Módulo11:

CUERPO DE LOS CUOCIENTES

En este módulo veremos propiedades fundamentales de ideales de anillos, definiendo algunos de ellos con sus características principales. Cabe destacar la construcción del cuerpo de los cuocientes de un dominio de integridad, siendo esta construcción una de las extensiones a cuerpo más usuales que se puede abstraer de un dominio.

Definición 1: Sea A un anillo y J un ideal de A. Diremos que J es un ideal principal de A si J es un ideal generado por un único elemento $a \in A$.

Notación: "J es un ideal generado por el elemento a", será anotado por $J = \langle a \rangle$

Ejemplo 1:

Sea $A = \mathbb{Z}_{12}$ un anillo y $N = \langle \bar{2} \rangle$ y $J = \langle \bar{3} \rangle$ tal que $N, J \lhd A$. N y J son ideales principales de A pues son generados por únicos elementos respectivamente.

Definición 2: Sea A un anillo y M un ideal propio de A (es decir $M \neq A$). Diremos que M es un ideal maximal de A si $M \subset I \subset A$ entonces $M = I$ ó $I = A$, donde $I \lhd A$.

Ejemplo 2:

$3\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$, donde $3\mathbb{Z} = \{r / r = 3 \cdot t, \ t \in \mathbb{Z}\}$.

Demostración

i) Sea I un ideal de $\mathbb{Z}$ tal que $3\mathbb{Z} \subset I \subset \mathbb{Z}$, por demostrar que $3\mathbb{Z} = I$ ó $I = \mathbb{Z}$

Como $I = n\mathbb{Z}$ y $3\mathbb{Z} \subset n\mathbb{Z}$, debemos probar que $I = \mathbb{Z}$. Ahora bien, sabemos que $3 \in 3\mathbb{Z}$, luego $3 \in n\mathbb{Z}$ por hipótesis. Si $3 \in n\mathbb{Z}$, entonces $3 = n \cdot t$ para algún $t \in \mathbb{Z}$. De lo anterior, diremos que n divide a 3, de esta forma por la Teoría de Números, se tiene que $n = \pm 1$ ó $n = \pm 3$. Luego si $n = \pm 1$, entonces $I = n\mathbb{Z} = \mathbb{Z}$ o si $n = \pm 3$, entonces $I = 3\mathbb{Z}$

Por lo tanto $3\mathbb{Z}$ es ideal maximal de $\mathbb{Z}$.

Notación: Si "a divide a b" lo anotaremos como $a \mid b$

Definición 3: Sea A un anillo y P un ideal propio de A. Diremos que P es un ideal primo de A si $a \cdot b \in P$ entonces $a \in P$ ó $b \in P$.

Ejemplo 3:

$3\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$.

En Efecto:

Si $a \cdot b \in 3\mathbb{Z}$, por demostrar que $a \in 3\mathbb{Z}$ ó $b \in 3\mathbb{Z}$

Si $a \cdot b \in 3\mathbb{Z}$, entonces $a \cdot b = 3 \cdot t \quad ; t \in \mathbb{Z}$. Luego $3 | a \cdot b$, lo que implicará que $3 | a$ ó $3 | b$

Si $3 | a$ entonces $a = 3s$; para algún $s \in \mathbb{Z}$, luego evidentemente $a \in 3\mathbb{Z}$.

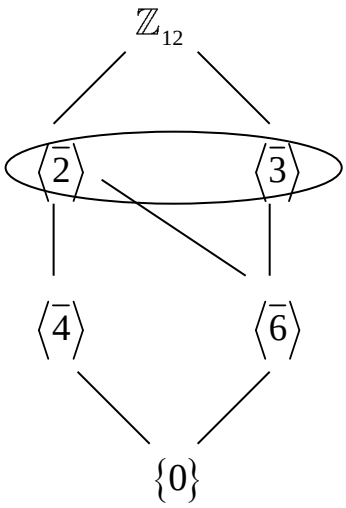
Análogamente, si $3 | b$ entonces $b = 3r$; para algún $r \in \mathbb{Z}$, de esta manera $b \in 3\mathbb{Z}$. Por lo tanto $3\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$.

Observación: Todo ideal maximal en un anillo conmutativo con identidad es un ideal primo.

Ejemplo 4:

Encontrar todos los ideales primos e ideales maximales de $\mathbb{Z}_{12}$.

Sea el conjunto $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$, determinaremos los ideales maximales de $\mathbb{Z}_{12}$ a través de la red de ideales.



Luego los ideales maximales de $\mathbb{Z}_{12}$ son $\langle\overline{2}\rangle$ y $\langle\overline{3}\rangle$. Ahora, los ideales primos de $\mathbb{Z}_{12}$ son $\langle\overline{2}\rangle$ y $\langle\overline{3}\rangle$, ya que si $a \cdot b \in \langle\overline{2}\rangle$ entonces $a \in \langle\overline{2}\rangle$ o $b \in \langle\overline{2}\rangle$. De igual manera si $a \cdot b \in \langle\overline{3}\rangle$ entonces $a \in \langle\overline{3}\rangle$ o $b \in \langle\overline{3}\rangle$.

Por lo tanto los ideales maximales de $\mathbb{Z}_{12}$ son ideales primos del mismo.

Proposición: Sea A un anillo conmutativo con identidad, entonces:

1) P es un ideal primo de A si y sólo si A/P es un Dominio de Integridad.
2) M es un ideal maximal de A si y sólo si A/M es cuerpo.

Demostración:

1) $\Rightarrow$] Hipótesis: P es un ideal primo de A

Tesis: A/P es un Dominio de Integridad.

Bastaría demostrar que A/P es un anillo con identidad y sin divisores de cero.

i) Por ver que A/P es un anillo con identidad

Debe existir un $(x+P)\in A/P$, para todo $(a+P)\in A/P$ tal que

$(a+P)\cdot(x+P)=(x+P)\cdot(a+P)=(a+P)$

Consideremos $(a+P)\cdot(x+P)=(a+P)$

Entonces $a\cdot x+P=a+P$

Luego, $x=1$

Por lo tanto la identidad de A/P es $(1+P)$

ii) Ahora verificaremos que A/P es sin divisores de cero

David Hilbert (1862–1943)

Se trata del matemático más famoso del siglo XX. Amigo íntimo de Dedekind, con quien publicó en 1882 un célebre trabajo sobre curvas algebraicas, ofreciendo una fundamentación al modo de la **teoría de ideales** en cuerpos de números, que abría el camino hacia la geometría algebraica del mismo siglo . La influencia de Weber, y a través de él la tradición de Gauss, Riemann y Dedekind, sería decisiva para Hilbert.
Realiza profundos resultados en álgebra, teoría de números, geometría y teoría de funciones y las venturas y desventuras de sus intentos de resolver la cuestión de los fundamentos de la matemática. En el año de su muerte, se le celebraba como aquel "a quien el mundo consideró durante las últimas décadas como el más grande matemático vivo".

Sea $(a+P),\ (b+P)\in A/P$ y $(0+P)$ neutro de A/P tal que $(a+P)\cdot(b+P)=0+P$, debemos demostrar que $(a+P)=0+P$ ó $(b+P)=0+P$

Si $(a+P)\cdot(b+P)=0+P$

$$\Rightarrow a\cdot b+P=0+P$$
$$\Rightarrow (a\cdot b-0)\in P$$
$$\Rightarrow a\cdot b\in P$$

Luego por hipótesis (P es ideal primo) $a\in P$ ó $b\in P$,

Como $a\in P$ entonces $a+P=P$

O bien, $b\in P$ entonces $b+P=P$

En consecuencia A/P es sin divisores de cero.

Por lo tanto de i) y ii) A/P es un Dominio de Integridad cuando P es un ideal primo de A

$\Leftarrow]]$ Hipótesis: A/P es un Dominio de Integridad.

Tesis: P es un ideal primo de A, es decir, si $a\cdot b\in P$ debemos demostrar que $a\in P$ o $b\in P$.

Si $a\cdot b\in P\Rightarrow a\cdot b+P=P\Rightarrow (a+P)\cdot(b+P)=P$.

