Algebra Moderna

Ejercicios Capitulo IV.1

Por: Alvarado Cabrera Lorenzo Antonio

Problema 1.3. Verifique que los cuaternios $\mathbb{H}$ forman un anillo (no conmutativo) con división.

Demostración. –

- La propia definición de suma y producto de cuaterniones es tal que son operaciones cerradas.

- La asociatividad de las operaciones se hereda de la asociatividad de las operaciones de $\mathbb{R}$.

- Las operaciones tienen sus elementos neutros.

$$\begin{aligned}(a+bi+cj+dk)\oplus(0+0i+0j+0k) &= (a+0)+(b+0)i+(c+0)j+(d+0)k \\ &= a+bi+cj+dk\end{aligned}$$

$$\begin{aligned}(a+bi+cj+dk)\oplus(1+0i+0j+0k) &= (a\cdot 1-b\cdot 0-c\cdot 0-d\cdot 0) \\ &\quad +(a\cdot 0+b\cdot 1+c\cdot 0-d\cdot 0)i \\ &\quad +(a\cdot 0+c\cdot 1+d\cdot 0-b\cdot 0)j \\ &\quad +(a\cdot 0+d\cdot 1+b\cdot 0-c\cdot 0) \\ = a+bi+cj+dk\end{aligned}$$

- Existe inverso de la suma, y de la multiplicación (anillo con división)

$$(a+bi+cj+dk)\oplus((-a)+(-b)i+(-c)j+(-d)k) = (a-a)+(b-b)i+(c-c)j+(d-d)k = 0$$

$$(a+bi+cj+dk)^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a-bi-cj-dk)$$

- Se cumple la ley distributiva, heredada por $\mathbb{R}$.

Por tanto es un anillo con división.

■

Problema 1.7. Pruebe que un subanillo no trivial Γ de un dominio entero Λ es un subdominio de Λ si, y solo si, Γ contiene al elemento identidad de Λ.

Demostración. –
$\Rightarrow$] Supongamos que Γ es subdominio de Λ, entonces dado que $1_\Gamma 1_\Lambda = 1_\Gamma = 1_\Gamma 1_\Gamma \Rightarrow 1_\Gamma 1_\Lambda - 1_\Gamma 1_\Gamma = 0 \Rightarrow 1_\Gamma(1_\Lambda - 1_\Gamma) = 0$ pero como Γ es subdominio entonces $1_\Gamma = 0$ o $1_\Lambda - 1_\Gamma = 0$, el primero no es posible, por lo que necesariamente $1_\Lambda = 1_\Gamma$, por lo que contiene al elmento identidad.
$\Leftarrow$] El regreso siempre se da, pues. Ahora sean $x, y \in \Gamma$ tales que $xy = 0$, pero al ser $x, y \in \Lambda$ y como es dominio entero entonces $x = 0$ o $y = 0$ por lo que es dominio entero.

■

Problema 1.11. En la notación de la Definición 1.12 pruebe que, si g existe, esta determinada en forma única, el cual es denotado con f^{-1} y se llama inverso de f.

Demostración. – En efecto, supongamos que existe otra funcion $h : \Lambda' \to \Lambda$ tal que $h \circ f = 1_\Lambda$ y $f \circ h = 1_{\Lambda'}$ Entonces tendremos que

$$f \circ g = 1_{\Lambda'} = f \circ h \ \Rightarrow f \circ g = f \circ h$$

entonces componiendo del lado izquierdo

$$\Rightarrow g \circ (f \circ g) = g \circ (f \circ h) \quad \Rightarrow \quad (g \circ f) \circ g = (g \circ f) \circ h$$

pero como $g \circ f = 1_\Lambda$ entonces

$$\Rightarrow \quad 1_\Lambda \circ g = 1_\Lambda \circ h \quad \Rightarrow \quad g = h$$

por tanto, es única.

