Universidad Nacional Autónoma de México
Facultad de Ciencias

MATEMÁTICAS

Algebra Moderna II

2da lista de ejercicios

Por: Lorenzo Antonio Alvarado Cabrera

---

1. POLINOMIOS

Problema 1.1. –

Demuestra el **Teorema 2.1.10**. Es decir,

Sean A, B anillos y $\phi : A \to B$ morfismo de anillos, entonces existe $\hat{\phi} : A[x] \to B[x]$ morfismo de anillos, dado por

$$\hat{\phi}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \phi(a_i) x^i.$$

Demostración: Veamos que la función efectivamente es un morfismo.

- Esta bien definida, pues para cada $a_i \in A$ se tiene que $\Phi(a_i) \in B$ y entonces $\sum \Phi(a_i)x^i \in B[x]$

- Sean $p(x), q(x) \in A[x]$ con $p(x) = \sum_{i=0}^{n} a_i x^i$ y $q(x) = \sum_{i=0}^{n} b_i x^i$, entonces

$$\hat{\Phi}(p(x)+q(x)) = \hat{\Phi}(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i) \underset{def}{=} \hat{\Phi}(\sum_{i=0}^{n} (a_i + b_i) x^i) \underset{def}{=} \sum_{i=0}^{n} \Phi(a_i + b_i) x^i$$
$$\underset{\Phi \text{ morfismo}}{=} \sum_{i=0}^{n} [\Phi(a_i) + \Phi(b_i)] x^i = \sum_{i=0}^{n} [\Phi(a_i)x^i + \Phi(b_i)x^i] = \sum_{i=0}^{n} \Phi(a_i)x^i + \sum_{i=0}^{n} \Phi(b_i)x^i$$
$$= \hat{\Phi}(p(x)) + \hat{\Phi}(q(x))$$

por lo tanto, $\hat{\Phi}(p(x)+q(x)) = \hat{\Phi}(p(x)) + \hat{\Phi}(q(x))$.

- Sean $p(x), q(x) \in A[x]$ con $p(x) = \sum_{i=0}^{n} a_i x^i$ y $q(x) = \sum_{i=0}^{n} b_i x^i$, entonces

$$\hat{\Phi}(p(x)q(x)) = \hat{\Phi}(\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{n} b_i x^i) \underset{def}{=} \hat{\Phi}(\sum_{i=0}^{n} (c_i) x^i) \underset{def}{=} \sum_{i=0}^{n} \Phi(c_i) x^i \underset{def}{=} \sum_{i=0}^{n} \Phi(\sum_{k+j=i} a_k b_j) x^i$$

$$\underset{\Phi \text{ morfismo}}{=} \sum_{i=0}^{n} [\sum_{k+j=i} \Phi(a_k b_j)] x^i \underset{\text{morfismo}}{=} \sum_{i=0}^{n} [\sum_{k+j=i} \Phi(a_k)\Phi(b_j)] x^i = \sum_{i=0}^{n} \Phi(a_i) x^i \sum_{i=0}^{n} \Phi(b_i) x^i$$

$$= \hat{\Phi}(p(x))\hat{\Phi}(q(x))$$

por lo tanto, $\hat{\Phi}(p(x)q(x)) = \hat{\Phi}(p(x))\hat{\Phi}(q(x))$.

Por todo lo anterior concluimos que $\hat{\Phi}$ es morfismo de anillos.

■

Problema 1.2. –

Demuestra el **Lema 2.1.11**. Es decir,

Sean R un anillo conmutativo unitario y $f(x)$, $g(x)$ polinomios no cero en $R[x]$. Entonces

a) Si $f(x)g(x)$ tiene grado, entonces

$$\text{grad}(f(x)g(x)) \leq \text{grad}(f(x)) + \text{grad}(g(x)).$$

b) Si $f(x) + g(x)$ tiene grado, entonces

$$\text{grad}(f(x) + g(x)) \leq \text{máx}\{\text{grad}(f(x)), \text{grad}(g(x))\}.$$

Demostración:

a) Consideremos $f, g \in R[x]$ con $f := (a_0, a_1, ..., a_n, 0, ...)$ y $g := (b_0, b_1, ..., b_m, 0, ...)$, entonces tenemos que $grad(f) = n$ y $grad(g) = m$ *PD* $grad(f \cdot g) \leq n + m$ *PD* $\forall k > m + n$ se tiene que $(fg)(k) = 0$.

