UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
DEPARTAMENTO DE MATEMATICA

ANILLOS E IDEALES

TRABAJO DE GRADUACION PRESENTADO POR

Rafael Antonio Arèvalo

PREVIO A LA OPCION DEL TITULO DE

LICENCIADO EN MATEMATICA

OCTUBRE DE 1984.

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA

UNIVERSIDAD DE EL SALVADOR

R E C T O R

Dr. MIGUEL ANGEL PARADA

SECRETARIO GENERAL

Dra. ANA GLORIA CASTANEDA DE MONTOYA

FACULTAD DE INGENIERIA Y ARQUITECTURA

D E C A N O

Ing. MANUEL ANTONIO CAÑAS LAZO

S E C R E T A R I O

Ing. RENE MAURICIO MEJIA MENDEZ

DIRECTOR DEL DEPARTAMENTO DE MATEMATICA

Lic. JOSE JAVIER RIVERA LAZO

COORDINADOR Y ASESOR: Lic. JOSE JAVIER RIVERA LAZO

INDICE

CAPITULO VI

INTRODUCCION

El presente trabajo tiene por objeto ampliar nuestros conocimientos matemáticos sobre las estructuras algebráicas. El tema central consiste en el desarrollo de la Teoría de ideales.

En el Capítulo I se define un conjunto con dos operaciones binarias que cumplen ciertas propiedades elementales y que se denomina Anillo. En el Capítulo II se trata de la definición y ejemplos de subconjuntos de Anillos, con características especiales, llamados Ideales. Asimismo, y aprovechando la idea de los grupos Cocientes, se definen los anillos cocientes. El Capítulo III, mediante los conceptos de "divisor de cero" y "Unidades, se definen anillos, llamados: Dominios de integridad y campos, y además se discute el importante tema de los ideales principales. Una, también importante, clase de ideales se analiza en el Capítulo IV, estos son los ideales maximales y los ideales primos. Con estos conceptos se trabaja en el Capítulo V para definir dos conjuntos de gran trascendencia: El Nil-radical y el Radical de Jacobson. Finalmente, en el Capítulo VI, se estudian varias operaciones elementales que pueden verificarse con ideales.

CAPITULO I

ANILLOS Y HOMOMORFISMOS DE ANILLOS

1.1 ANILLO, ANILLO ABELIANO, ANILLO CONMUTATIVO CON IDENTIDAD.

1.1.1 DEFINICION.

Un anillo A es un conjunto con dos operaciones binarias: ADICION (+) Y MULTIPLICACION (·), tales que para cualesquiera x, y, z ε A se verifican las propiedades siguientes:

1) $(x+y) + z = x + (y+z)$ (Ley asociativa de la adición).

2) $x+y = y+x$ (Ley conmutativa de la adición).

3) A tiene un elemento cero, que se denota por 0, tal que: (Existéncia de elemento neutro aditivo).

$$x+0 = 0+x = x$$

4) Para cada x ε A existe -x A tal que: (Existencia de elemento inverso aditivo).

$$x + (-x) = 0$$

5) $(x.y).z = x.(y+z)$ (Ley asociativa de la multiplicación).

6) $x.(y+z) = x.y + x.z$ (Ley distributiva de la multiplicación con respecto a la adición).
y $(y+z).x = y.x + z.x$

Es decir, $<A,+,\cdot>$ es un anillo si:

i) $<A,+>$ es un grupo abeliano,

ii) $<A,\cdot>$ es un semigrupo y

iii) La multiplicación es distributiva con respecto a la adición.

1.1.2 DEFINICION.

Un anillo A en el que la multiplicación es conmutativa, es decir que, para cualesquiera $x, y \in A$ se tiene que: $x.y = y.x$, se llama ANILLO CONMUTATIVO O ANILLO ABELIANO.

1.1.3 DEFINICION.

Un anillo A en el que existe elemento neutro para el producto, es decir que, existe $1 \in A$ tal que: $x.1 = 1.x = x$, se llama ANILLO UNITARIO.

1.1.4 DEFINICION.

Un anillo conmutativo y que tiene elemento neutro para el producto se llama ANILLO CONMUTATIVO CON IDENTIDAD.

1.1.5 NOTA: En este trabajo la palabra "anillo" significa - ANILLO CONMUTATIVO CON IDENTIDAD.

1.1.6 EJEMPLOS.

1.1.6.1 $\langle \mathbb{Z}, +, \cdot \rangle$ es el anillo de los enteros y es un anillo conmutativo con identidad.

1.1.6.2 $\langle \mathbb{Q}, +, \cdot \rangle$ es el anillo de los racionales y es un anillo conmutativo con identidad.

1.1.6.3 $\langle \mathbb{R}, +, \cdot \rangle$ es el anillo de los reales y es un anillo conmutativo con identidad.

1.1.6.4 El conjunto de los enteros pares, con las operaciones suma y producto, es un anillo conmutativo no unitario.

1.1.7 PROPOSICION.

En un anillo A se cumplen las siguientes propiedades:

i) El cero es único,

ii) La identidad en A es única,

iii) Si $x \in A$, entonces $-x \in A$ es único,

iv) Se cumple la ley cancelativa para la adición,

v) $x.0 = 0.x = 0$,

vi) Para cada $x, y \in A$, $(-x).y = -(x.y) = x.(-y)$,

vii) Para cada $x \in A$, $-(-x) = x$.

DEMOSTRACION:

i) Supongamos que existe $z \in A$ tal que: $x+z = x$, para todo $x \in A$, entonces:

$0 + z = 0$ (Por hipótesis Z es neutro).

$z + 0 = z$ (Por la propiedad 3 de la definición 1.1.1)

Luego $z = 0$ (Sustituyendo $0 + z = z + 0$ por z)

ii) Supongamos que existe $e \in A$ tal que: $x.e = x$, para todo $x \in A$, entonces:

$1.e = 1$ (Por hipótesis e es neutro en el producto).

$e.1 = e$ (Por definición 1.1.3, $1 \in A$ es neutro para el producto)

Luego $e = 1$ (Sustituyendo $1.e = e.1 = e$)

iii) Supongamos que existe $s \in A$ que verifica que -

$x + s = 0$, entonces:

$-x = -x + 0$ (Existencia de elemento neutro aditivo).

$-x = -x + x+s$ (Por hipótesis $x+s = 0$)

$-x = [-x + x] + s$ (Ley Asociativa de la Adición).

$-x = 0 + s$ (Por propiedad 4 de definición 1.1.1)

$-x = s$ (Existencia de elemento neutro aditivo).

Luego el inverso aditivo es único.

iv) Si $x, y, z \in A$ y $x + y = z + y$, entonces $x = z$.

$x + y = z + y$ (Por hipótesis)

$(x+y) + (-y) = (z+y) + (-y)$ (Como $y \in A$ por propiedad 4 de definición 1.1.1 existe $-y \in A$ el cual podemos sumarlo a la derecha).

$x + [y+(-y)] = z + [y+(-y)]$ (Ley asociativa de la adición).

$x + 0 = z + 0$ (Existencia de inverso aditivo).

$x = z$ (Existencia de elemento neutro aditivo).

Luego: en un anillo A se cumple la ley cancelativa de la suma.

v) $a.0 = 0 + a.0$ (Existencia de elemento neutro aditivo).

$a.(0+0) = 0 + a.0$ (Como cero es neutro $0=0+0$).

$a.0 + a.0 = 0 + a.0$ (Ley distributiva).

$a.0 = 0$ (Ley cancelativa de la suma)

vi) Probaremos primero que $(-x).y = -(x.y)$

$x + (-x) = 0$ (Existencia de inverso aditivo).

$[x + (-x)].y = 0.y$ (Multiplicando por y a la derecha)

$x.y + (-x).y = 0$ (Ley distributiva y v) de esta misma proposición).

Luego $(-x).y = -(x.y)$ (El inverso aditivo es único).

Ahora probaremos que $x.(-y) = -(x.y)$

$y + (-y) = 0$ (Existencia de inverso aditivo).

$x.[y+(-y)] = x.0$ (Multiplicando por x a la izquierda).

$x.y + x.(-y) = 0$ (Ley distributiva y v) de esta misma proposición).

Luego $x.(-y) = -(x.y)$ (El inverso aditivo es único).

vi) $x + (-x) = 0$ (Existencia de inverso aditivo).

Luego $-(-x) = x$ (El inverso aditivo es único).

1.1.8 NOTA: Definiremos la diferencia entre a y b como $a-b = a + (-b)$.

1.1.9 PROPOSICION.

En un anillo A si $1 = 0$, es decir que si para cada $x \in A$ se tiene $x = x.1 = x.0 = 0$, entonces $A = \{0\}$.

DEMOSTRACION: (Por doble inclusión).

"C"

$x \in A \Rightarrow x = x.1$ (A es un anillo unitario)

$\Rightarrow x = x.0$ $(1 = 0)$

$\Rightarrow x = 0$ (Por v) de proposición 1.1.7)

$\Rightarrow A \subset \{0\}$ (x es un elemento cualquiera de A

"⊃"

$0 \in A$ (Por propiedad 3 de definición 1.1.1)

$\Rightarrow \{0\} \subset A$ (Definición de inclusión).

Luego: Como $A \subset \{0\}$ y $\{0\} \subset A$, $A = \{0\}$.

La proposición anterior establece que A es el ANILLO - CERO que denotaremos por $\{0\}$.

1.1.10 DEFINICION.

$S \subset A$, $S \neq \Phi$, es un subanillo de A si S es cerrado respecto a la multiplicación y la adición y contiene el elemento identidad de A.

1.1.11 EJEMPLOS.

1.1.11.1 $\{0\}$ y A son subanillos de A, llamados subanillos impropios.

1.1.11.2 Z es un subanillo del conjunto Q.

1.2 HOMOMORFISMOS DE ANILLOS.

1.2.1 DEFINICION.

Un homomorfismo de anillos es una aplicación f de un anillo A en un anillo B tal que:

i) $f(x + y) = f(x) + f(y)$

ii) $f(x.y) = f(x).\ f(y)$

iii) $f(1) = 1$

Significa que f de A en B es un homomorfismo de anillos si f respeta la adición, la multiplicación y el elemento idéntico.

La igualdad dada en i) significa que f es homomorfismo de grupos abelianos, consecuentemente si 0 denota el cero de A lo mismo que el cero de B debemos concluir que:

iv) $f(0) = 0$, ya que

$f(0) = f(0 + 0) = f(0) + f(0)$ (Por i))

$-f(0) + f(0) = -f(0) + [f(0) + f(0)]$ (Sumando $-f(0)$ a la izquierda).

$0 = [-f(0)+f(0)] + f(0)$ (Ley asociativa de la suma y existencia de inverso aditivo en el anillo B)

$0 = 0 + f(0)$ (Existencia de inverso aditivo en B).

v) $f(-x) = -f(x)$, ya que

$0 = f(0)$ (Por iv))

$0 = f[x + (-x)]$ (Existencia de inverso aditivo en A)

$0 = f(x) + f(-x)$ (Por i))

Luego $f(-x) = -f(x)$ (Porque el inverso aditivo es único).

vi) $f(x-y) = f(x) - f(y)$, ya que

$f(x-y) = f[x + (-y)]$ (Nota 1.1.8)

$= f(x) + f(-y)$ (Por i))

$= f(x) - f(y)$ (Por v))

1.2.2 PROPOSICION.

Si S es un subanillo de A, la aplicación idéntica de S en A es un homomorfismo de anillos. Es decir:

$f : S \to A : x \rightsquigarrow x$ es un homomorfismo de anillos.

DEMOSTRACION:

i) $f(x + y) = x + y$

$= f(x) + f(y)$ (Por definición de aplicación idéntica).

ii) $f(xy) = xy$

$= f(x).f(y)$ (Por definición de aplicación idéntica).

iii) $1 \in S$ (Por ser S subanillo de A), entonces

$f(1) = 1$ (Por definición de aplicación idéntica).

1.2.3 PROPOSICION.

Si f de A en B y g de B en C son homomorfismos de anillos, entonces la composición de f con g es también un homomorfismo de anillos.

DEMOSTRACION.

i) $(g_{\circ}f)(x+y) = g[f(x+y)]$ (Por definición de composición de funciones).

$= g[f(x)+f(y)]$ (f es un homomorfismo).

$= g[f(x)]+g[f(y)]$ (g es un homomorfismo).

$= (g_{\circ}f)(x) + (g_{\circ}f)(y)$ (Por definición de composición de funciones).

ii) $(g_{\circ}f)(xy) = g[f(xy)]$ (Por definición de composición de funciones).

$= g[f(x)f(y)]$ (f es un homomorfismo).

$= g[f(x)]g[f(y)]$ (g es un homomorfismo)

$= [g_{\circ}f](x)[g_{\circ}f](y)$ (Por definición de composición de funciones).

iii) $(g_{\circ}f)(1) = g[f(1)]$ (Por definición de composición de funciones).

$= g(1)$ (f es un homomorfismo).

$= 1$ (g es un homomorfismo).

Luego la composición $g_{\circ}f : A \to C$ cumple con las tres propiedades de la definición 1.2.1, entonces es un homomorfismo de anillos.

CAPITULO II

IDEALES. ANILLOS COCIENTES.