■

Problema 1.15. Pruebe que los inversos izquierdo y derecho de una unidad en un anillo con uno coinciden.

Demostración. – Sea $a \in A$ tal que tiene inverso derecho b e inverso izquierdo c, entonces

$$b = 1 \cdot b = (ca)b = c(ab) = c \cdot 1 = c$$

entonces $b = c$.

■

Algebra Moderna

Ejercicios Capitulo IV.2

Por: Alvarado Cabrera Lorenzo Antonio

Problema 2.2. Compruebe que el dominio entero $\mathbb{Z}$ no es un campo.

Demostración. – En efecto, pues 2 no tiene inverso multiplicativo, ya que si existiera $n \in \mathbb{Z}$ tal que $2n = 1$ por la paridad.

■

Problema 2.6. Demuestre que los inversos izquierdo y derecho de una unidad en un anillo con uno Λ coinciden, y que el conjunto de unidades es un grupo bajo la multiplicación, denotado Λ^*.

Demostración. – Lo primero que se pide ya fue probado en el ejercicio 1.15 Capitulo IV.1. Por otro lado,

- La operación es cerrada, pues dados $a, b \in \Lambda^*$ tenemos que

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1$$

por lo que $ab \in \Lambda^*$.
- La operación es asociativa heredada por el anillo.
- Existen inversos, dada la definición del propio grupo.
- El neutro es el mismo que el anillo.

Por tanto, es un grupo.

■

Algebra Moderna

Ejercicios Capitulo IV.3

Por: Alvarado Cabrera Lorenzo Antonio

Problema 3.2.

(i) Sea Λ un anillo con uno. Compruebe que el conjunto $\Pi = \{\varphi : \mathbb{Z}_{>0} \to \Lambda : \varphi(n) = 0\}$ para casi toda $n \in \mathbb{Z}_{>0}$ posee una estructura de anillo definiendo dos operaciones binarias mediante

$$\varphi + \xi : \ (\varphi + \xi)(n) = \varphi(n) + \xi(n)$$

$$\varphi\xi : \ (\varphi\xi)(n) = \sum_{j=0}^{n} \varphi(j)\xi(n-j)$$

(ii) Para cada $x \in \Lambda$, definamos una función que depende de x denotada f_x mediante

$$f_x(n) = \begin{cases} x & \text{si } n = 0 \\ 0 & \text{e.o.c} \end{cases}$$

Así $f_x \in \Pi$ y la asignación dada por $x \to f_x$ define una función $f : \Lambda \to \Pi$. Compruebe que f es un monomorfismo y que $f(1)$ es la identidad de Π.

(iii) En el Teorema 3.2 compruebe que: h es homomorfismo, $h(t) = y$, $h \circ f = g$ y que h es única. Establezca que cualquier elemento de Π puede escribirse de manera única como

$$\varphi = \lambda_0 + \lambda_1 t^1 + \cdots + \lambda_n t^n$$

donde $\lambda_i \in \Lambda$ y $\lambda_i = \varphi(n)$ para $i = 0, 1, .., n$.

Demostración. –

(i) Probaremos que es un anillo.

- Las operaciones son asociativas. Sean $\varphi, \gamma, \mu \in \Pi$ entonces (usando el hecho de que Λ es anillo con 1),

$$\begin{aligned}(\varphi + (\gamma + \mu))(n) &= \varphi(n) + (\gamma + \mu)(n) = \varphi(n) + \gamma(n) + \mu(n) \underset{\Lambda \text{ anillo}}{=} (\varphi(n) + \gamma(n)) + \mu(n) \\ &= (\varphi + \gamma)(n) + \mu(n) = ((\varphi + \gamma) + \mu)(n)\end{aligned}$$

