Módulo 12:

FACTORIZACIÓN EN ANILLOS CONMUTATIVOS

En este módulo, se desarrollarán algunos teoremas y definiciones asociados al concepto de divisibilidad de números, pero vistos desde la mirada del anillo conmutativo al cual pertenecen dichos números, los cuales son elementos de éste. Además se desarrollan las características más relevantes de los dominios más importantes y la relación entre éstos como estructuras y el comportamiento de sus elementos. Es importante la introducción de los conceptos de elementos (o números) primos, irreducibles y más aún las ideas de elementos maximales (mcd) y minimales (mcm) de factorización, propios de la teoría de números.

Definición 1: Sea A un anillo conmutativo con identidad, dados $a, b \in A$ diremos que a divide a b si existe $c \in A$ tal que $b = a \cdot c$

Nota: a divide a b lo anotaremos como $a \mid b$.

Proposiciones: Sea $a, b, b_1, b_2, d, d_1, d_2 \in A$ anillo conmutativo con identidad, se tiene:

1.- $a \mid b$ entonces $a \mid b \cdot d$, $\forall d \neq 0$

2.- $a \mid b_1$ y $a \mid b_2$ entonces $a \mid b_1 + b_2$

3.- $a \mid b_1$ y $a \mid b_2$ entonces $a \mid b_1 \cdot d_1 + b_2 \cdot d_2$

Demostración:

1.- Si $a \mid b$ entonces existe $c \in A$ tal que $b = a \cdot c$, aplicando $\cdot d$ por la derecha se tiene, $b \cdot d = (a \cdot c) \cdot d$, se tiene $b \cdot d = a \cdot (c \cdot d)$, por asociatividad en A, luego tomando $c \cdot d = e \in A$, resulta $b \cdot d = a \cdot e$

Es decir $a \mid b \cdot d$, por lo tanto si $a \mid b$ entonces $a \mid b \cdot d$, $\forall d \neq 0$

2.- Si $a \mid b_1$, $a \mid b_2$ por demostrar $a \mid b_1 + b_2$

Si $a \mid b_1$ entonces existe $r \in A$ tal que $b_1 = a \cdot r$

Si $a \mid b_2$ entonces existe $t \in A$ tal que $b_2 = a \cdot t$

De ambas condiciones se tiene

$$b_1 + b_2 = a \cdot r + a \cdot t$$

Luego $b_1 + b_2 = a \cdot (r + t)$, por distributividad, podemos decir que $a \mid b_1 + b_2$, por lo tanto $a \mid b_1 + b_2$ cuando $a \mid b_1$ y $a \mid b_2$

3.- Si $a \mid b_1$, $a \mid b_2$ por demostrar $a \mid b_1 \cdot d_1 + b_2 \cdot d_2$

Si $a \mid b_1$ entonces existe $r \in A$ tal que $b_1 = a \cdot r$, aplicando $\cdot d_1$ por la derecha, con $d_1 \in A$, nos resulta $b_1 \cdot d_1 = a \cdot r \cdot d_1$

Ahora, si $a \mid b_2$ entonces existe $t \in A$ tal que $b_2 = a \cdot t$, aplicando $\cdot d_2$ por la derecha, con $d_2 \in A$, se tiene $b_2 \cdot d_2 = a \cdot t \cdot d_2$

De ambas condiciones obtenemos:

$b_1 \cdot d_1 + b_2 \cdot d_2 = a \cdot r \cdot d_1 + a \cdot t \cdot d_2$

$b_1 \cdot d_1 + b_2 \cdot d_2 = a \cdot (r \cdot d_1 + t \cdot d_2)$ por distributividad, con $r \cdot d_1 + t \cdot d_2 \in A$

Luego $a \mid b_1 \cdot d_1 + b_2 \cdot d_2$, por lo tanto $a \mid b_1 \cdot d_1 + b_2 \cdot d_2$ cuando $a \mid b_1$ y $a \mid b_2$.

Definición 2: Sea A anillo conmutativo con identidad, diremos que a es asociado con b si existe $u \in U(A)$ tal que $a = u \cdot b$, con $a, b \in A$.

Ejemplo 1:

En $\mathbb{Z}$, determinaremos los asociados de (-2)

$$(-2) = (-1) \cdot 2, \text{ por asociatividad en } \mathbb{Z}$$

$$(-2) = 1 \cdot (-2)$$

Luego los asociados de (-2) son 2 y (-2)

Ejemplo 2:

En $\mathbb{Q}$ existen infinitos asociados.

Observación: La relación $(\sim)$ "ser asociado con" es una relación de equivalencia, en efecto:

i) $\sim$ es reflexiva: $a \sim a \quad \forall a \in A$

$$a = 1 \cdot a$$

Por lo tanto a es asociado con a

ii) $\sim$ es simétrica:

Para todo $a, b \in A$, si $a \sim b$ entonces $b \sim a$. Si $a \sim b$ entonces existe $u \in U(A)$ tal que $a = u \cdot b$, aplicando $\cdot u^{-1}$ por la izquierda se tiene tal que $a = u \cdot b,$. Notar que si $u \in U(A)$ entonces $u^{-1} \in U(A)$.

Luego si $u^{-1} \cdot a = b$ entonces $b \sim a$

iii) $\sim$ es transitiva:

Para todo $a, b, c \in A$, si $a \sim b$ y $b \sim c$ entonces $a \sim c$.

1) Si $a \sim b$ entonces existe $u \in U(A)$ tal que $a = u \cdot b$

2) Si $b \sim c$ entonces existe $v \in U(A)$ tal que $b = v \cdot c$

Luego reemplazando (2) en (1) resulta:

$a = u \cdot (v \cdot c)$, luego por asociatividad se tiene

$a = (u \cdot v) \cdot c$, considerando $u \cdot v = w$, obtenemos

$a = w \cdot c$, con w unidad

Por lo tanto $a \sim c$

Proposición: Sea A un Dominio de Integridad, entonces a es asociado con b si y solo si $b \mid a$ y $a \mid b$

Demostración:

$\Rightarrow$] Hipótesis: a es asociado con b.

