Algebra Abstracta II: Tarea #1

Jonathan Andrés Niño Cortés

13 de febrero de 2015

Sección 7.1 8. Describa el centro de los Cuaterniones Hamiltonianos reales $\mathbb{H}$. Puebe que $\{a + bi|a, b \in \mathbb{R}\}$ es un subanillo de $\mathbb{H}$ que es un campo pero no esta contenido en el centro de $\mathbb{H}$.

Demostración. Los elementos de $\mathbb{H}$ los representamos como $a+bi+cj+dk$. Vamos a demostrar que el centro esta conformado por los elementos de la forma $x \in \mathbb{H}$ con $x \in \mathbb{R}$. Obsérvese que $x * (a + bi + cj + dk) = (a + bi + cj + dk) * x = ax + bxi + cxj + dxk$.

Ahora obsérvese que si b, c o d son diferentes de 0, entonces $a + bi + cj + dk$ no conmuta con todos los elementos de $\mathbb{H}$. Supongamos que $b \neq 0$, o $d \neq 0$ y tomemos el elemento j.

Por un lado,

$$(a + bi + cj + dk) * j \quad = \quad -c - di + aj + bk$$

Por otra parte,

$$j * (a + bi + cj + dk) \quad = \quad -c + di + aj - bk$$

Vemos que, por nuestra suposición, no conmutan entre si.

De igual manera, si suponemos que $c \neq 0$, entonces tomamos el elemento i. Vemos que,

$$(a + bi + cj + dk) * i \quad = \quad -b + ai + dj - ck$$

y

$$i * (a + bi + cj + dk) \quad = \quad -b + ai - dj + ck$$

Ahora probemos que $\{a + bi|a, b \in \mathbb{R}\}$ son un subanillo de $\mathbb{H}$ que es un campo.

Primero probemos que es cerrado bajo substracción

$$(a + bi) - (c + di) = (a - c) + (b - d)i$$

que esta en el conjunto porque los reales son cerrados bajo substracción. Ahora probemos que es cerrado bajo multiplicación

$$(a + bi) * (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

que esta en el conjunto porque los reales son cerrados bajo multiplicación y substracción. $\square$

Ahora probemos que es conmutativo

$$\begin{aligned}(a+bi)*(c+di) &= ac+adi+bci+bdi^2=(ac-bd)+(ad+bc)i\\(c+di)*(a+bi) &= ca+ai+dai+dbi^2=(ca-dc)+(da+cb)i\end{aligned}$$

Vemos que los dos resultados son iguales porque la multiplicación de los reales es conmutativa. Finalmente probemos que es un campo. Tomemos un elemento $a+bi$ diferente de 0. Por propiedades de los complejos sabemos que si es diferente de 0 entonces existe un inverso multiplicativo y se puede calcular como el conjungado dividido la norma al cuadrado.

En efecto,

$$\frac{(a+bi)*(a-bi)}{a^2+b^2}=\frac{a^2-abi+abi-b^2i^2}{a^2+b^2}=\frac{a^2+b^2}{a^2+b^2}=1$$

Por lo tanto, el conjunto es un campo. Finalmente el campo no pertenece al centro porque hay elementos que no conmutan con todos los elementos de $\mathbb{H}$. Cualquier $a+bi$ con $b\neq 0$, no pertenece al centro como se demostro anteriormente.

Sección 7.1 13. Un elemento $x \in \mathbb{R}$ se llama nilpotente si $x^m = 0$ para algún $m \in \mathbb{Z}^+$.

(a) Muestre que si $n = a^k b$ para algunos enteros a y b entonces $\overline{ab}$ es un elemento nilpotente de $\mathbb{Z}/n\mathbb{Z}$.

Demostración. Probamos que $\overline{ab}^k = \overline{0}$.