Sabemos que para cada $k > m + n$ se tiene que $(fg)(k) = \sum_{i+j=k} f(i)g(j)$ y notemos que si $i > n$, tendremos que entonces $f(i) = 0$ pues $grad(f) = n$ y de forma similar si $i \leq n$ entonces $j = k - i \geq k - n > m + n - n = m$ con lo que $g(j) = 0$ pues $grad(g) = m$ $\therefore$ $\sum_{i+j=k} f(i)g(j) = 0$ $\Rightarrow$ $(fg)(k) = 0$ por lo que a partir de k hay puros ceros.

Sin embargo, dado que $(fg)(m + n) = \sum_{i+j=n+m} f(i)g(j) = f(n)g(m)$ podría pasar que $f(n)g(m) = 0$ pues $R[x]$ es un anillo cualquiera, por lo que concluimos $grad(fg) \leq m + n = grad(f) + grad(g)$.

■

b) Consideremos $f, g \in R[x]$ con $f := (a_0, a_1, ..., a_n, 0, ...)$ y $g := (b_0, b_1, ..., b_m, 0, ...)$, entonces tenemos que $grad(f) = n$ y $grad(g) = m$ *PD* $grad(f + g) \leq \max\{n, m\}$ *PD* $grad(f + g) \leq m$ y $grad(f + g) \leq n$.

Sabemos que para cada $k > m$ se tiene que $(f+g)(k) = f(k) + g(k)$ pero como $grad(g) = m$ entonces $g(k) = 0$ por lo que $(f+g)(k) = f(k)$, con lo que $grad(f+g) \leq grad(f) = n$.
Análogamente si $k > n$ se tiene que $(f+g)(k) = f(k) + g(k)$ pero como $grad(f) = n$ entonces $f(k) = 0$ por lo que $(f+g)(k) = g(k)$, con lo que $grad(f+g) \leq grad(g) = m$.

De estos dos casos concluimos que $grad(f+g) \leq m$ y $grad(f+g) \leq n$ por lo que $grad(f+g) \leq \max\{n, m\} = \max\{grad(f), grad(g)\}$.

■

2. DOMINIOS ENTEROS

Problema 2.1. –

Demuestra el otro caso del **Teorema 2.2.5**. Es decir,

Sea R un anillo. Entonces, R es un anillo sin divisores derechos de cero si, y solamente si, satisface la ley de cancelación derecha para la multiplicación.

Demostración:

$\Rightarrow]$ Sea $a \in R - \{0\}$ y $b, c \in R$ tal que $ba = ca \Rightarrow ba - ca = 0 \Rightarrow (b-c)a = 0$ pero a no es divisor derecho del cero $\Rightarrow b - c = 0 \Rightarrow b = c$ por lo que se cumple la ley de cancelación.

$\Leftarrow]$ Sean $a \in R - \{0\}$ y $b \in R$ tal que $ba = 0$. Como $ba = 0 = 0 \cdot a$ y se cumple la ley de cancelación, se tiene que $0 = b$, por lo que no hay ningún divisor derecho de cero.