Tesis: $b \mid a$ y $a \mid b$.

Como a es asociado con b, entonces existe $u \in U(A)$ tal que $a = u \cdot b$

Por lo tanto $b \mid a$.

Por otro lado como $a = u \cdot b$ entonces $b = u^{-1} \cdot a$, al aplicar $\cdot u^{-1}$ por la izquierda, con $u^{-1} \in A$, se cumple que $a \mid b$, por lo tanto $b \mid a$ y $a \mid b$ cuando a es asociado con b.

$\Leftarrow$] Hipótesis: $b \mid a$ y $a \mid b$.

Tesis: a es asociado con b.

Por hipótesis se tiene:

i) Si $b \mid a$ entonces existe $c \in A$ tal que $a = c \cdot b$

ii) Si $a \mid b$ entonces existe $d \in A$ tal que $b = a \cdot d$

Luego al sustituir ii) en i) por propiedades del anillo A (DI) se tiene que:

$a = c \cdot (a \cdot d) = c \cdot (d \cdot a) = (c \cdot d) \cdot a$

En efecto de lo anterior $c \cdot d = 1$, siempre que $a \neq 0$, es decir $c \in U(A)$ luego $a = c \cdot b$, o bien $d \in U(A)$ entonces $b = a \cdot d$, por lo tanto a es asociado con b cuando $b \mid a$ y $a \mid b$.

Definición 3: Sea A un Dominio de Integridad, considerando $p \neq 0$, $p \in A$, diremos que p es un elemento primo de A si:

$$p \notin U(A) \text{ y } p \mid a \cdot b \text{ entonces } p \mid a \text{ o } p \mid b$$

Definición4: Sea A un Domino de Integridad, diremos que $c \in A$ es irreducible si $c \neq 0$ y $c \notin U(A)$ además $a \mid c$ entonces a es asociado con c o bien $a \in U(A)$.

Ejemplo 3:

Verificar que $5 \in \mathbb{Z}$ es irreducible, tal que $U(\mathbb{Z}) = \{-1, 1\}$

Ahora según las condiciones se tiene que $5 \neq 0$ y $5 \notin U(A)$

Además, como $1 \mid 5$ entonces existe $5 \in \mathbb{Z}$ tal que $5 = 1 \cdot 5$. Luego 1 no es asociado con 6 pero $1 \in U(A)$. Por otro lado, como $5 \mid 5$ entonces existe $1 \in \mathbb{Z}$ tal que $5 = 5 \cdot 1$. Luego 5 es asociado con 5 o $5 \notin U(A)$.

Por lo tanto $6 \in \mathbb{Z}$ es un elemento irreducible.

Proposición: Sea A un Dominio de Integridad. Si $p \in A$ es primo, entonces p es irreducible.

Demostración:

Si p es primo enotnces $p \neq 0$ y $p \notin U(A)$.

Además, si $a \mid p$, con $a \in A$, entonces existe $b \in A$ tal que $p = a \cdot b$.

Como $1 \in A$, se tiene que $1 \cdot p = a \cdot b$. Luego $p \mid a \cdot b$, es decir $p \mid a$ o $p \mid b$. Como $p \mid a$ y además $a \mid p$ entonces a es asociado con p.

Si $p \mid b$ entonces existe $c \in A$ tal que $b = p \cdot c$ pero $p = a \cdot b$ luego $p = a \cdot p \cdot c$, esto implica que $p = p \cdot a \cdot c$ por ser A un Dominio de Integridad, luego $a \cdot c = 1$, por lo tanto $a \in U(A)$ $\left(\text{o bien } c \in U\left(A\right)\right)$.

En consecuencia p es irreducible cuando p es un primo , con A un $D.I.$.

Ejemplo 4:

Sea A un anillo conmutativo con identidad, A no tiene nilpotentes distintos de cero si y solo si $a^2 = 0$ entonces $a = 0$

Demostración:

$\Rightarrow]$ Hipótesis: A no tiene nilpotentes distintos de cero.

Tesis: $a^2 = 0$ entonces $a = 0$

Por hipótesis se tiene que $a \in A,\ a \neq 0$ tal que $a^n = 0,$ entonces $a = 0,\ \forall n \in \mathbb{Z}$.

Por lo tanto en particular se tiene que si $a^2 = 0$ entonces $a = 0$.

$\Leftarrow]$ Hipótesis: $a^2 = 0$ entonces $a = 0$

Tesis: A no tiene nilpotentes distintos de cero.

Supongamos que $b \in A$ nilpotente entonces $b^n = 0,\ \forall n \in \mathbb{Z}$ con n el menor entero con esta propiedad, en consecuencia $b^{n-1} \neq 0$, es decir, $\left(b^{n-1}\right)^2 = b^{n-1} \cdot b^{n-1} = b^n \cdot b^{n-2} = 0 \cdot b^{n-2}$, luego $\left(b^{n-1}\right)^2 = 0$, por lo tanto $b^{n-1} = 0$ ¡Contradicción! , pues $b^{n-1} \neq 0$.