Por un lado tenemos que $\overline{ab}^k = \overline{a}^k \overline{b}^k$, ya que el anillo es conmutativo. Además de la suposición que $n = a^k b$ reduciendo módulo n obtenemos que $\overline{a}^k \overline{b} = \overline{0}$. Por lo tanto, $\overline{ab}^k = \overline{a}^k \overline{b}^k = \overline{0} * \overline{b}^{(k-1)} = \overline{0}$. □

(b) Si $a \in \mathbb{Z}$ es un entero, muestra que el elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ es nilpotente si y solo si cualquier primo divisor de n es también un divisor de a. En particular, determina los elementos nilpotentes de $\mathbb{Z}/72\mathbb{Z}$ explicitamente.

Demostración. Por el teorema fundamental de la aritmética podemos escribir $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ con p_i primo y $\alpha_i > 0$ para todo i tal que $0 \leq i \leq n$. Por la suposición anterior podemos escribir $a = p_1^{\beta_1} \cdots p_n^{\beta_n} b$ con $b \in \mathbb{Z}$, $\beta_i > 0$ para todo i tal que $0 \leq i \leq n$. Entonces podemos tomar $k = \max(\{\alpha_i | 0 \leq i \leq n\})$. De esta manera $a^k = p_1^{\beta_1 k} \cdots p_n^{\beta_n k} b^k$ y podemos ver que n divide a a^k. Por lo tanto, a es nilpotente.

Para el converso obsérvese que si a es nilpotente entonces $a^k = nb$ para algún $b \in \mathbb{Z}$. Por lo tanto, $a^k = p_1^{\alpha_1} \cdots p_n^{\alpha_n} b$. De aquí podemos concluir que cualquier primo que divide a n también divide a a. Pero esto implica que dentro de la expansión en primos de a^k estan incluidos estos primos y por lo tanto también estan incluidos en la expansión de a.

Utilizando el resultado anterior concluimos que los elementos nilpotentes de $\mathbb{Z}/72\mathbb{Z}$ $(72 = 2^3 3^2)$ son $\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}, \overline{54}, \overline{60}$ y $\overline{66}$. □

(c) Sea R el anillo de funciones del grupo no vacío X a un campo F. Pruebe que R no contiene elementos nilpotentes diferentes a $\mathbf{0}$.

Demostración. Sabemos que los elementos nilpotentes también son divisores de $\mathbf{0}$. También sabemos que en este anillo los divisores de $\mathbf{0}$, son aquellas funciones f que mapean elementos de X a 0, por que podemos definir una función g tal que $g(x) = 0$ si $f(x) \neq 0$ y $g(x) = 1$ si $f(x) = 0$, y claramente $fg = \mathbf{0}$. Consideremos una función f dentro del conjunto de divisores de $\mathbf{0}$ diferentes a $\mathbf{0}$. Por lo tanto debe haber un $x \in X$ tal que $f(x) \neq 0$. Notese que $f(x)$ es una unidad porque F es un campo y $f(x)$ es diferente de 0. Para que esta función sea nilpotente debe existir un mínimo $k > 0$ tal que $f(x)^k = 0$. Si suponemos que este k existe entonces llegamos a una contradicción porque entonces $f(x) * f(x)^{k-1} = 0$ y por lo tanto $f(x)$ seria un divisor de 0, lo cual es una contradicción ya que $f(x)$ es una unidad. □

Sección 7.2 3. Defina el conjunto $R[[x]]$ de *series de potencias formales* en el indeterminado x con coeficientes de R como todas las sumas infinitas formales

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots .$$

Defina la adición y multiplicación de la misma manera que las series de potencias con coeficiente reales o complejos, i.e., adición y multiplicación polinomial extendida a series de potencias como si fueran "polinomios de infinito grado".

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) x^n$$

(a) Pruebe que $R[[x]]$ es un anillo conmutativo con 1.

Demostración. Primero demostramos que $R[[x]]$ con la operación $+$ es un grupo conmutativo.

