Representaciones de grupos finitos

Cándido Martín González

Universidad de Málaga

http://agt2.cie.uma.es/TR.htm

19 de octubre de 2018

Sea R un anillo conmutativo y unitario con unidad. Un R-módulo A se dice que es una R-álgebra si esta dotada de una aplicación

$$A \times A \to A$$

que es R-lineal en cada variable. Dicha operación (llamada producto en lo sucesivo) se denotará usualmente por la simple yuxtaposición o por un punto $\cdot$. Si dicha operación es asociativa diremos que A es una R-álgebra asociativa. En esta parte de la asignatura, todas las álgebras que consideremos serán asociativas.

Si una R-álgebra A tiene elemento neutro para el producto, diremos que es un álgebra con unidad. Las álgebras que consideraremos en este capítulo serán siempre álgebras con unidad. Un álgebra (asociativa) y con unidad $1 \in A$ diremos que es un álgebra de división si

$$\forall x \in A \setminus \{0\}, \exists y \in A \colon xy = yx = 1.$$

Álgebras de división reales

Cuando el anillo base R sea un cuerpo, $R = K$, toda K-álgebra es un espacio vectorial por tanto tiene sentido hablar de su dimensión (como espacio vectorial). Como ejemplos de álgebras reales (es decir $\mathbb{R}$-álgebras), podemos citar $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$. El álgebra $\mathbb{H}$ de los cuaterniones de Hamilton consiste en un espacio vectorial de dimensión cuatro con una base $\{1, i, j, k\}$ cuya tabla de multiplicar se resume en

$$i^2 = j^2 = k^2 = ijk = -1.$$

La tabla de multiplicar completa de $\mathbb{H}$ es

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Por ejemplo, para deducir que $ij = k$ hacemos

$$ijk = -1 \Rightarrow ijk^2 = -k \Rightarrow ij = k.$$

Por lo tanto $\mathbb{H} = \{\lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k : \lambda_i \in \mathbb{R}\}$.
La aplicación lineal $\mathbb{H} \to \mathbb{H}$ dada por $x \mapsto \overline{x}$ donde

$$\overline{\lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k} := \lambda_0 1 - \lambda_1 i - \lambda_2 j - \lambda_3 k$$

satisface las propiedades

$$\overline{xy} = \overline{y}\ \overline{x}, \qquad \overline{\overline{x}} = x$$

para todos $x, y \in \mathbb{H}$. Esta aplicación se llama conjugación cuaterniónica.

Teorema

Para cada $x \in \mathbb{H}$ se tiene $x\overline{x} = \|x\|^2$ donde la norma viene dada por $\|x\|^2 = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2$ siendo $x = \lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k$.

Corolario

$\mathbb{H}$ es un álgebra de división

Dem. Si $x \neq 0$ se tiene $\|x\| \neq 0$ luego $x^{-1} = \|x\|^{-2}\bar{x}$.

En un álgebra A de dimensión finita, sobre un cuerpo K, todo elemento $x \in A$ es raíz de un polinomio mónico mínimal

$$m(x) = 0.$$

La minimalidad quiere dedir que si otro polinomio f verifica que $f(x) = 0$, entonces f es un múltiplo de m.

Demostremos que cada $x \in A$ es raíz de un polinomio mónico: consideremos las potencias de x:

$$1 = x^0, x, x^2, \ldots, x^n, \ldots$$

Como A es de dimensión finita dicho conjunto no puede ser linealmente independiente para todo n. Luego existe un n tal que $1 = x^0, x, x^2, \ldots, x^n$ es linealmente dependiente.

Dicho n se puede tomar mínimo. Por tanto existen escalares $\lambda_i \in K$ con $\lambda_n \neq 0$ tales que $\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n = 0$. Dividiendo entre λ_n vemos que x es raíz de un polinomio mónico de grado n mínimo.

Ahora consideramos el anillo de ideales $K[T]$ en la indeterminada T. Este es un dominio de ideales principales y el conjunto

$$I := \{p \in K[T] : p(x) = 0\}$$

es un ideal de $K[T]$. Por tanto dicho ideal es principal. Luego existe un polinomio mónico $m \in K[T]$ tal que $I = (m)$. Esto demuestra la minimalidad de m.