Luego, $a+P=P$ por ser A/P sin divisores de cero, por lo tanto $a\in P$

Ahora, por otro lado se tiene que $b+P=P$, por lo tanto $b\in P$.

En consecuencia P es un ideal primo de A cuando A/P es un Dominio de Integridad.

Por lo tanto P es un ideal primo de A si y sólo si A/P es un Dominio de Integridad.

$2) \Rightarrow]\!]$ Hipótesis: M es un ideal maximal de A.

Tesis: A/M es cuerpo. Debemos demostrar que todos los elementos de A/M salvo el $0_{A/M}$ sean invertibles.

Sea $(a+M) \in A/M$ con $(a+M) \neq 0_{A/M} = M$, es decir $a \notin M$, debemos encontrar $(b+M) \in A/M$ tal que $(a+M)\cdot(b+M) = 1+M$.

Consideremos $I = \langle M, a \rangle = \{ m + c \cdot a \,/\, m \in M,\ a \in (A-M),\ c \in A \}$, debemos verificar que $I \lhd A$.

En efecto,

i) Claramente $I \subset A$, además $I \neq \varnothing$ pues $0_A \in I$

ii) Dados $(m_1 + c_1 \cdot a),\ (m_2 + c_2 \cdot a) \in I$, por demostrar que $(m_1 + c_1 \cdot a) - (m_2 + c_2 \cdot a) \in I$

Se tiene que $(m_1 + c_1 \cdot a) \in I$ tal que $m_1 \in M,\ a \in (A-M),\ c_1 \in A$

Además, $(m_2 + c_2 \cdot a) \in I$ tal que $m_2 \in M,\ a \in (A-M),\ c_2 \in A$

Ahora bien,

$(m_1 + c_1 \cdot a) - (m_2 + c_2 \cdot a) = (m_1 - m_2) + (c_1 - c_2)\cdot a$, con y $c_1 - c_2 = c \in A$

Por lo tanto $(m_1 + c_1 \cdot a) - (m_2 + c_2 \cdot a) = (m + c \cdot a) \in I$.

iii) Dados $b \in A,\ (m + c \cdot a) \in I$ por demostrar $\begin{cases} \text{a)}\ b \cdot (m + c \cdot a) \in I \\ \text{b)}\ (m + c \cdot a) \cdot b \in I \end{cases}$

Ahora bien,

a) $b \cdot (m + c \cdot a) = b \cdot m + b \cdot c \cdot a$, con $b \cdot m = m' \in M$ y $b \cdot c = c' \in A$

Por lo tanto $b \cdot (m + c \cdot a) = (m' + c' \cdot a) \in I$

Por otro lado se tiene

b) $(m+c\cdot a)\cdot b = m\cdot b + c\cdot a\cdot b$

$= m\cdot b + c\cdot b\cdot a$, por ser A un anillo conmutativo

Consideremos $m\cdot b = m' \in I$ y $c\cdot b = c' \in I$

Por lo tanto $(m+c\cdot a)\cdot b = (m'+c'\cdot a) \in I$

En consecuencia de i), ii) y iii) $I \lhd A$

Además, como M ideal maximal A se tiene de $M \subset \langle M, a\rangle \subset A$, $m_1 = m_1 + 0\cdot a$

Por lo tanto podemos asegurar que $\langle M,\ a\rangle = A$

Como A es un anillo con identidad, si $1 \in A$ entones $1 \in \langle M, a\rangle$

Luego $1 = m + c\cdot a$, con $m \in M$, $c \in A$

Entonces $1 + M = (m + c\cdot a) + M$

Entonces $1 + M = c\cdot a + M$

En consecuencia $1 + M = (c + M)\cdot(a + M)$

Luego, el inverso $(a+M)$ es $(c+M)$, por lo que podemos afirmar que todos los elementos de A/M salvo el 0 son invertibles.

Por lo tanto A/M es cuerpo.

$\Leftarrow]$ Hipótesis: A/M es cuerpo.

Tesis: M es un ideal maximal de A, es decir, debemos demostrar que si $M \subset I \subset A$ entonces $M = I$ ó $I = A$.

Si $M = I$, supongamos que $M \subset I$, luego debemos demostrar que $I = A$

Como $M \subset I$ entonces existe $a \in I$ tal que $a \notin M$

$a + M \neq M$, como A/M es cuerpo entonces existe $(b+M) \in A/M$ tal que

$$(a+M)\cdot(b+M)=1+M$$

$$\Rightarrow a\cdot b+M=1+M$$

$$\Rightarrow a\cdot b-1\in M$$

Luego, $a\cdot b-1=m$, $\forall\, m\in M$.

pero $a\cdot b\in I$, ya que $a\in I$ y $m\in I$ pues $M\subset I$.

Por lo tanto $a\cdot b-m\in I$ entonces $1\in I$

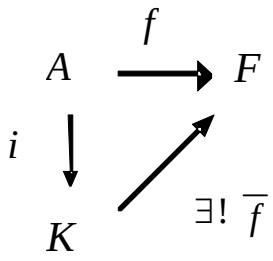
Luego $I=A$

En consecuencia M es maximal de A cuando A/M es cuerpo.

Por lo tanto M es un ideal maximal de A si y sólo si A/M es cuerpo.

Teorema

Sea A un Dominio de Integridad, podemos construir un cuerpo K y un homomorfismo $i:A\longrightarrow K$, tal que si F es otro cuerpo y $f:A\longrightarrow F$ un homomorfismo, entonces existe una única función $\overline{f}:F\longrightarrow$ K tal que $\overline{f}\circ i=f$



La solución de este problema universal se llama el *Cuerpo de los Cuocientes de* A.

Demostración

Primero se construirá K a partir de un dominio A, dotándole a K una estructura de cuerpo, para luego definir la función i como un homomorfismo de A en K.

1) Construiremos K a partir de un dominio A.

En $A\times\left(A-\{0\}\right)$ se define la siguiente relación $(a_1,b_1)\sim(a_2,b_2)\Leftrightarrow a_1\cdot b_2=b_1\cdot a_2$; donde $a_1,a_2,b_1,b_2\in A$.

Diremos que la relación $\sim$ es una relación de equivalencia, pues cumple las propiedades de ser refleja, simétrica y transitiva, en efecto:

i) $\sim$ es una relación refleja

Para todo $(a,b)\in A$, se debe cumplir que $(a,b)\sim(a,b)$.

En efecto, $(a,b)\sim(a,b)\Leftrightarrow a\cdot b=b\cdot a$, con $a,b\in A$dominio de integridad, lo cual en particular verifica que $(A,\cdot)$ es conmutativo.

Por lo tanto la relación $\sim$ es refleja.

ii) $\sim$ es una relación simétrica

Para todo $(a,b),(c,d)$ que pertenece a $A\times\left(A-\{0\}\right)$. Si $(a,b)\sim(c,d)$, entonces $(c,d)\sim(a,b)$.

En efecto, $(a,b)\sim(c,d)\Leftrightarrow a\cdot d=b\cdot c$

$\Leftrightarrow b\cdot c=a\cdot d$, por la simetría de la igualdad

$\Leftrightarrow c\cdot b=d\cdot a$, por conmutatividad en $(A,\cdot)$

$\Leftrightarrow(c,d)\sim(a,b)$

Por lo tanto la relación $\sim$ es simétrica.

iii) $\sim$ es una relación transitiva

Para todo $(a,b),(c,d),(e,f)$ que pertenece a $A\times\left(A-\{0\}\right)$. Si $(a,b)\sim(c,d)$ y $(c,d)\sim(e,f)$, entonces $(a,b)\sim(e,f)$.

Es evidente que $(a,b)\sim(c,d)\Leftrightarrow a\cdot d=b\cdot c$.

Además, $(c,d)\sim(e,f)\Leftrightarrow c\cdot f=d\cdot e$

Luego operando ambas igualdades, se tiene $a\cdot d\cdot c\cdot f=b\cdot c\cdot d\cdot e$, cancelando $d\cdot c$ en Adominio de integridad, tenemos $a\cdot f=b\cdot e$, obteniendo como consecuencia que $(a,b)\sim(e,f)$. Por lo tanto $\sim$ es una relación transitiva.