$$\begin{aligned}(\varphi(\gamma\mu))(n) &= \sum_{j=0}^{n} \varphi(j)(\gamma\mu)(n-j) = \sum_{j+i=n} \varphi(j)(\gamma\mu)(i) = \sum_{j+i=n} \varphi(j) \sum_{k+l=i} \gamma(k)\mu(l) \\ &= \sum_{j+i=n} \sum_{k+l=i} \varphi(j)\gamma(k)\mu(l) = \sum_{j+k+l=n} \varphi(j)\gamma(k)\mu(l) = \sum_{j+k+l=n} \varphi(k)\gamma(l)\mu(i) \\ &= \sum_{j+i=n} \left(\sum_{k+l=i} \varphi(k)\gamma(l)\right)\mu(i) = \sum_{j+i=n} (\varphi\gamma)(i)\mu(i) = ((\varphi\gamma)\mu)(n)\end{aligned}$$

- Las operaciones tienen neutro. Siendo la función idénticamente cero para la suma y la función $1(n) = 1$ si $n = 0$ y cero en todo lo demás.

$$(\varphi + 0)(n) = \varphi(n) + 0(n) = \varphi(n)$$

$$(\varphi \cdot 1)(n) = \sum_{j=0}^{n} \varphi(j)1(n-j) = 0 + \cdots + 0 + \varphi(n)1(0) = \varphi(n)$$

- La suma tiene elemento inverso. Siendo $(-\varphi)(n) := -\varphi(n)$.

- La operación suma es conmutativa, heredado por Λ.

- Las operaciones distribuyen. Sean $\varphi, \gamma, \mu \in \Pi$, entonces

$$(\varphi(\gamma+\mu))(n) = \sum_{j=0}^{n} \varphi(j)(\gamma+\mu)(n-j) = \sum_{j=0}^{n} \varphi(j)\big[\gamma(n-j) + \mu(n-j)\big]$$
$$\underset{\Lambda \text{ anillo}}{=} \sum_{j=0}^{n} \big[\varphi(j)\gamma(n-j) + \varphi(j)\mu(n-j)\big] = \sum_{j=0}^{n} \varphi(j)\gamma(n-j) + \sum_{j=0}^{n} \varphi(j)\mu(n-j)$$
$$= (\varphi\gamma)(n) + (\varphi\mu)(n)$$

Por lo tanto, es un anillo. ■

(ii) En efecto es monomorfismo.

- Sean $x, y \in \Lambda$ entonces $f(x+y) = f_{x+y}$ donde $f_{x+y} : \mathbb{Z}_{\geq 0} \to \Lambda$ es tal que

$$f_{x+y}(n) = \begin{cases} x+y & \text{si } n = 0 \\ 0 & \text{e.o.c} \end{cases} = \begin{cases} x & \text{si } n = 0 \\ 0 & \text{e.o.c} \end{cases} + \begin{cases} y & \text{si } n = 0 \\ 0 & \text{e.o.c} \end{cases} = f_x(n) + f_y(n)$$

por lo que $f(x+y) = f_{x+y} = f_x + f_y = f(x) + f(y)$, por lo que es homeomorfismo. De forma equivalente para el producto.

- Es inyectivo, pues si consideramos $x, y \in \Lambda$ tales que $f(x) = f(y) \Rightarrow f_x = f_y$ como funciones por lo que son iguales en cada entero, por lo que en particular $f_x(0) = f_y(0) \Rightarrow x = y$, por tanto, es monomorfismo.

- Por lo que hicimos en el inciso anterior, tenemos que justamente la función $f(1)$ es la identidad.

(iii) Tenemos los siguientes.

- Sean $\varphi, \gamma \in \Pi$, entonces

$$h(\varphi + \gamma) = g((\varphi+\gamma)(0)) + \sum_{n=1}^{\infty} g((\varphi+\gamma)(n))y^n$$

$$= g(\varphi(0) + \gamma(0)) + \sum_{n=1}^{\infty} g(\varphi(n) + \gamma(n))y^n$$

$$\underset{\text{g homomor}}{=} g(\varphi(0)) + g(\gamma(0)) + \sum_{n=1}^{\infty} g(\varphi(n))y^n + \sum_{n=1}^{\infty} g(\gamma(n))y^n$$

$$h(\varphi) + h(\gamma)$$

Por tanto, es homomorfismo.