Ejemplo 5:

Sea $\left(\mathbb{Z}[i],\ +,\ \cdot\right)$ un Dominio de Integridad tal que $\mathbb{Z}[i]=\left\{a+bi\,/\,a,\ b\in\mathbb{Z},\ i^2=-1\right\}$. Determinar $U\left(\mathbb{Z}[i]\right)$

Demostración:

Determinaremos que $\mathbb{Z}[i]$es invertible, es decir, dado $(a+bi)\in\mathbb{Z}[i]$ por encontrar $(c+di)\in\mathbb{Z}[i]$ tal que $(a+bi)\cdot(c+di)=1+0i$

Se tiene:

$(a+bi)\cdot(c+di)=1+0i$

$a\cdot c+(b\cdot c+a\cdot d)i-b\cdot d=1+0i$

En efecto, i) $a\cdot c-b\cdot d=1$ y ii) $b\cdot c+a\cdot d=0$

Ahora bien, aplicando $\cdot a$ en i) por la izquierda se tiene

$a^2\cdot c-a\cdot b\cdot d=a$

Por otro lado, aplicando $\cdot b$ en ii) por la izquierda obtenemos

$b^2\cdot c+b\cdot a\cdot d=0$

Claramente $b^2\cdot c=-b\cdot a\cdot d$ y sustituyendo este valor resulta

$a^2\cdot c+b^2\cdot c=a$

$c\cdot\left(a^2+b^2\right)=a$

En consecuencia $c=\dfrac{a}{a^2+b^2}$, ahora como $a\cdot d=-b\cdot c$, resulta $d=\dfrac{-b\cdot c}{a}$, luego sustituyendo c se obtiene $d=\dfrac{-b}{a^2+b^2}$:

Si $a\neq 0$ entonces $a\leq a^2$

Si $b\neq 0$ entonces $a<a^2+b^2$

Considerando $b=0$ se obtiene $c=\frac{a}{a^2}=\frac{1}{a}$, por lo tanto $a=\pm 1$.

Por otro lado si $b\neq 0$ entonces $b\leq b^2$

Además, si $a\neq 0$ resulta $b<a^2+b^2$

Tomando $a=0$ se tiene $d=\frac{-b}{b^2}=\frac{-1}{b}$, resulta $b=\pm 1$.

En consecuencia $\mathbb{Z}[i]$ es invertible, con las $U(\mathbb{Z}[i])=\{1,\ -1,\ i,\ -i\}$.

Ejemplo 6:

Considerando el complejo 2. Encontrar los asociados a 2 en $\mathbb{Z}[i]$.

Nota: a es asociado a b si $a=u\cdot b$ es invertible.

En efecto, existe $u\in\mathbb{Z}[i]$ tal que $2=u\cdot 2$

$$2=(-1)\cdot(-2)$$

$$2=(1)\cdot(2)$$

$$2=(i)\cdot(-2i)$$

$$2=(-i)\cdot(2i)$$

Por lo tanto los asociados a 2 en $\mathbb{Z}[i]$ son $\{2,\ -2,\ 2i,\ -2i\}$.

Definición 5: Sea A un Dominio de Integridad, $a_1,\ a_2,...,\ a_n\in A$ entonces $m\in A$ es el mínimo común múltiplo de $a_1,\ a_2,...,\ a_n$ si:

1.- $a_i\,|\,m \quad , \ \forall i=1,n$

2.- Si $c\in A,\ \ a_i\,|\,c$ entonces $m\,|\,c$

Definición 6: Sea A un Dominio de Integridad, $a_1,\ a_2,...,\ a_n \in A$ y d es el máximo común divisor de $a_1,\ a_2,...,\ a_n$ si:

1.- $d \mid a_i \quad , \forall i = 1,n$

2.- Si existe $c \in A$ tal que $c \mid a_i$ entonces $c \mid d, \ \forall i = 1,n$

Notación: d es el máximo común divisor de $a_1,\ a_2,...,\ a_n$ lo anotaremos como $d = mcd\left\{a_1,\ a_2,...,\ a_n\right\}$.

Proposición: Sea A un Dominio de Integridad, $a_1,\ a_2,...,\ a_n \in A$ y d es el máximo común divisor de $a_1,\ a_2,...,\ a_n$ entonces:

$L = mcd\left\{a_1,\ a_2,...,\ a_n\right\} = \left\{u \cdot d \,/\, u \in U(A)\right\} = S$

Demostración:

Por demostrar que $L = S$, es decir debemos verificar que i) $L \subset S$ y ii) $S \subset L$, en efecto:

i) Sea $d_1 \in mcd\left\{a_1,\ a_2,...,\ a_n\right\}$ por demostrar que $d_1 \in \left\{u \cdot d \,/\, u \in U(A)\right\}$

Como $d_1\ mcd\left\{a_1, a_2, ..., a_n\right\}$ entonces $d_1 \mid d$

Además por hipótesis se tiene que d es $mcd\left\{a_1, a_2, ..., a_n\right\}$ entonces $d \mid d_1$, luego d y d_1 son asociados, es decir $d_1 = u \cdot d$, con $u \in U(A)$, por lo tanto $d_1 \in S$.

ii) Sea $u \cdot d \in S$, con $u \in U(A)$, por demostrar que $u \cdot d \in L = mcd\left\{a_1, a_2, ..., a_n\right\}$, es decir, debemos demostrar:

1.- $u \cdot d \mid a_i \ , \ \forall i = 1,n$

2.- Si existe $c \in A$ tal que $c \mid a_i$ entonces $c \mid u \cdot d, \ \ \forall i = 1,n$

1.- Como $d = mcd\{a_1, a_2, ..., a_n\}$ entonces $d \mid a_i \ , \ \forall i = 1,n$

Por lo tanto $a_i = d \cdot x \quad$, con $x \in A$

Considerando $u \cdot u^{-1} = 1$ tenemos:

$a_i = \left(u \cdot u^{-1}\right) d \cdot x$, con A dominio de integridad se tiene

$a_i = u \cdot d \cdot \left(u^{-1} \cdot x\right), \ \ u^{-1} \cdot x = y \in A$

Por lo tanto $a_i = \left(u \cdot d\right) \cdot y$ entonces $u \cdot d \mid a_i \quad , \forall i = 1,n$

2.- Si existe $c \in A$ tal que $c \mid a_i$ por demostrar $c \mid u \cdot d, \ \ \forall i = 1,n$

Como $d = mcd\{a_1, a_2, ..., a_n\}$ entonces $c \mid d$, luego $d = c \cdot x$, aplicando $\cdot u$ por la izquierda nos resulta $u \cdot d = u \cdot (c \cdot x)$, además como A es un dominio de integridad

Entonces $u \cdot d = c \cdot \left(u \cdot x\right)$

Luego $c \mid u \cdot d$

Por lo tanto de 1) y 2) $u \cdot d \in L$ cuando $u \cdot d \in S$

Ejemplo 7:

El *mcd* (máximo común divisor) entre 4 y 6 es ± 2 y difieren en una unidad.