2.1 IDEALES.

2.1.1 DEFINICION.

Si un subconjunto no vacío S de un anillo A es un subgrupo aditivo y es cerrado bajo la multiplicación, entonces $\langle S, +, \cdot \rangle$ es un anillo. S es llamado subanillo de A. Dos subanillos triviales de A son $\{0\}$ y A. Si $S \neq \{0\}$ y $S \neq A$, entonces S es llamado subanillo propio de A.

2.1.2 DEFINICION.

Un ideal I de un anillo A es un subconjunto de A que es un subgrupo aditivo y tal que $A\,I \subseteq I$ (es decir - $x \in A$ y $y \in I$ implica $xy \in I$). $\{0\}$ y A son ideales de A, denominados ideales triviales.

Nótese que un ideal I de A es un subanillo de A tal que $xy \in I$ para todo $x \in A$ y $y \in I$.

2.1.3 PROPOSICION.

$\{0\}$ es un ideal en A.

DEMOSTRACION:

i) $\{0\} \subset A$ (O es el elemento neutro para la suma en A)

ii) $x \in \{0\} \Rightarrow x \in A$ ($\{0\} \subset A$)

$\Rightarrow x-x = 0 \in \{0\}$ (Existencia de elemento inverso aditivo en un anillo)

Luego $\{0\}$ es un subgrupo aditivo de A.

iii) Para todo $x \in A$ y $y \in \{0\}$, $xy = 0 \in \{0\}$, entonces $A\{0\} \subset \{0\}$.

Luego $\{0\}$ es un ideal en A.

2.2 ANILLOS COCIENTES.

Si I es un ideal de A, entonces I es un subgrupo aditivo de A consecuentemente podemos formar el grupo cociente[1/] como sigue:

$$\frac{A}{I} = \{x + I \ / \ x \in A\}$$

donde $x + I = \{x + z \ / \ z \in I\}$

1/ (Proposición 2.2.4).

2.2.1 PROPOSICION.

Para cualesquiera $x,y \in A$,

$x + I = y + I \iff x - y \in I$

DEMOSTRACION.

" => "

Sean $m \in x + I$ y $n \in y + I$ tales que

$m = n$.

$m \in x + I \Rightarrow m = x + z$ tal que $z \in I$ (Por definición de $x + I$).

$n \in y + I \Rightarrow n = y + z'$ tal que $z' \in I$ (Por definición de $x + I$).

$m = n \Rightarrow x + z = y + z'$ (Sustituyendo por su igual).

$\Rightarrow x - y = z' - z$ (Como A e I son grupos y $\in A$ y $z \in I$ implica que existen $-y \in A$ y $-z \in I$).

Como I es ideal de A y por ende un anillo, entonces $z' - z \in I$, entonces $x - y \in I$.

" <= "

Por doble inclusión probaremos que si

$x - y \in I \Rightarrow x + I = y + I$

Sea $m = x + z$, $z \in I$. $x - y = n$, para algún $n \in I$,

$x = n + y$.

$m = x + z = (n+y) + z$ (Sustituyendo x por su igual)

$m = (y+n) + z$ (Ley conmutativa)

$m = y + (n+z)$ (Ley asociativa)

Luego $m \in y + I$ ($n+z \in I$ ya que $n \in I$ y $z \in I$ e I es un ideal)

Como $m = x+z \in y+I$, $x+I \subset y+I$.

Sea $p = y+t$, $t \in I$. $x-y = q$, para algún $q \in I$,

$y = x - q$.

$p = y+t = (x-q) + t$ (Sustituyendo y por su igual)

$p = x + (-q+t)$ (Ley asociativa)

$p = x + (t - q)$ (Ley conmutativa)

Luego $p \in x + I$ ($t - q \in I$ ya que $t, -q \in I$ e I es ideal).

Como $p = y+t \in x+I$, $y+I \quad x+I$

$\therefore$ $x + I = y + I$

2.2.2 COROLARIO.

$x + I = I \iff x \in I$

DEMOSTRACION.

$x + I = I \iff x + I = 0 + I$ (0 es neutro)

$\Leftrightarrow x - 0 \in I$ (Proposición 2.1.1)

$\Leftrightarrow x \in I$ (0 es neutro)

2.2.3 DEFINICION.

Definiremos la adición (+) en $\frac{A}{I}$ por

$(x + I) + (y + I) = (x + y) + I$ y la multiplicación ($\circ$) por

$(x + I).(y + I) = (x.y) + I$

Demostraremos que estas operaciones están bien definidas.

La adición está bien definida si $x + I = x' + I$ y $y + I = y' + I$ implica que $(x + y) + I = (x' + y') + I$.

$x + I = x' + I \Rightarrow x - x' \in I$ (Por proposición 2.2.1)

$y + I = y' + I \Rightarrow y - y' \in I$ (Por proposición 2.2.1)

$(x - x') + (y - y') \in I$ (I es un ideal)

$(x + y) - (x' + y') \in I$ (Ley asociativa y distributiva en I)

$(x + y) + I = (x' + y') + I$ (Por proposición 2.2.1)

Luego la suma en $\frac{A}{I}$ está bien definida.

Bajo la misma hipótesis de que $x + I = x' + I$ y $y + I = y' + I$ se tiene que $x - x' = u$ y $y' - y' = v$

para algún $u, v \in I$, esto por proposición 2.2.1; entonces:

$$xy = (x' + u)(y' + v) \quad (x = x' + u \text{ y } y = y' + v)$$

$$xy = x'y' + uy' + x'v + uv$$

Puesto que I es un ideal $uy', x'v, uv \in I$, luego la suma $uy' + x'v + uv$ está en I, entonces $xy - x'y' = uy' + x'v + uv$ también está en I. Por proposición 2.2.1

$$xy + I = x'y' + I$$

Luego la multiplicación está bien definida en $\frac{A}{I}$.

2.2.4 PROPOSICION.

El conjunto $\frac{A}{I}$ con las operaciones definidas en 2.2.3 es un anillo conmutativo con identidad denominado "el anillo cociente" (o anillo conmutativo con identidad).

DEMOSTRACION.

i) $\langle \frac{A}{I}, + \rangle$ es un grupo conmutativo.

ASOCIATIVIDAD.

$$[(x+I) + (y+I)] + (z+I) = [(x+y)+I]+(z+I) \quad \text{(Definición 2.2.3)}$$

$$= [(x+y) + z] + I \quad \text{(Definición 2.2.3)}$$

$= [x + (y+z)] + I$ (Ley Asociativa en A)

$= (x+I) + [(y+z)+I]$ (Definición 2.2.3)

$= (x+I)+[(y+I)+(z+I)]$ (Definición 2.2.3)

CONMUTATIVIDAD.

$(x+I) + (y+I) = (x+y) + I$ (Definición 2.2.3)

$= (y+x) + I$ (Conmutatividad en A)

$= (y+I) + (x+I)$ (Definición 2.2.3)

EXISTENCIA DE ELEMENTO NEUTRO.

El cero para la adición en $\frac{A}{I}$ es I.

PRUEBA.

$(x+I) + I = (x + I) + (0 +I)$ ($0 \varepsilon I \Rightarrow 0 + I = I$ por Corolario 2.2.2)

$= (x + 0) + I$ (Definición 2.2.3)

$= x + I$ (0 es neutro en A).

EXISTENCIA DE ELEMENTO INVERSO ADITIVO.

Para cada $x + I \varepsilon \frac{A}{I}$ existe $- (x + I) = -x + I$ tal que $(x+I) + (-x+I) = I$ (el cero del anillo cocien te)

PRUEBA.

$(x+I) + (-x+I) = (x - x) + I$ (Definición 2.2.3)

$= 0 + I$ (-x es el inverso de x en A)

$= I$ ($0 \in I \Rightarrow 0 + I = I$ por Corolario 2.2.2

ii) $< \frac{A}{I} , \cdot >$ es un semigrupo.

ASOCIATIVIDAD.

$[(x+I)\ (y+I)](y+I) = [(xy)+I\ (y+I)]$ (Definición 2.2.3)

$= (xy)z + I$ (Definición 2.2.3)

$= x(yz) + I$ (Asociatividad en A)

$= (x+I)\ [(yz)+I]$ (Definición 2.2.3)

$= (x+I)[(y+I)(z+I)]$ (Definición 2.2.3)

iii) LA MULTIPLICACION ES DISTRIBUTIVA RESPECTO A LA ADICION.

$(x+I)[(y+I)+(z+I)] = (x+I)[(y+z)+I]$ (Definición 2.2.3)

$= x\ (y+z) + I$ (Definición 2.2.3)

$= (xy + xz) + I$ (Distributividad en A)

$= (xy + I)+(xz+I)$ (Definición 2.2.3)

$= (x+I)(y+I)+(x+I)(z+I)$ (Def. 2.2.3)

Además como A es un anillo conmutativo con identidad (Nota 1.1.5) el anillo cociente $\frac{A}{I}$ también es un anillo conmutativo con identidad.

a) La multiplicación en $\frac{A}{I}$ es conmutativa.

Sean $(x + I)$, $(y + I) \in \frac{A}{I}$, entonces:

$$(x + I)(y + I) = xy + I \quad \text{(Definición 2.2.3)}$$

$$= yx + I \quad \text{(xy } \in \text{ A y A es un anillo conmutativo).}$$

$$= (y+I)(x+I) \quad \text{(Definición 2.2.3)}$$

b) Existe $1 + I \in \frac{A}{I}$ tal que $(x + I)(1 + I) = (x + I)$. $1 + I$ es llamado elemento idéntico del anillo cociente.

Sean $(x + I)$, $(1 + I) \in \frac{A}{I}$, entonces:

$$(x + I)(1 + I) = x.1 + I \quad \text{(Definición 2.2.3)}$$

$$= x + I \quad \text{(1 } \in \text{ A por Nota 1.1.5)}$$

Con a) y b) concluye la prueba de que $\frac{A}{I}$ es un "anillo conmutativo con identidad".

2.2.5 PROPOSICION.

La aplicación $\phi : A \to \frac{A}{I}$; $x \rightsquigarrow x + I$ es un homomorfis

mo suryectivo.

DEMOSTRACION.

i) $\phi(x + y) \stackrel{?}{=} \phi(x) + \phi(y)$

$\phi(x + y) = (x+y) + I$ (Por definición de ϕ)

$= (x+I) + (y+I)$ (Por definición 2.2.3)

$= \phi(x) + \phi(y)$ (Por definición de ϕ)

ii) $\phi(xy) \stackrel{?}{=} \phi(x)\,\phi(y)$

$\phi(xy) = (xy) + I$ (Por definición de ϕ)

$= (x+I)\,(y+I)$ (Por definición de 2.2.3)

$= \phi(x)\,\phi(y)$ (Por definición de ϕ)

iii) $1 \in A$ y $1 + I \in \frac{A}{I}$, entonces $\phi(1) = 1+I$, es decir $\phi(1)$ es igual al idéntico del producto en $\frac{A}{I}$.

iv) ϕ es un homomorfismo suryectivo.

$y + 1 \in \frac{A}{I} \Rightarrow y+I = \phi(y)$, (Por definición de ϕ)

con $y \in A$

$\therefore$ ϕ es suryectivo.

2.2.6 PROPOSICION.

Existe una correspondencia biyectiva que conserva el orden entre los ideales J de A que contienen a I, y los ideales K de $\frac{A}{I}$, dada por $J = \phi^{-1}(K)$.

Sea I C A un ideal en A,

$M = \{J \subset A \ / \ J \text{ ideal en } A \text{ e } I \subset J\}$,

$N = \{K \subset \frac{A}{I} \ / \ K \text{ es un ideal}\}$.

Existe $f : M \to N$ tal que si $J \subset T$, entonces $f(J) \subset f(T)$ y f biyectiva.

Sea $f : M \to N : J \rightsquigarrow f(J) = K = \{x+I \ / \ x \in J\}$

i) "K es un elemento de N".

$x+I, y+I \in K \Rightarrow x,y \in J \ (f(J) = K = \{x+I/x \in J\})$

$\Rightarrow x+y \in J$ (J es ideal en A)

$\Rightarrow (x+I) + (y+I) = (x+y) + I \in K \ (x+y \in J)$

Luego K es cerrado respecto a la suma.

$x+I \in K \Rightarrow x \in J \ (f(J) = K = \{x+I \ / \ x \in J\})$

$\Rightarrow -x \in J$ (J es un ideal en A)

$\Rightarrow -x + I \in K$ (Por definición de K)

Luego K es subgrupo aditivo de $\frac{A}{I}$.

$x+I \in \frac{A}{I} \Rightarrow x \in A$ (Por definición de $\frac{A}{I}$)

$y+I \in K \Rightarrow y \in J$ (Por definición de K)

$(x+I)(y+I) = xy + I$ (Definición 2.2.3)

$\Rightarrow xy \in J$ (J es un ideal en A)

$\Rightarrow (x+I)(y+I) \in K$ (Por Definición de K)

$\Rightarrow f(J) = K \subset \frac{A}{I}$ (x+I es un elemento - cualquiera de $\frac{A}{I}$)

Luego $f(J) = K$ es un ideal en $\frac{A}{I}$.

ii) "f es biyectiva"

f es inyectiva.

Supongamos $f(J) = f(J')$, entonces

$x + I \in f(J) \Rightarrow x + I \in f(J')$

$\Rightarrow x \in J$ y $x \in J'$

$\Rightarrow J \subset J'$

$y + I \in f(J') \Rightarrow y + I \in f(J)$

$\Rightarrow y \in J'$ y $y \in J$

$\Rightarrow J' \subset J$

Luego J = J' y f es inyectiva.

f es sobreyectiva.