- Se tiene

$$h(t) = g(t(0)) + \sum_{n=1}^{\infty} g(t(n))y^n = g(0) + g(t(1))y + \sum_{n=2}^{\infty} g(t(n))y^n = g(0) + g(1)y + \sum_{n=2}^{\infty} g(0)y^n$$

$$= 0 + 1y + \sum_{n=2}^{\infty} 0y^n = y$$

- Se tiene que para $x \in \Lambda$

$$(h \circ f)(x) = h(f(x)) = h(f_x) = g(f_x(0)) + \sum_{n=1}^{\infty} g(f(n))y^n = g(x) + \sum_{n=1}^{\infty} g(0)y^n = g(x)$$

por lo que $h \circ f = g$.

■

Problema 3.6.
(i) Defina $h' : \Xi \to \Delta'$ mediante $h'(a,b) = g(a)/g(b)$. Compruebe que h' esta bien definida.
(ii) Por la parte (i) $h'(a,b)$ depende solamente de la clase de equivalencia a/b, por lo tanto, defina una función $h : K \to \Delta'$. Pruebe que h es un homomorfismo tal que $h \circ f = g$

Demostración. –
(i) Esto es inmediato de hecho de que Δ' es un anillo con división. Por tanto, todo elemento tiene inverso.
(ii) Definimos $h : K \to \Delta'$ dada por $h(a/b) = g(a)/g(b)$, entonces para $a/b, c/d \in K$

$$h(a/b + c/d) = h((ad + bc)/b\,d) = g(ad + bc)/g(bd) = (g(ad) + g(bc))/g(b)g(d)$$
$$= (g(a)g(d) + g(b)g(c))/g(b)g(d) = g(a)/g(b) + g(c)/g(d) = h(a/b) + h(c/d)$$

$$h(a/b \cdot c/d) = h(ac/b\,d) = g(ac)/g(bd) = g(a)g(c)/g(b)g(d)$$
$$= g(a)/g(b) \cdot g(c)/g(d) = h(a/b)h(c/d)$$

Por lo que es homomorfismo. Y además

$$h(f(x)) = h(x/1) = g(x)/g(1) = g(x)/1 = g(x)$$

por lo que $h \circ f = g$.

■

Problema 3.10. Pruebe que

(i) $\mathbb{Z}$ es un dominio de ideales principales.

(ii) Demuestre que si K es un campo, el anillo de polinomios $K[t]$ es un dominio de ideales principales.

(iii) Pruebe que si Δ es un dominio entero finito, entonces $\Delta[t]$ es un dominio entero.

Demostración. –

(i) Consideremos un ideal I de $\mathbb{Z}$. Entonces descartando el ideal trivial supongamos que $I \neq \{0\}$ con ello debe de existir un elemento mínimo en I, digamos $x \in I$. Veamos que entonces I esta generado por este elemento.
Para esto una contención es inmediata, para la otra sea $y \in I$, por el algoritmo de Euclides sabemos que existen $q, r \in \mathbb{Z}$ con $0 \leq r < x$ tal que $y = xq + r$, entonces $r = y - xq \in I$, pues $x, y \in I$ sin embargo si pasara que $r \neq 0$ entonces tendríamos un elemento mas chico que x lo cual no es posible, por lo que necesariamente $r = 0$, de modo que $y = xq$ por lo que $y \in \langle x \rangle$, entonces $I = \langle x \rangle$ asi todo ideal de los enteros es principal, por lo que es un dominio de ideales principales.