El *MCM* (mínimo común múltiplo) entre 4 y 6 es ± 12 y difieren en una unidad.

Notación: El *mcd* entre a y b lo anotaremos por (a, b).

El *MCM* entre a y b lo anotaremos por $[a,b]$.

Proposición: Sean $a, b \in A$ con (a, b) y $[a, b]$ el *mcd* y *MCM* respectivamente entre a y b, se cumple que $u \cdot a \cdot b = (a, b) \cdot [a, b]$, con $u \in U(A)$.

Demostración:

Se tiene que $[a, b] \mid a \cdot b$ entonces existe $x \in A$ tal que $a \cdot b = [a, b] \cdot x$

Basta probar que x es $mcd(a, b)$, es decir, debemos demostrar que:

i) $x \mid a$ y $x \mid b$

ii) Si $c \mid a$ y $c \mid b$ por demostrar $c \mid x$, en efecto:

i) Se sabe que $a \mid [a, b]$ entonces existe $y \in A$ tal que $[a, b] = a \cdot y$

Además se sabe que $a \cdot b = [a,b] \cdot x$, luego sustituyendo se tiene:

$$a \cdot b = (a \cdot y) \cdot x$$

$$a \cdot b = a \cdot y \cdot x$$

Luego $b = y \cdot x$, por lo tanto $x \mid b$.

Por otro lado se sabe que $b \mid [a,b]$, entonces existe $z \in A$ tal que $[a,b] = b \cdot z$.

Además sabemos de lo anterior que $a \cdot b = [a,b] \cdot x$

Luego sustituyendo tenemos:

$$a \cdot b = (b \cdot z) \cdot x$$

$$a \cdot b = b \cdot z \cdot x$$

En consecuencia $a = z \cdot x$, luego nos resulta $x \mid a$.

ii) Si $c \mid a$ y $c \mid b$ debemos demostrar que $c \mid x$.

a) Si $c \mid a$ entonces existe $s \in A$ tal que $a = c \cdot s$.

b) Además, si $c \mid b$ entonces existe $t \in A$ tal que $b = c \cdot t$.

Como $a = c \cdot s$ aplicando $\cdot t$ por la derecha obtenemos $a \cdot t = c \cdot s \cdot t$ luego $a \mid c \cdot s \cdot t$, por otro lado como $b = c \cdot t$, aplicando $\cdot s$ por la derecha nos resulta $b \cdot s = c \cdot t \cdot s$, luego $b \mid c \cdot s \cdot t$.

Ahora si $a \mid c \cdot s \cdot t$ y $b \mid c \cdot s \cdot t$ entonces $[a,b] \mid c \cdot s \cdot t$

$[a,b] \mid c \cdot s \cdot t$ entonces existe $v \in A$ tal que $c \cdot s \cdot t = [a,b] \cdot v$, aplicando $\cdot c$ por la izquierda y sustituyendo a) y b) se tiene:

$$c \cdot s \cdot c \cdot t = c \cdot [a,b] \cdot v$$

$$a \cdot b = c \cdot [a,b] \cdot v$$

$$a \cdot b = [a,b] \cdot x$$

Por lo tanto $[a,b] \cdot x = c \cdot [a,b] \cdot v$

En consecuencia si $x = c \cdot v$ entonces $c \mid x$, es decir x es $mcd(a,b)$.

Definición 7: Sea A un Dominio de Integridad, diremos que A es un dominio euclideano $(D.E.)$ si existe: $\eta : A - \{0\} \to \mathbb{Z}_0^+$, función valor absoluto tal que:

1.- $\eta(a \cdot b) \geq \eta(a)$

2.- Dados $a, b \in A$ con $b \neq 0$, existen $q, r \in A$ tal que $a = b \cdot q + r$, donde $r = 0$.

$$R = 0 \ \ ó \ \ \eta(R) < \eta(b)$$

Ejemplo 8:

Determinar si existe en $A = \mathbb{Z}[i]$ una función valor absoluto η.

Sea $\eta : \mathbb{Z}[i] - \{0\} \to \mathbb{Z}_0^+$

$$a + bi \mapsto \eta(a + bi) = a^2 + b^2$$

Claramente se verifica que:

$\eta(a+bi)=(a+bi)\cdot\left(\overline{a+bi}\right)=(a+bi)\cdot(a-bi)=a^2+b^2\geq 0, \forall a,b\in\mathbb{R}.$

Definición 8: Sea A un Dominio de Integridad, diremos que A es un dominio de ideales principales $(D.I.P.)$ si todos los ideales de A son principales.

Proposición: Si A un $D.E.$ entonces A es un $D.I.P.$

Demostración:

Consideremos el conjunto $\{\eta(a)/a\in I-\{0\},\ I\lhd A\}$, luego se tiene que $\eta(a)\geq\eta(1)$ $\left(a=a\cdot 1\quad \eta(a\cdot 1)\geq\eta(1)\right)$.

Luego el conjunto $\{\eta(a)/a\in I-\{0\}\}$ está acotado inferiormente, por lo tanto podemos escoger $a\in I-\{0\}$ tal que $\eta(b)\geq\eta(a)$, $\forall b\in I-\{0\}$ $a\in I$ ideal, $\langle a\rangle\subset I$.

Sea $b\in I$, dados a,b en A que es $D.E.$ se tiene que existen $q,\ r$ tal que $b=a\cdot q+r$ con $r=0$ o $\eta(r)<\eta(a)$.

Si $r=0$ entonces $b=a\cdot q$, como $b\in\langle a\rangle$ se tiene $I\subset(a)$ en consecuencia $I=\langle a\rangle$, ahora si $\eta(r)<\eta(a)$ y $b=a\cdot q+r$ resulta $r=b-a\cdot q$, con $b\in I,\ a\cdot q\in I$, luego $r\in I$.

