

Universidad Nacional Autónoma de México Facultad de Ciencias

Álgebra superior 2

Tarea examen 1 Elías López Rivera

elias.lopezr@ciencias.unam.mx

Fecha: 27/10/2024



Lema 1

Sea R un anillo conmutativo con 1 se cumple que $-(ac) = a(-c) \ \forall \ a, c \in R$

Demostración.

Sean $a, c \in R$, notemos que por la distributividad del producto sobre la suma:

$$ac + a(-c) = a(c + (-c))$$

Como $(-c) \in R$ es inverso para c:

$$ac + a(-c) = a(c + (-c)) = a(0)$$

Como en cualquier anillo conmutativo con 1 se cumple que a(0) = 0, para todo $a \in R$:

$$ac + a(-c) = a(c + (-c)) = a(0) = 0$$

Como en un anillo conmutativo con 1 los inversos son únicos se tiene que necesariamente -(ac) = a(-c)

A partir de los naturales \mathbb{N} define $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ donde $(n,m)\sim (k,l)$ si y solo si n+l=m+k. Induce las operaciones de suma y producto en \mathbb{Z} utilizando aquellas de \mathbb{N} , demuestra que están bien definidas (en el sentido de que no dependen de los representantes) y demuestra que el resultado es un anillo conmutativo con 1 que contiene a \mathbb{N}

Definimos $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$:

$$[(n,m)] \oplus [(r,s)] = [(n+r,m+s)]$$

Donde + es la suma definida en \mathbb{N} .

Definimos $\odot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$:

$$[(n,m)] \odot [(r,s)] = [(nr+ms, mr+ns)]$$

donde + es la suma definida en \mathbb{N} y \cdot es el producto en \mathbb{N}

Veamos que \oplus no depende de los representantes:

Demostración.

Sean [(n, m)], [(r, s)], [(l, k)], [(f, g)], tal que [(n, m)] = [(l, k)] y [(r, s)] = [(f, g)], tenemos entonces que:

$$(n,m) \sim (l,k) \implies n+k=m+l$$

$$(r,s) \sim (f,g) \implies r+g=s+f$$

Por tanto usando que + en \mathbb{N} es asociativa y conmutativa (ignorando paréntesis):

$$n + k + r + q = m + l + s + f$$

Por tanto tenemos que:

$$[(n,m)] \oplus [(r,s)] = (n+r,m+s) \sim (l+f,k+q) = [(l,k)] \oplus [(f,q)]$$

Como ambos elementos estás relacionados sus clases de equivalencias son iguales:

$$[(n,m)] \oplus [(r,s)] = [(l,k)] \oplus [(f,g)]$$

Ahora veamos que ⊙ no depende de los representantes:

Demostración.

Sean [(n,m)], [(r,s)], [(l,k)], [(f,g)], tal que [(n,m)] = [(l,k)] y [(r,s)] = [(f,g)], tenemos entonces que:

$$(n,m) \sim (l,k) \implies n+k=m+l$$

$$(r,s) \sim (f,g) \implies r+g=s+f$$

Por tanto tenemos que:

$$r(n+k) + s(m+l) + l(r+q) + k(s+f) = r(m+l) + s(n+k) + l(s+f) + k(r+q)$$

Utilizando la distributividad del producto sobre la suma de \mathbb{N} asi como sus respectivas conmutatividades obtenemos:

$$rn + rk + sm + sl + lr + lg + ks + kf = mr + lr + ns + ks + sl + fl + rk + gk$$

Como las leves de cancelación son validas para la suma en N:

$$nr + ms + gl + kf = mr + ns + lf + kg$$

Por tanto tenemos que:

$$[(n,m)] \odot [(r,s)] = (nr + ms, mr + ns) \sim (lf + kg, gl + kf) = [(l,k)] \odot [(f,g)]$$

omo ambos elementos estás relacionados sus clases de equivalencias son iguales:

$$[(n,m)]\odot[(r,s)]=[(l,k)]\odot[(f,g)]$$

Demostraremos que $(\mathbb{Z}, \oplus, \odot)$ es un anillo conmutativo con 1

i) (\mathbb{Z}, \oplus) es grupo abeliano:

• a) Conmutatividad

$$\forall [(n,m)], [(r,s)] \in \mathbb{Z} : ([(n,m)] \oplus [(r,s)] = [(r,s)] \oplus [(n,m)])$$

Página 3 de 15

Demostración.