■

Problema 2.2. –

a) Demuestra la **Proposición 2.2.16**. Es decir,
Sean D un dominio entero y $f(x)$, $g(x)$ polinomios no cero en $D[x]$. Entonces

$$\operatorname{grad}(f(x)g(x)) = \operatorname{grad}(f(x)) + \operatorname{grad}(g(x)).$$

b) Presenta un ejemplo de R un anillo conmutativo unitario y $f(x)$, $g(x)$ polinomios en $R[x]$, tales que

$$\operatorname{grad}(f(x)g(x)) < \operatorname{grad}(f(x)) + \operatorname{grad}(g(x)).$$

Demostración:

$a]$Sea $n = \operatorname{grad}(f(x))$ y $m = \operatorname{grad}(g(x))$, entonces tenemos que $\forall k > n + m$

$$(fg)(k) = \sum_{i=1}^{k} f(i)g(k-i) = \sum_{i=1}^{n} f(i)g(k-i) + \sum_{i=n+1}^{k} f(i)g(k-i)$$

pero para la primera suma, como $1 \leq i \leq n$ y $k > n+m \Rightarrow k-i > m$, por lo que $g(k-i) = 0$, análogamente para la segunda suma, como $n+1 \leq i \leq k \Rightarrow i > n$, por lo que $f(i) = 0$, entonces, $(fg)(k) = 0 \quad \forall k > m+n$.

Solo vasta ver que $(fg)(n+m) \neq 0$, en efecto, tenemos que

$$(fg)(n+m) = \sum_{i=1}^{n+m} f(i)g(k-i) = \sum_{i=1}^{n-1} f(i)g(n+m-i) + f(n)g(m) + \sum_{i=n+1}^{n+m} f(i)g(n+m-i)$$

y nuevamente para la primera suma, como $1 \leq i \leq n-1 \Rightarrow n+m-i \geq m+1$, por lo que $g(n+m-i) = 0$, análogamente para la segunda suma, $i \geq n+1$, por lo que $f(i) = 0$, entonces, $(fg)(n+m) = f(n)g(m)$ y dado que D es dominio entero, dado que f y g no son el polinomio cero tendremos que $f(n) \neq 0$ y $g(m) \neq 0 \Rightarrow f(n)g(m) \neq 0$, lo que queríamos demostrar, por lo que obtenemos que

$$\text{grad}(fg) = n+m = \text{grad}(f) + \text{grad}(f)$$

$\blacksquare$

b]Sean $\overline{1} + \overline{2}x + \overline{3}x^2,\ \overline{1} + \overline{2}x^2 \in \mathbb{Z}_6[x]$, tendremos que el ultimo factor de su producto será $\overline{2} \cdot \overline{3}x^2 = \overline{6}x^2 = \overline{0}x^2 = \overline{0}$, por lo que el grado del producto será menor a 4, que es la suma de los grados de los polinomios.

$\blacksquare$

3. IDEALES PRINCIPALES Y DIVISIVILIDAD

Problema 3.1. –

Demuestra el **Lema 2.3.3**, Es decir,

Sean R un anillo conmutativo y $a, b, c \in R$.

a) La divisibilidad es transitiva. Es decir, si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

b) Si $a \mid b$ y $a \mid c$ entonces $a \mid b+c$ y $a \mid b-c$.

c) Si $a \mid b$ entonces $a \mid bc$.

Demostración:

a]Sean $a, b, c \in R$ tales que $a \mid b$ y $b \mid c$ entonces $\exists d, e \in R$ tales que $b = da$ y $c = eb$, por lo que $c = e(da) = (ed)a$, es decir, $a \mid c$.

$\blacksquare$

b] Sean $a, b, c \in R$ tales que $a \mid b$ y $b \mid c$ entonces $\exists d, e \in R$ tales que $b = da$ y $c = eb$, por lo que

- $b+c=da+eb=da+eda=(d+ed)a$, es decir, $a \mid b+c$
- $b-c=da-eb=da-eda=(d-ed)a$, es decir, $a \mid b-c$

■

c] Sean $a,b,c \in R$ tales que $a \mid b$ entonces $\exists d \in R$ tales que $b=da$, por lo que $bc=dac=(dc)a$, es decir, $a \mid bc$ (esta última se da pues es anillo conmutativo)

■

4. DOMINIOS M.C.D

Problema 4.1. –

Demuestra la **Proposición 2.4.3**. Es decir,

Sea R un anillo conmutativo unitario, $a,b \in R$ y $u \in R$ unidad. Si $d=(a,b)$ entonces $du=(a,d)$, es decir, si d es el mcm de a y b, entonces cualquier asociado de d también lo es.