Sea P c $\frac{A}{I}$, entonces existe J ε A tal que

f(J) = P.

Por definición de f(J) debe existir J tal que,

P = {x + I / x ε J}, entonces, sea J = {x/x + I ε P};

"J es ideal en A"

x,y ε J => x + I, y + I ε P

=> (x + I) + (y + I) ε P

° => (x + y) + I ε P

=> x + y ε J

Luego J es cerrado respecto a la suma.

x ε J => x + I ε P

=> -x + I ε P

=> -x ε J

Luego J es un subgrupo de A.

x ε A => x + I ε P

y ε J => y + I ε P

$\Rightarrow (x + I)(y + I) \in P$

$\Rightarrow xy + I \in P$

$\Rightarrow xy \in J$

Luego $AJ \subset J$

$\therefore$ J es un ideal en A.

Finalmente, probaremos que f preserva el orden es decir $J \subset H \Rightarrow f(J) \subset f(H)$.

$x + I \in f(J) \Rightarrow x \in J \quad (f(J) = \{x + I / x \in J\})$

$\Rightarrow x \in H \quad (J \subset H)$

$\Rightarrow x + I \in f(H) \quad (f(H) = \{x + I / x \in H\})$

$\Rightarrow f(J) \subset f(H)$

2.2.7 DEFINICION.

Si $f : A \to B$ es un homomorfismo de anillos, llamaremos núcleo de f, llamado también Kerf, al conjunto:

$$Kerf = \{x \in A / f(x) = 0\}$$

2.2.8 PROPOSICION.

Si $f : A \to B$ es un homomorfismo cualquiera de anillos

a) El núcleo de f = Kerf es un ideal,

b) La imagen de A = f(A) es un subanillo de B,

c) f induce un isomorfismo de anillos,

d) Si I c B es un ideal, entonces f^{-1} (I) es un ideal.

DEMOSTRACION.

a) <u>El Kerf es un Ideal.</u>

i) Kerf c A (Definición 2.2.7)

ii) Kerf $\neq \phi$ ($0 \in A$ y $f(0) = 0$ ya que f es homomorfismo).

iii) Sean $x,y \in$ Kerf, entonces

$f(x) = 0$ y $f(y) = 0$ (Por definición 2.2.7)

$f(x) + f(y) = 0$ ($f(x), f(y) \in B$, B es un anillo).

$f(x+y) = f(x) + f(y) = 0$ (f es un homomorfismo de A en B)

$\therefore$ $x + y \in$ Kerf (Por definición 2.2.7)

Significa que el Kerf es cerrado respecto a la suma.

vi) Por propiedad de homomorfismo

$f(-x) = -f(x) = -0 = 0 \Rightarrow (x \in Kerf \Rightarrow -x \in Kerf)$.

Por i - iv) el Kerf es un subgrupo aditivo de A.

v) Si $x \in A$ y $z \in Kerf$, entonces

$x z \in A$, ya que $z \in Kerf \rightarrow z \in A$ y A es un anillo.

$f(x z) = f(x)\ f(z)$ (f es un homomorfismo)

$= f(x).0$ ($z \in Kerf$)

$= 0$ (Por proposición 1.1.7 v))

Luego $xz \in Kerf$ (Definición 2.2.7)

Por i) - v) Kerf es un ideal de A.

b) f(A) es un Subanillo de B.

$f(A) = \{y \in B / f(x) = y$, para algún $x \in A\}$

$f(A) \neq \phi$, ya que como f es un homomorfismo.

$f(0) = 0$, entonces $0 \in f(A)$.

Sean $y, y' \in f(A)$, entonces existen $x, x' \in A$ tal -

que $f(x) = y$ y $f(x') = y'$, como f es homomorfismo $f(x) + f(x') = f(x + x') = y + y' \in f(A)$. Significa que f(A) es cerrado, respecto a la suma. Asímismo $f(x)\, f(x') = f(xx') = yy' \in f(A)$. Significa que f(A) es cerrado respecto a la multiplicación.

Además si $y = f(x)$, $-y = -f(x) = f(-x)$, por propiedad de homomorfismo, entonces $-y \in f(A)$. Por tanto f(A) es un subanillo de B (por Definición 2.1.1.).

c) F induce un Isomorfismo de Anillos.

Sea $g : \frac{A}{Kerf} \to f(A) : x + Kerf \rightsquigarrow f(x)$, g es un homomorfismo biyectivo.

i) g está bien definida. Esto es: $x + Kerf = x' + Kerf$, entonces $g(x + Kerf) = g(x' + Kerf)$. En efecto.

$x + Kerf = x' + Kerf \iff x - x' \in Kerf$ (Proposición 2.2.1)

$\iff f(x-x') = 0$ (Definición de Kerf)

$f(x-x') = 0 \to f(x) - f(x') = 0$ (Por Propiedad de homomorfismo)

$\rightarrow f(x) = f(x')$ (El inverso aditivo es único)

$\rightarrow g(x+Kerf) = g(x'+Kerf)$ (Definición de g)

ii) g es un homomorfismo.

$$g[(x + Kerf) + (y + Kerf)] = g[(x+y) + Kerf]$$

$$= f(x + y)$$

$$= f(x) + f(y)$$

$$= g(x + Kerf) + g(y+Kerf)$$

Luego g respeta la adición.

$$g[(x+Kerf)(y + Kerf)] = g[xy + Kerf]$$

$$= f(xy)$$

$$= f(x)\ f(y)$$

$$= g(x + Kerf)\ g(y + Kerf)$$

$g(1 + Kerf) = f(1) = 1$. Significa que g respeta la identidad.

iii) g es sobreyectivo.

$f(x) \in f(A) \Rightarrow f(x) = g\ (x + Kerf)$

$$\Rightarrow x + Kerf \in \frac{A}{Kerf}$$

iv) g es inyectivo.

Sean $g(x + Kerf), g(y + Kerf) \in f(A)$ tales que $g(x + Kerf) = g(y + Kerf)$ (Hipótesis)

$f(x) = f(y)$ (Definición de g)

$f(x) + (-f(y) = f(y) + (-f(y))$ (Existencia de inverso aditivo en B)

$f(x) + f(-y) = f(y) + f(-y)$ (Proposición de Homomorfismo).

$f(x-y) = f(y-y) = f(0) = 0$ (f es homomorfismo)

$x-y \in Kerf \rightarrow x+Kerf=y+Kerf$ (Prop. 2.2.1)

d) Si I c B es un ideal $f^{-1}(I)$ es un ideal. Definamos

$$f^{-1}(I) = \{x \in A / f(x) \in I\}$$

i) $f^{-1}(I) \neq \phi$ ya que como I es un ideal de B $0 \in I$ y $0 = f(0)$ puesto que f es homomorfismo, entonces $0 \in f^{-1}(I)$.

ii) $x \in f^{-1}(I) \rightarrow f(x) \in I$; (Por definición de $f^{-1}(I)$)

$y \in f^{-1}(I) \rightarrow f(y) \in I$

$\rightarrow -f(y) \in I$ (I es un ideal)

$\rightarrow f(-y) \in I$ (Por propiedad de homomorfismo $-f(x) = f(-x)$)

$\rightarrow f(x)+f(-y) \in I$ (I es un ideal)

$\rightarrow f(x-y) \in I$ (Por propiedad de homomorfismo $f(x)+f(-y) = f(x-y)$

$x-y \in f^{-1}(I)$ (Por def. de $f^{-1}(I)$)

Luego $f^{-1}(I)$ es un subgrupo aditivo de A.

iii) Sea $y \in f^{-1}(I)$, entonces $f(y) \in I$ (Por definición de $f^{-1}(I)$) además para todo $x \in A$, $f(x) \in B$ ya que f es un homomorfismo de A en B. Como I es un ideal en B, $f(x)\, f(y) \in I$, entonces por propiedad de homomorfismo, $f(x)\, f(y) = f(xy) \in I$, como $xy \in A$ también $xy \in f^{-1}(I)$, entonces $A\, f^{-1}(I) \subset f^{-1}(I)$.

Por tanto $f^{-1}(I)$ es un ideal en A.

CAPITULO III

DIVISORES DE CERO. ELEMENTOS NILPOTENTES. UNIDADES.

3.1 DIVISORES DE CERO.

3.1.1 DEFINICION.

Un divisor de cero en un anillo A es un elemento x - que "divide cero", es decir para el cual existe un - $y \neq 0$ en A tal que $xy = 0$.

3.1.2 EJEMPLOS.

a) Sea A el anillo de las matrices cuadradas y sean C, B $\in$ A tal que:

$$C = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix}$$

entonces:

$$B.C = \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore$ c "divide cero".

b) Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ no tienen divisores de cero. Es decir, en cada sistema $xy = 0$ implica siempre o bien $x = 0$ o bien $y = 0$.

3.1.3 DEFINICION.

Un anillo A sin divisores de cero distintos de cero - (y en el cual $1 \neq 0$) se denomina "DOMINIO DE INTEGRIDAD".

3.1.4 PROPOSICION.

En un dominio de integridad A se cumple la ley de cancelación para la multiplicación.

DEMOSTRACION:

Sean $x,y,z \in A$, con $z \neq 0$, tales que

$xz = yz$	(Por hipótesis)
$xz - yz = 0$	(Sumando el inverso de yz a la derecha)
$(x-y)z = 0$	(Ley distributiva)
$x - y = 0$	(Como A es dominio de integridad no tiene divisores de cero).
$x = y$	(Sumando a la derecha el inverso - de -y).

3.1.5 PROPOSICION.

El conjunto Z de los números enteros es un dominio de integridad.

DEMOSTRACION:

Sea $x,y \in Z$ tales que $xy = 0$ para algún $y \neq 0$, como $Z \subset Q$ existe $\frac{1}{y} \in Q$, entonces

$(xy)\frac{1}{y} = 0.\frac{1}{y}$ (Multiplicando a la derecha por $\frac{1}{y}$)

$x.(y.\frac{1}{y}) = 0$ (Ley asociativa y v de proposición 1.1.7)

$x.1 = 0$ (Existencia de inverso multiplicativo en Q).

$x = 0$ (1 es neutro en el producto).

3.2 ELEMENTOS NILPOTENTES.

3.2.1 DEFINICION.

Un elemento $x \in A$ es nilpotente si $x^n = 0$ para algún $n > 0$.

3.2.2 PROPOSICION.

Si $x \in A$, $x \neq \{0\}$ ($\{0\}$ el anillo cero) es un elemento nilpotente, entonces x es divisor de cero.

DEMOSTRACION:

Para que $x \in A$ sea divisor de cero debe existir $y \neq 0$ en A tal que $xy = 0$.

Sea n el menor entero positivo tal que $x^n = 0$, entonces $x^{n-1} \neq 0$, entonces:

$x^n = 0$ Para algún $n > 0$ (hipótesis)

$x.x^{n-1} = 0$ (Por propiedad de producto de potencias iguales).

luego x es divisor de cero porque x^{n-1} es distinto de cero ya que n es el menor entero positivo que hace $x^n = 0$.

3.2.3 NOTA:

La recíproca de la proposición 3.2.2 no se cumple en general, es decir,

"$x \in A$ es divisor de cero" $\not\Rightarrow$ "$x \in A$ es nilpotente".

POR EJEMPLO:

Sabemos que $c = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}$ es un divisor de cero ya que existe $B = \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix}$ tal que $B.C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, sin em - bargo $\begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}^n \neq 0$ para todo $n \in \mathbb{N}$.

En efecto:

Para $n = 2$, $\begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 0 & 1 \end{pmatrix}$

Para $n = 3$, $\begin{pmatrix} 0 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & - \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}$

.
.
.

Para n par . . . $A = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}^n = \begin{pmatrix} 0 & -2 \\ 0 & 2 \end{pmatrix}$

Para n impar . . . $A = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}^n = \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}$

3.3 UNIDADES.

3.3.1 DEFINICION

Una unidad en un anillo A es un elemento x que "divi-

de 1", es decir para el cual existe un elemento - $y \neq 1$ en A tal que $xy = 1$.

3.3.2 PROPOSICION.

Si $x \in$ es una unidad en A el elemento $y \in A$ está unívocamente determinado por x; se escribe x^{-1} o $\frac{1}{x}$

DEMOSTRACION:

Sea x una unidad en A, esto es $xy = 1$ para algún - $y \in A$, $y \neq 1$. Sea $xz = 1$ para algún $z \in A$, $z \neq 1$. A probar que $y = z$.

$xy = 1 \Rightarrow z(xy) = z.1$ (Multiplicando por x a la izquierda)

$\Rightarrow (zx)y = z$ (Asociatividad y existencia de idéntico).

$\Rightarrow 1.y = z$ (Por hipótesis z también es unidad).

$\Rightarrow y = z$ (1 es neutro en el - producto).

Luego y es único.

3.3.3 PROPOSICION.

Las unidades en A forman un grupo abeliano multi - plicativo.

DEMOSTRACION:

Bastará probar cierre y existencia de elemento inver so las demás propiedades se heredan del anillo. Cie rre.