Sean $[(n,m)],[(r,s)] \in \mathbb{Z}$, tenemos que:

$$[(n,m)] \oplus [(r,s)] = [(n+r,m+s)]$$

Como + es conmutativa en \mathbb{N} :

$$[(n,m)] \oplus [(r,s)] = [(n+r,m+s)] = [(r+n,s+m)] = [(r,s)] \oplus [(n,m)]$$

• b) Asociatividad

$$\forall \ [(n,m)], [(r,s)], [(t,u)] \in \mathbb{Z} : (\ [(n,m)] \oplus (\ [(r,s) \oplus [(t,u)]]\) = (\ [(n,m)] \oplus [(r,s)]\) \oplus [(t,u)]\)$$

Demostración.

Sean $[(n,m)],[(r,s)],[(t,u)]\in\mathbb{Z},$ tenemos que:

$$[(n,m)] \oplus ([(r,s) \oplus [(t,u)]]) = [(n+(r+t),m+(s+u))]$$

Debido a que + es asociativa en \mathbb{N} :

$$[(n,m)] \oplus ([(r,s) \oplus [(t,u)]]) = [(n+(r+t),m+(s+u))]$$

$$=\left[\left((n+r)+t,(m+s)+u\right)\right]=\left(\left.\left[(n,m)\right]\oplus\left[(r,s)\right]\right)\oplus\left[(t,u)\right]$$

• c) Existencia de neutro

$$\exists \ [(0,0)] \in \mathbb{Z} : (\forall \ [(n,m)] \in \mathbb{Z} : [(n,m)] \oplus [(0,0)] = [(n,m)])$$

Demostración.

Sea $[(n, m)] \in \mathbb{Z}$, veamos que:

$$[(n,m)] \oplus [(0,0)] = [(n+0,m+0)]$$

Como $0 \in \mathbb{N}$ es neutro para + se tiene que:

$$[(n,m)] \oplus [(0,0)] = [(n+0,m+0)] = [(n,m)]$$

• d) Existencia de inversos

$$\forall [(n,m)] \in \mathbb{Z}(\exists [(m,n)] \in \mathbb{Z} : [(m,n)] \oplus [(n,m)] = [(0,0)])$$

Demostración.

Sean $[(m, n)], [(n, m)] \in \mathbb{Z}$, se cumple que:

$$[(n,m)] \oplus [(m,n)] = [(n+m,m+n)]$$

Por la conmutatividad de + en \mathbb{N} y que $0 \in \mathbb{N}$ es neutro para +

$$(n+m) + 0 = (m+n) + 0 \implies (n+m, m+n) \sim (0,0)$$

Como ambos elementos estan relacionados bajo la relación de equivalencia \sim , tenemos que sus clases de equivalencia son necesariamente iguales:

$$[(n+m, m+n)] = [(0,0)]$$

Por tanto:

$$[(n,m)] \oplus [(m,n)] = [(n+m,m+n)] = [(0,0)]$$

De \mathbf{a} , \mathbf{b} , \mathbf{c} , \mathbf{d}) se sigue que (\mathbb{Z} , \oplus) es un grupo abeliano.

ii) Demostraremos que (\mathbb{Z}, \odot) es un monoide conmutativo.

• a) Conmutatividad

$$\forall [(n,m)], [(r,s)] \in \mathbb{Z}([(n,m)] \odot [(r,s)] = [(r,s)] \odot [(n,m)])$$

Demostración.