Luego, de (i), (ii) y (iii) se puede verificar claramente que $\sim$ es una relación de equivalencia.

Considerando $\sim$ una relación de equivalencia, ésta particionará al conjunto $A\times\left(A-\{0\}\right)$ en clases de equivalencia respecto a la relación, definiendo a K de la siguiente manera:

$$K:=\left.A\times\left(A-\{0\}\right)\right/_{\sim}$$

Donde los elementos de este conjunto son todas las clases de equivalencia $\overline{(a,b)}=\overline{\left(\frac{a}{b}\right)}$, donde $a\in A$ y $b\in\left(A-\{0\}\right)$.

2) Dotaremos a K de estructura de cuerpo, definiendo las operaciones suma como siguen:

(Suma) $+:K\times K\to K$

$$\left(\overline{(a,b)},\overline{(c,d)}\right)\mapsto\overline{(a,b)}+\overline{(c,d)}=\overline{(a\cdot d+b\cdot c,b\cdot d)}$$

La operación (+) está bien definida en K, pues si consideramos

$\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right)=\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)$,con $\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right),\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)\in K\times K$,

tendremos que $\left(\overline{a\cdot d+b\cdot c,b\cdot d}\right)=\left(\overline{m\cdot v+n\cdot u,n\cdot v}\right)$, con $\left(\overline{a\cdot d+b\cdot c,b\cdot d}\right),\left(\overline{m\cdot v+n\cdot u,n\cdot v}\right)\in K$.

Si $\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right)=\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)$, con $\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right),\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)\in K\times K$,

entonces tenemos que:

$\left(\overline{a,b}\right)=\left(\overline{m,n}\right)$ y a su vez $\left(\overline{c,d}\right)=\left(\overline{u,v}\right)$, lo que implica que

$(a,b)\sim(m,n)$ y $(c,d)\sim(u,v)$, lo que significa por la relación que

(i) $a\cdot n=b\cdot m$ y (ii) $c\cdot v=d\cdot u$

Luego, multiplicando la expresión en (i) por $d\cdot v$ y en (ii) por $b\cdot n$ tenemos que

$a\cdot n\cdot d\cdot v=b\cdot m\cdot d\cdot v$ y $c\cdot v\cdot b\cdot n=d\cdot u\cdot b\cdot n$

Ahora sumando ambas expresiones obtenemos

$a\cdot n\cdot d\cdot v+c\cdot v\cdot b\cdot n=b\cdot m\cdot d\cdot v+d\cdot u\cdot b\cdot n$; por ser A un dominio de integridad se cumple

$a\cdot d\cdot n\cdot v+b\cdot c\cdot n\cdot v=b\cdot d\cdot m\cdot v+b\cdot d\cdot n\cdot u$; por distributividad en A

$(a\cdot d+b\cdot c)\cdot n\cdot v=b\cdot d\cdot(m\cdot v+n\cdot u)$; por definición de $\sim$

$(a\cdot d+b\cdot c,b\cdot d)\sim(m\cdot v+n\cdot u,n\cdot v)$, lo que implica

$\left(\overline{a\cdot d+b\cdot c,b\cdot d}\right)=\left(\overline{m\cdot v+n\cdot u,n\cdot v}\right)$

Es evidente demostrar que $(K,+)$es un Grupo Abeliano, pues cumple con las propiedades de conmutatividad, asociatividad, elemento neutro y elemento inverso.

i) $(K,+)$ es conmutativo:

Para todo $\left(\overline{a,b}\right),\left(\overline{c,d}\right)\in K$, se tiene que $\left(\overline{a,b}\right)+\left(\overline{c,d}\right)=\left(\overline{c,d}\right)+\left(\overline{a,b}\right)$, con $a,b,c,d\in A$ dominio de integridad.

En efecto, resulta evidente que si $\left(\overline{a,b}\right)+\left(\overline{c,d}\right)=\left(\overline{a\cdot d+b\cdot c,b\cdot d}\right)$; por conmutatividad de $(A,\cdot)$ en A

$$=\left(\overline{d\cdot a+c\cdot b,d\cdot b}\right);\text{ por conmutatividad de }(A,+)\text{ en }A$$

$$=\left(\overline{c\cdot b+d\cdot a,d\cdot b}\right);\text{ por definición de }+\text{ en }K$$

$$=\left(\overline{c,d}\right)+\left(\overline{a,b}\right)$$

Por lo tanto $(K,+)$ es un conmutativo.

ii) $(K,+)$ es asociativo:

Para todo $\left(\overline{a,b}\right),\left(\overline{c,d}\right),\left(\overline{e,f}\right)\in K$, se tiene que $\left(\overline{a,b}\right)+\left[\left(\overline{c,d}\right)+\left(\overline{e,f}\right)\right]=\left[\left(\overline{c,d}\right)+\left(\overline{a,b}\right)\right]+\left(\overline{e,f}\right)$, con $a,b,c,d\in A$ dominio de integridad. En efecto, por definición de $+$ en K y propiedades en A, se tiene:

$$\left(\overline{a,b}\right)+\left[\left(\overline{c,d}\right)+\left(\overline{e,f}\right)\right]=\left(\overline{a,b}\right)+\left(\overline{c\cdot f+d\cdot e,d\cdot f}\right)$$

$$=\left(\overline{a\cdot d\cdot f+b\cdot(c\cdot f+d\cdot e),b\cdot d\cdot f}\right)$$

$$=\left(\overline{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e,b\cdot d\cdot f}\right)$$

$$=\left(\overline{(a\cdot d+b\cdot c)\cdot f+b\cdot d\cdot e,b\cdot d\cdot f}\right)$$

$$=\left(\overline{a\cdot d+b\cdot c,b\cdot d}\right)+\left(\overline{e,f}\right)$$

$$=\left[\left(\overline{a,b}\right)+\left(\overline{c,d}\right)\right]+\left(\overline{e,f}\right)$$

Por lo tanto $(K,+)$ es asociativo.

iii) $(K,+)$ tiene elemento neutro:

Existe un único elemento $(\overline{x,y})\in K$, tal que $(\overline{a,b})+(\overline{x,y})=(\overline{a,b})=(\overline{x,y})+(\overline{a,b})$ para todo $(\overline{a,b})\in K$.

Supongamos que $(\overline{a,b})+(\overline{x,y})=(\overline{a,b})$, luego por la igualdad de clases y por la definición de la relación $\sim$ se tiene:

$(\overline{a\cdot y+b\cdot x,b\cdot y})=(\overline{a,b})$, lo que implica $(a\cdot y+b\cdot x,b\cdot y)\sim(a,b)$, luego $(a\cdot y+b\cdot x)\cdot b=b\cdot y\cdot a$, es decir $a\cdot b\cdot y+b^2\cdot x=a\cdot b\cdot y$.

Esto se cumplirá siempre que $y\in A-\{0\}$ y $x=0$.

De manera similar se verifica por la izquierda. Por lo tanto $(K,+)$ tiene elemento neutro, y es $(\overline{0,y})$.

iv) $(K,+)$ tiene elemento inverso

Para todo $(\overline{a,b})\in K$, existe un único $(\overline{u,v})\in K$, tal que $(\overline{a,b})+(\overline{u,v})=(\overline{0,y})=(\overline{u,v})+(\overline{a,b})$.

Supongamos que $(\overline{a,b})+(\overline{u,v})=(\overline{0,y})$, luego por la igualdad de clases y por la definición de la relación $\sim$ se tiene:

$(\overline{a\cdot v+b\cdot u,b\cdot v})=(\overline{0,y})$, lo que implica $(a\cdot v+b\cdot u,b\cdot v)\sim(0,y)$, luego $(a\cdot v+b\cdot u)y=b\cdot v\cdot 0$, es decir $(a\cdot v+b\cdot u)y=0$; como $y\in A-\{0\}$ y A dominio de integridad, se tiene $a\cdot v+b\cdot u=0$. Esta igualdad se verifica siempre que $(v=b\ \wedge\ u=-a)\vee(v=-b\ \wedge\ u=a)$.