Teorema

Sea A un álgebra de dimensión finita sobre un cuerpo K algebraicamente cerrado. Si A es de división, entonces $A \cong K$.

Dem. Sea $x \in A$ y m su polinomio minimal. Dicho polinomio se descompone en producto de polinomios de primer grado:

$$m = m_1 \cdots m_k$$

con $m_i \in K[T]$ cada uno de ellos de primer grado.

Entonces

$$0 = m(x) = m_1(x) \cdots m_k(x)$$

y como A es de división, alguno de los factores es nulo. Por tanto $m_i(x) = 0$ para algún i. Como m_i es de primer grado, $m_i = aT + b$ con $a, b \in K$ y $a \neq 0$. Luego $ax + b1 = 0$ y por tanto $x = -a^{-1}b1$. Hemos demostrado que todo elemento es múltiplo escalar de 1.

$$A = K1 \cong K.$$

Corolario

Toda álgebra compleja de división y de dimensión finita es isomorfa a $\mathbb{C}$.

¿Y qué se puede decir de las álgebras reales de división y dimensión finita?

Proposición

Sea A una $\mathbb{R}$-álgebra de división de dimensión finita (unital). Entonces todo el polinomio minimal de cada elemento de A es de grado ≤ 2.

Dem. Sea $x \in A$, si $x = \lambda 1 \in \mathbb{R}1$ entonces x satisface el polinomio $T - \lambda$. Supongamos que x no es escalar. Sea m su polinomio minimal. Sabemos que $m = \prod_i m_i$ donde cada m_i es un polinomio irreducible de $\mathbb{R}[T]$ (por lo tanto cada m_i es de grado uno o dos).

Como $0 = m(x) = \prod_i m_i(x)$, al ser A un álgebra de división, concluimos que para algún i se tienen $m_i(x) = 0$. Por tanto x es raíz de un polinomio de grado dos (al no ser escalar x, no puede ser raíz de un polinomio de grado uno).

Hemos demostrado que en un álgebra real de división y de dimensión finita A, los elementos no escalares son raíz de polinomios de segundo grado:

$$\forall x \in A \setminus \mathbb{R}1, \exists p, q \in \mathbb{R} : x^2 = px + q.$$

(esto es lo que se llama un álgebra cuadrática)

Recordemos de la teoría de extensiones de cuerpos:

Teorema

Si F es un cuerpo extensión de $\mathbb{R}$ con $\dim_{\mathbb{R}}(F)$ finita, entonces $F \cong \mathbb{R}$ o $F \cong \mathbb{C}$.

Sketch de la demo.

$$F \cong \mathbb{R}[T]/(p)$$

donde p es un polinomio irreducible de $\mathbb{R}[T]$. Luego p es de grado 1 o 2. Como $\dim_{\mathbb{R}}(F) = \dim_{\mathbb{R}} \mathbb{R}[T]/(p) = \text{grado}(p)$ concluimos que F es de dimensión 1 o 2 como $\mathbb{R}$-espacio.

Si $\dim_{\mathbb{R}}(F) = 1$ se tiene $F \cong \mathbb{R}$.
Si $\dim_{\mathbb{R}}(F) = 2$ y tomamos $x \in F \setminus \mathbb{R}1$ existen $p, q \in \mathbb{R}$ tales que $x^2 = px + q$. Entonces $y := x - p/2$ verifica

$$y^2 = x^2 - px + p^2/4 = q + p^2/4 \in \mathbb{R}1.$$

Tenemos entonces $y \in F \setminus \mathbb{R}1$ cuyo cuadrado es un escalar k. Veamos que dicho k es negativo:

$$y^2 = k$$

Si $k \geq 0$ tenemos

$$0 = y^2 - k1 = (y - \sqrt{k}1)(y + \sqrt{k}1)$$

luego $y = \sqrt{k}1$ o $y = -\sqrt{k}1$ contradicción. Luego $y^2 = k1$ con $k < 0$. Definamos entonces

$$i := y/\sqrt{-k}.$$

Es fácil ver que $i^2 = -1$ y que $\{1, i\}$ es linealmente independiente con lo que $F = \mathbb{R} \oplus \mathbb{R}i \cong \mathbb{C}$.