Sean x_1, x_2 unidades en A, entonces:

$x_1 y = 1$ para algún $y \varepsilon A$, $y \neq 1$ (Defin. 3.3.1)

$x_2 z = 1$ para algún $z \varepsilon A$ $z \neq 1$ (Defin. 3.3.1)

Luego $(x,y)(x_2 z) = 1.(x_2 z) = 1.1$ (Multiplicando a - la derecha por - $x_2 z$)

$x_1 (y x_2 z) = 1$ (Ley asociativa)

$x_1 (x_2 y z) = 1$ (Ley conmutativa)

$(x_1 x_2)(yz) = 1$ (Ley asociativa)

Como $y \neq 1$ y $z \neq 1$, entonces $yz \neq 1$, entonces por definición 3.3.1 $x_1 x_2$ es una unidad en A; signifi-

ca que el conjunto de unidades en A es cerrado respecto al producto.

"EXISTENCIA DE INVERSO"

Por proposición 3.3.2 Si x es unidad en A existe $x^{-1} = \frac{1}{x}$ tal que $xx^{-1} = 1$, entonces x^{-1} es el inverso de x.

3.3.4 PROPOSICION.

Los múltiplos **a**x de un elemento $x \in A$ forman un ideal denominado "Ideal principal". Este ideal se denota por $[x]$, es decir,

$[x] = \{ax / a \in A$ y x es un elemento dado de A$\}$.

DEMOSTRACION.

$[x] \subset A$ ya que para todo $a \in A$ y $x \in A$ $ax \in A$ (A es anillo).

Sean $m,n \in [x]$, $m = ax$ para algún $a \in A$ y $n = bx$ para algún $b \in A$. Entonces

$m - n = ax - bx = (a-b)x$ (Por ley distributiva)

Como $a-b \in A$ por ser A un anillo $(a-b)x \in [x]$, entonces $m-n \in [x]$; lo que demuestra que $[x]$ es un subgrupo de A.

Sea $y \in A$ y $m \in [x]$, $m = ax$ para algún $a \in A$.

$ym = y(ax) = (ya)x \in [x]$, porque $ya \in A$. Entonces $A[x] \subset [x]$.

Por tanto $[x]$ es un ideal de A.

3.3.5 NOTA:

El ideal principal $[x]$ se dice que es generado por $x \in A$. x es el generador de $[x]$. El ideal generado por cero $[0] = \{0\}$.

3.3.6 PROPOSICION.

$[x] = A \iff x$ es una unidad en A.

DEMOSTRACION.

" => "

$1 \in [x]$; ya que $[x] = A$ y A es un anillo conmutativo con identidad, entonces:

$ax = 1$; ya que $[x] = \{ax / a \in A$ y x dado en $A\}$.

$\therefore$ x es una unidad en A por definición 3.3.1.

" "
<=

$m \in [x] \Rightarrow m = ax$ (Proposición 3.3.4)

$\Rightarrow m \in A$ (A es un anillo)

$\Rightarrow [x] \subset A$ (m es un elemento cualquiera de $[x]$).

Ahora sea $y \in A$ y $xz = 1$, para algún $z \in A$, (x es unidad en A), entonces:

$y(xz) = y.1$ (Multiplicando por $xz = 1$ a la derecha)

$y(zx) = y$ (Conmutatividad y existencia de elemento idéntico para el producto).

$(yz)\, x = y$ (Asociatividad en el anillo A)

$(yz)\, x \in [x]$ ($yz \in A$)

$y \in [x]$ (Sustituyendo por su igual)

$A \subset x$ (Y es un elemento cualquiera de A)

$\therefore [x] = A$.

3.3.7 COROLARIO.

$A = [1]$

DEMOSTRACION.

Si $[1]$ es ideal generado por 1, entonces $[1] = \{x.1 / x \in A\} = \{x / x \in A\}$, ya que 1 es idéntico en A, entonces $[1] = A$.

3.3.8 DEFINICION.

Un anillo A en el que $1 \neq 0$ y cada elemento no nulo es una unidad es llamado cuerpo.

3.3.9 PROPOSICION.

Todo cuerpo es también un dominio de integridad.

DEMOSTRACION.

Sean $x,y \in A$ (A cuerpo) tal que $xy = 0$ y $y \neq 0$, entonces existe $y^{-1} \in A$ tal que $xy^{-1} = 1$

$(xy)y^{-1} = 0.y^{-1}$ (Multiplicando a la derecha por y^{-1}).

$x(yy^{-1}) = 0$ (Asociatividad en A y V de - proposición 1.1.7)

$x.1 = 0$ (Por proposición 3.3.2)

$x = 0$ (1 es el elemento neutro del producto en A).

Significa que A no tiene divisores de cero, entonces por definición 3.1.3 A es un dominio de integridad.

3.3.10 NOTA:

La recíproca de la proposición 3.3.9 no es generalmente cierta, ya que Z el conjunto de los números enteros es un dominio de integridad (Proposición 3.1.5), pero a excepción 1, $-1 \in Z$ ningún otro elemento tiene inverso multiplicativo, por tanto Z no es un cuerpo.

3.3.11 PROPOSICION.

Sea A un anillo, $A \neq \{0\}$, las siguientes afirmaciones son equivalentes.

i) A es un cuerpo.

ii) Los únicos ideales de A son $\{0\}$ y $[1] = A$, es decir un cuerpo no tiene ideales propios.

iii) Cada homomorfismo de A en un anillo no nulo B es inyectivo.

DEMOSTRACION.

i => ii

Si $I \neq \{0\}$ es un ideal de A y $x \in I$, $x \neq 0$, x es unidad porque A es un cuerpo, entonces $[x] = A = [1]$ por proposición 3.3.6 y 3.3.7 de - donde $[1] = [x] \subset I$. Además como I es ideal de A, $I \subset A$. Por tanto $I = A = [1]$. Por otra parte en proposición 2.1.3 se probó que {0} es un ideal de A.

ii => iii

Sea $\phi : A \to B$ un homomorfismo de anillos, entonces Ker ϕ es un ideal de A (Proposición 2.2.7) - Ker $\phi = [1]$ ó Ker $\phi = \{0\}$ (Por ii), pero Ker $\phi \neq [1]$ (Porque $\phi(1) = 1$ por propiedad de homomorfismo), entonces Ker $\phi = \{0\}$, por tanto ϕ es inyectiva (Por - Proposición 2.2.6).

iii => i

Sea x un elemento de A que no es una unidad. - Entonces $[x] \neq [1]$ (Por proposición 3.3.6) Por tanto $B = \frac{A}{[x]}$ no es el anillo {0} ya que $1 + [x] \neq [x]$ porque si $1 + [x] = [x]$, $1 \in [x]$ (Por corolario 2.2.2).

lo cual es contrario a la hipótesis de que x no es - una unidad. Sea $\phi : A \to B$ el homomorfismo natural, con núcleo $[x]$ (el cero del anillo cociente). Por - hipótesis ϕ es inyectiva, entonces $[x] = \{0\}$, por nota 3.3.5 $x = 0$, por tanto A es un cuerpo (Definición 3.3.8).

CAPITULO IV

IDEALES PRIMOS E IDEALES MAXIMALES.

4.1 IDEALES PRIMOS.

4.1.1 DEFINICION.

Un ideal P en A es primo si $P \neq A$

y si $x\,y \in P \Rightarrow x \in P$ o $y \in P$.

4.1.2 PROPOSICION.

P es primo si y sólo si $\frac{A}{P}$ es un dominio de integri_

dad.

" => " "P es primo => $\frac{A}{P}$ es un dominio de integridad

Sean $(a + P)$, $(b + P) \in \frac{A}{P}$ tales que:

$(a + P)\,(b + P) = ab + P = P$ (hipótesis)

$ab + P = P \Rightarrow ab \in P$ (Corolario 2.2.2)

$\Rightarrow a \in P$ ó $b \in P$ (P es primo)

$\Rightarrow a+P = P$ ó

$b+P = P$ (Corolario 2.2.2)

$\Rightarrow \frac{A}{P}$ es un dominio de integridad ya que

como P es el cero del anillo cociente, se cumple la

definición 3.1.3.

" => " "$\frac{A}{P}$ es un dominio de integridad => P es primo".

a) $P \neq A$

Si $P = A \Rightarrow \frac{A}{P} = \frac{A}{A}$ (Por sustitución)

$\Rightarrow A = 0 = 1$ (A es el cero del anillo cociente y 1+A = A es - la unidad)

$\Rightarrow \frac{A}{P}$ no es domi- nio de integri dad. (Definición 3.1.3).

$\Rightarrow P \neq 0$ (Por hipótesis $\frac{A}{P}$ es dominio de integridad)

b) $ab \in P \Rightarrow ab + P = P$ (Corolario 2.2.2)

$\Rightarrow (a+P)(b+P) = P$ (Definición 2.2.3)

$\Rightarrow a + P = P$ ó

$b + P = P$ ($\frac{A}{P}$ es un dominio de integridad)

$\Rightarrow a \in P$ ó

$b \in P$ (Corolario 2.2.2)

$\therefore$ P es Primo (Definición 4.1.1)

4.1.3 PROPOSICION.

El ideal cero ($\{0\}$) es primo si y sólo si es un dominio de integridad.

" => "

Sean $x,y \in A$ tal que $xy = 0$ (hipótesis), entonces $xy \in \{0\}$, como $\{0\}$ es primo $x \in \{0\}$ ó $y \in \{0\}$, luego $x = 0$ ó $y = 0$; se cumple entonces la definición - 3.1.3 y por consiguiente A es un dominio de integridad.

" => "

a) Como A es un dominio de integridad $1 \neq 0$, entonces $[\overline{1}] \neq \{0\}$.

b) Por otra parte: Si $xy \in \{0\}$ => $xy \in A$ ($\{0\}$ es ideal de A).

=> $xy = 0$ (Por definición - de $\{0\}$).

=> $x=0$ ó $y=0$ (xy está en el dominio de integridad A).

$\therefore$ $\{0\}$ es un ideal primo en A (Definic. 4.1.1)

OBSERVACION:

Que {0} es un ideal se probó en proposición 2.1.3.

4.1.4 PROPOSICION.

Si $f : A \to B$ es un homomorfismo de anillos y K es un ideal primo en B, entonces $f^{-1}(K)$ es un ideal primo en A.

$$f^{-1}(K) = \{x \in A \ / \ f(x) \in K\}.$$

DEMOSTRACION:

a) $f^{-1}(K)$ es un ideal de A.

$f^{-1}(K) \neq \phi$ ya que $o \in f^{-1}(K)$ porque como f es homomorfismo $f(0) = 0 \in K$ ya que K es un ideal en B.

Sean $a,b \in f^{-1}(K)$, entonces $a,b \in A$ y $f(a)$, $f(b) \in K$. Como K es un ideal $f(a) - f(b) \in K$, pero $f(a) - f(b) = f(a) + f(-b) = f(a-b)$ (Por propiedad de homomorfismo), entonces $f(a-b) \in K$ y $a-b \in f^{-1}(K)$.

Luego $f^{-1}(K)$ es un subgrupo de A.

Sean $m \in A$ y $n \in f^{-1}(K)$, entonces: n también está en A. Además $f(m) \in B$ y $f(n) \in K$. Como K es ideal en B $f(m)\ f(n) \in K$, pero $f(m)\ f(n) = f(mn)$ (Por propiedad de homomorfismo), entonces $f(mn) \in K$ y $mn \in f^{-1}(K)$. Por consiguiente $A\ f^{-1}(K) \subset f^{-1}(K)$.

Por tanto $f^{-1}(K)$ es un ideal en A.

b) Probaremos que $f^{-1}(K)$ es primo.

$1 \in f^{-1}(K) \Rightarrow f(1) = 1 \in K$ (Por propiedad de homomorfismo)

$\Rightarrow K = [1] = B$ (Corolario 3.3.7)

$\Rightarrow$ K no es primo (Definición 4.1.1)

Pero K es primo $\Rightarrow 1 \notin f^{-1}(K)$

$\Rightarrow f^{-1}(K) \neq [1] = A.$ (Corolario 3.3.7)

Por otra parte:

$ab \in f^{-1}(K) \Rightarrow f(ab) \in K$ (Por definición de $f^{-1}(K)$).

$\Rightarrow f(a)\ f(b) \in K$ (Por propiedad de homomorfismo).

$\Rightarrow f(a) \in K$ ó

$b(b) \in K$ (K es primo)

$\Rightarrow a \in f^{-1}(K)$ ó

$b \in f^{-1}(K)$ (Por definición $f^{-1}(K)$)

$\therefore f^{-1}(K)$ es un ideal Primo en A.

4.2 IDEALES MAXIMALES.

4.2.1 DEFINICION.

Un ideal M en A es maximal si $M \neq A$ y no existe ningún ideal I, $I \neq A$ e $I \neq M$, tal que $M \subset I \subset A$.

4.2.2 PROPOSICION.

M es maximal $\Leftrightarrow \frac{A}{M}$ es un cuerpo.

DEMOSTRACION.

" $\Rightarrow$ "

Para demostrar que $\frac{A}{M}$ es un cuerpo hay que demostrar que todo elemento no nulo de $\frac{A}{M}$ tiene inverso multiplicativo.

Sea $p + M \in \frac{A}{M}$ tal que $p + M \neq M$ (hipótesis), entonces $p \notin M$ (por Corolario 2.2.2)

Consideremos el conjunto $I = [p, M]$ (Ideal generado por P y M).

$$I = \{a + px \;/\; a \in M \wedge x \in A\}$$

$M \subset I$, ya que para todo $a \in M$, $a = 1 + p.0$.

¿I es un ideal en A?