Asociatividad:

$$\begin{aligned}
(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n) + \sum_{n=0}^{\infty} c_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n + \sum_{n=0}^{\infty} c_n x^n \\
&= \sum_{n=0}^{\infty} ((a_n + b_n) + c_n) x^n \\
&\quad \text{(por asociatividad de + en } R) \\
&= \sum_{n=0}^{\infty} (a_n + (b_n + c_n)) x^n \\
&= \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} (b_n + c_n) x^n \\
&= \sum_{n=0}^{\infty} a_n x^n + (\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n)
\end{aligned}$$

Conmutatividad:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n \\
&\quad \text{(por conmutatividad de + en } R\text{)} \\
&= \sum_{n=0}^{\infty} (b_n + a_n) x^n \\
&= \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n
\end{aligned}$$

Identidad aditiva: Sea $\theta_i = 0, \forall i \geq 0$. Entonces la serie $\sum \theta_n x^n$ es la identidad.

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} \theta_n x^n &= \sum_{n=0}^{\infty} (a_n + \theta_n) x^n \\
&= \sum_{n=0}^{\infty} (a_n + 0) x^n \\
&= \sum_{n=0}^{\infty} a_n x^n
\end{aligned}$$

$\sum \theta_n x^n + \sum a_n x^n = \sum a_n x^n$ por la conmutatividad demostrada anteriormente.

Inverso: Sea $\sum a_n x^n$ una serie y tomese la serie $\sum -a_n x^n$. Se puede observar que la suma de estas series es igual a la serie $\sum \theta_n x^n$.

Ahora vamos a demostrar que la multiplicación es asociativa.

Observación: La multiplicación se puede definir equivalentemente como

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (\sum_{i,j \in \mathbb{N}, i+j=n} a_i b_j) x^n$$

Utilizando esta definición podemos ver que

$$\begin{aligned}
(\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n) \times \sum_{n=0}^{\infty} c_n x^n &= \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j) x^n \times \sum_{n=0}^{\infty} c_n x^n \\
&= \sum_{n=0}^{\infty} (\sum_{m+k=n} (\sum_{i+j=m} a_i b_j) c_k) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j+k=n} a_i b_j c_k) x^n
\end{aligned}$$

Por otra parte

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n \times (\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} c_n x^n) &= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} (\sum_{j+k=n} b_j c_k) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+m=n} (a_i \sum_{j+k=m} b_j c_k)) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j+k=n} (a_i b_j c_k) x^n
\end{aligned}$$

Vemos que son iguales.

Conmutatividad:

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j) x^n$$

Por otro lado vemos que

$$\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} (\sum_{i+j=n} b_i a_j) x^n$$

Obsérvese que $\sum_{i+j=n} a_i b_j = \sum_{i+j=n} a_j b_i$ por un simple reordenamiento de términos y a su vez $\sum_{i+j=n} a_j b_i = \sum_{i+j=n} b_i a_j$ porque el anillo R es conmutativo. Luego las dos series conmutan.

Identidad multiplicativa: La serie $1 = \sum_{n=0}^{\infty} e_n x^n$ donde el término $e_0 = 1$ y cuyos demás términos son 0, es la identidad multiplicativa.

Distributividad:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n \times (\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n) &= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} (b_n + c_n) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i (b_j + c_j)) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j + a_i c_j) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j + \sum_{i+j=n} a_i c_j) x^n \\
&= \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j) x^n + \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i c_j) x^n \\
&= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} c_n x^n
\end{aligned}$$

Por otra parte $\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} e_n x^n = \sum_{n=0}^{\infty} a_n x^n$ por la conmutatividad de la multiplicación demostrada anteriormente. $\square$

(b) Muestre que $1 - x$ es una unidad en $R[[x]]$ con inverso $1 + x + x^2 + \cdots$.

Demostración. Se puede observar que la multiplicación da como resultado

$$(1-x) \times \sum_{n=0}^{\infty} x^n = 1 + \sum_{n=1}^{\infty} (1 * x^n - x * x^{n-1}) = 1 + \sum_{n=1}^{\infty} (x^n - x^n) = 1$$

$\square$

(c) Pruebe que $\sum_{n=0}^{\infty} a_n x^n$ es una unidad en $R[[x]]$ si y solo si a_0 es una unidad en R.