Demostración: En efecto, sea $d=(a,b)$ y veamos que du también es máximo común divisor. Como $d=(a,b)$ tenemos que $d \mid a$ y $d \mid b$ entonces $\exists c,e \in R$ tales que $a=cd$ y $b=ed$ por lo que $a=cu^{-1}ud$ y $b=eu^{-1}ud \Rightarrow a=(cu^{-1})ud$ y $b=(eu^{-1})ud$ entonces $du \mid a$ y $du \mid b$ (por conmutativad). Ahora sea $q \in R$ tal que $q \mid a$ y $q \mid b$, entonces como $d=(a,b)$ tendremos que $q \mid d$ por lo que por el *problema 3.1* $q \mid du \therefore du=(a,b)$.

■

5. PRIMOS E IRREDUCIBLES

Problema 5.1. –

Demuestra la **Proposición 2.5.4**. Es decir,

Sea D un dominio entero. Si $p \in D$ es primo (irreducible) y $q \in D$ es asociado a p entonces p es primo (irreducible).

Demostración:

Caso 1: Sea $p \in D$ primo y $q \in D$ asociado a p entonces $q=pu$ con u unidad.

Así sean $a,b \in D$ tales que $q \mid ab \Rightarrow pu \mid ab \Rightarrow \exists c \in D$ tal que $ab=c \cdot pu \Rightarrow ab=(cu)p$ por conmutatividad, por lo que $p \mid ab$ y como p es primo $p \mid a$ o $p \mid b$. Si $p \mid a$ entonces existe $d \in D$

tal que $a = dp \Rightarrow a = du^{-1}up \Rightarrow a = (du^{-1})pu \Rightarrow pu \mid a \Rightarrow q \mid a$ y de forma similar si $p \mid b$ entonces $q \mid b$, por lo que q es primo.

Caso 2 :Sea $p \in D$ irreducible y $q \in D$ asociado a p entonces $q = pu$ con u unidad.
Así sean $a, b \in D$ tales que $ab = q \Rightarrow ab = pu \Rightarrow abu^{-1} = p$ entonces como p es irreducible tendremos que a o bu^{-1} es invertible. Si a es invertible terminamos, si bu^{-1} es invertible tendremos que existe $c \in D$ tal que $(bu^{-1})c = 1 \Rightarrow b(u^{-1}c) = 1$ por lo que b es invertible, con esto q es irreducible.

■

Problema 5.2. –
Considera

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

como subanillo de $\mathbb{C}$.

a) Muestra que $a = 2 + \sqrt{-5}$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$.
b) Muestra que $b = 2 - \sqrt{-5}$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$.
c) Muestra que 3 es irreducible en $\mathbb{Z}[\sqrt{-5}]$.
d) Muestra que a y b no son primos en $\mathbb{Z}[\sqrt{-5}]$.
e) Concluye que $\mathbb{Z}[\sqrt{-5}]$ no es DFU.
f) Muestra que $\mathbb{Z}[\sqrt{-5}]$ es dominio entero.
g) Concluye que $\mathbb{Z}[\sqrt{-5}]$ es un ejemplo de un dominio entero que no es DFU.

Demostración: Antes de empezar los incisos demostraremos que 1 y -1 son los únicos invertibles en $\mathbb{Z}[\sqrt{-5}]$. En efecto sea $a + b\sqrt{-5}$ invertible, entonces existe $x + y\sqrt{-5}$ tal que $(x + y\sqrt{-5})(a + b\sqrt{-5}) = 1$, entonces $\left|x + y\sqrt{-5}\right|^2 \left|a + b\sqrt{-5}\right|^2 = 1 \Rightarrow (x^2 + 5y^2)(a^2 + 5b^2) = 1$, entonces necesariamente $a^2 + 5b^2 = 1$, y si pasara que $b \neq 0$ tendríamos que $b^2 \geq 1 \Rightarrow a^2 + 5b^2 \geq 5$ lo cual es imposible, por lo que $b = 0$ y entonces $a^2 = 1 \Rightarrow a = \pm 1$, con lo que los únicos invertibles son 1 y -1.