Lema

Si A es un álgebra real de división de dimensión finita mayor que 1, siempre existe un elemento cuyo cuadrado es -1.

Teorema de Frobenius

Teorema

Toda álgebra real de división y de dimensión finita es isomorfa a $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$.

Como corolario, las álgebras reales de división y dimensión finita solo pueden tener dimensión 1, 2 o 4.

Dem. del T. de Frobenius

Sea D una $\mathbb{R}$-álgebra de división de dim. finita. Sea F un subespacio conmutativo de D de dimensión máxima. Definamos el centralizador de F en D como el subespacio

$$C_D(F) := \{x \in D : xy = yx,\ \forall y \in F\}.$$

Se tiene $F \subset C_D(F)$. Veamos que $F = C_D(F)$.

Tomemos $x \in C_D(F)$, entonces $F \subset F + \mathbb{R}x$ y por maximalidad de F se tiene $F = F + \mathbb{R}x$ lo que implica $x \in F$.

$$F = C_D(F).$$

Vemos que F es cerrado para el producto: si $x, y \in F$ entonces para cada $f \in F$ se tiene $xyf = xfy = fxy$ luego $xy \in C_D(F) = F$.

Vemos que F es cerrado para la inversion: si $x \in F$ entonces $xf = fx$ para todo $f \in F$. Luego $f = x^{-1}fx$ luego $fx^{-1} = x^{-1}f$ por tanto $x^{-1} \in C_D(F) = F$.

F es un cuerpo.

(por lo tanto $F \cong \mathbb{R}$ o $F \cong \mathbb{C}$ como vimos antes). Ahora, si $\dim(D) = 1$ tenemos $D = \mathbb{R}$ y en este caso hemos terminado. Suponemos pues $\dim(D) > 1$. Por el Lema previo existe un elemento i de cuadrado -1.

Estamos en el caso $\dim(D) > 1$ y $\exists i \in D$ tal que $i^2 = -1$. Entonces F no puede ser $F = \mathbb{R}1$ porque $\mathbb{R}1 \oplus \mathbb{R}i$ es un subespacio conmutativo de dimensión 2 lo que contradice la maximalidad de F. Por lo tanto podemos tomar $F = \mathbb{R}1 \oplus \mathbb{R}i \cong \mathbb{C}$. D es un F-espacio vectorial por la izquierda Definamos

$$S\colon D \to D, \text{ tal que } S(x) = xi$$

para cada x. Esta aplicación es F-lineal y como $S^2 = -1_D$, es diagonalizable.

Como S es raíz del polinomio $T^2 + 1 = 0$ los únicos posibles autovalores son $\pm i$. Sea $D_+ := \{x \in D : xi = ix\}$ es espacio propio de autovalor i,
$D_- := \{x \in D : xi = -ix\}$ es espacio propio de autovalor $-i$. Se tiene $D_+ \cap D_- = 0$ y $D = D_+ + D_-$.
Esto último obedece a la igualdad

$$x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi)$$

donde $x - ixi \in D_+$, $x + ixi \in D_-$.

$$D = D_+ \oplus D_-$$

$$D_+D_+ \subset D_+,\ D_-D_- \subset D_+,\ D_+D_- \subset D_-,\ D_-D_+ \subset D_-.$$

Por otra parte $D_+ \subset C_D(F) = F \subset D$ luego $D_+ = \mathbb{R}1 \oplus \mathbb{R}i$. Si $D_- = 0$ hemos demotrado que $D = D_+ \cong \mathbb{C}$. Supongamos $D_- \neq 0$.
Si fijamos $z \in D_- \setminus \{0\}$, la aplicación $D_+ \to D_-$ tal que $x \mapsto zx$ es un isomorfismo de espacios vectoriales (su inversa en $x \mapsto z^{-1}x$). Por lo tanto $\dim(D_+) = \dim(D_-)$ y $\dim(D) = 2\dim(D_+)$.