Demostración. Tomemos una serie $\sum_{n=0}^{\infty} a_n x^n$ y supongamos que existe $\sum_{n=0}^{\infty} b_n x^n$ tal que

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) x^n = 1.$$

En primer lugar se debe de cumplir que el coeficiente c_0 de la serie producto sea 1. Vemos que $c_0 = a_0 b_0$ por lo que esto solo se puede cumplir si a_0 es una unidad.

Ahora supongamos que a_0 es una unidad y por lo tanto existe b_0 tal que $c_0 = a_0 b_0 = 1$. Ahora se deben encontrar el resto de los b_n's de tal manera que $\sum_{k=0}^{n} a_k b_{n-k} = 0$. Entonces definimos b_n recursivamente como $-b_0 \sum_{j=1}^{n} a_k b_{n-k}$. De tal manera que para $n > 0$

$$\begin{aligned}
\sum_{k=0}^{n} a_k b_{n-k} &= a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k} \\
&= a_0(-b_0 \sum_{j=1}^{n} a_k b_{n-k}) + \sum_{k=1}^{n} a_k b_{n-k} \\
&= a_0 b_0(- \sum_{j=1}^{n} a_k b_{n-k}) + \sum_{k=1}^{n} a_k b_{n-k} \\
&= (- \sum_{j=1}^{n} a_k b_{n-k}) + \sum_{k=1}^{n} a_k b_{n-k} \\
&= 0
\end{aligned}$$

$\square$

Sección 7.2 3. Pruebe que el centro del anillo $M_n(R)$ es el conjunto de matrices escalares.

Demostración. Las matrices escalares son aquellas de la forma $M = \lambda I$, con $\lambda \in R$.

Por un lado si M es una matriz escalar entonces pertenece al centro porque tomando cualquier matriz $A \in M(R)$

$$MA = \lambda IA = \lambda AI = A\lambda I = AM$$

Ahora probemos que si M no es escalar entonces no pertenece al centro. Por ejemplo, supongamos primero que no es una matriz diagonal, entonces existe una entrada a_{ij} tal que $i \neq j$, y $a_{ij} \neq 0$. Entonces tomemos la matriz E_{ji} cuyas entradas son 0, exceptuando la entrada ji que es 1. Veamos que estas matrices no conmutan entre si.

La entrada (j, j) de la matriz $A = E_{ji}M$ es igual a

$$\sum_{k=0}^{n} e_{jk}m_{kj} = e_{ji}m_{ij} = m_{ij}$$

Por otra parte la entrada (j, j) de la matriz $B = ME_{ji}$ es

$$\sum_{k=0}^{n} m_{jk}e_{kj} = 0$$

porque ningún e_kj puede ser igual a e_{ji} debido a nuestra suposición que $i \neq j$

Ahora supongamos que M es una matriz diagonal pero que existen i, j tales que $m_{ii} \neq m_{jj}$ y tomemos la matriz E_{ij} tal que todas sun entradas son 0 menos la entrada ij.

La entrada (i, j) de la matriz $A = E_{ij}M$ es igual a

$$\sum_{k=0}^{n} e_{ik}m_{kj} = e_{ij}mjj = mjj$$

Por otra parte la entrada (i, j) de la matriz $B = ME_{ji}$ es

$$\sum_{k=0}^{n} m_{ik}e_{kj} = m_{ii}e_{ij} = m_{ii}$$

Y vemos que son diferentes por nuestra suposición. $\square$

Sección 7.3 10. Decida cual de los siguientes son ideales del anillo $\mathbb{Z}[x]$:

(a) el conjunto de todos los polinomios cuyo término constante es un múltiplo de 3

Demostración. Como el anillo es conmutativo solo es necesario verificar que la multiplicación es cerrada por izquierda o por derecha, no por las dos. Este si es un ideal. El conjunto es un subgrupo aditivo porque la resta de dos poliminos cuyo término constante es múltiplo de 3 da como resultado un elemento cuyo término constante es también múltiplo de 3.