En consecuencia $\eta(r)\geq\eta(a)$ ¡contradicción!

Por lo tanto $\eta(r)<\eta(a)$, pues a se escogió minimal.

Por lo tanto la única posibilidad es que $r=0$ y que $I=\langle a\rangle$.

Proposición: Si A es un $D.I.P.$ y $a_1, a_2, ..., a_n \in A$ entonces existe $d = mcd\{a_1, a_2, ..., a_n\}$ y $\langle d \rangle = \langle a_1, a_2, ..., a_n \rangle$.

Demostración:

Como A es $D.I.P.$ y $\langle d \rangle = \langle a_1, a_2, ..., a_n \rangle$ (recordar que todo ideal principal de A está generado por un elemento) por demostrar que $d = mcd\{a_1, a_2, ..., a_n\}$, es decir, debemos demostrar que:

i) $d \mid a_i$, $\forall i = 1, n$.

ii) Si existe $c \in A$ tal que $c \mid a_i$ entonces $c \mid d$, $\forall i = 1, n$

Si $d \mid a_i$, $\forall i = 1, n$ entonces $c \mid d$, con $c \in A$, luego,

i) Como $a_i \in \langle a_1, a_2, ..., a_n \rangle$, $\forall i = 1, n$

Resulta $a_i = 0 \cdot a_1 + 0 \cdot a_2 + ... + 1 \cdot a_i + 0 \cdot a_{i+1} + 0 \cdot a_n$, por lo tanto $a_i \in \langle d \rangle$ de lo anterior $a_i = t \cdot d$ con $t \in A$ tal que $d \mid a_i$, $\forall i = 1, n$, en consecuencia $d \in \langle d \rangle$.

ii) Ahora bien, como $d \in \langle a_1, a_2, ..., a_n \rangle$

Se tiene que $d = x_1 \cdot a_1 + x_2 \cdot a_2 + ... + x_n \cdot a_n$, con $x_1, x_2, ..., x_n \in A$

Como $c \mid a_i$, $\forall i = 1, n$ entonces existen $t_i \in A$ tal que $a_i = c \cdot t_i$, $\forall i = 1, n$

Luego, $d = x_1 \cdot t_1 \cdot c + x_2 \cdot t_2 \cdot c + ... + x_n \cdot t_n \cdot c$, factorizando por c resulta $d = c \cdot (x_1 \cdot t_1 + x_2 \cdot t_2 + ... + x_n \cdot t_n)$, con $(x_1 \cdot t_1 + x_2 \cdot t_2 + ... + x_n \cdot t_n) = s \in A$, por lo tanto si $d = c \cdot s$ entonces $c \mid d$.

En consecuencia de i) y ii) se tiene que $d = mcd\{a_1, a_2, ..., a_n\}$.

Proposición: Si A es un $D.I.P.$ entonces p es primo si y solo si p es irreducible.

Demostración:

$\Rightarrow$] Demostrado pues basta que A sea un Dominio de Integridad.

$\Leftarrow$] Hipótesis: p es irreducible en A un $D.I.P.$

Tesis: p es primo, es decir, debemos demostrar que si $p \notin U(A)$ y $p \mid a \cdot b$ entonces $p \mid a$ o $p \mid b$.

Consideremos el ideal $\langle p \rangle$. Se afirma que es maximal, pues p es irreducible.

Ahora, si $\langle p \rangle \subset I \subset A$ debemos demostrar $\langle p \rangle = I$ o $I = A$.

Pues bien, sabemos que $I \lhd A$ luego $I = \langle s \rangle$, $\forall s \in A$, como $\langle p \rangle \subset \langle s \rangle$, si $p \in \langle s \rangle$ entonces $p = s \cdot t$, con $t \in A$, luego $s \mid p$, en efecto $s \in U(A)$ o s es asociado con p. Ahora si $s \in U(A)$ entonces $\langle s \rangle = A$

Por otro lado si s es asociado con p entonces $s = u \cdot p$, con $u \in U(A)$.

Luego $\langle s \rangle \subset \langle p \rangle$, pero $\langle p \rangle \subset \langle s \rangle$, en consecuencia, podemos decir que $\langle p \rangle = \langle s \rangle$, por lo tanto si $\langle p \rangle$ es maximal es primo.

Ahora bien, si $p \mid a \cdot b$ entonces existe $k \in A$ tal que $a \cdot b = k \cdot p$, luego si $a \cdot b \in \langle p \rangle$ entonces $a \in \langle p \rangle$ o $b \in \langle p \rangle$.

En consecuencia si $a \in \langle p \rangle$ entonces $a = s \cdot p$, con $s \in A$, luego $p \mid a$.

Además, si $b \in \langle p \rangle$ entonces $b = r \cdot p$, con $r \in A$, luego $p \mid b$.

Proposición: Sea A un $D.I.P.$ entonces toda cadena ascendente de ideales es estacionaria, es decir si $I_1 < I_2 < ... \; I_n < I_{n+1}$ una sucesión de ideales, existe n tal que $I_n = I_{n+1} = ...$

Demostración:

Como A es un $D.I.P.$ entonces $I_i = \langle a_i \rangle, \forall i = 1, n$.

Luego se tiene que, $\langle a_1 \rangle \subset \langle a_2 \rangle \subset ... \subset \langle a_n \rangle \subset ...$, ahora tomemos

$\bigcup_{i \in I} \langle a_i \rangle = I$ un ideal de A, $\forall i = 1, n$.

Si $x, y \in \bigcup_{i \in I} \langle a_i \rangle$ entonces $x \in \langle a_i \rangle, y \in \langle a_j \rangle$ ya que $\langle a_i \rangle \subset \langle a_j \rangle$, con $x, y \in \langle a_j \rangle$

Por lo tanto $x + y \in \langle a_j \rangle$

Considerando $\bigcup_{i \in I} \langle a_i \rangle = \langle a \rangle = I$, $\forall a \in A$, entonces $\langle a_i \rangle \subset \bigcup_{i \in I} \langle a_i \rangle$, $\forall i = 1, n$

es decir, $\langle a_i \rangle \subset \langle a \rangle = I \quad (I_n = I_{n+1} = ...)$.