Notar que la expresión también se verifica por la izquierda.

En consecuencia el inverso aditivo de $\left(\overline{a,b}\right)\in K$ será $\left(\overline{-a,b}\right)\in K$.

Cabe agregar que $\left(\overline{-a,b}\right)=\left(\overline{a,-b}\right)=-\left(\overline{a,b}\right)$.

De (i), (ii), (iii) y (iv) diremos que $\left(K,+\right)$ es un Grupo Abeliano.

Ahora es evidente demostrar que $\left(K,\cdot\right)$ es un Grupo Abeliano, es decir, que cumple las propiedades de conmutatividad, asociatividad, elemento neutro y elemento inverso con respecto a la operación producto que se define.

(Producto) $\cdot: K\times K\to K$

$$\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right)\mapsto\left(\overline{a,b}\right)\cdot\left(\overline{c,d}\right)=\left(\overline{a\cdot c,b\cdot d}\right)=\left(\overline{\frac{a\cdot c}{b\cdot d}}\right)$$

Es claro que esta operación está bien definida en el conjunto K, como se muestra a continuación:

Si para todo $\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right),\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)\in K\times K$ se verifica $\left(\left(\overline{a,b}\right),\left(\overline{c,d}\right)\right)=\left(\left(\overline{m,n}\right),\left(\overline{u,v}\right)\right)$ entonces $\left(\overline{a,b}\right)=\left(\overline{m,n}\right)$ y $\left(\overline{c,d}\right)=\left(\overline{u,v}\right)$, lo que implica $\left(a,b\right)\sim\left(m,n\right)$ y $\left(c,d\right)\sim\left(u,v\right)$, de aquí (i) $a\cdot n=b\cdot m$ y (ii) $c\cdot v=d\cdot u$.

Multiplicando (i) y (ii) se tiene $a\cdot n\cdot c\cdot v=b\cdot m\cdot d\cdot u$, luego por asociatividad y conmutatividad en el dominio de integridad A tenemos: $\left(a\cdot c\right)\cdot\left(n\cdot v\right)=\left(b\cdot d\right)\cdot\left(m\cdot u\right)$. De acuerdo a la relación $\sim$, tenemos $\left(a\cdot c\right)\cdot\left(b\cdot d\right)\sim\left(n\cdot v\right)\cdot\left(m\cdot u\right)$, lo que implica que $\left(\overline{a\cdot c,b\cdot d}\right)=\left(\overline{n\cdot v,m\cdot u}\right)$. En consecuencia, $\left(\overline{a\cdot c}\right)\cdot\left(\overline{b\cdot d}\right)=\left(\overline{n\cdot v}\right)\cdot\left(\overline{m\cdot u}\right)$,

De lo anterior, diremos que la operación producto está bien definida en K.

Ahora dejaremos como ejercicio al lector demostrar que se verifica la conmutatividad y asociatividad respecto de $\cdot$ en K.

Así también afirmamos que el neutro es la clase $\left(\overline{x,x}\right)\in K$ para todo $x\in A$ y el inverso multiplicativo de la clase $\left(\overline{x,y}\right)\in K-\{0\}$ es la clase $\left(\overline{y,x}\right)\in K$. También es fácil probar la distributividad de $\cdot$ con respecto a la $+$ en K, y con ello dotamos a $\left(K,+_K,\cdot_K\right)$ de estructura de cuerpo.

3) Definiremos la función i como un homomorfismo de A en K tal que para todo $a\in A$, $i(a)=\left(\overline{a,1}\right)=\frac{a}{1}$.

La función i, conocida como función inmersión, está bien definida, es decir para todo $n,m\in A$ si $n=m$ se cumple que $i(n)=i(m)$.

Supongamos que $n=m$; luego operando $\cdot 1_A$ por la izquierda, además por igualdad de clases, y por la definición de la relación $\sim$ se tiene:

$n\cdot 1=m\cdot 1$, luego, $(n,1)\sim(m,1)$, lo que implica $\left(\overline{n\cdot 1}\right)=\left(\overline{m\cdot 1}\right)$, ahora por definición la función i, se tiene que $i(n)=i(m)$.

Por lo tanto la función inmersión i está bien definida, de A sobre K

Ahora bien, es claro ver que la función i es un homomorfismo, pues verifica las siguientes condiciones:

(i) $i(a+_A b)=i(a)+_K i(b)$, con $a,b\in A$.

En efecto, $i\left(a+_A b\right)=\left(\overline{a+_A b,1}\right)=\left(\overline{a+_A b,1\cdot_A 1}\right)=\left(\overline{a\cdot 1+_A 1\cdot b,1\cdot_A 1}\right)$

$$=\left(\overline{a,1}\right)+_K\left(\overline{b,1}\right)=i(a)+_K i(b)$$

Por lo tanto $i(a+_A b)=i(a)+_K i(b)$

(ii) $i(a\cdot_A b)=i(a)\cdot_K i(b)$, con $a,b\in A$

En efecto, $i\left(a\cdot_A b\right)=\left(\overline{a\cdot_A b,1}\right)=\left(\overline{a\cdot_A b,1\cdot_A 1}\right)=\left(\overline{a,1}\right)\cdot_K\left(\overline{b,1}\right)$

$$=i\left(a\right)\cdot_K i\left(b\right)$$

Por lo tanto $i(a\cdot_A b)=i(a)\cdot_K i(b)$.

Luego la función inmersión i es un homomorfismo de A sobre K.

Ahora bien, dado el homomorfismo $f:A\to F$ tal que para todo $a\in A$, $f(a)\in F$, debemos encontrar una función $\overline{f}$ de K en F que sea un homomorfismo, de tal manera que $\overline{f}\circ i=f$.

Ahora, si definimos la función $\overline{f}$ con dominio en K y valores en F tal que para todo $\left(\overline{a,b}\right)\in K$, $\overline{f}\left(\overline{a,b}\right)=\dfrac{f\left(a\right)}{f\left(b\right)}$ con $f\left(b\right)\neq 0_F$, es claro probar que $\overline{f}$ es un homomorfismo. Para ello demostraremos que:

i) $\overline{f}$ está bien definida.

En efecto, si $\left(\overline{p,q}\right)=\left(\overline{u,v}\right)$ entonces $\left(p,q\right)\sim\left(u,v\right)$, esto implica que por la relación $\sim$, $p\cdot v=q\cdot u$, aplicando f, que es un homomorfismo, tenemos $f\left(p\cdot v\right)=f\left(q\cdot u\right)=f\left(p\right)\cdot f\left(v\right)=f\left(q\right)\cdot f\left(u\right)$, ahora como F es un cuerpo, $\dfrac{f\left(p\right)}{f\left(q\right)}=\dfrac{f\left(u\right)}{f\left(v\right)}$, y por definición de $\overline{f}$ se tiene que $\overline{f}\left(\overline{p,q}\right)=\overline{f}\left(\overline{u,v}\right)$. Por lo tanto $\overline{f}$ está bien definida de K en F.

ii) $\overline{f}$ es un homomorfismo

En efecto, con $\alpha, \beta \in K$ y por ser f es un homomorfismo se tiene:

a) $\overline{f}\left(\alpha +_K \beta\right) = \overline{f}\left(\overline{(a,1)} + \overline{(b,1)}\right) = \overline{f}\left(\overline{(a\cdot 1 + 1\cdot b, 1\cdot 1)}\right) = \overline{f}\left(\overline{(a+b,1)}\right) =$

$\dfrac{f(a+b)}{f(1)} = \dfrac{f(a)}{f(1)} + \dfrac{f(b)}{f(1)} = \overline{f}\,\overline{(a,1)} + \overline{f}\,\overline{(b,1)} = \overline{f}(\alpha) + \overline{f}(\beta)$. También,

b) $\overline{f}\left(\alpha \cdot \beta\right) = \overline{f}\left(\overline{(a,1)} \cdot \overline{(b,1)}\right) = \overline{f}\left(\overline{(a\cdot b, 1\cdot 1)}\right) = \overline{f}\left(\overline{(a\cdot b,1)}\right) = \dfrac{f(a\cdot b)}{f(1)}$

$= \dfrac{f(a)}{f(1)} \cdot \dfrac{f(b)}{f(1)} = \overline{f}\,\overline{(a,1)} \cdot \overline{f}\,\overline{(b,1)} = \overline{f}(\alpha) \cdot \overline{f}(\beta)$

Por lo tanto, de (a) y (b) tenemos que la función $\overline{f}$ de K en F es un homomorfismo.

iii) Se verifica unicidad de $\overline{f}$ y $\overline{f} \circ i = f$, quedando éstas de ejercicio para el lector.