Sean $[(n,m)], [(r,s)] \in \mathbb{Z}$ tenemos que:

$$[(n,m)]\odot[(r,s)]=[(nr+ms,mr+ns)]$$

Como el producto de \mathbb{N} y la suma de \mathbb{N} es conmutativo:

$$[(n,m)]\odot[(r,s)] = [(nr+ms, mr+ns)] = ([rn+sm, sn+rm]) = [(r,s)]\odot[(n,m)]$$

• b) Asociatividad

$$\forall \ [(n,m)], [(r,s)], [(t,u)] \in \mathbb{Z} : (\ [(n,m)] \odot (\ [(r,s) \odot [(t,u)]]\) = (\ [(n,m)] \odot [(r,s)]\) \odot [(t,u)]\)$$

Demostración.

$$[(n,m)] \odot (\,[(r,s)\odot[(t,u)]]\,) = [(n,m)] \odot [(rt+su,st+ru)] = [(n(rt+su)+m(st+ru),m(rt+su)+n(st+ru))]$$

Aplicando la distributividad del producto sobre la suma \mathbb{N} :

$$[(n,m)] \odot ([(r,s) \odot [(t,u)]]) = [(n(rt) + n(su) + m(st) + m(ru), m(rt) + m(su) + n(st) + n(ru))]$$

Aplicando la asociatividad del procuto de \mathbb{N}

$$[(n,m)] \odot ([(r,s) \odot [(t,u)]]) = [((nr)t + (ns)u + (ms)t + (mr)u, (mr)t + (ms)u + (ns)t) + (nr)u]$$

Aplicando de nuevo la distributividad del producto sobre la suma de $\mathbb N$

$$[(n,m)] \odot ([(r,s) \odot [(t,u)]]) = [(t(nr+ms) + u(ns+mr), t(mr+ns) + u(ms+nr)u+)]$$

$$= [(nr+ms, ns+mr)] \odot [(t,u)]$$

$$= ([(n,m)] \odot [(r,s)]) \odot [(t,u)])$$

• c) Existencia de neutro

$$\exists [1,0] \in \mathbb{Z}(\forall [(n,m)] \in \mathbb{Z} : [(n,m)] \odot [(0,1)] = [(n,m)])$$

Demostración.

Tomemos $[(n,m)] \in \mathbb{Z}$, tenemos que:

$$[(n,m)] \odot [(0,1)] = [(n0+m1,m0+n1)]$$

Como el producto en \mathbb{N} cumple que $n0 = 0 \ \forall n \in \mathbb{N}$ y 1 es neutro para el producto tenemos que:

$$[(n,m)] \odot [(0,1)] = [(n0+m1,m0+n1)] = [(0+m,0+n)]$$

Como 0 es neutro para + en \mathbb{N} finalmente:

$$[(n,m)] \odot [(0,1)] = [(n,m)]$$

De a), b), c) tenemos que (\mathbb{Z}, \odot) es un monoide conmutativo

iii) Demostraremos la distributividad de \odot sobre \oplus en \mathbb{Z} (solo lo haremos por la derecha pues tanto \odot como \oplus son conmutativas)

$$\forall [(n,m)], [(r,s)], [(l,t)] \in \mathbb{Z} : ([(n,m)] \odot ([(r,s)] \oplus [(l,t)]) = ([(n,m)] \odot [(r,s)]) \oplus ([(n,m)] \odot [(l,t)]))$$

Demostración.

Sean [(n,m)], [(r,s)], $[(l,t)] \in \mathbb{Z}$ se sigue que:

$$[(n,m)] \odot ([(r,s)] \oplus [(l,t)]) = [(n,m)] \odot [(r+l,s+t)] = [(n(r+l)+m(s+t),m(r+l)+n(s+t))]$$

Como el producto de \mathbb{N} se distribuye sobre su suma:

$$[(n,m)] \odot ([(r,s)] \oplus [(l,t)]) = [(nr+nl+ms+mt, mr+ml+ns+nt)]$$

Usando la conmutatividad del producto y de la suma en N:

$$[(n,m)] \odot ([(r,s)] \oplus [(l,t)]) = [(nr+ms,mr+ns)] \oplus [(nl+mt,ml+nt)] = ([(n,m)] \odot [(r,s)]) \oplus ([(n,m)] \odot [(l,t)])$$

De i), ii), iii) tenemos que $(\mathbb{Z}, \oplus, \odot)$ es un anillo conmutativo con 1

Ahora definimos la función $i: \mathbb{N} \to \mathbb{Z}$, de tal manera que i(n) = [(n,0)], si reestringimos i de la siguiente manera $i: \mathbb{N} \to i[\mathbb{N}] \subset \mathbb{Z}$, donde $i[\mathbb{N}]$ es la imagen de \mathbb{N} bajo i obtenemos una función suprayectiva, bastaria probar que i es inyectiva para argumentar la biyección entre \mathbb{N} y un subconjunto de \mathbb{Z} , lo que nos animaria a decir que \mathbb{N} esta contenido en \mathbb{Z} , procedemos a demostrarlo:

Demostración.