Ahora como $a \in \langle a \rangle$ se tiene que, $a \in \bigcup_{i \in I} \langle a_i \rangle$ entonces existe n tal que $a \in \langle a_n \rangle$, luego $\langle a \rangle \subset \langle a_n \rangle$, en efecto $\langle a \rangle = \langle a_n \rangle$, además $\langle a_{n+1} \rangle \subset \bigcup_{i \in I} \langle a_i \rangle = \langle a \rangle = \langle a_n \rangle$, en consecuencia $\langle a_{n+1} \rangle \subset \langle a_n \rangle$ y por la cadena $\langle a_n \rangle \subset \langle a_{n+1} \rangle$, se tiene que $\langle a_n \rangle = \langle a_{n+1} \rangle$.

Proposición: Sea A un $D.I.P.$, $p_1, ..., p_s$ y $q_1, ..., q_r$ elementos irreducibles, con $u \in U(A)$ y $a \in A$ tal que:

$a = p_1 \cdot ... \cdot p_s = u \cdot q_1 \cdot ... \cdot q_r$ entonces se tiene que $r = s$ y p_i es asociado a q_i, $\forall i = 1, s$

Demostración:

Supongamos que $r \leq s$

Ahora como $a = p_1 \cdot ... \cdot p_s$ entonces $p_1 \mid a$ es decir $p_1 \mid u \cdot q_1 \cdot ... \cdot q_r$

Además p_1 es irreducible y A es $D.I.P.$ entonces p_1 es primo.

Por lo tanto $p_1 \mid q_j$, $\forall j = 1, n$, en particular $p_1 \mid q_1$, pues se puede renombrar los q_i.

Si $p_1 \mid q_1$ entonces existe $t_1 \in U(A)$ tal que $q_1 = p_1 \cdot t_1$, luego $p_1 \cdot ... \cdot p_s = u \cdot p_1 \cdot t_1 \cdot q_2 \cdot ... \cdot q_r$, es decir $p_1 \cdot ... \cdot p_s = p_1 \cdot u \cdot t_1 \cdot q_2 \cdot ... \cdot q_r$, pues A es un $D.I.P.$; luego aplicando $\cdot p$ por la izquierda obtenemos $p_2 \cdot ... \cdot p_s = u \cdot t_1 \cdot q_2 \cdot ... \cdot q_r$.

Razonar análogamente para $p_2 \mid q_2$ y así sucesivamente, obteniendo $p_r \cdot ... \cdot p_s = u \cdot t_1 \cdot ... \cdot q_r$.

Se tiene $p_{r+1} \cdot ... \cdot p_s = u \cdot t_1 \cdot ... \cdot t_r$, luego $u^{-1} \cdot t^{-1} \cdot ... \cdot t^{-1} \cdot (p_{r+1} \cdot ... \cdot p_s) = 1$

Por lo tanto $p_{r+1}, ..., p_s$ son invertibles ¡Contradicción!

En consecuencia $r = s$.

Proposición: Sea A un Dominio de Integridad entonces A es un dominio de factorización única $(D.F.U.)$ si $a \in A - \{0\}$, con $a \notin U(A)$ entonces:

1.- a es producto de elementos irreducibles.

2.- $a = p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$ con q_j, p_i irreducibles entonces $r = s$ y cada p_i es asociado a q_i.

Demostración:

Como A es un $D.I.P.$, por propiedad anterior se cumple 2).

Faltaría sólo probar 1), se tiene:

Sea $a \in A - \{0\}$ y $a \notin U(A)$, supongamos que existen a(es) que no son producto de irreducibles, sean ellos $a_1, ..., a_n, ... \in A$ y consideremos la cadena de ideales: $\langle a_1 \rangle \subset \langle a_2 \rangle \subset ... \subset \langle a_n \rangle \subset ...$

Se tiene que existe n tal que $\langle a_n \rangle = \langle a_{n+1} \rangle$ por ser A un $D.I.P.$, luego a_n no es irreducible, es decir existen b, $c \in A$ con b y c no unidades tal que $a_n = b \cdot c$, por lo tanto $\langle a_n \rangle \subset \langle b \rangle$, además $\langle a_n \rangle \subset \langle c \rangle$

Pero los elementos b y c no son del tipo de los a_i, luego ellos son producto de irreducibles y $b \cdot c$ también lo es, por lo tanto a_n es producto de irreducibles ¡Contradicción!

En consecuencia a es producto de elementos irreducibles.

Proposición: Si A es un $D.I.P.$ entonces A es un $D.F.U.$

Observación: $D.E. \Rightarrow D.I.P. \Rightarrow D.F.U.$

Proposición: Sea A un $D.F.U.$ si $p \in A$ es un elemento irreducible entonces p es primo.

Demostración:

Si $p \in A - \{0\}$ y $p \notin U(A)$ por demostrar $p \mid a \cdot b$ luego $p \mid a$ o $p \mid b$.

Si $p \mid a \cdot b$ entonces existe $t \in A$ tal que $a \cdot b = p \cdot t$, con $a, b \in A$

Como A es un $D.F.U.$ entonces existen p_i irreducibles tal que $a = p_1 \cdot ... \cdot p_r$, además existe q_j irreducibles tal que $b = q_1 \cdot ... \cdot q_s$, y también existe t_i irreducibles tal que $t = t_1 \cdot ... \cdot t_u$, luego $p_1 \cdot ... \cdot p_r \cdot q_1 \cdot ... \cdot q_s = p \cdot t_1 \cdot ... \cdot t_u$, por lo tanto p es asociado con algún $p_i, \forall i = \overline{1,n}$ o algún $q_j, \forall i = \overline{1,n}$.