Teorema: Sea A un anillo conmutativo con identidad entonces existe M ideal maximal de A.

Demostración:

Sea $F = \{I_i / I_i \lhd A, i \in \mathbb{N}\} \neq A$ con F no vacío, puesto que $0 \in F$. Al ordenar F por inclusión de conjuntos, se tiene que $I_1 \subseteq I_2 \subseteq ... \subseteq I_i$, con $i \in \mathbb{N}$. Es claro que existe un $M = \bigcup_{i=1}^{n} I_i$ que es una cota superior de toda la cadena de ideales de A anillo, de acuerdo al Lema de Zorn. Luego $1 \notin I_i$ con $i \in \mathbb{N}$, por proposición de capítulo 1 (página X).

Por lo tanto $M = \bigcup_{i=1}^{n} I_i$ es un ideal maximal de A anillo.

Definición 4: Diremos que A es un anillo local si y sólo si posee un único ideal maximal.

Proposición: Sea A anillo conmutativo con identidad, se tiene que A es local y M su ideal maximal si y sólo si $U(A) = A - M$.

Demostración:

$\Rightarrow$] i) Sea $x \in U(A)$, entonces x es una unidad (invertible), con lo cual $x \notin M$, luego $x \in A - M$. Esto prueba que $U(A) \subseteq A - M$.

ii) Supongamos que $x \notin U(A)$, entonces x no es invertible, lo que implica que $x \in I$, con I ideal propio de A. Luego, como $I \subset M$ por ser M un ideal maximal, entonces $x \in M$, lo que implica que $x \notin A - M$. Por lo tanto $U(A) \subseteq A - M$.

$\Leftarrow$] i) Por verificar que M es maximal, es decir debe existir un $I \lhd A$ tal que $M \subset I \subset A$, lo que implicará que $M = I$ ó $I = A$.

Supongamos $M \subset I$, con $M \neq I$, por demostrar que $I = A$.

Si $M \subset I$ entonces existe un $y \in I$ tal que $y \notin M$, lo cual es evidente que $y \in A - M$, lo cual por hipótesis $y \in U(A)$. Luego como $y \in U(A)$ e $y \in I$, resulta evidente que $I = A$.

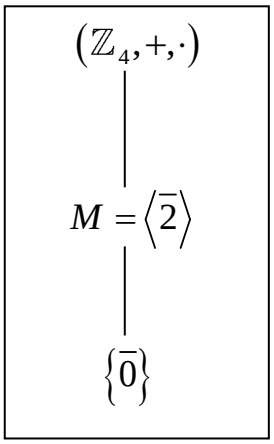
ii) Por verificar que M ideal maximal es único en el anillo A.

Sea N ideal maximal de A, entonces $U(A) = A - N$, lo que implica que $N \subseteq A - U(A)$, con $N \subseteq M$, pero como N es ideal maximal, es claro que $N = M$.

Luego de (i) y (ii), tenemos que M es un ideal maximal y es único.
Por lo tanto, de lo anterior, podemos decir que A es local y M su ideal maximal si y sólo si $U(A) = A - M$.

Ejemplo 7:

Consideremos el anillo $(\mathbb{Z}_4, +_{\text{mod}\,4}, \cdot_{\text{mod}\,4})$ conmutativo con identidad. Verificar que $(\mathbb{Z}_4, +_{\text{mod}\,4}, \cdot_{\text{mod}\,4})$ es un anillo local. Sea $M = \langle \bar{2} \rangle$, de tal manera que $U(\mathbb{Z}_4) = \mathbb{Z}_4 - M = \{\bar{1}, \bar{3}\}$. Podemos establecer una red de ideales, donde es evidente que $M = \langle \bar{2} \rangle$ es ideal maximal y es único.



|OPERACIONES CON IDEALES

Definición 5: Sea A un anillo y I, $J \lhd A$, se define:

a) $I + J = \{a + b / a \in I,\ b \in J\} \lhd A$, es el menor ideal que contiene a ambos ideales I y J.

b) $I \cdot J = \left\{ \sum_{i=1}^{n} a_i \cdot b_i / a_i \in I,\ b_i \in J,\ n \in \mathbb{N} \right\} \lhd A$.

c) $I : J = \{a \in A / a \cdot J \subseteq I\} \lhd A$.

Ejemplo 8:

Sea $A = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 16\mathbb{Z}$. Calcular $I + J$, $I \cdot J$, y $I : J$

Considerando que $I = 6\mathbb{Z} = \{a \in \mathbb{Z} / a = 6 \cdot t; t \in \mathbb{Z}\}$ y $J = 16\mathbb{Z} = \{b \in \mathbb{Z} / b = 16 \cdot t; t \in \mathbb{Z}\}$, ambos ideales de $\mathbb{Z}$, tenemos que:

a) $I + J = \{x \in \mathbb{Z} / x = a + b; a \in I,\ b \in J\}$

$= \{x \in \mathbb{Z} / x = a + b; a = 6 \cdot r \wedge b = 16 \cdot s\ ; r, s \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z} / x = a + b; a + b = 6 \cdot r + 16 \cdot s\ ; r, s \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z} / x = a + b; a + b = 2 \cdot (3 \cdot r + 8 \cdot s)\ ; r, s \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z} / x = a + b; a + b = 2 \cdot k\ ; k = 3 \cdot r + 8 \cdot s\ ; k, r, s \in \mathbb{Z}\} = 2\mathbb{Z}$

Por lo tanto $I + J = 2\mathbb{Z}$ (múltiplos de 2)

b) $I \cdot J = \left\{ \sum_{i=1}^{n} a_i \cdot b_i / a_i \in I,\ b_i \in J, i \in \mathbb{N} \right\}$

$= \{x \in \mathbb{Z} / x = a \cdot b; a \in I; b \in J\}$

$= \{x \in \mathbb{Z} / x = 6 \cdot t \cdot 16 \cdot k; t, k \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z} / x = 96 \cdot r; t \cdot k = r \in \mathbb{Z}\} = 96\mathbb{Z}$

Por lo tanto $I \cdot J = 96\mathbb{Z}$ (múltiplos de 96)

c) $I : J = \{r \in \mathbb{Z} / r \cdot J \subseteq I\}$

$= \{r \in \mathbb{Z} / r \cdot 16\mathbb{Z} \subseteq 6\mathbb{Z}\}$

$= \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$

Por lo tanto $I : J = 3\mathbb{Z}$ (múltiplos de 3).

Proposición: Sean I, J ideales de A anillo entonces $I \cdot J \subseteq I \bigcap J$

Demostración:

Sean I, J ideales de A, por demostrar $I \cdot J \subseteq I \bigcap J$, es decir debemos demostrar que si $x \in I \cdot J$, entonces $x \in I \bigcap J$. Es evidente que si $x \in I \cdot J$, entonces $x = \sum_{i=1}^{n} a_i \cdot b_i$, con $a_i \in I$, $b_i \in J$ y $i \in \mathbb{N}$. Luego podemos afirmar que:

i) $a_i \in I$ y $b_i \in A$ por ser $J \lhd A$, lo que implica que $a_i \cdot b_i \in I$, por lo tanto $x = \sum_{i=1}^{n} a_i \cdot b_i \in I$

ii) Por otra parte, $a_i \in A$ y $b_i \in J$ por ser $I \lhd A$, lo que implica que $a_i \cdot b_i \in J$, por lo tanto $x = \sum_{i=1}^{n} a_i \cdot b_i \in J$

Luego de (i) e (ii), tenemos que $x = \sum_{i=1}^{n} a_i \cdot b_i \in I \bigcap J$

Ejemplo 9:

Del ejemplo anterior, sea $A = \mathbb{Z}$, $I = 6\mathbb{Z} = \{a \in \mathbb{Z} / a = 6 \cdot t; t \in \mathbb{Z}\}$ y $J = 16\mathbb{Z} = \{b \in \mathbb{Z} / b = 16 \cdot t; t \in \mathbb{Z}\}$ tales que $I, J \lhd A$. Probar que $I \cdot J \subseteq I \bigcap J$.