Sean $m, n \in \mathbb{N}$ tal que i(n) = i(m), se sigue que:

$$i(n) = [(n, 0)] = [(m, 0)] = i(m)$$

Como las clases son iguales los representantes necesariamente están relacionados:

$$(n,0) \sim (m,0) \implies n+0 = m+0$$

De nuevo como $0 \in \mathbb{N}$ es neutro para + se sigue que:

$$n = m$$

Por tanto i es suprayectiva

Problema 2

Demuestra que para todo elemento $[(n,m)] \in \mathbb{Z}$ se satisface exactamente una de las siguientes afirmaciones:

- Existe $c \in \mathbb{N}/\{0\}$ tal que [(n,m)] = [(c,0)]
- [(n,m)] = [(0,0)]
- Existe $c \in \mathbb{N}/\{0\}$ tal que [(n,m)] = [(0,c)]

Demostración.

Sean $n, m \in N$ por tricotomia tenemos tres casos:

- *m* < *n*
- n=m
- n < m
- i) Primero tomemos que n < m, por la definición del orden en N tenemos que:

$$\exists c \in \mathbb{N}/\{0\}: n = m + c$$

Usando que 0 es neutro para la suma definida en \mathbb{N} , tenemos que:

$$n + 0 = m + c$$

Y por la relación de equivalencia definida anteriormente:

$$n+0=m+c \implies (n,m) \sim (c,0)$$

Como estos dos elementos están relacionados sus clases de equivalencia son iguales necesariamente:

$$[(n,m)] = [(c,0)]$$

ii) Ahora tomemos que n=m, usando nuevamente que el 0 es neutro para la suma de \mathbb{N} :

$$n + 0 = m + 0$$

De nuevo por la relación de equivalencia definida anterioemente:

$$n + 0 = m + 0 \implies (n, m) \sim (0, 0)$$

Como estos dos elementos están relacionados sus clases de equivalencia son iguales necesariamente:

$$[(n,m)] = [(0,0)]$$

iii) Finalmente tomamos el caso m < n, por la definición del orden en $\mathbb N$ tenemos que:

$$\exists c \in \mathbb{N}/\{0\}: m = n + c$$

Usando que 0 es neutro para la suma definida en \mathbb{N} , tenemos que:

$$n+c=m+0$$

Y por la relación de equivalencia definida anteriormente:

$$n+c=m+0 \implies (n,m) \sim (0,c)$$

Como estos dos elementos están relacionados sus clases de equivalencia son iguales necesariamente:

$$[(n,m)] = [(0,c)]$$

Demuestra que un elemento u de un anillo conmutativo con 1 tiene a lo más un inverso multiplicativo

Demostración.

Sea $a \in R$ tal que existe $u \in R$ con a(u) = 1, demostraremos que si se tiene que a(u') = 1, necesariamente u' = u:

$$a(u) = 1 = a(u')$$

Como $a(u') \in R$ tenemos que existe $-a(u') \in R$, sumando este de ambos lados:

$$a(u) + (-au') = a(u') + (-au') = 0$$

Aplicando el lema 1 tenemos que -au' = a(-u') y la distributividad del producto sobre la suma:

$$a(u) + (-au') = a(u + (-u')) = 0$$

Multiplicando ambos lados por u:

$$u(a(u + (-u'))) = 0u$$

Usando el hecho de que 0u = 0 para todo $u \in R$, y la asociatividad del producto:

$$(ua)(u + (-u')) = 0$$

Usando la conmutatividad del producto y nuestra hipótesis:

$$(ua)(u + (-u')) = (au)(u + (-u')) = 1(u + (-u')) = 0$$

Como 1 es neutro para el producto:

$$u + (-u') = 0 = u' + (-u')$$

Como las leyes de cancelación son validas para la suma en un anillo conmutativo con 1 se concluye que:

$$u = u'$$

Demuestra: $\forall a, b \in \mathbb{Z} (a > 0 \land b > 0 \ a^2 > b^2 \implies a > b)$

Demostración.