Ahora si p es asociado con p_i entonces $p = u \cdot p_i$, con $u \in U(A), \forall i = \overline{1,n}$ y si p es asociado con q_j entonces $p = v \cdot q_j$, con $v \in U(A), \forall j = \overline{1,n}$.

Si $p = u \cdot p_i$ entonces $p_i = u^{-1} \cdot p$, por lo tanto $a = p_1 \cdot ... \cdot u^{-1} \cdot p \cdot ... \cdot p_r$ luego $p \mid a$.

Ahora si $p = v \cdot q_j$ entonces $q_j = v^{-1} \cdot p$, por lo tanto $b = q_1 \cdot ... \cdot v^{-1} \cdot p \cdot ... \cdot q_1$, en efecto $p \mid b$.

Proposición: Sea A un $D.I.P.$ la ecuación $a \cdot x + b \cdot y = c$, con $a, b, c \in A$, tiene solución en A si y solo si $mcd(a,b) \mid c$.

Si u, v son soluciones de la ecuación en A entonces el conjunto de las soluciones de ésta ecuación es:

$$\{a - b_1 \cdot s, v + a_1 \cdot s / s \in A \text{ y } a_1 \cdot mcd(a,b) = a \text{ y } b_1 \cdot mcd(a,b) = b\}$$

Demostración:

$\Rightarrow$]] Hipótesis: Sean u, v soluciones de la ecuación $a \cdot x + b \cdot y = c$ en A un $D.I.P.$.

Tesis: $mcd(a,b) \mid c$

Como se tiene que u, v son soluciones, se cumple que $a\cdot u+b\cdot v=c$, luego c pertenece al ideal generado por a y b, o sea $c\in\langle a,b\rangle$, como $c\in\langle a,b\rangle$, entonces $c\in\langle d\rangle$ donde $d=mcd(a,b)$, con A un *D.I.P.*

Luego si $c\in\langle d\rangle$ entonces existe $k\in A$ tal que $c=d\cdot k$, por lo tanto $d\,|\,c$.

$\Leftarrow$] Hipótesis $mcd(a,b)\,|\,c$, con $a,b,c\in A$ un *D.I.P.*

Tesis: Por demostrar que u, v son soluciones de la ecuación $a\cdot x+b\cdot y=c$

Si $d\,|\,c$, con $d=mcd(a,b)$ entonces existe $t_1\in A$ tal que $c=d\cdot t_1$, luego $c\in\langle d\rangle=\langle a,b\rangle$, por lo tanto si $c\in\langle a,b\rangle$ entonces $c=a\cdot u_1+b\cdot v_1$ con $u_1,v_1\in A$, en consecuencia u_1, v_1 son soluciones de la ecuación $a\cdot x+b\cdot y=c$.

Ejercicios

1.- Sea A un Dominio de Integridad , con p, q irreducibles en A. Pruebe que el conjunto de los asociados a p coincide con el conjunto de los asociados a q, sabiendo que la intersección de estos conjuntos es no vacío.

2.- Sea A un *D.E.*, luego tenemos $\eta: A-\{0\}\to\mathbb{Z}$, una función. Pruebe que si a y b son asociados entonces $\eta(a)=\eta(b)$.

3.- Sea A un *D.I.P.* Pruebe que todo ideal primo de A es maximal.

4.- Sea A un *D.I.P.*, pruebe que si $d=\langle a,b\rangle$ si y solo si $\langle a\rangle+\langle b\rangle=\langle d\rangle$.

Desarrollo:

1.- Sea A un Dominio de Integridad , con p, q irreducibles en A. Pruebe que el conjunto de los asociados a p coincide con el conjunto de los asociados a q, sabiendo que la intersección de estos conjuntos es no vacío.

Sean $A=\{\text{asociados a } p\}$ y $B=\{\text{asociados a } q\}$, con $A\cap B\neq\varnothing$ por demostrar que $A=B$.

Si $x\in A\cap B$ entonces $x\in A$ y $x\in B$

Ahora, si $x\in A$ entonces x es asociado a p, luego $x=u\cdot p$, con $u\in U(A)$.

Por otro lado si $x\in B$ entonces x es asociado a q, luego $x=v\cdot q$, con $v\in U(A)$.

De ambas condiciones se tiene:

$u\cdot p=v\cdot q$, aplicando $\cdot u$ por la izquierda obtenemos $p=u^{-1}\cdot v\cdot q$, con $u^{-1}\cdot v=w\in U(A)$.

En consecuencia $p=w\cdot q$, por lo tanto podemos decir que p es asociado a q y que q es asociado a p.

Ahora bien, si $y\in A$ entonces $y=u_1\cdot p=u_1\cdot w\cdot q$, con $u_1\in U(A)$.

Por lo tanto y es asociado a q, luego $y\in B$

Por otro lado si $z\in B$ entonces $z=u_2\cdot q=u_2\cdot w^{-1}\cdot p$, con $u_2\in U(A)$

Por lo tanto z es asociado a p, luego $z\in A$.

En consecuencia $A=B$

2.- Sea A un *D.E.*, luego tenemos $\eta: A-\{0\}\to\mathbb{Z}$, una función. Pruebe que si a y b son asociados entonces $\eta(a)=\eta(b)$.

Si a es asociado a b debemos demostrar que $\eta(a)=\eta(b)$.

Como a es asociado a b, entonces existe $u\in U(A)$ tal que $a=u\cdot b$, luego $\eta(a)=\eta(u\cdot b)\geq\eta(b)$.

De lo anterior podemos deducir que $b=u^{-1}\cdot a$

Ahora $\eta(b)=\eta\left(u^{-1}\cdot a\right)\geq\eta(a)$

Por lo tanto $\eta(a)=\eta(b)$.

3.- Sea A un *D.I.P.* Pruebe que todo ideal primo de A es maximal.

Sea I ideal primo de A entonces $I=\langle p\rangle$, debemos demostrar que si $I\subset M\subset A$ entonces $I=M$ o $M=A$ y además A/I es cuerpo.