Como se sabe que $I \cdot J = \{x \in \mathbb{Z} / x = 96 \cdot r; r \in \mathbb{Z}\} = 96\mathbb{Z}$, basta con definir el conjunto $I \bigcap J$ y verificar la inclusión $I \cdot J \subseteq I \bigcap J$.

$$I \bigcap J = \{x \in \mathbb{Z} / x \in I \wedge x \in J\} = \{x \in \mathbb{Z} / x = 6 \cdot t \wedge x = 16 \cdot t; t \in \mathbb{Z}\}$$

$$= \{x \in \mathbb{Z} / x = 48 \cdot t; 48 = m.c.m.\{6,16\}, t \in \mathbb{Z}\} = 48\mathbb{Z}$$

Ahora pasaremos a verificar la inclusión $I \cdot J \subseteq I \bigcap J$, es decir debemos verificar que $96\mathbb{Z} \subseteq 48\mathbb{Z}$. Luego si $x \in I \cdot J$, entonces $x = 96 \cdot r$ con $r \in \mathbb{Z}$.

Ahora si $x \in I \bigcap J$, entonces $x = 48 \cdot t$; igualando $x \in \mathbb{Z}$ se tiene que $48 \cdot t = 96 \cdot r$, lo que implica que basta considerar $t = 2 \cdot r$, con $t, r \in \mathbb{Z}$.

Por lo tanto podemos decir que $96\mathbb{Z} \subseteq 48\mathbb{Z}$.

Proposición: Sean I, J ideales de A anillo si $I + J = A$ entonces $I \cdot J = I \bigcap J$

Demostración:

Sean I, J ideales de A anillo, si $I + J = A$ por demostrar que $I \cdot J = I \bigcap J$, es decir se debe demostrar que (i) $I \cdot J \subseteq I \bigcap J$ y (ii) $I \bigcap J \subseteq I \cdot J$. Sin embargo, $I \cdot J \subseteq I \bigcap J$ está demostrado según la proposición anterior, lo que implica que la demostración se reduce a $I \bigcap J \subseteq I \cdot J$, es decir si $x \in I \bigcap J$, por demostrar que $x \in I \cdot J$.

Si $x \in I \bigcap J$, implica que $x \in I$ y $x \in J$, ahora bien $x \in A$, pues I, $J \lhd A$. Si $x \in A$, entonces $x = a_i + b_i$ con $a_i \in I, b_i \in J$ y $i \in \mathbb{N}$. Como $J \lhd A$, $b_i \in A$ tenemos que $a_i \cdot b_i \in I$ con $a_i \in I$; y además como $I \lhd A$, $a_i \in A$ tenemos que $a_i \cdot b_i \in I$ con $b_i \in J$. Luego $a_i \cdot b_i \in I + J$, es decir $\sum_{i=1}^{n} a_i \cdot b_i \in I + J$, lo que implica por $I + J = A$ que $\sum_{i=1}^{n} a_i \cdot b_i \in A$.

Entonces para todo $x \in A$, $x = \sum_{i=1}^{n} a_i \cdot b_i$ tal que $a_i \in I, b_i \in J$ y $i \in \mathbb{N}$, lo que implica que $x \in I \cdot J$.

Por lo tanto de (i) e (ii), si $I + J = A$, entonces $I \cdot J = I \bigcap J$

Observación: Sea A un anillo conmutativo con identidad, I_1, I_2,..., I_n ideales de A tal que si $I_i + I_j = A$ con $i \neq j$ entonces $I_1 \cdot I_2 \cdot,,, \cdot I_n = I_1 \bigcap I_2 \bigcap ... \bigcap I_n$.

Esta observación se obtiene como generalización del teorema anterior.

Ejercicios

1.- Encuentre todos los ideales primos y maximales de $\mathbb{Z}_{12}$

2.- Pruebe que todo ideal de $\mathbb{Z}$ es principal.

3.- Si A/I es abeliano si y solo si $r\cdot s - s\cdot r \in I \quad , \forall r,s \in A.$

4.- Sea A un dominio de integridad finito. Si $a \neq 0 \in A$, pruebe que $\varphi = \{\varphi(x) \in A / x \in A; \varphi(x) = a\cdot x; a \in A\}$ (Use ese hecho para probar que todo Dominio de Integridad es cuerpo).

5.- Sea P un ideal propio de un anillo conmutativo A. Pruebe que P es un ideal primo de A si y sólo si $(A-P)$ es cerrado para el producto.

6.- Sea $A=\mathbb{Z}_{12}$, $I=\langle\bar{2}\rangle$ y $J=\langle\bar{3}\rangle$. Calcular $I+J$, $I\cdot J$ y $I:J$.

7.- Sea A anillo conmutativo con identidad tal que $x^n = x \quad \forall n>1$. Pruebe cada ideal primo de A es maximal.

8.- Un elemento $a \in A$, con A anillo con identidad es nilpotente si $a^n = 0$, para algún $n \in \mathbb{N}$. Pruebe que $Nil\left(A/I\right) = \{\bar{0}\}$

Desarrollo:

1.- Encuentre todos los ideales primos y maximales de $\mathbb{Z}_{12}$

Por la red de subanillos del ejemplo 5, tenemos que los ideales de $\mathbb{Z}_{12}$ son $\langle\bar{2}\rangle, \langle\bar{3}\rangle, \langle\bar{4}\rangle, \langle\bar{6}\rangle$. Ahora para probar que si son ideales primos o maximales de $\mathbb{Z}_{12}$ utilizaremos el teorema siguiente antes descrito:

Sea A un anillo conmutativo con identidad, entonces:

1) P es un ideal primo de A si y sólo si A/P es un dominio de integridad.
2) M es un ideal maximal de A si y sólo si A/M es cuerpo.

i) Luego ¿$\langle\bar{2}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$? , es decir de acuerdo al teorema ¿$\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es un cuerpo?

$\mathbb{Z}_{12}/\langle\bar{2}\rangle = \{a+\langle\bar{2}\rangle / a \in \mathbb{Z}_{12}\} = \{\bar{0}+\langle\bar{2}\rangle,\ \bar{1}+\langle\bar{2}\rangle\}$, ahora como $\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es un anillo cuociente y como $\mathbb{Z}_{12}$ es un anillo conmutativo con identidad, entonces $\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es un anillo cuociente conmutativo con identidad y es $\bar{1}_{\mathbb{Z}_{12}}+\langle\bar{2}\rangle$. Ahora sólo basta demostrar que $\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es sin divisores de cero, es decir si $a\cdot b=0$ entonces $a=0$ ó $b=0$ con $a,b\in \mathbb{Z}_{12}/\langle\bar{2}\rangle$.

Es evidente que $\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es sin divisores de cero, pues como tiene dos elementos, basta considerar $a=\bar{1}_{\mathbb{Z}_{12}}+\langle\bar{2}\rangle$, de tal manera que si $a\cdot b=0$, entonces $b=\bar{0}_{\mathbb{Z}_{12}}+\langle\bar{2}\rangle$, con $\bar{0}_{\mathbb{Z}_{12}}+\langle\bar{2}\rangle\in\mathbb{Z}_{12}/\langle\bar{2}\rangle$. Por lo tanto, $\mathbb{Z}_{12}/\langle\bar{2}\rangle$ es cuerpo, lo que implica que $\langle\bar{2}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$.

ii) ¿$\langle\bar{3}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$? , es decir de acuerdo al teorema ¿$\mathbb{Z}_{12}/\langle\bar{3}\rangle$ es un cuerpo?