Sea $z \in D_-$ no nulo. Como z satisface una ecuación de segundo grado $z^2 = pz + q$ donde $p, q \in \mathbb{R}$. Por otra parte $z \in D_-$ luego $zi = -iz$ y $z^2 i = iz^2$ lo que implica $pzi + qi = piz + qi$, es decir, $pzi = piz$ por tanto $p = 0$ y $z^2 \in \mathbb{R}1$.

$$z^2 = k1, \quad k \in \mathbb{R}$$

Si $k \geq 0$, tenemos

$$0 = z^2 - k1 = (z - \sqrt{k}1)(z + \sqrt{k}1)$$

luego $z = \pm\sqrt{k} \in \mathbb{R}$ una contradicción.
Así $k < 0$ y definiendo $j = z/\sqrt{-k}$ tenemos $j \in D_-$ tal que $j^2 = -1$. Definamos ahora $k = ij$.

$$k^2 = ijij = -i^2j^2 = j^2 = -1$$

$$ijk = kk = -1$$

por lo tanto

Además $1, i, j, k$ son linealmente idempendientes y $D = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ satisfaciéndose

$$i^2 = j^2 = k^2 = ijk = -1.$$

En resumen

$$D \cong \mathbb{H}.$$

Un álgebra A se dice que es simple si $A^2 \neq 0$ y sus únicos ideales son 0 y A.
Si un álgebra A tiene unidad son equivalentes:
(1) A es simple.
(2) Los únicos ideales de A son 0 y A.

Como consecuencia de la teoría de Wedderburn-Artin, si A es un álgebra simple y de dimensión finita sobre un cuerpo K, se tiene que A es isomorfa a un álgebra $M_n(D)$ (matrices $n \times n$ con coeficientes en D) donde D es una K-álgebra de división y dimensión finita.

Corolario

Si A es un álgebra compleja, simple y finito-dimensional,

$$A \cong M_n(\mathbb{C})$$

para un cierto natural n.

Si $M_n(\mathbb{C}) \cong M_k(\mathbb{C})$ entonces $n = k$.

Corolario

Si A es un álgebra real, simple y finito-dimensional, A es isomorfa a $M_n(\mathbb{R})$, a $M_n(\mathbb{C})$ o a $M_n(\mathbb{H})$ para algún n.

Si $M_n(D) \cong M_k(D)$ entonces $n = k$ (válido para $D = \mathbb{R}, \mathbb{C}$ o $\mathbb{H}$).
Además, $\forall n, k$ se tiene $M_n(\mathbb{R}) \ncong M_k(\mathbb{C})$, $M_n(\mathbb{R}) \ncong M_k(\mathbb{H})$, $M_n(\mathbb{C}) \ncong M_k(\mathbb{H})$.

Un álgebra A se dice semisimple si es suma directa de álgebras simples. Esto es equivalente a que A sea semisimple como módulo sobre si mismo a izquierda: ${}_AA$ es un A-módulo semisimple. Otra caracterización de la semisimplicidad de A es que todo A-submódulo de ${}_AA$ sea un sumando directo.

Teorema

A es un álgebra semisimple (de dimensión finita) sobre un cuerpo K algebraicamente cerrado si y solo si A es isomorfa a

$$M_{n_1}(K) \oplus \cdots \oplus M_{n_q}(K)$$

donde $n_i \in \mathbb{N}^*$. Los naturales n_i están determinados de forma única.

Teorema

A es un álgebra semisimple (de dimensión finita) sobre $\mathbb{R}$ si y solo si A es isomorfa a

$$M_{n_1}(D_1) \oplus \cdots \oplus M_{n_q}(D_q)$$

donde $n_i \in \mathbb{N}^*$ y cada D_i es $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$. Los naturales n_i y las álgebras D_i están determinados de forma única.

¿Salvo isomorfismo, cuántas álgebras complejas semisimples de dimensión ≤ 4 hay?

Dimensión 1: $\mathbb{C}$

Dimensión 2: $\mathbb{C}^2$

Dimensión 3: $\mathbb{C}^3$

Dimensión 4: $\mathbb{C}^4$, $M_2(\mathbb{C})$.

¿Salvo isomorfismo, cuántas álgebras reales semisimples de dimensión ≤ 4 hay?

Dimensión 1: $\mathbb{R}$

Dimensión 2: $\mathbb{R}^2$, $\mathbb{C}$

Dimensión 3: $\mathbb{R}^3$, $\mathbb{R} \oplus \mathbb{C}$

Dimensión 4: $\mathbb{R}^4$, $\mathbb{R}^2 \oplus \mathbb{C}$, $\mathbb{C}^2$, $\mathbb{H}$, $M_2(\mathbb{R})$.