$I \neq \phi$ porque $0 \in I$ ya que $0 = 0 + p.0$ y $0 \in M$ y $0 \in A$.

$z, z' \in I \Rightarrow z = a + px$ y $z' = b + py$, con $a,b \in M$ y $x,y \in A$.

$z+z' = (a + px) + (b + py) = (a+b) + P(x + y)$, con $a + b \in M$ y $x+y \in A$, entonces $z + z' \in I$. Luego I es cerrado con respecto a la suma. Además $- z = -(a + px) = - a - px = - a + p(-x)$, con $a \in M$ y $-x \in A$ entonces $-z \in I$.

Luego I es un subgrupo de A.

Sean $m \in A$ y $z \in I$, entonces $z = a+px$, con $a \in M$ y $x \in A$. Luego $mz = m(a + px) = ma + (mp)x$; como $ma \in M$ por ser M ideal en A y $mp \in A$, por ser A anillo, entonces $mz \in I$.

Por tanto I es un ideal en A.

Por otra parte $p \in I$, ya que $p = 0 + p.1$, y $p \notin M$, entonces $I \neq M$; con lo que se concluye que existe un ideal I en A tal que $M \subset I$ y como M es maximal (por hipótesis) $I = A$. Entonces $y \in A$ se puede escribir en la forma: $1 = a + p.x$, entonces:

$1 + M = (a + p.x) + M$

$= (a + M) + (px + M)$

$= M + (px + M)$ (Ya que $a \in M$ y por proposición $a \in M \Rightarrow a+M=M$)

$= px + M$ (M es el cero del anillo cociente $\frac{A}{M}$)

$= (p + M)\ (x + M)$ ($p, x \in A \Rightarrow (p+M)(p+M) = px + M$).

$(p + M)\ (x + A) = 1 + M \Rightarrow x + M$ es el inverso multiplicativo de $p + M \in \frac{A}{M}$; ya que $1 + M$ es el idéntico del anillo cociente.

$\therefore$ $\frac{A}{M}$ es un cuerpo (Definición 3.3.8)

" <= "

$\frac{A}{M}$ es un cuerpo a probar que M es maximal en A.

Supongamos que M no es maximal en A, implica que existe un ideal I c A, $I \neq M$ e $I \neq A$, tal que M c I C A. Probaremos que I = A con lo cual se contradice la hipótesis de que M no es maximal por lo tanto M es maximal.

Sea r un elemento cualquiera de A y p un elemento cualquiera de I - M, definiremos $(p + M)^{-1} (r + M) = S + M$, entonces:

$r + M = (p + M)(s + M)$ ($\frac{A}{M}$ es un cuerpo y porque como $p \notin M$, $p + M \neq M$)

$\Rightarrow r + M = ps + M$ (Por definición 2.2.3)

$\Rightarrow (r - ps) + M = M$ (Sumando a ambos miembros -ps)

$\Rightarrow r - ps \in M$ (Corolario 2.2.2)

$\Rightarrow r - ps \in I$ (Por hipótesis M c I)

$\Rightarrow r \in I$ (Por hipótesis $p \in I$)

Luego A c I y como por hipótesis, también, I C A; I = A. Por tanto M es maximal.

4.2.3 NOTA: La proposición de maximales correspondiente a la proposición 4.1.4 no es generalmente cier-

ta, es decir, si $f: A \to B$ es un homomorfismo de anillos y M es un ideal maximal en B esto no implica necesariamente que $f^{-1}(M)$ sea un ideal maximal en A.

Por ejemplo:

Sea $A = Z$ (anillo de los enteros) y $B = Q$ (anillo de los racionales) sin embargo $M = \{0\}$ es un maximal en Q, pero $f^{-1}(M) = f^{-1}(\{0\})$ no es un maximal en Z.

DEMOSTRACION:

Q es un cuerpo, entonces los únicos ideales de Q son $\{0\}$ y $[1] = Q$ (Proposición 3.3.11). Además $\{0\} \neq [1] = Q$, ya que $1 \neq 0$ en Q, por consiguiente $\{0\}$ es maximal - (definición 4.2.1).

Por otra parte $f : Z \to Q : x \rightsquigarrow x$ es un homomorfismo de anillos (Por proposición 1.2.2) y $[m] = m\,Z = \{x \in Z \,/\, m \text{ divide a } x\}$ para algún número natural m, $m \neq 1$ y $m \neq 0$, es un ideal en Z generado por m ; $\{0\} \subset [m]$ ya que $0 = m.0 \in [m]$, por consi - guiente $\{0\}$ no es un maximal en Z.

4.2.4 PROPOSICION.

Si M es maximal en A, M es primo.

DEMOSTRACION:

$ab \in M$ y $a \notin M \Rightarrow M \subset [a,M]$ (Ideal generado por a y M, similar al que se usó en la demostración de la proposición 4.2.2).

Como M es maximal $[a,M] = A$. Entonces,

$1 = ca + m$ para algún $c \in A$ y algún $m \in M$. Multiplicando por $b \in M$ tenemos $b = cab + mb$.

$b \in M$, $b \in A$; (ab $\in$ A y como mb $\in$ M por ser M ideal, entonces $b = cab + mb \in [a,M]$ (Por definición de $[a,M]$). Como ab $\in$ M, cab $\in$ M por ser M ideal de A, entonces cab + mb $\in$ M.

Luego b $\in$ M y por sonsiguiente M es primo.

4.2.5 PROPOSICION.

Cada anillo $A \neq \{0\}$ tiene por lo menos un ideal maximal.

(Esta proposición es una aplicación del Lema de Zorn

por lo que recordaremos, previo a la demostración, dicho lema).

4.2.5.1 DEFINICION.

Si R es una relación en A tal que:

i) $a \, R \, a$ Para todo $a \in A$ (R es reflexiva)

ii) $a \, R \, b$ y $b \, R \, a \Rightarrow a=b$ (R es antisimétrica)

iii) $a \, R \, b$ y $b \, R \, c \Rightarrow a \, R \, c$ (R es transitiva)

A es un conjunto ordenado.

Si existen $m,n \in A$ tal que $m \not R \, n$ y $n \not R \, m$, se dice que A es un conjunto parcialmente ordenado.

4.2.5.2 DEFINICION.

Una cadena en A es un subconjunto S de A tal que para todo $a,b \in S$, o bien $a \, R \, b$ ó $b \, R \, a$.

4.2.5.3 DEFINICION.

Si en un conjunto A, ordenado por la relación "$\leq$", existe $u \in A$ tal que $a \leq u$ para to-

do $a \in A$, diremos que u es el último elemento de A.

4.2.5.4 DEFINICION.

Si en un conjunto A, ordenado por la relación "$\leq$", existe $m \in A$ tal que, para todo $a \in A$, $m \leq a \Rightarrow a = m$, diremos que m es un elemento maximal.

4.2.5.5 LEMA DE ZORN.

"Si cada cadena (Conjunto total o linealmente ordenado) S en A tiene una cota superior en A, entonces A tiene, por lo menos, un elemento maximal".

DEMOSTRACION PROPOSICION 4.2.5.

Sea $\sum = \{T \subset A \ / \ T \text{ es un ideal en } A \text{ y } T \neq A\}$.

Ordenemos $\sum$ por la relación "C" (inclusión).

$\sum \neq \phi$ ya que $\{0\} \in \sum$ y $\{0\} \neq A$ es un ideal en A.

Sea $M = (P_i)_{i \in I}$ una cadena en $\sum$ de manera que para cada par de índices $i_1 \in I$ e $i_2 \in I$ $P_{i_1} \subset P_{i_2}$ o $P_{i_2} \subset P_{i_1}$.

Sea $T = \bigcup_{i\in I} P_i$, demostraremos que T es un ideal.

a) $T \neq \phi$ (ya que como al menos $\{0\} \in \sum$, $0 \in \bigcup_{i\in I} P_i$).

b) $x,y \in T \Rightarrow x \in P_{i_1}$ y $y \in P_{i_2}$; como estamos en una cadena $x,y \in P_{i_1}$ ó $x,y \in P_{i_2}$ y por ser los P_i ideales $x-y \in P_{i_1}$ ó $x-y \in P_{i_2}$, entonces $x-y \in \bigcup_{i\in I} P_i = T$ por lo que T es un subgrupo aditivo de A.

c) Sea $x \in \bigcup_{i\in I} P_i$, entonces $x \in P_i$ para algún $i\in I$, si $y \in A$, $xy \in P_i$ ya que los P_i son ideales en A; por consiguiente $xy \in \bigcup_{i\in I} P_i$. Luego $AT \subset T$.

$\therefore$ T es un ideal en A.

Por otra parte.

Como $1 \notin T$ puesto que $1 \notin P_i$ ya que $P_i \neq A$ por pertenecer a $\sum$, entonces $T \neq A$.

T es cota superior en $\sum$, ya que para un ideal $P_i \in M$, $P_i \subset \bigcup_{i\in I} P_i$, luego por el Lema de Zorn exis

te por lo menos un elemento maximal en $\sum$.

Ahora probaremos que si M es maximal en $\sum$, M es maximal en A.

Supongamos que M no es maximal en A, entonces existe L ideal en A tal que: $M \subset L$ y $L \neq A$, pero si $L \neq A$, entonces $L \in \sum$ de donde $M = L$. Por tanto M maximal en A.

4.2. 6 COROLARIO.

Si $I \neq A$ es un ideal en A, existe un ideal maximal de A que contiene a I.

DEMOSTRACION:

Sea $H = \{M/M \text{ ideal}, I \subset M, M \neq A\}$

$H \neq \phi$ ya que $I \subset H$.

Ordenemos H por inclusión y sea B una cadena de H.

$N = \bigcup_{\alpha \in B} I_\alpha \Rightarrow N \in H$ (Ya que $I_\alpha \subset N$, para todo $I_\alpha \in B$)

$\Rightarrow N \neq A$ (Por definición de H)

$\Rightarrow$ N es cota superior de B ($1 \notin N$)

=> H posee al menos un elemento maximal (por el Lema de Zorn).

=> N es maximal en A (Por proposición - 4.2.5)

.'. existe en A un maximal que contiene a I

4.2.7 PROPOSICION.

Cada elemento de A que no es una unidad está contenido en un ideal maximal.

DEMOSTRACION:

Sea $x \in A$ tal que x no es una unidad en A. Entonces $[x] \neq A$ (ya que si $[x] = A \Rightarrow x$ es unidad en A por proposición 3.3.6).

Luego por el Corolario 4.2.6 podemos asumir que existe un ideal maximal M en A tal que $[x] \subset M$, como x es el generador de $[x]$, $x \in [x]$.

.'. $x \in M$.

4.2.8 PROPOSICION.

Si A es un cuerpo A posee únicamente un ideal maximal.

DEMOSTRACION:

$A \neq \{0\}$ porque A es un cuerpo y un cuerpo es diferente del anillo $\{0\}$ (Por proposición 3.3.11).

Los únicos ideales de A son $\{0\}$ y $[1]$ (Propos. 3.3.11)

$[1]$ no es maximal en A porque $[1] = A$, pero como cada anillo $A \neq \{0\}$ tiene por lo menos un ideal maximal (Proposición 4.2.5), entonces el único ideal maximal de A es el ideal $\{0\}$.

4.2.9 DEFINICION.

Un anillo A° que tiene exactamente un ideal maximal M se denomina "Anillo local". El cuerpo $\frac{A}{M}$ se denomina "Cuerpo residual de A".

4.2.10 PROPOSICION.

Sea A un anillo y $M \neq [1]$ un ideal de A tal que $x \in A - M$ es una unidad en A. Entonces A es un anillo local y M su ideal maximal.

DEMOSTRACION:

Si $M \neq [1]$ es un ideal en A, existe $N \subset A$, N ideal -

maximal en A tal que M C N (Corolario 4.2.6). Sea $x \in N$, entonces x no es unidad en A ya que $N \neq [1]$ por ser maximal, entonces $x \notin A - M$ y $x \in M$ por lo que N C M. Luego $M = N$ (Por doble inclusión). Por tanto M es ideal maximal en A y es el único maximal en A ya que N fué seleccionado arbitrariamente.

$\therefore$ A es un anillo local y M su ideal maximal.

4.2.11 PROPOSICION.

Sea A un anillo y M un ideal maximal en A tal que cada elemento de $1 + M$ es una unidad en A. Entonces A es un anillo local.

DEMOSTRACION:

Sean $1 + M = \{1 + x \ / \ x \in M\}$ un conjunto de unidades en A, $x \in A - M$ y $[x] + M = \{ yx + m / y \in A \wedge m \in M \}$ el ideal generado por x,m. M c $[x] + M$ (ya que $0.b + m = m \in M$), entonces $[x] + M = [1]$ por ser M - maximal. Por tanto existe $y \in A$ y $t \in M$ tal que $yx + t = 1$; luego $yx = 1-t \in y + M$ (Porque $yx = 1 - t = 1 + (-t)$ y $(-t) \in M$) y por tanto yx es una unidad en A, entonces $yx \in A - M$.

$\therefore$ A es anillo local (Por proposición 4.2.10)

4.2.12 PROPOSICION.

En el anillo Z de los enteros.

a) Todo ideal es principal.

b) $[m]$ es primo $\Leftrightarrow$ $m = 0$ ó m es primo.

c) Si m es primo, $[m]$ es maximal.

d) Si m es primo, $\frac{Z}{[m]}$ es un campo de m elementos.