a] Sean $x + y\sqrt{-5},\ a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{5}]$ tales que $(x + y\sqrt{-5})(a + b\sqrt{-5}) = 2 + \sqrt{-5}$, entonces

$$\left|2 + \sqrt{-5}\right|^2 = \left|x + y\sqrt{-5}\right|^2 \left|a + b\sqrt{-5}\right|^2 \Rightarrow 4 + 5 = (x^2 + 5y^2)(a^2 + 5b^2)$$
$$(x^2 + 5y^2)(a^2 + 5b^2) = 9$$

entonces tenemos tres casos

• Si $x^2 + 5y^2 = 1$ y $a^2 + 5b^2 = 9$ terminamos

• Si $x^2+5y^2=9$ y $a^2+5b^2=1$ terminamos

• Si $x^2+5y^2=3$ y $a^2+5b^2=3$, tendríamos que $b=y=0$ pues de no serlo $x^2+5y^2\geq 5$ y $a^2+5b^2\geq 5$ lo cual es absurdo, entonces $x^2=3$ y $a^2=3$!!! pero esto no es posible, pues $x,a\in\mathbb{Z}$, por lo que este caso no es posible. Por lo tanto, $2+\sqrt{-5}$ es irreducible.

■

b] Es análogo al caso anterior pues $\left|2-\sqrt{-5}\right|^2=\left|2+\sqrt{-5}\right|^2$.

■

c] Igualmente es análogo, pues $|3|^2=\left|2-\sqrt{-5}\right|^2=\left|2+\sqrt{-5}\right|^2$.

■

d] Veamos que $2+\sqrt{-5}$ y $2-\sqrt{-5}$ no son primos. En efecto, para el primer caso tenemos que $2+\sqrt{-5}\mid 3\cdot 3$ pues $9=(2+\sqrt{-5})\,(2-\sqrt{-5})$, pero $2+\sqrt{-5}\nmid 3$ ya que 3 es irreducible. Análogamente el otro caso.

■

e] Por el inciso anterior podemos decir que no es un DFU ya que encontramos un irreducible que no es primo.

■

f] En efecto, como $\mathbb{C}$ son dominio entero y $\mathbb{Z}[\sqrt{-5}]$ es subanillo entonces será dominio entero.

■

g] En efecto, $\mathbb{Z}[\sqrt{-5}]$ es un ejemplo de un dominio entero que no es DFU.

■

Problema 5.3. –

Demuestra al menos uno de los casos que no demostramos del **Teorema 2.5.14**. Es decir,

Sea R un anillo unitario. Entonces todo ideal izquierdo ó derecho propio de R está contenido en un ideal respectivamente izquierdo ó derecho maximal de R.

Demostración: Estaba muy largo jaja : (

Problema 5.4. –

Sea R un anillo con uno. Demuestra que R es anillo con división, si y sólo si, los únicos ideales izquierdos y derechos de R son $\{0\}$ y R.

Demostración:

$\Rightarrow$]Supongamos que R es anillo con división, entonces todo elemento distinto del cero es invertible. Ahora sea $I\subseteq R$ ideal izquierdo, si $I=\{0\}$ terminamos, entonces supongamos que $I\neq\{0\}$ por lo tanto existe $a\in I$, $a\neq 0$, y dado que a es invertible tendremos por definición de ideal que $1=a^{-1}\cdot a\in I$ por lo que $I=R$ (proposición vista en clase). De forma análoga para ideales derechos.

$\Leftarrow$] Supongamos $\{0\}$ y R son los únicos ideales de R. Sea $a \in R$, sabemos que aR es ideal derecho de R, pero los únicos ideales son $\{0\}$ y R, pero $aR \neq \{0\}$ pues $a = a \cdot 1 \in aR$ por lo que $aR = R$, entonces como $1 \in R$ existe $b \in R$ tal que $1 = ab$, igualmente tenemos que Ra es ideal izquierdo de R y por las mismas razones se tiene que $Ra = R$ por lo que existe $c \in R$ tal que $1 = ca$, con esto tenemos que $c = c(ab) = (ca)b = b$ y entonces $1 = ab = ba$ por lo que a es invertible, y así, R es anillo con división.