$\mathbb{Z}_{12}/\langle\bar{3}\rangle=\{a+\langle\bar{3}\rangle/a\in\mathbb{Z}_{12}\}=\{\bar{0}+\langle\bar{3}\rangle,\ \bar{1}+\langle\bar{3}\rangle,\ \bar{2}+\langle\bar{3}\rangle\}$. Análogamente al caso anterior, $\mathbb{Z}_{12}/\langle\bar{3}\rangle$ es un anillo conmutativo con identidad. Sólo basta demostrar que es sin divisores de cero, es decir si $a\cdot b=0$ entonces $a=0$ ó $b=0$ con $a,b\in\mathbb{Z}_{12}/\langle\bar{3}\rangle$. Es evidente que $\mathbb{Z}_{12}/\langle\bar{3}\rangle$ es sin divisores de cero, pues si $a\cdot b=0$ con $a,b\in\mathbb{Z}_{12}/\langle\bar{3}\rangle$ basta considerar $a=\bar{0}_{\mathbb{Z}_{12}}+\langle\bar{3}\rangle$ para todo $b\in\mathbb{Z}_{12}/\langle\bar{3}\rangle$. Por lo tanto, $\mathbb{Z}_{12}/\langle\bar{3}\rangle$ es cuerpo, lo que implica que $\langle\bar{3}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$.

iii)¿$\langle\bar{4}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$? , es decir de acuerdo al teorema ¿$\mathbb{Z}_{12}/\langle\bar{4}\rangle$ es un cuerpo?

$\mathbb{Z}_{12}/\langle\bar{4}\rangle = \{\bar{0}+\langle\bar{4}\rangle,\ \bar{1}+\langle\bar{4}\rangle,\ \bar{2}+\langle\bar{4}\rangle,\ \bar{3}+\langle\bar{4}\rangle\}$. Es claro que $\mathbb{Z}_{12}/\langle\bar{4}\rangle$ es un anillo conmutativo con identidad. Pero en $\mathbb{Z}_{12}/\langle\bar{4}\rangle$ se tiene que $(\bar{2}+\langle\bar{4}\rangle)\cdot(\bar{3}+\langle\bar{4}\rangle) = \bar{6}+\langle\bar{4}\rangle = \bar{2}+\langle\bar{4}\rangle$ ¡Contradicción! ya que es con identidad $\bar{1}+\langle\bar{4}\rangle \neq \bar{3}+\langle\bar{4}\rangle$. Por lo tanto, $\mathbb{Z}_{12}/\langle\bar{4}\rangle$ no es cuerpo, lo que implica que $\langle\bar{4}\rangle$ no es ideal maximal de $\mathbb{Z}_{12}$.

Además $\mathbb{Z}_{12}/\langle\bar{4}\rangle$ no es un dominio de integridad ya que si $a\cdot b = 0$ entonces $a=0$ ó $b=0$ con $a,b \in \mathbb{Z}_{12}/\langle\bar{4}\rangle$, pero $(\bar{2}+\langle\bar{4}\rangle)\cdot(\bar{2}+\langle\bar{4}\rangle) = \bar{0}+\langle\bar{4}\rangle$, donde $\bar{2}+\langle\bar{4}\rangle \neq \bar{0}+\langle\bar{4}\rangle$. Por lo tanto, $\mathbb{Z}_{12}/\langle\bar{4}\rangle$ no es dominio de integridad, lo que implica que $\langle\bar{4}\rangle$ no es ideal primo de $\mathbb{Z}_{12}$.

iv) ¿$\langle\bar{6}\rangle$ es ideal maximal de $\mathbb{Z}_{12}$? , es decir de acuerdo al teorema ¿$\mathbb{Z}_{12}/\langle\bar{6}\rangle$ es un cuerpo?

$\mathbb{Z}_{12}/\langle\bar{6}\rangle = \{\bar{0}+\langle\bar{6}\rangle,\ \bar{1}+\langle\bar{6}\rangle,\ \bar{2}+\langle\bar{6}\rangle,\ \bar{3}+\langle\bar{6}\rangle,\bar{4}+\langle\bar{6}\rangle,\bar{5}+\langle\bar{6}\rangle\}$. Es claro que $\mathbb{Z}_{12}/\langle\bar{6}\rangle$ es un anillo conmutativo con identidad. Por verificar que que es sin divisores de cero, es decir si $a\cdot b=0$ entonces $a=0$ ó $b=0$, con $a,b\in\mathbb{Z}_{12}/\langle\bar{6}\rangle$. Pero $\left(\bar{3}+\langle\bar{6}\rangle\right)\cdot\left(\bar{3}+\langle\bar{6}\rangle\right)=\bar{6}+\langle\bar{6}\rangle=\bar{0}+\langle\bar{6}\rangle$, donde $\bar{3}+\langle\bar{6}\rangle\neq\bar{0}+\langle\bar{6}\rangle$. Por lo tanto, $\mathbb{Z}_{12}/\langle\bar{6}\rangle$ no es dominio de integridad, lo que implica que $\langle\bar{6}\rangle$ no es ideal primo de $\mathbb{Z}_{12}$. Es claro que $\langle\bar{6}\rangle$ tampoco es ideal maximal de $\mathbb{Z}_{12}$.

2.- Pruebe que todo ideal de $\mathbb{Z}$ es principal.

Si I es ideal de $\mathbb{Z}$, por demostrar que $I=\langle a\rangle=\{c\cdot a/c\in A\}$. Como $I\subset\mathbb{Z}$ por condición de ideal de $\mathbb{Z}$, entonces en I hay enteros. Sea $a\in I$ tal que a es el menor entero positivo, tal que si $x\in I$ y $a\in I$ con $x,a\in\mathbb{Z}$, entonces por el algoritmo de la división existe un $q,r\in\mathbb{Z}$, tal que $x=a\cdot q+r$ con $0\leq r<a$.

Luego si $x\in I$ y $a\in I$, es claro que $a\cdot q\in I$ por condición de ideal, por lo tanto $r=0$, pues $x=a\cdot q+r\in I$. Entonces $x=a\cdot q$, con $a\in I$ y $q\in\mathbb{Z}$. Por lo tanto I es un ideal principal generado por a. $\left(I=\langle a\rangle\right)$.

3.- Probar que A/I es abeliano si y sólo si $r\cdot s - s\cdot r \in I$, para todo $r,s \in A$

Demostración:

$\Rightarrow]$ Si A/I es abeliano, por demostrar que $r\cdot s - s\cdot r \in I$.

Si $x+I, y+I \in A/I$ implica que $(x+I)\cdot(y+I) = x\cdot y + I$, con $x\cdot y + I \in A/I$. Por otra parte $(y+I)\cdot(x+I) = y\cdot x + I$, con $y\cdot x + I \in A/I$. Considerando que A/I es abeliano, tenemos que $y\cdot x + I = x\cdot y + I$, lo que implica que $y\cdot x - x\cdot y \in I$, para todo $x, y \in A$. Por lo tanto, si A/I es abeliano, entonces $r\cdot s - s\cdot r \in I$.

$\Leftarrow]$ Si $r\cdot s - s\cdot r \in I$, por demostrar que A/I es abeliano.

Si $r\cdot s - s\cdot r \in I$, implica que $r\cdot s + I = s\cdot r + I$. Por definición del producto en el anillo cuociente, tenemos que por una parte $r\cdot s + I = (r+I)\cdot(s+I)$; de la misma manera $s\cdot r + I = (s+I)\cdot(r+I)$. Luego, $r\cdot s + I = (r+I)\cdot(s+I) = (s+I)\cdot(r+I) = s\cdot r + I$ lo que implica que $(r+I)\cdot(s+I) = (s+I)\cdot(r+I)$, con lo cual se prueba que A/I es abeliano para todo $r, s \in A$.