DEMOSTRACION:

a) "Todo ideal en Z es principal".

Sea I un ideal en Z.

$I = \{0\}$, entonces $I = \{mx / x=0 \text{ y } m \in Z\}$. Como cada elemento de Z es de la forma mx con $m \in Z$ y x fijo, I es ideal principal en Z.

$I \neq \{0\}$; si $a \in I$, entonces por ser I ideal $-a \in I$, entonces I contiene enteros positivos (ya que si $a < 0$, $-a > 0$ o viceversa).

Como Z^+ es bien ordenado I, contiene un entero positivo mínimo, sea e.

Sea $b \in I$, entonces $b = e.q + r$

con $q,r \in Z$ y $0 \leq r < e$. (Por el algoritmo de la división).

Como $b \in I$, $e.q \in I$ luego $r = 0$.

$(b = e.q + r)$.

Entonces $b = e.q < I = \{e.q/e \text{ fijo en } I \text{ y } q \in Z\}$

$\therefore$ I es un ideal principal en Z.

b) "$[m]$ es primo $\Leftrightarrow$ $m = 0$ ó m es primo".

" $\Rightarrow$ "

$[m]$ es primo $\Rightarrow$ $m = 0$ o m es primo

Supongamos:

$m \neq 0$ y m no primo; entonces m puede descomponerse en un conjunto de factores primos, porque $m \in Z$.

Sea $(X_i)_{i \in I}$ el conjunto de factores primos de m, es decir $m = x_1 . x_2 . x_3 \ldots . x_n$

$x_i \notin [m]$ $\forall_{i \in I}$ (ya que como x_i es primo no puede expresarse como mx, $x \in Z$).

$m = (x_1 \cdot x_2 \cdot x_3 \ldots x_{n-1})$. $x_n \in [m]$ no implica que $(x_1 \cdot x_2 \cdot x_3 \ldots x_n) \in [m]$ ó $x_n \in [m]$, entonces $[m]$ no es primo.

Pero esto es contrario a la hipótesis de que $[m]$ es primo. Luego m es primo.

" <= "

$m = 0$ ó m es primo => $[m]$ es primo.

$m = 0 \in Z$ => $[m]$ es un ideal primo en Z (Proposición 4.2.12.a)

Sea m un número primo y $[m] = \{p/p = mx, x \in Z\}$

Sean $x,y \in Z$ tal que $xy \in [m]$, entonces:

$xy = mk$, para algún $K \in Z$, entonces $m|xy$; luego $m|x$ o $m|y$, por ser m primo en Z.
Entonces $x = mz$ ó $y = mz$, para algún $z \in Z$, entonces $x \in [m]$ ó $y \in [m]$ y por tanto $[m]$ es primo. (Definición 4.4.1).

c) "Si m es primo, $[m]$ es maximal".

Supongamos que $[m]$ no es maximal, entonces existe $I \subset Z$, $I \neq Z$ e $I \neq [m]$ y $[m] \subset I$ (Por definición 4.2.1).

$x \in I$ y $x \notin [m] \Rightarrow x \neq mt$, para todo $t \in Z$.

$\Rightarrow$ m no divide a x.

$\Rightarrow$ El m.c.d. de xy m es 1.

Entonces podemos expresar 1 como una combinación lineal de x y m, es decir:

$1 = ax + bm$. Como I es un ideal de Z,

$a,b \in Z$ yz, $m \in I \Rightarrow ax, bm \in I$ y

entonces $1 = ax + bm \in I$ por lo que

$I = [1] = Z$. Por tanto $[m]$ es maximal en Z.

d) "Si m es primo, $\frac{Z}{[m]}$ es un campo de m elementos."

Por c) si m es primo, $[m]$ es maximal

entonces $\frac{Z}{[m]}$ es un campo. (Proposición 4.2.2)

$\frac{Z}{[m]}$ tiene m elementos ya que

$$\frac{Z}{[m]} = \{0 + [m], 1 + [m], 2 + [m], \ldots (m-1) + [m]\}$$

donde $[m] = \{a \in Z / a \equiv r \pmod{m}\}$

Ahora demostraremos que para cualquier $x \in Z$

$$r + [m] \quad \frac{Z}{[m]} \text{ , siempre que } 0 \leq r < m$$

$$\text{Sea } x \in Z \Rightarrow \begin{array}{l|l} x & m \\ \hline r & a \end{array} \qquad \text{(Teorema del residuo)}$$

$$\Rightarrow x = am + r \;;\; 0 \leq r < m$$

$$\Rightarrow x - r = am$$

$$\Rightarrow x - r \in [m] \qquad (am \in [m])$$

$$\Rightarrow (x - r) + [m] = [m] \qquad \text{(Corolario 2.2.2)}$$

$$(x + [m]) - (r + [m]) = [m]$$

$$x + [m] = [m] + (r + [m])$$

$$x + [m] = r + [m] \;;\; 0 \leq r < m$$

$$\Rightarrow r + [m] \in \frac{Z}{[m]} \quad \left(x + [m] \in \frac{Z}{[m]}\right)$$

Verificaremos ahora que los elementos de $\frac{Z}{[m]}$ son distintos.

Sean $r.q \in Z$, $0 \leq r < m \wedge 0 \leq q < m$

$$r \neq q \Rightarrow r + [m] = q + [m]$$

Supongamos que $r + [m] = q + [m]$.

$r \in r + [m]$ $\quad (r = 0.m)$

$\Rightarrow r \in q + [m]$ $\quad (r + [m] = q + [m])$

$\Rightarrow r = q + bm$ $\quad$ (Definición de $q + [m]$).

$\Rightarrow q = r$ $\quad$ (Teorema del residuo)

$\therefore \frac{Z}{[m]}$ es un campo de m elementos.

4.2.13 DEFINICION.

Un dominio de integridad en el que cada ideal es - principal llámase DOMINIO DE IDEALES PRINCIPALES.

4.2.14 PROPOSICION.

Si A es un dominio de ideales principales y $J \subset A$ es un ideal primo y $J \neq \{0\}$ entonces J es un ideal maximal.

DEMOSTRACION:

Supongamos que $J \subset A$ no es maximal, entonces existe $I \subset A$ tal que $J \subset I \subset A$, $I \neq J$ e $I \neq A$.

Como A es un Dominio de ideales principales:

$J = [x] = \{x.b/b \in A\}$ e $I = [y] = \{y.m/m \in A\}$,

$x \in J \Rightarrow x \in I$ (Por hipótesis $J \subset I$)

$\Rightarrow x = ym$, para algún $m \in A$. (I es el ideal generado por y)

$\Rightarrow y\ m \in J$ y $y \notin J$ ($J \subset I$ e $J \neq I$)

$\Rightarrow m \in J$ (Ya que J es primo)

$\Rightarrow m = b.x$ para algún $b \in A$. (J es el ideal generado por x).

$\Rightarrow x = ym = ymx$ (Sustituyendo m por su igual)

$\Rightarrow 1 = ym$ ($1.x = ymx$ y A es un dominio de integridad)

Luego $I = [y] = [1] = A$.

$\therefore$ J es un ideal maximal en A.

CAPITULO V

NILRADICAL Y RADICAL DE JACOBSON.

5.1 NILRADICAL.

5.1.1 DEFINICION.

El conjunto de todos los elementos nilpotentes en un anillo A se denomina "NILRADICAL" de A.

5.1.2 PROPOSICION.

Si N denota el nilradical de A entonces N es un ideal y el nilradical de $\frac{A}{N}$ tiene sólo un elemento.

DEMOSTRACION:

N es ideal en A.

a) Sea $x, y \in N$, entonces para algún $m > 0$ y para algún $n > 0$, $x^m = 0$ y $x^n = 0$

(N es el conjunto de todos los elementos nilpotentes en A).

$(x+y)^{m+n-1}$ es una suma de múltiplos enteros de productos $x^r y^s$, donde $r+s = m+n-1$

(Por el teorema del binomio que es válido en todo anillo conmutativo).

$x^r y^s = 0$ y $(x+y)^{m+n-1} = 0$

(Ya que $r < m$ y $s < n$ no pueden presentarse simultáneamente).

Luego $x+y$ es nilpotente.

(Porque existe $m+n-1 > 0$ tal que $(x+y)^{m+n-1} = 0$ y $m+n-1 > 0$ porque $m > 0$ y $n > 0$)

$\therefore x+y \in N$

b) $x \in N \Rightarrow x^m$ para algún $m > 0$.

(N es el conjunto de elementos nilpotentes).

$(-x)^n = (-1.x)^n = (-1)^n x^n = 0$ entonces $-x \in N$.

(Ya que $x^n = 0$).

Luego N es un subgrupo aditivo de A.

c) Sea $a \in A$ y $x \in N$. Si $x \in N$, $x^n = 0$ para algún $n > 0$. (N es el conjunto de los elementos nilpotentes).

$(ax)^n = a^n x^n = a^n . 0 = 0$ (x es nilpotente).

de donde $ax \in N$ y

$AN \subset N$.

Por tanto N es un ideal en A.

Probaremos ahora que el nilradical $\frac{A}{N}$ sólo tiene un elemento, esto equivale a probar que $\frac{A}{N}$ no tiene ningún elemento nilpotente distinto de cero.

Sea $x + N \in \frac{A}{N}$ un elemento nilpotente, entonces existe $n > 0$ tal que $(x + N)^n = N$, donde N es el cero del anillo cociente. Pero $(x + N)^n = x^n + N$ (Por la definición de producto en el anillo cociente), entonces $x^n + N = N$, luego, por Corolario 2.2.2 , $x^n \in N$; entonces existe $m > 0$ tal que $(x^n)^m = x^{nm} = 0$, de donde $x \in N$, entonces, por corolario nilpotente 2.2.2 $x + N = N$. Por tanto el único elemento del anillo cociente es N (El cero del anillo cociente).

5.1.3 PROPOSICION.

Sea $x \in A$. Entonces x es nilpotente si y sólo si x pertenece a todo ideal primo de A.

DEMOSTRACION:

" => "

Sea x nilpotente y P un ideal primo de A. Entonces existe $n > o$ tal que $x^n = 0$, $x^n \in P$ porque 0 está en todo ideal de A, luego $x \in P$ ya que $x^n = x.x.x...x$ (n veces) y P es primo.

" => "

Probaremos que si x **no es nilpotente** entonces existe un ideal primo en A que no contiene a **x.**

Supongamos que x no es nilpotente, entonces para todo $n > 0$ $x^n \neq 0$.

Sea $\sum$ el conjunto de ideales P tales que $x^n \notin P$ para todo $n > 0$. $\sum \neq \phi$ ya que $\{0\} \in \sum$ (Porque como $x^n \neq 0$, $x^n \notin \{0\}$).

Ordenamos $\sum$ por inclusión llegamos a que $\sum$ tiene elemento maximal. (Por el Lema de Zorn desarrollado en proposición 4.2.5).

Sea P maximal en $\sum$

$z,q \notin P \Rightarrow P \subset P + [z]$ (Porque $x \in P \Rightarrow x=x+0.z$)

$P \neq P + [z]$ (Porque $0+1.z = z \notin P$)

$P \subset P + [q]$ (Porque $x \in P \Rightarrow x = x + 0.q$)

$P \neq P + q$ (Porque $0 + 1.q = q \notin P$)

$\Rightarrow P + [z],\ P + [q]$ (Porque P ex maximal en $\sum$)

$\Rightarrow x^m \in P + [z]$ y $x^n \in P + [q]$ (Porque $x^m,\ x^n \notin \sum$)

para algunos m,n mayores que cero.

$\Rightarrow x^m = p + m.z$ para algún $m \in A$ y $p \in P$ ($P + [z] = \{p+m.z / p \in P \wedge m \in A\}$)

$x^n = p + n.q$ para algún $n \in A$ y $p \in P$. ($P + [q] = \{p+nq / p \in P \wedge n \in A\}$)

$\Rightarrow x^m.x^n = (p + m.z)(p + n.q)$

$= p^2 + mzp + nqp + mnzq$

Como p^2, mzp, nqp $\in$ P (por ser este ideal en A) y mnzq es un múltiplo de zq se tiene que:

$x^m.x^n = x^{m+n} \in P + [zq]$

$\Rightarrow P + [zq] \notin \sum$ (Por definición de $\sum$)

$\Rightarrow P + [zq] \neq P$ (Porque $P \in \sum$)

$\Rightarrow zq \notin P$ (Si $zq \in P \Rightarrow P + [zq] = P$)

$\Rightarrow$ P es primo.

Además $x \notin P$. ($P \in \sum$ y $x = x^n$ con $n = 1$).

5.2 RADICAL DE JACOBSON.

5.2.1 DEFINICION.

El conjunto R formado por la intersección de todos los ideales maximales en A se denomina RADICAL DE JACOBSON.

5.2.2 PROPOSICION.

$x \in R$ si y sólo si $1 - xy$ es una unidad en A para todo $y \in A$.

DEMOSTRACION:

" $\Rightarrow$ "

Supongamos que $1-xy$ no es una unidad en A, entonces $1-xy \in M$, M maximal en A (Por corolario 3.3.7).

Pero $x \in R \subset M$, entonces $x \in M$. $y \in A$ y $x \in M$, entonces $xy \in M$, puesto que M es ideal en A y por la misma razón M es cerrado respecto a la suma, luego $1 - xy + xy = 1 \in M$, entonces $M = [1] = A$, lo que es absurdo porque M es maximal en A. Por tanto $1 - xy$ es una unidad en A.