Descomposición de Peirce

Sea A una R-álgebra (con unidad). R es un anillo no necesariamente un cuerpo. Supongamos que

$$\{e_1, \ldots, e_n\}$$

es un sistema de idempotentes ortogonales (i.e. $e_i e_j = \delta_{ij} e_i$) tales que $\sum_1^n e_i = 1$. Sea $A_{ij} := e_i A e_j = \{e_i x e_j : x \in A\}$ para $i, j = 1, \ldots, n$. Entonces

$$A = \bigoplus_{i,j=1}^{n} A_{ij}$$

Dem. Sea $x \in A$,

$$x = 1x1 = (\sum_i e_i)x(\sum_i e_j) = \sum_{ij} e_i x e_j \in \sum_{ij} A_{ij}.$$

Esto prueba que $A = \sum_{ij} A_{ij}$. Se deja al lector demostrar que la suma es directa.

Si A es conmutativa y $i \neq j$ se tiene $A_{ij} = e_i A e_j = A e_i e_j = 0$. Además $A_{ii} = e_i A e_i = A e_i = e_i A$. Luego en el caso conmutativo la descomposición de Peirce es

$$A = \oplus_1^n A e_i.$$

Módulo libre

Sea R un anillo conmutativo y unitario. Sea X un conjunto, definimos el R-módulo libre generado por X como el R-módulo RX de todas las aplicaciones $f : X \to R$ de soporte finito. Recordemos que

$$\mathrm{Sop}(f) := \{x \in X : f(x) \neq 0\}.$$

$$RX = \{f : X \to R | \text{Sop}(f) \text{ es finito } \}.$$

$$X \to RX, x \mapsto f_x$$

donde $f_x : X \to R$ viene dada por $f_x(y) = \delta_{xy}$. Esta aplicación es inyectiva por lo que identificamos X con su imagen en RX. Todo elemento de RX es combinación lineal de ciertos f_x:

$$\forall f \in R(X), f = \sum_{x \in \text{Sop}(f)} f(x) f_x$$

Además el conjunto $\{f_x : x \in X\}$ es R-linealmente independiente. Por lo tanto es una base de RX, i.e. el R-módulo RX es libre. Cuando R es un cuerpo se obtiene el espacio vectorial libre generado por X. Como X se ha identificado con $\{f_x : x \in X\}$, podemos abusar un poco de la notación y escribir

$$RX = \{\sum_x \lambda_x x : \lambda_x \in R\}.$$

En caso de que $R = K$ un cuerpo, el K-espacio vectorial libre generado por un conjunto X es el conjunto de combinaciones lineales formales

$$\sum_x \lambda_x x$$

donde $x \in X$ y los escalares $\lambda_x \in K$ son nulos salvo un número finito.

Obviamente las operaciones que dan a RX estructura de R-módulo vienen dadas por

$$\sum_x \lambda_x x + \sum_x \mu_x x := \sum_x (\lambda_x + \mu_x) x,$$

$$\alpha \sum_x \lambda_x x := \sum_x \alpha \lambda_x x.$$

Si $X = G$ un grupo, entonces el R-módulo RG admite una estructura de R-álgebra

$$(\sum_g \lambda_g g)(\sum_h \mu_h h) := \sum_{g,h} \lambda_g \mu_h (gh).$$

Este álgebra RG es lo que se llama el "álgebra grupo" de G con coeficientes en R.

Ejemplo: $\mathbb{R}\mathbb{Z}_2$
$\mathbb{Z}_2 = \{1, u\}$ con $u^2 = 1$.

$$\mathbb{R}\mathbb{Z}_2 = \{\alpha 1 + \beta u \colon \alpha, \beta \in \mathbb{R}\}.$$

Busquemos los idempotentes de este álgebra $e = \alpha 1 + \beta u$,

$$e^2 = \alpha^2 1 + \beta^2 1 + 2\alpha\beta u = \alpha 1 + \beta u$$

$$\begin{cases} \alpha^2 + \beta^2 = \alpha \\ 2\alpha\beta = \beta \end{cases}$$

$$\begin{cases} \alpha^2 + \beta^2 = \alpha \\ 2\alpha\beta = \beta \end{cases}$$

Si $\beta \neq 0$ tenemos $\alpha = 1/2 \Rightarrow \beta = \pm 1/2$.

