_1, \ldots, s_d, x_1, \ldots, x_{n-d}\}$ de V, veamos ahora que $B'' = \{[x_1], \ldots, [x_{n-d}]\}$ es una base de V/S.

$\underline{B'' \text{ genera a } V/S}$: si $[x] \in V/S$, existen $a_1, \ldots, a_d, b_1, \ldots, b_{n-d} \in k$ tales que $x = \sum_{j=1}^{d} a_i s_i + \sum_{j=1}^{n-d} b_j x_j$. Tomando clase, es $[x] = \sum_{j=1}^{n-d} b_j [x_j]$.

Cocientes (cont.)

Proposición

Sea V un k-espacio vectorial de dimensión $n \in \mathbb{N}$ y $S \leq V$ un subespacio de dimensión d. Entonces $\dim_k V/S = n - d$.

Demostración.

Sea $B = \{s_1, \ldots, s_d\}$ una base de S. Podemos extender B a una base $B' = \{s_1, \ldots, s_d, x_1, \ldots, x_{n-d}\}$ de V, veamos ahora que $B'' = \{[x_1], \ldots, [x_{n-d}]\}$ es una base de V/S.

B'' genera a V/S: si $[x] \in V/S$, existen $a_1, \ldots, a_d, b_1, \ldots, b_{n-d} \in k$ tales que $x = \sum_{j=1}^{d} a_i s_i + \sum_{j=1}^{n-d} b_j x_j$. Tomando clase, es $[x] = \sum_{j=1}^{n-d} b_j [x_j]$.

B'' es l.i.: supongamos que existen $b_1, \ldots, b_{n-d}$ tales que $\sum_{j=1}^{n-d} b_j [x_j] = 0$. Esto dice que $\sum_{j=1}^{n-d} b_j x_j \in S$ y por lo tanto existe $a_1, \ldots, a_d \in k$ tales que $\sum_{j=1}^{n-d} b_j x_j = \sum_{j=1}^{d} a_i s_i$. Rescribiendo obtenemos una combinación de elementos de B' igualada a cero, y así $b_1 = \cdots = b_{n-d} = 0$. □

Cocientes (cont.)

Corolario

Sean V y W dos k-espacios vectoriales. Si $f : V \to W$ es una transformación k-lineal, entonces $\dim_k V = \dim_k \ker f + \dim_k \operatorname{im} f$.

Cocientes (cont.)

Corolario

Sean V y W dos k-espacios vectoriales. Si $f : V \to W$ es una transformación k-lineal, entonces $\dim_k V = \dim_k \ker f + \dim_k \operatorname{im} f$.

Demostración.

Por el primer teorema de isomorfismo es $V/\ker f \simeq \operatorname{im} f$ y entonces $\dim_k \operatorname{im} f = \dim_k V/\ker f = \dim_k V - \dim_k \ker f$. □

Cocientes (cont.)

Corolario

Sean V y W dos k-espacios vectoriales. Si $f : V \to W$ es una transformación k-lineal, entonces $\dim_k V = \dim_k \ker f + \dim_k \operatorname{im} f$.

Demostración.

Por el primer teorema de isomorfismo es $V/\ker f \simeq \operatorname{im} f$ y entonces $\dim_k \operatorname{im} f = \dim_k V/\ker f = \dim_k V - \dim_k \ker f$. □

Proposición

Si M es un A-módulo e $I \triangleleft A$ es tal que $I \cdot M = 0$, entonces M tiene una estructura de A/I-módulo via $[a] \cdot m = a \cdot m$.

Cocientes (cont.)

Corolario

Sean V y W dos k-espacios vectoriales. Si $f : V \to W$ es una transformación k-lineal, entonces $\dim_k V = \dim_k \ker f + \dim_k \operatorname{im} f$.

Demostración.

Por el primer teorema de isomorfismo es $V/\ker f \simeq \operatorname{im} f$ y entonces $\dim_k \operatorname{im} f = \dim_k V/\ker f = \dim_k V - \dim_k \ker f$. □

Proposición

Si M es un A-módulo e $I \triangleleft A$ es tal que $I \cdot M = 0$, entonces M tiene una estructura de A/I-módulo via $[a] \cdot m = a \cdot m$.

Idea de la demostración.

La hipótesis del enunciado nos dice que el morfismo $\rho : A \to \mathrm{End}_{\mathbb{Z}}(M)$ que le da estructura de A-módulo a M se factoriza por I. □

Ejercicios

Ejercicio

Un A-módulo M se dice cíclico si existe $x \in M$ tal que $Ax = M$. Probar que un módulo es cíclico si y sólo si existe un ideal a izquierda I de A tal que $A/I \simeq M$ como A-módulos.

Ejercicios

Ejercicio

Un A-módulo M se dice cíclico si existe $x \in M$ tal que $Ax = M$. Probar que un módulo es cíclico si y sólo si existe un ideal a izquierda I de A tal que $A/I \simeq M$ como A-módulos.

Ejercicio

Sea M un $k[X]$-módulo. Probar que si $B \subset M$ genera a M como k-espacio vectorial entonces es un sistema de generadores de M como $k[X]$-módulo. Dar un contraejemplo para la afirmación recíproca.

Ejercicios

Ejercicio

Un A-módulo M se dice cíclico si existe $x \in M$ tal que $Ax = M$. Probar que un módulo es cíclico si y sólo si existe un ideal a izquierda I de A tal que $A/I \simeq M$ como A-módulos.

Ejercicio

Sea M un $k[X]$-módulo. Probar que si $B \subset M$ genera a M como k-espacio vectorial entonces es un sistema de generadores de M como $k[X]$-módulo. Dar un contraejemplo para la afirmación recíproca.

Ejercicio

Sea M un A-módulo y $a \in A$ un elemento nilpotente. Probar que si $N \subset M$ es un submódulo de M tal que $M = aM + N$ entonces $M = N$.