4.- Sea A un dominio de integridad finito. Si $a \neq 0 \in A$, pruebe que $\varphi = \{\varphi(x) \in A / x \in A; \varphi(x) = a\cdot x, a \in A\}$ es inyectiva. Considerando lo anterior pruebe que todo dominio de integridad finito es un cuerpo.

Demostración:

Si $\varphi(x)=\varphi(y)$, por demostrar que $x=y$.

Si $\varphi(x)=\varphi(y)$, entonces se tiene por definición de φ tenemos que

$a\cdot x=a\cdot y$, considerando que A un dominio de integridad,

$x=y$

Por lo tanto la función φ es inyectiva, de A en A.

Considerando que A es finito, tenemos que para todo $\varphi(x)\in A$, existe un $x\in A$, tal que $\varphi(x)=a\cdot x$, con $a\in A$, lo que implica naturalmente que la función φ sea epiyectiva, de A sobre A. Por lo tanto la función φ es biyectiva.

De lo anterior, podemos decir $A=a\cdot A$, con $a\neq 0$. Para dotar a A de una estructura de cuerpo, sólo basta demostrar la existencia de elementos invertibles, pues A es un dominio de integridad.

Si A es un dominio de integridad, se tiene que existe elemento unidad $1\in A$, tal que para todo $a\in A$, se tiene que $1=a\cdot b$, para algún $b\in A$.

Es claro que existe dicho $b\in A$, pues $a\neq 0$, con $a\in A$, de tal manera que siempre se cumplirá $1=a\cdot b$ cuando A sea finito.

Por lo tanto, todo dominio de integridad finito es un A es un cuerpo finito.

5.- Sea P un ideal propio de un anillo conmutativo A. Pruebe que P es un ideal primo de A si y sólo si $(A-P)$es cerrado para el producto.

Demostración:

$\Rightarrow]]$ Si P es un ideal primo de A, por demostrar que $(A-P)$es cerrado para el producto.

Considerando como supuesto que $(A-P)$ no es cerrado para el producto, si $x,\ y \in (A-P)$, entonces $x\cdot y \notin (A-P)$; lo que implicará que $x\cdot y \notin A$ y $x\cdot y \in P$. Si $x\cdot y \in P$ entonces $x\in P$ y $y\in P$, lo que significa que P no es primo ¡contradicción con la hipótesis!. Por lo tanto $(A-P)$ es cerrado para el producto.

$\Leftarrow]]$ Si $(A-P)$es cerrado para el producto, por demostrar que P es un ideal primo de A.

Supongamos P un ideal no primo, es decir que si $x\cdot y\in P$ entonces $x\notin P$ y $y\notin P$. Pero si $x\notin P$ entonces $x\in(A-P)$ y análogamente, si $y\notin P$ entonces $y\in(A-P)$, considerando que el producto es cerrado en $(A-P)$, tenemos que $x\cdot y\in(A-P)$ es decir $x\cdot y\in A$ y $x\cdot y\notin P$ ¡Contradicción con el supuesto!. Por lo tanto, P es un ideal primo de A

6.- Sea $A=\mathbb{Z}_{12}$, $I=\langle\bar{2}\rangle$ y $J=\langle\bar{3}\rangle$. Calcular $I+J$, $I\cdot J$ y $I:J$

Sea $A=\mathbb{Z}_{12}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\overline{10},\overline{11}\}$; $I=\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$ y $J=\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9}\}$.

$I+J=\{x\in\mathbb{Z}_{12}/\,x=a+b;\,a\in I,\ b\in J\}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\overline{10},\overline{11}\}$

$I+J=\mathbb{Z}_{12}$, por lo tanto $I+J=\mathbb{Z}_{12}$

$I\cdot J=\{x\in\mathbb{Z}_{12}/\,x=a\cdot b;\,a\in I,\ b\in J\}=\{\bar{0},\bar{6}\}=6\mathbb{Z}_{12}$

Por lo tanto $I\cdot J=6\mathbb{Z}_{12}$

$I:J=\{r\in\mathbb{Z}_{12}/\,r\cdot J\subseteq I\}=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}=I=2\mathbb{Z}_{12}$

7.- Sea A anillo conmutativo con identidad tal que $x^n = x \quad ,\forall n>1$. Pruebe que cada ideal primo de A es maximal.

Demostración:

Sabemos que A/P es un dominio de integridad si y sólo si P es primo; y A/M es cuerpo si y sólo si M es maximal. Entonces probar que cada ideal primo de A es maximal es análogo a demostrar que todo A/P dominio de integridad implica ser un cuerpo.

Para demostrar que A/P es un cuerpo consiste en verificar que para todo elemento $\bar{x}$ no nulo (diferente de P) perteneciente a A/P es invertible.

Además si $x \in A$ entonces $\bar{x} \in A/P$, tal que $\bar{x} = x + P$. Pero por hipótesis se sabe que $x^n = x$ para $n>1$, lo que implica que $\bar{x}^n = (x+P)^n = x^n + P$, es decir que $x^n + P = x + P = \bar{x}$, luego $\bar{x}^n = \bar{x} \in A/P$. Si $\bar{x}^n = \bar{x}$, entonces $\bar{x}^{n-1} = \bar{1}$ con $\bar{1} \in A/P$ identidad ya que A es con identidad 1.

Luego, para todo elemento $\bar{x}$ no nulo perteneciente a A/P existe un elemento $\bar{x}^{n-2} \in A/P$ tal que $\bar{x} \cdot \bar{x}^{n-2} = \bar{x}^{n-2} \cdot \bar{x} = \bar{x}^{n-1} = \bar{1}$. Por lo tanto, A/P es invertible, lo que implica que A/P es un cuerpo; es decir de acuerdo al teorema ya mencionado, P es un ideal maximal de A.

8.- Un elemento $a \in A$, con A anillo con identidad es nilpotente si $a^n = 0$, para algún $n \in \mathbb{N}$. Pruebe que $\mathrm{Nil}\left(A/I\right) = \{\bar{0}\}$, con $I = \mathrm{Nil}(A)$.

Demostración:

Si $x+I \in \text{Nil}\left(A/I\right)$, entonces existe $n \in \mathbb{N}$ tal que $\left(x+I\right)^n = I$, ya que $I = \bar{0} + I$. Luego $\left(x+I\right)^n = x^n + I = I$, entonces $x^n \in I$.

Como $I = \text{Nil}\left(A\right)$, tenemos que $x^n \in \text{Nil}\left(\text{A}\right)$, lo que implica que existe un $r \in \mathbb{N}$ tal que $\left(x^n\right)^r = 0$. Luego $\left(x^n\right)^r = x^{n \cdot r} = x^s$ tal que $n \cdot r = s$ con $s \in \mathbb{N}$, entonces se tiene que $x^s = 0$. Por lo tanto $x \in \text{Nil}\left(\text{A}\right)$

Autoevaluación

1.- Determine si las siguientes afirmaciones son verdaderas o falsas. Justifique:

a) Existen dominios de integridad finitos que no son cuerpos.

b) Los ideales propios de $\mathbb{Z}_6$ son todos maximales.

c) Si A es dominio de integridad, entonces $A\times A$ también lo es.

d) Si $\mathbb{R}$ anillo conmutativo con identidad $1_{\mathbb{R}}$, no tiene ideales propios entonces $\mathbb{R}$ es cuerpo.

2.- Encuentre todos los ideales primos y maximales de $\mathbb{Z}_{24}$.

3.- Sea $f:A\to B$ un homomorfismo de anillos, P ideal primo de B. Pruebe que $f^{-1}(P)$ es un ideal primo.

4.- Pruebe o refute las siguientes aseveraciones:

a) $\mathbb{Q}$ es ideal de $\mathbb{R}$.

b) Todo anillo cuociente de un anillo conmutativo es un anillo conmutativo.

c) Sea A un anillo con identidad, probar que $\text{Nil}(A)=\{a\in A/\, a \text{ es nilpotente}\}$ es un ideal de A.

5.- Sean I, J y K ideales de A, pruebe:

a) $I\cdot(J+K)=I\cdot J+I\cdot K$

b) $I:J$ es un ideal de A.