Si tomamos cualquier polinomio y cualquier elemento en el ideal vemos que la multiplicacion también cae en el ideal porque el término constante tambien seria un multiplo de 3. □

(b) el conjunto de todos los polinomios cuyo coeficiente de x^2 es un múltiplo de 3

Demostración. Este no es un ideal. Tomese por ejemplo el polinomio $(3x^2 + 2x + 1)$ en el ideal, al multiplicarlo por $x + 1$, obtenemos $3x^3 + 5x^2 + 3x + 1$, que no esta en el ideal. □

(c) el conjunto de todos los polinomios cuyo término constante, coeficiente de x y coeficiente de x^2 son cero

Demostración. Este es un ideal. Es un subgrupo aditivo porque la resta de cualquier polinomio de esta forma vuelve a dar un polinomio de esta forma. Además si multiplicamos cualquier polinomio $\sum_{i=3}^{n} a_n x^n$ por un polinomio $\sum_{i=0}^{n} b_n x^n$. Obsérvese que $a_0 b_0 = 0, a_1 b_0 + a_0 b_0 = 0, a_2 b_0 + a_1 b_1 + a_0 b_2 = 0$. Vemos que la multiplicación da de nuevo un elemento en el ideal. Este puede verse como el ideal generado por x^3 □

(d) $\mathbb{Z}[x^2]$ (i.e., los polinomios en los cuales solamente las potencias pares de x aparecen)

Demostración. No es un ideal, tome por ejemplo x^2 en el ideal y el polinomio x. $x * x^2 = x^3$ no está en el ideal. □

(e) el conjunto de los polinomios cuyos coeficientes suman a cero

Demostración. Si es un ideal. Podemos probar esto utilizando el homomorfismo de evaluación en 1 $\phi(P(x)) = P(1)$. Este conjunto seria el kernel de este homomofismo. (Idea propuesta por Rafael Mantilla). □

(f) el conjunto de los polinomios $p(x)$ tal que $p'(0) = 0$, donde $p'(x)$ es la primera derivada usual de $p(x)$ con respecto a x.

Demostración. No es un ideal. Por ejemplo, el polinomio 1 esta en el conjunto porque su derivada siempre es 0. Pero $1 * x$ igual a x no esta en el conjunto pues su derivada evaluada en 0 es 1. □

Sección 7.3 13. Pruebe que el anillo $M_2(\mathbb{R})$ contiene un subanillo que es isomórfico a $\mathbb{C}$.

Demostración. Tome A el conjunto de todas las matrices de la forma

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

con $a, b \in \mathbb{R}$ Sea $\phi : A \mapsto \mathbb{C}$ la función definida como

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + ib$$

Vamos a demostrar que esta función es un homorfismo biyectivo de anillos.

La función es trivial por la buena definición de esta representación de los reales. Es inyectiva pues si $(a, b) \neq (c, d)$ entonces $a + ib \neq c + id$. Y es sobreyectiva porque para cualquier $a + ib \in \mathbb{C}$ existe una preimagen respectiva (a, b).

Por otro lado para probar que preserva la suma tomemos

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a+c & -b-d \\ b+d & a+c \end{pmatrix}\right)$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = (a+c) + (b+d)i$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = (a+bi) + (c+di)$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) + \phi\left(\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right)$$

Ahora probemos que preserva la multiplicación

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = \phi\left(\begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}\right)$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = (ac-bd) + (bc+ad)i$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = (a+bi) * (c+di)$$

$$\phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right)\phi\left(\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right)$$

Concluimos que A es isomorfo a $\mathbb{C}$, por lo tanto A es un subanillo de $M_2(R)$. $\square$