■

Problema 5.5. –
Sea R un anillo conmutativo con uno e I un ideal bilateral de R. Entonces R/I es un dominio entero si y sólo si I es un ideal primo de R.

Demostración:
$\Rightarrow$] Supongamos que R/I es un dominio entero. Sean $a, b \in R$ tales que $ab \in I$, entonces $ab + I = I \Rightarrow (a+I)(b+I) = 0_{R/I}$ pero como es un dominio entero se tiene que $a + I = 0_{R/I}$ o $b + I = 0_{R/I}$, es decir, $a \in I$ o $b \in I$, por lo que I es ideal primo.

$\Leftarrow$] Supongamos que I es ideal primo. Sean $a + I, b + I \in R/I$ tales que $(a+I)(b+I) = 0$, entonces $ab + I = I \Rightarrow ab \in I$ pero como es un ideal primo se tiene que $a \in I$ o $b \in I$, es decir, $a + I = 0$ o $b + I = 0$, por lo que R/I es dominio entero.

■

6. DOMINIOS DE FACTORIZACION UNICA

Problema 6.1. –
Considera

$$\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$$

como subanillo de $\mathbb{C}$.

a) Muestra que $\mathbb{Z}[2i]$ es un dominio entero
b) Muestra que 2, $2i$ y $-2i$ son irreducibles en $\mathbb{Z}[2i]$.
c) Muestra que 2 y $2i$ no son asociados $\mathbb{Z}[2i]$.
d) Muestra que $4 \in \mathbb{Z}[2i]$ tiene dos factorizaciones en irreducibles donde los irreducibles no son asociados.
e) Concluye que $\mathbb{Z}[2i]$ es un ejemplo de un dominio entero que no es DFU.

Demostración:

a] Como es subanillo de un dominio entero, también será dominio entero.

■

b] Veamos cuales son los únicos invertibles de $\mathbb{Z}[2i]$. Sea $a+2bi$ invertible, entonces existe $x+2yi$ tal que $(x+y2i)(a+b2i)=1$, entonces $|x+y2i|^2|a+b2i|^2=1 \Rightarrow (x^2+4y^2)(a^2+4b^2)=1$, entonces necesariamente $a^2+4b^2=1$, y si pasara que $b\neq 0$ tendríamos que $b^2\geq 1 \Rightarrow a^2+4b^2\geq 4$ lo cual es imposible, por lo que $b=0$ y entonces $a^2=1 \Rightarrow a=\pm 1$, con lo que los únicos invertibles son 1 y -1.

Ahora, sean $x+y2i,\ a+b2i\in\mathbb{Z}[2i]$ tales que $(x+y2i)(a+b2i)=2$, entonces

$$|2|^2=|x+y2i|^2|a+b2i|^2 \Rightarrow 4=(x^2+4y^2)(a^2+4b^2)$$

entonces tenemos tres casos

- Si $x^2+4y^2=1$ y $a^2+5b^2=4$ terminamos
- Si $x^2+5y^2=4$ y $a^2+5b^2=1$ terminamos
- Si $x^2+5y^2=2$ y $a^2+5b^2=2$, tendríamos que $b=y=0$ pues de no serlo $x^2+4y^2\geq 4$ y $a^2+4b^2\geq 4$ lo cual es absurdo, entonces $x^2=2$ y $a^2=2$!!! pero esto no es posible, pues $x,a\in\mathbb{Z}$, por lo que este caso no es posible. Por lo tanto, 2 es irreducible. Y los casos para 2i y -2i son análogos pues tienen el mismo modulo.

■

c] Las únicas unidades son 1 y -1, y efectivamente $2\neq(1)2i$ y $2\neq(-1)2i$ por lo que no son asociados.