Por proposición tenemos que segun la proposición $1 \, \forall \, a,b,c, \in \mathbb{Z} : (a < b \implies a+c < b+c)$, sea $-b^2 \in \mathbb{Z}$ el inverso aditivo de b^2 :

$$a^2 + (-b^2) > b^2 + (-b^2)$$

Por tanto:

$$a^2 - b^2 > 0$$

Luego tomemos (a + b)(a - b), aplicando la distributividad del producto sobre la suma

$$(a+b)(a-b) = (a(a+b) - b(a+b)) = a^2 + ab - b(a) - b(b)$$

Aplicando la conmutatividad y el lema 1:

$$(a + b)(a - b) = a^2 + ab - ab - b^2 = a^2 + b^2$$

Ahora por hipótesis $a>0 \land b>0$, por tanto a+b>0+a>0 esto por la proposición 1, luego tenemos que (a-b)>0, pues de otra manera por la proposición $2 \ \forall \ a,b \in \mathbb{Z}: (a>0 \land b<0 \implies ab<0)$ tendriamos que:

$$(a+b), (a-b) \in \mathbb{Z} : (a+b) > 0 \land (a-b) < 0 \implies a^2 - b^2 = (a+b)(a-b) < 0$$

Lo que contradice nuestra hipótesis, por tanto usando nuestra proposición 1 tenemos que:

$$a-b>0 \implies a-b+b>0+b \implies a>0$$

Demuestra que un dominio entero R se vale la ley de cancelación: $\forall a,b,c \in R (a \neq 0 \ ab = ac \implies b = c)$

Demostración.

Tomamos $a, b, c \in \mathbb{Z}$ tal que $a \neq 0$, tenemos que:

$$ab = ac$$

Como ac es un elemento del dominio entero R, entonces este tiene un único inverso $-(ac) \in R$, sumando por ambos lados tenemos que:

$$ab + (-ac) = ac + (-ac)$$

Como -(ac) se definio como el inverso bajo + de ac, se sigue que:

$$ab + (-ac) = 0$$

Como $ab, -(ac) \in R$, podemos aplicar el lema 1 y posteriormente la distribución del producto sobre la suma:

$$ab + (-ac) = ab + a(-c) = a(b + (-c)) = 0$$

Como R es dominio entero necesariamente a=0 o (b+(-c))=0, como por hipótesis $a\neq 0$, entonces (b+(-c))=0, por tanto sumando c a ambos lados de la igualdad:

$$b + (-c) + c = 0 + c \implies b + 0 = 0 + c \implies b = c$$

Demuestra que un elemento $\sum_{n=0}^{\infty} a_n x^n$ del anillo de series formales $\mathbb{Q}[[x]]$ con coeficientes en \mathbb{Q} es una unidad en $\mathbb{Q}[[x]]$ si y solo si $a_0 \neq 0$

$$\implies$$
) Si $\sum_{n=0}^{\infty} a_n x^n$ es una unidad en el anillo de series formales $\mathbb{Q}[[x]]$ con coeficientes en \mathbb{Q} , entonces $a_0 \neq 0$

Demostración.

Sea $\sum_{n=0}^{\infty} a_n x^n$ una unidad en $\mathbb{Q}[[x]]$ tenemos que se cumple:

$$\exists \sum_{n=0}^{n} b_n x^n \in \mathbb{Q}[[x]] : \sum_{n=0}^{\infty} a_n x^n \odot \sum_{n=0}^{\infty} b_n x^n = \bar{1}$$

Donde \odot es el producto definido en $\mathbb{Q}[[x]]$ y $\bar{1}$ es el neutro para este producto, por tanto aplicando la definición de este

$$\sum_{n=0}^{\infty} a_n x^n \odot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \sum_{k+l=n} a_n b_n x^n$$