Si $\beta = 0$, tenemos $\alpha = 0, 1$.

Por lo tanto los idempotentes de $\mathbb{R}\mathbb{Z}_2$ son $0, 1, \frac{1}{2}(1+u), \frac{1}{2}(1-u)$.

$e_1 = \frac{1}{2}(1+u), e_2 = \frac{1}{2}(1-u)$. Estos dos idempotentes son ortogonales

$$e_1 e_2 = \frac{1}{4}(1+u)(1-u) = \frac{1}{4}(1^2 - u^2) = 0$$

y su suma es 1. Por lo tanto la descomposición de Peirce nos da

$$\mathbb{R}\mathbb{Z}_2 = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \cong \mathbb{R} \oplus \mathbb{R}$$

ya que $\mathbb{R}e_1 \cong \mathbb{R}$ y $\mathbb{R}e_2 \cong \mathbb{R}$.

En realidad en la demostración anterior solo hemos utilizado que $1/2 \in \mathbb{R}$ por lo tanto el resultado es cierto para todo cuerpo de característica distinta de dos:
Si $\text{car}(K) \neq 2$ se tiene $K\mathbb{Z}_2 \cong K \oplus K$.

Teorema de Maschke

Teorema

Sea G un grupo finito y K un cuerpo cuya característica no divida al orden de G. Entonces el álgebra grupo KG es semisimple.

Dem. Sea $A := KG$ y V un A-submódulo de A. Tenemos que demostrar que V es un sumando directo de A. Para ello tomamos un subespacio vectorial W complementario de V, es decir, $A = V \oplus W$ como espacios vectoriales.

Sea $p\colon A \to A$ tal que $p(v) = v$ para cada $v \in V$ y $p(W) = 0$. La imagen de p está contenida en V y p es una aplicación lineal pero no es necesariamente un homomorfismo de A-módulos .

Definamos $q\colon A \to A$ mediante la fórmula

$$q(x) = \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}x).$$

Como car(K) no divide a $|G|$ el escalar $\frac{1}{|G|}$ pertenece a K lo que le da sentido a la fórmula de arriba. Por otra parte como la imagen de p es V cada elemento $gp(x) \in V$ para cada x. Luego la imagen de q está contenida en V.

Es fácil demostrar que $q(x+y) = q(x) + q(y)$ para cualesquiera $x, y \in A$. Veamos que $q(hx) = hq(x)$ para cada $h \in G$ y $x \in A$.

$$q(hx) = \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}hx) =$$

$$\frac{1}{|G|} \sum_{g \in G} hh^{-1}gp(g^{-1}hx) = h\frac{1}{|G|} \sum_{g \in G} h^{-1}gp(g^{-1}hx) =$$

$$h\frac{1}{|G|} \sum_{k \in G} kp(k^{-1}x) = hq(x).$$

Por lo tanto q es un homomorfismo de A-módulos $q\colon A \to A$. Además si $x \in V$ se tiene $g^{-1}x \in V$ luego $p(g^{-1}x) = g^{-1}x$ y $q(x) = x$. Veamos que $q^2 = q$. Como $q(x) \in V$, $q(q(x)) = q(x)$. Tenemos pues $q^2 = q$. Como q es un homomorfismo de A-módulos , $\ker(q)$ e $\mathrm{im}(q)$ son A-submódulos. Veamos que

$$A = \ker(q) \oplus \mathrm{im}(q).$$

$$A = \ker(q) \oplus \mathrm{im}(q).$$

Si $x \in \ker(q) \cap \mathrm{im}(q)$ tenemos $x = q(y)$ y además $0 = q(x) = q(q(y)) = q(y) = x$. Por tanto $\ker(q) \cap \mathrm{im}(q) = 0$.

Por otra parte para cada $a \in A$ se tiene $a = q(a) + a - q(a)$ donde $q(a) \in \mathrm{im}(q)$ y $a - q(a) \in \ker(q)$.

Como $V = \mathrm{im}(q)$ concluimos

$$A = \ker(q) \oplus V.$$