■

d] ¿No debería ser más bien 4i? Tenemos que $4i=(2i)(2)$ y $4i=(-2i)(-2)$ donde son irreducibles y no asociados.

■

e] Por el inciso anterior podemos decir que no es un DFU ya encontramos un elemento que no tiene factorización única.

■

7. CAMPO COCIENTE

Problema 7.1. –

Demuestra que la operación multiplicación en el campo de fracciones no depende del representante. Es decir,

Sea D un dominio entero. Definimos el conjunto:

$$M = \{(a,b) : a,b \in D \text{ y } b \neq 0\}$$

La relación de equivalencia sobre M:

$$(a,b) \sim (c,d), \text{ si y solo si, } ad = bc$$

Denotemos por $[a,b]$ la clase de equivalencia en M de (a,b) y sea $\mathbb{Q}(D)$ el conjunto de todos las clases de equivalencia $[a,b]$. Esto es,

$$\mathbb{Q}(D) = \{[a,b] \ : \ a,b \in D \, y \, b \neq 0\}$$

Y definamos la multiplicación para $[a,b],[c,d]\mathbb{Q}(D)$ como

$$[a,b][c,d] = [ac,bd]$$

Demuestra que si $[a,b],[a',b'],[c,d],[c',d'] \in \mathbb{Q}(D)$, con $[a,b]=[a',b']$ y $[c,d]=[c',d']$. Entonces $[ac,bd]=[a'c',b'd']$.

Demostración: En efecto, como $[a,b]=[a',b'] \;\Rightarrow\; (a,b) \sim (a',b')$ e igualmente como $[c,d]=[c',d'] \;\Rightarrow\; (c,c) \sim (c',d')$ y entonces $ab'=ba'$ y $cd'=dc'$ con lo que multiplicando estas dos tenemos que $ab'cd'=ba'dc' \;\Rightarrow\; acb'd'=bda'c' \;\Leftrightarrow\; [ac,bd]=[a'c',b'd']$

■

Problema 7.2. –

Sea D un dominio entero y sea $p \in \mathbb{Q}(D)$ no cero. Entonces existen $a,b \in D$ no cero tales que $(a,b)=1$ y $\frac{a}{b}=p$.

Corrección: D es dominio entero MCD.

Demostración: Como $p \in \mathbb{Q}(D)$, entonces existen $a,b \in D,\ d \neq 0$ tal que $p=[a,b] := \frac{a}{b}$.

Sea $d=(a,b)$ (que existe ya que D es dominio MCD), entonces $d \mid a$ y $d \mid b$ por lo que existen $s,t \in D$ tales que $a = sd$ y $b = td$ entonces $[a,b]=[s,t]$ pues $at = sdt = dts = bs$. Ahora sea $d'=(s,t)$ entonces $d' \mid s$ y $d' \mid t$ por lo que existen $s',t' \in D$ tales que $s = s'd'$ y $t = t'd'$, entonces, $a = s'd'd$ y $b = t'd'd' \;\Rightarrow\; dd' \mid a$ y $dd' \mid b$ y además $d \mid dd'$!! pero esto es absurdo pues d era un máximo común divisor, por lo que $d' = 1$. Y entonces los elementos buscados son $s,t \in D$ ya que son tales que $(s,t) = 1$ y $p = \frac{s}{t}$.

■

8. DOMINIOS EUCLIDEANOS

Problema 8.1. –

Sea D un dominio Euclidiano con valuación d. Entonces.

a) Si $0 \neq a \in D$ entonces $d(1) \leq d(a)$.

b) Sean $a \neq 0$, $b \neq 0 \in D$ tales que a es asociado de b. Entonces $d(a) = d(b)$.

c) Un elemento $0 \neq a \in D$ es invertible si, y sólo si, $d(a) = d(1)$.