" => "

Supongamos que $x \notin M$ para algún ideal maximal M en A. Entonces $M \subset M + [x]$ (Porque $m \in M$, $m = m + 0.x$) y $M \neq M + [x]$ (Porque $0 + 1.x = x \notin M$), luego $M + [x] = A$ (Porque M es maximal y $M \subset M + [x]$ y $M \neq M + [x]$)

Entonces $1 \in A$, $\hat{1} = m + xy$, para algún $m \in M$ y algún $y \in A$, de donde $m = 1 - xy \in M$ Consecuentemente $1 - xy$ no es una unidad (Por corolario 3.3.7), lo que es absurdo $1 - xy$ es una unidad. Por tanto $x \in M$, para todo M maximal, entonces $x \in \mathbb{R}$.

5.2.3 PROPOSICION.

a) Si $x \in A$ es nilpotente entonces $1+x$ es una unidad.

Por definición 3.2.1 una unidad en A es un ele

mento $x \in A$, para el cual existe un elemento $y \neq 1$ en A tal que $xy = 1$.

DEMOSTRACION:

Asumamos entonces que para $1 + x$ existe

$$Y = \sum_{i=0}^{n-1} (-1)^i x^i \neq 1 \quad \text{tal que:}$$

$$(1 + x)\, y = 1.$$

Para $n = 2$ $\quad Y = \sum_{i=0}^{1} (-1)^i x^i = 1 - x$

$$(1 + x)(1 - x) = 1 - x^2 = 1 - 0 = 1$$ ($x^2 = 0$ ya que x es nilpotente)

Para $n = 3$ $\quad Y = 1 - x + x^2$.

$$(1 + x)(1 - x + x^2) = 1 + x^3 = 1 + 0 = 1$$

Para $n = 4$ $\quad Y = 1 - x + x^2 - x^3$

$$(1 + x)(1 - x + x^2 - x^3) = 1 - x^4 = 1 - 0 = 1$$

En general para n ,par $y = 1 - x + x^2 - \ldots - x^{n-1}$

$$(1 + x)(1 - x + x^2 - \ldots - x^{n-1}) = 1 - x^n = 1 - 0 = 1$$

Y para n impar $Y = 1 - x + x^2 - \ldots + x^{n-1}$

$$(1 + x)(1 - x + x^2 - \ldots + x^{n-1}) = 1 + x^n = 1 + 0 = 1.$$

Como para $n \geq 2$ $= \sum_{i=0}^{n-1} (-1)^i x^i \neq$, entonces

$1 + x$ es una unidad.

b) Si $x \in A$, x Nilpotente y z es unidad, entonces $x + z$ es unidad.

DEMOSTRACION:

$x + z$ es unidad si $(x + z)\, k = 1$

Para algún $k \neq 1$ en A (Definición 3.2.1)

$x^n = 0$, para algún $n > 0$ (x es nilpotente)

$zy = 1$, para algún $z \neq 1$ (z es unidad)

$(xy)^n = x^n.y^n = 0.y^n = 0$ (Por ser x nilpotente)

=> xy es nilpotente.

=> $1 + xy$ es unidad (Por a de este misma - Proposición).

=> $(1 + xy_1)\, p = 1$ para algún $p \neq 1$. (Definición de unidad).

$\Rightarrow$ (zy + xy) P = 1 (Sustituyendo 1 por zy)

$\Rightarrow$ (3 + x) g P = 1 (Por Ley Distributiva)

$\therefore$ z + x es unidad ya que y $\neq$ 0 y P $\neq$ 0

zp $\neq$ 1 y (z + x) yp = 1.

5.2.4 PROPOSICION.

En el anillo A [x] (Anillo de polinomios en una indeterminada x con coeficientes en A) el nilradical es igual al radical de Jacobson.

Sea N el nilradical en el anillo A [x] y R el radical de Jacobson en el anillo A [x]. Probar que N = R.

c "

f ε N $\Rightarrow$ para todo g ε A[x] $((f.g)^n = f^n g^n$

fg es nilpotente $= 0.g^n = 0)$

$\Rightarrow$ -fg es nilpotente (-fg = f(-g))

$\Rightarrow$ 1 - fg es unidad (Proposición 5.2.3.a

$\Rightarrow$ f ε R (Proposición 5.2.2)

$\therefore$ N C R.

" ⊃ "

Esto es cierto ya que como todo ideal maximal es - primo R C N.

CAPITULO VI

OPERACIONES CON IDEALES

6.1 SUMA DE IDEALES.

6.1.1 DEFINICION.

Sean I,J dos ideales de A. El conjunto $I + J = \{x + y / x \in I, y \in J\}$ se llama "Suma de I y J".

6.1.2 PROPOSICION.

$I + J$ es el ideal generado por $I \cup J$.

DEMOSTRACION:

a) "I + J es un ideal".

$x+ y \in I + J$, $x = m + n$, $y = r + s$, $m,r \in I$, $n,s \in J$; $-y = - (r + s) = - r - s$; $x - y = (m - r) + (n - s)$; como $m - r \in I$ y $n - s \in J$ se tiene que $x - y \in I + J$. Luego, I + J es un subgrupo aditivo de A; además si $z \in A$ entonces $z (m + n) = zm + zn$ es un elemento de I + J ya que $zm \in I$ y $zn \in J$, o sea que $z x \in I + J$. Por tanto I + J es un ideal.

b) "$I \cup J \subset I + J$".

Sea $x \in I \cup J$; si $x \in I$, $x = 1 + 0$ es un elemento de $I + J$; si $x \in J$, $x = 0 + x$ es elemento de $I + J$; luego $I \cup J \subset I + J$.

c) "Sea T un ideal tal que $I \cup J \subset T$ entonces $I + J \subset T$".

Sea $x \in I + J$, $x = m + n$, $m \in I$, $n \in J$; $m + n \in T$ ya que $m \in I \cup J$ y $n \in I \cup J$; es decir $x \in T$, entonces $I + J \subset T$.

6.2 INTERSECCION DE IDEALES.

6.2.1 PROPOSICION.

"Si I y J son dos ideales $I \cap J$ es un ideal".

DEMOSTRACION:

Sea $x,y \in I \cap J$; $x \in I$, $x \in J$, $y \in I$, $y \in J$; $x-y \in I$ y $x-y \in J$ por ser I y J subgrupos; luego $x-y \in I \cap J$; por tanto $I \cap J$ es subgrupo.

Sea $Z \in A$ y $x \in I \cap J$; $x \in I$, $x \in J$; $zx \in I$ y $zx \in J$ por ser I y J ideales; luego $xz \in I \cap J$. Luego $I \cap J$ es un ideal.

6.3 PRODUCTO DE IDEALES.

6.3.1 DEFINICION.

Sean I y J dos ideales y sea

$K = \{xy \;/\; x \in I \;,\; y \in J\}$ este conjunto no es siempre un ideal, por lo que definimos:

$IJ = [K]$, es decir que I J es el ideal generado por los productos xy, con $x \in I$, $y \in J$.

6.3.2 PROPOSICION.

Si I, J y K son ideales en A entonces "$I(J + K) = IJ + IK$". ∎

DEMOSTRACION:

" $\subset$ "

Si $x \in I$, $y \in J$, $z \in K$, $x(y + z)$ es un elemento del generador de $I(J + K)$; pero $x(y + z) = xy + xz \Rightarrow x(y + z) \in IJ + IK$; luego $IJ + IK$ es un ideal que contiene al generador de $I\,(J + K)$ por tanto $I\,(J + K) \subset IJ + IK$.

" $\supset$ "

Sea $x \in IJ$; x es de la forma $x = \sum_{1}^{n} y_i\, z_i$, $y_i \in I$, $z_i \in J$;

$x = \sum_{1}^{n} y_i (z_i + 0)$, x es una suma finita de elementos de I (J + K); luego $x \varepsilon I (J + K)$; de donde IJ c I (J + K). De igual forma I K C I (J + K), de donde IJ $\cup$ IK c I(J + K); luego IJ + IK c I (J + K) (IJ $\cup$ IK es el generador de IJ + IK).

6.4 EJEMPLOS.

6.4.1 PROPOSICION.

Sea A = Z (anillo de los enteros) y sea I,J dos ideales de Z; si I = $[a]$ y J = $[b]$ entonces I+J = $[d]$ en donde d = m.c.d (a,b)

DEMOSTRACION:

$d \varepsilon I + J$, ya que el m.c.d (a,b) es una combinación lineal de a y b, es decir existen m , $n \varepsilon Z$ tales que d = ma + nb. Sea $x \varepsilon I$, $y \varepsilon J$; x = pa, y = qb (por ser I = $[a]$ y J = $[b]$); además como d es un divisor de a y de b existen r, $s \varepsilon Z$ tales que a = rd, b = sd, de donde x+y = pa + qb = prd + qsd = (pr + qs)d; luego si T es un ideal tal que $d \varepsilon T$ entonces $x+y \varepsilon T$, es decir I + J c T.

Por tanto I + J = $[d]$.

6.4.2 PROPOSICION.

Sea $A = Z$ (anillos de los enteros); si $a \in Z$ y $b \in Z$ e $I = [a]$ y $J = [b]$ entonces $I \cap J = [m]$, en donde $m = m.c.m\ (a,b)$.

DEMOSTRACION:

Como m es un múltiplo de a y de b entonces $m = pa$, $m = qb$, $p,q \in Z$; luego $m \in [a]$ y $m \in [b]$ es decir $m \in I$ y $m \in J$; luego $m \in I \cap J$. Sea ahora T un ideal tal que $m \in T$ y sea $x \in I \cap J$; como $x \in I$, $x = ra$; como $x \in J$, $x = rb$; luego x es múltiplo de a y de b; por ser m el m.c.m (a,b), x es múltiplo de m, es decir $x = zm$; así $x \in T$ porque $m \in T$. Luego $I \cap J \subset T$.

6.4.3 PROPOSICION.

En el anillo Z si $I=[a]$ y $J = [b]$ entonces $IJ = [ab]$

DEMOSTRACION:

$ab \in IJ$ ya que $a \in I$ y $b \in J$.

Sea ahora T un ideal tal que $ab \in T$ y probemos que $IJ \subset T$; si $x \in I$ y $y \in J$, $x = ma$, $y = nb$, de donde

$xy = manb = mn.ab$; así $xy \in T$; luego T es el ideal que contiene al generador de IJ; por tanto $IJ \subset T$.

6.4.4 PROPOSICION.

En Z : Si $I = [a]$, $J = [b]$, $a > 0$, $b > 0$ entonces $IJ = I \cap J$ si y sólo si a y b son primos entre sí.

DEMOSTRACION:

" => "

Sea $m = m.c.m(a.b)$; si $IJ = I \cap J$ entonces $[ab] = [m]$; luego $ab \in [m]$ y $m \in [ab]$ es decir $ab = km$ y $m = t.a.b$, de donde $m = tab = t\ km$ implica $tk = 1$; con $t > 0$ y $k > 0$, $t = k = 1$, es decir $ab = m$; así a y b son primos entre sí.

" <= "

Si a y b son primos entre sí, $ab = m = m.c.m.\ (a,b)$; luego $[ab] = [m]$ es decir $IJ = I \cap J$.

6.4.5 PROPOSICION.

Sean I, J dos ideales de un anillo A tales que $I + J = A$. Entonces $I \cap J = IJ$.

DEMOSTRACION:

" c "

Sea $x \in I \cap J$; $x \in I$, $x \in J$; sea $m \in I$, $n \in J$ tales que $1 = m+n$; entonces $x = x.1 = x(m+n) = xm + xn$; $xm \in IJ$ ya que $x \in J$ y $m \in I$; $xn \in IJ$ ya que $x \in I$ y $n \in J$; luego $x \in IJ$; por tanto $I \cap J \subset IJ$.

" $\supset$ "

Si $x \in I$ y $y \in J$, xy es un elemento del generador de IJ; $xy \in I$, $xy \in J$ porque I y J son ideales; luego $x \in I \cap J$; así, $I \cap J$ contiene al generador de IJ, de donde $IJ \subset I \cap J$.

$\therefore$ $I \cap J = IJ$.

6.5 IDEALES PRIMOS ENTRE SI.

6.5.1 DEFINICION.

Dos ideales I,J son primos entre sí, si $I + J = A$. Ya se probó que si I y J son primos entre sí entonces $I \cap J = IJ$. (Proposición 6.4.5). Además es fácil verificar que I y J son primos entre sí si y solo si existen $m \in I$, $n \in J$ tales que $1 = m + n$.

6.5.2 DEFINICION.

Si A y B son dos anillos su producto cartesiano A X B es un anillo conmutativo y unitario con las operaciones

$$(x,y) + (m,n) = (x + m,\ y + n)$$

$$(x,y) \cdot (m,n) = (xy\ ,\ mn)$$

Su elemento identidad es (1,1)

Las funciones $P_1 : A \times B \to A : (x,y) \rightsquigarrow x$

$$P_2 : A \times B \to B : (x,y) \rightsquigarrow y$$

Son dos homomorfismos de anillos llamados "proyecciones".

6.5.3 PROPOSICION.

Sea A un anillo y sea I y J dos ideales de A y sea ϕ el homomorfismo de anillos

$$\phi : A \longrightarrow \frac{A}{I} \times \frac{A}{J} : x \rightsquigarrow (x + I,\ x + J)$$

Entonces

1) ϕ es sobreyectiva si y sólo si I y J son primos entre sí.