Expandiendo esta serie de potencias y reescribiendo a $\bar{1}$ en su forma de serie de potencia:

$$\sum_{n=0}^{\infty} a_n x^n \odot \sum_{n=0}^{\infty} b_n x^n = a_0 b_0 + \sum_{n=1}^{\infty} \sum_{k+l=n}^{\infty} a_n b_n x^n = 1 + \sum_{n=0}^{\infty} 0 x^n$$

Como dos series de potencias son iguales si y solo si todos sus terminos son iguales:

$$a_0 b_0 = 1$$
 y $0 = \sum_{n=1}^{\infty} \sum_{k+l=n} a_n b_n x^n$

Por tanto a_0 es una unidad en \mathbb{Q} , lo que implica que es diferente de 0.

$$\Leftarrow$$
) Si $\sum_{n=0}^{\infty} a_n x^n$ es tal que $a_0 \neq 0$ entonces $\sum_{n=0}^{\infty} a_n x^n$ es unidad en $\mathbb{Q}[[x]]$

Demostración.

Como $a_n \neq 0$ entonces a_n es una unidad en \mathbb{Q} , por tanto construimos $\sum_{n=0}^{\infty} b_n x^n$, tal que:

$$\sum_{n=0}^{\infty} a_n x^n \odot \sum_{n=0}^{\infty} b_n x^n = \bar{1}$$

De donde se obtiene que:

$$a_0b_0 + \sum_{n=1}^{\infty} \sum_{l+k=n} a_l b_k x^n = 1 + \sum_{n=1}^{\infty} 0 x^n$$

Que es equivalente a:

$$a_0b_0 = 1 \quad \forall n \in \mathbb{N} \left(\sum_{l+k=n} a_l b_k = 0 \right)$$

De aqui se sigue inmediatamente que $b_0 = a_0^{-1}$ donde a_0^{-1} es el inverso multiplicativo de a_0 , ahora para obtener b_{n+1} con $n \ge 1$ proponemos un proceso recursivo, supongamos que para $0 \le r \le n$, tenemos calculados los valores b_r , para obtener b_{n+1} proponemos lo siguiente:

$$\sum_{k+l=n+1} a_k b_l = \sum_{k=0}^{n+1} a_{n+1-k} b_k = 0$$

Esta igualdad es valida ya que el producto es conmutativo en \mathbb{Q} , por tanto reescribiendo:

$$a_0 b_{n+1} + \sum_{k=0}^{n} a_{n+1-k} b_k = 0$$

Como $\sum_{k=0}^{n} a_{n+1-k}b_k \in \mathbb{Q}$ y este es un anillo afirmamos la existencia de $-\sum_{k=0}^{n} a_{n+1-k}b_k \in \mathbb{Q}$ por tanto como a_0^{-1} también existe proponemos que:

$$b_{n+1} = a_0^{-1} \left(-\sum_{k=0}^n a_{n+1-k} b_k \right)$$

Vemos que todos los terminos de esta suma son conocidas pues conocemos todos los b_r con $0 \le r \le n$, veamos que:

$$a_0 \left(a_0^{-1} \left(-\sum_{k=0}^n a_{n+1-k} b_k \right) \right) + \sum_{k=0}^n a_{n+1-k} b_k$$

Aplicando la asociatividad del producto y la propiedad del neutro multiplicativo en Q:

$$(a_0 a_0^{-1}) \left(-\sum_{k=0}^n a_{n+1-k} b_k \right) + \sum_{k=0}^n a_{n+1-k} b_k = -\sum_{k=0}^n a_{n+1-k} b_k + \sum_{k=0}^n a_{n+1-k} b_k = 0$$

Por tanto construimos la serie:

$$b_0 + a_0^{-1} \left(-\sum_{k=0}^{0} a_{1-k} b_k \right) x + a_0^{-1} \left(-\sum_{k=0}^{1} a_{2-k} b_k \right) x^2 + \dots + \left(\sum_{k=0}^{n} a_{n+1-k} b_k \right) x^{n+1} + \dots$$

Que es el inverso para $\sum_{i=0}^{\infty}\,a_n\,x^n$