Demostración:

(a) Como D es un DE entonces $d(1) \leq d(1 \cdot a)$ $\forall a \neq 0 \Rightarrow d(1) \leq d(a)$

(b) Como a y b son asociados existe $u \in D$ unidad tal que $b = a \cdot u$ y como D es un DE entonces $d(a) \leq d(u \cdot a) = d(b)$ y por otro lado $d(b) \leq d(u^{-1}b) = d(a)$ por lo que $d(a) = d(b)$.

(c) Por el primer inciso tenemos que $d(1) \leq d(a)$.

$\Rightarrow$] Como a es invertible existe a^{-1} tal que $aa^{-1} = 1$ entonces $d(1) \leq d(a) \leq d(a \cdot a^{-1}) = d(1)$ por lo que $d(a) = 1$.

$\Leftarrow$] Por ser d valuación tenemos que existen $q,r \in D$ tal que $1 = qa + r$ con $r = 0$ o $d(r) < d(a)$ pero lo segundo es imposible pues tendríamos que $d(1) \leq d(r) < d(a) = d(1)$ y entonces $d(1) < d(1)$!! por lo que $r = 0$ entonces $1 = qa$ por lo que a es invertible.

■

Problema 8.2. –

Definición Sea D un dominio entero. Definimos una norma Dedekind-Hasse como una función $N : D \to \mathbb{Z} \cup \{0\}$ tal que

a) $N(0) = 0$

b) Para cada $a, b \in D$, o bien $a \in \langle b \rangle$ o bien existe $c \in \langle a, b \rangle$ (no cero) tal que $0 < N(c) < N(b)$.

Vas a demostrar el siguiente resultado:

Proposición Si D dominio entero tiene una norma Dedekin-Hasse, entonces D es un DIP.

Sugerencia Dado $I \subseteq D$ un ideal, considera $b \in I$ un elemento no cero de norma minimal.

Demostración: Sea $I \subseteq D$ un ideal y $b \in I$ distinto de cero con norma mínima.

PD] $I = \langle b \rangle$. Por definición de ideal generado tenemos que $I \supseteq \langle b \rangle$ por lo que solo basta probar la otra contención.

Sea $a \in I$, entonces por hipótesis de norma de Dedekinf-Hasse $a \in \langle b \rangle$ o existe $c \in \langle a,b \rangle$ tal que $0 < N(c) < N(b)$, pero si pasara lo segundo tendríamos que $c \in \langle a,b \rangle \subseteq I \Rightarrow \exists c \in I$ tal que $N(c) < N(b)$!!! pero esto no es posible pues b era de norma mínima, por lo que $a \in \langle b \rangle$.

■

Problema 8.3. –

Definición Sea D un dominio entero y $\hat{D} = U(D) \cup \{0\}$. $u \in D \setminus \hat{D}$ es un *divisor lateral universal* si para todo $x \in D$ existe $z \in \hat{D}$ tal que $u \mid x - z$.

Demuestra que:

a) u es un divisor lateral universal si y sólo si para todo $x \in D$ existen $q \in D$ y z unidad o cero tal que $x = qu + z$

b) Si D es un dominio euclideano que no es un campo, entonces D tiene divisores laterales universales.

Demostración:

(a) En efecto, $u \in r \in D - \hat{D}$ es un divisor lateral universal si y solo si $\forall x \in D$ existe $z \in \hat{D}$ tal que $u|x - z$ si y solo si existe $q \in D$ tal que $x - z = qu \Leftrightarrow x = qu + z$.

(b) En efecto como D es dominio euclidiano (por tanto dominio entero) que no es campo entonces no todos sus elementos son invertibles, por lo que $\hat{D} \neq \varnothing$, con ello sean $u \in D - \hat{D}$ con valuación mínima y $x \in D$, entonces existen $q, r \in D$ tales que $x = qu + r$ con $r = 0$ o $d(r) < d(u)$, si pasara que $r \in \hat{D}$ entonces r es unidad o es cero y si pasara que $r \in D - \hat{D}$ entonces no podría pasar que $d(r) < d(u)$ por la elección de u por lo que $r = 0$, en cualquiera de los dos casos tenemos que r es unidad o es cero por lo que por el inciso anterior u es un divisor lateral universal.

■