2) ϕ es inyectiva si y sólo si $I \cap J = \{0\}$.

DEMOSTRACION:

a) "Si ϕ es sobreyectiva I y J son primos entre sí".

Sea $x \in A$ tal que $\phi(x) = (1 + I, J)$, entonces $x + 1 = 1 + I = I$ y $x + J = J$ es decir que $x - 1 \in I$ y $x \in J$; también $1 - x \in I$ y $-x \in J$, luego, $1 = m+n$, $m \in I$, $n \in J$, $m = 1 - x$, $n = -x$. Por tanto I y J son primos entre sí.

b) "Si I y J son primos entre sí, ϕ es sobreyecti-.va".

Como I y J son primos entre sí, existe $m \in I$, $n \in J$ tales que $1 = m + n$. Sea $(x + I, y + J)$ un elemento de $\frac{A}{I} \times \frac{A}{J}$, y sea $z = xn + ym$

Tendremos

$Z + I = xn + ym + I = xn + I$ (Ya que $ym + I = I$); pero $xn - x = x(n - 1) = - m$ es un elemento de I, de donde $xn + I = x + I$; por tanto $z + I = x + I$.

De igual forma $z + J = y + J$; así ϕ es sobreyectiva.

c) "Si ϕ es inyectiva, $I \cap J = \{0\}$"

Sea $x \in I \cap J$; se tiene que $x + I = I$ y $x + J = J$, es decir que $\phi(x) = (x + I, x + J) = (I,J)$; pero también $\phi(0) = (0 + I, 0 + J) = (I,J)$, es decir que $\phi(x) = \phi(0)$; como ϕ es inyectiva, $x = 0$; luego $I \cap J = \{0\}$.

d) "Si $I \cap J = \{0\}$, ϕ es inyectiva"

Sea $x,y \in A$ tales que $\phi(x) = \phi(y)$, es decir $(x + I, x + J) = (y + I, y + J)$; por igualdad de pares ordenados, $x + I = y + I$ y $x + J = y + J$; de donde $x - y \in I$ y $x - y \in J$; $x - y \in I \cap J$, luego $x - y = 0$, o sea $x = y$, Por tanto ϕ es inyectiva.

6.5.4 PROPOSICION.

Si I y J son dos ideales primos y K es un ideal incluido en $I \cup J$ entonces $K \subset I$ ó $K \subset J$.

DEMOSTRACION:

Supongamos que $K \not\subset I$ y $K \not\subset J$; existen $x \in K$, $y \in K$ tales que $x \notin I$ y $y \notin J$. Si $x \notin I$, $x \notin I \cup J$. Si

$y \notin J$, $y \notin I \cup J$. Supongamos $x \in J$ y $y \in I$; entonces $x + y \notin I$, pues si no x sería un elemento de I; también $x + y \notin J$, porque si no, y sería un elemento de J. Por tanto hemos probado que si $K \not\subset I$ y $K \not\subset J$ entonces $K \not\subset I \cup J$.

6.5.5 PROPOSICION.

Sea K un ideal primo y sean I y J dos ideales tales que $I \cap J \subset K$. Entonces $I \subset K$ ó $J \subset K$.

DEMOSTRACION:

Supongamos que $I \not\subset K$ y $J \not\subset K$; existe entonces $x \in I$, $y \in J$ tales que $x \notin K$, $y \notin K$; $z = xy$ es un elemento de $I \cap J$ y $z \notin K$ (Porque K es primo).

Luego: $(I \not\subset K, J \not\subset K) \Rightarrow I \cap J \not\subset K$.

6.6 IDEAL COCIENTE.

6.6.1 DEFINICION.

Sean I,J dos ideales de un anillo A; el conjunto $(I:J) = \{x \in A / xJ \subset I\}$ es llamado "ideal cociente de I y J".

6.6.2 PROPOSICION.

Sean I, J, K tres ideales. Entonces:

1) $(I:J)$ es un ideal.

2) $I \subset (I:J)$

3) $(I:J)J \subset I$

4) $((I:J):K) = ((I:K):J) = (I:JK)$

5) $(I \cap J:K) = (I:K) \cap (J:K)$

6) $(I:J+K) = (I:J) \cap (I:J)$

DEMOSTRACION:

1) "$(I:J)$ es ideal"

i) Sea $x \in (I:J)$, $y \in (I:J)$, $z \in J$.

Entonces $xz \in I$, $yz \in I$; luego

$$(x - y)z = xz - yz \text{ es un elemento de } I.$$

Por tanto $x - y \in (I:J)$.

ii) Sean $x \in (I:J)$, $y \in A$, $z \in J$. Tendremos:

$(yx)z = y(xz) \in I$ ya que $xz \in I$ e I es ideal

Luego, por i), ii) (I:J) es ideal.

2) "I c (I:J)"

Sean x ε I, y ε J; xy ε I por ser I un ideal; luego x ε (I:J), entonces I c (I:J).

3) "(I:J) J c I".

Sean x ε (I:J), y ε J; xy ε I por definición de (I:J). Luego (I:J) J c I.

4) a) "((I:K):K) c (I:JK))"

Sean x ε (I:J):K), y ε J, z ε K;

xz ε (I:J) y (xz)y ε I (Por definición de ideal cociente);

Luego x(yz) = (xz)y ε I, de donde x ε (I:JK)

b) "(I:JK) c ((I:J):K)"

Sean x ε (I:JK) y ε K, z ε J;

tendremos (xy)z = x(yz) ε I. Luego

xy ε (I:J) y x ε (I:J):K

De a) y b): ((I:J):K) = (I:JK)

c) Como (I:JK) = (I:KJ) (Por ser KJ = JK) se tiene

$((I:J):K) = (I:JK) = (I:KJ) =$

$((I:K):J)$.

5) a) "$(I \cap J:K) \subset (I:K) \cap (J:K)$"

Sean $x \in (I \cap J:K)$, $y \in K$; $xy \in I \cap J$, $xy \in I$, $xy \in J$, de donde $x \in I:K$ y $x \in (J:K)$

b) "$(I:K) \cap (J:K) \subset (I \cap J:K)$"

Si $x \in (I:K) \cap (J:K)$ y $y \in K$ tendremos $xy \in I$ y $xy \in J$, ó sea $xy \in I \cap J$.

6) a) "$(I:J+K) \subset (I:J) \cap (I:K)$"

Sean $x \in (I:J + K)$, $y \in J$, $z \in K$;

$y \in J + K$, $z \in J + K$; luego $xy \in I$ y $xz \in I$, por tanto $x \in (I:J)$ y $x \in (I:K)$.

b) "$(I:J) \cap (I:K) \subset (I:J+K)$"

Sean $x \in (I:J) \cap (I:K)$

$y \in J$, $z \in K$; tendremos

$x (y + z) = xy + xz \in I$, ya que $xy \in I$, $xz \in I$.

6.7 RADICAL DE UN IDEAL.

6.7.1 DEFINICION.

Si I es un ideal de un anillo A, se llama "radical de I" al conjunto $r(I) = \{x \in A / x^n \in I$, para algún $n > 0\}$

6.7.2 PROPOSICION.

Sea I un ideal y $\phi : A \to \frac{A}{I}$ es el homomorfismo de anillos: $x \rightsquigarrow x + I$. Entonces

1) $x \in r(I) \iff x + I$ es nilpotente en $\frac{A}{I}$.

2) $r(I)$ es un ideal.

3) $I \subset r(I)$.

4) $r(r(I)) = f(I)$

5) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$, J un ideal.

6) $r(I) = A \iff I = A$

7) $r(I+J) = r(r(I) + r(J))$.

8) Si I es primo $r(I^n) = I$ para todo $n > 0$.

DEMOSTRACION:

1) a) Si $x \in r(I)$, $x^n \in I$ para un $n > 0$; entonces

ces $(x + I)^n = x^n + I = I$, de donde $x + I$ es nilpotente en $\frac{A}{I}$.

b) Si $(x + I)$ es nilpotente en $\frac{A}{I}$ entonces $(x + I)^n = I$ para cierto n; luego $x^n + I = (\lambda + I)^n = I$ implica que $x^n \in I$; luego, $x \in r(I)$.

Por tanto, $x \in r(I) \iff x + I$ es nilpotente en $\frac{A}{I}$.

2) "r(I) es un ideal".

Según la parte 1, $r(I) = \phi^{-1}(R)$ en donde R es el nilradical de $\frac{A}{I}$; luego r(I) es un ideal, ya que R es un ideal de $\frac{A}{I}$ y ϕ es un homomorfismo de anillos.

3) "I c r(I)"

$x \in I \Rightarrow x^n \in I$ para todo n; luego $x \in r(I)$.

4) "r(r(I)) = r(I)"

a) $x \in r(r(I)) \Rightarrow x^n \in r(I)$ para cierto $n > 0$.
$\Rightarrow (x^n)^m \in I$ para cierto m.
$\Rightarrow x^{nm} \in I \Rightarrow x \in r(I)$

Luego $r(r(I)) \subset r(I)$.

b) En general, $I \subset r(I)$; luego $\underline{r}(I) \subset r(r(I))$.

5) "$r(IJ) = r(I \cap J) = r(I) \cap r(J)$"

a) "$r(IJ) \subset r(I \cap J)$"

Sea $x \in r(IJ)$; existe $n > 0$ tal que $x^n \in IJ$; como $IJ \subset I \cap J$, $x^n \in I \cap J$; luego $x \in r(I \cap J)$.

b) "$r(I \cap J) \subset r(I) \cap r(J)$"

Sea $x \in r(I \cap J)$; existe $n > 0$ tal que $x^n \in I \cap J$; $r^n \in I$ y $x^n \in J$; luego $x \in r(I)$ y $x \in r(J)$.

c) "$r(I) \cap r(J) \subset r(IJ)$"

Sea $x \in r(I) \cap r(J)$; existe $m,n > 0$ tales que $x^m \in I$, $x^n \in J$; de donde $x^{m+n} = x^m x^n$ es un elemento de IJ; así $x \in r(IJ)$.

De a), b), c) tenemos la igualdad

$r(IJ) = r(I \cap J) = r(I) \cap r(J)$

6) "$r(I) = A \iff I = A$"

a) "$r(I) = A \Rightarrow I = A$"

Como $1 \in r(I)$, existe $n > 0$ tal que $1^n \in I$; luego $1 \in I$ ya que $1^n = 1$; por tanto $I = A$.

b) $I = A \Rightarrow r(I) = A$

$x \in A \Rightarrow x \in I \Rightarrow x \in r(I)$. Luego $A = r(I)$

7) "$r(I+J) = r(r(I) + r(J))$"

a) "$r(I+J) \subset r(r(I) + r(J))$"

Sea $x \in r(I+J)$; existe $n > 0$ tal que $x^n \in I + J$; como $I \subset r(I)$ y $J \subset r(J)$ tenemos que $x^n \in r(I) + r(J)$. Luego $x \in r(r(I) + r(J))$.

b) "$r(r(I) + r(J)) \subset r(I + J)$"

Sea $x \in r(r(I) + r(J))$; existe $n > 0$ tal que $x^n \in r(I) + r(J)$; sea $y \in r(I)$, $z \in r(J)$ tales que $x^m = y + z$;

existen $m > 0$, $r > 0$ tales que $y^m \in I$,

$$z^r \in J;\ (y + z)^{m+r} = \sum_{i=0}^{m+r} \binom{m+r}{i} y^i\ z^{m+r-i};$$

en esta sumatoria, los primeros m+1 sumandos son elementos de J y los demás sumandos son elementos de I; luego, se tiene un elemento de I + J. Luego $x^{n(m+r)} = (y + z)^{m+r} \in I + J$; así, $x \in r(I + J)$.

8) "Si I es primo y $n > 0$ entonces $r(I^n) = I$"

Como $I^n \subset I$, $r(I^n) \subset r(I)$. Sean $x \in r(I^n)$; existe $m > 0$ tal que $x^m \in I$; como I es primo $x \in I$. Luego, $r(I^n) \subset I$.

Sea $x \in I$, $x^n \in I^n$; luego $x \in r(I^n)$ Así, $I \subset r(I^n)$

Por tanto: $r(I^n) = I$.

BIBLIOGRAFIA

1. M. F. ATIYAH AND J. J. MACDONALD.
"Introduction to Conmutative Algebra".
Addison - Wesley Publishing Company.

2. FRANK AYRES Jr.
"Algebra Moderna".
Serie de Compendios Schaum. Mc Graw-Hill.

3. GARRETT BIRKHOFF. SAUDER.
"Aglgebra Moderna".
Editorial Vicens-Vives. Barcelona.

4. MISCHA COTLAN y CORA RATTU DE SADOSKY.
"Introducción al Algebra"
Editorial Universitaria de Buenos Aires.

5. A. CLARK.
"Elementos de Algebra Abstracta".
Editorial Alhambra.

6. RICHARD V. ANDREE.
"Selections from Modern Abstract Algebra".
Henry Molt and Company. New York.

7. RICHARD E. JOHNSON.
"University Algebra".
Prentice-Hall, Inc. Englewood Cliffs, New Jersey.

8. J. ELDON WHITESITT.

"Principles of Modern Algebra".

Addison-Wesley Publishing Company, Inc.

nvdr