Demostración:

Para todo $\overline{a}\neq\overline{0}$ perteneciente a A/I son invertibles.

Si $\overline{a}=a+\langle p\rangle\neq\overline{0}$ entonces $a\notin\langle p\rangle$

Como $a\notin\langle p\rangle$ el ideal $\langle a,\, p\rangle=\langle c\rangle$, con $c\in A$

Si $c=1$ o c es unidad entonces $\langle a,\, p\rangle=\langle 1\rangle=A$, es decir $a\cdot x+p\cdot s=1$, con $x,\ s\in A$, en efecto:

$$(a\cdot x+p\cdot s)+\langle p\rangle=1+\langle p\rangle$$

$$a\cdot x+\langle p\rangle+p\cdot s+\langle p\rangle=1+\langle p\rangle$$

$$a\cdot x+\langle p\rangle=1+\langle p\rangle$$

$$(a+\langle p\rangle)\cdot(x+\langle p\rangle)=1$$

Ahora debemos demostrar que $\langle c\rangle = A = \langle 1\rangle$.

Tenemos que $\langle a,\ p\rangle = \langle c\rangle$, luego:

a) Si $a \in \langle a,\ p\rangle$ entonces $a \in \langle c\rangle$ luego existe $t \in A$ tal que $a = t \cdot c$

b) Si $p \in \langle a,\ p\rangle$ entonces $p \in \langle c\rangle$ luego existe $r \in A$ tal que $p = r \cdot c$

Ahora $p \in \langle p\rangle$ por lo tanto $r \cdot c \in \langle p\rangle$ entonces $r \in \langle p\rangle$ o $c \in \langle p\rangle$, con $\langle p\rangle$ primo.

Si $r \in \langle p\rangle$ entonces $r = f \cdot p$, con $f \in A$, en b) se tiene que:

$p = f \cdot p \cdot c$ es decir $f \cdot c = 1$, luego $c \in U(A)$, y $\langle c\rangle \in A$

Si $c \in \langle p\rangle$ entonces $c = s \cdot p$, con $s \in A$, en a) se tiene que:

$a = t \cdot s \cdot p$ luego $a \in \langle p\rangle$ ¡Contradicción!

Ahora $p = r \cdot s \cdot p$, luego $r \cdot s = 1$, es decir r es unidad, por lo tanto p es asociado a c, en consecuencia $\langle p\rangle = \langle c\rangle$ ¡Contradicción!

4.- Sea A un $D.I.P.$, pruebe que si $d = \langle a, b\rangle$ si y solo si $\langle a\rangle + \langle b\rangle = \langle d\rangle$.

$\Leftarrow]$ Hipótesis: $\langle a\rangle + \langle b\rangle = \langle d\rangle$, con $a, b, d \in A$ un $D.I.P.$

Tesis: $d = mcd\{a, b\}$, es decir, debemos demostrar que:

i) $d \mid a$ y $d \mid b$

ii) Si existe un $c \in A$ tal que $c \mid a$ y $c \mid b$ entonces $c \mid d$.

Demostración:

i) Sea $a \in \langle a\rangle + \langle b\rangle = \langle d\rangle$ tenemos que $a = 1 \cdot a + 0 \cdot b$ luego $a \in \langle d\rangle$ entonces existe $t \in A$ tal que $a = t \cdot d$, por lo tanto $d \mid a$.

Por otro lado sea $b \in \langle a \rangle + \langle b \rangle = \langle d \rangle$ luego se tiene que $b = 0 \cdot a + 1 \cdot b$, en efecto $b \in \langle d \rangle$ entonces existe $s \in A$ tal que $b = s \cdot d$, por lo tanto $d \mid b$.

ii) a) Si $c \mid a$ entonces existe $r_1 \in A$ tal que $a = r_1 \cdot c$.

b) Si $c \mid b$ entonces existe $r_2 \in A$ tal que $b = r_2 \cdot c$.

Luego si $d \in \langle d \rangle = \langle a \rangle + \langle b \rangle$ y sustituyendo a) y b) obtenemos:

$$\begin{aligned} d &= m \cdot a + n \cdot b \\ &= m \cdot r_1 \cdot c + n \cdot r_2 \cdot c \\ &= (m \cdot r_1 + n \cdot r_2) \cdot c \ , \quad (m \cdot r_1 + n \cdot r_2) = r_3 \in A \\ &= r_3 \cdot c \end{aligned}$$

Por lo tanto $c \diagup d$

$\Rightarrow]\!]$ Hipótesis: $d = mcd\{a, b\}$, con $a, b, d \in A$ un $D.I.P.$

Tesis: $\langle a \rangle + \langle b \rangle = \langle d \rangle$.

Se tiene que $\langle a \rangle + \langle b \rangle = \langle c \rangle$ entonces se cumple que $c \mid a$ y $c \mid b$.

Luego c es un mcd y como d también lo es entonces son asociados, por lo tanto $c = u \cdot d$, con $u \in U(A)$, en consecuencia $\langle c \rangle = \langle d \rangle$.

Autoevaluación

1.- Sea A un $D.E.$, con $a \in U(A)$. Pruebe que:

a) $\eta(a \cdot b) = \eta(b)$, considerando $\eta : A - \{0\} \to \mathbb{Z}_0^+$

b) $\eta(a) = \eta(1)$

2.- Si m es un MCM entre a y b si y solo si $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$

3.- Si A es un $D.I.P.$ entonces p es primo si y solo si p es irreducible.

4.- Todo asociado a un irreducible es un irreducible.

5.- Sea A un Dominio de Integridad, con p, q irreducibles

Si $A_q = \{r \in A / r$ es asociado a $q\}$

$B_p = \{s \in A / s$ es asociado a $p\}$

Pruebe $A_q = B_p$ sabiendo que $A_q \cap B_p \neq \varnothing$

6.- Sea A un $D.I.P.$ Pruebe que todo ideal primo de A es maximal.