(ii) De forma similar consideremos un ideal I de $K[t]$. Entonces descartando el ideal trivial supongamos que $I \neq \{0\}$ con ello debe de existir un polinomio en I con grado minimo, digamos $f \in I$. Veamos que entonces I esta generado por este elemento.
Para esto una contención es inmediata, para la otra sea $g \in I$, por el algoritmo de Euclides para polinomios sabemos que existen $q, r \in K[t]$ con $0 \leq \deg(r) < \deg(g)$ tal que $g = fq + r$, entonces $r = g - fq \in I$, pues $f, g \in I$ sin embargo si pasara que $r \neq 0$ entonces tendríamos un polinomio de grado menor a f lo cual no es posible, por lo que necesariamente $r = 0$, de modo que $g = fq$ por lo que $g \in \langle f \rangle$, entonces $I = \langle f \rangle$, por lo que es un dominio de ideales principales.

(iii) Sean $f, g \in \Delta[t]$ no cero tales que $f(t)g(t) = 0$, entonces si llamamos a, b los coeficientes principales de f y g, entonces tendríamos que en el producto cera el polinomio cero si y solo si $ab = 0$, pero esto como Δ es dominio entero esto solo pasa si $a = 0$ o $b = 0$, en cuyo caso necesariamente tendremos que $f(t) = 0$ o $g(t) = 0$.

■

Problema 3.14. Sea K un campo. Pruebe que un polinomio en $K[t]$ es irreducible si, y solo si, el ideal generado por el es máximo.

Demostración. – Como K es campo, entonces $K[t]$ es dominio de ideales principales.
$\Leftarrow]$ Sea $r \in K[t]$ y supongamos que $\langle r \rangle$ es maximal. Sean $a, b \in K[t]$ tales que $ab = r$, luego $\langle r \rangle = \langle ab \rangle \subseteq \langle a \rangle$. Entonces $\langle a \rangle = \langle r \rangle$ o $\langle a \rangle = K[t]$. EN el primer caso tendríamos que entonces $r \mid a$ y $a \mid r$. Por lo que debe de existir $u \in D$ unidad tal que $au = r$, pero $ab = r$, y entonces por la regla de cancelación $b = u$, luego b es unidad y r irreducible.

$\Rightarrow]$ Sea $r \in K[t]$ irreducible, y sea $J \subset K[t]$ ideal bilateral tal que $\langle r \rangle \subseteq J$. Por ser un dominio de ideales principales existe $s \in K[t]$ tal que $J = \langle s \rangle$. Por lo que $\langle r \rangle \subseteq \langle s \rangle$, lo que implica que $s \mid r$, es decir, existe $t \in K[t]$ tal que $st = r$. Por ser r irreducible entonces s o t son unidades. Si t es unidad, entonces $r \mid s$, es decir $\langle s \rangle \subseteq \langle r \rangle$, lo que prueba que $\langle r \rangle = J$.

■

Problema 3.18. Pruebe que
(i) $(t - a)$ es un factor de un polinomio $f(t) \in K[t]$ si, y solo si, a es una raíz de $f(t)$.
(ii) Pruebe que cualquier polinomio no trivial de grado m en $K[t]$ tiene a lo mas m raíces en K

Demostración. –
(i) Supongamos que a es una raíz de $f(t)$. Como $p(t) = t - a$ es tal que $p(a) = 0$ y es monico, entonces $t - a \mid p(t)$. Por otra parte, si $t - a \mid f(t)$, entonces existe $q(t) \in K[t]$ tal que $f(t) = q(t)(t - a)$, de donde $0 = 0q(a) = (a - a)q(a) = f(a)$, entonces a es raíz de f.

(ii) Es inmediato del anterior, pues si suponemos que $f(t)$ tiene una raíz, entonces $f(t) = (t - a)q(t)$ donde $grad(q) < grad(f)$, y lo mismo podemos suponer para q de forma sucesiva, donde este procedimiento no puede pasar de m pasos pues $grad(f) = m$, siendo entonces que tendrá a lo más m raíces.

■